



Zahlentheorie

Thomas Huber

1. November 2008

Inhaltsverzeichnis

1 Grundlagen	2
1.1 Teilbarkeit	2
1.2 ggT und kgV	4
1.3 Abschätzungen	8
2 Kongruenzen	11
2.1 Definitionen	11
2.2 Die φ -Funktion und der Satz von Euler-Fermat	14
2.3 Der Chinesische Restsatz	17
2.4 Quadratische Reste und höhere Potenzen.	18
3 Faktorisierungen	20
4 Ziffern und Zahlssysteme	24
4.1 Zahlen und ihre Ziffern	24
4.2 Darstellung einer Zahl in Basis b	26
5 Varia	28
5.1 Die Gaussklammer	28
6 IMO Aufgaben	31

1 Grundlagen

1.1 Teilbarkeit

Im Folgenden sind a und b ganze Zahlen. Gibt es ein $k \in \mathbb{Z}$ mit $a = kb$, dann sagt man, a sei durch b *teilbar* oder b sei ein *Teiler* von a . In Zeichen: $b|a$. Jede ganze Zahl n ist durch ± 1 und $\pm n$ teilbar und jede ganze Zahl ist ein Teiler von 0. Ist $a > 0$, dann hat sich eingebürgert, dass man unter den *Teilern* von a nur die positiven Teiler versteht. $p \in \mathbb{N}$ heisst *prim* oder *Primzahl*, wenn p und 1 die einzigen Teiler von p sind.

Es gelten die folgenden einfachen aber wichtigen Fakten:

- $a|b$ und $b|c \implies a|c$
- $a|b_1, \dots, a|b_n$, dann gilt für beliebige ganze Zahlen c_1, \dots, c_n

$$a \mid \sum_{i=1}^n b_i c_i.$$

- $a|b$ und $c|d \implies ac|bd$
- p prim und $p|ab \implies p|a$ oder $p|b$
- $a \in \mathbb{N}, b \in \mathbb{Z}$ und $a|b \implies b = 0$ oder $a \leq |b|$

Beispiel 1. *Finde alle natürlichen Zahlen x, y mit*

$$x^2 - y! = 2001.$$

Lösung. 2001 ist durch 3 teilbar aber nicht durch 9. Ist $y \geq 3$, dann ist $y!$ durch 3 teilbar, also auch x . Dann ist x^2 aber sogar durch 9 teilbar. Für $y \geq 6$ ist auch $y!$ durch 9 teilbar, also müsste dies auch für 2001 gelten, was nicht der Fall ist. Es bleiben die Möglichkeiten $y = 1, 2, 3, 4, 5$, durchtesten dieser Fälle liefert die einzige Lösung $(x, y) = (45, 4)$. □

Bekanntlich kann man ganze Zahlen stets mit Rest teilen. Genauer lautet diese Aussage wie folgt:

Satz 1.1 (Division mit Rest). *Seien a, b ganze Zahlen mit $b > 0$. Dann existieren eindeutig bestimmte ganze Zahlen q und r mit $0 \leq r < b$, sodass gilt*

$$a = qb + r, \tag{1}$$

r heisst Rest der Division und es ist $r = 0$ genau dann, wenn $b|a$.

Einer der zentralen Punkte der ganzen Zahlentheorie ist die Tatsache, dass jede natürliche Zahl eindeutig als Produkt von Primzahlen geschrieben werden kann:

Theorem 1.2 (Primfaktorzerlegung). *Zu jeder natürlichen Zahl a existieren verschiedene Primzahlen p_1, p_2, \dots, p_r und natürliche Zahlen n_1, n_2, \dots, n_r mit*

$$a = p_1^{n_1} p_2^{n_2} \cdots p_r^{n_r}.$$

Die p_i und die n_i sind durch a eindeutig bestimmt.

Man beweist diesen Satz induktiv mit Hilfe der Division mit Rest, wir gehen aber nicht darauf ein. Der Fall $a = 1$ entspricht dem leeren Produkt auf der rechten Seite, d.h. es gibt überhaupt keine Primfaktoren und es gilt $r = 0$. Dieser Satz hat viele wichtige Konsequenzen, wir erwähnen hier zwei davon. Sei $a = p_1^{n_1} p_2^{n_2} \cdots p_r^{n_r}$ die Primfaktorzerlegung der natürlichen Zahl a , dann gilt:

- a besitzt genau $(n_1 + 1)(n_2 + 1) \cdots (n_r + 1)$ verschiedene positive Teiler.
- a ist genau dann eine m -te Potenz einer natürlichen Zahl, wenn alle Exponenten n_k durch m teilbar sind.

Als weitere Anwendung bringen wir noch ein klassisches Resultat, das auf EUKLID zurückgeht:

Satz 1.3. *Es gibt unendlich viele Primzahlen.*

Beweis. Nehme an, es gäbe nur endlich viele Primzahlen p_1, p_2, \dots, p_n und betrachte die Zahl $N = p_1 p_2 \cdots p_n + 1$. Wegen $N > 1$ gibt es nach Theorem 1.2 einen Primteiler q von N . Nun ist N aber durch keine der Primzahlen p_k teilbar, denn sonst würde $p_k \mid 1$ folgen, was absurd ist. Also ist q verschieden von p_1, p_2, \dots, p_n , im Widerspruch zur Annahme. □

Aufgaben:

1. Finde alle natürlichen Zahlen n mit $n + 1 \mid n^2 + 1$.
2. Seien $a \neq c$ zwei ganze Zahlen. Gilt $a - c \mid ab + cd$, dann auch $a - c \mid ad + bc$.
3. Zu jeder natürlichen Zahl n gibt es n aufeinanderfolgende natürliche Zahlen, von denen keine prim ist.
4. Zeige, dass es unendlich viele natürliche Zahlen n gibt, sodass $2n$ ein Quadrat, $3n$ eine dritte Potenz und $5n$ eine fünfte Potenz ist.
5. (CH 04) Finde alle natürlichen Zahlen a, b und n , sodass die folgende Gleichung gilt:

$$a! + b! = 2^n$$

6. Seien a, b, c natürliche Zahlen mit $a \mid b^2, b \mid c^2, c \mid a^2$. Zeige

$$abc \mid a^7 + b^7 + c^7.$$

7. (CH 06) Finde alle Tripel (p, q, r) von Primzahlen, sodass auch die drei Differenzen $|p - q|$, $|q - r|$ und $|r - p|$ alle Primzahlen sind.
8. Bestimme alle natürlichen Zahlen d , für die eine natürliche Zahl n existiert, sodass d ein Teiler ist von $n^2 + 1$ und von $(n + 1)^2 + 1$.
9. (CH 04) Bestimme alle natürlichen Zahlen n mit genau 100 verschiedenen positiven Teilern, sodass mindestens 10 dieser Teiler aufeinanderfolgende Zahlen sind.
10. Sind $a, b > 0$ und gilt $a \mid b^2, b^2 \mid a^3, a^3 \mid b^4, b^4 \mid a^5 \dots$, dann ist $a = b$.
11. (CH 99) Es seien m und n zwei positive ganze Zahlen, sodass $m^2 + n^2 - m$ durch $2mn$ teilbar ist. Zeige, dass m eine Quadratzahl ist.

12. (CH 08) Finde alle natürlichen Zahlen n , sodass die Anzahl positiver Teiler von n gleich dem drittkleinsten positiven Teiler von n ist.
13. (IMO 70) Finde alle natürlichen Zahlen n , für die sich die Menge $\{n, n+1, n+2, n+3, n+4, n+5\}$ in zwei Teilmengen zerlegen lässt, sodass das Produkt der Zahlen in beiden Teilmengen dasselbe ist.
14. (IMO 89) Zu jedem n gibt es n aufeinanderfolgende Zahlen, von denen keine eine Primzahlpotenz ist.

1.2 ggT und kgV

Für zwei ganze Zahlen a, b bezeichnet $\text{ggT}(a, b)$ den *grössten gemeinsamen Teiler* von a und b , mit anderen Worten die grösste positive Zahl, die ein Teiler von a und ein Teiler von b ist. $\text{kgV}(a, b)$ bezeichnet das *kleinste gemeinsame Vielfache*, also die kleinste positive Zahl, die a und b als Teiler besitzt. Analog definiert man den ggT und das kgV von mehr als zwei Zahlen und verwendet die abkürzende Notation (a_1, a_2, \dots, a_n) und $[a_1, a_2, \dots, a_n]$ für den ggT bzw. das kgV. Formal kann man den ggT wie folgt charakterisieren:

Es ist äquivalent:

- 1) $c = \text{ggT}(a, b)$
- 2) $c > 0$ ist ein Teiler von a und b und für jede positive Zahl x gilt $x \mid a, x \mid b \implies x \mid c$.

Analoges gilt für das kgV. Ist $\text{ggT}(a, b) = 1$, dann heissen a und b *teilerfremd*. Es gelten die folgenden Fakten:

- $\text{ggT}(a, b) = \text{ggT}(b, a)$
- $\text{ggT}(a, b, c) = \text{ggT}(\text{ggT}(a, b), c)$
- $c \mid ab$ und $\text{ggT}(a, c) = 1 \implies c \mid b$
- $a \mid c, b \mid c$ und $\text{ggT}(a, b) = 1 \implies ab \mid c$
- Ist $d = \text{ggT}(a, b)$, dann existieren *teilerfremde* ganze Zahlen x und y mit $a = xd$ und $b = yd$. Ausserdem ist dann $\text{kgV}(a, b) = xyd$ (vgl. Satz 1.4).
- Sind a, b teilerfremde natürliche Zahlen, sodass ab eine m -te Potenz ist, dann sind a und b beide m -te Potenzen.

Unter Verwendung der Primfaktorzerlegung lassen sich ggT und kgV explizit angeben:

Satz 1.4. Seien $a = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_r^{\alpha_r}$ und $b = p_1^{\beta_1} p_2^{\beta_2} \dots p_r^{\beta_r}$ die Faktorisierungen von a und b mit verschiedenen Primzahlen p_k und Exponenten $\alpha_k, \beta_k \geq 0$, dann gilt

$$\begin{aligned} \text{ggT}(a, b) &= p_1^{\min\{\alpha_1, \beta_1\}} p_2^{\min\{\alpha_2, \beta_2\}} \dots p_r^{\min\{\alpha_r, \beta_r\}} \\ \text{kgV}(a, b) &= p_1^{\max\{\alpha_1, \beta_1\}} p_2^{\max\{\alpha_2, \beta_2\}} \dots p_r^{\max\{\alpha_r, \beta_r\}} \end{aligned}$$

Ausserdem folgt daraus mit Hilfe der Formel $\min\{x, y\} + \max\{x, y\} = x + y$ sofort

$$\text{ggT}(a, b) \cdot \text{kgV}(a, b) = ab.$$

Beispiel 2. (Russland 95) Seien m und n natürliche Zahlen mit

$$\text{ggT}(m, n) + \text{kgV}(m, n) = m + n.$$

Zeige, dass eine der beiden Zahlen durch die andere teilbar ist.

Lösung. Sei d der grösste gemeinsame Teiler von m und n . Schreibe $m = ad, n = bd$, dann gilt $\text{kgV}(m, n) = abd$ nach Satz 1.4. Die Gleichung wird zu $d + abd = ad + bd$ oder $d(ab - a - b + 1) = 0$. Faktorisieren der linken Seite gibt $d(a - 1)(b - 1) = 0$, also ist $a = 1$ oder $b = 1$. Im ersten Fall gilt $m = d$, also $m \mid n$, im zweiten Fall folgt analog $n \mid m$. □

Mit den Formeln in Satz 1.4 lässt sich der ggT im Prinzip immer berechnen. Das Problem dabei ist der enorme Aufwand, grosse Zahlen zu faktorisieren. Es gibt aber zum Glück ein einfaches und sehr effizientes Berechnungsverfahren, nämlich den *EUKLID'schen Algorithmus*, der auch vom theoretischen Standpunkt aus interessant ist. Grundlage dafür ist die Tatsache, dass für alle ganzen Zahlen a, b und n die folgende Gleichung gilt:

$$(a, b) = (a, b + na). \tag{2}$$

Beweis. Es genügt, dies für $n = \pm 1$ zu zeigen, der allgemeine Fall folgt dann durch wiederholte Anwendung. Ist c ein gemeinsamer Teiler von a und b , dann teilt c auch $b \pm a$, also gilt $(a, b) \mid (a, b \pm a)$. Sei umgekehrt c ein gemeinsamer Teiler von a und $b + a$ bzw. $b - a$, dann teilt c auch $(b + a) - a = b$ bzw. $(b - a) + a = b$. Daraus folgt $(a, b \pm a) \mid (a, b)$. □

Als Zahlenbeispiel berechnen wir damit $(2541, 1092)$, indem wir die Gleichung (2) solange anwenden, bis das Ergebnis klar ist:

$$\begin{aligned} (2541, 1092) &= (2541 - 2 \cdot 1092, 1092) = (357, 1092) \\ &= (1092 - 3 \cdot 357, 357) = (21, 357) \\ &= (357 - 17 \cdot 21, 21) = (0, 21) = 21. \end{aligned}$$

Die Idee ist offenbar, dass man mit dem Rest der Division der grösseren durch die kleinere Zahl weiterrechnet. Formalisiert wird das im

Algorithmus 1.5 (EUKLID). *Berechnung von (a, b) für $a, b \geq 0$.*

1. Setze $a_1 = \max\{a, b\}$ und $a_2 = \min\{a, b\}$ sowie $n = 2$.
2. Schreibe $a_{n-1} = q_n a_n + a_{n+1}$ mit $0 \leq a_{n+1} < a_n$ (Division mit Rest).
3. Ist $a_{n+1} = 0$, dann gilt $(a, b) = a_n$, sonst erhöhe n um 1 und gehe zu Schritt 2.

Die Richtigkeit dieses Algorithmus ergibt sich unmittelbar aus (2). Für unser Zahlenbeispiel sind dann also die folgenden Rechnungen anzustellen:

$$\begin{aligned} 2541 &= 2 \cdot 1092 + 357 \\ 1092 &= 3 \cdot 357 + 21 \\ 357 &= 17 \cdot 21 + 0. \end{aligned}$$

Weil die Division in der letzten Zeile aufgeht, gilt also $(2541, 1092) = 21$.

