Rigorous Elementary Mathematics

Volume 3: Number Theory

Samer Seraj

Existsforall Academy

Copyright

ISBN 978-1-7389501-2-6

Acknowledgements

> "At the age of eleven, I began Euclid, with my brother as tutor. This was one of the great events of my life, as dazzling as first love. I had not imagined there was anything so delicious in the world. From that moment until I was thirty-eight, mathematics was my chief interest and my chief source of happiness."
>
> – *Bertrand Russell, Autobiography*

> "Mathematicians, like Proust and everyone else, are at their best when writing about their first love."
>
> – *Gian-Carlo Rota, Discrete Thoughts*

I express my gratitude to:

- The Almighty Creator, for providing me with this blessed and privileged life.
- My parents, for financing my mathematical education, and for supporting me during the time that this book series was written.
- My friends, for their companionship and for listening to me talk about mathematics.
- Euclid, for writing the *Elements*, which showed the world the meaning of eternal rigour.

Special thanks is extended to Warren Bei for reading the manuscript and offering numerous suggestions, many of which were implemented. Xingjian (Jimmy) Wang helped to fix typographical mistakes. Any remaining mathematical errors or mistakes in the typesetting that remain are my responsibility alone.

Contents

Preface

> "In studying a philosopher, the right attitude is neither reverence nor contempt, but first a kind of hypothetical sympathy, until it is possible to know what it feels like to believe in his theories, and only then a revival of the critical attitude, which should resemble, as far as possible, the state of mind of a person abandoning opinions which he has hitherto held. Contempt interferes with the first part of this process, and reverence with the second. Two things are to be remembered: that a man whose opinions and theories are worth studying may be presumed to have had some intelligence, but that no man is likely to have arrived at complete and final truth on any subject whatever."
>
> – *Bertrand Russell, A History of Western Philosophy*

Mathematics is the study of ultimate regularity. Regularity entails order or predictability. Its antithesis is chaos. When there is regularity, there are discernible objects at play. In other words, there is structure. Wherever there is structure, there is symmetry. Symmetry means that, while one aspect of the object changes, another remains unchanged. The present trilogy is an effort to rigorously systematize and provide an exposition of those aspects of elementary mathematics that appeal to the author. In the course of writing, it became evident that there are three recurring themes among the proof techniques used, all of which are forms of symmetry:

1. The discrete Fubini's principle instructs us to write the same thing in two different ways. For example, we have applied this principle in several instances:
   - Switching between iterating over the rows of a matrix and iterating over the columns of a matrix is applied to prove the generalized Chinese remainder theorem (Corollary 6.8).
   - Switching the order of indexing variables in a nested sum (or product) is used in the proof of Legendre's formula (Theorem 8.9).
   - Using associativity of a operation, such as for the multiplication of formal polynomials or generating functions, possibly combined with modular arithmetic, appears in a proof of Lucas's theorem (Theorem 8.17).
   - Double counting, which counts the number of elements of a set in two different ways to produce a combinatorial identity, is used in the presented proof of quadratic reciprocity (Theorem 11.25).
2. Antisymmetry in a partial order is a powerful method of proof that lets us break down the strong notion of equality into the conjunction of two individually weaker statements. The three most common examples in elementary number theory are:

- The most common usage of antisymmetry in number theory is that of divisibility, which says that we have equality of positive integers $n = m$ if and only if both $n \mid m$ and $m \mid n$. It is used in many places, in particular throughout Chapter 1.
- Real number equality can be split into two inequality relations, meaning $x = y$ if and only if both $x \leq y$ and $y \leq x$. This is used in the proofs of the gcd and lcm formulas in Theorem 2.18.
- Set equality can be broken into two subset relations, specifically $A = B$ if and only if both $A \subseteq B$ and $B \subseteq A$. For example, it is used in Theorem 3.20.

3. Modding out by an equivalence relation allows us to focus on the essential properties of objects which are preserved under the relation. In elementary number theory, the most important example of an equivalence relation is modular arithmetic, which is the backbone of this book.

It is our hope that the reader will keep these proof techniques in mind while reading the book, and that the impression of the importance of symmetry will grow as the reader encounters the methods time and again.

The intended audience consists of students of math contests, competitions, and olympiads who want want to take a rigorous second look at the results that they might be accustomed to taking for granted, and teachers, coaches, and trainers who want to reinforce their own understanding of what they teach.

Suggestions, comments, and error submissions would be greatly appreciated. These may include suggestions for strengthening or generalizing theorems, and additional material. Messages may be sent to

academy@existsforall.com

Samer Seraj
Mississauga, Ontario, Canada
March 27, 2023

Chapter 1

Divisibility

> "Mathematics is the queen of the sciences, and number theory is the queen of mathematics."
>
> – *Carl Friedrich Gauss*

Number theory may be described as the study of the integers. Inevitably, this leads to excursions through other kinds of numbers, such as the rationals, reals and, remarkably, even the complex numbers. Hardy once claimed in his famous essay, *A Mathematician's Apology*, that "No one has yet discovered any warlike purpose to be served by the theory of numbers... and it seems unlikely that anyone will do so for many years. [10]" This turned out to be quite incorrect, since at present times, number theory has invaluable applications in computer science and cryptography. So it is worth pursuing both for the sake of curiosity about the integers and technological reasons. As we will see, the study of integers quickly leads to the revelation that these basic objects hold incredible and unexpected patterns.

1.1 Division and Remainders

Theorem 1.1 (Well-ordering principle)**.** Let X be a non-empty subset of the integers $\mathbb{Z}$ such that X has a lower bound, meaning

$$\exists b \in \mathbb{Z}, \forall x \in X, x \geq b.$$

Then X has a minimal or least element, meaning

$$\exists m \in X, \forall x \in X, x \geq m.$$

Thanks to the antisymmetry of real inequalities, if there are two minimal elements m_1, m_2, they must be equal (due to $m_1 \geq m_2$ and $m_2 \geq m_1$), so the minimal element is unique.

We all have performed the long division algorithm to find the remainder and quotient upon division of a dividend by a divisor. The following theorem proves that a quotient and remainder always exist.

Theorem 1.2 (Euclidean division)**.** Suppose a and b are integers such that b is non-zero. Then there exist unique integers q and r such that $a = qb + r$ and $0 \leq r < |b|$. Here, a is called the **dividend**, b the **divisor**, q the **quotient** and r the **remainder**.

Proof. This will be the kind of proof that shows existence followed by uniqueness. The idea is to start with a on the number line, and look at the double-ended arithmetic sequence that contains a and has common difference b. This "tiles" the number line into segments of equal length b. So let

$$S = \{a - qb : q \in \mathbb{Z}\}.$$

Based on experience with long division, we wish to find the smallest non-negative element of this set, for which we will use the well-ordering principle. To use the well-ordering principle, the set of non-negative elements of S needs to be non-empty: If $a \geq 0$, then we can take $q = 0$. If $a < 0$, then we can take $q = ab$, which gives

$$a - qb = a - ab^2 = a(1 - b^2) \geq 0$$

since a is negative, and $b^2 \geq 1$ since b is a non-zero integer. By the well-ordering principle, $S \cap \mathbb{Z}_{\geq 0}$ has a minimal element r, so $r = a - qb \geq 0$ for some integer q. Now we just need it to hold that $r < |b|$. Suppose, for contradiction, that $r \geq |b|$. Then

$$0 \leq r - |b| = a - qb \pm b = a - b(q \pm 1),$$

where the $\pm$ sign is positive if b is positive and negative if b is negative. This would mean that $r - |b|$ is a non-negative element of S while being strictly smaller than r (since $|b|$ is positive), which contradicts the minimality of r. Thus, $r < |b|$. In number theory, it is common to use this technique of finding a minimal element and then showing that this element must have a desirable quality because otherwise it would contradict the property of minimality.
With existence of q and r under our belt, we will now show uniqueness. Suppose there are two pairs of integers (q, r) and (q', r') such that

$$a = qb + r, \text{ and } 0 \leq r < |b|,$$
$$a = q'b + r', \text{ and } 0 \leq r' < |b|.$$

Subtracting the equations yields

$$(q - q')b = r' - r,$$

so $r' - r$ is a multiple of b. But the bounds on r and r' lead to

$$-|b| < r' - r < |b|,$$

so the only way that $r' - r$ could be a multiple of b is if $r = r'$. Then $(q - q')b = r' - r = 0$ yields $q = q'$ as well, since we can divide by $b \neq 0$. ■

Definition 1.3. Let $a \neq 0$ and b be integers. Then a **divides** b if there exists an integer c such that $ac = b$. This is denoted by $a \mid b$ and its negation is denoted by $a \nmid b$. If $a \mid b$ holds, then we say that a is a **factor** or **divisor** of b and that b is a **multiple** of a. By the condition $a \neq 0$ (which exists since there is no meaning for division by $a = 0$), it does not make sense to speak of 0 as being a divisor of 0. However, the equation $0 \cdot 0 = 0$ does hold, so it may be acceptable in some circumstances to temporarily define that $0 \mid 0$ for the sake of convenience. A **proper divisor** of b is any positive divisor a of b such that $a \neq b$.

Corollary 1.4. For each pair of positive integers (t, m), the quantity $\left\lfloor \frac{t}{m} \right\rfloor$ is the number of multiples of m in $[t] = \{1, 2, \ldots, t\}$ and it is the quotient in the Euclidean division of t by m.

Proof. By Euclidean division, there exists a quotient q and remainder r such that

$$t = qm + r, \text{ and } 0 \leq r < m.$$

Then the multiples of m in $[t]$ are $\{m, 2m, \ldots, qm\}$, which has cardinality

$$q = q + 0 = q + \left\lfloor \frac{r}{m} \right\rfloor = \left\lfloor q + \frac{r}{m} \right\rfloor = \left\lfloor \frac{qm + r}{m} \right\rfloor = \left\lfloor \frac{t}{m} \right\rfloor.$$

As a consequence, we can write the Euclidean division equation as $t = \left\lfloor \frac{t}{m} \right\rfloor \cdot m + r$. ■

Lemma 1.5. We can make the following inaugural observations about divisibility. Let $a \neq 0$ and b be integers.

1. 1 and a are divisors of a
2. $a \mid 0$ and, even if we allowed divisibility by 0, $0 \nmid a$
3. $a \mid b$ holds if and only if $\pm a \mid \pm b$ for any choices of the two $\pm$ signs. For this reason, it is usually sufficient to work with only positive a and b. We will rarely speak of negative divisors or negative multiples.
4. If $b \neq 0$ and $a \mid b$, then $|a| \leq |b|$.

Proof. These are all immediate consequences of the definition of divisibility:

1. Since $1 \cdot a = a$, both 1 and a divide a.
2. Using $a \cdot 0 = 0$, we get $a \mid 0$. If it were true that $0 \mid a$ then there would exist an integer c such that $0 \cdot c = a$, causing the contradictory implication that $a = 0$.
3. The equation $ac = b$ is equivalent to each of the following equations:

$$(-a)c = -b, (-a)(-c) = b, a(-c) = -b.$$

4. If $a \mid b$, then there exists an integer c such that $ac = b$. Since b is non-zero, c is also non-zero (it is easier to see the contrapositive that $c = 0$ implies $b = 0$). This leads to

$$|b| = |ac| = |a| \cdot |c| \geq |a| \cdot 1 = |a|,$$

where we have used the fact that $|c| \geq 1$.

■

Lemma 1.6 (Antisymmetry of divisibility)**.** If a and b are integers such that $a \mid b$ and $b \mid a$, then $a = \pm b$ where either sign might hold. An important special case of this result is that, if n is an integer such that $n \mid \pm 1$, then $n = 1$ or $n = -1$. If a and b are positive, then we can conclude that $a = b$, which means that the divisibility of positive integers is imbued with antisymmetry. This is a powerful formal tool that we will use repeatedly.

Proof. If $a \mid b$ and $b \mid a$, then we may assume that a and b are non-zero. Then $|a| \leq |b|$ and $|b| \leq |a|$. By the antisymmetry of real inequalities, $|a| = |b|$, so $a = \pm b$. If a and b are both known to be positive, then $a = b$. If $n \mid \pm 1$ then, since we automatically know that $\pm 1 \mid n$, this result yields $n = 1$ or $n = -1$. ■

Definition 1.7. The integers in the double-ended arithmetic sequence

$$(\ldots, -4, -2, 0, 2, 4, \ldots)$$

are called the **even** numbers. The complement

$$(\ldots, -5, -3, -1, 1, 3, 5, \ldots)$$

is also a double-ended arithmetic sequence and its elements are called the **odd** numbers. Whether an integer is even or odd is called its **parity**; every integer has a well-defined parity.

Number theory frequently involves casework based on parity. Parity is also useful in combinatorics, such as in proofs of the impossibility of certain configurations of dominoes on chessboards. In that regard, parity is an instance of the invariance principle [6].

Problem 1.8. Prove the following properties of parity:

1. Suppose n is an integer. Show that n is even if and only if there exists an integer m such that $n = 2m$, and that n is odd if and only if there exists an integer m such that $n = 2m - 1$. Equivalently, we can choose an m such that $n = 2m + 1$.

2. The sum of any finite number of even integers is even. The sum of any odd number of odd numbers is odd. The sum of any even number of odd numbers is even.

3. The product of an even integer with any other integers is even. The product of finitely many odd numbers is odd.

Theorem 1.9. Some basic properties of divisibility are as follows. Let a, b, c, d be integers and whenever we speak of any of them as divisors, we will assume that they are non-zero.

1. If $a \mid b$ and $b \mid c$, then $a \mid c$. This key property is called transitivity.

2. If $a \mid b$, then $a \mid bc$.

3. If $a \mid b$ and $c \mid d$, then $ac \mid bd$.

4. If $d \mid a$ and $d \mid b$, then for all integers x and y, $d \mid ax + by$.

Proof. These can be deduced in a straightforward manner from the definition of divisibility. For example, multiplying $a\alpha = b$ and $b\beta = c$ together yields $ab \cdot \alpha\beta = bc$. Then $a \cdot \alpha\beta = c$, which proves transitivity. We leave the rest as an exercise to the reader. ■

Definition 1.10. If a and b are real numbers, then numbers of the form $ax + by$ are called **linear combinations** of a and b, though it needs to be made clear before usage of the term whether x, y are integers, rationals, reals or otherwise. The notion of linear combinations can be generalized to n elements, like

$$a_1x_1 + a_2x_2 + \cdots + a_nx_n.$$

This is an extremely important concept in linear algebra. For us, it will reappear in Bézout's lemma (Theorem 1.16).

Definition 1.11. Let k be a positive integer and $T = (a_1, a_2, \ldots, a_k)$ be a k-tuple of integers such that *at least one* of the a_i is non-zero. The **greatest common divisor** of T is denoted by and defined as

$$\begin{aligned}\gcd(T) &= \gcd(a_1, a_2, \ldots, a_k) \\ &= \max\{d \in \mathbb{Z} : d \mid a_1, d \mid a_2, \ldots, d \mid a_k\},\end{aligned}$$

where we need that at least one of the a_i is non-zero, otherwise arbitrarily large d exist and so there is no maximum. Note that 1 is an element of the set above from which the maximum is taken and $a_1a_2 \cdots a_k$ is a (very weak) upper bound on the elements of the set, so a maximum does exist by a variation of the well-ordering principle; each element of that set is called a **common divisor** of T. For convenience of notation, $\gcd(a_1, a_2, \ldots, a_k)$ maybe denoted by $(a_1, a_2, \ldots, a_k)$, despite the potential confusion with Euclidean coordinates or, in the $k = 2$ case, open interval notation.

Definition 1.12. Let k be a positive integer and $T = (a_1, a_2, \ldots, a_k)$ be a k-tuple of integers such that *all* of the a_i are non-zero. The **least common multiple** of T is denoted by and defined as

$$\begin{aligned}\operatorname{lcm}(T) &= \operatorname{lcm}(a_1, a_2, \ldots, a_k) \\ &= \min\{d \in \mathbb{Z}_+ : a_1 \mid d, a_2 \mid d, \ldots, a_k \mid d\},\end{aligned}$$

where none of the a_i can be zero since we do not allow divisors to be zero in the definition of divisibility. The product $a_1a_2 \cdots a_k$ is in the set from which the minimum is taken, so there does exist a minimum by the well-ordering principle; each element of the set is called a **common multiple** of T. For convenience of notation, $\operatorname{lcm}(a_1, a_2, \ldots, a_k)$ maybe denoted by $[a_1, a_2, \ldots, a_k]$, though one has to take precautions to prevent confusing it with closed interval notation in the $k = 2$ case.

Note that $d \in \mathbb{Z}_+$ in the definition of lcm because if we had defined it using $d \in \mathbb{Z}$ (like in the definition of gcd), then there would be negative common multiples arbitrarily close to negative infinity. This would prevent there from being a "lowest" common multiple. So we choose from only among the positive options.

Definition 1.13. Let k be a positive integer and $T = (a_1, a_2, \ldots, a_k)$ be a k-tuple of integers such that $a_i \neq 0$ for some $i \in [k]$. If $k = 2$ and $\gcd(a_1, a_2) = 1$, then a_1 and a_2 are said to be **relatively prime** or **coprime**. Some people denote this relationship by $a \perp b$, but this notation does not extend well to the following generalization. If $\gcd(T) = 1$, then the a_i are said to be relatively prime (altogether), though we often need the stronger relation of T being **pairwise coprime**, which means that $\gcd(a_i, a_j) = 1$ for each pair $(i, j) \in [k] \times [k]$ such that $i \neq j$.

Example. It is possible for a k-tuple of integers to be relatively prime without being pairwise coprime. For example, if $T = (2 \cdot 3, 2 \cdot 5, 3 \cdot 5)$, then each pair is not coprime, but there is no positive integer other than 1 that divides all three elements. However, every pairwise coprime k-tuple is relatively prime.

Problem 1.14. Show that, if a is a non-zero integer, then $\gcd(a, 0) = |a|$. Deduce that $(0, a) = 1$ if and only if $a = \pm 1$.

Problem 1.15. For all integers n, prove that n and $n + 1$ are coprime, and that

$$\gcd(n, n+2) = \begin{cases} 1 & \text{if } n \text{ is odd} \\ 2 & \text{if } n \text{ is even} \end{cases}.$$

1.2 Bézout's Lemma

The following result, called Bézout's lemma, is a beautiful and practically useful way of characterizing the greatest common divisor function. It is usually stated for only the $n = 2$ case, which is the most common one in applications, but we have stated a more general version, with additional consequences.

Theorem 1.16 (Bézout's lemma)**.** Suppose n is a positive integer and $T = (a_1, a_2, \ldots, a_n)$ is an n-tuple of integers, at least one of which is non-zero. Let

$$D = \{a_1x_1 + a_2x_2 + \cdots + a_nx_n : (x_1, x_2, \ldots, x_n) \in \mathbb{Z}^n\},$$
$$d = \gcd(a_1, a_2, \ldots, a_n).$$

Then the following statements hold:

1. $\min(D \cap \mathbb{Z}_+)$ exists and equals d.
2. Every common divisor of T divides d, and every divisor of d is a common divisor of T.
3. Every element of D is a multiple of d, and every multiple of d is an element of D.

Proof. This looks like a job for the well-ordering principle. The set $D \cap \mathbb{Z}_+$ is non-empty because if $a_i \neq 0$ (we have defined that such an index i must exist), then we can choose x_i to equal a_i and $x_j = 0$ for $j \neq i$. This constructs the element

$$a_1x_1 + a_2x_2 + \cdots + a_nx_n = a_i^2 > 0.$$

By the well-ordering principle, $D \cap \mathbb{Z}_+$ has a minimal element. Let

$$m = \min(D \cap \mathbb{Z}_+) = a_1x_1 + a_2x_2 + \cdots + a_nx_n.$$

We will show that m is a common divisor of T and that every common divisor of T divides m, thereby simultaneously proving the first two assertions. For any $i \in [n]$, Euclidean division of a_i by m yields

$$a_i = mq_i + r_i, \text{ and } 0 \leq r_i < m.$$

Then

$$r_i = a_i - mq_i = a_i - q_i \cdot \sum_{k=1}^{n} a_kx_k \in D.$$

If r_i were positive, then it would be a positive element of D that is less than m, which would contradict the minimality of m. So it must be true that $r_i = 0$, which means $a_i = mq_i$ and that $m \mid a_i$. This argument holds for all $i \in [n]$, so m is a common divisor of T. This method of forcing a remainder to be equal to 0 in order to avoid a contradiction is an exceedingly common technique, even in higher mathematics such as abstract algebra.
Now suppose c is a common divisor of T. Let $(u_1, u_2, \ldots, u_n)$ be the n-tuple of integers such that

$$(cu_1, cu_2, \ldots, cu_n) = (a_1, a_2, \ldots, a_n).$$

Then

$$m = \sum_{k=1}^{n} a_kx_k = \sum_{k=1}^{n} cu_kx_k = c\left(\sum_{k=1}^{n} u_kx_k\right),$$

so $c \mid m$. Thus, m is the greatest common divisor d. Conversely, by transitivity of divisibility, any divisor of d is a common divisor of T.
For the third assertion, say

$$d' = \sum_{k=1}^{n} a_kx'_k$$

is some element of D. By Euclidean division of d' by d,

$$d' = dq + r, \text{ and } 0 \leq r < d.$$

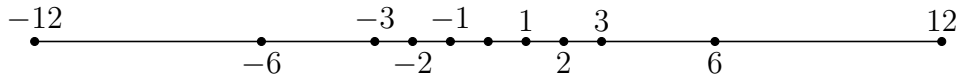
Then

$$\begin{aligned} r &= d' - dq \\ &= \sum_{k=1}^{n} a_kx'_k - q \cdot \sum_{k=1}^{n} a_kx_k \\ &= \sum_{k=1}^{n} a_k(x'_k - qx_k), \end{aligned}$$

which is an element of D. To avoid the contradiction that r is a positive element of D that is smaller than d, it must be true that $r = 0$. Thus, $d' = dq$, meaning $d \mid d'$. Conversely, for any integer t, the multiple of d

$$td = t \cdot \sum_{k=1}^{n} a_kx_k = \sum_{k=1}^{n} a_k(tx_k)$$

is an element of D.
Visually, we can imagine that the number line is divided at all the multiples of d. These are all the elements of D. And the common divisors of T lie in the interval $[-d, d]$ with each one having a mirror image across 0. Below is an example of how to visualize this for $d = 6$.



■

Corollary 1.17. If $A = (a_1, \ldots, a_n)$ and $B = (b_1, \ldots, b_m)$ are tuples of integers such that each tuple contains at least one non-zero entry, then

$$\gcd(A, B) = \gcd(\gcd(A), \gcd(B)),$$

where the left side is the greatest common divisor of the concatenation (this means to be joined together)

$$(a_1, \ldots, a_n, b_1, \ldots, b_m).$$

The proof of this result can easily be extended to several tuples so that

$$(A_1, A_2, \ldots, A_k) = ((A_1), (A_2), \ldots, (A_k)),$$

but we will focus on the $k = 2$ case as it is easier conceptually and in terms of notation. As a consequence, the greatest common divisor of a tuple can be computed recursively like

$$\gcd(a_1, \ldots, a_{n-1}, a_n) = \gcd(\gcd(a_1, \ldots, a_{n-1}), a_n),$$

as long as we have an algorithm for the $n = 2$ case.

Proof. The overarching idea of the proof is to use antisymmetry of the divisibility relation. Firstly, $\gcd(A, B)$ divides every $a \in A$ and every $b \in B$. So $\gcd(A, B)$ is a common divisor of A and is also a common divisor of B, so by Bézout's lemma, $\gcd(A, B) \mid \gcd(A)$ and $\gcd(A, B) \mid \gcd(B)$. So $\gcd(A, B)$ is a common divisor of $\gcd(A)$ and $\gcd(B)$, so by Bézout's lemma,

$$\gcd(A, B) \mid \gcd(\gcd(A), \gcd(B)).$$

In the other direction, we know that $\gcd(\gcd(A), \gcd(B))$ divides $\gcd(A)$ and $\gcd(B)$. Since $\gcd(A)$ divides every $a \in A$ and $\gcd(B)$ divides every $b \in B$, transitivity of divisibility yields that $\gcd(\gcd(A), \gcd(B))$ divides all $a \in A$ and all $b \in B$. This means $\gcd(\gcd(A), \gcd(B))$ is a common divisor of the concatenation (A, B), so by Bézout's lemma, it must divide $\gcd(A, B)$. By antisymmetry of divisibility,

$$\gcd(A, B) = \gcd(\gcd(A), \gcd(B)).$$

■

Corollary 1.18. The following are some basic properties of the greatest common divisor that we can derive from Bézout's lemma. Let a and b be integers such that at least one of the two is non-zero, and c be a non-zero integer. Then:

1. $(a, b) = 1$ if and only if there exist integers x, y such that $ax + by = 1$.
2. $\dfrac{a}{(a,b)}$ and $\dfrac{b}{(a,b)}$ are coprime. This comes up surprisingly often.
3. If a, b are both non-zero, then $a \mid c$ and $b \mid c$ if and only if $\dfrac{ab}{(a,b)} \,\Big|\, c$. We will prove that $\dfrac{ab}{(a,b)} = [a, b]$ in Corollary 1.23, which means every common multiple of a, b is a multiple of $[a, b]$ and every multiple of $[a, b]$ is a common multiple of a, b; this will be generalized to n-tuples in Theorem 1.21. Also, note that in the special case where $(a, b) = 1$, this result states that $a \mid c$ and $b \mid c$ if and only if $ab \mid c$; this special case will be generalized as the faux-Chinese remainder theorem (Theorem 2.10).

Proof. Let a, b, c be as stated.

1. By Bézout's lemma, if $(a, b) = 1$ then there exist integers x, y such that $ax + by = 1$. Conversely, suppose such x, y exist. Since (a, b) divides a and b, it also divides the linear combination $ax + by = 1$. The only positive divisor of 1 is 1, so $(a, b) = 1$.
2. By Bézout's lemma, there exist integers x, y such that $ax + by = (a, b)$. Dividing both sides by (a, b), we get
$$\frac{a}{(a,b)} \cdot x + \frac{b}{(a,b)} \cdot y = 1.$$
Note that $\dfrac{a}{(a,b)}$ and $\dfrac{b}{(a,b)}$ are integers because the greatest common divisor of a tuple of integers must divide each of those integers. By the last part, the greatest common divisor of $\dfrac{a}{(a,b)}$ and $\dfrac{b}{(a,b)}$ is equal to 1.
3. For the harder direction, suppose $a \mid c$ and $b \mid c$. Then there exist integers u, v such that $au = c$ and $bv = c$. Again, let x, y be integers such that $ax + by = (a, b)$. Multiplying both sides by uv yields
$$axuv + byuv = uv(a, b),$$
and by substitution, this is equivalent to $c(xv + yu) = uv(a, b)$. So c divides $uv(a, b)$. Working backwards from the desired conclusion, we can take the following reversible steps:
$$\begin{aligned} \frac{ab}{(a,b)} \,\Big|\, c \\ \frac{ab}{(a,b)} \cdot \alpha &= c \\ \frac{c}{u} \cdot \frac{c}{v} \cdot \alpha &= c(a, b) \\ c \cdot \alpha &= uv(a, b) \\ c \mid uv(a, b), \end{aligned}$$

where α is some integer. In the other direction, suppose $\frac{ab}{(a,b)} \Big| c$. Since $a \Big| a \cdot \frac{b}{(a,b)}$ and $b \Big| b \cdot \frac{a}{(a,b)}$, we get from transitivity of divisibility that $a \mid c$ and $b \mid c$.

■

Corollary 1.19 (Gauss's divisibility lemma)**.** Let $a \neq 0$ be an integer, and b and c be integers. If $a \mid bc$ and $(a, b) = 1$, then $a \mid c$. A generalization is that if $a \mid bc$, then $\frac{a}{(a,b)} \Big| c$. We will see in Lemma 2.9 a frequently-occurring special case of Gauss's lemma called Euclid's lemma that applies to prime divisors.

Proof. Since a and b are coprime, there exist integers x and y such that $ax + by = 1$. Then

$$cax + cby = c.$$

Since $a \mid ca$ and, by hypothesis, $a \mid bc$, linear combinations yields $a \mid c$. We can use this to generalize itself as follows.
Suppose $a \mid bc$. Then there exists an integer α such that $a\alpha = bc$. Then

$$\frac{a}{(a,b)} \cdot \alpha = \frac{b}{(a,b)} \cdot c,$$

so $\frac{a}{(a,b)} \Big| \frac{b}{(a,b)} \cdot c$. Since $\frac{a}{(a,b)}$ and $\frac{b}{(a,b)}$ are coprime, Gauss's lemma yields that $\frac{a}{(a,b)} \Big| c$.

■

Problem 1.20. Let a, b, c be integers such that $a = 0$ only if b, c are both non-zero (this condition allows us to speak of all gcd's in the following sentence). Prove that $(a, bc) = 1$ if and only if $(a, b) = 1$ and $(a, c) = 1$.

Theorem 1.21. Let $A = (a_1, \ldots, a_n)$ be a tuple of non-zero integers. Then $\operatorname{lcm}(a_1, \ldots, a_n)$ divides every common multiple of A. As a consequence, if $B = (b_1, \ldots, b_m)$ is another tuple of non-zero integers, then

$$\operatorname{lcm}(A, B) = \operatorname{lcm}(\operatorname{lcm}(A), \operatorname{lcm}(B)),$$

where the left side is the least common multiple of the concatenation

$$(a_1, \ldots, a_n, b_1, \ldots, b_m).$$

The proof of this result can easily be extended to several tuples so that

$$[A_1, A_2, \ldots, A_k] = [[A_1], [A_2], \ldots, [A_k]].$$

Thus, the least common multiple of a tuple can be computed recursively like

$$\operatorname{lcm}(a_1, \ldots, a_{n-1}, a_n) = \operatorname{lcm}(\operatorname{lcm}(a_1, \ldots, a_{n-1}), a_n),$$

assuming we have an algorithm for the $n = 2$ case. In fact, we just need an algorithm for the gcd of two entries because Corollary 1.23 shows a way to convert their gcd to their lcm.

Proof. For the first part, let $\ell = \text{lcm}(A)$. Suppose m is a common multiple of A. By Euclidean division of m by ℓ, there exists a quotient q and remainder r such that

$$m = \ell q + r, \text{ and } 0 \leq r < \ell.$$

Then $r = m - \ell q$ is also divisible by every $a \in A$, so r is a common multiple of A. In order for r to not contradict the minimality of ℓ, it must be true that $r = 0$. Thus, $m = \ell q$ is a multiple of q.
For the second part, we will use antisymmetry of the divisibility relation, as in the proof of Corollary 1.17. Firstly, $\text{lcm}(A, B)$ is divisible by every $a \in A$ and every $b \in B$. This means that $\text{lcm}(A, B)$ is a common multiple of A and is a common multiple of B, so by the first part, $\text{lcm}(A) \mid \text{lcm}(A, B)$ and $\text{lcm}(B) \mid \text{lcm}(A, B)$. So $\text{lcm}(A, B)$ is a common multiple of $\text{lcm}(A)$ and $\text{lcm}(B)$, and again by the first part,

$$\text{lcm}(\text{lcm}(A), \text{lcm}(B)) \mid \text{lcm}(A, B).$$

In the other direction, we know that $\text{lcm}(\text{lcm}(A), \text{lcm}(B))$ is divisible by $\text{lcm}(A)$ and $\text{lcm}(B)$. Since every $a \in A$ divides $\text{lcm}(A)$ and every $b \in B$ divides $\text{lcm}(B)$, transitivity of divisibility yields that all $a \in A$ and all $b \in B$ divide $\text{lcm}(\text{lcm}(A), \text{lcm}(B))$ This means $\text{lcm}(\text{lcm}(A), \text{lcm}(B))$ is a common multiple of the concatenation (A, B), so by the first part of the theorem, it must be divisible by $\text{lcm}(A, B)$. By antisymmetry of divisibility,

$$\text{lcm}(A, B) = \text{lcm}(\text{lcm}(A), \text{lcm}(B)).$$

■

There are many other properties of the greatest common divisor and least common multiple that are too numerous to list; we will see some of them as they crop up in practice. The course of action that we recommend for the reader is to get a feeling for how factors and multiples work through the properties that we have listed, and then hypothesize and prove any other properties as needed in order to solve specific problems. Once we get to primes and prime factorization in Chapter 2, the greatest common divisor and least common multiple will become easier to conceptualize and their properties will appear more natural.

1.3 Euclidean Algorithm

With general observations about divisibility and the gcd and lcm functions out of the way, we will now work towards finding efficient algorithms for computing them.

Lemma 1.22. Let a and b be integers such that at least one of the two is non-zero, and m be an integer. Then:

1. If m is positive, then $\gcd(ma, mb) = m \cdot \gcd(a, b)$.
2. If m is a positive common divisor of a and b, then $\gcd\left(\frac{a}{m}, \frac{b}{m}\right) = \frac{1}{m} \cdot \gcd(a, b)$.

3. For any integer m, it holds that $\gcd(a, b) = \gcd(a + mb, b)$. The cases where $m = \pm 1$ are often helpful. This is commonly, but incorrectly, called the Euclidean algorithm, so we will call it the faux-Euclidean algorithm; we will see the true Euclidean algorithm in Theorem 1.24.

Proof. Let a, b, m be as stated. Our main tools will be the antisymmetry of divisibility and Bézout's lemma.

1. By Bézout's lemma, there exist integers α and β such that

$$\gcd(ma, mb) = \alpha ma + \beta mb = m(\alpha a + \beta b).$$

Bézout also tells us that $\alpha a + \beta b$ is a multiple of $\gcd(a, b)$, so

$$m \cdot \gcd(a, b) \mid \gcd(ma, mb).$$

In the other direction, Bézout's lemma says that there exist integers γ and δ such that $\gamma a + \delta b = \gcd(a, b)$. Then

$$m \cdot \gcd(a, b) = m(\gamma a + \delta b) = \gamma(ma) + \delta(mb).$$

By Bézout, we know that $\gamma(ma) + \delta(mb)$ is a multiple of $\gcd(ma, mb)$, so

$$\gcd(ma, mb) \mid m \cdot \gcd(a, b).$$

Putting the two together directions together with antisymmetry proves that

$$m \cdot \gcd(a, b) = \gcd(ma, mb).$$

2. Since $\dfrac{a}{m}$ and $\dfrac{b}{m}$ are integers in this part, we can apply the last part to get

$$m \cdot \gcd\left(\frac{a}{m}, \frac{b}{m}\right) = \gcd\left(m \cdot \frac{a}{m}, m \cdot \frac{b}{m}\right) = \gcd(a, b),$$

which is equivalent to the desired identity.

3. As $\gcd(a, b)$ divides a and b, $\gcd(a, b)$ divides their linear combination $a + mb$. Then $\gcd(a, b)$ is a common divisor of $a + mb$ and b. By Bézout's lemma,

$$\gcd(a, b) \mid \gcd(a + mb, b).$$

By applying this result, $\gcd(a + mb, b)$ divides

$$\gcd(a + mb + (-m)b, b) = \gcd(a, b).$$

By antisymmetry, we are done.

■

Corollary 1.23. If a and b are non-zero integers, then $(a,b)[a,b] = |ab|$. This means that we can find an algorithm for computing (a,b), then it will lead to an algorithm for computing $[a,b]$ as well. A special case of this result is that if $(a,b) = 1$, then $|ab| = [a,b]$.

Proof. We may assume without loss of generality that the integers are positive because $(a,b) = (|a|,|b|)$ and $[a,b] = [|a|,|b|]$. By dividing both sides of $(a,b)[a,b] = ab$ by $(a,b)^2$, it is equivalent to prove that

$$\left[\frac{a}{(a,b)}, \frac{b}{(a,b)}\right] = \frac{a}{(a,b)} \cdot \frac{b}{(a,b)}.$$

This might be easier to prove than the original equation because the two constituent numbers $c = \dfrac{a}{(a,b)}$ and $d = \dfrac{b}{(a,b)}$ satisfy the additional hypothesis of being coprime. Since $c \mid [c,d]$, there exists an integer x such that $cx = [c,d]$. But $d \mid [c,d] = cx$ as well and $(c,d) = 1$, so Gauss's divisibility lemma states that $d \mid x$. Then $cd \leq cx = [c,d]$. Since $[c,d]$ is the least common multiple of c and d, and cd is a common multiple of c and d, we also have the reverse inequality $[c,d] \leq cd$. By antisymmetry, $cd = [c,d]$, as desired. ■

Theorem 1.24 (Euclidean algorithm)**.** Suppose a and b are positive integer such that $a \geq b$. Then there exists a non-negative integer N such that, by repeated application of Euclidean division, a sequence of $N+1$ quotient-remainder pairs (q_i, r_i) can be found as follows:

$$\begin{aligned}
a &= q_0 b + r_0, \text{ and } 0 \leq r_0 < b, \\
b &= q_1 r_0 + r_1, \text{ and } 0 \leq r_1 < r_0, \\
r_0 &= q_2 r_1 + r_2, \text{ and } 0 \leq r_2 < r_1, \\
r_1 &= q_3 r_2 + r_3, \text{ and } 0 \leq r_3 < r_2, \\
&\vdots \\
r_{N-3} &= q_{N-1} r_{N-2} + r_{N-1}, \text{ and } 0 \leq r_{N-1} < r_{N-2}, \\
r_{N-2} &= q_N r_{N-1} + r_N, \text{ and } 0 = r_N.
\end{aligned}$$

So N is the step at which the remainder is 0, assuming we label the first line as step 0. If $N = 0$ or $N = 1$, we define $r_{-1} = b$ and $r_{-2} = a$ to make sense of the equation in the final line. Then $\gcd(a,b) = r_{N-1}$.

Proof. To prove the validity of this algorithm, we have to prove that it terminates, meaning a non-negative integer N exists at which point $r_N = 0$, and that $r_{N-1} = (a,b)$. The process certainly terminates because Euclidean division tells us that

$$a \geq b > r_0 > r_1 > r_2 > r_3 > \cdots,$$

so the remainders r_i are strictly decreasing starting with r_0. Since the r_i are non-negative, the party must end at some point and we hit zero. As for proving that $r_{N-1} = (a,b)$, we can use the faux-Euclidean algorithm

$$(p + mq, q) = (p, q)$$

to get

$$\begin{aligned}(a,b) &= (q_0b + r_0, b) = (r_0, b) = (b, r_0)\\ &= (q_1r_0 + r_1, r_0) = (r_1, r_0) = (r_0, r_1)\\ &= (q_2r_1 + r_2, r_1) = (r_2, r_1) = (r_1, r_2)\\ &= (q_3r_2 + r_3, r_2) = (r_3, r_2) = (r_2, r_3)\\ &\vdots\\ &= (q_{N-1}r_{N-2} + r_{N-1}, r_{N-2}) = (r_{N-1}, r_{N-2}) = (r_{N-2}, r_{N-1})\\ &= (q_Nr_{N-1} + r_N, r_{N-1}) = (r_N, r_{N-1}) = (r_{N-1}, 0)\\ &= r_{N-1}.\end{aligned}$$

As an example,

$$\begin{aligned}(48,18) &= (2\cdot 18 + 12, 18) = (12, 18) = (18, 12)\\ &= (1\cdot 12 + 6, 12) = (6, 12) = (12, 6)\\ &= (2\cdot 6, 6) = (0, 6) = (6, 0)\\ &= 6.\end{aligned}$$

■

The Euclidean algorithm is a highly efficient process for computing the gcd function of two integers. Multiplicative problems, such as factoring, are generally more complicated to solve than additive problems, but the Euclidean algorithm amazingly reduces the multiplicative problem of determining the greatest common divisor of two integers to an efficient additive process.

Example 1.25. Show that if a, b, c are non-zero integers such that $(a, c) = 1$, then $(ab, c) = (b, c)$. Use this to prove that if a, m, n are positive integers such that $a \geq 2$ and $m \geq n$, then

$$(a^m - 1, a^n - 1) = a^{(m,n)} - 1.$$

In particular, if $n \mid m$, then

$$a^n - 1 \mid a^m - 1.$$

Solution. We will use antisymmetry of divisibility to show that $(ab, c) = (b, c)$. In one direction, (b, c) is a common divisor of b, c, so (b, c) is a common divisor of ab, c, and finally $(b, c) \mid (ab, c)$. In the other direction, since $d = (ab, c)$ is a common divisor of ab and c, we know that $d \mid ab$ and $d \mid c$. If we could show that $(d, a) = 1$ then it would follow from Gauss's lemma and $d \mid ab$ that $d \mid b$. Then combining $d \mid b$ and $d \mid c$ would give $d \mid (b, c)$, as desired. So it boils down to showing that $(d, a) = 1$. Since (d, a) divides $d = (ab, c)$ and a, and (ab, c) divides ab and c, we get from transitivity of divisibility that (d, a) divides a and c. Thus, (d, a) divides $(a, c) = 1$, so $(d, a) = 1$. Now we head over to the main result.
By Euclidean division, there exists a quotient q_0 and remainder r_0 such that

$$m = q_0n + r_0, \text{ and } 0 \leq r_0 < n.$$

By the faux-Euclidean algorithm and the first part of this example,

$$\begin{aligned}(a^m-1,a^n-1) &= (a^{q_0n+r_0}-1,a^n-1)\\ &= ((a^{q_0n+r_0}-1)-(a^n-1),a^n-1)\\ &= (a^n(a^{n(q_0-1)+r_0}-1),a^n-1)\\ &= (a^{n(q_0-1)+r_0}-1,a^n-1).\end{aligned}$$

Repeating this step as many times as needed, we get

$$(a^m-1,a^n-1)=(a^{r_0}-1,a^n-1)=(a^n-1,a^{r_0}-1),$$

where $r_0<n$. Continuing this process, we see that the exponents of a at the end of each stage matches the sequence of remainders in the Euclidean algorithm, which can be formally proven by induction. As such, we eventually reach $r_{N-1}=(m,n)$ and $r_N=0$ to get

$$\begin{aligned}(a^m-1,a^n-1) &= (a^{r_N}-1,a^{r_{N-1}}-1),\\ &= (a^0-1,a^{(m,n)}-1)\\ &= a^{(m,n)}-1.\end{aligned}$$

If $n\mid m$, then

$$(a^m-1,a^n-1)=a^{(m,n)}-1=a^n-1,$$

so $a^n-1\mid a^m-1$. ■

Problem 1.26. Prove that, for all odd positive integers m and n,

$$(2^m+1,2^n+1)=3,$$

showing that numbers of the form $2^\ell+1$ for odd positive integers ℓ are almost pairwise coprime.

Recall that Bézout's lemma (Theorem 1.16) asserts the existence of integers x and y such that $ax+by=\gcd(a,b)$, but it does not tell us how to find such integers. The Euclidean algorithm provides a way of finding x and y. Ordinarily, a method involving substitutions into the Euclidean division equations in the Euclidean algorithm is used, but this process is prone to human error. We will instead show an alternative method using matrices because the computation is more direct thanks to an explicit formula. Moreover, the formula has a nice degree of symmetry among its components.

Definition 1.27. Informally, if m and n are positive integers, then an $m\times n$ **matrix** is an array or table of numbers with m rows and n columns. More formally, it is an indexing function whose indexing set is $[m]\times[n]$. The **matrix multiplication** of 2×2 matrices is defined by

$$\begin{pmatrix}a & b\\ c & d\end{pmatrix}\cdot\begin{pmatrix}p & q\\ r & s\end{pmatrix}=\begin{pmatrix}ap+br & aq+bs\\ cp+dr & cq+ds\end{pmatrix}$$

and similarly a 2×2 matrix times a column vector is computed as

$$\begin{pmatrix}a & b\\ c & d\end{pmatrix}\cdot\begin{pmatrix}p\\ q\end{pmatrix}=\begin{pmatrix}ap+bq\\ cp+dq\end{pmatrix}.$$

The multiplication of larger matrices follows a similar definition. Matrix multiplication is associative, but not commutative. The multiplication of a matrix by a scalar (for us, a scalar is a real number but a more general definition involving field elements exists in abstract algebra), called **scalar multiplication**, is defined as

$$\alpha \cdot \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} \alpha a & \alpha b \\ \alpha c & \alpha d \end{pmatrix}.$$

We call

$$I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

the 2×2 **identity matrix** because $IM = MI$ for every 2×2 matrix M, as the reader should verify. The identity matrix is like the number 1 in the multiplication of real numbers since multiplying any matrix by I gives back that matrix.

Definition 1.28. The **determinant** of a 2×2 matrix is

$$\det \begin{pmatrix} a & b \\ c & d \end{pmatrix} = ad - bc.$$

Problem 1.29. For 2×2 matrices M and N, prove that

$$\det(M \cdot N) = \det(M) \cdot \det(N).$$

This is called the multiplicative property of the determinant.

Theorem 1.30 (Extended Euclidean algorithm)**.** Suppose a and b are positive integers such that $a \geq b$. Let the sequence of ordered pairs of quotients and remainders from applying the Euclidean algorithm (Theorem 1.24) to a and b be $\{(q_i, r_i)\}_{i=0}^{N}$ where $N+1$ is the number of Euclidean divisions in this instance of applying the Euclidean algorithm (so $r_N = 0$). Let

$$\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} = \begin{pmatrix} q_0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} q_1 & 1 \\ 1 & 0 \end{pmatrix} \cdots \begin{pmatrix} q_N & 1 \\ 1 & 0 \end{pmatrix}.$$

Letting

$$x = (-1)^{N+1}\delta,$$
$$y = (-1)^{N}\beta,$$

the Bézout equation $ax + by = (a, b)$ is satisfied.

Proof. First we will show that $\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \begin{pmatrix} r_{N-1} \\ 0 \end{pmatrix} = \begin{pmatrix} a \\ b \end{pmatrix}$. By working upwards from the final Euclidean division equation in the Euclidean algorithm, we can use induction to get

$$\begin{pmatrix} q_N & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} r_{N-1} \\ 0 \end{pmatrix} = \begin{pmatrix} q_N r_{N-1} \\ r_{N-1} \end{pmatrix} = \begin{pmatrix} r_{N-2} \\ r_{N-1} \end{pmatrix}$$
$$\begin{pmatrix} q_{N-1} & 1 \\ 1 & 0 \end{pmatrix} \left[\begin{pmatrix} q_N & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} r_{N-1} \\ 0 \end{pmatrix} \right] = \begin{pmatrix} q_{N-1} & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} r_{N-2} \\ r_{N-1} \end{pmatrix} = \begin{pmatrix} r_{N-3} \\ r_{N-2} \end{pmatrix}$$
$$\vdots$$
$$\begin{pmatrix} q_0 & 1 \\ 1 & 0 \end{pmatrix} \left[\begin{pmatrix} q_1 & 1 \\ 1 & 0 \end{pmatrix} \cdots \begin{pmatrix} q_N & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} r_{N-1} \\ 0 \end{pmatrix} \right] = \begin{pmatrix} q_0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} b \\ r_0 \end{pmatrix} = \begin{pmatrix} q_0 b + r_0 \\ b \end{pmatrix} = \begin{pmatrix} a \\ b \end{pmatrix}.$$

Secondly, note that the multiplicative property of the determinant implies that

$$\begin{aligned}\alpha\delta - \beta\gamma &= \det \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \\ &= \det \left[\begin{pmatrix} q_0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} q_1 & 1 \\ 1 & 0 \end{pmatrix} \cdots \begin{pmatrix} q_N & 1 \\ 1 & 0 \end{pmatrix} \right] \\ &= \det \begin{pmatrix} q_0 & 1 \\ 1 & 0 \end{pmatrix} \det \begin{pmatrix} q_1 & 1 \\ 1 & 0 \end{pmatrix} \cdots \det \begin{pmatrix} q_N & 1 \\ 1 & 0 \end{pmatrix} = (-1)^{N+1}\end{aligned}$$

As a result, if we let $R = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$ and $S = (-1)^{N+1} \begin{pmatrix} \delta & -\beta \\ -\gamma & \alpha \end{pmatrix}$, where S, R are called inverses of each other (matrix inverses were discussed alongside linear independence and dependence in Volume 1), it holds that

$$\begin{aligned}SR &= (-1)^{N+1} \begin{pmatrix} \delta & -\beta \\ -\gamma & \alpha \end{pmatrix} \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \\ &= (-1)^{N+1} \begin{pmatrix} \delta\alpha - \beta\gamma & \delta\beta - \beta\delta \\ -\gamma\alpha + \alpha\gamma & -\gamma\beta + \alpha\delta \end{pmatrix} \\ &= (-1)^{N+1} \begin{pmatrix} (-1)^{N+1} & 0 \\ 0 & (-1)^{N+1} \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}.\end{aligned}$$

Thus, by multiplying the left side of each side of the equation

$$\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \begin{pmatrix} r_{N-1} \\ 0 \end{pmatrix} = \begin{pmatrix} a \\ b \end{pmatrix}$$

by $S = (-1)^{N+1} \begin{pmatrix} \delta & -\beta \\ -\gamma & \alpha \end{pmatrix}$, we get

$$\begin{pmatrix} r_{N-1} \\ 0 \end{pmatrix} = (-1)^{N+1} \begin{pmatrix} \delta & -\beta \\ -\gamma & \alpha \end{pmatrix} \begin{pmatrix} a \\ b \end{pmatrix},$$

and equating the top coordinates yields

$$\gcd(a, b) = r_{N-1} = a[(-1)^{N+1}\delta] + b[(-1)^N\beta],$$

so the pair $(x, y) = ((-1)^{N+1}\delta, (-1)^N\beta)$ is one solution to the equation in Bézout's lemma. ■

By Bézout's lemma, the extended Euclidean algorithm is useful for computing multiplicative inverses in modular arithmetic. This will make sense after we study modular arithmetic in Chapter 4.

Chapter 2

Primes

> "Mathematicians have tried in vain to this day to discover some order in the sequence of prime numbers, and we have reason to believe that it is a mystery into which the human mind will never penetrate."
>
> – *Leonhard Euler*

Just as the number 1 is the additive building block of the positive integers, the primes are their multiplicative building blocks. In many ways, number-theoretic questions can be reduced to questions about prime numbers. As such, the primes will be one of our starting points for investigating number theory. We will begin by looking into how to identify primes, see some useful lemmas about primes, and end by looking at a powerful representation of integers called the prime factorization.

2.1 Primes and Composites

The additive structure of $\mathbb{Z}_+$ is easy to understand: we begin with 1 and repeatedly add copies of 1 to itself to produce the rest of $\mathbb{Z}_+$. The multiplicative structure is more mysterious. Breaking down a positive integer a into $a = bc$, where b and c are positive integers, is called "factoring" a. A positive integer that cannot be factored non-trivially into two positive integers, where trivial means one of the factors is 1, is a multiplicative building block. Such an integer is known as a *prime*. Just as 1 is additively atomic, primes are multiplicatively indivisible. A formal definition is as follows.

Definition 2.1. A **prime** number is a positive integer $p \neq 1$ whose only positive factors are 1 and p. We will explain why 1 is excluded from the primes when we get to the uniqueness of prime factorizations. A **prime power** is an integer equal to p^k for some prime p and positive integer k; to be clear, primes are prime powers but $p^0 = 1$ is not a prime power for our purposes. A **composite** number n is a positive integer that has a positive factor other than 1 or n.

The exact distribution of the primes among the positive integers is unknown. The best existing results are asymptotic approximations of the distribution, such as the famous prime number theorem. There is also Bertrand's postulate, which states the existence of a prime strictly between n and $2n-2$ for any integer $n \geq 4$. The additive structure of primes is even more difficult to approach (though it is reasonable to question why we would want to add multiplicative generators in the first place!). Some significant ideas are:

- Dirichlet's theorem on primes in arithmetic progressions: For every ordered pair of coprime positive integers (a, d), there exist infinitely many primes in the arithmetic sequence
$$(a + (n - 1)d)_{n=1}^{\infty}.$$
- Green-Tao theorem: For any positive integer N, there exists an arithmetic sequence of N elements that are all primes.
- Twin prime conjecture: There exist infinitely many ordered pairs of primes (p, q) such that $q - p = 2$. While this is a very old and well-known problem that remains unsolved, progress was made by Yitang Zhang in 2013 whose life story is as dramatic as his theorem.

These are deep questions. Our aims will be more modest.

Lemma 2.2. The number 1 has no divisor other than itself, so it is neither prime nor composite. An integer is a prime if and only if it has exactly two distinct positive factors. Subsequently, all integers greater than 1 are either prime or composite, but never both.

Proof. If 1 were composite, it would have to have a positive factor k other than 1, which would make k strictly less than 1, which is impossible. So 1 cannot be composite. And, by the definition of a prime, 1 is not prime. Thus, 1 is neither prime nor composite.
Let p be a prime. By definition, the only positive factors of a prime p are 1 and p. Since 1 is not a prime, $p \geq 2$, so $p \neq 1$. Thus, p has exactly two positive factors, which are 1 and p. Conversely, if an integer p has exactly two positive factors, then it fits the definition of a prime. This biconditional result is a decent reason to exclude 1 from the primes because 1 has only one positive factor, as we established, but the real reason for excluding 1 will be introduced in Theorem 2.12.
Now suppose $n \geq 2$ is an integer. It is clear from the definitions of primes and composites that n cannot be both. All we need to do is show that n is prime or composite. Logically, if P and Q are propositions, $P \vee Q$ is equivalent to $(\neg P) \implies Q$. So we aim to prove that if n is not prime, then it is composite. If n is not prime, then n has a positive factor other than 1 and n. This is the definition of a composite number. ■

Lemma 2.3. The only even prime is 2.

Proof. Let n be a positive integer. We will show that $2n$ is a prime if and only if $n = 1$. If $n = 1$, then $2n = 2$. If 2 had a positive divisor other than 2 or 1, then it would lie strictly between 1 and 2, which is an interval that contains no integers. So 2 is not composite, making it prime. Conversely, if $n \geq 2$, then n is a factor of $2n$ other than $2n$ or 1, so $2n$ cannot be prime. ■

Lemma 2.4. If n is an integer greater than 1, then n has a prime factor.

Proof. The proof is by strong induction on $n \geq 2$. In the base case $n = 2$, we know that 2 is a prime factor of 2 from Lemma 2.3. Now suppose there exists an integer $n \geq 2$ such that for all integers m such that $2 \leq m \leq n$, m has a prime factor. We will show that this implies that $n + 1$ has a prime factor. If $n + 1$ is prime, then we are done because it

is a prime factor of itself. If $n+1$ is composite, then it has a positive factor k such that $2 \leq k \leq (n+1)-1 = n$. By the strong induction hypothesis, k has a prime factor p. Then $p \mid k$ and $k \mid n+1$, so the transitivity of divisibility yields $p \mid n+1$. ■

Theorem 2.5 (Infinitude of primes)**.** There are infinitely many prime integers.

Proof. Suppose, for contradiction, that there are finitely many primes $p_1, p_2, \ldots, p_k$. Let

$$n = p_1 p_2 \cdots p_k + 1.$$

None of the p_i divide n, because otherwise it would be true that $p \mid 1$. But n is greater than or equal to 2, so n must have a prime factor by Lemma 2.4. Thus, this list of primes is incomplete, which is a contradiction.
As a historical note, this argument is an adaptation of the proof that Euclid supplied in his *Elements* over two thousand years ago. We will see generalizations of this proof for special classes of primes in Section 12.2. ■

Given a positive integer, we might want to know whether it is prime or composite. The following is a standard primality test of which one should be aware.

Theorem 2.6. Suppose $n \geq 4$ is an integer. Then n is a prime if and only if, for all primes p such that $p \leq \sqrt{n}$, p does not divide n.

Proof. Let $n \geq 4$ be an integer. We will prove the contrapositive in each direction: n is composite if and only if there exists a prime $p \leq \sqrt{n}$ such that $p \mid n$.
For one direction, suppose n is composite. Then $\sqrt{n} \geq 2$. If n is a square, then $\sqrt{n}$ is an integer that is a proper divisor of n that is greater than or equal to $\sqrt{4} = 2$. Then $\sqrt{n}$ has a prime factor p, and since $\sqrt{n}$ divides n, transitivity of divisibility asserts that $p \leq \sqrt{n}$ is a prime that divides n. For the other case, suppose $\sqrt{n}$ is not an integer. Since n is composite and non-square, there exist unequal positive divisors a, b of n such that $ab = n$ and neither is 1 or n. We may assume that $a < b$ since n is not a square in this case. We will show that $a < \sqrt{n} < b$. Indeed,

$$\begin{aligned} a, b < \sqrt{n} &\implies ab < (\sqrt{n})^2 = n, \\ \sqrt{n} < a, b &\implies n = (\sqrt{n})^2 < ab, \end{aligned}$$

both of which are contradictions. And if either of a, b is $\sqrt{n}$ then so is the other, which is a case that we have already worked out. So

$$1 < a < \sqrt{n} < b < n.$$

Since $a > 1$, a has a prime factor p, and applying transitivity to $p \mid a$ and $a \mid n$ yields $p \mid n$. This p suffices since $p \leq a < \sqrt{n}$.
For the other direction, suppose there exists a prime $p \leq \sqrt{n}$ such that $p \mid n$. Then p satisfies

$$1 < p \leq \sqrt{n} < n.$$

So p is a positive factor of n other than 1 or n, which means n must be composite. ■

There are numerous other primality tests that exist, some of which always work and some of which are correct only most of the time. A relatively recent breakthrough is the AKS primality test, which distinguishes between primes and composites quite quickly in general. As an interesting side note, the AKS test is a "galactic algorithm," meaning it is faster than other algorithms for sufficiently large inputs, but the point at which that happens is beyond the size of inputs that come up in practice.

Theorem 2.7 (Sieve of Eratosthenes)**.** There is an ancient algorithm for finding all primes up to and including a positive integer n. For example, for $n = 100$, it produces the following table:

	2	3	~~4~~	5	~~6~~	7	~~8~~	~~9~~	~~10~~
11	~~12~~	13	~~14~~	~~15~~	~~16~~	17	~~18~~	19	~~20~~
~~21~~	~~22~~	23	~~24~~	~~25~~	~~26~~	~~27~~	~~28~~	29	~~30~~
31	~~32~~	~~33~~	~~34~~	~~35~~	~~36~~	37	~~38~~	~~39~~	~~40~~
41	~~42~~	43	~~44~~	~~45~~	~~46~~	47	~~48~~	~~49~~	~~50~~
~~51~~	~~52~~	53	~~54~~	~~55~~	~~56~~	~~57~~	~~58~~	59	~~60~~
61	~~62~~	~~63~~	~~64~~	~~65~~	~~66~~	67	~~68~~	~~69~~	~~70~~
71	~~72~~	73	~~74~~	~~75~~	~~76~~	~~77~~	~~78~~	79	~~80~~
~~81~~	~~82~~	83	~~84~~	~~85~~	~~86~~	~~87~~	~~88~~	89	~~90~~
~~91~~	~~92~~	~~93~~	~~94~~	~~95~~	~~96~~	97	~~98~~	~~99~~	~~100~~

The process is as follows: we box the prime 2 and cross out all of its multiples in the table by counting upwards by 2's. The next uncrossed number is a prime p, so we box it and cross out all of its multiples by counting by p's. The process is continued until we reach the final uncrossed number, which is again a prime. If a number is already crossed out, there is no need to cross it out more than once. In fact, we only have to cross out multiples of numbers up to and including the number that is the floor function of half of the highest number in the table, which in this case is 50, and every uncrossed number after that step is prime.

Proof. To prove that the algorithm or "sieve" works, we need to show that we can hit a number such that all lower numbers have either been boxed or crossed out if and only if that number is a prime. This is true because a number can have avoided being crossed out if and only if it is not divisible by any of the primes below it, and that condition is true if and only if the number is itself a prime.

If the highest integer in the table is n, and m is an integer such that $m > \left\lfloor \frac{n}{2} \right\rfloor$, then for every integer $k \geq 2$, it holds that

$$km \geq 2 \cdot \left(\left\lfloor \frac{n}{2} \right\rfloor + 1 \right) > 2 \cdot \frac{n}{2} = n,$$

so every positive multiple of m (other than m itself) falls outside of the table. Thus, if every number up to and including $\left\lfloor \frac{n}{2} \right\rfloor$ has been processed (by either being crossed out, or boxed and its multiples being crossed out), then any remaining uncrossed numbers in the table are primes. ■

Lemma 2.8. Let m be a positive integer, n be a non-zero integer, and $(q_1, q_2, \ldots, q_m)$ be an m-tuple of integers. Then

$$\gcd(n, q_1, q_2, \ldots, q_m) = 1$$

if and only if, for each prime factor p of n, there exists a q_i such that $p \nmid q_i$. The contrapositive can be useful too:

$$\gcd(n, q_1, q_2, \ldots, q_m) > 1$$

if and only if there exists a prime factor p of n such that every q_i is divisible by p.

Proof. We will prove the contrapositive. If $(n, q_1, q_2, \ldots, q_m)$ is not a coprime tuple altogether, then there exists a common factor $d \geq 2$ of all $m + 1$ entries. This common factor must have a prime factor p that divides all of the entries by transitivity of divisibility. Thus, there is a prime factor of n that divides all of the q_i. Conversely, if there is a prime factor p of n that divides all of the q_i, then

$$\gcd(n, q_1, q_2, \ldots, q_m) \geq p > 1,$$

and that is what we wanted to see. ■

2.2 Prime Factorization

Lemma 2.9 (Euclid's lemma)**.** Suppose a and b are integers and p is a prime. If $p \mid ab$, then $p \mid a$ or $p \mid b$. Consequently, it can be proven by induction that if n is a finite product of some integers, and p divides n, then p divides at least one of those integers.

Proof. We will show that this is a special case of Gauss's divisibility lemma (Corollary 1.19). Let p, a, b be as stated in the hypothesis. The assertion that $p \mid a$ or $p \mid b$ is logically equivalent to saying that: if $p \nmid a$, then $p \mid b$. So suppose $p \nmid a$. Then $\gcd(p, a) = 1$ because the only factor of p other than p is 1. By Gauss's lemma, $p \mid b$. For the more general result, we have just proven the base case in an induction argument. Suppose the result is true for some integer $k \geq 2$, meaning if a prime p divides $a_1 a_2 \cdots a_k$ for some integer $k \geq 2$ and integers a_i, then p divides some a_i. Tacking on an extra a_{k+1}, if

$$p \mid a_1 a_2 \cdots a_k a_{k+1},$$

then $p \mid a_1 a_2 \cdots a_k$ or $p \mid a_{k+1}$ by the base case. In the latter case we are automatically done, and in the former case we can invoke the induction hypothesis. ■

Theorem 2.10 (Faux-Chinese remainder theorem)**.** If an integer d can be factored into a product of pairwise coprime integers

$$d = d_1 d_2 \cdots d_k$$

for some integer $k \geq 2$, and an integer n is divisible by each of the factors d_i, then n is divisible by d. The converse of course holds by transitivity of divisibility, that is $d \mid n$ implies that each d_i divides n, even without the coprimality condition. People often refer to this as the Chinese remainder theorem (Theorem 6.6), but it is just a tiny special case of CRT, so we will call it the faux-Chinese remainder theorem.

Proof. We will prove the general result by induction on $k \geq 2$. The base case $k = 2$ was proven in Corollary 1.18. Suppose the result holds for some integer $k \geq 2$ and let

$$d = d_1 d_2 \cdots d_k d_{k+1}$$

such that the d_i are pairwise coprime and each d_i divides n. Let $m = d_1 d_2 \cdots d_k$, so that $d = m d_{k+1}$. By the induction hypothesis, $m \mid n$. And d_{k+1} divides n as well. It must be true that $\gcd(m, d_{k+1}) = 1$, otherwise some prime would divide both d_{k+1} and some other d_i by Euclid's lemma, contradicting that they are coprime. Thus, the base case implies that $d = m d_{k+1} \mid n$. ■

Problem 2.11. Find a counterexample to Theorem 2.10 when the coprimality condition is dropped.

Theorem 2.12 (Fundamental theorem of arithmetic)**.** If $n > 1$ is an integer, then there exists a unique positive integer k and a unique k-tuple of distinct primes $p_1 < p_2 < \cdots < p_k$ and a unique k-tuple of positive integers $(e_1, e_2, \ldots, e_k)$ such that

$$n = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}.$$

This form is called the **prime factorization** of n. For negative integers less than -1, we can simply use the prime factorization of its absolute value and tack on a negative sign.

Proof. We will prove existence of the prime factorization by strong induction, and then uniqueness by contradiction. For the base case, $n = 2$ is a prime, so 2^1 is a prime factorization. Now suppose there exists an integer $n \geq 2$ such that, for all integers m such that $2 \leq m \leq n$, m has a prime factorization. For the inductive step, we want to show that $n+1$ has a prime factorization. If $n+1$ is prime, then we are done as in the base case. If $n+1$ is composite, then there exist integers a and b such that

$$1 < a \leq b < n + 1$$

and $ab = n + 1$. By the strong induction hypothesis, a and b have prime factorizations, and thus so does their product $ab = n + 1$. This proves the existence of prime factorizations.
For uniqueness, suppose, for contradiction, that the set of integers greater than 1 with more than one prime factorization is non-empty. By the well-ordering principle, this set has a minimal element n. Let two of its distinct prime factorizations be

$$n = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k} = q_1^{f_1} q_2^{f_2} \cdots q_j^{f_j}.$$

By Euclid's lemma, p_1 divides some q_i. Since p_1 and q_i are both primes, $p_1 = q_i$. Dividing both sides of the above equation by $p_1 = q_i$ yields the integer

$$m = p_1^{e_1 - 1} p_2^{e_2} \cdots p_k^{e_k} = q_1^{f_1} q_2^{f_2} \cdots q_i^{f_i - 1} \cdots q_j^{f_j}.$$

This new number m cannot equal to 1 because then we would have $n = p_1 = q_i$, which would contradict that these two prime factorizations are distinct. So $m \geq 2$. If these two prime factorizations of m are distinct, then it would contradict the minimality of n among the integers with multiple distinct prime factorizations. So they must be the same prime factorization. But that also leads to a contradiction because multiplying both sides of the equation by $p_1 = q_i$ implies that the two prime factorizations of n are also not distinct. Either way, we have a contradiction. ■

Problem 2.13. One way of motivating the exclusion of 1 from the primes is that the uniqueness of the prime factorization breaks down if 1 is included among the primes. Why?

There exist algorithms for determining the prime factorization of an integer, but there is no known algorithm that is very fast. For our purposes, it will suffice to manually check for divisibility by primes, do long division to find the quotient and then repeat the process with the quotient. To make this process easier, we will find divisibility tricks in Section 7.2 to test divisibility by small primes, given the base-10 representation of the original integer.

Definition 2.14. Let p be a prime. In the unique prime factorization of an integer $n \geq 2$, the exponent of p is called the **multiplicity** of p in n. In more advanced mathematics, like abstract algebra, it is called the **p-adic valuation** of n. It is denoted by $\nu_p(n)$. In the case that $p \nmid n$, we define $\nu_p(n) = 0$. The prime factorization of n may be thought of as a multiset whose domain is the set of distinct prime factors of n and the image of each prime is its multiplicity.

Lemma 2.15. For primes p, integers a, b and positive integers n, the following logarithm-like properties of the ν_p function hold:

$$\begin{aligned} \nu_p(a^n) &= n \cdot \nu_p(a) \\ \nu_p(ab) &= \nu_p(a) + \nu_p(b) \\ \nu_p\left(\frac{a}{b}\right) &= \nu_p(a) - \nu_p(b) \text{ if } b \mid a \end{aligned}$$

Moreover,

$$\nu_p(a+b) \geq \min(\nu_p(a), \nu_p(b)).$$

Proof. These all follow from the prime factorizations of a and b. For example, the first one is proven by

$$a^n = (p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k})^n = p_1^{ne_1} p_2^{ne_2} \cdots p_k^{ne_k}.$$

The only slightly non-trivial property is the final one, and it follows from factoring out $p^{\min(\nu_p(a),\nu_p(b))}$ from $a+b$, which is possible since this factor divides both a and b. ■

Problem 2.16. Prove the following statement or find a counterexample: If m and n are positive integers such that $m \leq n$, then for every prime p, $\nu_p(d) \leq \nu_p(n)$.

Lemma 2.17. Let n and d be positive integers. Then $d \mid n$ if and only if, for every prime p, $\nu_p(d) \leq \nu_p(n)$.

Proof. If, for every prime p, $\nu_p(d) \leq \nu_p(n)$, then upon division of the prime factorization of n by the prime factorization of d, it is clear that we have an integer, which means $d \mid n$. In the other direction, suppose $d \mid n$. Since $p^{\nu_p(d)} \mid d$, transitivity of divisibility yields $p^{\nu_p(d)} \mid n$, so the prime factorization of n has at least $\nu_p(d)$ copies of p in it. Thus, $\nu_p(d) \leq \nu_p(n)$. ■

Theorem 2.18. Let a and b be positive integers. Let the collected set of prime factors of a and b be $\{p_1, p_2, \ldots, p_k\}$. Let the (modified) prime factorizations of these two numbers be

$$a = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$$
$$b = p_1^{f_1} p_2^{f_2} \cdots p_k^{f_k},$$

where we have modified the prime factorizations to include all prime factors of both numbers for the sake of uniformity, so some of the e_i and f_i might be 0 (but never $e_i = 0$ and $f_i = 0$ at the same time). Then

$$\gcd(a, b) = p_1^{\min(e_1, f_1)} p_2^{\min(e_2, f_2)} \cdots p_k^{\min(e_k, f_k)}$$
$$\operatorname{lcm}(a, b) = p_1^{\max(e_1, f_1)} p_2^{\max(e_2, f_2)} \cdots p_k^{\max(e_k, f_k)},$$

As a consequence, we get a second proof of the fact that, if a and b are any non-zero integers, then

$$\gcd(a, b) \cdot \operatorname{lcm}(a, b) = |ab|.$$

Proof. By transitivity of divisibility, since $\gcd(a, b)$ is a common divisor of a and b, $\gcd(a, b)$ cannot have any prime factors other than the p_i. So

$$\gcd(a, b) = p_1^{g_1} p_2^{g_2} \cdots p_k^{g_k}$$

where the g_i are some non-negative integers. Since

$$d = p_1^{\min(e_1, f_1)} p_2^{\min(e_2, f_2)} \cdots p_k^{\min(e_k, f_k)}$$

is a common divisor of a and b, d divides $\gcd(a, b)$. By Lemma 2.17, $\min(e_i, f_i) \leq g_i$ for each $i \in [k]$. By the same lemma,

$$\gcd(a, b) \mid a \implies g_i \leq e_i,$$
$$\gcd(a, b) \mid b \implies g_i \leq f_i,$$

so $g_i \leq \min(e_i, f_i)$. By antisymmetry, $g_i = \min(e_i, f_i)$ for every i, and so $\gcd(a, b) = d$. For the $\operatorname{lcm}(a, b)$ formula, let

$$c = p_1^{\max(e_1, f_1)} p_2^{\max(e_2, f_2)} \cdots p_k^{\max(e_k, f_k)},$$

which is a common multiple of a and b. By Lemma 2.17, $a \mid c$ and $b \mid c$, so c is a positive common multiple of a and b. Then $\operatorname{lcm}(a, b) \mid c$, and so there exist non-negative integers h_i such that

$$\operatorname{lcm}(a, b) = p_1^{h_1} p_2^{h_2} \cdots p^{h_k}.$$

By the lemma again, $h_i \leq \max(e_i, f_i)$ for each i. Again by the lemma,

$$a \mid \operatorname{lcm}(a, b) \implies e_i \leq h_i,$$
$$b \mid \operatorname{lcm}(a, b) \implies f_i \leq h_i,$$

so $\max(e_i, f_i) \leq h_i$. By antisymmetry, $\max(e_i, f_i) = h_i$ for every i, and so $\operatorname{lcm}(a, b) = c$.

Using the fact that

$$\min(e_i, f_i) + \max(e_i, f_i) = e_i + f_i,$$

the prime factorization formulas for $\gcd(a, b)$ and $\operatorname{lcm}(a, b)$ lead to

$$\gcd(a, b) \cdot \operatorname{lcm}(a, b) = ab.$$

If a and b are not necessarily positive, then we can use this formula to enhance itself and get

$$\gcd(a, b) \cdot \operatorname{lcm}(a, b) = \gcd(|a|, |b|) \cdot \operatorname{lcm}(|a|, |b|) = |ab|.$$

Note that we have to take care of the cases where $|a| = 1$ or $|b| = 1$ separately since they are not covered by the prime factorization formulas, but these cases are very easy to handle. (Actually, the prime factorization formulas do cover the cases where $a = 1$ or $b = 1$ if we define empty products to be equal to 1 but a separate mental verification would be needed for them to feel safe anyway.) ■

We leave it to the reader to generalize the argument in Theorem 2.18 to find formulas based on prime factorization for the gcd and lcm of more than two integers. The formulas are in terms of minimal and maximal prime powers, exactly as one would expect, except with more involved notation. It is easy to see from this general prime factorization formula for the gcd function that the gcd function is commutative and associative. As a consequence, we always get the gcd if we apply any valid assignment of pairs of parentheses to a tuple and interpret each pair of corresponding parentheses as an application of the gcd function, and the entries can be ordered arbitrarily. This can be attributed to the corresponding commutative and associative properties of the min function, and the same idea applies to the lcm function thanks to the corresponding properties of the max function. For example,

$$(w, x, y, z) = ((w, x), (y, z)) = ((x, y), z, w),$$
$$[w, x, y, z] = [[w, x, y], z] = [x, [z, y], w].$$

Theorem 2.19. The two-variable gcd function is multiplicative with one fixed entry, meaning that if a, b, c are non-zero integers such that $(a, b) = 1$, then

$$(ab, c) = (a, c)(b, c).$$

However, it is not true that if $(a, b) = 1$, then $[ab, c] = [a, c][b, c]$.

Proof. Suppose $(a, b) = 1$. Using the identity $m(x, y) = (mx, my)$, which holds for all positive integers m,

$$\begin{aligned}(a, c)(b, c) &= (a(b, c), c(b, c)) = ((ab, ac), (cb, c^2)) \\ &= (ab, ac, cb, c^2) = (ab, (ac, cb, c^2)) \\ &= (ab, c(a, b, c)).\end{aligned}$$

By assumption, $(a, b) = 1$, so $(a, b, c) = 1$ as well. Thus,

$$(a, c)(b, c) = (ab, c(a, b, c)) = (ab, c).$$

For the disproof of the analogue for the least common multiple, we can use the last part and the identity that relates gcd and lcm to separately compute the two expressions

$$[ab, c] = \frac{abc}{(ab, c)} = \frac{abc}{(a, c)(b, c)}$$
$$[a, c][b, c] = \frac{ac}{(a, c)} \cdot \frac{bc}{(b, c)},$$

and these two expressions are equal if and only if $c = 1$, which is certainly not always the case. ■

Problem 2.20. Prove that, if a, b, c are non-zero integers such that c is non-zero or both a, b are non-zero (this ensures that all gcd's used next exist), and if $(a, c) = 1$, then $(ab, c) = (b, c)$.

Problem 2.21. Let a, b, c be integers. Show that the following "distributive laws" hold:

1. If b and c are non-zero, then $(a, [b, c]) = [(a, b), (a, c)]$.
2. If a, b, c are all non-zero, then $[a, (b, c)] = ([a, b], [a, c])$.

Definition 2.22. If a is an integer and n is a positive integer, then a^n is called a **perfect n^{th} power**. Some special cases are the **perfect square** a^2 and the **perfect cube** a^3. For short, we just say "n^{th} power" or "square" or "cube."

Example. For every positive integer n, $0^n = 0$, so 0 is every kind of perfect power. The same argument applies to 1 in the place of 0.

The following result captures the most common problem-solving techniques involving the divisibility of perfect powers.

Lemma 2.23 (Power divisibility lemmas)**.** Let a, b, c and m, n be positive integers. Then:

1. a is an n^{th} power if and only if for all primes p, $n \mid \nu_p(a)$.
2. If a prime p divides a^n, then $p^n \mid a^n$.
3. $(a, b) = 1$ if and only if $(a^n, b^m) = 1$.
4. If $a^n = b^m$ and $(m, n) = 1$, then a is an m^{th} power and b is an n^{th} power.
5. If $c^n = ab$ and $(a, b) = 1$, then a and b are also n^{th} powers.
6. $a^n \mid b^n$ if and only if $a \mid b$

Proof. Let a, b, c and m, n be as stated.

1. If $a = b^n$ for some integer b, let the prime factorization of b be

$$b = p_1^{e_i} p_2^{e_2} \cdots p_k^{e_k}.$$

Then

$$a = b^n = p_1^{ne_i} p_2^{ne_2} \cdots p_k^{ne_k}.$$

So n divides the multiplicity of each prime factor of a.

Conversely, suppose that for all primes p, it holds that $n \mid \nu_p(a)$. Let the set of prime factors of a be $\{p_1, p_2, \ldots, p_k\}$ and let the multiplicity of p_i be ne_i for each i to account for the multiplicity being divisible by n. Then

$$a = p_1^{ne_i} p_2^{ne_2} \cdots p_k^{ne_k} = (p_1^{e_i} p_2^{e_2} \cdots p_k^{e_k})^n,$$

so a is an n^{th} power.

2. Suppose p is a prime such that $p \mid a^n$. By the generalized Euclid's lemma, $p \mid a$ so $\nu_p(a) \geq 1$. Then
$$\nu_p(a^n) = n \cdot \nu_p(a) \geq n \cdot 1 = n.$$

3. In one direction, we assume that $(a, b) = 1$. Suppose, for the sake of contradiction, that $(a^n, b^m) > 1$. Then a prime p divides (a^n, b^m). Since (a^n, b^m) divides a^n and b^m, transitivity of divisibility yields $p \mid a^n$ and $p \mid b^m$. By Euclid's lemma, $p \mid a$ and $p \mid b$. By Bézout's lemma, since p is a common divisor of a and b, $p \mid (a, b)$. This contradicts the fact that $(a, b) = 1$ has no prime factors. Thus, our initial assumption was wrong and instead $(a^n, b^m) = 1$.

   In the other direction, we assume that $(a^n, b^m) = 1$. Suppose, for the sake of contradiction, that $(a, b) > 1$. Then there exists a prime p such that $p \mid a$ and $p \mid b$. Then $p \mid a^n$ and $p \mid b^m$ as well, which contradicts the assumption that $(a^n, b^m) = 1$.

4. Suppose $a^n = b^m$ and $(m, n) = 1$. For any prime p, it holds that
$$n \cdot \nu_p(a) = \nu_p(a^n) = \nu_p(b^m) = m \cdot \nu_p(b).$$
   By Gauss's divisibility lemma, since $\gcd(m, n) = 1$, we find that $n \mid \nu_p(b)$ and $m \mid \nu_p(a)$. Since this is true for every prime, the first result tells us that a is an m^{th} power and b is an n^{th} power.

5. Suppose $c^n = ab$ and $(a, b) = 1$. A prime p divides c^n if and only if p divides ab. By Euclid's lemma, p divides ab if and only if $p \mid a$ or $p \mid b$. Since $(a, b) = 1$, p cannot divide both a and b. Thus, the prime factors of c are partitioned into those that divide a and those that divide b, and none of them divide both. Moreover, for each prime p,
$$n \cdot \nu_p(c) = \nu_p(c^n) = \nu_p(ab) = \nu_p(a) + \nu_p(b).$$
   Since $\nu_p(a)$ and $\nu_p(b)$ cannot both be positive (meaning one of them is 0), one of them is positive and divisible by n. Since this is true for every prime that divides c^n, we get that a and b are both n^{th} powers by the first result.

6. If $a \mid b$, then there exists an integer c such that $ac = b$. Taking this to the n^{th} power yields $a^n c^n = b^n$, so $a^n \mid b^n$. Conversely, suppose $a^n \mid b^n$. By the first result, the prime factorizations of a^n and b^n take the form (modified to include the primes factors of both numbers and therefore possibly with some multiplicities equal to 0)
$$a^n = p_1^{ne_1} p_2^{ne_2} \cdots p_k^{ne_k},$$
$$b^n = p_1^{nf_1} p_2^{nf_2} \cdots p_k^{nf_k}.$$

Since $a^n \mid b^n$, it holds, for each index i, that $ne_i \geq nf_i$ by Lemma 2.17. Then

$$\frac{a^n}{b^n} = p_1^{n(e_1-f_1)} p_2^{n(e_2-f_2)} \cdots p_k^{n(e_k-f_k)}$$

is an integer that is an n^{th} power. So there exists a positive integer

$$c = p_1^{e_1-f_1} p_2^{e_2-f_2} \cdots p_k^{e_k-f_k}$$

such that $a^n c^n = b^n$. Taking n^{th} roots yields $ac = b$, so $a \mid b$.

We encourage the reader to look into cases when these lemmas may be extended from positive a, b, c to non-negatives or possibly all integers, or some mix. ■

Lemma 2.24. For every non-zero rational number r, there exist unique non-zero integers a and b such that $r = \frac{a}{b}$ and b is positive and $\gcd(a, b) = 1$. Consequently, if $r = \frac{c}{d}$ for some integers c and d, then there exists an integer k such that $a = kc$ and $b = kd$. The fraction $\frac{a}{b}$ is called the **lowest form** or **least representation** of r.

Proof. We will show existence followed by uniqueness. By the definition of a non-zero rational number, there exist non-zero integers s, t such that $r = \frac{s}{t}$. Since $\frac{s}{t} = \frac{-s}{-t}$, we may assume without loss of generality that $t > 0$, which will be used in the uniqueness portion of the proof. Then $\frac{s}{t} = \frac{\left(\frac{s}{(s,t)}\right)}{\left(\frac{t}{(s,t)}\right)}$. Since $\left(\frac{s}{(s,t)}, \frac{t}{(s,t)}\right) = 1$, this proves existence of a, b.
Now suppose there exist two pairs of non-zero integers (a, b) and (α, β) such that b, β are positive and $\gcd(a, b) = \gcd(\alpha, \beta) = 1$ and

$$\frac{a}{b} = \frac{\alpha}{\beta}.$$

Then $a\beta = b\alpha$. Since $\gcd(a, b) = 1$ we get $b \mid \beta$, and since $\gcd(\alpha, \beta) = 1$ we get $\beta \mid b$ by Gauss's divisibility lemma (Corollary 1.19). As b and β are both positive, $b = \beta$ by antisymmetry, and so $a = \alpha$ too. Thus, we have uniqueness.
If

$$r = \frac{a}{b} = \frac{c}{d}$$

for some integers c and d, then $ad = bc$. Since $(a, b) = 1$, we get $a \mid c$, so we let k be the integer such that $ak = c$. Then $ad = bak$ and that leads to $d = bk$ as well, since $a \neq 0$. Thus, the lowest form "generates" all other representations of the same rational number. ■

Theorem 2.25. Let $n \geq 2$ and $t \geq 2$ be integers. Show that, if $\sqrt[t]{n}$ is not an integer, then it is not rational. So roots of positive integers are divided into integers and irrationals, and they never fall among the non-integer rationals.

Proof. Suppose $\sqrt[t]{n}$ is a positive rational number r whose lowest form is $\frac{a}{b}$ for some positive integers a, b. Taking t^{th} powers, we get

$$n = \frac{a^t}{b^t} \implies nb^t = a^t.$$

If p is a prime that divides n (such a prime exists since $n \geq 2$), then $p \mid a^t$ as well, and so $p^t \mid a^t$. Then $p^t \mid nb^t$, but since b and a are coprime, $p^t \mid n$. So we can factor out p^t from n. We can continue in this way by factoring out t^{th} powers of primes from n. Let us skip to the end of the process and factor out the maximal t^{th} power integer m^t that divides n, and let s be the integer such that $n = m^t s$. So

$$m^t b^t s = a^t$$

and every prime that divides s has multiplicity strictly less than t. This equation implies that $m^t \mid a^t$ and so $m \mid a$. Then

$$b^t s = \left(\frac{a}{m}\right)^t,$$

where $\dfrac{a}{m}$ is an integer that is coprime to b. If $a \neq m$, then $\dfrac{a}{m}$ has a prime factor p. Then p^t divides both sides of the equation, and since $\dfrac{a}{m}$ and b are coprime, p^t divides s by Gauss's divisibility lemma, which contradicts the fact that no prime factor of s can have multiplicity t or greater. So in fact $a = m$, which implies that $b^t s = 1$, and so $b = s = 1$. Thus, $\sqrt[t]{n}$ is an integer. ■

It is interesting to note that irrationals are not mere abstract constructions. For example, the irrational number $\sqrt{2}$ is the length of the hypotenuse of the right isosceles triangle whose legs each have length 1. Legend says that the discovery of some variation of this result was so shocking to the Pythagoreans, who were unaware of the existence of irrational numbers, that, being at sea at the time, they drowned the discoverer, Hippasus.

