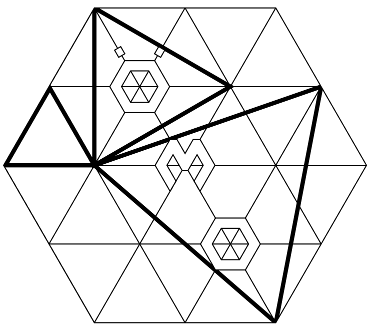
Zahlentheorie für den Junior-Regionalwettbewerb der Österreichischen Mathematik-Olympiade

Clemens Heuberger*

Version September 2019

Inhaltsverzeichnis



*Clemens Heuberger, Institut für Mathematik, Alpen-Adria-Universität Klagenfurt, Universitätsstraße 65–67, 9020 Klagenfurt am Wörthersee, `clemens.heuberger@aau.at`.

1 Dezimaldarstellung

Wir bezeichnen die Menge der ganzen Zahlen mit $\mathbb{Z} := \{\dots, -2, -1, 0, 1, 2, \dots\}$. Die nicht-negativen ganzen Zahlen heißen auch *natürliche Zahlen*, wir schreiben $\mathbb{N} := \{0, 1, 2, 3, \dots\}$.

Satz 1.1. *Jede positive ganze Zahl n kann eindeutig als*

$$n = 10^\ell a_\ell + a_{\ell-1} 10^{\ell-1} + \cdots + a_2 10^2 + a_1 10 + a_0$$

mit Ziffern $a_0, \dots, a_\ell \in \{0, \dots, 9\}$ und $a_\ell \neq 0$ geschrieben werden. Wir schreiben auch $n = (a_\ell \dots a_0)_{10}$ und nennen das die Dezimaldarstellung von n.

Die Voraussetzung $a_\ell \neq 0$ ist für die Eindeutigkeit erforderlich, sonst gäbe es mit verschiedenen Anzahlen von führenden Nullen verschiedene Dezimaldarstellung.

Man bezeichnet a_0 auch als Einerziffer von n, a_1 als Zehnerziffer, usw.

Definition 1.2. Die *Ziffernsumme* einer Zahl $n = (a_\ell \dots a_0)_{10}$ ist $a_\ell + a_{\ell-1} + \cdots + a_1 + a_0$. Ihre *Querdifferenz* ist $a_0 - a_1 + a_2 - a_3 + \cdots$.

Zum Beispiel ist die Ziffernsumme von 2014 gleich $2 + 0 + 1 + 4 = 7$ und die Querdifferenz von 2014 gleich $4 - 1 + 0 + 2 = 5$. Beachte, dass bei der Querdifferenz die Vorzeichen von rechts (der Einerstelle) her bestimmt werden, sodass die Einerstelle immer positiv gewertet wird, die Zehnerstelle immer negativ usw. Bei der Ziffernsumme ist die Reihenfolge der Ziffern egal.

2 Teilbarkeit

Definition 2.1. Sei d eine positive[1] ganze und a eine ganze Zahl. Dann heißt d ein Teiler von a, wenn es eine ganze Zahl k mit $d \cdot k = a$ gibt. Wir schreiben $d \mid a$.

Somit ist d genau dann ein Teiler von a, wenn der Bruch $\frac{a}{d}$ eine ganze Zahl ist.

Satz 2.2. *Sei d eine positive ganze und a, b ganze Zahlen.*

1. *Wenn $d \mid a$ und $d \mid b$, so gilt auch $d \mid (a + b)$.*
2. *Wenn $d \mid a$ und $d \mid b$, so gilt auch $d \mid (a - b)$.*
3. *Wenn $d \mid a$, so gilt auch $d \mid a \cdot b$.*

Beweis.

1. Da $d \mid a$ und $d \mid b$, gibt es ganze Zahlen k und ℓ mit $a = dk$ und $b = d\ell$, somit gilt durch Herausheben auch
$$a + b = dk + d\ell = d(k + \ell),$$
somit ist also d ein Teiler von $a + b$.
2. Analog.
3. Wenn $d \mid a$, so gibt es eine ganze Zahl k mit $a = dk$. Dann gilt aber auch $ab = dkb = d(kb)$, es ist also d ein Teiler von ab.

