52. Österreichische Mathematik-Olympiade

Bundeswettbewerb – Finale – Lösungen

4./5. Juni 2021

Aufgabe 1. *Seien a, b und c paarweise verschiedene natürliche Zahlen.*

Man beweise

$$\frac{a^3+b^3+c^3}{3} \geq abc + a + b + c.$$

Wann gilt Gleichheit?

(Karl Czakler)

Lösung 1. Es gilt

$$a^3 + b^3 + c^3 - 3abc = \frac{1}{2}(a+b+c)((a-b)^2 + (b-c)^2 + (c-a)^2). \tag{1}$$

Wenn man nicht weiß, dass $(a+b+c)$ den Ausdruck $a^3+b^3+c^3-3abc$ teilt, kann man das auch dadurch erhalten, dass man $a^3+b^3+c^3$ in elementarsymmetrischen Funktionen $e_1 = a+b+c$, $e_2 = ab+bc+ca$ und $e_3 = abc$ ausdrückt.

Wir nehmen jetzt o. B. d. A. an, dass $a > b > c \geq 0$. Da es sich um ganze Zahlen handelt, wird das zu $a - b \geq 1$, $b - c \geq 1$ und $a - c \geq 2$.

Damit erhalten wir aus der Gleichung (1), dass

$$a^3 + b^3 + c^3 - 3abc \geq \frac{1}{2}(a+b+c)(1+1+4) = 3(a+b+c)$$

und alles ist gezeigt.

Gleichheit gilt dabei für $a = b+1$, $b = c+1$ und $a = c+2$, also für die Tripel $(t+2, t+1, t)$ und alle ihre Permutationen, wobei t eine natürliche Zahl ist.

(Karl Czakler) □

Lösung 2. Wir setzen o. B. d. A. voraus, dass $a < b < c$ gilt. Da es sich um natürliche Zahlen handelt, bedeutet das $a + 1 \leq b$ und $b + 1 \leq c$. Um diese Nebenbedingungen zu vereinfachen, führen wir Schlupfvariablen für die Differenzen ein, das bedeutet $b = a + x + 1$ und $c = b + y + 1 = a + x + y + 2$ mit $x, y \geq 0$.

Wenn man das einsetzt, alles ausmultipliziert und auf dieselbe Seite bringt, erhält man die äquivalente Ungleichung

$$2x^3/3 + y^3/3 + 3x^2 + x^2a + x^2y + y^2a + y^2x + 2y^2 + 2x + 3y + 3ax + 3ay + 4xy + axy \geq 0.$$

Diese Ungleichung ist trivialerweise richtig, da links alle Terme größer gleich 0 sind. Da die Terme $2x$ und $3y$ auftreten, muss bei Gleichheit $x = y = 0$ gelten, für diese Werte gilt aber natürlich auch Gleichheit. Damit sind die Gleichheitsfälle drei aufeinanderfolgende natürliche Zahlen in beliebiger Anordnung.

(Theresia Eisenkölbl) □

Aufgabe 2. *Herr Ganzgenau möchte sein Teehäferl ganz genau vorne aus der Mikrowelle herausnehmen. Die Mikrowelle von Herrn Ganzgenau möchte da aber so ganz genau gar nicht mitspielen.*

Ganz genau gesagt spielen die beiden das folgende Spiel:

Sei n eine positive ganze Zahl. In n Sekunden macht der Drehteller der Mikrowelle eine vollständige Umdrehung. Bei jedem Einschalten der Mikrowelle wird eine ganzzahlige Anzahl von Sekunden entweder im oder gegen den Uhrzeigersinn gedreht, sodass es n mögliche Positionen gibt, auf denen das Teehäferl stehen bleiben kann. Eine dieser Positionen ist ganz genau vorne.

