Zahlentheorie

Axel Schüler, Mathematisches Institut, Univ. Leipzig

mailto:schueler@mathematik.uni-leipzig.de

24.10.2002

Zur Zahlentheorie rechnen wir Aufgaben, die über dem Bereich $\mathbb{N} = \{1, 2, \dots\}$ der natürlichen oder über den ganzen Zahlen $\mathbb{Z} = \{0, \pm 1, \pm 2, \dots\}$ zu lösen sind. In vielen Olympiadeaufgaben kommen ganze oder natürliche Zahlen vor. Daher sollte man das entsprechende Handwerkszeug — die Eigenschaften des größten gemeinsamen Teilers und die Kongruenzrechnung — beherrschen und sicher anwenden können. Dies verkürzt lange Lösungswege enorm.

Die Grundgleichung der Zahlentheorie

Zu jeder ganzen Zahl a und jeder natürlichen Zahl m gibt es stets ein Paar q, r von ganzen Zahlen, so dass gilt:

$$a = qm + r \quad \text{mit} \quad 0 \le r < m \quad \textit{Grundgleichung der Zahlentheorie.}$$

Dabei heißt r der *kleinste Rest* zu gegebenem a und m.

Beispiel 1 Wenn $a = 8$ und $m = 5$, so sind $q = 1$ und $r = 3$, denn $8 = 1{\cdot}5 + 3$.
Wenn $a = 8$ und $m = 9$, so sind $q = 0$ und $r = 8$, denn $8 = 0{\cdot}9 + 8$.
Wenn $a = -5$ und $m = 3$, dann sind $q = -2$ und $r = 1$, denn $-5 = (-2)3 + 1$.

Diese Grundgleichung der Zahlentheorie, die man auch einfach als Division mit Rest bezeichnen kann, bildet die Grundlage für den EUKLIDischen Algorithmus zur Bestimmung des größten gemeinsamen Teilers zweier Zahlen a und b (siehe unten).

Teilbarkeitslehre

Man sagt, dass die ganze Zahl $a \in \mathbb{Z}$ durch die ganze Zahl $m \in \mathbb{Z}$ *teilbar* ist, wenn a ohne Rest durch m teilbar ist; d. h. es gibt ein $q \in \mathbb{Z}$ mit

$$a = qm.$$

Wir sagen m *teilt* a, symbolisch $m \mid a$.

Definition 1 Es seien $a, m \in \mathbb{Z}$. Dann gilt m *teilt* a, falls es eine ganze Zahl q gibt mit $a = qm$.

Als *Teiler* einer Zahl a betrachtet man üblicherweise nur die natürlichen Zahlen, die a teilen (nicht aber die negativen ganzen Zahlen, die a teilen).

Bemerkung 1 Null teilt keine ganze Zahl außer Null selbst. Jede ganze Zahl teilt aber die Null.

Satz 1 *Es seien a, b und c ganze Zahlen. Dann gilt*

1. *Wenn $a \mid b$ und $b \mid c$, dann auch $a \mid c$ (Transitivität der Teilbarkeitsbeziehung).*
2. *Wenn $a \mid b$ und $a \mid c$, so $a \mid (b + c)$.*
3. *Wenn $a \mid b$ und $a \mid (b + c)$, so $a \mid c$.*
4. *Wenn $a \mid b$ oder $a \mid c$, so $a \mid bc$.*
5. *Wenn $a \mid c$ und $b \mid c$ und a und b sind teilerfremd, so $ab \mid c$.*
6. *Wenn $ab \mid c$, so $a \mid c$ und $b \mid c$.*

Definition 2 Eine natürliche Zahl heißt *Primzahl*, wenn sie genau zwei verschiedene Teiler hat, nämlich 1 und sich selbst.

Satz 2 *(a) Jede natürliche Zahl größer als* 1 *ist entweder Primzahl oder sie lässt sich abgesehen von der Reihenfolge auf genau eine Art als Produkt von Primzahlen schreiben.*
(b) Es gibt unendlich viele Primzahlen.

Der größte gemeinsame Teiler

Definition 3 Die natürliche Zahl d heißt größter gemeinsamer Teiler der ganzen Zahlen a und b, falls gilt:

(a) $d \mid a$ und $d \mid b$ und
(b) für alle $t \in \mathbb{Z}$ gilt, wenn $t \mid a$ und $t \mid b$, so $t \mid d$.

Symbolisch schreiben wir dafür $d = (a, b)$.

Man kann sich die Eigenschaft (b) leicht mit Hilfe der *Menge der gemeinsamen Teiler* veranschaulichen. Die Menge der gemeinsamen Teiler von $a = 48$ und $b = 60$ ist

$$\{1, 2, 3, 4, 6, 12\}.$$

Tatsächlich gilt für $t = 1, 2, 3, 4, 6$ und 12, dass $t \mid 12$ erfüllt ist. Also ist 12 der größte gemeinsame Teiler. Natürlich ist 12 auch „größer“ als alle anderen Teiler. Doch die *Größerrelation* soll hier keine Rolle spielen, sondern ausschließlich die Teilbarkeitsrelation.
Der größte gemeinsame Teiler (ggT) zweier Zahlen ist also derjenige gemeinsame Teiler, der von allen anderen gemeinsamen Teilern geteilt wird. Das Wesen des EUKLIDischen Algorithmus zur Bestimmung des ggT liegt in der simplen Formel

$$(a, b) = (a - b, b),$$

die man anhand der obigen Definition leicht nachweist (Wie? — Zeige dass die beiden Mengen der gemeinsamen Teiler übereinstimmen!). Es sei $a > b > 0$, dann kann man die obige Differenzbildung so lange fortsetzen bis $a - b - b - \cdots - b < b$. Dies entspricht aber gerade der Division von a durch b mit Rest, $a = q \cdot b + r$ und wir haben gezeigt, dass gilt

$$(a, b) = (a - b, b) = (a - 2b, b) = \cdots = (a - qb, b) = (r, b).$$

Nun ist r die kleinere Zahl und man kann r solange von b abziehen, bis der Rest $b - r - r \cdots - r$ kleiner als r ist usw. Als Ergenbis erhalten wir immer kleinere Zahlen bis schließlich die Division aufgeht und wir haben dann $(a, b) = \cdots = (d, 0) = d$. Verfolgt man die Rechnung zurück, so erkennt man außerdem, dass sich d ganzzahlig aus a und b kombinieren lässt, das heißt, es existieren A, $B \in \mathbb{Z}$ mit

$$d = Aa + Bb. \tag{1}$$

Beispiel 2 Bestimmung von $(87, 51)$.