Satz 1.6 (BÉZOUT). Sind a, b teilerfremd, dann gibt es ganze Zahlen x, y mit

$$xa + yb = 1.$$

Allgemeiner: Ist $d = \text{ggT}(a, b)$, dann existieren ganze Zahlen x, y mit

$$xa + yb = d.$$

Beweis. Das folgt unmittelbar aus dem Euklidischen Algorithmus: Aus der vorletzten Zeile des Algorithmus erhält man die Gleichung $\text{ggT}(a, b) = a_n$. Setzt man diesen Ausdruck für a_n in die $(n-1)$ -te Zeile ein und iterativ die entstehenden Ausdrücke für a_k in die $(k-1)$ -te Zeile für immer kleinere k , dann folgt schliesslich eine Gleichung der Form $\text{ggT}(a, b) = xa + yb$. \square

In unserem Beispiel erhält man der Reihe nach

$$\begin{aligned} 21 &= 1 \cdot 1092 - 3 \cdot 357 \\ &= 1 \cdot 1092 - 3(2541 - 2 \cdot 1092) \\ &= (-3) \cdot 2541 + 7 \cdot 1092. \end{aligned}$$

Als Anwendung besprechen wir noch die lineare Diophant'sche Gleichung in zwei Variablen.

Satz 1.7. Seien a, b, c ganze Zahlen. Die Gleichung

$$ax + by = c$$

hat genau dann eine Lösung (x, y) mit $x, y \in \mathbb{Z}$, wenn $d = \text{ggT}(a, b) \mid c$. Ist dies der Fall und (x_0, y_0) eine Lösung, dann sind alle Lösungen gegeben durch

$$(x, y) = \left(x_0 + k \cdot \frac{b}{d}, y_0 - k \cdot \frac{a}{d} \right), \quad k \in \mathbb{Z}.$$

Beweis. Nehme an, (x, y) sei eine Lösung. Dann ist d ein Teiler der linken Seite, also auch von c . Ist umgekehrt $d \mid c$, dann folgt die Existenz einer Lösung (x_0, y_0) direkt aus dem Satz von Bézout. Sei (x, y) eine weitere Lösung, dann gilt $a(x - x_0) + b(y - y_0) = c - c = 0$, also

$$\frac{a}{d} \cdot (x - x_0) = -\frac{b}{d} \cdot (y - y_0).$$

Nun sind a/d und b/d teilerfremd, daher ist $(x - x_0)$ durch b/d teilbar und $(y - y_0)$ durch a/d . Daraus folgt unmittelbar, dass alle Lösungen von der angegebenen Gestalt sind. Einsetzen zeigt, dass es auch wirklich Lösungen sind. \square

Aufgaben

- (IMO 59) Zeige, dass für jedes natürliche n der folgende Bruch irreduzibel ist:

$$\frac{21n + 4}{14n + 3}$$

- Jede natürliche Zahl > 6 ist die Summe zweier teilerfremder natürlicher Zahlen > 1 .
- (CH 05) Seien m, n zwei teilerfremde natürliche Zahlen. Zeige, dass dann auch die beiden Zahlen $m^3 + mn + n^3$ und $mn(m + n)$ teilerfremd sind.

4. (Spanien 96) Seien a, b natürliche Zahlen, sodass

$$\frac{a+1}{b} + \frac{b+1}{a}$$

eine ganze Zahl ist. Zeige, dass der grösste gemeinsame Teiler von a und b nicht grösser als $\sqrt{a+b}$ ist.

5. (CH 01) Finde die zwei kleinsten natürlichen Zahlen n , sodass die Brüche

$$\frac{68}{n+70}, \frac{69}{n+71}, \frac{70}{n+72}, \dots, \frac{133}{n+135}$$

alle irreduzibel sind.

6. (Kanada 97) Bestimme die Anzahl Paare (x, y) positiver ganzer Zahlen mit $x \leq y$, die die folgenden Gleichungen erfüllen:

$$\text{ggT}(x, y) = 5! \quad \text{und} \quad \text{kgV}(x, y) = 50!$$

7. Seien a, b, c, d natürliche Zahlen mit $ab = cd$. Zeige, dass die Zahl $a^2 + b^2 + c^2 + d^2$ keine Primzahl ist.

8. (Russland 95) Für die Folge natürlicher Zahlen a_1, a_2, a_3, \dots gelte $\text{ggT}(a_i, a_j) = \text{ggT}(i, j)$ für alle $i \neq j$. Zeige, dass $a_i = i$ gilt für alle $i \geq 1$.

9. (Deutschland 96) Ein Stein startet bei $(1, 1)$ und bewegt sich auf der Koordinatenebene nach den folgenden Regeln:

(a) Vom Feld (a, b) aus kann der Stein auf $(2a, b)$ oder $(a, 2b)$ ziehen.

(b) Vom Feld (a, b) aus kann der Stein auf das Feld $(a-b, b)$ ziehen, falls $a > b$, oder auf das Feld $(a, b-a)$, falls $b > a$.

Für welche natürlichen Zahlen x, y kann der Stein auf das Feld (x, y) ziehen?

10. (CH 05) Bestimme alle nichtleeren Mengen M natürlicher Zahlen, sodass für je zwei (nicht notwendigerweise verschiedene) Elemente a, b aus M auch

$$\frac{a+b}{\text{ggT}(a, b)}$$

in M liegt.

11. (USA 72) Wie üblich bezeichnen (\dots) und $[\dots]$ den ggT und das kgV der eingeklammerten Zahlen. Zeige, dass für alle natürlichen Zahlen a, b, c gilt

$$\frac{[a, b, c]^2}{[a, b][b, c][c, a]} = \frac{(a, b, c)^2}{(a, b)(b, c)(c, a)}$$

12. (IMO 81) Für welche $n > 2$ gibt es eine Menge von n aufeinanderfolgende natürliche Zahlen, sodass die grösste dieser Zahlen ein Teiler ist des kleinsten gemeinsamen Vielfachen der übrigen $n-1$ Zahlen? Für welche n gibt es genau eine solche Menge?

13. (Japan 96) Seien m, n natürliche Zahlen mit $\text{ggT}(m, n) = 1$. Berechne

$$\text{ggT}(5^m + 7^m, 5^n + 7^n).$$

1.3 Abschätzungen

Ein sehr wichtiges Element beim Lösen von zahlentheoretischen Problemen ist das Abschätzen von bestimmten Grössen. Oft kann man dadurch alles auf ein paar wenige Fälle reduzieren, die dann einfach zu lösen sind, oder man kommt überhaupt erst weiter so. Es geht dabei darum, bei Gleichungen irgendwie das Wachstumsverhalten der involvierten Grössen gegeneinander abzuwägen. Was damit genau gemeint ist, sehen wir nun an einer Reihe recht verschiedener Beispiele.

Beispiel 3. *Finde alle natürlichen Zahlen n mit $n^2 + 11 \mid n^3 + 13$.*

Was hat das nun mit Abschätzungen zu tun? Schauen wir uns an:

Lösung. $n^2 + 11$ ist ein Teiler von $n^3 + 13$, also auch von $n(n^2 + 11) - (n^3 + 13) = 11n - 13$. Offenbar ist $n = 1$ keine Lösung, für $n \geq 2$ ist aber $11n - 13 > 0$ und da diese Zahl durch $n^2 + 11$ teilbar sein soll, muss gelten

$$n^2 + 11 \leq 11n - 13.$$

Hier ist nun also die Abschätzung. Da die linke Seite quadratisch in n ist, die rechte nur linear, kann diese Ungleichung nur für kleine Werte von n erfüllt sein. Sie ist äquivalent zu $n^2 - 11n + 24 = n(n - 11) + 24 \leq 0$. Für $n \geq 12$ gilt nun aber stets $n(n - 11) + 24 \geq 12 \cdot 1 + 24 > 0$, folglich ist $n \leq 11$. Durchtesten dieser Fälle ergibt die beiden Lösungen $n = 3$ und $n = 8$. □

Der entscheidende Punkt war hier die einfache Bemerkung, dass aus $a \mid b$ und $b > 0$ stets $|a| \leq b$ folgt. Dieses Prinzip ist oft anwendbar, auch bei einer ganzen Reihe von IMO Aufgaben. Merkt es euch!

Beispiel 4. *(England 95) Bestimme alle Lösungen in natürlichen Zahlen der Gleichung*

$$\left(1 + \frac{1}{a}\right) \left(1 + \frac{1}{b}\right) \left(1 + \frac{1}{c}\right) = 2.$$

Hier ist die rechte Seite konstant, die linke wird offenbar immer kleiner, wenn a, b und c grösser werden. Sind alle drei Variablen sehr gross, dann ist jeder der Faktoren rechts ungefähr gleich 1 und die Gleichung kann nicht erfüllt sein. Dies müssen wir nun präzisieren.

Lösung. Die Gleichung ist symmetrisch in a, b und c , wir können daher OBdA $a \geq b \geq c$ annehmen. Dann ist die linke Seite einerseits gleich 2, andererseits aber höchstens gleich $(1 + 1/c)^3$. Eine kurze Rechnung zeigt aber, dass $(1 + 1/c)^3 < 2$ gilt für $c \geq 4$, folglich ist $c \leq 3$. Wir unterscheiden nun drei Fälle:

$c = 1$: Wegen $(1 + 1/a) > 1$ und $(1 + 1/c) = 2$ ist die linke Seite grösser als 2, ein Widerspruch.

$c = 2$: Die Gleichung wird zu $(1 + 1/a)(1 + 1/b) = 4/3$ und ähnlich wie oben erhält man die Abschätzung $4/3 \leq (1 + 1/b)^2$, also $b \leq 6$. Wegen $(1 + 1/a) > 1$ ist ausserdem $b \geq 4$. Einsetzen der 3 möglichen Werte für b liefert die Lösungen $(7, 6, 2)$, $(9, 5, 2)$ und $(15, 4, 2)$.

$c = 3$: Die Gleichung wird zu $(1 + 1/a)(1 + 1/b) = 3/2$ und analog zu vorher erhält man $b \leq 4$ und $b \geq c = 3$. Einsetzen ergibt die Lösungen $(8, 3, 3)$ und $(5, 4, 3)$.

Insgesamt sind die Lösungen also alle symmetrischen Vertauschungen von

$$(7, 6, 2), (9, 5, 2), (15, 4, 2), (8, 3, 3), (5, 4, 3).$$

□

Durch mehrfaches Abschätzen haben wir der Reihe nach obere Schranken für c und b gefunden und mussten dann noch einige wenige Fälle durchprobieren. Mit Teilbarkeitsbetrachtungen allein hätte man diese Aufgabe wohl kaum gelöst.

Beispiel 5. Bestimme alle Lösungen in natürlichen Zahlen der Gleichung

$$abc = ab + bc + ca + 12.$$

Hier wächst die linke Seite offenbar stärker als die rechte, wenn a, b und c alle gross werden. Die linke ist vom Grad 3, die rechte nur vom Grad 2 + Störterm. Wie können wir das quantifizieren?

Lösung. OBdA sei $a \geq b \geq c$. Wie wir uns überlegt haben, muss c klein sein. In der Tat, für $c \geq 4$ erhalten wir sofort $abc \geq 4ab \geq ab + bc + ca + 4^2 > ab + bc + ca + 12$, Widerspruch. Also ist $c \leq 3$.

$c = 3$: $3ab = ab + 3a + 3b + 12 \Leftrightarrow ab + (a-3)(b-3) = 21$. Wegen $a \geq b \geq 3$ ist dann $ab \leq 21$ und für (a, b) kommen nur die Paare $(7, 3), (6, 3), (5, 3), (4, 3), (3, 3), (5, 4), (4, 4)$ in Frage. Durchtesten zeigt, dass davon nur das erste eine Lösung ist.

$c = 2$: $2ab = ab + 2a + 2b + 12 \Leftrightarrow (a-2)(b-2) = 16$. Wegen $a \geq b \geq 2$ erhalten wir die Lösungen $(a, b) = (18, 3), (10, 4), (6, 6)$.

$c = 1$: $ab = ab + a + b + 12 \Leftrightarrow a + b = -12$ hat keine positive Lösung.

Insgesamt sind die Lösungen (a, b, c) die symmetrischen Vertauschungen von

$$(18, 3, 2), (10, 4, 2), (6, 6, 2), (7, 3, 3).$$

□

Beispiel 6. Bestimme alle positiven ganzzahligen Lösungen von $x^3 - y^3 = xy + 61$.

Hier ist die linke Seite von der Ordnung 3, die rechte hat Ordnung 2, dennoch kann man offensichtlich die linke Seite auch für grosse x und y klein halten. Das Argument der letzten Aufgabe ist hier also nicht direkt anwendbar. Vielmehr ist entscheidend, wie gross die Differenz der beiden Zahlen ist. Mit ihr wächst die linke Seite stärker als die rechte.

Lösung. Um dies genauer zu ergründen, setzen wir $d = x - y$. Da die rechte Seite der Gleichung stets positiv ist, gilt $d > 0$. Einsetzen liefert $(y+d)^3 - y^3 = (y+d)y + 61 \Leftrightarrow (3d-1)y^2 + (3d^2-d)y + d^3 = 61$, insbesondere ist $d^3 \leq 61$, also $d \leq 3$, denn die beiden Klammern links sind nicht negativ. Für $d = 1$ erhalten wir die Gleichung $y^2 + y - 30 = 0$ mit der einzigen positiven Lösung $y = 5 \Rightarrow x = 6$. Für $d = 2, 3$ haben die entsprechenden Gleichungen keine ganzzahligen Lösungen. Das einzige Lösungspaar ist $(x, y) = (6, 5)$.

□

Eine weitere wichtige Tatsache ist, dass zwischen zwei *aufeinanderfolgenden* Quadraten (n -ten Potenzen, Zweierpotenzen etc.) keine weitere liegt. Damit kommt man z.B. oft dann weiter, wenn man Grössen hat, die in der Nähe einer Quadratzahl liegen und von denen man weiss, dass sie selbst eine sind.

