# 52. Österreichische Mathematik-Olympiade

Kurs für Internationale „Mathematik macht Freu(n)de“ – Aufgabenblatt für den 17. Oktober 2020

## Ablauf

Dieses Aufgabenblatt wurde von Moritz Hiebler zusammengestellt.

Wir freuen uns auf deine Fragen und Lösungsvorschläge per E-Mail.

Am 13. Oktober 2020 wird das Blatt mit Tipps zur Lösung ausgewählter Aufgaben ergänzt. Moritz Hiebler bespricht die Aufgaben mit euch im virtuellen Olympiade-Kurs am 17. Oktober 2020 von 13:15–15:00 Uhr. Kurz darauf ergänzen wir das Blatt um ausgewählte Lösungsvorschläge und Angaben zu den Quellen der Aufgaben.

Schreibe uns, wenn du bei den virtuellen Kursen dabei sein möchtest. Du bist jederzeit willkommen!

# Ordnung

## Aufgaben

**Aufgabe 1.** Seien $a$ und $n$ positive ganze Zahlen mit $a \geq 2$. Zeige, dass $n \mid \varphi(a^n - 1)$.

**Aufgabe 2.** Bestimme die Anzahl der natürlichen Zahlen $N < 1\,000\,000 = 10^6$ mit folgender Eigenschaft: Es gibt einen ganzzahligen Exponenten $1 \leq k \leq 43$, sodass 2012 ein Teiler von $N^k - 1$ ist.

**Aufgabe 3.** Finde alle Tripel $(p, q, r)$ von Primzahlen, die

$$p \mid q^r + 1, \qquad q \mid r^p + 1, \qquad r \mid p^q + 1$$

erfüllen.

**Aufgabe 4.** Beweise, dass es zu jeder nichtnegativen ganzen Zahl $n$ eine Primzahl $p$ gibt, für welche die Dezimalbruchdarstellung von $1/p$ die Periodenlänge $2^n$ hat.

**Aufgabe 5.** Seien $k$ eine positive ganze Zahl und $p > 5$ eine Primzahl, sodass die Dezimalbruchdarstellung von $1/p$ Periodenlänge $2k$ besitzt. Seien $A$ und $B$ jene Zahlen im Dezimalsystem, die aus den Ziffern an den Nachkommastellen 1 bis $k$ bzw. $k + 1$ bis $2k$ gebildet werden. Beweise, dass $A + B$ im Dezimalsystem aus $k$ Neunern besteht.

**Aufgabe 6.** Zeige, dass $2^n - 1$ für keine ganze Zahl $n > 1$ durch $n$ teilbar ist.

**Aufgabe 7.** Beweise, dass $n \mid 2^n + 1$ für unendlich viele positive ganze Zahlen $n$ gilt.

**Aufgabe 8.** Zeige, dass $2^{n-1} + 1$ für keine ganze Zahl $n > 1$ durch $n$ teilbar ist.

## Tipps zu ausgewählten Aufgaben

**Aufgabe 1.** Was ist $\operatorname{ord}_{a^n-1}(a)$?

**Aufgabe 2.** Zeige erst $\operatorname{ord}_{2012}(N) \leq 2$.

**Aufgabe 3.** Wähle $p$ minimal und berechne $\operatorname{ord}_r(p)$.

**Aufgabe 4.** Beweise zunächst, dass besagte Periodenlänge gleich $\operatorname{ord}_p(10)$ ist.

**Aufgabe 5.** Zeige $10^k - 1 \mid 10^k A + B$ und schließe mit Größenabschätzungen.

**Aufgabe 6.** Berechne $\operatorname{ord}_p(2)$ für den kleinsten Primteiler $p$ von $n$.

**Aufgabe 7.** Verwende das LTE-Lemma.

**Aufgabe 8.** Betrachte $\mathrm{v}_2(n-1)$ und $\operatorname{ord}_p(2)$ für alle Primteiler $p$ von $n$.

# Lösungsvorschläge zu ausgewählten Aufgaben

Lösungsvorschläge von Moritz Hiebler, bearbeitet vom MmF-Team

**Aufgabe 1.**

Offenbar gilt $a^n \equiv 1 \pmod{a^n - 1}$. Für ganzzahlige $0 < j < n$ erhalten wir außerdem aus $1 < a^j < a^n$, also $0 < a^j - 1 < a^n - 1$, sofort $a^n - 1 \nmid a^j - 1$, d. h. $a^j \not\equiv 1 \pmod{a^n - 1}$. Darum ist $\operatorname{ord}_{a^n-1}(a) = n$, woraus nach den Eigenschaften der Ordnung $n = \operatorname{ord}_{a^n-1}(a) \mid \varphi(a^n - 1)$ folgt.