$$(87, 51) = (87 - 51, 51) = (36, 51) = (36, 15) = (36 - 2 \cdot 15, 15) = (6, 15) = (6, 3) = 3.$$

Das selbe als Divisionsschema:

$$\begin{aligned} 87 &= 1 \cdot 51 + 36, & 36 &= 87 - 1 \cdot 51, \\ 51 &= 1 \cdot 36 + 15, & 15 &= 51 - 1 \cdot 36, \\ 36 &= 2 \cdot 15 + 6, & 6 &= 36 - 2 \cdot 15, \\ 15 &= 2 \cdot 6 + \underline{3}, & 3 &= 15 - 2 \cdot 6, \\ 6 &= 2 \cdot 3, \end{aligned}$$

Setzt man nun nacheinander von oben nach unten die rechten Seiten des obigen Systems ineinander ein, so erhält man schrittweise $15 = 2 \cdot 51 - 87$, $6 = 3 \cdot 87 - 5 \cdot 51$ und schließlich $3 = 12 \cdot 51 - 7 \cdot 87$.

Tatsächlich hat unter allen gemeinsamen Teilern von a und b nur der ggT (a, b) eine Darstellung wie in (1). Dies zeigt man wieder einfach mit der obigen Definition des ggT (Wie?). Insbesondere sind a und b genau dann teilerfremd, wenn es ganze Zahlen A und B gibt mit $1 = Aa + Bb$.

Satz 3 *Es seien $a, b \in \mathbb{Z}$. Dann gilt $d = (a, b)$ genau dann, wenn*

(a) *$d \mid a$ und $d \mid b$ und*
(b) *Es gibt ganze Zahlen A und B mit $d = Aa + Bb$.*

Die ganzen Zahlen a und b sind genau dann teilerfremd, d. h. $(a, b) = 1$, wenn es ganze Zahlen A und B gibt mit $1 = Aa + Bb$.

Das allgemeine Schema des EUKLIDischen Algorithmus lautet:

$$\begin{aligned}
a &= bq_1 + r_2, & 0 < r_2 < b,\\
b &= r_2q_2 + r_3, & 0 < r_3 < r_2,\\
r_2 &= r_3q_3 + r_4, & 0 < r_4 < r_3,\\
&\dots\\
r_{n-2} &= r_{n-1}q_{n-1} + \underline{r_n}, & 0 < r_n < r_{n-1},\\
r_{n-1} &= r_nq_n.
\end{aligned}$$

Der letzte auftretende Rest ist 0 und der ggT ist der letzte von Null verschiedene Rest. Wir haben also

$$(a, b) = (b, r_2) = (r_2, r_3) = \cdots = (r_{n-1}, r_n) = r_n.$$

Aufgabe 1 Bestimme $(1573, 637)$ und stelle den ggT als ganzzahlige Linearkombination von 1576 und 637 dar!

Lösung:

$$\begin{aligned}
1573 &= 637 \cdot 2 + 299, & 299 &= 1573 - 637 \cdot 2,\\
637 &= 299 \cdot 2 + 39, & 39 &= 637 - 299 \cdot 2,\\
299 &= 39 \cdot 7 + 26, & 26 &= 299 - 39 \cdot 7,\\
39 &= 26 \cdot 1 + \underline{13}, & 13 &= 39 - 26 \cdot 1,\\
26 &= 13 \cdot 2.
\end{aligned}$$

Die schrittweise Rückrechnung liefert die Darstellung des ggT als Linearkombination von a nud b:

$$\begin{aligned}
13 &= 39 - 299 + 39 \cdot 7 &&= 39 \cdot 8 - 299,\\
&= (637 - 299 \cdot 2) \cdot 8 - 299 &&= 637 \cdot 8 - 299 \cdot 17,\\
&= 637 \cdot 8 - (1573 - 637 \cdot 2) \cdot 17 &&= 637 \cdot 42 - 1573 \cdot 17.
\end{aligned}$$

Aufgabe 2 Mit Hilfe des EUKLIDischen Algorithmus bestimme man den größten gemeinsamen Teiler von 6188 und 4709 und stelle ihn als ganzzahlige Linearkombination von 6188 und 4709 dar.

Satz 4 *Eigenschaften des größten gemeinsamen Teilers:*

$$\begin{aligned}
(n, ab) &= (n, b), & &\textit{falls} \quad (n, a) = 1,\\
n \mid ab &\Rightarrow n \mid b, & &\textit{falls} \quad (n, a) = 1,\\
(a, m) \cdot (a, n) &\mid (a, mn), & &\textit{falls} \quad (m, n) = 1,\\
\textit{Wenn} \quad (a, b) &= d, & &\textit{so} \quad (a/d, b/d) = 1.
\end{aligned}$$

Rechnen mit Kongruenzen

Es sei m eine feste natürliche Zahl. Für zwei ganze Zahlen a und b schreiben wir

$$a \equiv b \pmod{m} \quad \text{sprich: „}a \text{ ist kongruent } b \text{ modulo } m\text{“},$$

falls

$$m \mid (b - a)$$

oder anders ausgedrückt, es gibt ein $q \in \mathbb{Z}$ mit $a = b + qm$. Mit anderen Worten: a ist kongruent b modulo m, wenn a und b bei der Division durch m den selben Rest lassen.