Zu Beginn dreht die Mikrowelle das Teehäferl auf eine der n möglichen Positionen. Danach gibt Herr Ganzgenau in jedem Zug eine ganzzahlige Anzahl von Sekunden ein, und die Mikrowelle entscheidet, entweder im oder gegen den Uhrzeigersinn diese Anzahl von Sekunden lang zu drehen.

Für welche n kann Herr Ganzgenau erzwingen, das Teehäferl nach endlich vielen Zügen ganz genau vorne aus der Mikrowelle nehmen zu können?

(Birgit Vera Schmidt)

Antwort. Herr Ganzgenau kann genau dann den Sieg erzwingen, wenn n eine Zweierpotenz ist.

Lösung. **Herleitung.**

Wir gehen das Spiel rückwärts an und überlegen als erstes, wie eine Situation aussehen könnte, von der aus Herr Ganzgenau in einem einzigen Zug gewinnen kann. Das geht eigentlich nur, wenn das Teehäferl genau gegenüber von der Mikrowellentür steht, also „hinten", was nur bei geradem n überhaupt möglich ist. In diesem Fall tippt Herr Ganzgenau $n/2$ Sekunden ein, und die Mikrowelle hat nur noch die Wahl, entweder im oder gegen den Uhrzeigersinn das Häferl nach „vorne" zu drehen.

Wir „sehen", dass von allen anderen Positionen aus die Mikrowelle immer mindestens eine Option hat, das Häferl nicht nach „vorne" zu drehen, werden uns aber erst später im Detail damit auseinandersetzen.

Damit die Mikrowelle den Sieg verhindern kann, muss sie also vermeiden, das Häferl jemals auf der Position „vorne" oder der Position „hinten" abzustellen.

Wir gehen einen weiteren Schritt zurück und überlegen, wie Herr Ganzgenau die Mikrowelle genau dazu zwingen könnte. Dies gelingt ihm auf jeden Fall dann, wenn das Teehäferl genau zwischen diesen zwei Positionen steht, also entweder bei $n/4$ oder bei $3n/4$, wenn wir die Positionen so im Uhrzeigersinn mit den Zahlen von 1 bis n beschriften, dass n „vorne" ist. In diesem Fall (der nur eintreten kann, wenn n durch 4 teilbar ist) tippt Herr Ganzgenau $n/4$ ein, womit die Mikrowelle das Häferl entweder nach „vorne" stellen muss und sofort verliert, oder es nach „hinten" stellt und einen Zug später verliert.

Wir vermuten wieder, dass für alle Positionen außer diesen vier die Mikrowelle immer die Möglichkeit hat, das Häferl weder „vorne" noch „hinten" stehen zu lassen, verschieben den Beweis aber auf später.

Vorerst gehen wir einen weiteren Schritt zurück und sehen, dass Herr Ganzgenau von den Positionen $n/8$, $3n/8$, $5n/8$ und $7n/8$ aus (falls diese ganzzahlig sind, also n durch 8 teilbar ist) jeweils $n/8$ eintippen kann und wieder auf einer der vier Positionen landet, von denen aus wir die Gewinnstrategie bereits kennen.

Dies lässt sich fortsetzen: Sei k die größte natürliche Zahl, sodass 2^k ein Teiler von n ist, d. h. n habe die Form $n = m \cdot 2^k$ mit einer passenden ungeraden positiven ganzen Zahl m. Dann kann Herr Ganzgenau von allen Positionen der Form

$$a \cdot \frac{n}{2^k} = a \cdot m \tag{2}$$

mit einer positiven ganzen Zahl $1 \leq a \leq 2^k$ aus die beschriebene Gewinnstrategie verwenden. Im Fall, dass n eine Zweierpotenz ist (also $m = 1$), sind das alle n Positionen, sodass Herr Ganzgenau für solche n den Sieg immer erzwingen kann.