**Aufgabe 2.**

Erfüllt ein $N \in \mathbb{Z}$ diese Bedingungen, so ist $N$ notwendig teilerfremd zu 2012 und $\operatorname{ord}_{2012}(N)$ sowohl ein Teiler von $k \leq 43$ als auch von $\lambda(2012) = \operatorname{kgV}(\lambda(4), \lambda(503)) = \operatorname{kgV}(2, 502) = 502$. Da aber $502 = 2 \cdot 251$ nur 1 und 2 als positive Teiler kleiner oder gleich 43 besitzt, muss $\operatorname{ord}_{2012}(N) \mid 2$ und daher jedenfalls $N^2 \equiv 1 \pmod{2012}$, d. h. $2012 \mid N^2 - 1$, erfüllen. Folglich ist $N$ ungerade und 503 ein Teiler von $N^2 - 1 = (N-1)(N+1)$, also entweder ein Teiler von $N - 1$ oder von $N + 1$. Wir schließen $N = 503n \pm 1$ für ein $n \in \mathbb{Z}$ und, damit $N$ ungerade ist, $n = 2m$ für ein $m \in \mathbb{Z}$.
Umgekehrt gilt für jedes $N = 1006m \pm 1$, $m \in \mathbb{Z}$ neben $N^2 \equiv 1 \pmod 4$ entweder $503 \mid N + 1$ oder $503 \mid N - 1$, womit 2012 die Zahl $N^2 - 1$ teilt.
Es bleiben daher nur die natürlichen Zahlen kleiner als $10^6$ der Form $1006m \pm 1$ mit $m \in \mathbb{Z}$ zu zählen, und davon gibt es wegen $10^6 = 994 \cdot 1006 + 36$ genau $2 \cdot 994 + 1 = 1989$ Stück (zwei Nachbarn von jedem positiven Vielfachen von 1006 kleiner als $10^6$ sowie die Zahl 1 als einziger „natürlicher“ Nachbar der Zahl $0 \cdot 1006 = 0$).

**Aufgabe 3.**

Aufgrund von $p \nmid q^r$, $q \nmid r^p$ und $r \nmid p^q$ müssen die Primzahlen paarweise verschieden sein. Da weiters die Bedingungen bei zyklischer Vertauschung von $(p, q, r)$ gleich bleiben, dürfen wir o. B. d. A. annehmen, dass $p$ die kleinste der drei Primzahlen ist. Aus $r \mid p^q - 1$, also $p^q \equiv -1 \pmod r$, erhalten wir durch Quadrieren $p^{2q} \equiv 1 \pmod r$ und folglich $\operatorname{ord}_r(p) \mid 2q$, womit für $\operatorname{ord}_r(p)$ nur 1, 2, $q$ oder $2q$ (als positive Teiler von $2q$) infrage kommen.
Bei $\operatorname{ord}_r(p) \in \{1, 2\}$ gilt $p^2 \equiv 1 \pmod r$, d. h. äquivalent $r \mid p^2 - 1 = (p-1)(p+1)$, und daher $r \mid p - 1$ oder $r \mid p + 1$. Jedenfalls muss $r \leq p + 1$ gelten, was wegen $p < r$ auf $r = p + 1$ und das wiederum aus Paritätsgründen auf $r = 3$, $p = 2$ führt. Folglich ist $q > 2$ ein Primteiler von $p^r + 1 = 3^2 + 1 = 10$, was $q = 5$ erzwingt. Man prüft leicht nach, dass (2, 5, 3) (und daher auch (3, 2, 5) und (5, 3, 2)) tatsächlich die gewünschten Bedingungen erfüllen.
Es bleibt noch $\operatorname{ord}_r(p) \in \{q, 2q\}$ zu behandeln. In diesem Fall gilt jedoch $q \mid \operatorname{ord}_r(p) \mid \varphi(r) = r - 1$, somit $r \equiv 1 \pmod q$ und schließlich $0 \equiv r^p + 1 \equiv 1^p + 1 \equiv 2 \pmod q$ nach Voraussetzung, was wegen $q > p \geq 2$ unmöglich ist.