Beispiel 3 $73 \equiv 38 \pmod{7}$, weil $7 \mid (73 - 38)$, d. h. $7 \mid 35$.
$29 \equiv -59 \pmod{1}1$, weil $11 \mid (29 + 59)$, d. h. $11 \mid 88$.
Man schreibt auch $71 \equiv 23 \equiv 7 \equiv -1 \equiv -9 \pmod{8}$, weil alle diese Zahlen bei Division durch 8 den selben Rest lassen.
Nach Definition ist $a \equiv 0 \pmod{m}$ gleichbedeutend mit $m \mid a$.

Zum Beweis von Eigenschaften von Kongruenzen ist es wichtig, dass man sie in Gleichungen zurück verwandeln kann: $a \equiv b \pmod{m}$ heißt, dass es eine ganze Zahl $q \in \mathbb{Z}$ gibt mit $a = qm + b$.

Eigenschaften von Kongruenzen

Satz 5 *Es sei $m \in \mathbb{N}$ eine natürliche Zahl und es seien $a, b, c \in \mathbb{Z}$ ganze Zahlen. Dann gilt:*
$a \equiv a \pmod{m}$ *(Reflexivität).*
Wenn $a \equiv b \pmod{m}$, *dann* $b \equiv a \pmod{m}$ *(Symmetrie).*
Wenn $a \equiv b \pmod{m}$ *und* $b \equiv c \pmod{m}$, *dann* $a \equiv c \pmod{m}$ *(Transitivität).*

Beweise diese Eigenschaften! Benutze den obigen Hinweis!
Man überzeugt sich leicht davon, dass die folgenden Rechenregeln gelten:

Satz 6 *(a) Es seien $a, b, c, d \in \mathbb{Z}$, $m, n \in \mathbb{N}$ und*

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

Dann gilt:

$$a \pm c \equiv b \pm d \pmod{m},$$
$$ac \equiv bd \pmod{m},$$
$$a^n \equiv b^n \pmod{m},$$
$$an \equiv bn \pmod{mn}.$$

(b) Es sei p eine Primzahl und $a, b, c \in \mathbb{Z}$.

$$\text{Wenn} \quad ab \equiv 0 \pmod{p}, \quad \text{dann gilt} \quad a \equiv 0 \pmod{p} \quad \text{oder} \quad b \equiv 0 \pmod{p},$$
$$\text{Wenn} \quad an \equiv bn \pmod{mn}, \quad \text{dann} \quad a \equiv b \pmod{m}. \tag{2}$$
$$\text{Wenn} \quad ac \equiv bc \pmod{m} \quad \text{und} \quad (c, m) = d, \quad \text{so} \quad a \equiv b \pmod{m/d} \tag{3}$$
$$\text{Wenn} \quad ac \equiv bc \pmod{m} \quad \text{und} \quad (c, m) = 1, \quad \text{so} \quad a \equiv b \pmod{m}. \tag{4}$$

Beweisskizze. Als Beispiel beweisen wir die zweite Behauptung von (a) . Die Voraussetzungen besagen, dass es ganze Zahlen p und q gibt mit

$$a = pm + b \quad \text{und} \quad c = qm + d.$$

Multipliziert man diese beiden Gleichungen miteinander, so hat man

$$ac = pqm^2 + pmd + qmb + bd = m(pqm + pd + qb) + bd.$$

Die bedeutet aber, dass es eine ganze Zahl $r = pqm + pd + qb$ gibt mit $ac = mr + bd$ oder $ac \equiv bd \pmod{m}$, was zu zeigen war. Wir zeigen (4): Wegen $(m, c) = 1$ gibt es ganze Zahlen A und B mit

$$cA + mB = 1 \quad \text{(Charakterisierung der Teilerfremdheit).}$$

Multipliziert man diese Gleichung mit $a-b$ und beachtet, dass nach Voraussetzung $m \mid (a-b)c$ gilt, also ein $q \in \mathbb{Z}$ existiert mit $(a-b)c = qm$, so hat man

$$\begin{aligned} (a-b)cA + (a-b)mB &= a-b \\ qmA + (a-b)mB &= a-b \\ m(qA + (a-b)B) &= a-b. \end{aligned}$$

Das heißt aber $a \equiv b \pmod{m}$. Die Behauptung (3) folgt nun, wenn man beachtet, dass $(c/d, m/d) = 1$ genau dann, wenn $(c, m) = d$ gilt und außerdem (2) benutzt (was sehr leicht zu zeigen ist).

Man beachte, dass man eine Kongruenz nur dann durch die ganze Zahl c kürzen darf — bei unverändertem Modul m —, wenn c und der Modul m teilerfremd sind. Beispiele zu den letzten beiden Eigenschaften:

$45 \equiv 27 \pmod{6}$ und $(9, 6) = 3$, also $5 \equiv 3 \pmod{2}$ (Division durch 9).

$72 \equiv 27 \pmod{5}$ und $(9, 5) = 1$, also $8 \equiv 3 \pmod{5}$ (Division durch 9).

