Rund um Kreisteilungspolynome

Moritz Hiebler

1. September 2023

Inhaltsverzeichnis

1 Einheitswurzeln

Zur Definition von Kreisteilungspolynomen müssen wir erst Einheitswurzeln erklären. Zur Übersichtlichkeit und Ästhetik im späteren Verlauf fassen wir uns bewusst allgemein. In diesem Abschnitt sei $R = \mathbb{C}$ oder $R = \mathbb{Z}/m\mathbb{Z}$ für ein ganzes $m \geq 2$. Weiters bezeichne 1_R die Zahl 1 für $R = \mathbb{C}$ bzw. die Restklasse von 1 modulo m für $R = \mathbb{Z}/m\mathbb{Z}$.[1]

Definition 1.1. Sei n eine positive ganze Zahl. Ein Element $\alpha \in R$ heißt

- ◇ eine *n-te Einheitswurzel (in R)*, falls $\alpha^n = 1_R$ gilt, und
- ◇ eine *primitive n-te Einheitswurzel (in R)*, falls außerdem $\alpha^k \neq 1_R$ für alle ganzen $1 \leq k < n$ gilt.

Die Menge aller n-ten Einheitswurzeln in $\mathbb{C}$ sei mit E_n, die aller primitiven n-ten Einheitswurzeln in $\mathbb{C}$ mit P_n bezeichnet. Ein Element $\alpha \in R$ heißt Einheitswurzel, falls es eine positive ganze Zahl n gibt, sodass α eine n-te Einheitswurzel ist.

Bemerkung. Wir erläutern diese Begrifflichkeiten noch ein wenig:

- ◦ Wenn aus dem Zusammenhang klar ist, welcher Menge das Element α zugrundeliegt, so spricht man einfach von Einheitswurzeln, ohne „in R“ zu spezifizieren.
- ◦ Statt „Einheitswurzel in $\mathbb{Z}/m\mathbb{Z}$“ werden wir auch „Einheitswurzel modulo m“ als Sprechweise verwenden.

[1] Der Buchstabe „R“ rührt daher, dass all diese Mengen (mit den entsprechenden Verknüpfungen) Beispiele für sogenannte *Ringe* sind.

- Die Gleichung $\alpha^n = 1_R$ bedarf im Fall $R = \mathbb{Z}/m\mathbb{Z}$ wohl einer Erklärung: Wir rechnen hierbei mit Restklassen[2] und bezeichnen mit $\overline{x}$ die Restklasse einer ganzen Zahl x modulo m (wobei m als bekannt vorausgesetzt). Dann ist α eine Restklasse modulo m, also gleich $\overline{a}$ für ein $a \in \mathbb{Z}$. Mit diesen Bezeichnungen gilt

$$\alpha^n = 1_R \quad \Longleftrightarrow \quad \overline{a}^n = \overline{a^n} = \overline{1} \quad \Longleftrightarrow \quad a^n \equiv 1 \pmod{m};$$

  wir beschäftigen uns also mit speziellen Kongruenzen modulo m.

- Der Begriff „primitiv“ zeichnet bestimmte Einheitswurzeln aus: Eine primitive n-te Einheitswurzel ist eine n-te Einheitswurzel, die für kein kleineres $1 \leq k < n$ eine k-te Einheitswurzel ist. Wir beweisen in Lemma 1.2 gleich einen genaueren Zusammenhang.

Bevor wir die beiden zugrundeliegenden Ringtypen separat betrachten und dort auf Beispiele eingehen, wollen wir erst ein allgemeines Resultat beweisen:

Lemma 1.2. *Sei $n > 0$ ganz und $\alpha \in R$ eine n-te Einheitswurzel in R. Dann gibt es genau eine positive ganze Zahl d, sodass α eine primitive d-te Einheitswurzel ist. Diese Zahl erfüllt $d \mid n$.*

Sind umgekehrt k und ℓ positive ganze Zahlen mit $k \mid \ell$, so ist jede k-te Einheitswurzel auch eine ℓ-te Einheitswurzel.

Beweis. Von allen positiven ganzen Zahlen k, für die α eine k-te Einheitswurzel ist[3], sei d die kleinste. Dann ist α nach Konstruktion eine primitive d-te Einheitswurzel und aufgrund der Minimalitätsvoraussetzung in der Definition ist d auch eindeutig bestimmt.

Für die Teilbarkeitseigenschaft dividieren wir n durch d mit Rest: Sei $n = qd + r$ für nichtnegative ganze Zahlen q und r mit $0 \leq r < d$. Dann gilt

$$1_R = \alpha^n = \alpha^{qd+r} = \alpha^{qd} \cdot \alpha^r = \left(\alpha^d\right)^q \cdot \alpha^r = 1_R^q \cdot \alpha^r = 1_R \cdot \alpha^r = \alpha^r,$$

also ist α eine r-te Einheitswurzel. Wegen der Minimalität von d kommt somit nur $r = 0$ in Frage, was $n = qd$ und daher $d \mid n$ zur Folge hat.

Ist schließlich $\alpha \in R$ eine k-te Einheitswurzel, so gilt $\alpha^k = 1_R$ und deshalb auch $\alpha^\ell = \left(\alpha^k\right)^{\ell/k} = 1_R^{\ell/k} = 1_R$, womit α auch eine ℓ-te Einheitswurzel ist (beachte: $\ell/k \in \mathbb{Z}$ nach Voraussetzung). □

1.1 Einheitswurzeln in $\mathbb{Z}/m\mathbb{Z}$

Um sich mit Einheitswurzeln ein wenig vertraut zu machen, beginnen wir mit einem einführenden *Beispiel.* Wir betrachten die Zweierpotenzen bezüglich den Moduln $m \in \{5, 6, 7, 8\}$:

n	1	2	3	4	5	6	7	8	9
2^n	2	4	8	16	32	64	128	256	512
$2^n \pmod 5$	2	4	3	1	2	4	3	1	2
$2^n \pmod 6$	2	4	2	4	2	4	2	4	2
$2^n \pmod 7$	2	4	1	2	4	1	2	4	1
$2^n \pmod 8$	2	4	0	0	0	0	0	0	0

Mit der Notation $\overline{2}_m$ für die Restklasse von 2 modulo m für dieses Beispiel können wir schließen:

- In $\mathbb{Z}/5\mathbb{Z}$ ist $\overline{2}_5$ eine vierte und eine achte Einheitswurzel, wobei sie nur eine primitive vierte Einheitswurzel ist (vgl. Lemma 1.2). Die Tabelle zeigt außerdem, dass $\operatorname{ord}_5(2) = 4 = \varphi(5)$ gilt und 2 daher eine Primitivwurzel modulo 5.

- In $\mathbb{Z}/6\mathbb{Z}$ ist $\overline{2}_6$ keine Einheitswurzel, weil alle Zweierpotenzen mit 6 den Teiler 2 gemeinsam haben und damit nie kongruent zu 1 modulo 6 werden können. Die Ordnung von 2 modulo 6 kann aus diesem Grund auch nicht definiert werden und Überlegungen zu Primitivwurzeln sind ebenfalls sinnlos.

[2] womit das Gleichheitszeichen legitimiert wird

[3] solche gibt es nach Voraussetzung, wie die Zahl n selbst

- In $\mathbb{Z}/7\mathbb{Z}$ ist $\overline{2}_7$ eine primitive dritte Einheitswurzel und somit nach Lemma 1.2 eine dritte, sechste und neunte Einheitswurzel, wie wir auch aus obiger Tabelle entnehmen können. Wegen $\operatorname{ord}_7(2) = 3$ und und $\varphi(7) = 6$ ist 2 keine Primitivwurzel modulo 7, obwohl $\overline{2}_7$ eine sechste Einheitswurzel ist.
- In $\mathbb{Z}/8\mathbb{Z}$ ist $\overline{2}_8$ offenbar auch keine Einheitswurzel aus demselben Grund wie für $m = 6$; hier zeigt es sich nur drastischer. Eine Ordnung kann auch hier nicht definiert werden.

Dieses Beispiel legt nahe, dass Einheitswurzeln modulo m, $m \geq 2$ ganz, eng mit der Ordnung modulo m verwandt sind. Im folgenden Satz präzisieren wir diese Vermutung, indem wir (primitive) Einheitswurzeln in $\mathbb{Z}/m\mathbb{Z}$ durch die zugehörige Ordnung modulo m charakterisieren und damit auch die Begriffe primitive Einheitswurzeln und Primitivwurzeln modulo m zueinander in Beziehung stellen.

Für eine ganze Zahl x bezeichnen wir dabei mit $\overline{x}$ die Restklasse von x modulo m. Den Beweis überlassen wir zur Festigung des Gelernten zur Übung.

Satz 1 (Einheitswurzeln in $\mathbb{Z}/m\mathbb{Z}$)**.** *Seien $m \geq 2$ und a ganze Zahlen. Dann gelten für alle ganzen $n > 0$ die folgenden Aussagen:*

1. *Genau dann ist $\overline{a}$ eine n-te Einheitswurzel in $\mathbb{Z}/m\mathbb{Z}$, wenn a zu m teilerfremd ist und $\operatorname{ord}_m(a) \mid n$ gilt.*
2. *Genau dann ist $\overline{a}$ eine primitive n-te Einheitswurzel in $\mathbb{Z}/m\mathbb{Z}$, wenn a zu m teilerfremd ist und $\operatorname{ord}_m(a) = n$ gilt.*
3. *Genau dann ist a eine Primitivwurzel modulo m, wenn $\overline{a}$ eine primitive $\varphi(m)$-te Einheitswurzel in $\mathbb{Z}/m\mathbb{Z}$ ist.*

Beweis.

□

1.2 Einheitswurzeln in $\mathbb{C}$

Damit alle Begrifflichkeiten verständlich sind, gehen wir im folgenden Unterkapitel ein paar Grundlagen zu komplexen Zahlen durch.

1.2.1 Exkurs/Wiederholung zu komplexen Zahlen

Komplexe Zahlen z sind definitionsgemäß von der Form $z = x + \mathrm{i}\,y$ für x, $y \in \mathbb{R}$, wobei $\mathrm{i} \in \mathbb{C}$ die imaginäre Einheit mit $\mathrm{i}^2 = -1$ bezeichnet. Man sagt in diesem Fall, z sei in *kartesischen* Koordinaten bzw. in *additiver Darstellung* gegeben, $\operatorname{Re}(z) \coloneqq x$ heißt der *Realteil von z* und $\operatorname{Im}(z) \coloneqq y$ der *Imaginärteil von z*. Durch Addition in kartesischen Koordinaten ergibt sich sofort $\operatorname{Re}(z + w) = \operatorname{Re}(z) + \operatorname{Re}(w)$ bzw. $\operatorname{Im}(z + w) = \operatorname{Im}(z) + \operatorname{Im}(w)$, man sagt auch, die Abbildungen $\operatorname{Re}\colon \mathbb{C} \to \mathbb{R}$ und $\operatorname{Im}\colon \mathbb{C} \to \mathbb{R}$ sind beide additiv.

Für $z \neq 0$ (d. h. $(x, y) \neq (0, 0)$) kann man z (als Vektor von 0 nach $x + \mathrm{i}\,y$ in der Gauß'schen Zahlenebene gedacht) auch eindeutig durch seinen Betrag $|z| \coloneqq r = \sqrt{x^2 + y^2} > 0$ und den mit

der positiven reellen Achse eingeschlossenen Winkel φ wie folgt angeben: z/r hat die Form $x_0 + \mathrm{i}\, y_0$ für die reellen Zahlen $x_0 \coloneqq x/r$, $y_0 \coloneqq y/r$, die $x_0^2 + y_0^2 = 1$ erfüllen. Daher ist $(x_0, y_0) \in \mathbb{R}^2$ ein Punkt auf dem Einheitskreis und kann als $(\cos(\varphi), \sin(\varphi))$ für einen eindeutigen Winkel $\varphi \in [0, 2\pi)$ (in Radianten) geschrieben werden. Dementsprechend gilt

$$\frac{z}{r} = x_0 + \mathrm{i}\, y_0 = \cos(\varphi) + \mathrm{i}\, \sin(\varphi) \qquad \Longleftrightarrow \qquad z = r \cdot (\cos(\varphi) + \mathrm{i}\, \sin(\varphi)).$$

Wenn wir die abkürzende Schreibweise $\mathrm{e}^{\mathrm{i}t} \coloneqq \cos(t) + \mathrm{i}\, \sin(t)$ für $t \in \mathbb{R}$ verwenden[4], erhalten wir die Darstellung von z in *Polarkoordinaten* (oder auch *multiplikative Darstellung*) $z = r \cdot \mathrm{e}^{\mathrm{i}\varphi}$.

In Polarkoordinaten lassen sich komplexe Zahlen in der erhofften Art und Weise multiplizieren: Für beliebige reelle Zahlen α und β gilt

$$\begin{aligned}\mathrm{e}^{\mathrm{i}\alpha} \cdot \mathrm{e}^{\mathrm{i}\beta} &= (\cos(\alpha) + \mathrm{i}\, \sin(\alpha)) \cdot (\cos(\beta) + \mathrm{i}\, \sin(\beta)) = \\ &= \big(\cos(\alpha)\cos(\beta) - \sin(\alpha)\sin(\beta)\big) + \mathrm{i}\, \big(\sin(\alpha)\cos(\beta) + \cos(\alpha)\sin(\beta)\big) = \\ &= \cos(\alpha + \beta) + \mathrm{i}\, \sin(\alpha + \beta) = \mathrm{e}^{\mathrm{i}(\alpha+\beta)}\end{aligned}$$

aufgrund der Additionstheoreme für Sinus und Cosinus. (Umgekehrt liefert die obige Rechnung eine sehr praktische Variante, um die Additionstheoreme herzuleiten!)

Sind nun z, $w \in \mathbb{C} \setminus \{0\}$ mit $z = r \cdot \mathrm{e}^{\mathrm{i}\varphi}$ und $w = s \cdot \mathrm{e}^{\mathrm{i}\psi}$ für reelle Zahlen r, $s > 0$ und φ, $\psi \in [0, 2\pi)$, so gilt

$$z \cdot w = (r \cdot \mathrm{e}^{\mathrm{i}\varphi}) \cdot (s \cdot \mathrm{e}^{\mathrm{i}\psi}) = rs \cdot \mathrm{e}^{\mathrm{i}\varphi} \cdot \mathrm{e}^{\mathrm{i}\psi} = rs \cdot \mathrm{e}^{\mathrm{i}(\varphi+\psi)}$$

gemäß der obigen Rechnung. Das liefert auch die geometrische Interpretation zur Multiplikation zweier komplexer Zahlen in Polarkoordinaten: Die Radien (Beträge) werden multipliziert, d. h. $|zw| = |z| \cdot |w|$, und die Winkel werden addiert (wobei Winkel modulo 2π zu nehmen sind).[5] Insbesondere ist $z^n = r^n \cdot \mathrm{e}^{\mathrm{i}n\varphi}$ für positive ganze Zahlen n, wie man leicht durch vollständige Induktion zeigt.