□

[1] Man kann diese Definition und die folgenden Resultate leicht auf beliebige ganze Zahlen d erweitern. Aus der Definition folgt dann, dass $0 \mid a$ genau dann gilt, wenn $a = 0$.

3 Primzahlen

Definition 3.1. Eine positive ganze Zahl $p \geq 2$ heißt *Primzahl*, wenn ihre einzigen positiven Teiler 1 und p selbst sind.

Beispiele für Primzahlen sind damit 2, 3, 5, 7, 11, 13, 17, 19; keine Primzahlen sind $4 = 2 \cdot 2$, $6 = 2 \cdot 3$, $8 = 2 \cdot 4$, $9 = 3 \cdot 3$, $10 = 2 \cdot 5$, usw.

Die Zahl 1 *ist keine Primzahl*, weil die Definition dies ausgeschlossen hat.

Satz 3.2. *Jede ganze Zahl*[2] $n \geq 2$ *kann in der Form*

$$n = p_1^{k_1} p_2^{k_2} \dots p_t^{k_t}$$

mit verschiedenen Primzahlen $p_1, \dots, p_t$ *und positiven ganzen Zahlen* $k_1, \dots, k_t$ *dargestellt werden.*

Diese Darstellung ist bis auf die Reihenfolge der Faktoren eindeutig.

Wir nennen das die Primfaktordarstellung *oder* Primfaktorzerlegung *von* n.

Es gelten zum Beispiel $2 = 2^1$, $6 = 2^1 \cdot 3^1$, $8 = 2^3$, $144 = 2^4 \cdot 3^2$, $2002 = 2 \cdot 7 \cdot 11 \cdot 13$, $111 = 3 \cdot 37$.

Dieser Satz ist keineswegs selbstverständlich, wie allgemeinere Zahlbereiche zeigen, sondern muss (mit den angegebenen Definitionen) bewiesen werden. Für die Existenz ist das recht leicht; die Eindeutigkeit erfordert genauere Überlegungen und wird hier ausgelassen.

Beweis der Existenz. Wir nehmen indirekt an, dass nicht alle ganzen Zahlen $n \geq 2$ eine Primfaktordarstellung besitzen. Dann gibt es eine kleinste ganze Zahl $n \geq 2$, die keine Primfaktordarstellung besitzt. Dieses n kann keine Primzahl sein (sonst wäre ja bereits eine Primfaktordarstellung von n gefunden). Daher gibt es einen Teiler a von n mit $1 < a < n$. Somit gilt $n = ab$ für ein passendes b, ebenfalls mit $1 < b < n$. Da a und b jeweils Primfaktordarstellungen besitzen (n war ja die kleinste Zahl ohne Primfaktordarstellung), können die Primfaktordarstellungen von a und b miteinander multipliziert werden, woraus sich eine Primfaktordarstellung von n ergibt. □

Beispiel 3.3 (LWA 2013/1, Richard Henner)**.** Man bestimme alle natürlichen Zahlen $n > 1$, für die Folgendes gilt:

Die Summe der Zahl n und ihres zweitgrößten Teilers ist 2013.

Teilbarkeit und Primfaktordarstellung hängen eng miteinander zusammen.

Satz 3.4. *Seien* a *und* b *positive ganze Zahlen. Dann gilt* $a \mid b$ *genau dann, wenn jede Primzahl in der Primfaktordarstellung von* b *mindestens so oft vorkommt wie in der von* a.

Beweis. Wir nehmen zunächst an, dass $a \mid b$. Daher gibt es eine natürliche Zahl c mit $b = ac$. Wir schreiben die Primfaktordarstellungen von a, b und c als

$$a = p_1^{k_1} \dots p_r^{k_r}, \qquad b = p_1^{\ell_1} \dots p_r^{\ell_r}, \qquad c = p_1^{m_1} \dots p_r^{m_r}$$

für passende natürliche Zahlen $k_1, \dots, k_r, \ell_1, \dots, \ell_r, m_1, \dots, m_r$. Aufgrund der eindeutigen Primfaktordarstellung gelten $\ell_1 = k_1 + m_1, \dots, \ell_r = k_r + m_r$. Damit folgen $\ell_1 \geq k_1, \dots, \ell_r \geq k_r$, wie gefordert.