Beispiel 4 1. Auf welche Ziffer endet 7^7? *Lösung.* Man erhält die letzte Ziffer einer Zahl, wenn man sie modulo 10 betrachtet. So ist zum Beispiel $1234 \equiv 44 \equiv 64 \equiv 2004 \equiv 4 \pmod{10}$, da alle diese Zahlen auf 4 enden. Wir gehen schrittweise vor und multiplizieren die vorangegangene Kongruenz immer weiter mit 7:

$$\begin{aligned} &7^1 \equiv 7 \pmod{10}, && 7^2 \equiv 49 \equiv 9 \pmod{10} \\ &7^3 \equiv 9 \cdot 7 \equiv 3 \pmod{10}, && 7^4 \equiv 3 \cdot 7 \equiv 1 \pmod{10} \\ &7^7 \equiv 7^4 \cdot 7^3 \equiv 3 \cdot 1 \equiv 3 \pmod{10}. \end{aligned}$$

Also endet 7^7 auf 3.

2. Auf welche Ziffer endet 999^{999}? Es gilt

$$999^{999} \equiv 9^{999} \equiv (-1)^{999} \equiv -1 \equiv 9 \pmod{10}.$$

3. Ist $21^{39} + 39^{21}$ durch 45 teilbar?

Lösung: Eine Zahl ist durch 45 teilbar genau dann, wenn sie durch 5 und durch 9 teilbar ist. Wir betrachten die Teilbarkeit von $z = 21^{39} + 39^2$ durch 9 ohne Kongruenzrechnung. Offenbar

sind 21 und 39 beide durch 3 teilbar, also sind 21^2 und 39^2 beide durch 9 teilbar und somit auch die höheren Potenzen. Also ist $9 \mid z$. Ferner gilt

$$21^{39} + 39^{21} \equiv 1^{39} + (-1)^{21} \equiv 1 + (-1) \equiv 0 \pmod{10}.$$

Also ist auch $9 \mid z$ und somit $45 \mid z$.

Beispiel 5 (9er- und 11er-Regel) Für eine natürliche Zahl $z = \overline{a_n a_{n-1} \cdots a_1 a_0}$ sei

$$A(z) = a_0 - a_1 + a_2 - + \cdots + (-1)^n a_n$$

die alternierende Quersumme; die Quersumme sei $Q(z) = a_0 + \cdots + a_n$. Dann gilt:

$$z \equiv Q(z) \pmod 9 \qquad \text{und} \quad z \equiv A(z) \pmod{11}$$

Insbesondere gilt $9|z$ genau dann, wenn $9|Q(z)$ und $11|z$ genau dann, wenn $11|A(z)$.
Lösung: Es gilt im Dezimalsystem:

$$z = \overline{a_n a_{n-1} \cdots a_1 a_0} = 10^n a_n + 10^{n-1} a_{n-1} + \cdots + 10a_1 + a_0.$$

Betrachtet man diese Gleichung modulo 9 und beachtet dabei, dass für alle $k \in \mathbb{N}$ gilt $10^k \equiv 1^k \equiv 1 \pmod 9$, so hat man

$$z \equiv a_n + a_{n-1} + \cdots + a_1 + a_0 = Q(z) \pmod 9.$$

Beachtet man dagegen $10^k \equiv (-1)^k \pmod{11}$ und betrachtet die obige Gleichung modulo 11, so hat man

$$z \equiv (-1)^n a_n + (-1)^{n-1} a_{n-1} + \cdots - a_1 + a_0 \equiv A(z) \pmod{11}.$$

Die zweite Behauptung folgt nun einfach aus der Transitivität der Kongruenzrelation: Wenn $9 \mid Q(z)$, so $Q(z) \equiv 0 \pmod 9$. Also ist $z \equiv 0 \pmod 9$ und somit $9 \mid z$. Die Umkehrung folgt analog und auch der Beweis für die 11er-Regel.

Beispiel 6 Überprüfe die Richtigkeit der folgenden Rechnungen modulo 9 und modulo 11!
$z = 24^4 \cdot 12 + 17^3 \cdot 21 + 32^5 \cdot 4 = 138302213$
Lösung: Wir benutzen die Quersumme bei der 9er-Regel:

$$\begin{aligned} z &\equiv 6^4 \cdot 3 + 8^3 \cdot 3 + 5^5 \cdot 4 \stackrel{?}{\equiv} 1 + 3 + 8 + 3 + 2 + 2 + 1 + 3 \pmod 9 \\ &\equiv 36^2 \cdot 3 + (-1)^3 \cdot 3 + 25 \cdot 125 \cdot 4 \stackrel{?}{\equiv} 5 \pmod 9 \\ &\equiv 0 + (-1) \cdot 3 + 7 \cdot 8 \cdot 4 \stackrel{?}{\equiv} 5 \pmod 9 \\ &\equiv 0 - 3 + 7 \cdot (-1) \cdot 4 \equiv -3 - 28 \equiv -4 \stackrel{?}{\equiv} 5 \pmod 9 \end{aligned}$$

Die Kongruenz modulo 9 ist erfüllt. Wir benutzen die alternierende Quersumme fürs Überprüfen modulo 11:

$$\begin{aligned} z &\equiv 2^4 \cdot 1 + 6^3 \cdot (-1) + (-1)^5 \cdot 4 \stackrel{?}{\equiv} 3 - 1 + 2 - 2 + 0 - 3 + 8 - 3 + 1 \pmod{11} \\ &\equiv 5 + 36 \cdot 6 \cdot (-1) - 4 \stackrel{?}{\equiv} 5 \pmod{11} \\ &\equiv 5 - 18 - 4 \equiv -17 \equiv 5 \stackrel{?}{\equiv} 5 \pmod{11} \end{aligned}$$

Die Kongruenz modulo 11 ist ebenfalls erfüllt. Die Gleichung könnte also richtig sein. (Sie ist es!)