Für den späteren Gebrauch erwähnen wir auch die komplexe Konjugation: Ist $z = x + \mathrm{i}\, y$ mit x, $y \in \mathbb{R}$ eine komplexe Zahl in kartesischen Koordinaten, so definiert man $\overline{z} \coloneqq x - \mathrm{i}\, y \in \mathbb{C}$ als die zu z *komplex konjugierte* Zahl. Zweifache Anwendung liefert $\overline{\overline{z}} = z$, also wieder die ursprüngliche Zahl. Weiters gelten

$$z + \overline{z} = 2x = 2\,\mathrm{Re}(z), \qquad z - \overline{z} = 2y = 2\,\mathrm{Im}(z) \quad \text{und} \quad z \cdot \overline{z} = x^2 - \mathrm{i}^2\, y^2 = x^2 + y^2 = |z|^2\,, \tag{1}$$

was es ermöglicht, statt mit der additiven Darstellung komplexer Zahlen nur mit der komplexen Konjugation zu arbeiten. Zudem kann auch der Betrag mithilfe der komplexen Konjugation ausgedrückt werden. Aus (1) folgt noch $z \in \mathbb{R} \iff \mathrm{Im}(z) = 0 \iff z = \overline{z}$ sowie $1/z = \overline{z}/\,|z|^2$ für $z \neq 0$. Insbesondere kann durch jede von null verschiedene komplexe Zahl geteilt werden. Darüber hinaus erhalten wir

$$\begin{gathered}z + w + \overline{z + w} = 2\,\mathrm{Re}(z + w) = 2\,\mathrm{Re}(z) + 2\,\mathrm{Re}(w) = z + \overline{z} + w + \overline{w} \\ zw \cdot \overline{zw} = |zw|^2 = |z|^2 \cdot |w|^2 = z\overline{z} \cdot w\overline{w},\end{gathered}$$

was $\overline{z + w} = \overline{z} + \overline{w}$ und $\overline{zw} = \overline{z} \cdot \overline{w}$ impliziert. Die Multiplikativität gilt nach Division durch zw zwar zunächst nur für z, $w \in \mathbb{C} \setminus \{0\}$, aber für $z = 0$ oder $w = 0$ ist sie ebenso offensichtlich erfüllt. Die komplexe Konjugation ist folglich mit Addition und Multiplikation verträglich.

Beispielsweise erhalten wir für alle z, $w \in \mathbb{C}$ durch Kombination dieser Rechenregeln

$$|z + w|^2 = (z + w)\overline{(z + w)} = (z + w)(\overline{z} + \overline{w}) = z\overline{z} + z\overline{w} + \overline{z\overline{w}} + w\overline{w} = |z|^2 + 2\,\mathrm{Re}(z\overline{w}) + |w|^2\,. \tag{2}$$

[4] Die sogenannte *Euler'sche Formel* kann durch die Theorie von Potenzreihen auch mathematisch präzisiert werden. Wir sehen es hier nur als Abkürzung an.

[5] Das gilt offenbar auch für $z = 0$ oder $w = 0$, nur verlieren die Winkel dann an Bedeutung.

1.2.2 Zurück zu den komplexen Einheitswurzeln

In Analogie zum Fall $R = \mathbb{Z}/m\mathbb{Z}$ können wir auch für Einheitswurzeln in $\mathbb{C}$ die sogenannte Ordnung definieren:

Definition 1.3. Sei ω eine Einheitswurzel in $\mathbb{C}$. Die gemäß Lemma 1.2 eindeutig bestimmte positive ganze Zahl d, für die $\omega \in P_d$ gilt, heißt die *Ordnung* von ω und wird hier mit $\operatorname{ord}(\omega)$ bezeichnet.

Gemäß Lemma 1.2 ist somit $\operatorname{ord}(\omega)$ die kleinste positive ganze Zahl d mit $\omega^d = 1$. Wie auch in $\mathbb{Z}/m\mathbb{Z}$ können wir auch die Ordnung von Potenzen einer Einheitswurzel in Abhängigkeit ihrer eigenen Ordnung bestimmen:

Lemma 1.4. *Sei ω eine Einheitswurzel in $\mathbb{C}$, $d \coloneqq \operatorname{ord}(\omega)$ und k eine positive ganze Zahl. Dann gilt*

$$\operatorname{ord}\bigl(\omega^k\bigr) = \frac{d}{\operatorname{ggT}(d,k)}.$$

Beweis. Der Kürze halber schreiben wir $t \coloneqq \operatorname{ggT}(d,k)$. Wir müssen nach Definition die kleinste positive ganze Zahl ℓ mit $1 = (\omega^k)^\ell = \omega^{k\ell}$ finden. Das tritt gemäß Lemma 1.2 genau dann ein, wenn $d \mid k\ell$ und $\ell \in \mathbb{Z}_{>0}$ minimal mit dieser Eigenschaft ist. Allerdings erhalten wir

$$d \mid k\ell \qquad \Longleftrightarrow \qquad \frac{d}{t} \;\Big|\; \frac{k}{t} \cdot \ell \qquad \Longleftrightarrow \qquad \frac{d}{t} \;\Big|\; \ell,$$

da d/t und k/t zueinander teilerfremd sind. Die kleinste positive ganze Zahl ℓ, die Letzteres erfüllt, ist also $d/t = d/\operatorname{ggT}(d,k)$, wie gewünscht. □

Nach diesem theoretischen Intermezzo, das später noch von Nutzen sein wird, kehren wir zurück zur Berechnung komplexer Einheitswurzeln. Sei $n > 0$ ganz. Laut Definition sind die n-ten Einheitswurzeln in $\mathbb{C}$ genau die komplexen Nullstellen des Polynoms $X^n - 1$. Unter Ausnutzung unserer Kenntnisse zum Lösen von Polynomgleichungen können wir für kleine n die Einheitswurzeln explizit in kartesischen Koordinaten bestimmen.

Beispiel. Wir berechnen E_n und P_n für $n \in \{1,2,3,4\}$:

1. Das Polynom $X^1 - 1$ hat genau die Nullstelle 1, daher $E_1 = P_1 = \{1\}$.
2. Für $n = 2$ gilt $X^2 = 1 = (X-1)(X+1)$ und wir können die Einheitswurzeln als Nullstellen direkt ablesen. Es folgt $E_2 = \{-1, 1\}$ und $P_2 = \{-1\}$, da 1 bereits eine erste Einheitswurzel ist.
3. Bei $n = 3$ können wir wieder den Linearfaktor $X - 1$ abspalten und erhalten $X^3 - 1 = (X-1)(X^2+X+1)$. Die Nullstellen von X^2+X+1 ergeben sich mittels der quadratischen Lösungsformel – wir erhalten
$$E_3 = \left\{1, \frac{-1-\mathrm{i}\sqrt{3}}{2}, \frac{-1+\mathrm{i}\sqrt{3}}{2}\right\} \qquad \text{und} \qquad P_3 = \left\{\frac{-1-\mathrm{i}\sqrt{3}}{2}, \frac{-1+\mathrm{i}\sqrt{3}}{2}\right\}.$$
4. Im Fall $n = 4$ liefert die Abspaltung der primitiven ersten und zweiten Einheitswurzeln $X^4 - 1 = (X-1)(X+1)(X^2+1)$. Die Nullstellen von X^2+1 sind i und $-\mathrm{i}$ (laut Definition). Damit gilt $E_4 = \{1, -1, \mathrm{i}, -\mathrm{i}\}$ und $P_4 = \{\mathrm{i}, -\mathrm{i}\}$.

Die Darstellung von Einheitswurzeln mittels Wurzeln in kartesischen Koordinaten wird mit wachsendem n immer schwieriger und liefert keinen Mehrwert für das Verständnis (siehe bereits für $n = 5$). Wir wenden uns daher der Darstellung in Polarkoordinaten zu, in der sie viel einfacher zu beschreiben sind.

Proposition 1.5. *Für jede positive ganze Zahl n gilt*

$$E_n = \left\{ \mathrm{e}^{\mathrm{i}2\pi j/n} \;\middle|\; j \in \mathbb{Z},\ 0 \le j < n \right\}$$

und

$$P_n = \left\{ \mathrm{e}^{\mathrm{i}2\pi j/n} \;\middle|\; j \in \mathbb{Z},\ 0 \le j < n,\ \mathrm{ggT}(j,n) = 1 \right\}.$$

Beweis. Wir kürzen in diesem Beweis $z_j := \mathrm{e}^{\mathrm{i}2\pi j/n}$ für ganzes $0 \le j < n$ ab. Wegen $z_j^n = (\mathrm{e}^{\mathrm{i}2\pi j/n})^n = \mathrm{e}^{\mathrm{i}2\pi j} = \cos(2\pi j) + \mathrm{i}\sin(2\pi j) = 1$ ist z_j für jedes ganze $0 \le j < n$ eine n-te Einheitswurzel in $\mathbb{C}$. Da umgekehrt jede n-te Einheitswurzel auch Nullstelle des Polynoms $X^n - 1$ ist, dieses Polynom in $\mathbb{C}$ genau n Nullstellen hat und wir bereits n verschiedene gefunden haben (man zeichne diese als Punkte am komplexen Einheitskreis!), kann es keine weiteren geben.

Zu den primitiven Einheitswurzeln: Für ganzzahlige $0 \le j < n$ und $1 \le k < n$ gilt

$$z_j^k = 1 \iff \mathrm{e}^{\mathrm{i}2\pi kj/n} = 1 \iff \cos\left(\frac{2\pi kj}{n}\right) = 1 \quad \text{und} \quad \sin\left(\frac{2\pi kj}{n}\right) = 0 \iff \frac{kj}{n} \in \mathbb{Z},$$

da die Cosinusfunktion den Wert 1 genau für ganzzahlige Vielfache von 2π annimmt (und an diesen Stellen auch die Sinusfunktion null ist).

Sind j und n teilerfremd, so ist $n \mid k \cdot j$ zu $n \mid k$ äquivalent, was aufgrund der Wahl von k nicht auftreten kann. In solchen Fällen ist z_j eine primitive n-te Einheitswurzel.

Andererseits führt bei $\mathrm{ggT}(j,n) =: d > 1$ die Wahl $k = n/d < n$ zu $kj/n = j/d \in \mathbb{Z}$ und daher nach obiger Äquivalenzkette auf $z_j^k = 1$, womit alle anderen n-ten Einheitswurzeln (z_j mit j nicht zu n teilerfremd) als nicht primitiv nachgewiesen sind. □

Aufgrund dieser Proposition können wir für jedes positive ganze n konkret $\mathrm{e}^{\mathrm{i}2\pi/n}$ als eine primitive n-te Einheitswurzel angeben (falls das in einer Aufgabe gebraucht wird). Ebenfalls wird nach Definition von $\mathrm{e}^{\mathrm{i}\varphi}$ (spätestens hier) klar, dass alle komplexen Einheitswurzeln auf dem Einheitskreis liegen, d. h. Betrag 1 haben. Für solche Zahlen, also $z \in \mathbb{C}$ mit $|z| = 1$, gilt $1/z = |z|^2 / z = \overline{z}$, die zu z komplex konjugierte Zahl ist also gleichzeitig ihr Inverses.

Wir kommen jetzt zu einer sehr nützlichen Eigenschaft von Einheitswurzeln: Wir können mit ihrer Hilfe in Polynomen (oder auch in Potenzreihen) alle Koeffizienten extrahieren, deren Indizes Vielfache einer vorgegebenen positiven ganzen Zahl n sind. Grundlage dafür ist zum einen die Beobachtung, dass für n-te Einheitswurzeln α die Gleichung

$$1 + \alpha + \cdots + \alpha^{n-1} = \begin{cases} n, & \text{für } \alpha = 1 \\ \frac{\alpha^n - 1}{\alpha - 1} = 0, & \text{für } \alpha \ne 1 \end{cases} \tag{3}$$

gilt und zum anderen, dass für eine *primitive* n-te Einheitswurzel ω die Aussage $\omega^k = 1$ zu $n \mid k$ äquivalent ist (vgl. Lemma 1.2). Setzen wir also ω^k für α in (3) ein, so haben wir mit

$$\frac{1}{n}(1 + \omega^k + \cdots + \omega^{k(n-1)}) = \frac{1}{n} \sum_{j=0}^{n-1} \omega^{kj}$$

einen Ausdruck gefunden, der genau für alle Vielfachen k von n den Wert 1 annimmt und 0 sonst. Dieser Kunstgriff kann in bestimmten Aufgaben sehr nützlich sein (oder sie gar erst zugänglich machen).

Beispiel. Möglicherweise bereits bekannt ist dieses Verfahren im Fall $n = 2$. Die primitive zweite Einheitswurzel ist $\omega = -1$ und wir möchten alle Koeffizienten mit geraden Indizes in einem polynomiellen Ausdruck extrahieren. Um konkret zu bleiben: Wir möchten beispielsweise die Summe

$$S := \sum_{j=0}^{1010} \binom{2020}{2j} 2^{2j} = \binom{2020}{0} + \binom{2020}{2} \cdot 2^2 + \binom{2020}{4} \cdot 2^4 + \cdots$$

berechnen. Nach dem binomischen Lehrsatz kennen wir die Summe über alle $0 \leq k \leq 2020$ (gesucht ist sie aber nur über Summanden mit geradem Index). Mit dem obigen Trick (Multiplikation des Ausdrucks mit 1 für gerade Indizes und mit 0 für ungerade) ergibt sich unter Beachtung von $4^j = 2^{2j}$ die Identität

$$\begin{aligned} S = \sum_{k=0}^{2020} \binom{2020}{k} \cdot 2^k \cdot \frac{1}{2}\big(1 + (-1)^k\big) = \\ = \frac{1}{2} \sum_{k=0}^{2020} \binom{2020}{k} \cdot 2^k + \frac{1}{2} \sum_{k=0}^{2020} \binom{2020}{k} (-2)^k = \\ = \frac{(1+2)^{2020} + (1-2)^{2020}}{2} = \frac{3^{2020} + 1}{2}. \end{aligned}$$

Ein wenig abstrakter formuliert: Für das Polynom $p \coloneqq (1+X)^{2020} = \sum_{k=0}^{2020} a_k X^k \in \mathbb{Z}[X]$ (mit $a_k = \binom{2020}{k}$) haben wir

$$\begin{aligned} p(2) &= \sum_{k=0}^{2020} a_k 2^k = a_0 + a_1 \cdot 2 + a_2 \cdot 2^2 + a_3 \cdot 2^3 + \cdots \\ p(-2) &= \sum_{k=0}^{2020} a_k (-2)^k = a_0 - a_1 \cdot 2 + a_2 \cdot 2^2 - a_3 \cdot 2^3 + \cdots \end{aligned}$$

addiert, damit sich alle Terme mit ungeraden Indizes auslöschen. Da in $p(2) + p(-2)$ alle Terme mit geraden Indizes doppelt auftreten, müssen wir das Ergebnis noch durch 2 dividieren. Die Vorgehensweise oben dreht diese Idee nur um.

Bemerkung. Man kann diesen Trick noch ein wenig variieren: Für $\omega \in P_n$ ist beispielsweise $\omega^{k-1} = 1 \iff n \mid k-1 \iff k \equiv 1 \pmod{n}$. Wenn wir also $\alpha = \omega^{k-1}$ in (3) einsetzen, liefert das den Ausdruck $\frac{1}{n} \sum_{j=0}^{n-1} \omega^{(k-1)j}$, der genau dann 1 ist, wenn $k \equiv 1 \pmod{n}$, und 0 sonst. So können wir alle Koeffizienten mit Indizes kongruent zu 1 modulo n extrahieren.