Wir vermuten nun, dass für jedes n, das keine reine Zweierpotenz ist (also $m > 1$), die Mikrowelle den Sieg verhindern kann. Wir wissen bereits, dass sie dazu alle Positionen vermeiden muss, die sich wie in (2) darstellen lassen, also durch m teilbar sind. Es genügt aber auch zu zeigen, dass von jeder Position, die nicht durch m teilbar ist, zumindest eine der beiden Drehrichtungen wieder zu einer nicht durch m teilbaren Position führt. Damit wird insbesondere auch „vorne" $= n = 2^k \cdot m$ dauerhaft vermieden, womit Herr Ganzgenau nicht gewinnen kann. Mit modulo-Betrachtungen ist diese Behauptung aber sehr schnell gezeigt, wie wir im Folgenden noch sauber aufschreiben werden.

Da wir Herrn Ganzgenau und der Mikrowelle nicht die gesamte Herleitung als Spielanleitung mitgeben wollen, schreiben wir die jeweiligen Strategien jetzt noch konkret auf:

Strategie.

Die Positionen seien von 1 bis n beschriftet, und die Position „vorne" habe die Nummer n.

Im Fall $n = 1$ gibt es nur die Position „vorne", Herr Ganzgenau gewinnt also immer.

Sei n eine Zweierpotenz. Falls das Teehäferl zu Beginn auf einer ungeraden Position steht, so gibt Herr Ganzgenau eine Sekunde ein, womit unabhängig von der Drehrichtung das Teehäferl danach jedenfalls auf einer geraden Position steht. (Steht das Teehäferl bereits auf einer geraden Position, so überspringt er diesen Schritt.)

Steht das Teehäferl nun bei einer Position, die durch 2, aber nicht durch 4 teilbar ist, so gibt er 2 ein, andernfalls überspringt er den Schritt wieder.

Somit kann er erzwingen, dass nach spätestens ℓ Schritten das Teehäferl jedenfalls bei einer durch 2^ℓ teilbaren Position steht (indem er im ℓ-ten Schritt entweder $2^{\ell-1}$ eingibt oder nichts tut, je nachdem, ob die aktuelle Position bereits durch 2^ℓ teilbar ist oder nicht).

Sei nun n keine Zweierpotenz, d.h. n habe die Form $n = m \cdot 2^k$, wobei $m > 1$ eine passende ungerade ganze Zahl ist. Die Mikrowelle kann nun verhindern, dass die aktuelle Position jemals kongruent 0 modulo m wird. Dazu dreht sie das Teehäferl zu Beginn auf die Position 1 (oder eine beliebige andere nicht durch m teilbare Position).

Danach hat sie in jedem Zug die Wahl, das Teehäferl von der aktuellen Position a entweder auf $a+b$ oder auf $a-b$ modulo n zu drehen (wobei b die von Herrn Ganzgenau eingegebene Sekundenanzahl ist). Nehmen wir an, diese wären beide durch m teilbar, dann wäre auch ihre Differenz $2b$ durch m teilbar. Da m ungerade ist, ist damit b durch m teilbar. Dann wäre aber auch $(a-b)+b = a$ durch m teilbar, im Widerspruch dazu, dass zu Beginn des Zuges das Teehäferl auf einer nicht durch m teilbaren Position gestanden ist. Daher hat die Mikrowelle in jedem Zug mindestens eine Möglichkeit zur Auswahl, die wieder nicht durch m teilbar ist (und somit insbesondere nicht die Zahl n selbst ist).

(Birgit Vera Schmidt) □

Aufgabe 3. *Man bestimme alle Tripel (a, b, c) natürlicher Zahlen a, b und c, für die*

$$a^{b+20}(c-1) = c^{b+21} - 1$$

erfüllt ist.