Chapter 3

Arithmetic Functions

> "If I were to awaken after having slept for a thousand years, my first question would be: Has the Riemann hypothesis been proven?"
>
> – *David Hilbert*

Arithmetic functions take positive integers and state some property of the input in terms of complex numbers (usually integers). These functions often satisfy convenient arithmetic properties that might allow us to compute the functions easily, especially if we know the prime factorization of the input. We will look at some of the most important arithmetic functions here, including divisor functions and Euler's totient function.

3.1 Divisor Functions

Definition 3.1. An **arithmetic function** is a function whose domain is $\mathbb{Z}_+$ and whose range is a subset of the complex numbers $\mathbb{C}$. For those who are not familiar with the complex numbers, it is fine to assume that $\mathbb{R}$ is the codomain. There are several important special classes of arithmetic functions:

- Completely multiplicative: for all integers a and b, $f(ab) = f(a)f(b)$
- Multiplicative: for all coprime integers a and b, $f(ab) = f(a)f(b)$
- Completely additive: for all integers a and b, $f(ab) = f(a) + f(b)$
- Additive: for all coprime integers a and b, $f(ab) = f(a) + f(b)$

Note that functions that satisfy any one of these properties can be evaluated by breaking down the input into factors; in the multiplicative and additive cases, those factors need to be coprime. In particular, the prime factorization is a prime candidate (pun intended) for a factorization into coprime factors.

Example. An example of an arithmetic function is, for any fixed prime p, the p-adic valuation $\nu_p(n)$, which is completely additive.

Definition 3.2. For each positive integer n, let $\omega(n)$ denote the number of distinct prime factors of n, and let $\Omega(n)$ denote the number of prime factors of n if each prime factor is counted as many times as its multiplicity in n; these are called the **prime omega functions**. If the prime factorization of n is

$$n = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k},$$

then

$$\omega(n) = k,$$
$$\Omega(n) = e_1 + e_2 + \cdots + e_k.$$

So ω is additive and Ω is completely additive.

These prime omega functions will appear on occasion in the analysis of other arithmetic functions, such as in Lemma 3.13 and Lemma 3.16.

Definition 3.3. If n is a non-zero integer, then the notation $\sum_{d|n}$ denotes a sum that iterates over all positive divisors d of n. For each real number x, the $x^{\textbf{th}}$ **divisor function** $\sigma_x : \mathbb{Z}_+ \to \mathbb{R}$ is defined by

$$\sigma_x(n) = \sum_{d|n} d^x.$$

For $x = 0$, this gives the number of positive divisors of n, and we call this the **tau function** τ. For $x = 1$, this gives the sum of the positive divisors of n, and we call this the **sigma function** σ.

Theorem 3.4 (Divisor function formula)**.** For each real number x and positive integer n, if the prime factorization of n is $n = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$, then

$$\begin{aligned}\sigma_x(n) &= \prod_{i=1}^{k} (1 + p_i^x + p_i^{2x} + \cdots + p_i^{e_i x}) \\ &= \begin{cases} (e_1+1)(e_2+1)\cdots(e_k+1) = \tau(n) & \text{if } x = 0 \\ \displaystyle\prod_{i=1}^{k} \frac{p_i^{(e_i+1)x} - 1}{p_i^x - 1} & \text{if } x \neq 0 \end{cases}.\end{aligned}$$

As a consequence, σ_x is multiplicative for each real x.

Proof. By the definition of σ_x, we would like to show that the terms in the expansion of

$$\prod_{i=1}^{k} (1 + p_i^x + p_i^{2x} + \cdots + p_i^{e_i x})$$

form exactly the set

$$D = \{d^x : d \in \mathbb{Z}_+, d \mid n\}$$

with no repetitions. By the distributive law, the expansion consists of all expressions that are each the product of exactly one term from each multiplicand $1 + p_i^x + p_i^{2x} + \cdots + p_i^{e_i x}$. These form the set

$$T = \{p_1^{t_1 x} p_2^{t_2 x} \cdots p_k^{t_k x} : (t_1, t_2, \ldots, t_k) \in [e_1]^* \times [e_2]^* \times \cdots \times [e_k]^*\},$$

where $[m]^* = \{0, 1, 2, \ldots, m\}$ denotes a section of the non-negative integers. Recall from Lemma 2.17 that $d \mid n$ if and only if, for each prime p, $\nu_p(d) \leq \nu_p(n)$. So by the prime factorization of n, the positive divisors of n are exactly the set of integers

$$d = p_1^{f_1} p_2^{f_2} \cdots p_k^{f_k}$$

such that $0 \leq f_i \leq e_i$ for each $i \in [k]$. By taking the x^{th} power of each divisor, $D = T$ and we are done.

The observation about the $x = 0$ case is immediate from the formula, and the (somewhat) closed form for the $x \neq 0$ cases follows from the formula for a geometric series. The proof of σ_x being multiplicative is a matter of noticing that the same prime cannot divide two coprime integers and then applying the derived formula for σ_x. ■

Example 3.5. For each positive integer n, denote by $\pi(n)$ the product of the positive divisors of n. Show that

$$\pi(n) = \prod_{d \mid n} d = n^{\frac{\tau(n)}{2}}.$$

This formula always yields an integer despite the fact that it involves a fractional exponent which is not always an integer.

Solution. The idea is that, for each positive divisor d of n, there exists a positive integer c such that $dc = n$. Moreover the same c cannot correspond to different d's, meaning the map that goes from d to c is injective. Also, if d maps to c, then c maps to d. So it looks like the positive divisors of n come in unordered pairs that each multiply to n. So if the $\tau(n)$ positive divisors of n split into $\dfrac{\tau(n)}{2}$ unordered pairs and the product of each pair is n, then the desired formula holds.

However, there is a snag, which is that such a split is possible if and only if n is not a square. If n not a square, then every such pair has two distinct elements and we are good to go. If n is a square, then there will be a pair whose elements are both $\sqrt{n}$, and so our idea requires a modification. If n is a square, then removing $\sqrt{n}$ from the set of positive divisors yields $\tau(n) - 1$ positive divisors. These split into $\dfrac{\tau(n) - 1}{2}$ unordered pairs of positive divisors such that the product of each pair is n. Thus, the product of all of the divisors is still

$$n^{\frac{\tau(n)-1}{2}} \cdot \sqrt{n} = n^{\frac{\tau(n)-1}{2}} \cdot n^{\frac{1}{2}} = n^{\frac{\tau(n)}{2}}.$$

Note that this always yields an integer because if n is not a square then $\tau(n)$ will have a factor of 2 due to n having a prime factor with odd multiplicity, and if n is a square then $\tau(n)$ is odd but the denominator of 2 can be applied as a square root to n.

Interestingly, the same formula holds in both cases, and indeed there is a clean, unified proof, reminiscent of Gauss's trick for an arithmetic series:

$$(\pi(n))^2 = \left(\prod_{d \mid n} d \right)^2 = \left(\prod_{d \mid n} d \right) \left(\prod_{d \mid n} \frac{n}{d} \right) = \prod_{d \mid n} \left(d \cdot \frac{n}{d} \right) = \prod_{d \mid n} n = n^{\tau(n)}.$$

Taking the square root of both sides completes the slick proof. ■

Problem 3.6. For each positive integer n, show that the number of divisors of n^2 that are less than n is $\dfrac{\tau(n^2)-1}{2}$.

Problem 3.7. For each positive integer n, prove that the ratio of the number of even positive divisors of n to the number of odd positive divisors of n is $\nu_2(n)$.

Lemma 3.8. If n is a positive integer with prime factorization

$$n = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k},$$

then, for each positive integer m, the number of positive divisors of n that are m^{th} powers is

$$\prod_{i=1}^{k} \left(\left\lfloor \frac{e_i}{m} \right\rfloor + 1 \right).$$

Proof. By Corollary 1.4, for each positive integer t, the number of multiples of m in $[t]$ is $\left\lfloor \dfrac{t}{m} \right\rfloor$. By Lemma 2.23, n is an m^{th} power if and only if, for all primes p, $\nu_p(n)$ is a multiple of m. The result then follows from the prime factorization of n and the multiplication principle from combinatorics. Note that the $+1$ in each multiplicand comes from the fact that the multiplicity that is equal to 0 has to be included. ■

Definition 3.9. An integer n is said to be **squarefree** if the only square that divides it is 1. Equivalently, the multiplicity of each prime that divides n is 1.

As a quick exercise, the reader should prove that, for any positive squarefree integer n, the number of positive divisors of n is $2^{\omega(n)}$, and that $\omega(n) = \Omega(n)$. On a separate note, it is good to keep in mind that, in number theory, it is sometimes productive to do casework on whether an integer is squarefree or has a non-trivial square divisor.

3.2 Dirichlet Convolution

Definition 3.10. Euler's totient function is the arithmetic function that, for each positive integer input n, returns the number of integers in $[n]$ that are coprime to n. It is denoted by the symbol φ.

Though it may not seem so at first sight, Euler's totient function is of great importance in mathematics and especially number theory. This section on the Dirichlet convolution is motivated by the desire to find a formula for Euler's totient function.

Definition 3.11. If f and g are arithmetic functions, then the **Dirichlet convolution** of the ordered pair (f, g) is an arithmetic function $f * g : \mathbb{Z}_+ \to \mathbb{R}$, defined by

$$(f*g)(n) = \sum_{d|n} f(d) g\left(\frac{n}{d}\right) = \sum_{\substack{ab=n \\ (a,b)\in[n]\times[n]}} f(a)g(b).$$

While this definition may seem like it is out of the blue, it follows naturally from the multiplication of Dirichlet generating functions of arithmetic functions, but that would be too advanced for us. We have dealt with ordinary generating functions in Volume 2. The Dirichlet convolution is rich in structure, as we will see.

Lemma 3.12. The Dirichlet convolution is commutative and associative.

Proof. Commutativity follows from the simple manipulation

$$(f*g)(n) = \sum_{\substack{ab=n\\(a,b)\in[n]\times[n]}} f(a)g(b) = \sum_{\substack{ba=n\\(b,a)\in[n]\times[n]}} g(b)f(a) = (g*f)(n).$$

For associativity, we will expand each side of

$$(f*(g*h))(n) = ((f*g)*h)(n)$$

and show that they are equal. The left side is

$$\begin{aligned}(f*(g*h))(n) &= \sum_{\substack{ab=n\\(a,b)\in[n]\times[n]}} f(a)((g*h)(b))\\ &= \sum_{\substack{ab=n\\(a,b)\in[n]\times[n]}} f(a) \sum_{\substack{cd=b\\(c,d)\in[n]\times[n]}} g(c)h(d)\\ &= \sum_{\substack{ab=n\\(a,b)\in[n]\times[n]}} \sum_{\substack{cd=b\\(c,d)\in[n]\times[n]}} f(a)g(c)h(d).\end{aligned}$$

We claim that this equals

$$\sum_{\substack{acd=n\\(a,c,d)\in[n]^3}} f(a)g(c)h(d).$$

This should be true because the first way of writing the sum splits n into an ordered pair of factors (a,b) and then splits the second factor into an ordered pair of factors (c,d), whereas the second way of writing the sum immediately splits n into an ordered triple of factors (a,c,d). We could do this more formally by showing that the two sets of triples (a,c,d) correspond to each other using set inclusion in either direction, but the result is clear enough that we do not need that level of formality. In the same way, the right side of the associativity identity is equal to

$$\begin{aligned}((f*g)*h)(n) &= \sum_{\substack{xy=n\\(x,y)\in[n]\times[n]}} ((f*g)(x))h(y)\\ &= \sum_{\substack{xy=n\\(x,y)\in[n]\times[n]}} \left[\left(\sum_{\substack{zw=x\\(z,w)\in[n]\times[n]}} f(z)g(w)\right)h(y)\right]\\ &= \sum_{\substack{xy=n\\(x,y)\in[n]\times[n]}} \sum_{\substack{zw=x\\(z,w)\in[n]\times[n]}} f(z)g(w)h(y) = \sum_{\substack{zwy=n\\(z,w,y)\in[n]^3}} f(z)g(w)h(y).\end{aligned}$$

Since the left and right sides are the same, except for a change in indexing variables, the two are equal. ■

Lemma 3.13. The arithmetic function $\varepsilon : \mathbb{Z}_+ \to \mathbb{R}$, defined by

$$\varepsilon(n) = \begin{cases} 1 & \text{if } n = 1 \\ 0 & \text{if } n \neq 1 \end{cases}$$

is an identity for the Dirichlet convolution, in the sense that $f * \varepsilon = f$ for any arithmetic function f. Moreover, this function ε, called the **unit function**, is unique in having this property.

Proof. Indeed, when we look at the sum

$$(f * \varepsilon)(n) = \sum_{d|n} f(d)\varepsilon\left(\frac{n}{d}\right),$$

we can see that the only summand that does not equal 0 is for $d = n$, in which case the summand is

$$f(n)\varepsilon\left(\frac{n}{d}\right) = f(n)\varepsilon(1) = f(n).$$

As we learned in the study of binary operations, if an identity exists for a binary operation, it is unique. However, this proof so far has been a mere mechanical verification. It does not show us how to come across the right definition of ε in the first place. We can deduce the definition of ε as follows. We know that we want it to hold that $f = f * \varepsilon$ for every arithmetic function f. Then

$$f(1) = \varepsilon(1)f(1).$$

By choosing f to be an arithmetic function for which $f(1) \neq 0$, such as $f = \tau$, we get $\varepsilon(1) = 1$. For $n > 1$, we proceed by strong induction on $\Omega(n) \geq 1$. In the base case, we have n equal to a prime p, so

$$f(p) = \varepsilon(1)f(p) + \varepsilon(p)f(1) = f(p) + \varepsilon(p)f(1),$$

which leads to $\varepsilon(p) = 0$. Now suppose there exists a positive integer $n \geq 2$ such that $\varepsilon(m) = 0$ for all integers m such that $1 \leq \Omega(m) < n$. Using the strong induction hypothesis, all intermediate terms in the following sum disappear:

$$\begin{aligned} f(n) &= \sum_{d|n} \varepsilon(d)f\left(\frac{n}{d}\right) \\ &= \varepsilon(1)f(n) + \varepsilon(n)f(1) \\ &= f(n) + \varepsilon(n)f(1), \end{aligned}$$

so $\varepsilon(n) = 0$. Note that the initial part of the proof is still needed because it shows that this ε is sufficient as an identity (so an identity exists), whereas the motivated second part shows that the definition of ε is necessary for an identity (so the identity is unique). ■

Definition 3.14. Let 1 denote the arithmetic function that outputs 1 for every input. Note that

$$(f * 1)(n) = \sum_{d|n} f(d)1\left(\frac{n}{d}\right) = \sum_{d|n} f(d).$$

This is called the **summation function** of f and it is denoted by S_f.

Problem 3.15. Compute S_ε, S_1, and S_{Id}, where Id is the arithmetic function whose output always equals its input, so $\mathrm{Id}(n) = n$ for all n.

Lemma 3.16. Let μ be an arithmetic function. Then $S_\mu = \varepsilon$ if and only if μ is defined by

$$\mu(n) = \begin{cases} (-1)^{\omega(n)} & \text{if } n \text{ is squarefree} \\ 0 & \text{if } n \text{ is not squarefree} \end{cases}.$$

In particular, $\mu(1) = (-1)^{\omega(1)} = (-1)^0 = 1$. This μ is called the **Möbius function**.

Proof. Suppose μ is an arithmetic function that satisfies

$$\varepsilon(n) = S_\mu(n) = \sum_{d|n} \mu(d)$$

for every positive integer n. So

$$\sum_{d|n} \mu(d) = \begin{cases} 1 \text{ if } n = 1 \\ 0 \text{ if } n \neq 1 \end{cases}.$$

We want to deduce the value of μ at every positive integer input. If $n = 1$, then it is immediate that $\mu(1) = \varepsilon(1) = 1$. For squarefree n, we will proceed by strong induction on $\omega(n) = m \geq 0$ with the desire to prove that $\mu(n) = (-1)^{\omega(n)}$. The base case has $m = 0$ and $n = 1$, which we have already computed. Suppose the result holds for all positive squarefree integers up to but not including some positive squarefree integer $m \geq 1$. Let the prime factorization of an integer n be $n = p_1 p_2 \cdots p_m$. By invoking the strong induction hypothesis, we get

$$0 = \sum_{d|n} \mu(d) = \sum_{k=0}^{m} \sum_{\substack{J \subseteq [m] \\ |J| = k}} \mu\left(\prod_{j \in J} p_j\right) = \mu(n) + \sum_{k=0}^{m-1} (-1)^k \binom{m}{k}.$$

By the binomial theorem, we know that $\displaystyle\sum_{k=0}^{m} (-1)^k \binom{m}{k} = (1-1)^m = 0$ (this was covered in Volume 2), so $\mu(n) = (-1)^m$, as desired.

For non-squarefree n, we will proceed by strong induction on $\Omega(n) = m \geq 2$ to prove that $\mu(n) = 0$. In the base case $m = 2$, let p be a prime so that $n = p^2$. Then

$$0 = \mu(1) + \mu(p) + \mu(p^2) = 1 + (-1)^1 + \mu(p^2) = \mu(p^2).$$

Suppose the result holds for all positive non-squarefree integers up to but not including some positive non-squarefree integer $m \geq 3$. Let the prime factorization of an integer n be $n = p_1^{e_1} p_2^{e_2} \cdots p_m^{e_m}$. By invoking the strong induction hypothesis and using the result for squarefree inputs, we get

$$\begin{aligned} 0 = \sum_{d|n} \mu(d) &= \sum_{\substack{d|n \\ d \text{ squarefree}}} \mu(d) + \sum_{\substack{d|n \\ d \text{ non-squarefree}}} \mu(d) \\ &= \sum_{k=0}^{m} \sum_{\substack{J \subseteq [m] \\ |J|=k}} \mu\left(\prod_{j \in J} p_j\right) + \mu(n) = \sum_{k=0}^{m} (-1)^k \binom{m}{k} + \mu(n) \\ &= \mu(n). \end{aligned}$$

This proves that the given definition of the μ function is necessary for it to be true that $S_\mu = \varepsilon$. It remains to be shown that it is sufficient, meaning it actually satisfies the property that $S_\mu = \varepsilon$. If $n = 1$, then

$$S_\mu(1) = \sum_{d|1} \mu(d) = \mu(1) = 1.$$

If $n \neq 1$ and has prime factorization $n = p_1^{e_1} p_2^{e_2} \cdots p_m^{e_m}$, then

$$\begin{aligned} S_\mu(n) = \sum_{d|n} \mu(d) &= \sum_{\substack{d|n \\ d \text{ squarefree}}} \mu(d) + \sum_{\substack{d|n \\ d \text{ non-squarefree}}} 0 \\ &= \sum_{k=0}^{m} \sum_{\substack{J \subseteq [m] \\ |J|=k}} \mu\left(\prod_{j \in J} p_j\right) = \sum_{k=0}^{m} \sum_{\substack{J \subseteq [m] \\ |J|=k}} (-1)^k \\ &= \sum_{k=0}^{m} (-1)^k \binom{m}{k} = 0. \end{aligned}$$

Note that we could have done the sufficiency proof first and then invoked the fact that inverses are unique for associative binary operations to get that μ is also necessary. This is because μ is defined to be the "inverse" of the 1 function under the Dirichlet convolution (since $\varepsilon = S_\mu = \mu * 1$). However, manually figuring out in the first step how μ looks provided greater motivation for pursuing it in the sufficiency proof. Otherwise, it would have been a soulless verification. ■

Problem 3.17. Show that ε is completely multiplicative and μ is multiplicative.

Theorem 3.18 (Möbius inversion formula)**.** Let f and g be arithmetic functions. Then

$$f = \mu * g$$

if and only if $g = S_f$.

Proof. Thanks to the machinery that we have built up, such as commutativity and associativity and the computations of certain Dirichlet convolutions and summation functions, the proof of each direction is quite easy. Using the definition $S_f = f * 1$, we compute

$$\mu * S_f = \mu * (1 * f) = (\mu * 1) * f = S_\mu * f = \varepsilon * f = f.$$

For the converse, the assumption $f = \mu * g$ leads to

$$S_f = 1 * f = 1 * (\mu * g) = (1 * \mu) * g = S_\mu * g = \varepsilon * g = g.$$

■

The "if" direction of the Möbius inversion formula is very useful because it allows us to recover f from S_f, and we will use this idea to compute Euler's totient function. This notion of "recovery" (or partial recovery) is very important in mathematics in general.

Problem 3.19 (Product Möbius inversion). Let f, g be arithmetic functions. Then

$$g(n) = \prod_{d|n} f(d)$$

for all $n \in \mathbb{Z}_+$ if and only if

$$f(n) = \prod_{d|n} g\left(\frac{n}{d}\right)^{\mu(d)}$$

for all $n \in \mathbb{Z}_+$. We will use this result when we study cyclotomic polynomials in Section 13.2.

Theorem 3.20. If f and g are multiplicative arithmetic functions, then their Dirichlet convolution $f * g$ is also multiplicative. As a consequence, f is multiplicative if and only if its summation function S_f is multiplicative.

Proof. We wish to show that, for all coprime positive integers m and n,

$$((f * g)(m))((f * g)(n)) = ((f * g)(mn)).$$

The left side can be written as

$$\begin{aligned}((f * g)(m))((f * g)(n)) &= \left(\sum_{ab=m} f(a)g(b)\right)\left(\sum_{cd=n} f(c)g(d)\right) \\ &= \sum_{\substack{ab=m \\ cd=n}} f(a)g(b)f(c)g(d) \\ &= \sum_{\substack{ab=m \\ cd=n}} f(ac)g(bd)\end{aligned}$$

where the variables a, b, c, d can only be positive. Note that we have used the multiplicativity of f and g with the fact that $(a, c) = (b, d) = (m, n) = 1$. We want this sum to equal

$$(f * g)(mn) = \sum_{rs=mn} f(r)g(s).$$

To do this, we will show that the sets

$$S = \{(r,s) \in \mathbb{Z}_+^2 : \exists a,b,c,d \in \mathbb{Z}_+ \text{ s.t. } ac = r, bd = s, ab = m, cd = n\},$$
$$T = \{(r,s) \in \mathbb{Z}_+^2 : rs = mn\}$$

are equal by proving set inclusion in either direction. The $S \subseteq T$ inclusion is easy: if $(r,s) \in S$, then

$$rs = acbd = abcd = mn,$$

so $(r,s) \in T$. The $T \subseteq S$ inclusion is more subtle and we will need to invoke the coprimality of m,n for it. Suppose $(r,s) \in T$. It would be nice if we could factor r into ac and s into bd while fulfilling $ab = m$ and $cd = n$. So we want to find a,b,c,d such that

$$a \text{ is "the piece" of } r \text{ in } m,$$
$$c \text{ is "the piece" of } r \text{ in } n,$$
$$b \text{ is "the piece" of } s \text{ in } m,$$
$$d \text{ is "the piece" of } s \text{ in } n.$$

Let us make this more formal. Since m and n are coprime, and r and s each divide mn, the multiplicativity of the gcd function with one entry fixed (Theorem 2.19) yields

$$(r,m)(r,n) = (r,mn) = r,$$
$$(s,m)(s,n) = (s,mn) = s.$$

Thus, given a pair (r,s) from the second set, we consider choosing

$$a = (r,m), c = (r,n), b = (s,m), d = (s,n).$$

Indeed, the final two conditions are also met as follows. Firstly,

$$mn = rs = (r,m)(r,n)(s,m)(s,n) = abcd.$$

Since a,b are divisors of m and $\gcd(m,n) = 1$, a and b are coprime to n. From $abcd = mn$, we get that ab divides mn and so ab divides m by Gauss's divisibility lemma. Similarly, cd divides n. Then $(ab)(cd) \leq mn = abcd$ with equality holding if and only if $ab = m$ and $cd = n$. Since equality must hold, we get $ab = m$ and $cd = n$. As we showed earlier by the multiplicativity of gcd, $ac = r$ and $bd = s$. So $(r,s) \in S$.
For the corollary, we will use the Möbius inversion formula. If f is multiplicative, then so is $S_f = f * 1$, since 1 is multiplicative. If S_f is multiplicative, then so is $f = \mu * S_f$ by the multiplicativity of μ. ■

There is much more that can be said about the Dirichlet convolution. In particular, there is a notion of Dirichlet inverses that we have glazed over. Moreover, there are innumerable interrelations between classical arithmetic functions under the application of the Dirichlet convolution; one such relation is the subject of Problem 3.22.

3.3 Euler's Totient Function

With our general discussion of the Dirichlet convolution complete, we are ready to compute φ. The plan is to compute the summation function S_φ, observe that it is multiplicative, and then smoothly compute a formula for φ in terms of the prime factorization of the input.

Theorem 3.21. For any positive integer n, $S_\varphi(n) = n$. More succinctly, $S_\varphi = \mathrm{Id}$. Consequently, since Id is multiplicative, φ is multiplicative by Theorem 3.20.

Proof. The idea is to double count the number of entries in the tuple

$$T = \left(\frac{1}{n}, \frac{2}{n}, \ldots, \frac{n-1}{n}, \frac{n}{n}\right) = \left(\frac{a_1}{b_1}, \frac{a_2}{b_2}, \ldots, \frac{a_{n-1}}{b_{n-1}}, \frac{a_n}{b_n}\right),$$

where for each $i \in [n]$, a_i and b_i are the unique positive integers such that $\dfrac{a_i}{b_i} = \dfrac{i}{n}$ and $\gcd(a_i, b_i) = 1$. By Lemma 2.24, each b_i divides n. For each d such that $d \mid n$, we claim that the number of b_i that equal d is $\varphi(d)$: Fixing d, if $b_i = d$ then $(a_i, d) = 1$. Since $a_i \in [d]$, there are at most $\varphi(d)$ fractions $\dfrac{a_j}{b_j}$ in T with $b_j = d$. There are at least $\varphi(d)$ such fractions as well because for each $a_j \in [d]$ such that $(a_j, d) = 1$,

$$\frac{a_j}{d} = \frac{a_j \cdot \frac{n}{d}}{n}$$

is a distinct element of T. Thus, there are $\varphi(d)$ fractions in T whose least denominator is d. Since there are n entries in total in T, summing over all of the possible divisors d of n yields

$$\sum_{d \mid n} \varphi(d) = n \implies S_\varphi = \mathrm{Id}.$$

■

Problem 3.22. Prove that $\varphi * \tau = \sigma$.

Problem 3.23. Let a, b be integers such that at least one of the two is non-zero. Prove that

$$\sum_{k \mid a \text{ and } k \mid b} \varphi(k) = \gcd(a, b),$$

where the sum is taken over all positive common divisors k of a and b.

Theorem 3.24. If n is a positive integer with prime factorization $n = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$, then

$$\begin{aligned}\varphi(n) &= p_1^{e_1 - 1}(p_1 - 1) p_2^{e_2 - 1}(p_2 - 1) \cdots p_k^{e_k - 1}(p_k - 1) \\ &= n \cdot \left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right) \cdots \left(1 - \frac{1}{p_k}\right).\end{aligned}$$

In particular, $\varphi(1) = 1$.

Proof. The only element of [1] that is coprime to 1 is 1 (the single element), which agrees with the given two formulas because the empty product is defined to be 1. So we may assume now that $n \geq 2$.
Since $S_\varphi = \mathrm{Id}$ is multiplicative, so is φ by Theorem 3.20. So it suffices to find what φ equals for prime powers, as we can then applying it to the maximal prime powers in the prime factorization of n. Let $n = p^m$ for some prime p and positive integer m. The positive integers in $[p^m]$ that are coprime to p^m are exactly the non-multiples of p. Since there are $\dfrac{p^m}{p} = p^{m-1}$ multiples of p in $[p^m]$, the number of non-multiples of p is $p^m - p^{m-1} = p^{m-1}(p-1)$. This proves the first formula. The second formula follows from the first by factoring out an extra copy of each distinct prime factor. ■

Note that, in general, if it is possible to prove that an arithmetic function is multiplicative without using an explicit formula for the function, then a general formula can be pieced together using the prime factorization of the input by finding what the formula equals when it is restricted to prime powers inputs.

Corollary 3.25. Let a be an integer. If $a \geq 3$, then $\varphi(a) \geq 2$. If $a \geq 2$, then $\varphi(a) \leq a - 1$, with equality holding if and only if a is prime; this biconditional equality case will repeatedly be useful. If a is composite, then we can sharpen the upper bound to

$$\varphi(a) \leq a - \sqrt{a},$$

with equality holding if and only if a is the square of a prime.

Proof. If $a \geq 3$ is an integer, then 1 and $a - 1$ are distinct integers in $[a]$ that are coprime to a, so $\varphi(a) \geq 2$. The upper bound $a - 1$ holds for $a \geq 2$ because a is not coprime a, but the rest of the $a - 1$ elements of $[a]$ are fair game for being coprime to a. If a is a prime, then $\varphi(a) = a - 1$ and equality holds in the bound. Conversely, if $\varphi(a) = a - 1$, then none of the primes strictly below a divide a, otherwise one of the elements of $[a - 1]$ would fail to be coprime to a and we would not have $\varphi(a) = a - 1$. By the standard primality test (Theorem 2.6), a is prime in this direction.
Suppose a is composite. Due to the fact that a composite integer has a factorization into two non-trivial *coprime* factors when it is not a prime power, we will do casework on when a is a prime power and when it is not. If a is not a prime power, then there exist coprime positive integers x and y such that $a = xy$. For example, we can choose x to be a maximal prime power that divides a (this is the highest power of a specific prime that non-trivially divides a) and y to be the quotient of a divided by x. By the multiplicativity of φ,

$$\varphi(a) = \varphi(xy) = \varphi(x)\varphi(y) \leq (x-1)(y-1) = xy - x - y + 1.$$

By the trivial inequality, $(\sqrt{x} - \sqrt{y})^2 > 0$ leads to $x + y > 2\sqrt{xy}$. Then our bound becomes

$$\varphi(a) < xy + 1 - 2\sqrt{xy} < xy - \sqrt{xy} = a - \sqrt{a}.$$

So the inequality holds in this case, and strictly so. Now suppose a is a prime power p^k for some prime p and integer $k \geq 2$. Then

$$\varphi(n) = \varphi(p^k) = p^k - p^{k-1}.$$

Using the fact that $k - 1 \geq \frac{k}{2}$ if and only if $k \geq 2$ with equality holding if and only if $k = 2$, we get the bound

$$\varphi(n) \leq p^k - p^{\frac{k}{2}} = a - \sqrt{a},$$

with equality holding if and only if $k = 2$. Thus, equality holds in this upper bound for composite a if and only if a is the square of a prime. ■

This inequality can be further sharpened in other cases, which the reader may wish to explore.

Corollary 3.26. Let p be a prime and $p_1, p_2, \ldots, p_k$ be distinct primes. Then

$$\varphi(p) = p - 1,$$
$$\varphi(p_1 p_2 \cdots p_k) = (p_1 - 1)(p_2 - 1) \cdots (p_k - 1).$$

The following corollaries contain the most useful general properties of the φ function of which we are aware. The results largely follow from the second formula for φ

$$\varphi(n) = n \prod_{p|n} \left(1 - \frac{1}{p}\right),$$

where the product is over all distinct *prime* factors of p of n.

Corollary 3.27. If a and b are positive integers, then $a \mid b$, then $\varphi(a) \mid \varphi(b)$.

Proof. If $a \mid b$, then the set of prime factors of a is a subset of the set of prime factors of b. Thus,

$$\frac{\varphi(b)}{\varphi(b)} = \frac{b}{a} \cdot \frac{\prod_{p|b} \left(1 - \frac{1}{p}\right)}{\prod_{p|a} \left(1 - \frac{1}{p}\right)}$$

is an integer because $a \mid b$ and each multiplicand in the denominator exists as a distinct multiplicand in the numerator. ■

Corollary 3.28. If a and b are positive integers, then

$$\varphi(ab) = \varphi(a)\varphi(b) \cdot \frac{\gcd(a, b)}{\varphi(\gcd(a, b))}.$$

This generalizes φ's multiplicativity identity $\varphi(ab) = \varphi(a)\varphi(b)$ from the coprime case to all integers a, b. Some consequences are that

$$\varphi(2a) = \begin{cases} 2\varphi(a) & \text{if } 2 \mid a \\ \varphi(a) & \text{if } 2 \nmid a \end{cases},$$
$$\varphi(a^n) = a^{n-1} \cdot \varphi(a),$$

where n is any positive integer.

Proof. Firstly, we write

$$\varphi(ab) = ab \prod_{p|ab} \Big(1 - \frac{1}{p}\Big).$$

By the prime factorization formula for the least common multiple of two non-zero integers, we know that a prime p divides ab if and only if p divides $[a, b]$. So

$$\varphi(ab) = ab \prod_{p|[a,b]} \Big(1 - \frac{1}{p}\Big).$$

Inspired by the fact that

$$(a, b) \cdot [a, b] = ab,$$

we conjecture that

$$\prod_{p|(a,b)} \Big(1 - \frac{1}{p}\Big) \cdot \prod_{p|[a,b]} \Big(1 - \frac{1}{p}\Big) = \prod_{p|a} \Big(1 - \frac{1}{p}\Big) \cdot \prod_{p|b} \Big(1 - \frac{1}{p}\Big).$$

This would be very convenient because then we could deduce that

$$\begin{aligned}
\varphi(ab) &= ab \prod_{p|[a,b]} \Big(1 - \frac{1}{p}\Big) \\
&= ab \cdot \frac{\prod_{p|a} \left(1 - \frac{1}{p}\right) \cdot \prod_{p|b} \left(1 - \frac{1}{p}\right)}{\prod_{p|(a,b)} \left(1 - \frac{1}{p}\right)} \\
&= \frac{a \prod_{p|a} \left(1 - \frac{1}{p}\right) \cdot b \prod_{p|b} \left(1 - \frac{1}{p}\right)}{(a, b) \prod_{p|(a,b)} \left(1 - \frac{1}{p}\right)} \cdot (a, b) \\
&= \varphi(a)\varphi(b) \cdot \frac{(a, b)}{\varphi((a, b))}.
\end{aligned}$$

So let us aim to prove the conjecture. In the following argument, p always denotes only primes. In a product of the form $\displaystyle\prod_{p|[a,b]}$, we are iterating over primes that divide at least one of a or b. Similar to when we worked on the principle of inclusion-exclusion for two sets in Volume 2, this set can be partitioned into three sets: p divides a but not b; p divides b but not a; p divides both a and b. Note that a prime p divides both a and b if and only if p divides (a, b). Thus,

$$\prod_{p|(a,b)} \Big(1 - \frac{1}{p}\Big) \prod_{p|[a,b]} \Big(1 - \frac{1}{p}\Big) = \prod_{p|a, p\nmid b} \Big(1 - \frac{1}{p}\Big) \cdot \prod_{p\nmid a, p|b} \Big(1 - \frac{1}{p}\Big) \cdot \left[\prod_{p|a,p|b} \Big(1 - \frac{1}{p}\Big)\right]^2.$$

Rearranging the product, we get

$$\left[\prod_{p|a,p\nmid b} \Big(1 - \frac{1}{p}\Big) \cdot \prod_{p|a,p|b} \Big(1 - \frac{1}{p}\Big)\right] \cdot \left[\prod_{p\nmid a,p|b} \Big(1 - \frac{1}{p}\Big) \cdot \prod_{p|a,p|b} \Big(1 - \frac{1}{p}\Big)\right].$$

This is equal to the desired

$$\prod_{p|a}\left(1-\frac{1}{p}\right)\cdot\prod_{p|b}\left(1-\frac{1}{p}\right).$$

Now we address the corollaries. Firstly, by the result we just proved,

$$\varphi(2a)=\varphi(2)\varphi(a)\cdot\frac{(2,a)}{\varphi((2,a))}=\begin{cases}2\varphi(a) & \text{if } 2\mid a\\ \varphi(a) & \text{if } 2\nmid a\end{cases}.$$

Another consequence is that, if $n\geq 2$, then

$$\varphi(a^n)=\varphi(a)\varphi(a^{n-1})\cdot\frac{(a,a^{n-1})}{\varphi((a,a^{n-1}))}=\varphi(a^{n-1})a,$$

since $(a,a^{n-1})=a$. Using this identity as the inductive step, we can show by induction on n that

$$\varphi(a^n)=a^{n-1}\varphi(a).$$

The base case $n=1$ is trivial. ■

Problem 3.29. Prove that, if a and b are positive integers, then

$$\varphi(\gcd(a,b))\cdot\varphi(\operatorname{lcm}(a,b))=\varphi(a)\cdot\varphi(b).$$

Corollary 3.30. Let a be a positive integer. If a has r distinct odd prime factors, then

$$\nu_2(\varphi(a))\geq r.$$

Moreover, if $\nu_2(a)=s\geq 1$ then $\nu_2(\varphi(a))\geq s-1+r$ Consequently, $\varphi(a)$ is even if $a\geq 3$.

Proof. Let the prime factorization of a be

$$a=2^s p_1^{e_1}p_2^{e_2}\cdots p_r^{e_r},$$

where $p_1,p_2,\ldots,p_r$ are distinct odd primes, s is a non-negative integer and the e_i are positive integers. According to the formula for φ, the product

$$(p_1-1)(p_2-1)\cdots(p_r-1)$$

divides $\varphi(a)$. Since each p_i is odd, 2 divides each p_i-1, and so 2^r divides $\varphi(a)$ by transitivity of divisibility. And if $s\geq 1$, then 2^{s-1} is an extra power of 2 that divides $\varphi(a)$, so 2^{s-1+r} divides $\varphi(a)$.
For the last assertion, we do casework on whether $a\geq 3$ is a power of 2. If a is not a power of 2, then it has an odd prime factor, and so 2 divides $\varphi(a)$ by the first part. If $a\geq 3$ is a power of 2, then $a=2^m$ for some integer $m\geq 2$. Then 2^{m-1} is a non-trivial power of 2 that divides $\varphi(a)$. So $\varphi(a)$ is even for all integers $a\geq 3$. ■

Chapter 4

Modular Arithmetic

> "The first analogy that came to my mind is of immersing the nut in some softening liquid, and why not simply water? From time to time you rub so the liquid penetrates better, and otherwise you let time pass. The shell becomes more flexible through weeks and months - when the time is ripe, hand pressure is enough, the shell opens like a perfectly ripened avocado!"
>
> – *Alexander Grothendieck*

> "From [Grothendieck] and his example, I have also learned not to take glory in the difficulty of a proof: difficulty means we have not understood. The ideal is to be able to paint a landscape in which the proof is obvious. I admire how often he succeeded in reaching this ideal."
>
> – *Pierre Deligne, Notices of the AMS*

In the Euclidean division of integers, if the divisor is a positive integer n, then the set of possible remainders is $\{0, 1, 2, \ldots, n-1\}$. Modular arithmetic can be thought of as a way of doing arithmetic on the set of remainders. In a more formal sense, the objects of modular arithmetic are not the integers that are the remainders themselves, but equivalence classes of the integers that we define according to what remainder they leave upon division by n. This incredible idea of partitioning the integers into classes according to their remainders has far-reaching ramifications in the theory of numbers and the whole of mathematics.

4.1 Modular Operations

Definition 4.1. For each integer $n \geq 1$, the relation among the integers of **congruence modulo** n is defined by: $a \sim b$ if and only of a and b leave the same remainder upon Euclidean division by n. If it is true, then we say that a **is congruent to** b **modulo** n and denote it by

$$a \equiv b \pmod{n},$$

and this relation is called a **congruence**. In the case of the negation, we says that a and b are **incongruent modulo** n and denoted it by

$$a \not\equiv b \pmod{n}.$$

The divisor n is called the **modulus** and the plural of this term is **moduli**.

Example. Although a modulus of $n = 1$ is rarely used, it does come up. In such cases, we recommend mentally verifying the result does in fact hold for this modulus because a modulus of $n = 1$ behaves a little different from moduli $n > 1$. A representation that we often use is: $a \equiv b \pmod{n}$ if and only if there exists an integer k such that $a = b+kn$. Using the representation, we can see that every integer is congruent to every other integer modulo 1. If needed, one may also speak of the 0 modulus, which, according to this representation implies that each integer is congruent to no integer but itself modulo 0, meaning it behaves just like equality in $\mathbb{Z}$. So the modulus of 0 behaves precisely opposite to the modulus of 1.

Lemma 4.2. Let n be a positive integer. For every pair of integers a and b,

$$a \equiv b \pmod{n} \iff n \mid a - b.$$

Proof. For one direction, suppose a and b leave the same remainder upon Euclidean division by n. Then

$$a = q_1 n + r,$$
$$b = q_2 n + r,$$

where q_1 and q_2 are quotients and r is the common remainder. Subtracting the equations yields

$$a - b = (q_1 - q_2)n,$$

so $n \mid a - b$.
Conversely, suppose $n \mid a - b$. By Euclidean division,

$$a = q_1 n + r_1, \text{ and } 0 \leq r_1 < n,$$
$$b = q_2 n + r_2, \text{ and } 0 \leq r_2 < n,$$

where the quotient-remainder pairs for a and b are (q_1, r_2) and (q_2, r_2), respectively. Again, subtracting the equations yields

$$a - b = (q_1 - q_2)n + (r_1 - r_2).$$

Since n divides $a - b$ and $(q_1 - q_2)n$, n divides $r_1 - r_2$. Adding the remainder inequalities $0 \leq r_1 < n$ and $-n < -r_2 \leq 0$ yields

$$-n < r_1 - r_2 < n.$$

The only multiple of n in the interval $(-n, n)$ is 0, so $r_1 = r_2$, as desired. ■

Theorem 4.3. For each integer $n \geq 1$, congruence modulo n is an equivalence relation.

Proof. We have to verify the three properties: reflexivity, symmetry, and transitivity. Let a, b, c be integers. The results below follow using the equivalent definition of congruence in Lemma 4.2.

- Reflexivity: $a - a = 0$ is divisible by n.

- Symmetry: if n divides $a - b$, then n also divides $b - a = -(a - b)$.
- Transitivity: if n divides $a - b$ and $b - c$, then n also divides their sum

$$(a - b) + (b - c) = a - c.$$

■

Definition 4.4. Suppose n is a positive integer. The equivalence classes modulo n are called **congruence classes** or **residue classes** modulo n. If a and b are in the same residue class, then it can be said that b is a **residue** of a. Note that negative integers also inhabit each residue class, and that the definition does not only apply to positive integers. The residue class of an integer a is denoted by $[a]$, just like the notation for equivalence classes. This overloads the notation because $[a]$ also represents the a^{th} section of the positive integers. If it is necessary to distinguish the class $[a]$ from the section $[a] = \{1, 2, \ldots, a\}$, we will denote the class by $\overline{a}$.

Number theory often involves doing casework on congruence classes, given a certain modulus. The modulus 2 is especially useful, as it results in essentially an argument by casework on parity. Now that we have all of the basic definitions of number theory in place, here is a summary of common methods of binary casework in number theory that we have mentioned so far:

- Squarefree or divisible by the square of a prime
- Prime power or has two distinct prime factors
- Power of 2 or divisible by an odd prime
- Composite or prime
- Even or odd parity
- Numbers that are coprime or share a non-trivial common factor

Moreover, the numbers 0 or 1 often have to be treated as special cases as the argument that works for other integers do not necessarily apply to these cases, or the arguments apply in some "empty" sense that requires a separate mental verification anyway.

Definition 4.5. Let n be a positive integer. A set of exactly n integers, with exactly one representative from each congruence class modulo n, is called a **complete residue system** modulo n. The particular such set

$$[n - 1]^* = \{0, 1, 2, \ldots, n - 1\}$$

is called the **least residue system** modulo n. If r is an element of a least residue system and a is a representative from the residue class of r, then r is said to be the **least residue** (technically, the least *non-negative* residue) of a.

Now we will develop modular arithmetic, which will allow us to manipulate congruences like equations. We will see that addition, negation, subtraction, and multiplication occur naturally as one would expect. However, division and multiplicative inverses are possible in only some cases, though that is what makes it the most interesting aspect of basic modular arithmetic in some ways.

Theorem 4.6. Let n be a positive integer, and a, b, c, d be integers. Congruences can be manipulated like equations as follows:

1. Addition and multiplication: If $a \equiv b \pmod{n}$, then

$$\begin{aligned} a + c &\equiv b + c \pmod{n}, \\ ac &\equiv bc \pmod{n}. \end{aligned}$$

   Consequently, if $c \equiv d \pmod{n}$ as well, then

$$\begin{aligned} a + c &\equiv b + d \pmod{n}, \\ ac &\equiv bd \pmod{n}. \end{aligned}$$

   Repeatedly applying the latter to same congruence yields

$$a^k \equiv b^k \pmod{n}$$

   for any positive integer k, where a^k is defined as $\underbrace{a \cdot a \cdots a}_{k \text{ copies of } a}$ if k is positive. We will discuss non-positive exponents k in Definition 4.14 as they are not always valid.

2. Negation and subtraction: If $a \equiv b \pmod{n}$, then

$$-a \equiv -b \pmod{n}.$$

   Subsequently, if $c \equiv d \pmod{n}$ as well, then the two congruences can be added to yield

$$c - a \equiv d - b \pmod{n}.$$

   This allows for additive cancellation, meaning

$$a + c \equiv b + c \pmod{n} \implies a \equiv b \pmod{n}.$$

Proof. Almost all of these follow from the fact that $x \equiv y \pmod{n}$ if and only if $n \mid x - y$, which is Lemma 4.2. The only non-trivial manipulations are:

$$\begin{aligned} a + c \equiv b + c \equiv b + d &\pmod{n}, \\ ac \equiv bc \equiv bd &\pmod{n}. \end{aligned}$$

We leave the fleshing out of the details to the reader. ∎

Problem 4.7. Prove that a polynomial with integer exponents can be applied to both sides of a true congruence, and the resulting congruence will still be true. That is, if $f \in \mathbb{Z}[x]$, then

$$a \equiv b \pmod{n} \implies f(a) \equiv f(b) \pmod{n}.$$

One should be careful to not apply this haphazardly with other functions, such an exponential functions, as the result might simply be false.

Problem 4.8. Determine all moduli n in which 1 and -1 occupy the same residue class.

Definition 4.9. Suppose n is a positive integer and a is an integer. By Euclidean division of a by n, there exists a quotient q and a remainder r such that

$$a = nq + r, \text{ and } 0 \leq r < n.$$

Recall from Definition 4.5 that this r is called the least residue of a modulo n. If it is valid to replace a with r in a congruence, then this replacement is called **reduction** modulo n. Sometimes it is hard to find r, so we might replace a with some integer s (of any sign) that is not r, but is still closer to 0 than a; in this case, we may still refer to the replacement of a with s as a reduction.

Example. Since $10 \equiv 3 \pmod{7}$, 10^k may be reduced to 3^k modulo 7 for any positive integer k so that $10^k \equiv 3^k \pmod{7}$. Note that it is rarely the case the the exponents are cut down instead of the base in a congruence. However, there are theorems that sometimes allow for making exponents smaller, such as a generalization of Euler's congruence (Corollary 4.27).

Problem 4.10. If p is a prime and a is an integer, then classify all integers x such that

$$x^2 \equiv a^2 \pmod{p}.$$

With all of the basic arithmetic operations understood except division, we now turn to the question of what it means to multiplicatively invert integers in a modulus. By "in a modulus," we mean "modulo some positive integer n."

Definition 4.11. Let n be a positive integer and a be an integer. If there is a positive integer b such that $ab \equiv 1 \pmod{n}$, then b is said to be a **modular multiplicative inverse** or just an **inverse** of a, and a is said to be **invertible** or a **unit** modulo n. Note that a and b are symmetric in this relation, meaning each is an inverse of the other.

Theorem 4.12. If n is a positive integer and a is an integer, then a has an inverse modulo n if and only if $\gcd(a, n) = 1$. In this case, the inverse of a is unique in the sense that all inverses fall into the same congruence class and all elements of that class are inverses of a. An element of this class may be denoted by a^{-1} and the whole class by $[a]^{-1} = [a^{-1}]$. One such a^{-1} may be found using the extended Euclidean algorithm, which allows us to find the entire class as

$$[a]^{-1} = \{a^{-1} + kn : k \in \mathbb{Z}\}.$$

Proof. If $n = 1$, then all integers are congruent to each other, so every integer is an inverse of every integer. This is consistent with the stated theorem because $(a, 1) = 1$ for every integer a.
Now suppose $n \geq 2$ and let a be an integer. Suppose exists an integer b such that $ab \equiv 1 \pmod{n}$. This is true if and only if $n \mid ab-1$ if and only if there exists an integer d such that $ab - 1 = dn$. By a corollary of Bézout's lemma (Corollary 1.18), this is possible if and only if $(a, n) = 1$. Moreover, the extended Euclidean algorithm (Theorem 1.30) allows us to find suitable b and d, thereby giving us b and the entire congruence class of b. For any integer k,

$$ab \equiv 1 \pmod{n} \implies a(b + kn) \equiv 1 \pmod{n},$$

so the set of inverses of a includes the congruence class of b modulo n. Moreover, if c is an integer such that $ac \equiv 1 \pmod{n}$, then subtracting it from $ab \equiv 1 \pmod{n}$ yields

$$a(b - c) \equiv 0 \pmod{n}.$$

We can multiply both sides by b to cancel out the a and get $b \equiv c \pmod{n}$. Therefore, the set of inverses of a is precisely the congruence class of b modulo n. ■

Corollary 4.13. Let n be a positive integer, and a and b be integers that are coprime to n. Then a and b are units modulo n, so we pick any two inverses a^{-1} and b^{-1}. Then the following congruences are equivalent:

$$\begin{aligned} a &\equiv b \pmod{n}, \\ ab^{-1} &\equiv 1 \pmod{n}, \\ b^{-1} &\equiv a^{-1} \pmod{n}. \end{aligned}$$

Proof. First we multiply both sides of the first congruence by b^{-1} to get the second congruence, and then we multiplying both sides of the second congruence by a^{-1} to get the third congruence. Now going from bottom to top, we multiply by a and then multiply by b. ■

Definition 4.14. If n is a positive integer and a is an integer that is coprime to n, then for any positive integer k, we define the notation a^{-k} to denote $(a^{-1})^k$, provided that an inverse a^{-1} of a has been fixed or the result at hand is independent of the choice of an inverse. We also define

$$a^0 \equiv a \cdot a^{-1} \equiv 1 \pmod{n}.$$

Note that we do not define b^k modulo n when k is non-positive if b is not coprime to n. One can verify that normal exponent laws hold for modular exponents. That is, if a, b and i, j are integers, then

$$\begin{aligned} a^i \cdot a^j &\equiv a^{i+j} \pmod{n}, \\ (a^i)^j &\equiv a^{ij} \pmod{n}, \\ a^i \cdot b^i &\equiv (ab)^i \pmod{n}, \end{aligned}$$

where any non-positive exponent automatically restricts its corresponding base to being coprime to n.

Theorem 4.15. Suppose n and d are positive integers, and a and b are integers. Then the following useful division-like properties of congruences hold:

1. If $d \mid n$ and $a \equiv b \pmod{n}$, then $a \equiv b \pmod{d}$.
2. It holds that
$$ad \equiv bd \pmod{n} \iff a \equiv b \left(\mod \frac{n}{(n,d)}\right).$$
There are three special cases of interest:
   - If $(d, n) = 1$, then the latter congruence is $a \equiv b \pmod{n}$.
   - If $d \mid n$, then the latter congruence is $a \equiv b \left(\mod \frac{n}{d}\right)$.
   - If $n \mid d$, then the latter congruence is $a \equiv b \pmod{1}$, which is true for all integers a and b.

Proof. We will use the first part to prove the second part.

1. By assumption, $d \mid n$ and $n \mid a - b$. By transitivity of divisibility, $d \mid a - b$, which is what we wanted.
2. If $ad \equiv bd \pmod{n}$, then there exists an integer k such that
$$(a - b)d = kn.$$
We can divide both sides of this equation by (d, n), which is a divisor of n. This yields the congruence
$$a \cdot \frac{d}{(d,n)} \equiv b \cdot \frac{d}{(d,n)} \left(\mod \frac{n}{(d,n)}\right).$$
Since $\gcd\left(\frac{d}{(d,n)}, \frac{n}{(d,n)}\right) = 1$, we may cancel $\frac{d}{(d,n)}$ from both sides of the congruence to get what we want. The converse is true by the last part because our steps were reversible.

■

Thus, "solving" linear congruences such as $ax + b \equiv c \pmod{d}$ boils down to either showing that no solutions exist or dividing out by common factors of $a, c-b, d$, and finding an inverse of the remaining coefficient of x in order to isolate x. Note that first reducing all constants a, b, c to their least residues modulo n is usually helpful.

Problem 4.16. Let n and d be positive integers such that $d \mid n$, and a and b be integers. Someone conjectures that if $a \equiv b \pmod{d}$, then $a \equiv b \pmod{n}$. Find a counterexample pair (a, b) for each pair (d, n) such that $d \neq n$ (note that this means that $n \neq 1$, otherwise we would be forced to have $d = n = 1$).

Definition 4.17. Let n be a positive integer. The set of residue classes modulo n is denoted by $\mathbb{Z}/n\mathbb{Z}$ or $\mathbb{Z}_n$. With some straightforward work, it can be shown that the following operations are well-defined, meaning the choices of representatives make no difference modulo n. For all integers a and b,

$$\begin{aligned} [a] + [b] &= [a + b], \\ -[a] &= [-a], \\ [a] \cdot [b] &= [ab], \\ [a]^{-1} &= [a^{-1}], \end{aligned}$$

where the final equation makes sense if and only if a is coprime to the modulus n. In the language of abstract algebra, $\mathbb{Z}/n\mathbb{Z}$ is a commutative ring. We will not need to deal with operations on $\mathbb{Z}/n\mathbb{Z}$, so the reader may skip over this definition if it is confusing.

Example. If $n = 1$, then $\mathbb{Z}/1\mathbb{Z} = \{\mathbb{Z}\}$ because there is just one big congruence class containing all of the integers. If $n = 0$ is allowed, then

$$\mathbb{Z}/0\mathbb{Z} = \{\{n\} : n \in \mathbb{Z}\},$$

which is the set of singletons from the integers.

Definition 4.18. Suppose n is a positive integer. A **reduced residue class** modulo n is a residue class modulo n that contains an element that is coprime to n, and so all elements of the class are coprime to n. That last part is true because the faux-Euclidean algorithm implies that if $(a, n) = 1$, then

$$(a + kn, n) = (a, n) = 1$$

for any integer k. So the congruence classes modulo n come in two flavours: those whose elements are all coprime to n, and those that do not contain any elements that are coprime to n. A **reduced residue system** modulo n is a set containing one representative from each of the $\varphi(n)$ reduced residue classes modulo n. The **least reduced residue system** is the unique reduced residue system that is a subset of the least residue system $[n-1]^* = \{0, 1, 2 \ldots, n-1.\}$ The set of all reduced residue classes modulo n is denoted by $(\mathbb{Z}/n\mathbb{Z})^*$ or $\mathbb{Z}_n^*$.

Example. For any integer a, a reduced residue system modulo 1 is given by $\{a\}$. This works even if $a = 0$. This further shows that the modulus of 1 is rather strange. One should not overlook it however, as the "continuous" version of the modulus of 1 is essentially a circle in mathematical analysis, and it comes up from time to time. For example, we saw how, for any irrational α, $\{n\alpha : n \in \mathbb{Z}\}$ modulo 1 is dense in $[0, 1)$ when we studied the pigeonhole principle in Volume 2.

Theorem 4.19. Let n be a positive integer and R be a reduced residue systems modulo n. Let a and b be integers. Then a and b are both coprime to n if and only if ab is coprime to n. As a consequence, $[a] \in (\mathbb{Z}/n\mathbb{Z})^*$ and $[b] \in (\mathbb{Z}/n\mathbb{Z})^*$ if and only if $[ab] \in (\mathbb{Z}/n\mathbb{Z})^*$, one direction of which states that $(\mathbb{Z}/n\mathbb{Z})^*$ is closed under multiplication. In this case, an inverse of ab is $b^{-1}a^{-1}$ for any choice of b^{-1} and a^{-1}.

Proof. By Problem 1.20, since $n \neq 0$, it is a consequence of Bézout's lemma that $(n, ab) = 1$ if and only if $(n, a) = 1$ and $(n, b) = 1$. In this case, we can multiply together $aa^{-1} \equiv 1 \pmod{n}$ and $bb^{-1} \equiv 1 \pmod{n}$ to get

$$(ab)(b^{-1}a^{-1}) \equiv 1 \pmod{n}$$

to get that $b^{-1}a^{-1}$ is an inverse of ab. ■

Recall from Corollary 3.25 that $\varphi(n) \leq n-1$ for all positive integers n, with equality holding if and only if n is prime. Thus, a reduced residue system has maximal size if and only if the modulus is prime. For those with some familiarity with abstract algebra, this means that the commutative ring $\mathbb{Z}/n\mathbb{Z}$ is a field if and only if n is prime.

Example 4.20. Prove that $n = 1$ is the only modulus in which $(\mathbb{Z}/n\mathbb{Z})^*$ is closed under addition.

Solution. Let the modulus be n. Then $(\mathbb{Z}/n\mathbb{Z})^*$ contains $[1]$ and $[n-1]$ because $(n, 1) = (n, n-1) = 1$ for every integer n. Adding them together yields

$$[1] + [n-1] = [1 + (n-1)] = [n] = [0].$$

The only way that $(\mathbb{Z}/n\mathbb{Z})^*$ contains $[0]$ is if $n = 1$, because 0 is not invertible if $n > 1$. ■

Problem 4.21. Let $n \geq 3$ be an integer and R be a reduced residue system modulo n. Prove that

$$\sum_{r \in R} r \equiv 0 \pmod{n}.$$

4.2 Wilson, Euler, and Fermat

As a capstone to our study of basic modular arithmetic, we will now see three significant computational tools in modular arithmetic. They are attributed to Wilson, Euler, and Fermat.

Theorem 4.22 (Wilson's theorem)**.** If $n \geq 2$ is an integer, then

$$(n-1)! \equiv \begin{cases} -1 \pmod{n} & \text{if } n \text{ is prime} \\ 2 \pmod{n} & \text{if } n = 4 \\ 0 \pmod{n} & \text{if } n \text{ is composite, } n \neq 4 \end{cases}.$$

As such, n is prime if and only if $(n-1)! \equiv -1 \pmod{n}$.

Proof. Let $n \geq 2$ be an integer. If $n = 2$, then

$$(n-1)! \equiv 1 \equiv -1 \pmod{2}.$$

If n is an odd prime, then the idea is that $[n-1]$ consists of an even number of elements, all of which are coprime to n; in fact, $[n-1]$ is a reduced residue system modulo n that

contains the inverse of every element. By the solution to Problem 4.10, we know that the only self-inverse elements are 1 and $n-1$, meaning the rest of the elements uniquely pair up and cancel each other out multiplicatively in $(n-1)!$. Thus,

$$(n-1)! \equiv 1 \cdot (n-1) \equiv -1 \pmod{n}.$$

If n is composite, then there exist factors a and b of n such that $2 \leq a \leq b \leq n-1$ and $n = ab$. If a and b can be selected such that the strict inequality $a < b$ holds, then a and b are distinct multiplicands of the product

$$(n-1)! = \prod_{k=1}^{n-1} k.$$

Thus, $ab \mid (n-1)!$, so

$$(n-1)! \equiv 0 \pmod{n}.$$

If it is the case that it must be true that $a = b$, then there is only one factor $p = a = b$ of n in the interval $[1, n-1]$ and p must be prime, otherwise there will be another factor in the interval. This forces n to be a power of p because n can be divisible by no other prime. In fact, it must be true that $n = p^2$ because n being any higher power of p would cause other factors of n to exist in the interval $[1, n-1]$. If $p = 2$ and so $n = 4$, then

$$(n-1)! \equiv 3! \equiv 2 \pmod{4}.$$

If p is an odd prime, then

$$2 < p \implies 2 < p < 2p < p^2,$$

so p and $2p$ are distinct multiplicands of the product $(n-1)!$, meaning $2p^2 \mid (n-1)!$ and so

$$(n-1)! \equiv 0 \pmod{n}.$$

This completes all of the casework and we have completely classified the residues of $(n-1)!$ modulo n. ■

Interestingly, it was Lagrange, and not Wilson, who first proved Wilson's theorem, adding evidence to Stigler's law of eponymy, which states that "no scientific discovery is named after its original discoverer." A generalization of Wilson's theorem was proven by Gauss, though Gauss omitted the proof in article 78 of his famous work, *Disquisitiones Arithmeticae*, for the sake of "brevity" [8]. We present a proof of Gauss's generalization in Theorem 9.26.

Problem 4.23. Prove that, if p is an odd prime, then $\dfrac{p \pm 1}{2}$ are integers and that

$$\left[\left(\frac{p-1}{2}\right)!\right]^2 \equiv (-1)^{\frac{p+1}{2}} \pmod{p}.$$

This shows that, if $p \equiv 1 \pmod{4}$, then there exists an integer x such that $x^2 \equiv -1 \pmod{p}$. We will see the converse when we study quadratic reciprocity.

Lemma 4.24. Suppose n is a positive integer and

$$\{r_1, r_2, \ldots, r_{\varphi(n)}\}$$

is a reduced residue system. If a is an integer such that $\gcd(a, n) = 1$, then

$$\{ar_1, ar_2, \ldots, ar_{\varphi(n)}\}$$

is a reduced residue system as well. Equivalently, we are saying that if we take a representative from each congruence class in $(\mathbb{Z}/n\mathbb{Z})^*$ and multiply each chosen representative by an integer a coprime to n, then the numbers still represent every reduced residue class modulo n, though likely in a different order (like a permutation).

Proof. We will show that for all $i, j \in [\varphi(n)]$, it holds that $(ar_i, n) = 1$, and if $i \neq j$, then $ar_i \not\equiv ar_j \pmod{n}$. Indeed, since $(a, n) = 1$ and $(r_i, n) = 1$, it is true by Problem 1.20 that $(ar_i, n) = 1$. For the second assertion, we will prove the contrapositive. If $ar_i \equiv ar_j \pmod{n}$, then using $(a, n) = 1$, we can cancel a from both sides to get $r_i \equiv r_j \pmod{n}$. Since the r_k form a reduced residue system, they are from distinct residue classes, so we must have $i = j$. ■

Theorem 4.25 (Euler's congruence)**.** Suppose n is a positive integer and a is an integer. Then

$$a^{\varphi(n)} \equiv 1 \pmod{n}$$

if and only if $(a, n) = 1$. As such, if $(a, n) = 1$, then $a^{\varphi(n)-1}$ is an inverse of a modulo n.

Proof. Let n be a positive integer. For one direction, suppose a is an integer that is coprime to n. By Lemma 4.24, if

$$\{r_1, r_2, \ldots, r_{\varphi(n)}\}$$

is a reduced residue system modulo n. then so is

$$\{ar_1, ar_2, \ldots, ar_{\varphi(n)}\}.$$

As a result, the product of the elements of one set is equal to the product of the elements of the other set modulo n, so

$$\prod_{k=1}^{\varphi(n)} r_k \equiv \prod_{k=1}^{\varphi(n)} ar_k \equiv a^{\varphi(n)} \prod_{k=1}^{\varphi(n)} r_k \pmod{n}.$$

All of the r_k can be cancelled from both sides of the congruence because they are coprime to n, which gives us the congruence

$$a^{\varphi(n)} \equiv 1 \pmod{n}.$$

Conversely, suppose this congruence holds and we want to show that $(a, n) = 1$. The congruence implies that there exists an integer k such that

$$a^{\varphi(n)} - kn = 1.$$

Since $\varphi(n) \geq 1$, the first term $a^{\varphi(n)}$ is greater than or equal to a, so (a, n) divides both sides of the equation. As the right side of the equation is 1, we get $(a, n) = 1$.
For the second assertion, if $n \geq 3$, then $\varphi(n) \geq 2$ and so it is easy to see that from Euler's congruence that $a^{\varphi(n)-1}$ is an inverse of a modulo n because

$$a \cdot a^{\varphi(n)-1} \equiv 1 \pmod{n}.$$

In the $n = 1$ and $n = 2$ cases, the only congruence class in which a can lie is the congruence class of 1 because $(a, n) = 1$. In these two cases, $\varphi(n) - 1 = 0$, and $a^0 \equiv 1 \pmod{n}$ is indeed an inverse of a modulo n. Note that this exponential expression $a^{\varphi(n)-1}$ is likely to be more computationally intensive to find, reduce, and work with than finding an inverse using Bézout's lemma and the extended Euclidean algorithm. However, $a^{\varphi(n)-1}$ has the advantage of being a simple algebraic expression in closed form, and therefore potentially more useful in general proofs. ■

Euler's congruence gives us a way of reducing exponents if the base a is coprime to n. Try out the following problem.

Problem 4.26. Suppose n is a positive integer and a is an integer that is coprime to n. Show that, if i and j are integers such that

$$i \equiv j \pmod{\varphi(n)},$$

then

$$a^i \equiv a^j \pmod{n}.$$

Use this idea to find the remainder when 12^{202} is divided by 7.

One can ask if such a reduction result exists for bases a that are not coprime to n. To this end, a result that rarely appears in the literature is the following problem, though it is included as a problem in [13].

Corollary 4.27 (Modified Euler's congruence)**.** If n is a positive integer and a is any integer (not necessarily coprime to n), then

$$a^n \equiv a^{n-\varphi(n)} \pmod{n}.$$

Note that we can multiply both sides of the congruence by powers of a (that have positive exponents) to show that

$$a^k \equiv a^{k-\varphi(n)} \pmod{n}$$

for every integer $k \geq n$. In some cases, an integer $k < n$ maybe also be possible, but this cannot be asserted in general because if n is prime, then it would imply that the exponent on the right side is

$$k - \varphi(n) = k - (n-1) < n - (n-1) = 1,$$

which would not be acceptable if $(n, a) > 1$. The $(a, n) = 1$ case of this extension of Euler implies Euler's congruence.

Proof. We want to show that n divides

$$a^n - a^{n-\varphi(n)} = a^{n-\varphi(n)}(a^{\varphi(n)} - 1).$$

The result is easy for $n = 1$, so we will assume that $n \geq 2$ as this will allow us to use the prime factorization of n,

$$n = p_1^{e_1} p_2^{e_2} \cdots p_m^{e_m}.$$

It is equivalent to show that each $p_i^{e_i}$ divides $a^{n-\varphi(n)}(a^{\varphi(n)} - 1)$ because the maximal prime powers pi^{e_i} are pairwise coprime. We will deal with two cases: $p_i \nmid a$ or $p_i \mid a$. In the first case, we may apply Euler's congruence to get

$$a^{\varphi(n)} \equiv a^{\varphi(p_i^{e_i})\varphi\left(\frac{n}{p_i^{e_i}}\right)} \equiv 1^{\varphi\left(\frac{n}{p_i^{e_i}}\right)} \equiv 1 \pmod{p_i^{e_i}}.$$

So in this case, $p_i^{e_i}$ divides $a^{\varphi(n)} - 1$. If $p_i \mid a$, then we would like to show that $p_i^{e_i}$ divides the other factor $a^{n-\varphi(n)}$. It suffices to show that $n - \varphi(n) \geq e_i$ because each copy of the base a contains at least one factor equal to p_i by the assumption $p_i \mid a$. We apply a combinatorial argument: the definition of $\varphi(n)$ is the number of elements of $[n]$ that are coprime to n, so $n - \varphi(n)$ counts the number of elements of $[n]$ that are *not* coprime to n. Since $p_i, p_i^2, \ldots, p_i^{e_i}$ are e_i elements of $[n]$ that are not coprime to a due to the assumption $p_i \mid a$, the inequality

$$n - \varphi(n) \geq e_i$$

holds.
If $(a, n) = 1$, then we can multiply both sides of the congruence by $a^{\varphi(n)-n}$, where the negative exponent is acceptable because a is coprime to n, to get $a^{\varphi(n)} \equiv 1 \pmod{n}$. This is Euler's congruence, albeit by circular logic, since we used Euler to self-strengthen into its own generalization. ■

Corollary 4.28 (Fermat's little theorem)**.** Suppose p is a prime and a is an integer. If $p \nmid a$, then

$$a^{p-1} \equiv 1 \pmod{p}.$$

Equivalently, if a is any integer, then $a^p \equiv a \pmod{p}$. Moreover, if $p \nmid a$, then a^{p-2} is an inverse of a modulo p.

Proof. This is a direct consequence of Euler's congruence (Theorem 4.25) and its modified variation (Corollary 4.27) because $\varphi(p) = p - 1$ for primes p. ■

Definition 4.29. The contrapositive of Fermat's little theorem states that: "Suppose a and $n \geq 2$ are integers. If

$$a^{n-1} \not\equiv 1 \pmod{n},$$

then $n \mid a$ or n is composite." So if $a^{n-1} \not\equiv 1 \pmod{n}$ and $n \mid a$, then n is composite, in which case a is said to be a **Fermat witness** to the fact that n is composite.

Definition 4.30. The (untrue) converse of Fermat's little theorem states that: "Suppose a and $n \geq 2$ are integers. If

$$b^{n-1} \equiv 1 \pmod{n},$$

then $n \nmid b$ and n is prime." It is certainly true that $n \nmid b$ in this case, thanks to the congruence in the hypothesis and Bézout's lemma, but there are counterexamples to the assertion that n must be prime. If $b^{n-1} \equiv 1 \pmod{n}$ yet n is composite, then b is called a **Fermat liar** and n is called a **Fermat pseudoprime** to base b. In fact, there exist (infinitely many) composite integers n such that, for *all* integers b coprime to n,

$$b^{n-1} \equiv 1 \pmod{n}.$$

Such n are called **Carmichael numbers**. In other words, an integer $n \geq 2$ is a Carmichael number if and only if n is a Fermat pseudoprime to base b for all integers b that are coprime to n.

Problem 4.31. Show that $561 = 3 \cdot 11 \cdot 17$ is a Carmichael number. This is the smallest Carmichael number, though there is no need for the reader to prove this minimality property.

Korselt's criterion (Theorem 9.28) is a biconditional condition for identifying Carmichael numbers.

Problem 4.32. At the time of writing, Lehmer's totient problem in an unsolved problem in number theory that which asks whether there exists a composite integer n such that $\varphi(n) \mid n - 1$. Prove that if such an n exists, then it is a Carmichael number.

Chapter 5

Diophantine Analysis

> "It is impossible to separate a cube into two cubes, or a fourth power into two fourth powers, or in general, any power higher than the second, into two like powers. I have discovered a truly marvelous proof of this, which this margin is too narrow to contain."
>
> – *Pierre de Fermat*

Across mathematics, there are scenarios in which it is desirable to find solutions to multivariable equations in the integers or rationals. When such discrete solutions are required, the equation is called a Diophantine equation. We begin the study of Diophantine analysis with a kind of equation that can be arranged so that one side is a factored expressed with the other side equal to a constant. We will then develop the "modular arithmetic contradiction trick" to prove the non-existence of solutions to a polynomial Diophantine equation by reducing the equation to a congruence in a specially chosen modulus. Then we will use slopes from Cartesian geometry to classify all positive integer triples that satisfy the equation from the Pythagorean theorem. Finally, we will end with a technique called infinite descent that will allow us to solve a case of Fermat's last theorem.

5.1 Fudging and Factoring

Definition 5.1. A **Diophantine equation** is a multivariable equation such that we seek only the integer solutions. The definition is flexible because sometimes solutions from a different subset of the real (or possibly complex) numbers are sought, such as the rationals or only the positive integers. The equation is usually composed of arithmetic operations on the variables, occasionally including exponentiation. The most common Diophantine equations are polynomials, though it is not uncommon to have variables as a part of an exponent.

Example. **Elliptic curves** are Diophantine equations of the form

$$y^2 = x^3 + ax + b$$

for constants a and b, where the right side is called a "depressed cubic." If $a = 0$ and b is a non-zero integer, then it is called a **Mordell curve**. Elliptic curves are important in modern cryptography.

Diophantine equations are named after Diophantus of Alexandria, who studied them in ancient Greece. Let us look at some famous examples of Diophantine equations whose solution sets have been completely found.

Theorem 5.2 (Fermat's last theorem)**.** There exists no triple of positive integers (a, b, c) and an integer $n \geq 3$ such that

$$a^n + b^n = c^n.$$

Fermat's last theorem is the most famous of all Diophantine equations and perhaps the most famous mathematical problem in history. Despite stupendous efforts, it took over 350 years after it was conjectured (or rather, Fermat claimed that he found a proof, without leaving a record) for a correct proof to emerge. The main mathematician behind the proof was Andrew Wiles.

Theorem 5.3 (Catalan's conjecture)**.** The only solution to

$$x^a - y^b = 1$$

with integers $a, b > 1$ and integers $x, y > 0$ is

$$3^2 - 2^3 = 1.$$

So no two other perfect powers are consecutive integers.

Catalan's conjecture now a proven theorem, thanks to Preda Mihăilescu, and it took *only* 158 years after it was conjectured!

Theorem 5.4 (Pell's equation)**.** If $D \geq 2$ is an integer, then the equation

$$x^2 - Dy^2 = 1$$

has an integer solution (x, y) with $y \neq 0$. This allows us to assert the existence of a solution (x_1, y_1) with the minimal positive y-coordinate. Then all positive solutions (x_k, y_k) can be generated as

$$x_k + y_k\sqrt{D} = (x_1 + y_1\sqrt{D})^k,$$

where we expand the right side and collect like terms to form the unique expression on the left side for each positive integer k. There are variants of this equation that correspond to replacing the constant 1 on the right side by other integers such as -1.

A problem-based book dedicated to Pell's equation was authored by my friend and mentor, Dr. Edward Barbeau [3].
Standard questions pertaining to the analysis of a Diophantine equation include:

- Do there exist any solutions?
- Are there finitely many solutions or infinitely many?
- Can a closed formula or any kind of formula be found that generates all solutions?
- If there is no known way of capturing all solutions in closed form, can an infinite family of solutions be parametrized, possibly in polynomial or recursive form?
- Can an algorithm be written to produce all solutions such that it is more efficient than simply plugging in all possible inputs and checking if the equation is satisfied?

One of the most effective elementary techniques for solving Diophantine equations is to rearrange the terms so that one side of the equation is the product of $k \geq 2$ expressions $f_1 \cdot f_2 \cdots f_k$, where each factor represents an integer and the other side of the equation is an integer constant c. Upon determining the prime factorization of c, casework can be done on all possible k-tuples of integers $(f_1, f_2, \ldots, f_k)$ such that

$$f_1 \cdot f_2 \cdots f_k = c.$$

This involves solving systems of equations. There is no guarantee that this will produce all, or any, solutions as the practical value of this method depends on the complexity (or rather, simplicity) of the factors f_i, meaning how the variables within each expression f_i are structured. As k increases, the number of k-tuples increases, making the casework more tedious. While studying combinatorial compositions in Volume 2, we computed the exact number of k-tuples $(f_1, f_2, \ldots, f_k)$ in terms of the multiplicities in the prime factorization of c.

Example 5.5. If p is a fixed odd prime, then determine all pairs of integers (x, y) such that $x^2 - y^2 = p$, in terms of p.

Solution. By the difference of squares factorization, we want to solve

$$(x - y)(x + y) = p.$$

If (x, y) is an integer solution, then $x - y$ and $x + y$ are both integers. The only pair of integers that multiply to the prime p are

$$(1, p), (p, 1), (-1, -p), (-p, -1).$$

Note that we are even looking at permutations of the same factors of p but sprinkled across different factors on the left side so that, for example, $(1, p)$ and $(p, 1)$ require separate consideration. So order matters. Moreover, forgetting negative factors is a common mistake when using this method; even if we are seeking only positive solutions, negative factors can lead to them. Now, we could solve each case separately, but it is more efficient to solve them simultaneously via a general system of equations that satisfies all of the equations. If (a, b) is a pair of integers satisfying

$$(x - y, x + y) = (a, b),$$

then

$$(x, y) = \left(\frac{b + a}{2}, \frac{b - a}{2} \right).$$

Concisely written, the possible pairs are

$$\left(\pm \frac{p + 1}{2}, \pm \frac{p - 1}{2} \right),$$

where the two $\pm$ signs are independent of each other. These coordinates are indeed integers because p is odd. In this case, the factors were simple and every solution found works. However, extraneous solutions can sometimes exist, so it is a good idea to check if the solutions found via this method actually work and are within the desired domain of numbers, or to use only reversible steps during the process like we did. ■

Definition 5.6. In a Diophantine equation, the question comes up of "how much" of the constant term should be strategically placed on each side of the equation in order to induce a factorization on one side with the other side being a constant. There is not always an answer and, when there is an answer, it is not always to place the entire constant on one side. Placing constants on each side of the equation to include this kind of factoring is called **fudging**.

Theorem 5.7. The most common instances of fudging revolve around the factorization

$$(ax+b)(cy+d) = (ac)xy + (ad)x + (bc)y + bd.$$

Some of the coefficients can often be taken to be ± 1, such as

$$\begin{aligned} xy + x + y &= (x+1)(y+1) - 1, \\ xy - x - y &= (x-1)(y-1) - 1. \end{aligned}$$

Sometimes, it is fruitful to multiply through by a constant before fudging, such as

$$\begin{aligned} cxy + ax + by = d &\iff c^2xy + cax + cby = cd \\ &\iff c^2xy + cax + cby + ab = ab + cd \\ &\iff (cx+b)(cy+a) = ab + cd. \end{aligned}$$

Problem 5.8. Let p be a fixed prime. In terms of p, determine all integers n such that $n-p$ divides n.

Fudging and factoring was useful when we classified the Platonic solids and determined their features using planar graph theory in Volume 2, by an argument of Coxeter.

5.2 Choosing a Special Modulus

There is a technique that is sometimes possible to use to prove that a polynomial Diophantine equation has no integer solutions. As a reminder, integer polynomial equations have the form

$$a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 = 0,$$

or rearrangements of such an equation, where the a_i are integers. This technique is perhaps best introduced by an illuminating example.

Example 5.9. Find all integer solutions (x, y) of

$$x^3 - 117y^3 = 5.$$

Solution. This Diophantine equation was mentioned in a 1969 paper by Lewis who said it "is known to have at most 18 integral solutions but the exact number is unknown." The equation was investigated in at least one other paper using advanced methods until Udrescu pointed out the trick below. For references to these papers, see [12].

Suppose (x, y) is an integer solution. The coefficient 117 factors as $3^2 \cdot 13$. Modulo the factor 9, the equation reduces to

$$x^3 \equiv 5 \pmod{9}.$$

The possible residue classes resulting from cubing integers and reducing modulo 9 are:

$$\begin{aligned} 0^3 \equiv 3^3 \equiv 6^3 \equiv 0 \pmod{9}, \\ 1^3 \equiv 4^3 \equiv 7^3 \equiv 1 \pmod{9}, \\ 2^3 \equiv 5^3 \equiv 8^3 \equiv 8 \pmod{9}. \end{aligned}$$

None of these are 5, so there can be no integer solutions to the original Diophantine equation. As Lewis also stated in his paper, "As you might expect, there is some artistry in choosing the appropriate modulus." ■

In general, we can try to reduce a polynomial Diophantine equation modulo a special modulus n. If there are m variables remaining in the reduced expression (after some coefficients have possibly disappeared), we can substitute all n^m possible assignments of residues into the variables and check if the congruence is ever satisfied. If not, then there can be no integer solutions to the original equation. To the best of our knowledge, there is no commonly used name for this method, nor is there a deterministic way of finding an excellent modulus in which to implement this method for a particular equation. We will refer to the method as the "modular arithmetic contradiction trick." Thankfully, it is possible to provide two heuristics for choosing the modulus:

- Coefficients: Find the prime factorization of the coefficients of the terms in the polynomial expression (these are the aforementioned a_i). Choose a modulus that is a common factor of several or many of the coefficients. This will cause those terms to disappear. Annihilating terms means less computation in the step where residue assignments are substituted into variables. If there are large exponents, it might be possible to reduce them using the modified Euler's congruence (Corollary 4.27).

- Exponents: If the equation has been arranged to have a polynomial on the left side and a constant (like zero) on the right side, then the idea is to choose a modulus in which the total number of residues classes that can be occupied by the polynomial is small compared to the modulus. In some naïve sense of probability, this should reduce the chances of the residue class on the left coinciding with the residue class of the constant on the right, thereby preventing a collision and allowing the contradiction technique to work. Finding such a modulus *a priori* can be difficult practically, so we can instead focus on particular terms x^k and think about moduli for which they occupy very few residue classes. Restricting the residue classes of specific terms is not sufficient to restrict the residue classes of the whole polynomial, but it is necessary because the number of residue classes of a polynomial is equal to at least the number of residue classes of each of its terms. Euler's congruence and Fermat's little theorem can help here, and as we will see in Theorem 5.11, so can Sophie Germain primes, which are defined below. This heuristic can also be used to avoid moduli that allow the polynomial or its terms to occupy too many residue classes.

Combining the above heuristics, if we can pick a modulus in which many terms disappear and the remaining terms fall into a small number of residue classes each, then there is hope of never fulfilling the congruence. Picking the right modulus is not yet a science, but one should seek a confluence of factors. As the famed investor Charlie Munger would put it, we want a "lollapalooza effect."
Here are some common applications of the second heuristic for the modular arithmetic contradiction trick:

- The squares modulo 8 are $0, 1, 4$.
- The cubes modulo 9 are $-1, 0, 1$.
- The fourth powers modulo 20 are $0, 1, 5, 16$.
- The fifth powers modulo 11 are $-1, 0, 1$.

The example with fifth powers can be generalized using Sophie Germain primes as follows.

Definition 5.10. If p is a positive integer such that p and $2p+1$ are both primes, then p is called a **Sophie Germain prime** and $2p+1$ is called the corresponding **safe prime**. It is unknown if there are infinitely many Sophie Germain primes. The first few are:

$$2, 3, 5, 11, 23, 29, 41, 53, 83, 89, \ldots$$

Theorem 5.11. If p is a Sophie Germain prime, then an integer a is the residue of a p^{th} power modulo the corresponding safe prime $2p+1$ if and only if the residue of a modulo $2p+1$ is one of $-1, 0, 1$.

Proof. Suppose p is a Sophie Germain prime. If the safe prime $2p+1$ divides a, then $a^p \equiv 0 \pmod{2p+1}$. For every integer a such that $2p+1$ does not divide a, Fermat's little theorem gives

$$a^{2p} \equiv 1 \pmod{2p+1}.$$

Equivalently,

$$a^p \equiv \pm 1 \pmod{2p+1}.$$

So the only possible residues of p^{th} powers modulo $2p+1$ are $0, \pm 1$.
Now we will show that each of these three possibilities is always achievable. As we have already shown, 0 is achievable. It is always possible to achieve 1 because

$$1^p \equiv 1 \pmod{2p+1}.$$

Finally, for -1 we do casework on $p = 2$ versus odd primes p. If $p = 2$, then

$$2^2 \equiv 4 \equiv -1 \pmod{2 \cdot 2 + 1}.$$

If p is an odd Sophie Germain prime, then

$$(-1)^p \equiv -1 \pmod{2p+1}.$$

■

Problem 5.12. Prove that there exist no integers x and y such that

$$x^6 = 6y^3 + 5.$$

Problem 5.13. Find all triples of integers (n, m, k) such that

$$\binom{m}{4} = n^2 + 2 + 7k.$$

5.3 Rational Slopes

If a and b are the legs of a right triangle and c is the hypotenuse, then the Pythagorean theorem says that

$$a^2 + b^2 = c^2.$$

An ancient problem asks what triples of positive integers (a, b, c), such as $(3, 4, 5)$, satisfy this equation. In addition to geometric reasons, it is historically interesting to consider this problem because it is the second degree analogue of Fermat's last theorem.

Definition 5.14. A **Pythagorean triple** is an ordered triple of positive integers (a, b, c) such that $a^2 + b^2 = c^2$. Note that a Pythagorean triple can be scaled up by a positive integer factor k to produce another Pythagorean triple (ka, kb, kc). In the other direction, if a Pythagorean triple (a, b, c) cannot be scaled down, meaning $\gcd(a, b, c) = 1$, then (a, b, c) is said to be a **primitive** Pythagorean triple. Each Pythagorean triple is either primitive or a scaled up version of one. As an important side note, $\gcd(a, b, c) = 1$ for a Pythagorean triple (a, b, c) if and only if a, b, c are pairwise coprime because the equation $a^2 + b^2 = c^2$ implies that any common factor of two of the three numbers must also divide the third number.

Example. It is a good idea to memorize the smaller Pythagorean triples. Some common primitive ones are:

$$\begin{array}{ll} (3, 4, 5), & (8, 15, 17), \\ (5, 12, 13), & (12, 35, 37), \\ (7, 24, 25), & (20, 21, 29). \\ (9, 40, 41), & \\ (11, 60, 61), & \end{array}$$

See if you can find a pattern in the left column.