Beispiel 7 (7er-Regel) Es sei n eine natürliche Zahl. Trennt man von n die letzte Ziffer ab, multipliziert sie mit 2 und subtrahiert das Ergebnis vom verbliebenen Teil von n, so erhält man n'.
Beweise, dass n genau dann durch 7 teilbar ist, wenn n' durch 7 teilbar ist!
Ist etwa $n = 1001$, dann ist $n' = 100 - 2 \cdot 1 = 98$ und $n'' = 9 - 2 \cdot 8 = -7$. Weil n'' durch 7 teilbar ist, so auch 98 und 1001.
Lösung: Ist a die letzte Ziffer von n, so kann man n schreiben als $n = 10A + a$ mit einer natürlichen Zahl A, die eine Stelle weniger hat als n. Nach der Regel ist dann $n' = A - 2a$ und die Behauptung lautet: $7 \mid 10A + a$ genau dann, wenn $7 \mid A - 2a$. Nun gilt aber

$$10n' + 21a = 10(A - 2a) + 21a = 10A - 20a + 21a = 10A + a = n.$$

Betrachtet man nun diese Gleichung modulo 7, so hat man

$$3n' \equiv n \pmod 7.$$

Insbesondere folgt aus $n' \equiv 0 \pmod 7$ sofort $n \equiv 0 \pmod 7$ und aus $n \equiv 0 \pmod 7$ folgt $3n' \equiv 0 \pmod 7$. Wegen $(3, 7) = 1$ kann man aber die letzte Kongruenz durch 3 teilen und hat dann $n' \equiv 0 \pmod 7$, was zu zeigen war.

Aufgabe 3 Bestimme den ggT von folgenden Zahlenpaaren mit Hilfe des Euklidischen Algorithmus!
a) (869, 553) b) (4743, 4123) c) (1632, 833) d) (4140, 3666)

Aufgabe 4 Bestimme den ggT der 4 Zahlen $3774, 2886, 1702$ und 777!

Aufgabe 5 (a) Beweise: Jede Primzahl $p > 3$ lässt bei der Division durch 6 den Rest 1 oder -1!
(b)Beweise: Für jede Primzahl $p > 3$ gilt $24 \mid (p^2 - 1)$!

Aufgabe 6 Wahr oder falsch? Begründe!

$$\begin{aligned}
-14 &\equiv 46 \pmod 5 \\
42 &\equiv -21 \pmod 7 \\
6538 &\equiv 6508 \pmod 6 \\
875 &\equiv 161 \pmod 9 \\
875 &\equiv 161 \pmod 3 \\
401276 &\equiv 25362 \pmod{11} \\
401276 &\equiv 25362 \pmod 9 \\
401276 &\equiv 25362 \pmod{99} \\
1728435 &\equiv 1464315 \pmod 6 \\
1728435 &\equiv 1464315 \pmod{15} \\
1728435 &\equiv 1464315 \pmod{18} \\
1728435 &\equiv 1464315 \pmod{20} \\
1728435 &\equiv 1464315 \pmod{22}
\end{aligned}$$

Aufgabe 7 Wahr oder falsch? Begründe!
(a) $1111 \equiv 111 \equiv 11 \pmod{100}$ (b) $1001 \equiv 10011001 \equiv 0 \pmod{13}$
(c) $2^{10} \equiv 1 \pmod{11}$ (d) $2^{12} \equiv 1 \pmod{13}$ (e) $2^{14} \equiv 1 \pmod{15}$

Aufgabe 8 Beweise die Transitivität der Kongruenzrelation, d. h. für alle natürliche Zahlen $m \in \mathbb{N}$ und alle ganzen Zahlen $a, b, c \in \mathbb{Z}$ gilt:
Wenn $a \equiv b \pmod{m}$ und $b \equiv c \pmod{m}$, dann $a \equiv c \pmod{m}$!

Aufgabe 9 Vereinfache durch Division auf beiden Seiten!

$$\begin{aligned} 64 &\equiv 40 \pmod{12} & 32 &\equiv -16 \pmod{12} \\ 21 &\equiv 6 \pmod{15} & 135 &\equiv 15 \pmod{8} \\ -45 &\equiv 60 \pmod{7} & 196 &\equiv 378 \pmod{91} \\ 65 &\equiv 117 \pmod{26} & 906 &\equiv 663 \pmod{243} \\ -11 &\equiv 121 \pmod{6} & 306 &\equiv 663 \pmod{357} \\ 56 &\equiv -24 \pmod{16} \end{aligned}$$

Aufgabe 10 Gegeben seien zwei ganze Zahlen $a, b \in \mathbb{Z}$, die bei der Division durch 24 die Reste 5 bzw. 7 lassen. Beweise, dass die Differenz ihrer Quadrate durch 24 teilbar ist!

Aufgabe 11 Gegeben seien zwei ganze Zahlen $a, b \in \mathbb{Z}$, die bei der Division durch 7 die Reste 3 bzw. 4 lassen. Beweise, dass die Differenz ihrer Quadrate durch 7 teilbar ist!

Aufgabe 12 Überprüfe die Richtigkeit der folgenden Rechnungen modulo 9 und modulo 11!
a) $56903 \cdot 48721 = 2772371063$
b) $47773 \cdot 535353 = 25577708869$
c) $91453 \cdot 60817 = 5561890171$ oder 5561897101
d) $1683^2 + 79^4 + 17^9 + 23^8 = 196940644348$
e) $138^2 \cdot 21 + 46^3 \cdot 19 + 37^4 \cdot 23 = 45361311$
f) $24^4 \cdot 12 + 17^3 \cdot 21 + 32^5 \cdot 4 = 138302213$

Aufgabe 13 Auf welche Ziffer enden die folgenden Produkte?
a) $z = 3826^{12} \cdot 417^5 \cdot 1992^6 \cdot 2439^5$
b) $z = 3826^{12} \cdot 574^8 \cdot 2964^9 \cdot 39^{26}$
c) $z = 741^7 \cdot 543 \cdot 39726^{13}$

Aufgabe 14 Beweise folgende Sätze:
a) $44 \mid 43^7 - 87^{13}$.
b) $51 \mid 171^n - 33^{2n}$ für alle natürlichen Zahlen $n \in \mathbb{N}$.
c) $55 \mid 5324^{2n+1} + 396^{2n}$ für alle natürlichen Zahlen $n \in \mathbb{N}$.
d) $63 \mid 154^{2n} + 98^{2n+1}$ für alle natürlichen Zahlen $n \in \mathbb{N}$.