Beispiel 7. (Deutschland 95) Finde alle Paare (x, y) nichtnegativer ganzer Zahlen, welche die folgende Gleichung erfüllen:

$$x^3 + 8x^2 - 6x + 8 = y^3.$$

Lösung. Hier kann man nicht viel Abschätzen, was das Wachstum betrifft. Die Idee ist die folgende: Die linke Seite muss ja eine dritte Potenz sein (nämlich y^3), liegt aber irgendwie auch nahe bei x^3 . Das wollen wir quantifizieren. Wir suchen also mal in der Nähe von x :

$$\begin{aligned}(x+2)^3 &= x^3 + 6x^2 + 12x + 8, \\(x+3)^3 &= x^3 + 9x^2 + 27x + 27.\end{aligned}$$

Betrachtet man jeweils den Koeffizient von x^2 , dann scheint das erste eher kleiner, das zweite eher grösser als die linke Seite unserer Gleichung zu sein. Rechnen wir es aus:

$$\begin{aligned}(x+2)^3 &< x^3 + 8x^2 - 6x + 8 \Leftrightarrow 2x^2 - 18x > 0 \Leftrightarrow x > 9, \\(x+3)^3 &> x^3 + 8x^2 - 6x + 8 \Leftrightarrow x^2 + 33x + 15 > 0 \quad \text{gilt für alle } x \geq 0.\end{aligned}$$

Für $x > 9$ liegt die linke Seite also zwischen zwei dritten Potenzen und muss selbst eine sein, Widerspruch. Daher ist $x \leq 9$ und durchtesten dieser Fälle liefert die beiden Lösungen $(0, 2)$ und $(9, 11)$. □

Aufgaben

1. Finde alle Tripel (x, y, z) natürlicher Zahlen mit

$$\frac{1}{x} + \frac{2}{y} - \frac{3}{z} = 1.$$

2. Zeige, dass die Gleichung

$$y^2 = x(x+1)(x+2)(x+3)$$

keine Lösung in positiven ganzen Zahlen besitzt.

3. (IMO 76) Finde die grösste Zahl, die sich als Produkt von natürlichen Zahlen mit Summe 1976 schreiben lässt.
4. (CH 06) Bestimme alle Lösungen in natürlichen Zahlen der Gleichung

$$\text{kgV}(a, b, c) = a + b + c.$$

5. (CH 07) Bestimme alle Paare (a, b) natürlicher Zahlen, sodass $a^2 + 3b$ und $b^2 + 3a$ beides Quadratzahlen sind.
6. (IMO 98) Bestimme alle Paare natürlicher Zahlen (a, b) , sodass $a^2b + a + b$ durch $ab^2 + b + 7$ teilbar ist.
7. (IMO 92) Man bestimme alle ganzen Zahlen a, b, c mit $1 < a < b < c$, sodass

$$\frac{abc - 1}{(a-1)(b-1)(c-1)}$$

eine ganze Zahl ist.

8. Sei n eine natürliche Zahl und $1 = d_1 < d_2 < \dots < d_k = n$, $k \geq 15$ seien die positiven Teiler von n . Es gelte

$$n = d_{13} + d_{14} + d_{15},$$

bestimme alle solchen n .

9. (CH 08) Finde alle Tripel (a, b, c) natürlicher Zahlen, sodass gilt:

$$a \mid bc - 1, \quad b \mid ca - 1, \quad c \mid ab - 1.$$

10. Finde alle ganzzahligen Lösungen der Gleichung

$$y^2 + y = x^4 + x^3 + x^2 + x.$$

11. (IMO 94) Bestimme alle geordneten Paare (m, n) natürlicher Zahlen, sodass der Bruch

$$\frac{n^3 + 1}{mn - 1}$$

eine ganze Zahl ist

2 Kongruenzen

2.1 Definitionen

Seien $a, b \in \mathbb{Z}$ und m eine natürliche Zahl. Ist m ein Teiler von $a - b$, dann sagen wir, a und b seien *kongruent modulo m* , in Zeichen

$$a \equiv b \pmod{m}.$$

Oft schreibt man auch einfach $a \equiv b (m)$. Sind a und b nicht kongruent, dann schreibt man $a \not\equiv b \pmod{m}$. Mit Hilfe der Division mit Rest,

$$\begin{aligned} a &= km + r, \\ b &= lm + s, \end{aligned}$$

folgt unmittelbar, dass a und b genau dann kongruent sind modulo m , wenn $r = s$ gilt. Insbesondere ist $a \equiv 0 (m)$ genau dann, wenn $m \mid a$. Bei der Kongruenzrechnung zählt also nur der Rest einer Zahl bei Division durch m . Man fasst nun alle Zahlen, die bei Division durch m denselben Rest lassen, zu einer Menge zusammen, einer sogenannten *Restklasse* modulo m . Es gibt also genau m verschiedene Restklassen modulo m , die zum Beispiel von den Zahlen $0, 1, \dots, m-1$ repräsentiert werden. Die Zahlen 17, -8 und 2 liegen zum Beispiel alle in derselben Restklasse modulo 5, jedoch in drei verschiedenen Restklassen modulo 7. Genau wie gewöhnliche Zahlen lassen sich auch Kongruenzen addieren und multiplizieren.

Satz 2.1. Seien a, b, c, d ganze Zahlen mit $a \equiv c$ und $b \equiv d (m)$, dann gilt

$$\begin{aligned} a \pm b &\equiv c \pm d \pmod{m}, \\ ab &\equiv cd \pmod{m}. \end{aligned}$$

Beweis. Nach Voraussetzung gibt es ganze Zahlen k, l mit $a - c = km, b - d = lm$. Daraus folgt nun

$$(a + b) - (c + d) = (a - c) + (b - d) = km + lm = (k + l)m,$$

nach Definition bedeutet dies aber $a + b \equiv c + d \pmod{m}$. Analog zeigt man $a - b \equiv c - d \pmod{m}$. Es gilt weiter

$$ab - cd = a(b - d) + d(a - c) = a(lm) + d(km) = (al + dk)m,$$

folglich $ab \equiv cd \pmod{m}$. □

Als direkte Konsequenz ergibt sich auch noch die folgende Rechenregel:

$$a \equiv b \pmod{m} \implies a^k \equiv b^k \pmod{m}, \quad k \geq 0.$$

Es sei aber schon hier ausdrücklich darauf hingewiesen, dass eine entsprechende Regel für die Exponenten **nicht** gilt:

$$k \equiv l \pmod{m} \not\Rightarrow a^k \equiv a^l \pmod{m}$$

Zum Beispiel ist $1 \equiv 4 \pmod{3}$, aber $2^1 \not\equiv 2^4 \pmod{3}$! Dieses Phänomen wird Gegenstand des nächsten Abschnitts sein.

Eine weitere Schwierigkeit ist die Division, die genau wie bei den gewöhnlichen ganzen Zahlen nicht uneingeschränkt zur Verfügung steht. Auch darauf kommen wir später zurück. An dieser Stelle fügen wir jedoch eine sehr wichtige Kürzungsregel an, die für die meisten praktischen Zwecke ausreichend ist.

Satz 2.2. *Ist c teilerfremd zu m , dann kann man Kongruenzen mit c kürzen:*

$$ca \equiv cb \pmod{m} \implies a \equiv b \pmod{m}.$$

Beweis. Nach Voraussetzung ist m ein Teiler von $ca - cb = c(a - b)$. Da m und c teilerfremd sind, gilt sogar $m \mid a - b$, also $a \equiv b$. □

Beispiel 8. *Aus jeder Menge von 5 ganzen Zahlen kann man immer 3 auswählen, deren Summe durch 3 teilbar ist.*

Lösung. Jede Zahl ist kongruent zu 0, 1 oder 2 modulo 3. Wir nehmen zuerst an, es gäbe drei Elemente a, b, c mit $a \equiv 0, b \equiv 1$ und $c \equiv 2 \pmod{3}$. Dann ist $a + b + c \equiv 0 + 1 + 2 \equiv 0 \pmod{3}$, deren Summe also durch 3 teilbar. Gibt es keine drei solchen Zahlen, dann sind nach dem Schubfachprinzip drei der fünf Zahlen kongruent modulo 3, deren Summe also durch 3 teilbar. □

Beispiel 9. *(England 2000) Zeige, dass für jede natürliche Zahl n*

$$121^n - 25^n + 1900^n - (-4)^n \tag{3}$$

durch 2000 teilbar ist.

Lösung. Wir zeigen, dass (2) durch 16 und durch 125 teilbar ist. Daraus folgt die Behauptung. Dazu berechnen wir den Ausdruck zuerst modulo 16. Es gilt $121 \equiv 25 \pmod{16}$, also auch $121^n \equiv 25^n \pmod{16}$. Ebenso ist $1900 \equiv -4 \pmod{16}$, also $1900^n \equiv (-4)^n \pmod{16}$. Insgesamt erhalten wir

$$(121^n - 25^n) + (1900^n - (-4)^n) \equiv 0 + 0 = 0 \pmod{16}.$$

Modulo 125 können wir ähnlich vorgehen. Es ist nämlich $121 \equiv -4 \pmod{125}$, also $121^n \equiv (-4)^n \pmod{125}$, sowie $1900 \equiv 25 \pmod{125}$ und daher $1900^n \equiv 25^n \pmod{125}$. Insgesamt also wieder

$$(121^n - (-4)^n) + (1900^n - 25^n) \equiv 0 + 0 = 0 \pmod{125}.$$

□

Beispiel 10. Sei n nicht durch 2 und nicht durch 5 teilbar. Zeige, dass es ein Vielfaches von n der Form $111 \dots 11$ gibt.

Lösung. Betrachte die Zahlen

$$\begin{array}{r} 1 \\ 11 \\ 111 \\ \vdots \\ \underbrace{111 \dots 11}_{n+1} \end{array} \pmod{n}$$

Zwei dieser Zahlen müssen nach dem Schubfachprinzip dieselbe Restklasse modulo n haben. Deren Differenz ist dann durch n teilbar und von der Form $111 \dots 11000 \dots 00 = 10^r \cdot \underbrace{111 \dots 11}_s$. Da n teilerfremd ist zu 10, ist n sogar ein Teiler von $\underbrace{111 \dots 11}_s$.

□

Beispiel 11. (Irland 96) Sei p eine Primzahl und a, n positive und ganze Zahlen, die die Gleichung

$$2^p + 3^p = a^n$$

erfüllen. Zeige, dass dann $n = 1$ gilt.

Lösung. Für $p = 2$ ist $2^p + 3^p = 13$, also $n = 1$. Sei nun $p > 2$, also insbesondere ungerade. Die LS der Gleichung faktorisiert dann als $(2 + 3)(2^{p-1} - 2^{p-2} \cdot 3 + \dots - 2 \cdot 3^{p-2} + 3^{p-1})$ und ist daher durch 5 teilbar. Also ist auch die RS, also auch a durch 5 teilbar. Wir nehmen jetzt $n > 1$ an, dann ist die RS durch 25 teilbar, also auch die LS. Dann muss aber $(2^{p-1} - 2^{p-2} \cdot 3 + \dots - 2 \cdot 3^{p-2} + 3^{p-1})$ durch 5 teilbar sein. Wir berechnen diesen Ausdruck nun modulo 5 und verwenden dabei die Kongruenz $3 \equiv -2 \pmod{5}$:

$$2^{p-1} - 2^{p-2} \cdot 3 + \dots - 2 \cdot 3^{p-2} + 3^{p-1} \equiv 2^{p-1} - 2^{p-2}(-2) + \dots - 2(-2)^{p-2} + (-2)^{p-1} = p2^{p-1} \pmod{5} \quad (5).$$

Da 2 und 5 teilerfremd sind, folgt daraus $p \equiv 0 \pmod{5}$, also $p = 5$, denn p ist prim. Für $p = 5$ erhalten wir aber $2^p + 3^p = 5^2 \cdot 11$ und das ist ein Widerspruch zu $n > 1$.

□

Aufgaben

1. Ist $m > 1$ und a eine ganze Zahl, dann ist genau einer der Zahlen

$$a, a + 1, a + 2, \dots, a + m - 1$$

durch m teilbar.

2. $p, p + 4$ und $p + 14$ sind Primzahlen. Finde p .
3. Sind x und y ungerade natürliche Zahlen, dann ist $x^2 + y^2$ keine Quadratzahl.
4. Zeige, dass es unendlich viele Primzahlen der Form $4k + 3$ gibt.
5. Gilt $9 \mid a^2 + ab + b^2$, dann sind a und b durch 3 teilbar.
6. Für welche ganzen Zahlen n ist $n^2 + 3n + 5$
 - (a) durch 11 teilbar?
 - (b) durch 121 teilbar?
7. Seien $a_1, a_2, \dots, a_n \in \{-1, 1\}$, sodass gilt

$$a_1a_2 + a_2a_3 + \dots + a_{n-1}a_n + a_na_1 = 0.$$

Zeige, dass $4 \mid n$.

8. (IMO 87) Zeige, dass es keine Funktion $f : \mathbb{N}_0 \rightarrow \mathbb{N}_0$ gibt mit

$$f(f(n)) = n + 1987.$$

9. (Russland 97) Finde alle Paare von Primzahlen p, q mit $p^3 - q^5 = (p + q)^2$.
10. (CH 03) Gegeben sind ganze Zahlen $0 < a_1 < a_2 < \dots < a_{101} < 5050$, zeige, dass man daraus immer vier verschiedene a_k, a_l, a_m, a_n auswählen kann mit

$$5050 \mid (a_k + a_l - a_m - a_n).$$

2.2 Die φ -Funktion und der Satz von Euler-Fermat

In diesem Abschnitt gehen wir das Problem an, grosse Potenzen modulo m zu berechnen. Als Hilfsmittel benötigen wir eine arithmetische Funktion, die wir jetzt definieren und untersuchen.

Definition 2.1. Für eine natürliche Zahl m ist die EULERSche φ -Funktion definiert durch

$$\varphi(m) = \#\{a \in \mathbb{Z} \mid 1 \leq a \leq m, \text{ggT}(a, m) = 1\}.$$

Sie ist also die Anzahl zu m teilerfremder positiver Zahlen kleiner m .