**Aufgabe 4.**

Zuerst bemerken wir, dass die Zahl $1/p$ genau dann rein-periodisch mit Periodenlänge $\ell$ ist, wenn

$$\frac{1}{p} = 0.\, a_1 a_2 \cdots \qquad \text{und} \qquad 10^\ell \cdot \frac{1}{p} = a_1 a_2 \cdots a_\ell .\, a_{\ell+1} a_{\ell+2} \cdots \tag{1}$$

(im Dezimalsystem, also $0 \leq a_n < 10$ für alle $n \in \mathbb{Z}_{>0}$) die gleichen Nachkommastellen besitzen und $\ell$ die kleinste Zahl mit dieser Eigenschaft ist. Gleichung (1) kann man aber auch als $10^\ell/p - 1/p \in \mathbb{Z}$

oder $p \mid 10^\ell - 1$ oder $10^\ell \equiv 1 \pmod{p}$ schreiben. Definitionsgemäß gilt somit $\ell = \operatorname{ord}_p(10)$ (und diese existiert wegen $p > 5$).
Nach dieser Vorüberlegung ist zu beweisen, dass zu jedem ganzen $n \geq 0$ eine Primzahl $p$ mit $\operatorname{ord}_p(10) = 2^n$ existiert. Bei $n = 0$ erfüllt $p = 3$ diese Eigenschaft. Von nun an sei $n > 0$. Wir suchen zuerst Primzahlen $p$ mit $10^{2^n} \equiv 1 \pmod{p}$. Für diese ergibt sich $\operatorname{ord}_p(10) \mid 2^n$ und daraus $\operatorname{ord}_p(10) = 2^a$ für ein ganzes $0 \leq a \leq n$. Bei $a = n$ haben wir eine passende Primzahl gefunden, und sonst gilt $a \leq n-1$, was $\operatorname{ord}_p(10) = 2^a \mid 2^{n-1}$ sowie $10^{2^{n-1}} \equiv 1 \pmod{p}$ erzwingt.
Wenn also $10^{2^{n-1}} \equiv -1 \pmod{p}$ für eine Primzahl $p$ gilt, muss $p$ notwendigerweise ungerade sein und somit führt $a \leq n-1$ auf den Widerspruch $1 \not\equiv -1 \pmod{p}$. Nachdem die besagte Kongruenz gleichwertig mit $p \mid 10^{2^{n-1}} + 1$ ist, wählen wir schließlich $p$ als einen beliebigen Primteiler der Zahl $10^{2^{n-1}} + 1$.

**Aufgabe 5.**

Laut Voraussetzung gilt

$$\frac{1}{p} = 0.\overline{AB} \qquad \text{und} \qquad 10^{2k} \cdot \frac{1}{p} = AB.\overline{AB}$$

im Dezimalsystem. Daraus erhalten wir $10^{2k}/p - 1/p = 10^k A + B$ oder äquivalent $(10^k - 1)(10^k + 1) = 10^{2k} - 1 = p(10^k A + B)$. Folglich ist $p$ ein Teiler von $10^k - 1$ oder von $10^k + 1$. Wäre aber $p$ ein Teiler von $10^k - 1$, so hätten schon $10^k \cdot 1/p$ und $1/p$ die gleichen Nachkommastellen und es folgte $A = B$, im Widerspruch zur Minimalität der Periodenlänge.[1] Wir schließen

$$\frac{10^k + 1}{p} = \frac{10^k A + B}{10^k - 1} \in \mathbb{Z} \qquad \Longrightarrow \qquad 0 \equiv 10^k A + B \equiv 1 \cdot A + B \pmod{10^k - 1}.$$

Folglich teilt $10^k - 1$ auch die Zahl $A + B$. Da $A$ und $B$ verschieden sowie höchstens $k$-stellig sind, ergibt sich $0 < A + B < 2 \cdot (10^k - 1)$. Daher kommt nur $A + B = 10^k - 1$ in Frage und das ist die Zahl $9 \cdots 9$ aus $k$ Neunern.

**Aufgabe 6.**

Nehmen wir an, $n \mid 2^n - 1$ gilt für eine ganze Zahl $n > 1$. Für den kleinsten Primteiler $p$ von $n$ folgt dann $2^n \equiv 1 \pmod{p}$, also ist $p$ ungerade und es gilt $\operatorname{ord}_p(2) \mid n$. Außerdem muss aber $\operatorname{ord}_p(2)$ ein Teiler von $\varphi(p) = p - 1$ und damit kleiner als $p$, der kleinste echte positive Teiler von $n$, sein. Das liefert $\operatorname{ord}_p(2) = 1$ sowie $p \mid 2^1 - 1 = 1$, einen Widerspruch.

