Zahlentheorie II

Thomas Huber

Aktualisiert: 1. August 2016
vers. 1.2.1

Inhaltsverzeichnis

1 Kongruenzen I

1.1 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,

$$a = km + r,$$
$$b = lm + s,$$

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 $0, 1, \ldots, m-1$ *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 1.1. *Seien a, b, c, d ganze Zahlen mit $a \equiv c$ und $b \equiv d\ (m)$, dann gilt*

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

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 $a + b \equiv c + d\ (m)$. Analog zeigt man $a - b \equiv c - d\ (m)$. Es gilt weiter

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

folglich $ab \equiv cd\ (m)$. □

Als direkte Konsequenz ergibt sich auch noch die folgende Rechenregel:

$$a \equiv b \quad (m) \quad \Longrightarrow \quad a^k \equiv b^k \quad (m), \qquad k \in \mathbb{N}.$$

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

$$k \equiv l \quad (m) \quad \not\Longrightarrow \quad a^k \equiv a^l \quad (m)$$

Zum Beispiel ist $1 \equiv 4$ (3), aber $2^1 \not\equiv 2^4$ (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 1.2. *Ist c teilerfremd zu m, dann kann man Kongruenzen mit c kürzen:*

$$ca \equiv cb \quad (m) \quad \Longrightarrow \quad a \equiv b \quad (m).$$

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 1. *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 $c \equiv 2$ (3). Dann ist $a + b + c \equiv 0 + 1 + 2 \equiv 0$ (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 2 (England 2000)**.** *Zeige, dass für jede natürliche Zahl n*

$$121^n - 25^n + 1900^n - (-4)^n \tag{1}$$

durch 2000 *teilbar ist.*

Lösung. Wir zeigen, dass (1) durch 16 und durch 125 teilbar ist. Daraus folgt die Behauptung. Dazu berechnen wir den Ausdruck zuerst modulo 16. Es gilt $121 \equiv 25 \ (\equiv 9)$ (16), also auch $121^n \equiv 25^n$ (16). Ebenso ist $1900 \equiv -4$ (16), also $1900^n \equiv (-4)^n$ (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 $121 \equiv -4$ (125), also $121^n \equiv (-4)^n$ (125), sowie $1900 \equiv 25$ (125) und daher $1900^n \equiv 25^n$ (125). Insgesamt also wieder

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

□

Beispiel 3. *Sei n nicht durch 2 und nicht durch 5 teilbar. Zeige, dass es ein Vielfaches von n der Form $111\ldots11$ gibt.*

Lösung. Betrachte die Zahlen

$$\begin{matrix} 1 \\ 11 \\ 111 \\ \vdots \\ \underbrace{111\ldots11}_{n+1} \end{matrix} \qquad (\mathrm{mod}\ n)$$

Zwei dieser Zahlen müssen nach dem Schubfachprinzip dieselbe Restklasse modulo n haben. Deren Differenz ist dann durch n teilbar und von der Form $111\ldots11000\ldots00 = 10^r \cdot \underbrace{111\ldots11}_{s}$. Da n teilerfremd ist zu 10, ist n sogar ein Teiler von $\underbrace{111\ldots11}_{s}$. □

Beispiel 4. *(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 $(2+3)(2^{p-1} - 2^{p-2} \cdot 3 + \ldots - 2 \cdot 3^{p-2} + 3^{p-1})$ 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 $(2^{p-1} - 2^{p-2} \cdot 3 + \ldots - 2 \cdot 3^{p-2} + 3^{p-1})$ durch 5 teilbar sein. Wir berechnen diesen Ausdruck nun modulo 5 und verwenden dabei die Kongruenz $3 \equiv -2\ (5)$:

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

Da 2 und 5 teilerfremd sind, folgt daraus $p \equiv 0\ (5)$, 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 $n > 1$. □

1.2 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 1.1. Für eine natürliche Zahl m ist die Eulersche *φ-Funktion* definiert durch

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

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

Satz 1.3. *Die φ-Funktion besitzt folgende Eigenschaften:*

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

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

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

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

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 $1\le a\le m$, 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 1.4 (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 $a_1,a_2,\ldots,a_{\varphi(m)}$ die positiven Zahlen $<m$, die zu m teilerfremd sind. Betrachte die Zahlen $aa_1,aa_2,\ldots,aa_{\varphi(m)}$. Wir behaupten, dass sie eine Permutation der Zahlen $a_1,a_2,\ldots,a_{\varphi(m)}$ modulo m bilden. Da a und a_k teilerfremd sind zu m, gilt dies auch für aa_k. Nehme nun an, es gelte $aa_k\equiv aa_l\ (m)$, dann folgt $a_k\equiv a_l$, also $a_k=a_l$ wegen $1\le a_k,a_l\le m$. Also bilden die aa_k tatsächlich eine Permutation der a_k und daraus folgt nun

$$\begin{aligned}a_1a_2\cdots a_{\varphi(m)} &\equiv (aa_1)(aa_2)\cdots(aa_{\varphi(m)})\\ &\equiv a^{\varphi(m)}(a_1a_2\cdots a_{\varphi(m)})\\ \Longrightarrow\quad 1 &\equiv a^{\varphi(m)} \pmod{m}.\end{aligned}$$