Satz 2.3. Die φ -Funktion besitzt folgende Eigenschaften:

- (i) Die φ -Funktion ist multiplikativ, das heisst

$$(m, n) = 1 \implies \varphi(mn) = \varphi(m)\varphi(n).$$

- (ii) Besitzt m die Primfaktorzerlegung $m = p_1^{n_1} p_2^{n_2} \dots p_r^{n_r}$, dann gilt

$$\begin{aligned} \varphi(m) &= m \left(1 - \frac{1}{p_1}\right) \left(1 - \frac{1}{p_2}\right) \dots \left(1 - \frac{1}{p_r}\right) \\ &= p_1^{n_1-1} p_2^{n_2-1} \dots p_r^{n_r-1} (p_1 - 1)(p_2 - 1) \dots (p_r - 1). \end{aligned}$$

Beweis. Wir zeigen nur (ii). Für $m = p^n$ ist a genau dann teilerfremd zu m , wenn a nicht durch p teilbar ist. Es gibt genau $p^n/p = p^{n-1}$ durch p teilbare Zahlen a mit $1 \leq a \leq m$, also ist $\varphi(m) = p^n - p^{n-1} = p^{n-1}(p-1)$. Die angegebene Formel folgt nun aus (i), wenn man diese Rechnung auf jede Primzahl p_k anwendet. □

Das entscheidende Resultat in diesem Abschnitt ist nun der Folgende Satz, der die Rechnung mit Potenzen modulo m stark vereinfacht.

Satz 2.4 (Euler-Fermat). *Ist m eine natürliche Zahl und $(a, m) = 1$, dann gilt*

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

Beweis. Wir verwenden im Folgenden die Kürzungsregel für Kongruenzen ohne Vorwarnung. Seien $a_1, a_2, \dots, a_{\varphi(m)}$ die positiven Zahlen $< m$, die zu m teilerfremd sind. Betrachte die Zahlen $aa_1, aa_2, \dots, aa_{\varphi(m)}$. Wir behaupten, dass sie eine Permutation der Zahlen $a_1, a_2, \dots, a_{\varphi(m)}$ modulo m bilden. Da a und a_k teilerfremd sind zu m , gilt dies auch für aa_k . Nehme nun an, es gelte $aa_k \equiv aa_l \pmod{m}$, dann folgt $a_k \equiv a_l$, also $a_k = a_l$ wegen $1 \leq a_k, a_l \leq m$. Also bilden die aa_k tatsächlich eine Permutation der a_k und daraus folgt nun

$$\begin{aligned} a_1 a_2 \cdots a_{\varphi(m)} &\equiv (aa_1)(aa_2) \cdots (aa_{\varphi(m)}) \\ &\equiv a^{\varphi(m)} (a_1 a_2 \cdots a_{\varphi(m)}) \\ \implies 1 &\equiv a^{\varphi(m)} \pmod{m}. \end{aligned}$$

□

Wegen $\varphi(p) = p-1$ für jede Primzahl p folgt daraus als Spezialfall unmittelbar

Korollar 2.5 (Kleiner Satz von Fermat). *Ist p eine Primzahl und a nicht durch p teilbar, dann gilt*

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

Ausserdem folgt daraus für jedes a (a kann durch p teilbar sein) die folgende Kongruenz:

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

Beispiel 12. *Zeige $7 \mid 2222^{5555} + 5555^{2222}$*

Lösung. Wir berechnen die beiden Zahlen modulo 7 mit Hilfe des kleinen Satzes von Fermat. Es ist $2222 \equiv 3$ und $5555 \equiv 4 \pmod{7}$. Ausserdem ist $\varphi(7) = 6$ und die Division mit Rest liefert $2222 = 370 \cdot 6 + 2$ sowie $5555 = 925 \cdot 6 + 5$. Mit Fermat folgt daraus modulo 7

$$\begin{aligned} 2222^{5555} &\equiv 3^{5555} = 3^{925 \cdot 6 + 5} = (3^6)^{925} \cdot 3^5 \equiv 1^{925} \cdot 243 \equiv 5 \\ 5555^{2222} &\equiv 4^{2222} = 4^{370 \cdot 6 + 2} = (4^6)^{370} \cdot 4^2 \equiv 1^{370} \cdot 16 \equiv 2. \end{aligned}$$

Addition dieser beiden Kongruenzen ergibt die Behauptung. □

Beispiel 13. *Seien a, b teilerfremd. Zeige, dass es natürliche Zahlen m, n gibt mit*

$$a^m + b^n \equiv 1 \pmod{ab}.$$

Lösung. Setze $m = \varphi(b)$, $n = \varphi(a)$. Dann folgt mit Euler-Fermat $a^m + b^n \equiv a^{\varphi(b)} + 0 \equiv 1 \pmod{b}$, da a und b teilerfremd sind. Analog gilt $a^m + b^n \equiv 0 + b^{\varphi(a)} \equiv 1 \pmod{a}$. Daher ist $a^m + b^n - 1$ kongruent 0 modulo a und b , also durch a und b teilbar, also auch durch ab (a und b sind teilerfremd). Das ist die Behauptung. □

Der Satz von Euler-Fermat sagt also aus, dass für $m > 0$ und $(a, m) = 1$ eine der Potenzen a, a^2, a^3, \dots kongruent 1 modulo m ist (nämlich $a^{\varphi(m)}$). Dies hat zur Folge, dass diese Potenzen modulo m *periodisch* sind mit Periode $\varphi(m)$. Es gilt nämlich $a^{k+\varphi(m)} = a^k \cdot a^{\varphi(m)} \equiv a^k \pmod{m}$. Im allgemeinen ist $\varphi(m)$ nicht die kleinstmögliche Periode, aber ein Vielfaches davon. Denn sei d die kleinste positive ganze Zahl mit $a^d \equiv 1 \pmod{m}$ (also die kleinste Periode), dann gilt sicher $d \leq \varphi(m)$. Schreibe nun $\varphi(m) = kd + r$ mit $0 \leq r < d$, dann folgt $1 \equiv a^{\varphi(m)} = (a^d)^k \cdot a^r \equiv a^r$. Wegen der Minimalität von d folgt daraus $r = 0$, das heisst $d \mid \varphi(m)$. Dieses d heisst auch die *Ordnung* von a modulo m und ist im allgemeinen schwierig zu berechnen. Für kleine Werte von m findet man diese kleinste Periode am besten durch probieren. Wir werden später auf diese Thematik zurückkommen, geben jetzt aber schon mal einen Vorgeschmack darauf, was man mit dieser Periodizität alles beweisen kann.

Beispiel 14. Sei n eine ungerade natürliche Zahl. Zeige, dass die Dezimaldarstellung von $2^{2n}(2^{2n+1} - 1)$ mit den Ziffern 28 endet.

Lösung. Die beiden letzten Ziffern einer Zahl sind kongruent zu ihr modulo 100. Wir werden daher zeigen, dass $A = 2^{2n}(2^{2n+1} - 1) - 28$ durch 100 teilbar ist für alle ungeraden Zahlen n . Nun ist 2^{2n} für $n \geq 1$ immer durch 4 teilbar, also auch A . Es genügt daher, die Teilbarkeit durch 25 zu zeigen. Da n ungerade ist, substituieren wir $n = 2k + 1$ und erhalten $A = 4 \cdot 16^k(8 \cdot 16^k - 1) - 28$. Wir berechnen jetzt die Potenzen von 16 modulo 25:

$$16^0 \equiv 1, \quad 16^1 \equiv 16, \quad 16^2 \equiv 6, \quad 16^3 \equiv 21, \quad 16^4 \equiv 11, \quad 16^5 \equiv 1 \pmod{25}$$

Sie wiederholen sich also mit Periode 5, das heisst, wir müssen nur die Fälle $k = 0, 1, 2, 3, 4$ betrachten:

$$\begin{aligned} k = 0 & : & A & \equiv 4(8 - 1) - 28 \equiv 0 \\ k = 1 & : & A & \equiv 4 \cdot 16(8 \cdot 16 - 1) - 28 \equiv 14 \cdot 2 - 28 \equiv 0 \\ k = 2 & : & A & \equiv 4 \cdot 6(8 \cdot 6 - 1) - 28 \equiv (-1) \cdot (-3) - 28 \equiv 0 \\ k = 3 & : & A & \equiv 4 \cdot 21(8 \cdot 21 - 1) - 28 \equiv 9 \cdot 17 - 28 \equiv 0 \\ k = 4 & : & A & \equiv 4 \cdot 11(8 \cdot 11 - 1) - 28 \equiv 19 \cdot 12 - 28 \equiv 0 \end{aligned}$$

In jedem Fall ist also A durch 25 teilbar, damit sind wir fertig. □

Beispiel 15. Finde alle natürlichen Zahlen x, y für die gilt $3^x - 2^y = 7$.

Lösung. Wir nehmen zuerst $y \geq 3$ an. Dann ist $3^x \equiv 7 \pmod{8}$. Eine kurze Rechnung zeigt aber, dass 3^x immer kongruent 1 oder 3 ist (mod 8), in diesem Fall gibt es also keine Lösungen. Gilt $y = 1$, dann folgt $x = 2$. Für $y = 2$ hat die Gleichung keine Lösung. Das einzige Lösungspaar ist daher $(2, 1)$. □

Oft kann man zeigen, dass ein Ausdruck gewisse Werte nicht annehmen kann, indem man ihn modulo eine geeignete Zahl reduziert. Dies ist der Grundgedanke der folgenden Aufgabe.

Beispiel 16. Seien m, n natürliche Zahlen. Finde die kleinste natürliche Zahl A , die sich in der Form $|36^m - 5^n|$ schreiben lässt.

Lösung. Für $m = 1$ und $n = 2$ ist $A = 11$. Wir zeigen nun, dass dies der kleinste mögliche Wert ist. Da 5 und 36 teilerfremd sind, kann A nicht durch 2, 3 oder 5 teilbar sein, also ist sicher $A \neq 0, 2, 3, 4, 5, 6, 8, 9, 10$. Wir müssen jetzt noch $A = 1$ und $A = 7$ ausschliessen. Aus $A = 1$ oder $A = 7$ folgt $36^m - 5^n = 1, -1, 7, -7$. Modulo 10 gilt $36^m \equiv 6$ und $5^n \equiv 5$ für alle

$m, n \geq 1$. Folglich ist $36^m - 5^n \equiv 6 - 5 \equiv 1 \pmod{10}$ und damit gilt $36^m - 5^n \neq -1, 7, -7$. Modulo 4 erhält man $36^m - 5^n \equiv 0 - 1^n \equiv 3$, also ist auch $36^m - 5^n = 1$ unmöglich. Dies beendet den Beweis. □

Aufgaben

1. (IMO 64) Finde alle natürlichen Zahlen n , sodass $2^n - 1$ durch 7 teilbar ist. Zeige, dass $2^n + 1$ nie durch 7 teilbar ist.
2. Zeige: $13 \mid 2^{70} + 3^{70}$.
3. Finde alle natürlichen Zahlen n , sodass $3 \mid n \cdot 2^n - 1$.
4. (IMO 78) Seien m und n natürliche Zahlen mit $m < n$. Die drei letzten Dezimalziffern von 1978^m und 1978^n sind dieselben. Finde m und n , sodass $m + n$ möglichst klein ist.
5. Sei n eine ungerade natürliche Zahl. Zeige, dass n ein Teiler ist von $2^{n!} - 1$.
6. Ist n gerade, dann gilt $323 \mid 20^n + 16^n - 3^n - 1$.
7. Finde alle natürlichen Zahlen x, y, z, t und n , für die gilt

$$n^x + n^y + n^z = n^t.$$

8. FERMAT hat behauptet, alle Zahlen der Form $F_n = 2^{2^n} + 1$ seien prim. Dies ist jedoch falsch, EULER hat als erster gezeigt, dass $641 \mid F_5$. Verifiziere dies.
9. Bestimme die zwei letzten Ziffern von $7^{7^{7^7}}$.

2.3 Der Chinesische Restsatz

Oft möchte man Rechnungen modulo m ausführen, wobei m eine zusammengesetzte Zahl ist. zum Beispiel $m = m_1 m_2$ mit m_1 und m_2 teilerfremd. Es wäre aber viel einfacher, wenn man modulo m_1 und m_2 rechnen könnte. Kann man daraus das Ergebnis modulo m rekonstruieren? Eine vollständige Antwort gibt der folgende Satz.

Satz 2.6 (Chinesischer Restsatz). *Seien m_1, m_2, \dots, m_r paarweise teilerfremde natürliche Zahlen und a_1, a_2, \dots, a_r beliebig. Dann hat das System von Kongruenzen*

$$\begin{aligned} x &\equiv a_1 && \pmod{m_1} \\ x &\equiv a_2 && \pmod{m_2} \\ &\vdots && \vdots \\ x &\equiv a_r && \pmod{m_r} \end{aligned}$$

eine ganzzahlige Lösung x . Diese ist eindeutig bestimmt modulo $m_1 m_2 \cdots m_r$.

Beispiel 17. *Wir geben ein Zahlenbeispiel. Für x gelte*

$$\begin{aligned} x &\equiv 3 && \pmod{5} \\ x &\equiv 2 && \pmod{7}. \end{aligned}$$

Gesucht ist die Restklasse von x modulo 35.

Lösung. Aus der ersten Kongruenz folgt $x \equiv 3, 8, 13, 18, 23, 28$ oder 33 modulo 5 . Aus der zweiten analog $x \equiv 2, 9, 16, 23$ oder 30 modulo 7 . Die einzige Restklasse modulo 35 , die beide Bedingungen erfüllt, ist 23 . Also ist $x \equiv 23 \pmod{35}$ die einzige Lösung des Systems von Kongruenzen, im Einklang mit Satz 2.6

□

Beispiel 18. (IMO 89) Zu jedem n gibt es n aufeinanderfolgende Zahlen, von denen keine eine Primzahlpotenz ist.