(Walther Janous)

Antwort. $\{(1, b, 0) : b \in \mathbb{N}\} \cup \{(a, b, 1) : a, b \in \mathbb{N}\}$

Lösung 1. Man erkennt zunächst, dass die rechte Seite faktorisiert:

$$a^{b+20}(c-1) = (c^{b+20} + c^{b+19} + \cdots + c + 1)(c-1).$$

Der Fall $c = 1$ ist jedenfalls extra (und sehr einfach) zu behandeln. Für $c \neq 1$ vereinfacht sich die Gleichung zu

$$a^{b+20} = c^{b+20} + c^{b+19} + \cdots + c + 1.$$

Wir unterscheiden daher die beiden Fälle für c.

- $c = 1$ führt (siehe oben) auf
$$0 = 0.$$
  Deshalb sind für a und b beliebige natürliche Zahlen Lösungen.

- Für $c \neq 1$ können wir (siehe oben) durch $c-1$ dividieren und erhalten die äquivalente Gleichung

  $$a^{b+20} = c^{b+20} + c^{b+19} + \cdots + c + 1.$$

  Offensichtlich gilt

  $$c^{b+20} + c^{b+19} + \cdots + c + 1 > c^{b+20}.$$

  Daher muss $a \geq c+1$ gelten. Wegen des binomischen Lehrsatzes gilt

  $$\begin{aligned} a^{b+20} &\geq (c+1)^{b+20} \\ &= c^{b+20} + \binom{b+20}{1} c^{b+19} + \cdots + \binom{b+20}{b+19} c + 1 \\ &\geq c^{b+20} + c^{b+19} + \cdots + c + 1 \\ &= a^{b+20}. \end{aligned}$$

  Beide auftretenden Ungleichungen müssen daher Gleichungen sein.

  Wir betrachten insbesondere die zweite Ungleichung. Wegen

  $$\binom{b+20}{1} = b + 20 > 1$$

  kann diese aber nur eine Gleichung sein, wenn $c = 0$ ist. Im Fall $c > 0$ ist die zweite Ungleichung strikt und führt daher zu einem Widerspruch, und es gibt keine Lösung.

  Im verbleibenden Fall $c = 0$ ist die resultierende Gleichung

  $$a^{b+20} = 1$$

  leicht zu lösen. Da a eine natürliche Zahl ist, muss $a = 1$ sein. (Dies folgt auch aus der notwendigen Beziehung $a = c + 1$.) Damit darf aber b eine beliebige natürliche Zahl sein.

Alternativ erkennt man direkt unter der Annahme $c > 0$, dass

$$\begin{aligned} c^{b+20} &< c^{b+20} + c^{b+19} + \cdots + c + 1 \\ &< c^{b+20} + \binom{b+20}{1} c^{b+19} + \cdots + \binom{b+20}{b+19} c + 1 \\ &= (c+1)^{b+20} \end{aligned}$$

gilt. Daher liegt a^{b+20} in diesem Fall strikt zwischen c^{b+20} und $(c+1)^{b+20}$, was für natürliche Zahlen unmöglich ist. (Der Fall $c = 0$ muss dann noch extra wie oben behandelt werden.)

(Michael Drmota) □

Lösung 2. Grobe Abschätzung der Größenordnungen lässt uns schnell vermuten, dass a größer als c sein muss, gleichzeitig aber nicht viel größer sein darf.

In beiden Fällen werden wir jeweils eine Abschätzung vornehmen, von der wir leicht sehen, dass sie für ausreichend große Zahlen gilt, und erst im Anschluss überlegen, ab wo sie zutrifft.

Damit wir sicher sein können, dass $(c-1)$ positiv ist, sind die Fälle $c = 0$ und $c = 1$ vorab schnell erledigt und führen auf die Lösungen $(1, b, 0)$ und $(a, b, 1)$ für a, $b \in \mathbb{N}$. Sei ab jetzt $c \geq 2$.

Fall 1: Nehmen wir an, es wäre $a \leq c$. Dann gilt

$$a^{b+20}(c-1) \leq c^{b+20}(c-1) = c^{b+21} - c^{b+20} < c^{b+21} - 1,$$

wobei die letzte Ungleichung wegen $c \geq 2$ gilt.