Wir beweisen nun die umgekehrte Richtung. Wir schreiben die Primfaktordarstellungen von a und b als

$$a = p_1^{k_1} \dots p_r^{k_r}, \qquad b = p_1^{\ell_1} \dots p_r^{\ell_r},$$

für passende natürliche Zahlen $k_1, \dots, k_r$ und $\ell_1, \dots, \ell_r$. Nach Voraussetzung gelten $\ell_1 \geq k_1, \dots, \ell_r \geq k_r$. Wir betrachten

$$c = p_1^{\ell_1 - k_1} \dots p_r^{\ell_r - k_r}.$$

Nach den Voraussetzungen ist c eine positive ganze Zahl mit $b = ac$. Daher gilt wie gefordert $a \mid b$. □

[2] Wenn man das leere Produkt als Primfaktorzerlegung von 1 ansieht, gilt der Satz auch für $n = 1$.

4 Größter gemeinsamer Teiler, kleinstes gemeinsames Vielfaches

Definition 4.1. Seien a und b positive[3] ganze Zahlen.

1. Die größte positive ganze Zahl d, die sowohl a als auch b teilt, heißt *größter gemeinsamer Teiler* von a und b, wir schreiben $d = \operatorname{ggT}(a, b)$.

2. Die kleinste positive ganze Zahl m, die sowohl von a als auch von b geteilt wird, heißt *kleinstes gemeinsames Vielfaches* von a und b, wir schreiben $m = \operatorname{kgV}(a, b)$.

Mit Hilfe der Primfaktordarstellung, genauer gesagt, mit Hilfe von Satz 3.4, kann man den ggT und das kgV zweier (nicht allzu großer) Zahlen einfach bestimmen. Wir illustrieren das am Beispiel von 144 und 480.

Zunächst bestimmen wir die Primfaktordarstellungen der beiden Zahlen:

$$144 = 2^4 \cdot 3^2, \qquad 480 = 2^5 \cdot 3 \cdot 5.$$

Die Primzahl 2 muss in $d = \operatorname{ggT}(144, 480)$ genau 4-mal auftreten: mehr ist nicht möglich, weil sonst d nach Satz 3.4 kein Teiler von 144 mehr wäre, weniger würde zu einem kleineren gemeinsamen Teiler führen. Ebenso muss die Primzahl 3 genau einmal in d vorkommen; die Primzahl 5 kann nicht vorkommen, alle übrigen Primzahlen auch nicht. Damit gilt $d = \operatorname{ggT}(144, 480) = 2^4 \cdot 3 = 48$. Wir haben also für jede Primzahl den kleineren der beiden Exponenten in den Primfaktordarstellungen der beteiligten Zahlen gewählt.

Für das kleinste gemeinsame Vielfache nimmt man jeweils den größeren der beiden Exponenten: In unserem Fall also $m = \operatorname{kgV}(144, 480) = 2^5 \cdot 3^2 \cdot 5 = 1440$.

Definition 4.2. Zwei positive[4] ganze Zahlen a und b heißen *teilerfremd* oder *relativ prim*, wenn $\operatorname{ggT}(a, b) = 1$ gilt.

Beispielsweise sind 10 und 21 teilerfremd, weil $\operatorname{ggT}(10, 21) = 1$.

Verschiedene Primzahlen sind jedenfalls teilerfremd.