Aufgabe 15 Es sei $z = n^3 + 2n$. Durch welche natürliche Zahl (gößer als 1) ist z dann stets teilbar? Beweise Deine Vermutung!

Aufgabe 16 Beweise: Wenn die Summe $a^3 + b^3 + c^3$ dreier Kubikzahlen durch 7 teilbar ist, so ist wenigstens eine der Ausgangszahlen a, b oder c durch 7 teilbar.

Aufgabe 17 Es sei $z = n^{12} - n^8 - n^4 + 1$ und n nicht durch 3 teilbar.
a) Zeige, dass dann gilt $3 \mid z$!
b) Zeige, dass dann gilt $9 \mid z$!

Aufgabe 18 (13er-Regel) Es sei n eine natürliche Zahl. Trennt man von n die letzte Ziffer ab, multipliziert sie mit 4 und addiert das Ergebnis zum verbliebenen Teil von n, so erhält man n'.
Beweise, dass n genau dann durch 13 teilbar ist, wenn n' durch 13 teilbar ist!
Finde selbst eine 17er-Regel und beweise sie!

Lineare diophantische Gleichungen und lineare Kongruenzen

Eine lineare diophantische Gleichung $ax + by = c$ mit gegebenen $a, b, c \in \mathbb{Z}$ ist genau dann lösbar, wenn $(a, b) \mid c$. Diese Bedingung ist offensichtlich notwendig, denn wenn $t \mid a$ und $t \mid b$, dann teilt t auch die gesamte linke Seite, also $t \mid c$.
Eine lösbares diophantisches Gleichungssystem mit n (unabhängigen) Gleichungen und m Variablen hat i. a. $m - n$ freie Parameter. Ziel ist es, diese ganzzahlige parametrische Lösung zu finden. Dazu gibt es ein systematisches Verfahren, das auf dem Euklidischen Algorithmus beruht. Man kann aber auch durch geeignete Wahl des Moduls die Gleichung schrittweise vereinfachen.

Aufgabe 19 Welche Paare (x, y) von ganzen Zahlen erfüllen die diophantische Gleichung $47x - 111y = 89$?

Lösung: Wir betrachten die obige Gleichung modulo 3 und erhalten $2x \equiv 2 \pmod 3$ und wegen $(2, 3) = 1$ also $x \equiv 1 \pmod 3$ bzw. $x = 3t+1$. Setzt man dies in die Ausgangsgleichung ein, fasst zusammen und dividiert durch 3, so hat man $47t - 37y = 14$. Wir betrachten diese Gleichung modulo 37 und haben $10t \equiv 14 \pmod 3 7$ oder $5t \equiv 7 \pmod 3 7$. Um weiter durch 5 teilen zu können, müssen wir einen Repräsentanten von 7 (mod 3)7 finden, der durch 5 teilbar ist, etwa $7 \equiv 7 + 4 \cdot 37 \equiv 155 \equiv 5 \cdot 31 \pmod 3 7$. Also gilt $t \equiv 31 \pmod 3 7$ bzw. $t = 37s - 6$ und somit $x = 111s - 17$. Setzt man dies ein, so hat man $y = 47s - 8$.

Aufgabe 20 36 Schüler sollen mit je einem Buch ausgezeichnet wrden. Es gibt Bücher für $9,50\,\text{DM}$, $11,00\,\text{DM}$ und $13,75\,\text{DM}$. Insgesamt stehen $400\,\text{DM}$ zur Verfügung, die restlos aufgebraucht werden sollen. Welche Varianten zum Kauf der Bücher gibt es?

Aufgabe 21 Bestimme die Lösungsmenge der folgenden linearen Kongruenzen!

a) $2x \equiv 4 \pmod 5$	h)$24x \equiv 13 \pmod 4$
b) $3x \equiv 4 \pmod 5$	i) $121x \equiv 88 \pmod{22}$
c) $5x \equiv 6 \pmod 7$	k) $25x \equiv 12 \pmod 5$
d) $23x \equiv 42 \pmod 5$	l) $23x \equiv 13 \pmod 9$
e) $56x \equiv 10 \pmod{84}$	m) $39x \equiv 30 \pmod{51}$
f) $19x \equiv 18 \pmod{17}$	n) $45x \equiv 27 \pmod 6$
g) $123x \equiv 87 \pmod{10}$	o) $10x \equiv 16 \pmod{28}$

Aufgabe 22 Löse in natürlichen Zahlen $10x + 18y + 15z = 404$!

Aufgabe 23 Wie viele Lösungen in natürlichen Zahlen besitzt $9x + 11y = 1996$?

Aufgabe 24 Man beweise: Es seien a und b ganze Zahlen und $11a + 2b$ ist durch 19 teilbar. Dann ist auch $18a + 5b$ durch 19 teilbar.

Teilbarkeit durch 3, 5 und 11, Quersummen

Aufgabe 25 Man denke sich alle natürlichen Zahlen von 1 bis 1000 fortlaufend auf folgende Weise hingeschrieben

$$1234567891011 \cdots 9991000.$$

Beweise, dass die so entstandene Zahl nicht durch 2001 teilbar ist!

Lösung: Die obige Zahl hat die Gestalt $z = \sum_{n=1}^{1000} n \cdot 10^{a_n}$ mit gewissen Exponenten a_n. Wir berechnen ihren Rest modulo 3:

$$z \equiv \sum_{n=1}^{1000} n \equiv \frac{1}{2} 1000 \cdot 1001 \equiv 500 \cdot 2 \equiv 1 \pmod 3.$$

Somit ist z nicht durch 3 teilbar, also auch nicht durch 2001.