Fall 2: Sei nun $a \geq c + 1$.

Dann gilt

$$\begin{aligned} a^{b+20}(c-1) &\geq (c+1)^{b+20}(c-1) \\ &= (c+1)^{b+18}(c+1)^2(c-1) \\ &\geq (c+1)^{b+18}c^3 \\ &> c^{b+21}-1, \end{aligned}$$

wobei $(c+1)^2(c-1) \geq c^3 \iff c^2-c-1>0$ wegen $c \geq 2$ gilt.

(Birgit Vera Schmidt) □

Aufgabe 4. *Sei α eine reelle Zahl. Man bestimme alle Funktionen $f\colon \mathbb{R} \to \mathbb{R}$ mit*

$$f(f(x)+y) = f(x^2-y) + \alpha f(x)y$$

für alle x, $y \in \mathbb{R}$.

(Walther Janous)

Antwort. Die Lösungsfunktionen sind

- für $\alpha \neq 0$: $f(x)=0$, $x \in \mathbb{R}$
- für $\alpha = 4$ zusätzlich noch $f(x) = x^2$, $x \in \mathbb{R}$
- für $\alpha = 0$: $f(x) = -x^2$, $x \in \mathbb{R}$, oder $f(x) = c$, $x \in \mathbb{R}$, wobei c eine beliebige reelle Zahl ist

Lösung. Wir setzen zuerst die Argumente $f(x)+y$ und x^2-y gleich, was zu $y = (x^2 - f(x))/2$ führt.

Durch Einsetzen von $y = (x^2 - f(x))/2$ ergibt sich also

$$\alpha f(x)(x^2 - f(x)/2 = 0.$$

Diese Gleichung legt es nahe, die zwei Fälle $\alpha \neq 0$ bzw. $\alpha = 0$ zu unterscheiden.

(a) Im Fall von $\alpha \neq 0$ folgt sofort, dass für jede reelle Zahl x die Bedingung $f(x)=0$ oder $f(x)=x^2$ erfüllt sein muss, also jedenfalls $f(0)=0$.

- Man sieht, dass die Funktion $f(x)=0$, $x \in \mathbb{R}$, eine Lösung ist, und bestätigt dies durch eine Probe.
- Als nächstes überlegen wir, wie es sich mit der Funktion $f(x)=x^2$, $x \in \mathbb{R}$, verhält. Für sie lautet unsere Funktionalgleichung

  $$(x^2+y)^2 = (x^2-y)^2 + \alpha x^2 y \iff 2x^2y = -2x^2y + \alpha x^2 y \iff (\alpha-4)x^2y = 0.$$

  Die letzte Gleichung ist aber genau dann für alle reellen Zahlen x und y gültig, wenn $\alpha = 4$. Deshalb gibt es in diesem Fall die zusätzliche Lösung $f(x) = x^2$, $x \in \mathbb{R}$.
- Wir müssen nun noch untersuchen, ob es Zahlen x, $y \in \mathbb{R} \setminus \{0\}$ mit $f(y) = y^2$ and $f(x) = 0$ gibt. Angenommen, x und y wären zwei derartige Zahlen. Für sie folgt aus der Funktionalgleichung $f(y) = f(x^2-y)$. Wegen $f(y) = y^2 \neq 0$ gelten $f(x^2-y) \neq 0$ und damit $f(x^2-y) = (x^2-y)^2$. Deshalb ergibt sich

  $$y^2 = (x^2-y)^2 = x^4 - 2x^2y + y^2,$$

  d.h. $y = x^2/2$. Daraus folgt aber, dass y die *einzige* reelle Zahl mit $f(y) = y^2$ ist. (Denn für y_1 mit $y_1 \neq y$ und $f(y_1) = y_1^2$ würde wie zuerst $y_1 = x^2/2$, also $y_1 = y$, folgen.) Deshalb muss $f(z) = 0$ für alle $z \in \mathbb{R} \setminus \{y\}$ sein. Auf Grund der vorherigen Überlegungen würde sich daraus aber $y = z^2/2$ für alle $z \in \mathbb{R} \setminus \{y\}$ ergeben, ein offensichtlicher Widerspruch.