Problem 5.15 (Euclid's formula). Show that, for any positive integers m and n such that $m \geq n$, a Pythagorean triple is given by

$$(m^2 - n^2, 2mn, m^2 + n^2).$$

Show that this does not parametrize all Pythagorean triples by finding a Pythagorean triple that is not captured by this formula. To avoid a trivial example, make sure to place an even integer in the second entry; for example, $(4, 3, 5)$ is a trivial example of a Pythagorean triple that is not captured by the formula.

Problem 5.16. In the examples below Definition 5.14, we placed the Pythagorean triples (a, b, c) in two columns so that $c = b + 1$ in each example in the left column. Prove that (a, b, c) is such a triple if and only if there exists a positive integer k such that

$$(a, b, c) = (2k + 1, 2k(k + 1), 2k(k + 1) + 1).$$

Note that the k must be unique since it can be isolated in terms of a as $k = \dfrac{a-1}{2}$.

Now we turn to the general problem of parametrizing all primitive Pythagorean triples uniquely. As a result, we will be able to uniquely parametrize *all* Pythagorean triples as well by scaling up the primitive ones by positive integer factors.

Theorem 5.17 (Parametrization of primitive Pythagorean triples)**.** If (a, b, c) is a primitive Pythagorean triple, then exactly one of a or b is even. Choosing b to be the even one, there exist unique positive integers t and s such that $t > s$ and

$$(a, b, c) = (t^2 - s^2, 2ts, t^2 + s^2).$$

These t and s turn out to be coprime and of different parity. Conversely, if t and s are positive coprime integers of different parity such that $t > s$, then $(t^2 - s^2, 2ts, t^2 + s^2)$ is a primitive Pythagorean triple where $2ts$ is the even entry.

Proof. There is more than one way to prove this result. We will show the least ad hoc method because it can be applied to a larger class of second degree equations. The basic idea is to transform the homogeneous Pythagorean equation into an inhomogeneous one,

$$a^2 + b^2 = c^2 \longrightarrow x^2 + y^2 = 1,$$

and then find all of the *rational* solutions of the new equation using the Cartesian geometry of the curve. Let us begin.

If (a, b, c) satisfies $a^2 + b^2 = c^2$, then $\left(\dfrac{a}{c}\right)^2 + \left(\dfrac{b}{c}\right)^2 = 1$. Since $(a, c) = (b, c) = 1$, the fractions $\dfrac{a}{c}$ and $\dfrac{b}{c}$ are in lowest form. If we could find every pair of rational numbers (x, y) such that $x^2 + y^2 = 1$, then we can analyze how x and y look when each has a numerator and a denominator that are coprime.

Note that $(-1, 0)$ is a rational solution to $x^2 + y^2 = 1$. Moreover, if (x, y) is a different rational point on this curve, then the slope of the line through $(-1, 0)$ and (x, y) is $\dfrac{y}{x+1}$, which is rational; we do not have to worry about the denominator being 0 because the curve $x^2 + y^2 = 1$ is a circle which has no other points at $x = -1$ and so the line in question is non-vertical. The key insight at this step is that the converse holds: we claim that if a line of rational slope r goes through $(-1, 0)$, then it intersects the circle at exactly one other point, and this point happens to have rational coordinates. We will find these coordinates now. The equation of the line is

$$\frac{y - 0}{x + 1} = r \implies y = rx + r.$$

Substituting this into $x^2 + y^2 = 1$ and isolating x using the quadratic formula yields

$$x = \frac{-r^2 \pm 1}{1 + r^2},$$

where we can choose the $\dfrac{1 - r^2}{1 + r^2}$ option because the other option gives the generating point $(-1, 0)$. Then

$$(x, y) = (x, rx + r) = \left(\frac{1 - r^2}{1 + r^2}, \frac{2r}{1 + r^2} \right).$$

By iterating over all rational r, this formula generates all rational points on the circle $x^2+y^2 = 1$, other than $(-1, 0)$. Let $r = \dfrac{s}{t}$, where s and t are coprime integers. Then

$$(x, y) = \left(\frac{1 - \left(\frac{s}{t}\right)^2}{1 + \left(\frac{s}{t}\right)^2}, \frac{2 \cdot \frac{s}{t}}{1 + \left(\frac{s}{t}\right)^2} \right) = \left(\frac{t^2 - s^2}{t^2 + s^2}, \frac{2ts}{t^2 + s^2} \right).$$

Remembering how we went from the original homogeneous equation to the circle curve, this means that for every Pythagorean triple (a, b, c), there exist coprime integers s and t such that

$$\left(\frac{a}{c}, \frac{b}{c} \right) = \left(\frac{t^2 - s^2}{t^2 + s^2}, \frac{2ts}{t^2 + s^2} \right).$$

To make $\dfrac{b}{c}$ positive, st must be positive and so s and t must both be positive or both be negative; we can choose them to both be positive since the negative choice does not change the coordinates (a, b, c). Moreover, to ensure that $\dfrac{a}{c}$ is positive, it must be true that $t > s$.

Now we will work on showing that the fractions $\dfrac{t^2 - s^2}{t^2 + s^2}$ and $\dfrac{2ts}{t^2 + s^2}$ are in lowest form so that we can relate the numerators $t^2 - s^2$ and $2ts$ and denominator $t^2 + s^2$ to (a, b, c). We start with showing that t and s cannot have the same parity. It is not possible for t and s to both be even because they are coprime. If t and s were both odd, then both the numerator and denominator of $\dfrac{2ts}{t^2 + s^2}$ are even, so we can write it as $\dfrac{st}{\left(\frac{t^2+s^2}{2}\right)}$. Since $\dfrac{b}{c}$ is the least form of the same fraction, b must divide st, which is impossible since we chose b to be even. Thus, both t, s cannot be odd. So t and s have opposite parity, which makes $t^2 + s^2$ odd. Since t and s are defined to be coprime, we can deduce from the faux-Euclidean algorithm that

$$\begin{aligned}(t^2 - s^2, t^2 + s^2) &= (2t^2, t^2 + s^2) = (t^2, t^2 + s^2) \\ &= (t^2, s^2) = (t, s) = 1,\end{aligned}$$

where we used a power divisibility lemma (Lemma 2.23) at the end. This means both sides of $\dfrac{a}{c} = \dfrac{t^2 - s^2}{t^2 + s^2}$ are the lowest forms of the same rational number, so $a = t^2 - s^2$ and $c = t^2 + s^2$ and $b = c \cdot \dfrac{2ts}{t^2 + s^2} = 2ts$.

To prove uniqueness, suppose α and β are positive integers such that

$$(t^2 - s^2, 2ts, t^2 + s^2) = (a, b, c) = (\alpha^2 - \beta^2, 2\alpha\beta, \alpha^2 + \beta^2).$$

Then

$$t^2 = \frac{c + a}{2} = \alpha^2 \implies t = \alpha,$$
$$s^2 = \frac{c - a}{2} = \beta^2 \implies s = \beta,$$

since t, s, α, β are all positive. This proves uniqueness.
Conversely, we know from Euclid's formula that

$$(t^2 - s^2, 2ts, t^2 + s^2)$$

forms a Pythagorean triple. If t and s are coprime and of opposite parity, then we showed a moment earlier than $\gcd(t^2 - s^2, t^2 + s^2) = 1$, so

$$\gcd(t^2 - s^2, 2ts, t^2 + s^2) = 1$$

as well, making this Pythagorean triple a primitive one. ■

This geometric method works for other two-variable quadratic Diophantine equations when we are seeking rational solutions, as long as we can guess one rational solution that can then be used as a generator for all other rational solutions. However, we are unaware of whether this method *always* works whenever one solution can be guessed, so the reader should take care to verify that every step logically follows in any specific implementation of this technique. Note that, even if we are asked for only integer solutions, it can be effective to find all rational solutions and then determine in which cases the denominators in the solution exactly divide the corresponding numerators. This just might be easier than directly finding all integer solutions, because rational numbers have the advantage of forming a field and fields allow for division without remainder.

5.4 Infinite Descent

Infinite descent is a form of proof by contradiction that exploits the well-ordering principle, and equivalently the principle of induction. Its two equivalent forms are as follows. Let

$$P(1), P(2), P(3), \ldots$$

be a sequence of mathematical statements. Assume that the set

$$\{P(i) : i \in \mathbb{Z}_+, P(i) \text{ is true}\}$$

is non-empty. Then there are two equivalent ways of formulating the infinite descent technique:

- By the well-ordering principle, there must exist a minimal positive integer k such that $P(k)$ is true. Find a positive integer j such that $P(j)$ is true, yet $j < k$, where the proof usually uses $P(k)$ and its supposed minimality. This contradicts the minimality of $P(k)$, so none of the $P(i)$ are true.

- Show that, if k is a positive integer such that $P(k)$ is true, then there exists a positive integer j such that $j < k$ and $P(j)$ is true. By induction, this means that there is an infinite monotonically decreasing (hence, the term "infinite descent") sequence of positive integer indices at which the $P(i)$ are true. This contradicts the fact that the positive integers are bounded below, so none of the $P(i)$ are true.

In particular, infinite descent can be used as a method of proving that a Diophantine equation has no solutions outside of a certain class. Typically, this means that we have to:

1. Cordon off certain solutions, which are usually trivial in some sense, like having variables equal to 0.

2. Show that the non-trivial solutions that potentially exist, under some countable ordering that causes them to be bounded below in this ordering, leads to a contradiction of the infinite descent type.

So, while the modular arithmetic contradiction trick asserts the non-existence of any solution whatsoever, infinite descent often only states that there are no non-trivial solutions. This is not much of a drawback because we can simply manually check whether there are solutions corresponding to variables equal to 0 or whatever else "trivial" means for a specific Diophantine equation. With the generalities out of the way, let us see an example. Note that we will make use of some of the power divisibility lemmas (Lemma 2.23).

Example 5.18 (Quartic Fermat's last theorem)**.** If (x, y, z) is a triple of integers such that $x^4 + y^4 = z^2$, then $xyz = 0$, which is equivalent to saying that at least one of the three variables is equal to 0. As a consequence, this establishes Fermat's last theorem for degree four, since fourth powers are covered by the square z^2.

Solution. Suppose, for the sake of contradiction that a solution to $x^4 + y^4 = z^2$ exists where none of x, y, z are zero. Since each variable is taken to an even power, we may assume that a solution exists where x, y, z are all positive. By the well-ordering principle, there exists a solution (x, y, z) where z is minimal since it is bounded below by 1. Note that (x^2, y^2, z) is a Pythagorean triple. If we could show that it is a primitive triple, then we could use the parametrization of primitive Pythagorean triples (Theorem 5.17). Let $\gcd(x, y, z) = d$ and let x_0, y_0, z_0 be the quotients of dividing x, y, z respectively by d. Then the equation becomes

$$(dx_0)^4 + (dy_0)^4 = (dz_0)^2 \implies d^2x_0^4 + d^2y_0^4 = z_0^2.$$

Then $d^2 \mid z_0^2$ and so $d \mid z_0$. Letting z_1 be the integer such that $dz_1 = z_0$ turns the equation into

$$d^2x_0^4 + d^2y_0^4 = (dz_1)^2 \implies x_0^4 + y_0^4 = z_1^2.$$

So (x_0, y_0, z_1) is a solution to the original equation where $z_1 = \dfrac{z_0}{d} = \dfrac{z}{d^2}$, which is a strictly smaller integer than z, unless $d = 1$. To prevent contradicting the minimality of z, it must be true that $\gcd(x, y, z) = 1$, which makes (x^2, y^2, z) a primitive Pythagorean triple.
Thanks to the symmetry of x and y in the equation $x^4 + y^4 = z^2$, we may assume without loss of generality that x^2 is odd and y^2 is even. By the parametrization of all primitive Pythagorean triples, there exist coprime positive integers t and s of opposite parity such that $t > s$ and

$$\begin{aligned} x^2 &= t^2 - s^2, \\ y^2 &= 2ts, \\ z &= t^2 + s^2. \end{aligned}$$

If t is even and s is odd, then

$$x^2 = t^2 - s^2 \equiv -1 \equiv 3 \pmod 4,$$

which is impossible because a square can only be 0 or 1 modulo 4. So t is odd and s is even. Since $y^2 = 2ts = t(2s)$ and $(t, 2s) = (t, s) = 1$, there exist coprime positive integers a, b_0 such that $t = a^2$ and $2s = b_0^2$. Then there exists an integer b such that $b_0 = 2b$, so $2s = b_0^2$ becomes $s = 2b^2$ after some reduction. This means

$$x^2 = t^2 - s^2 = (a^2)^2 - (2b^2)^2.$$

Again, $(x, 2b^2, a^2)$ is a Pythagorean triple. Since $(a, b) = 1$, it then holds that $(2b^2, a^2) = (b^2, a^2) = 1$, so the triple is primitive. Again by the parametrization of primitive Pythagorean triples, there exist coprime positive integers c, d with opposite parity such that

$$(x, 2b^2, a^2) = (c^2 - d^2, 2cd, c^2 + d^2).$$

The fact that $b^2 = cd$ means that c and d are coprime squares. So $c = v^2$ and $d = w^2$ for some positive integers v and w. This means

$$a^2 = c^2 + d^2 = v^4 + w^4$$

solves the original equation. However,

$$a \leq a^2 = t \leq t^2 < t^2 + s^2 = z,$$

which contradicts the minimality of z. This is our infinite descent contradiction, and so at least one of x, y, z must be 0 if the equation $x^4 + y^4 = z^2$ holds.
Subsequently, there are no positive integers (x, y, z) such that $x^4 + y^4 = z^4$, since $z^4 = (z^2)^2$, which proves the fourth degree case of Fermat's last theorem. This proof shows how infinite descent proofs, or solutions to Diophantine equations, or even elementary number theoretic proofs in general, can be idiosyncratic. It is difficult to project a general structure to Diophantine analysis, other than by outlining some common methods as we have done. ■

Problem 5.19. Find all ordered triples of integers (x, y, z) such that $6x^2 + 2y^2 = z^2$.

While infinite descent typically derives a contradiction by finding a value of one of the variables in the equation that is smaller than a presumed minimum value of the variable, it is not necessary that a variable itself is the object of minimization. Any function of the variables (such as the sum of the variables) is equally valid as a quantity whose minimum we wish to contradict. As shown in the following example, **Vieta jumping** produces the contradictory solution through Vieta's formulas for quadratics.

Example 5.20. Note that $\dfrac{1^2+1^2+1}{1\cdot 1} = 3$. Prove that, in general, if $(x, y) \in \mathbb{Z}_+^2$ such that $xy \mid x^2+y^2+1$, then

$$\frac{x^2+y^2+1}{xy} = 3.$$

Solution. Suppose $\dfrac{x^2+y^2+1}{xy} = k \neq 3$ has a positive integer solution (x, y, k). Let $(x, y) = (a, b) \in \mathbb{Z}_+^2$ be a solution to $\dfrac{x^2+y^2+1}{xy} = k$ that minimizes $x + y$. Due to the symmetry of x and y in this equation, we may assume without loss of generality that $a \geq b$. Suppose, for contradiction, that $a = b$. Then

$$\frac{2a^2+1}{a^2} = k \implies 1 = (k-2)a^2,$$

which forces

$$k-2 \mid 1 \implies k-2 = 1 \implies k = 3,$$

which contradicts our assumption that $k \neq 3$. So we know that $a > b$ or, equivalently, $a \geq b+1$.
Now we manipulate

$$\begin{aligned}\frac{x^2+y^2+1}{xy} = k &\implies x^2+y^2+1 = kxy \\ &\implies x^2+(-ky)x+(y^2+1) = 0.\end{aligned}$$

For $y = b$, a solution to the quadratic

$$x^2+(-kb)x+(b^2+1) = 0$$

is $x = a$. There must exist a second solution $x = c \in \mathbb{C}$ such that, by Vieta's formulas,

$$\begin{aligned}a+c &= kb, \\ ac &= b^2+1.\end{aligned}$$

The former proves that

$$c = kb-a \in \mathbb{Z}$$

and the latter proves that

$$c = \frac{b^2+1}{a} > 0$$

(note that a is positive, so we were able to divide by this non-zero quantity), so $c \in \mathbb{Z}_+$. We will prove that the solution $(x, y) = (c, b)$ undercuts $(x, y) = (a, b)$ by satisfying

$$c + b < a + b.$$

Working backwards, this is equivalent to

$$c < a \iff \frac{b^2 + 1}{a} < a \iff b^2 + 1 < a^2.$$

This is contradicted by the fact that

$$a \geq b + 1 \implies a^2 \geq (b + 1)^2 = b^2 + 2b + 1 > b^2 + 1.$$

Thus, $k \neq 3$ is impossible, forcing $k = 3$. ■

Problem 5.21. Note that $\dfrac{2^2 + 1^2}{2 \cdot 1 - 1} = 5$. Prove that, in general, if $(x, y) \in \mathbb{Z}_+^2$ such that $xy \neq 1$ and $xy - 1 \mid x^2 + y^2$, then

$$\frac{x^2 + y^2}{xy - 1} = 5.$$

Chapter 6

Linear Diophantine Equations

> "At the beginning of this century a self-destructive democratic principle was advanced in mathematics (especially by Hilbert), according to... the value of a mathematical achievement is determined, not by its significance and usefulness as in other sciences, but by its difficulty alone, as in mountaineering. This principle quickly led mathematicians to break from physics and to separate from all other sciences. In the eyes of all normal people, they were transformed into a sinister priestly caste... Bizarre questions like Fermat's problem or problems on sums of prime numbers were elevated to supposedly central problems of mathematics."
>
> – *Vladimir Arnold, The Mathematical Intelligencer*

Diophantine equations come in many forms. We have seen some of the basic techniques for analyzing them, but innumerable other equations remain that are not amenable to these methods. We will now study Diophantine equations that correspond to linear equations and systems of linear equations, as well as a variation called the Frobenius coin problem that replaces the linear combinations in Bézout's lemma with conical combinations.

6.1 Bézout Revisited

Definition 6.1. A **linear Diophantine equation** is

$$ax + by = c,$$

where a, b, c are fixed integers such that both of a, b are non-zero and x, y are variables that represent integers. This definition can be generalized to equations with more variables, but we will not be looking at such equations for the most part.

Theorem 6.2 (Classification of solutions to linear Diophantine equations)**.** A linear Diophantine equation $ax+by = c$ has a solution (x, y) in the integers if and only if c is a multiple of $\gcd(a, b)$. Such a solution can be found using the extended Euclidean algorithm. If (x_1, y_1) is one solution, then all solutions can be generated from it as

$$\left(x_1 - k \cdot \frac{b}{(a,b)}, y_1 + k \cdot \frac{a}{(a,b)}\right)_{k \in \mathbb{Z}}$$

Proof. The assertion about existence is a part of Bézout's lemma (Theorem 1.16). As we know, the extended Euclidean algorithm (Theorem 1.30) provides one solution. So all we have to do is generate all solutions using one solution. Suppose (x_1, y_1) is a solution. We will show that (x_2, y_2) is a solution if and only if there exists an integer k such that

$$(x_2, y_2) = \left(x_1 - k \cdot \frac{b}{(a,b)}, y_1 + k \cdot \frac{a}{(a,b)} \right).$$

In one direction, it is easy to verify that all such points are solutions because, for any integer k,

$$\begin{aligned} ax_2 + by_2 &= a\left(x_1 - k \cdot \frac{b}{(a,b)} \right) + b\left(y_1 + k \cdot \frac{a}{(a,b)} \right) \\ &= ax_1 + by_1 = c. \end{aligned}$$

In the other direction, if it holds that $ax_2 + by_2 = c$, then subtracting it from $ax_1 + by_1 = c$ yields

$$a(x_1 - x_2) = b(y_2 - y_1).$$

Equivalently,

$$\frac{a}{(a,b)} \cdot (x_1 - x_2) = \frac{b}{(a,b)} \cdot (y_2 - y_1).$$

Since $\frac{a}{(a,b)}$ and $\frac{b}{(a,b)}$ are coprime, $\frac{a}{(a,b)}$ divides $y_2 - y_1$. So there exists an integer k such that

$$y_2 = y_1 + k \cdot \frac{a}{(a,b)},$$

and also

$$x_2 = x_1 - \frac{b}{a}(y_2 - y_1) = x_1 - k \cdot \frac{b}{(a,b)}.$$

Thus, the two directions show that this parametrization captures all solutions and captures only solutions. ∎

Definition 6.3. A **lattice point** is a point with integer coordinates in Euclidean space $\mathbb{R}^n$.

Corollary 6.4. Let m and n be positive integers. The number of lattice points on the line segment from $(0,0)$ to (m,n), excluding $(0,0)$ but including (m,n), is $\gcd(m,n)$.

Proof. Since m is positive, it allows us to speak of the slope $\frac{n}{m} = \frac{y}{x}$, where (x,y) is a lattice point on the segment. Note that the segment at least has the lattice point (m,n), so it is not nonsensical to speak of (x,y). The equation of the line through our segment is

$$(-n)x + my = 0.$$

By the classification of solutions to linear Diophantine equations, all lattice points on this line are given by

$$\left(m - k \cdot \frac{m}{\gcd(-n,m)}, n + k \cdot \frac{-n}{\gcd(-n,m)} \right)_{k \in \mathbb{Z}}.$$

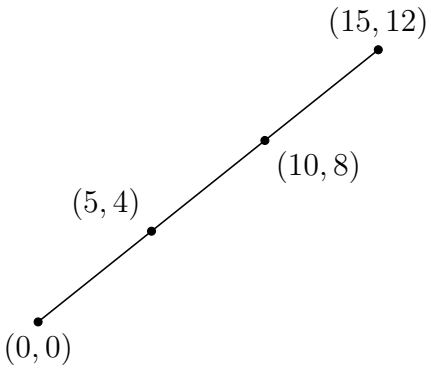
This is equivalent to

$$\left(m - k \cdot \frac{m}{\gcd(m,n)}, n - k \cdot \frac{n}{\gcd(m,n)}\right)_{k \in \mathbb{Z}}.$$

In order for the point to lie on the desired segment, the following inequalities must hold:

$$0 < m - k \cdot \frac{m}{\gcd(n,m)} \leq m,$$
$$0 < n - k \cdot \frac{n}{\gcd(n,m)} \leq n.$$

These are both equivalent to $0 \leq k < \gcd(m,n)$. Therefore, there are $\gcd(m,n)$ such integers k, as expected. For example, we can visualize the concrete case of $\gcd(15,12) = 3$ as shown below.



■

The geometric result in Corollary 6.4 will be useful in our proof of quadratic reciprocity (Theorem 11.25).

Problem 6.5. For each integer a and prime p, find infinitely many positive integers x such that

$$x^x \equiv a \pmod{p}.$$

6.2 Chinese Remainder Theorem

Note that $ax + by = c$ holds if and only if it is true that

$$\frac{a}{(a,b)}x + \frac{b}{(a,b)}y = \frac{c}{(a,b)}.$$

This equation has a solution if and only if the congruence

$$\frac{a}{(a,b)}x \equiv \frac{c}{(a,b)} \left(\mod \frac{b}{(a,b)}\right)$$

has a solution. Since $\frac{a}{(a,b)}$ is coprime to $\frac{b}{(a,b)}$, this congruence has a solution if and only if we can solve

$$x \equiv \frac{c}{(a,b)} \left(\frac{a}{(a,b)} \right)^{-1} \left(\mod \frac{b}{(a,b)} \right).$$

So one way of describing our work in Section 6.1 is that we were solving equations equivalent to congruences of the form

$$x \equiv d \pmod{n}.$$

With the classification of solutions to linear Diophantine equations complete, we turn our attention to a *system* of such congruences.

Theorem 6.6 (Chinese remainder theorem (CRT))**.** Let $k \geq 2$ be an integer, $n_1, n_2, \ldots, n_k$ be pairwise coprime positive integers, and $a_1, a_2, \ldots, a_k$ be any integers. Then there exists an integer x that simultaneously satisfies the congruences

$$\begin{aligned} x &\equiv a_1 \pmod{n_1}, \\ x &\equiv a_2 \pmod{n_2}, \\ &\vdots \\ x &\equiv a_k \pmod{n_k}. \end{aligned}$$

Let $N = n_1 n_2 \cdots n_k$. If x_0 is a solution, then all solutions are given by

$$(x_0 + m \cdot N)_{m \in \mathbb{Z}},$$

which in turn produces a unique solution in the interval $[0, N)$.

Proof. We proceed by induction on $k \geq 2$. The base case $k = 2$ is the most involved step and the rest will follow relatively smoothly. In the base case, our system is

$$\begin{aligned} x &\equiv a_1 \pmod{n_1}, \\ x &\equiv a_2 \pmod{n_2}. \end{aligned}$$

To get some hints about a solution x_0, we look at necessary criteria. If x_0 is a solution, then there exist integers m_1, m_2 such that

$$\begin{aligned} x &= a_1 + m_1 n_1, \\ x &= a_2 + m_2 n_2. \end{aligned}$$

Subtracting the equations, we get

$$m_1 n_1 - m_2 n_2 = a_2 - a_1.$$

This reminds us of the equation in Bézout's lemma. Based on this insight, we try to generate such an equation. Since n_1 and n_2 are coprime, there exist integers c_1 and c_2 such that

$$c_1 n_1 + c_2 n_2 = 1.$$

Multiplying through by $a_2 - a_1$ yields

$$\begin{aligned}(a_2 - a_1)c_1n_1 + (a_2 - a_1)c_2n_2 &= a_2 - a_1\\ (a_2 - a_1)c_1n_1 + a_1 &= (a_1 - a_2)c_2n_2 + a_2.\end{aligned}$$

If we take x_0 to be the number that is equal to both sides of the last equation, then indeed,

$$\begin{aligned}x_0 &\equiv a_1 \pmod{n_1},\\ x_0 &\equiv a_2 \pmod{n_2}.\end{aligned}$$

Now we will show that x is a solution if and only if

$$x \equiv x_0 \pmod{n_1n_2}.$$

In one direction, if this congruence holds, then x is a solution to the original system because we may replace the modulus n_1n_2 with n_1 or n_2 since they both divide n_1n_2. In the other direction, if x is a solution to the original system of congruences, then both x and x_0 are congruent to a_1 modulo n_1 and a_2 modulo n_2, so

$$\begin{aligned}x &\equiv x_0 \pmod{n_1},\\ x &\equiv x_0 \pmod{n_2}.\end{aligned}$$

This means n_1 and n_2 both divide $x - x_0$, and since these two moduli are coprime, $n_1n_2 \mid x - x_0$, by the faux-Chinese remainder theorem (Theorem 2.10). This establishes the base case.

For the induction hypothesis, suppose the theorem holds for some integer $k \geq 2$. Let there be a system of $k+1$ congruences that satisfy the hypotheses of the Chinese remainder theorem. By the induction hypothesis, there exists an integer x' satisfying the first k congruences and that all solutions x to the first k congruences are the solutions to

$$x \equiv x' \pmod{n_1n_2\cdots n_k}.$$

So an integer x_0 satisfies all $k+1$ congruences if and only if it satisfies the two congruences

$$\begin{aligned}x_0 &\equiv x' \pmod{n_1n_2\cdots n_k},\\ x_0 &\equiv a_{k+1} \pmod{n_{k+1}}.\end{aligned}$$

By the base case, such an x_0 exists and all solutions are given by

$$(x_0 + m \cdot n_1n_2\cdots n_kn_{k+1})_{m\in\mathbb{Z}}.$$

This completes the induction.

According to the arguments in the base case and inductive step, iterated applications of the extended Euclidean algorithm (to simultaneously solve pairs of congruences for c_1 and c_2) allows for the computation of a simultaneous solution to all k congruences. This then leads to all solutions, as stated.

As for the minimal positive solution, if we pick any solution, then performing Euclidean division by $N = n_1n_2\cdots n_k$ yields a remainder that is a solution in the interval $[0, N)$. This must be the unique solution in that interval because all consecutive solutions differ by N. ■

Problem 6.7. Prove that, if p and q are distinct prime numbers, then

$$p^{q-1} + q^{p-1} \equiv 1 \pmod{pq}.$$

The ordinary Chinese remainder theorem works only for pairwise coprime moduli, but we will now extend it to the greatest extent possible. Most sources do not state this generalization, but we are happy to include it (it does appear as a problem in [13]).

Corollary 6.8 (Generalized Chinese remainder theorem)**.** Let $k \geq 2$ be an integer, and $n_1, n_2, \ldots, n_k$ be positive integers, and $a_1, a_2, \ldots, a_k$ be any integers. Then there exists an integer x that simultaneously satisfies the congruences

$$\begin{aligned} x &\equiv a_1 \pmod{n_1}, \\ x &\equiv a_2 \pmod{n_2}, \\ &\vdots \\ x &\equiv a_k \pmod{n_k} \end{aligned}$$

if and only if

$$a_i \equiv a_j \pmod{\gcd(n_i, n_j)}$$

for all pairs $(i, j) \in [k] \times [k]$. In this case, if x_0 is a solution, then all solutions are given by

$$(x_0 + m \cdot \operatorname{lcm}(n_1, n_2, \ldots, n_k))_{m \in \mathbb{Z}},$$

which in turn produces a unique solution in the interval $[0, \operatorname{lcm}(n_1, n_2, \ldots, n_k))$.

Proof. First we tackle the biconditional classification of when some integer x simultaneously solves all of the congruences. For one direction, suppose there exists an integer x that satisfies the k congruences. Since for every $(i, j) \in [k] \times [k]$, (n_i, n_j) divides the moduli n_i and n_j, the two congruences

$$\begin{aligned} x &\equiv a_i \pmod{(n_i, n_j)}, \\ x &\equiv a_j \pmod{(n_i, n_j)}. \end{aligned}$$

hold and so

$$a_i \equiv a_j \pmod{(n_i, n_j)}$$

for every pair $(i, j) \in [k] \times [k]$.
The converse is more difficult. Suppose the conclusion of the last direction holds. The method will be more motivated if we work backwards a bit from the desired conclusion. The idea is to use the maximal prime powers divisors of the n_i as moduli instead of the n_i themselves. Let the complete list of prime factors of all of the moduli n_i be $p_1, p_2, \ldots, p_m$, though not every prime on this list necessarily divides every n_i. For each $\alpha \in [k]$ and $\beta \in [m]$, let

$$\nu_{p_\beta}(n_\alpha) = e_{\alpha,\beta},$$

where the e is unrelated to Euler's constant. For each $\alpha \in [k]$, an integer x satisfies the congruence

$$x \equiv a_\alpha \pmod{n_\alpha}$$

if and only if it satisfies the m congruences

$$\begin{aligned} x &\equiv a_\alpha \pmod{p_1^{e_{\alpha,1}}}, \\ x &\equiv a_\alpha \pmod{p_2^{e_{\alpha,2}}}, \\ &\vdots \\ x &\equiv a_\alpha \pmod{p_m^{e_{\alpha,m}}}. \end{aligned}$$

So x is a solution to the original system of k congruences if and only if x solves

$$x \equiv a_\alpha \pmod{p_\beta^{e_{\alpha,\beta}}}$$

for every pair $(\alpha, \beta) \in [k] \times [m]$. It may be helpful to think of a $k \times m$ matrix of congruences, in which the entry at row $\alpha \in [k]$ and column $\beta \in [m]$ is the above congruence. We aim to construct a solution to this system of km congruences. As some foreshadowing, we will pull a move that is highly reminiscent of the discrete Fubini's principle: instead of fixing α and iterating through β's, we will fix β and iterate through α's.
Let us return to the hypothesis, which is that, for each $(i, j) \in [k] \times [k]$,

$$a_i \equiv a_j \pmod{(n_i, n_j)}.$$

Switching over to the prime power representation of the gcd function, the hypothesis implies that for each $(i, j) \in [k] \times [k]$ and each $\beta \in [m]$,

$$a_i \equiv a_j \pmod{p_\beta^{\min(e_{i,\beta}, e_{j,\beta})}}.$$

For a fixed β, the minimum function can be computed explicitly if we choose one of the indices i, j to be the index at which the multiplicity of p_β is maximal among the moduli n_α. Let $\gamma_\beta \in [k]$ be the modulus index at which $e_{\gamma_\beta,\beta}$ is maximal among all $e_{\alpha,\beta}$ as α varies and β is fixed. Now we pull our Fubini move. Let $x_\beta = a_{\gamma_\beta}$. Then we get that x_β simultaneously solves the k congruences

$$\begin{aligned} x_\beta \equiv a_{\gamma_\beta} \equiv a_1 &\pmod{p_\beta^{e_{1,\beta}}}, \\ x_\beta \equiv a_{\gamma_\beta} \equiv a_2 &\pmod{p_\beta^{e_{2,\beta}}}, \\ &\vdots \\ x_\beta \equiv a_{\gamma_\beta} \equiv a_k &\pmod{p_\beta^{e_{k,\beta}}}. \end{aligned}$$

So far, we have solved each column (representing fixed primes) of our $k \times m$ matrix of congruences. Now we can pull together the rows as well because, by the Chinese remainder theorem, there exists an integer x such that

$$\begin{aligned} x &\equiv x_1 \pmod{p_1^{e_{\gamma_1,1}}}, \\ x &\equiv x_2 \pmod{p_2^{e_{\gamma_2,2}}}, \\ &\vdots \\ x &\equiv x_k \pmod{p_k^{e_{\gamma_k,k}}}. \end{aligned}$$

This x satisfies all km congruences since lower powers of these primes divide these maximal prime power moduli, so we are done with proving the biconditional existence criterion.
It remains to generate all solutions from one solution. Suppose x_0 is a solution to the original k congruences. We will show that x is a solution if and only if

$$x \equiv x_0 \pmod{\operatorname{lcm}(n_1, n_2, \ldots, n_k)}.$$

In one direction, if this congruence holds for some x, then

$$x \equiv x_0 \pmod{n_i}$$

for each $i \in [k]$, since

$$n_i \mid \operatorname{lcm}(n_1, n_2, \ldots, n_k).$$

In the other direction, if x is a solution to the original k congruences, then

$$\begin{aligned} x &\equiv a_i \pmod{n_i}, \\ x_0 &\equiv a_i \pmod{n_i} \end{aligned}$$

for each $i \in [k]$. Then

$$x \equiv x_0 \pmod{n_i},$$

so each n_i divides $x - x_0$. That means the maximal prime powers

$$p_1^{e_{\gamma_1,1}}, p_2^{e_{\gamma_2,2}}, \ldots, p_k^{e_{\gamma_k,k}}$$

all divide $x - x_0$. By the prime factorization formula for the least common multiple, the product of these maximal prime powers is $\operatorname{lcm}(n_1, n_2, \ldots, n_k)$. Since the maximal prime powers are pairwise coprime to each other, their product $\operatorname{lcm}(n_1, n_2, \ldots, n_k)$ divides $x - x_0$ by Theorem 2.10, which means

$$x \equiv x_0 \pmod{\operatorname{lcm}(n_1, n_2, \ldots, n_k)}.$$

Euclidean division of any solution by $\operatorname{lcm}(n_1, n_2, \ldots, n_k)$ produces the minimal non-negative solution, which necessarily lives in the interval $[0, \operatorname{lcm}(n_1, n_2, \ldots, n_k))$. ■

Further examples of theorems in the style of the Chinese remainder theorem are given in Theorem 11.2, Problem 11.4, and Problem 11.5.

6.3 Frobenius, Sylvester, and Schur

Definition 6.9. Recall that, in a linear Diophantine equation $ax + by = c$ where a, b, c are fixed integers and x, y are integer variables, the quantity $ax+by$ is called a linear combination of a and b (see Definition 1.10). If x and y are restricted to being non-negative integers, then $ax + by$ is called a **conical combination** of a and b, and $ax + by$ is said to be **achievable** as a conical combination of a and b; if an integer is not achievable, then we call it **non-achievable**.

We know from Bézout's lemma that if at least one of a, b is non-zero, then the set of linear combinations $ax + by$ is precisely the set of multiples of $\gcd(a, b)$, including non-positive multiples. It is natural to inquire about the conical analogue of Bézout: what is the set of numbers that are achievable as a conical combination of two positive integer denominations a and b? This, along with its generalization to n denominations, is called the **Frobenius coin problem**.

Example 6.10. Find all non-negative integers that are non-achievable as a conical combination of 3 and 7, meaning $3x + 7y$ for non-negative integers x, y.

Solution. We split the non-negative integers into three columns according to the congruence classes modulo 3:

$$\begin{array}{ccc} \vdots & \vdots & \vdots \\ 15 & 16 & 17 \\ 12 & 13 & \boxed{14} \\ 9 & 10 & 11 \\ 6 & \boxed{7} & 8 \\ 3 & 4 & 5 \\ \boxed{0} & 1 & 2 \end{array}$$

Fortunately, or perhaps for a deeper reason, the first three multiples of 7, that is $0, 7, 14$, lie in different columns. These three are achievable, as are all numbers lying anywhere in the same column above each of them because those numbers are $0, 7$, or 14 plus a multiple of 3. That leaves $1, 2, 4, 5, 8, 11$ because they lie directly below one of $0, 7, 14$. Trying the $4 \cdot 2 = 8$ pairs (x, y) resulting from $x \in \{0, 1, 2, 3\}$ and $y \in \{0, 1\}$ shows that we never achieve any of $1, 2, 4, 5, 8, 11$. We do not need to check any higher x or y because $3 \cdot 4 + 7 \cdot 0 = 12$ and $3 \cdot 0 + 7 \cdot 2 = 14$, both of which exceed the highest non-achievable candidate 11. Thus, the non-achievable integers are $1, 2, 4, 5, 8, 11$. ■

Lemma 6.11. Suppose n is a positive integer and $\{r_0, r_1, \ldots, r_{n-1}\}$ is a complete residue system modulo n. If a is an integer coprime to n, then

$$\{ar_0, ar_1, \ldots, ar_{n-1}\}$$

is also a complete residue system modulo n. Equivalently, we are saying that if we take a representative from each congruence class in $\mathbb{Z}/n\mathbb{Z}$ and multiplying each chosen representative by a, then the numbers still represent every residue class modulo n, though usually in a different order (like a non-trivial permutation).

Proof. If suffices to show that, for all $i, j \in \{0, 1, \ldots, n-1\}$, if $i \neq j$, then

$$ar_i \neq ar_j \pmod{n}.$$

We will prove the contrapositive. If $ar_i \equiv ar_j \pmod{n}$, then we can cancel a from both sides of the congruence because $(a, n) = 1$, so $r_i \equiv r_j \pmod{n}$. Since the r_k all lie in distinct congruence classes modulo n, it must be true that $i = j$. ■

Theorem 6.12 (Sylvester's theorem)**.** If m and n are coprime positive integers, then all sufficiently large integers are achievable as a conical combination of m and n. Moreover, for each $x \in \{0, 1, \ldots, n-1\}$, mx is the smallest achievable integer that is congruent to mx modulo n. This has two consequences:

- The greatest non-achievable integer is

$$m(n-1) - n = mn - m - n.$$

  So all integers that are greater than or equal to

$$mn - m - n + 1 = (m-1)(n-1)$$

  are achievable.

- Having characterized all non-achievable non-negative integers, we can count the set of such numbers to have cardinality

$$\frac{(m-1)(n-1)}{2}.$$

Proof. If $m = 1$ or $n = 1$, then all non-negative integers are achievable and the theorem is easy to verify in this case. So we will assume that $m \geq 2$ and $n \geq 2$ (though one of them must be at least 3 since they are coprime and so both cannot be 2 at the same time). Throughout this proof, it will help to keep the following example of an $m \times n$ matrix in mind, where $m = 3$ and $n = 7$:

$$\begin{array}{ccccccc} \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 14 & \boxed{15} & 16 & 17 & \boxed{18} & 19 & 20 \\ 7 & 8 & \boxed{9} & 10 & 11 & \boxed{12} & 13 \\ \boxed{0} & 1 & 2 & \boxed{3} & 4 & 5 & \boxed{6} \end{array}.$$

Note that $3{\cdot}0, 3{\cdot}1, \ldots, 3{\cdot}(7-1)$ all fell into different columns, so they reside in different residue classes modulo 7. Moreover, for each $x \in \{0, 1, 2, 3, 4, 5, 6\}$, the column of numbers in which $3x$ lies has an interesting property: the numbers directly above $3x$ are all achievable and the numbers directly below $3x$ are all non-achievable. We will prove these properties in general. Note that, considering that the same facts are symmetrically reflected in Example 6.10, it means m and n occupy symmetric roles in the theorem and so either this $m \times n$ matrix or its $n \times m$ variant can be used.
Suppose m and n are coprime positive integers. By Lemma 6.11, since $\{0, 1, \ldots, n-1\}$ is a complete residue system modulo n, so is

$$\{m \cdot 0, m \cdot 1, \ldots, m \cdot (n-1)\}.$$

This explains why they all land in different columns, meaning residue classes modulo n. For any $x \in \{0, 1, \ldots, n-1\}$ and positive integer y, $mx + ny$ is achievable, which explains why all numbers directly above each mx is achievable. Thus, all sufficiently large non-negative integers are achievable.

Now we will go after the numbers below each mx. Suppose, for contradiction, that $mx - ny$ is achievable for some positive integer y. By the definition of being achievable, there exist non-negative integers a and b such that

$$mx - ny = ma + nb,$$

which is equivalent to

$$m(x - a) = n(y + b).$$

Since $(m, n) = 1$, we get that $m \mid b + y$, so there exists an integer q such that $mq = b + y$. This q must be positive since m and y are positive and b is non-negative. Substituting this into $m(x - a) = n(y + b)$ yields $m(x - a) = nmq$, so

$$nq + a = x < n \implies a < n(1 - q).$$

But a is non-negative, whereas n is positive and $1 - q$ is non-positive. This forces

$$0 \leq a < n(1 - q) \leq 0,$$

so $0 < 0$, which is the contradiction that we have been seeking.
It is time for the two listed deductions.

- In the column (meaning residue class) of mx, the highest non-achievable integer is $mx - n$. The mx cover all the columns and the greatest x is $n - 1$, so the overall highest non-achievable integer is

  $$m(n - 1) - n = mn - m - n.$$

  As a consequence, every integer from

  $$mn - m - n + 1 = (m - 1)(n - 1)$$

  onward is achievable, though there may be achievable integers less than it as well.

- We have to prove that the sum of the number of numbers directly below mx in the matrix, for $x \in \{0, 1, \ldots, n - 1\}$, equals $\dfrac{(m - 1)(n - 1)}{2}$. For each x, we want to know the number of times that we can subtract n from mx and remain in the non-negative integers. Calling this number s, we get

  $$mx - ns \geq 0 \iff s \leq \frac{mx}{n} \iff s \leq \left\lfloor \frac{mx}{n} \right\rfloor.$$

  So we are seeking to evaluate

  $$\sum_{x=0}^{n-1} \left\lfloor \frac{mx}{n} \right\rfloor.$$

  By Euclidean division, there exists a quotient q_x and remainder r_x such that

  $$mx = nq_x + r_x, \text{ and } 0 \leq r_x < n.$$

This allows us to evaluate the sum as

$$\sum_{x=0}^{n-1} \left\lfloor \frac{mx}{n} \right\rfloor = \sum_{x=0}^{n-1} \left\lfloor q_x + \frac{r_x}{n} \right\rfloor = \sum_{x=0}^{n-1} q_x$$
$$= \sum_{x=0}^{n-1} \frac{mx - r_x}{n} = \frac{m}{n} \sum_{x=0}^{n-1} x - \frac{1}{n} \sum_{x=0}^{n-1} r_x.$$

The remainders r_x must all the distinct, otherwise it would not be true that the mx all lie in different residue classes. So

$$\{r_0, r_1, \ldots, r_{n-1}\} = \{0, 1, \ldots, n-1\},$$

though not necessarily in the same order. Thus, the sum equals

$$\frac{m}{n} \cdot \frac{(n-1)n}{2} - \frac{1}{n} \cdot \frac{(n-1)n}{2} = \left(\frac{m}{n} - \frac{1}{n}\right) \cdot \frac{(n-1)n}{2} = \frac{(m-1)(n-1)}{2}.$$

■

Problem 6.13. If m and n are coprime positive integers, then prove that for every integer k, the pair $\{k, mn - m - n - k\}$ consists of two distinct integers and exactly one of the two is achievable as a conical combination of m and n.

Corollary 6.14. Sylvester's theorem resolves the Frobenius coin problem for two relatively prime positive integers m and n. If m and n are positive integers (that are not necessarily coprime), then the analysis is as follows.

1. If a non-negative integer c is achievable, then c is a multiple of (m, n). All sufficiently large multiples of (m, n) are achievable and the highest multiple of (m, n) that is not achievable is
$$\operatorname{lcm}(m, n) - m - n.$$
2. The quantity $\operatorname{lcm}(m, n) - m - n$ is positive if and only if $m \nmid n$ or $n \nmid m$. In this case, the number of non-negative integers less than or equal to $\operatorname{lcm}(m, n) - m - n$ that are non-achievable is
$$\left(\frac{m}{(m, n)} - 1\right)\left(\frac{n}{(m, n)} - 1\right)\left((m, n) - \frac{1}{2}\right) - (m, n) + 1.$$

Both of these results reduce to Sylvester's theorem in the case that m and n are coprime.

Proof. Suppose m and n are positive integers.

1. If c is achievable then it is a conical combination of m and n. Every conical combination is a linear combination, and by Bézout's lemma, every linear combination of m and n is a multiple of (m, n). Thus, c is a multiple of (m, n). Now let $mx + ny$ be a conical combination of m and n. The equation $c = mx + ny$ is true if and only if
$$\frac{c}{(m, n)} = \frac{m}{(m, n)} x + \frac{n}{(m, n)} y.$$

Note that $\dfrac{m}{(m,n)}$ and $\dfrac{n}{(m,n)}$ are coprime. By Sylvester's theorem, all integers greater than

$$\frac{mn}{(m,n)^2} - \frac{m}{(m,n)} - \frac{n}{(m,n)}$$

are achievable as conical combinations of $\dfrac{m}{(m,n)}$ and $\dfrac{n}{(m,n)}$. Scaling up the corresponding Bézout equations by a factor of (m,n), we find that all multiples of (m,n) that are greater than

$$(m,n)\left[\frac{mn}{(m,n)^2} - \frac{m}{(m,n)} - \frac{n}{(m,n)}\right] = \operatorname{lcm}(m,n) - m - n$$

are achievable as conical combinations of m and n. However, if $\operatorname{lcm}(m,n) - m - n$ were achievable, then by scaling down its equation by a factor of (m,n) would imply that

$$\frac{\operatorname{lcm}(m,n) - m - n}{(m,n)} = \frac{mn}{(m,n)^2} - \frac{m}{(m,n)} - \frac{n}{(m,n)}$$

is achievable as a conical combination of $\dfrac{m}{(m,n)}$ and $\dfrac{n}{(m,n)}$. This contradicts Sylvester's theorem. As a side note, if $(m,n) = 1$, we get Sylvester's $mn - m - n$ bound.

2. If $m \mid n$, then

$$\operatorname{lcm}(m,n) - m - n = n - m - n = -m < 0$$

and if $n \mid m$, then

$$\operatorname{lcm}(m,n) - m - n = m - m - n = -n < 0.$$

Conversely, suppose $m \nmid n$ and $n \nmid m$. Then

$$\operatorname{lcm}(m,n) - m - n = \frac{mn}{(m,n)} - m - n = m\left(\frac{n}{(m,n)} - 1\right) - n.$$

Letting $k = \dfrac{n}{(m,n)}$, we get $n = k \cdot (m,n)$. If $k = 1$, then it would be true that $n = (m,n)$, which is equivalent to $n \mid m$, which is a contradiction. So $k \geq 2$, which implies

$$m\left(\frac{n}{(m,n)} - 1\right) - n \geq m - n.$$

We can symmetrically prove that

$$\operatorname{lcm}(m,n) - m - n = n\left(\frac{m}{(m,n)} - 1\right) - m \geq n - m.$$

Together, the two inequalities yield

$$\operatorname{lcm}(m,n) - m - n \geq |m - n|.$$

Since neither of m, n divides the other, they are not equal and so their absolute difference must be at least 1. Thus, $|m-n| \geq 1$ and so $\operatorname{lcm}(m,n) - m - n > 0$.

Now we know that $[0, \operatorname{lcm}(m,n) - m - n]$ is a well-defined and non-singleton closed interval. The non-achievable integers in this interval come in two categories: those that are multiples of (m,n) and so *might* be a conical combination, and those that are not multiples of (m,n) and so are automatically out of the running. There are

$$\operatorname{lcm}(m,n) - m - n + 1$$

integers in the interval, out of which

$$\frac{\operatorname{lcm}(m,n) - m - n}{(m,n)} + 1$$

are multiples of (m,n). Note that we added $+1$ in each count in order to account for 0. By subtracting, the number of elements of the interval that are not multiples of (m,n) is

$$\operatorname{lcm}(m,n) - m - n - \frac{\operatorname{lcm}(m,n) - m - n}{(m,n)}.$$

Removing the non-multiples of (m,n) from $[0, \operatorname{lcm}(m,n) - m - n]$ yields the set

$$S = \{0, (m,n), 2 \cdot (m,n), \ldots, \operatorname{lcm}(m,n) - m - n\}.$$

We will use scaling again now. It is true that $k \cdot (m,n) = mx + ny$ for some integer k such that

$$0 \leq k \leq \frac{\operatorname{lcm}(m,n) - m - n}{(m,n)} = \frac{mn}{(m,n)^2} - \frac{m}{(m,n)} - \frac{n}{(m,n)}$$

if and only if

$$k = \frac{m}{(m,n)}x + \frac{n}{(m,n)}y.$$

Since the upper bound $\dfrac{mn}{(m,n)^2} - \dfrac{m}{(m,n)} - \dfrac{n}{(m,n)}$ on k is in the form of Sylvester's result where the denominations of the conical representations are the coprime integers $\dfrac{m}{(m,n)}$ and $\dfrac{n}{(m,n)}$, Sylvester says that the number of non-achievable integers $k \cdot (m,n)$ in S is

$$\frac{1}{2}\left(\frac{m}{(m,n)} - 1\right)\left(\frac{n}{(m,n)} - 1\right) = \frac{1}{2} \cdot \frac{\operatorname{lcm}(m,n) - m - n}{(m,n)} + \frac{1}{2}.$$

Letting the value of either side of this identity equal to $\dfrac{x}{2}$, we find that the total number of non-achievable integers in the interval is

$$\begin{aligned}
&\operatorname{lcm}(m,n) - m - n - \frac{\operatorname{lcm}(m,n) - m - n}{(m,n)} + \frac{x}{2} \\
&= (x-1)(m,n) - (x-1) + \frac{x}{2} \\
&= x(m,n) - (m,n) - x + 1 + \frac{x}{2} \\
&= x\left((m,n) - \frac{1}{2}\right) - (m,n) + 1,
\end{aligned}$$

which becomes the formula that we wanted once we substitute in x. Testing $(m, n) = 1$, we get $\dfrac{(m-1)(n-1)}{2}$ from Sylvester's theorem.

■

As the reader might have noticed, if m and n are coprime positive integers and N is a non-negative integer, then the equation

$$mx + ny = N$$

from the Frobenius coin problem is reminiscent of Bézout's lemma. Indeed, there is a proof of the bound from Sylvester's theorem using Bézout's lemma, and it helps with proving Schur's theorem.

Theorem 6.15. Let m and n be coprime positive integers. Then Bézout's lemma and the classification of all solutions of a linear Diophantine equation may be combined to prove that $mn - m - n$ is not achievable and that all integers greater than $mn - m - n$ are achievable. The key is that the linear combination in Bézout's lemma can be made to be a conical combination.

Proof. We will prove that $mn - m - n$ is not achievable, and that all greater integers are achievable. Suppose, for contradiction, that

$$mn - m - n = mx + ny$$

for some non-negative integers x and y. Rearranging, we get

$$m(n - 1 - x) = n(y + 1).$$

Since m and n are coprime, $n \mid x + 1$ and $m \mid y + 1$. As $x + 1 \geq 1$ and $y + 1 \geq 1$, it holds that $x + 1 \geq n$ and $y + 1 \geq m$. This leads to

$$\begin{aligned} mn - m - n &= mx + ny \\ &\geq m(n-1) + n(m-1) = 2mn - m - n. \end{aligned}$$

Then $mn \leq 0$ which is a contradiction since m and n are positive.
Let N be an integer greater than or equal to $mn - m - n + 1$. Since $(m, n) = 1$, Bézout's lemma gives us integers x and y (not necessarily non-negative) such that

$$mx + ny = N.$$

By the classification of all solutions to a linear Diophantine equation (Theorem 6.2), all solutions are given by

$$(x + kn, y - km)$$

over all integers k. We want to find a solution such that both components are non-negative. The trouble is that, as one component goes up, the other components goes down. To be economical in dealing with this conservation-like property, we let y_0 be the minimal $y - km$.

That is, by Euclidean division of y by m, there exists a unique quotient q and unique remainder y_0 such that

$$y - qm = y_0, \text{ and } 0 \leq y_0 < m.$$

Let $x_0 = x + qn$ be the corresponding first coordinate. We want to show that x_0 is non-negative, just like y_0. Note that

$$mn - m - n < N = mx_0 + ny_0.$$

By rearranging, this is equivalent to

$$\frac{n}{m}(m - 1 - y_0) < x_0 + 1.$$

It suffices to show that $\frac{n}{m}(m - 1 - y_0) \geq 0$, which is true because $y_0 < m$. ■

The Frobenius coin problem has not been solved completely for any case beyond two denominations, though many partial results exist; see [1] for a survey of advances. Although exact formulas do not yet exist for the point after which all integers are achievable, the following theorem shows that such a point does always exist and it provides a weak general bound that reduces to Sylvester's bound in the case of two denominations. Sharper bounds are known but are more difficult to establish.

Theorem 6.16 (Schur's theorem)**.** Let $k \geq 2$ be an integer and $(n_1, n_2, \ldots, n_k)$ be a k-tuple of positive integers such that

$$\gcd(n_1, n_2, \ldots, n_k) = 1,$$
$$n_1 \leq n_2 \leq \cdots \leq n_k.$$

Then, for all integers N such that $N \geq (n_1 - 1)(n_k - 1)$, there exists a k-tuple of non-negative integers $(a_1, a_2, \ldots, a_k)$ such that

$$N = n_1a_1 + n_2a_2 + \cdots + n_ka_k.$$

In the $n = 2$ case, this agrees with Sylvester's bound.

Proof. We will prove the assertion by induction on $k \geq 2$. Sylvester's theorem takes care of the base case $k = 2$. Suppose the result holds for some $k \geq 2$. Let

$$1 \leq n_1 \leq n_2 \leq \cdots \leq n_k \leq n_{k+1}$$

be $k + 1$ positive integers such that

$$\gcd(n_1, n_2, \ldots, n_k, n_{k+1}) = 1.$$

In order to use the induction hypothesis, we need to drop one of the n_i somehow. The natural candidates are the ends, n_1 and n_{k+1}, but these are both required to be in the concluding inequality

$$N \geq (n_1 - 1)(n_{k+1} - 1),$$

so the next best options are n_2 and n_k. Let us try to drop the former. A conical combination

$$N = n_1a_1 + n_2a_2 + \cdots + n_ka_k + n_{k+1}a_{k+1}$$

exists if and only if

$$\frac{N - n_2a_2}{d} = \frac{n_1}{d}a_1 + \frac{n_3}{d}a_3 + \cdots + \frac{n_k}{d}a_k + \frac{n_{k+1}}{d}a_{k+1},$$

where $d = \gcd(n_1, n_3, \ldots, n_k, n_{k+1})$. We divided by d to ensure that

$$\gcd\left(\frac{n_1}{d}, \frac{n_3}{d}, \ldots, \frac{n_k}{d}, \frac{n_{k+1}}{d}\right) = 1.$$

Since

$$\gcd(n_1, n_2, \ldots, n_k, n_{k+1}) = 1,$$

this means that $\gcd(n_2, d) = 1$. First of all, we need to find a non-negative integer a_2 such that $\dfrac{N - n_2a_2}{d}$ is actually a non-negative integer t, which is equivalent to solving the equation $N = n_2a_2 + dt$ for non-negative integers a_2 and t. Since any integer N is a multiple of

$$\gcd(n_2, d) = \gcd(n_2, n_1, n_3, \ldots, n_k, n_{k+1}) = 1,$$

we know by the proof of Theorem 6.15 that such a pair of non-negative integers (a_2, t) exists with $a_2 \leq d - 1$. So $\dfrac{N - n_2a_2}{d} = t$ is an integer. We need to show that $t = \dfrac{N - n_2a_2}{d}$ is achievable as a conical combination of

$$\left(\frac{n_1}{d}, \frac{n_3}{d}, \ldots, \frac{n_k}{d}, \frac{n_{k+1}}{d}\right)$$

for all N such that

$$N \geq (n_1 - 1)(n_{k+1} - 1).$$

(Note that t depends on N.) By the induction hypothesis, this works for all N such that

$$\frac{N - n_2a_2}{d} \geq \left(\frac{n_1}{d} - 1\right)\left(\frac{n_{k+1}}{d} - 1\right),$$

or equivalently

$$N \geq n_2a_2 + \frac{1}{d}(n_1 - d)(n_{k+1} - d).$$

So it suffices to prove that the desired bound is a weakening of the known bound, meaning

$$(n_1 - 1)(n_{k+1} - 1) \geq n_2a_2 + \frac{1}{d}(n_1 - d)(n_{k+1} - d).$$

Since $a_2 \leq d - 1$, it suffices to get rid of a_2 altogether and prove that

$$(n_1 - 1)(n_{k+1} - 1) \geq n_2(d - 1) + \frac{1}{d}(n_1 - d)(n_{k+1} - d).$$

Working backwards, we can expand and rearrange this to get that it is equivalent to prove that

$$(d-1)(n_1 n_{k+1} - d(n_2+1)) \geq 0.$$

If $d = 1$, then the inequality holds as an equality and we are done. So suppose $d > 1$. We want to prove that

$$n_1 n_{k+1} \geq d(n_2+1).$$

Since $d \mid n_1$, we know that $n_1 \geq d$ and it suffices to show that $n_{k+1} > n_2$. Suppose otherwise, for the sake of contradiction. Since the n_i are in non-decreasing order, this would mean that

$$n_2 = n_3 = \cdots = n_k = n_{k+1}.$$

Then

$$d = \gcd(n_1, n_3, \ldots, n_k, n_{k+1}) = \gcd(n_1, n_2),$$

so $d \mid n_2$. Since we have established that $\gcd(n_2, d) = 1$, this forces $d = \gcd(n_2, d) = 1$, which contradicts that we are working in the case where $d > 1$. This finally completes the proof. ■

Chapter 7

Base Representations I

> "If somebody tells you a rule, break it. That's the only way to move things forward."
>
> – *Hans Zimmer, Masterclass*

From an early age, we are taught that each positive integer can be uniquely represented in base-10. Then we learn to extend these representations to 0 and negative integers, rationals, reals and complex numbers. We learn to do arithmetic computations using simple algorithms as far as feasible. After obtaining some degree of mathematical maturity, one may return to these basics to question the foundations. We will begin our study of bases by considering what exactly is meant by the uniqueness of the representation, looking at how the standard computational algorithms apply to other bases, and converting the same integer between different bases. We will wrap up by studying the divisibility information that is encoded in base representations of integers.

7.1 Base Arithmetic

Having familiarity with base-10 representations and computations under our belt, some questions that can be asked about general bases are:

- What other bases exist, meaning ways of uniquely or nearly uniquely representing numbers using symbols?
- Which numbers in what bases have unique representations? In the non-unique cases, can we classify all possible representations?
- Why do we use base-10? Have other bases been used in the past or are other bases applied elsewhere? If we could choose a new worldwide base, what desirable qualities should it have?
- What is an efficient way of converting the same number from one base to another?
- How can computations of arithmetic operations be done in a given base?
- What patterns can be noticed in the representations of particular kinds of numbers in a given base? "Particular" is in reference to definable qualities, such as being a rational number or an even integer.

Definition 7.1. The simplest way of representing a positive integer n in writing is to place a sequence of symbols "1," one after another, from left to right, where the number of symbols is the number of 1's that need to be added up to equal to n. This system, akin to tallying, is called **base-**1 or the **unary numeral system**. For example,

$$2 = 1 + 1 = 11_1,$$
$$5 = 1 + 1 + 1 + 1 + 1 = 11111_1,$$

assuming we interpret the far left sides of these equations in base-10 and the far right sides in base-1. To make it clear that an integer is being written in unary, we use a subscript of 1, like 11_1 and 11111_1.

An issue with unary is that it is inefficient in terms of the amount of space that it takes up as $n \to \infty$. Considering that a new symbol 0 would be needed to denote zero anyway (unless we wish to confusingly begin with denoting zero by 1, one by 11, and so on!), there are more efficient alternatives that use multiple symbols. Possibly because we have a total of ten fingers and ten toes, we use a system of 10 symbols called base-10. Since the reader has intuitive experience in working with base-10, we will not delay in describing positional notation using bases in general, every instance of which is exponentially more efficient than unary.

Definition 7.2. For each integer $b \geq 2$, a **base-b form** or a **b-ary form** is a sequence of symbols of the form

$$\pm(x_m x_{m-1} \dots x_1 x_0 . y_1 y_2 y_3 \dots)_b,$$

where m is any non-negative integer and the symbols x_i and y_j are chosen from among b distinct predefined symbols that represent the integers $0, 1, \dots, b-1$. There is the restriction that $x_m = 0$ if and only if $m = 0$. This form represents the real number

$$\pm \left(x_m b^m + x_{m-1} b^{m-1} + \dots + x_1 b + x_0 + \frac{y_1}{b} + \frac{y_2}{b^2} + \frac{y_3}{b^3} + \dots \right),$$

and this expression with the addition of terms is called the **base-b expansion** of the number. The $\pm$ sign is used to denote whether the real number being represented is positive or negative, though the sign and parentheses are dropped for non-negative real numbers. The x_i and y_j are called the base-b **digits** of the number being represented, with x_m being called the **leading digit** and x_0 the **units digit**. The dot in between the x_i and y_j is called the **radix point**. The subscript b is called the **base number** or simply the **base**; if no subscript is used, we may assume that base-10 is being used, unless otherwise specified. When using base-b forms, we say that we are working in **base-b**.

Example. The possible digits in base-10 are $0, 1, 2, 3, 4, 5, 6, 7, 8, 9$, though other symbols are used in many other languages. For bases $b < 10$, we can recycle the same symbols as in base-10 up to and including the symbol $b-1$. For bases $b > 10$, we can tack on more symbols for digits such as the letters from the English language: $10_{10} = A, 11_{10} = B$, and so on. If we run out of English letters there are more symbols in other languages, such as Greek. Some areas of math use Hebrew letters (for other purposes), so that is a possibility too.

Theorem 7.3 (Basis representation theorem for integers)**.** If $b \geq 2$, then each integer has a representation as a b-ary form

$$\pm(x_m x_{m-1} \dots x_1 x_0 . y_1 y_2 y_3 \dots)_b,$$

and there exists a unique form such that $y_j = 0$ for all positive integers j (to understand why this latter property is important for uniqueness, read about *dual representations* in Theorem 10.1). Conversely, every form of the latter type clearly represents an integer due to its base-b expansion. As the y_j's are all 0, it is fine to not include them in the unique form

$$\pm(x_m x_{m-1} \dots x_1 x_0)_b,$$

which allows us to write down only finitely many symbols to represent the integer.

It is tedious to prove the basis representation theorem, so we will skip over it.

Example. Base-2 is called **binary**, base-3 is called **ternary**, and base-4 is called **quaternary**. There are many other names for specific bases, such as **decimal** for base-10 and **hexadecimal** for base-16. Historically, Babylonians used base-60 and Mayans used base-20, but not many people used any bases other than $10, 20$, and 60. There are also some exotic numeral systems such as:

- A base where integers can be represented as sums of Fibonacci numbers where the selection of Fibonacci numbers in the sum is unique under certain restrictions. The interested reader can investigate *Zeckendorf's theorem*.
- Balanced ternary, which is like base-3, but the digits represent $-1, 0, 1$ instead of $0, 1, 2$.

Binary is the language of computers, and base-b for b equal to higher powers of 2, such as hexadecimal, can also be useful in computer science.

Problem 7.4. Let d be a positive integer. In base $b \geq 2$, how many positive integers are there with *exactly* d digits and how many non-negative integers are there with *at most* d digits?

Example 7.5. Show that the number digits of a positive integer n in base-b is $\lfloor \log_b n \rfloor + 1$.

Solution. Let the base-b form of n be

$$\begin{aligned} n &= x_m x_{m-1} \dots x_1 x_0, \\ &= x_m b^m + x_{m-1} b^{m-1} + \dots + x_1 b + x_0, \end{aligned}$$

where $x_m \neq 0$. We wish to express m in terms of n and b. The idea is to use approximations and logarithms to isolate the m in the exponent b^m. Since $0 \leq x_i \leq b-1$ for each i, and $x_m \geq 1$,

$$\begin{aligned} 1 \cdot b^m &\leq x_m b^m + x_{m-1} b^{m-1} + \dots + x_1 b + x_0 \\ &\leq (b-1)(b^m + b^{m-1} + \dots + b + 1) \\ &= b^{m+1} - 1, \end{aligned}$$

where the last line can be obtained from the formula for a geometric series or simply quoted as a case of the well-known difference of powers factorization. So $b^m \leq n < b^{m+1}$. Taking base-b logarithms, we get

$$m \leq \log_b n < m + 1.$$

By a property of the floor function, this is equivalent to $m = \lfloor \log_b n \rfloor$. Accounting for the units digit (which has the subscript or index of 0 in our notation), the answer is $m + 1 = \lfloor \log_b n \rfloor + 1$. ■

There are two standard questions that arise once we have defined positional notation using bases:

- What are efficient ways of performing the main four arithmetic operations on integers that are represented as b-ary forms?
- What is an efficient way of converting the same integer from one base to another?

We will show examples of these computations from which the general procedures will become clear.

Example 7.6. Do the following computations in base-5:

- Addition with carrying: $4302_5 + 1243_5$
- Subtraction with borrowing: $4302_5 - 1343_5$
- Multiplication of integers with more than one digit: $412_5 \times 42_5$
- Long division with remainder: $414_5 \div 3_5$

Solution. We extend the standard pen-and-paper algorithms for these operations in base-10 to base-5:

$$\begin{array}{cccccc} & {}^{1}4 & {}^{1}3 & {}^{1}0 & 2_5 \\ + & 1 & 2 & 4 & 3_5 \\ \hline 1 & 1 & 1 & 0 & 0_5 \end{array} \qquad \begin{array}{cccccc} & {}^{3}\not{4} & {}^{12}\not{3} & {}^{4}\not{0} & 12_5 \\ - & 1 & 3 & 4 & 3_5 \\ \hline & 2 & 4 & 0 & 4_5 \end{array}$$

$$\begin{array}{cccccc} & & {}^{1}4 & {}^{1}1 & 2_5 \\ & \times & & 4 & 2_5 \\ \hline & 1 & {}^{1}3 & 2 & 4 \\ 3 & 2 & 0 & 3 & 0 \\ \hline 3 & 3 & 4 & 0 & 4_5 \end{array} \qquad \begin{array}{cccc} & 1 & 2 & 1_5 \\ \hline 3_5 & 4 & 1 & 4_5 \\ - & 3 & & \\ \hline & 1 & 1 & \\ - & 1 & 1 & \\ \hline & & 0 & 4 \\ & - & & 3 \\ \hline & & & 1_5 \end{array}$$

Therefore, the answers are 11100_5, 2404_5, 33404_5, and 121_5 with remainder 1_5. Take note of the addition algorithm in particular because the number of carries will be analyzed in Kummer's formula for the p-adic valuation of binomial coefficients in Theorem 8.15. ■

Example 7.7. Convert $B73A6_{12}$ to base-10, where $A = 10_{10}$ and $B = 11_{10}$. Also convert 178_{10} to base-4.

Solution. The first conversion is easy:

$$\begin{aligned} B73A6_{12} &= 11 \cdot 12^4 + 7 \cdot 12^3 + 3 \cdot 12^2 + 10 \cdot 12 + 6, \\ &= 228096 + 12096 + 432 + 120 + 6 \\ &= 240750_{10}. \end{aligned}$$

The second conversion is more involved. One idea is to find the digits in descending order, starting from the leading digit, in a manner reminiscent of the greedy algorithm from computer science. However, this would require us to find the smallest power of the base number greater than the integer, which would mean computing powers or logarithms. Let us instead try to find the digits in ascending order, starting with the units digit. Let $x_m x_{m-1} \dots x_1 x_0$ be the 4-ary form of 178_{10}, so that

$$178_{10} = x_m 4^m + x_{m-1} 4^{m-1} + \cdots + x_1 4 + x_0.$$

Reducing modulo 4, we get

$$178_{10} \equiv 2 \pmod 4,$$

so $x_0 = 2$ since $0 \leq x_0 < 4$. The reduction modulo 4 can be done by long (Euclidean) division. Then

$$44 = \frac{178 - 2}{4} = x_m 4^{m-1} + x_{m-1} 4^{m-2} + \cdots + x_1.$$

Again, reducing this modulo 4, we get

$$x_1 \equiv 0 \pmod 4,$$

so $x_1 = 0$. What is left over now is

$$11 = \frac{44 - 0}{4} = x_m 4^{m-2} + x_{m-1} 4^{m-3} + \cdots + x_2.$$

Continuing this process, we get $x_2 = 3$ and $x_3 = 2$, at which point we are done because the leftover bit equals 0 (try out the process and see). Thus,

$$178_{10} = 2302_4.$$

■

It should be clear that the method in Example 7.7 of reducing the integer modulo the target base number using Euclidean division works in general. In general, if conversion to and from base-10 is understood, then conversion from any base-b to any base-c is doable because base-10 can be used as an intermediary base for the conversion. That is, we would go from

base-b to base-10 to base-c. Moreover, the conversion process for negative integers boils down to the process for positive integers because it is simply a matter of tacking on a negative sign. The observation that all non-units digits disappear modulo the target base number will have further consequences when we study divisibility rules in Section 7.2 and we will see a generalization of this disappearance or annihilation phenomenon in Section 10.2.

Example 7.8. Imagine that an alien arrives on Earth and asks us about our standard positional notation. We reply that we use base-10. The alien is puzzled and asks us what base we are using when we say that we are using base "10." We say that the "10" is written in base-10. The conversation continues in this manner, potentially for the rest of eternity. How can we break the cycle by unambiguously explaining the base number?

Solution. The unary base representation

$$n = \underbrace{11\cdots1}_{n \text{ copies of } 1}{}_1$$

is unambiguous because the subscript 1 means the quantity "one" in every base $b \geq 1$. That is, even though 1 is a digit in every base, it holds that $1_b = 1_c$ for all bases b and c. In fact, it is the only non-zero digit that is a digit in every base. Thus, we may indicate our standard base as

$$10_{10} = 1111111111_1.$$

Of course, how we would indicate the meaning of the symbol 1 as "one" is another matter. Credit goes to Jonathan Love for proposing this solution when I posed the problem during our undergraduate years. ■

7.2 Divisibility Rules

Doing arithmetic in a particular base means all of our integers are represented in that base, and all of our manual computations are done with this base in the background. There should be information generated by this system of notation that we can use, similar to how industrial by-products can be used to create a new product instead of being classified as waste, or like using computational power that would otherwise be wasted. For example, each base-b system encodes information pertaining to Euclidean division of each integer with the base as the divisor, as we saw when doing base conversions: If n is a positive integer, then the units digit of n in base-b is the remainder r_0 upon Euclidean division of n by b, and the tens digit is the remainder r_1 upon Euclidean division of $\dfrac{n - r_0}{b}$ by b, and so on until the leftover part is 0. Amazingly, all of this information is available to us for free by virtue of the chosen base of a society. Let us make use of it. We will begin by proving divisibility rules in our standard base-10 and then mention how the results can be generalized to other bases via the same methods of proof.

Theorem 7.9. Let the base-10 form of a positive integer n be

$$n = x_m x_{m-1} \ldots x_1 x_0.$$

The non-trivial positive divisors of the base number 10 are $2, 5, 10$. If d is any one of these and t is a positive integer, then d^t divides n if and only if

$$d^t \mid x_{t-1}x_{t-2}\ldots x_1x_0.$$

We can append sufficiently many 0's to the far left of the form if $t-1 > m$ though in that case the test is not helpful. In other words, all digits x_i for integers $i \geq t$ do not matter in divisibility by d^t. This test is particularly effective for small t, such as $t = 1, 2, 3$, because those cases require very little computation. For $t = 1$, the criteria are equivalent to:

- $2 \mid n$ if and only if the units digit of n is $0, 2, 4, 6$, or 8. Consequently, an integer is odd if and only if its units digit is $1, 3, 5, 7$, or 9.
- $5 \mid n$ if and only if the units digit of n is 0 or 5.
- $10 \mid n$ if and only if the units digit of n is 0. This is the intersection of the divisibility criteria for 2 and 5 since 2 and 5 are coprime integers whose product is 10.

These biconditional criteria for $t = 1$ are necessary criteria for divisibility by d^t for all $t \geq 1$ because lower powers of d divide higher powers, so the negation of the criteria implies non-divisibility by d^t for $t \geq 1$. Note that 10^t divides n if and only if n has a right tail end of at least t digits equal to 0.

Proof. This boils down to reducing the base-10 expansion modulo d^t. For indices $i \geq t$, d^t divides $x_i 10^i$, so all of those terms disappear modulo d^t. For example,

$$n = x_m 10^m + x_{m-1}10^{m-1} + \cdots + x_1 10 + x_0. \equiv 10x_1 + x_0 \pmod{2^2}.$$

So $4 \mid n$ if and only if 4 divides the integer whose base-10 form is x_1x_0. The observations about $t = 1$ follow from analyzing the individual units digits $0, 1, 2, \ldots, 9$. Finally, for $t \geq 1$, a $(t-1)$-digit integer has value at most $10^t - 1 < 10^t$, so the only way that 10^t divides $x_{t-1}x_{t-2}\ldots x_1x_0$ is if

$$x_{t-1} = x_{t-2} = \cdots = x_1 = x_0 = 0.$$

■

Theorem 7.10. Let the base-10 form of a positive integer be

$$n = x_m x_{m-1}\ldots x_1x_0.$$

If d is 3 or 9, then $d \mid n$ if and only if

$$d \mid x_m + x_{m-1} + \cdots + x_1 + x_0.$$

Moreover, $11 \mid d$ if and only if

$$11 \mid (-1)^m x_m + (-1)^{m-1}x_{m-1} + \cdots - x_1 + x_0.$$

Proof. The first property is true because, for any integer $t \geq 0$ and d equal to 3 or 9,

$$10^t \equiv 1 \pmod{d}.$$

So the base expansion of n melts into

$$\begin{aligned} n &= 10^m x_m + 10^{m-1} x_{m-1} + \cdots + 10x_1 + x_0, \\ &\equiv x_m + x_{m-1} + \cdots + x_1 + x_0 \pmod{d}. \end{aligned}$$

Thus, $n \equiv 0 \pmod{d}$ if and only if

$$x_m + x_{m-1} + \cdots + x_1 + x_0 \equiv 0 \pmod{d}.$$

Similarly, if the divisor is 11, then

$$10^t \equiv (-1)^t \pmod{11},$$

so the base expansion becomes

$$\begin{aligned} n &= 10^m x_m + 10^{m-1} x_{m-1} + \cdots + 10x_1 + x_0, \\ &\equiv (-1)^m x_m + (-1)^{m-1} x_{m-1} + \cdots - x_1 + x_0 \pmod{d}. \end{aligned}$$

Thus, $n \equiv 0 \pmod{11}$ if and only if the sum of the digits of n with alternating signs is divisible by 11. ■

For the divisibility rule of 11, one might remember the fact that signs have to alternate in the sum, but one might forget whether the units digit should be given a positive or negative sign in the sum. This is not a matter of concern because the two possible sums, depending on whether the units digit is taken to be positive or negative, are negatives of each other. So 11 divides both sums or neither.

Corollary 7.11. Recall from Theorem 2.10 that, if d can be factored into $d = d_1 d_2 \cdots d_k$, where the d_i are $k \geq 2$ pairwise coprime positive integers, and an integer n is divisible by every d_i, then $d \mid n$. This leads to divisibility rules, for example, for $d = 6 = 2 \cdot 3$ and $12 = 3 \cdot 4$ in base-10. The coprimality is important because, for example, the factorization $12 = 2 \cdot 6$ is unhelpful.

Problem 7.12. Let f be the function that takes positive integers and outputs the sum of the digits of the input's base-10 representation. Let n be a positive integer. Prove that if $f(n) = f(2n)$, then $9 \mid n$.

Problem 7.13. There are no known divisibility rules for 7 that are as convenient as the others that we have seen. But the following two observations hold:

1. If $n = 10x + y$ is an integer where x and y are some integers, then $7 \mid n$ if and only if $7 \mid x - 2y$. Prove that this is true. This observation can be applied repeatedly to determine whether n is divisible by 7. For example, 98 is divisible by 7 if and only if $9 - 2 \cdot 8 = -7$ is divisible by 7, which is indeed the case. As a hint, it might be useful to use the fact that the smallest positive integer k such that $3^k \equiv 1 \pmod{7}$ is $k = 6$.

2. A positive integer n is divisible by 7 if and only if breaking up the base-10 form of n into chunks of 3-digit integers (except perhaps the leftmost chunk, which might have 1 or 2 digits instead of 3 digits) and adding up the resulting integers with alternating signs yields an integer that is divisible by 7. Prove that this works. For example, 8641969 is divisible by 7 if and only if the sum of the length-3 chunks of alternating signs

$$8 - 641 + 969$$

is divisible by 7. Since

$$8 - 641 + 969 = 336 = 7 \cdot 48$$

is divisible by 7, 7 also divides 8641969.

For very large integers, we can apply the second result, followed by several iterations of the first. As a side note that is more for novelty than practical usage, $7 \mid 10^6 - 1$. So large multiples of 7 can be broken into a sum of chunks of 6 consecutive digits, and this sum is divisible by 7 if and only if the original number is divisible by 7.

As a general note, when neither of two primes have a convenient divisibility test in base-10, it can be easy to mistake their product for a prime. Small primes that do not have a good divisibility test in base-10 include:

$$7, 13, 17, 19, 23, 29, 31, 37.$$

There are better uses of time and memory than to memorize the pairwise products of all of these numbers, but it is a good idea to memorize the product of 7 with each of the other numbers:

$\times$	13	17	19	23	29	31	37
7	91	119	133	161	203	217	259

It is also helpful to remember that $7 \cdot 11 \cdot 13 = 1001$ and $27 \cdot 37 = 999$.

Theorem 7.14. Based on the divisibility rules discussed for base-10, we can develop divisibility rules in all other bases. Let $b \geq 2$ be the base, d be the divisor, k be a positive integer, and

$$n = (x_m x_{m-1} \dots x_1 x_0)_b$$

be the dividend.

1. If $d \mid b$, then $d^k \mid n$ if and only if

$$d \mid (x_{k-1} x_{k-2} \dots x_1 x_0)_b.$$

2. If $d \mid b - 1$, then $d \mid n$ if and only if

$$d \mid x_m + x_{m-1} + \dots + x_1 + x_0.$$

3. If $d \mid b+1$, then $d \mid n$ if and only if

$$d \mid (-1)^m x_m + (-1)^{m-1} x_{m-1} + \cdots - x_1 + x_0.$$

4. If n is a product of pairwise coprime integers, each of which has a divisibility rule in base-b, then a divisibility rule for n is the logical conjunction of the rules for each of the aforementioned pairwise coprime factors of n.

5. Further rules can be derived if $d \mid b^k$ or $d \mid b^k - 1$ or $d \mid b^k + 1$, like we showed with $d = 7$ and $10^3 + 1 = 1001$. However, the usefulness of these additional tests in manual computations decreases as k increases because the "simplification" might still involve computations that are difficult to perform by hand.

Personally, I feel that $30 = 2 \cdot 3 \cdot 5$ is an excellent candidate for a new worldwide base due to the numerous divisibility rules that it accommodates, without needing too many distinct symbols for the digits. There are also benefits of base-30 with regards to terminating b-ary forms that will become evident when we study patterns in the base representations of rational numbers in Chapter 10. In fact, it is rather odd that base-30 was not used anywhere historically since it has half the number of symbols as the Babylonian base-60 system while having many of the same benefits in terms of divisibility rules and terminating forms.

Chapter 8

Combinatorial Expressions

> "A large part of mathematics which becomes useful developed with absolutely no desire to be useful, and in a situation where nobody could possibly know in what area it would become useful; and there were no general indications that it ever would be so."
>
> – *John von Neumann*

Some mathematicians are fascinated by divisibility properties of combinatorial expressions, such as the multiplicity of a particular prime in a factorial or binomial coefficient, or the remainder of such a number in a certain modulus. One example that we have already seen is Wilson's theorem. We will now see some unnamed and unattributed, yet important results, alongside celebrated theorems of Legendre, Kummer, and Lucas, and some of their corollaries.

8.1 Factorials and Binomial Coefficients

According to Wilson's theorem (Theorem 4.22), if $p \geq 2$ is an integer, then

$$(p-1)! \equiv -1 \pmod{p} \iff p \text{ is a prime.}$$

This is a number theoretic property of a combinatorial expression. Another example, one from the divisibility of binomial coefficients this time, is that the n^{th} Catalan number is

$$\frac{1}{n+1}\binom{2n}{n}.$$

This proves the non-trivial fact that $n+1$ always divides $\binom{2n}{n}$ because we proved in Volume 2 that this formula satisfies a recurrence relation on integers by a counting argument via Bertrand's ballot problem. Let us see some more examples of such standalone results before diving into somewhat more structured theorems.

Example 8.1. For each positive integer k, show that the product of any k consecutive integers is divisible by $k!$.

Solution. If 0 is included among the k integers, then the product is 0, which is certainly divisible by $k!$. If all of the k integers are negative, then multiplying their product by $(-1)^k$

reduces it to the final case, where all k of the integers are positive. In that case, if n is the largest of the k integers, then the product is

$$n(n-1)(n-2)\cdots(n-k+1) = \frac{n!}{(n-k)!} = \binom{n}{k} \cdot k!.$$

Since $\binom{n}{k}$ is an integer, $k!$ divides the $\binom{n}{k} \cdot k!$. This argument exploits the non-trivial fact that binomial coefficients are integers, despite being expressible in a formula that involves a heavy amount of division. Such is the power of combinatorial facts. ■

Example 8.2. Prove that there exist arbitrarily long finite sequences of positive integers whose terms are all composite.

Solution. For any positive integers n and k such that $1 \leq k \leq n$, the factorization

$$n! + k = k \cdot \left(\frac{n!}{k} + 1\right)$$

holds, where $\dfrac{n!}{k}$ is an integer because k is one the multiplicands in the product

$$n! = n(n-1)(n-2)\cdots 2 \cdot 1.$$

In order to engineer $n! + k$ into being composite, we choose its factor k to satisfy $2 \leq k$. Then, for any integer $n \geq 2$,

$$(n! + k)_{k=2}^{n}$$

is a sequence of $n-1$ consecutive positive integers that are all composite. ■

Problem 8.3. Prove that, for any prime p and any integer $k \in [p-1]$, $\binom{2p-k-1}{p-k}$ is divisible by p.

Such individual curiosities are endless. A mathematician who has written much about arithmetic properties of binomial coefficients is Andrew Granville. Let us put aside singular problems and move towards more generally applicable theorems.

Theorem 8.4 (Hermite's divisibility theorem)**.** Let n and k be integers such that $n \geq k \geq 1$. Then

$$\frac{n}{(n,k)} \,\Bigg|\, \binom{n}{k}.$$

In particular, if $(n,k) = 1$, then $n \,\Big|\, \binom{n}{k}$

Proof. By a simple combinatorial identity from Volume 2,

$$\binom{n}{k} = \frac{n}{k}\binom{n-1}{k-1} = \frac{\left(\frac{n}{(n,k)}\right)}{\left(\frac{k}{(n,k)}\right)}\binom{n-1}{k-1} = \frac{n}{(n,k)} \cdot \left[\binom{n-1}{k-1} \div \frac{k}{(n,k)}\right].$$

Since $\dfrac{n}{(n,k)}$ and $\dfrac{k}{(n,k)}$ are coprime, $\dfrac{k}{(n,k)}$ divides $\dbinom{n-1}{k-1}$ by Gauss's divisibility lemma, making the factor $\dbinom{n-1}{k-1} \div \dfrac{k}{(n,k)}$ an integer. Therefore, $\dfrac{n}{(n,k)}$ divides $\dbinom{n}{k}$. ■

Corollary 8.5. If $n \geq 2$ is an integer, then n is prime if and only if all of the binomial coefficients

$$\binom{n}{1}, \binom{n}{2}, \ldots, \binom{n}{n-1}$$

are divisible by n.