Aufgabe 26 Bildet man aus einer im 10er System geschriebenen Zahl durch beliebiges Vertauschen der ersten, dritten, fünften usw. Ziffer und beliebiges Vertauschen der zweiten, vierten, usw. Ziffer eine neue Zahl, dann ist die Differenz aus der Ausgangszahl und der neuen Zahl durch 99 teilbar.

Lösung: Für eine natürliche Zahl $z = \overline{a_n a_{n-1} \cdots a_1 a_0}$ sei $A(z) = a_0 - a_1 + a_2 - + \cdots + (-1)^n a_n$ die alternierende Quersumme und $Q(z) = a_0 + \cdots + a_n$ die Quersumme. Wegen $10^k \equiv (-1)^k \pmod 1 1$ und $10^k \equiv 1 \pmod 9$ gilt $z \equiv A(z) \pmod 1 1$ und $z \equiv Q(z) \pmod 9$. Durch die oben beschriebene Vertauschung der Ziffern ändert sich aber die alternierende Quersumme $A(z)$ der Zahl nicht und natürlich auch nicht die Quersumme $Q(z)$. Also gilt für die vertauschte Zahl z', dass $z' \equiv A(z') = A(z) \equiv z \pmod 1 1$, $z' \equiv Q(z') = Q(z) \equiv z \pmod 9$. Hieraus folgt $9 \mid (z' - z)$ und $11 \mid (z' - z)$. Wegen der Teilerfremdheit $(9, 11) = 1$ folgt $99 \mid (z' - z)$ und damit die Behauptung.

Quadratreste

Aufgabe 27 Die natürlichen Zahlen (x, y, z) heißen *pythagoräisches Tripel*, wenn $x^2 + y^2 = z^2$ gilt. Beweise, dass in jedem pythagoräischen Tripel eine durch 5 teilbare Zahl vorkommt!

Aufgabe 28 (a) Jede natürliche Zahl der Form $4k + 3$ lässt sich nicht als Summe von zwei Quadraten schreiben.
(b) Jede natürliche Zahl der Form $8k + 6$ lässt sich nicht als Summe von zwei Quadraten schreiben.
(c) Jede natürliche Zahl der Form $8k + 7$ lässt sich nicht als Summe von drei Quadraten schreiben.

Aufgabe 29 (a) Man beweise, dass für alle natürliche Zahl n die Zahlen $3n - 1$, $5n \pm 2$, $6n + 2$, $7n - 1$, $7n - 2$ und $7n + 3$ keine Quadratzahlen sind!
(b) Für welche natürlichen Zahlen n sind die Zahlen $6n + 2$ und $7n + 3$ nicht teilerfremd?
(c) Beweise, dass für keine natürliche Zahl n das Produkt $(6n + 2)(7n + 3)$ eine Quadratzahl ist!

Aufgabe 30 Es gibt keine Quadratzahl A, die aus genau 600 Sechsen und einigen Nullen besteht.

Lösung: Wenn A eine Quadratzahl ist, so endet A auf eine gerade Anzahl von Nullen. Streicht man diese Endnullen, so erhält man eine Quadratzahl $2B$, wobei B aus lauter Dreien besteht, also ungerade ist. $2B$ enthält also nur einen Faktor 2 und ist somit keine Quadratzahl.

Aufgabe 31 Eine 9-stellige natürliche Zahl A, die auf 5 endet und alle Ziffern bis auf die 0 enthält, kann keine Quadratzahl sein.

Lösung: Da A auf 5 endet, ist $A = x^2 = (10a+5)^2 = 100a^2 + 100a + 25 = 100a(a+1) + 25$. Nun ist aber $a(a+1) \equiv 0, 2, 6 \pmod 1 0$. Auf 0 und 2 kann $a(a+1)$ nicht enden, also ist die drittletzte Ziffer 6. Damit gilt $125 = 5^4 \mid A = 1000B + 625$; also $25 \mid x$. Somit gilt $x = 100b + 25$ oder $x = 100b + 75$. Quadriert man dies, so erhält man wie oben, dass die viertletzte Ziffer 0 oder 5 ist.

Potenzreste

Es sei p eine Primzahl und $a \in \mathbb{N}$. Dann gilt $a^p \equiv a \pmod p$ (FERMATscher Satz). Ist a nicht durch p teilbar, so kann man kürzen und es gilt $a^{p-1} \equiv 1 \pmod p$. Ist $m \in \mathbb{N}$ und $\varphi(m)$ die Anzahl der zu m teilerfremden Restklassen modulo m (*prime Restklassen*), dann gilt für alle $a \in \mathbb{N}$ mit $(a, m) = 1$

$$a^{\varphi(m)} \equiv 1 \pmod m. \tag{5}$$

Dies ist der EULER-FERMATsche Satz. Für Primzahlpotenzen gilt $\varphi(p^\alpha) = p^{\alpha-1}(p-1)$ und für teilerfremde Zahlen m, n ist $\varphi(mn) = \varphi(m)\varphi(n)$. Diese Funktion $\varphi(n)$ heißt EULERsche Funktion. Im allgemeinen ist $\varphi(m)$ nicht die kleinste Zahl k mit $a^k \equiv 1 \pmod m$. Zum Beispiel ist $3^5 \equiv 243 \equiv 1 \pmod 1 1$, aber es gilt $\varphi(11) = 10$. Diese kleinste Zahl k ist aber stets ein Teiler von $\varphi(m)$. Damit ist klar, dass die Folge der Potenzreste $(a^n \pmod m)$ periodisch mit der Periode k ist (vorausgesetzt, dass $(a, m) = 1$).