(b) Für $\alpha = 0$ lautet die Funktionalgleichung

$$f(f(x) + y) = f(x^2 - y). \tag{3}$$

- Weil jede konstante Funktion ersichtlich eine Lösung ist, untersuchen wir im Weiteren, ob es nichtkonstante Lösungsfunktionen gibt.
- Wenn man sich elementare algebraische Operationen vergegenwärtigt, errät man $f(x) = -x^2$, $x \in \mathbb{R}$, als Lösung und überprüft dies mit einer Probe.
- Wir nehmen nun an, es gäbe eine reelle Zahl a mit $f(a) = b \neq -a^2$ und daher $d = b + a^2 \neq 0$. Mit $x = a$ ergibt sich aus der Funktionalgleichung (3), dass $f(b + y) = f(a^2 - y)$ für alle $y \in \mathbb{R}$. Mit $y = z - b$ haben wir daher $f(z) = f(d - z)$ für alle $z \in \mathbb{R}$. Folglich erhalten wir (mit $x = z$ und $x = d - z$) aus der Funktionalgleichung (3), dass

$$f(z^2 - y) = f(f(z) + y) = f(f(d - y) + y) = f((d - z)^2 - y).$$

Es gilt demnach

$$f(z^2 - y) = f((d - z)^2 - y)$$

für alle reellen Zahlen y und z. Mit $y = z^2$ ergibt sich $f(0) = f(d^2 - 2dz)$ für alle $z \in \mathbb{R}$. Wegen $d \neq 0$ durchläuft das zweite Argument aber alle reellen Zahlen und f ist daher konstant.

(Theresia Eisenkölbl, Clemens Heuberger, Walther Janous) □

Aufgabe 5. *Sei $ABCD$ ein konvexes Sehnenviereck mit den Diagonalen AC und BD. Jeder der vier Eckpunkte wird an der Diagonale gespiegelt, auf der er nicht liegt.*

(a) Man untersuche, wann die vier so erhaltenen Punkte auf einer Geraden liegen und gebe eine möglichst einfache äquivalente Bedingung an das Sehnenviereck $ABCD$ dafür an.

(b) Man zeige, dass in allen anderen Fällen die vier so erhaltenen Punkte auf einem Kreis liegen.

(Theresia Eisenkölbl)

Lösung. (a) Wir bezeichnen die Punkte, die wir der Reihe nach durch die Spiegelungen von A, B, C und D erhalten mit A', B', C' bzw. D' und den Schnittpunkt der beiden Diagonalen mit S. Da bei der Spiegelung die Punkte A und C an derselben Geraden BD gespiegelt werden und der Punkte S unter derselben Spiegelung invariant ist, wird die ganze Gerade ASC an BD gespiegelt zu $A'SC'$. Analog wird BSD gespiegelt an AC zu $B'SD'$.

Wenn wir den kleineren Winkel zwischen den beiden Geraden mit φ bezeichnen, dann entspricht das einer Drehung der Geraden AC mit Zentrum S in Richtung BD um den Winkel 2φ sowie einer Drehung der Geraden BD mit Zentrum S in Richtung AC um den Winkel 2φ.

Somit ist der Winkel zwischen den beiden Geraden $A'SC'$ und $B'SD'$ der Winkel 3φ. Damit dieser Winkel ein Vielfaches von 180° ist, muss der ursprüngliche Winkel 0° oder 60° sein. Der erste Fall ist aber nicht möglich, da die Punkte eines Sehnenvierecks nicht auf einer Geraden liegen.