**Aufgabe 7.**

Nach kurzem Probieren mit kleinen Werten von $n$ gewinnen wir die Vermutung, dass alle Dreierpotenzen die Aussage erfüllen. Nun ist aber $3^k \mid 2^{3^k} + 1$ äquivalent zu $\mathrm{v}_3(2^{3^k} + 1) \geq k$ für alle positiven ganzen Zahlen $k$. Wegen $2 \equiv -1 \not\equiv 0 \pmod{3}$ erhalten wir aus der additiven Form des LTE-Lemmas für die ungerade Potenz $n = 3^k$

$$\mathrm{v}_3\left(2^{3^k} + 1\right) = \mathrm{v}_3(2+1) + \mathrm{v}_3\left(3^k\right) = 1 + k \geq k$$

für alle positiven ganzen Zahlen $k$.

[1] Mit der Feststellung am Beginn der Lösung von Aufgabe 4 kann man auch aus $\operatorname{ord}_p(10) = 2k$ erkennen, dass $10^k \not\equiv 1 \pmod{p}$.

**Aufgabe 8.**

Wir nehmen an, für ein $n > 1$ gilt $n \mid 2^{n-1} + 1$. Für jeden Primteiler $p$ von $n$ bedeutet das $2^{n-1} \equiv -1 \pmod p$ und folglich $2^{2(n-1)} \equiv 1 \pmod p$. Daher ist $p$ ungerade, $\operatorname{ord}_p(2) \mid 2(n-1)$, aber $\operatorname{ord}_p(2) \nmid n-1$ (sonst wäre $1 \equiv -1 \pmod p$ und $p = 2$). Da sich aber die Primfaktorzerlegungen von $n-1$ und $2(n-1)$ nur um einen Faktor 2 unterscheiden, muss $\operatorname{ord}_p(2)$ gleich viele Zweier wie $2(n-1)$ enthalten, und zwar um einen mehr als $n-1$. Mit $e := \mathrm{v}_2(n-1)$ lässt sich demnach $2^{e+1} \mid \operatorname{ord}_p(2) \mid \varphi(p) = p-1$ oder äquivalent $p \equiv 1 \pmod{2^{e+1}}$ folgern. Durch Multiplikation aller Primteiler von $n$ (in entsprechender Vielfachheit) erhalten wir $n \equiv 1 \pmod{2^{e+1}}$, also den Widerspruch $e + 1 \leq \mathrm{v}_2(n-1) = e$.

# Quellenangaben zu den Aufgaben

**Aufgabe 1.**

aus [4], §17, Aufgabe 11. Lösungsvorschlag von Moritz Hiebler, überarbeitet vom MmF-Team.

**Aufgabe 2.**

aus [3], *Österreichische Mathematik-Olympiade 2012*, Aufgabe 5 von Gerd Baron. Lösungsvorschlag von Moritz Hiebler, überarbeitet vom MmF-Team.

**Aufgabe 3.**

aus [1], *USA Team Selection Test 2003*, Tag 1, Aufgabe 3 von Reid Barton. Übersetzung und Lösungsvorschlag von Moritz Hiebler, überarbeitet vom MmF-Team.

**Aufgabe 4.**

aus [2], Kapitel 3.3, Aufgabe 239 c). Lösungsvorschlag von Moritz Hiebler, überarbeitet vom MmF-Team.

**Aufgabe 5.**

aus [2], Kapitel 3.3, Aufgabe 241 b). Lösungsvorschlag von Moritz Hiebler, überarbeitet vom MmF-Team.

**Aufgabe 6.**

aus [5], Aufgabe 20. Übersetzung und Lösungsvorschlag von Moritz Hiebler, überarbeitet vom MmF-Team.

**Aufgabe 7.**

aus [5], Aufgabe 20a. Übersetzung und Lösungsvorschlag von Moritz Hiebler, überarbeitet vom MmF-Team.

**Aufgabe 8.**

aus [1], Aufgabe 7.1.17. Übersetzung und Lösungsvorschlag von Moritz Hiebler, überarbeitet vom MmF-Team.

# Literatur

[1] T. Andreescu and D. Andrica. *Number Theory: Structures, Examples, and Problems*. Birkhäuser, 2009.

[2] A. Bartholomé, J. Rung, and H. Kern. *Zahlentheorie für Einsteiger*. Vieweg+Teubner, 7th edition, 2010.

[3] Gerd Baron et al. *Österreichische Mathematik-Olympiaden 2009–2018: Aufgaben und Lösungen*. Nova MD, 2019.

[4] G. Scheja and U. Storch. *Lehrbuch der Algebra*, volume 1. B. G. Teubner Stuttgart, 2nd edition, 1994.

[5] W. Sierpiński. *250 Problems in Elementary Number Theory*. American Elsevier Pub. Co, 1970.