Lösung. Wir geben einen sehr eleganten Beweis mit Hilfe des Chinesischen Restsatzes. Wähle $2n$ verschiedene Primzahlen p_1, p_2, \dots, p_n und q_1, q_2, \dots, q_n . Betrachte nun folgendes System:

$$\begin{aligned} x &\equiv -1 && \pmod{p_1 q_1} \\ x &\equiv -2 && \pmod{p_2 q_2} \\ &\vdots && \vdots \\ x &\equiv -n && \pmod{p_n q_n} \end{aligned}$$

Nach dem Chinesischen Restsatz besitzt es eine ganzzahlige Lösung x , wobei wir $x > 0$ annehmen können. Nun ist das System gerade so konstruiert, dass $x+k$ die beiden verschiedenen Primteiler p_k und q_k besitzt für $1 \leq k \leq n$. Die n Zahlen $x+1, x+2, \dots, x+n$ sind also keine Primpotenzen.

□

2.4 Quadratische Reste und höhere Potenzen.

Eine der wichtigsten Tatsachen in der Zahlentheorie ist, dass nicht jede Zahl ein Quadrat ist modulo m . Wir geben gleich mal Beispiele, um zu zeigen, was damit gemeint ist.

Beispiel 19. Finde alle Lösungen in nichtnegativen ganzen Zahlen der folgenden Gleichung

$$x^2 + y^2 = 2^n + 3.$$

Lösung. Die Idee ist, die Gleichung modulo 4 zu betrachten. Wesentlich ist dabei, dass es wenige Quadrate modulo 4 gibt. Ist $x \equiv 0$ oder $\equiv 2 \pmod{4}$, also gerade, dann gilt $x^2 \equiv 0 \pmod{4}$. Ist $x \equiv 1$ oder $\equiv 3 \pmod{4}$, also ungerade, dann folgt $x^2 \equiv 1 \pmod{4}$. Ein Quadrat ist also immer $\equiv 0$ oder $1 \pmod{4}$. Damit nimmt die linke Seite der Gleichung nur die Werte $0, 1$ oder 2 an. Wir nehmen nun $n \geq 2$ an. Dann ist die rechte Seite aber $\equiv 3 \pmod{4}$, die Gleichung also nicht erfüllt. Die verbleibenden 2 Fälle liefern dann die Lösungen $(x, y, n) = (2, 0, 0), (0, 2, 0), (2, 1, 1)$ und $(1, 2, 1)$.

□

Wir listen die quadratischen Reste für ein paar wichtige Moduln auf:

$$\pmod{3} \quad \begin{array}{c|ccc} n & 0 & 1 & 2 \\ \hline n^2 & 0 & 1 & 1 \end{array}$$

$$\pmod{5} \quad \begin{array}{c|ccccc} n & 0 & 1 & 2 & 3 & 4 \\ \hline n^2 & 0 & 1 & 4 & 4 & 1 \end{array}$$

$$\pmod{4} \quad \begin{array}{c|cccc} n & 0 & 1 & 2 & 3 \\ \hline n^2 & 0 & 1 & 0 & 1 \end{array}$$

$$\pmod{8} \quad \begin{array}{c|ccccccc} n & 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ \hline n^2 & 0 & 1 & 4 & 1 & 0 & 1 & 4 & 1 \end{array}$$

$$\pmod{16} \quad \begin{array}{c|cccccccc} n & 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ \hline n^2 & 0 & 1 & 4 & 9 & 0 & 9 & 4 & 1 & 0 \end{array}$$

Die folgende Aufgabe stammt aus der australischen Landesausscheidung und wurde nur von sehr wenigen Schülern gelöst. Es ist in der Tat äusserst schwierig, mit algebraischen Umformungen und der Theorie der quadratischen Gleichungen direkt zu zeigen, dass keine ganzzahlige Lösung des Gleichungssystems existiert. Betrachtet man das Problem aber modulo 16, wird es fast trivial.

Beispiel 20. (Australien 01)

Zeige, dass keine vier ganzen Zahlen x, y, z, w existieren mit

$$\begin{aligned}x^2 &= 10w - 1 \\y^2 &= 13w - 1 \\z^2 &= 85w - 1\end{aligned}$$

Lösung. Nehme an, solche Zahlen existieren. Quadrate sind kongruent $0, 1, 4, 9$ modulo 16. Ist $w \equiv 0, 2, 3, 4, 6, 7, 8, 10, 11, 12, 14, 15 \pmod{16}$, dann wäre nach der ersten Gleichung $x^2 \equiv 15, 3, 13, 7, 11, 5, 15, 3, 13, 7, 11, 5 \pmod{16}$, ein Widerspruch. Ist $w \equiv 1, 13 \pmod{16}$, dann folgt $y^2 \equiv 12, 8 \pmod{16}$, was ebenfalls unmöglich ist. Ist schliesslich $w \equiv 5, 9 \pmod{16}$, dann gilt $z^2 \equiv 8, 12 \pmod{16}$, Widerspruch. Folglich gibt es keine vier solchen Zahlen. □

Wir haben gesehen, wie wirkungsvoll es sein kann, ein Problem modulo m zu reduzieren, da nicht alle Restklassen modulo m Quadrate sind und man so viel an Information gewinnt. Das alles funktioniert nicht nur für Quadrate, sondern allgemein für k -te Potenzen. Dazu ist folgende Regel zu beachten:

Sind k -te Potenzen involviert, dann wähle m als Zweierpotenz oder so, dass $k \mid \varphi(m)$.

Wir können dies hier nicht vollständig begründen, aber dennoch motivieren, die Idee ist die folgende: Treten wenige k -te Potenzen modulo m auf, dann gibt es wahrscheinlich auch ein $a \not\equiv 1 \pmod{m}$ mit $a^k \equiv 1 \pmod{m}$. Nach dem Satz von Euler-Fermat, bzw. der darauf folgenden Diskussion auf Seite 16, kann dies für $(a, m) = 1$ nur dann der Fall sein, wenn $k \mid \varphi(m)$.

Hat man also zum Beispiel mit dritten Potenzen zu tun, dann muss man m so wählen, dass $3 \mid \varphi(m)$ gilt. Die einfachste Möglichkeit ist $m = 7$. In der Tat zeigt ein kleiner Vergleich zwischen $m = 7$ und $m = 11$ den Unterschied deutlich:

n	0	1	2	3	4	5	6	n	0	1	2	3	4	5	6	7	8	9	10
n^3	0	1	1	6	1	6	6	n^3	0	1	8	5	9	4	7	2	6	3	10
(mod 7)								(mod 11)											

Das folgende Beispiel war das schwierigste Problem der Balkan Olympiade 98:

Beispiel 21. (BalkMO 98)

Zeige, dass die folgende Gleichung keine ganzzahlige Lösung besitzt

$$y^2 = x^5 - 4.$$

Lösung. Es sind zweite und fünfte Potenzen im Spiel, nach obiger Faustregel sollten wir daher ein m bestimmen mit $2 \mid \varphi(m)$ und $5 \mid \varphi(m)$ und die Gleichung modulo m reduzieren. Die einfachste Möglichkeit ist $m = 11$. Eine kurze Rechnung zeigt, dass Quadrate $\equiv 0, 1, 3, 4, 5, 9 \pmod{11}$ und fünfte Potenzen $\equiv 0, 1, 10 \pmod{11}$ sind. Nehme an, die Gleichung habe eine Lösung (x, y) . Dann ist die linke Seite der Gleichung $\equiv 0, 1, 3, 4, 5, 9 \pmod{11}$ und die rechte Seite $\equiv 6, 7, 8 \pmod{11}$, Widerspruch. Die Gleichung besitzt also keine ganzzahligen Lösungen. □

Aufgaben

1. Zeige, dass für jede Primzahl $p > 3$ gilt $p^2 \equiv 1 \pmod{24}$.
2. Zeige: Sind p und $p^2 + 2$ Primzahlen, dann ist auch $p^3 + 2$ prim.
3. Sei $q = p_1 p_2 \cdots p_n$ das Produkt der ersten n Primzahlen. Zeige, dass $q - 1$ keine Quadratzahl ist.
4. (CH 98) Finde alle Primzahlen p , sodass $p^2 + 11$ genau 6 positive Teiler besitzt.
5. Zeige, dass die Gleichung $y^2 = x^3 + 7$ keine ganzzahligen Lösungen besitzt.
6. Ist $n \in \mathbb{N}$, sodass $2n + 1$ und $3n + 1$ beides Quadrate sind, dann gilt $40 \mid n$.
7. (MMO 1984) Finde alle ganzzahligen Lösungen der Gleichung $19x^3 - 84y^2 = 1984$.
8. Für $a, b, c, d, e \in \mathbb{N}$ gilt $a^4 + b^4 + c^4 + d^4 = e^4$. Zeige, dass mindestens drei der fünf Zahlen gerade sind, dass mindestens drei durch 5 teilbar sind und dass mindestens zwei mit der Ziffer 0 enden.
9. (CH 02) n sei eine positive ganze Zahl mit mindestens vier verschiedenen positiven Teilern. Die vier kleinsten unter diesen Teilern seien d_1, d_2, d_3, d_4 . Finde alle solchen Zahlen n , für die gilt
$$d_1^2 + d_2^2 + d_3^2 + d_4^2 = n.$$
10. (IMO 86) Sei d eine positive ganze Zahl $\neq 2, 5, 13$. Zeige: In der Menge $\{2, 5, 13, d\}$ gibt es zwei Elemente a, b , für die $ab - 1$ keine Quadratzahl ist.
11. (IMO 96) a, b sind natürliche Zahlen, sodass $15a + 16b$ und $16a - 15b$ beides Quadrate sind. Man bestimme den kleinsten möglichen Wert, den das kleinere der beiden Quadrate annehmen kann.
12. Zeige, dass 19^{19} nicht die Summe einer dritten und einer vierten Potenz ist.

3 Faktorisierungen

Äusserst wichtig in der Zahlentheorie und an der IMO im speziellen sind Faktorisierungen. Denn oft gewinnt man Informationen wie Teilbarkeit, Kongruenzen etc. über die Faktoren, die dann weiterhelfen können. Es geht dabei immer um polynomiale Ausdrücke in einer oder mehreren Variablen, die man faktorisieren möchte. Es gibt viele Methoden, wie dies gemacht werden kann, jedoch gehört das eher in die Theorie der Polynome. Wir beschränken uns hier also primär auf die Zahlentheoretischen Anwendungen. Im Zentrum stehen dabei ganz einfache Tatsachen, die aber richtig angewendet grosse Wirkung erzielen können.

Zur Erinnerung ein paar Fakten:

- $a \mid bc$ und $(a, b) = 1 \implies a \mid c$
- Sind a und b teilerfremd und ist $ab = x^k$ eine k -te Potenz, dann sind a und b selbst k -te Potenzen
- Ist p eine Primzahl und $ab = p^k$ eine p -Potenz, dann sind auch a und b p -Potenzen.
- Ist p prim und gilt $ab = p$, dann hat einer der beiden Faktoren Betrag 1.

- $a, b \in \mathbb{N}, a \mid b \implies b \leq a$

Im folgenden geben wir als Erinnerung eine Übersicht über die Binomischen Formeln. In vielen Fällen genügen sie schon, eine geeignete Faktorisierung zu finden. Die klassische Binomische Formel ist natürlich

$$(x + y)^n = \sum_{k=1}^n \binom{n}{k} x^k y^{n-k}$$

Dabei sind x, y beliebige reelle Zahlen und $n \geq 0$ ganz. Den Beweis führt man entweder kombinatorisch (Interpretation der Binomialkoeffizienten) oder via Induktion. Die folgenden Identitäten gehen mehr in Richtung Faktorisieren eines Ausdrucks (nämlich der linken Seite). Die erste gilt für **alle** natürlichen n :

$$x^n - y^n = (x - y)(x^{n-1} + x^{n-2}y + \dots + xy^{n-2} + y^{n-1})$$

Diese nur für **ungerade** n :

$$x^n + y^n = (x + y)(x^{n-1} - x^{n-2}y + \dots - xy^{n-2} + y^{n-1})$$

Und die hier nur für **gerade** n :

$$x^n - y^n = (x + y)(x^{n-1} - x^{n-2}y + \dots - xy^{n-2} + y^{n-1})$$

Hier sei nochmal ausdrücklich auf den Spezialfall mit Exponent 2 hingewiesen:

$$\begin{aligned} (x + y)^2 &= x^2 + 2xy + y^2 \\ (x - y)^2 &= x^2 - 2xy + y^2 \\ x^2 - y^2 &= (x + y)(x - y) \end{aligned}$$

Insbesondere ist eine Differenz zweier Quadrate immer faktorisiertbar. Diese wichtige Tatsache überträgt sich leider nicht auf Summen von Quadraten. In der Tat kann man aber auch $x^2 + y^2$ faktorisieren, falls $2xy$ ebenfalls ein Quadrat ist. Im einfachsten Fall erhält man so die wichtige **Identität von Sophie Germain**:

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

Es ist natürlich einfach, diese Identität nachzuprüfen, viel interessanter ist jedoch die Frage, wie man sie finden könnte. Hier ist eine kurze Herleitung, die man sich merken sollte:

$$\begin{aligned} x^4 + 4y^4 &= (x^4 + 4x^2y^2 + y^4) - 4x^2y^2 = (x^2 + 2y^2)^2 - (2xy)^2 \\ &= (x^2 + 2xy + 2y^2)(x^2 - 2xy + 2y^2) \end{aligned}$$

Jetzt ist aber Zeit für ein paar Beispiele.

Beispiel 22. (Griechenland 95)

Finde alle natürlichen Zahlen n , sodass $2^4 + 2^7 + 2^n$ ein Quadrat ist.