Die vier neuen Punkte liegen also genau dann auf einer Geraden, wenn die Diagonalen des gegebenen Sehnenvierecks einen Winkel von 60° einschließen.

(b) Da bei der Spiegelung nicht nur die Kollinearität von ASC und BSD erhalten bleibt, sondern auch die Lage von S jeweils zwischen den beiden Punkten und die Abstände zu den Punkten, ist es naheliegend, die Potenz von S bezüglich des Umkreises von $ABCD$ ins Spiel zu bringen.

Aufgrund der Spiegelungen gilt

$$SA = SA',\ SB = SB',\ SC = SC',\ SD = SD',$$

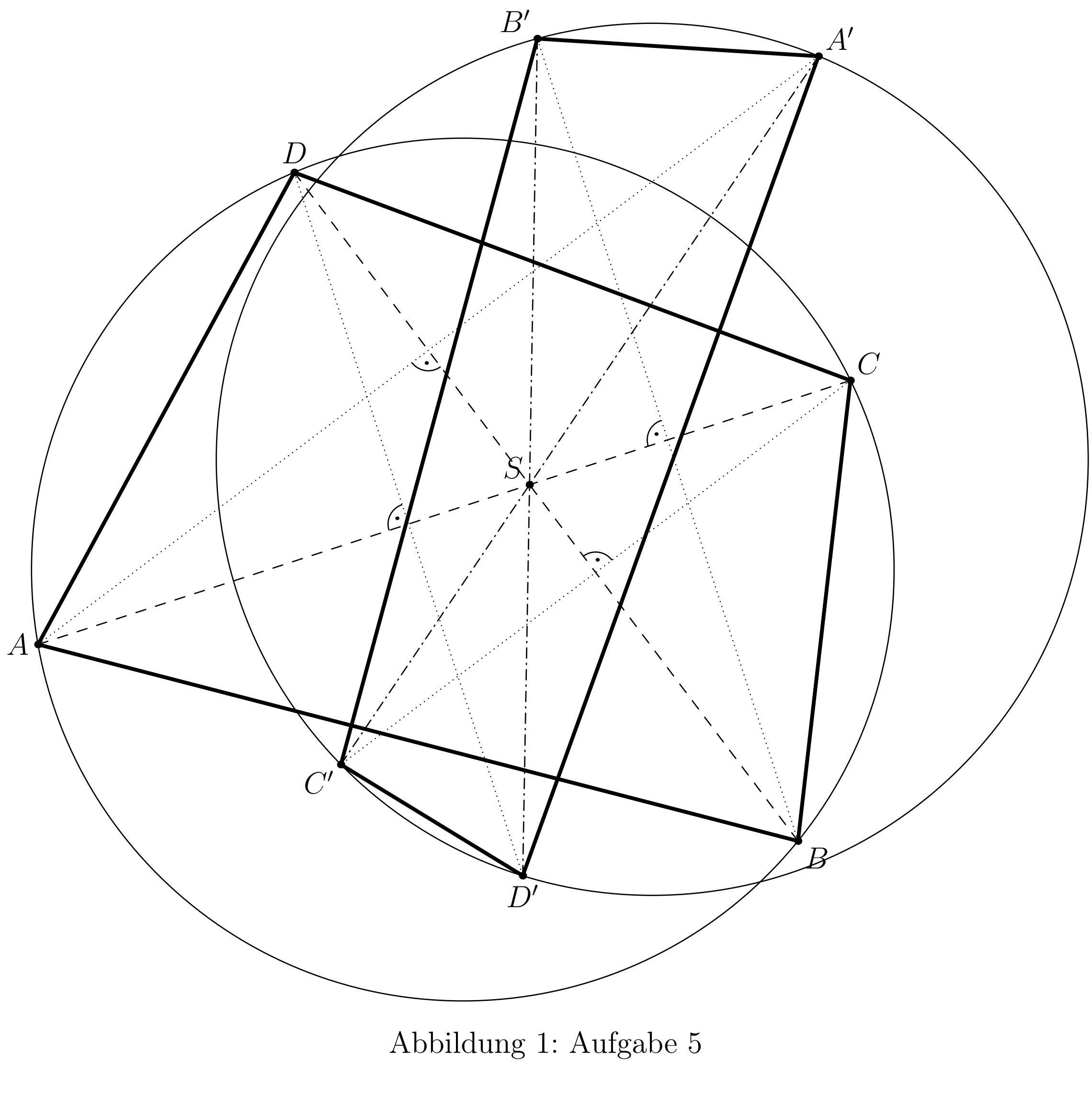

Abbildung 1: Aufgabe 5

und da $ABCD$ ein Sehnenviereck ist, gilt

$$SA \cdot SC = SB \cdot SD.$$

Damit erhalten wir

$$SA' \cdot SC' = SA \cdot SC = SB \cdot SD = SB' \cdot SD'.$$

Da die Geraden $A'SC'$ und $B'SD'$ nach Voraussetzung nicht zusammenfallen, gilt nach der Umkehrung des Satzes über die Potenz des Punktes S, dass die vier Punkte A', B', C' und D' auf einem gemeinsamen Kreis liegen.

(Theresia Eisenkölbl) $\square$

Aufgabe 6. *Seien p eine ungerade Primzahl und M eine Menge, die aus $\frac{p^2+1}{2}$ Quadratzahlen besteht.*

Man untersuche, ob sich aus dieser Menge p Elemente auswählen lassen, deren arithmetisches Mittel eine ganze Zahl ist.

(Walther Janous)

Antwort. Ja! In M können sogar (mit Hilfe eines Schubfachschlusses) p Elemente gefunden werden, die in derselben Restklasse modulo p liegen.