Proof. If n is a prime, then $(n,k) = 1$ for every integer $k \in [n-1]$. By Theorem 8.4, $\dfrac{n}{(n,k)} = n$ divides $\dbinom{n}{k}$. Conversely, suppose n is composite. Let p be any prime factor of n, and let $m = \dfrac{n}{p}$ where it is true that $2 \leq m \leq n-1$. Moreover, since n is assumed to be composite, $2 \leq p \leq n-1$. We will show that n does not divide $\dbinom{n}{p}$, which will prove the existence of a binomial coefficient in the given list that is not divisible by n. By the formula for a binomial coefficient,

$$\begin{aligned}\binom{n}{p} &= \frac{n(n-1)(n-2)\cdots(n-p+1)}{p(p-1)(p-2)\cdots 2 \cdot 1} \\ &= m \cdot \frac{(n-1)(n-2)\cdots(n-p+1)}{(p-1)(p-2)\cdots 2 \cdot 1},\end{aligned}$$

where we used $m = \dfrac{n}{p}$. The products in the numerator and denominator in

$$\alpha = \frac{(n-1)(n-2)\cdots(n-p+1)}{(p-1)(p-2)\cdots 2 \cdot 1}$$

each consists of $p-1$ consecutive integers. By Example 8.1, the denominator $(p-1)!$ divides the numerator, so α is an integer. Suppose, for contradiction, that $n = mp$ divides $\dbinom{n}{p} = m\alpha$. Then p divides α. But n is divisible by p, which means that none of the $p-1$ integers right before it, which are the multiplicands of the numerator of α, are divisible by p (this is due to how multiples of an integer are spaced out among the integers). By the contrapositive of Euclid's lemma, α is not divisible by p either, which is a contradiction. Thus, n does not divide $\dbinom{n}{p}$. ■

Corollary 8.6 (Frobenius endomorphism)**.** If x and y are integers and p is a prime, then

$$(x+y)^p \equiv x^p + y^p \pmod{p}.$$

It follows by induction on integers $k \geq 1$ that

$$(x+y)^{p^k} \equiv x^{p^k} + y^{p^k} \pmod{p}.$$

For those interested in abstract algebra, this is the essential ingredient in proving that, in a commutative ring of characteristic p, the Frobenius endomorphism $r \mapsto r^p$ is a ring homomorphism.

Proof. By Corollary 8.5 and the binomial theorem, all intermediate terms disappear modulo p to give

$$(x+y)^p \equiv \sum_{i=0}^{p} \binom{p}{i} x^i y^{p-i} \equiv \binom{p}{0} y^p + \binom{p}{p} x^p \equiv x^p + y^p \pmod{p},$$

since all of the intermediate terms disappear. ■

Example 8.7. Wolstenholme's theorem says that, for any non-negative integers $a \geq b$ and prime $p \geq 5$,

$$\binom{ap}{bp} \equiv \binom{a}{b} \pmod{p^3}.$$

This is not known to have an easy proof, but we challenge the reader to prove the following weaker result: If a and b are non-negative integers such that $a \geq b$, then for any prime p,

$$\binom{ap}{bp} \equiv \binom{a}{b} \pmod{p}.$$

As a hint, the Frobenius endomorphism could be helpful.

Solution. To bring the binomial coefficient $\binom{ap}{bp}$ into play, we will use the binomial theorem to expand

$$(x+1)^{ap} = \sum_{i=0}^{ap} \binom{ap}{i} x^i,$$

where $\binom{ap}{bp}$ is one of the coefficients in the expansion because

$$a \geq b \geq 0 \implies ap \geq bp \geq 0.$$

A different way of expanding the same binomial expression, except reduced modulo p using the Frobenius endomorphism, is

$$((x+1)^p)^a \equiv (x^p+1)^a \equiv \sum_{j=0}^{a} \binom{a}{j} x^{jp} \pmod{p}.$$

By comparing the coefficients of x^{bp} in the two expansions modulo p ($i = bp$ and $j = b$), we find that

$$\binom{ap}{bp} \equiv \binom{a}{b} \pmod{p}.$$

■

In the solution to Example 8.7, the congruence of formal polynomials (where "formal" means that x is just a dummy variable that is a tool for organizing information instead of representing a number) simply means that coefficients of pairs of terms to the same powers of x on opposite sides of the equation are congruent modulo the modulus. Technically, this depends on multiplication in the ring of formal polynomials being associative. We have proven this in the more general context of generating functions in Volume 2.

Example 8.8 (Eisenstein's criterion on p^{th} cyclotomic polynomial)**.** A polynomial $f \in \mathbb{Z}[x]$ is said to be **irreducible** over $\mathbb{Q}$ if there do not exist two non-constant polynomials g and h in $\mathbb{Q}[x]$ such that $f = gh$. Eisenstein's criterion states that a polynomial

$$f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \in \mathbb{Z}[x]$$

is irreducible over $\mathbb{Q}$ if there exists a prime p such that all of the following conditions hold:

- p divides each of $a_0, a_1, \ldots, a_{n-1}$
- p does not divide a_n
- p^2 does not divide a_0

Taking Eisenstein's criterion for granted, prove that, for any prime p, the p^{th} cyclotomic polynomial

$$\Phi_p(x) = 1 + x + x^2 + \cdots + x^{p-1}$$

is irreducible over $\mathbb{Q}$. (For the reader's reference, the same formula does *not* hold for the n^{th} cyclotomic polynomial when n is not a prime. See Section 13.2 for an extended discussion in cyclotomic polynomials.)

Solution. Clearly, Eisenstein's criterion cannot be applied directly to $\Phi_p(x)$ because all of the coefficients are 1. We will apply Eisenstein indirectly by applying a shift to the polynomial by some integer $a \in \mathbb{Q}$. That is, we claim that $f(x)$ is irreducible over $\mathbb{Q}$ if and only if $f(x+a)$ is irreducible over $\mathbb{Q}$ for any rational a. This is easily seen by considering the contrapositive: $f(x)$ can be factored over $\mathbb{Q}$ if and only if $f(x+a)$ can be factored over $\mathbb{Q}$ because:

$$\begin{aligned} f(x) = g(x)h(x) &\implies f(x+a) = g(x+a)h(x+a) \\ f(x+a) = r(x)s(x) &\implies f(x) = r(x-a)s(x-a). \end{aligned}$$

So we perform a shift by +1 in order to get binomial coefficients:

$$\begin{aligned} f(x+1) &= 1 + (x+1) + (x+1)^2 + \cdots + (x+1)^{p-1} \\ &= \frac{(x+1)^p - 1}{(x+1) - 1} \\ &= \binom{p}{1} + \binom{p}{2}x + \binom{p}{3}x^2 + \cdots \binom{p}{p-1}x^{p-2} + \binom{p}{p}x^{p-1} \\ &= p + \binom{p}{2}x + \binom{p}{3}x^2 + \cdots + \binom{p}{p-1}x^{p-2} + x^{p-1}. \end{aligned}$$

Note that this matches the value of $f(x+1)$ at $x = 0$ as well as all over real values; we mention this since the $x = 0$ case has to be handled separately as $x \neq 0$ in $\dfrac{(x+1)^p - 1}{(x+1) - 1}$ to prevent division by 0. All of the conditions of Eisenstein's criterion are fulfilled, where we have invoked Corollary 8.5 for asserting that the middle terms are all divisible by p. ■

8.2 Legendre, Kummer, and Lucas

To conclude our study of number theoretic properties of combinatorial expressions, we will study three famous results in this area, attributed to Legendre, Kummer, and Lucas.

Theorem 8.9 (Legendre's formula)**.** If p is a prime and n is a positive integer, then the number of times that p divides $n!$ is

$$\nu_p(n!) = \sum_{k=1}^{\infty} \left\lfloor \frac{n}{p^k} \right\rfloor.$$

Despite giving the appearance of an infinite sum, this is actually a finite sum because all terms of sufficiently high index are 0. Moreover, if the base-p form of n is

$$n = (a_m a_{m-1} \ldots a_1 a_0)_p,$$

then another way of calculating the same quantity is

$$\nu_p(n!) = \frac{n - s_p(n)}{p-1},$$

where $s_p(n)$ is the sum of the base-p digits

$$a_m + a_{m-1} + \cdots + a_1 + a_0.$$

Proof. Let the highest power of p that is less than or equal to n be p^m, where we note that m matches the same variable in the second formula stated. For each $j \in [m]$, let t_j be the number of integers $i \in [n]$ such that $\nu_p(i) = j$, so p divides i *exactly* j times. Then

$$\nu_p(n!) = \sum_{k=1}^{n} \nu_p(i) = \sum_{j=1}^{m} j t_j = \sum_{j=1}^{m} \sum_{k=1}^{j} t_j.$$

By the discrete Fubini's principle, we can switch the order of the sums so that this is equal to

$$\sum_{k=1}^{m}\sum_{j=k}^{m} t_j.$$

Here, the inner sum counts the number of integers $i \in [n]$ such that p divides i *at least* k times. So the inner sum is the number of multiples of p^k in $[n]$, which is equal to $\left\lfloor \frac{n}{p^k} \right\rfloor$ by Corollary 1.4. This proves the first formula for $\nu_p(n!)$. Can you think of a counterexample where the formula does not work when p is replaced by a composite number?
Now we tackle the formula with the sum of digits. For each index $k \in [m]$,

$$\begin{aligned}\frac{n}{p^k} &= \frac{a_m p^m + a_{m-1}p^{m-1} + \cdots + a_1 p + a_0}{p^k} \\ &= a_m p^{m-k} + a_{m-k-1}p^{m-1} + \cdots + a_{k+1}p + a_k + \frac{a_{k-1}p^{k-1} + \cdots + a_1 p + a_0}{p^k}.\end{aligned}$$

The fraction at the end is bounded above by

$$\begin{aligned}\frac{(p-1)p^{k-1} + \cdots + (p-1)p + (p-1)}{p^k} &= \frac{(p-1)(p^{k-1} + \cdots + p + 1)}{p^k} \\ &= \frac{p^k - 1}{p^k} = 1 - \frac{1}{p^k} < 1.\end{aligned}$$

So once we take the floor function, the fraction disappears and we are left with

$$\left\lfloor \frac{n}{p^k} \right\rfloor = \sum_{j=k}^{m} a_j p^{j-k}.$$

By the first formula for $\nu_p(n!)$ and the discrete Fubini's principle again,

$$\begin{aligned}\nu_p(n!) &= \sum_{k=1}^{m} \left\lfloor \frac{n}{p^k} \right\rfloor = \sum_{k=1}^{m}\sum_{j=k}^{m} a_j p^{j-k} \\ &= \sum_{j=1}^{m}\sum_{k=1}^{j} a_j p^{j-k} = \sum_{j=1}^{m} a_j (p^{j-1} + \cdots + p^2 + p + 1) \\ &= \sum_{j=1}^{m} \frac{a_j(p^j - 1)}{p-1} \\ &= \frac{1}{p-1} \cdot \left(\sum_{j=1}^{m} a_j p^j - \sum_{j=1}^{m} a_j \right) = \frac{1}{p-1} \cdot \left(\sum_{j=0}^{m} a_j p^j - \sum_{j=0}^{m} a_j \right) \\ &= \frac{n - s_p(n)}{p-1}.\end{aligned}$$

Note that we used $a_0 p^0 - a_0 = 0$ in the second-last step to reach the final expression. ■

Problem 8.10. Let p be a prime, $n \geq 2$ be an integer, and let $s_p(n)$ denote the sum of the digits of the base-p representation of n. Prove that

$$\nu_p(n) = \frac{1 - s_p(n) + s_p(n-1)}{p-1}.$$

Problem 8.11. Prove that, if p is a prime and k is a positive integer, then

$$\nu_p(p^k!) = \frac{p^k - 1}{p-1}.$$

Problem 8.12. Prove that, if $m \geq 2$ is an integer with prime factorization

$$m = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$$

and n is a positive integer, then the maximal power of m that divides n is

$$\min\left\{ \left\lfloor \frac{\nu_{p_i}(n)}{e_i} \right\rfloor : i \in [k] \right\}.$$

If n is replaced by the factorial $n!$, then the numerator in each fraction can be computed efficiently using Legendre's formula. Use this to determine the number of 0's with which the base-10 form of 99! ends.

Lemma 8.13. Let $n \geq 2$ be an integer. Then the sequence of numbers

$$\binom{n}{0}, \binom{n}{1}, \binom{n}{2}, \ldots, \binom{n}{\lfloor \frac{n}{2} \rfloor}$$

is monotonically increasing. Consequently, the sequence

$$\binom{n}{\lceil \frac{n}{2} \rceil}, \ldots, \binom{n}{n-2}, \binom{n}{n-1}, \binom{n}{n}$$

is monotonically decreasing.

Proof. We can start with the inequality

$$\binom{n}{k-1} < \binom{n}{k}$$

and take the following reversible steps:

$$1 < \frac{\binom{n}{k}}{\binom{n}{k-1}} = \frac{\left(\frac{n!}{k!(n-k)!}\right)}{\left(\frac{n!}{(k-1)!(n-k+1)!}\right)} = \frac{(k-1)!(n-k+1)!}{k!(n-k)!} = \frac{n-k+1}{k}$$

$$\iff 2k < n+1 \iff 2k \leq n \iff k \leq \frac{n}{2} \iff k \leq \left\lfloor \frac{n}{2} \right\rfloor.$$

This proves the monotonically increasing property. The symmetry property

$$\binom{n}{k} = \binom{n}{n-k}$$

of Pascal's triangle implies that, after the middle point of the row, the binomial coefficients monotonically decline in value. ∎

Example 8.14. Find all non-negatives integers n and k such that $\binom{n}{k}$ is a prime power.

Solution. By writing out the rows of Pascal's triangle up to row $n = 8$, we notice patterns beginning to emerge among the prime power entries.

$$
\begin{array}{ccccccccccccccccc}
 & & & & & & & 1 & & & & & & & & & \\
 & & & & & & 1 & & 1 & & & & & & & & \\
 & & & & & 1 & & \boxed{2} & & 1 & & & & & & & \\
 & & & & 1 & & \boxed{3} & & \boxed{3} & & 1 & & & & & & \\
 & & & 1 & & \boxed{4} & & 6 & & \boxed{4} & & 1 & & & & & \\
 & & 1 & & \boxed{5} & & 10 & & 10 & & \boxed{5} & & 1 & & & & \\
 & 1 & & 6 & & 15 & & 20 & & 15 & & 6 & & 1 & & & \\
1 & & \boxed{7} & & 21 & & 35 & & 35 & & 21 & & \boxed{7} & & 1 & & \\
1 & & \boxed{8} & & 28 & & 56 & & 70 & & 56 & & 28 & & \boxed{8} & & 1
\end{array}
$$

The far left and far right diagonals consist of all 1's, and this is always true because

$$\binom{n}{0} = \binom{n}{n} = 1.$$

So the numbers at the extreme left and right ends of each row are not prime powers. Moving into the triangle by one place from the left and right, we notice that n is a prime power if and only if

$$\binom{n}{1} = \binom{n}{n-1} = n$$

is a prime power for $n \geq 2$. However, there seem to be no other prime powers, so we will take it upon ourselves to prove that: If n and k are integers such that $2 \leq k \leq n-2$ (note that this means $n \geq 4$), then $\binom{n}{k}$ is not a prime power.

Suppose n and k are integers as stated above and suppose, for contradiction, and $\binom{n}{k}$ is a power of some prime p. By Legendre's formula and the formula for a binomial coefficient in terms of factorials,

$$\nu_p\left[\binom{n}{k}\right] = \sum_{i=1}^{\infty}\left(\left\lfloor\frac{n}{p^i}\right\rfloor - \left\lfloor\frac{k}{p^i}\right\rfloor - \left\lfloor\frac{n-k}{p^i}\right\rfloor\right).$$

Letting m be the integer such that p^m is the highest power of p that is less than or equal to n, we can reduce this infinite sum to the finite sum

$$\nu_p\left[\binom{n}{k}\right] = \sum_{i=1}^{m}\left(\left\lfloor\frac{n}{p^i}\right\rfloor - \left\lfloor\frac{k}{p^i}\right\rfloor - \left\lfloor\frac{n-k}{p^i}\right\rfloor\right).$$

By the well-known floor function sum bounds (covered in Volume 1)

$$\lfloor x\rfloor + \lfloor y\rfloor \leq \lfloor x+y\rfloor \leq \lfloor x\rfloor + \lfloor y\rfloor + 1,$$

we find that

$$\left\lfloor \frac{k}{p^i} \right\rfloor + \left\lfloor \frac{n-k}{p^i} \right\rfloor \geq \left\lfloor \frac{k}{p^i} + \frac{n-k}{p^i} \right\rfloor - 1 = \left\lfloor \frac{n}{p^i} \right\rfloor - 1.$$

Rearranging, we get

$$\left\lfloor \frac{n}{p^i} \right\rfloor - \left\lfloor \frac{k}{p^i} \right\rfloor - \left\lfloor \frac{n-k}{p^i} \right\rfloor \leq 1,$$

which, by Legendre, leads to

$$\nu_p \left[\binom{n}{k} \right] \leq \sum_{i=1}^{m} 1 = m.$$

This allows us to produce the bound

$$\binom{n}{k} = p^{\nu_p\left[\binom{n}{k}\right]} \leq p^m \leq n.$$

By Lemma 8.13, a binomial coefficient in row n of Pascal's triangle is n or smaller for only the first two or last two entries in that row. Therefore, $\binom{n}{k}$ is a prime power if and only if n is a prime power and $k = 1$ or $k = n - 1$. ■

Theorem 8.15 (Kummer's theorem)**.** If p is a prime, and n and k are integers such that $n \geq k \geq 0$, then $\nu_p \left[\binom{n}{k} \right]$ is equal to the number of carries that occur in the standard addition algorithm when the base-p forms of k and $n - k$ are added to get the base-p form of n.

Proof. We need to undertake the unusual task of making precise when carrying occurs and how to count the number of carries in the standard addition algorithm. These are not questions that are ordinarily asked because we usually blindly implement the addition algorithm. Let the base-p forms of $k, n-k, n$ be

$$\begin{aligned} k &= (a_m a_{m-1} \dots a_1 a_0)_p, \\ n-k &= (b_m b_{m-1} \dots b_1 b_0)_p, \\ n &= (c_m c_{m-1} \dots c_1 c_0)_p, \end{aligned}$$

where the forms of k and $n-k$ are modified by padding leading digits equal to 0 (i.e. on the left) if needed to match the number of digits of n. There are two benefits of this padding: we have a uniform number of digits on which to perform computations across all three forms, and there will not be any carrying in the final leftmost step of the addition (why?). It is never necessary to pad the form of n with 0's because the number of digits in the original forms of k and $n - k$ are less than or equal to the number of digits in the form of n since $k \leq n$ and $n - k \leq n$.

Carrying occurs at a particular step if the sum of a_i, b_i and the carried part of the previous step is p or greater. So we recognize the carried components recursively as

$$d_0 = \begin{cases} 0 & \text{if } a_0 + b_0 < p \\ 1 & \text{if } a_0 + b_0 \geq p \end{cases},$$

or, if i is an integer such that $1 \leq i < m$,

$$d_i = \begin{cases} 0 & \text{if } a_i + b_i + d_{i-1} < p \\ 1 & \text{if } a_i + b_i + d_{i-1} \geq p \end{cases},$$

and there is no carrying in the final step as mentioned before, thanks to the potential padding, since otherwise n would have a leading digit even farther to the left than c_m. As we know from the addition algorithm,

$$c_i = \begin{cases} a_0 + b_0 - pd_0 & \text{if } i = 0 \\ a_i + b_i + d_{i-1} - pd_i & \text{if } 1 \leq i \leq m-1 \\ a_m + b_m + d_{m-1} & \text{if } i = m \end{cases}.$$

By the second form of Legendre's formula (Theorem 8.9) and the complete additivity of ν_p,

$$\begin{aligned} \nu_p\left[\binom{n}{k}\right] &= \nu_p\left(\frac{n!}{k!(n-k)!}\right) \\ &= \nu_p(n!) - \nu_p(k!) - \nu_p((n-k)!) \\ &= \frac{n - s_p(n)}{p-1} - \frac{k - s_p(k)}{p-1} - \frac{n-k-s_p(n-k)}{p-1} \\ &= \frac{s_p(k) + s_p(n-k) - s_p(n)}{p-1}. \end{aligned}$$

After the digits are regrouped to be together according to their indices in the numerator, the numerator is equal to

$$\begin{aligned} &(a_0 + b_0 - c_0) + (a_1 + b_1 - c_1) + \cdots + (a_m + b_m - c_m) \\ &= pd_0 + (pd_1 - d_0) + (pd_2 - d_1) + \cdots + (pd_{m-1} - d_{m-2}) - d_{m-1} \\ &= (p-1)d_0 + (p-1)d_1 + \cdots + (p-1)d_{m-2} + (p-1)d_{m-1} \\ &= (p-1)(d_0 + d_1 + \cdots + d_{m-1}). \end{aligned}$$

Thus, $\nu_p\left[\binom{n}{k}\right] = d_0 + d_1 + \cdots + d_{m-1}$, which is the total number of carries, as required. ■

Problem 8.16. Let n be a positive integer. Prove that 4 divides $\binom{2n}{n}$ if and only if n is not 1 or any other power of 2.

Theorem 8.17 (Lucas's theorem)**.** Let a and b be non-negative integers such that $a \geq b$. Let p be a prime and the base-p forms of a and b be

$$\begin{aligned} a &= (a_m a_{m-1} \ldots a_1 a_0)_p, \\ b &= (b_m b_{m-1} \ldots b_1 b_0)_p, \end{aligned}$$

where at most one of these two forms is modified by padding sufficiently many leading digits equal to 0 if needed so that both forms have the same number of digits. Then

$$\binom{a}{b} = \prod_{k=0}^{m} \binom{a_k}{b_k} \pmod{p},$$

where we use the convention that $\binom{x}{y} = 0$ if $x < y$. This implies the second form of Lucas's theorem, which asserts that

$$\binom{a}{b} \equiv \binom{\lfloor a/p \rfloor}{\lfloor b/p \rfloor} \binom{a_0}{b_0} \pmod{p}.$$

Proof. The following proof was published by Nathan Fine [7]. One way of expanding $(1+x)^a$ is

$$(1+x)^a = \sum_{i=0}^{a} \binom{a}{i} x^i,$$

by the binomial theorem. Since

$$a = a_m p^m + a_{m-1} p^{m-1} + \cdots + a_1 p + a_0,$$

another method of expansion is

$$\begin{aligned}(1+x)^a &= (1+x)^{a_m p^m + a_{m-1} p^{m-1} + \cdots + a_1 p + a_0} \\ &= ((1+x)^{p^m})^{a_m} ((1+x)^{p^{m-1}})^{a_{m-1}} \cdots ((1+x)^p)^{a_1} (1+x)^{a_0}.\end{aligned}$$

Modulo p, the Frobenius endomorphism (Corollary 8.6) tells us that this is congruent to

$$\prod_{i=0}^{m} (1+x^{p^i})^{a_i} \equiv \prod_{i=0}^{m} \left(\sum_{j=0}^{a_i} \binom{a_i}{j} x^{p^i j} \right) \pmod{p}.$$

If $a_i = 0$ for some i, then the inner sum at the corresponding index i is interpreted as $\binom{0}{0} = 1$. Since the a_i are digits in base-p, it holds for each index i that $0 \leq a_i \leq p-1$. Thanks to the convention that $\binom{x}{y} = 0$ if $x < y$, we can bump up the upper bound of j from a_i to $p-1$ for each i to get the more uniform-looking expression

$$\prod_{i=0}^{m} \left(\sum_{j=0}^{p-1} \binom{a_i}{j} x^{j p^i} \right).$$

Expanding this product of sums, where each sum has p terms, yields terms in which the exponent of x is of the form

$$j_0 p^0 + j_1 p^1 + \cdots + j_m p^m$$

with corresponding coefficient

$$\binom{a_0}{j_0}\binom{a_1}{j_1}\cdots\binom{a_m}{j_m},$$

with the lower components j_ℓ lying in $[p-1]^*$. There are p^m such terms and collecting like terms is unnecessary because all of those exponents are unique integers, due to the uniqueness of base-p forms of integers. Therefore, by comparing the coefficients of x^b in the two expansions modulo p, we find that

$$\binom{a}{b} = \prod_{k=0}^{m}\binom{a_k}{b_k} \pmod{p}.$$

For the second form, note that the base-p expansions of a and b tell us that

$$\lfloor a/p \rfloor = (a_m a_{m-1}\ldots a_1)_p,$$
$$\lfloor b/p \rfloor = (b_m b_{m-1}\ldots b_1)_p,$$

By the first form of Lucas's theorem,

$$\binom{\lfloor a/p \rfloor}{\lfloor b/p \rfloor} \equiv \binom{a_m}{b_m}\binom{a_{m-1}}{b_{m-1}}\cdots\binom{a_1}{b_1} \pmod{p}.$$

The second form follows by multiplying both sides by $\binom{a_0}{a_0}$ and using the first form of Lucas's theorem on the right side. ■

Example 8.18. For any prime p and positive integer n such that $n \geq p$, prove that

$$\binom{n}{p} \equiv \left\lfloor \frac{n}{p} \right\rfloor \pmod{p}.$$

Solution. This looks like a job for Lucas. Let the base-p representation of n be

$$n = (a_k a_{k-1}\ldots a_1 a_0)_p.$$

The base-p representation of p is 10_p. By Lucas's theorem,

$$\binom{n}{p} \equiv \binom{a_k}{0}\binom{a_{k-1}}{0}\cdots\binom{a_2}{0}\binom{a_1}{1}\binom{a_0}{0} \equiv \binom{a_1}{1} \equiv a_1 \pmod{p}.$$

On the other hand, we can compute that

$$\begin{aligned}\left\lfloor \frac{n}{p} \right\rfloor &= \left\lfloor \frac{a_k p^k + a_{k-1}p^{k-1} + \cdots + a_2 p^2 + a_1 p + a_0}{p} \right\rfloor \\ &= a_k p^{k-1} + a_{k-1}p^{k-2} + \cdots + a_2 p + a_1 + \left\lfloor \frac{a_0}{p} \right\rfloor \\ &\equiv a_1 \pmod{p},\end{aligned}$$

where we used the fact that $0 \leq a_0 < p$ in the last step to compute $\left\lfloor \frac{a_0}{p} \right\rfloor = 0$. Equating the two results in a congruence modulo p yields what we wanted. ■

Problem 8.19. Let p be a prime, and k and n be positive integers. Prove that

$$\binom{p^n k}{p^n} \equiv k \pmod{p}.$$

Example 8.20. Let $n \geq 2$ be an integer and $\alpha = \gcd\left[\binom{n}{1}, \binom{n}{2}, \ldots, \binom{n}{n-1}\right]$. Prove that

$$\alpha = \begin{cases} 1 & \text{if } n \text{ is not a prime power} \\ p & \text{if } n \text{ is a power of a prime } p \end{cases}.$$

Solution. Let the prime factorization of n be

$$n = p_1^{e_1} p_2^{e_2} \cdots p_m^{e_m}.$$

Since $n = \binom{n}{1}$ is among the $n-1$ integers in the list, it suffices, in the case where n is not a prime power, to show that, for each prime factor p_i, there is a binomial coefficient in the list that is not divisible by p_i. Let $n_i = \dfrac{n}{p_i^{e_i}}$. By Problem 8.19,

$$\binom{n}{p_i^{e_i}} = \binom{n_i p_i^{e_i}}{p_i^{e_i}} \equiv n_i \not\equiv 0 \pmod{p_i}.$$

So there is no prime factor of $\binom{n}{1} = n$ that divides all $\binom{n}{i}$ for $i \in [n-1]$, resulting in $\alpha = 1$.

On the other hand, suppose $n = p^k$ for some prime p and positive integer k. Since $\alpha \,\Big|\, \binom{p^k}{1}$, the only prime that can divide α is p. By a variant of the Frobenius endomorphism for formal polynomials,

$$(x+y)^{p^k} \equiv x^{p^k} + y^{p^k} \pmod{p},$$

so p does in fact divide each of

$$\binom{p^k}{1}, \binom{p^k}{2}, \ldots, \binom{p^k}{p^k - 1}.$$

All we need to do is show that $\nu_i\left[\binom{p^k}{i}\right] = 1$ for some $i \in [p^k - 1]$. We will show this for $i = p^{k-1}$ because the simplicity of the base-p forms of powers of p make it easy to apply Kummer. By Kummer's theorem, $\nu_p\left[\binom{p^k}{p^{k-1}}\right]$ is the number of carries that occur when p^{k-1} and $p^k - p^{k-1} = p^{k-1}(p-1)$ are added using the addition algorithm in base-p. The

base-p forms of p^{k-1} and $p^{k-1}(p-1)$ are

$$p^{k-1} = 1 \underbrace{00\ldots0}_{k-1 \text{ digits of } 0},$$
$$p^{k-1}(p-1) = (p-1) \underbrace{00\ldots0}_{k-1 \text{ digits of } 0}.$$

The only carrying that occurs is at on the far left when adding the digits 1 and $p-1$. Since there is only one carry, $\nu_p\left[\binom{p^k}{p^{k-1}}\right] = 1$ and $\alpha = p$. We left this example for the end because it nicely combines the Frobenius endomorphism, Lucas, and Kummer. ■

Chapter 9

Modular Exponentiation

> "Not only is the above combinatorial proof much shorter than our previous proof, but it also makes the reason for the simple answer completely transparent. It is often the case, as occurred here, that the first proof to come to mind turns out to be laborious and inelegant, but that the final answer suggests a simpler combinatorial proof."
>
> – *Richard Stanley, Enumerative Combinatorics I*

> "First of all, [the classification of finite simple groups] takes so many pages to prove; it seems to me the degree of understanding must be pretty limited if that is the only way it can be done."
>
> – *Michael Atiyah, The Mathematical Intelligencer*

Given a binary operation on a set, a question that can be asked is whether one element or several elements can be used to "generate" the whole set of elements by repeatedly applying the binary operation to the special elements. For example, adding 1 to itself repeatedly generates the positive integers, and the same is true for finite products of primes. This question of determining "building blocks" is worth pursuing with other mathematical structures. In a particular, we will now look at the extent to which the powers of an element modulo n generates all elements modulo n.

9.1 Multiplicative Order

Let us investigate additive and multiplicative generation in modular arithmetic. The additive question is not difficult so we will relegate it to the next problem, and then focus on the multiplicative question. Consider the following example:

$$\begin{aligned}
0 &\equiv 0 \pmod 6,\\
1+1+1+1+1+1 &\equiv 0 \pmod 6,\\
2+2+2 &\equiv 0 \pmod 6,\\
3+2 &\equiv 0 \pmod 6,\\
4+4+4 &\equiv 0 \pmod 6,\\
5+5+5+5+5+5 &\equiv 0 \pmod 6.
\end{aligned}$$

Adding enough copies of a residue a to itself to get 0 is just one step away from adding enough copies of a to itself to get a again, causing a loop. So this area of exploration mimics the cyclic nature of clocks.

Problem 9.1. Let n be a positive integer. For each integer a, we are interested in

$$ka = \underbrace{a + a + \cdots + a}_{k \text{ copies of } a}$$

as k ranges over the integers. If k is negative, then we interpret it as $ka = (-k)(-a)$ which is the sum of $-k$ copies of $-a$, or as the negative of $(-k)a$ which is the negative of $-k$ copies of a.

1. For any integer a, show that $ka \equiv 0 \pmod{n}$ if and only if k is a multiple of $\dfrac{n}{(a,n)}$. Deduce that the smallest positive integer k such that $ka \equiv 0 \pmod{n}$ is $\dfrac{n}{(a,n)}$, and that the number of residue classes represented by the elements of $R = \{ka : k \in \mathbb{Z}\}$ is $\dfrac{n}{(a,n)}$.
2. Show that $R = \{ka : k \in \mathbb{Z}\}$ contains a representative from every residue class modulo n if and only if $(a, n) = 1$, and that, in this case, any n consecutive terms

   $$\{ia, (i+1)a, \ldots, (i+n-1)a\}$$

   form a complete residue system.

Problem 9.1 resolves the questions of additive cyclicity, which allows us to turn to the more intricate problem of multiplicative generation.

Definition 9.2. For a positive integer n and an integer a coprime to n, the **order** of a modulo n is defined as the smallest positive integer k such that

$$a^k \equiv 1 \pmod{n}.$$

By Euler's congruence (Theorem 4.25), one possible value of k is $\varphi(n)$, so such a minimal positive k must exist by the well-ordering principle and it lies in $[\varphi(n)]$. The order of a modulo n is denoted by $\operatorname{ord}_n(a)$.

Note that this sense of order cannot apply to integers a that are not coprime to n because (a, n) has to divide 1 due to the equation version of the congruence $a^k \equiv 1 \pmod{n}$. We will explore a notion similar to order for such a in Theorem 10.17.

Problem 9.3. Let n be a positive integer, a be an integer coprime to n, and i, j be distinct integers. Show that, if

$$a^i \equiv a^j \equiv 1 \pmod{n},$$

then $a^{(i,j)} \equiv 1 \pmod{n}$. Note that since i, j are distinct, at least one of them is non-zero, which allows the greatest common divisor (i, j) to exist.

There are no excellent known ways of computing the order of a integer in a modulus in general, but we can make some helpful observations as follows.

Theorem 9.4. For any positive integer n, an integer a coprime to n, and an integer k,

$$a^k \equiv 1 \pmod{n}$$

if and only if k is a multiple of $\mathrm{ord}_n(a)$. As a consequence:

1. $\mathrm{ord}_n(a)$ divides $\varphi(a)$
2. $a^i \equiv a^j$ if and only if $i \equiv j \pmod{\mathrm{ord}_n(a)}$
3. Letting $m = \mathrm{ord}_n(a)$, the residues classes represented by the elements of
$$S = \{1, a, a^2, \ldots, a^{m-1}\}$$
are all distinct and all powers of a modulo n fall into one of these classes.

Proof. We will use a common trick from number theory: by taking a remainder, the minimality (in some sense) of some positive integer will be contradicted unless the remainder equals 0. Clearly, if k is a multiple of $\mathrm{ord}_n(a)$, then $a^k \equiv 1 \pmod{n}$. For the converse, suppose for contradiction that there is an integer k that is not a multiple of $\mathrm{ord}_n(a)$ such that

$$a^k \equiv 1 \pmod{n}.$$

By Euclidean division of k by $\mathrm{ord}_n(a)$, we get

$$k = q \cdot \mathrm{ord}_n(a) + r, \text{ and } 0 < r < \mathrm{ord}_n(a).$$

Then

$$\begin{aligned} a^r &= a^{k - q \cdot \mathrm{ord}_n(a)} \\ &= a^k \cdot (a^{\mathrm{ord}_n(a)})^{-q} \\ &\equiv 1^k \cdot 1^{-q} \equiv 1 \pmod{n}, \end{aligned}$$

contradicting the fact that $\mathrm{ord}_n(a)$ is the minimal positive exponent that sends a to 1. For the consequences:

1. By Euler's congruence,
$$a^{\varphi(n)} \equiv 1 \pmod{n}.$$
So $\varphi(n)$ is a multiple of $\mathrm{ord}_n(a)$.
2. If i and j are integers, then we can take the following biconditional steps:
$$\begin{aligned} a^i \equiv a^j \pmod{n} &\iff a^{i-j} \equiv 1 \pmod{n} \\ &\iff \mathrm{ord}_n(a) \mid i - j \\ &\iff i \equiv j \pmod{\mathrm{ord}_n(a)}. \end{aligned}$$

3. In order to not contradict the last point, the $m = \text{ord}_n(a)$ consecutive powers of a in S must all lie in different residues. If a^k is some power of a for an integer k, then Euclidean division of k by m yields
$$a^k \equiv a^{qm+r} \equiv a^r \pmod{n}.$$
Since $0 \leq r < m$, a^k is congruent to some power a^r in S.

■

The following is an exceptional case in which we can compute an infinite sequence of orders.

Problem 9.5. Take the following steps for all integers $n \geq 3$:

1. Prove by induction on n that $\nu_2\left(5^{2^{n-2}} - 1\right) = n$.
2. Show that the $\text{ord}_{2^n}(5) = 2^{n-2}$.
3. Deduce that $S = \left\{\pm 5^k : k \in \left[2^{n-2}\right]\right\}$ is a reduced residue system modulo 2^n.

This problem will be helpful when we are counting modular power residues in Problem 11.9.

Example 9.6. Let n be a positive integer and $a \geq 2$ be an integer. Prove that
$$n \mid \varphi(a^n - 1).$$

Solution. This is a classic problem that students of group theory are typically asked to prove, but it is amenable to elementary methods. If we could show that $\text{ord}_{(a^n-1)}(a) = n$, then it would follow that $n \mid \varphi(a^n - 1)$ due to Euler's congruence. Note that
$$a^n - 1 \equiv 0 \pmod{a^n - 1},$$
so $a^n \equiv 1 \pmod{a^n - 1}$. This by itself proves the result for $n = 1$ since there are no lower powers of a in that case. For $n = 2$, we need to show that for all $k \in [n-1]$,
$$a^k \not\equiv 1 \pmod{a^n - 1}.$$
If it were true that
$$a^k - 1 \equiv 0 \pmod{a^n - 1},$$
then $a^n - 1 \mid a^k - 1$. Since $a \geq 2$, the divisor $a^n - 1$ and dividend $a^k - 1$ are both positive, which forces
$$a^n - 1 \mid a^k - 1 \implies a^n - 1 \leq a^k - 1 \implies n \leq k.$$
This contradicts the fact that $k \in [n-1]$. Thus, $\text{ord}_{(a^n-1)}(a) = n$ and so $n \mid \varphi(a^n - 1)$. ■

Problem 9.7 (Lehmer's theorem). As we know, a full converse to Fermat's little theorem that establishes primality of the modulus is impossible due to the existence of Carmichael numbers. As a partial converse, prove Lehmer's theorem (it appears in [11]): Let $n \geq 2$ be an integer. If there exists an integer a such that
$$a^{n-1} \equiv 1 \pmod{n},$$
and for all prime factors p of $n - 1$,
$$a^{\frac{n-1}{p}} \not\equiv 1 \pmod{n},$$
then n is prime. As a hint, first prove that $\text{ord}_n(a) = n - 1$.

The following is a very useful way of computing an order using another order.

Theorem 9.8. If n is a positive integer and a is an integer coprime to n, then for any integer k,

$$\operatorname{ord}_n(a^k) = \frac{\operatorname{ord}_n(a)}{(k, \operatorname{ord}_n(a))}.$$

In particular,

$$\operatorname{ord}_n(a^k) = \begin{cases} \dfrac{\operatorname{ord}_n(a)}{k} & \text{if } k \mid \operatorname{ord}_n(a) \\ \operatorname{ord}_n(a) & \text{if } (k, \operatorname{ord}_n(a)) = 1 \end{cases}.$$

Proof. Let $\operatorname{ord}_n(a) = m$ and $\operatorname{ord}_n(a^k) = t$. Then

$$\begin{aligned} a^m &\equiv 1 \pmod{n}, \\ a^{kt} \equiv (a^k)^t &\equiv 1 \pmod{n}. \end{aligned}$$

By the fact that m is the order, we get

$$m \mid kt \implies \frac{m}{(k,m)} \,\Big|\, \frac{k}{(k,m)} \cdot t \implies \frac{m}{(k,m)} \,\Big|\, t,$$

since $\dfrac{m}{(k,m)}$ and $\dfrac{k}{(k,m)}$ are coprime. The reverse division $t \;\Big|\; \dfrac{m}{(k,m)}$ holds by similar reasoning and the definition of t because

$$(a^k)^{\frac{m}{(k,m)}} = (a^m)^{\frac{k}{(k,m)}} \equiv 1^{\frac{k}{(k,m)}} \equiv 1 \pmod{n}.$$

By antisymmetry, $t = \dfrac{m}{(k,m)}$. The two special cases follow immediately. ∎

Theorem 9.9. Let n be a positive integer and a, b be integers that are both coprime to n. If $(\operatorname{ord}_n(a), \operatorname{ord}_n(b)) = 1$, then

$$\operatorname{ord}_n(ab) = \operatorname{ord}_n(a) \cdot \operatorname{ord}_n(b).$$

Proof. We will approach the proof via the antisymmetry of divisibility. By the definition of order,

$$\begin{aligned} (ab)^{\operatorname{ord}_n(a)\cdot\operatorname{ord}_n(b)} &= \left(a^{\operatorname{ord}_n(a)}\right)^{\operatorname{ord}_n(b)} \cdot \left(b^{\operatorname{ord}_n(b)}\right)^{\operatorname{ord}_n(a)} \\ &= 1^{\operatorname{ord}_n(b)} \cdot 1^{\operatorname{ord}_n(a)} \equiv 1 \pmod{n}, \end{aligned}$$

which proves that

$$\operatorname{ord}_n(ab) \mid \operatorname{ord}_n(a) \cdot \operatorname{ord}_n(b).$$

The reverse divisibility property

$$\operatorname{ord}_n(a) \cdot \operatorname{ord}_n(b) \mid \operatorname{ord}_n(ab)$$

remains to be shown. Since $(\text{ord}_n(a), \text{ord}_n(b)) = 1$, it suffices to show that $\text{ord}_n(a)$ and $\text{ord}_n(b)$ each individually divide $\text{ord}_n(ab)$. The information that we have available is that

$$a^{\text{ord}_n(ab)} \cdot b^{\text{ord}_n(ab)} = (ab)^{\text{ord}_n(ab)} \equiv 1 \pmod{n}.$$

Raising this congruence to the power of $\text{ord}_n(a)$ and $\text{ord}_n(b)$ yields

$$a^{\text{ord}_n(ab)\cdot\text{ord}_n(b)} \equiv 1 \pmod{n},$$
$$b^{\text{ord}_n(ab)\cdot\text{ord}_n(a)} \equiv 1 \pmod{n}.$$

The fact that $\text{ord}_n(a)$ and $\text{ord}_n(b)$ are coprime come in handy now because

$$\text{ord}_n(a) \mid \text{ord}_n(ab) \cdot \text{ord}_n(b) \implies \text{ord}_n(a) \mid \text{ord}_n(ab),$$
$$\text{ord}_n(b) \mid \text{ord}_n(ab) \cdot \text{ord}_n(a) \implies \text{ord}_n(b) \mid \text{ord}_n(ab).$$

Antisymmetry finishes the job. ■

Problem 9.10. Let m, n be coprime positive integers and a be an integer that is coprime to both of m, n. Prove that

$$\text{ord}_{mn}(a) = \text{lcm}(\text{ord}_m(a), \text{ord}_n(a)).$$

The question now is, given a modulus n, for which integers a is it true that the powers of a modulo n form an entire reduced residue system modulo n? We have seen more generally, via order, the residues that the powers of a *do* generate. In the next section, we will look at the maximal case of a whole reduced residue system being generated.

9.2 Primitive Roots

We saw in Problem 9.1 that an integer a additively generates a complete residue system modulo a positive integer n if and only if $(a, n) = 1$. We will soon look at the moduli n for which there exist an integer g whose powers generate a reduced residue system modulo n, and the properties of such integers g. Before we do that, let us explore the impossibility of the other two related problems:

1. For $n \geq 2$, the residues 1 and $n - 1$ are both coprime to n, yet

   $$1 + (n - 1) \equiv n \equiv 0 \pmod{n}.$$

   So, in the additive problem, if the multiples of a include a reduced residue system modulo n, they must also include a multiple of n. Since the class of 0 is not a part of a reduced residue system for the $n \geq 2$, this means the multiples of a cannot generate *only* a reduced residue system. At least one other element that is not coprime to n will creep in.

2. It is also not possible for the powers of an integer a to generate a complete residue system modulo n if $n \geq 2$. This is because elements of the class of 0 are not included among the powers of a if a is coprime to n, and elements of the class of 1 are not included among the powers of a if a if not coprime to n. Either way, we cannot obtain a complete residue system modulo n.

Definition 9.11. For a positive integer n, an integer g that is coprime to n is said to be a **primitive root modulo** n if $\text{ord}_n(g) = \varphi(n)$, which is the maximal possible order, due to Euler's congruence and the definition of order. The great power of a primitive root is that when it exists, it is precisely the case in which the powers of an element g contain a representative from every reduced residue class modulo n (and no other residue classes) by Theorem 9.4. In particular,

$$\{1, g, g^2, \ldots, g^{\varphi(n)-1}\}$$

is a reduced residue system modulo n.

Theorem 9.12 (Primitive root theorem)**.** There exists a primitive root modulo an integer n if and only if n is from among $1, 2, 4, p^k, 2p^k$ where p is any odd prime and k is any positive integer.

Proof. Proving this theorem is a time-consuming task. It is the longest standalone proof in this text. Nonetheless, we will supply it by proving a sequence of seven lemmas, which are summarized as follows:

1. There exists a primitive root in each of the moduli $1, 2, 4$.
2. If $n = 2^k$ for an integer $k \geq 3$, then n has no primitive root.
3. If an odd prime p divides n and n has a primitive root, then $n = p^k$ or $n = 2p^k$ for some positive integer k.
4. If p is a prime, then a polynomial modulo p has no more distinct roots modulo p than the degree of the polynomial. This can be combined with Fermat's little theorem to show that, for any positive divisor d of $p - 1$, the polynomial $x^d - 1$ has exactly d distinct roots modulo p.
5. For each odd prime p, there is a primitive root modulo p.
6. A primitive root modulo an odd prime can be "lifted" largely intact into being a primitive root modulo higher powers of the same prime. Thus, if p is an odd prime, then there is a primitive root modulo p^k for every positive integer k.
7. If n is an odd positive integer that has a primitive root, then $2n$ also has a primitive root. Thus, if p is an odd prime, then for every positive integer k, there is a primitive root modulo $2p^k$.

Sadly, we are unaware of a simple proof of this classification that is reminiscent of a bijective combinatorial argument that avoids casework; hence, we have chosen the chapter's epigraphs appropriately. ■

The following lemmas and their proofs together slay the dragon that is the primitive root theorem.

Lemma 9.13. There is a primitive root modulo each of $1, 2, 4$.

Proof. Every integer is in the same equivalence class modulo 1, so any integer is a primitive root modulo 1. Modulo 2, a primitive root is 1. Modulo 4, a primitive root is 3. ■

Lemma 9.14. If $k \geq 3$ is an integer, then for every odd integer m,

$$m^{2^{k-2}} \equiv 1 \pmod{2^k}.$$

So every integer that is coprime to 2^k falls short of having the order $\varphi(2^k) = 2^k - 2^{k-1} = 2^{k-1}$, meaning there is no primitive root modulo 2^k.

Proof. We will prove this by induction on $k \geq 3$. In the base case $k = 3$, it remarkably holds that

$$1^2 \equiv 3^2 \equiv 5^2 \equiv 7^2 \equiv 1 \pmod{8}.$$

Suppose the result holds for some integer $k \geq 3$. By this induction hypothesis, for any odd integer a,

$$a^{2^{k-2}} \equiv 1 \pmod{2^k}.$$

This is equivalent to saying that there exists an integer t such that

$$a^{2^{k-2}} = 1 + t2^k.$$

Squaring this equation, we get

$$a^{2^{k-1}} = 1 + t2^{k+1} + t^2 2^{2k} \equiv 1 \pmod{2^{k+1}}.$$

This completes the induction and proves the assertion. ■

Lemma 9.15. Suppose n has a primitive root and an odd prime p as a factor. Then there exists a positive integer k such that $n = p^k$ or $n = 2p^k$.

Proof. Let $n = tp^k$ where $k = \nu_p(n)$ is the maximal exponent which produces a power of p that divides n, so that $p \nmid t$. We want it to be the case that $t = 1$ or $t = 2$. So we will go for the contrapositive: we assume that $t \geq 3$ and we aim to show that there is no element of order $\varphi(n)$ by computing that the next-largest exponent $\dfrac{\varphi(n)}{2}$ sends every integer a coprime to n to 1. By Corollary 3.30, $\varphi(m)$ is even for $m \geq 3$. Since $(t, p^k) = 1$, we can use the multiplicativity of φ along with Euler's congruence to compute that

$$a^{\frac{\varphi(n)}{2}} \equiv \left(a^{\varphi(t)}\right)^{\frac{\varphi(p^k)}{2}} \equiv 1^{\frac{\varphi(p^k)}{2}} \equiv 1 \pmod{t},$$
$$a^{\frac{\varphi(n)}{2}} \equiv \left(a^{\varphi(p^k)}\right)^{\frac{\varphi(t)}{2}} \equiv 1^{\frac{\varphi(t)}{2}} \equiv 1 \pmod{p^k}.$$

This means that t and p^k are coprime integers that divide $a^{\frac{\varphi(n)}{2}} - 1$, so the same property holds for the product $tp^k = n$ of the two moduli, by the faux-Chinese remainder theorem. Therefore, each integer a coprime to n has order at most $\dfrac{\varphi(n)}{2}$, preventing a from being a primitive root. ■

Lemma 9.16 (Lagrange's polynomial theorem)**.** Suppose p is a prime and let

$$f(x) = a_0 + a_1x + a_2x^2 + \cdots + a_kx^k$$

be a polynomial with integer coefficients. We say that an integer x_0 is a root of f modulo p if

$$f(x_0) \equiv 0 \pmod{p}.$$

We claim that either all of the coefficients of f are divisible by p which means every integer is a root of f modulo p, or if a_k is the largest coefficient of f this is not divisible by p then f has at most k incongruent roots modulo p. As a corollary, if t is a positive divisor of $p-1$, then $f(x) = x^t - 1$ has *exactly* t distinct roots modulo p. Note that Lagrange is useless if $k \geq p$ since there are p residue classes in total, so of course the roots fall into at most k of the classes.

Proof. We will prove the result by induction on integers $k \geq 0$. In the base case $k = 0$, $f(x) = a_0$ cannot have a root if $a_0 \not\equiv 0 \pmod{p}$. Now suppose the result holds for some integer $k \geq 0$. Let p be a prime and

$$f(x) \equiv a_0 + a_1x + a_2x^2 + \cdots + a_kx^k + a_{k+1}x^{k+1} \pmod{p}$$

be a polynomial such that $p \nmid a_{k+1}$. If f has k or fewer distinct roots modulo n, then we are done. So what we will do is show that if f has *at least* $k+1$ distinct roots $x_1, x_2, \ldots, x_{k+1}$ modulo p, then f has *exactly* $k+1$ distinct roots modulo n. We cannot blindly use our polynomial factorization theorems, such as the fundamental theorem of algebra, because we are dealing with integer roots only, not to mention we are operating in a modulo system. However, we can still borrow the idea of factoring and define the polynomial with integer coefficients

$$g(x) = a_{k+1}(x - x_1)(x - x_2)\cdots(x - x_{k+1}).$$

We temporarily define the "degree" of an integer polynomial to mean the highest exponent such that the corresponding coefficient is not divisible by p. Then $f - g$ has degree strictly less than $k+1$ because the $a_{k+1}x^{k+1}$ terms of f and g knock each other out. But $f - g$ has the $k+1$ roots $x_1, x_2, \ldots, x_{k+1}$. By the induction hypothesis, this forces $f - g$ to be congruent to the 0 polynomial modulo p, meaning all of the coefficients of $f - g$ are divisible by p. So, for every root x_0 of f,

$$0 \equiv f(x_0) \equiv g(x_0) \equiv a_{k+1}(x_0 - x_1)(x_0 - x_2)\cdots(x_0 - x_{k+1}) \pmod{p}.$$

By Euclid's lemma, this forces $x_0 \equiv x_i$ for some $i \in [k+1]$, so there can be no further distinct roots of f modulo p. As is often the case with polynomials, factoring saved the day.
Now suppose t is a positive divisor of $p-1$. By Fermat's little theorem,

$$x^{p-1} - 1 \equiv 0 \pmod{p}$$

for every integer $x \in [p-1]$, so the polynomial $x^{p-1} - 1$ has $p-1$ incongruent roots modulo p, which is the maximal possible allotment by Lagrange's theorem. The trick to involving t is to let $s = \dfrac{p-1}{t}$ and use the difference of powers factorization to get

$$x^{p-1} - 1 = (x^t)^s - 1 = (x^t - 1)(1 + x^t + x^{2t} + \cdots + x^{(s-1)t}).$$

By Lagrange's theorem, the first factor $x^t - 1$ has at most t roots and the second factor

$$1 + x^t + x^{2t} + \cdots + x^{(s-1)t}$$

has at most $(s-1)t$ roots. By Euclid's lemma, p divides their product $x^{p-1} - 1$ if and only if p divides at least one of the two factors. So x_0 is a root of $x^{p-1} - 1$ if and only if x_0 is a root of one of the two factors. Since

$$t + (s-1)t = st = p - 1,$$

if either of the two factors fall short of the Lagrange upper bound on the number of roots that it can have, then $x^{p-1} - 1$ will not have $p - 1$ roots, which is a contradiction. Therefore, $x^t - 1$ has exactly t roots. Note that the two factors cannot share any roots either because then we would again fall short. ■

Lemma 9.17. If p is an odd prime, then p has a primitive root.

Proof. Let p be an odd prime and let the prime factorization of $p - 1$ be

$$p - 1 = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}.$$

If we can find an element of order $p_i^{e_i}$ for each $i \in [k]$, then we can multiply them together to find an element of order $p - 1$ by Theorem 9.9 because the maximal prime powers $p_i^{e_i}$ are pairwise coprime. The following argument works for all $i \in [k]$. For ease of notation, we replace p_i with q and e_i with t. The idea is that we are seeking a root r of $x^{q^t} - 1$ modulo p that is not a root of $x^{q^s} - 1$ for any non-negative integer $s < t$; we will now flesh this out. By the corollary to Lagrange's theorem, there are exactly q^t incongruent roots of $x^{q^t} - 1$ modulo p. If r is such a root, then

$$r^{q^t} \equiv 1 \pmod{p}.$$

Then $\operatorname{ord}_p(r) \mid q^t$, so $\operatorname{ord}_p(r) = q^s$ for some integer $s \in [t]^*$. If $s = t$, then we are done. if $s < t$, then we get the congruence

$$r^{q^s} \equiv 1 \pmod{p},$$

and taking it to the power of q several times ($t - 1 - s$ times to be precise), we get

$$r^{q^{t-1}} \equiv 1 \pmod{p},$$

so r is a root of $x^{q^{t-1}} - 1$ modulo p. By the corollary to Lagrange's theorem, there are exactly q^{t-1} such roots modulo p. So even if we remove the roots of all of the $x^{q^s} - 1$ over all non-negative integers $s < t$ from the q^t roots of $x^{q^t} - 1$, we are left with

$$q^t - q^{t-1} = q^{t-1}(q-1) = \varphi(q^t) \geq 1$$

roots of $x^{q^t} - 1$ of order q^t. Thus, a primitive root exists modulo p by multiplying together elements of order $p_1^{e_1}, p_2^{e_2}, \ldots, p_k^{e_k}$. ■

Lemma 9.18. If p is an odd prime and k is a positive integer, then there exists a primitive root modulo p^k.

Proof. We know that there exists a primitive root g modulo p. The idea is to "lift" g as a primitive root modulo higher powers of p. Since g is a primitive root,

$$g^{p-1} \equiv 1 \pmod{p}.$$

In matters of divisibility in number theory, if a certain congruence holds, we might wonder what is the maximal power of the modulus in which the congruence still holds, since going from higher to lower powers always works but the opposite is not necessarily true; for example, see the comment about Wolstenholme's theorem in Example 8.7. If p divides $g^{p-1} - 1$ again, meaning $p^2 \mid g^{p-1} - 1$, then

$$g^{p-1} \equiv 1 \pmod{p^2}.$$

This would mean that g is not a primitive root modulo p^2 because $\varphi(p^2) = p(p-1) > p-1$ for odd primes p. This is a problem, so we will assume that

$$g^{p-1} \not\equiv 1 \pmod{p^2}$$

and deal with the other case later. Under this assumption, we will show by induction on $k \geq 1$ that g is a primitive root modulo p^k.
The base case $k = 1$ is the assumption for this lifting argument. Suppose the result holds for some positive integer k. Let

$$m = \operatorname{ord}_{p^{k+1}}(g).$$

Then

$$g^m \equiv 1 \pmod{p^{k+1}},$$

and reducing it modulo p^k yields

$$g^m \equiv 1 \pmod{p^k}.$$

By the induction hypothesis, $\operatorname{ord}_{p^k}(g) = \varphi(p^k)$, so $\varphi(p^k) \mid m$. By Euler's congruence,

$$g^{\varphi(p^{k+1})} \equiv 1 \pmod{p^{k+1}},$$

so $m \mid \varphi(p^{k+1})$. Now we know that there exist integers a and b such that

$$\begin{aligned} \varphi(p^k)a &= m, \\ mb &= \varphi(p^{k+1}). \end{aligned}$$

Combining them, we get that

$$\varphi(p^k)ab = mb = \varphi(p^{k+1}).$$

According to the formula for φ,

$$ab = \frac{\varphi(p^{k+1})}{\varphi(p^k)} = \frac{p^{k+1}(p-1)}{p^k(p-1)} = p.$$

So one of the following two cases must hold:

$$(a, b) = (1, p) \implies m = \varphi(p^k),$$
$$(a, b) = (p, 1) \implies m = \varphi(p^{k+1}).$$

We want the latter to be true in order to prove that g is a primitive root modulo p^{k+1}, so we will show by induction on integers $k \geq 1$ that

$$g^{\varphi(p^k)} \not\equiv 1 \pmod{p^{k+1}},$$

in order to disprove the former case. The base case is given by our assumption that

$$g^{p-1} \not\equiv 1 \pmod{p^2}.$$

Suppose the result holds for some integer $k \geq 1$. By Euler's congruence,

$$g^{\varphi(p^k)} \equiv 1 \pmod{p^k},$$

so there exists and integer t such that

$$g^{\varphi(p^k)} = 1 + tp^k.$$

By the binomial theorem,

$$g^{\varphi(p^{k+1})} = g^{p\varphi(p^k)} \equiv (1 + tp^k)^p \equiv \sum_{i=0}^{p} \binom{p}{i} (tp^k)^i \pmod{p^{k+2}}.$$

The first two terms are $1 + p \cdot tp^k = 1 + tp^{k+1}$. We claim that the rest of the terms disappear because p^{k+2} divides each of them. For $2 \leq i \leq p - 1$, the coefficient $\binom{p}{i}$ is divisible by p (see Corollary 8.5), and the factor p^{ki} is a power of p. Indeed,

$$(1 + ki) - (k + 2) = k(i - 1) - 1 \geq 1 \cdot (2 - 1) - 1 \geq 0.$$

The final term has the factor p^{kp}, and indeed

$$kp - (k + 2) = k(p - 1) - 2 \geq 1 \cdot (3 - 1) - 2 = 0.$$

So

$$g^{\varphi(p^{k+1})} \equiv 1 + tp^{k+1} \pmod{p^{k+2}}.$$

If this were congruent to 1 (we don't want this), then tp^{k+1} would be divisible by p^{k+2}, which would force t to be divisible by p. Why is this a problem? Recall that t was defined as the integer such that $g^{\varphi(p^k)} = 1 + tp^k$. If p divides t, then

$$g^{\varphi(p^k)} \equiv 1 \pmod{p^{k+1}},$$

which contradicts the induction hypothesis. Thus,

$$g^{\varphi(p^{k+1})} \not\equiv 1 \pmod{p^{k+2}},$$

which completes the inner induction and thereby the outer induction. (This was an induction within an induction, so perhaps by borrowing Christopher Nolan's movie concept, we should call it inception.)
Finally, recall that we assumed that $g^{p-1} \not\equiv 1 \pmod{p^2}$ in the last case. Now we will deal with the case where

$$g^{p-1} \equiv 1 \pmod{p^2}.$$

Since it is not possible to lift g by itself, we try the next best option and try to lift $g+p$, which is still a primitive root modulo p. All we need to do is prove that

$$(g+p)^{p-1} \not\equiv 1 \pmod{p^2},$$

and then the proof of the first case will apply readily since the non-congruence $g^{p-1} \not\equiv 1 \pmod{p^2}$ is the only condition that we needed earlier for g to work. By the binomial theorem,

$$(g+p)^{p-1} = \sum_{i=0}^{p-1} \binom{p-1}{i} g^i p^{p-1-i}.$$

Since

$$p-1-i \geq 2 \iff i \leq p-2,$$

only the last two terms remain modulo p^2. So

$$\begin{aligned}(g+p)^{p-1} &\equiv \binom{p-1}{p-2} g^{p-2} p^{p-1-(p-2)} + \binom{p-1}{p-1} g^{p-1} \\ &\equiv (p-1) g^{p-2} p + g^{p-1} \\ &\equiv -g^{p-2} p + 1 \pmod{p^2},\end{aligned}$$

where we used the hypothesis $g^{p-1} \equiv 1 \pmod{p^2}$ in the last step. If this were congruent to 1, then it would cause p^2 to divide $g^{p-2}p$. Then $p \mid g$, which is impossible for a primitive root g modulo p. Thus, the lengthiest part of the proof of the primitive root theorem is complete. ■

Lemma 9.19. If n is an odd positive integer that has a primitive root g, then whichever of g or $g+n$ is odd is primitive root modulo $2n$.

Proof. Let g be a primitive root modulo an odd positive integer n. Then g could be even or odd. But if there is a primitive root h modulo $2n$, then h must be odd, otherwise it will not be coprime to $2n$. So we will deal with two cases: g is odd and g is even.

- If g odd, then

  $$(g, 2n) = (g, n) = 1.$$

  By Euler's congruence,

  $$g^{\varphi(n)} = g^{\varphi(2)\varphi(n)} = g^{\varphi(2n)} \equiv 1 \pmod{2n}.$$

  If there exists a smaller positive integer $k < \varphi(n) = \varphi(2n)$ such that

  $$g^k \equiv 1 \pmod{2n},$$

  then $g^k \equiv 1 \pmod{n}$ as well by reducing the modulus, which contradicts the fact that g is a primitive root modulo n.

- If g is even, then we try the next best option after g, which is $g+n$. Note that $g+n$ is still a primitive root modulo n. There is some hope that this will work since $g+n$ is odd in this case. By the faux-Euclidean algorithm,

$$(g+n, 2n) = (g+n, n) = (g, n) = 1,$$

so Euler's congruence gives

$$(g+n)^{\varphi(n)} \equiv (g+n)^{\varphi(2)\varphi(n)} = (g+n)^{\varphi(2n)} \equiv 1 \pmod{2n}.$$

As in the previous case, if

$$(g+n)^k \equiv 1 \pmod{2n}$$

for some integer $k < \varphi(n) = \varphi(2n)$, then $(g+n)^k \equiv 1 \pmod{n}$ as well, which causes g to fail to be a primitive root modulo n.

Therefore, whichever of g or $g+n$ is odd is a primitive root modulo $2n$. ■

Thus, we have completed the proof of the primitive root theorem.

Theorem 9.20. If g is a primitive root modulo a positive integer n, then m is an integer such that g^m is a primitive root modulo n if and only if $(m, \varphi(n)) = 1$. As such, there are exactly $\varphi(\varphi(n))$ distinct primitive roots modulo n, if n has a primitive root in the first place.

Proof. Suppose g is a primitive root modulo n. By Theorem 9.8, g^m is also a primitive root modulo n if and only if

$$\varphi(n) = \operatorname{ord}_n(g^m) = \frac{\operatorname{ord}_n(g)}{(m, \operatorname{ord}_n(g))} = \frac{\varphi(n)}{(m, \varphi(n))}.$$

Simplifying, this equation is equivalent to $(m, \varphi(n)) = 1$. The set

$$\left\{g, g^2, \ldots, g^{\varphi(n)-1}, g^{\varphi(n)}\right\}$$

is a reduced residue system modulo n, so it contains all distinct primitive roots modulo n as a subset. The number of exponents m from this set that are coprime to $\varphi(n)$ is exactly the number of elements $m \in [\varphi(n)]$ that are coprime to $\varphi(n)$, which are counted by $\varphi(\varphi(n))$. Therefore, this is the number of primitive roots modulo n, if there is at least one primitive root modulo n. ■

Problem 9.21. Suppose n is a positive integer for which a primitive root exists. Recall that Theorem 9.4 states that the order of every integer coprime to n must divide $\varphi(n)$. Prove that, for each positive divisor d of $\varphi(n)$, there exists an integer of order d modulo n. Extend this result by showing that there are exactly $\varphi(d)$ incongruent integers modulo n of order d.

As a display of the usefulness of primitive roots, we will end the chapter with a pair of applications. Before we can get into the first one, some preliminary legwork is necessary. A part of the initial work, specifically Lemma 9.23, would be easier with the abstract machinery of group theory, but we have managed to do without it. For the rest of the section, for each positive integer n, let $\mathbb{Z}_n$ denote a complete residue system modulo n, and let $\mathbb{Z}_n^*$ denote a reduced residue system modulo n. We begin with asking the reader to work on the non-reduced analogue of Lemma 9.23.

Problem 9.22. Let n and d be positive integers such that $d \mid n$. Prove that the function $f : \mathbb{Z}_n \to \mathbb{Z}_d$ that reduces each input modulo d is surjective, with the preimage of each output having exactly $\dfrac{n}{d}$ elements. Note that this function is well-defined in the sense that two numbers congruent to each other modulo n reduce to the same element modulo d, meaning they are also congruent modulo d.

Lemma 9.23. Let n and d be positive integers such that $d \mid n$. Then the (well-defined) function $g : \mathbb{Z}_n^* \to \mathbb{Z}_d^*$ that reduces each input modulo d is surjective, with the preimage of each output having exactly $\dfrac{\varphi(n)}{\varphi(d)}$ elements (which is an integer by Corollary 3.27 because $d \mid n$).

Proof. It does not work to take the elements of $\mathbb{Z}_n^*$ corresponding to the integers in

$$\{0, 1, 2, \ldots, d-1\}$$

that are coprime to d and reduce them modulo d because these elements might not be coprime to n and therefore they might not even be in the domain $\mathbb{Z}_n^*$. Instead, the idea is to go slowly by shaving off single primes from n until we reach d: If we can prove surjectivity in the case where $n = dp$ for a prime p, then an induction argument will complete the proof by extracting out more primes (which are not necessarily distinct) from n and composing the corresponding sequence of (surjective) reductions. Suppose $n = dp$ for some prime p. Let b be an integer such that $(b, d) = 1$, so we want to construct an integer a such that $(a, n) = 1$ and $a \equiv b \pmod{d}$. We split the argument into two cases:

1. If $p \nmid b$, then $(b, p) = 1$ and $(b, d) = 1$ together imply that

   $$1 = (b, dp) = (b, n),$$

   due to Problem 1.20. So we can choose $a = b$.

2. If $p \mid b$, then $(b, n) = (b, dp)$ is divisible by p and so it is not 1. As a result, we cannot choose a to be b again, so we try the next possibility in the class of b modulo d, which is $b + d$. Note that $p \nmid d$, otherwise p will divide both b and d, causing the contradiction $p \mid (b, d) = 1$. As a result $p \nmid b + d$, otherwise the opposite, $p \mid b + d$, combined with $p \mid b$ would cause the contradiction $p \mid d$. By the faux-Euclidean algorithm,

   $$\begin{cases} (b + d, d) = (b, d) = 1, \\ (b + d, p) = 1 \end{cases} \implies (b + d, n) = (b + d, dp) = 1.$$

   So choosing $a = b + d$ works in this case.

Now we need to show that the preimages of all outputs have the same cardinality, $\dfrac{\varphi(n)}{\varphi(d)}$. The idea is to show that the preimages of 1 modulo d and the preimages of a different (meaning non-unity) element m modulo d correspond to each other. Formally speaking, we will show that there exists an injection from $g^{-1}(1)$ to $g^{-1}(m)$, and that there exists an injection from

$g^{-1}(m)$ to $g^{-1}(1)$; this allows us to invoke the finite Schröder-Bernstein theorem (discussed in Volume 2 alongside the pigeonhole principle), which establishes that the two preimages have the same cardinality. Let

$$g^{-1}(1) = \{a_1, a_2, \ldots, a_k\},$$

which we know to be non-empty by surjectivity of g. Let $m \in \mathbb{Z}_d^*$ be arbitrary but fixed, and let $h \in g^{-1}(m)$, where h must exist by surjectivity of g. We claim that $\{ha_1, ha_2, \ldots, ha_k\}$ are all distinct elements of $g^{-1}(m)$. These reduce to m modulo d because, for each index $i \in [k]$,

$$\begin{cases} a_i & \equiv 1 \pmod{d}, \\ h & \equiv m \pmod{d} \end{cases} \implies ha_i \equiv m \pmod{d} \implies ha_i \in g^{-1}(m).$$

The ha_i are distinct because

$$ha_i \equiv ha_j \pmod{d} \implies a_i \equiv a_j \pmod{d}$$

by the invertibility of h modulo d, so

$$|g^{-1}(1)| \leq |g^{-1}(m)|.$$

In the other direction, let

$$g^{-1}(m) = \{b_1, b_2, \ldots, b_\ell\}$$

and let $c \in g^{-1}(m^{-1})$, where m^{-1} is the inverse of m modulo d. All of the elements of $\{cb_1, cb_2 \ldots, cb_\ell\}$ map to 1 because, for each index $i \in [\ell]$,

$$\begin{cases} b_i & \equiv m \pmod{d}, \\ c & \equiv m^{-1} \pmod{d} \end{cases} \implies cb_i \equiv 1 \pmod{d} \implies cb_i \in g^{-1}(1).$$

Simliar to the earlier argument, the cb_i are distinct modulo d because

$$cb_i \equiv cb_j \pmod{d} \implies b_i \equiv b_j \pmod{d}$$

by the invertibility of c modulo d, so

$$|g^{-1}(m)| \leq |g^{-1}(1)|.$$

By antisymmetry,

$$|g^{-1}(1)| = |g^{-1}(m)|$$

for each $m \in \mathbb{Z}_d^*$. Therefore, all such preimages have the same cardinality and they partition $\mathbb{Z}_n^*$ into $|\mathbb{Z}_d^*|$ pieces, each of which has cardinality $\dfrac{|\mathbb{Z}_n^*|}{|\mathbb{Z}_d^*|} = \dfrac{\varphi(n)}{\varphi(d)}$. ■

Lemma 9.24. If $n \geq 3$ is an integer and g is a primitive root modulo n, then

$$g^{\frac{\varphi(n)}{2}} \equiv -1 \pmod{n}.$$

The exponent is an integer because we proved in Corollary 3.30 that $\varphi(n)$ is even for $n \geq 3$.

Proof. It is clear that $\text{ord}_n(-1) = 2$ because an exponent of 1 does not send -1 to 1, yet

$$(-1)^2 \equiv 1 \pmod{n}.$$

Moreover,

$$\text{ord}_n\left(g^{\frac{\varphi(n)}{2}}\right) = \frac{\text{ord}_n(g)}{\left(\frac{\varphi(n)}{2}, \text{ord}_n(g)\right)} = \frac{\varphi(n)}{\left(\frac{\varphi(n)}{2}, \varphi(n)\right)} = 2.$$

So if we can show that there is a unique element of order 2 modulo n, then $g^{\frac{\varphi(n)}{2}}$ and -1 will be forced to be congruent to each other. The distinct elements modulo n are

$$g^1, g^2, g^3, \ldots, g^{\varphi(n)}.$$

Suppose i is an indexing exponent from this set such that

$$2 = \text{ord}_n(g^i) = \frac{\text{ord}_n(g)}{(i, \text{ord}_n(g))} = \frac{\varphi(n)}{(i, \varphi(n))}.$$

Rearranging the equation leads to

$$\frac{\varphi(n)}{2} = (i, \varphi(n)),$$

which divides i. The only multiples of $\dfrac{\varphi(n)}{2}$ in $[\varphi(n)]$ are $\dfrac{\varphi(n)}{2}$ itself and the next multiple $\varphi(n)$. The latter is inadmissible because

$$g^{\varphi(n)} \equiv 1 \pmod{n}$$

has order 1. So there is a unique element of order 2, which can be written as $g^{\frac{\varphi(n)}{2}}$ or as -1 modulo n. Thus, the two are congruent modulo n. ■

Problem 9.25. Prove that, if $a \in \mathbb{Z}$, $n \geq 3$ is an integer, and $k \in \mathbb{Z}_+$ such that

$$a^k \equiv -1 \pmod{n}$$

and this congruence is true for no positive exponent lower than k, then $\text{ord}_n(a) = 2k$.

Recall Wilson's theorem (Theorem 4.22), after which we commented that there exists a generalization of it due to Gauss. The following proof of Gauss's generalization of Wilson's theorem is due to Keith Conrad. He developed it after I made the superficial observation that Gauss' generalization follows the same casework as in the primitive root theorem, and I asked whether a non-superficial link exists, such as deriving one result from another. In my opinion, Conrad's proof is superior to the classic one in [14] because Conrad's is less ad hoc and it illuminates the relation to primitive roots.

Theorem 9.26 (Gauss's generalization of Wilson's theorem)**.** If n is a positive integer, then

$$\prod_{\substack{k \in [n] \\ (k,n)=1}} k \equiv \begin{cases} -1 \pmod{n} & \text{if } n = 1, 2, 4, p^\alpha, 2p^\alpha \\ 1 \pmod{n} & \text{otherwise} \end{cases},$$

where p is any odd prime and α is any positive integer.

Proof. Here is an overview of cases into which we will partition the positive integers n:

1. n is odd
   (a) $n = 1$
   (b) n is a prime power
   (c) n is not a prime power
2. n is even, so $n = 2^\beta m$ for some positive integer β and odd integer m
   (a) $m = 1$
      i. $\beta = 1$ or $\beta = 2$
      ii. $\beta \geq 3$
   (b) $m \geq 3$
      i. $\beta = 1$
         A. m is a prime power
         B. m is not a prime power
      ii. $\beta \geq 2$

For each positive integer n, let $\displaystyle\prod_{\substack{k\in[n]\\(k,n)=1}} k$ be denoted by P_n. The key idea behind most of the cases where primitive roots do not exist is that, if $d \mid n$, then

$$P_n \equiv P_d^{\frac{\varphi(n)}{\varphi(d)}} \pmod{d},$$

since $\dfrac{\varphi(n)}{\varphi(d)}$ multiplicands in P_n are reduced to each multiplicand in P_d by Lemma 9.23. Moreover, the multiplicativity of φ implies that if d and $\dfrac{n}{d}$ are coprime, then

$$\varphi(n) = \varphi\left(d \cdot \frac{n}{d}\right) = \varphi(d)\varphi\left(\frac{n}{d}\right) \implies \frac{\varphi(n)}{\varphi(d)} = \varphi\left(\frac{n}{d}\right).$$

We will also be using the fact that $\varphi(a)$ is even for all integers $a \geq 3$ (Corollary 3.30). Here are the proofs for the cases stated above:

1. Suppose n is odd.
   (a) If $n = 1$, the result is trivial since every integer lives in the same congruence class.
   (b) If n is a prime power, let $n = p^\alpha$ for some odd prime p and positive integer α. Then n has a primitive root g, which allows us to to compute

$$P_n = \prod_{\substack{k\in[n]\\(k,n)=1}} k \equiv \prod_{i\in[\varphi(n)]} g^i \equiv g^{1+2+\cdots+\varphi(n)}$$
$$\equiv g^{\frac{\varphi(n)(\varphi(n)+1)}{2}} \equiv \left(g^{\frac{\varphi(n)}{2}}\right)^{\varphi(n)+1} \equiv (-1)^{\varphi(n)+1} \equiv -1 \pmod{n},$$

   where we used Lemma 9.24 and the fact that $\varphi(n) + 1$ is odd at the end.

(c) If n is not a prime power, then at least two distinct primes divide it. Let p^α be a maximal prime power dividing n. Then there exists an odd integer $m \geq 3$ coprime to p^α such that $n = p^\alpha m$. Using the idea mentioned before we began working on the cases,

$$P_n \equiv P_{p^\alpha}^{\frac{\varphi(n)}{\varphi(p^\alpha)}} \equiv P_{p^\alpha}^{\varphi(m)} \equiv (-1)^{\text{even}} \equiv 1 \pmod{p^\alpha},$$

where we used 1(b). Since this is true for every maximal prime power dividing n, we can piece them together using the faux-Chinese remainder theorem (Theorem 2.10) to get that n divides $P_n - 1$, which is what we want.

2. Suppose n is even, so $n = 2^\beta m$ for some positive integer β and odd positive integer m.

(a) Suppose $m = 1$.

i. If $\beta = 1$, then $n = 2$, whence $P_2 \equiv 1 \equiv -1 \pmod 2$. If $\beta = 2$, then $n = 4$, whence $P_4 \equiv 1 \cdot 3 \equiv 3 \equiv -1 \pmod 4$.

ii. Suppose $\beta \geq 3$. This is the most manual of the cases and does not use primitive roots. In P_n, just like in the proof of Wilson's theorem, all multiplicands that are not their own inverse modulo n uniquely pair up with their inverse to produce 1 modulo n. So what we are really seeking is the product of the multiplicands x in P_n that satisfy $x^2 \equiv 1 \pmod{2^\beta}$. By difference of squares, this is equivalent to

$$(x-1)(x+1) \equiv 0 \pmod{2^\beta}.$$

So $(x-1)(x+1)$ is even and the two factors have the same parity so $x-1$ and $x+1$ are both even, which is equivalent to saying that x is odd. Moreover, the faux-Euclidean algorithm tells us that

$$\gcd(x-1, x+1) = \gcd(x-1, 2)$$

must be 2 (and not 1) since both entries are even. This leaves us with four ways in which the 2^β can be distributed across the factors $x-1$ and $x+1$:

- If $2^\beta \mid x-1$, then $x \equiv 1 \pmod{2^\beta}$.
- If $2^\beta \mid x+1$, then $x \equiv -1 \pmod{2^\beta}$.
- If $2^{\beta-1} \mid x-1$, then $x = 2^{\beta-1}t+1$ for some integer t, which can be squared to show that it is indeed self-inverse modulo 2^β. If t is even, then we get the first case, so suppose t is odd. It is easy to prove that every odd t leads to the same residue modulo 2^β, so we pick $t = 1$ for the sake of simplicity.
- If $2^{\beta-1} \mid x+1$, then $x = 2^{\beta-1}t - 1$ for some integer t, which again can be squared to show that it is self-inverse. As before, if t is even, then we get the second case, so suppose t is odd. Again, every odd t leads to the same residue modulo 2^β, so we pick $m = 1$ for simplicity.

Therefore,

$$P_n \equiv 1 \cdot (-1) \cdot (2^{\beta-1}+1) \cdot (2^{\beta-1}-1) \equiv -(2^\beta - 1) \equiv 1 \pmod n.$$

(b) Suppose $m \geq 3$.

i. Suppose $\beta = 1$.

A. If m is a prime power, then there exists a primitive root g modulo n. The proof is exactly the same as the computation of P_n in the case where n is an odd prime power, which is case 1(b).

B. If m is not a prime power, then by 1(c),

$$\begin{cases} P_n \equiv P_m^{\frac{\varphi(n)}{\varphi(m)}} \equiv 1^{\varphi(2)} \equiv 1 & \pmod{m}, \\ P_n \equiv P_2^{\frac{\phi(n)}{\phi(2)}} \equiv 1^{\phi(m)} \equiv 1 & \pmod{2} \end{cases} \implies P_n \equiv 1 \pmod{n},$$

where we used the fact that all multiplicands of P_2 are odd, and we used the faux-Chinese remainder theorem to bring the two congruences together in the end.

ii. Suppose $\beta \geq 2$. Firstly, taking P_n modulo m,

$$P_n \equiv P_m^{\frac{\varphi(n)}{\varphi(m)}} = P_m^{\varphi(2^\beta)} \begin{cases} (-1)^{\varphi(2^\beta)} & \pmod{m} \text{ if } m \text{ is a prime power} \\ 1^{\varphi(2^\beta)} & \pmod{m} \text{ if } m \text{ is not a prime power} \end{cases},$$

where we used 1(b) and 1(c). Either way,

$$P_n \equiv (\pm 1)^{\text{even}} \equiv 1 \pmod{m}.$$

Secondly, taking P_n modulo 2^β,

$$P_n \equiv P_{2^\beta}^{\frac{\varphi(n)}{\varphi(2^\beta)}} \equiv P_{2^\beta}^{\varphi(m)} \begin{cases} (-1)^{\varphi(m)} & \pmod{2^\beta} \text{ if } \beta = 2 \\ 1^{\varphi(m)} & \pmod{2^\beta} \text{ if } \beta \geq 3 \end{cases},$$

where we used both parts of 2(a). Either way,

$$P_n \equiv (\pm 1)^{\text{even}} \equiv 1 \pmod{2^\beta}$$

again. As before, we can put the two cases (modulo m and modulo 2^m) together using the faux-Chinese remainder theorem to get

$$P_n \equiv 1 \pmod{n}.$$

■

Corollary 9.27. Let n be a positive integer. Then $\prod_{\substack{k \in [n] \\ (k,n)=1}} k \equiv -1$ if and only if n has a primitive root, and $\prod_{\substack{k \in [n] \\ (k,n)=1}} k \equiv 1$ if and only if n does not have a primitive root.

Now we will prove a biconditional criterion for identifying Carmichael numbers, which will require only part of the full power the primitive root theorem.

Theorem 9.28 (Korselt's criterion)**.** An integer n is a Carmichael number if and only if all of the following three conditions hold:

- n is composite
- n is squarefree
- For each prime factor p of n, it holds that $p-1 \mid n-1$.

Proof. For one direction, suppose n is a Carmichael number. By definition, n is composite. Suppose, for contradiction that n is not squarefree. Then there exists a prime factor p of n such that $n = p^k m$ for some integer $k \geq 2$ and m such that $p \nmid m$. The idea is to use the Chinese remainder theorem to assert the existence of a contradictory integer x such that

$$\begin{aligned} x &\equiv a \pmod{p^k}, \\ x &\equiv b \pmod{m}, \end{aligned}$$

where a and b are fixed integers that we will choose strategically as the proof unfolds. In a nutshell, we are troublemakers looking to cause a contradiction in the mathematical universe and our weapon of choice is the Chinese remainder theorem. If a and b are chosen judiciously so that they are coprime to their respective moduli, then x will be coprime to both moduli, which will give us the additional information that

$$x^{n-1} \equiv 1 \pmod{n},$$

since n is assumed to be a Carmichael number. Reducing modulo p^2, which divides n, we get

$$x^{n-1} \equiv 1 \pmod{p^2}.$$

Then

$$\begin{aligned} x \equiv a \pmod{p^k} &\implies x^{n-1} \equiv a^{n-1} \pmod{p^k} \\ &\implies x^{n-1} \equiv a^{n-1} \pmod{p^2} \\ &\implies a^{n-1} \equiv 1 \pmod{p^2}. \end{aligned}$$

So far, what we have said about a is true for any choice of a and b that lead to x being coprime to n, but we want to derive a contradiction by choosing specific a and b. Choosing $a = 1$ does not cause any trouble, but choosing $a = 1 + p$ leads to

$$1 \equiv a^{n-1} \equiv (1+p)^{n-1} \equiv \sum_{i=0}^{n-1} \binom{n-1}{i} p^i \equiv 1 + (n-1)p \pmod{p^2},$$

because all other terms in the binomial expansion get annihilated modulo p^2. This leads to the congruence

$$n \equiv 1 \pmod{p},$$

which is untrue because $p \mid n$. All we need to do is pick a b so that x is coprime to n, so we select the simplest option $b = 1$. With $a = 1 + p$ coprime to p^k and $b = 1$ coprime to m, it

must be true that x is coprime to both by the faux-Euclidean algorithm, and therefore x is coprime to the product of the moduli $p^k m = n$, as needed to utilize the congruence following from the fact that n is a Carmichael number. Thus, n is squarefree.
To prove the $p-1 \mid n-1$ condition, note that $p-1$ and $n-1$ look like they fit the character of exponents (for example, in Fermat's little theorem) more than they fit the nature of moduli. So we will seek to find an element of order $p-1$ in some modulus, where the exponent of $n-1$ also sends the element to 1. This will cause it to be true that $p-1 \mid n-1$. Accordingly, if g is a primitive root modulo p, which we know to exist, then $\text{ord}_p(g) = p-1$. By CRT, there exists an integer x that satisfies the system of congruences

$$\begin{aligned} x &\equiv g \pmod{p}, \\ x &\equiv 1 \pmod{n/p}, \end{aligned}$$

since $\left(p, \dfrac{n}{p}\right) = 1$ due to n being squarefree. Since g and 1 are coprime to their respective moduli, x is coprime to the product of the moduli $p \cdot \dfrac{n}{p} = n$. As n is assumed to be a Carmichael number, we then get

$$x^{n-1} \equiv 1 \pmod{n} \implies x^{n-1} \equiv 1 \pmod{p}.$$

Since x is an element of order $p-1$ modulo p, it holds that $p-1 \mid n-1$. This completes one direction of the proof.
For the other direction, suppose n is composite, squarefree and has the property is $p-1 \mid n-1$ for any prime factor p of n. Let the prime factorization of n be

$$n = p_1 p_2 \cdots p_k.$$

Let a be any integer that is coprime to n. For each prime p_i, we find that $p_i \nmid a$ due to the coprimality of a and n. So by Fermat's little theorem,

$$a^{p_i - 1} \equiv 1 \pmod{p_i}.$$

Since $p_i - 1 \mid n - 1$,

$$a^{n-1} \equiv (a^{p_i-1})^{\frac{n-1}{p_i-1}} \equiv 1 \pmod{p_i}.$$

So all of the prime factors p_i divide $a^{n-1}-1$ and, as the p_i are pairwise coprime, their product $p_1 p_2 \cdots p_k = n$ also divides $a^{n-1} - 1$. Therefore, n is a Carmichael number. ■

Problem 9.29. Let n be a positive integer. Prove that $a^{n-1} \equiv 1 \pmod{n}$ for all $a \in \mathbb{Z}$ coprime to n if and only if $a^n \equiv a \pmod{n}$ for all $a \in \mathbb{Z}$. As a hint, you may use the definition of Carmichael numbers (Definition 4.30) and Korselt's criterion (Theorem 9.28).