Lösung. Wir suchen also alle n , sodass gilt $2^n = m^2 - 2^4 - 2^7 = m^2 - 144$ für eine natürliche Zahl m . Dies können wir faktorisieren als $2^n = (m + 12)(m - 12)$, also sind $m + 12$ und $m - 12$ zwei Zweierpotenzen, deren Differenz 24 ist. Die einzigen solchen Zweierpotenzen sind $8 = 2^3$ und $32 = 2^5$, also ist $m = 20$ und $n = 8$. □

Beispiel 23. *Zeige, dass das Produkt von vier aufeinanderfolgenden natürlichen Zahlen keine Quadratzahl ist.*

Lösung. Es gilt $n(n + 1)(n + 2)(n + 3) = n^4 + 6n^3 + 11n^2 + 6n = n^2(n^2 + 3n + 1) + 3n(n^2 + 3n + 1) + (n^2 + 3n + 1) - 1 = (n^2 + 3n + 1)^2 - 1$. Das heisst, dieses Produkt ist immer um 1 kleiner als eine Quadratzahl. Die einzigen zwei Quadratzahlen mit Differenz 1 sind aber 0 und 1, wegen $n(n + 1)(n + 2)(n + 3) \geq 24$ kann dies also nie ein Quadrat sein. □

Beispiel 24. *Finde alle Primzahlen der Form $n^n + 1$, die kleiner als 10^{19} sind.*

Lösung. Für $n = 1$ erhalten wir die Primzahl 2. Ist n ungerade, dann ist $n^n + 1$ gerade, also nicht prim. Ist nun $n > 1$ gerade, dann können wir schreiben $n = 2^t u$ mit $t \geq 1$ und u ungerade. Ist $u > 1$, dann können wir die binomische Formel anwenden und wie folgt faktorisieren:

$$n^n + 1 = \left(n^{2^t}\right)^u + 1^u = (n^{2^t} + 1)(\dots),$$

Dabei sind beide Faktoren grösser als 1, die Zahl also nicht prim. Daher muss $u = 1$ sein und $n = 2^t$. Für $t = 1$ erhalten wir die Primzahl 5, sei nun $t > 1$. Wir schreiben wieder $t = 2^s v$ mit v ungerade. Ist $v > 1$, dann folgt wieder mit den binomischen Formeln

$$n^n + 1 = \left(2^{2^s n}\right)^v + 1^v = (2^{2^s n} + 1)(\dots),$$

wobei beide Faktoren grösser als 1 sind. Damit muss $v = 1$ und $n = 2^{2^s}$ sein. Für $s = 1$ erhalten wir $4^4 + 1 = 275$, eine Primzahl. Für $s \geq 2$ gilt aber $n^n + 1 \geq 16^{16} + 1 > 10^{19}$. Die einzigen solchen Primzahlen sind daher 2, 5 und 257. □

Beispiel 25. *(Kürschak 78) Zeige, dass $n^4 + 4^n$ nie eine Primzahl ist für $n > 1$.*

Lösung. Ist n gerade, dann ist auch $n^4 + 4^n$ gerade und grösser als 2, also keine Primzahl. Ist n ungerade, dann schreiben wir $n = 2k + 1$ mit $k \geq 1$. Nun folgt mit Sophie Germain

$$\begin{aligned} n^4 + 4^n &= n^4 + 4^{2k+1} = n^4 + 4(2^k)^4 \\ &= (n^2 + 2 \cdot n \cdot 2^k + 2(2^k)^2)(n^2 - 2 \cdot n \cdot 2^k + 2(2^k)^2) \\ &= (n^2 + 2^{k+1}n + 2^n)(n^2 - 2^{k+1}n + 2^n). \end{aligned}$$

Der erste Faktor ist immer grösser als 1. Mit $2^n - 2^{k+1}n = 2^{k+1}(2^k - 2k - 1)$ und einer trivialen Abschätzung folgt, dass für $k \geq 1$ auch der Zweite Faktor grösser als 1 ist. Folglich ist auch in diesem Fall $n^4 + 4^n$ nie prim. □

Das folgende Beispiel zeigt sehr schön, wie die Modulorechnung eingesetzt werden kann, um Informationen über die Exponenten zu erhalten, die dann wiederum zu einer geeigneten Faktorisierung führen.

Beispiel 26. *Finde alle natürlichen Zahlen x, y, z , sodass gilt*

$$2^x + 3^y = z^2.$$

Lösung. Wir betrachten die Gleichung modulo 3. Die rechte Seite ist $\equiv 0, 1$, andererseits gilt $2^x \equiv 1$ für x gerade und $2^x \equiv 2$ für x ungerade. Daraus folgt, dass x gerade sein muss, also insbesondere ist $x \geq 2$. Wir betrachten die Gleichung nun modulo 4. Da z ungerade ist, muss die rechte Seite $\equiv 1 \pmod{4}$ sein, also $3^y \equiv 1$. Dies ist genau dann der Fall, wenn $y = 2s$ gerade ist. Nun können wir faktorisieren:

$$2^x = (z - 3^s)(z + 3^s).$$

Die beiden Faktoren rechts sind Zweierpotenzen ≥ 2 . Ihr grösster gemeinsamer Teiler muss ausserdem $2 \cdot 3^s$ teilen, ist also gleich 2. Daher gilt $z - 3^s = 2$ und $z + 3^s = 2^{x-1}$. Subtrahiert man die erste von der zweiten Gleichung und teilt durch 2, dann folgt $3^s + 1 = 2^{x-2}$ und damit auch $x > 2$. Für $x = 4$ ergibt sich die Lösung $y = 2$ und $z = 5$. Ist $x \geq 6$, dann muss $3^s + 1$ durch 16 teilbar sein. Eine kurze Rechnung zeigt aber $3^s \equiv 1, 3, 9, 11 \pmod{16}$, Widerspruch. Die einzige Lösung ist daher $(x, y, z) = (4, 2, 5)$. □

Beispiel 27. Zeige, dass für alle positiven ganzen Zahlen $n > 1$ und a, b gilt

$$\text{ggT}(n^a - 1, n^b - 1) = n^{\text{ggT}(a,b)} - 1.$$

Lösung. Sei $d = \text{ggT}(a, b)$ und schreibe $a = dk$ und $b = dl$. Nun folgt mit den Binomischen Formeln $n^a - 1 = (n^d)^k - 1^k = (n^d - 1)(n^{d(k-1)} + n^{d(k-2)} + \dots + n^d + 1)$, also ist $n^d - 1 \mid n^a - 1$. die analoge Rechnung für b ergibt somit $n^d - 1 \mid \text{ggT}(n^a - 1, n^b - 1)$.

Umgekehrt existieren nach Bezout positive ganze Zahlen x, y mit $ax - by = d$. Dann gilt $(n^a - 1) \mid (n^{ax} - 1)$ und $(n^b - 1) \mid (n^{by} - 1)$ und ausserdem

$$(n^{ax} - 1) - (n^{by} - 1) = n^{by}(n^d - 1).$$

Nun teilt $\text{ggT}(n^a - 1, n^b - 1)$ die linke Seite dieser Gleichung, also auch die rechte. Wegen $\text{ggT}(n^{by}, n^b - 1) = 1$ teilt dies sogar $n^d - 1$. Insgesamt folgt also $\text{ggT}(n^a - 1, n^b - 1) = n^{\text{ggT}(a,b)} - 1$. □

Aufgaben

1. Zeige, dass für alle ganzen Zahlen n gilt $30 \mid n^5 - n$.
2. Ist n keine Primzahl, dann ist auch $2^n - 1$ nicht prim. Besitzt n einen ungeraden Faktor > 1 , dann ist $2^n + 1$ nicht prim.
3. (IMO 68) Zeige, dass es unendlich viele natürlichen Zahlen m gibt, sodass $n^4 + m$ für keine natürliche Zahl n prim ist.
4. Zeige, dass für $n > 2$ die Zahl $2^{2^n-2} + 1$ nie prim ist.
5. Gibt es Primzahlen p, q, r mit $p^2 + q^3 = r^4$?
6. (Österreich 95) Wieviele a) gerade b) ungerade natürliche Zahlen n gibt es, sodass n ein Teiler ist von $3^{12} - 1$, nicht aber von $3^k - 1$ für $k = 1, 2, \dots, 11$?
7. Finde alle positiven ganzen Lösungen der Gleichung

$$|3^x - 2^y| = 1.$$

8. Mehrere verschiedene ganze Zahlen liegen zwischen zwei aufeinander folgenden Quadratzahlen. Zeige, dass ihre paarweisen Produkte alle verschieden sind.

9. Finde alle natürlichen Zahlen x, y, z , sodass gilt

$$x^4 + y^4 + z^4 - 2x^2y^2 - 2y^2z^2 - 2z^2x^2 = 189.$$

10. Ist $4^{545} + 545^4$ eine Primzahl?

11. (CH 03) Finde die grösste natürliche Zahl n , die für jede ganze Zahl a ein Teiler ist von $a^{25} - a$.

12. Sei $n \geq 0$. Zeige, dass $2^{2^n} + 2^{2^{n-1}} + 1$ mindestens n verschiedene Primteiler besitzt.

13. Finde alle positiven ganzen Lösungen der Gleichung

$$3^x + 4^y = 5^z.$$

14. Zeige, dass die Zahl $(5^{125} - 1)/(5^{25} - 1)$ zusammengesetzt ist.

15. Beweise, dass die Zahl 1280000401 zusammengesetzt ist.

16. Ist $4^n + 2^n + 1$ eine Primzahl, dann ist n einer Dreierpotenz.

17. (CSO 95) Sei p eine ungerade Primzahl. Finde alle Paare x, y nichtnegativer ganzer Zahlen, sodass gilt

$$p^x - y^p = 1.$$

4 Ziffern und Zahlssysteme

4.1 Zahlen und ihre Ziffern

Beispiel 28. Zeige, dass eine 9-stellige Zahl, in der jede Ziffer ausser der 0 genau einmal vorkommt und die mit 5 endet, keine Quadratzahl sein kann.

Lösung. Nehme an, A sei so eine neunstellige Zahl mit $A = B^2$. Da A mit einer 5 endet, ist sie ungerade und durch 5 teilbar, also gilt dies auch für B . Schreibe $B = 10b + 5$, dann gilt $B^2 = 100b^2 + 100b + 25 = 100b(b + 1) + 25$. Daraus folgt, dass die zweitletzte Ziffer von A eine 2 sein muss. Ausserdem zeigt die Tabelle

b	0	1	2	3	4	5	6	7	8	9
$b(b + 1) \bmod 10$	0	2	6	2	0	0	2	6	2	0

dass die drittletzte Ziffer von A eine 0, 2 oder 6 sein muss. Nun kommt aber 0 nicht als Ziffer vor und 2 steht schon an zweitletzter Stelle, also ist die drittletzte Ziffer von A eine 6. Es gilt daher $A = 1000c + 625$, also ist A durch 5^3 teilbar. Da A ein Quadrat ist, also sogar durch $5^4 = 625$. Daraus folgt, dass c durch 5 teilbar ist, die viertletzte Ziffer von A ist also 0 oder 5. Beides ist aber unmöglich, da 0 nicht vorkommen darf und 5 schon verbraucht ist. \square

Beispiel 29. Wir starten mit einer natürlichen Zahl a_1 und erzeugen damit eine Folge natürlicher Zahlen a_1, a_2, a_3, \dots wie folgt: a_{n+1} entsteht aus a_n , indem wir am Ende von a_n eine Ziffer $\neq 9$ anhängen. Zeige, dass unendliche viele Folgenglieder zusammengesetzt (also nicht prim) sind.

Lösung. Wir versuchen, die Folge so zu konstruieren, dass nur endlich viele Folgeglieder zusammengesetzt sind. Eine mehrstellige Zahl, die mit einer der Ziffern 0, 2, 4, 5, 6, 8 endet, ist durch 2 oder 5 teilbar, also nicht prim. Diese Ziffern dürfen wir also ab einer bestimmten Stelle in der Folge nicht mehr anhängen. Bleiben noch 1, 3 und 7. Jedes Mal, wenn wir ein 1 oder 7 anhängen, ändert sich die Restklasse modulo 3 um 1. Hängen wir eine 3 an, dann ändert sich natürlich nichts. Das heisst, spätestens nach dem dritten Anhängen einer 1 oder 7 erhalten wir eine durch 3 teilbare Zahl. Daher dürfen wir auch 1 und 7 nur endliche Male anhängen. Ab einer bestimmten Stelle der Folge verwenden wir also nur noch die 3. Ist nun $p = a_n$ prim, dann ist eine der nächsten p Zahlen ebenfalls durch p teilbar, also nicht prim. Dies folgt aus der Tatsache, dass eine der Zahlen $1, 11, 111, \dots, \underbrace{111 \dots 11}_p$ durch p teilbar ist, denn $\text{ggT}(p, 10) = 1$ (vergleiche Beispiel 10). Daher können wir nicht vermeiden, dass unendlich viele Folgeglieder zusammengesetzt sind. □

Aufgaben

1. Die vierstellige Zahl $aabb$ ist ein Quadrat. Wie lautet sie?
2. Ist eine Zahl der Form $\underbrace{111 \dots 11}_n$ prim, dann ist n prim.
3. Zeige, dass in der Folge $1, 31, 331, 3331, \dots$ unendlich viele zusammengesetzte Zahlen vorkommen.
4. Zeige, dass $1982 \mid 222 \dots 22$ (1982 Zweien).
5. (IMO 60) Finde alle dreistelligen, durch 11 teilbaren natürlichen Zahlen N , sodass $N/11$ gleich der Summe der Quadrate der Ziffern von N ist.
6. Finde alle vierstelligen Zahlen $abcd$, sodass gilt $4 \cdot abcd = dcba$.
7. (England 96) Das Paar

$$(M, N) = (3600, 2500)$$

hat viele Eigenschaften. Beide Zahlen sind vierstellig und es gibt genau zwei Stellen wo in M und N dieselbe Ziffer steht. An den beiden anderen Stellen ist die Ziffer in M um genau 1 grösser als jene in N . Ausserdem sind beides Quadrate. Finde alle Paare (M, N) vierstelliger Zahlen mit all diesen Eigenschaften.

8. Die Dezimaldarstellung von A besteht aus 600 Sechsen und einigen Nullen. Kann A eine Quadratzahl sein?
9. Zeige

$$\underbrace{11 \dots 1}_{2n} = \underbrace{22 \dots 2}_n + (\underbrace{33 \dots 3}_n)^2.$$
10. Für eine natürliche Zahl n bezeichne \bar{n} die Zahl, die man erhält, wenn man die Reihenfolge der Ziffern von n umkehrt (z.B. $n = 1623$, $\bar{n} = 3261$). Für k gelte $k \mid n \implies k \mid \bar{n}$ für alle n . Zeige $k \mid 99$.