□

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

Korollar 1.5 (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 5. *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 $5555 \equiv 4$ (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

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

Addition dieser beiden Kongruenzen ergibt die Behauptung. □

Beispiel 6. *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 $a^m + b^n \equiv a^{\varphi(b)} + 0 \equiv 1$ (b), da a und b teilerfremd sind. Analog gilt $a^m + b^n \equiv 0 + b^{\varphi(a)} \equiv 1$ (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 $a, a^2, a^3, \ldots$ 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 $a^{k+\varphi(m)} = a^k \cdot a^{\varphi(m)} \equiv a^k$ (m). Im Allgemeinen ist $\varphi(m)$ nicht die kleinstmögliche Periode, aber ein Vielfaches davon. Denn sei d die kleinste positive ganze Zahl mit $a^d \equiv 1$ (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 7. *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:

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

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

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

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

Beispiel 8. *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 $\pmod 8$, 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 9. *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. □

1.3 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 1.6 (Chinesischer Restsatz)**.** *Seien $m_1, m_2, \ldots, m_r$ paarweise teilerfremde natürliche Zahlen und $a_1, a_2, \ldots, a_r$ beliebig. Dann hat das System von Kongruenzen*

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

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

Beispiel 10. *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 $x \equiv 23$ (35) die einzige Lösung des Systems von Kongruenzen, im Einklang mit Satz 1.6 □

Beispiel 11. *(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 $p_1, p_2, \ldots, p_n$ und $q_1, q_2, \ldots, q_n$. Betrachte nun folgendes System:

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

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 $x{+}1, x{+}2 \ldots, x{+}n$ sind also keine Primpotenzen. □

1.4 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 12. *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 $\equiv 2$ (4), also gerade, dann gilt $x^2 \equiv 0$ (4). Ist $x \equiv 1$ oder $\equiv 3$ (4), also ungerade, dann folgt $x^2 \equiv 1$ (4). Ein Quadrat ist also immer $\equiv 0$ oder 1 (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 $\equiv 3$ (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:

(mod 3)

n	0	1	2
n^2	0	1	1

(mod 5)

n	0	1	2	3	4
n^2	0	1	4	4	1

(mod 4)

n	0	1	2	3
n^2	0	1	0	1

(mod 8)

n	0	1	2	3	4	5	6	7
n^2	0	1	4	1	0	1	4	1

(mod 16)

n	0	1	2	3	4	5	6	7	8
n^2	0	1	4	9	0	9	4	1	0

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 13 (Australien 01)**.** *Zeige, dass keine vier ganzen Zahlen x, y, z, w existieren mit*

$$x^2 = 10w - 1$$
$$y^2 = 13w - 1$$
$$z^2 = 85w - 1$$

Lösung. Nehme an, solche Zahlen existieren. Quadrate sind kongruent $0, 1, 4, 9$ modulo 16. Ist $w \equiv 0, 2, 3, 4, 6, 7, 8, 10, 11, 12, 14, 15$ (16), dann wäre nach der ersten Gleichung $x^2 \equiv 15, 3, 13, 7, 11, 5, 15, 3, 13, 7, 11, 5$ (16), ein Widerspruch. Ist $w \equiv 1, 13$ (16), dann folgt $y^2 \equiv 12, 8$ (16), was ebenfalls unmöglich ist. Ist schliesslich $w \equiv 5, 9$ (16), dann gilt $z^2 \equiv 8, 12$ (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 $a \not\equiv 1 \ (m)$ mit $a^k \equiv 1 \ (m)$. Nach dem Satz von Euler-Fermat, bzw. der darauf folgenden Diskussion auf Seite 6, 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^3	0	1	1	6	1	6	6

(mod 7)

n	0	1	2	3	4	5	6	7	8	9	10
n^3	0	1	8	5	9	4	7	2	6	3	10

(mod 11)

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

Beispiel 14 (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 $\equiv 0, 1, 3, 4, 5, 9 \ (11)$ und fünfte Potenzen $\equiv 0, 1, 10 \ (11)$ sind. Nehme an, die Gleichung habe eine Lösung (x, y). Dann ist die linke Seite der Gleichung $\equiv 0, 1, 3, 4, 5, 9$ (11) und die rechte Seite $\equiv 6, 7, 8 \ (11)$, Widerspruch. Die Gleichung besitzt also keine ganzzahligen Lösungen. □

2 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 erziehlen können.