The following is a long problem that explores a variety of convergent themes.

Problem 9.30 (Carmichael's lambda). We may refine $\varphi(n)$ in Euler's congruence as follows. For positive integers n, the **Carmichael lambda function** is denoted and defined as

$$\lambda(n) = \min\{m \in \mathbb{Z}_+ : \forall a \in \mathbb{Z}_+, (a, n) = 1 \implies a^m \equiv 1 \pmod{n}\}.$$

So it is the minimal positive integer exponent that takes all integers coprime to the modulus to unity. Prove the following:

1. If $m \in \mathbb{Z}_+$ satisfies $a^m \equiv 1 \pmod{n}$ for all a coprime to n, then $\lambda(n) \mid m$.
2. Prove that $\lambda(n) \mid \varphi(n)$. Give an example of $n \in \mathbb{Z}_+$ such that $\lambda(n) = \varphi(n)$ and another example where $\lambda(n) \neq \varphi(n)$.
3. If $s, t \in \mathbb{Z}_+$ such that $s \mid t$, then $\lambda(s) \mid \lambda(t)$.
4. For integers $k \geq 3$, $\lambda(2^k) = 2^{k-2}$. For $k = 1$, $\lambda(2) = 1$. For $k = 2$, $\lambda(4) = 2$.
5. For odd primes p and $k \in \mathbb{Z}_+$,
$$\lambda(p^k) = \varphi(p^k) = p^{k-1}(p-1).$$
6. If $s, t \in \mathbb{Z}_+$, then $\lambda([s,t]) = [\lambda(s), \lambda(t)]$, where the square brackets refer to the lowest common multiple. Subsequently, if s, t are coprime, then $\lambda(st) = [\lambda(s), \lambda(t)]$.
7. For an integer $n \geq 2$ with prime factorization $n = p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r}$, we can compute
$$\lambda(n) = [\lambda(p_1^{e_1}), \lambda(p_2^{e_2}), \ldots, \lambda(p_r^{e_r})].$$
This is Carmichael's theorem.
8. For $n \in \mathbb{Z}_+$, there exists $a \in \mathbb{Z}$ coprime to n such that $\operatorname{ord}_n(a) = \lambda(n)$. In fact,
$$\lambda(n) = \max\{\operatorname{ord}_n(b) : b \in \mathbb{Z}, (b, n) = 1\}.$$
9. For $n, d \in \mathbb{Z}_+$, there exists $a \in \mathbb{Z}$ coprime to n such that $\operatorname{ord}_n(a) = d$ if and only if $d \mid \lambda(n)$.

In Volume 2, when discussing basic Ramsey theory, we covered Schur's disproof of Fermat's Last Theorem for any positive integer exponent m modulo all sufficiently large primes p. The proof involved an application of primitive roots.

Chapter 10

Base Representations II

> "Why are numbers beautiful? It's like asking why is Beethoven's Ninth Symphony beautiful. If you don't see why, someone can't tell you. I know numbers are beautiful. If they aren't beautiful, nothing is."
>
> – *Paul Erdős*

We saw in Theorem 7.3 that each integer has a unique base-b representation for each integer $b \geq 2$, under the restriction that the digits to the right of the radix point are taken to be 0. Now we will look at what happens when we extend this idea to rationals. Despite the fact that we take this representation for granted on a daily basis, it holds non-trivial patterns that can take a fair amount of number theory to analyze. We will largely skirt around worrying about what it means to express irrational numbers using base-b forms, as that would bring up issues pertaining to the convergence of infinite series; to deal with those technicalities, we would need the tools of calculus. Even defining real numbers takes some effort. In the second half of the chapter, we will look at cyclic patterns in the rightmost digits of the powers of an integer.

10.1 Repeating Forms

Theorem 10.1 (General basis representation theorem)**.** For any integer $b \geq 2$, each real number r has a representation as a base-b form

$$r = \pm(x_m x_{m-1} \ldots x_1 x_0 . y_1 y_2 y_3 \ldots)_b,$$

and each such form represents a real number in the sense that the base-b expansion equals an infinite sum that converges to a real number. The representation of r is unique unless $y_i = 0$ for all sufficiently large i or $y_i = b - 1$ for all sufficiently large i, except for $r = 0$ which has only one representation $0.000\ldots$. If $y_i = 0$ for all sufficiently large i or $y_i = b - 1$ for all sufficiently large i, then that number has exactly two base-b representations, one of each of the two kinds described. We call these the **dual representations** of the number, and the one with the tail of 0's will be called the **canonical representation**.

We will not go through the proof of this result because it involves the convergence of infinite series.

Example. In base-10, two ways of representing eleven are

$$11.000\ldots = 10.999\ldots.$$

Every integer in every base has exactly two representations in this way, though we almost always prefer the canonical one. In that case, we drop the tail of 0's to the right of the radix point so that we can write down the number using only finitely many symbols.

Theorem 10.2 (Dual representations conversion)**.** If $b \geq 2$ is an integer and ℓ is a positive integer, then

$$(0.\underbrace{00\ldots0}_{\ell \text{ digits of } 0}(b-1)(b-1)(b-1)\ldots)_b = (0.\underbrace{00\ldots0}_{\ell-1 \text{ digits of } 0}1000\ldots)_b.$$

If $\ell = 0$, then we can say that

$$0.(b-1)(b-1)(b-1)\ldots = 1.000\ldots.$$

This provides a way of converting between dual representations in general. We leave it to the reader to extend the idea to when $(b-1)$'s encroach into the left side of the radix point, like $100.000\ldots = 99.999\ldots$.

Proof. By the formula for an infinite geometric series,

$$\begin{aligned}
0.\underbrace{00\ldots0}_{\ell \text{ digits of } 0}(b-1)(b-1)(b-1)\ldots &= \frac{b-1}{b^{\ell+1}} + \frac{b-1}{b^{\ell+2}} + \frac{b-1}{b^{\ell+3}} + \cdots \\
&= \frac{b-1}{b^{\ell+1}} \cdot \left(1 + \frac{1}{b} + \frac{1}{b^2} + \cdots\right) \\
&= \frac{b-1}{b^{\ell+1}} \cdot \frac{1}{1-\frac{1}{b}} = \frac{1}{b^\ell} \\
&= 0.\underbrace{00\ldots0}_{\ell-1 \text{ digits of } 0}1000\ldots,
\end{aligned}$$

where the forms on the far left and far right of the sequence of equalities are both in base-b. The argument is identical for the $\ell = 0$ case. ■

Definition 10.3. There are several types of base-b forms that will be interesting to us when we investigate rational numbers, so we will define them now, ahead of time. Let

$$r = \pm(x_m x_{m-1}\ldots x_1 x_0.y_1 y_2 y_3\ldots)_b$$

be a base-b form.

- The form is said to be **eventually periodic** if there exists a positive integers k and j such that, for all indices $i \geq k$, it holds that $y_i = y_{i+j}$. Let w be the smallest possible k for which a j exists and let t be the smallest j that corresponds to w. If $w = 1$, then the form is called **purely periodic**. For an eventually periodic form, its **pre-period** is $y_1 y_2\ldots y_{w-1}$ (this is empty if $w = 1$) and the pre-period's **length** is $w - 1$. The **repetend** of the form is $y_w y_{w+1}\ldots y_{w+t-1}$ and the **period** is j. We can represent an eventually periodic form by

  $$r = \pm(x_m x_{m-1}\ldots x_1 x_0.y_1 y_2\ldots y_{k-1}\overline{y_k y_{k+1}\cdots y_{k+j-1}})_b,$$

  where the bar over the repetend is called a **vinculum.** In this form, it is preferable but not necessary to use the minimal k and j.

- The form is said to be **terminating** if $y_i = 0$ for all sufficiently large i. So there is a tail a 0's, an occurrence that is already important to us because they represent exactly the real numbers with dual forms. In particular integers terminate because $y_i = 0$ for all i in the canonical forms of integers.

Example. A terminating form is 8.125. An eventually periodic form is

$$1.1234565656\ldots = 1.1234\overline{56}.$$

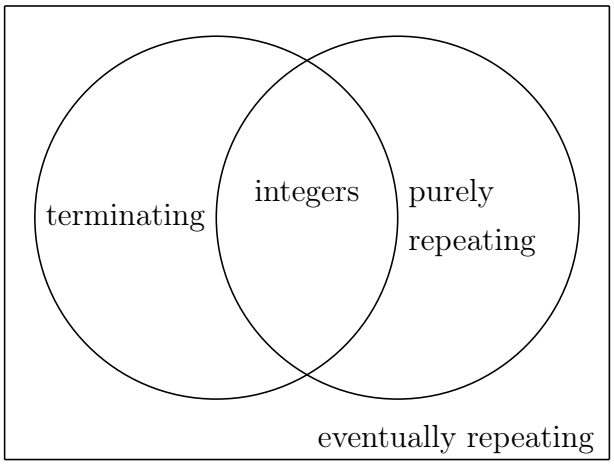
A purely periodic form is

$$10.383838\ldots = 10.\overline{38}.$$

The subset structure of these are as follows:

- Terminating forms and purely periodic forms are both subsets of eventually repeating forms.
- Terminating forms and purely periodic forms are not subsets of each other in either direction.
- The intersection of terminating forms and purely periodic forms is exactly the integers.

This information is captured by the following Venn diagram:



Now we will show that the rationals are precisely those numbers with eventually periodic forms. We will also analyze what fractions lead to terminating or purely repeating forms in which bases, and how we can measure the pre-period length and period.

Lemma 10.4. If r is a real number and $b \geq 2$ is an integer, let the base-b form of r be

$$r = \pm(x_m x_{m-1} \ldots x_1 x_0 . y_1 y_2 y_3 \ldots)_b.$$

Then multiplying r by b shifts the radix point over by one digit to the right, and dividing by b has the opposite effect. As an equation, this means that

$$b \cdot r = \pm(x_m x_{m-1} \ldots x_1 x_0 y_1 . y_2 y_3 \ldots)_b.$$

If there are no y_i's, it just means that we are appending a 0 to the right of $\pm(x_m x_{m-1} \ldots x_1 x_0)_b$ to get

$$\pm(x_m x_{m-1} \ldots x_1 x_0 0)_b.$$

Proof. This is immediately true from the base-b expansion of r because

$$b \cdot b^k = b^{k+1}$$

for every integer k, regardless of whether k is non-negative or negative. ■

Despite its simple proof, this shifting phenomenon in Lemma 10.4 of multiplication by the base number will be our main tool in proving the upcoming theorems. In the next few results, we will assume without loss of generality that the rational number being discussed is positive or that the form in question has a positive sign. This is fine because the argument readily extends to the negative case, and the zero case is trivial.

Theorem 10.5. Let $b \geq 2$ be an integer. Let α be an eventually periodic base-b form. Then:

1. α represents a rational number.
2. If α is terminating, then all of the distinct prime factors in the denominator of the lowest fraction of the rational number represented by α are also prime factors of b.
3. If α is purely periodic, then the denominator of the lowest fraction of the rational number represented by α is coprime to b.

Proof. Let α and b be as stated.

1. Let the form be
$$\alpha = a_m a_{m-1} \dots a_1 . b_1 b_2 \dots b_n \overline{c_1 c_2 \dots c_k}.$$
The trick to getting only integers in an equation involving α is to multiply α by a high enough power of b to produce a purely periodic form - in two different ways, and subtract the two to remove everything to the right of the radix point. In essence, we are taking advantage of the repetend's repeating nature. In action, we can obtain that
$$b^{n+k}\alpha - b^n \alpha = a_m a_{m-1} \dots a_1 b_1 b_2 \dots b_n c_1 c_2 \dots c_k - a_m a_{m-1} \dots a_1 b_1 b_2 \dots b_n$$
is an integer. Calling the integer on the right side β, the equation becomes
$$\alpha b^n (b^k - 1) = \beta,$$
which in turns gives us that
$$\alpha = \frac{\beta}{b^n (b^k - 1)}$$
is rational.
2. Let the terminating form be
$$\alpha = a_m a_{m-1} \dots a_1 . b_1 b_2 \dots b_n.$$
Then
$$b^n \alpha = a_m a_{m-1} \dots a_1 b_1 b_2 \dots b_n$$

is an integer. Letting the integer on the right side be β, we get

$$\alpha = \frac{\beta}{b^n},$$

so the denominator in the lowest fraction of the rational number represented by α divides b^n, which means every distinct prime factor of the former also divides b by Euclid's lemma.

3. Let the purely repeating form be

$$\alpha = a_m a_{m-1} \dots a_1.\overline{c_1 c_2 \dots c_k}.$$

Then

$$b^k\alpha - \alpha = a_m a_{m-1} \dots a_1 c_1 c_2 \dots c_k - a_m a_{m-1} \dots a_1$$

is an integer. Letting the integer on the right side be β, we get

$$\alpha = \frac{\beta}{b^k - 1},$$

so the denominator in the lowest fraction of the rational number represented by α is coprime to b. This is because that denominator divides $b^k - 1$, and $b^k - 1$ is coprime to b for any positive integer k.

■

Theorem 10.6. Let $b \geq 2$ be an integer. A positive rational number $r = \frac{x}{y}$, where x and y are positive coprime integers, has a terminating form in base-b if and only if every distinct prime that divides y is also a prime factor of b (the multiplicities of the prime factors of y do not matter). In this case, the pre-period length is the smallest non-negative integer w such that $y \mid b^w$, regardless of which of the two dual representations is used. Note that x is irrelevant.

Proof. We may assume without loss of generality that $0 < r < 1$ because we can do Euclidean division of x by y to show that the result holds if and only if it holds in the case of the remainder divided by y. If r has a (canonical) terminating base-b form, then Theorem 10.5 asserts that every distinct prime factor of y is a prime factor of b.
Conversely, if every distinct prime factor of y is a prime factor of b, then there exists a non-negative integer m such that $y \mid b^m$ (see Problem 10.7). The trick is to write

$$r = \frac{x}{y} = \frac{\left(x \cdot \frac{b^m}{y}\right)}{b^m},$$

where the numerator $x \cdot \dfrac{b^m}{y}$ is an integer. This quotient represents a terminating form since the numerator is an integer which has a terminating form and division by the denominator b^m simply shifts the radix point of the numerator.

Now we want to find the pre-period length. Let w be the smallest non-negative integer such that $y \mid b^w$. By the above argument, $x \cdot \dfrac{b^w}{y}$ is an integer, so it is the case that $y_i = 0$ for all $i > w$. To show that w is the minimal such number, note that if $y_i = 0$ for all $i > k$ for some non-negative integer k, then $\dfrac{x}{y} \cdot b^k$ is an integer. Since x and y are coprime, this implies that $y \mid b^k$. By the minimality of w, we get $k \geq w$. Thus, w is the smallest index at which all subsequent digits are zero. Finally, the pre-period length is the same in either of the dual representations and the period is 1 in both cases (the repetend is just 0 in a terminating form), so this theorem applies to both. ■

Problem 10.7. Let $b \geq 2$ be an integer with prime factorization $b = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$, let y be a positive integer with prime factorization $y = p_1^{f_1} p_2^{f_2} \cdots p_k^{f_k}$ where some of the f_i might be 0. In Theorem 10.6, we assumed that there exists a non-negative integer m such that $y \mid b^m$. Prove that m exists and that the minimal m equals

$$s = \max\left\{\left\lceil \frac{f_i}{e_i} \right\rceil : i \in [k]\right\}.$$

Theorem 10.8. Let $b \geq 2$ be an integer. Every positive rational number has a base-b form that is eventually periodic. If $r = \dfrac{x}{y}$, where x and y are coprime positive integers, let y be factored into two positive integers uv so that all distinct prime factors of u are prime factors of b and $(v, b) = 1$ (such a decomposition can be seen to exist using the prime factorizations of y and b). Then the period of the base-b form of r is $\mathrm{ord}_v(b)$, and the pre-period length is the smallest non-negative integer w such that $u \mid b^w$. Note that x is irrelevant. To be clear, these formulas do hold in the special cases of terminating and purely periodic cases; if r has dual forms, then the formulas yield the same results for both forms. As such:

- r has a terminating base-b form if and only if $v = 1$, which is equivalent to saying that all distinct prime factors of y are prime factors of b
- r is purely periodic in base-b if and only if $u = 1$, which is equivalent to saying that y and b are coprime
- r is an integer if and only if $u = 1$ and $v = 1$ at once, which make sense because then the denominator y is 1

Thus, the rational number r terminates in some bases and does not terminate in other bases, but the form is always eventually periodic.

Proof. As in the proof of Theorem 10.6, we may assume without loss of generality that $0 < r < 1$. Let a base-b form of r be $0.x_1x_2x_3\ldots$, where we choose the terminating form if r has dual representations. To prove that this form is eventually periodic, we will show that there exist positive integers k and j such that for all positive integers $i \geq k$, $x_i = x_{i+j}$. We let u and v be as defined, and we let w be the smallest non-negative integer such that $u \mid b^w$ and we let $t = \mathrm{ord}_v(b)$. We will show that k can be taken to be w and j can be taken to be t, and that these are the smallest possible k and j. We can assume that we are working in the non-terminating case because the terminating case is equivalent to Theorem 10.6, the

results of which match what is stated here. This assumption gives us the advantage of not having to deal with dual representations, so we instead have unique forms. The idea is to shift the radix point of b by multiplying by powers of b. Omitting the minimality criteria for a moment, the assignments $k = w$ and $j = t$ work if and only if, in the forms

$$\frac{x}{y} \cdot b^{w+t} = x_1 x_2 \dots x_{w+t} . x_{w+t+1} x_{w+t+2} \dots,$$
$$\frac{x}{y} \cdot b^{w} = x_1 x_2 \dots x_{w} . x_{w+1} x_{w+2} \dots,$$

the parts to the right of the radix points match, which is true if and only if

$$0.x_{w+1} x_{w+2} \dots = 0.x_{w+t+1} x_{w+t+2} \dots$$

if and only if

$$\frac{x}{y} \cdot b^{w+t} - \frac{x}{y} \cdot b^{w}$$

is an integer. Indeed,

$$\frac{x}{y} \cdot b^{w+t} - \frac{x}{y} \cdot b^{w} = \frac{x}{y} \cdot b^{w}(b^t - 1) = x \cdot \frac{b^w}{u} \cdot \frac{b^t - 1}{v}$$

is an integer because $u \mid b^w$ and $b^t \equiv 1 \pmod{v}$ by the definitions of u, v, w, t. Thus, the base-b form of r is eventually repeating.

With the fact that r is eventually repeating established, we need to prove the minimality of w as k and t as j. Let γ and δ be positive integers such that

$$r = \frac{x}{y} = 0.c_1 c_2 \dots c_\gamma \overline{d_1 d_2 \dots d_\delta}.$$

Then

$$\frac{x}{y} \cdot b^{\gamma+\delta} - \frac{x}{y} \cdot b^{\gamma} = c_1 c_2 \dots c_\gamma d_1 d_2 \dots d_\delta - c_1 c_2 \dots c_\gamma$$

is an integer. So

$$\frac{x}{y} \cdot b^{\gamma}(b^\delta - 1) = x \cdot \frac{b^\gamma}{u} \cdot \frac{b^\delta - 1}{v}$$

is an integer. Since every prime factor of u is a prime factor of b, either $u = 1$ or $u \nmid b^\delta - 1$. And $(v, b) = 1$, so either $v = 1$ or $v \nmid b^\delta$. In any of the cases, we are forced into getting $u \mid b^\gamma$ and $b^\delta \equiv 1 \pmod{v}$. By the minimality properties embedded in the definitions of w and t, we get $\gamma \geq w$ and $\delta \geq t$. This proves that w is the minimal k and t is the minimal j. So the pre-period length is w and the period is t.

By the definition of w, the base-b form of r is purely periodic if and only if $w = 0$. If $w = 0$, then $u \mid b^w$ becomes $u \mid 1$, which forces $u = 1$. Conversely, if $u = 1$, then $w = 0$ is the smallest non-negative integer such that $u \mid b^w$. So $w = 0$ if and only if $u = 1$ if and only if $(y, b) = (uv, b) = (v, b) = 1$.

Separately, we know from Theorem 10.6 that r has a terminating form if and only if all distinct prime factors of y are prime factors of y, which is equivalent to saying that $v = 1$. ■

Problem 10.9. Find the following:

1. The reduced fraction in base-10 that is equal to 0.125_{10}
2. The terminating base-10 form of the fraction $\left(\frac{3}{40}\right)_{10}$
3. The reduced fraction in base-10 that is equal to $0.10\overline{37}_{10}$
4. The base-10 form of the the fraction $\left(\frac{1}{7}\right)_{10}$

We have not included an exercise about converting from an eventually periodic base-b form to an eventually periodic base-c form because one way of answering such a question is by converting the base-b form to a base-b fraction to a base-c fraction by converting the numerator and denominator independently, and finally by converting this to a base-c form. Thus, this kind of a conversion reduces to the other kinds of conversions in this exercise alongside the base conversions of integers.

Definition 10.10. While we will not define real numbers in general, we will note that reals that are not rational are exactly those reals that do not have an eventually periodic base-b form in some base (and therefore, every base). These numbers are called **irrational**. It follows from the preceding results that irrational numbers cannot be expressed as fractions.

Example. We showed in Theorem 2.25 that if $n \geq 2$ and $t \geq 2$ are integers such that $\sqrt[t]{n}$ is not an integer, then it is not rational. Thus, if n is not a perfect t^{th} power, then there are no base $b \geq 2$ in which $\sqrt[t]{n}$ has an eventually periodic base-b form.

Theorem 10.11 (Uncountability of real numbers)**.** It is not possible to write down an infinite list that contains all of the real numbers. In more technical language, this means that the real numbers are not countable, unlike the integers and rational numbers. This means the cardinality of $\mathbb{R}$ is a "higher" infinity than the countable cardinality of $\mathbb{Z}_+$ or $\mathbb{Z}$ or $\mathbb{Q}$, thereby proving the incredible fact that there exist different levels of infinity.

Proof. We will use a technique called Cantor diagonalization, which also has important implications in computability theory, such as in the halting problem. Suppose, for contradiction, that there exists a way of writing down a list of all real numbers, which more formally means that there exists a bijection from $\mathbb{Z}_+$ to $\mathbb{R}$. This implies that the infinite subset of real numbers in the interval $(0, 1)$ are also countable because if we can list the real numbers, then we can go through the list and pick out the real numbers in $(0, 1)$, forming a list of all such numbers. Alternatively, we can notice that the function $f : (0, 1) \to \mathbb{R}$, defined by

$$f(x) = \tan\left[\frac{\pi}{2}\left(x - \frac{1}{2}\right)\right],$$

is a bijection. So $(0, 1)$ is countable (or not countable) if and only if the same is true for $\mathbb{R}$. We have picked the interval $(0, 1)$ because their base-10 forms are convenient in that they

are positive and the only digit to the left of the radix point is 0. Our goal is to construct a real number that is missed in the list. We put the real numbers in the list in decimal form:

$$\begin{array}{cccccccc}
0 & . & \boxed{y_{1,1}} & y_{1,2} & y_{1,3} & y_{1,4} & y_{1,5} & \cdots \\
0 & . & y_{2,1} & \boxed{y_{2,2}} & y_{2,3} & y_{2,4} & y_{2,5} & \cdots \\
0 & . & y_{3,1} & y_{3,2} & \boxed{y_{3,3}} & y_{3,4} & y_{3,5} & \cdots \\
0 & . & y_{4,1} & y_{4,2} & y_{4,3} & \boxed{y_{4,4}} & y_{4,5} & \cdots \\
0 & . & y_{5,1} & y_{5,2} & y_{5,3} & y_{5,4} & \boxed{y_{5,5}} & \cdots \\
\vdots & & & & & & & \ddots
\end{array}$$

where numbers with dual representations are written in their canonical form. The digits in the diagonal from the top-left to the bottom-right have been boxed because our tactic is to construct a decimal form

$$r = 0.z_1z_2z_3z_4z_5\ldots$$

such that z_i is different from $y_{i,i}$ for each positive integer i. This continual conflict along the diagonal will ensure that this form of r does not match the written form of any of the numbers on the list. We are almost done, but there is one issue that can occur which is that this form of r might end with a tail of 9's and possibly be equal to one of the numbers in the list, despite having a different form. To prevent this, we assign the digits z_i somehow from the nine digits $\{0, 1, 2, 3, 4, 5, 6, 7, 8\}$ without ever using the digit 9. This bridges the only gap in the proof. ■

10.2 Tail of Digits of Integers

Definition 10.12. Recall from Definition 4.9 that "reducing" an integer a modulo a positive integer b usually means to find the remainder r upon Euclidean division of a by b. As such,

$$a \equiv r \pmod{b}.$$

Just like how reducing a modulo b yields the units digit of the base-b form of a, it can also be observed that reducing a modulo b^k for any positive integer k yields the rightmost k digits of the base-b form of a. This should be clear from the base-b expansion because all terms of sufficiently large index get annihilated modulo b^k:

$$\begin{aligned}
a &= (x_mx_{m-1}\ldots x_1x_0)_b \\
&= b^mx_m + b^{m-1}x^{m-1} + \cdots + bx_1 + x_0 \\
&\equiv b^{k-1}x_{k-1} + b^{k-2}x^{k-2} + \cdots + bx_1 + x_0 \\
&\equiv (x_{k-1}x_{k-2}\ldots x_1x_0)_b \pmod{b^k}.
\end{aligned}$$

We call these rightmost k digits the **k-tail** of the base-b form of a. If $k-1 > m$, this concept does not make such sense and is not too useful, but we can force it to make sense by padding the form of a with sufficiently many leading digits equal to 0.

Younger students are often aware of the fact that "units digits are affected by only units digits" in arithmetic calculations. This can be made formal and generalized as follows.

Lemma 10.13. Let $b \geq 2$ be an integer. Let α and β be positive integers with base-b forms

$$\alpha = x_m x_{m-1} \dots x_1 x_0,$$
$$\beta = y_n y_{n-1} \dots y_1 y_0$$

If k is a positive integer such that $k-1$ does not exceed m or n, and z is the k-tail of $\alpha + \beta$ and w is the k-tail of $\alpha\beta$, then

$$z \equiv \alpha + \beta = (x_{k-1} x_{k-2} \dots x_1 x_0) + (y_{k-1} y_{k-1} \dots y_1 y_0) \pmod{b^k},$$
$$w \equiv \alpha \cdot \beta = (x_{k-1} x_{k-2} \dots x_1 x_0) \cdot (y_{k-1} y_{k-1} \dots y_1 y_0) \pmod{b^k}.$$

Thus, to compute the k-tail of $\alpha + \beta$ or $\alpha \cdot \beta$, it suffices to compute only the sum or product of the k-tails of α and β, and reduce it modulo b^k. An important special case is $k = 1$, which shows that the units digit of $\alpha + \beta$ or $\alpha \cdot \beta$ can be computed by computing the sum or product of the units digits of α and β, and reducing it modulo b.

Proof. The proof of this result is immediate from the observations in Definition 10.12. There is a related result for non-positive integers α and β too, whose details we leave to the reader to write out; the arithmetic is essentially the same. ■

Example 10.14. What cyclic patterns occur when each units digit in base-10 is taken to the power of each positive integer?

Solution. Let a and k be positive integers. We can construct the following list by manual computation and prove it by induction on $k \geq 1$.

- If the units digit of a is $0, 1, 5$, or 6, then the units digit of a^k can only be $0, 1, 5$, or 6, respectively. For further results on this kind of "idempotent" property, see [15], which is a paper written by the author (at the time of this writing, it has been accepted for publication in the Mathematical Association of America's *Mathematics Magazine*).
- If the units digit of a is 4, then the units digit of a^k cycles as
$$4 \to 6 \to 4 \to \cdots.$$
- If the units digit of a is 9, then the units digit of a^k cycles as
$$9 \to 1 \to 9 \to \cdots.$$
- If the units digit of a is 2, then the units digit of a^k cycles as
$$2 \to 4 \to 8 \to 6 \to 2 \to \cdots.$$
- If the units digit of a is 3, then the units digit of a^k cycles as
$$3 \to 9 \to 7 \to 1 \to 3 \to \cdots.$$

- If the units digit of a is 7, then the units digit of a^k cycles as
$$7 \to 9 \to 3 \to 1 \to 7 \to \cdots .$$
- If the units digit of a is 8, then the units digit of a^k cycles as
$$8 \to 4 \to 2 \to 6 \to 8 \to \cdots .$$

Powers of an integer in a modulus seem to have a cyclic nature. As we will see, this is "eventually" true in each case. ■

Problem 10.15. Find the units digit of 3^{2021}.

Example 10.16. Find a cyclic pattern in the powers of 20 modulo 72.

Solution. We will keep computing powers of 20 modulo 72 until we hit a residue that is a repeat of a previous residue in this sequence. Such a collision must exist because there are infinitely many powers and only finitely many possible residues, so we can apply the pigeonhole principle. This process yields
$$20 \to 40 \to 8 \to 16 \to 32 \to 64 \to 56 \to 40.$$
So
$$20^2 \equiv 20^8 \pmod{72}$$
and induction shows that the residues
$$40 \to 8 \to 16 \to 32 \to 64 \to 56 \to \cdots$$
continue to cycle henceforth. The initial residue of 20 is akin to a rational form's pre-period. This example showcases that, while a cyclic pattern does eventually occur, it is not necessarily immediate. ■

We can connect the powers of a modulo n to eventually periodic forms of rational numbers via the following result.

Theorem 10.17. Let $b \geq 2$ and $n \geq 2$ be non-coprime integers (the coprime case is solved by the theory of multiplicative order). Then there must exist distinct positive integers r, s such that
$$b^r \equiv b^s \pmod{n},$$
and so the residues modulo n of the sequence $b, b^2, b^3, b^4, \ldots$ is periodic starting at some point. This means that there exist positive integers k and j such that for all integers $i \geq k$,
$$b^i \equiv b^{i+j} \pmod{n}.$$

Let w be the smallest possible k for which a j exists and t be the smallest j corresponding to w, so that the number of powers before the earliest member of the cycling residues appears is $w - 1$ and the number of powers in a minimal cycle is t. We can decompose n as $n = uv$, where all distinct prime factors of u are prime factors of b and $(v, b) = 1$. Then w is the smallest non-negative integer such that $u \mid b^w$ (w must be positive because u is not 1, due to b and n not being coprime) and $t = \mathrm{ord}_v(b)$. In conjunction with the theory of multiplicative order, this result provides a complete multiplicative analogue of Problem 9.1.

Proof. It follows from the pigeonhole principle that r and s exist because there are n residue classes modulo n, whereas there is a countably infinite number of positive integer exponents to which b can be raised. Once r and s are known to exist, induction easily shows that the residues of the powers b are eventually cyclic; this allows us to define k and j, and then w and t. Using the congruence

$$b^{w+t} \equiv b^w \pmod{n},$$

there exists an integer x such that

$$b^{w+t} = b^w + xn \implies \frac{1}{n} = \frac{x}{b^w(b^t - 1)}.$$

Let γ be the smallest non-negative integer such that $u \mid b^\gamma$ (note that γ must be positive) and let $\delta = \mathrm{ord}_v(b)$. Since $\frac{1}{n}$ is in lowest form and $n = uv$, it means that

$$uv \mid b^w(b^t - 1).$$

By the definitions of u and v and the same argument as in Theorem 10.8, we get that $u \mid b^w$ and $b^t \equiv 1 \pmod{v}$. By the minimality properties of of γ and δ, it holds that $w \geq \gamma$ and $t \geq \delta$. So we will have to prove the reverse inequalities as well in order to be able to invoke antisymmetry.
By Theorem 10.8,

$$\frac{1}{n} = 0.c_1c_2\ldots c_\gamma\overline{d_1d_2\ldots d_\delta}$$

for some such digits. Then

$$\frac{1}{n} \cdot b^{\gamma+\delta} - \frac{1}{n} \cdot b^\gamma,$$

which means

$$b^\gamma \equiv b^{\gamma+\delta} \pmod{n}.$$

By induction, we can show that for all integers $i \geq \gamma$,

$$b^i \equiv b^{i+\delta} \pmod{n}.$$

But w and t are the minimal such positive integers, so $\gamma \geq w$ and $\delta \geq t$. By antisymmetry, $w = \gamma$ and $t = \delta$. ■

Chapter 11

Modular Power Residues

> "I could show it implied all the standard reciprocity laws. I called it the General Reciprocity Law and tried to prove it but couldn't, even after many tries... You see, from the very beginning I had the idea to use the cyclotomic fields, but they never worked, and now I suddenly saw that all this time I had been using them in the wrong way - and in half an hour I had it."
>
> – *Emil Artin*

In modular arithmetic, one can ask about what residues are occupied by the set of perfect k^{th} powers modulo n. There are two fundamental problems in this area that we will study: counting how many such residues exist and identifying efficiently whether a given residue is such a residue. These are generally not easy problems. We will make some observations for the general cases and then algorithmically solve the identification problem in the quadratic case by showcasing a classic proof of the famed quadratic reciprocity theorem.

11.1 General Power Residues

Definition 11.1. Let $n \geq 2$ and $k \geq 2$ and a be integers. Then a is a $k^{\textbf{th}}$ **power residue** modulo n if there exists an integer x such that

$$x^k \equiv a \pmod{n}.$$

For $k = 2, 3, 4$, we call these **quadratic**, **cubic**, and **quartic** residues, respectively. This is akin to taking roots in modular arithmetic. If such an x does not exist, then we call a a $k^{\textbf{th}}$ **power non-residue** modulo n. Note that some sources require residues to be coprime to the modulus, but we have not made this restriction. We will call such an integer a a **reduced** $k^{\textbf{th}}$ **power residue** modulo n if the coprimality is important in a certain context, and otherwise we will not mention the property. Modulo n, we will denote the set of k^{th} power residue classes by $R_k(n)$ and the set of reduced k^{th} power residue classes by $S_k(n)$. Note that if a is a k^{th} power residue modulo n, then then so is every element of the congruence class of a modulo n, and similarly for reduced k^{th} power modulo n. For ease of notation and language, we might speak of a particular integer instead of its congruence class being in $R_k(n)$ or $S_k(n)$.

Let $n \geq 2$ and $k \geq 2$ be fixed integers. The "counting problem" of power residues asks for the number of k^{th} power residues modulo n. The "identification problem" of power residues asks whether we can find an efficient algorithm for deciding whether or not a given residue a

is a k^{th} power residue modulo n. These are problems that are difficult to answer in general. We will make some headway but will not give complete answers for the most part. There is also the "root-taking problem" that asks for the list of all, or at least the number of, incongruent residues x whose k^{th} powers are congruent to some fixed integer a; this is the modular analogue of asking for the list of k^{th} roots of a complex number. We will hardly touch this last problem.

Theorem 11.2 (CRT for power residues)**.** Let $t \geq 2$ be an integer, $n_1, n_2, \ldots, n_t$ be pairwise coprime positive integers, and $a_1, a_2, \ldots, a_t$ be any integers. The Chinese remainder theorem asserts the existence of an integer a that simultaneously satisfies the congruences

$$\begin{aligned} a &\equiv a_1 \pmod{n_1}, \\ a &\equiv a_2 \pmod{n_2}, \\ &\vdots \\ a &\equiv a_t \pmod{n_t}, \end{aligned}$$

and that all solutions are given by those integers that are congruent to x modulo $N = n_1 n_2 \cdots n_t$. Let $k \geq 2$ be an integer. Our claim now is that $a_i \in R_k(n_i)$ for every $i \in [t]$ if and only if $a \in R_k(N)$. Similarly, $a_i \in S_k(n_i)$ for every $i \in [t]$ if and only if $a \in S_k(N)$.

Proof. The big issue is that CRT speaks of a common solution without mentioning anything about the structure of the k^{th} powers. We will have to overcome this lack of information somehow. In one direction, it is clear that if a is a k^{th} power modulo N, then it is a k^{th} power modulo n_i for each $i \in [t]$ because $n_i \mid N$.
So we turn our concern to the other direction. Let a be the common CRT solution to the system of congruences in the theorem statement, where a is unique up to congruence modulo N. We want a to be a k^{th} power residue modulo N, assuming that there exist an integer b_i for each $i \in [t]$ such that

$$b_i^k \equiv a_i \pmod{n_i}.$$

All we can do at this point is apply CRT again to get an integer b such that

$$\begin{aligned} b &\equiv b_1 \pmod{n_1}, \\ b &\equiv b_2 \pmod{n_2}, \\ &\vdots \\ b &\equiv b_t \pmod{n_t}, \end{aligned}$$

where b is unique up to congruence modulo N. Then we find that

$$\begin{aligned} b^k \equiv b_1^k \equiv a_1 \equiv a &\pmod{n_1}, \\ b^k \equiv b_2^k \equiv a_2 \equiv a &\pmod{n_2}, \\ &\vdots \\ b^k \equiv b_t^k \equiv a_t \equiv a &\pmod{n_t}, \end{aligned}$$

which proves that

$$b^k \equiv a \pmod{N}$$

because the n_i are pairwise coprime. Therefore, the common solution a is a k^{th} power modulo N, as is every integer in its residue class modulo N.
This result can be restricted to reduced k^{th} power residues as follows. By the faux-Euclidean algorithm, $(a, n_i) = (a_i, n_i)$ for each $i \in [t]$. The multiplicativity of the two-entry gcd function with one entry fixed then yields

$$\begin{aligned}(a_1, n_1)(a_2, n_2) \cdots (a_t, n_t) &= (a, n_1)(a, n_2) \cdots (a, n_t) \\ &= (a, n_1 n_2 \cdots n_t) \\ &= (a, N).\end{aligned}$$

Therefore, $(a, N) = 1$ if and only if $(a_i, n_i) = 1$ for every $i \in [t]$. ■

Corollary 11.3. Let $t \geq 2$ be an integer, $n_1, n_2, \ldots, n_t$ be pairwise coprime positive integers, and $N = n_1 n_2 \cdots n_t$. Then there exist bijections

$$\begin{aligned}r_k &: R_k(n_1) \times R_k(n_2) \times \cdots \times R_k(n_t) \to R_k(N), \\ s_k &: S_k(n_1) \times S_k(n_2) \times \cdots \times S_k(n_t) \to S_k(N).\end{aligned}$$

This proves that the arithmetic cardinality functions $|R_k(n)|$ and $|S_k(n)|$ are multiplicative in n when k is fixed.

Proof. We use the maps that are the restrictions of the CRT map to k^{th} power residues or their reduced variants. Theorem 11.2, shows that these are indeed maps with the domains and ranges given by

$$\begin{aligned}r_k &: R_k(n_1) \times R_k(n_2) \times \cdots \times R_k(n_t) \to R_k(N), \\ s_k &: S_k(n_1) \times S_k(n_2) \times \cdots \times S_k(n_t) \to S_k(N).\end{aligned}$$

Since the mapping

$$(a_1, a_2, \ldots, a_t) \mapsto a,$$

where a is the common solution to the t congruences, has a being unique modulo N, r_k and its restriction s_k are injective. We mentioned in the proof of Theorem 11.2 that every integer in $R_k(N)$ is a k^{th} power residue modulo every n_i, so r_k is also surjective (work this out!). The restricted map s_k is also surjective because we proved that $(a, N) = 1$ if and only if $(a_i, n_i) = 1$ for every $i \in [t]$. Therefore, r_k and s_k are bijective. By the bijection and multiplication principles in combinatorics,

$$\begin{aligned}|R_k(n_1)| \cdot |R_k(n_2)| \cdots |R_k(n_t)| &= |R_k(N)|, \\ |S_k(n_1)| \cdot |S_k(n_2)| \cdots |S_k(n_t)| &= |S_k(N)|,\end{aligned}$$

so $|R_k(n)|$ and $|S_k(n)|$ are multiplicative functions in the variable n for any fixed k. ■

Therefore, to compute $|R_k(n)|$ and $|S_k(n)|$, it suffices to compute them on the maximal prime powers in the prime factorization of the input n. The following result resolves much of the identification problem for S_k, while resolving the counting problem for S_k in the case of odd prime power moduli (and providing information in the case of a modulus that is 2 or 4).

Problem 11.4 (CRT tor polynomial outputs). This problem generalizes Theorem 11.2 from k^{th} powers to polynomials with integer coefficients. Given $f \in \mathbb{Z}[x]$ and $n \in \mathbb{Z}_+$, let $R_f(n)$ denote the set of (distinct) outputs of $f(x)$ modulo n (note that it suffices to consider only $x = 0, 1, 2, \ldots, n-1$). Prove that, if n_1, n_2 are coprime positive integers, then there exists a bijection

$$\Psi_f : R_f(n_1) \times R_f(n_2) \to R_f(n_1 n_2).$$

As a result, the multiplication principle from combinatorics tells us that

$$|R_f(n_1 n_2)| = |R_f(n_1)| \cdot |R_f(n_2)|.$$

Problem 11.5 (CRT for polynomial roots). Given $f \in \mathbb{Z}[x]$ and $n \in \mathbb{Z}_+$, let $S_f(n)$ denote the set of (distinct) integer solutions of

$$f(x) \equiv 0 \pmod{n}$$

(note that it suffices to consider only $x = 0, 1, 2, \ldots, n-1$). Let n_1, n_2 be coprime positive integers. Prove that:

1. There exists a solution modulo $n_1 n_2$ if and only if there exists a solution modulo n_1 and a solution modulo n_2.
2. There exists a bijection

$$\Xi_f : S_f(n_1) \times S_f(n_2) \to S_f(n_1 n_2).$$

Consequently,

$$|S_f(n_1 n_2)| = |S_f(n_1)| \cdot |S_f(n_2)|,$$

even if one of the sets is empty.

Theorem 11.6 (Generalized Euler's criterion)**.** If $n \geq 2$ is an integer with a primitive root, $k \geq 2$ is an integer, and a is an integer coprime to n, then a is a k^{th} power residue modulo n if and only if

$$a^\ell \equiv 1 \pmod{n},$$

where $\ell = \dfrac{\varphi(n)}{(k, \varphi(n))}$. As a consequence, $|S_k(n)| = \ell$.

Proof. In one direction, suppose a is a k^{th} power residue modulo n. Then there exists an integer x such that

$$x^k \equiv a \pmod{n}.$$

Since a is coprime to n, so is x. By Euler's congruence,

$$a^\ell = a^{\frac{\varphi(n)}{(k,\varphi(n))}} \equiv \left(x^k\right)^{\frac{\varphi(n)}{(k,\varphi(n))}} \equiv \left(x^{\varphi(n)}\right)^{\frac{k}{(k,\varphi(n))}} \equiv 1^{\frac{k}{(k,\varphi(n))}} \equiv 1 \pmod{n}.$$

Conversely, suppose

$$a^\ell \equiv 1 \pmod{n}.$$

Let g be a primitive root modulo n, and let $j \in [\varphi(n)]$ satisfy $g^j \equiv a \pmod{n}$. Working backwards, there exists an integer x such that

$$x^k \equiv a \pmod{n}$$

if and only if

$$(g^i)^k \equiv g^j \pmod{n}$$

for some integer i. Since the order of g is $\varphi(n)$, this is true if and only if there exists an integer i such that

$$ik \equiv j \pmod{\varphi(n)}.$$

By Bézout's lemma, such an i exists if and only if $(k, \varphi(n)) \mid j$. This is what we will aim to prove. We know that

$$g^{\frac{j\varphi(n)}{(k,\varphi(n))}} \equiv a^\ell \equiv 1 \pmod{n}.$$

Since the order of g is $\varphi(n)$, it follows that

$$\varphi(n) \left| \frac{j\varphi(n)}{(k,\varphi(n))} \right. \implies (k,\varphi(n)) \mid j.$$

This resolves the first part of the theorem.
For the second part, we are seeking the number of distinct reduced k^{th} powers modulo n. By the first part, a is such a residue if and only if $a^\ell \equiv 1 \pmod{n}$. Note that $a^\ell \equiv 1 \pmod{n}$ if and only if the order of a modulo n is a divisor of $\ell = \dfrac{\varphi(n)}{(k,\varphi(n))}$. By Problem 9.21, if d is a divisor of $\varphi(n)$, then the number of distinct elements of order d is $\varphi(d)$. By the arithmetic summation function S_φ of φ (Theorem 3.21), summing this over all divisors of d gives

$$S_\varphi(d) = \sum_{c \mid d} \varphi(c) = d.$$

So taking $d = \dfrac{\varphi(n)}{(k,\varphi(n))}$ (which is indeed a divisor of $\varphi(n)$) yields that $|S_k(n)| = \dfrac{\varphi(n)}{(k,\varphi(n))}$. ∎

Corollary 11.7. If p is a prime, and $k \geq 2$ and a are integers such that $p \nmid a$, then a is a k^{th} power residue modulo p if and only if

$$a^{\frac{p-1}{(k,p-1)}} \equiv 1 \pmod{p}.$$

Then

$$|S_k(p)| = \frac{p-1}{(k,p-1)} = |R_k(p)| - 1$$

In the quadratic $k = 2$ case, if p is an odd prime, then we can evaluate $(k, p-1) = 2$. We will further investigate the quadratic case in the next section as there is much more to be said about it.

Proof. The only non-trivial deduction from the generalized Euler's criterion is that

$$|R_k(p)| = |S_k(p)| + 1.$$

This is true because, modulo a prime p, every non-zero element of a complete residue system is an element of the corresponding reduced residue system. It is always true that $S_k(p) \subseteq R_k(p)$ up to congruence of elements, and since p is a prime, the only element in $R_k(p)$ that is not in $S_k(p)$ is 0 (or any other element divisible by p). This accounts for the $+1$. ■

Example 11.8. Let $k \geq 2$ and $n \geq 2$ be integers. Prove the following statements.

1. The k^{th} power map modulo an integer n is bijective on the set of reduced residue classes modulo n if and only if $(k, \varphi(n)) = 1$. Consequently, if $n \geq 3$ and $2 \mid k$, then there exists at least one reduced residue class modulo n in $S_k(n)$ that is not represented in the image of the map.

2. Let n have a primitive root g. Then g is a k^{th} power residue modulo n if and only if $(k, \varphi(n)) = 1$. Subsequently, g cannot be a quadratic residue if $n \geq 3$.

Solution. The proofs of the second set of statements will depend on the first.

1. A map is bijective if and only if it has an inverse, so we will construct an inverse. On one end of the implication, Bézout's lemma says that $(k, \varphi(n)) = 1$ if and only if there exist integers x and y such that $kx - \varphi(n)y = 1$. Then, for every integer a coprime to n,

   $$(a^x)^k \equiv (a^k)^x \equiv a^{kx} \equiv a^{1+\varphi(n)y} \equiv a \cdot (a^{\varphi(n)})^y \equiv a \pmod{n}.$$

   So the x^{th} power map is an inverse of the k^{th} power map. Conversely, suppose the k^{th} power map is bijective on the set of invertible residue classes. Suppose, for the sake of contradiction, that $(k, \varphi(n)) = d$ is greater than 1. Since d is a factor of $\varphi(n)$, there exists an element b of order d by Problem 9.21. Because $d \neq 1$, $b \not\equiv 1 \pmod{n}$, yet

   $$b^k \equiv 1 \equiv 1^k \pmod{n},$$

   so the k^{th} power map is not injective, which is a contradiction. Thus, $(k, \varphi(n)) = 1$.

   Now we address the consequence. If $n \geq 3$, then $\varphi(n)$ is even. So if k is also even, then our result implies that not every reduced residue class will be represented among the reduced k^{th} powers modulo n.

2. If the primitive root g is a k^{th} power residue, then there exists an integer x such that $x^k \equiv g \pmod{n}$. Then every power of g is a k^{th} power as well. Since the powers of g generate a reduced residue system, this implies that $(k, \varphi(n)) = 1$ by the last part. Conversely by the last part again, if $(k, \varphi(n)) = 1$, then every integer coprime to n, including g, is represented in $S_k(n)$. If $n \geq 3$, then $\varphi(n)$ is even. Then in the special case $k = 2$, the fact that $(k, \varphi(n)) = 2 > 1$ implies that g is not quadratic residue.

■

Problem 11.9. While combining the last part of Theorem 11.6 with the multiplicative property in Corollary 11.3 allows us to compute $|S_k(n)|$ when $\nu_2(n) \leq 2$, it does not tell us what happens when $\nu_2(n) \geq 3$. To do this, we will have to separately compute $|S_k(2^n)|$ for $n \geq 3$, since the primitive root method used for odd prime powers does not work in this case. Let $k \geq 2$ and $n \geq 3$ be fixed integers. As proven in Problem 9.5, the invertible elements modulo 2^n are given by the $\varphi(2^n) = 2^{n-1}$ distinct elements of

$$S = \left\{ \pm 5^i : i \in [2^{n-2}] \right\}.$$

Use Example 11.8 to prove that

$$|S_k(2^n)| = \begin{cases} \dfrac{2^{n-2}}{(k, 2^{n-2})} & \text{if } 2 \mid k \\ 2^{n-1} & \text{if } 2 \nmid k \end{cases}.$$

As a hint, the quantity $\nu_2(k) = j$ will be helpful.

Thus, Problem 11.9 shows how to compute $|S_k(n)|$. In [17], Stangl found formulas for $|R_2(n)|$. Extending Stangl's methods, the author of this book derived a general formula for $|R_k(n)|$ and published it [16]. The formula is as follows.

Definition 11.10. Let ϵ be the parity function. So for integers t, $\epsilon(t) = \begin{cases} 0 & \text{if } 2 \mid t \\ 1 & \text{if } 2 \nmid t \end{cases}$.

Theorem 11.11. Let p be a prime, and $k \geq 2$ and $m \geq 1$ be integers. Let r be the remainder of m upon division by k. Let

$$\begin{aligned} \alpha &= \frac{p-1}{(k, p-1)}, \\ \beta &= (\nu_p(k) + 1)(1 - \epsilon(k))(1 - \epsilon(p)) + \nu_p(k)\epsilon(p), \\ \gamma &= \begin{cases} k & \text{if } k \mid m \\ r & \text{if } k \nmid m \end{cases}. \end{aligned}$$

Then

$$\begin{aligned} |R_k(p^m)| &= \alpha \cdot \left(\frac{p^k}{p^{\beta+1}} \cdot \frac{p^m - p^\gamma}{p^k - 1} + \left\lceil \frac{p^\gamma}{p^{\beta+1}} \right\rceil \right) + 1 \\ &= \alpha \cdot \left\lceil \frac{1}{p^{\beta+1}} \cdot \frac{p^{m+k} - p^\gamma}{p^k - 1} \right\rceil + 1, \end{aligned}$$

(Note that the $\dfrac{p^k}{p^{\beta+1}} \cdot \dfrac{p^m - p^\gamma}{p^k - 1}$ term is necessarily an integer, so it can be absorbed into the ceiling term $\left\lceil \dfrac{p^\gamma}{p^{\beta+1}} \right\rceil$ as shown.)

In a sense, the pursuit of this formula led to the writing of this book, and the writing of the book led to the derivation of the formula. The proof depends on numerous number-theoretic technicalities of which the author was unaware before writing Volume 3.

11.2 Quadratic Residues

The generalized Euler's criterion gives a partial solution to the identification problem of power residues. In general, what we want is a mechanism for deciding whether a given residue a is a k^{th} power residue modulo n, where the method should be more efficient than computing all k^{th} power residues modulo n and checking if any one is congruent to a. Identifying higher order powers is not an easy task, but a simple process exists for quadratic residues modulo odd primes. It involves what Gauss privately called the Theorema Aureum, or the "Golden Theorem." This is the law of quadratic reciprocity that we will charge towards now.

Theorem 11.12 (Euler's criterion)**.** If p is an odd prime and a is an integer, then

$$a^{\frac{p-1}{2}} \equiv \begin{cases} 1 \pmod{p} & \text{if } a \text{ is a non-zero quadratic residue modulo } p \\ -1 \pmod{p} & \text{if } a \text{ is a quadratic non-residue modulo } p \\ 0 \pmod{p} & \text{if } a \equiv 0 \pmod{p} \end{cases}.$$

Proof. Of course, $0^{\frac{p-1}{2}} \equiv 0 \pmod{p}$. We also know from the generalized Euler's criterion (Theorem 11.6) that if $p \nmid a$, then a is a quadratic residue modulo p if and only if

$$a^{\frac{p-1}{2}} \equiv 1 \pmod{p}.$$

The remaining question is what happens if a is a quadratic non-residue modulo p. In that case, let g be a primitive root modulo p and $i \in [p-1]$ be an integer such that

$$g^i \equiv a \pmod{p}.$$

If i were even, then

$$a \equiv g^i \equiv (g^{\frac{i}{2}})^2 \pmod{p}$$

would be a quadratic residue modulo p, contrary to the assumption. So $i = 2j+1$ for some non-negative integer j. Then

$$a^{\frac{p-1}{2}} \equiv (g^{2j+1})^{\frac{p-1}{2}} \equiv (g^{p-1})^j \cdot g^{\frac{p-1}{2}} \equiv g^{\frac{p-1}{2}} \pmod{p}.$$

By difference of squares,

$$\left(g^{\frac{p-1}{2}} - 1\right)\left(g^{\frac{p-1}{2}} + 1\right) \equiv g^{p-1} - 1 \equiv 0 \pmod{p}.$$

So one of the following must be true:

$$g^{\frac{p-1}{2}} \equiv 1 \pmod{p},$$
$$g^{\frac{p-1}{2}} \equiv -1 \pmod{p}.$$

The former is impossible because it would contradict the minimality of $\varphi(p) = p-1$ as the smallest positive exponent to send the primitive root g to 1. Therefore,

$$a^{\frac{p-1}{2}} \equiv g^{\frac{p-1}{2}} \equiv -1 \pmod{p}.$$

Note that this amazing fact that $a^{\frac{p-1}{2}}$ returns the same residue for every quadratic non-residue does not carry over to k^{th} powers modulo n in general. For example, if n has a primitive root, then the generalized Euler's criterion says that the number of k^{th} power residues that are coprime to n is $\dfrac{\varphi(n)}{(k,\varphi(n))}$; we also know from the same theorem that an integer a coprime to n is a k^{th} power residue modulo n if and only if

$$a^{\frac{\varphi(n)}{(k,\varphi(n))}} \equiv 1 \pmod{n}.$$

The problem is that the expression on the left side can take on several or even many residues modulo n, not just two, as a ranges over all integers coprime to n. We can use the generalized Euler's criterion to say that the number of distinct residues modulo n taken on by the expression $a^{\frac{\varphi(n)}{(k,\varphi(n))}}$ is

$$\frac{\varphi(n)}{\left(\frac{\varphi(n)}{(k,\varphi(n))},\varphi(n)\right)} = \frac{\varphi(n)}{\left(\frac{\varphi(n)}{(k,\varphi(n))}\right)} = (k,\varphi(n)).$$

This is rarely equal to 2, so it cannot be claimed that $a^{\frac{\varphi(n)}{(k,\varphi(n))}}$ is always equal to some special residue modulo, such as -1 for every reduced k^{th} power non-residue a modulo n. And all of this does not even scratch the surface of what happens if a is not coprime to the modulus n. The case of a quadratic exponent and prime modulus is indeed special. ■

Corollary 11.13. Let p be an odd prime, and let a, b be integers. Then the following convenient closure-like properties hold modulo p.

- If one of a, b is divisible by p, then ab is divisible by p.
- If a, b are non-zero (meaning non-divisible by p) quadratic residues, then ab is a non-zero quadratic residue.
- If a, b are quadratic non-residues, then ab is a non-zero quadratic residue. (Yes, that's right!)
- If one of a, b is a non-zero quadratic residue and one of a, b is a quadratic non-residue, then ab is a quadratic non-residue.

Proof. The first property is trivial from the perspective of divisibility. So now we will assume that both a, b are non-divisible by p, and therefore $p \nmid ab$ as well by the contrapositive of Euclid's lemma. The other three properties are true by Euler's criterion because

$$a^{\frac{p-1}{2}} \cdot b^{\frac{p-1}{2}} \equiv (ab)^{\frac{p-1}{2}} \pmod{p}$$

and

$$\begin{aligned} 1 \cdot 1 &\equiv 1 \pmod{p}, \\ (-1) \cdot (-1) &\equiv 1 \pmod{p}, \\ (-1) \cdot 1 &\equiv -1 \pmod{p}. \end{aligned}$$

■

Definition 11.14. If p is an odd prime and a is an integer, then the **Legendre symbol** is defined as

$$\left(\frac{a}{p}\right) = \begin{cases} 0 & \text{if } a \equiv 0 \pmod{p} \\ 1 & \text{if } a \text{ if a non-zero quadratic residue modulo } p \\ -1 & \text{if } a \text{ if a quadratic non-residue modulo } p \end{cases}$$

I had an undergraduate acquaintance who used to pronounce the Legendre symbol as "a leg p" where the 'g' is pronounced as a 'j.' This pronunciation works well.

Corollary 11.15 (Legendre symbol properties)**.** The following are some properties of the Legendre symbol that should be clear from our work so far:

1. Euler's criterion says that
$$\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod{p}.$$
This holds even if $p \mid a$.

2. It is worth defining the Legendre symbol because, by Corollary 11.13, the function
$$\left(\frac{\cdot}{p}\right) : \mathbb{Z} \to \{0, -1, 1\},$$
where the dot is the input and p is a fixed odd prime, is completely multiplicative.

3. A fact that we would like to emphasize is that, if $p \nmid a$, then $\left(\frac{a}{p}\right)^2 = 1$, which allows us to multiply both sides of an equation by a Legendre symbol in order to change the side on which it appears (assuming the Legendre symbol is originally in a product). As a meaningless example, if $p \nmid a$ then
$$\left(\frac{a}{p}\right)(x-y)^2 = z \implies (x-y)^2 = \left(\frac{a}{p}\right)z.$$

Problem 11.16. The purpose of the following steps is to complete the final one, which is about counting the number of points on a circle in modular arithmetic.

1. Let p be a prime and k be a positive integer. Prove that
$$S = \sum_{i=1}^{p} i^k \equiv \begin{cases} -1 \pmod{p} & \text{if } p-1 \mid k \\ 0 \pmod{p} & \text{if } p-1 \nmid k \end{cases}.$$

2. Prove that, for any odd prime p and any integer c, the number of solutions x to
$$x^2 \equiv c \pmod{p}$$
is $\left(\frac{c}{p}\right) + 1$.

3. Let p be an odd prime and a be an integer. Find a closed formula for the number of solutions (x, y) modulo p of

$$x^2 + y^2 \equiv a \pmod{p}.$$

The answer should show that, if $a \not\equiv 0 \pmod{p}$, then the formula depends only on p and not a, meaning the number of lattice points of a "circle" of non-zero radius modulo an odd prime p depends only on the modulus and not the radius.

Problem 11.17. Let p be a prime that is congruent to 3 modulo 4. Prove that if a is an integer such that $\left(\frac{a}{p}\right) = 1$, then there are exactly two distinct integers x modulo p such that $x^2 \equiv a \pmod{p}$. These "square roots" of a, so to speak, are congruent to $\pm a^{\frac{p+1}{4}}$.

Problem 11.18. Prove that, if p is a prime congruent to 3 modulo 4, then each quadratic non-residue modulo p is congruent to the negation of some quadratic residue modulo p. This is used in Theorem 12.15.

Corollary 11.19 (First supplement to quadratic reciprocity)**.** If p is an odd prime, then

$$\left(\frac{-1}{p}\right) = \begin{cases} 1 & \text{if } p \equiv 1 \pmod{4} \\ -1 & \text{if } p \equiv 3 \pmod{4} \end{cases}.$$

Proof. By Euler's criterion,

$$\left(\frac{-1}{p}\right) \equiv (-1)^{\frac{p-1}{2}} \pmod{p}.$$

- If $p \equiv 1 \pmod{4}$, then $\dfrac{p-1}{2}$ is even. So $(-1)^{\frac{p-1}{2}} = 1$, making -1 a non-zero quadratic residue modulo p.
- If $p \equiv 3 \pmod{4}$, then $\dfrac{p-1}{2}$ is odd. So $(-1)^{\frac{p-1}{2}} = -1$, making -1 a quadratic non-residue modulo p.

■

Example 11.20. Recall that a Mordell curve is a special elliptic curve

$$y^2 = x^3 + n$$

for a fixed non-zero integer n. Mordell proved that every such equation has only finitely many (possibly zero) integer points (x, y). The proof is advanced, but we can show the non-existence of solutions in some cases via the modular arithmetic contradiction trick. Prove that $y^2 = x^3 + 7$ has no integer solutions. This equation appears in Engel's book [6]. A number of examples of such proofs, including this one, have been collected by Keith Conrad in [5].

Solution. The proof that we will show is due to V. A. Lebesgue, with the original paper referenced in Conrad's aforementioned article. The trick is to use the sum of cubes factorization to rewrite the equation as

$$\begin{aligned} y^2 + 1 = x^3 + 8 &= (x+2)(x^2 - 2x + 4) \\ &= (x+2)((x-1)^2 + 3). \end{aligned}$$

Now we do casework on the parity of x. If x is even, then $2 \mid x+2$ and $4 \mid (x-1)^2 + 3$, so

$$y^2 \equiv -1 \pmod 8.$$

This is impossible because the only odd square modulo 8 is 1 and the even squares are unsuitable. So x is odd. This implies that

$$(x-1)^2 + 3 \equiv 3 \pmod 4.$$

Since $(x-1)^2 + 3$ is a product of odd primes, let p be any such prime factor. Since $p \mid (x-1)^2 + 3$, it is then true that

$$y^2 \equiv -1 \pmod p.$$

By the first supplement to quadratic reciprocity, this implies that $p \equiv 1 \pmod 4$. However, we can assert that there is an odd prime $q \equiv 3 \pmod 4$ that divides $(x-1)^2 + 3$ because otherwise $(x-1)^2 + 3$ would be a product of only primes congruent to 1 (mod 4), whose product would also be congruent to 1 (mod 4) instead of the established 3 (mod 4). Thus, we have a contradiction and so there are no integer solutions.
This proof showcases that the modular arithmetic contradiction trick (see Section 5.2) can take on more involved forms and can even utilize the theory of quadratic residues! ■

Lemma 11.21 (Gauss's lemma on quadratic residues)**.** Let p be an odd prime and a be an integer that is not divisible by p. Let t be the number of integers in

$$R = \left\{ a, 2a, 3a, \ldots, \frac{p-1}{2} \cdot a \right\}$$

who least positive residue is greater than $\frac{p}{2}$. Then $\left(\frac{a}{p}\right) = (-1)^t$.

Proof. What makes this result rather strange is that we do not ordinarily mix inequalities with modular arithmetic. One can come across this result by playing around with the possibility of combining a function that reflects least residues across $\frac{p}{2}$ on the number line with taking a product like in Wilson's theorem. Let us see how this works out.
To get $(-1)^t$, we need a product in which the number of times that -1 appears is the number of elements of R whose least positive residue is greater than $\frac{p}{2}$. The critical idea, which will

also be used in the upcoming Eisenstein's lemma (Lemma 11.24), is to let $r(x)$ be the least non-negative residue of x modulo p and then define the reflection function

$$\|\cdot\| : \mathbb{Z}\backslash\{mp : m \in \mathbb{Z}\} \to \left[\frac{p-1}{2}\right]$$
$$x \mapsto \begin{cases} r(x) & \text{if } 1 \leq r(x) \leq \dfrac{p-1}{2} < \dfrac{p}{2} \\ p - r(x) & \text{if } \dfrac{p}{2} < \dfrac{p+1}{2} \leq r(x) \leq p-1 \end{cases}.$$

It can be verified that $\left[\frac{p-1}{2}\right]$ is in fact a codomain of $\|\cdot\|$ since $r(x) \in [p-1]$. We claim that $\|\cdot\|$ is bijective when restricted to the domain R. Since R and $\left[\frac{p-1}{2}\right]$ both have $\frac{p-1}{2}$ elements, it suffices to prove injectivity. Suppose i and j are elements of $\left[\frac{p-1}{2}\right]$ such that $\|ia\| = \|ja\|$. Then one of the following must be true:

$$ia \equiv ja \pmod{p},$$
$$ia \equiv p - ja \pmod{p}.$$

Cancelling a from both sides of both congruences, we get $i \equiv \pm j \pmod{p}$. If $i \equiv j \pmod{p}$, then $i = j$ since they are both integers in $\left[\frac{p-1}{2}\right]$. If $i \equiv -j \pmod{p}$, then $p \mid i + j$. Since $i, j \in \left[\frac{p-1}{2}\right]$, we have

$$2 \leq i + j \leq p - 1,$$

so it is not possible that p divides $i + j$. Therefore, $i = j$ and we have injectivity, leading to bijectivity.

Now we will pull our Wilson-type move. In increasing order, let the set of least residues of the elements of R be

$$\{\beta_1, \beta_2 \ldots, \beta_s, \gamma_1, \gamma_2 \ldots, \gamma_t\},$$

where $\beta_s < \frac{p}{2} < \gamma_1$ and $s + t = \frac{p-1}{2}$. Then we can compute the product $\prod_{k=1}^{\frac{p-1}{2}} \|ka\|$ in two different ways modulo p. Using the fact that $\|\cdot\| : R \to \left[\frac{p-1}{2}\right]$ is bijective,

$$\prod_{k=1}^{\frac{p-1}{2}} \|ka\| = \left(\frac{p-1}{2}\right)!.$$

On the other hand, we can use the least residues β_i and γ_j to get

$$\prod_{k=1}^{\frac{p-1}{2}} \|ka\| = \left(\prod_{i=1}^{s} \beta_i\right)\left(\prod_{j=1}^{t} (p-\gamma_j)\right) \equiv (-1)^t \cdot \left(\prod_{i=1}^{s} \beta_i \prod_{j=1}^{t} \gamma_j\right)$$
$$\equiv (-1)^t \cdot \prod_{k=1}^{\frac{p-1}{2}} ka \equiv (-1)^t \cdot \left(\frac{p-1}{2}\right)! \cdot a^{\frac{p-1}{2}} \pmod{p}.$$

Equating the two expressions modulo p yields

$$\left(\frac{p-1}{2}\right)! \equiv (-1)^t \cdot \left(\frac{p-1}{2}\right)! \cdot a^{\frac{p-1}{2}} \pmod{p}.$$

This is equivalent to

$$a^{\frac{p-1}{2}} \equiv (-1)^t \pmod{p},$$

which gives us what we want due to Euler's criterion and the definition of the Legendre symbol. ■

Corollary 11.22 (Second supplement to quadratic reciprocity)**.** If p is an odd prime, then

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}} = \begin{cases} 1 & \text{if } p \equiv \pm 1 \pmod 8 \\ -1 & \text{if } p \equiv \pm 3 \pmod 8 \end{cases}.$$

Proof. By Gauss's lemma, $\left(\frac{2}{p}\right) = (-1)^t$, where t is the number of elements of

$$R = \left\{2 \cdot 1, 2 \cdot 2, \ldots, 2 \cdot \frac{p-1}{2}\right\} = \{2, 4, \ldots, p-1\}$$

whose least residues (the elements are their own least residues in this case) are greater than $\frac{p}{2}$. Note that $2k > \frac{p}{2}$ if and only if $k > \frac{p}{4}$. The number of such k in $\left[\frac{p-1}{2}\right]$ is

$$\frac{p-1}{2} - \left\lfloor \frac{p}{4} \right\rfloor.$$

We want the parity of t. Trying out the various possible residues of p modulo 8 yields

$$t = \frac{p-1}{2} - \left\lfloor \frac{p}{4} \right\rfloor = \begin{cases} 4q + 2q \equiv 0 \pmod 2 & \text{if } p = 8q+1 \\ 4q + 1 + 2q \equiv 1 \pmod 2 & \text{if } p = 8q+3 \\ 4q + 2 + 2q + 1 \equiv 1 \pmod 2 & \text{if } p = 8q+5 \\ 4q + 3 + 2q + 1 \equiv 0 \pmod 2 & \text{if } p = 8q+7 \end{cases}$$

Thus, t is even if and only if $p \equiv \pm 1 \pmod 8$. We leave it to the reader to check that the identity $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$ holds in each of the four odd residue classes modulo 8. ■

Problem 11.23. In 1949, Chowla made a conjecture reminiscent of Pinoccio's desire to be a real boy. He conjectured that if k is a positive integer and a is an integer such that a is a k^{th} power residue modulo every prime p, then a is a perfect k^{th} power among the integers. Disprove this conjecture by taking $a = 2^4$ and $k = 8$. However, show that this conjecture is true if we expand the "every prime p" condition to "every positive integer n." As a side note, Ankeny and Rogers established in [2] that Chowla's original conjecture holds if and only if $8 \nmid k$.

Lemma 11.24 (Eisenstein's lemma)**.** Let p be an odd prime and a be an odd integer that is not divisible by p. Letting

$$\varepsilon_p(a) = \sum_{k=1}^{\frac{p-1}{2}} \left\lfloor \frac{ka}{p} \right\rfloor,$$

it holds that

$$\left(\frac{a}{p}\right) = (-1)^{\varepsilon_p(a)}.$$

Proof. By Gauss's lemma on quadratic residues (Lemma 11.21), we wish to prove that

$$\varepsilon_p(a) \equiv t \pmod 2,$$

where t is the number of elements of

$$R = \left\{a, 2a, \ldots, \frac{p-1}{2} \cdot a\right\}$$

whose least residues modulo p are greater than $\dfrac{p}{2}$. To simultaneously bring floor functions and least residues into play, we apply Euclidean division to get

$$ka = pq_k + r_k, \text{ and } 0 < r_k < p.$$

Note that $r_k \neq 0$ because p divides neither k nor a. Then

$$\frac{ka}{p} = q_k + \frac{r_k}{p} \implies \left\lfloor \frac{ka}{p} \right\rfloor = q_k.$$

Instead of multiplying the ka as in Gauss's lemma, we try adding them here to get

$$\sum_{k=1}^{\frac{p-1}{2}} ka = p \cdot \sum_{k=1}^{\frac{p-1}{2}} q_k + \sum_{k=1}^{\frac{p-1}{2}} r_k = p \cdot \sum_{k=1}^{\frac{p-1}{2}} \left\lfloor \frac{ka}{p} \right\rfloor + \sum_{k=1}^{\frac{p-1}{2}} r_k.$$

Using the notation from the proof of Gauss's lemma, we can rewrite the remainders r_k in terms of the β_i and γ_j so that the above sums equals

$$a \cdot \sum_{k=1}^{\frac{p-1}{2}} k = p \cdot \varepsilon_p(a) + \sum_{i=1}^{s} \beta_i + \sum_{j=1}^{t} \gamma_j$$

Recall that

$$\{\beta_1, \beta_2 \ldots, \beta_s, p-\gamma_1, p-\gamma_2 \ldots, p-\gamma_t\} = \left[\frac{p-1}{2}\right],$$

which yields the sum

$$\sum_{k=1}^{\frac{p-1}{2}} k = \sum_{i=1}^{s} \beta_i + \sum_{j=1}^{t} (p-\gamma_j).$$

Subtracting this from the previous equation yields

$$(a-1) \cdot \sum_{k=1}^{\frac{p-1}{2}} k = p \cdot \varepsilon_p(a) + 2 \cdot \sum_{j=1}^{t} \gamma_j - pt.$$

Using the fact a is odd, we can reduce this modulo 2 to get

$$p \cdot \varepsilon_p(a) \equiv pt \pmod 2.$$

Finally, we can cancel p from both sides because p is odd and so it is coprime to the modulus 2. ■

Theorem 11.25 (Law of Quadratic Reciprocity)**.** If p and q are odd primes, then, in the notation of Eisenstein's lemma (Lemma 11.24),

$$\varepsilon_p(q) + \varepsilon_q(p) = \frac{p-1}{2} \cdot \frac{q-1}{2}.$$

As a consequence, we gain an efficient computational tool, the law of quadratic reciprocity:

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}}.$$

Proof. If we can prove the initial identity, then

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\varepsilon_p(q)} \cdot (-1)^{\varepsilon_q(p)} = (-1)^{\varepsilon_p(q)+\varepsilon_q(p)},$$

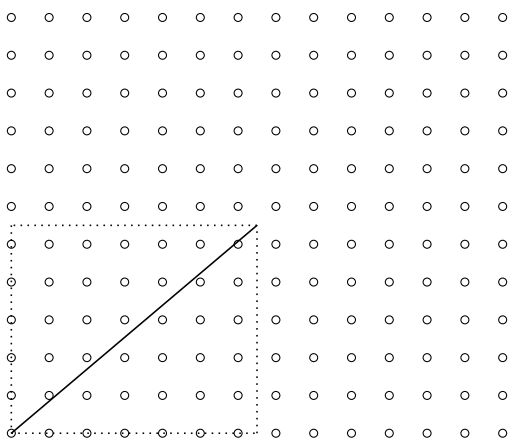
and the rest follows from Eisenstein's lemma. So our goal is to prove the algebraic identity that

$$\sum_{i=1}^{\frac{p-1}{2}} \left\lfloor \frac{iq}{p} \right\rfloor + \sum_{j=1}^{\frac{q-1}{2}} \left\lfloor \frac{jp}{q} \right\rfloor = \frac{p-1}{2} \cdot \frac{q-1}{2}.$$

In an astonishing medley of ideas from geometry, combinatorics, and number theory, we will provide a proof of this identity by double counting on the Cartesian plane. Specifically, we will count the number of lattice points in the interior of the rectangle with vertices at

$$(0,0), \left(\frac{p}{2}, 0\right), \left(0, \frac{q}{2}\right), \left(\frac{p}{2}, \frac{q}{2}\right)$$

in two ways, where by "interior" we mean that we exclude any lattice points on the boundary. Below is an example for $p = 13$ and $q = 11$.



The key is to draw the diagonal from the bottom-left corner $(0,0)$ to the top-right corner $\left(\frac{p}{2},\frac{q}{2}\right)$. The equation of this diagonal is $y = \frac{q}{p}\cdot x$ and at each x-coordinate under it, $x = 1, 2, \ldots, \frac{p-1}{2}$, the number of lattice points strictly above $(x,0)$ and strictly below the diagonal is $\left\lfloor \frac{xq}{p} \right\rfloor$ by the definition of the floor function. So the number of lattice points in the interior of the triangle with vertices $(0,0), \left(\frac{p}{2},0\right), \left(\frac{p}{2},\frac{q}{2}\right)$ is

$$\sum_{i=1}^{\frac{p-1}{2}} \left\lfloor \frac{iq}{p} \right\rfloor = \varepsilon_p(q).$$

Similarly, we can use the y-axis on the remaining triangle with vertices $(0,0), \left(0,\frac{q}{2}\right), \left(\frac{p}{2},\frac{q}{2}\right)$ to get that the number of lattice points in its interior is

$$\sum_{j=1}^{\frac{q-1}{2}} \left\lfloor \frac{jp}{q} \right\rfloor = \varepsilon_q(p).$$

Moreover, since $\gcd(p,q) = 1$, the interior of the line segment from $(0,0)$ to (p,q) contains no lattice points by Corollary 6.4, so there are no lattice points on the drawn diagonal of our rectangle. Thus, the total number of lattice points in the interior of the rectangle is

$$\varepsilon_p(q) + \varepsilon_q(p),$$

which we can alternatively count as $\frac{p-1}{2}\cdot\frac{q-1}{2}$. This completes the proof. ■

Mathematicians initially found it difficult to prove the law of quadratic reciprocity. Euler and Legendre conjectured it without proof, and Gauss said "... for a whole year, it tormented it and absorbed my greatest efforts until at last I obtained a proof..." By the end of his life, Gauss had six published proofs and two unpublished proofs of the law of quadratic reciprocity. At the time of writing, Heidelberg University has a web page with 247 proofs listed [18]!

Example 11.26. The form

$$\left(\frac{p}{q}\right) = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}\left(\frac{q}{p}\right)$$

of quadratic reciprocity can be more useful in practice than the original symmetric form. Use this to determine whether -14 is a quadratic residue modulo 31.

Solution. By the complete multiplicativity of the Legendre symbol in the upper entry,

$$\left(\frac{14}{31}\right) = \left(\frac{-1}{31}\right)\left(\frac{2}{31}\right)\left(\frac{7}{31}\right).$$

By the first supplement to quadratic reciprocity (Corollary 11.19),

$$31 \equiv -1 \pmod 4 \implies \left(\frac{-1}{31}\right) = -1.$$

By the second supplement to quadratic reciprocity (Corollary 11.22),

$$31 \equiv -1 \pmod 8 \implies \left(\frac{2}{31}\right) = 1.$$

By quadratic reciprocity (Theorem 11.25),

$$\begin{aligned}\left(\frac{7}{31}\right) &= (-1)^{\frac{7-1}{2}\cdot\frac{31-1}{2}}\left(\frac{31}{7}\right) = -\left(\frac{31}{7}\right) = -\left(\frac{3}{7}\right)\\ &= -(-1)^{\frac{3-1}{2}\cdot\frac{7-1}{2}}\left(\frac{7}{3}\right) = \left(\frac{7}{3}\right) = \left(\frac{1}{3}\right) = 1,\end{aligned}$$

where we used the fact that $1^2 \equiv 1 \pmod 3$ in the final step. The last step typically involves some such minor manual computation. Therefore,

$$\left(\frac{14}{31}\right) = \left(\frac{-1}{31}\right)\left(\frac{2}{31}\right)\left(\frac{7}{31}\right) = (-1)\cdot 1\cdot 1 = -1,$$

so -14 is not a quadratic residue modulo 31.
This example displays the effectiveness of quadratic reciprocity as a computational tool for the identification of quadratic residues and non-residues. ■

Next, we present an example similar to Problem 11.23, but in the quadratic case and modulo primes instead.

Example 11.27. Prove that, if $a \in \mathbb{Z}$ is a quadratic residue modulo all primes beyond some lower bound, then a is a perfect square in the integers.

Solution. If $a = 0$, the result is trivial, so suppose $a \neq 0$. The strategy will be to slice off the largest square factor of a, and to show that the leftover squarefree part can only be 1, thereby establishing that the original integer a was a square.
Suppose $a = bc^2$, where b is the (possibly negative) squarefree part of a. If q is a prime that is greater than c^2, then q is not a prime factor of c, so

$$x^2 \equiv a \pmod{q} \implies (xc^{-1})^2 \equiv \frac{a}{c^2} \equiv b \pmod{q}.$$

Then b, like a, is a quadratic residue modulo all sufficiently large primes. We wish to show that $b = 1$, which will suffice in proving that $a = bc^2 = c^2$ is a square in the integers. Suppose $b \neq 1$, for the sake of contradiction. Then

$$b = \pm p_1 p_2 \cdots p_m$$

for some positive integer m and distinct primes p_i. We will derive a contradiction by finding an infinite sequence of primes s such that $\left(\frac{b}{s}\right) = -1$, which will contradict the fact that b is a quadratic residue modulo all sufficiently large primes (we need just one sufficiently large s).
Suppose, for contradiction, that one of prime factors of b, say p_m, is odd. Then p_m has a primitive root g, which we know to be a quadratic non-residue by Example 11.8. By the Chinese remainder theorem, the system of congruences

$$\begin{aligned} x &\equiv 1 \pmod{8p_1 p_2 \cdots p_{m-1}}, \\ x &\equiv g \pmod{p_m} \end{aligned}$$

has a simultaneous solution y, and all integer solutions are given by $(y + 8p_1 p_2 \cdots p_m \cdot n)_{n \in \mathbb{Z}}$ (the 8 is there so that we can exploit the second supplement to quadratic reciprocity in a moment). By the fact that y satisfies both congruences, y must be coprime to 8 and all of the p_i, so

$$\gcd(y, 8p_1 p_2 \cdots p_m) = 1.$$

Now we will use a non-elementary theorem, which is why this is an example and not a problem. By Dirichlet's theorem on primes in arithmetic progressions, there exist infinitely many primes in the arithmetic sequence

$$(y + 8p_1 p_2 \cdots p_m \cdot n)_{n=1}^{\infty}.$$

Picking any such prime s, we know from the second and first supplements to quadratic reciprocity that

$$\begin{aligned} s \equiv y \equiv 1 \pmod{8} &\implies \left(\frac{2}{s}\right) = 1, \\ s \equiv y \equiv 1 \pmod{4} &\implies \left(\frac{-1}{s}\right) = 1. \end{aligned}$$

By quadratic reciprocity, the second line also implies

$$\left(\frac{p_i}{s}\right) = (-1)^{\frac{s-1}{2}\cdot\frac{p_i-1}{2}}\left(\frac{s}{p_i}\right) = \left(\frac{s}{p_i}\right) = \begin{cases} 1 & \text{if } i \neq m \\ -1 & \text{if } i = m \end{cases}$$

for indices $i \in [m]$, since

$$\begin{aligned} s \equiv y \equiv 1 \pmod{p_i},\ i \neq m, \\ s \equiv y \equiv g \pmod{p_m}. \end{aligned}$$

Then, for any s in the sequence of primes provided by Dirichlet,

$$\left(\frac{b}{s}\right) = \left(\frac{\pm 1}{s}\right) \cdot \left[\prod_{i=1}^{m-1}\left(\frac{p_i}{s}\right)\right] \cdot \left(\frac{p_m}{s}\right) = 1 \cdot \left(\prod_{i=1}^{m} 1\right) \cdot (-1) = -1,$$

which contradicts the fact that b is a quadratic residue modulo all sufficiently large primes, as long as s is taken to be among those sufficiently large primes. Thus, we have the inner contradiction based on the assumption that one of the p_i is odd, so none of the p_i are odd. Since we assumed that $b \neq 1$ in the outer contradiction and b cannot have an odd prime factor, this means $b \in \{-1, 2, -2\}$. There are issues with all three of these options: If we take $t \equiv 3 \pmod 8$ to be a sufficiently large prime, then

$$\left(\frac{-1}{t}\right) = \left(\frac{2}{t}\right) = -1,$$

and if we take $t \equiv 5 \pmod 8$ to be a sufficiently large prime, then

$$\left(\frac{-2}{t}\right) = \left(\frac{-1}{t}\right)\left(\frac{2}{t}\right) = 1 \cdot (-1) = -1.$$

These results contradict the fact that b needs to be a quadratic residue modulo all sufficiently large primes. Therefore, we have a contradiction with the assumption that $b \neq 1$, so $b = 1$. ■

The law of quadratic reciprocity, along with its two supplements, computationally resolve the problem of identifying quadratic residues modulo primes. Extending this result to composite modulo is not clean, to the best of our knowledge. By Theorem 11.2, it suffices to solve the problem in the case of prime power moduli because a is a k^{th} power residue modulo n if and only if a is a k^{th} power residue modulo each maximal prime power divisor of n; we will not analyze the prime power case. Moreover, moving on to higher power residues is difficult. There do exist results about cubic reciprocity, quartic reciprocity, and so on, but they are messier and they lie beyond the scope of our exposition. We offer the following problem as a partial result in the case of quadratic residues in composite moduli.

Problem 11.28. As an extension of the Legendre symbol, if $n \geq 2$ is an odd positive integer with prime factorization

$$n = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$$

and a is an integer, then the **Jacobi symbol** is defined as

$$\left(\frac{a}{p_1}\right)^{e_1}\left(\frac{a}{p_2}\right)^{e_2}\cdots\left(\frac{a}{p_k}\right)^{e_k}.$$

So it is a product of Legendre symbols. Note that the Jacobi symbol inherits the complete multiplicativity of the Legendre symbol, and that the former reduces to the latter if the lower entry n is a prime. Prove that:

1. If a is not coprime to n, then $\left(\frac{a}{n}\right) = 0$.

2. If a is a quadratic residue modulo n and $(a, n) = 1$, then $\left(\frac{a}{n}\right) = 1$. If $\left(\frac{a}{n}\right) = -1$, then a is a quadratic non-residue modulo n.

3. It is possible that $\left(\frac{a}{n}\right) = 1$ even though a is a quadratic non-residue modulo n. This shows the limitations of the Jacobi symbol in comparison to the Legendre symbol.