Aufgabe 1.1. Seien m, n positive ganze Zahlen und $m \geq 2$. Weiters sei $R = \mathbb{Z}/m\mathbb{Z}$ oder $R = \mathbb{C}$ und $\alpha \in R$ eine primitive n-te Einheitswurzel in R. Zeige:

1. Für jedes ganze $0 \leq j < n$ mit $\mathrm{ggT}(j, n) = 1$ ist α^j eine primitive n-te Einheitswurzel.
2. Es gibt entweder keine oder mindestens $\varphi(n)$ primitive n-te Einheitswurzeln in R.
3. Folgere (erneut) die Anzahl der Primitivwurzeln modulo m.
4. Bestimme die Anzahl der primitiven n-ten Einheitswurzeln in $\mathbb{C}$.
5. Finde m und n so, dass es mehr als $\varphi(n)$ primitive n-te Einheitswurzeln in $\mathbb{Z}/m\mathbb{Z}$ gibt.

Aufgabe 1.2. Bestimme E_n und P_n für $n \in \{5, 6, 8, 12\}$ in kartesischen Koordinaten und stelle diese Mengen jeweils in der Gauß'schen Zahlenebene dar.

Aufgabe 1.3. Verwende die Multiplikativität des Betrages komplexer Zahlen für den Beweis folgender Aussage: Sind m und n beide als Summe zweier Quadratzahlen darstellbar, so auch $m \cdot n$.

Aufgabe 1.4. Für jede positive ganze Zahl n sei a_n die Anzahl aller Teilmengen der Menge $\{1, \ldots, n\}$ mit einer durch 3 teilbaren Anzahl an Elementen. Man bestimme eine Rekursionsformel für die Folge $(a_n)_{n \geq 1}$.

Aufgabe 1.5 (Donau-Wettbewerb 2005)**.** Sei n eine positive ganze Zahl und

$$S_n := \binom{n}{1} + \binom{n}{3} \cdot 2005 + \binom{n}{5} \cdot 2005^2 + \cdots = \sum_{k=0}^{\lfloor \frac{n-1}{2} \rfloor} \binom{n}{2k+1} 2005^k.$$

Man zeige, dass $2^{n-1} \mid S_n$.

Aufgabe 1.6 (Rumänien 2004)**.** Seien m und n positive ganze Zahlen, wobei m ungerade sei. Man beweise, dass

$$3^m n \,\Big|\, \sum_{k=0}^{m} \binom{3m}{3k} (3n-1)^k.$$

2 Lifting The Exponent (LTE)

In diesem Abschnitt wollen wir beschreiben, mit welcher Vielfachheit eine Primzahl p in Ausdrücken der Form $a^n - b^n$ mit $a, b \in \mathbb{Z}$ und positivem ganzen n auftritt. Als Vorbereitung können wir eine Potenz von p bereits aus den beiden einzelnen Faktoren herausheben. Nach den Rechenregeln für die Vielfachheit gilt nämlich

$$\mathrm{v}_p(a^n - b^n) \geq \min(\mathrm{v}_p(a^n), \mathrm{v}_p(b^n)) = \min(n\mathrm{v}_p(a), n\mathrm{v}_p(b)) = n \min(\mathrm{v}_p(a), \mathrm{v}_p(b))$$

und Gleichheit tritt in dieser Ungleichung ein, falls $\mathrm{v}_p(a) \neq \mathrm{v}_p(b)$. In diesem Fall ist die Vielfachheit also bereits bestimmt.

Wenden wir uns daher dem spannenderen Fall $\mathrm{v}_p(a) = \mathrm{v}_p(b) =: e$ zu. Schreiben wir nun $a = p^e A$ und $b = p^e B$ für ganze Zahlen A und B mit $p \nmid AB$, so erhalten wir

$$a^n - b^n = (p^e A)^n - (p^e B)^n = p^{en}(A^n - B^n),$$

und folglich $\mathrm{v}_p(a^n - b^n) = en + \mathrm{v}_p(A^n - B^n)$. Wir betrachten im Weiteren nur den Fall, dass die letztere Vielfachheit nicht null ist, also

$$p \mid A^n - B^n \qquad \Longleftrightarrow \qquad A^n \equiv B^n \pmod{p} \tag{4}$$

gilt. Da B nicht durch p teilbar ist, folgt $\mathrm{ggT}(B, p) = 1$ und daher hat die Kongruenz $BC \equiv 1 \pmod{p}$ eine (modulo p eindeutige) Lösung $C \in \mathbb{Z}$. Multiplikation der Kongruenz in (4) mit C^n ergibt $(AC)^n \equiv 1 \pmod{p}$. Damit ist die Restklasse von AC modulo p eine n-te Einheitswurzel und eine primitive d-te Einheitswurzel in $\mathbb{Z}/p\mathbb{Z}$ für $d \coloneqq \mathrm{ord}_p(AC)$ (vgl. Lemma 1.2 und Satz 1). Also erhalten wir $(AC)^d \equiv 1 \pmod{p}$ und durch Multiplikation mit B^d die äquivalente Kongruenz $A^d \equiv B^d \pmod{p}$.[6]

Setzen wir nun abschließend $x \coloneqq A^d$, $y \coloneqq B^d$ und $k \coloneqq n/d$, so ergibt sich

$$A^n - B^n = \left(A^d\right)^{n/d} - \left(B^d\right)^{n/d} = x^k - y^k \qquad \text{und} \qquad x \equiv y \not\equiv 0 \pmod{p}$$

mit x, $y \in \mathbb{Z}$ und positivem ganzen k (vgl. Lemma 1.2).

Die Vielfachheit von p in genau solchen Ausdrücken behandelt

Satz 2 (LTE-Lemma)**.** *Seien p eine Primzahl, x, $y \in \mathbb{Z}$ mit $x \equiv y \not\equiv 0 \pmod{p}$ und sei k eine positive ganze Zahl. Dann gilt:*

1. *Für $p \neq 2$ ist*
$$\mathrm{v}_p(x^k - y^k) = \mathrm{v}_p(x - y) + \mathrm{v}_p(k). \tag{5}$$
2. *Für $p = 2$ und ungerades k ist $\mathrm{v}_2(x^k - y^k) = \mathrm{v}_2(x - y)$.*
3. *Für $p = 2$ und gerades k ist*
$$\mathrm{v}_2(x^k - y^k) = \mathrm{v}_2(x^2 - y^2) + \mathrm{v}_2(k) - 1.$$

Bemerkung. Bevor wir uns dem Beweis des LTE-Lemmas zuwenden, ein paar Kommentare und Beobachtungen:

- Die wichtigste Formel ist (5). Sie gilt auch in Fall 2 und sogar in Fall 3 für $x \equiv y \equiv 1 \pmod{4}$ (weil dann $\mathrm{v}_2(x + y) = 1$ gilt), also immer bis auf den Sonderfall $p = 2$, k gerade, $x \not\equiv y \pmod{4}$. Die Gliederung in drei Fälle soll nur der Verständlichkeit dienen.
- Wegen $x - y \mid x^k - y^k$ (bzw. $x^2 - y^2 \mid x^k - y^k$ für gerades k) ist $\mathrm{v}_p(x - y) \leq \mathrm{v}_p(x^k - y^k)$ (bzw. $\mathrm{v}_2(x^2 - y^2) \leq \mathrm{v}_2(x^k - y^k)$ für gerades k) nicht verwunderlich. Die zentrale Bedeutung des LTE-Lemmas ist jedoch, die Differenz der beiden Vielfachheiten exakt bestimmen zu können.

[6] Die Theorie von Einheitswurzeln ist in diesem Kontext nicht notwendig. Es genügt bereits, über die Ordnung Bescheid zu wissen.

- Wenn wir x, y und $p \neq 2$ fixieren und eine ganze Zahl $r > 0$ vorgeben, können wir durch geeignete Wahl von k (z. B. $k = p^r$) erreichen, dass sich der Exponent (d. h. die Vielfachheit) von p in $x^k - y^k$ gegenüber dem in $x - y$ um genau r erhöht. Wir können den Exponenten also nach Belieben „liften“ – das erklärt möglicherweise die Namensherkunft.[7]
- Der häufigste Fehler in der Anwendung des LTE-Lemmas besteht darin, die Bedingung $x \equiv y \not\equiv 0 \pmod{p}$ (oder äquivalent: $p \mid x - y$ und $p \nmid xy$) nicht zu überprüfen – was aber nach der Ausführung am Anfang des Kapitels offenbar ausschlaggebend ist! Für eine korrekte Lösung **bitte immer berücksichtigen!**

Wenden wir uns nun dem Beweis von Satz 2 zu: Wir werden erst zwei Spezialfälle als Lemmata zeigen und diese dann zu einem Beweis für $p \neq 2$ zusammensetzen. Für $p = 2$ werden wir eine direktere Methode verwenden.

Der erste Spezialfall: Wenn k von p nicht geteilt wird, wenn also $\mathrm{v}_p(k) = 0$ gilt, so besagen die ersten beiden Fälle von Satz 2, dass sich die Vielfachheit von p in $x^k - y^k$ gegenüber der in $x - y$ nicht ändert.[8]

Lemma 2.1. *Seien p eine Primzahl, x, $y \in \mathbb{Z}$ mit $x \equiv y \not\equiv 0 \pmod{p}$ und sei k eine positive ganze Zahl mit $p \nmid k$. Dann gilt*

$$\mathrm{v}_p(x^k - y^k) = \mathrm{v}_p(x - y).$$

Beweis. Wegen der Faktorisierung $x^k - y^k = (x - y)\sum_{j=0}^{k-1} x^{k-1-j}y^j$ und den Rechenregeln für die Vielfachheit ist

$$\mathrm{v}_p(x^k - y^k) = \mathrm{v}_p(x - y) + \mathrm{v}_p\Big(\sum_{j=0}^{k-1} x^{k-1-j}y^j\Big), \tag{6}$$

und laut Voraussetzung gilt

$$\sum_{j=0}^{k-1} x^{k-1-j}y^j \equiv \sum_{j=0}^{k-1} x^{k-1-j}x^j = \sum_{j=0}^{k-1} x^{k-1} = k \cdot x^{k-1} \not\equiv 0 \pmod{p},$$

weil weder k noch x durch p teilbar ist. Daher ist auch diese Summe nicht durch p teilbar und die letztgenannte Vielfachheit in (6) gleich null, was noch zu zeigen war. □

Der zweite Spezialfall: Für $p \neq 2$ und $k = p$ liefert die Formel (5), dass sich die Vielfachheit von p in $x - y$ beim Übergang zu $x^p - y^p$ um genau 1 erhöht. Im Beweis von Satz 2 werden wir dieses Resultat dann iterativ verwenden (mathematisch formal über vollständige Induktion).

Lemma 2.2. *Seien $p \neq 2$ eine Primzahl und x, $y \in \mathbb{Z}$ mit $x \equiv y \not\equiv 0 \pmod{p}$. Dann gilt*

$$\mathrm{v}_p(x^p - y^p) = \mathrm{v}_p(x - y) + 1.$$

Beweis. Für $x = y$ ist die Aussage wahr (beachte: $\mathrm{v}_p(0) = \infty$) und wir dürfen daher $x \neq y$ voraussetzen. Sei nun $t \coloneqq \mathrm{v}_p(x - y) \in \mathbb{Z}_{>0}$, also $x = y + p^t r$ für eine ganze Zahl r mit $p \nmid r$. Aus dem binomischen Lehrsatz ergibt sich

$$\begin{aligned} x^p - y^p = (y + p^t r)^p - y^p &= \left(\sum_{j=0}^{p} \binom{p}{j} y^{p-j}(p^t r)^j\right) - y^p = \\ &= \cancel{y^p} + p \cdot y^{p-1}p^t r + \frac{p(p-1)}{2}y^{p-2}(p^t r)^2 + Kp^{3t} - \cancel{y^p} = \\ &= p^{t+1}\left(y^{p-1}r + \frac{p-1}{2}y^{p-2}r^2 \cdot p^t + K \cdot p^{2t-1}\right) \end{aligned}$$

[7] Für $p = 2$ können wir das nicht nach Belieben; bei vorgegebenen x und y kann das schiefgehen. (Gegenbeispiel!)
[8] Man beachte, dass hier $p = 2$ keinen Sonderfall darstellt!

für eine ganzzahlige Konstante K, die durch Zusammenfassen der Terme für $j \geq 3$ entsteht.[9] Aus $p \neq 2$ folgt $(p-1)/2 \in \mathbb{Z}$ und wegen $2t - 1 \geq t \geq 1$ sind somit die letzten beiden Ausdrücke in obiger Klammer durch p teilbare ganze Zahlen; nach Voraussetzung ist das $y^{p-1}r$ aber nicht. Insgesamt ist der Ausdruck in der Klammer nicht durch p teilbar und die Vielfachheit von p in $x^p - y^p$ beträgt damit $t + 1 = \mathrm{v}_p(x - y) + 1$. □

Beweis von Satz 2. Zuerst bemerken wir, dass Fall 2 durch Lemma 2.1 bereits bewiesen ist.

Nun sei $k = p^\alpha K$ für nichtnegative ganze Zahlen α und K mit $p \nmid K$. Es ist also $\alpha = \mathrm{v}_p(k)$. Wegen

$$x^k - y^k = x^{p^\alpha K} - y^{p^\alpha K} = \left(x^{p^\alpha}\right)^K - \left(y^{p^\alpha}\right)^K, \qquad p \nmid K \qquad \text{und} \qquad x^{p^\alpha} \equiv y^{p^\alpha} \not\equiv 0 \pmod{p}$$

ist Lemma 2.1 anwendbar und liefert $\mathrm{v}_p(x^k - y^k) = \mathrm{v}_p\left(x^{p^\alpha} - y^{p^\alpha}\right)$.

Im Fall $p \neq 2$ zeigen wir nun $\mathrm{v}_p\left(x^{p^\alpha} - y^{p^\alpha}\right) = \mathrm{v}_p(x - y) + \alpha$ durch Induktion nach α. Als Induktionsbasis $\alpha = 0$ haben wir nichts zu beweisen. Für den Induktionsschritt von α auf $\alpha + 1$ bemerken wir, dass wegen

$$x^{p^{\alpha+1}} - y^{p^{\alpha+1}} = \left(x^{p^\alpha}\right)^p - \left(y^{p^\alpha}\right)^p \qquad \text{und} \qquad x^{p^\alpha} \equiv y^{p^\alpha} \not\equiv 0 \pmod{p}$$

die Voraussetzungen von Lemma 2.2 erfüllt sind und daher

$$\mathrm{v}_p\left(x^{p^{\alpha+1}} - y^{p^{\alpha+1}}\right) = \mathrm{v}_p\left(x^{p^\alpha} - y^{p^\alpha}\right) + 1 = \mathrm{v}_p(x - y) + \alpha + 1$$

aus Lemma 2.2 und der Induktionsannahme folgt.