Zur Erinnerung ein paar Fakten:

- $a \mid bc$ und $(a, b) = 1 \Longrightarrow a \mid c$
- 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.
- $a, b \in \mathbb{N},\ a \mid b \quad \Longrightarrow \quad a \leq b$

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

$$\boxed{(x+y)^n = \sum_{k=0}^{n} \binom{n}{k} x^k y^{n-k}}$$

Dabei sind x, y beliebige reele 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:

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

Diese nur für **ungerade** n:

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

Und die hier nur für **gerade** n:

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

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

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

Insbesondere ist eine Differenz zweier Quadrate immer faktorisierbar. 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**:

$$\boxed{x^4 + 4y^4 = (x^2 + 2xy + 2y^2)(x^2 - 2xy + 2y^2)}$$

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:

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

Jetzt ist aber Zeit für ein paar Beispiele.

Beispiel 15 (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 16. *Zeige, dass das Produkt von vier aufeinanderfolgenden natürlichen Zahlen keine Quadratzahl ist.*

Lösung. Es gilt

$$\begin{aligned} n(n+1)(n+2)(n+3) &= n^4 + 6n^3 + 11n^2 + 6n \\ &= n^2(n^2 + 3n + 1) + 3n(n^2 + 3n + 1) + (n^2 + 3n + 1) - 1 \\ &= (n^2 + 3n + 1)^2 - 1. \end{aligned}$$

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 17. *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:

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

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

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

wobei beide Faktoren grösser als 1 sind. Damit muss $v = 1$ und $n = 2^{2^s}$ sein. Für $s = 1$ erhalten wir $4^4 + 1 = 257$, 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 18 (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 19. *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 20. *Zeige, dass für alle positiven ganzen Zahlen $n > 1$ und a, b gilt*

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

Lösung. Sei $d = \mathrm{ggT}(a, b)$ und schreibe $a = dk$ und $b = dl$. Nun folgt mit den Binomischen Formeln $n^a - 1 = (n^d)^k - 1^k = (n^d - 1)(n^{d(k-1)} + n^{d(k-2)} + \ldots + n^d + 1)$, also ist $n^d - 1 \mid n^a - 1$. Die analoge Rechnung für b ergibt somit $n^d - 1 \mid \mathrm{ggT}(n^a - 1, n^b - 1)$.
Umgekehrt existieren nach Bézout 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 $\mathrm{ggT}(n^a - 1, n^b - 1)$ die linke Seite dieser Gleichung, also auch die rechte. Wegen $\mathrm{ggT}(n^{by}, n^b - 1) = 1$ teilt dies sogar $n^d - 1$. Insgesamt folgt also $\mathrm{ggT}(n^a - 1, n^b - 1) = n^{\mathrm{ggT}(a,b)} - 1$. □

3 Ziffern und Zahlsysteme

3.1 Zahlen und ihre Ziffern

Beispiel 21. *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. □

Beispiel 22. *Wir starten mit einer natürlichen Zahl* a_1 *und erzeugen damit eine Folge natürlicher Zahlen* $a_1, a_2, a_3, \ldots$ *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 Folgeglieder 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 viele 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 $1, 11, 111, \ldots, \underbrace{111\ldots11}_{p}$ durch p teilbar ist, denn $\mathrm{ggT}(p, 10) = 1$ (vergleiche Beispiel 3). Daher können wir nicht vermeiden, dass unendlich viele Folgeglieder zusammengesetzt sind. □

3.2 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 3.1. *Sind $b \geq 2$ und $x \geq 0$ ganze Zahlen, dann gibt es ein r und ganze Zahlen $a_0, a_1, \ldots, a_r$ mit $0 \leq a_k \leq b-1$, $0 \leq k \leq r$, sodass gilt*

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

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 $x = (a_r a_{r-1} \ldots a_1 a_0)_{(b)}$.

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

Algorithmus 3.2 (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 $x_{k+1} = \frac{x_k - a_k}{b}$. Ist dies $= 0$, dann beende den Algorithmus, sonst erhöhe k um 1 und gehe zu Schritt 2.*

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

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 23. *(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, $n = (x_r x_{r-1} \ldots x_0)_{(2)}$ und lese diese Zahl im Dreiersystem um a_n zu erhalten, setze also $a_n = (x_r x_{r-1} \ldots x_0)_{(3)}$. Man kann es auch anders sagen: wir nehmen diejenigen Zahlen, die im Dreiersystem geschrieben nur die Ziffern 0 und 1 haben. Nun ist

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

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 übereinsteimmen, also wenn $k = m$, Widerspruch. □

Beispiel 24. *Sei $f : \mathbb{N} \to \mathbb{N}$ 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 stimme 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 Induktionsvorraussetzung 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 $n = 1023 = 1111111111_{(2)}$. □