Aus der eindeutigen Primfaktordarstellung folgt folgendes wesentliches Resultat:

Satz 4.3 (Fundamentallemma der Arithmetik)**.** *Seien a, b, c ganze Zahlen, $a \mid bc$ und $\operatorname{ggT}(a, b) = 1$. Dann gilt $a \mid c$.*

Beweis. Wir beweisen hier das Fundamentallemma der Arithmetik unter der Voraussetzung, dass die eindeutige Primfaktorzerlegung gilt.[5]

Sei p eine Primzahl, die a teilt. Wir wählen den größten Exponenten k, sodass $p^k \mid a$. Da a und b teilerfremd sind, tritt die Primzahl p in der Primfaktordarstellung von b nicht auf. Da andererseits $a \mid bc$, muss p^k ein Teiler von bc sein und daher p mindestens mit Exponenten k in bc auftreten. Da p nicht in b auftritt, muss p^k ein Teiler von c sein.

Da diese Überlegung für alle Primteiler von a gilt, muss a ein Teiler von c sein. □

Beispiel 4.4 (LWA 2012/1, Walther Janous)**.** Es seien a, b, c und d vier ganze Zahlen, für die

$$7a + 8b = 14c + 28d$$

gilt.

Man zeige, dass das Produkt $a \cdot b$ immer durch 14 teilbar ist.

[3] Man kann das auf ganze Zahlen a, b mit der Maßgabe verallgemeinern, dass nicht a und b gleichzeitig 0 sein dürfen.

[4] Oder $a, b \in \mathbb{Z}$, nicht beide 0.

[5] In „Wahrheit" verwendet man üblicherweise das Fundamentallemma der Arithmetik, um die Eindeutigkeit der Primfaktorzerlegung zu zeigen; man muss sich also einen alternativen Beweis des Fundamentallemmas zurechtlegen.

5 Kongruenzen

Für eine natürliche Zahl a und eine positive ganze Zahl m sagen wir, a lässt Rest r bei Division durch m, wenn $r \in \{0, \dots, m-1\}$ und es eine ganze Zahl q mit $a = qm + r$ gibt. Das ist genau der Rest, der bei der „üblichen“ Division von a durch m herauskommt.

Definition 5.1. Seien a, b natürliche Zahlen und $m \geq 2$ eine ganze Zahl. Dann heißen a und b *kongruent modulo* m, wenn sie bei Division durch m den gleichen Rest lassen. Wir schreiben in diesem Fall $a \equiv b \pmod{m}$.

So gilt zum Beispiel $17 \equiv 42 \pmod{5}$, weil beide den Rest 2 bei Division durch 5 lassen: $17 = 3 \cdot 5 + 2$ und $42 = 8 \cdot 5 + 2$. Ebenso erhält man

$$2 \equiv 7 \pmod{5}, 7 \equiv 12 \pmod{5}, 12 \equiv 17 \pmod{5}, \dots$$

Wir notieren einmal folgende einfache Eigenschaft:

Satz 5.2. *Wenn $a \equiv b \pmod{m}$ und $b \equiv c \pmod{m}$, so gilt auch $a \equiv c \pmod{m}$.*

Beweis. Laut Definition lassen a und b bei Division durch m den gleichen Rest, nennen wir ihn r. Weiters lassen b und c bei Division durch m den gleichen Rest, nennen wir ihn s. Da der Rest von b bei Division durch m eindeutig ist, muss $r = s$ gelten; somit lassen a und c bei Division durch m denselben Rest, sind also kongruent modulo m. □

Da also $2 \equiv 7 \pmod{5}$ und $7 \equiv 12 \pmod{5}$, gilt auch $2 \equiv 12 \pmod{5}$. Das hätten wir natürlich auch leicht direkt berechnen können; der Satz erlaubt uns jedoch, eine „Kongruenzen-Kette“ der Form

$$2 \equiv 7 \equiv 12 \equiv 17 \equiv 22 \equiv 27 \equiv 32 \equiv 37 \equiv 42 \equiv \cdots \pmod{5}$$

aufzustellen.

Für andere Überlegungen erweist es sich als zweckmäßig, die Definition der Kongruenz umzuformulieren.

Satz 5.3. *Seien a, b und m positive*[6] *ganze Zahlen. Dann gilt $a \equiv b \pmod{m}$ genau dann, wenn $m \mid (a - b)$.*

Beweis. Nach unserer Definition folgt aus $a \equiv b \pmod{m}$, dass es ganze Zahlen r, q_1, q_2 gibt, sodass $a = q_1 m + r$, $b = q_2 m + r$, somit also

$$a - b = (q_1 m + r) - (q_2 m + r) = q_1 m + r - q_2 m - r = q_1 m - q_2 m = (q_1 - q_2)m,$$

m ist also ein Teiler von $a - b$.