Es bleibt noch der Fall $p = 2$, $\alpha \geq 1$ (also k gerade) abzuhandeln: Die Voraussetzung ist hier, dass x und y ungerade sind. Wir verwenden die Faktorisierung

$$x^{2^\alpha} - y^{2^\alpha} = (x^2 - y^2) \prod_{j=1}^{\alpha-1} \left(x^{2^j} + y^{2^j}\right),$$

die sich durch fortwährende Aufspaltung von $x^{2^{j+1}} - y^{2^{j+1}} = \left(x^{2^j}\right)^2 - \left(y^{2^j}\right)^2$ in die Faktoren $x^{2^j} - y^{2^j}$ und $x^{2^j} + y^{2^j}$ für $j = \alpha - 1, \ldots, 1$ ergibt. Jeder der Faktoren im Produkt ist die Summe zweier ungerader Quadratzahlen und damit kongruent zu 2 modulo 4, d. h. es gilt $\mathrm{v}_2\left(x^{2^j} + y^{2^j}\right) = 1$ für jedes ganze $1 \leq j \leq \alpha - 1$. Das ergibt insgesamt

$$\mathrm{v}_2\left(x^{2^\alpha} - y^{2^\alpha}\right) = \mathrm{v}_2(x^2 - y^2) + \sum_{j=1}^{\alpha-1} \mathrm{v}_2\left(x^{2^j} + y^{2^j}\right) = \mathrm{v}_2(x^2 - y^2) + \alpha - 1$$

und das war wegen $\alpha = \mathrm{v}_2(k)$ noch zu zeigen. □

Für den Fall, dass k ungerade ist, können wir sogar die Vielfachheit in Ausdrücken der Form $x^k + y^k$ bestimmen:

Satz 3. *Seien p eine Primzahl, x, $y \in \mathbb{Z}$ mit $x \equiv -y \not\equiv 0 \pmod{p}$ und sei $k \in \mathbb{Z}_{>0}$ ungerade. Dann gilt*

$$\mathrm{v}_p(x^k + y^k) = \mathrm{v}_p(x + y) + \mathrm{v}_p(k).$$

Beweis. Setzen wir $z := -y \in \mathbb{Z}$, so erhalten wir $x \equiv z \not\equiv 0 \pmod{p}$, $x - z = x + y$ und $x^k - z^k = x^k - (-y)^k = x^k + y^k$, weil k ungerade ist. Die Aussage folgt nun durch Zusammenfassen der ersten beiden Fälle aus Satz 2 für x und z. Der dritte Fall kann nämlich nach Voraussetzung (k ungerade) nicht eintreten. □

Für eine erste Anwendung des LTE-Lemmas zeigen wir ein theoretisches Resultat über Primitivwurzeln:

[9] Die Summe enthält wegen $p \geq 3$ tatsächlich solche Summanden.

Beispiel. Wir beweisen, dass es modulo 2^e mit ganzem $e \geq 3$ keine Primitivwurzeln geben kann und dass die Zahl 3 modulo 2^e die größtmögliche Ordnung 2^{e-2} besitzt.[10]

Sei dazu a eine zu 2^e teilerfremde ganze Zahl, d. h. a sei ungerade. Wir wollen die Ordnung $\mathrm{ord}_{2^e}(a)$ von a modulo 2^e bestimmen, also die kleinste positive ganze Zahl k mit

$$a^k \equiv 1 \pmod{2^e} \quad \Longleftrightarrow \quad 2^e \mid a^k - 1 \quad \Longleftrightarrow \quad \mathrm{v}_2(a^k - 1) \geq e.$$

Die letztgenannte Vielfachheit können wir mit dem LTE-Lemma genau bestimmen, nachdem die Voraussetzung $a \equiv 1 \not\equiv 0 \pmod 2$ offenbar erfüllt ist.

Für ungerades k ist $\mathrm{v}_2(a^k - 1^k) = \mathrm{v}_2(a - 1)$ laut dem zweiten Fall im LTE-Lemma. Diese Vielfachheit kann nur dann größer oder gleich e sein, wenn $a \equiv 1 \pmod{2^e}$ gilt; in diesem Fall ist die Ordnung aber gleich 1.

Für gerades k ergibt sich aus dem dritten Fall im LTE-Lemma, dass

$$\mathrm{v}_2(a^k - 1) = \mathrm{v}_2(a^k - 1^k) = \mathrm{v}_2(a^2 - 1) + \mathrm{v}_2(k) - 1 \geq \mathrm{v}_2(k) + 2, \tag{7}$$

weil $a^2 - 1$ für ungerade Zahlen immer zumindest durch $8 = 2^3$ teilbar ist. Für $k = 2^{e-2}$ ist diese Vielfachheit also für ein beliebiges ungerades $a \in \mathbb{Z}$ sicher größer oder gleich e. Folglich ist $a^{2^{e-2}} \equiv 1 \pmod{2^e}$ und die Ordnung von a modulo 2^e ein Teiler von 2^{e-2}.

Eine Primitivwurzel g modulo 2^e müsste teilerfremd zu 2^e sein und $\mathrm{ord}_{2^e}(g) = \varphi(2^e) = 2^{e-1}$ erfüllen. Das kann aber nach dem eben Gezeigten nicht passieren.

Setzen wir außerdem $a = 3$ in (7) ein, so gilt wegen $3^2 - 1 = 8 = 2^3$ das Gleichheitszeichen in der Abschätzung; die Ordnung von 3 modulo 2^e kann also nicht kleiner als 2^{e-2} sein (weil der Zweier zumindest $e - 2$ Mal in der Primfaktorzerlegung von k auftreten muss).

Aufgabe 2.1. Bestimme die größte ganze Zahl n, sodass $2023^{2024} \equiv 1 \pmod{2^n}$ gilt.

Aufgabe 2.2. Seien a und b positive reelle Zahlen, sodass $a^n - b^n$ für alle $n \in \mathbb{Z}_{>0}$ positive ganze Zahlen sind. Beweise, dass a und b ganzzahlig sind.

Aufgabe 2.3. Finde alle ganzen Zahlen $a, b > 1$ mit $b^a \mid a^b - 1$.

Aufgabe 2.4 (Österreich-Polen-Wettbewerb 2003)**.** Eine positive ganze Zahl heiße *alpin*, wenn sie $2^u + 1$ für eine ungerade ganze Zahl $u \geq 1$ teilt. Beweise, dass das Produkt zweier alpiner Zahlen wieder alpin ist.

Aufgabe 2.5 (Irland 1996)**.** Sei p eine Primzahl und seien a, k positive ganze Zahlen. Beweise, dass $2^p + 3^p = a^k$ nur für $k = 1$ gelten kann.

Aufgabe 2.6. Sei $k > 1$ eine ganze Zahl. Man beweise, dass es unendlich viele positive ganze Zahlen n mit

$$n \mid 1^n + 2^n + \cdots + k^n$$

gibt.

[10] Damit beweisen wir insbesondere, dass für die Carmichael-Funktion $\lambda(2^e) = 2^{e-2}$ bei $e \geq 3$ gilt.

3 Kreisteilungspolynome

Wir sind aus Abschnitt 1 ausreichend gerüstet, um das Kernthema dieser Arbeit in Angriff zu nehmen: Kreisteilungspolynome. Nach der Definition folgen einige Resultate zu ihrer Berechnung und im nächsten Abschnitt werden wir ihre Primteiler (und damit die Form all ihrer Teiler) untersuchen.

Definition 3.1. Sei n eine positive ganze Zahl. Das Polynom

$$\Phi_n \coloneqq \prod_{\omega \in P_n} (X - \omega) \in \mathbb{C}[X]$$

heißt das n-te Kreisteilungspolynom.

Bemerkung. Nach Definition ist daher Φ_n das normierte Polynom mit komplexen Koeffizienten, das genau alle primitiven n-ten Einheitswurzeln als Nullstellen hat.

3.1 Berechnung und Eigenschaften

Man beachte in der folgenden Ausführung, dass mit dem Symbol $d \mid n$ konventionsgemäß ber alle *positiven* Teiler d der Zahl n iteriert wird.

Um eine einfache Berechnungsmethode für Kreisteilungspolynome zu erhalten, ziehen wir Lemma 1.2 für $R = \mathbb{C}$ heran: Demzufolge gilt

$$E_n = \bigcup_{d \mid n} P_d, \tag{8}$$

denn jede n-te Einheitswurzel ist auch eine primitive d-te für einen positiven Teiler d von n (das beweist „$\subseteq$“) und aus $d \mid n$ folgt, dass jede d-te Einheitswurzel auch eine n-te ist (also gilt „$\supseteq$“). Zusätzlich ist die Vereinigung in (8) disjunkt, weil eine komplexe Zahl nach Definition nur primitive d-te Einheitswurzel für höchstens ein d sein kann (siehe auch dazu Lemma 1.2). Das liefert

$$\prod_{\omega \in E_n} (X - \omega) = \prod_{d \mid n} \Bigg(\prod_{\omega \in P_d} (X - \omega) \Bigg) = \prod_{d \mid n} \Phi_d.$$

Die linke Seite ist ein normiertes Polynom, das genau alle komplexen n-ten Einheitswurzeln als Nullstellen hat, also $X^n - 1$. Wir erhalten zusammenfassend

Lemma 3.2. *Sei n eine positive ganze Zahl. Dann gilt*

$$X^n - 1 = \prod_{d \mid n} \Phi_d \qquad \textit{oder äquivalent} \qquad \Phi_n = \frac{X^n - 1}{\prod_{\substack{d \mid n \\ d < n}} \Phi_d}. \tag{9}$$

Beispiel. Als Veranschaulichung für den vorangegangenen Beweis im Fall $n = 12$: Sei $\omega \coloneqq \mathrm{e}^{\mathrm{i}2\pi/12}$. Dann gilt

$$\begin{aligned} P_{12} &= \{\omega^1, \omega^5, \omega^7, \omega^{11}\}, & P_6 &= \{\omega^2, \omega^{10}\}, & P_4 &= \{\omega^3, \omega^9\} = \{\mathrm{i}, -\mathrm{i}\}, \\ P_3 &= \{\omega^4, \omega^8\}, & P_2 &= \{\omega^6\} = \{-1\}, & P_1 &= \{\omega^0\} = \{1\}, \end{aligned}$$

wie man leicht mit Proposition 1.5 überprüft. Die entsprechende Gruppierung liefert

$$\begin{aligned} X^{12} - 1 = {} & \big[(X - \omega^1)(X - \omega^5)(X - \omega^7)(X - \omega^{11})\big] \cdot \big[(X - \omega^2)(X - \omega^{10})\big] \\ & \cdot \big[(X - \omega^3)(X - \omega^9)\big] \cdot \big[(X - \omega^4)(X - \omega^8)\big] \cdot (X - \omega^6) \cdot (X - \omega^0) \\ & = \Phi_{12} \cdot \Phi_6 \cdot \Phi_4 \cdot \Phi_3 \cdot \Phi_2 \cdot \Phi_1 \end{aligned}$$

Beispiel. Wir berechnen Φ_n für ganze Zahlen $1 \leq n \leq 14$ und werden dann alle Zwischenergebnisse in separaten Resultaten zusammenfassen.

Für $n = 1$ ergibt sich aus $P_1 = \{1\}$ direkt $\Phi_1 = X - 1$.

Auch für $n = 2$ können wir direkt $\Phi_2 = X - (-1) = X + 1$ (aus $P_2 = \{-1\}$) schließen, aber auch Lemma 3.2 heranziehen:

$$\Phi_2 = \frac{X^2 - 1}{\Phi_1} = \frac{X^2 - 1}{X - 1} = X + 1.$$

Für $n = 3$ gilt

$$\Phi_3 = \frac{X^3 - 1}{\Phi_1} = \frac{X^3 - 1}{X - 1} = X^2 + X + 1.$$

Wir erkennen hier vielleicht schon ein Muster für Primzahlen. Hierbei tritt nur der eine Faktor $\Phi_1 = X - 1$ im Nenner von (9) auf. Ganz allgemein folgt

Lemma 3.3. *Sei p eine Primzahl. Dann gilt*

$$\Phi_p = \frac{X^p - 1}{X - 1} = X^{p-1} + X^{p-2} + \cdots + 1. \tag{10}$$

Beispiel (Fortsetzung). Mit dieser Formel können wir direkt Φ_2, Φ_3, Φ_5, Φ_7 und Φ_{11} ermitteln.

Wir setzen unsere Berechnungen nun für $n = 4$ und $n = 8$ fort:

$$\Phi_4 = \frac{X^4 - 1}{\Phi_2 \cdot \Phi_1} = \frac{(X^2)^2 - 1}{X^2 - 1} = X^2 + 1 = \Phi_2(X^2)$$
$$\Phi_8 = \frac{X^8 - 1}{\Phi_1 \cdot \Phi_2 \cdot \Phi_4} = \frac{X^8 - 1}{X^4 - 1} = X^4 + 1 = \Phi_4(X^2) = \Phi_2(X^4)$$

Wir könnten jetzt induktiv $\Phi_{2^e} = X^{2^{e-1}} + 1 = \Phi_2(X^{2^{e-1}})$ für positive ganze Zahlen e zeigen, werden aber in Satz 4 noch ein allgemeineres Resultat herleiten, das nach dem Durchrechnen der kleinen Fälle noch klarer sein wird.

Zurück also zu den Rechnungen:

$$\Phi_6 = \frac{X^6 - 1}{\Phi_1 \cdot \Phi_2 \cdot \Phi_3} = \frac{(X^3)^2 - 1}{\Phi_2 \cdot (X^3 - 1)} = \frac{X^3 + 1}{X + 1} = \frac{\Phi_2(X^3)}{\Phi_2} = X^2 - X + 1 \tag{11}$$
$$\Phi_9 = \frac{X^9 - 1}{\Phi_1 \cdot \Phi_3} = \frac{(X^3)^3 - 1}{X^3 - 1} = X^6 + X^3 + 1 = \Phi_3(X^3)$$
$$\Phi_{10} = \frac{X^{10} - 1}{\Phi_1 \cdot \Phi_2 \cdot \Phi_5} = \frac{X^{10} - 1}{(X^5 - 1)(X + 1)} = \frac{X^5 + 1}{X + 1} = \frac{\Phi_2(X^5)}{\Phi_2} = X^4 - X^3 + X^2 - X + 1 \tag{12}$$

Schließlich gelten noch

$$\Phi_{12} = \frac{X^{12} - 1}{\Phi_1 \cdot \Phi_2 \cdot \Phi_3 \cdot \Phi_4 \cdot \Phi_6} = \frac{X^{12} - 1}{\Phi_4 \cdot (X^6 - 1)} = \frac{X^6 + 1}{X^2 + 1} = X^4 - X^2 + 1 = \Phi_6(X^2),$$
$$\Phi_{14} = \frac{X^{14} - 1}{\Phi_1 \cdot \Phi_2 \cdot \Phi_7} = \frac{X^{14} - 1}{(X^7 - 1)(X + 1)} = \frac{X^7 + 1}{X + 1} = \frac{\Phi_2(X^7)}{\Phi_2} = X^6 - X^5 + \cdots - X + 1. \tag{13}$$

Es liegt daher die Vermutung nahe, dass die Berechnung von Φ_n durch die Primfaktorzerlegung von n bestimmt wird. Wir überprüfen noch $n = 2^2 \cdot 3 = 18$ und erhalten

$$\Phi_{18} = \frac{X^{18} - 1}{\Phi_1 \cdot \Phi_2 \cdot \Phi_3 \cdot \Phi_6 \cdot \Phi_9} = \frac{X^{18} - 1}{\Phi_2 \cdot \Phi_6 \cdot (X^9 - 1)}$$
$$= \frac{X^9 + 1}{(X + 1)(X^2 - X + 1)} = \frac{(X^3)^3 + 1}{X^3 + 1} = X^6 - X^3 + 1 = \Phi_6(X^3).$$

Damit erhärtet sich die Vermutung, dass $\Phi_{pn} = \Phi_n(X^p)$ für Primteiler p von n gilt.