Aufgabe 32 Welchen Rest lässt 2^{32} bei der Division durch 641?

Aufgabe 33 Es sei $A = 3^{105} + 4^{105}$. Beweise, dass $7 \mid A$. Bestimme die Reste von A bei der Division durch 11 und 13!

Aufgabe 34 (a) Wenn die Summe zweier natürlicher Zahlen durch 7 teilbar ist, so ist die Summe ihrer siebenten Potenzen durch 49 teilbar.
(b) Ist die Summe von drei Kubikzahlen durch 7 teilbar, so ist mindestens eine von ihnen durch 7 teilbar.

Aufgabe 35 Auf welche beiden Ziffern endet $7^{7^{7^7}} - 7^{7^7}$?

Lösung: Wir berechnen die Periode von $7^n \pmod{100}$:

$$7^1 \equiv 7 \pmod{100}, \quad 7^2 \equiv 49 \pmod{100}, \quad 7^3 \equiv 43 \pmod{100}, \quad 7^4 \equiv 01 \pmod{100}$$

Also ist die Periodenlänge 4. Nun ist $7^n \equiv (-1)^n \equiv -1 \pmod 4$ wenn n eine ungerade Zahl ist. Folglich gilt $7^{7^{7^7}} \equiv 7^{7^7} \equiv 7^3 \equiv 43 \pmod{100}$ und damit endet $7^{7^{7^7}} - 7^{7^7}$ auf zwei Nullen.

Teilbarkeit und Primfaktorzerlegung

Primzahlen größer als 3 haben die Gestalt $6n \pm 1$. Quadrate von ungeraden natürlichen Zahlen sind stets kongruent 1 modulo 8. Die folgenden Formeln spielen immer wieder eine wichtige Rolle beim Ausklammern von Faktoren.

$$a^n - b^n = (a-b)(a^{n-1} + a^{n-2}b + \cdots + b^{n-1},$$
$$a^u + b^u = (a+b)(a^{u-1} - a^{u-2}b + - \cdots + b^{u-1}), \quad \text{falls } u \text{ ungerade,}$$
$$(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k}.$$

Aufgabe 36 (a) Man beweise, dass für jede natürliche Zahl n die Zahl $n^6 - n^2$ durch 10 teilbar ist!
(b) Man beweise, dass für jede ungerade natürliche Zahl n die Zahl $n^{12} - n^8 - n^4 + 1$ durch 512 teilbar ist!

Aufgabe 37 Man denke sich die Primzahlen ≥ 5 der Größe nach fortlaufend nummeriert:

Primzahl	5	7	11	13	17	19	$\cdots$
Nummer	1	2	3	4	5	6	$\cdots$

Man beweise, dass jede Primzahl größer ist als das Dreifache ihrer Nummer.

Aufgabe 38 (a) Ist die Summe dreier Primzahlen, jede größer als 3, durch 3 teilbar, dann sind die Differenzen je zweier dieser Primzahlen durch 6 teilbar.
(b) Sind p und q Primzahlen größer als 3, dann ist die Differenz ihrer Quadrate durch 24 teilbar.

Aufgabe 39 Es gibt kein Polynom $f(x)$ mit ganzzahligen Koeffizienten, so dass $f(7) = 11$ und $f(11) = 13$ gilt.

Lösung: Für jedes Polynom f mit ganzzahligen Koeffizienten gibt es ein Polynom $q(x)$ mit ganzzahligen Koeffizienten, so dass $f(x) = f(a) + (x-a)q(x)$. Setzt man insbesondere $x = b$ ein, so hat man $(b-a) \mid (f(b) - f(a))$. Dies ist aber für die oben gegebenen Werte nicht erfüllt, da $11 - 7 = 4 \not| (13 - 11)$.

Aufgabe 40 Die Gleichung $x^2 + y^2 + z^2 = 2xyz$ hat keine Lösung in ganzen Zahlen bis auf $x = y = z = 0$.

Lösung: Es sei 2^k die höchste Zweierpotenz, die in (x, y, z) auftritt, also $x = 2^k x_1, y = 2^k y_1$ und $z = 2^k z_1$. Setzt man dies ein, so erhält man $x_1^2 + y_1^2 + z_1^2 = 2^{k+1} x_1 y_1 z_1$. Somit ist die linke Seite durch 2 teilbar. Wegen der Wahl von k ist genau eine der Zahlen, etwa x_1, gerade und die anderen beiden ungerade; $x_1 = 2x_2$. Dann ist aber

$$y_1^2 + z_1^2 = 2^{k+2} x_2 y_1 z_1 - 4x_2^2 \equiv 0 \pmod 4.$$

Dies widerspricht aber $y_1^2 + z_1^2 \equiv 2 \pmod 4$.

Aufgabe 41 Ist $2^n - 1$ eine Primzahl, so auch n. Ist $2^n + 1$ eine Primzahl, so ist n eine Zweierpotenz.

Aufgabe 42 Eine Zahl aus 3^n gleichen Ziffern ist durch 3^n teilbar.

Lösung: Induktiv. Offenbar genügt es, die Aufgabe für die Ziffer 1 zu zeigen. Für $n = 1$ gilt $3^1 \mid 111$. Nun sei die Zahl z aus 3^n Einsen bereits durch 3^n teilbar. Die Zahl z' aus 3^{n+1} Einsen hat dann die Gestalt

$$z' = \overline{zzz} = z10^{2\cdot 3^n} + z10^{3^n} + z = z(10^{2\cdot 3^n} + 10^{3^n} + 1).$$

Da $3^n \mid z$ und der Ausdruck in der Klammer durch 3 teilbar ist, folgt die Behauptung.

Attribution Section

schueler (2004-09-09): Contributed to KoSemNet
graebe (2004-09-09): Prepared along the KoSemNet rules