Chapter 12

Special Forms of Integers

> "... a prolonged meditation on the subject has satisfied me that the existence of any one such [odd perfect number] - its escape, so to say, from the complex web of conditions which hem it in on all sides - would be little short of a miracle."
>
> – *James Sylvester, Sur les nombres dits de Hamilton*

It's time for some fun. We have developed a strong repertoire of number theoretic knowledge, and we will employ any or all of the tools at our disposal to analyze a variety of special forms in which numbers appear. These include Fermat numbers, Mersenne numbers and perfect numbers. Finally, we will look at ways of extending Euclid's proof of the infinitude of primes to primes in certain residues classes of particular moduli.

12.1 Fermat, Mersenne, and Perfect Numbers

A part of number theory is the analysis of particular subsets of the integers. Some common questions are of the following kind:

- Given a particular mathematical expression, such as a univariate or multivariable polynomial, what integer outputs can be achieved by integer inputs? What about prime outputs?
- More generally, what integers or primes satisfy some stated property?
- If an integer has to satisfy certain criteria, such as being the output of a polynomial with integer coefficients, in what residue classes can it lie, given a particular modulus?

If a number theorist who pursues such questions is asked to justify the existence of this field of investigation, the response may simply be that these questions are inherently interesting to the human mind or that they have historical interest due to being posed in antiquity. Nonetheless, the solution to such questions can lead to applications, such as the search for very large prime numbers, which can be used in computer science. Similarly, the pursuit of such questions can lead to practical by-products in the form of lemmas such as efficient primality tests and factorization algorithms.

Definition 12.1. A **Fermat number** is an integer equal to $2^{2^n} + 1$ for some non-negative integer n. It is denoted by F_n, despite the possible confusion with Fibonacci numbers. If a Fermat number is prime, then it is called a **Fermat prime**.

Example. Fermat numbers remain mysterious because it is unknown if there are infinitely many primes (or infinitely many composites or both) among them. In fact, the only known Fermat primes are F_0, F_1, F_2, F_3, F_4, and, after that,

$$F_5 = 641 \cdot 6700417$$

is not prime. This can be seen by reducing the true equation

$$2^{32} + 1 = 641 \cdot 2^{28} - (641 - 1)^4 + 1$$

to 0 modulo 641.

Problem 12.2. Show that if m is a positive integer that is not a power of 2, then $2^m + 1$ is composite. Thus, there are no additional primes if the set of Fermat numbers is extended from the numbers of the form $2^{2^n} + 1$ for non-negative n to numbers of the form $2^m + 1$ for positive m.

Theorem 12.3 (Pépin's test)**.** The n^{th} Fermat number $F_n = 2^{2^n} + 1$ for a positive integer n is a prime if and only if

$$3^{\frac{F_n - 1}{2}} \equiv -1 \pmod{F_n}.$$

Proof. In one direction, suppose

$$3^{\frac{F_n - 1}{2}} \equiv -1 \pmod{F_n}.$$

Squaring, we get

$$3^{F_n - 1} \equiv 1 \pmod{F_n}.$$

So $(3, F_n) = 1$ and $\text{ord}_{F_n}(3) \mid F_n - 1 = 2^{2^n}$. Then $\text{ord}_{F_n}(3)$ is a power of 2 that is less than or equal to 2^{2^n}, but it can be no lower, otherwise squaring the order congruence enough times would yield

$$3^{2^{2^n - 1}} \equiv 1 \pmod{F_n},$$

which would contradict the initially assumed congruence

$$3^{2^{2^n - 1}} \equiv -1 \pmod{F_n},$$

since $F_n \neq 2$. So $\text{ord}_{F_n}(3) = 2^{2^n} = F_n - 1$ By Euler's congruence,

$$3^{\varphi(F_n)} \equiv 1 \pmod{F_n},$$

so $F_n - 1 \mid \varphi(F_n)$ which leads to $F_n - 1 \leq \varphi(F_n)$. A fact that holds by the definition of the φ function is that $\varphi(F_n) \leq F_n - 1$, so antisymmetry yields

$$\varphi(F_n) = F_n - 1,$$

which can be true only if F_n is prime.
Conversely, suppose F_n is prime. By Euler's criterion,

$$3^{\frac{F_n - 1}{2}} \equiv \left(\frac{3}{F_n}\right) \pmod{F_n}.$$

By quadratic reciprocity,

$$\left(\frac{3}{F_n}\right) = \left(\frac{F_n}{3}\right)(-1)^{\frac{3-1}{2}\cdot\frac{F_n-1}{2}} = \left(\frac{F_n}{3}\right),$$

and by Euler's criterion,

$$\left(\frac{F_n}{3}\right) \equiv F_n^{\frac{3-1}{2}} \equiv F_n \pmod 3.$$

We can then compute that

$$F_n = 2^{2^n} + 1 = (-1)^{2^n} + 1 = 1 + 1 \equiv -1 \pmod 3.$$

Since -1 is not a quadratic residue modulo 3,

$$\left(\frac{3}{F_n}\right) = \left(\frac{F_n}{3}\right) = -1,$$

so by Euler's criterion,

$$3^{\frac{F_n-1}{2}} \equiv -1 \pmod{F_n}.$$

■

Definition 12.4. A **Mersenne number** is an integer $M_n = 2^n - 1$ for some non-negative integer n. If a Mersenne number is a prime, then it is called a **Mersenne prime**.

Example. Unlike the Fermat primes, which seem to have come to a halt after F_4, Mersenne primes seem to continue without end. There are 51 known Mersenne primes at the time of writing, with the largest of them being the largest known prime overall.

Example 12.5. Let m and n be positive integers. Prove that M_m and M_n are coprime if and only if m and n are coprime.

Solution. Related to the Euclidean algorithm, we know from Example 1.25 that

$$(2^m - 1, 2^n - 1) = 2^{(m,n)} - 1.$$

This equals 1 if and only if:

$$2^{(m,n)} - 1 = 1 \iff 2^{(m,n)} = 2^1 \iff (m, n) = 1.$$

■

Problem 12.6. Let $n \geq 2$ be an integer. Show that if n is composite, then $M_n = 2^n - 1$ is composite. As a contrapositive, we get that if $M_p = 2^p - 1$ is prime, then p is prime.

Example 12.7. Prove that, if p is an odd prime and q is a prime that divides M_p, then

$$q \equiv \pm 1 \pmod 8.$$

Solution. Since $M_p = 2^p - 1$ is odd, q must be odd too. The hypothesis is that

$$2^p \equiv 1 \pmod{q}.$$

We can manipulate this into

$$\left(2^{\frac{p+1}{2}}\right)^2 \equiv 2 \pmod{p}.$$

So 2 is a quadratic residue modulo q. By the second supplement to quadratic reciprocity, $q \equiv \pm 1 \pmod 8$. ■

Problem 12.8 (Ramanujan-Nagell numbers). The Ramanujan-Nagell equation is the Diophantine equation

$$2^y - 7 = x^2.$$

Ramanujan conjectured that the only positive integer solutions for x are

$$x = 1, 3, 5, 11, 181,$$

and Nagell proved it later. Use this complete solution set to determine all Mersenne numbers that are also triangular numbers. (Triangular numbers are those that are the sum of the first n positive integers for a positive integer n. In this problem, we count 0 as triangular.)

Definition 12.9. A **perfect number** is a positive integer n such that n is the sum of its proper positive divisors (as in, excluding n itself), meaning

$$n = \sigma(n) - n.$$

Example. The first few examples of perfect numbers are

$$6, 28, 496, 8128.$$

The study of perfect numbers goes back to at least ancient Greece. Fundamental questions, such as whether there are infinitely many perfect numbers and whether there are any odd perfect numbers, remain unanswered.

Theorem 12.10 (Euclid-Euler theorem)**.** An integer n is an even perfect number if and only if there exists a Mersenne prime M_p such that $n = 2^{p-1}M_p$. Thus, the fate of the infinitude of Mersenne primes and even perfect numbers are intertwined, though neither is known.

Proof. First we prove Euclid's direction. Supposing $M_p = 2^p - 1$ is prime, we want to show that

$$2^{p-1}M_p = 2^{p-1}(2^p - 1)$$

is an even perfect number. Since 2^p is a power of 2 and $2^p - 1$ is odd, the multiplicativity of σ yields

$$\sigma(2^{p-1}M_p) = \sigma(2^{p-1}(2^p - 1)) = \sigma(2^{p-1})\sigma(2^p - 1).$$

The positive factors of $2^{p-1} - 1$ sum to

$$1 + 2 + 2^2 + \cdots + 2^{p-1} = 2^p - 1.$$

Moreover, $2^p - 1$ is a prime so its positive factors sum to $1 + (2^p - 1) = 2^p$. Then

$$\begin{aligned}\sigma(2^{p-1}M_p) &= (2^p - 1)2^p \\ \sigma(2^{p-1}M_p) - 2^{p-1}M_p &= (2^p - 1)2^p - 2^{p-1}(2^p - 1) \\ &= (2^p - 1)(2^p - 2^{p-1}) \\ &= 2^{p-1}M_p.\end{aligned}$$

Therefore, $2^{p-1}M_p$ is a perfect number. If $p = 0$ or $p = 1$, then $M_0 = 0$ and $M_1 = 1$ are not primes, so $p \geq 2$ which makes $2^{p-1}M_p$ even.
In Euler's direction, suppose $n = 2^k m$ is an even perfect number, where m is odd and $k \geq 1$. Since n is perfect, the multiplicativity of σ yields

$$\begin{aligned}2^k m = n &= \sigma(n) - n = \sigma(2^k m) - 2^k m \\ &= \sigma(2^k)\sigma(m) - 2^k m = (2^{k+1} - 1)\sigma(m) - 2^k m.\end{aligned}$$

Rearranging, we get

$$(2^{k+1} - 1)\sigma(m) = 2^{k+1}m.$$

Since 2^{k+1} and $2^{k+1} - 1$ are consecutive integers and so are coprime, $2^{k+1} - 1$ divides m. So we can write

$$\sigma(m) = 2^{k+1} \cdot \frac{m}{2^{k+1} - 1}.$$

Two divisors of m are m and $\dfrac{m}{2^{k+1} - 1}$. If they were equal, then we would have $k = 0$, which contradicts the evenness of n, so these two are distinct divisors of m. The highly interesting point is that their sum is

$$m + \frac{m}{2^{k+1} - 1} = 2^{k+1} \cdot \frac{m}{2^{k+1} - 1} = \sigma(m),$$

so there are no positive divisors of m but these two. This proves that m is prime. It is not possible that $m = 1$, otherwise it cannot have a divisor of $2^{k+1} - 1 \geq 2^{1+1} - 1 = 3$. So it must be true that $\dfrac{m}{2^{k+1} - 1} = 1$, which proves that $m = 2^{k+1} - 1$ is a Mersenne number. Thus, m is a Mersenne prime. ■

As a historical note, Euclid and Euler each proved a different direction of this theorem, approximately 2000 years apart! It is a more dramatic example of the case of Steiner proving the converse of Pitot's theorem in geometry slightly over 120 years after Pitot proved his direction.

Example 12.11. Find all positive integers n such that

$$\varphi(\sigma(2^n)) = 2^n.$$

Solution. As in the proof of the Euler-Euclid theorem (Theorem 12.10), first we compute

$$\sigma(2^n) = 1 + 2 + 2^2 + \cdots + 2^n = 2^{n+1} - 1.$$

So we want to solve

$$\varphi(2^{n+1}-1) = 2^n$$

for positive integers n. Suppose n is such a solution. We proved in Example 9.6 that a property of the φ function is that $m \mid \varphi(a^m - 1)$, so $n+1$ divides $\varphi(2^{n+1}-1) = 2^n$. Then $n+1$ is a power of 2, meaning there exists a non-negative integer k such that $n = 2^k - 1$ and we want to solve

$$\varphi(2^{2^k} - 1) = 2^{2^k - 1}.$$

Trying $k = 0$ shows that it satisfies the equation, so we may now assume that $k \geq 1$. The product

$$(2^{2^0}+1)(2^{2^1}+1)(2^{2^2}+1)\cdots(2^{2^{k-1}}+1)$$

may be evaluated as $2^{2^k} - 1$ by multiplying the product by $2^{2^0} - 1 = 1$ and successively using difference of squares; this is a product version of telescoping. To use the multiplicativity of φ on this product, we will have to prove that any pair of distinct Fermat numbers are coprime. Fermat numbers are odd, so suppose p is an odd prime that divides both $2^{2^i}+1$ and $2^{2^j}+1$ where $i < j$. Then

$$\begin{aligned} 2^{2^i} &\equiv -1 \pmod{p}, \\ 2^{2^j} &\equiv -1 \pmod{p}. \end{aligned}$$

However, raising the first congruence to the exponent 2^{j-i} yields

$$2^{2^j} \equiv \left(2^{2^i}\right)^{2^{j-i}} \equiv (-1)^{2^{j-i}} \equiv 1,$$

which contradicts the second congruence since $p \neq 2$. This proves that each pair of distinct Fermat numbers are coprime. Then we can invoke the multiplicativity of φ to get

$$\begin{aligned} \varphi(2^{2^k}-1) = \varphi\left(\prod_{i=0}^{k-1}(2^{2^i}+1)\right) &= \prod_{i=0}^{k-1}\varphi(2^{2^i}+1) \\ &\leq \prod_{i=0}^{k-1} 2^{2^i} = 2^{\sum_{i=0}^{k-1} 2^i} = 2^{2^k-1}. \end{aligned}$$

This is almost what we wanted to see, but it is an inequality instead of an equation. Equality holds if and only if $\varphi(2^{2^i}+1) = 2^{2^i}$ for $i = 0, 1, 2, \ldots, k-1$. This is equivalent to each of these $2^{2^i}+1$ being prime, and in fact a Fermat prime. The known Fermat primes are F_0, F_1, F_2, F_3, F_4 and it is known that F_5 is not a prime. So the possible k are $k = 0, 1, 2, 3, 4, 5$ which leads to the solutions

$$n = 2^k - 1 = 0, 1, 3, 7, 15, 31.$$

We have found all of the solutions and none of them are extraneous because the equality condition for the inequality that we used is biconditional. ■

12.2 Primes in Special Forms

A general problem in number theory is to determine the nature of the set of primes of a certain form. This can involve determining whether there are infinitely many primes in the set, finding how they are distributed, or even classifying all of them. The following is among the most famous of such results.

Theorem 12.12 (Dirichlet's theorem on primes in arithmetic progressions)**.** If a and d are coprime positive integers, then there are infinitely many primes in the arithmetic sequence $(a + (n-1)d)_{n=1}^{\infty}$.

A general proof of Dirichlet's theorem is difficult, but we will prove some special cases shortly as the topic of this section. Dirichlet's theorem is the simplest, that is linear, case of the following conjecture.

Conjecture 12.13 (Bunyakovsky conjecture)**.** We notice that, in order for a univariate polynomial $f \in \mathbb{Z}[x]$ to have infinitely many prime outputs $f(n)$ for positive integers n, it is necessary that:

- The leading coefficient of f is positive.
- f cannot be factored into gh for any non-integer $g, h \in \mathbb{Z}[x]$, meaning f is irreducible over $\mathbb{Z}$.
- There is no prime that divides all elements of the sequence of integers $(f(n))_{n=1}^{\infty}$.

Bunyakovsky conjectured that these criteria are also sufficient for f to take on infinitely many prime outputs for positive integer inputs.

No degree of the Bunyakovsky conjecture has been proven, except for the linear case by Dirichlet. Proofs for even particular polynomials can be difficult. The following are some available results in the multivariable variation.

- The Friedlander-Iwaniec theorem from 1997 uses methods from sieve theory to prove that there are infinitely many primes of the form $a^2 + b^4$ for positive integers a and b.
- A similar theorem of Heath-Brown asserts the existence of infinitely many primes of the form $a^3 + 2b^3$ for positive integers a and b.

Such results are generally uncommon. In a recent book [9], Andrew Granville has summarized historically important and recent advances, like those of Maynard, pertaining to the research program "One can ask for prime values of polynomials in two or more variables." The univariate cases are especially tenacious, since all multivariable cases follow from the univariate cases. Even the simplest quadratic case, Landau's fourth problem, which is stated below, remains unsolved.

Conjecture 12.14 (Landau's fourth problem)**.** Are there infinitely many primes of the form $n^2 + 1$ for positive integers n?

A use of quadratic reciprocity is in the so-called inverse problem: Given an integer a, determine all odd primes p such that $\left(\frac{a}{p}\right) = 1$. We have already seen examples in the first (Corollary 11.19) and second (Corollary 11.22) supplements to quadratic reciprocity, where $a = -1$ and $a = 2$, respectively. Let us approach this problem now as it will help us with Dirichet's theorem.

Theorem 12.15 (Inverse quadratic reciprocity)**.** Let q and p be distinct odd primes.

1. If $q \equiv 1 \pmod 4$, then $\left(\frac{q}{p}\right) = 1$ if and only if $\left(\frac{p}{q}\right) = 1$.
2. If $q \equiv 3 \pmod 4$, then $\left(\frac{q}{p}\right) = 1$ if and only if there exists an odd integer a such that $q \nmid a$ and
$$\begin{aligned} p &\equiv a^2 \pmod{4q}, \text{ or} \\ p &\equiv -a^2 \pmod{4q}. \end{aligned}$$

Proof. This proof involves a fair amount of casework, but everything coalesces into a cohesive result in the end.

1. The first case $q \equiv 1 \pmod 4$ is easy because, by quadratic reciprocity,
$$\left(\frac{q}{p}\right) = (-1)^{\frac{q-1}{2}\cdot\frac{p-1}{2}} \cdot \left(\frac{p}{q}\right) = \left(\frac{p}{q}\right),$$
since $\dfrac{q-1}{2}$ is even if and only if $q \equiv 1 \pmod 4$.
2. So now we can focus on the second and more complicated case. Suppose $q \equiv 3 \pmod 4$. By quadratic reciprocity,
$$\left(\frac{q}{p}\right) = (-1)^{\frac{q-1}{2}\cdot\frac{p-1}{2}} \cdot \left(\frac{p}{q}\right) = (-1)^{\frac{p-1}{2}}\left(\frac{p}{q}\right),$$
since $\dfrac{q-1}{2}$ is odd if $q \equiv 3 \pmod 4$. In one direction, suppose $p \equiv \pm a^2 \pmod{4p}$ for some odd integer a such that $q \nmid a$. We will do casework on the choice of the sign $\pm$.
   - If the $+$ sign holds, then $p \equiv a^2 \equiv 1 \pmod 4$ because a is odd. By quadratic reciprocity,
   $$\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}}\left(\frac{p}{q}\right) = \left(\frac{a^2}{q}\right) = \left(\frac{1}{q}\right) = 1.$$
   - If the -1 sign holds, then $p \equiv -a^2 \equiv -1 \equiv 3 \pmod 4$, again because a is odd. By quadratic reciprocity and its first supplement,
   $$\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}}\left(\frac{p}{q}\right) = (-1)\left(\frac{-a^2}{q}\right) = -\left(\frac{-1}{q}\right) = (-1)^{\frac{p+1}{2}} = 1.$$

In the other direction, suppose $\left(\frac{q}{p}\right) = 1$. Based on the fact that $1 = \left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}}\left(\frac{p}{q}\right)$ in this case, we can perform signs analysis to get two cases.

- Suppose $(-1)^{\frac{p-1}{2}} = 1$ and $\left(\frac{p}{q}\right) = 1$. Then $p \equiv 1 \pmod 4$ and there exists an integer a such that
$$p \equiv a^2 \pmod q.$$
We may assume without loss of generality that a is odd, because if it is not, we may replace a with the odd integer $a + q$ without issue. Then
$$p \equiv 1 \equiv a^2 \pmod 4$$
because a is odd. Combined with the other congruence, we get the desired congruence
$$p \equiv a^2 \pmod{4q}.$$
- Suppose $(-1)^{\frac{p-1}{2}} = -1$ and $\left(\frac{p}{q}\right) = -1$. Then $p \equiv 3 \pmod 4$, and by Problem 11.18, there exists an integer a such that
$$p \equiv -a^2 \pmod q.$$
We may assume without loss of generality that a is odd because otherwise we may again replace a with the odd integer $a + q$ without issue. Then
$$p \equiv -1 \equiv -a^2 \pmod 4$$
again because a is odd. Combined with the first congruence, we get the desired congruence
$$p \equiv -a^2 \pmod{4q}.$$

In either case, the constructed a satisfies $(a, q) = 1$ because $(p, q) = 1$, so $q \nmid a$.

■

So it turns out that, given a fixed odd prime q, the odd primes p, for which $\left(\frac{q}{p}\right) = 1$, lie in neat congruence classes. We leave it to the reader to think about how this, in combination with the complete multiplicativity of the Legendre symbol (in the upper entry) and the two supplements to quadratic reciprocity and sign analysis, solves the inverse problem for all integers a and not just primes q.

Example 12.16. Determine all odd primes p such that 3 is a quadratic residue modulo p. Repeat the question with 3 replaced b 5.

Solution. We will be using Theorem 12.15. For the first example, since $3 \equiv 3 \pmod 4$, $\left(\frac{3}{p}\right) = 1$ if and only if $p \equiv \pm a^2 \pmod{12}$ where a is odd and $3 \nmid a$. The possibilities for a are $1, 5, 7, 11$, the squares of all of which are 1 modulo 12. So the biconditional criterion for odd primes p satisfying $\left(\frac{3}{p}\right) = 1$ is that $p \equiv \pm 1 \pmod{12}$.

For the second example, since $5 \equiv 1 \pmod 4$, $\left(\frac{5}{p}\right) = 1$ if and only if $\left(\frac{p}{5}\right) = 1$. The squares of $1, 2, 3, 4$ are all among ± 1 modulo 5, so the biconditional criterion for odd primes p satisfying $\left(\frac{5}{p}\right) = 1$ is that $p \equiv \pm 1 \pmod 5$. ■

Lemma 12.17. Let p be an odd prime. Some cases of the inverse quadratic reciprocity problem that will be useful to us are:

1. For a fixed integer a, $\left(\frac{-a^2}{p}\right) = 1$ if and only if $p \equiv 1 \pmod 4$.
2. $\left(\frac{-2}{p}\right) = 1$ if and only if $p \equiv 1, 3 \pmod 8$
3. For any odd prime q,
$$\left(\frac{-q}{p}\right) = (-1)^{\frac{p-1}{2} \cdot \frac{q+1}{2}} \cdot \left(\frac{p}{q}\right).$$
As a consequence, $\left(\frac{-3}{p}\right) = 1$ if and only if $p \equiv 1 \pmod 6$

Proof. Most of these problems are not merely direct applications of Theorem 12.15, which is why we have placed them here separately.

1. It follows from the complete multiplicativity of the Legendre symbol that
$$\left(\frac{-a^2}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{a^2}{p}\right) = \left(\frac{-1}{p}\right) \cdot 1 = \left(\frac{-1}{p}\right).$$
The rest follows from the first supplement to quadratic reciprocity.
2. As we derived in the solution to Problem 11.23,
$$\begin{aligned}\left(\frac{-2}{p}\right) &= \left(\frac{-1}{p}\right)\left(\frac{2}{p}\right) \\ &= (-1)^{\frac{p-1}{2}} \cdot (-1)^{\frac{p^2-1}{8}} \\ &= (-1)^{\frac{(p-1)(p+5)}{8}}.\end{aligned}$$

We want to know when $\dfrac{(p-1)(p+5)}{8}$ is even, which is the same as asking for $16 = 2^4$ to divide $(p-1)(p+5)$. By the faux-Euclidean algorithm,

$$\nu_2((p-1, p+5)) = \nu_2((p-1, 6)) = 1 + \nu_2\left(\left(\frac{p-1}{2}, 3\right)\right) = 1,$$

so one of the two even numbers $p-1$ and $p+5$ is divisible by 2 only once. This means 16 divides $(p-1)(p+5)$ if and only if 8 divides $p-1$ or $p+5$. Thus, the biconditional criterion is that $p \equiv 1 \pmod 8$ or $p \equiv -5 \equiv 3 \pmod 8$.)

3. By quadratic reciprocity and its first supplement,

$$\begin{aligned}\left(\frac{-q}{p}\right) &= \left(\frac{-1}{p}\right)\left(\frac{q}{p}\right) \\ &= (-1)^{\frac{p-1}{2}} \cdot (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}\left(\frac{p}{q}\right) \\ &= (-1)^{\frac{p-1}{2}\cdot\frac{q+1}{2}}\left(\frac{p}{q}\right).\end{aligned}$$

As a consequence,

$$\left(\frac{-3}{p}\right) = (-1)^{\frac{p-1}{2}\cdot\frac{3+1}{2}}\left(\frac{p}{3}\right) = \left(\frac{p}{3}\right).$$

The only non-zero square modulo 3 is $1^2 \equiv 2^2 \equiv 1 \pmod 3$, so

$$\left(\frac{-3}{p}\right) = 1 \iff \left(\frac{p}{3}\right) = 1 \iff p \equiv 1 \pmod 3.$$

The last condition is equivalent to it being true that $p \equiv 1 \pmod 6$ or $p \equiv 4 \pmod 6$. The latter is impossible because it would cause p be to even. Thus, $p \equiv 1 \pmod 6$.

■

Modulo 2, the only remainders are 0 and 1. We already know that the only prime in the former residue class is 2 (Lemma 2.3), and Euclid tells us that there are infinitely many primes in the latter residue class. Let us see what we can achieve with regards to proving special cases of Dirichlet's result via Euclid's method.

Theorem 12.18. In an reformulation of Euclid's proof, we can show that there are infinitely many primes $p \equiv 1 \pmod 2$ as follows. The technique is to assume that there are finitely many odd primes $p_1, p_2, \ldots, p_m$, and insert the constant $N = 2p_1p_2 \cdots p_m$ into the polynomial $f(x) = x + 1$. Then any prime that divides $f(N)$ is not in the list, but there must be such an odd prime, which contradicts the assumed finite nature of the odd primes. This proof can be extended to some more congruence classes as listed in the following table, though the complete list of such proofs is infinite.

Congruence class	Polynomial $f(x)$	Constant N
$p \equiv 1 \pmod 2$	$x+1$	$2p_1p_2\cdots p_m$
$p \equiv 1 \pmod 4$	x^2+1	$2p_1p_2\cdots p_m$
$p \equiv 3 \pmod 4$	$4x-1$	$p_1p_2\cdots p_m$
$p \equiv 1 \pmod 6$	$3x^2+1$	$2p_1p_2\cdots p_m$
$p \equiv 5 \pmod 6$	$6x-1$	$p_1p_2\cdots p_m$
$p \equiv 1 \pmod 8$	x^4+1	$2p_1p_2\cdots p_m$
$p \equiv 3 \pmod 8$	x^2+2	$p_1p_2\cdots p_m$
$p \equiv 5 \pmod 8$	x^2+4	$p_1p_2\cdots p_m$
$p \equiv 7 \pmod 8$	x^2-2	$p_1p_2\cdots p_m$

Moreover, these are the only residue classes into each of which infinitely many primes can fall modulo $2, 4, 6, 8$. The choice of whether to include 2 as a factor of N is a matter of what we need to do to make $f(N)$ odd so that we can claim that all of the prime factors of $f(N)$ are odd.

Proof. We will prove these results in a sequence of separate theorems, but they are organized here for the reader's convenience. What we will do here is show that the converse of Dirichlet's theorem holds, in order to established the completeness of the results for the listed moduli: If there are infinitely many primes p that fall into the residue class of an integer a modulo $n \geq 2$, then $(a, n) = 1$. Moreover, all such primes p satisfy $p \nmid n$.
Let $n \geq 2$ be an integer and a be an integer. Suppose there are infinitely many primes p such that $p \equiv a \pmod n$. By Bézout's lemma, $(a, n) \mid p$. So $(a, n) = 1$ or $(a, n) = p$. It is time for casework.

- If $(a, n) = 1$, then we are halfway done. For the second part, if it happens to be the case that $p \mid n$, then the congruence $p \equiv a \pmod n$ would imply that $p \mid a$, which would cause the contradiction that

$$(a, n) \geq p > 1.$$

- If $(a, n) = p$, then $p \mid n$. Moreover, any prime q such that $q \equiv a \pmod n$ would be divisible by p, which contradicts the primality of q, unless $q = p$. So there can be at most one prime in the congruence class of a modulo n, which contradicts the assumption of infinitely many primes in this congruence class. This whole case is bogus.

This establishes the converse of Dirichlet's theorem and the fact that the residues listed in the above table are the only ones in their respective moduli whose congruence classes can contain infinitely many primes. Proving Dirichlet's theorem itself is much harder. ■

Theorem 12.19. There are infinitely many primes $p \equiv 1 \pmod 4$, and there are infinitely many primes $p \equiv 1 \pmod 6$.

Proof. These two instances of Dirichlet's theorem have been placed together because both proofs rely on the fact that all primes that divide a certain form must fall into one specific residue class.

1. Suppose, for contradiction, that there exist just finitely many primes $p \equiv 1 \pmod 4$, and let them be $p_1, p_2, \ldots, p_m$. Let

$$\begin{aligned} N &= 2p_1p_2\cdots p_m \\ f(x) &= x^2 + 1 \\ M &= f(N) = (2p_1p_2\cdots p_m)^2 + 1. \end{aligned}$$

   Let q be a prime that divides $M \geq 2^2 - 1 = 3$. Since M is odd, so is q. Since

$$(2p_1p_2\cdots p_m)^2 \equiv -1 \pmod q,$$

   the first supplement to quadratic reciprocity gives that

$$\left(\frac{-1}{q}\right) = 1 \implies q \equiv 1 \pmod 4.$$

   This is a contradiction because the prime q cannot equal any of the p_i, otherwise we would have $q \mid 1$. So q is contradicts the finite nature of the list of p_i, and there must exist infinitely many primes $p \equiv 1 \pmod 4$.

2. If a prime q divides $f(N) = 3N^2 + 1$ for some positive integer N, then N^{-1} exists because $q \nmid N$ and

$$(N^{-1})^2 \equiv -3 \pmod q.$$

   If N is even, then $f(N)$ and q are odd. By Lemma 12.17,

$$\left(\frac{-3}{q}\right) = 1 \implies q \equiv 1 \pmod 6.$$

   Suppose, for contradiction, that there exist just finitely many primes $p \equiv 1 \pmod 6$, and let them be $p_1, p_2, \ldots, p_m$. Let

$$\begin{aligned} N &= 2p_1p_2\cdots p_m \\ f(x) &= 3x^2 + 1 \\ M &= f(N) = 3(2p_1p_2\cdots p_m)^2 + 1. \end{aligned}$$

   Let q be a prime that divides $M \geq 3\cdot 2^2 + 1 = 13$. Since N is even, our earlier observation implies that $q \equiv 1 \pmod 6$. But q cannot be equal to any of the p_i, otherwise, it will be the case that $q \mid 1$. Thus, we have a found a new prime q that is congruent to 1 (mod 6) that was not on our original list, which is a contradiction.

■

Theorem 12.20. There exist infinitely many primes $p \equiv 3 \pmod 4$, and there are infinitely many primes $p \equiv 5 \pmod 6$.

Proof. These two results have been grouped together because they rely on a similar property in both cases: all odd primes are congruent to $\pm 1 \pmod 4$ and all odd primes (other than 3) are congruent to $\pm 1 \pmod 6$.

1. Suppose, for contradiction, that there exist only finitely many primes $p \equiv 3 \pmod 4$, and let them be $p_1, p_2, \ldots, p_m$. Let

$$\begin{aligned} N &= p_1 p_2 \cdots p_m \\ f(x) &= 4x - 1 \\ M &= f(N) = 4p_1 p_2 \cdots p_m - 1. \end{aligned}$$

   Let q be a prime that divides $M \geq 4 - 1 = 3$. Since M is odd, so is q. Then $q \equiv 1 \pmod 4$ or $q \equiv -1 \pmod 4$. Note that q cannot equal any of the p_i, otherwise we would have $q \mid -1$. Since the p_i supposedly exhaust all primes congruent to $3 \pmod 4$, all prime factors q of M must be congruent to $1 \pmod 4$. But then their product M would satisfy $M \equiv 1 \pmod 4$, whereas we know that

$$M = 4N - 1 \equiv 3 \pmod 4.$$

   This is a contradiction and there must exist infinitely many primes $p \equiv 3 \pmod 4$.

2. This proof is essentially a repeat of the previous one, except with 4 replaced by 6 and $f(x) = 4x - 1$ replaced by $f(x) = 6x - 1$. The only extra observation that we have to make is that an odd prime q that divides

$$M = 6p_1 p_2 \cdots p_m - 1$$

   cannot be 3, so $q \equiv \pm 1 \pmod 6$. We recommend that the reader write up the details.

■

Theorem 12.21. There exist infinitely many primes p such that $p \equiv 1 \pmod 8$.

Proof. Let $f(x) = x^4 + 1$. Suppose, for contradiction, that there are only finitely many primes $p_1, p_2 \ldots, p_m$ such that $p_i \equiv 1 \pmod 8$. Let $N = 2p_1 p_2 \cdots p_m$. Then

$$f(N) = N^4 + 1 = (2p_1 p_2 \cdots p_m)^4 + 1 \geq 2^4 + 1 = 17 > 2$$

is odd, so it has an odd prime factor q. Since q is not 2 and is not from among the p_i, we will aim to get a contradiction by showing that $q \equiv 1 \pmod 8$. Since $q \mid f(N)$,

$$N^4 \equiv -1 \pmod q \implies N^8 \equiv (-1)^2 \equiv 1 \pmod q.$$

So $\operatorname{ord}_q(N) \in \{1, 2, 4, 8\}$, but $\operatorname{ord}_p(N)$ can also be no lower than 8 because then squaring the order congruence a few times would yield $N^4 \equiv 1 \pmod q$, which is a contradiction, since $q \neq 2$. Thus, $\operatorname{ord}_q(N) = 8$. Since $q \nmid N$ (otherwise we end up with $q \mid 1$), Fermat's little theorem gives

$$N^{q-1} \equiv 1 \pmod q,$$

so $\operatorname{ord}_q(N) \mid q - 1$. Therefore, $q \equiv 1 \pmod 8$, as desired. ■

Problem 12.22. For each fixed positive integer n, prove that there exist infinitely many primes p such that $p \equiv 1 \pmod{2^n}$. Our recommendation is to study the proof of Theorem 12.21 and generalize it.

Theorem 12.23. There are infinitely many primes p of each of the following kinds:

1. $p \equiv 3 \pmod 8$
2. $p \equiv 5 \pmod 8$
3. $p \equiv 7 \pmod 8$

Proof. The proofs are standard Euclidean ones, reminiscent of the proof of Theorem 12.19. The difference is the reason for why they have been grouped together here: certain chosen forms in each case will be divisible by primes from two residue classes rather than just one. We start by showing the polynomials and making some useful observations related to the inverse problem of quadratic reciprocity.

1. If a prime q divides $f(N) = N^2 + 2$, then
$$N^2 \equiv -2 \pmod q.$$
If N is odd, then so is q and by Lemma 12.17,
$$\left(\frac{-2}{q}\right) = 1 \implies q \equiv 1, 3 \pmod 8.$$

2. If a prime q divides $f(N) = N^2 + 4$, then
$$N^2 \equiv -4 \pmod q.$$
If N is odd, then so is q and by Lemma 12.17,
$$\left(\frac{-2^2}{q}\right) = 1 \implies q \equiv 1 \pmod 4 \implies q \equiv 1, 5 \pmod 8.$$

3. If a prime q divides $f(N) = N^2 - 2$, then
$$N^2 \equiv 2 \pmod q.$$
If N is odd, then so is q and by the second supplement to quadratic reciprocity (Corollary 11.22),
$$\left(\frac{2}{q}\right) = 1 \implies q \equiv 1, 7 \pmod 8.$$

The method is to assume that there are finitely many primes of the respective type as usual, and take their product to be N. Then a contradiction can be derived if we assume that all of the prime factors of $f(N)$ are congruent to 1 (mod 8), thereby producing a new prime q that was not on the original finite list but is still a prime of their type. We leave the details to the reader. ∎

Theorem 12.24. Let p be a prime. Then there exist infinitely many primes q such that $q \equiv 1 \pmod{p}$.

Proof. Suppose, for contradiction, that there are only finitely many primes $p_1, p_2, \ldots, p_m$ that are congruent to 1 modulo p. Let

$$N = pp_1p_2 \cdots p_k,$$

which equals just p if there are no p_i. The p^{th} cyclotomic polynomial may be denoted by and defined as

$$\Phi_p(x) = 1 + x + x^2 + \cdots + x^{p-1} = \frac{x^p - 1}{x - 1}.$$

Keep in mind that this formula does not work for general cyclotomic polynomials, but it suffices for our case since p is prime.
Let q be a prime factor of $\Phi_p(N)$, which exists since

$$\Phi_p(N) \geq 1 + p \geq 1 + 2 = 3.$$

We plan to show that $q \equiv 1 \pmod{p}$, and that q is not p and is not from among the p_i. The second part is easy:

$$\begin{aligned} \Phi_p(N) &\equiv 0 \pmod{q}, \\ \Phi_p(N) &\equiv 1 \pmod{p \text{ or } p_i}, \end{aligned}$$

so q is distinct from p and the p_i. Moreover, $q \nmid N$ from the first congruence, so it is possible to define

$$m = \operatorname{ord}_q(N),$$

meaning m is the smallest positive integer such that $N^m \equiv 1 \pmod{q}$. Since $q \mid \Phi_p(N)$ and $\Phi_p(N) \mid N^p - 1$, transitivity of divisibility yields

$$N^p \equiv 1 \pmod{q}.$$

Since the order divides all other such exponents, $m \mid p$. As p is a prime, $m = 1$ pr $m = p$. By Fermat's little theorem,

$$N^{q-1} \equiv 1 \pmod{q},$$

so $m \mid q - 1$ as well, meaning $q \equiv 1 \pmod{m}$. Thus, the desired congruence $q \equiv 1 \pmod{q}$ is true if $m = p$.
Suppose, for contradiction, that $m = 1$ and $q \not\equiv 1 \pmod{p}$. If we can derive a contradiction, we will have proven that $m = p$ or $q \equiv 1 \pmod{p}$. The former implies the latter, so we will win either way. Let us begin. Since $m = \operatorname{ord}_q(N)$, we get

$$N \equiv N^m \equiv 1 \pmod{q},$$

so $q \mid N - 1$. With this as the base case, we will show by induction that, for any positive integer k, q^k divides $N - 1$. By infinite descent, this forces it to be true that $N = 1$, which we know to be false because $N \geq p \geq 2$. Assume the induction hypothesis for some positive

integer k, meaning that $q^k \mid N-1$. Since $q^k \mid N-1$ by assumption and $q \mid \Phi_p(N)$, additivity of the ν_q function yields that

$$(N-1)\Phi_p(N) = N^p - 1$$

is divisible by q^{k+1}. Equivalently,

$$N^p \equiv 1 \pmod{q^{k+1}}.$$

By Euler's congruence,

$$N^{\varphi(q^{k+1})} = N^{q^k(q-1)} \equiv 1 \pmod{q^{k+1}}.$$

Then $t = \operatorname{ord}_{q^{k+1}}(N)$ divides both p and $q^k(q-1)$. So $t = 1$ or $t = p$. If $t = p$, then from $t \mid q^k(q-1)$, we get that $p \mid q-1$, which contradicts our initial assumption that $q \not\equiv 1 \pmod{p}$. So $t = 1$, in which case we have

$$N \equiv N^t \equiv 1 \pmod{q^{k+1}}.$$

So q^{k+1} divides $N-1$, which completes the induction. Thus, $q \equiv 1 \pmod{p}$, which means our original list of primes p_i was incomplete and there must be infinitely many primes congruent to 1 modulo p.

This proof can be generalized to prove the existence of infinitely many primes $q \equiv 1 \pmod{n}$ for any integer $n \geq 2$. The general proof needs the n^{th} cyclotomic polynomial. See Theorem 13.30 ■

We have more or less reached the known extremity to which our present tools can take us for proving cases of Dirichlet's theorem. Proofs can be constructed for other residue classes in certain moduli, but they are not very different in structure from the examples that we have shown, though the polynomials might become increasingly complicated in appearance and analysis. Schur proved in 1912 that such "Euclidean proofs" exist if the square of the residue is congruent to 1 in the modulus, and the converse is also known to be true.

On the note of primes in special forms, there are also results of the following kind which state what kind of primes, or more generally integers, satisfy a particular form:

- Fermat's two-square theorem: An odd prime p is the sum of the squares of two integers $x^2 + y^2$ if and only if $p \equiv 1 \pmod{4}$. More generally, an integer $n \geq 2$ is of this form if and only if the multiplicity of each prime factor that is congruent to 3 (mod 4) is even in the prime factorization of the integer.

- Legendre's three-square theorem: A positive integer is the sum of the squares of three integers $x^2 + y^2 + z^2$ if and only if it is *not* of the form $4^a(8b+7)$ for non-negative integers a and b.

- Lagrange's four-square theorem: Every positive integer can be written as the sum of the squares of four integers $x^2 + y^2 + z^2 + w^2$. This is the smallest case of Waring's problem, which asks whether, for each integer $k \geq 2$, there exists a positive integer m such that every positive integer can be expressed as the sum of k^{th} powers of at most m positive integers. Hilbert non-constructively proved the existence of m for all integers $k \geq 2$.

These are all theorems whose proofs are involved and idiosyncratic, so we will not touch on them. The enterprising reader is encouraged to look at proofs elsewhere.

Chapter 13

Difference and Sum of Powers

> "Mathematics is an experimental science, and definitions do not come first, but later on. They make themselves, when the nature of the subject has developed itself."
>
> – *Oliver Heaviside, On operations in physical mathematics II*

> "The key issue for me is finding the right definitions, finding the right notions that really capture the essence of some mathematical phenomenon. I often have some vague vision of what I want to understand, but I'm often missing the words to really say that... suddenly it clicks, and suddenly I can say what I always wanted to say."
>
> – *Peter Scholze, ICM 2018*

We end the volume with some heavy machinery pertaining to the intersection of polynomials and number theory. The "lifting the exponent lemma" and Zsigmondy's theorem are two sledgehammers in problem-solving that address divisibility properties of expressions of the form $x^n \pm y^n$. We will prove the LTE lemma, then develop the theory of cyclotomic polynomials and cyclotomic values, and finally use it all to prove Zsigmondy's theorem.

13.1 Lifting the Exponent

The LTE lemma answers the question of how $\nu_p(a^n \pm b^n)$ can be evaluated largely in terms of $\nu_p(a \pm b)$, among other minor terms, given that p is a prime. The word "lifting" comes from the fact that the exponents n are lifted or removed from the expression $a^n \pm b^n$ to allow us to instead work with $a \pm b$.
The following result will be our workhorse for proving the LTE lemma.

Lemma 13.1. Let p be an odd prime (we will point out where the proof fails for $p = 2$) and $a, b \in \mathbb{Z}$ such that $p \nmid a$ and $p \nmid b$. If $p \mid a - b$, then

$$\nu_p(a^p - b^p) = \nu_p(a - b) + 1.$$

Consequently, but separately, if $p \mid a + b$, then

$$\nu_p(a^p + b^p) = \nu_p(a + b) + 1.$$

Proof. The difference of powers factorization tells us that

$$a^p - b^p = (a - b)(a^{p-1} + a^{p-2}b + \cdots + ab^{p-2} + b^{p-1}).$$

Let the second factor on the right side be denoted by $f(a,b)$ so that

$$a^p - b^p = (a-b)\cdot f(a,b).$$

Then

$$\nu_p(a^p - b^p) = \nu_p(a-b) + \nu_p(f(a,b)).$$

To prove that $\nu_p(a^p - b^p) = \nu_p(a-b)+1$, it suffices to prove that $p \mid f(a,b)$ but $p^2 \nmid f(a,b)$. The first is easy because, by $a \equiv b \pmod p$,

$$f(a,b) \equiv a^{p-1} + a^{p-2}a + \cdots + aa^{p-2} + a^{p-1} \equiv pa^{p-1} \equiv 0 \pmod p.$$

For the second part, since $p \mid a-b$, let $k \in \mathbb{Z}$ be such that $b = a + kp$. Upon substitution and expansion, we find that

$$\begin{aligned} f(a,b) &= \sum_{t=0}^{p-1} a^{p-1-t}b^t = \sum_{t=0}^{p-1} a^{p-1-t}(a+kp)^t \\ &= \sum_{t=0}^{p-1}\left[a^{p-1-t}\sum_{j=0}^{t}\binom{t}{j}a^{t-j}(kp)^j\right]. \end{aligned}$$

Due to the $(kp)^j$ factor, only the $j=0$ and $j=1$ terms of each inner sum avoid annihilation modulo p^2. Modulo p^2, we are left with

$$\begin{aligned} \sum_{t=0}^{p-1}\left[a^{p-1-t}\cdot(a^t + ta^{t-1}(kp))\right] &= \sum_{t=0}^{p-1}(a^{p-1} + tkpa^{p-2}) \\ &= pa^{p-1} + kpa^{p-2}\cdot\sum_{t=0}^{p-1} t \\ &= pa^{p-1} + kpa^{p-2}\cdot\frac{(p-1)p}{2} \\ &= pa^{p-1} + p^2\cdot ka^{p-2}\cdot\frac{p-1}{2}, \end{aligned}$$

where $\dfrac{p-1}{2}$ is an integer since p is an odd prime (this is precisely where the proof fails for $p=2$). Reducing modulo p^2, we get

$$f(a,b) \equiv pa^{p-1} \not\equiv 0 \pmod{p^2}$$

because $p \nmid a$.

For the second result, assuming $p \mid a+b$, we let $c = -b$ and use the first part to get

$$\begin{aligned} \nu_p(a^p + b^p) &= \nu_p(a^p - (-b)^p) \\ &= \nu_p(a^p - c^p) \\ &= \nu_p(a-c) + 1 \\ &= \nu_p(a+b) + 1. \end{aligned}$$

The manipulation $a^p + b^p = a^p - (-b)^p$ was possible because p is odd. ■

Theorem 13.2 (Lifting the exponent lemma (LTE))**.** Let $a, b \in \mathbb{Z}$, $n \in \mathbb{Z}_+$, and p be a prime such that $p \nmid a$ and $p \nmid b$. Then:

1. For all primes p, including $p = 2$:

   (a) If $p \nmid n$ and $p \mid a - b$, then

   $$\nu_p(a^n - b^n) = \nu_p(a - b).$$

   (b) If $p \nmid n$ and $p \mid a + b$ and n is odd, then

   $$\nu_p(a^n + b^n) = \nu_p(a + b).$$

2. For all odd primes p:

   (a) If $p \mid a - b$, then

   $$\nu_p(a^n - b^n) = \nu_p(a - b) + \nu_p(n).$$

   (b) If $p \mid a + b$ and n is odd, then

   $$\nu_p(a^n + b^n) = \nu_p(a + b) + \nu_p(n).$$

3. For $p = 2$:

   (a) If $2 \nmid n$ and $2 \mid a - b$, then

   $$\nu_2(a^n - b^n) = \nu_p(a - b).$$

   This is the $p = 2$ case of 1(a).

   (b) If $2 \mid n$ and $2 \mid a - b$, then

   $$\begin{aligned} \nu_2(a^n - b^n) &= \nu_2(a - b) + \nu_2(a + b) + \nu_2(n) - 1 \\ &= \nu_2(a^2 - b^2) + \nu_2\left(\frac{n}{2}\right). \end{aligned}$$

   (c) Regardless of the parity of n, if $4 \mid a - b$, then

   $$\nu_2(a^n - b^n) = \nu_2(a - b) + \nu_2(n).$$

   This can be split into the $2 \nmid n$ and $2 \mid n$ cases, and respectively proven as special cases of 3(a) and 3(b).

Proof. We will prove this list of results in the stated sequence:

1. Let p be any prime.

(a) Suppose $p \nmid n$ and $p \mid a-b$. Since

$$a^n - b^n = (a-b)(a^{n-1} + a^{n-2}b + \cdots + ab^{n-2} + b^{n-1}),$$

in order to prove

$$\nu_p(a^n - b^n) = \nu_p(a-b),$$

it suffices to prove that

$$p \nmid a^{n-1} + a^{n-2}b + \cdots + ab^{n-2} + b^{n-1}.$$

Indeed, using the fact that $a \equiv b \pmod{p}$, we get

$$\begin{aligned} &a^{n-1} + a^{n-2}b + \cdots + ab^{n-2} + b^{n-1} \\ &\equiv a^{n-1} + a^{n-2}a + \cdots + aa^{n-2} + a^{n-1} \\ &\equiv na^{n-1} \pmod{p}, \end{aligned}$$

which is not 0 modulo p because p divides neither n nor a.

(b) Suppose $p \nmid n$ and $p \mid a+b$ and n is odd. Let $c = -b$ so that $p \mid a-c$. By 1(a) and the fact that n is odd,

$$\begin{aligned} \nu_p(a^n + b^n) &= \nu_p(a^n - (-b)^n) \\ &= \nu_p(a^n - c^n) \\ &= \nu_p(a-c) \\ &= \nu_p(a+b). \end{aligned}$$

2. Let p be an odd prime.

(a) Suppose $p \mid a-b$. Let $n = p^t m$ for some $t \in \mathbb{Z}_{\geq 0}$ and $m \in \mathbb{Z}_+$ such that $p \nmid m$. By 1(a),

$$\nu_p(a^n - b^n) = \nu_p((a^{p^t})^m - (b^{p^t})^m) = \nu_p(a^{p^t} - b^{p^t}).$$

The muscle behind the rest of the proof is Lemma 13.1, which allows us to extract one prime factor p at a time from p^t to get

$$\begin{aligned} \nu_p(a^{p^t} - b^{p^t}) &= \nu_p((a^{p^{t-1}})^p - (b^{p^{t-1}})^p) = \nu_p(a^{p^{t-1}} - b^{p^{t-1}}) + 1 \\ &= \nu_p((a^{p^{t-2}})^p - (b^{p^{t-2}})^p) + 1 = \nu_p(a^{p^{t-2}} - b^{p^{t-2}}) + 2 \\ &\vdots \\ &= \nu_p(a-b) + t \\ &= \nu_p(a-b) + \nu_p(n). \end{aligned}$$

When 1(a) was used and each step where Lemma 13.1 was used, we needed the fact that $p \mid a^k - b^k$ for any positive integer k, which is true because $p \mid a-b$ by assumption and $a-b \mid a^k - b^k$.

(b) Suppose $p \mid a+b$ and n is odd. Let $c = -b$ so that $p \mid a-c$. By 2(a) and the fact that n is odd,

$$\begin{aligned}\nu_p(a^n + b^n) &= \nu_p(a^n - (-b)^n) \\ &= \nu_p(a^n - c^n) \\ &= \nu_p(a-c) + \nu_p(n) \\ &= \nu_p(a+b) + \nu_p(n).\end{aligned}$$

3. Let $p = 2$.

(a) Suppose $2 \nmid n$ and $2 \mid a-b$. By taking $p = 2$ in 1(a), we get

$$\nu_2(a^n - b^n) = \nu_2(a-b).$$

(b) Suppose $2 \mid n$ and $2 \mid a-b$. Let $n = 2^t m$, where $t, m \in \mathbb{Z}_+$ satisfy $2 \nmid m$. By 1(a),

$$\nu_2(a^n - b^n) = \nu_2((a^{2^t})^m - (b^{2^t})^m) = \nu_2(a^{2^t} - b^{2^t}).$$

By a decomposition via repeated usage of the difference of squares factorization (similar to the one used in Example 12.11), this is

$$\begin{aligned}\nu_2(a^{2^t} - b^{2^t}) &= \nu_2\left[(a^{2^{t-1}} + b^{2^{t-1}})(a^{2^{t-2}} + b^{2^{t-2}}) \cdots (a^{2^1} + b^{2^1})(a+b)(a-b)\right] \\ &= \nu_2(a^{2^{t-1}} + b^{2^{t-1}}) + \nu_2(a^{2^{t-2}} + b^{2^{t-2}}) + \cdots \\ &\quad + \nu_2(a^{2^1} + b^{2^1}) + \nu_2(a+b) + \nu_2(a-b).\end{aligned}$$

Since $2 \nmid a$ and $2 \nmid b$, it means a and b are both odd. Then, for every positive integer k,

$$\begin{aligned}a, b \equiv 1 \pmod 2 &\implies a, b \equiv \pm 1 \pmod 4 \\ &\implies a^2, b^2 \equiv 1 \pmod 4 \\ &\implies a^{2^k}, b^{2^k} \equiv 1 \pmod 4 \\ &\implies a^{2^k} + b^{2^k} \equiv 2 \pmod 4 \\ &\implies \nu_2(a^{2^k} + b^{2^k}) = 1.\end{aligned}$$

Therefore,

$$\begin{aligned}\nu_2(a^n - b^n) &= \nu_2(a-b) + \nu_2(a+b) + t - 1 \\ &= \nu_2(a-b) + \nu_2(a+b) + \nu_2(n) - 1 \\ &= \nu_2(a^2 - b^2) + \nu_2\left(\frac{n}{2}\right).\end{aligned}$$

Again, note that $a-b \mid a^k - b^k$ for all positive integers k. Since $2 \mid a-b$ in this case, we get $2 \mid a^k - b^k$, which we needed when we applied 1(a) at the beginning to $k = 2^t$.

(c) Suppose n has either parity and $4 \mid a-b$. We can weaken $4 \mid a-b$ to $2 \mid a-b$, which is a condition that we will need in order to apply 3(a) and 3(b). There are two cases based on parity of n:

i. Suppose $2 \nmid n$. Then we use 3(a) to get

$$\begin{aligned}\nu_2(a^n - b^n) &= \nu_2(a-b) \\ &= \nu_2(a-b) + 0 \\ &= \nu_2(a-b) + \nu_2(n).\end{aligned}$$

ii. Suppose $2 \mid n$. The fact that $4 \mid a-b$ is equivalent to saying that there exists an integer s such that $a - b = 4s$. Then

$$a + b = 4s + 2b = 2(2s + b).$$

Since b is odd, $2s + b$ is odd as well, so

$$\nu_2(a+b) = \nu_2(2(2s+b)) = 1.$$

By 3(b), we get

$$\begin{aligned}\nu_2(a^n - b^n) &= \nu_2(a-b) + \nu_2(a+b) + \nu_2(n) - 1 \\ &= \nu_2(a-b) + 1 + \nu_2(n) - 1 \\ &= \nu_2(a-b) + \nu_2(n).\end{aligned}$$

In either case ($2 \nmid n$ or $2 \mid n$), the result holds.

■

Problem 13.3. As presented in Theorem 13.2, the LTE lemma is long-winded and difficult to remember. Show that all of the cases can be derived if we take the following two cases for granted: For $a, b \in \mathbb{Z}$, $n \in \mathbb{Z}_+$, and primes p such that $p \nmid a$ and $p \nmid b$, it holds that

$$\nu_p(a^n - b^n) = \nu_p(a-b) + \nu_p(n),$$

where we assume that $p \mid a-b$ if p is odd or we assume that $4 \mid a-b$ if $p = 2$. Due to the number of cases in LTE, we recommend remembering this problem and the derivations stated in its solution, instead of the plethora of cases originally given.

Problem 13.4. Let p be an odd prime, n be a positive integer, and a, b be integers that are not divisible by p. Let

$$k = \operatorname{ord}_p(ab^{-1}) = \operatorname{ord}_p(a^{-1}b).$$

Prove that k is the least positive integer such that $p \mid a^k - b^k$. Then prove that

$$p \mid a^n - b^n \iff k \mid n.$$

Finally, prove that in either case (and therefore both),

$$\nu_p(a^n - b^n) = \nu_p(a^k - b^k) + \nu_p\left(\frac{n}{k}\right).$$

13.2 Cyclotomic Polynomials

Cyclotomic polynomials are special polynomial factors of $x^n - 1$ that zero in on having specific roots. They have surprising inherent properties, and even more surprising connections to divisibility. In this section, we will focus on studying and computing cyclotomic polynomials by themselves.

Definition 13.5. For $n \in \mathbb{Z}_+$, a complex number ζ is said to be an n^{th} **root of unity** if $\zeta^n = 1$. If ζ is an n^{th} root of unity, then the **order** of ζ is denoted and defined by

$$\text{ord}(\zeta) = \min\{k \in \mathbb{Z}_+ : \zeta^k = 1\}.$$

If $\text{ord}(\zeta) = n$, then ζ is said to be a **primitive** n^{th} root of unity.

Theorem 13.6. Let n, k be positive integers and $\zeta \in \mathbb{C}$ be a primitive n^{th} root of unity. Then

$$\begin{aligned} \zeta^k = 1 &\iff n \mid k \\ \text{ord}(\zeta^k) &= \frac{n}{\gcd(k,n)} \\ \text{ord}(\zeta^k) = n &\iff \gcd(k,n) = 1. \end{aligned}$$

Proof. We will prove the results in sequence. Assume $\zeta^k = 1$. By Euclidean division of k by n, there exists a quotient $q \in \mathbb{Z}$ and an integer remainder $0 \leq r < n$ such that

$$k = qn + r.$$

As a result,

$$\zeta^r = \zeta^{k-qn} = \zeta^k \cdot (\zeta^n)^{-q} = 1.$$

If $r > 0$, then this contradicts the minimality of n as the order of ζ. Thus, $k = qn$ or $n \mid k$. Conversely, suppose $n \mid k$. Then there exists $q \in \mathbb{Z}$ such that $k = qn$. So

$$\zeta^k = (\zeta^n)^q = 1^q = 1.$$

Now we will prove that $k \cdot \text{ord}(\zeta^k) = \text{lcm}(k, n)$, leading to

$$\text{ord}(\zeta^k) = \frac{\text{lcm}(k,n)}{k} = \frac{n}{\gcd(k,n)}.$$

Note that

$$\zeta^{k \cdot \text{ord}(\zeta^k)} = (\zeta^k)^{\cdot \text{ord}(\zeta^k)} = 1.$$

By the first part, we get

$$n \mid k \cdot \text{ord}(\zeta^k).$$

Since

$$k \mid k \cdot \text{ord}(\zeta^k)$$

as well, it means $k \cdot \text{ord}(\zeta^k)$ is a common multiple of k and n, so

$$\text{lcm}(k,n) \mid k \cdot \text{ord}(\zeta^k).$$

For the other direction of this divisibility relation, we note that

$$1 = 1^{\frac{\text{lcm}(k,n)}{n}} = (\zeta^n)^{\frac{\text{lcm}(k,n)}{n}} = \zeta^{\text{lcm}(k,n)} = (\zeta^k)^{\frac{\text{lcm}(k,n)}{k}}.$$

This means

$$\text{ord}(\zeta^k) \left| \frac{\text{lcm}(k,n)}{k} \right. \implies k \cdot \text{ord}(\zeta^k) \mid \text{lcm}(k,n).$$

We are done proving the second part by the antisymmetry of divisibility. The third part is a trivial consequence of the formula in the second part. ■

Corollary 13.7. For each $n \in \mathbb{Z}_+$, the number of primitive n^{th} roots of unity is $\varphi(n)$.

Proof. There exist exactly n distinct n^{th} roots of unity, as proven in Volume 1. Among these, we know that $\zeta = e^{\frac{2\pi i}{n}}$ "generates" all of them as

$$S = \{\zeta^k : k \in [n]\}.$$

If $\text{ord}(\zeta) < n$, then the powers of ζ would cycle over fewer than all of the n^{th} roots of unity. So ζ is a primitive n^{th} root of unity. Among the elements of S, where there are $\varphi(n)$ indices k such that $\gcd(k,n) = 1$. By Theorem 13.6, $\varphi(n)$ is the number of primitive n^{th} roots of unity. ■

Corollary 13.8. If n is a positive integer, then

$$n = \sum_{d|n} \varphi(d),$$

where the sum is taken over all positive divisors d of n.

Proof. This was proven in an ad hoc manner in Theorem 3.21. Now we will provide a more natural proof by double counting the number of roots of unity in two ways. There are, of course, exactly n distinct n^{th} roots of unity. On the other hand, let ζ be an n^{th} root of unity. By Theorem 13.6, $\zeta^n = 1$ if and only if $\text{ord}(\zeta) \mid n$. For each divisor d of n, Corollary 13.7 tells us that, since every primitive d^{th} roots of unity is an n^{th} root of unity, the number of primitive d^{th} roots of unity is $\varphi(d)$. So the total number of n^{th} roots of unity is

$$n = \sum_{d|n} \varphi(d).$$

■

Corollary 13.9. If ζ is any primitive n^{th} root of unity, then

$$S = \{\zeta^k : k \in [n]\}$$

is the set of all n^{th} roots of unity and

$$T = \{\zeta^k : k \in [n], \gcd(k,n) = 1\}$$

is the set of all primitive n^{th} roots of unity.

Proof. The listed elements of S in its given presentation must be distinct, otherwise there would exist distinct indices $j, k \in [n]$ such that

$$\zeta^k = \zeta^j \implies \zeta^{|k-j|} = 1,$$

leading to $\text{ord}(\zeta) \leq |k-j| < n$. There exist precisely n distinct n^{th} roots of unity; since S has n distinct elements and raising each to the exponent n yields 1, S is precisely the set of all n^{th} roots of unity.
Similarly, the elements of T must be distinct. By Theorem 13.6, if $\gcd(k, n) = 1$, then $\text{ord}(\zeta^k) = n$. According to Corollary 13.7, the number of primitive n^{th} roots of unity is $\varphi(n)$; since T has $\varphi(n)$ distinct elements and each is a primitive n^{th} roots of unity, T is precisely the set of all primitive n^{th} roots of unity. ■

Definition 13.10. For each $n \in \mathbb{Z}_+$, $\mathbf{n^{th}}$ **cyclotomic polynomial** is denoted and defined as

$$\Phi_n(x) = \prod_{\substack{\zeta^n = 1 \\ \text{ord}(\zeta) = n}} (x - \zeta).$$

By Corollary 13.9, if ζ is a primitive n^{th} root of unity, then

$$\Phi_n(x) = \prod_{\substack{k \in [n] \\ \gcd(k,n) = 1}} (x - \zeta^k).$$

Note that, by Corollary 13.7, $\deg(\Phi_n(x)) = \varphi(n)$.

Example. The expansions of the first few cyclotomic polynomials may be computed as:

$$\begin{aligned}
\Phi_1(x) &= x - 1 \\
\Phi_2(x) &= x + 1 \\
\Phi_3(x) &= x^2 + x + 1 \\
\Phi_4(x) &= x^2 + 1 \\
\Phi_5(x) &= x^4 + x^3 + x^2 + x + 1 \\
\Phi_6(x) &= x^2 - x + 1 \\
\Phi_7(x) &= x^6 + x^5 + x^4 + x^3 + x^2 + x + 1 \\
\Phi_8(x) &= x^4 + 1
\end{aligned}$$

Theorem 13.11. For each positive integer n,

$$x^n - 1 = \prod_{d|n} \Phi_d(x).$$

Proof. We will show that the complex roots on each side are the same with the same multiplicities (in fact, all multiplicities will turn out to be 1). On the left, the roots of $x^n - 1$ are precisely the n^{th} roots of unity, each with multiplicity 1. Looking to the right, we know that each n^{th} root of unity is a primitive root d^{th} root of unity for some divisor d of n, by Theorem 13.6, and so it is a root of exactly one $\Phi_d(x)$ with multiplicity 1. Since the roots of $x^n - 1$ are exactly the roots that occur on the right, including multiplicity, and since both sides are monic, the two sides represent the same polynomial. ■

Problem 13.12. For primes p and q, prove that:

1. $x^q - 1 = \Phi_q(x)\Phi_1(x)$
2. $\Phi_p(x) = x^{p-1} + x^{p-2} + \cdots + x^2 + x + 1 = \dfrac{x^p - 1}{x - 1}$.

   Using Eisenstein's criterion, we showed that this is irreducible in Example 8.8. In fact, all cyclotomic polynomials are irreducible, but a proof of this is both beyond our scope and unnecessary for our exposition.
3. $x^{pq} - 1 = \Phi_{pq}(x)\Phi_p(x)\Phi_q(x)\Phi_1(x)$
4. $\Phi_q(x^p) = \Phi_{pq}(x)\Phi_q(x)$
5. $(x^{pq} - 1)\Phi_{pq}(x) = \Phi_q(x^p)\Phi_p(x^q)\Phi_1(x)$
6. Finally,
$$\Phi_{pq}(x) = \frac{(x^{pq} - 1)(x - 1)}{(x^p - 1)(x^q - 1)}.$$

Theorem 13.13. For each $n \in \mathbb{Z}_+$, $\Phi_n(x)$ is an element of $\mathbb{Z}[x]$, meaning it is a polynomial with integer coefficients.

Proof. We will proceed by strong induction. In the base case $n = 1$, it is obvious that
$$\Phi_1(x) = x - 1 \in \mathbb{Z}[x].$$
Now suppose there exists $n \in \mathbb{Z}$ such that $\Phi_m(x) \in \mathbb{Z}[x]$ for each $m \in [n]$. Our goal is to show that, under this hypothesis,
$$\Phi_{n+1}(x) \in \mathbb{Z}[x].$$
First we define the polynomial
$$p(x) = \prod_{\substack{d \mid n+1 \\ d \neq n+1}} \Phi_d(x)$$
so that, by Theorem 13.11,
$$x^{n+1} - 1 = \prod_{d \mid n+1} \Phi_d(x) = \Phi_{n+1}(x) \cdot p(x).$$
By the induction hypothesis, $p(x) \in \mathbb{Z}[x]$ because it is the product of integer polynomials. By the Euclidean division of polynomials (covered in Volume 1) of $x^{n+1} - 1$ by the monic integer polynomial $p(x)$, there exists a quotient $q(x)$ and remainder $r(x)$, both in $\mathbb{Z}[x]$ such that
$$x^{n+1} - 1 = p(x)q(x) + r(x), \deg(r) < \deg(p) = n + 1 - \varphi(n + 1).$$
Since $r = x^{n+1} - 1 - pq$ has at least $n + 1 - \varphi(n + 1)$ roots (due to $x^{n+1} - 1$ and $p(x)$ both having all $n + 1 - \varphi(n + 1)$ non-primitive n^{th} roots of unity as roots), which exceeds $\deg(r)$, it means r is the 0 polynomial. Therefore,
$$p(x)q(x) = x^{n+1} - 1 = \Phi_{n+1}(x)p(x) \implies \Phi_{n+1}(x) = q(x) \in \mathbb{Z}[x],$$

where $p(x)$ could be cancelled from both sides because it is not the 0 polynomial. A key component of this proof was the fact that the Euclidean division of an integer polynomial by a *monic* integer polynomial produces a quotient and remainder in $\mathbb{Z}[x]$ as well. ■

Theorem 13.14. For each $n \in \mathbb{Z}_+$, we have the explicit formula

$$\Phi_n(x) = \prod_{d|n} (x^d - 1)^{\mu\left(\frac{n}{d}\right)}.$$

Note that μ can take on negative values, so the disadvantage of needing polynomial division subtracts from the formula's niceness.

Proof. Since Theorem 13.11 tells us that

$$x^n - 1 = \prod_{d|n} \Phi_d(x),$$

the multiplication variant of the Möbius inversion formula (Problem 3.19) yields

$$\begin{aligned} \Phi_n(x) &= \prod_{d|n} (x^{\frac{n}{d}} - 1)^{\mu(d)} \\ &= \prod_{ab=n} (x^a - 1)^{\mu(b)} \\ &= \prod_{d|n} (x^d - 1)^{\mu\left(\frac{n}{d}\right)}. \end{aligned}$$

■

Example 13.15. For all positive integers n, prove that

$$\mu(n) = \sum_{\substack{k \in [n] \\ \gcd(k,n)=1}} e^{\frac{2\pi k i}{n}}.$$

In other words, $\mu(n)$ is the sum of the primitive n^{th} roots of unity.

Solution. For non-constant polynomials f, let $[f(x)]_{-1}$ denote the coefficient of the term of second-highest degree (this coefficient is possibly 0). According to Vieta's formula, this is the negative of the sum of the (not necessarily distinct) roots of f divided by the leading coefficient. As a result of this interpretation, if f, g are non-constant monic polynomials, then

$$[f(x) \cdot g(x)]_{-1} = [f(x)]_{-1} + [g(x)]_{-1}.$$

Also, for any real constant c,

$$c \cdot [f(x)]_{-1} = [c \cdot f(x)]_{-1}.$$

In particular, we will use this for $c = -1$.

Since the primitive n^{th} roots of unity are the roots of $\Phi_n(x)$, each with multiplicity 1, it is true that

$$-\sum_{\substack{k\in[n]\\ \gcd(k,n)=1}} e^{\frac{2\pi k i}{n}} = [\Phi_n(x)]_{-1}.$$

So it suffices to prove that

$$\mu(n) = [-\Phi_n(x)]_{-1}$$

Since μ is characterized as the unique arithmetic function whose arithmetic summation function is $S_\mu = \varepsilon$ (Lemma 3.16), it suffices to prove that

$$\sum_{d|n} [-\Phi_d(x)]_{-1} = \varepsilon(n).$$

Indeed,

$$\begin{aligned}\sum_{d|n} [\Phi_d(x)]_{-1} &= \left[\prod_{d|n} \Phi_d(x)\right]_{-1}\\ &= [x^n - 1]_{-1}\\ &= \begin{cases} 0 & \text{if } n > 1\\ -1 & \text{if } n = 1\end{cases}\\ &= -\varepsilon(n).\end{aligned}$$

Taking the negative of this equation completes the proof. ■

Problem 13.16. For each integer $n \geq 2$, prove that the cyclotomic polynomial $\Phi_n(x)$ is symmetric in the sense that its coefficients (in the natural order or its reverse) form a palindrome.

Theorem 13.17. Let p and q be distinct primes. Then the coefficients of $\Phi_p(x^q)\Phi_q(x^p)$ are all among $\{0, 1\}$. As a consequence, we will show that the coefficients of $\Phi_{pq}(x)$ are all among $\{-1, 0, 1\}$. As a side note that we do not prove, the first counterexample to the proposition that the coefficients of *all* cyclotomic polynomials are in $\{-1, 0, 1\}$ is given by $\Phi_n(x)$ for $n = 3 \cdot 5 \cdot 7$, which is the product of the first three odd primes.

Proof. The following proof is an exposition of one due to Gary Brookfield, who published it in Mathematics Magazine [4]. According to Problem 13.12,

$$\begin{aligned}\Phi_q(x^p) &= (x^p)^{q-1} + (x^p)^{q-2} + \cdots + (x^p)^2 + x^p + 1,\\ \Phi_p(x^q) &= (x^q)^{p-1} + (x^q)^{p-2} + \cdots + (x^q)^2 + x^q + 1.\end{aligned}$$

Upon expansion of $\Phi_q(x^p)\Phi_p(x^q)$ and before collecting like terms, each term is of the form x^{rp+qs}, for $0 \leq r \leq q-1$ and $0 \leq s \leq p-1$. It suffices to prove that each exponent $rp + qs$ is unique in the expansion, so that the coefficients remain as 1 after like terms are collected (there will be nothing to collect). Suppose, for contradiction that

$$\begin{aligned}r_0 p + s_0 q &= r_1 p + s_1 q\\ p(r_0 - r_1) &= q(s_1 - s_0).\end{aligned}$$

By Euclid's lemma and the restrictions on the intervals of r and s,

$$\begin{aligned} r_0 \equiv r_1 \pmod{q} &\implies r_0 = r_1, \\ s_0 \equiv s_1 \pmod{p} &\implies s_0 = s_1. \end{aligned}$$

For the second part, Problem 13.12 tells us

$$(x^{pq}-1)\Phi_{pq}(x) = \Phi_q(x^p)\Phi_p(x^q)(x-1).$$

Since

$$\deg(\Phi_{pq}(x)) = \varphi(pq) = (p-1)(q-1) < pq,$$

the terms of $x^{pq}\Phi_{pq}(x)$ and $-\Phi_{pq}(x)$ require no collecting between each other upon expansion of

$$(x^{pq}-1)\Phi_{pq}(x) = x^{pq}\Phi_{pq}(x) - \Phi_{pq}(x).$$

So the set of coefficients of $(x^{pq}-1)\Phi_{pq}(x)$ is the same as the union of the set of coefficients of $\Phi_{pq}(x)$ and the latter's negatives, and a subset of this union is the set of coefficients of $\Phi_{pq}(x)$ itself. As

$$(x^{pq}-1)\Phi_{pq}(x) = \Phi_q(x^p)\Phi_p(x^q)(x-1),$$

it suffices to prove that the coefficients of the right side are all among $\{-1,0,1\}$ in order to prove that the coefficients of $\Phi_{pq}(x)$ are all among $\{-1,0,1\}$ as well. This expands as

$$x\Phi_q(x^p)\Phi_p(x^q) - \Phi_q(x^p)\Phi_p(x^q).$$

By the first part, the coefficients of $x\Phi_q(x^p)\Phi_p(x^q)$ are in $\{0,1\}$ and the coefficients of $-\Phi_q(x^p)\Phi_p(x^q)$ are in $\{0,-1\}$. The possible sums of coefficients are

$$0+0=1, 0+(-1)=-1, 1+0=1, 1+(-1)=0.$$

Therefore, the coefficients of $\Phi_{pq}(x)$ are all among $\{-1,0,1\}$. ■

Theorem 13.18. If p is a prime and n is a positive integer, then

$$\Phi_{pn}(x) = \begin{cases} \Phi_n(x^p) & \text{if } p \mid n \\ \dfrac{\Phi_n(x^p)}{\Phi_n(x)} & \text{if } p \nmid n \end{cases}.$$

As a consequence, if p is a prime, and n, k are positive integers, then

$$\Phi_{p^k n}(x) = \begin{cases} \Phi_n(x^{p^k}) & \text{if } p \mid n \\ \dfrac{\Phi_n(x^{p^k})}{\Phi_n(x^{p^{k-1}})} & \text{if } p \nmid n \end{cases}.$$

This further implies that

$$\Phi_{p^k n}(a) \mid \Phi_n(a^{p^k})$$

for all integers a, primes p, and positive integers n and k.

Proof. Suppose p is a prime and n is a positive integer. Suppose $p \mid n$. By Theorem 13.14,

$$\Phi_{pn}(x) = \prod_{d \mid pn} (x^{\frac{pn}{d}} - 1)^{\mu(d)}.$$

We can split the product into the $d \mid n$ and $d \nmid n$ cases to get

$$\Phi_{pn}(x) = \prod_{\substack{d \mid pn \\ d \mid n}} (x^{\frac{pn}{d}} - 1)^{\mu(d)} \cdot \prod_{\substack{d \mid pn \\ d \nmid n}} (x^{\frac{pn}{d}} - 1)^{\mu(d)}.$$

In the left product, the $d \mid pn$ condition is subsumed by the stronger $d \mid n$ condition. In the right product, let $k \in \mathbb{Z}_+$ satisfy $dk = pn$ since $d \mid pn$. Moreover, by $p \mid n$, there exists $j \in \mathbb{Z}_+$ such that $pj = n$. Then $dk = p^2 j$. Suppose, for contradiction, that at least one of the p's in the p^2 belongs to to k instead of d on the left. Then

$$\frac{k}{p} \cdot d = pj \implies d \mid pj \implies d \mid n,$$

which is a contradiction. Thus, the combination of $d \mid pn$ and $d \nmid n$, along with $p \mid n$, implies $p^2 \mid d$. Then d is not squarefree, and so $\mu(d) = 0$. Thus, in the $p \mid n$ case,

$$\Phi_{pn}(x) = \prod_{d \mid n} ((x^p)^{\frac{n}{d}} - 1)^{\mu(d)} = \Phi_n(x^p).$$

In the $p \nmid n$ case, we split

$$\Phi_{pn}(x) = \prod_{d \mid pn} (x^{\frac{pn}{d}} - 1)^{\mu(d)}$$

into the $p \mid d$ and $p \nmid d$ cases to get

$$\Phi_{pn}(x) = \prod_{\substack{d \mid pn \\ p \mid d}} (x^{\frac{pn}{d}} - 1)^{\mu(d)} \cdot \prod_{\substack{d \mid pn \\ p \nmid d}} (x^{\frac{pn}{d}} - 1)^{\mu(d)}.$$

In the left product, for each divisor d of pn, $p \mid d$ implies that there exists $k \in \mathbb{Z}_+$ such that $d = pk$. Then

$$\prod_{\substack{d \mid pn \\ p \mid d}} (x^{\frac{pn}{d}} - 1)^{\mu(d)} = \prod_{pk \mid pn} (x^{\frac{pn}{pk}} - 1)^{\mu(pk)} = \prod_{k \mid n} (x^{\frac{n}{k}} - 1)^{\mu(pk)}.$$

Suppose, for contradiction, that $p \mid k$. Then $p^2 \mid d$ because of $d = pk$. Since $d \mid pn$, we get $p^2 \mid pn$ or $p \mid n$, which contradicts the assumption that $p \nmid n$. Thus $p \nmid k$, which allows us to invoke the multiplicativity of μ to get

$$\mu(pk) = \mu(p)\mu(k) = -\mu(k).$$

This yields that the above left product is

$$\prod_{\substack{d \mid pn \\ p \mid d}} (x^{\frac{pn}{d}} - 1)^{\mu(d)} = \prod_{k \mid n} (x^{\frac{n}{k}} - 1)^{-\mu(k)} = \frac{1}{\Phi_n(x)}.$$

In the right product, $p \nmid d$ combined with $d \mid pn$ is equivalent to $d \mid n$, which results in the right product being

$$\prod_{\substack{d \mid pn \\ p \nmid d}} (x^{\frac{pn}{d}} - 1)^{\mu(d)} = \prod_{d \mid n} ((x^p)^{\frac{n}{d}} - 1)^{\mu(d)} = \Phi_n(x^p).$$

Therefore, if $p \nmid n$, then

$$\Phi_{pn}(x) = \frac{\Phi_n(x^p)}{\Phi_n(x)}.$$

The stated consequence follows from extracting one prime factor p at a time and applying the result that we just proved:

$$\Phi_{p^k n}(x) = \Phi_{p^{k-1} n}(x^p) = \cdots = \Phi_{pn}(x^{p^{k-1}}) = \begin{cases} \Phi_n(x^{p^k}) & \text{if } p \mid n \\ \dfrac{\Phi_n(x^{p^k})}{\Phi_n(x^{p^{k-1}})} & \text{if } p \nmid n \end{cases}.$$

This immediately implies the stated further implication. ■

Corollary 13.19. Let n and m be positive integers. If each distinct prime divisor of m is also divisor of n, then

$$\Phi_{mn}(x) = \Phi_n(x^m).$$

Subsequently, if v is the product of the distinct prime factors of n, called the **radical** of n, then

$$\Phi_n(x) = \Phi_v(x^{\frac{n}{v}}).$$

Proof. By Theorem 13.18, if the prime factorization of m is

$$m = p_1^{e_1} p_2^{e_2} \cdots p_t^{e_t}$$

and if each p_i divides n, then extracting one maximal prime power of m at a time yields

$$\begin{aligned} \Phi_{mn}(x) &= \Phi_{\frac{m}{p_1^{e_1}} \cdot n}(x^{p_1^{e_1}}) \\ &= \Phi_{\frac{m}{p_1^{e_1} p_2^{e_2}} \cdot n}(x^{p_1^{e_1} p_2^{e_2}}) \\ &\vdots \\ &= \Phi_{1 \cdot n}(x^{p_1^{e_1} p_2^{e_2} \cdots p_t^{e_t}}) \\ &= \Phi_n(x^m). \end{aligned}$$

Now let v be the radical of n, as defined in the statement. Then every prime factor of $\dfrac{n}{v}$ is a divisor of v. Let $n = kv$ for some $k \in \mathbb{Z}_+$. By the first part,

$$\Phi_n(x) = \Phi_{kv}(x) = \Phi_v(x^k) = \Phi_v(x^{\frac{n}{v}}).$$

■

Problem 13.20. Prove that:

1. If $n > 1$ is an odd integer, then
$$\Phi_{2n}(x) = \Phi_n(-x).$$
2. If p is an odd prime, then
$$\Phi_{2p}(x) = \sum_{i=0}^{p-1} (-1)^i x^i = 1 - x + x^2 - \cdots + x^{p-1}.$$
3. If p is a prime and k is a positive integer, then
$$\begin{aligned}\Phi_{p^k}(x) &= \sum_{i=0}^{p-1} x^{ip^{k-1}} \\ &= 1 + x^{p^{k-1}} + x^{2p^{k-1}} + \cdots + x^{(p-1)p^{k-1}}.\end{aligned}$$
In particular, if ℓ is a positive integer, then
$$\Phi_{2^\ell}(x) = x^{2^{\ell-1}+1}.$$
4. If p is an odd prime and ℓ, k are positive integers, then
$$\begin{aligned}\Phi_{2^\ell p^k}(x) &= \sum_{i=0}^{p-1} (-1)^i x^{i \cdot 2^{\ell-1} p^{k-1}} \\ &= 1 - x^{2^{\ell-1}p^{k-1}} + x^{2 \cdot 2^{\ell-1}p^{k-1}} - x^{3 \cdot 2^{\ell-1}p^{k-1}} + \cdots + x^{(p-1) \cdot 2^{\ell-1}p^{k-1}}.\end{aligned}$$

13.3 Cyclotomic Values

Having studied cyclotomic polynomials in their own context in Section 13.2, we will now apply them in number theory. The first observation we make is that, since Theorem 13.13 says that every cyclotomic polynomial is in $\mathbb{Z}[x]$, it implies that integer inputs result in integer outputs. In fact, we can prove that all outputs are positive as follows.

Theorem 13.21. For all integers $n \geq 3$ and for all $x \in \mathbb{R}$, $\Phi_n(x) > 0$.

Proof. Since Φ_n is a polynomial in $\mathbb{Z}[x]$ (specifically, we currently only care about the coefficients being real), all of whose roots are in $\mathbb{C}\backslash\mathbb{R}$ due to $n \geq 3$, it cannot output both positive and negative values: if both a positive and a negative value were achieved, then the continuity of real polynomials, combined with the intermediate value theorem, would imply that a real root exists in between, which is a contradiction. So the outputs of Φ_n are all positive or all negative. Since the leading coefficient of Φ_n is positive, the outputs of all sufficiently large inputs are positive, implying that the outputs of *all* inputs are positive in this case. As a side note, for $n \geq 3$,
$$\deg(\Phi_n(x)) = \varphi(n)$$

is even. This makes sense, since polynomials of odd degree have opposite end behaviours of y as $x \to +\infty$ versus $x \to -\infty$, which implies that both positive and negative values exist, resulting in the existence of a real root. ■

Problem 13.22. For each integer $n \geq 2$, show that $\Phi_n(0) = 1$.

Problem 13.23. Compute that, if p is a prime and k is a positive integer then $\Phi_{p^k}(1) = p$, and if $n \geq 2$ is not a prime power then $\Phi_n(1) = 1$.

Lemma 13.24. If $n \geq 2$ is an integer, and p is a prime such that $x^n - 1$ has a double root, $a \in \mathbb{Z}$, modulo p, then $p \mid n$.

Proof. Since a is a double root of $x^n - 1$ modulo p, there exists a polynomial $g \in \mathbb{Z}[x]$ such that

$$x^n - 1 \equiv (x - a)^2 \cdot g(x) \pmod{p}.$$

Using the substitution $y = x - a$, the congruence becomes

$$(y + a)^n - 1 \equiv y^2 \cdot g(y + a) \pmod{p}.$$

Comparing the coefficients of y on each side shows that it is na^{n-1} on the left and 0 on the right. So $p \mid na^{n-1}$. Since a is a root of $x^n - 1$, we know that

$$a^n \equiv 1 \pmod{p},$$

so $p \nmid a$. Thus, $p \mid na^{n-1}$ leads to $p \mid n$ via Euclid's lemma. ■

Lemma 13.25. If p is a prime, $n \geq 2$ is an integer, d is a proper divisor of n, and a is an integer such that $p \mid \Phi_n(a)$ and $p \mid \Phi_d(a)$, then $p \mid n$.

Proof. We know the decomposition

$$x^n - 1 = \prod_{c \mid n} \Phi_c(x).$$

Moreover, $\Phi_n(x)$ and $\Phi_d(x)$ are distinct multiplicands in this product. As a result, a is a double root of $x^n - 1$. By Lemma 13.24, $p \mid n$. ■

Theorem 13.26. Let p be a prime and n be a positive integer. Let $t \in \mathbb{Z}_{\geq 0}$ and $m \in \mathbb{Z}_+$ be such that $n = p^t m$ and $p \nmid m$. If a is an integer such that $p \mid \Phi_n(a)$, meaning a is an integer root of Φ_n modulo p, then $p \nmid a$ and

$$\operatorname{ord}_p(a) = m.$$

- The specific case where $t = 0$ says that, if $p \nmid m$, then

  $$p \mid \Phi_m(a) \implies \operatorname{ord}_p(a) = m.$$

  As a consequence, if $p \nmid m$, then

  $$p \mid \Phi_m(a) \implies p \equiv 1 \pmod{m}.$$

  In other words, every prime divisor p of $\Phi_m(a)$ satisfies $p \mid m$ or $m \mid p - 1$.