Aus (11), (12), aber auch aus (10) leiten wir die Vermutung ab, dass $\Phi_{pn} = \Phi_n(X^p)/\Phi_n$ für Primzahlen p gilt, die keine Primteiler von n sind. Wir werden beide Resultate in Satz 4 beweisen und sie danach zur rekursiven Berechnung von Kreisteilungspolynomen nutzen.

Tragen wir aber zuerst noch einige andere Beobachtungen zusammen:

- ◇ Alle Polynome Φ_n für $1 \leq n \leq 14$ sind normiert und haben ganzzahlige Koeffizienten, sogar nur solche aus $\{-1, 0, 1\}$.
- ◇ Es gilt $\deg(\Phi_n) = \varphi(n)$ (worauf wahrscheinlich auch die Namensgebung zurückzuführen ist).
- ◇ Bis auf $n = 1$ ist der konstante Koeffizient von Φ_n immer 1.
- ◇ Φ_n ist für $n > 1$ selbstreziprok.[11]
- ◇ Für ungerade ganze Zahlen $3 \leq u \leq 7$ gilt $\Phi_{2u} = \Phi_u(-X)$. (siehe (11), (12) und (13)).

Abgesehen vom ersten Punkt gelten diese Beobachtungen für alle ganzen Zahlen $n > 0$ bzw. alle ungeraden Zahlen $u \geq 3$. Das erste Gegenbeispiel, dass Koeffizienten vom Betrag größer als 1 auftreten, stellt Φ_{105} dar, dessen Koeffizient bei X^7 gleich -2 ist. Wir erhalten

Proposition 3.4 (Eigenschaften von Kreisteilungspolynomen)**.** *Sei n eine positive ganze Zahl. Dann gelten folgende Aussagen:*

(a) $\Phi_n \in \mathbb{Z}[X]$*, d. h.* Φ_n *ist ein normiertes Polynom mit ganzzahligen Koeffizienten*

(b) $\deg(\Phi_n) = \varphi(n)$

(c) $\Phi_n(0) = 1$ *für* $n > 1$

(d) Φ_n *ist für* $n > 1$ *selbstreziprok*

(e) $\Phi_n(x) > 0$ *für* $n \geq 3$ *und alle reellen Zahlen* x

Bemerkung. Beweise zu Kreisteilungspolynomen können oft auf zweierlei Arten geführt werden: einerseits induktiv unter Verwendung der Produktdarstellung aus Lemma 3.2, andererseits direkt durch Beweis von Eigenschaften der primitiven n-ten Einheitswurzeln unter Berufung auf Definition 3.1. Wir werden im Folgenden beiden Beweisarten begegnen und es erweist sich als gute Übung, bei 3.4.(c) und 3.4.(d) jeweils auch die andere Beweisvariante auszuprobieren.

Beweis. Den Beweis von 3.4.(a) führen wir über vollständige Induktion. Die Induktionsbasis bildet $\Phi_1 = X - 1$. Für den Induktionsschritt setzen wir die Gültigkeit von 3.4.(a) für alle positiven ganzen Zahlen kleiner als n voraus und zeigen die Aussage für n.[12] Dazu ziehen wir Lemma 3.2 heran: Es ist $X^n - 1 = \Phi_n \cdot p$, wobei p das Polynom im Nenner von (9) bezeichnet, das nach Induktionsvoraussetzung normiert ist und ganzzahlige Koeffizienten besitzt. Division von $X^n - 1$ durch p mit Rest über $\mathbb{Z}[X]$ liefert eindeutige Polynome q, $r \in \mathbb{Z}[X]$ mit $X^n - 1 = q \cdot p + r$ und $\deg(r) < \deg(p)$. Der Vergleich der Leitkoeffizienten garantiert, dass q normiert ist. Wir können diese Division mit Rest aber auch in $\mathbb{C}[X]$ auffassen; dann liefert die Eindeutigkeit $r = 0$ und $q = \Phi_n \in \mathbb{Z}[X]$. Auch die Normiertheit überträgt sich von q auf Φ_n und beschließt die Induktion.

Aus Definition 3.1 und Proposition 1.5 folgt direkt $\deg(\Phi_n) = |P_n| = \varphi(n)$, also 3.4.(b).

Eigenschaft 3.4.(c) zeigen wir ebenfalls induktiv und bemerken zuerst, dass $\Phi_1(0) = -1$ gilt. Die Induktionsbasis ist durch $\Phi_2(0) = 0 + 1 = 1$ gegeben. Für den Induktionsschritt $< n \to n$ greifen wir wieder auf (9) zurück und erhalten

$$\Phi_n(0) = \frac{0^n - 1}{\Phi_1(0) \cdot \prod\limits_{\substack{d|n \\ 1<d<n}} \Phi_d(0)} = \frac{-1}{(-1) \cdot 1} = 1,$$

[11] Ein Polynom $p = \sum_{k=0}^{d} a_k X^k \in \mathbb{C}[X]$ mit $a_d \neq 0$ heißt *selbstreziprok*, wenn $a_{d-k} = a_k$ für alle ganzen Zahlen $0 \leq k \leq d$ oder äquivalent $p = X^d \cdot p(1/X)$ gilt.

[12] Im Folgenden werden wir für diese Variante der vollständigen Induktion kurz $< n \to n$ im Induktionsschritt schreiben.

wie gewünscht.

Zur Abwechslung zeigen wir 3.4.(d) direkt. Wegen $\omega \in P_n \iff \omega^{-1} \in P_n$ gilt

$$\begin{aligned} X^{\varphi(n)} \cdot \Phi_n\left(\frac{1}{X}\right) &= X^{\varphi(n)} \prod_{\omega \in P_n} \left(\frac{1}{X} - \omega\right) = \prod_{\omega \in P_n} (1 - \omega X) \\ &= \prod_{\omega \in P_n} \left[(-\omega)(X - \omega^{-1})\right] = \prod_{\omega \in P_n} (0 - \omega) \cdot \prod_{\omega \in P_n} (X - \omega^{-1}) \\ &= \Phi_n(0) \cdot \prod_{\zeta \in P_n} (X - \zeta) = \Phi_n, \end{aligned}$$

wobei die letzte Gleichheit 3.4.(c) (und damit $n > 1$) verwendet.

Für den Beweis von 3.4.(e) gruppieren wir P_n in Paare konjugiert komplexer Zahlen. Da keine reellen primitiven n-ten Einheitswurzeln für $n \geq 3$ existieren, ist das auch möglich. (Beachte auch $\omega \in P_n \iff \omega^{-1} = \overline{\omega} \in P_n$.) Jedes dieser Paare entspricht einem von $\varphi(n)/2$ Faktoren

$$(x - \omega)(x - \overline{\omega}) = x^2 - 2\,\mathrm{Re}(\omega)x + 1 = \big(x - \mathrm{Re}(\omega)\big)^2 + 1 - \mathrm{Re}(\omega)^2$$

von $\Phi_n(x)$, die wegen $\mathrm{Re}(\omega)^2 < 1$ alle positiv sind. Multiplikation ergibt $\Phi_n(x) > 0$. □

Aus $\Phi_n \in \mathbb{Z}[X]$ erhalten wir in Kombination mit Lemma 3.2 ein Resultat, das wir im weiteren Verlauf für die Teilbarkeit benötigen werden:

Korollar 3.5. *Sei n eine positive ganze Zahl, $d < n$ ein Teiler von n und $k \coloneqq n/d$. Dann gilt*

$$\Phi_n \;\Big|\; \frac{X^n - 1}{X^d - 1} = \sum_{j=0}^{k-1} (X^d)^j = 1 + X^d + \cdots + (X^d)^{k-1} \qquad \text{in } \mathbb{Z}[X].$$

Bemerkung. Der Zusatz „in $\mathbb{Z}[X]$“ bedeutet, dass das Quotientenpolynom $(X^n - 1)/[(X^d - 1)\Phi_n]$ ein Polynom mit ganzzahligen Koeffizienten ist.

Beachte außerdem, dass die rechte Seite bereits im Beweis des LTE-Lemmas, genauer in Lemma 2.1, eine wichtige Rolle gespielt hat.

Beweis. Es bezeichne hier $T(x)$ die Menge aller positiven Teiler einer ganzen Zahl x. Nach Lemma 3.2 ist $X^n - 1$ das Produkt der Polynome Φ_t für $t \in T(n)$. Da $T(d) \subseteq T(n)$ und $n \in T(n) \setminus T(d)$ (wegen $d < n$) gelten, ist Φ_n ein Teiler von

$$\prod_{t \in T(n) \setminus T(d)} \Phi_t = \frac{\prod_{t \in T(n)} \Phi_t}{\prod_{t \in T(d)} \Phi_t} = \frac{X^n - 1}{X^d - 1} = \frac{(X^d)^k - 1}{X^d - 1} = \sum_{j=0}^{k-1} (X^d)^j$$

in $\mathbb{Z}[X]$ (denn alle Φ_t für $t \mid n$ haben ganzzahlige Koeffizienten). Hierbei folgt die letzte Gleichung aus der Formel für die endliche geometrische Reihe. □

Als Nächstes wenden wir uns einer Variante der Gleichung (9) mit „+“ statt „−“ zu, die in weiterer Folge auch die oben vermutete Identität (15) beweist.

Proposition 3.6. *Sei $u \geq 3$ eine ungerade ganze Zahl. Dann gelten*

$$X^u + 1 = \prod_{d \mid u} \Phi_{2d} \qquad \text{und} \tag{14}$$

$$\Phi_{2u} = \Phi_u(-X). \tag{15}$$

Beweis. Aufgrund der Faktorisierung

$$X^u + 1 = \frac{X^{2u} - 1}{X^u - 1} = \frac{\prod_{t|2u} \Phi_t}{\prod_{t|u} \Phi_t} = \prod_{\substack{t|2u \\ t\nmid u}} \Phi_t$$

müssen wir nur mehr die positiven Teiler t von $2u$ bestimmen, die nicht u selbst teilen. Schreiben wir $t = 2^e d$ für einen Teiler d von u und $e \in \{0, 1\}$, so ist $t \nmid u$ äquivalent zu $e = 1$, also erstreckt sich das Produkt in obiger Faktorisierung genau über alle Φ_{2d} für $d \mid u$. Das beweist (14).

Für (15) gehen wir wieder induktiv vor, bemerken aber zuvor $\Phi_2(-X) = -X + 1 = -\Phi_1$. Die Induktionsbasis für $u = 3$ ergibt sich durch Kombination der Gleichungen (10) und (11). Der Induktionsschritt $< u \to u$ beruht auf der eben bewiesenen Faktorisierung (14):

$$\begin{aligned}
(X^u + 1)\Phi_u(-X) &= \big(\Phi_2 \cdot \prod_{\substack{d|u \\ 1<d<u}} \Phi_{2d} \cdot \Phi_{2u}\big) \cdot \Phi_u(-X) \\
&= [-\Phi_1(-X)] \cdot \prod_{\substack{d|u \\ 1<d<u}} \Phi_d(-X) \cdot \Phi_u(-X) \cdot \Phi_{2u} \\
&= -\prod_{d|u} \Phi_d(-X) \cdot \Phi_{2u} \\
&= -\big[(-X)^u - 1\big] \cdot \Phi_{2u} = (X^u + 1) \cdot \Phi_{2u},
\end{aligned}$$

wobei in der zweiten Zeile die Induktionsvoraussetzung (jeder Teiler einer ungeraden Zahl ist selbst ungerade!) und in der letzten Zeile Lemma 3.2 herangezogen wurde. Kürzen von $X^u + 1$ beendet die Induktion. □

Schließlich zeigen wir, wie oben angekündigt, die rekursiven Formeln zur Berechnung von Φ_N aus der Primfaktorzerlegung von N:

Satz 4. *Sei n eine positive ganze Zahl und p eine Primzahl. Dann gilt*

$$\Phi_{pn} = \begin{cases} \Phi_n(X^p), & \text{falls } p \mid n, \\ \Phi_n(X^p)/\Phi_n, & \text{falls } p \nmid n. \end{cases}$$

Beweis. Bei $p \nmid n$ ist $\Phi_n \cdot \Phi_{pn} = \Phi_n(X^p)$ zu zeigen. Da alle auftretenden Polynome $X^{pn} - 1$ teilen und dieses Polynom nur einfache Nullstellen besitzt, gilt selbiges auch für dessen Faktoren. Die Menge der Nullstellen der linken Seite ist $P_n \cup P_{pn}$, die der rechten Seite besteht aus allen $z \in \mathbb{C}$, für die $z^p \in P_n$ gilt. Es bleibt folglich $(\omega \in P_n \ \vee\ \omega \in P_{pn}) \iff \omega^p \in P_n$ für komplexe Zahlen ω zu beweisen, denn dann haben die beiden normierten Polynome auf der linken und rechten Seite dieselben einfachen Nullstellen und stimmen somit überein.

Sei zuerst $\omega \in P_n$, also $\operatorname{ord}(\omega) = n$. Lemma 1.4 liefert $\operatorname{ord}(\omega^p) = n/\operatorname{ggT}(n, p) = n$, also auch $\omega^p \in P_n$. Sei als Nächstes $\omega \in P_{pn}$. Dann ergibt sich aus Lemma 1.4 in gleicher Manier $\operatorname{ord}(\omega^p) = np/\operatorname{ggT}(np, p) = n$ und das beweist „$\Longrightarrow$“.

Sei umgekehrt $\omega \in \mathbb{C}$ mit $\omega^p \in P_n$. Nach Definition gilt wiederum $\omega^{pn} = (\omega^p)^n = 1$, also $\omega \in E_{pn}$. Daher existiert die Ordnung $d \coloneqq \operatorname{ord}(\omega)$ und erfüllt $n = \operatorname{ord}(\omega^p) = d/\operatorname{ggT}(d, p)$. Die beiden Möglichkeiten $\operatorname{ggT}(d, p) \in \{1, p\}$ führen auf $d = n$ bzw. $d = pn$, was für „$\Longleftarrow$“ noch zu zeigen war und den Beweis für den Fall $p \nmid n$ beschließt.

Betrachten wir nun den Fall $p \mid n$, in dem wir noch $\Phi_{pn} = \Phi_n(X^p)$ nachweisen müssen. Analog zum ersten Fall genügt es zu zeigen, dass die Mengen der Nullstellen übereinstimmen, d. h. $\omega \in P_{pn} \iff \omega^p \in P_n$.