Sei umgekehrt m ein Teiler von $a - b$ und ohne Beschränkung der Allgemeinheit gelte $a < b$. Sei r der Rest von a bei Division durch m. Wir können also $a = qm + r$ für ein passendes q schreiben. Weiters ist $b - a$ ein Vielfaches von m, wir schreiben also $b - a = km$ für ein passendes m. Somit gilt

$$b = a + km = (qm + r) + km = qm + km + r = (q + k)m + r,$$

b lässt also Rest r bei Division durch m. □

Die wesentliche Eigenschaft von Kongruenzen ist, dass man mit Kongruenzen „rechnen darf“. Die Grundlage bildet folgender Satz.

Satz 5.4. *Seien $a \equiv b \pmod{m}$ und $c \equiv d \pmod{m}$. Dann gelten auch*

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

[6] Für allgemeine a, b und $m \in \mathbb{Z}$ erweist es sich als günstiger, diese Aussage als Definition der Kongruenz heranzuziehen. Dann sind je zwei Zahlen kongruent modulo 1. Zwei ganze Zahlen sind genau dann kongruent modulo 0, wenn sie gleich sind.

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

3. $ac \equiv bd \pmod{m}$*.*

Beweis. 1. Da nach Voraussetzung $a \equiv b \pmod{m}$ und $c \equiv d \pmod{m}$ gelten, gibt es nach Satz 5.3 ganze Zahlen k und ℓ mit $a - b = km$ und $c - d = \ell m$. Es ergibt sich daraus $a = b + km$ und $c = d + \ell m$. Um zu zeigen, dass $a + c \equiv b + d \pmod{m}$, genügt es nach Satz 5.3 zu zeigen, dass $(a+c)-(b+d)$ durch m teilbar ist. Wir berechnen diesen Ausdruck:

$$(a + c) - (b + d) = (b + km + d + \ell m) - (b + d) = km + \ell m = (k + \ell)m.$$

Daraus folgt, dass $(a + c) - (b + d)$ durch m teilbar ist.

2. Analog.

3. Wie im ersten Punkt erhalten wir $a = b + km$ und $c = d + \ell m$ für passende ganze Zahlen k und ℓ. Wir müssen zeigen, dass $ac - bd$ durch m teilbar ist und schreiben daher diesen Ausdruck um:

$$\begin{aligned} ac - bd &= (b + km)(d + \ell m) - bd = (bd + kmd + \ell md + k\ell m^2) - bd = kmd + \ell md + k\ell m^2 \\ &= m(kd + \ell d + k\ell m). \end{aligned}$$

Offensichtlich ist damit $ac - bd$ durch m teilbar.

□

Das ermöglicht es zum Beispiel, den Rest von $11 \cdot 13 + 17 \cdot 19 + 21 \cdot 23$ bei Division durch 10 zu berechnen: Da $11 \equiv 1 \pmod{10}$, $13 \equiv 3 \pmod{10}$, $17 \equiv 7 \pmod{10}$, $19 \equiv 9 \pmod{10}$, $21 \equiv 1 \pmod{10}$ und $23 \equiv 3 \pmod{10}$, dürfen wir wie folgt „ersetzen“:

$$11 \cdot 13 + 17 \cdot 19 + 21 \cdot 23 \equiv 1 \cdot 3 + 7 \cdot 9 + 1 \cdot 3 = 3 + 63 + 3 \equiv 3 + 3 + 3 \equiv 9 \pmod{10}.$$

Vereinfacht wurde das dadurch, dass jede Zahl zu ihrer Einerziffer im Dezimalsystem kongruent modulo 10 ist.

Diese Ersetzungen werden jedoch falsch, wenn man sie im *Exponenten* durchführt: Es gilt zwar $2 \equiv 5 \pmod{3}$ und $3 \equiv 0 \pmod{3}$, aber nicht $8 \equiv 2^3 \equiv 5^0 \equiv 1 \pmod{3}$.