- The converse of this specific case (where $t = 0$) holds as well: if $p \nmid m$, then

$$\operatorname{ord}_p(a) = m \implies p \mid \Phi_m(a).$$

Proof. Let p and $n = p^t m$ be as stated. Suppose $a \in \mathbb{Z}$ such that $p \mid \Phi_n(a)$. Since $\Phi_n(a) \mid a^n - 1$, it means $a^n \equiv 1 \pmod{p}$, leading to $p \nmid a$. As a preliminary observation, Fermat's little theorem tells us that

$$a^p \equiv a \pmod{p},$$

so taking repeated exponents of p yields

$$a^{p^k} \equiv a^{p^{k-1}} \equiv \cdots \equiv a^p \equiv a \pmod{p}$$

for all positive integers k. As a result,

$$a^n = a^{p^k m} \equiv a^{p^{k-1} m} \equiv \cdots \equiv a^m \pmod{p}.$$

Since $p \mid \Phi_n(a)$ and $\Phi_n(a) \mid a^n - 1$, it holds that

$$a^m \equiv a^n \equiv 1 \pmod{p}.$$

Letting $k = \operatorname{ord}_p(a)$, we know that $k \mid m$. We wish to show that $k = m$, so suppose, for the sake of contradiction, that k is a proper divisor of m. From

$$a^k \equiv 1 \pmod{p},$$

we get

$$p \mid a^k - 1 = \prod_{d \mid k} \Phi_d(a).$$

By Euclid's lemma, there exists a divisor d of k such that $p \mid \Phi_d(a)$. If we could show that $p \mid \Phi_m(a)$ as well, then Lemma 13.25 would imply that $p \mid m$, which would be our desired contradiction.
So now we will show that $p \mid \Phi_m(a)$ to complete the proof. Using the fact that $\Phi_m(x) \in \mathbb{Z}[x]$ and $a^{p^t} \equiv a \pmod{p}$, we find that

$$\Phi_m(a^{p^t}) \equiv \Phi_m(a) \pmod{p}.$$

According to Theorem 13.18,

$$\Phi_n(a) = \Phi_{p^t m}(a) \mid \Phi_m(a^{p^t}).$$

Since $p \mid \Phi_n(a)$ is given,

$$\Phi_m(a) \equiv \Phi_m(a^{p^t}) \equiv \Phi_n(a) \equiv 0 \pmod{p}.$$

Thus, the assumption is that k is a proper divisor of m is incorrect, and so $k = m$.
As for the two bulleted points:

- The corollary for $t = 0$ is immediate. It is simply the case where $p \nmid n$. In this case, if $p \mid \Phi_m(a)$, then $\text{ord}_p(a) = m$. Since $p \nmid a$, Fermat's little theorem says that

$$a^{p-1} \equiv 1 \pmod{p}.$$

  So $m \mid p - 1$. We can think of it as the $p \leq m$ case leading to $p \mid m$, and the $m < p$ case leading to $m \mid p - 1$.

- For the converse of the first bulleted point, suppose $t = 0$ again and that $\text{ord}_p(a) = m$. Then $a^m \equiv 1 \pmod{p}$, which implies

$$a^m - 1 = \prod_{d \mid m} \Phi_d(a).$$

  We wish to show that $p \mid \Phi_m(a)$. So suppose, for contradiction, that $p \nmid \Phi_m(a)$. Then, by Euclid's lemma, there exists a proper divisor $d \mid m$ such that $p \mid \Phi_d(a)$. Since $\Phi_d(a) \mid a^d - 1$, we get $p \mid a^d - 1$, meaning

$$a^d \equiv 1 \pmod{p}.$$

  But $d < m$, as d is a proper divisor of m, which contradicts the fact that $m = \text{ord}_p(a)$ is the least positive exponent that sends a to 1 modulo p.

■

Corollary 13.27. Let m and n be distinct positive integers, and a be an integer such that

$$\gcd(\Phi_m(a), \Phi_n(a)) > 1.$$

Then there exists a non-zero integer k (possibly negative) such that $\dfrac{n}{m} = p^k$, where p is a prime factor of $\gcd(\Phi_m(a), \Phi_n(a))$. As a further consequence,

$$\gcd(\Phi_m(a), \Phi_n(a)) = p^\ell$$

for some positive integer ℓ.

Proof. Let p be a prime such that

$$p \mid \gcd(\Phi_m(a), \Phi_n(a)).$$

Then there exist positive integers b, c and integers s, t such that

$$\begin{aligned} m &= p^b s, \ p \nmid s, \\ n &= p^c t, \ p \nmid t. \end{aligned}$$

By Theorem 13.26,

$$\begin{aligned} p \mid \Phi_m(a) &\implies \text{ord}_p(a) = s, \\ p \mid \Phi_n(a) &\implies \text{ord}_p(a) = t, \end{aligned}$$

so $s = t$. Then

$$\frac{n}{m} = \frac{p^c t}{p^b s} = p^{c-b}.$$

We take $k = c - b$. Note that $c \neq b$, or else we would have $n = m$, contradicting that n, m are distinct.
The further consequence has to be true because, otherwise, $\frac{n}{m}$ will equal to the power of more than one prime, which is a contradictory situation. ■

Corollary 13.28. Let m and n be distinct positive integers and a be an integer. If p is a prime such that $p \nmid mn$, then at least one of $\Phi_m(a)$ or $\Phi_n(a)$ is not divisible by p.

Proof. Let m, n, and a be as stated. We will prove the contrapositive. Assume $p \mid \Phi_m(a)$ and $p \mid \Phi_n(a)$. Then

$$p \mid \gcd(\Phi_m(a), \Phi_n(a)),$$

implying that this gcd is strictly greater than 1. By Corollary 13.27, there exists a non-zero integer k such that $n = p^k m$. So $p \mid n$ if $k > 0$, or $p \mid m$ if $k < 0$. Either way, $p \mid mn$. This proves the contrapositive of the desired statement. ■

Problem 13.29. Let p be a prime and a be an integer. Prove that every prime factor p of

$$\Phi_q(a) = 1 + a + a^2 + \cdots + a^{q-1}$$

satisfies $p \equiv 1 \pmod{q}$ or $p = q$.

The following is an interesting application of cyclotomic polynomials and cyclotomic values that effortlessly generalizes Theorem 12.24.

Theorem 13.30. For any positive integer n, there exist infinitely many primes p such that

$$p \equiv 1 \pmod{n}.$$

Proof. We may assume that $n \geq 2$ because the result for $n = 1$ simply says that there are infinitely many primes, which was known to Euclid. Suppose, for contradiction, that there exist only finitely many primes p such that $p \equiv 1 \pmod{n}$. Let S be their product, and let T be the product of all distinct primes dividing n (recall that this is called the radical of n). Let $R = S \cdot T$. Since $n \geq 2$, n actually has a prime factor, which tells us that $R > 1$. As $\Phi_n(x)$ is a non-constant polynomial with leading coefficient 1,

$$\Phi_n(R^k) > 1$$

for all sufficiently large positive integers k. We fix such a k and let q be a prime factor of $\Phi_n(R^k)$. Then

$$q \mid \Phi_n(R^k) \mid (R^k)^n - 1,$$

so q cannot be a prime factor of R. By the definition of $R = S \cdot T$, this means that $q \not\equiv 1 \pmod{n}$ and $q \nmid n$. The contradictory issue is that, by Theorem 13.26, every prime divisor q of $\Phi_n(R^k)$ must satisfy $q \mid n$ or $n \mid q - 1$, whereas we have proven precisely the negation of this. ■

13.4 Zsigmondy's Theorem

We begin the final part of the journey towards Zsigmondy's theorem by defining a "homogenized" two-variable version of cyclotomic polynomials, and studying its properties.

Definition 13.31. If n is a positive integer, and a and b are integers, let

$$\Psi_n(a,b) = \prod_{d|n} (a^{\frac{n}{d}} - b^{\frac{n}{d}})^{\mu(d)}.$$

Lemma 13.32. Let n be a positive integer, and a and $b \neq 0$ be integers. Then

$$\Psi_n(a,b) = b^{\varphi(n)} \cdot \Phi_n\left(\frac{a}{b}\right),$$

which is always an integer, and, in fact, it is necessarily positive if $n \geq 3$. As a consequence of the first identity,

$$\prod_{d|n} \Psi_d(a,b) = a^n - b^n.$$

Proof. An initial "normalization" shows that

$$\begin{aligned}
\Psi_n(a,b) &= \prod_{d|n} (a^{\frac{n}{d}} - b^{\frac{n}{d}})^{\mu(d)} \\
&= \prod_{d|n} b^{\frac{n}{d}\cdot\mu(d)} \cdot \left(\left(\frac{a}{b}\right)^{\frac{n}{d}} - 1\right)^{\mu(d)} \\
&= \prod_{d|n} b^{\frac{n}{d}\cdot\mu(d)} \cdot \prod_{d|n} \left(\left(\frac{a}{b}\right)^{\frac{n}{d}} - 1\right)^{\mu(d)} \\
&= b^{\sum_{d|n} \frac{n}{d}\cdot\mu(d)} \cdot \Phi_n\left(\frac{a}{b}\right).
\end{aligned}$$

By Theorem 3.21, $\mathrm{Id} = S_\varphi$, so the Möbius inversion formula (Theorem 3.18) implies $\varphi = \mu * \mathrm{Id}$. As a result, the exponent on b is

$$\sum_{d|n} \frac{n}{d} \cdot \mu(d) = (\mathrm{Id} * \mu)(n) = \varphi(n).$$

The expression

$$\Psi_n(a,b) = b^{\varphi(n)} \cdot \Phi_n\left(\frac{a}{b}\right)$$

necessarily represents an integer because $\deg(\Phi_n) = \varphi(n)$, so multiplication by $b^{\varphi(n)}$ clears all denominators of $\Phi_n\left(\frac{a}{b}\right)$. For $n \geq 3$, the exponent $\varphi(n)$ of b is even and Φ_n is always above the x-axis by Theorem 13.21, so $\Psi_n(a,b)$ has to be positive.

For the second identity, we use the first identity and $S_\varphi = \mathrm{Id}$ to get

$$\begin{aligned}\prod_{d|n} \Psi_d(a,b) &= \prod_{d|n} b^{\varphi(d)} \cdot \Phi_d\left(\frac{a}{b}\right) \\ &= \prod_{d|n} b^{\varphi(d)} \cdot \prod_{d|n} \Phi_d\left(\frac{a}{b}\right) \\ &= b^{\sum_{d|n}\varphi(d)} \cdot \prod_{d|n} \Phi_d\left(\frac{a}{b}\right) \\ &= b^n \cdot \left(\left(\frac{a}{b}\right)^n - 1\right) = a^n - b^n.\end{aligned}$$

■

Lemma 13.33. If p is a prime, n is a positive integer, and a and $b \neq 0$ are integers, then

$$\Psi_{pn}(a,b) = \begin{cases} \Psi_n(a^p, b^p) & \text{if } p \mid n \\ \dfrac{\Psi_n(a^p,b^p)}{\Psi_n(a,b)} & \text{if } p \nmid n \end{cases}.$$

Proof. By Theorem 13.18,

$$\begin{aligned}\Psi_{pn}(a,b) &= b^{\varphi(pn)} \cdot \Phi_{pn}\left(\frac{a}{b}\right) \\ &= \begin{cases} b^{p\varphi(n)} \cdot \Phi_n\left(\dfrac{a^p}{b^p}\right) & \text{if } p \mid n \\ \dfrac{b^{(p-1)\varphi(n)} \cdot \Phi_n\left(\frac{a^p}{b^p}\right)}{\Phi_n\left(\frac{a}{b}\right)} & \text{if } p \nmid n \end{cases} \\ &= \begin{cases} (b^p)^{\varphi(n)} \cdot \Phi_n\left(\dfrac{a^p}{b^p}\right) & \text{if } p \mid n \\ \dfrac{(b^p)^{\varphi(n)} \cdot \Phi_n\left(\frac{a^p}{b^p}\right)}{b \cdot \Phi_n\left(\frac{a}{b}\right)} & \text{if } p \nmid n \end{cases} \\ &= \begin{cases} \Psi_n(a^p,b^p) & \text{if } p \mid n \\ \dfrac{\Psi_n(a^p,b^p)}{\Psi_n(a,b)} & \text{if } p \nmid n \end{cases}.\end{aligned}$$

Note that we used the fact that

$$\varphi(pn) = \begin{cases} p\varphi(n) & \text{if } p \mid n \\ \varphi(p)\varphi(n) = (p-1)\varphi(n) & \text{if } p \nmid n \end{cases}$$

when working with the exponent of the external b. ■

Now we will begin to combine the LTE lemma with the homogeneous variants of cyclotomic polynomials.

Problem 13.34. Let p be a prime, and a and $b \neq 0$ be integers that are not divisible by p. Let n be a positive integer and k be the smallest positive integer such that $p \mid a^k - b^k$ (k is known to exist by Problem 13.4). Prove that, if $p \mid \Psi_n(a,b)$, then $k \mid n$. Note that, by contrapositive,

$$k \nmid n \implies \nu_p(\Psi_n(a,b)) = 0.$$

Lemma 13.35. Let p be an odd prime and a, b be integers that are not divisible by p (in particular, $b \neq 0$). Let n be a positive integer and k be the minimal positive integer such that $p \mid a^k - b^k$. then

$$\nu_p(\Psi_n(a,b)) = \begin{cases} \nu_p(a^k - b^k) & \text{if } n = k \\ 1 & \text{if } \exists t \in \mathbb{Z}_+ : n = p^t k, p \nmid k \\ 0 & \text{otherwise} \end{cases}.$$

Proof. We will handle the cases in succession:

1. If $n = k$, then

$$\begin{aligned} \nu_p(a^k - b^k) &= \nu_p\left(\prod_{d \mid k} \Psi_d(a,b)\right) \\ &= \nu_p(\Psi_k(a,b)) + \sum_{\substack{d \mid k \\ d \neq k}} \nu_p(\Psi_d(a,b)). \end{aligned}$$

   By Problem 13.34, the sum on the right has all summands equal to 0 because proper divisors d of k cannot be divisible by k. So, in the $n = k$ case,

$$\nu_p(\Psi_n(a,b)) = \nu_p(a^k - b^k).$$

2. Since $p \mid a^k - b^k$, LTE 2(a) (Theorem 13.2) says that, for any positive integer t,

$$\begin{aligned} \nu_p(a^{p^t k} - b^{p^t k}) &= \nu_p((a^k)^{p^t} - (b^k)^{p^t}) \\ &= \nu_p(a^k - b^k) + \nu_p(p^t) \\ &= \nu_p(a^k - b^k) + t. \end{aligned}$$

   A second way of computing the same quantity via cyclotomic theory is

$$\begin{aligned} \nu_p(a^{p^t k} - b^{p^t k}) &= \nu_p\left(\prod_{d \mid p^t k} \Psi_d(a,b)\right) \\ &= \sum_{d \mid p^t k} \nu_p(\Psi_d(a,b)). \end{aligned}$$

   By Problem 13.34, the sum over $d \mid p^t k$ can be restricted to those divisors d of $p^t k$ that are themselves divisible by k, because otherwise $\nu_p(\Psi_d(a,b)) = 0$. Equating the two

computations yields

$$\begin{aligned}\nu_p(a^k - b^k) + t &= \sum_{\substack{d \mid p^t k \\ k \mid d}} \nu_p(\Psi_d(a,b)) \\ &= \sum_{s=0}^{t} \nu_p(\Psi_{p^s k}(a,b)) \\ &= \nu_p(\Psi_k(a,b)) + \sum_{s=1}^{t} \nu_p(\Psi_{p^s k}(a,b)).\end{aligned}$$

By part (1),

$$\nu_p(\Psi_k(a,b)) = \nu_p(a^k - b^k),$$

so cancelling them from the ends gives

$$\sum_{s=1}^{t} \nu_p(\Psi_{p^s k}(a,b)) = t.$$

This holds for all positive integers t, so we can use it to prove by strong induction on integers $s \geq 1$ that

$$\nu_p(\Psi_{p^s k}(a,b)) = 1.$$

Taking $s = t$ returns the second case of the stated formula.

3. In the third case, we may assume that $k \mid n$, as, otherwise, Problem 13.34 would say that if $k \nmid n$, then $\nu_p(\Psi_n(a,b)) = 0$ automatically. So let $n = p^t m k$ for a non-negative integer t (which might be 0) and a positive integer m such that $p \nmid m$. Since $p \nmid m$ and

$$p \mid a^k - b^k \mid a^{p^t k} - b^{p^t k},$$

LTE 1(a) (Theorem 13.2) says that

$$\begin{aligned}\nu_p(a^n - b^n) &= \nu_p((a^{p^t k})^m - (b^{p^t k})^m) \\ &= \nu_p(a^{p^t k} - b^{p^t k}).\end{aligned}$$

Due to $p^t k \mid n$, we know that

$$a^{p^t k} - b^{p^t k} \mid a^n - b^n,$$

and the above LTE application says that

$$\nu_p\left(\frac{a^n - b^n}{a^{p^t k} - b^{p^t k}}\right) = \nu_p(a^n - b^n) - \nu_p(a^{p^t k} - b^{p^t k}) = 0.$$

Part (2) handled $m = 1$, so we may assume that $m > 1$. As a result of the assumption that $m > 1$, $\Psi_n(a,b)$ survives in the numerator of the right side of

$$\frac{a^n - b^n}{a^{p^t k} - b^{p^t k}} = \frac{\prod_{d \mid n} \Psi_d(a,b)}{\prod_{d \mid p^t k} \Psi_d(a,b)}$$

after all the bottom-right multiplicands cancel with their identical copies in the top-right (a copy of each bottom one exists in the top since $p^t k \mid n$). Thus,

$$0 \leq \nu_p(\Psi_n(a,b)) \leq \nu_p\left(\frac{a^n - b^n}{a^{p^t k} - b^{p^t k}}\right) = 0,$$

so antisymmetry of real inequalities tells us that $\nu_p(\Psi_n(a,b)) = 0$ in the third case.

■

Lemma 13.36. Let $p = 2$ and a, b be integers that are not divisible by 2, so they are odd (in particular, $b \neq 0$). Let n be a positive integer. Then:

$$\nu_2(\Psi_n(a,b)) = \begin{cases} \nu_2(a-b) & \text{if } n = 1 \\ \nu_2(a+b) & \text{if } n = 2 \\ 1 & \text{if } \exists t \in \mathbb{Z}_+ : n = 2^t, t \geq 2 \\ 0 & \text{otherwise} \end{cases}.$$

Proof. We will handle the cases in succession:

1. If $n = 1$, then
$$\Psi_1(a,b) = b^{\varphi(1)} \cdot \Phi_1\left(\frac{a}{b}\right) = b \cdot \left(\frac{a}{b} - 1\right) = a - b,$$
so
$$\nu_2(\Psi_1(a,b)) = \nu_2(a-b).$$

2. If $n = 2$, then
$$\Psi_2(a,b) = b^{\varphi(2)} \cdot \Phi_2\left(\frac{a}{b}\right) = b \cdot \left(\frac{a}{b} + 1\right) = a + b,$$
so
$$\nu_2(\Psi_2(a,b)) = \nu_2(a+b).$$

3. For the third case, let $n = 2^t$ where $t \geq 2$ is an integer. Since $2 \mid a - b$ due to a, b both being odd, LTE 3(b) (Theorem 13.2) says that, for any integer $t \geq 2$,
$$\begin{aligned} \nu_2(a^{2^t} - b^{2^t}) &= \nu_2(a-b) + \nu_2(a+b) + \nu_2(2^t) - 1 \\ &= \nu_2(a-b) + \nu_2(a+b) + t - 1. \end{aligned}$$
Another way of computing the same quantity via cyclotomic theory and parts (1) and (2) is
$$\begin{aligned} \nu_2(a^{2^t} - b^{2^t}) &= \nu_2\left(\prod_{d \mid 2^t} \Psi_d(a,b)\right) \\ &= \nu_2(\Psi_1(a,b)) + \nu_2(\Psi_2(a,b)) + \sum_{s=2}^{t} \nu_2(\Psi_{2^s}(a,b)) \\ &= \nu_2(a-b) + \nu_2(a+b) + \sum_{s=2}^{t} \nu_2(\Psi_{2^s}(a,b)). \end{aligned}$$

Equating the two expressions for $\nu_2(a^{2^t} - b^{2^t})$ and simplifying yields

$$\nu_2(a-b) + \nu_2(a+b) + t - 1 = \nu_2(a-b) + \nu_2(a+b) + \sum_{s=2}^{t} \nu_2(\Psi_{2^s}(a,b))$$

$$t - 1 = \sum_{s=2}^{t} \nu_2(\Psi_{2^s}(a,b)).$$

As this is true for all integers $t \geq 2$, it may be shown by strong induction on integers $s \geq 2$ that

$$\nu_2(\Psi_{2^s}(a,b)) = 1.$$

Taking $s = t$ proves the third case of the formula.

4. In the fourth case, let $n = 2^t m$ for a non-negative integer t (where t is possibly 0) and a positive integer m such that $2 \nmid m$. Due to the oddness of a and b,

$$2 \mid a - b \mid a^{2^t} - b^{2^t}.$$

Since $2 \nmid m$, LTE 1(a) (Theorem 13.2) tells us

$$\begin{aligned} \nu_2(a^n - b^n) &= \nu_2((a^{2^t})^m - (b^{2^t})^m) \\ &= \nu_2(a^{2^t} - b^{2^t}). \end{aligned}$$

Using $2^t \mid n$, we know that

$$a^{2^t} - b^{2^t} \mid a^n - b^n,$$

so the above application of LTE says that

$$\nu_2\left(\frac{a^n - b^n}{a^{2^t} - b^{2^t}}\right) = \nu_2(a^n - b^n) - \nu_2(a^{2^t} - b^{2^t}) = 0.$$

Part (3) took care of $m = 1$, so we may assume that $m > 1$, which means $\Psi_n(a,b)$ survives in the numerator of the right side of

$$\frac{a^n - b^n}{a^{2^t} - b^{2^t}} = \frac{\prod_{d|n} \Psi_d(a,b)}{\prod_{d|2^t} \Psi_d(a,b)}$$

after all the bottom multiplicands on the right side cancel with their identical copies in the top of the right side (a copy of each bottom one exists in the top because $2^t \mid n$). Thus,

$$0 \leq \nu_2(\Psi_n(a,b)) \leq \nu_2\left(\frac{a^n - b^n}{a^{2^t} - b^{2^t}}\right) = 0,$$

and the antisymmetry of real inequalities completes the proof by saying $\nu_2(\Psi_n(a,b)) = 0$ in the fourth case.

■

We will need the following bounds in the proof of Zsigmondy's theorem.

Lemma 13.37. If $n \geq 3$ is an integer and $x > 1$ is a real number, then

$$(x-1)^{\varphi(n)} \leq \Phi_n(x) \leq (x+1)^{\varphi(n)}.$$

As a consequence, if $n \geq 3$ is an integer and a and b are integers such that $a > b \neq 0$, then

$$(a-b)^{\varphi(b)} \leq \Psi_n(a,b) \leq (a+b)^{\varphi(n)}.$$

Proof. We will use the original definition that

$$\Phi_n(x) = \prod_{\substack{\zeta^n=1 \\ \text{ord}(\zeta)=n}} (x-\zeta),$$

where there are $\varphi(n)$ multiplicands. Any root of unity ζ lies on the unit circle, meaning its complex modulus is $|\zeta| = 1$. By the complex triangle inequality (see Volume 1),

$$x - 1 = |x| - |\zeta| \leq |x - \zeta| \leq |x| + |\zeta| = x + 1.$$

Since $x > 1$, we know that $x-1$ is positive. Thus, taking the $\varphi(n)$-fold product of inequalities of the form

$$x - 1 \leq |x - \zeta| \leq x + 1,$$

we get

$$(x-1)^{\varphi(n)} \leq \prod_{\substack{\zeta^n=1 \\ \text{ord}(\zeta)=n}} |x-\zeta| \leq (x+1)^{\varphi(n)}.$$

The rest follows from Theorem 13.21, which says that $\Phi_n(x)$ is positive for $n \geq 3$, so

$$\prod_{\substack{\zeta^n=1 \\ \text{ord}(\zeta)=n}} |x-\zeta| = |\Phi_n(x)| = \Phi_n(x).$$

For the second part, we will use Lemma 13.32, which says

$$\Psi_n(a,b) = b^{\varphi(n)} \cdot \Phi_n\left(\frac{a}{b}\right).$$

Substituting $x = \dfrac{a}{b} > 1$ into the bounds derived in the first part, we find that

$$\left(\frac{a}{b} - 1\right)^{\varphi(n)} \leq \Phi_n\left(\frac{a}{b}\right) \leq \left(\frac{a}{b} + 1\right)^{\varphi(n)}.$$

Multiplying through by $b^{\varphi(b)}$ (which is positive, since $\varphi(n)$ is even for $n \geq 3$) yields

$$(a-b)^{\varphi(b)} \leq b^{\varphi(n)} \cdot \Phi_n\left(\frac{a}{b}\right) \leq (a+b)^{\varphi(b)},$$

which is equivalent to what we seek. ∎

We are ready for Zsigmondy now.

Definition 13.38. Let a, b be coprime positive integers such that $a > b$. Let $n \geq 2$ be an integer. A **primitive prime divisor** of the triple (a, b, n) is a prime p such that $p \mid a^n - b^n$ but $p \nmid a^k - b^k$ for all $k \in [n-1]$.

Theorem 13.39 (Zsigmondy's theorem)**.** Let a and b be coprime positive integers such that $a > b$. Let $n \geq 2$ be a positive integer.

1. For $n = 2$, if $(a, b, 2)$ does not have a primitive prime divisor, then $a + b = 2^t$ for some positive integer t.
2. For $n \geq 3$, if (a, b, n) does not have a primitive prime divisor, then $(a, b, n) = (2, 1, 6)$.

By contrapositive, the triple (a, b, n) has a primitive prime divisor in every other case.

Proof. Let a, b, n be as stated.

1. Suppose $n = 2$ and that $(a, b, 2)$ has no primitive prime divisor. Since $a > b$ are positive integers, we know that $a - b \geq 1$ and $a \geq 1$ and $b \geq 1$. Then
$$a^2 - b^2 = (a - b)(a + b) \geq a + b \geq 2,$$
so there must exist a prime p such that
$$p \mid a + b \mid a^2 - b^2.$$
Since a primitive prime divisor does not exist for $a^2 - b^2$, p must also divide the only level that exists below $a^2 - b^2$, which is $a - b$. Then
$$p \mid (a + b) + (a - b) = 2a,$$
$$p \mid (a + b) - (a - b) = 2b.$$
If $p \neq 2$, then $p \nmid 2$, so Euclid's lemma gives $p \mid a$ from the first line and $p \mid b$ from the second line, which contradicts the coprimality of a and b. So the only prime that divides $a + b$ is 2, meaning $a + b$ is a non-trivial power of 2. Explicitly, there must exist a positive integer t such that $a + b = 2^t$.

2. Now suppose $n \geq 3$ and that (a, b, n) has no primitive prime divisor. Our aim is to restrict the integers a, b, and n through divisibility properties and bounds until we are left with no choice except $(a, b, n) = (2, 1, 6)$. Initially, we will gain insights into the integer triple (a, b, n) by studying $\Psi_n(a, b)$. If $\Psi_n(a, b)$ has no prime factors, then
$$\Psi_n(a, b) = 1.$$
Otherwise, let p be a prime factor of $\Psi_n(a, b)$. Since
$$p \mid \Psi_n(a, b) \mid a^n - b^n,$$
it means p is a prime factor of $a^n - b^n$. By assumption, p cannot be primitive, so there exists a minimal $k \in [n-1]$ such that $p \mid a^k - b^k$. Note that if $p \mid a$ or $p \mid b$ then, by $p \mid a^n - b^n$, we get $p \mid a$ and $p \mid b$, contradicting the coprimality of a and b. Then $p \nmid a$ and $p \nmid b$, which is good news because it allows us to invoke the strength of the classifications in Lemma 13.35 and Lemma 13.36 to study the divisibility structure of n. We consider the $p \geq 3$ and $p = 2$ cases separately:

(a) Suppose $p \geq 3$. Since $p \mid \Psi_n(a,b)$, we know that $\nu_p(\Psi_n(a,b)) \geq 1$. In the classification listed in Lemma 13.35, this allows us to eliminate the "otherwise" case. Moreover, we stated that $k \in [n-1]$, so we can eliminate the $n = k$ case. Thus, we are left with $n = p^t k$ for some positive integer t such that $p \nmid k$. In this case, the classification says

$$\nu_p(\Psi_n(a,b)) = 1.$$

(b) Suppose $p = 2$. Once again, $p \mid \Psi_n(a,b)$ leads to $\nu_2(\Psi_n(a,b)) \geq 1$. Looking at the classification listed in Lemma 13.36, this eliminates the "otherwise" case. Moreover, the fact that $n \geq 3$ eliminates the $n = 1$ and $n = 2$ cases. This leaves us with $n = 2^t$ for some integer $t \geq 2$. In this case, the classification says

$$\nu_2(\Psi_n(a,b)) = 1.$$

Note that, since $2 \nmid a$ and $2 \nmid b$, it means a and b are both odd, so $2 \mid a^1 - b^1$, implying $k = 1$. As such, we can say that $n = 2^t k$.

In both of the $p \geq 3$ and $p = 2$ cases, $n = p^t k$ for some positive integer t and where k is the least positive integer such that $p \mid a^k - b^k$. Since t is positive, $p \mid n$. We claim that p is in fact the largest prime factor of n. Suppose q (distinct from p) is another prime factor of n. Then the fact that $n = p^t k$ tells us that $q \mid k$, so $q \leq k$. By Problem 13.4, $k = \operatorname{ord}_p(ab^{-1})$. By Fermat's little theorem, $k \mid p-1$, so $k < p$. Thus,

$$q \leq k < p,$$

showing that p is strictly greater than every prime factor $q \neq p$ of n. To summarize our knowledge so far: if p is a prime factor of $\Psi_n(a,b)$ and $n \geq 3$ and (a,b,n) has no primitive prime divisor, then p is the largest prime that divides n. Since the largest prime that divides n is unique, $\Psi_n(a,b)$ must equal p^ℓ for some positive integer ℓ. In the casework above, we proved that

$$\nu_p(\Psi_n(a,b)) = 1$$

for both $p \geq 3$ and $p = 2$, so $\ell = 1$. Therefore, either $\Psi_n(a,b)$ has no prime factors, in which case $\Psi_n(a,b) = 1$, or $\Psi_n(a,b) = p$, where p is the largest prime factor of n. Either way, the fact that $a - b \geq 1$ and $\varphi(n) \geq p - 1$, combined with the lower bound in Lemma 13.37, gives

$$\begin{aligned} p &\geq \Psi_n(a,b) \\ &\geq (a-b)^{\varphi(n)} \\ &\geq (a-b)^{p-1}. \end{aligned}$$

We wish to weaken this lower bound so that the inequality is exclusively in terms of p, while hopefully keeping the lower bound strong, thereby giving restrictive insights into p and perhaps other aspects of (a,b,n) along the way. We will now consider $a - b \geq 2$ and $a - b = 1$ separately.

(a) Suppose $a - b \geq 2$. Then

$$p \geq (a-b)^{p-1} \geq 2^{p-1}.$$

By induction on integers $s \geq 3$, we can show that $2^{s-1} > s$, forcing $p = 2$. Then $p = 2 = 2^{p-1}$, meaning all intermediate expressions are equal too, as in

$$p = \Psi_n(a,b) = (a-b)^{\varphi(n)} = (a-b)^{p-1} = 2^{p-1}.$$

Then

$$\varphi(n) = p - 1 = 2 - 1 = 1,$$

contradicting the fact that $\varphi(n) \geq 2$ under our assumption of $n \geq 3$. So it is impossible that $a - b \geq 2$.

(b) Now we know that $a - b = 1$. Recall that $n = p^t k$ where p is the largest prime factor of n, and t and k are a positive integers such that $p \nmid k$. We will break our analysis of n up into the cases $t \geq 2$ and $t = 1$.

i. Suppose $t \geq 2$. By Lemma 13.33 and the lower bound in Lemma 13.37,

$$\begin{aligned} p &\geq \Psi_n(a,b) \\ &= \Psi_{p^t k}(a,b) \\ &= \Psi_{p^{t-1}k}(a^p, b^p) \\ &\geq (a^p - b^p)^{\varphi(p^{t-1}k)} \\ &\geq a^p - b^p. \end{aligned}$$

Using the substitution $a = b + 1$, we can further weaken the lower bound to

$$\begin{aligned} p &\geq a^p - b^p \\ &= (b+1)^p - b^p \\ &= \sum_{j=0}^{p-1} \binom{p}{j} b^j \\ &\geq 1 + pb \\ &\geq p + 1. \end{aligned}$$

Though this is exceedingly weak, it still gives us the contradiction $p \geq p + 1$. Thus, the $t \geq 2$ case is impossible.

ii. Now we know that $t = 1$, causing $n = pk$ where $p \nmid k$. We still have the stated goal of getting a lower bound for p purely in terms of p. Using Lemma 13.33, using both the lower and upper bounds in Lemma 13.37, and using the sub-

stitution $a = b + 1$,

$$\begin{aligned} p &\geq \Psi_n(a,b) \\ &= \Psi_{pk}(a,b) \\ &= \frac{\Psi_k(a^p,b^p)}{\Psi_k(a,b)} \\ &\geq \frac{(a^p-b^p)^{\varphi(k)}}{(a+b)^{\varphi(k)}} \\ &= \left(\frac{(b+1)^p-b^p}{(b+1)+b}\right)^{\varphi(k)}. \end{aligned}$$

Since we showed above that the numerator is bounded below by $1+pb$, which is itself bounded below by $2b+1$, it means the base $\left(\frac{(b+1)^p-b^p}{(b+1)+b}\right)$ is at least 1. This allows us to use the bound $\varphi(k) \geq 1$ to get

$$p \geq \left(\frac{(b+1)^p-b^p}{(b+1)+b}\right)^{\varphi(k)} \geq \frac{(b+1)^p-b^p}{(b+1)+b}.$$

By reverse-telescoping, we find that

$$\begin{aligned} p &\geq \frac{(b+1)^p-b^p}{(b+1)+b} \\ &= \frac{\sum_{c=1}^{b}\left[(c+1)^p-c^p\right]}{2b+1} \\ &\geq \frac{\sum_{c=1}^{b}(2^p-1)}{2b+1} \\ &= \frac{b(2^p-1)}{2b+1} \\ &\geq \frac{2^p-1}{3}, \end{aligned}$$

where we used the fact that

$$(x+1)^p - x^p = \sum_{i=0}^{p-1}\binom{p}{i}x^i$$

is an increasing function for $x \geq 1$, and, in the last step, we used

$$\frac{b}{2b+1} \geq \frac{1}{3} \iff 3b \geq 2b+1 \iff b \geq 1.$$

By induction on integers $s \geq 4$, we can show that

$$\frac{2^s-1}{3} > s$$

or, more easily, $2^s > 3s + 1$. So $\dfrac{2^p - 1}{3} > p$ for all primes $p > 3$, leaving us with $p = 2$ or $p = 3$. We are working with $a - b = 1$, so a and b have opposite parities, implying $a^n - b^n$ is odd. Since $p \mid a^n - b^n$, p must be odd, which eliminates the possibility that $p = 2$ and forces $p = 3$. Much earlier, we proved that $k < p$, so $k = 1$ or $k = 2$. We consider these possibilities now.

A. Suppose $k = 1$. Then $n = pk = 3$, leading to

$$\begin{aligned} 3 = p &\geq \Psi_n(a, b) \\ &= \Psi_3(a, b) \\ &= a^2 + ab + b^2 \\ &= (b + 1)^2 + (b + 1)b + b^2 \geq 7, \end{aligned}$$

since $b \geq 1$. This is a contradiction that allows us to omit this case. Note that we used the fact that

$$\Phi_3(x) = \frac{x^3 - 1}{x - 1} = x^2 + x + 1$$

and homogenized it to get $\Psi_3(a, b)$.

B. Suppose $k = 2$. Then $n = pk = 6$, leading to

$$\begin{aligned} 3 = p &\geq \Psi_n(a, b) \\ &= \Psi_6(a, b) \\ &= a^2 - ab + b^2 \\ &= (b + 1)^2 - (b + 1)b + b^2 \\ &= b^2 + b + 1 \geq 3, \end{aligned}$$

since $b \geq 1$. By antisymmetry, $b^2 + b + 1 = 3$, solving which gives only one positive solution: $b = 1$. Then $a = b + 1 = 2$. Note that we used the fact that

$$\Phi_6(x) = \Phi_3(-x) = x^2 - x + 1$$

to get $\Psi_6(a, b)$. Therefore, we have reduced the $n \geq 3$ case to checking whether $(a, b, n) = (2, 1, 6)$ has a primitive prime divisor.

Indeed, $(a, b, n) = (2, 1, 6)$ does not have a primitive prime divisor:

$$2^6 - 1^6 = 63 = 3^2 \cdot 7,$$

so the only candidates for primitive prime divisors are 3 and 7. Yet $7 \mid 2^3 - 1^3$ and $3 \mid 2^2 - 1^2$, so both candidates fail to be a primitive prime divisor of $(2, 1, 6)$.

■

Corollary 13.40 (Zsigmondy's theorem for addition)**.** Let a and b be coprime positive integers such that $a > b$. Let $n \geq 2$ be an integer (unlike the addition cases of the LTE lemma, we do not require that n be odd here). If $(a, b, n) \neq (2, 1, 3)$, then there exists a prime divisor of $a^n + b^n$ that does not divide $a^k + b^k$ for all $k \in [n - 1]$, and also does not divide $a^k - b^k$ for all $k \in [2n - 1]$.

Proof. Suppose $(a,b,n) \neq (2,1,3)$. Then $(a,b,2n) \neq (2,1,6)$. Recall that the cases of Zsigmondy for which there might be no primitive prime divisors are (a,b,n) such that:

$$\begin{aligned}(a,b,m) &= (2,1,6),\\ m &= 2, \exists t \in \mathbb{Z}_+ : a+b = 2^t.\end{aligned}$$

Since it is assumed that $n \geq 2$, we get $2n \geq 4 > 2$, so $(a,b,2n)$ also does not satisfy the condition for the second exception. By Zsigmondy, since both exceptions have been eliminated, that means $(a,b,2n)$ has a primitive prime divisor p. So p satisfies

$$p \mid a^{2n} - b^{2n} = (a^n - b^n)(a^n + b^n),$$

but $p \nmid a^k - b^k$ for all $k \in [2n-1]$. Then since $n \in [2n-1]$, this implies that $p \nmid a^n - b^n$. By Euclid's lemma, $p \mid a^n + b^n$. So it is candidate for our desired prime. This turns out to be the case because $2k \in [2n-1]$ for all $k \in [n-1]$, so

$$p \nmid a^{2k} - b^{2k} = (a^k - b^k)(a^k + b^k)$$

for all $k \in [n-1]$. By the contrapositive of Euclid's lemma,

$$p \nmid a^k + b^k$$

for all $k \in [n-1]$.
In the exceptional case, $(a,b,n) = (2,1,3)$, we can check that $a^n + b^n = 2^3 + 1^3 = 9 = 3^2$ has only 3 as a prime factor, but $3 \mid a + b = 3$ as well. ■

Unlike the LTE lemma, the proof of Zsigmondy (and its addition version) was long and difficult, requiring more than just a few basic principles. As such, we recommend memorizing the result over remembering the proof.

Problem 13.41. Prove that, for all integers $a \geq 2$ and $n \geq 3$ such that $(a,b) \neq (2,6)$, there exists a prime p such that $\operatorname{ord}_p(a) = n$. What goes wrong with $(a,b) = (2,6)$? Also, give an example of an integer $a \geq 2$ that fails for $n = 2$.

Problem 13.42. Strengthen Zsigmondy's theorem for addition as follows. Let p be a prime and a, b be coprime positive integers such that $a > b$. Let $n \geq 2$ be an integer and p be a prime divisor of $a^n + b^n$ that does not divide $a^k + b^k$ for all $k \in [n-1]$. Prove that $p \nmid a^k + b^k$ for all $k = n+1, n+2, \ldots, 3n-1$. As a hint, you might need Problem 9.25.

Example 13.43. Let n be a positive integer and $p_1, p_2, \ldots, p_n$ be distinct primes greater than or equal to 5. Prove that $2^{p_1 p_2 \cdots p_n} + 1$ has at least 2^{2^n} positive divisors.

Solution. Let n and the p_i be as stated. Note that $p_i \neq 2, 3$ since $p_i \geq 5$ for all $i \in [n]$, so all of the p_i are odd, and $q = p_1 p_2 \cdots p_n$ is odd and not divisible by 3. Since $a + b \mid a^k + b^k$ for all positive integers a, b, and k such that k is odd, it tells us that $2^d + 1 \mid 2^q + 1$ for every positive divisor d of q. Let the positive divisors of q, in ascending order, be

$$1 = d_1 < d_2 < \cdots < d_{\tau(q)} = q,$$

where

$$\tau(q) = \tau(p_1 p_2 \cdots p_n) = 2^n.$$

Each triple $(2, 1, d_i)$ has $3 \nmid d_i$ and so $d_i \neq 3$. By Zsigmondy's theorem, for each $i \in [2^n]\backslash\{1\}$, there exists a prime r_i such that $r_i \mid 2^{d_i} + 1$ but $r_i \nmid 2^{d_j} + 1$ for each $j \in [i-1]$. Note that we have intentionally excluded $i = 1$ for now because here $i - 1 = 0$ so the set $[i-1]$ does not exist. Going through

$$i = 2, 3, \ldots, 2^n - 1, 2^n$$

produces a new prime r_i each time that was not previously in this list of primes and that divides $2^q + 1$. The reason that each r_i is distinct is that if $r_{i_1} = r_{i_2}$ for some indices $i_1, i_2 \in [2^n]\backslash\{1\}$ such that $i_1 < i_2$, then the fact that $r_{i_1} \mid 2^{d_{i_1}} - 1$ would contradict the fact that $r_{i_2} \nmid 2^{d_{i_1}} - 1$. Finally, $3 = 2^{d_1} + 1$ is the last new prime in the coffin that divides $2^q - 1$, and it is new because otherwise there would exist an $r_i = 3$ for $i \geq 2$ that divides $2^{d_1} - 1$. ■

Problem 13.44. Let $a, b, n \in \mathbb{Z}_+$ such that a, b are coprime and $2 \nmid n$ and $3 \nmid n$. Prove that:

1. If $a - b \geq 1$, then
$$\tau(a^n + b^n) \geq 2^{\tau(n)}.$$
2. If $a - b \geq 2$, then
$$\tau(a^n - b^n) \geq 2^{\tau(n)}.$$

Appendices

Appendix A

Solutions

> "Philosophers and psychiatrists should explain why it is that we mathematicians are in the habit of systematically erasing our footsteps. Scientists have always looked askance at this strange habit of mathematicians, which has changed little from Pythagoras to our day."
>
> – *Gian-Carlo Rota*

Solution 1.8. The representation in the first part will help to prove the second and third parts.

1. Let n be an integer. By definition, the even integers are produced by conjoining the arithmetic sequences $(2m)_{m=0}^{\infty}$ and $(2(-m))_{m=1}^{\infty}$. So n is an even integer if and only if n is a multiple of 2. The odd integers are produced by conjoining the arithmetic sequences $(2m-1)_{m=1}^{\infty}$ and $(2(-m)-1)_{m=0}^{\infty}$. So n is odd if and only if n is one less than a multiple of 2. Since

   $$n = 2m - 1 = 2(m-1) + 1,$$

   the other representation works too.

2. Let $2n_1, 2n_2, \ldots, 2n_k$ be even integers. Then their sum

   $$2n_1 + 2n_2 + \cdots + 2n_k = 2(n_1 + n_2 + \cdots + n_k)$$

   is also even. Let $2n_1 - 1, 2n_2 - 1, \ldots, 2n_k - 1$ be odd integers. Then their sum is

   $$(2n_1 - 1) + (2n_2 - 1) + \cdots + (2n_k - 1) = 2(n_1 + n_2 + \cdots + n_k) - k,$$

   which is even if k is even and odd if k is odd.

3. Multiplying an even integer $2n$ by any other integers will produce an even integer because the factor of 2 will remain. It can be proven by induction on integers $k \geq 1$ that the product of odd integers is odd. The inductive step is

   $$(2n+1)(2m+1) = 4mn + 2n + 2m + 1 = 2(2mn + n + m) + 1.$$

Solution 1.14. Since $\gcd(a, 0) \mid a$, we know that $(a, 0) \leq |a|$. But $|a|$ is a common divisor of a and 0, so $|a| \leq (a, 0)$, since $(a, 0)$ is the *greatest* among common divisors. By antisymmetry, $(a, 0) = |a|$. It follows that $(a, 0) = 1$ if and only if $|a| = 1$ if and only if $a = \pm 1$.

Solution 1.15. Let n be an integer. If d is a positive common divisor of n and $n+1$, then d also divides their linear combination $(n+1)\cdot 1 + n\cdot(-1) = 1$. So $d = 1$, which means $\gcd(n, n+1) = 1$.
If c is a positive common divisor of n and $n+2$, then c also divides their linear combination $(n+2)\cdot 1 + n\cdot(-1) = 2$. Since 2 is a prime, $c = 1$ or $c = 2$. Thus, $\gcd(n, n+2) \leq 2$. If n is odd, then $2 \nmid n$, so $c = 1$, in which case $\gcd(n, n+2) = 1$. If n is even, then $2 \mid n$ and $2 \mid n+2$, so $\gcd(n, n+2) \geq 2$. By antisymmetry, $\gcd(n, n+2) = 2$.
If these arguments seem a bit too elaborate to be of practical use, it should be gladdening to know that we will see a much faster way of computing the greatest common divisor of two integers, called the Euclidean algorithm.

Solution 1.20. For one direction, suppose $(a, bc) = 1$. By Bézout's lemma, there exist integers x and y such that $ax + bcy = 1$. Two other ways of writing this equation are

$$\begin{aligned} ax + b(cy) &= 1 \\ ax + c(by) &= 1, \end{aligned}$$

so $(a, b) = 1$ and $(a, c) = 1$ as well.
Conversely, suppose $(a, b) = 1$ and $(a, c) = 1$. By Bézout's lemma, there exist integers x, y, u, v such that

$$\begin{aligned} ax + by &= 1, \\ au + cv &= 1. \end{aligned}$$

Multiplying these two equations together and collecting the terms strategically yields

$$a(axu + cxv + byu) + b(cyv) = (ax + by)(au + cv) = 1.$$

This is a linear combination of a and bc that equals 1, so $(a, bc) = 1$.

Solution 1.26. Since

$$\begin{aligned} 2^m - 1 \mid (2^m - 1)(2^m + 1) = 2^{2m} - 1, \\ 2^n - 1 \mid (2^n - 1)(2^n + 1) = 2^{2n} - 1, \end{aligned}$$

we know that

$$(2^m - 1, 2^n - 1) \mid (2^{2m} - 1, 2^{2n} - 1) = 2^{(2m,2n)} - 1 = 4^{(m,n)} - 1 \mid 3,$$

where we used Example 1.25. On the other hand, since m, n are both odd, $3 \mid 2^m + 1$ and $3 \mid 2^n + 1$, so $3 \mid (2^m + 1, 2^n + 1)$. We conclude that $(2^m + 1, 2^n + 1) = 3$ from the antisymmetry of divisibility.

Solution 1.29. We will use the matrices $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ and $N = \begin{pmatrix} p & q \\ r & s \end{pmatrix}$. Their product is

$$M \cdot N = \begin{pmatrix} ap + br & aq + bs \\ cp + dr & cq + ds \end{pmatrix}.$$

We find that

$$\begin{aligned}\det(M \cdot N) &= (ap+br)(cq+ds) - (aq+bs)(cp+dr) \\ &= adps + bcqr - adqr - bcps \\ &= (ad-bc)(ps-qr) \\ &= \det(M) \cdot \det(N).\end{aligned}$$

Solution 2.11. One example is that $18 = 6 \cdot 3$: even though both $3 \mid 12$ and $6 \mid 12$, it is not true that $18 \mid 12$.

Solution 2.13. For any non-negative integer exponent t, it holds that $1^t = 1$. So if 1 were a prime then, for example, both $1^2 \cdot 2^1$ and $1^3 \cdot 2^1$ would be prime factorizations of 2. This would prevent prime factorizations from being unique, which would cause issues in proofs that rely on the uniqueness of this representation.

Solution 2.16. This statement is untrue. For example, $8 < 10$ but $\nu_2(8) = 3 > 1 = \nu_2(10)$.

Solution 2.20. As shown in the proof of Theorem 2.19, it is true in general that

$$(a,c)(b,c) = (ab, c(a,b,c)).$$

Since $(a,c) = 1$, and as a result, $(a,b,c) = 1$, it holds that $(b,c) = (ab,c)$.

Solution 2.21. It is easy to verify that the first identity holds if $a = 0$. So we may now assume that a, b, c are all non-zero. By the prime factorization formulas for gcd and lcm, it suffices to prove that

$$\begin{aligned}\min(x, \max(y,z)) &= \max(\min(x,y), \min(x,z)), \\ \max(x, \min(y,z)) &= \min(\max(x,y), \max(x,z)).\end{aligned}$$

Both identities are symmetric in y and z, so we may assume without loss of generality that $y \leq z$. Thus, it suffices to prove that, in this case,

$$\begin{aligned}\min(x,z) &= \max(\min(x,y), \min(x,z)), \\ \max(x,y) &= \min(\max(x,y), \max(x,z)).\end{aligned}$$

We leave it to the reader to manually verify that these two identities hold in the three possible orderings:

$$\begin{aligned}x \leq y \leq z, \\ y \leq x \leq z, \\ y \leq z \leq x,\end{aligned}$$

which have been found by considering the possible locations of x relative to y and z on the number line.

Solution 3.6. As we saw when finding a formula for the π function in Example 3.5, the positive divisors of n^2 (which is a square), excluding $\sqrt{n^2} = n$, split into $\dfrac{\tau(n^2)-1}{2}$ disjoint unordered pairs of distinct divisors $\{c, d\}$ such that $cd = n^2$. Since c and d are distinct, we label them as c and d so that $c < d$. Recall from the proof of the square root primality test (Theorem 2.6) that $c < n < d$ because otherwise $cd < n$ or $cd > n$. Thus, exactly one element c of each pair is less than n, and the answer is the number of pairs $\dfrac{\tau(n^2)-1}{2}$.
As a side note, this proof used the special form of complementary counting that we mentioned briefly as a problem after the subtraction principle in combinatorics. We also used bijective counting here.

Solution 3.7. If 2 does not divide n, then there are no even divisors, so the answer is $0 = \nu_2(n)$. If $\nu_2(n) > 0$, then let E be the non-empty set of even positive divisors of n, and O be the set of odd positive divisors of n which is also non-empty due to the trivial divisor 1. The idea is that we can construct all of the even positive divisors by multiplying each odd positive divisor by each power of 2 that divides n. Formally, we define a map

$$\begin{aligned} f : E &\to O \\ d &\mapsto \frac{d}{2^{\nu_2(d)}}, \end{aligned}$$

which shears off all powers of 2 from the prime factorization of d. This is a $\nu_2(n)$-to-1 correspondence because for each odd positive divisor q of n, there are $\nu_2(n)$ even positive divisors of n that map to q: that is, q times 2^t for each $t \in [\nu_2(n)]$. By the k-to-1 correspondence principle from combinatorics,

$$|O| = \frac{|E|}{\nu_2(n)} \implies \frac{|E|}{|O|} = \nu_2(n),$$

which is the ratio that we wanted to see.

Solution 3.15. We compute these summation functions as follows for all positive integers n:

$$\begin{aligned} S_\varepsilon(n) &= \sum_{d|n} \varepsilon(d) = \varepsilon(1) = 1, \\ S_1(n) &= \sum_{d|n} 1(d) = \sum_{d|n} 1 = \tau(n), \\ S_{\mathrm{Id}}(n) &= \sum_{d|n} \mathrm{Id}(d) = \sum_{d|n} d = \sigma(n). \end{aligned}$$

Thus, $S_\varepsilon = 1, S_1 = \tau$, and $S_{\mathrm{Id}} = \sigma$.

Solution 3.17. Let a and b be positive integers. We wish to show that $\varepsilon(ab) = \varepsilon(a)\varepsilon(b)$ and, if $(a, b) = 1$ then $\mu(ab) = \mu(a)\mu(b)$. If either of a, b is not equal to 1, then $ab \neq 1$ and

$$\varepsilon(ab) = 0 = \varepsilon(a)\varepsilon(b).$$

If $a = b = 1$, then

$$\varepsilon(ab) = \varepsilon(1) = 1 = 1 \cdot 1 = \varepsilon(1)\varepsilon(1) = \varepsilon(a)\varepsilon(b).$$

Now suppose a and b are coprime. If either of a, b is non-squarefree, then ab is non-squarefree and

$$\mu(ab) = 0 = \mu(a)\mu(b).$$

If a and b are both squarefree then, using the fact that a and b are coprime, ab is squarefree, and

$$\mu(ab) = (-1)^{\omega(ab)} = (-1)^{\omega(a)+\omega(b)} = (-1)^{\omega(a)} \cdot (-1)^{\omega(b)} = \mu(a)\mu(b).$$

Here, we have used the additivite property of the ω function.

Solution 3.19. Attempting to deduce this from the Möbius inversion formula by taking real logarithms does not work because arithmetic functions may be complex-valued. We have to prove the result from scratch. Suppose

$$g(n) = \prod_{d|n} f(d).$$

By substitution, we compute

$$\begin{aligned}
\prod_{d|n} g\left(\frac{n}{d}\right)^{\mu(d)} &= \prod_{d|n} \left(\prod_{c|\frac{n}{d}} f(c) \right)^{\mu(d)} = \prod_{d|n} \prod_{c|\frac{n}{d}} f(c)^{\mu(d)} \\
&= \prod_{\substack{(d,c,b)\in[n]^3 \\ dcb=n}} f(c)^{\mu(d)} \\
&= \prod_{c|n} \prod_{d|\frac{n}{d}} f(c)^{\mu(d)} = \prod_{c|n} f(c)^{\sum_{d|\frac{n}{c}} \mu(d)} = \prod_{c|n} f(c)^{S_\mu\left(\frac{n}{c}\right)} \\
&= f(n),
\end{aligned}$$

where we used the fact that $S_\mu = \varepsilon$ in the final step.
For the other direction, suppose

$$f(n) = \prod_{d|n} g\left(\frac{n}{d}\right)^{\mu(d)}.$$

By substitution, we compute

$$\begin{aligned}
\prod_{d|n} f(d) &= \prod_{d|n} \prod_{c|d} g\left(\frac{d}{c}\right)^{\mu(c)} \\
&= \prod_{\substack{(b,c,a)\in[n]^3 \\ bca=n}} g\left(\frac{bc}{c}\right)^{\mu(c)} = \prod_{\substack{(b,c,a)\in[n]^3 \\ bca=n}} g(b)^{\mu(c)} \\
&= \prod_{b|n} \prod_{c|\frac{n}{b}} g(b)^{\mu(c)} \\
&= \prod_{b|n} g(b)^{\sum_{c|\frac{n}{b}} \mu(c)} = \prod_{b|n} g(b)^{S_\mu\left(\frac{n}{b}\right)} = g(n),
\end{aligned}$$

where we used the fact that $S_\mu = \varepsilon$ again at the end.

Solution 3.22. By Problem 3.15, Theorem 3.21, and the associativity of the Dirichlet convolution,

$$\varphi * \tau = \varphi * (1 * 1) = (\varphi * 1) * 1 = \mathrm{Id} * 1 = \sigma.$$

Solution 3.23. By Bézout's lemma, k is a positive common divisor of a and b if and only if k is a positive divisor of $\gcd(a, b)$. So

$$\sum_{k|a \text{ and } k|b} \varphi(k) = \sum_{k|\gcd(a,b)} \varphi(k).$$

This is the summation function of φ evaluated at $\gcd(a, b)$, so the result follows from Theorem 3.21.

Solution 3.29. In the proof of Corollary 3.28, we proved that, if p denotes only primes, then

$$\prod_{p|(a,b)} \left(1 - \frac{1}{p}\right) \cdot \prod_{p|[a,b]} \left(1 - \frac{1}{p}\right) = \prod_{p|a} \left(1 - \frac{1}{p}\right) \cdot \prod_{p|b} \left(1 - \frac{1}{p}\right).$$

By applying the second formula for φ, we get that this is equivalent to

$$\frac{\varphi((a, b))}{(a, b)} \cdot \frac{\varphi([a, b])}{[a, b]} = \frac{\varphi(a)}{a} \cdot \frac{\varphi(b)}{b}.$$

By using the identity $(a, b) \cdot [a, b] = ab$, we can clear the denominators to get

$$\varphi((a, b)) \cdot \varphi([a, b]) = \varphi(a) \cdot \varphi(b).$$

Solution 4.7. The method is to use induction on the degree of the polynomial, The base case of constant polynomials clearly holds. Suppose the result holds for polynomials of degree $m - 1$. Now let

$$f(x) = c_m x^m + c_{m-1} x^{m-1} + \cdots + c_2 x^2 + c_1 x + c_0$$

be a polynomial of degree m and suppose

$$a \equiv b \pmod{n}$$

We can use Theorem 4.6 to get

$$\begin{aligned} a^m &\equiv b^m \pmod{n} \\ c_m a^m &\equiv c_m b^m \pmod{n}. \end{aligned}$$

By the induction hypothesis,

$$c_{m-1} a^{m-1} + \cdots + c_2 a^2 + c_1 a + c_0 \equiv c_{m-1} b^{m-1} + \cdots + c_2 b^2 + c_1 b + c_0 \pmod{n}.$$

All we have to do is add the two congruences now, which is a valid operation, as shown in Theorem 4.6.

Solution 4.8. The congruence $1 \equiv -1 \pmod{n}$ is equivalent to $1 + 1 \equiv 2 \equiv 0 \pmod{n}$, which is equivalent to $n \mid 2$. Thus, $n = 1$ or $n = 2$, both of which work.

Solution 4.10. By difference of squares, this congruence is equivalent to

$$(x - a)(x + a) \equiv 0 \pmod{p}.$$

So the prime p divides $(x - a)(x + a)$. By Euclid's lemma, $p \mid x - a$ or $p \mid x + a$. Thus, $x \equiv \pm a \pmod{p}$. The converse holds as well because these congruences can be squared, so this criterion is biconditional. As a side note, these two possibilities are the same if and only if $a \equiv -a \pmod{p}$ if and only if p divides $2a$ if and only if $p = 2$ or $p \mid a$ by Euclid's lemma again.
Also note the special case: $a^2 \equiv 1 \pmod{p}$ if and only if $a \equiv \pm 1 \pmod{p}$. This case comes up from time to time because, as we will see in a moment, this classifies the integers that are multiplicative "self-inverses" modulo the prime p.

Solution 4.16. Assuming $d \mid n$, we will prove the negation of the statement, which is that $a \equiv b \pmod{d}$ and $a \not\equiv b \pmod{n}$. We need to construct integers a and b. Let $a = d + 1$ and $b = 1$ so that

$$a - b \equiv 0 \pmod{d},$$

yet $0 < a - b = d < n$. There is no multiple of n in the open interval $(0, n)$, so it is impossible that $n \mid a - b$.

Solution 4.21. Since the result is about congruence modulo n, we may assume without loss of generality that R is the least reduced residue system modulo n. Reminiscent of Gauss's trick for summing an arithmetic series, the idea is to use the pairing that results from the observation

$$a \in R \iff (a, n) = 1 \iff (n - a, n) \in R.$$

So we can pair up elements of R as a and $n - a$. Since the sum of each pair is n and the number of pairs is $\dfrac{\varphi(n)}{2}$ (Corollary 3.30 showed that $\varphi(n)$ is always even for $n \geq 3$),

$$\sum_{r \in R} r \equiv n \cdot \frac{\varphi(n)}{2} \equiv 0 \pmod{n}.$$

The only possible snag is that a and $n - a$ might not be distinct modulo n. We will show that this cannot happen. If they were congruent, then

$$a \equiv n - a \pmod{n} \implies 2a \equiv 0 \pmod{n} \implies n \mid 2,$$

where the last implication uses the fact that $(n, a) = 1$. This contradicts the assumption that $n \geq 3$. Thus, the result holds. Incidentally, we have proven the stronger result that

$$\sum_{\substack{k \in [n] \\ (k,n)=1}} k = n \cdot \frac{\varphi(n)}{2}$$

for all integers $n \geq 3$.

Solution 4.23. The rational numbers $\dfrac{p \pm 1}{2}$ are integers because p is an odd integer, which makes $p \pm 1$ divisible by 2. The idea is to pair up the multiplicands in the expression $(p-1)!$ from Wilson's theorem in a style reminiscent of Gauss's pairing trick for an arithmetic series:

$$\begin{aligned} -1 \equiv (p-1)! &\equiv [1 \cdot (p-1)] \cdot [2 \cdot (p-2)] \cdots \left[\frac{p-1}{2} \cdot \frac{p+1}{2}\right] \\ &\equiv \prod_{k=1}^{\frac{p-1}{2}} k(p-k) \equiv \prod_{k=1}^{\frac{p-1}{2}} -k^2 \\ &\equiv (-1)^{\frac{p-1}{2}} \cdot \left[\left(\frac{p-1}{2}\right)!\right]^2 \pmod{p}, \end{aligned}$$

which leads to the desired congruence after multiplying both sides by $(-1)^{\frac{p-1}{2}}$.

Solution 4.26. Suppose $\varphi(n)$ divides $i - j$. By Euler's congruence,

$$a^{\varphi(n)} \equiv 1 \pmod{n}$$

because a is coprime to n. Since $\dfrac{i-j}{\varphi(n)}$ is an integer,

$$a^{i-j} \equiv (a^{\varphi(n)})^{\frac{i-j}{\varphi(n)}} \equiv 1 \pmod{n},$$

so $a^i \equiv a^j \pmod{n}$.
For the application, we can find the remainder of $(12-7)^{202} = 5^{202}$ instead. Note that $\varphi(7) = 6$ and $202 \equiv 4 \pmod{6}$. Since the base 5 is coprime to the modulus 7,

$$5^{202} \equiv 5^4 \equiv (25)^2 \equiv 4^2 \equiv 2 \pmod{7}.$$

So the remainder is 2. This idea of reducing bases via Euclidean division by the modulus and reducing exponents using Euler's congruence is very effective in computations.

Solution 4.31. Let b be an integer that is coprime to 561. Then none of the prime factors $3, 11, 17$ of 561 divide b. By Fermat's little theorem,

$$\begin{aligned} b^2 &\equiv 1 \pmod{3}, \\ b^{10} &\equiv 1 \pmod{11}, \\ b^{16} &\equiv 1 \pmod{17}. \end{aligned}$$

Since $\operatorname{lcm}(2, 10, 16) = 80$, we may raise these congruences to higher powers to get

$$\begin{aligned} b^{80} &\equiv (b^2)^{40} \equiv 1 \pmod{3}, \\ b^{80} &\equiv (b^{10})^8 \equiv 1 \pmod{11}, \\ b^{80} &\equiv (b^{16})^5 \equiv 1 \pmod{17}. \end{aligned}$$

So $b^{80} - 1$ is divisible by $3 \cdot 11 \cdot 17 = 561$ because these three primes are pairwise relatively prime. Thus,

$$\begin{aligned} b^{80} &\equiv 1 \pmod{561}, \\ b^{560} &\equiv (b^{80})^7 \equiv 1 \pmod{561}. \end{aligned}$$

This proves that 561 is a Carmichael number.

Solution 4.32. Suppose n is a composite integer such that $\varphi(n) \mid n - 1$. By Euler's congruence, for any integer a that is coprime to n,

$$a^{\varphi(n)} \equiv 1 \pmod{n}.$$

Since $\dfrac{n-1}{\varphi(n)}$ is an integer by assumption,

$$a^{n-1} \equiv (a^{\varphi(n)})^{\frac{n-1}{\varphi(n)}} \equiv 1 \pmod{n}.$$

Thus, n is a Carmichael number.

Solution 5.8. If $n - p$ divides n, then there exists an integer k such that

$$(n-p)k = n$$

Rearranging, this is equivalent to

$$\begin{aligned} (n-p)k &= (n-p) + p, \\ (n-p)(k-1) &= p. \end{aligned}$$

So $n = a + p$, where a is any factor of p. Since p is a prime, its only factors are $1, -1, p, -p$. Therefore, the only possible values of n are

$$p + 1, p - 1, 2p, 0,$$

all of which can be verified to work.

Solution 5.12. There is a confluence of good indicators with the prime modulus 7:

- By Fermat's little theorem, x^6 can only be 0 or 1 modulo 7.
- The exponent 3 is a Sophie Germain prime whose corresponding safe prime is 7, so y^3 can only be $-1, 0, 1$ modulo 7.
- The coefficient 6 does not disappear modulo 7, but we can replace it with -1, which will simplify computations a bit.

Trying out all six possible elements of

$$(x^6, y^3) \in \{0, 1\} \times \{-1, 0, 1\},$$

we get the possibilities

$$x^6 - 6y^3 \equiv x^6 + y^3 \equiv \begin{cases} -1 \pmod 7 & \text{if } (x^6, y^3) \equiv (0, -1), \\ 0 \pmod 7 & \text{if } (x^6, y^3) \equiv (0, 0), \\ 1 \pmod 7 & \text{if } (x^6, y^3) \equiv (0, 1), \\ 0 \pmod 7 & \text{if } (x^6, y^3) \equiv (1, -1), \\ 1 \pmod 7 & \text{if } (x^6, y^3) \equiv (1, 0), \\ 2 \pmod 7 & \text{if } (x^6, y^3) \equiv (1, 1), \end{cases}$$

None of the possibilities $-1, 0, 1, 2$ are congruent to 5 modulo 7, so there is no solution in the integers to this Diophantine equation.

Solution 5.13. We will show that there are no solutions. Assume, for the sake of contradiction that (n, m, k) is an integer solution. Using the formula for binomial coefficients

$$\binom{r}{s} = \frac{r!}{s!(r - s!)}$$

and clearing the denominators, the equation is equivalent to

$$m(m-1)(m-2)(m-3) = 24(n^2 + 2 + 7k).$$

A technique of which the reader should be aware is that, when there is a product or sum of consecutive integers like $m(m-1)(m-2)(m-3)$, it can be fruitful to translate the variable to be the average of those numbers. With sums, this produces cancellations, and with products this produces differences of squares. In this case, the average is

$$a = \frac{m + (m-1) + (m-2) + (m-3)}{4} = m - \frac{3}{2}.$$

By substitution, the left side becomes

$$\begin{aligned} m(m-1)(m-2)(m-3) &= \left(a + \frac{3}{2}\right)\left(a + \frac{1}{2}\right)\left(a - \frac{1}{2}\right)\left(a - \frac{3}{2}\right) \\ &= \left(a^2 - \frac{9}{4}\right)\left(a^2 - \frac{1}{4}\right) \\ &= a^4 - \frac{5}{2}a^2 + \frac{9}{16} \\ &= \left(a^2 - \frac{5}{4}\right)^2 - 1, \end{aligned}$$

where we completed the square in the variable a^2 in the last step. Popping $a = m - \frac{3}{2}$ back in turns the equation into

$$(m^2 - 3m + 1)^2 - 1 = 24(n^2 + 2 + 7k),$$

which we can rearrange into

$$(m^2 - 3m + 1)^2 = 24n^2 + 7(24k + 7).$$

This looks like a job for the modulus of 7, which produces the congruence

$$(m^2 - 3m + 1)^2 \equiv 3n^2 \pmod 7.$$

The squares modulo 7 are $0, 1, 2, 4$, so the only way that one square is three times another square modulo 7 is if both are divisible by 7. This means that

$$m^2 - 3m + 1 \equiv 0 \pmod 7.$$

By adding $7m + 3 \equiv 3 \pmod 7$ to the congruence, and then completing the square in m on the left side, the congruence is equivalent to

$$(m + 2)^2 \equiv 3 \pmod 7.$$

None of the squares modulo 7 are congruent to 3, so we have our contradiction and there are no integer solutions.

Solution 5.15. We can algebraically verify that

$$\begin{aligned}(m^2 - n^2)^2 + (2mn)^2 &= m^4 - 2m^2n^2 + n^4 + 4m^2n^2 \\ &= m^4 + 2m^2n^2 + n^4 \\ &= (m^2 + n^2)^2.\end{aligned}$$

For the counterexample, note that if

$$(a, b, c) = (m^2 - n^2, 2mn, m^2 + n^2)$$

is a Pythagorean triple, then $\dfrac{c + a}{2} = m^2$ needs to be a square. In the most basic example $(3, 4, 5)$ we find that $\dfrac{5 + 3}{2} = 2^2$. But scaling it up by a factor of 2 yields $(6, 8, 10)$, in which case $\dfrac{10 + 6}{2} = 2^3$ is not a square. Thus, $(6, 8, 10)$ is not captured by Euclid's formula.

Solution 5.16. In the sufficient direction, it is straightforward to verify that such a triple actually forms a Pythagorean triple because

$$(2k + 1)^2 + (2k(k + 1))^2 = (2k(k + 1) + 1)^2.$$

We leave the details of the computation to the reader. The necessary direction is a bit more involved. If $c = b + 1$ in a Pythagorean triple (a, b, c), then the equation

$$a^2 + b^2 = (b + 1)^2$$

can be reduced to $a^2 = 2b+1$. So a^2 is odd, which means a is odd. Let k be the non-negative integer such that $a = 2k + 1$. Then

$$b = \frac{a^2 - 1}{2} = \frac{(2k + 1)^2 - 1}{2} = 2k(k + 1).$$

Thus,

$$c = b + 1 = 2k(k+1) + 1.$$

A point that is easily missed is that we must show that k cannot be 0, thereby proving that k is positive. Indeed, if $k = 0$, then $b = 2k(k+1) = 0$, which is not acceptable in a Pythagorean triple.

Solution 5.19. We can observe that $(0, 0, 0)$ is a solution. Suppose, for the sake of contradiction that there exists a solution with $z \neq 0$. We are picking z because if we can force z to be 0, then x and y must also be zero, since the sum of some squares equals zero if and only if each number being squared is itself zero. Since the variables are being squared, we may assume that $z > 0$.
The left side of the equation is divisible by 2, so $2 \mid z$. Let z_0 be the integer such that $z = 2z_0$. Then the equation becomes

$$6x^2 + 2y^2 = 4z_0^2 \implies 3x^2 + y^2 = 2z_0^2.$$

Modulo 3, this equation becomes the congruence

$$y^2 - 2z_0^2 \equiv 0 \pmod 3.$$

The only squares modulo 3 are 0 and 1. Trying out all four possible elements of

$$(y^2, z_0^2) \in \{0, 1\} \times \{0, 1\},$$

we get the possibilities

$$y^2 - 2z_0^3 \equiv y^2 + z_0^3 \equiv \begin{cases} 0 \pmod 3 & \text{if } (y^2, z_0^2) \equiv (0, 0), \\ 1 \pmod 3 & \text{if } (y^2, z_0^2) \equiv (0, 1), \\ 1 \pmod 3 & \text{if } (y^2, z_0^2) \equiv (1, 0), \\ 2 \pmod 3 & \text{if } (y^2, z_0^2) \equiv (1, 1). \end{cases}$$

So the only way that $y \equiv 2z_0^2 \pmod 3$ is if y and z_0 are each divisible by 3. Let y_1 be the integer such that $y = 3y_1$, and z_1 be the integer such that $z_0 = 3z_1$. This turns the equation into

$$3x^2 + 9y_1^2 = 18z_1^2 \implies x^2 + 3y_1^2 = 6z_1^2.$$

Then $3 \mid x$, so let x_1 be the integer such that $x = 3x_1$. Then the equation becomes

$$9x_1^2 + 3y_1^2 = 6z_1^2 \implies 3x_1^2 + y_1^2 = 2z_1^2.$$

But this is in the same form as the first equation that we derived by dividing the original equation by 2 to get $3x^2 + y^2 = 2z_0^2$. So we multiply our latest equation by 2 to finally get

$$6x_1^2 + 2y_1^2 = (2z_1)^2.$$

Going back through the substitutions, we find that

$$(x_1, y_1, 2z_1) = \left(\frac{x}{3}, \frac{y}{3}, \frac{2z_0}{3}\right) = \left(\frac{x}{3}, \frac{y}{3}, \frac{z}{3}\right).$$

This is a solution to the original equation where the third variable $2z_1 = \dfrac{z}{3}$ is strictly smaller than z. We can thus find an infinitely descending set of solutions with the third variable equal to

$$z, \frac{z}{3}, \frac{z}{3^2}, \frac{z}{3^3}, \dots.$$

These are all integers only if $z = 0$. Therefore $z = 0$, which leads to $x = y = 0$ too.
As is often the case when infinite descent is applied to Diophantine equations, this argument involved an infinite sequence of divisions. Moreover, note that this solution nicely combined infinite descent with the essence of the modular arithmetic contradiction trick.

Solution 5.21. Let $(x, y) = (a, b) \in \mathbb{Z}_+^2$ be a solution to $\dfrac{x^2 + y^2}{xy - 1} = k \neq 5$ that minimizes $x + y$. Due to the symmetry of x and y in the equation, we may assume without loss of generality that $a \geq b$. Suppose, for contradiction, that $a = b$. Then

$$\begin{aligned} \frac{2a^2}{a^2 - 1} = k &\implies 2a^2 = ka^2 - k \\ &\implies k = (k-2)a^2 \\ &\implies k - 2 \mid k. \end{aligned}$$

Since $k - 2 < k$, we get $k - 2 \leq \dfrac{k}{2}$, as half of k is an upper bound on proper divisors of k. Then

$$k - 2 \leq \frac{k}{2} \implies 2k - 4 \leq k \implies k \leq 4,$$

leaving us with the possibilities $k = 1, 2, 3, 4$. In the respective cases, $a^2 = \dfrac{k}{k-2}$ is -1, undefined, 3 and 2, none of which are squares. Thus, we know that $a > b$ or, equivalently, $a \geq b + 1$.
Now we manipulate

$$\begin{aligned} \frac{x^2 + y^2}{xy - 1} = k &\implies x^2 + y^2 = kxy - k \\ &\implies x^2 + (-ky)x + (y^2 + k) = 0. \end{aligned}$$

For $y = b$, a solution to the quadratic

$$x^2 + (-kb)x + (b^2 + k) = 0$$

is $x = a$. There must exist a second solution $x = c \in \mathbb{C}$ such that, by Vieta's formulas,

$$\begin{aligned} a + c &= kb \\ ac &= b^2 + k. \end{aligned}$$

The former tells us that

$$c = kb - a \in \mathbb{Z}$$

and the latter proves that

$$c = \frac{b^2 + k}{a} > 0$$

(since a is positive, it is non-zero, so we were able to divide by it). Combining the two, we get $c \in \mathbb{Z}_+$. We will prove that the solution $(x, y) = (c, b)$ undercuts $(x, y) = (a, b)$ by satisfying $c + b < a + b$. Working backwards, we get the equivalences,

$$\begin{aligned} c < a &\iff \frac{b^2 + k}{a} < a \\ &\iff k < a^2 - b^2 \\ &\iff \frac{a^2 + b^2}{ab - 1} < (a + b)(a - b). \end{aligned}$$

Using the fact that $a - b \geq 1$, a sufficient condition on this being true is

$$\begin{aligned} \frac{a^2 + b^2}{ab - 1} < a + b &\iff a^2 + b^2 < (a + b)(ab - 1) \\ &\iff a^2 + b^2 < a^2b + ab^2 - a - b \\ &\iff a + b < a^2b + ab^2 - a^2 - b^2 \\ &\iff a + b < a^2(b - 1) + b^2(a - 1). \end{aligned}$$

If $a, b \geq 2$, then this inequality holds, allowing us to climb all the way back to $c < a$ at the beginning of the chain. So we have to remove the cases where $a = 1$ or $b = 1$. Since it was shown that $a > b$, only the $b = 1$ case needs to be addressed. Then

$$\begin{aligned} k &= \frac{a^2 + b^2}{ab - 1} \\ &= \frac{a^2 + 1}{a - 1} \\ &= \frac{(a - 1)^2 + 2a}{a - 1} \\ &= a - 1 + \frac{2a}{a - 1}, \end{aligned}$$

implying $a - 1 \mid 2$. There are two cases now:

$$\begin{aligned} a - 1 = 1 &\implies a = 2 \implies (a, b) = (2, 1), \\ a - 1 = 2 &\implies a = 3 \implies (a, b) = (3, 1). \end{aligned}$$

In either case,

$$k = \frac{a^2 + b^2}{ab - 1} = 5,$$

which contradicts the initial assumption that $k \neq 5$.

Solution 6.5. We may assume without loss of generality that $0 \leq a < p$ because a can be replaced by its least residue modulo p. If $a = 0$, then it is fine to set $x = pk$ for any positive

integer k. So we can focus on a such that $1 \leq a \leq p-1$. In this case, Fermat's little theorem says that

$$\begin{aligned} a^{p-1} &\equiv 1 \pmod{p}, \\ a^p &\equiv a \pmod{p}. \end{aligned}$$

By modular reduction of the base and the exponent (the latter by Fermat's little theorem), for all integers m and n,

$$(a+pn)^{p+(p-1)m} \equiv a^p \equiv a \pmod{p}.$$

So we just need to find infinitely many pairs of positive integers (m, n) such that

$$a + pn = p + (p-1)m.$$

This equation is equivalent to the linear Diophantine equation

$$pn + (p-1)(-m) = p - a.$$

Since

$$p \cdot 1 + (p-1) \cdot (-1) = 1,$$

we can multiply through by $p - a$ and so construct one solution

$$(-m, n) = (-(p-a), p-a).$$

By the theory of linear Diophantine equations, all solutions $(-m, n)$ to

$$(p-1)(-m) + pn = p - a$$

are then generated as

$$\begin{aligned} -m &= -(p-a) - pk, \\ n &= (p-a) + (p-1)k \end{aligned}$$

for all integers k. Then our prospective base and exponent are

$$\begin{aligned} a + pn &= a + p((p-a) + (p-1)k), \\ p + (p-1)m &= p + (p-1)((p-a) + pk), \end{aligned}$$

respectively, where we pick only the non-negative integers k in order to ensure that the base and exponent are positive. It is easy to check by expansion that both the base and exponent in this construction equal

$$p^2(k+1) - p(a+k) + a,$$

so we have found an infinite family of solutions, as sought.

Solution 6.7. Modulo p and q individually, we may use Fermat's little theorem to find that this expression is congruent to

$$\begin{aligned} p^{q-1} + q^{p-1} &\equiv 0 + 1 \equiv 1 \pmod{p}, \\ p^{q-1} + q^{p-1} &\equiv 1 + 0 \equiv 1 \pmod{q}. \end{aligned}$$

Either by the faux-Chinese remainder theorem (since p and q are coprime) or by observing that $p^{q-1}+q^{p-1}$ is the common CRT solution modulo p and q, the desired congruence holds.

Solution 6.13. If $k = mn - m - n - k$ for some integer k, then rearranging the equation yields

$$2k + 1 = (m - 1)(n - 1).$$

This is impossible because $2k+1$ is odd, whereas if $(m-1)(n-1)$ were odd, then both $m-1$ and $n-1$ would have to be odd, and so m and n would both have to be even, contradicting that $(m, n) = 1$. So k and $mn - m - n - k$ are distinct for all integers k.
If k and $mn - m - n - k$ were both achievable, then their sum $mn - m - n$ would also be achievable as a conical combination, which contradicts Sylvester's theorem. Finally, we wish to show that there exists an achievable number in each pair $\{k, mn - m - n - k\}$. If $k > mn - m - n$, then k is achievable by Sylvester's theorem and $mn - m - n - k < 0$ is non-achievable because it is negative. If $k < 0$, then $mn - m - n - k > mn - m - n$ and so $mn - m - n - k$ is achievable by Sylvester's theorem and $k < 0$ is not achievable because it is negative. Thus, we have to focus on k being in the closed interval $[0, mn - m - n]$. Note that the two chains of inequalities

$$\begin{aligned} 0 \leq k &\leq mn - m - n, \\ 0 \leq mn - m - n - k &\leq mn - m - m, \end{aligned}$$

are equivalent, so k lies in this closed interval if and only if $mn - m - n - k$ does as well. So the integers in $[0, mn - m - n]$ split into

$$\frac{mn - m - n + 1}{2} = \frac{(m - 1)(n - 1)}{2}$$

disjoint pairs $\{k, mn - m - n - k\}$ for

$$k \in \left\{0, 1, 2, \ldots, \frac{mn - m - n - 1}{2}\right\}.$$

By Sylvester's theorem, there are exactly $\dfrac{(m - 1)(n - 1)}{2}$ non-achievable non-negative integers, all of which lie in $[0, mn-m-n]$. This leaves the same number of achievable numbers in the same interval. If, for the sake of contradiction, any one of the pairs $\{k, mn - m - n - k\}$ contains *two* non-achievable numbers, then we would have $\dfrac{(m - 1)(n - 1)}{2} - 1$ available pairs containing a total of $\dfrac{(m - 1)(n - 1)}{2}$ achievable integers. By the pigeonhole principle, it would force some pair to have two achievable integers, which contradicts the fact that each pair must have a non-achievable integer. Thus, each pair has exactly one achievable integer.

Solution 7.4. In the basis representation theorem for integers, note that the condition that "$x_m = 0$ if and only if $m = 0$" implies that the leading digit of a non-zero integer cannot be 0. It is good to be aware of this fact in combinatorial problems about digits because, for example, if an integer has 0 as a digit, then a permutation of the digits of this integer might

have 0 as the leading digit, which is not allowed. This principle is relevant to us now because we want to avoid constructing forms that have leading digit 0.
For positive integers with exactly d digits, there are $b-1$ possibilities for the leading digit because we want to avoid 0, and there are b possibilities for each of the remaining $d-1$ digits. By the multiplication principle from combinatorics, the answer is $(b-1)\cdot b^{d-1}$.
Now we tackle non-negative integers with at most d digits. A complicated method is to sum the formula from the first part over all k such that $1 \leq k \leq d$. This method ends up working (and the reader could try it out as a bit of practice with geometric series), but there is a cleverer and quicker way of reach the same end: for integers with fewer than d digits, pad 0's to the left of its leading digit until it has exactly d "digits." By the multiplication principle, there are b^d possible non-negative integers with at most d digits. More formally, we have used the bijection principle from combinatorics here.

Solution 7.12. Let n be a positive integer. Suppose $f(n) = f(2n)$. By modular reduction,

$$\begin{aligned} f(n) &\equiv n \pmod 9, \\ f(2n) &\equiv 2n \pmod 9. \end{aligned}$$

Using $f(n) = f(2n)$, we get

$$2n \equiv n \pmod 9 \implies n \equiv 0 \pmod 9,$$

so $9 \mid n$.

Solution 7.13. The first proof is a matter of using the hint to get $3^5 \equiv 3^{-1} \equiv 5 \pmod 7$. The second proof uses the fact that $1001 = 10^3 + 1$ is divisible by 7. Here are the details:

- The integer n is divisible by 7 if and only if

  $$n = 10x + y \equiv 0 \pmod 7.$$

  This congruence is equivalent to

  $$3x + y \equiv 0 \pmod 7.$$

  We want to prove that $x - 2y \equiv 0 \pmod 7$, which is equivalent to

  $$x + 5y \equiv 0 \pmod 7.$$

  Multiplying both sides of $3x + y \equiv 0 \pmod 7$ by 3^5 yields

  $$3^6 x + 3^5 y \equiv 0 \pmod 7.$$

  Since $3^6 \equiv 1 \pmod 7$ and $3^5 \equiv 5 \pmod 7$, we are done because all of our steps were reversible. In particular, we can take y to be the units digit of n, which then fixes x.

- Note that $10^3 + 1 = 1001 = 7 \cdot 11 \cdot 13$ is divisible by 7. As such,

$$10^3 \equiv -1 \pmod 7.$$

Every integer is a sum of a multiple of 1000^1 plus a multiple of 1000^2 plus a multiple of 1000^3 and so on, by grouping digits into chunks of 3 (except perhaps the final group). For example,

$$8641969 = 10^6 \cdot 8 + 10^3 \cdot 641 + 10^0 \cdot 969.$$

For odd k,

$$10^{3k} \equiv (-1)^k \equiv -1 \pmod 7.$$

For even k,

$$10^{3k} \equiv (-1)^k \equiv 1 \pmod 7.$$

Thus, we get a sum of three-digit integers with alternating signs, as desired. The same idea provides a divisibility trick for divisibility by 13 since $13 \mid 1001$.