Aus $\omega \in P_{pn}$ ergibt Lemma 1.4 wieder $\operatorname{ord}(\omega^p) = pn/\operatorname{ggT}(pn, p) = n$, also „$\Longrightarrow$“. Umgekehrt schließen wir wie im ersten Fall, dass $\omega \in E_{pn}$ und daher die Ordnung $d \coloneqq \operatorname{ord}(\omega)$ existiert und $n = \operatorname{ord}(\omega^p) = d/\operatorname{ggT}(d, p)$ erfüllt. Insbesondere folgt $p \mid n \mid d$ und daher $\operatorname{ggT}(d, p) = p$. Wir erhalten also $n = d/p \iff d = pn \iff \omega \in P_{pn}$, was schließlich auch „$\Longleftarrow$“ beweist. □

Korollar 3.7. *Sei n eine positive ganze Zahl und p eine Primzahl mit $p \nmid n$. Für alle positiven ganzen Zahlen e gilt dann*

$$\Phi_{p^e n} = \frac{\Phi_n\big(X^{p^e}\big)}{\Phi_n\big(X^{p^{e-1}}\big)}.$$

Beweis. Wir führen den Beweis mittels vollständiger Induktion nach e. Aus dem zweiten Fall in Satz 4 folgt die Induktionsbasis $e = 1$. Im Induktionsschritt $e \to e+1$ erhalten wir aus dem ersten Fall in Satz 4 und der Induktionsvoraussetzung somit

$$\Phi_{p^{e+1}n} = \Phi_{p^e n}\big(X^p\big) = \frac{\Phi_n\Big((X^p)^{p^e}\Big)}{\Phi_n\Big((X^p)^{p^{e-1}}\Big)} = \frac{\Phi_n\big(X^{p^{e+1}}\big)}{\Phi_n\big(X^{p^e}\big)},$$

wie gewünscht. □

Zum Abschluss geben wir noch Größenabschätzungen für die Werte der Kreisteilungspolynome für reelle Zahlen größer als 1, die wir später noch brauchen werden.

Lemma 3.8. *Sei n eine positive ganze Zahl und $x > 1$ eine reelle Zahl. Dann gilt*

$$(x-1)^{\varphi(n)} \le \Phi_n(x) \le (x+1)^{\varphi(n)}, \tag{16}$$

wobei Gleichheit in der linken Ungleichung genau für $n = 1$ (und $x > 1$ beliebig) und in der rechten genau für $n = 2$ (und $x > 1$ beliebig) eintritt.

Beweis. Für $n = 1$ gilt diese Ungleichungskette mit Gleichheit bei der linken Ungleichung. Sei also von nun an $n > 1$. Aus (2) ergibt sich

$$|x-\omega|^2 = |x|^2 + 2\,\mathrm{Re}(x\overline{(-\omega)}) + |\omega|^2 = x^2 - 2\,\mathrm{Re}(\overline{\omega})x + 1$$

für alle $\omega \in P_n$, woraus wegen $\mathrm{Re}(\overline{\omega}) = \mathrm{Re}(\omega) \in [-1, 1]$ nach Quadratergänzung und Wurzelziehen

$$x - 1 \le |x - \omega| \le x + 1$$

für alle $\omega \in P_n$ folgt, mit Gleichheit genau für $\omega = 1$ in der linken Ungleichung und $\omega = -1$ in der rechten. (Man überzeuge sich auch geometrisch davon!) Wegen $|\Phi_n(x)| = \Phi_n(x)$ nach Proposition 3.4.(e) liefert Multiplikation aller dieser Ungleichungen genau (16). Gleichheit tritt genau dann ein, wenn sie für alle Faktoren eintritt, was bei der linken Ungleichung nur für $n = 1$ und bei der rechten genau für $n = 2$ geschieht. □

Aufgabe 3.1. Zeige $n = \sum_{d|n} \varphi(d)$ in Hinblick auf die Zerlegung in (8).

Aufgabe 3.2. Überprüfe die bekannte Formel für $\varphi(n)$ mittels Gradüberlegungen in Proposition 4.

Aufgabe 3.3. Bestimme $\Phi_n(1)$ für alle positiven ganzen Zahlen n.

Aufgabe 3.4 (Österreich-Polen-Wettbewerb 2004)**.** Bestimme alle positiven ganzen Zahlen n, sodass $n^{10} + n^5 + 1$ eine Primzahl ist.

3.2 Teilbarkeit und Primteiler

Nach der ausführlichen Einführung zu Kreisteilungspolynomen im letzten Unterabschnitt sammeln wir zunächst einige naheliegende Folgerungen.

Lemma 3.9. *Sei n eine positive ganze Zahl, p eine Primzahl und $a \in \mathbb{Z}$. Weiters sei $d < n$ ein positiver Teiler von n und $k := n/d$. Dann gelten folgende Aussagen:*

(a) $\Phi_n(a)$ teilt die Zahl $\sum_{j=0}^{k-1}(a^d)^j = (a^d)^{k-1} + \cdots + a^d + 1$.

(b) Aus $n = \mathrm{ord}_p(a)$ *folgt* $p \mid \Phi_n(a)$.

Bemerkung. Schreiben wir α für die Restklasse von a modulo p, so besagt 3.9.(b) genau $\Phi_n(\alpha) = \overline{0}$ dass also jede primitive n-te Einheitswurzel α in $\mathbb{Z}/p\mathbb{Z}$ eine Nullstelle von Φ_n (in $\mathbb{Z}/p\mathbb{Z}$) ist.[13] Ruft man sich Definition 3.1 in Erinnerung, könnte man auf die Analogie hoffen, dass auch die umgekehrte Schlussfolgerung, jede Nullstelle von Φ_n in $\mathbb{Z}/p\mathbb{Z}$ sei eine primitive n-te Einheitswurzel in $\mathbb{Z}/p\mathbb{Z}$, zutrifft. Wir werden nach dem Beweis des Lemmas (mit Einschränkungen an n) auf dieses Ziel hinarbeiten.

Beweis. Aussage 3.9.(a) ergibt sich durch Einsetzen von $a \in \mathbb{Z}$ in Korollar 3.5.

Zu 3.9.(b): Aus $n = \mathrm{ord}_p(a)$ folgt $p \mid a^n - 1 = \prod_{k|n} \Phi_k(a)$, also gibt es einen positiven Teiler k von n mit $p \mid \Phi_k(a)$. Allerdings würde $k < n$ auch $p \mid \Phi_k(a) \mid a^k - 1$, d. h. $a^k \equiv 1 \pmod{p}$ ergeben, im Widerspruch zur Definition der Ordnung. Es gilt doch $k = n$ und $p \mid \Phi_n(a)$. □

An die Bemerkung anknüpfend, besagt die Definition der Kreisteilungspolynome für komplexe Zahlen ω gerade

$$\Phi_n(\omega) = 0 \qquad \Longleftrightarrow \qquad \omega \text{ ist eine primitive } n\text{-te Einheitswurzel.} \tag{17}$$

Das eben bewiesene Lemma 3.9.(b) zeigt, dass „$\Longleftarrow$“ auch für Restklassen $\omega \in \mathbb{Z}/p\mathbb{Z}$ gültig bleibt. Auf „$\Longrightarrow$“ können wir ohne Einschränkungen nicht hoffen, zum Beispiel ist $\Phi_6(2) = 2^2 - 2 + 1 = 3$, also $\Phi_6(\overline{2}) = \overline{0}$ (modulo 3), obwohl $\overline{2}$ eine zweite, und keine primitive sechste Einheitswurzel modulo 3 ist. Allerdings unterscheiden sich 2 und 6 nur um den Faktor 3, also eine Potenz der in Frage stehenden Primzahl. Tatsächlich gilt

Lemma 3.10. *Sei n eine positive ganze Zahl, p eine Primzahl und $a \in \mathbb{Z}$. Ist p ein Primteiler von $\Phi_{pn}(a)$, so auch von $\Phi_n(a)$.*

Beweis. Aus Satz 4 folgt $p \mid \Phi_{pn}(a) \mid \Phi_n(a^p)$ (in beiden Fällen). Da aber laut dem kleinen Satz von Fermat $a^p \equiv a \pmod{p}$ gilt, erhalten wir $\Phi_n(a) \equiv \Phi_n(a^p) \equiv 0 \pmod{p}$ oder äquivalent $p \mid \Phi_n(a)$. □

Mit dieser Vorbereitung können wir daher bei $p \mid \Phi_n(a)$ durch sukzessives Herausdividieren von p aus n annehmen, dass p kein Primteiler von n ist, und erhalten dann folgendes Analogon zu (17) in $\mathbb{Z}/p\mathbb{Z}$:

Proposition 3.11. *Sei n eine positive ganze Zahl, p eine Primzahl und $a \in \mathbb{Z}$. Genau dann ist die Restklasse von a modulo p eine primitive n-te Einheitswurzel in $\mathbb{Z}/p\mathbb{Z}$, wenn sie eine Nullstelle von Φ_n modulo p ist und $p \nmid n$ gilt; in Formeln:* $\mathrm{ord}_p(a) = n \iff (p \mid \Phi_n(a) \ \wedge \ p \nmid n)$.

Beweis. Gemäß Satz 1 und den Rechenregeln für Kongruenzen müssen wir tatsächlich nur die im Satz angeführte Formel zeigen. Hierbei erhalten wir bei „$\Longrightarrow$“ aus Lemma 3.9.(b) bereits $p \mid \Phi_n(a)$. Wäre nun n durch p teilbar, ergäbe sich gemäß Lemma 3.10 auch $p \mid \Phi_{n/p}(a) \mid a^{n/p} - 1$, also $a^{n/p} \equiv 1 \pmod{p}$, im Widerspruch zu $\mathrm{ord}_p(a) = n$.

Zu „$\Longleftarrow$“: Wegen $p \mid \Phi_n(a) \mid a^n - 1$ existiert die Ordnung $d := \mathrm{ord}_p(a)$ und ist ein Teiler von n. Wäre $d < n$, so ergäbe sich für $k := n/d$ mittels Lemma 3.9.(a) aus $p \mid \Phi_n(a) \mid (a^d)^{k-1} + \cdots + a^d + 1$ auch

$$0 \equiv (a^d)^{k-1} + \cdots + a^d + 1 \equiv 1^{k-1} + \cdots + 1 + 1 = k \pmod{p},$$

also $p \mid k \mid n$, im Widerspruch zur Annahme. Somit gilt $\mathrm{ord}_p(a) = d = n$. □

Man beachte hier die Ähnlichkeit zum Beweis von Lemma 2.1. Könnten wir $a^d \neq 1$ voraussetzen, wäre sogar das LTE-Lemma anwendbar gewesen. Um aber auch $a = 1$ und $a = -1$ miteinzubeziehen, haben wir den Beweis quasi wiederholt.

[13] Beachte zur Richtigkeit dieser Gleichung, dass das Einsetzen von Restklassen in Polynome $p \in \mathbb{Z}[X]$ mit ganzzahligen Koeffizienten wegen $a \equiv b \pmod{m} \implies p(a) \equiv p(b) \pmod{m}$ für a, b, $m \in \mathbb{Z}$ tatsächlich wohldefiniert ist.

Unter einem anderen Gesichtspunkt betrachtet: Falls wir eine positive ganze Zahl n und $a \in \mathbb{Z}$ gegeben haben und eine Primzahl p mit $\operatorname{ord}_p(a) = n$ suchen, können wir jeden Primteiler der ganzen Zahl $\Phi_n(a)$ dafür heranziehen. In diesem Fall ist n nach Definition die kleinste positive ganze Zahl, für die $a^n - 1$ durch p teilbar ist. Diese Situation wird im folgenden Abschnitt 4 (in einer leicht allgemeineren Situation) von zentraler Bedeutung sein, siehe Definition 4.1.

Aus Proposition 3.11 folgt unmittelbar

Korollar 3.12. *Sei n eine positive ganze Zahl und $a \in \mathbb{Z}$. Jeder Primteiler p von $\Phi_n(a)$ erfüllt entweder $p \mid n$ oder $p \equiv 1 \pmod{n}$.*

Beweis. Im Fall $p \nmid n$ sind die Voraussetzungen von Proposition 3.11 erfüllt und wir erhalten $\operatorname{ord}_p(a) = n$. Aus $\operatorname{ord}_p(a) \mid \varphi(p)$ ergibt sich $n \mid p-1 \iff p \equiv 1 \pmod{n}$. □

Eine weitere erstaunliche Folgerung lässt sich mittels Proposition 3.11 über gemeinsame Teiler von Werten der Kreisteilungspolynome treffen:

Korollar 3.13. *Seien $n < N$ positive ganze Zahlen und $a \in \mathbb{Z}$. Ist p ein gemeinsamer Primteiler von $\Phi_n(a)$ und $\Phi_N(a)$, so ist N/n eine Potenz von p.*

Beweis. Schreibe $n = p^e m$ und $N = p^E M$ für nichtnegative ganze Zahlen e, E, m und M mit $p \nmid m$ und $p \nmid M$. Durch mehrmalige Anwendung von Lemma 3.10 erhalten wir $p \mid \Phi_m(a)$ und $p \mid \Phi_M(a)$. Aus Proposition 3.11 folgt daher $m = \operatorname{ord}_p(a) = M$ und somit ist $N/n = p^{E-e}$ eine Potenz von p. □

Wir kommen schließlich zum Hauptresultat, das die bisherigen Ergebnisse zusammenfasst und zusätzlich auch eine Aussage über die Vielfachheit von Primteilern trifft:

Satz 5. *Seien n eine positive ganze Zahl, p eine Primzahl mit $p \nmid n$ und $a \in \mathbb{Z}$. Weiters sei $N = p^e n$ für eine positive ganze Zahl e.*

Ist p ein Primteiler der Zahl $\Phi_N(a)$, so folgt

$$p \mid \Phi_n(a), \qquad \operatorname{ord}_p(a) = n \qquad \text{und} \qquad p \equiv 1 \pmod{n}.$$

Bis auf den Fall $p = N = 2$ gilt außerdem $p^2 \nmid \Phi_N(a)$, also $\mathrm{v}_p\big(\Phi_N(a)\big) = 1$.

Bemerkung. Für $p = N = 2$ ist 2 ein Primteiler von $a + 1$, also a eine ungerade Zahl und wir können keine Aussagen über $\mathrm{v}_2(a+1)$ treffen. Dieser Spezialfall ist auch derjenige, der beim LTE-Lemma die Fallunterscheidung notwendig gemacht hat (bei $a \equiv 3 \pmod 4$ müssen wir ja die allgemeinere Formel verwenden).

Beachte auch, dass wir über $\mathrm{v}_p\big(\Phi_n(a)\big)$ nichts aussagen (können). Im Fall $n = 1$ wird das besonders evident und $n = 1$ stellt hier keinen Sonderfall dar, beispielsweise gilt auch $\Phi_3(22) = 22^2 + 22 + 1 = 507 = 3 \cdot 13^2$, also $13^2 \mid \Phi_3(22)$.

Beweis. Die abgesetzte Formel ist eine Kombination von Lemma 3.10 (in e-maliger Anwendung) und Proposition 3.11 (zusammen mit der Folgerung $n = \operatorname{ord}_p(a) \mid \varphi(p) = p - 1$). Zu zeigen bleibt also nur $p^2 \nmid \Phi_N(a)$ für $(p, N) \neq (2, 2)$.

Dazu schreiben wir $d \coloneqq N/p = p^{e-1} n$. Gemäß Lemma 3.10 gilt $p \mid \Phi_N(a) \mid \sum_{j=0}^{p-1} (a^d)^j$.

Für $a^d = 1$ hat diese Summe den Wert p und $p^2 \nmid \Phi_N(a)$ ist offensichtlich.

Für $p = 2$ muss zunächst zum Erfüllen der Voraussetzung $p \mid \Phi_N(a)$ auch $2 = p \equiv 1 \pmod{n}$ gelten, was nur für $n = 1$ eintreten kann. Folglich ist $N = 2^e \geq 2$ eine Zweierpotenz. Für $N \neq 2$ ist daher $d = 2^{e-1}$ ebenfalls gerade und wir erhalten $1 + a^d \equiv 2 \pmod 4$ für die oben genannte Summe, was wiederum $2^2 \nmid \Phi_N(a)$ impliziert.