Auch bei Division gilt das im Allgemeinen nicht[7]: Dividiert man die wahre Kongruenz $0 \equiv 4 \pmod{4}$ durch 2, so erhält man die falsche Kongruenz $0 \equiv 2 \pmod{4}$.

Kongruenzen modulo kleiner Moduln kann man durch Kenntnis der Ziffern im Dezimalsystem bestimmen:

Satz 5.5. *Sei*

$$n = (a_\ell a_{\ell-1} \dots a_2 a_1 a_0)_{10}$$

eine natürliche Zahl mit ihrer Dezimaldarstellung. Dann gilt:

1. $n \equiv a_0$ (mod 2 *bzw.* 5)*; eine Zahl ist modulo* 2 *und modulo* 5 *zu ihrer letzten Ziffer kongruent;*

2. $n \equiv (a_1 a_0)_{10} \pmod{4}$*; eine Zahl ist modulo* 4 *zu der aus ihren letzten beiden Ziffern gebildeten Zahl kongruent;*

3. $n \equiv (a_2 a_1 a_0)_{10} \pmod{8}$*; eine Zahl ist modulo* 8 *zu der aus ihren letzten drei Ziffern gebildeten Zahl kongruent;*

4. $n \equiv a_\ell + a_{\ell-1} + \dots + a_2 + a_1 + a_0$ (mod 3 *bzw.* 9)*; eine Zahl ist modulo* 9 *(und daher auch modulo* 3*) zu ihrer Ziffernsumme kongruent;*

[7] Die korrekte Rechenregel für die Division von Kongruenzen ist etwas komplizierter als die für Addition, Subtraktion und Multiplikation: Wenn $a \equiv b \pmod{m}$ und $c \mid a$ sowie $c \mid b$, so gilt auch $\frac{a}{c} \equiv \frac{b}{c} \pmod{\frac{m}{\mathrm{ggT}(m,c)}}$.

5. *$n \equiv a_0 - a_1 + a_2 - + \ldots \pm a_\ell \pmod{11}$; eine Zahl ist modulo 11 zu ihrer Querdifferenz kongruent.*

Beweis. 1. Wegen $10 \equiv 0 \pmod{2 \text{ bzw. } 5}$ gilt $a_k 10^k \equiv 0 \pmod{2 \text{ bzw. } 5}$ für alle $k \geq 1$. Daher gilt $n = a_\ell 10^\ell + \cdots + a_1 10^1 + a_0 \equiv 0 + \cdots + 0 + a_0 \pmod{2 \text{ bzw. } 5}$.

2. Wegen $4 \mid 100$ und $100 \mid 10^k$ für alle $k \geq 2$ gilt $a_k 10^k \equiv 0 \pmod 4$ für alle $k \geq 2$. Daher gilt $n \equiv 0 + 0 + \cdots + 10a_1 + a_0 = (a_1 a_0)_{10} \pmod 4$.

3. $8 \mid 1000$ und dann weiter wie bei 2.

4. Wegen $10 \equiv 1 \pmod{3 \text{ bzw. } 9}$ gilt $10^k \equiv 1^k = 1 \pmod{3 \text{ bzw. } 9}$ für alle $k \geq 1$. Somit gilt

$$n = a_\ell 10^\ell + \cdots + a_1 10^1 + a_0 \equiv a_\ell + a_{\ell-1} + \cdots + a_2 + a_1 + a_0 \pmod{3 \text{ bzw. } 9}.$$

5. Wegen $10 \equiv -1 \pmod{11}$ gilt $10^k \equiv (-1)^k \pmod{11}$, also

$$n = a_0 + a_1 10^1 + \cdots + a_\ell 10^\ell \equiv a_0 - a_1 + a_2 - + \cdots \pm a_\ell \pmod{11}.$$

□

Daraus folgen unmittelbar die bekannten *Teilbarkeitsregeln*:

Eine Zahl ist genau dann durch ... teilbar,	wenn es ... ist.
2 bzw. 5	ihre letzte Ziffer
4	die Zahl aus ihren letzten beiden Ziffern
8	die Zahl aus ihren letzten drei Ziffern
3 bzw. 9	ihre Ziffernsumme
11	ihre Querdifferenz

Schließlich kann man durch die Betrachtung von Kongruenzen modulo kleiner Moduln manchmal Widersprüche aufzeigen und damit zeigen, dass gewisse Gleichungen in ganzen Zahlen unlösbar sind. Gleichungen, deren Lösungen man nur in den ganzen Zahlen sucht, nennt man auch *Diophantische Gleichungen*. Ein wesentliches Hilfsmittel dazu ist die Kenntnis der Reste von Quadraten.

Satz 5.6. *Sei $x \in \mathbb{Z}$. Dann ist*

1. *x^2 kongruent zu 0 oder 1 modulo 3,*

2. *x^2 kongruent zu 0 oder 1 modulo 4,*

3. *x^2 kongruent zu 0, 1 oder 4 modulo 5,*

4. *x^2 kongruent zu 0, 1 oder 4 modulo 8,*

5. *x^2 kongruent zu 0, 1, 4, 5, 6, 9 modulo 10.*

Beweis. Wir zeigen das Resultat modulo 4, alle übrigen Resultate folgen analog. Da x kongruent zu einer der Zahlen 0, 1, 2 oder 3 ist, ist (nach Satz 5.4) x^2 kongruent zu $0^2 = 0$, $1^2 = 1$, $2^2 = 4 \equiv 0$ oder $3^2 = 9 \equiv 1 \pmod 4$. □

Beispiel 5.7 (LWA 2010/1, Birgit Vera Schmidt)**.** Man zeige, dass 2010 nicht als Differenz zweier Quadratzahlen dargestellt werden kann.

A Lösungen

Lösung von Beispiel 3.3. Wir unterscheiden zwei Fälle.

Fall 1 Es sei n ungerade. Dann ist auch der zweitgrößte Teiler von n ungerade und die Summe daher gerade, also nicht 2013. Es gibt also keine ungerade Lösung.

Fall 2 Es sei n gerade. Dann ist der zweitgrößte Teiler von n gleich $\frac{n}{2}$. Dann haben wir die Gleichung $n + \frac{n}{2} = 2013$ zu lösen. Diese Gleichung hat genau eine Lösung, nämlich 1342, und das ist auch eine gerade Zahl.

Daher ist 1342 die (einzige) Lösung unserer Aufgabe. □

Lösung von Beispiel 4.4. Aus $8b = 7 \cdot (2c + 4d - a)$ und $\mathrm{ggT}(7, 8) = 1$ erkennt man nach dem Fundamentallemma der Arithmetik (Satz 4.3), dass b durch 7 teilbar sein muss. Folglich ist $b = 7e$, e ganz. Damit wird die gegebene Gleichung zu

$$a + 8e = 2c + 4d.$$

Daraus folgt sofort, dass a durch 2 teilbar sein muss. Die Behauptung $14 \mid a \cdot b$ ergibt sich schließlich wegen $\mathrm{ggT}(2, 7) = 1$. □

Lösung von Beispiel 5.7. Wir nehmen an, dass es zwei solche Quadratzahlen gibt, dass also

$$x^2 - y^2 = 2010$$

gilt.

Wir betrachten diese Gleichung modulo 4. Nach Satz 5.6 sind Quadrate ganzer Zahlen kongruent zu 0 oder zu 1 modulo 4.

Damit gibt es für die linke Seite die Möglichkeiten

$$\begin{aligned} 0 - 0 &\equiv 0 \pmod 4 \\ 0 - 1 &\equiv 3 \pmod 4 \\ 1 - 0 &\equiv 1 \pmod 4 \\ 1 - 1 &\equiv 0 \pmod 4 \end{aligned}$$

Da aber die rechte Seite $2010 \equiv 2 \pmod 4$ ist, ist die Gleichung modulo 4 niemals erfüllt. Damit gibt es keine derartigen Zahlen. □