11. (IMO 62) Bestimme die kleinste natürliche Zahl, die mit der Ziffer 6 endet, sodass die Zahl viermal so gross wird, wenn man die letzte Ziffer an den Anfang der Zahl verschiebt.

12. (Südafrika 97) Finde alle natürlichen Zahlen mit der Eigenschaft, dass wenn man die erste Ziffer ans Ende der Zahl verschiebt, dann ist das Resultat $3\frac{1}{2}$ mal so gross wie die ursprüngliche Zahl.
13. (Shortlist 90) Finde alle natürlichen Zahlen n , sodass jede Zahl, die im Dezimalsystem geschrieben aus $n - 1$ Einsen und einer Sieben besteht, prim ist.

4.2 Darstellung einer Zahl in Basis b

So wie man üblicherweise Zahlen im Zehnersystem (Dezimalsystem) schreibt, kann man statt 10 genausogut jede andere ganze Zahl $b \geq 2$ als Basis verwenden. Genauer gilt folgendes:

Satz 4.1. *Sind $b \geq 2$ und $x \geq 0$ ganze Zahlen, dann gibt es ein r und ganze Zahlen a_0, a_1, \dots, a_r mit $0 \leq a_k \leq b - 1$, $0 \leq k \leq r$, sodass gilt*

$$x = a_r b^r + a_{r-1} b^{r-1} + \dots + a_1 b + a_0.$$

Die a_k und r sind durch x eindeutig bestimmt.

Die Summe im Satz nennt man dann die **Darstellung von x in der Basis b** oder **b -adische Darstellung** von x . Für $b = 10$ erhält man die gute alte Dezimaldarstellung, für $b = 2$ die **Binärdarstellung**. Die a_k im Satz sind also die Ziffern von x , geschrieben in Basis b . Analog zur üblichen Schreibweise verwendet man die Notation $x = (a_r a_{r-1} \dots a_1 a_0)_{(b)}$.

Wie berechnet man die Darstellung von x in der Basis b ? Dazu gibt es ein einfaches Verfahren:

Algorithmus 4.2 (b -adische Darstellung).

1. Setze $x_0 = x$ und $k = 0$.
2. Sei a_k der Rest bei der Division von x_k durch b .
3. Setze $x_{k+1} = (x_k - a_k)/b$. Ist dies $= 0$, dann beende den Algorithmus, sonst erhöhe k um 1 und gehe zu Schritt 2.

Es ist dann $x = (a_r a_{r-1} \dots a_1 a_0)_{(b)}$

Zum Beispiel ist $10000_{(10)} = 10011100010000_{(2)} = 4723_{(13)}$.

Die Darstellung von Zahlen zu verschiedenen Basen kann in vielen Fällen sehr nützlich sein. Wir können die Anwendungsmöglichkeiten bei weitem nicht alle demonstrieren, möchten aber doch einen kleinen Einblick geben mit den folgenden Beispielen.

Beispiel 30. (IMO 83) *Kann man 1983 verschiedene natürliche Zahlen < 100000 finden, von denen keine drei eine arithmetische Folge bilden?*

Lösung. Ja, kann man. Wir konstruieren eine Folge a_n mit der gewünschten Eigenschaft. Schreibe zuerst n im Binärsystem, $n = (x_r x_{r-1} \dots x_0)_{(2)}$ und lese diese Zahl im Dreiersystem um a_n zu erhalten, setze also $a_n = (x_r x_{r-1} \dots x_0)_{(3)}$. Man kann es auch anders sagen: wir nehmen diejenigen Zahlen, die im Dreiersystem geschrieben nur die Ziffern 0 und 1 haben. Nun ist

$$a_{1983} = a_{111101111111}_{(2)} = 11110111111_{(3)} = 87844 < 100000,$$

wir müssen also noch zeigen, dass keine drei dieser Zahlen eine arithmetische Folge bilden. $x < y < z$ bilden genau dann eine arithmetische Folge, wenn $x + z = 2y$. Nehme an, es gelte $a_k + a_m = 2a_l$ für $1 \leq k < l < m \leq 1983$. Im Dreiersystem kommen auf der rechten Seite

nur die Ziffern 0 und 2 vor. Die beiden Zahlen links hingegen bestehen nur aus den Ziffern 0 und 1. Diese Gleichung kann also nur dann stimmen, wenn die Basis-3-Darstellungen von a_k und a_m übereinstimmen, also wenn $k = m$, Widerspruch. □

Beispiel 31. Sei $f : \mathbb{N} \rightarrow \mathbb{N}$ eine Funktion mit den folgenden Eigenschaften:

- (1) $f(1) = 1$
- (2) $f(2n) = f(n)$
- (3) $f(2n + 1) = f(2n) + 1$

Finde den grösstmöglichen Wert von $f(n)$ für $1 \leq n \leq 2003$.

Lösung. Wir betrachten alles in Basis 2 (vielleicht sind die vielen 2en in den Gleichungen für f ein Hinweis darauf). Aus der natürlichen Zahl n entsteht $2n$, indem man rechts an die Binärdarstellung eine Null anhängt. Analog entsteht $2n + 1$ durch Anhängen einer Eins. Die ersten paar Werte lauten $f(1_{(2)}) = 1$, $f(10_{(2)}) = 1$, $f(11_{(2)}) = 2$, $f(100_{(2)}) = 1$. Wir zeigen mit vollständiger Induktion, dass $f(n)$ die Anzahl Einsen in der Binärdarstellung von n ist. Dies ist richtig für $n = 1$ und stimmt für alle Zahlen $< n$. Ist n gerade, also $n = 2k$, dann haben n und k gleichviele Einsen in der Binärdarstellung und tatsächlich folgt mit (2) auch $f(n) = f(k)$, die Induktionsvoraussetzung ergibt die Behauptung. Ist n ungerade, also $n = 2k + 1$, dann besitzt n genau eine Eins mehr in der Binärdarstellung als k . Mit (3) folgt $f(n) = f(k) + 1$ und die Behauptung ergibt sich wieder aus der Induktionsvoraussetzung. Wir müssen jetzt lediglich noch bestimmen, wieviele Einsen eine Zahl $n \leq 2003$ in Basis 2 haben kann. Wegen $2^{11} = 2048 > 2003$ hat n höchstens 11 Stellen. Wegen $11111111111_{(2)} = 2047 > 2003$ können aber nicht 11 Einsen auftreten. Daher gilt $f(n) \leq 10$. Gleichheit gilt für $n = 1023 = 1111111111_{(2)}$. □

Aufgaben

1. Finde alle Funktionen $f : \mathbb{N} \rightarrow \mathbb{R}$ mit $f(1) = 1$ und

$$f(n) = \begin{cases} 1 + f\left(\frac{n-1}{2}\right), & n \text{ ungerade,} \\ 1 + f\left(\frac{n}{2}\right), & n \text{ gerade.} \end{cases}$$

2. (IMO 88) Für $f : \mathbb{N} \rightarrow \mathbb{N}$ gelte $f(1) = 1$, $f(3) = 3$ und für jedes $n \in \mathbb{N}$

- (a) $f(2n) = f(n)$,
- (b) $f(4n + 1) = 2f(2n + 1) - f(n)$,
- (c) $f(4n + 3) = 3f(2n + 1) - 2f(n)$.

Finde die Anzahl $n \leq 1988$ mit $f(n) = n$.

3. (China 95) Nehme an, für $f : \mathbb{N} \rightarrow \mathbb{N}$ gelte $f(1) = 1$ und für alle $n \in \mathbb{N}$

- (a) $3f(n)f(2n + 1) = f(2n)(1 + 3f(n))$,
- (b) $f(2n) < 6f(n)$.

Finde alle Lösungen der Gleichung $f(k) + f(m) = 293$.

4. (IMO 70) Es gelte $0 \leq x_i < b$ für $i = 0, 1, \dots, n$ und ausserdem $x_n, x_{n-1} > 0$. Sei $a > b$ und $x_n x_{n-1} \dots x_0$ sei in Basis a gelesen die Zahl A und in Basis b gelesen die Zahl B . Ähnlich sei $x_{n-1} x_{n-2} \dots x_0$ in Basis a gelesen die Zahl A' und in Basis b gelesen die Zahl B' . Zeige, dass gilt $A'B < AB'$.
5. (USA 96) Entscheide, ob es eine Menge X ganzer Zahlen gibt, sodass die Gleichung $a + 2b = n$ für jede ganze Zahl n genau eine Lösung mit $a, b \in X$ hat.

5 Varia

5.1 Die Gaussklammer

Für eine reelle Zahl x bezeichnet $\lfloor x \rfloor$ die grösste ganze Zahl $\leq x$. Zum Beispiel gilt $\lfloor 5 \rfloor = 5$, $\lfloor -2.6 \rfloor = -3$ und $\lfloor \pi \rfloor = 3$. Man nennt $\lfloor \cdot \rfloor$ auch *Gaussklammer*. Die ganze Zahl $\lfloor x \rfloor$ ist eindeutig bestimmt durch die Ungleichungen

$$\lfloor x \rfloor \leq x < \lfloor x \rfloor + 1.$$

Man kann diese auch umschreiben zu

$$x - 1 < \lfloor x \rfloor \leq x.$$

Für eine reelle Zahl x bezeichnet $\{x\} = x - \lfloor x \rfloor$ den *gebrochenen Teil* von x . Zum Beispiel gilt $\{-3.1\} = 0.9$, $\{\pi\} = 0.1415\dots$, insbesondere ist stets $\{x\} \geq 0$ mit Gleichheit genau dann, wenn x ganz ist.

Eine wichtige Beobachtung bei der Lösung von Problemen, wo Gaussklammern involviert sind, ist folgende: Zwischen zwei aufeinanderfolgenden ganzen Zahlen liegt keine weitere. Dies führt auf folgendes erstaunliches Resultat:

Beispiel 32. Seien α und β positive irrationale Zahlen mit $\frac{1}{\alpha} + \frac{1}{\beta} = 1$. Dann enthalten die beiden Folgen $\lfloor \alpha m \rfloor$ und $\lfloor \beta n \rfloor$ zusammen jede natürliche Zahl genau einmal.

Lösung. Wir zeigen zuerst, dass die beiden Folgen disjunkt sind. Nehme also an, es gelte $\lfloor \alpha m \rfloor = \lfloor \beta n \rfloor = q$. Dann gilt $q < \alpha m < q + 1$ sowie $q < \beta n < q + 1$, dabei stehen die strengen Ungleichheitszeichen, da α und β irrational sind. Folglich gilt

$$\frac{m}{q+1} < \frac{1}{\alpha} < \frac{m}{q}, \quad \frac{n}{q+1} < \frac{1}{\beta} < \frac{n}{q}.$$

Addition dieser Ungleichungen liefert

$$\frac{m+n}{q+1} < 1 < \frac{m+n}{q} \quad \Rightarrow \quad q < m+n < q+1,$$

was nicht möglich ist. Also gilt $\lfloor \alpha m \rfloor \neq \lfloor \beta n \rfloor$.

Nun zeigen wir, dass jede natürliche Zahl in einer der beiden Folgen vorkommt. Nehme an, die Zahl q komme nicht vor. Dann gibt es nichtnegative ganze Zahlen m und n mit

$$\alpha m < q < q+1 < \alpha(m+1), \quad \beta n < q < q+1 < \beta(n+1).$$

$$\frac{m}{q} < \frac{1}{\alpha} < \frac{m+1}{q+1}, \quad \frac{n}{q} < \frac{1}{\beta} < \frac{n+1}{q+1}.$$

Addition dieser Ungleichungen ergibt

$$\frac{m+n}{q} < 1 < \frac{m+n+2}{q+1} \Rightarrow m+n < q < q+1 < m+n+2.$$

Dies ist ein Widerspruch, da zwischen $m+n$ und $m+n+2$ keine zwei ganzen Zahlen Platz haben.

□

Beispiel 33. Zeige, dass die Folge $a_n = \lfloor n + \sqrt{n} + 1/2 \rfloor$ alle natürlichen Zahlen enthält, ausser die Quadratzahlen.

Lösung. Nehme an, m komme in der monotonen Folge a_n nicht vor. Dann gibt es eine natürliche Zahl n mit

$$n + \sqrt{n} + \frac{1}{2} < m < m+1 < n+1 + \sqrt{n+1} + \frac{1}{2}.$$

Daraus folgt der Reihe nach

$$\begin{aligned} \sqrt{n} &< m - n - \frac{1}{2} < \sqrt{n+1} \\ \Rightarrow n &< (m-n)^2 - (m-n) + \frac{1}{4} < n+1 \\ \Rightarrow n - \frac{1}{4} &< (m-n)^2 - (m-n) < n + \frac{3}{4}, \end{aligned}$$

und daher $(m-n)^2 - (m-n) = n$, also ist $m = (m-n)^2$ eine Quadratzahl. Der Beweis wird nun durch ein einfaches Zählargument abgeschlossen. Es gibt genau k positive Quadratzahlen $\leq k^2 + k$ und genau k^2 Zahlen der Form $\lfloor n + \sqrt{n} + 1/2 \rfloor$. Also ist $\lfloor n + \sqrt{n} + 1/2 \rfloor$ die n -te Nichtquadratzahl.

□

Es gibt einige Grössen, die sich bequem mit Hilfe der Gaussklammer hinschreiben lassen.

- Die Anzahl natürlicher Zahlen $\leq n$, die durch a teilbar sind, ist gleich $\lfloor \frac{n}{a} \rfloor$.
- Sei p eine Primzahl. Die grösste p -Potenz, die $n!$ teilt, ist gleich

$$\left\lfloor \frac{n}{p} \right\rfloor + \left\lfloor \frac{n}{p^2} \right\rfloor + \left\lfloor \frac{n}{p^3} \right\rfloor + \dots$$

Denn es gibt genau $\lfloor \frac{n}{p} \rfloor$ Vielfache von p , die $\leq n$ sind. Jede dieser Zahlen liefert einen Faktor p in der Primfaktorzerlegung von $n!$. Nun sind aber genau $\lfloor \frac{n}{p^2} \rfloor$ dieser Zahlen sogar durch p^2 teilbar und liefern einen weiteren Faktor p , usw.