Es bleibt noch der Fall $a^d \neq 1$ und $p \neq 2$ zu behandeln. Hier können wir die Summe als endliche geometrische Reihe berechnen und erhalten

$$\Phi_N(a) \,\Big|\, \frac{a^{pd} - 1}{a^d - 1} \quad \Longrightarrow \quad \mathrm{v}_p\big(\Phi_N(a)\big) \leq \mathrm{v}_p\left(\frac{a^{pd} - 1}{a^d - 1}\right) = \mathrm{v}_p\Big((a^d)^p - 1^p\Big) - \mathrm{v}_p(a^d - 1).$$

Wegen $\operatorname{ord}_p(a) = n \mid d$ gilt aber $a^d \equiv 1 \not\equiv 0 \pmod p$. Die letztgenannte Vielfachheit vereinfacht sich laut dem LTE-Lemma (Satz 2) aber zu $\mathrm{v}_p(p) = 1$ und somit gilt auch hier $p^2 \nmid \Phi_N(a)$. □

Wir demonstrieren die Verwendung der eben bewiesenen Resultate an einem

Beispiel. Wir bestimmen alle Primzahlen p, sodass $x^2+x+1=py$ Lösungen x, $y\in\mathbb{Z}$ besitzt.

Variante 1 (ohne Kreisteilungspolynome): Für $p=2$ ist das offenbar nicht möglich, für $p=3$ liefert $x=y=1$ eine Lösung. Wir setzen ab sofort $p>3$ voraus. Dann ist die gegebene Gleichung zu $4py=4x^2+4x+4=(2x+1)^2+3$ äquivalent, insbesondere gilt $(2x+1)^2\equiv -3 \pmod p$, folglich ist -3 ein quadratischer Rest modulo p. Aus dem quadratischen Reziprozitätsgesetz erhalten wir

$$1=\left(\frac{-3}{p}\right)=\left(\frac{-1}{p}\right)\cdot\left(\frac{3}{p}\right)=(-1)^{\frac{p-1}{2}}\cdot(-1)^{\frac{3-1}{2}\cdot\frac{p-1}{2}}\left(\frac{p}{3}\right)=\left(\frac{p}{3}\right),$$

was genau für $p\equiv 1 \pmod 3$ stimmt. Ist umgekehrt $p\equiv 1 \pmod 3$, so können wir gemäß obiger Rechnung ein $a\in\mathbb{Z}$ mit $a^2\equiv -3 \pmod p$ finden. Mit a erfüllt auch $a+p$ (mit von a verschiedener Parität) diese Kongruenz, daher gibt es jedenfalls eine ungerade ganze Zahl u mit $p\mid u^2+3$. Da u^2+3 durch 4 teilbar ist und p ungerade, folgt $4p\mid u^2+3$. Schreiben wir $x:=(u-1)/2$ und $y:=(u^2+3)/4p$, haben wir die gewünschten ganzzahligen Lösungen gefunden.

Variante 2: Rufen wir uns $\Phi_3=X^2+X+1$ in Erinnerung, wollen wir also alle möglichen Primteiler p von $\Phi_3(x)$ für ganze Zahlen x bestimmen. Korollar 3.12 liefert $p\mid 3$ oder $p\equiv 1 \pmod 3$. Der Fall $p\mid 3$, also $p=3$, wird wie oben durch $x=y=1$ abgedeckt. Für den Fall $p\equiv 1 \pmod 3$ müssen wir hingegen laut Lemma 3.9.(b) nur eine ganze Zahl x mit $\operatorname{ord}_p(x)=3$ finden. Für eine Primitivwurzel w modulo p liefert aber die Zahl $x=w^{(p-1)/3}$ ein solches Beispiel, denn $x^1\not\equiv 1\not\equiv x^2 \pmod p$ wegen $1\le\frac{p-1}{3}\le\frac{2(p-1)}{3}<p-1=\operatorname{ord}_p(w)$ nach Definiton einer Primitivwurzel, aber $x^3=w^{p-1}\equiv 1 \pmod p$, dementsprechend gilt $\operatorname{ord}_p(x)=3$.

Aufgabe 3.5 (ÖMO ZWF 2010)**.** Sei

$$f(n):=\sum_{k=0}^{2010}n^k=1+n+\cdots+n^{2010}.$$

Zeige für jede ganze Zahl m mit $2\le m\le 2010$, dass es keine nichtnegative ganze Zahl n gibt, für die $f(n)$ durch m teilbar ist.

Aufgabe 3.6 (Bulgarien TST)**.** Bestimme alle positiven ganzen Zahlen m und n, für die n ein Teiler von $1+m^{3^n}+m^{2\cdot 3^n}$ ist.

Aufgabe 3.7 (IMO-Shortlist 2006)**.** Bestimme alle x, $y\in\mathbb{Z}$ mit $x\neq 1$, die der Gleichung

$$\frac{x^7-1}{x-1}=y^5-1$$

genügen.

Aufgabe 3.8 (IMO 2003)**.** Sei p eine Primzahl. Beweise, dass es eine Primzahl q gibt, sodass n^p-p für keine ganze Zahl n durch q teilbar ist.

4 Der Satz von Zsigmondy

Nach der profunden Einführung zu Teilbarkeit bei Kreisteilungspolynomen können wir schließlich den folgenden Satz von Zsigmondy mit relativ wenig Aufwand beweisen.

Satz 6 (Zsigmondy)**.** *Seien $a > b > 0$ und $n > 1$ ganze Zahlen mit $\mathrm{ggT}(a, b) = 1$. Dann gibt es einen Primteiler von $a^n - b^n$, der keine der Zahlen $a^k - b^k$ für $k \in \{1, \dots, n-1\}$ teilt, bis auf die Ausnahmen*

- $2^6 - 1^6$ *und*
- $a^2 - b^2$*, wenn $a + b$ eine Zweierpotenz ist.*

Primzahlen mit der im Satz beschriebenen Eigenschaft erhalten eine (historisch gewachsene) Bezeichnung.

Definition 4.1. Seien $a > b > 0$ und $n > 1$ ganze Zahlen mit $\mathrm{ggT}(a, b) = 1$. Eine Primzahl p heiße *primitiver Primteiler für (a, b) der Ordnung n*, falls $p \mid a^n - b^n$, aber $p \nmid a^k - b^k$ für alle $k \in \{1, \dots, n-1\}$ gilt.

Bemerkung. Zu dieser Definitionen scheinen mehrere Bemerkungen angebracht:

1. Wenn a und b als bekannt vorausgesetzt werden können, sprechen wir einfach von primitiven Primteilern der Ordnung n.
2. Die in der Literatur übliche Bezeichnung *primitiver Primteiler von $a^n - b^n$* hat den Nachteil, dass sie nur eine Zahl, aber nicht a, b oder n spezifiziert. So ist beispielsweise 3 ein primitiver Primteiler von $(8, 1)$ der Ordnung 2, denn $3 \mid 8^2 - 1 = 63$, aber nicht primitiver Primteiler von $(4, 1)$ der Ordnung 3, denn $3 \mid 4^1 - 1$, obwohl $4^3 - 1 = 63 = 8^2 - 1$ dieselbe Zahl spezifiziert. Wir werden daher immer zumindest auch die Ordnung anführen.

Um die allgemeine Variante von Satz 6 für $a^n - b^n$ statt nur für $a^n - 1$ zu erhalten, beschäftigen wir uns erst mit einer Methode, die aus Polynomen in einer Variablen homogene Polynome in zwei Variablen erzeugt.

4.1 Homogenisierung von Polynomen

Wir werden im Verlauf dieses Kapitels vor allem mit Polynomen in zwei Variablen rechnen, die folgende Definition ist aber auch für Polynome mit mehr als zwei Variablen sinnvoll.

Definition 4.2. Ein Polynom heißt *homogen* vom Grad $d \geq 0$, falls (nach Zusammenfassen aller Terme) sämtliche auftretenden Monome denselben Grad d besitzen.

Beispiel. In $\mathbb{C}[X]$, also für Polynome mit komplexen Koeffizienten in einer Variablen, sind nur die Monome $a \cdot X^n$ für $a \in \mathbb{C}$, $n \in \mathbb{Z}_{\geq 0}$ homogen (vom Grad n).

Für zwei Variablen X, Y gibt es mehrere Möglichkeiten für Monome, so sind zum Beispiel die Polynome $4X^3 + 5X^2Y - \frac{2}{3}Y^3$, $X^2 + \mathrm{i}\,Y^2$ und πXY^{2023} homogen (jeweils vom Grad 3, 2 bzw. 2024; das letzte Polynom ist überhaupt ein Monom). Nicht homogen sind $X^2 + 1$ oder $X^2Y + Y^3 - Y^2$.

Für univariate Polynome vom Grad d können wir durch „Auffüllen“ der auftretenden Monome mit der neuen Polynomvariable auf Grad d ein homogenes Polynom vom Grad d in zwei Variablen erzeugen. Da wir dieses *Homogenisieren* nur in einer Variablen benötigen, geben wir die Definition auch nur für diesen Fall an.

Definition 4.3. Sei $0 \neq f \in \mathbb{C}[X]$ ein univariates Polynom mit komplexen Koeffizienten, schreibe $f = \sum_{k=0}^{d} c_k X^k$ mit $c_d \neq 0$. Die *Homogenisierung* ${}^{\mathrm{h}}f \in \mathbb{C}[X, Y]$ von f ist dann gegeben durch

$$ {}^{\mathrm{h}}f \coloneqq \sum_{k=0}^{d} c_k X^k Y^{d-k} = Y^d \cdot \sum_{k=0}^{d} c_k \left(\frac{X}{Y}\right)^k = Y^d \cdot f\left(\frac{X}{Y}\right). $$

Beispiel. Zum Beispiel ist die Homogenisierung von $4X^3 + \pi X - 5$ gleich $4X^3 + \pi XY^2 - 5Y^3$.

Für ganze Zahlen $n > 0$ gilt weiters

$$^{\mathrm{h}}(X^n - 1) = X^n - Y^n.$$

Nachdem wir in Abschnitt 3 das Polynom $X^n - 1$ so gründlich untersucht haben, können wir viele Resultate darüber auch auf zwei Variablen übertragen. Homogene Polynome in zwei Variablen verhalten sich nämlich in vielen Belangen sehr ähnlich wie die zugehörigen Polynome in einer Variablen (die man durch Setzen von $Y = 1$ zurückerhält). Von zentraler Bedeutung für unsere Untersuchungen sind daher die homogenisierten Kreisteilungspolynome.

Lemma 4.4. *Sei $n > 0$ eine ganze Zahl und p eine Primzahl. Dann gelten die folgenden Aussagen:*

(i) Ist $0 \neq f \in \mathbb{C}[X, Y]$ ein homogenes Polynom vom Grad d, so gilt $f(tx, ty) = t^d \cdot f(x, y)$ für alle komplexen Zahlen x, y und t.

(ii) $X^n - Y^n = \prod_{d|n} {}^{\mathrm{h}}\Phi_n$

(iii) $^{\mathrm{h}}\Phi_n \in \mathbb{Z}[X, Y]$*, d. h. die Koeffizienten von* $^{\mathrm{h}}\Phi_n$ *sind alle ganzzahlig*

(iv) Es gilt

$$^{\mathrm{h}}\Phi_{pn} = \begin{cases} {}^{\mathrm{h}}\Phi_n(X^p, Y^p), & \text{falls } p \mid n, \\ \frac{{}^{\mathrm{h}}\Phi_n(X^p, Y^p)}{{}^{\mathrm{h}}\Phi_n}, & \text{falls } p \nmid n. \end{cases}$$

(v) Für ganze Zahlen $a > b > 0$ gilt $(a - b)^{\varphi(n)} \leq {}^{\mathrm{h}}\Phi_n(a, b) \leq (a + b)^{\varphi(n)}$ mit Gleichheit in der linken Ungleichung genau für $n = 1$ und in der rechten genau für $n = 2$.

Beweis. Ad 4.4.(i): Schreibe $f = \sum_{j=0}^{d} c_j X^j Y^{d-j}$ für komplexe Zahlen $c_0, \ldots, c_d$. Dann folgt

$$t^d \cdot f(x, y) = \sum_{j=0}^{d} c_j x^j y^{d-j} t^d = \sum_{j=0}^{d} c_j (tx)^j (ty)^{d-j} = f(tx, ty).$$

Aussage 4.4.(iii) rührt daher, dass Φ_n und $^{\mathrm{h}}\Phi_n$ dieselben Koeffizienten besitzen und diese nach Proposition 3.4.(a) sämtlich ganzzahlig sind.

Die Aussagen 4.4.(ii), 4.4.(iv) und 4.4.(v) ergeben sich durch Einsetzen der Definition von Homogenisierung in die jeweiligen Aussagen in Lemma 3.2, Satz 4 und Lemma 3.8. □

Aufgabe 4.1 (MEMO 2011)**.** Seien A und B disjunkte nichtleere Mengen, für die $A \cup B = \{1, 2, 3, \ldots, 10\}$ gilt. Zeige, dass es Elemente $a \in A$ und $b \in B$ gibt, sodass die Zahl $a^3 + ab^2 + b^3$ durch 11 teilbar ist.

4.2 Beweis des Satzes

Mit dieser Vorbereitung sind wir schließlich in der Lage, den Satz 6 von Zsigmondy zu zeigen.

Beweis von Satz 6. Seien $a > b > 0$ teilerfremde ganze Zahlen, $n > 1$ und p ein beliebiger Primteiler von $a^n - b^n$. Bei $p \mid b$ folgte $p \mid (a^n - b^n) + b^n$, also $p \mid a^n \implies p \mid a$, im Widerspruch zu $\mathrm{ggT}(a, b) = 1$. Daher sind p und b auch teilerfremd und es folgt die Existenz einer ganzen Zahl $c > 0$ mit $bc \equiv 1 \pmod{p}$. (Beachte, dass die Restklasse von c von p abhängt.) In dieser Situation formulieren wir nachstehend ein Lemma, bei dem wir insbesondere auf die Äquivalenz von 4.5.(i) und 4.5.(iv) abzielen.

Lemma 4.5. *Genau dann teilt p die Zahl $^{\mathrm{h}}\Phi_n(a, b)$, wenn sie $\Phi_n(ac)$ teilt.*

Zudem sind die folgenden Aussagen äquivalent:

(i) p ist ein primitiver Primteiler für (a, b) der Ordnung n.

(ii) *p ist ein primitiver Primteiler für $(ac, 1)$ der Ordnung n.*

(iii) *Es gilt* $\operatorname{ord}_p(ac) = n$.

(iv) *Es gilt* $p \mid {}^{\mathrm{h}}\Phi_n(a,b)$ *und* $p \nmid n$.

Beweis von Lemma 4.5. Aus den Unterpunkten (i) und (iii) von Lemma 4.4 folgt zusammen mit den Rechenregeln für Kongruenzen

$$ {}^{\mathrm{h}}\Phi_n(a,b) \cdot c^{\varphi(n)} = {}^{\mathrm{h}}\Phi_n(ac,bc) \equiv {}^{\mathrm{h}}\Phi_n(ac,1) = \Phi_n(ac) \pmod{p}, \tag{18} $$

was wegen $p \nmid c$ die erste Aussage beweist.