Solution 8.3. By the formula for binomial coefficients,

$$\binom{2p-k-1}{p-k} = \frac{(2p-k-1)!}{(p-k)!(p-1)!}.$$

We can get $2p - k - 1 \geq p$ from $p - 1 \geq k$, so p divides the factorial in the numerator. However, $p-k$ and $p-1$ are both less than or equal to $p-1$, so p does not divide any of the multiplicands in the factorials $(p-k)!$ and $(p-1)!$ in the denominator. Thus, the integer $\binom{2p-k-1}{p-k}$ is divisible by p.

Solution 8.10. We will use the second form of Legendre's formula, which says that

$$\nu_p(n!) = \frac{n - s_p(n)}{p-1}$$

for all positive integers n. Using the fact that $n = \dfrac{n!}{(n-1)!}$, we get

$$\begin{aligned}
\nu_p(n) &= \nu_p\left(\frac{n!}{(n-1)!}\right) \\
&= \nu_p(n!) - \nu_p((n-1)!) \\
&= \frac{n - s_p(n)}{p-1} - \frac{(n-1) - s_p(n-1)}{p-1} \\
&= \frac{1 - s_p(n) + s_p(n-1)}{p-1}.
\end{aligned}$$

Solution 8.11. According to Legendre's formula,

$$\begin{aligned}\nu_p(p^k!) &= \left\lfloor \frac{p^k}{p} \right\rfloor + \left\lfloor \frac{p^k}{p^2} \right\rfloor + \cdots + \left\lfloor \frac{p^k}{p^k} \right\rfloor \\ &= p^{k-1} + p^{k-2} + \cdots + p + 1 \\ &= \frac{p^k - 1}{p - 1},\end{aligned}$$

where we used the formula for a geometric series in the last step.

Solution 8.12. We will temporarily extend ν_p notation so that, for any integer $t \geq 2$ and positive integer q, $\nu_t(q)$ denotes the highest non-negative integer s such that $t^s \mid q$. As is sometimes the case when we want to prove a result for all positive integers and the prime case has been established, we next go for the prime powers m. Let $m = p^e$ for some prime p and positive integer e (unrelated to Euler's constant). We want to know the highest power of p^e that divides n. By the definition of ν_p, the highest power of p that divides n is $\nu_p(n)$. So we are looking for the highest integer that, when multiplied by e, is less than or equal to $\nu_p(n)$. By Euclidean division, this is equal to $\left\lfloor \frac{\nu_p(n)}{e} \right\rfloor$.
This explains a part of the stated formula now, and it suffices to prove that

$$\nu_m(n) = \min\left\{\nu_{p_i^{e_i}}(n) : i \in [k]\right\}.$$

Let the left side be $\nu_m(n) = s$ and the right side by $\min\left\{\nu_{p_i^{e_i}}(n) : i \in [k]\right\} = w$. We will show that $w \leq s$ and $w \geq s$, which will allow us to invoke antisymmetry to get $w = s$. Suppose, for contradiction, that $w > s$. Then all k of the $\nu_{p_i^{e_i}}(n)$ are strictly greater than s. Since

$$m^w = (p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k})^w = (p_1^{e_1})^w (p_2^{e_2})^w \cdots (p_k^{e_k})^w,$$

and the prime powers $(p_i^{e_i})^w$ are pairwise coprime and each divides n, their product m^w divides n. But this contradicts the fact that m^s is the maximal power of m that divides n. So our assumption was wrong and it is instead true that $w \leq s$. To show that $w \geq s$ as well, note that since $m^s \mid n$, transitivity of divisibility gives us that, for all i,

$$p_i^{e_i} \mid m \implies (p_i^{e_i})^s \mid m^s \implies (p_i^{e_i})^s \mid n.$$

Thus, $\nu_{p_i^{e_i}}(n) \geq s$ for each i, and taking the minimum of the left side of this inequality over all i yields $w \geq s$. Therefore, $w = s$ by antisymmetry.
In the concrete example, we are looking for $\nu_{10}(99!)$. Since the prime factorization of 10 is $2^1 \cdot 5^1$, the formula states that the answer is the smaller of $\sum_{k=1}^{\infty} \left\lfloor \frac{99}{2^k} \right\rfloor$ and $\sum_{k=1}^{\infty} \left\lfloor \frac{99}{5^k} \right\rfloor$. We do not actually have to compute both because the latter is less than or equal to the former, by comparing the two sums term-by-term. Thus, the answer is

$$\left\lfloor \frac{99}{5} \right\rfloor + \left\lfloor \frac{99}{25} \right\rfloor = 19 + 3 = 22.$$

This particular computation was not difficult because the multiplicity of 2 and 5 are equal in 10, not to mention both multiplicities are equal to 1.

Solution 8.16. By Kummer's theorem, $\nu_2\left[\binom{2n}{n}\right]$ is the number of times that carrying occurs in the application of the addition algorithm to the binary forms of n and $2n-n=n$. Thus, $\nu_2\left[\binom{2n}{n}\right]$ is the number of non-zero digits in the binary form of n. This is greater than 1 if and only if there is more than one digit equal to 1, in which case n is not a power of 2. This is because, for every non-negative integer k,

$$(2^k)_2 = 1\ \underbrace{00\ldots0}_{k \text{ digits of } 0}\ .$$

Solution 8.19. Let the base-p form of k be $a_m a_{m-1}\ldots a_1 a_0$. Then the base-$p$ forms of $p^n k$ and p^n are

$$p^n k = a_m a_{m-1}\ldots a_1 a_0\ \underbrace{00\ldots0}_{n \text{ digits of } 0}\ ,$$
$$p^n = 1\ \underbrace{00\ldots0}_{n \text{ digits of } 0}\ .$$

By Lucas's theorem,

$$\binom{p^n k}{p^n} \equiv \binom{a_m}{0}\binom{a_{m-1}}{0}\cdots\binom{a_1}{0}\binom{a_0}{1}\prod_{i=1}^{n}\binom{0}{0} \equiv \binom{a_0}{1} \equiv a_0 \pmod{p}.$$

Since a_0 is the units digit of k in base-p, we end up with $a_0 \equiv k \pmod{p}$.

Solution 9.1. Suppose n is a positive integer and that a is an integer.

1. We can perform the following reversible manipulations:

$$\begin{aligned} ka &\equiv 0 \pmod{n}, \\ k\cdot\frac{a}{(a,n)} &\equiv 0 \left(\mod \frac{n}{(a,n)}\right), \\ k &\equiv 0 \left(\mod \frac{n}{(a,n)}\right), \end{aligned}$$

   where we used the fact that $\dfrac{a}{(a,n)}$ and $\dfrac{n}{(a,n)}$ are coprime in the final step in order to invert $\dfrac{a}{(a,n)}$. Thus, n divides ka if and only if $\dfrac{n}{(a,n)}$ divides k. And the smallest positive multiple of $\dfrac{n}{(a,n)}$ is $\dfrac{n}{(a,n)}$ itself. This means that if we were to keep adding a to itself, then we would reach 0 once we have $\dfrac{n}{(a,n)}$ copies of a. So there are at

most $\frac{n}{(a,n)}$ residue classes represented in R. Similarly, we can perform the reversible manipulations

$$\begin{aligned} ia &\equiv ja \pmod{n}, \\ i \cdot \frac{a}{(a,n)} &\equiv j \cdot \frac{a}{(a,n)} \left(\mod \frac{n}{(a,n)} \right), \\ i &\equiv j \left(\mod \frac{n}{(a,n)} \right), \end{aligned}$$

which shows that each ka for $k \in \left[\frac{n}{(a,n)} \right]$ is distinct modulo n. So R contains at least $\frac{n}{(a,n)}$ residue classes, causing the upper bound and lower bound to coincide. Thus, the set

$$\left\{ 1 \cdot a, 2 \cdot a, \ldots, \frac{n}{(a,n)} \cdot a \right\}$$

of $\frac{n}{(a,n)}$ elements contains all distinct residues among multiples of a modulo n and they all lie in distinct residue classes modulo n.

2. By the last part, R contains all residue classes modulo n if and only if $\frac{n}{(a,n)} = n$, which is true if and only if $(a,n) = 1$. In this case,

$$ia \equiv ja \pmod{n}$$

if and only if

$$i \equiv j \pmod{n},$$

so i and j must differ by a multiple n. Thus, all of the elements of the n consecutive multiples of s

$$\{ia, (i+1)a, \ldots, (i+n-1)a\}$$

come from different residue classes, making it a complete residue system modulo n.

Solution 9.3. By Bézout's lemma, there exist integers x and y such that

$$ix + jy = (i,j).$$

Thus,

$$a^{(i,j)} = a^{ix+jy} = (a^i)^x \cdot (a^j)^y \equiv 1^x \cdot 1^y \equiv 1 \pmod{n}.$$

As a reminder, what allows us to manipulate the exponents in such a way is that a is coprime to n, as non-positive exponents are not even defined when the base is not coprime to the modulus (see Definition 4.14).

Solution 9.5. Each step leads to the next one.

1. We will show by induction on $n \geq 3$ that, for each integer $n \geq 3$, there exists an odd integer x_n such that $5^{2^{n-2}} = 1 + x_n \cdot 2^n$. Since x_n will be shown to be odd, no power of 2 higher than 2^n can divide $5^{2^{n-2}} - 1$, while it is true that 2^n does divide $5^{2^{n-2}} - 1$. Thus, we will have proven that $\nu_2\left(5^{2^{n-2}} - 1\right) = n$.

   The base case $n = 3$ holds because

   $$5^{2^{3-2}} - 1 = 24 = 3 \cdot 2^3.$$

   Now suppose $5^{2^{n-2}} = 1 + x_n \cdot 2^n$ for some integer $n \geq 3$ and odd integer x_n. Squaring the equation yields

   $$5^{2^{n-1}} = 1 + x_n \cdot 2^{n+1} + x_n^2 \cdot 2^{2n} = 1 + x_n(1 + x_n 2^{n-1}) \cdot 2^{n+1} \equiv 1 \pmod{2^{n+1}}.$$

   Since x_n is odd and $n \geq 3$, so is

   $$x_{n+1} = x_n(1 + x_n 2^{n-1}).$$

2. We know from the first part that

   $$5^{2^{n-2}} \equiv 1 \pmod{2^n}.$$

   So the order of 5 modulo 2^n must divide 2^{n-2}. Suppose, for contradiction, that there exists an integer i such that $3 \leq i \leq n$ and $5^{2^{n-i}} \equiv 1 \pmod{2^n}$. Squaring this sufficiently many times (taking it to an exponent of 2^{i-3}, to be precise) we get $5^{2^{n-3}} \equiv 1 \pmod{2^n}$. So there exists an integer y_n such that

   $$5^{2^{n-3}} = 1 + y_n 2^n.$$

   Squaring this yields

   $$5^{2^{n-2}} = 1 + y_n 2^{n+1} + y_n^2 2^{2n} = 1 + (2y_n + y_n^2 2^n)2^n,$$

   which implies that the x_n from the last part is the even number $2y_n + y_n^2 2^n$. This is a contradiction.

3. Note that the order of 5 modulo 2^n is $2^{n-2} = \dfrac{\varphi(2^n)}{2}$ and that the elements of S are all invertible modulo 2^n. We will show that S consists of precisely all of the units (that is, invertible elements, which are the odd integers in this case) by showing that none of the 5^i coincide with the -5^j modulo 2^n. If $5^i \equiv -5^j \pmod{2^n}$ then cancelling the smaller of the two powers from both sides (or either, if they are equal) would yield a power of 5 congruent to -1 modulo 2^n. It suffices to show that

   $$5^k \not\equiv -1 \pmod{2^n}$$

   for all k. If the congruence held, then we could reduce it to

   $$5^k \equiv -1 \equiv 3 \pmod{4}$$

using $4 \mid 2^n$. This is contradictory because

$$5^k \equiv 1^k \equiv 1 \pmod 4.$$

Therefore, there are no overlaps between the 5^i and -5^j. This produces

$$2 \cdot 2^{n-2} = 2^{n-1} = \varphi(2^n)$$

distinct units modulo 2^n, which is the maximal number and so this is the set of all units modulo 2^n.

Solution 9.7. Suppose such an integer a exists. We will aim to prove that

$$\operatorname{ord}_n(a) = n - 1,$$

as that will lead to

$$\varphi(n) \leq n - 1 = \operatorname{ord}_n(a) \leq \varphi(n).$$

This will flatten the inequalities into the equation $\varphi(n) = n - 1$, which will force n to be prime. Let us charge forward with this conclusion in mind.

By the congruence that we are given, $\operatorname{ord}_n(a) \mid n - 1$. So the set of prime factors of $\operatorname{ord}_n(a)$ is a subset of the set of prime factors of $n - 1$. Let the prime factorization of $n - 1$ be

$$n - 1 = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$$

and the prime factorization of $\operatorname{ord}_n(a)$ that is modified to (superficially) include all prime factors of $n - 1$ be

$$p_1^{f_1} p_2^{f_2} \cdots p_k^{f_k}.$$

Then

$$\frac{n-1}{\operatorname{ord}_n(a)} = \frac{p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}}{p_1^{f_1} p_2^{f_2} \cdots p_k^{f_k}} = p_1^{e_1 - f_1} p_2^{e_2 - f_2} \cdots p_k^{e_k - f_k}$$

is an integer, so $e_i \geq f_i$ for all $i \in [k]$.

What we would like to do is show that all of the reverse inequalities $e_i \leq f_i$ hold as well, which would imply that $n - 1 = \operatorname{ord}_n(a)$. This is where the given non-congruences come into play. Since $\operatorname{ord}_n(a)$ does *not* divide each $\dfrac{n-1}{p_j}$, this means

$$\frac{\left(\frac{n-1}{p_j}\right)}{\operatorname{ord}_n(a)} = \frac{1}{p_j} \cdot \frac{n-1}{\operatorname{ord}_n(a)} = \frac{1}{p_j} \cdot p_1^{e_1 - f_1} p_2^{e_2 - f_2} \cdots p_k^{e_k - f_k}$$

is not an integer. We already know that $e_i \geq f_i$ for each i, so the only possibility for why this division goes wrong is that $e_j - f_j - 1 < 0$, which is equivalent to $e_i \leq f_i$. By antisymmetry, we get $e_j = f_j$ for each $j \in [k]$, which completes the proof thanks to the earlier foresight.

Solution 9.10. We will use antisymmetry of divisibility to get the equality. Let $x = \operatorname{ord}_m(a)$ and $y = \operatorname{ord}_n(a)$, and we will denote

$$[x, y] = \operatorname{lcm}(\operatorname{ord}_m(a), \operatorname{ord}_n(a)).$$

Since x and y both divide their (lowest) common multiple $[x, y]$, let v, w be integers such that $xv = [x, y]$ and $yw = [x, y]$. Then

$$a^{[x,y]} \equiv (a^x)^v \equiv 1^v \equiv 1 \pmod{m},$$
$$a^{[x,y]} \equiv (a^y)^w \equiv 1^w \equiv 1 \pmod{n}.$$

Since m and n are coprime,

$$a^{[x,y]} \equiv 1 \pmod{mn},$$

which proves that $\text{ord}_{mn}(a) \mid [x, y]$. Now we have to go for the reverse divisibility property. From $a^{\text{ord}_{mn}(a)} \equiv 1 \pmod{mn}$, we get

$$a^{\text{ord}_{mn}(a)} \equiv 1 \pmod{m},$$
$$a^{\text{ord}_{mn}(a)} \equiv 1 \pmod{n},$$

so $x \mid \text{ord}_{mn}(a)$ and $y \mid \text{ord}_{mn}(a)$. This means $\text{ord}_{mn}(a)$ is a common multiple of x and y, which causes it to be true that $[x, y] \mid \text{ord}_{mn}(a)$. By antisymmetry, we are done.

Solution 9.21. Let n be a positive integer such that there is a primitive root g modulo n, and let d be a positive divisor of $\varphi(d)$. By Theorem 9.8, we are seeking a power g^i of g such that

$$d = \text{ord}_n(g^i) = \frac{\text{ord}_n(g)}{(i, \text{ord}_n(g))} = \frac{\varphi(n)}{(i, \varphi(n))},$$

which is equivalent to wanting

$$(i, \varphi(n)) = \frac{\varphi(n)}{d}.$$

One example of when this occurs is for $i = \dfrac{\varphi(n)}{d}$, but we are not satisfied with finding just one example. Some other examples that work are i that are multiples $k \cdot \dfrac{\varphi(n)}{d}$ of $\dfrac{\varphi(n)}{d}$ such that k is coprime to $\varphi(n)$. This makes us wonder whether all examples that work are multiples of $\dfrac{\varphi(n)}{d}$ (though not all such multiples will work). Suppose i is an integer such that $\text{ord}_n(g^i) = d$. By the Euclidean division of i by $\dfrac{\varphi(n)}{d}$, we get

$$i = q \cdot \frac{\varphi(n)}{d} + r, \text{ and } 0 \leq r < \frac{\varphi(n)}{d},$$

which is equivalent to

$$di = q \cdot \varphi(n) + dr, \text{ and } 0 \leq dr < \varphi(n).$$

We want to force $r = 0$, to do which we will show that $dr = 0$. Indeed,

$$g^{dr} = g^{di - q \cdot \varphi(n)} \equiv (g^i)^d \cdot (g^{\varphi(n)})^{-q} \equiv 1 \pmod{n}.$$

In order to avoid contradicting the minimality of $\varphi(n)$ as a positive exponent that sends to g to 1, we must have $dr = 0$ and so $r = 0$, since d is positive.

Thus, we are seeking all multiples i of $\dfrac{\varphi(n)}{d}$ that lead to incongruent g^i such that $(i, \varphi(n)) = \dfrac{\varphi(n)}{d}$. If $i = \dfrac{\varphi(n)}{d} \cdot k$ for some integer k, then the equation becomes

$$\left(\frac{\varphi(n)}{d} \cdot k, \varphi(n)\right) = \frac{\varphi(n)}{d} \iff (k, d) = 1.$$

The smallest positive multiple of $\dfrac{\varphi(n)}{d}$ is $\dfrac{\varphi(n)}{d}$ and the largest positive multiple before the powers start repeating is $\varphi(n)$. All multiples of $\dfrac{\varphi(n)}{d}$ in between them, inclusive, are exponents that lead to incongruent powers of g. Note that

$$\frac{\varphi(n)}{d} \leq \frac{\varphi(n)}{d} \cdot k \leq \varphi(n) \iff 1 \leq k \leq d.$$

Thus, we are seeking the number of elements k of $[d]$ such that $(k, d) = 1$. This is $\varphi(d)$ by the definition of Euler's totient function.

Solution 9.22. The elements of $\mathbb{Z}_n$ corresponding to the integers $\{0, 1, 2, \ldots, d-1\}$ reduce to $\mathbb{Z}_d$ modulo d, so the map is surjective. For the preimages, suppose $a, b \in \{0, 1, 2, \ldots, n-1\}$ such that

$$a \equiv b \pmod{d}.$$

This is true if and only of a and b differ by a multiple of d. Since $d \mid n$, the complete residue system $\{0, 1, 2, \ldots, n-1\}$ splits into d preimages of $\dfrac{n}{d}$ elements each. This may be illustrated by the example of $n = 12$ and $d = 4$, where the classes are

$$\{0, 4, 8\}, \{1, 5, 9\}, \{2, 6, 10\}, \{3, 7, 11\}.$$

Solution 9.25. Squaring the congruence yields

$$a^{2k} \equiv 1 \pmod{n},$$

so $\operatorname{ord}_n(a) \mid 2k$. Suppose, for the sake of contradiction, that $\operatorname{ord}_n(a) < 2k$. We know that $\operatorname{ord}_n(a) \neq k$ because an exponent of k sends a to -1, there exists a positive proper factor ℓ of k such that $\operatorname{ord}_n(a) = \ell$ or $\operatorname{ord}_n(a) = 2\ell$. In the former case,

$$-1 \equiv a^k \equiv (a^\ell)^{\frac{k}{\ell}} \equiv 1^{\frac{k}{\ell}} \equiv 1 \pmod{n},$$

which is a contradiction since $n \neq 2$. In the latter case,

$$a^{2\ell} \equiv 1 \pmod{n} \implies a^\ell \equiv \pm 1 \pmod{n}.$$

If $a^\ell \equiv 1 \pmod{n}$, then ℓ breaks the minimality of 2ℓ as the order of a modulo n. If $a^\ell \equiv -1 \pmod{n}$, then ℓ breaks the minimality of k as the exponent that sends a to -1.

Solution 9.29. In one direction, if $a^n \equiv a \pmod{n}$ for all $a \in \mathbb{Z}$, then take a to satisfy $(a, n) = 1$ and multiply both sides by a^{-1} to get $a^{n-1} \equiv 1 \pmod{n}$.
Conversely, suppose $a^{n-1} \equiv 1 \pmod{n}$ for all integers a coprime to n. Then n is a Carmichael number. By Korselt's criterion, n is squarefree, so $n = p_1 p_2 \cdots p_t$ for distinct primes p_i. The result is obvious for $t = 0$ and $n = 1$, so we may assume that $n \geq 2$, which actually has a prime factor. For each $i \in [t]$ and for any $a \in \mathbb{Z}$, Fermat's little theorem says

$$a^{p_i - 1} \equiv 1 \pmod{p_i} \text{ if } p_i \nmid a,$$

and

$$a \equiv 0 \pmod{p_i} \text{ if } p_i \mid a.$$

In the former case, since $p_i - 1 \mid n - 1$ by Korselt's criterion,

$$a^{n-1} \equiv 1 \pmod{p_i}.$$

Then p_i divides $a^{n-1} - 1$ or p_i divides a, so

$$p_i \mid a(a^{n-1} - 1) \implies a^n \equiv a \pmod{p_i}.$$

Since this is true for all p_i and the prime factors of n are pairwise coprime, we get $a^n \equiv a \pmod{n}$.

Solution 9.30. We prove the results in sequence:

1. By Euclidean division of m by $\lambda(n)$, there exists a quotient $q \in \mathbb{Z}$ and an integer remainder $0 \leq r < \lambda(n)$ such that

   $$m = \lambda(n)q + r.$$

   Then, for all integers a coprime to n,

   $$a^r \equiv a^{m - \lambda(n)q} \equiv a^m \cdot (a^{\lambda(n)})^{-q} \equiv 1 \pmod{n}.$$

   To avoid contradicting the minimality of $\lambda(n)$, it must be true that $r = 0$, causing $m = \lambda(n)q$ or $\lambda(n) \mid m$.

2. By Euler's congruence, for every integer a coprime to n,

   $$a^{\varphi(n)} \equiv 1 \pmod{n}.$$

   By part (1), $\lambda(n) \mid \varphi(n)$. For $n = 8$,

   $$1^2 \equiv 3^2 \equiv 5^2 \equiv 7^2 \equiv 1 \pmod{8},$$

   so $\lambda(8) = 2 \neq 4 = \varphi(8)$. On the other hand, for $n = 3$, it may be verified that the equality $\lambda(3) = 2 = \varphi(3)$ holds.

3. Suppose $s \mid t$. Then, for all integers a coprime to n,

   $$a^{\lambda(t)} \equiv 1 \pmod{t} \implies a^{\lambda(t)} \equiv 1 \pmod{s},$$

   by reducing the modulus. By part (1), $\lambda(s) \mid \lambda(t)$.

4. Let $k \geq 3$ be an integer. By the results of Problem 9.5, every odd integer a satisfies

$$a^{2^{k-2}} \equiv 1 \pmod{2^k},$$

so $\lambda(2^k) \leq 2^{k-2}$. According to the same problem, $\operatorname{ord}_{2^k}(5) = 2^{k-2}$, so $2^{k-2} \leq \lambda(2^k)$. The rest follows from antisymmetry. The small edge cases are easy to verify manually.

5. By Euler's congruence, for every integer a coprime to p^k,

$$a^{\varphi(p^k)} \equiv 1 \pmod{p^k},$$

so $\lambda(p^k) \leq \varphi(p^k)$. Since p^k has a primitive root, it means there exists an integer a coprime to p^k such that $\operatorname{ord}_{p^k}(a) = \varphi(p^k)$, so $\varphi(p^k) \leq \lambda(p^k)$. Antisymmetry turns it into an equality.

6. Recall that, for $x, y \in \mathbb{Z}_+$, $\operatorname{lcm}(x, y)$ is the least positive integer v such that $x \mid v$ and $y \mid v$. By part (3),

$$\begin{aligned} s \mid [s,t] &\implies \lambda(s) \mid \lambda([s,t]), \\ t \mid [s,t] &\implies \lambda(t) \mid \lambda([s,t]). \end{aligned}$$

Since all common multiples are divisible by the lcm,

$$[\lambda(s), \lambda(t)] \mid \lambda([s,t]).$$

For the other direction of the antisymmetry of divisibility, suppose $a \in \mathbb{Z}$ is coprime to $[s,t]$. Then $(a,s) = (a,t) = 1$. Using the fact that $\lambda(s)$ and $\lambda(t)$ divide $[\lambda(s), \lambda(t)]$, we get

$$\begin{aligned} a^{\lambda(s)} \equiv 1 \pmod{s} &\implies a^{[\lambda(s),\lambda(t)]} \equiv 1 \pmod{s}, \\ a^{\lambda(t)} \equiv 1 \pmod{t} &\implies a^{[\lambda(s),\lambda(t)]} \equiv 1 \pmod{t}. \end{aligned}$$

So $a^{[\lambda(s),\lambda(t)]} - 1$ is a common multiple of s, t, leading to

$$a^{[\lambda(s),\lambda(t)]} \equiv 1 \pmod{[s,t]}.$$

By part (1),

$$\lambda([s,t]) \mid [\lambda(s), \lambda(t)].$$

For the corollary, we need to only note that if s, t are coprime then $[s,t] = st$.

7. Using part (6), this follows from $\lambda(st) = [\lambda(s), \lambda(t)]$ for coprime integers s, t, since the maximal prime powers $p_i^{e_i}$ are pairwise coprime. The formulas in parts (4) and (5) for $\lambda(p^k)$, where p is a prime, allow for the computation of λ explicitly.

8. Let the prime factorization of n be $n = p_1^{e_1} p_2^{e_2} \cdots p_m^{e_m}$. For each $i \in [m]$, there exists $a_i \in \mathbb{Z}$ coprime to $p_i^{e_i}$ such that $\operatorname{ord}_{p_i^{e_i}}(a_i) = \lambda(p_i^{e_i})$ by the results and proofs of parts

(4) and (5) (use a primitive root modulo odd prime powers, and 5 modulo non-trivial powers of 2). By the Chinese remainder theorem, there exists $a \in \mathbb{Z}$ such that

$$a \equiv a_i \pmod{p_i^{e_i}}$$

for all $i \in [m]$. Since

$$a^{\operatorname{ord}_n(a)} \equiv 1 \pmod{n},$$

reducing modulo $p_i^{e_i}$ gives

$$a_i^{\operatorname{ord}_n(a)} \equiv a^{\operatorname{ord}_n(a)} \equiv 1 \pmod{p_i^{e_i}},$$

so

$$\lambda(p_i^{e_i}) = \operatorname{ord}_{p_i^{e_i}}(a_i) \mid \operatorname{ord}_n(a).$$

This leads to

$$\lambda(n) = [\lambda(p_1^{e_1}), \lambda(p_2^{e_2}), \ldots, \lambda(p_m^{e_m})] \mid \operatorname{ord}_n(a).$$

For the reverse divisibility relation, we know that $a^{\lambda(a)} \equiv 1 \pmod{n}$, so $\operatorname{ord}_n(a) \mid \lambda(n)$. Thus, the required $a \in \mathbb{Z}$ exists. For the maximality corollary, the fact that $\lambda(n)$ is the order of an element a shows that

$$\lambda(n) \leq \max\{\operatorname{ord}_n(b) : b \in \mathbb{Z}, (b, n) = 1\}.$$

For the opposite direction, we need to only observe that the exponent $\lambda(n)$ takes every b (coprime to n) to 1, so $\operatorname{ord}_n(b) \mid \lambda(n)$, meaning every element of the set is less than or equal to $\lambda(n)$.

9. According to part (8), there exists $a \in \mathbb{Z}$ coprime to n such that $\operatorname{ord}_n(a) = \lambda(n)$. Then, for each divisor $d \mid \lambda(n)$,

$$\operatorname{ord}_n\left(a^{\frac{\lambda(n)}{d}}\right) = \frac{\operatorname{ord}_n(a)}{\gcd\left(\frac{\lambda(n)}{d}, \operatorname{ord}_n(a)\right)} = \frac{\lambda(n)}{\gcd\left(\frac{\lambda(n)}{d}, \lambda(n)\right)} = d.$$

We conclude that if d is a positive divisor of $\lambda(n)$, then there exists an integer $b = a^{\frac{\lambda(n)}{d}}$ coprime to n of order d. Conversely, for any integer b coprime to n, since

$$b^{\lambda(n)} \equiv 1 \pmod{n},$$

we know that $\operatorname{ord}_n(b) \mid \lambda(n)$.

As a side note, we will apply the Carmichael lambda function to deduce a part of Korselt's criterion (Theorem 9.28). The most difficult part of proving Korselt's criterion was proving that $p - 1 \mid n - 1$ for each distinct prime factor p of n. This is true from several properties of the Carmichael lambda function as follows. If n is a Carmichael number, then $a^{n-1} \equiv 1 \pmod{n}$ for all integers a coprime to n. Then $\lambda(n) \mid n - 1$ by part (1). Moreover, by part (3), $\lambda(p_i^{e_i}) \mid \lambda(n)$ for every maximal prime power $p_i^{e_i}$ of n. By part (5),

$$\lambda(p_i^{e_i}) = \varphi(p_i^{e_i}) = p_i^{e_i - 1}(p_i - 1)$$

for odd p_i. Therefore,

$$p_i - 1 \mid \lambda(p_i^{e_i}) \mid \lambda(n) \mid n - 1.$$

Note that, for $p = 2$, $p - 1 = 1$ trivially divides $n - 1$, but this is irrelevant since Carmichael numbers are necessarily odd.

Solution 10.7. First we will show that $y \mid b^s$. By the definition of s, for each $i \in [k]$,

$$s \geq \left\lceil \frac{f_i}{e_i} \right\rceil \geq \frac{f_i}{e_i},$$

so $se_i \geq f_i$. By a property of the ν_p function, $y \mid b^s$. So m exists, as s is an example of an m. Letting w be the minimal non-negative m, we know that $w \leq s$. We just need to show that $w \geq s$ as well. Since $y \mid b^w$, it holds that $f_i \leq we_i$ for each $i \in [k]$. Then

$$\frac{f_i}{e_i} \leq w \implies \left\lceil \frac{f_i}{e_i} \right\rceil \leq w \implies s = \max\left\{ \left\lceil \frac{f_i}{e_i} \right\rceil : i \in [k] \right\} \leq w.$$

Therefore, $w = s$ and we are done.

Solution 10.9. The first two computations involve numbers that have terminating forms, whereas the latter two involve numbers that do not have terminating forms.

1. We compute that
$$0.125_{10} = \frac{125}{1000} = \frac{5^3}{10^3} = \frac{1}{2^3} = \left(\frac{1}{8}\right)_{10}.$$

2. We compute that
$$\left(\frac{3}{40}\right)_{10} = \frac{3}{2^3 \cdot 5} = \frac{3 \cdot 5^2}{2^3 \cdot 5^3} = \frac{75}{1000} = 0.075_{10}.$$

3. Let $x = 0.10\overline{37}$. Then $10^4 x = 1037.\overline{37}$ and $10^2 x = 10.\overline{37}$. Subtracting the two yields
$$10^4 x - 10^2 x = 1037 - 10 = 1027.$$
Therefore,
$$x = \frac{1027}{10^4 - 10^2} = \left(\frac{1027}{9900}\right)_{10}.$$

4. Note that the denominator is $7 = 1 \cdot 7$ where $1 \mid 10^0$ and $(7, 10) = 1$. By Theorem 10.8, the form is purely periodic (so there is no pre-period) and the period is
$$\operatorname{ord}_7(10) = \operatorname{ord}_7(3) = 6.$$
We let the base-10 form of $\frac{1}{7}$ be
$$0.y_1 y_2 y_3 \ldots,$$

which we know does not terminate. We know that $\frac{1}{7} \cdot 10^6 - \frac{1}{7} = \frac{10^6 - 1}{7}$ is an integer that is equal to the repetend

$$y_1 y_2 y_3 y_4 y_5 y_6.$$

We compute that

$$\frac{10^6 - 1}{7} = \frac{1000000 - 1}{7} = \frac{999999}{7} = 142857.$$

Therefore, $\left(\frac{1}{7}\right)_{10} = 0.\overline{142857}_{10}$.

These methods easily extend to cases where the rational number lies outside the interval $[0, 1)$, either by being negative or being greater than or equal to 1.

Solution 10.15. The key is to note that $3^4 \equiv 81 \equiv 1 \pmod{10}$. So, for any positive integer k,

$$3^{4k} \equiv (3^4)^k \equiv 1^k \equiv 1 \pmod{10}.$$

Since 2020 is divisible by 4, our answer is

$$3^{2021} \equiv 3^{2020} \cdot 3 \equiv 1 \cdot 3 \equiv 3 \pmod{10}.$$

Therefore, the units digit of 3^{2021} is 3.

Solution 11.4. Given $a_1, a_2 \in \mathbb{Z}$, the Chinese remainder theorem says that there exists $a \in \mathbb{Z}$ that is unique modulo $n_1 n_2$ such that

$$\begin{aligned} a &\equiv a_1 \pmod{n_1}, \\ a &\equiv a_2 \pmod{n_2}. \end{aligned}$$

We will show that

$$\begin{aligned} \Psi_f : R_f(n_1) \times R_f(n_2) &\to R_f(n_1 n_2) \\ (a_1, a_2) &\mapsto a \end{aligned}$$

is a well-defined function (meaning it has the specified codomain) and that it is a bijection. If $a_1 \in R_f(n_1)$ and $a_2 \in R_f(n_2)$ then there exist $b_1, b_2 \in \mathbb{Z}$ such that

$$\begin{aligned} a &\equiv a_1 \equiv f(b_1) \pmod{n_1}, \\ a &\equiv a_2 \equiv f(b_2) \pmod{n_2}. \end{aligned}$$

By the Chinese remainder theorem, there exists $b \in \mathbb{Z}$ such that

$$\begin{aligned} b &\equiv b_1 \pmod{n_1}, \\ b &\equiv b_2 \pmod{n_2}. \end{aligned}$$

Then applying f yields

$$f(b) \equiv f(b_1) \equiv a_1 \equiv a \pmod{n_1},$$
$$f(b) \equiv f(b_2) \equiv a_2 \equiv a \pmod{n_2}.$$

Since n_1, n_2 are coprime, we get

$$f(b) \equiv a \pmod{n_1 n_2},$$

meaning $a \in R_f(n_1 n_2)$ and the map is well-defined.
Now we will prove that the function Ψ_f is bijective. For injectivity, we note that the map is a restriction of the CRT map, which is itself injective, so any restriction must also be injective. For surjectivity, suppose $a \in R_f(n_1 n_2)$. Then there exists $b \in \mathbb{Z}$ such that

$$f(b) \equiv a \pmod{n_1 n_2}.$$

Reducing modulo n_1 and n_2 separately, we get

$$a \equiv f(b) \pmod{n_1},$$
$$a \equiv f(b) \pmod{n_2}.$$

Thus, $(f(b), f(b)) \mapsto a$ under the initial definition of Ψ_f, where the first $f(b)$ is taken modulo n_1 and the second $f(b)$ is taken modulo n_2.

Solution 11.5. The initial existence result is necessary for counting in the end because some of the solution sets might be empty, in which case we cannot establish a bijection in the second part.

1. For one direction of the existence result, it is clear that if $b \in \mathbb{Z}$ satisfies

   $$f(b) \equiv 0 \pmod{n_1 n_2},$$

   then reducing the congruence modulo n_1 and n_2 separately shows that b is also a solution modulo n_1 and n_2. Conversely, suppose $b_1, b_2 \in \mathbb{Z}$ satisfy

   $$f(b_1) \equiv 0 \pmod{n_1}.$$
   $$f(b_2) \equiv 0 \pmod{n_2}.$$

   By the Chinese remainder theorem, there exists $b \in \mathbb{Z}$ such that

   $$b \equiv b_1 \pmod{n_1},$$
   $$b \equiv b_2 \pmod{n_2}.$$

   Applying f yields

   $$f(b) \equiv f(b_1) \equiv 0 \pmod{n_1},$$
   $$f(b) \equiv f(b_2) \equiv 0 \pmod{n_2}.$$

   Since n_1, n_2 are coprime,

   $$f(b) \equiv 0 \pmod{n_1 n_1},$$

   showing that a is a solution modulo $n_1 n_1$.

2. Now we will address the bijection result. Given $b_1, b_2 \in \mathbb{Z}$, the Chinese remainder theorem asserts that there exists $b \in \mathbb{Z}$ that is unique modulo $n_1 n_2$ such that

$$\begin{aligned} b &\equiv b_1 \pmod{n_1}, \\ b &\equiv b_2 \pmod{n_2}. \end{aligned}$$

We will show that

$$\begin{aligned} \Xi_f : S_f(n_1) \times S_f(n_2) &\to S_f(n_1 n_2) \\ (b_1, b_2) &\mapsto b \end{aligned}$$

is a well-defined function (so it has the specified codomain) and that it is a bijection. If $b_1 \in S_f(n_1)$ and $b_2 \in S_f(n_2)$ then

$$\begin{aligned} f(b_1) &\equiv 0 \pmod{n_1}, \\ f(b_2) &\equiv 0 \pmod{n_2}. \end{aligned}$$

Applying the Chinese remainder theorem to the initial CRT congruences above, we get

$$\begin{aligned} f(b) \equiv f(b_1) &\equiv 0 \pmod{n_1}, \\ f(b) \equiv f(b_2) &\equiv 0 \pmod{n_2}. \end{aligned}$$

Since n_1, n_2 are coprime, we get

$$f(b) \equiv 0 \pmod{n_1 n_2},$$

meaning $b \in S_f(n_1 n_2)$ and the map is well-defined.

Finally, we will prove that the function Ξ_f is bijective. Injectivity is immediate because Ξ_f is a restriction of the CRT map, which itself is injective, and restricting the domain of an injective map preserves injectivity. For surjectivity, suppose $b \in S_f(n_1 n_2)$. Then

$$f(b) \equiv 0 \pmod{n_1 n_2}.$$

Reducing modulo n_1 and n_2 separately, we get

$$\begin{aligned} f(b) &\equiv 0 \pmod{n_1}, \\ f(b) &\equiv 0 \pmod{n_2}. \end{aligned}$$

Thus, $(b, b) \mapsto b$ under the initial definition of Ξ_f, where the first b in (b, b) is taken modulo n_1 and the second b is taken modulo n_2.

The counting result is immediate from the multiplication principle in combinatorics

Solution 11.9. This problem is mostly a matter of being able to compile and parse the stated previous results. Let $k = 2^j m$, where m is odd. If $j = 0$, then the exponent k is odd and so coprime to 2^n. Then by Example 11.8, all integers coprime to 2^n are in $S_k(2^n)$, so $|S_k(n)| = 2^{n-2}$. Now we can assume that $j \geq 1$. We can think of the k^{th} power map as

taking a power of m of each element of S followed by taking a power of 2^j of each element of S. Again by Example 11.8, the first map is irrelevant because it is a bijection on S. What really matters is the application of the second map to

$$S = \left\{\pm 5^i : i \in [2^{n-2}]\right\}.$$

Since $j \geq 1$, the even exponent makes the $\pm$ sign disappear, and so

$$T = \left\{(5^i)^{2^j} \pmod{2^n} : i \in [2^{n-2}]\right\}.$$

Not every $(5^i)^{2^j}$ is necessarily distinct modulo 2^n so we have count the number of distinct elements. We exchange exponents to rewrite each term as $(5^{2^j})^i$ for $i \in [2^{n-2}]$. By Lemma 9.14, we get

$$(5^{2^j})^{2^{n-2}} \equiv (5^{2^{n-2}})^{2^j} \equiv 1^{2^j} \equiv 1 \pmod{2^n},$$

and higher powers of 5^{2^j} are repeats of lower powers. So, modulo 2^n, all powers of 5^{2^j} are in T, and every element of T is a power of 5^{2^j}. Since powers of an element cycle if the element is coprime to the modulus, the number of distinct elements of $S_k(2^n)$ is

$$|S_k(2^n)| = \operatorname{ord}_{2^n}(5^{2^j}) = \frac{\operatorname{ord}_{2^n}(5)}{(2^j, \operatorname{ord}_{2^n}(5))} = \frac{2^{n-2}}{(2^j, 2^{n-2})} = \frac{2^{n-2}}{(k, 2^{n-2})}.$$

Solution 11.16. The steps will be completed in the sequence stated, as the first two steps help with the third one.

1. Let g be a primitive root modulo p. Since g is coprime to p, Lemma 6.11 tells us that

   $$\{1, 2, \ldots, p\} = \{1g, 2g, \ldots, pg\}$$

   modulo p. Then

   $$g^k \cdot S = \sum_{i=1}^{p} (gi)^k \equiv \sum_{i=1}^{p} i^k \equiv S \pmod{p}$$
   $$(g^k - 1) \cdot S \equiv 0 \pmod{p},$$

   so $g^k \equiv 1 \pmod{p}$ or $S \equiv 0 \pmod{p}$. Since $\operatorname{ord}_p(g) = p - 1$, we know that $g^k \equiv 1 \pmod{p}$ if and only if $p - 1 \mid k$, in which case

   $$S \equiv \sum_{i=1}^{p} i^k \equiv \sum_{i=1}^{p} (g^j)^k \equiv \sum_{i=1}^{p} (g^k)^j \equiv p - 1 \equiv -1 \pmod{p}.$$

   Otherwise, if $p - 1 \nmid k$, then $g^k \not\equiv 1 \pmod{p}$, so the only option is $S \equiv 0 \pmod{p}$.

2. We address the three possible cases, according to the value of $\left(\frac{c}{p}\right)$:

- If $\left(\frac{c}{p}\right) = 0$, then $c \equiv 0 \pmod{p}$, so the only solution to $x^2 \equiv c \pmod{p}$ is $x \equiv 0 \pmod{p}$.
- If $\left(\frac{c}{p}\right) = 1$, then there exists at least one solution. Let x_1 and x_2 be (not necessarily distinct) solutions. Then

$$\begin{aligned} x_2^2 &\equiv c \equiv x_1^2 \pmod{p} \\ (x_2 - x_1)(x_2 + x_1) &\equiv 0 \pmod{p} \\ x_2 &\equiv \pm x_1 \pmod{p}. \end{aligned}$$

  So there are at most two distinct solutions modulo p. Suppose there is just one, for the sake of contradiction. Then the two solutions $\pm x_1$ must actually be the same modulo p, so

$$x_1 \equiv -x_1 \pmod{p} \implies 2x_1 \equiv 0 \pmod{p}.$$

  Then $p \mid 2$ or $p \mid x_1$. The former is impossible because p is odd, and the latter is impossible because x_1 is a non-zero quadratic residue modulo p. So we have a contradiction, and there are exactly two distinct solutions modulo p.
- If $\left(\frac{c}{p}\right) = -1$, then a solution x cannot exist by the definition of the Legendre symbol.

In all three cases, the number of solutions matches the proposed formula $\left(\frac{c}{p}\right) + 1$.

3. The congruence is equivalent to $y^2 \equiv -x^2 + a \pmod{p}$. For each fixed $x \in [p]$, there are

$$\left(\frac{-x^2 + a}{p}\right) + 1 = \left(\frac{-1}{p}\right)\left(\frac{x^2 - a}{p}\right) + 1$$

solutions. By Euler's criterion, the binomial theorem, and the discrete Fubini's principle,

$$\begin{aligned} T = \sum_{i=1}^{p} \left(\frac{i^2 - a}{p}\right) &\equiv \sum_{i=1}^{p} (i^2 - a)^{\frac{p-1}{2}} \\ &\equiv \sum_{i=1}^{p} \sum_{j=0}^{\frac{p-1}{2}} \binom{\frac{p-1}{2}}{j} i^{2j} a^{\frac{p-1}{2} - j} \\ &\equiv \sum_{j=0}^{\frac{p-1}{2}} \left[\binom{\frac{p-1}{2}}{j} a^{\frac{p-1}{2} - j} \cdot \sum_{i=1}^{p} i^{2j} \right] \pmod{p}. \end{aligned}$$

Except for $j = 0$ and $j = \dfrac{p-1}{2}$, the first part of the problem says that

$$\sum_{i=1}^{p} i^{2j} \equiv 0 \pmod{p}.$$

For $j = 0$, this sum is p, which is also 0 modulo p. Finally, we are left with $j = \dfrac{p-1}{2}$, which yields

$$T \equiv \binom{\frac{p-1}{2}}{\frac{p-1}{2}} a^0(-1) \equiv -1 \pmod{p},$$

by the first part of the problem. By the definition of the Legendre symbol, the quantity T must be an integer in the interval $[-p, p]$. Since we now know that $T \equiv -1 \pmod{p}$, we get that $T = p - 1$ or $T = -1$. Now we split the argument into two cases: $p \mid a$ or $p \nmid a$:

- Suppose $p \mid a$. Then

  $$T = \sum_{i=1}^{p} \left(\frac{i^2 - a}{p}\right) = \sum_{i=1}^{p} \left(\frac{i^2}{p}\right) = p - 1,$$

  since non-zero squares have Legendre symbol 1, and a zero square has Legendre symbol 0.

- Suppose $p \nmid a$. Suppose, for contradiction, that $T = \displaystyle\sum_{i=1}^{p} \left(\frac{i^2 - a}{p}\right) = p - 1$. Since there are p terms, it is not difficult to see by the definition of the Legendre symbol that $p - 1$ of the summands must be 1, and 1 of the summands must be 0 (in particular, convince yourself that none of the summands can be -1). So some $i \in [p]$ satisfies

  $$\begin{aligned} i^2 - a &\equiv 0 \pmod{p} \\ i^2 &\equiv a \pmod{p} \\ (p-i)^2 &\equiv a \pmod{p}. \end{aligned}$$

  If $p - i \equiv i \pmod{p}$, then $p \mid 2i$, so $p \mid 2$ or $p \mid i \mid a$, both of which are contradictions. So $p - i$ is an index distinct from i that results in a summand of 0. But then T is capped at $p - 2$, which is a contradiction. So we are forced into $T = -1$ if $p \nmid a$.

Therefore, the number of solution (x, y) to $x^2 + y^2 \equiv a \pmod{p}$ is

$$\begin{aligned} \sum_{i=1}^{p} \left[\left(\frac{-1}{p}\right)\left(\frac{i^2 - a}{p}\right) + 1\right] &= \left(\frac{-1}{p}\right) \cdot \sum_{i=1}^{p} \left(\frac{i^2 - a}{p}\right) + p \\ &= \begin{cases} (-1)^{\frac{p-1}{2}} \cdot (p-1) + p & \text{if } p \mid a \\ (-1)^{\frac{p+1}{2}} + p & \text{if } p \nmid a \end{cases}. \end{aligned}$$

Indeed, the number of solutions is independent of a if a is non-zero modulo p.

Solution 11.17. Note that $\dfrac{p+1}{4}$ is an integer because $p \equiv 3 \pmod 4$.The integers $\pm a^{\frac{p+1}{4}}$ work because, by Euler's criterion,

$$\left(\pm a^{\frac{p+1}{4}}\right)^2 \equiv a^{\frac{p+1}{2}} \equiv a \cdot a^{\frac{p-1}{2}} \equiv a \pmod p.$$

Moreover, they are distinct because if $a^{\frac{p+1}{4}} \equiv -a^{\frac{p+1}{4}} \pmod p$, then taking them both to the same same side and cancelling the factor of 2 would imply that $p \mid a$ by Euler's criterion, which we know to be untrue. Finally, if $x^2 \equiv y^2 \pmod p$, then we know that $x \equiv \pm y \pmod p$, so there can be no more than two distinct "square roots" of a. So there are exactly two distinct square roots of a modulo p and they are congruent to $\pm a^{\frac{p+1}{4}}$.

Solution 11.18. Suppose b is an integer such that $\left(\dfrac{b}{p}\right) = -1$. Let $p = 4k+3$ for some non-negative integer k. By Euler's criterion,

$$-1 \equiv b^{\frac{p-1}{2}} \equiv b^{2k+1} \pmod p,$$

which implies that

$$b \equiv -(b^{k+1})^2 \pmod p.$$

So b is congruent to the negative of the quadratic residue $(b^{k+1})^2$ modulo p.

Solution 11.23. By the difference of squares factorization and the Sophie Germain factorization,

$$\begin{aligned} x^8 - 2^4 &= (x^4 - 2^2)(x^4 + 2^2) \\ &= (x^2 - 2)(x^2 + 2)(x^2 - 2x + 2)(x^2 + 2x + 2) \\ &= (x^2 - 2)(x^2 + 2)((x-1)^2 + 1)((x+1)^2 + 1). \end{aligned}$$

If we can show that, for each prime p there exists an integer x such that p divides this expression, then we will have shown that 2^4 is an example of an integer that is not an eight power of an integer but is an eighth power modulo every prime, thereby disproving Chowla's conjecture.

- If $p = 2$, then we can pick any even integer x and then $x^8 - 2^4$ will be divisible by 2. So we can assume that p is odd in the remaining cases, meaning $p \equiv \pm 1 \pmod 4$.
- If $p \equiv 1 \pmod 4$, then
$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}} = 1.$$
So there exists an integer x such that $p \mid (x-1)^2 + 1$. We could equally well use the factor $(x+1)^2 + 1$.
- If $p \equiv 3 \pmod 4$, then $p \equiv 3 \pmod 8$ or $p \equiv 7 \pmod 8$.

– If $p \equiv 7 \pmod 8$, then

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}} = (-1)^{(p-1)\cdot\frac{p+1}{8}} = 1.$$

So there exists an integer x such that $p \mid x^2 - 2$.

– If $p \equiv 3 \pmod 8$, then

$$\left(\frac{-2}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{2}{p}\right) = (-1)^{\frac{p-1}{2}} \cdot (-1)^{\frac{p^2-1}{8}} = (-1)^{(p-1)\cdot\frac{p+5}{8}} = 1.$$

So there exists an integer x such that $p \mid x^2 + 2$.

Now we tackle the weaker conjecture. We would like to use the prime factorization of a, but for that we need to know that $|a| \geq 2$. If $a = 0$ or $a = 1$, then a is a perfect power (in fact, of every kind) so we are done. If $a = -1$, then we do casework on whether $2 \mid k$. If $2 \mid k$ and $a = -1$ is a k^{th} power residue modulo every integer n, then -1 is a quadratic residue modulo every prime p. The first supplement to quadratic reciprocity then implies that every prime is congruent to $1 \pmod 4$, which is untrue. So in this case, -1 is not even a possible value of a, as the hypothesis cannot hold. If k is odd, then $(-1)^k = -1$, so -1 is indeed a perfect k^{th} power as an integer. Having taken care of $a = 0, \pm 1$, let the prime factorization of a be

$$a = \pm p_1^{e_1} p_2^{e_2} \cdots p_m^{e_m}$$

for some positive integer m. We want to show that e_i is a positive multiple of k for each $i \in [m]$. Interestingly, it is actually enough to only consider the magical modulus

$$\mu = p_1^{e_1+1} p_2^{e_2+1} \cdots p_m^{e_m+1}.$$

In this modulus, the hypothesis asserts that there exists an integer x such that

$$x^k \equiv a \pmod \mu.$$

Then, by considering the prime factorization of a, we find that

$$\begin{aligned} x^k &\equiv a \equiv 0 \pmod{p_i^{e_i}}, \\ x^k &\equiv a \not\equiv 0 \pmod{p_i^{e_i+1}}, \end{aligned}$$

for each $i \in [m]$. So the maximal power of p_i that divides x^k is $p_i^{e_i}$. Thus,

$$k \cdot \nu_{p_i}(x) = \nu_{p_i}(x^k) = \nu_{p_i}(a) = e_i,$$

which means $k \mid p_i$. Since this is true for every $i \in [m]$, a is a k^{th} power as an integer.

Solution 11.28. The first part will help with the second part.

1. If $(a, n) \neq 1$, then $p_i \mid a$ for some $i \in [k]$ and so $\left(\frac{a}{p_i}\right) = 0$, causing $\left(\frac{a}{n}\right) = 0$.

2. If $(a,n)=1$, then $\left(\frac{a}{p_i}\right)=\pm 1$ for each i, so $\left(\frac{a}{n}\right)=\pm 1$ as well. If a is a quadratic residue modulo n, then a is a quadratic residue modulo every prime factor of n. Then $\left(\frac{a}{p_i}\right)=1$ for each i, which yields $\left(\frac{a}{n}\right)=1$. For the second assertion, if $\left(\frac{a}{n}\right)=-1$, then $\left(\frac{a}{n}\right)\neq 0$, so the contrapositive of the first part of the problem shows that $(a,n)=1$. The rest is the contrapositive of what we just proved.

3. For the counterexample, the idea is to construct an integer a coprime to some n such that a is a quadratic non-residue modulo exactly two of the prime factors of n in order to get double (-1)'s to cancel out (and the fact that a is a non-residue moduli a prime factor of n implies that a is a non-residue modulo n). Then we will have $\left(\frac{a}{n}\right)=1$ even though a is a quadratic non-residue modulo n. Modulo 3, the only quadratic non-residue is 2. Modulo 5, again 2 is a quadratic non-residue. The list of quadratic residues modulo $3\cdot 5=15$ is $0,1,2,4,6,9,10$, which does not include 2. At the same time,
$$\left(\frac{2}{15}\right)=\left(\frac{2}{3}\right)\left(\frac{2}{5}\right)=(-1)\cdot(-1)=1,$$
even though 2 is a quadratic non-residue modulo 15.

Solution 12.2. Let $m=2^k a$, where k is a non-negative integer and $a>1$ is an odd integer. We want to prove that $2^m=1$ is composite, for which it suffices to find a factor that is strictly in between 1 and 2^m+1. Essentially by using the factorization for the sum of two odd powers, we try to divide by $2^{2^k}+1$. This gives
$$2^m+1=2^{2^k a}+1=\left(2^{2^k}\right)^a+1\equiv(-1)^a+1\equiv -1+1\equiv 0 \pmod{2^{2^k}+1}$$
and the factor $2^{2^k}+1$ lies in the desired interval because
$$1<2^{2^k}+1<2^{2^k a}+1=2^m+1.$$

Solution 12.6. If $n\geq 2$ is composite, then n has a factor a strictly between 1 and n. Inspired by the difference of powers factorization,
$$2^n-1\equiv(2^a)^{\frac{n}{a}}-1\equiv 1^{\frac{n}{a}}-1\equiv 0 \pmod{2^a-1}.$$
So 2^a-1 is a factor of 2^n-1 that satisfies the strict inequalities
$$1<2^a-1<2^n-1,$$
which means 2^n-1 is composite. The contrapositive follows immediately.

Solution 12.8. Suppose m and n are non-negative integers such that

$$M_n = 1 + 2 + \cdots + n = \frac{n(n+1)}{2}.$$

We can then perform the following reversible manipulations:

$$\begin{aligned} 2^m - 1 &= \frac{n(n+1)}{2} \\ 2^{m+1} - 2 &= n^2 + n \\ 2^{m+3} - 7 &= (2n+1)^2. \end{aligned}$$

According to Ramanujan-Nagell, the possible values of $2n+1$ are $1, 3, 5, 11, 181$. So the possible values of n are

$$0, 1, 2, 5, 90,$$

and so the triangular Mersenne numbers are

$$0, 1, 3, 15, 4095.$$

The numbers in this last list are called the Ramanujan-Nagell numbers.

Solution 12.22. We will generalize the proof of the fact that there are infinitely many primes $p \equiv 1 \pmod 8$. For each positive integer n, define the polynomial

$$P_n(x) = x^{2^{n-1}} + 1.$$

Suppose, for contradiction, that there are only finitely many primes $p_1, p_2 \ldots, p_m$ such that $p_i \equiv 1 \pmod{2^n}$. Let

$$N = 2p_1p_2 \cdots p_m.$$

Then N is even, which makes

$$f(N) = N^{2^{n-1}} + 1 = (2p_1p_2 \cdots p_m)^{2^{n-1}} + 1 \geq 2 + 1 = 3$$

odd, so it has an odd prime factor q. We can see that q cannot be 2 or be among the p_i, so it suffices to get a contradiction by showing that $q \equiv 1 \pmod{2^n}$. From the fact that q divides $f(N)$, we get

$$\begin{aligned} N^{2^{n-1}} &\equiv -1 \pmod q, \\ N^{2^n} &\equiv (-1)^2 \equiv 1 \pmod q. \end{aligned}$$

So $\operatorname{ord}_q(N)$ is a power of 2 that is less than or equal to 2^n, but it can be no lower than 2^n because otherwise we could take sufficiently many squares to get $N^{2^{n-1}} \equiv 1 \pmod q$, which is a contradiction since $q \neq 2$ ($q = 2$ is the only modulus where 1 is congruent to -1). So $\operatorname{ord}_q(N) = 2^n$. Since $q \nmid N$, Fermat's little theorem yields

$$N^{q-1} \equiv 1 \pmod q,$$

so $\operatorname{ord}_q(N)$ divides $q - 1$. Therefore, $q \equiv 1 \pmod{2^n}$, as desired.

Solution 13.3. We make the suppositions stated in the problem, and prove each case of the LTE lemma, as listed in Theorem 13.2:

1. Suppose p is a prime, possibly $p = 2$.

   (a) Suppose $p \nmid n$ and $p \mid a-b$. For odd p, it is immediately true from the supposition that
   $$\nu_p(a^n - b^n) = \nu_p(a - b)$$
   since $\nu_p(n) = 0$ follows from $p \nmid n$.
   Now suppose $p = 2$. If we can assume that $4 \mid a - b$, then it follows from the supposition for $p = 2$ that
   $$\nu_p(a^n - a^n) = \nu_p(a - b) + \nu_p(n) = \nu_p(a - b).$$
   So we suppose otherwise, that $a - b = 4t + 2$ for some integer t. Then
   $$a + b = 4t + 2 + 2b = 2(2t + 1 + b),$$
   where $2 \mid 2t + 1 + b$ because $2 \nmid b$. As a result, $4 \mid a + b$, and, by a quick modular arithmetic argument, $4 \mid a^n + b^n$ as well, due to the oddness of n. By the supposition for $p = 2$,
   $$\nu_2(a^n + b^n) = \nu_2(a^n - (-b)^n) = \nu_2(a - (-b)) + \nu_2(n) = \nu_2(a + b).$$
   In a moment, we will also need the fact that
   $$4 \mid (a - b)(a + b) = a^2 - b^2.$$
   Again, using the supposition for $p = 2$ and the above facts,
   $$\begin{aligned}\nu_2(a^n - b^n) &= \nu_2((a^2)^n - (b^2)^n) - \nu_2(a^n + b^n)\\ &= \nu_2(a^2 - b^2) + \nu_2(n) + \nu_2(a + b)\\ &= \nu_2(a - b) + \nu_2(a + b) - \nu_2(a + b)\\ &= \nu_2(a - b).\end{aligned}$$

   (b) Suppose $p \nmid n$ and $p \mid a+b$ and n is odd. As shown in the proof of LTE, it follows from 1(a) that
   $$\nu_p(a^n + b^n) = \nu_p(a + b).$$

2. Suppose p is an odd prime.

   (a) Suppose $p \mid a - b$. The odd case of the supposition states that
   $$\nu_p(a^n - b^n) = \nu_p(a - b) + \nu_p(n).$$

   (b) Suppose $p \mid a+b$ and n is odd. It was derived from 2(a) in the proof of LTE that
   $$\nu_p(a^n + b^n) = \nu_p(a + b) = \nu_p(n).$$

3. Suppose $p = 2$.

(a) Suppose $2 \nmid n$ and $2 \mid a-b$. This is the $p=2$ case of 1(a).

(b) Suppose $2 \mid n$ and $2 \mid a-b$. As shown in the proof of LTE, it follows from 1(a) that
$$\nu_2(a^n - b^n) = \nu_2(a-b) + \nu_2(a+b) + \nu_2(n) - 1.$$
The proof is a little long though, so it might be worth remembering this case separately.

(c) Suppose $4 \mid a-b$. The $p=2$ case of the supposition states that
$$\nu_2(a^n - b^n) = \nu_2(a-b) + \nu_2(n).$$

Solution 13.4. The following conditions are equivalent for all positive integers ℓ:
$$\begin{aligned}(ab^{-1})^\ell \equiv 1 \pmod p &\iff a^\ell \equiv b^\ell \pmod p \\ &\iff p \mid a^\ell - b^\ell.\end{aligned}$$
So the minimal $\ell \in \mathbb{Z}_+$ such that
$$p \mid a^\ell - b^\ell$$
is the same as the minimal $\ell \in \mathbb{Z}_+$ such that
$$(ab^{-1})^\ell \equiv 1 \pmod p,$$
the latter being
$$k = \operatorname{ord}_p(ab^{-1}) = \operatorname{ord}_p(a^{-1}b).$$
For the second part,
$$\begin{aligned}p \mid a^n - b^n &\iff a^n \equiv b^n \pmod p \\ &\iff (ab^{-1})^n \equiv 1 \pmod p \\ &\iff k = \operatorname{ord}_p(ab^{-1}) \mid n.\end{aligned}$$
Finally, in the case that $p \mid a^n - b^n$ or $k \mid n$ (and therefore both), the LTE lemma (Theorem 13.2) says that
$$\begin{aligned}\nu_p(a^n - b^n) &= \nu_p((a^k)^{\frac{n}{k}} - (b^k)^{\frac{n}{k}}) \\ &= \nu_p(a^k - b^k) + \nu_p\left(\frac{n}{k}\right),\end{aligned}$$
where we used $p \mid a^k - b^k$, as its required to use LTE in this way.

Solution 13.12. We prove these in succession, concluding with a formula for $\Phi_{pq}(x)$.

1. This follows from Theorem 13.11 because the only positive divisors of p are p and 1.

2. Using part (1),
$$\Phi_p(x) = \frac{x^p - 1}{\Phi_1(x)} = \frac{x^p - 1}{x - 1} = x^{p-1} + x^{p-2} + \cdots + x^2 + x + 1.$$

3. Theorem 13.11 takes care of it because the only positive divisors of pq are $pq, p, q, 1$.

4. By part (2),

$$\Phi_q(x^p) = \frac{(x^p)^q - 1}{x^p - 1} = \frac{x^{pq} - 1}{\Phi_p(x)\Phi_1(x)} \implies x^{pq} - 1 = \Phi_q(x^p)\Phi_p(x)\Phi_1(x).$$

   By part (3),

$$x^{pq} - 1 = \Phi_{pq}(x)\Phi_p(x)\Phi_q(x)\Phi_1(x).$$

   Equating the two and cancelling the common factors yields the desired formula.

5. By part (4),

$$\begin{aligned}\Phi_p(x^q) &= \Phi_{pq}(x)\Phi_p(x),\\ \Phi_q(x^p) &= \Phi_{pq}(x)\Phi_q(x).\end{aligned}$$

   By part (3),

$$\Phi_{pq}(x) = \frac{x^{pq} - 1}{\Phi_p(x)\Phi_q(x)\Phi_1(x)}.$$

   Consequently,

$$\begin{aligned}\Phi_q(x^p)\Phi_p(x^q)\Phi_1(x) &= \Phi_{pq}(x)\Phi_p(x)\Phi_{pq}(x)\Phi_q(x)\Phi_1(x)\\ &= \frac{x^{pq} - 1}{\Phi_p(x)\Phi_q(x)\Phi_1(x)} \cdot \Phi_p(x)\Phi_{pq}(x)\Phi_q(x)\Phi_1(x)\\ &= (x^{pq} - 1)\Phi_{pq}(x).\end{aligned}$$

6. By part (2),

$$\begin{aligned}\Phi_q(x^p) &= \frac{x^{pq} - 1}{x^p - 1},\\ \Phi_p(x^q) &= \frac{x^{pq} - 1}{x^q - 1}.\end{aligned}$$

   By part (5) and substitution,

$$\begin{aligned}\Phi_{pq}(x) &= \frac{\Phi_q(x^p)\Phi_p(x^q)\Phi_1(x)}{x^{pq} - 1}\\ &= \frac{\frac{x^{pq}-1}{x^p-1} \cdot \frac{x^{pq}-1}{x^q-1} \cdot (x - 1)}{x^{pq} - 1}\\ &= \frac{(x^{pq} - 1)(x - 1)}{(x^p - 1)(x^q - 1)}.\end{aligned}$$

The final conclusion could also be easily reached by using the formula in Theorem 13.14, avoiding all of the manipulations in this solution.

Solution 13.16. For this palindromic property, it is equivalent to prove

$$x^{\varphi(n)} \cdot \Phi_n\left(\frac{1}{x}\right) = \Phi_n(x).$$

According to Theorem 3.21, $\mathrm{Id} = S_\varphi$, so the Möbius inversion formula (Theorem 3.18) tells us that $\varphi = \mu * \mathrm{Id}$. As a result,

$$\begin{aligned}
x^{\varphi(n)} \cdot \Phi_n\left(\frac{1}{x}\right) &= x^{(\mu*\mathrm{Id})(n)} \cdot \prod_{d|n} \left(\frac{1}{x^d} - 1\right)^{\mu\left(\frac{n}{d}\right)} \\
&= x^{\sum_{d|n} d\cdot\mu\left(\frac{n}{d}\right)} \cdot \prod_{d|n} \left(\frac{1}{x^d} - 1\right)^{\mu\left(\frac{n}{d}\right)} \\
&= \prod_{d|n} (1 - x^d)^{\mu\left(\frac{n}{d}\right)} \\
&= (-1)^{\sum_{d|n} \mu\left(\frac{n}{d}\right)} \cdot \prod_{d|n} (x^d - 1)^{\mu\left(\frac{n}{d}\right)} \\
&= (-1)^{S_\mu(n)} \cdot \prod_{d|n} (x^d - 1)^{\mu\left(\frac{n}{d}\right)}.
\end{aligned}$$

Using the fact that $S_\mu = \varepsilon$ and $n \neq 1$, the power $(-1)^{S_\mu(n)}$ disappears, leaving us with

$$x^{\varphi(n)} \cdot \Phi_n\left(\frac{1}{x}\right) = \prod_{d|n} (x^d - 1)^{\mu\left(\frac{n}{d}\right)} = \Phi_n(x).$$

Therefore, all cyclotomic polynomials (except for $n = 1$) are symmetric.

Solution 13.20. We prove the results in succession:

1. If n is odd, then, by Theorem 13.18,

$$\begin{aligned}
\Phi_{2n}(x) &= \frac{\Phi_n(x^2)}{\Phi_n(x)} \\
&= \frac{\prod_{d|n} (x^{2d} - 1)^{\mu\left(\frac{n}{d}\right)}}{\prod_{d|n} (x^d - 1)^{\mu\left(\frac{n}{d}\right)}} = \frac{\prod_{d|n} \left[(x^d - 1)(x^d + 1)\right]^{\mu\left(\frac{n}{d}\right)}}{\prod_{d|n} (x^d - 1)^{\mu\left(\frac{n}{d}\right)}} \\
&= \prod_{d|n} (x^d + 1)^{\mu\left(\frac{n}{d}\right)} \\
&= (-1)^{\sum_{d|n} \mu\left(\frac{n}{d}\right)} \cdot \prod_{d|n} (-x^d - 1)^{\mu\left(\frac{n}{d}\right)} = (-1)^{\sum_{d|n} \mu(d)} \cdot \prod_{d|n} ((-x)^d - 1)^{\mu\left(\frac{n}{d}\right)} \\
&= (-1)^{S_\mu(n)} \cdot \Phi_n(-x).
\end{aligned}$$

   Since $n > 1$, $S_\mu(n) = \varepsilon(n) = 0$, so the expression is $\Phi_n(-x)$.

2. According to Problem 13.12,

$$\Phi_p(x) = 1 + x + x^2 + \cdots + x^{p-1}.$$

By part (1),

$$\Phi_{2p}(x) = \Phi_p(-x) = 1 - x + x^2 - \cdots + x^{p-1},$$

where the sign on the rightmost term x^{p-1} is positive because p is odd.

3. By Theorem 13.18,

$$\Phi_{p^k}(x) = \Phi_{p \cdot p^{k-1}}(x) = \Phi_p(x^{p^{k-1}}).$$

The rest follows from the formula

$$\Phi_p(x) = 1 + x + x^2 + \cdots + x^{p-1}$$

in Problem 13.12.

4. If p is an odd prime, and therefore not divisible by 2, then by Theorem 13.18,

$$\begin{aligned}\Phi_{2^\ell p^k}(x) &= \Phi_{2p \cdot 2^{\ell-1} p^{k-1}}(x) \\ &= \Phi_{2p \cdot p^{k-1}}(x^{2^{\ell-1}}) \\ &= \Phi_{2p}(x^{2^{\ell-1} p^{k-1}}).\end{aligned}$$

The result follows from the formula in part (2).

Solution 13.22. By the fact that

$$x^n - 1 = \prod_{d|n} \Phi_d(x)$$

from Theorem 13.11, we can use strong induction to show that

$$-1 = 0^n - 1 = (0-1) \cdot \prod_{\substack{d|n \\ d \neq 1}} \Phi_d(0) \implies \prod_{\substack{d|n \\ d \neq 1}} \Phi_d(0) = 1 \implies \Phi_n(0) = 1,$$

where, in the last step, we used the induction hypothesis that $\Phi_d(0) = 1$ for all $2 \leq d < n$. Note that the base case $n = 2$ holds because

$$\Phi_2(x) = x + 1 \implies \Phi_2(0) = 1,$$

and that a base of $n = 1$ would not work because

$$\Phi_1(x) = x - 1 \implies \Phi_1(0) = -1.$$

An alternate proof is that, by Theorem 13.14,

$$\Phi_n(x) = \prod_{d|n} (x^d - 1)^{\mu\left(\frac{n}{d}\right)} = \prod_{d|n} (x^{\frac{n}{d}} - 1)^{\mu(d)},$$

so we get

$$\Phi_n(0) = \prod_{d|n} (-1)^{\mu(d)} = (-1)^{\sum_{d|n} \mu(d)} = (-1)^{S_\mu(n)} = (-1)^{\varepsilon(n)}.$$

Since $\varepsilon(n) = 0$ for $n > 1$, we are done.

Solution 13.23. According to Problem 13.20,

$$\Phi_{p^k}(x) = 1 + x^{p^{k-1}} + x^{2p^{k-1}} + \cdots + x^{(p-1)p^{k-1}},$$

so $\Phi_{p^k}(1) = p$ for all primes p and positive integers k.
On the other hand, suppose n is not a prime power. Then the fact that

$$(x-1)(x^{n-1} + x^{n-2} + \cdots + x^2 + x + 1) = x^n - 1 = \prod_{d|n} \Phi_d(x)$$

leads to

$$x^{n-1} + x^{n-2} + \cdots + x^2 + x + 1 = \prod_{\substack{d|n \\ d\neq 1}} \Phi_d(x).$$

Substituting $x = 1$ yields

$$\prod_{\substack{d|n \\ d\neq 1}} \Phi_d(1) = n.$$

Let the prime factorization of n be

$$n = p_1^{e_1} p_2^{e_2} \cdots p_t^{e_t}.$$

For each (not necessarily maximal) prime power $p_i^{f_i}$ (with $1 \leq f_i \leq e_i$) that divides n, the first part of problem yields

$$\Phi_{p_i^{f_i}}(1) = p_i.$$

So, for each $i \in [n]$,

$$\Phi_{p_i^1}(1)\Phi_{p_i^2}(1) \cdots \Phi_{p_i^{e_i}}(1) = p_i^{e_i}.$$

As a result,

$$\prod_{i=1}^{t} \prod_{j=1}^{e_i} \Phi_{p_i^j}(1) = \prod_{i=1}^{t} p_i^{e_i} = n = \prod_{\substack{d|n \\ d\neq 1}} \Phi_d(1).$$

All of the multiplicands that appear on the left also appear on the right, so cancelling them leaves us with

$$\prod_{\substack{d|n \\ d \text{ not prime power}}} \Phi_d(1) = 1.$$

Since cyclotomic polynomials are positive everywhere, $\Phi_d(1) = 1$ for all non-prime power divisors d of n, including $d = n$.

Solution 13.29. If $p \mid \Phi_q(a)$, then Theorem 13.26 implies $q \mid p-1$ or $p \mid q$. The former case is equivalent to

$$p \equiv 1 \pmod{q}.$$

The latter case is equivalent to $p = q$ because p and q are primes.

Solution 13.34. Recall from Lemma 13.32 that

$$\prod_{d|n} \Psi_d(a,b) = a^n - b^n.$$

If $p \mid \Psi_n(a,b)$, then $p \mid a^n - b^n$. By Problem 13.4, we get $k \mid n$.

Solution 13.41. The problem statement is equivalent to saying that there exists a prime p such that $p \mid a^n - 1$ but $p \nmid a^k - 1$ for all $k \in [n-1]$. This is true by Zsigmondy's theorem for $b = 1$, with the only potential exception (when $n \geq 3$) being $(a,b,n) = (2,1,6)$. In that case, we need a prime p such that

$$p \mid a^n - 1 = 2^6 - 1 = 63 = 3^2 \cdot 7,$$

so $p = 3$ or $p = 7$. If $p = 3$, then $3 \mid 2^2 - 1 = a^2 - 1$. If $p = 7$, then $7 \mid 2^3 - 1 = a^3 - 1$. As state, every other case works by Zsigmondy.
If $n = 2$, let $a = 3$. If a suitable prime p exists, then

$$p \mid a^n - 1 = 3^2 - 1 = 8 = 2^3 \implies p = 2.$$

In this case,

$$\operatorname{ord}_p(a) = \operatorname{ord}_2(3) = 1 < 2 = n.$$

Solution 13.42. The statement that $p \mid a^k + b^k$ is equivalent to

$$(ab^{-1})^k \equiv -1 \pmod{p}.$$

Note that $p \neq 2$ because, if $p \mid a^n + b^n$, then a, b have the same parity (odd, due to coprimality), so $p \mid a^k + b^k$ for all positive integers k. So $p \geq 3$ is an odd prime. Since the true statement $p \mid a^n + b^n$ is equivalent to

$$(ab^{-1})^n \equiv -1 \pmod{p},$$

the statement that $(ab^{-1})^k \equiv -1 \pmod{p}$ is equivalent, by multiplication and its inverse division, to

$$(ab^{-1})^{k-n} \equiv 1 \pmod{p}.$$

We know that $(ab^{-1})^n \equiv -1 \pmod{p}$ and that this is true for no lower exponent, so Problem 9.25 tells us that $\operatorname{ord}_p(ab^{-1}) = 2n$. Thus, for integers k such that $1 \leq k - n \leq 2n - 1$, which is equivalent to $n + 1 \leq k \leq 3n - 1$,

$$(ab^{-1})^{k-n} \not\equiv 1 \pmod{p}.$$

Solution 13.44. In order to use Zsigmondy, we will require $n \geq 2$, so we will handle $n = 1$ separately first. In the addition case, $a + b \geq 1 + 1 \geq 2$ has a prime factor, so

$$\tau(a^1 + b^1) \geq 2 = 2^{\tau(1)}.$$

In the subtraction case, $a - b \geq 2$ has a prime factor, so

$$\tau(a^1 - b^1) \geq 2 = 2^{\tau(1)}.$$

Now assume $n \geq 2$ in both cases.

1. Addition: If d is a positive divisor of n, then the fact that $3 \nmid n$ implies $d \neq 3$, so the exceptional case of $(a, b, d) = (2, 1, 3)$ in Zsigmondy for addition is a triple that would not occur when $d \mid n$. In ascending order, let the positive divisors of n be

   $$1 = d_1 < d_2 < \cdots < d_{\tau(n)} = n.$$

   By Zsigmondy for addition, since $a > b$ are coprime, for each $i \in [\tau(n)]\backslash\{1\}$, there exists a prime r_i such that $r_i \mid a^{d_i} + b^{d_i}$, but $r_j \nmid a^{d_j} + b^{d_j}$ for all $j \in [i-1]$. We have intentionally skipped $i = 1$ for now because here $i - 1 = 0$, implying any argument involving the non-existent $[i-1]$ would be nonsensical. Iterating through

   $$i = 2, 3, \ldots, \tau(n) - 1, \tau(n)$$

   produces a new prime r_i each time that has not previously appeared in this list of primes and that divides $a^n + b^n$, since

   $$r_i \mid a^{d_i} + b^{d_i} \mid a^n + b^n$$

   by virtue of n and all of its divisors d_i being odd (recall $2 \nmid n$). The reason that each r_i is distinct is that if $r_{i_1} = r_{i_2}$ for some indices $i_1, i_2 \in [\tau(n)]\backslash\{1\}$ such that $i_1 < i_2$, then the fact that $r_{i_1} \mid a^{d_{i_1}} + b^{d_{i_1}}$ would contradict the fact that $r_{i_2} \nmid a^{d_{i_1}} + b^{d_{i_1}}$. There are $\tau(n) - 1$ of the r_i. Finally, for all $i \in [\tau(n)]\backslash\{1\}$,

   $$a + b \mid a^{d_i} + b^{d_i} \mid a^n + b^n,$$

   this introduces a prime factor r_1 of $a + b \geq 2$ that divides $a^n + b^n$ but is distinct from all of the other r_i. Indeed, r_1 is new because otherwise there would exist an $r_i = r_1$ for $i \geq 2$ that divides $a^1 + b^1$.

2. Subtraction: This case is almost exactly the same as the addition case. We use the ordinary Zsigmondy's theorem instead of Zsigmondy for addition instead though. The only other extra considerations are that are that $2 \nmid n$ omits the $(a, b, d_i) = (a, b, 2)$ exceptional cases of Zsigmondy, and either of the $2 \nmid n$ or $3 \nmid n$ conditions removes the $(a, b, d_i) = (2, 1, 6)$ case, and the fact that $a - b \geq 2$ ensures that $a - b$ has a final prime factor r_1 to offer.

List of Symbols

Arithmetic

$\mathbb{Z}$	integers
$\mathbb{Z}_+$	positive integers
$\mathbb{Z}_{\geq 0}$	non-negative integers
$\mathbb{Q}$	rational numbers
$\mathbb{Q}_+$	positive rationals
$\mathbb{Q}_{\geq 0}$	non-negative rationals
$\mathbb{R}$	real numbers
$\mathbb{R}_+$	positive reals
$\mathbb{R}_{\geq 0}$	non-negative reals
$\mathbb{C}$	complex numbers
$\pm$	plus or minus
$<, >$	strict inequality
$\leq, \geq$	non-strict inequality

Functions

$\lfloor \cdot \rfloor$	floor function
$\lceil \cdot \rceil$	ceiling function
max	maximum function
min	minimum function
gcd	greatest common divisor
lcm	least common multiple
det	determinant
$\nu_p(n)$	p-adic valuation
τ	number of positive divisors
σ	sum of positive divisors
σ_x	x^{th} divisor function
ω	number of distinct prime factors
Ω	number of non-distinct prime factors
π	product of positive divisors
$f * g$	Dirichlet convolution
ϵ	unit function
μ	Möbius function
$n!$	factorial
$\binom{n}{k}$	binomial coefficient
φ	Euler's totient function
$\text{ord}_n(a)$	order of a modulo n
$\left(\frac{a}{p}\right)$	Legendre symbol
$\Phi_p(x)$	p^{th} cyclotomic polynomial

Miscellaneous

$\exists$	existential quantifier
$\forall$	universal quantifier
$(a_i)_{i \in I}$	sequence indexed by I
$\sum$	summation notation
$\prod$	product notation
$a \mid b$	a divides b
$a \sim b$	equivalence relation
$a \equiv b \pmod{n}$	modular congruence
n_b	n is written in base-b

$F_n = 2^{2^n} + 1$ the n^{th} Fermat number

$M_n = 2^n - 1$ the n^{th} Mersenne number

Sets

$\varnothing$ empty set

$\in$ element of

$\notin$ not element of

$[n]$ $\{1, 2, \ldots, n\}$ for positive integers n

$[n]^*$ $\{0, 1, 2, \ldots, n\}$ for non-negative integers n

S^c set complement

$\cup$ set union

$\cap$ set intersection

$A \backslash B$ set difference

$A \times B$ Cartesian product of sets

A^n $\underbrace{A \times A \times \cdots \times A}_{n \text{ copies of } A}$

$\mathcal{P}(A)$ power set

$\subseteq$ subset

$\subsetneq$ proper subset

$\supseteq$ superset

Bibliography

"Everything of importance has been said before by somebody who did not discover it."

– *Alfred North Whitehead*

[1] J.L. Ramírez Alfonsín. *The Diophantine Frobenius Problem*. Oxford University Press, 2005.

[2] N. C. Ankeny and C. A. Rogers. "A Conjecture of Chowla". In: *Annals of Mathematics* Second Series 53.3 (1951), pp. 541–550.

[3] Edward J. Barbeau. *Pell's Equation*. Springer, 2003.

[4] Gary Brookfield. "The Coefficients of Cyclotomic Polynomials". In: *Mathematics Magazine* 89.3 (2016), pp. 179–188.

[5] Keith Conrad. *Examples of Mordell's Equation*. URL: https://kconrad.math.uconn.edu/blurbs/gradnumthy/mordelleqn1.pdf.

[6] Arthur Engel. *Problem-Solving Strategies*. Springer, 1998, pp. 1–23, 147.

[7] Nathan Fine. "Binomial Coefficients Modulo a Prime". In: *The American Mathematical Monthly* 54.10 (1947), pp. 589–592.

[8] Carl Friedrich Gauss. *Disquisitiones Arithmeticae*. Yale University Press, 1965, pp. 51–52.

[9] Andrew Granville. *Number Theory Revealed: A Masterclass*. American Mathematical Society, 2019, pp. 177–178.

[10] G. H. Hardy. *A Mathematician's Apology*. Cambridge University Press, 1941, p. 80.

[11] D. H. Lehmer. "Tests for Primality by the Converse of Fermat's Theorem". In: *Bulletin of the American Mathematical Society* 33.3 (1927), pp. 330–331.

[12] MathOverflow. *The modular arithmetic contradiction trick for Diophantine equations*. URL: https://mathoverflow.net/questions/134352/.

[13] Ivan Niven, Herbert S. Zuckerman, and Hugh L. Montgomery. *An Introduction to the Theory of Numbers, fifth edition*. John Wiley and Sons, 1991, pp. 73–74.

[14] Ore Oystein. *Number Theory and its History*. Dover, 1988, pp. 263–267.

[15] Samer Seraj. *An Idempotent Cryptarithm*. 2021. DOI: 10.48550/ARXIV.2106.00382. URL: https://arxiv.org/abs/2106.00382.

[16] Samer Seraj. "Counting general power residues". In: *Notes on Number Theory and Discrete Mathematics* 28.4 (2022), pp. 630–743.

[17] Walter D. Stangl. "Counting Squares in $\mathbb{Z}_n$". In: *Mathematics Magazine* 69.4 (1996), pp. 285–289.

[18] Heidelberg University. *Proofs of the Quadratic Reciprocity Law*. URL: https://www.mathi.uni-heidelberg.de/~flemmermeyer/fchrono.html.

Index

"We raise to degrees (of wisdom) whom We please: but over all endued with knowledge is one, the All-Knowing."
– *Qur'an 12:76*

About the Author

> "Why is it the words we write for ourselves are always so much better than the words we write for others?... You write your first draft with your heart. You rewrite with your head. The first key to writing is to write, not to think."
>
> – *Sean Connery, Finding Forrester*

> "If you would be a real seeker after truth, it is necessary that at least once in your life you doubt, as far as possible, all things."
>
> – *René Descartes*

Samer Seraj is the owner of Existsforall Academy Inc., which is a Canadian company that specializes in mathematical education. During his school years, his participation in math contests culminated in his qualification for the Canadian Mathematical Olympiad and the Asian Pacific Mathematics Olympiad in his senior year of high school. He then spent four years learning higher mathematics and earned his undergraduate degree in mathematics from Trinity College at the University of Toronto. At the time, he won two prestigious research grants, presented papers at several conferences, and was elected as President of the student body's Mathematics Union. After graduation, he worked for four years in a mix of roles as a mathematics instructor, curriculum developer, and personnel manager of a team of over five hundred educators at a company based in San Diego, California. More recently, he founded Existsforall Academy, where he enjoys teaching his students. His recent contributions to the Canadian mathematical community have included being a guest editor of the Canadian Mathematical Society's problem-solving journal, Crux Mathematicorum, sitting on the University of Waterloo CEMC's committee for the Problem of the Month, teaching courses at the University of Toronto's math outreach program, Math+, and serving as a trainer of Team Canada for the International Mathematical Olympiad.

https://existsforall.com/

ISBN 978-1-7389501-2-6