Lösung. Die Idee ist, unter den $\frac{p^2+1}{2}$ Quadratzahlen p Zahlen auszuwählen, die in derselben Restklasse modulo p sind. Klarerweise ist dann die Summe dieser p Zahlen durch p teilbar und damit das arithmetische Mittel eine ganze Zahl.

Bekanntermaßen durchlaufen die Quadratzahlen nicht alle Restklassen modulo p, sondern nur $1 + \frac{p-1}{2} = \frac{p+1}{2}$. (Dies ist einerseits die Restklasse 0, wenn man eine durch p teilbare Zahl quadriert. Wegen $a^2 \equiv (p-a)^2 \bmod p$ durchlaufen die Quadrate von Zahlen a, die nicht durch p teilbar sind, maximal die Hälfte der $p-1$ von Null verschiedenen Restklassen. Andererseits folgt aus $x^2 \equiv y^2 \bmod p$ die Beziehung $p \mid (x-y)(x+y)$ und damit $x \equiv y \bmod p$ oder $x \equiv -y \bmod p$. Daher durchlaufen die Quadrate von Zahlen a, die nicht durch p teilbar sind, genau die Hälfte der $p-1$ von Null verschiedenen Restklassen.)

Wir teilen nun die $\frac{p^2+1}{2}$ Quadratzahlen in die $\frac{p+1}{2}$ Restklassen auf, die für Quadratzahlen in Frage kommen. Wegen des Schubfachprinzips gibt es daher eine Restklasse, die wenigstens

$$\left\lceil \frac{(p^2+1)/2}{(p+1)/2} \right\rceil$$

dieser Zahlen enthält.

Wegen

$$\frac{(p^2+1)/2}{(p+1)/2} = \frac{p^2+1}{p+1} = \frac{p^2+p}{p+1} - \frac{p-1}{p+1} = p - \frac{p-1}{p+1}$$

und $0 < \frac{p-1}{p+1} < 1$ folgt

$$\left\lceil \frac{(p^2+1)/2}{(p+1)/2} \right\rceil = p,$$

was zu zeigen war.

(Michael Drmota) $\square$