Zu den äquivalenten Aussagen: Definitionsgemäß bedeutet 4.5.(i) genau $a^n \equiv b^n \pmod{p}$ und $a^k \not\equiv b^k \pmod{p}$ für ganze $1 \le k < n$, was nach Multiplikation mit c^n bzw. c^k zu $(ac)^n \equiv 1 \pmod{p}$ und $(ac)^k \not\equiv 1 \pmod{p}$ für ganze $1 \le k < n$, d. h. zu 4.5.(ii) äquivalent ist. Diese Aussage bedeutet aber nach Definition offenbar auch $\operatorname{ord}_p(ac) = n$, also 4.5.(iii). Laut Proposition 3.11 heißt 4.5.(iii) aber nichts anderes als $p \mid \Phi_n(ac)$ und $p \nmid n$, was wegen der zuerst gezeigten Aussage $p \mid \Phi_n(ac) \iff p \mid {}^{\mathrm{h}}\Phi_n(a,b)$ die noch offene Äquivalenz von 4.5.(iii) und 4.5.(iv) nachweist. □

Bemerkung. Da die Restklasse von c invers zu der von b modulo p ist, stellt auch die erste Aussage bei Beachtung von ${}^{\mathrm{h}}\Phi_n(a,b) = b^{\varphi(n)} \cdot \Phi_n(ab^{-1})$ keine große Überraschung dar. Was wir hier nachgerechnet haben, ist die Verträglichkeit des Übergangs dieser Gleichung von $\mathbb{Q}$ auf $\mathbb{Z}/p\mathbb{Z}$, was der Teilerfremdheit von p und b geschuldet ist.

Fortsetzung des Beweises von Satz 6. Wir nehmen im Folgenden an, dass es keinen primitiven Primteiler (für (a,b)) der Ordnung n gibt. Mit der Negation von Lemma 4.5 folgt nun, dass jeder Primteiler von ${}^{\mathrm{h}}\Phi_n(a,b)$ (der wegen ${}^{\mathrm{h}}\Phi_n(a,b) \mid a^n - b^n$ die Voraussetzungen für das Lemma erfüllt) auch ein Primteiler von n sein muss. Zu zeigen bleibt, dass eine der Ausnahmen in Satz 6 eintritt.

Sei p der kleinste Primteiler von ${}^{\mathrm{h}}\Phi_n(a,b)$. Dieser existiert wegen ${}^{\mathrm{h}}\Phi_n(a,b) > (a-b)^{\varphi(n)} \ge 1$ gemäß Lemma 4.4.(v) für $n > 1$. Unsere Annahme bedingt $p \mid n$, schreibe also $n = p^e d$ für positive ganze Zahlen e und d mit $p \nmid d$. Aus Lemma 4.5 erhalten wir $p \mid \Phi_n(ac)$, und aus Satz 5 (mit $N \coloneqq n$ und $n \coloneqq d$) dann $d = \operatorname{ord}_p(ac) \mid p-1$ insbesondere $d < p$. Gäbe es einen weiteren Primteiler $q \neq p$ von ${}^{\mathrm{h}}\Phi_n(a,b)$, so hieße das $q \mid n = p^e d$, folglich $q \mid d$ und $q \le d < p$, im Widerspruch zur Minimalität von p. Also muss ${}^{\mathrm{h}}\Phi_n(a,b)$ eine Potenz von p sein.

Sei $v \coloneqq \mathrm{v}_p\big({}^{\mathrm{h}}\Phi_n(a,b)\big) \ge 1$ und $c > 0$ am Anfang des Beweises so gewählt, dass $bc \equiv 1 \pmod{p^v}$. Dann gilt Kongruenz (18) sogar modulo p^v. Somit teilt p^v neben ${}^{\mathrm{h}}\Phi_n(a,b)$ auch $\Phi_n(ac)$ und die Vielfachheitsaussage in Satz 5 liefert für $(p,n) \neq (2,2)$ daher $v = 1$.

Behandeln wir gleich den Fall $p = n = 2$: Falls ${}^{\mathrm{h}}\Phi_2(a,b) = a + b$ einen ungeraden Primteiler r besitzt, so ist dieser wegen $a - b \equiv 2a \not\equiv 0 \pmod{r}$ kein Teiler von $a-b$ und folglich ein primitiver Primteiler für (a,b) der Ordnung 2. Die einzige Ausnahme stellt bei $n = 2$ also der Fall dar, dass $a + b$ eine Zweierpotenz ist, was tatsächlich eintreten kann (und als zweite Ausnahme in Satz 6 angeführt ist).

Für $(p,n) \neq (2,2)$ gilt ${}^{\mathrm{h}}\Phi_n(a,b) = p$, wobei $n = p^e d$ mit $d < p$. Zum Abschluss des Beweises werden wir zeigen, dass in diesem Fall $p = 3$, $e = 1$ und $d = 2$ gelten muss (was der ersten Ausnahme in Satz 6 entspricht). Aus Lemma 4.4.(v) folgt $p = {}^{\mathrm{h}}\Phi_n(a,b) > (a-b)^{\varphi(n)} \ge (a-b)^{p-1}$. Wäre $a - b \ge 2$, so erhielten wir unter Verwendung des binomischen Lehrsatzes den Widerspruch

$$ p > (a-b)^{p-1} \ge 2^{p-1} \ge \binom{p-1}{0} + \binom{p-1}{1} = p. $$

Folglich gilt $a - b = 1$, a und b haben unterschiedliche Parität und p ist als Teiler von $a^n - b^n$ ungerade. Wäre $e \ge 2$, so ergäbe sich aus Lemma 4.4.(iv) (mit n/p an Stelle von n) und dem binomischen Lehrsatz der Widerspruch

$$ p = {}^{\mathrm{h}}\Phi_n(a,b) = {}^{\mathrm{h}}\Phi_{n/p}(a^p,b^p) \ge (a^p - b^p)^{\varphi(n/p)} \ge a^p - b^p = (1+b)^p - b^p \ge 1 + pb > p. $$

Daher ergibt sich $e = 1$ und somit $n = pd$ mit $d < p$. Aus 4.4.(iv) und 4.4.(v) folgt

$$p = {}^{\mathrm{h}}\Phi_n(a,b) = \frac{{}^{\mathrm{h}}\Phi_d(a^p,b^p)}{{}^{\mathrm{h}}\Phi_d(a,b)} \geq \frac{(a^p-b^p)^{\varphi(d)}}{(a+b)^{\varphi(d)}} \geq \frac{a^p-b^p}{a+b} = \frac{(1+b)^p-b^p}{2b+1} \geq \frac{(1+b)^p-b^p}{3b},$$

wobei sich die mittlere Ungleichung aus $\frac{a^p-b^p}{a+b} = \frac{(a-b)(a^{p-1}+a^{p-2}b+\cdots+b^{p-1})}{a+b} > \frac{a^{p-1}+b^{p-1}}{a+b} \geq 1$ ergibt. Laut dem binomischen Lehrsatz gilt weiter

$$(1+b)^p - b^p = \sum_{k=0}^{p-1} \binom{p}{k} b^k > pb + \binom{p}{2} b^2 \geq pb + \frac{p(p-1)}{2} b = \frac{p(p+1)}{2} b$$

was insgesamt

$$p \geq \frac{(1+b)^p-b^p}{3b} > \frac{p(p+1)}{6} \quad \Longleftrightarrow \quad 6 > p+1$$

bedingt. Da p ungerade ist, bleibt daher nur $p = 3$ übrig. Wegen $d < p$ sind die einzigen Möglichkeiten für $n = pd$ nur $n = 3$ und $n = 6$.

Im Fall $n = 3$ ist $3 = p = {}^{\mathrm{h}}\Phi_3(a,b) = a^2 + ab + b^2$ wegen $a > b > 0$ unmöglich. Der Fall $n = 6$ hingegen liefert $3 = {}^{\mathrm{h}}\Phi_6(a,b) = a^2 - ab + b^2 = a(a-b) + b^2 = (1+b) + b^2$ und die einzige, noch mögliche Ausnahme $a = 2$, $b = 1$, was den Beweis beschließt. □

Tatsächlich existiert laut Lemma 4.5 wegen $3 = {}^{\mathrm{h}}\Phi_6(2,1)$ kein primitiver Primteiler für $(2,1)$ der Ordnung 6, was man auch leicht ohne Theorie nachprüft: Bei $2^6 - 1^6 = 63 = 3^2 \cdot 7$ kommt 3 bereits in $2^2 - 1^2$ und 7 in $2^3 - 1^3$ vor.

Wir stellen auch eine Variante von Satz 6 für Summen vor, die sich leicht aus dem eben bewiesenen Resultat ergibt:

Korollar 4.6. *Seien $a > b > 0$ und $n > 1$ ganze Zahlen mit $\mathrm{ggT}(a,b) = 1$. Dann gibt es einen Primteiler von $a^n + b^n$, der keine der Zahlen $a^k + b^k$ für $k \in \{1,\ldots,n-1\}$ teilt, außer bei $2^3 + 1^3$.*

Beweis. Sei p ein primitiver Primteiler für (a,b) der Ordnung $2n$, der laut dem Satz 6 von Zsigmondy bis auf $n = 3$ immer existiert. (Beachte, dass die zweite Ausnahme wegen $n > 1$ nicht eintritt.) Dann gilt $p \mid a^{2n} - b^{2n} = (a^n + b^n)(a^n - b^n)$, aber $p \nmid a^n - b^n$, also $p \mid a^n + b^n$. Für $k \in \{1,\ldots,n-1\}$ ist jedoch keine der Zahlen $a^k + b^k$ durch p teilbar, weil sonst auch $p \mid (a^k - b^k)(a^k + b^k) = a^{2k} - b^{2k}$ gelten würde, im Widerspruch dazu, dass p primitiver Primteiler der Ordnung $2n$ ist. □

Wir demonstrieren die Anwendung von Zsigmondys Satz an einem

Beispiel. Finde alle positiven ganzen Zahlen a, n und k mit $n > 1$ und $3^k - 1 = a^n$.

Betrachtung modulo 3 liefert $a^n \equiv -1 \pmod 3$ und da -1 kein quadratischer Rest modulo 3 ist, muss n ungerade sein. Dann ergibt $a + 1 \mid a^n + 1 = 3^k$, dass $a + 1 > 1$ selbst eine Dreierpotenz ist, insbesondere $3 \mid a^1 + 1^1$. Ist $(a,n) \neq (2,3)$, so liegt hier keine Ausnahme zu Korollar 4.6 vor und es gibt einen Primteiler von $a^n + 1$, der insbesondere nicht $a + 1$ teilt, im Widerspruch zu $a^n + 1 = 3^k$. Der Fall $(a,n) = (2,3)$ liefert die einzige Lösung mit $k = 2$.

Aufgabe 4.2 (IMO-Shortlist 2002)**.** Sei N eine positive ganze Zahl, die das Produkt von r Primzahlen ist, die alle größer als 3 sind. Zeige, dass $2^N + 1$ mindestens 4^r Teiler besitzt.

Aufgabe 4.3 (Rumänien TST 1994)**.** Zeige, dass die Folge $(3^n - 2^n)_{n \geq 1}$ keine geometrische Teilfolge der Länge ≥ 3 hat.

Aufgabe 4.4 (Italien TST 2003)**.** Bestimme alle Tripel (a,b,p) positiver ganzer Zahlen, für die p prim ist und die $2^a + p^b = 19^a$ erfüllen.

Aufgabe 4.5 (Polen)**.** Seien $p \neq q$ zwei ungerade Primzahlen. Beweise: $2^{pq} - 1$ besitzt mindestens drei verschiedene Primteiler.

Aufgabe 4.6 (Example 2 in [5])**.** Bestimme alle nichtnegativen ganzen Zahlen m und n, sodass $3^m - 5^n$ eine Quadratzahl ist.

Aufgabe 4.7 (Problem 1 in [5])**.** Bestimme alle ganzen Zahlen x, y und z mit $x^{2009} + y^{2009} = 7^z$.

Aufgabe 4.8 (IMO Shortlist 2000)**.** Finde alle Tripel (a, m, n) positiver ganzer Zahlen, sodass $a^m + 1$ die Zahl $(a + 1)^n$ teilt.

Aufgabe 4.9 (Japan 2011)**.** Finde alle Quintupel (a, n, p, q, r) positiver ganzer Zahlen, die der folgenden Gleichung genügen:

$$a^n - 1 = (a^p - 1)(a^q - 1)(a^r - 1)$$

Zur Entstehung

Die Idee zur allgemeinen Fassung von Abschnitt 1 ist bei der Lektüre von §54 in [6] entstanden, unter anderem findet man übrigens dort in §59 auch einen Beweis zur Irreduzibilität der Kreisteilungspolynome in $\mathbb{Q}[X]$. Einen elementareren findet man in [3, Theorem 4.17].

Abschnitt 2 ist fast gänzlich [1] nachempfunden, ein wenig ausführlicher, vielleicht sogar in noch einprägsamerer Form.

Der wohl umfangreichste Abschnitt 3 ist zunächst durch die Datei [2] motiviert worden, außerdem haben einige Übungsaufgaben aus [6, §54] die Propositionen bereichert. Die Darstellung weicht jedoch ein wenig von der in [2] ab, obwohl die Hauptresultate dorther stammen.

Die Hauptreferenz für den abschließenden Abschnitt 4 stellt [4] dar, auch wenn der Beweis durch die zuvor bewiesenen Resultate wesentlich gekürzt werden konnte. Es ist zu hoffen, dass die Beweisstruktur von der abgeänderten Notation und der Kürzung profitiert hat.

Die Aufgaben stammen aus verschiedensten Aufgabensammlungen, im letzten Abschnitt 4 sind die meisten aus [5] entnommen, wo auch noch einige andere zu finden sind.

Literatur

[1] Heuberger, Clemens: *Zahlentheorie für Internationale Bewerbe – Lifting the Exponent.* `https://oemo.at/OeMO/Downloads/datei/155`, 2021. Aufgerufen am 13. Juni 2023.

[2] Heuberger, Clemens: *Zahlentheorie für Internationale Bewerbe – Teilbarkeit von Kreisteilungspolynomen.* `https://oemo.at/OeMO/Downloads/datei/146`, 2021. Aufgerufen am 13. Juni 2023.

[3] Jacobson, Nathan: *Basic Algebra I, 2nd. ed.* Freeman and Company, 1995.

[4] Michels, Bart: *Zsigmondy's Theorem.* `https://bartmichels.github.io/files/zsigmondy_en.pdf`, 2014. Aufgerufen am 13. Juni 2023.

[5] PISOLVE: *The Zsigmondy Theorem.* `https://services.artofproblemsolving.com/download.php?id=YXR0YWNobWVudHMvOC9kL2QyOWE0NDFhNDRjMGExNjEwNzk2OGNlMzJlNTNlZGRlZDM5Y2U4&rn=WnNpZ21vbmR5IFRoZW9yZW0ucGRm`, 2011. Aufgerufen am 13. Juni 2023.

[6] Scheja, Günter und Uwe Storch: *Lehrbuch der Algebra: Unter Einschluss der linearen Algebra Teil 2.* Mathematische Leitfäden. B. G. Teubner Stuttgart, 1988.