Natürlich ist die Gaussklammer nicht additiv, das heisst, im Allgemeinen ist $\lfloor x+y \rfloor \neq \lfloor x \rfloor + \lfloor y \rfloor$. Es gelten jedoch die wichtigen Hermiteschen Identitäten:

Satz 5.1. Für jede natürliche Zahl n und jede reelle Zahl x gilt

$$\lfloor nx \rfloor = \lfloor x \rfloor + \left\lfloor x + \frac{1}{n} \right\rfloor + \left\lfloor x + \frac{2}{n} \right\rfloor + \dots + \left\lfloor x + \frac{n-1}{n} \right\rfloor.$$

Beweis. Wähle k so, dass gilt $k/n \leq \{x\} < (k+1)/n$. Die linke Seite hat dann den Wert $n[x] + k$. Auf der rechten Seite haben die ersten $n-k$ Summanden den Wert $[x]$, die übrigen k den Wert $[x] + 1$. Daraus folgt die Behauptung. □

Aufgaben

1. (APMO 01) Bestimme die grösste natürliche Zahl n , sodass die Anzahl natürlicher Zahlen $\leq n$, die durch 3 teilbar sind, gleich der Anzahl der natürlichen Zahlen $\leq n$ ist, die durch 5 oder 7 (oder beides) teilbar sind.
2. $2^n \nmid n!$.
3. (England 01) Definiere die Folge a_n durch

$$a_n = n + \lfloor \sqrt{n} \rfloor,$$

wobei $[x]$ die ganze Zahl bezeichnet, die am nächsten bei x liegt. Bestimme die kleinste natürliche Zahl k , sodass $a_k, a_{k+1}, \dots, a_{k+2000}$ eine Folge von 2001 aufeinanderfolgenden natürlichen Zahlen ist.

4. (Ibero 97) Sei $a \geq 1$ eine reelle Zahl mit folgender Eigenschaft: Ist m ein Teiler von n , dann ist $\lfloor am \rfloor$ ein Teiler von $\lfloor an \rfloor$. Zeige, dass a eine ganze Zahl ist.
5. (Balkan 98) Wieviele verschiedene ganze Zahlen können in der Form $\lfloor n^2/1998 \rfloor$ geschrieben werden für $n = 1, 2, \dots, 1997$?
6. (IMO 68) Sei n eine natürliche Zahl. Finde den Wert der Summe

$$\left\lfloor \frac{n+1}{2} \right\rfloor + \left\lfloor \frac{n+2}{4} \right\rfloor + \left\lfloor \frac{n+4}{8} \right\rfloor + \dots + \left\lfloor \frac{n+2^k}{2^{k+1}} \right\rfloor + \dots$$

7. (USA 97) Sei p_1, p_2, p_3, \dots die Folge der Primzahlen in aufsteigender Reihenfolge und sei x_0 eine reelle Zahl zwischen 0 und 1. Definiere für $k > 0$

$$x_k = \begin{cases} 0 & \text{wenn } x_{k-1} = 0 \\ \left\{ \frac{p_k}{x_{k-1}} \right\} & \text{wenn } x_{k-1} \neq 0 \end{cases}$$

Bestimme alle Werte von x_0 , für die die Folge irgendwann identisch 0 wird.

8. (Australien 92) Sei n eine natürliche Zahl. Finde die Anzahl reeller x mit $1 \leq x < n$, sodass gilt $x^3 = \lfloor x^3 \rfloor + (x - \lfloor x \rfloor)^3$.
9. (Australien 93) Finde alle natürlichen Zahlen n , sodass folgende Gleichung gilt:

$$\lfloor 2\sqrt{n} \rfloor = \lfloor \sqrt{n-1} + \sqrt{n+1} \rfloor + 1.$$

10. (Shortlist 96) Finde alle natürlichen Zahlen m und n , sodass gilt

$$\lfloor m^2/n \rfloor + \lfloor n^2/m \rfloor = \lfloor m/n + n/m \rfloor + mn.$$

6 IMO Aufgaben

1. (IMO 67) Seien k, m, n natürliche Zahlen, sodass $m + k + 1$ eine Primzahl grösser als $n + 1$ ist. Sei $c_s = s(s + 1)$. Zeige, dass

$$(c_{m+1} - c_k)(c_{m+2} - c_k) \cdots (c_{m+n} - c_k)$$

durch das Produkt $c_1 c_2 \cdots c_n$ teilbar ist.

2. (IMO 68) Finde alle natürlichen Zahlen n , sodass das Produkt der Ziffern von n im Dezimalsystem gleich $n^2 - 10n - 22$ ist.
3. (IMO 71) Zeige, dass es unendlich viele natürliche Zahlen der Form $2^n - 3$ gibt, die paarweise teilerfremd sind.
4. (IMO 74) Zeige, dass $\sum_{k=0}^n \binom{2n+1}{2k+1} 2^{3k}$ nie durch 5 teilbar ist.
5. (IMO 76) Finde die grösste Zahl, die sich als Produkt von natürlichen Zahlen mit Summe 1976 schreiben lässt.
6. (IMO 77) Sei $n > 2$ ganz. V_n sei die Menge der Zahlen $1 + kn$, wobei k eine natürliche Zahl ist. Eine Zahl in V_n heisst *unzerlegbar*, falls man sie nicht als Produkt von zwei Zahlen aus V_n schreiben kann. Zeige, dass es in V_n eine Zahl gibt, die sich auf mehr als eine Art schreiben lässt als Produkt von unzerlegbaren Zahlen aus V_n (Zerlegungen, die sich nur um die Reihenfolge der Faktoren unterscheiden, werden als gleich betrachtet).
7. (IMO 77) Seien a und b natürliche Zahlen. Wird $a^2 + b^2$ durch $a + b$ geteilt, dann ist der q der Quotient und r der Rest. Finde alle Paare (a, b) , sodass gilt $q^2 + r = 1977$.
8. (IMO 79) Seien m und n natürliche Zahlen, sodass

$$\frac{m}{n} = 1 - \frac{1}{2} + \frac{1}{3} - \frac{1}{4} + \cdots - \frac{1}{1318} + \frac{1}{1319}.$$

Zeige, dass m durch 1979 teilbar ist.

9. (IMO 81) Finde den grösstmöglichen Wert von $m^2 + n^2$, wobei m und n natürliche Zahlen ≤ 1981 sind, sodass gilt $(n^2 - mn - m^2)^2 = 1$.
10. (IMO 82) Sei n eine natürliche Zahl. Zeige, dass wenn die Gleichung

$$x^3 - 3xy^2 + y^3 = n$$

eine ganzzahlige Lösung x, y besitzt, dann besitzt sie mindestens drei solche Lösungen. Zeige, dass sie keine Lösung besitzt für $n = 2891$.

11. (IMO 83) Seien a, b, c natürliche Zahlen, die paarweise teilerfremd sind. Zeige, dass

$$2abc - ab - bc - ca$$

die grösste natürliche Zahl ist, die sich nicht in der Form $xab + ybc + zca$ mit nichtnegativen ganzen Zahlen x, y, z schreiben lässt.

12. (IMO 84) Finde ein Paar natürlicher Zahlen a, b , sodass $ab(a + b)$ nicht durch 7 teilbar ist, aber

$$(a + b)^7 - a^7 - b^7$$

durch 7^7 teilbar ist.

13. (IMO 84) Seien a, b, c, d ungerade ganze Zahlen mit $0 < a < b < c < d$ und $ad = bc$. Nehme an, es gibt natürliche Zahlen k, m , sodass gilt $a + d = 2^k$ und $b + c = 2^m$. Zeige, dass $a = 1$.
14. (IMO 85) Sei M eine Menge von 1985 natürlichen Zahlen, von denen keine einen Primteiler > 23 besitzt. Zeige, dass man vier verschiedene Zahlen aus M auswählen kann, deren Produkt eine vierte Potenz ist.
15. (IMO 87) Sei $n \geq 2$ eine ganze Zahl. Man beweise: Wenn $k^2 + k + n$ für alle ganzen Zahlen k mit $0 \leq k \leq \sqrt{\frac{n}{3}}$ eine Primzahl ist, dann ist $k^2 + k + n$ für alle ganzen Zahlen k mit $0 \leq k \leq n - 2$ eine Primzahl.
16. (IMO 88) Es seien a und b positive ganze Zahlen. Zeige, dass wenn

$$\frac{a^2 + b^2}{ab + 1}$$

eine ganze Zahl ist, dann ist es eine Quadratzahl.

17. (IMO 90) Man bestimme alle natürlichen Zahlen $n > 1$, für die $\frac{2^n + 1}{n^2}$ eine ganze Zahl ist.
18. (IMO 90) Zu Beginn ist eine ganze Zahl $n_0 > 1$ gegeben. Zwei Spieler A und B wählen abwechselnd ganze Zahlen n_1, n_2, n_3, \dots nach den folgenden Regeln:
 Nach der k -ten Runde kennt A die Zahl n_{2k} und wählt n_{2k+1} so, dass die Ungleichungen $n_{2k} \leq n_{2k+1} \leq n_{2k}^2$ gelten.
 Kennt nun B die Zahl n_{2k+1} , dann wählt er n_{2k+2} so, dass $\frac{n_{2k+1}}{n_{2k+2}} = p^r$ gilt, wobei p eine Primzahl und $r \geq 1$ eine natürliche Zahl ist.
 Spieler A gewinnt das Spiel, sobald er die Zahl 1990, B gewinnt, sobald er die Zahl 1 wählt.
 Für welche Werte von n_0 kann
- A einen Gewinn erzwingen,
 - B einen Gewinn erzwingen,
 - keiner der beiden Spieler einen Gewinn erzwingen?

19. (IMO 91) Es sei $S = \{1, 2, 3, \dots, 280\}$. Bestimme die kleinste natürliche Zahl n mit folgender Eigenschaft: In jeder n -elementigen Teilmenge von S gibt es 5 Elemente, die paarweise teilerfremd sind.
20. (IMO 91) Sei $n > 6$ eine natürliche Zahl und a_1, a_2, \dots, a_k diejenigen natürlichen Zahlen, die kleiner als n und teilerfremd zu n sind. Es gelte

$$a_2 - a_1 = a_3 - a_2 = \dots = a_k - a_{k-1} > 0.$$

Zeige, dass n entweder eine Primzahl oder eine Zweierpotenz ist.

21. (IMO 92) Für jede natürliche Zahl n bezeichne $s(n)$ die grösste ganze Zahl, für die gilt:
 Für jede ganze Zahl k , $1 \leq k \leq s(n)$ lässt sich n^2 als Summe von genau k Quadraten schreiben.
- Zeige, dass gilt $s(n) \leq n^2 - 14$ für alle $n \geq 4$.

(b) Finde eine natürliche Zahl n mit $s(n) = n^2 - 14$.

(c) Zeige, dass es unendlich viele natürliche Zahlen n gibt mit $s(n) = n^2 - 14$.

22. (IMO 94) Für eine natürliche Zahl k sei $f(k)$ die Anzahl Elemente in der Menge $\{k + 1, k + 2, \dots, 2k\}$, deren Binärdarstellung genau drei Einsen enthält.

(a) Zeige: Zu jeder natürlichen Zahl n gibt es mindestens ein k mit $f(k) = n$.

(b) Finde alle natürlichen Zahlen n , für die es genau ein k gibt mit $f(k) = n$.

23. (IMO 94) Man zeige, dass es eine Menge A natürlicher Zahlen mit folgender Eigenschaft gibt:

Zu jeder unendlichen Menge S von Primzahlen gibt es ein $k \geq 2$ und es existieren zwei natürliche Zahlen $m \in A$ und $n \notin A$, sodass jede dieser beiden Zahlen ein Produkt von k verschiedenen Elementen aus S ist.

24. (IMO 97) Finde alle ganzen Zahlen $a, b \geq 1$, sodass gilt $a^{b^2} = b^a$.

25. (IMO 98) Für jede natürliche Zahl n bezeichne $d(n)$ die Anzahl positiver Teiler von n . Finde alle natürlichen Zahlen k , für die es ein n gibt mit

$$\frac{d(n^2)}{d(n)} = k.$$

26. (IMO 99) Man bestimme alle Paare (n, p) natürlicher Zahlen, sodass gilt:

- p ist eine Primzahl,
- $n \leq 2p$,
- $(p - 1)^n + 1$ ist durch n^{p-1} teilbar.

27. (IMO 2000) Entscheide, ob es eine natürliche Zahl n gibt, sodass n genau 2000 verschiedene Primteiler besitzt und n ein Teiler ist von $2^n + 1$.

28. (IMO 01) Seien $a > b > c > d$ positive ganze Zahlen mit

$$ac + bd = (b + d + a - c)(b + d - a + c).$$

Zeige, dass $ab + cd$ keine Primzahl ist.

29. (IMO 02) Finde alle Paare $m, n \geq 3$ natürlicher Zahlen, sodass unendlich viele natürliche Zahlen a existieren, für die

$$\frac{a^m + a - 1}{a^n + a^2 - 1}$$

eine ganze Zahl ist.

30. (IMO 02) Sei $n \geq 2$ eine ganze Zahl mit positiven Teilern $1 = d_1 < d_2 < \dots < d_k = n$. Sei $D = d_1 d_2 + d_2 d_3 + \dots + d_{k-1} d_k$.

(a) Zeige, dass für alle n gilt $D \leq n^2$.

(b) Finde alle n , für die D ein Teiler ist von n^2 .

31. (IMO 03) Finde alle Paare (a, b) natürlicher Zahlen, sodass

$$\frac{a^2}{2ab^2 - b^3 + 1}$$

eine ganze Zahl ist.

32. (IMO 03) Sei p eine Primzahl. Zeige, dass es eine Primzahl q gibt, sodass für alle ganzen Zahlen n die Zahl $n^p - p$ nicht durch q teilbar ist.