

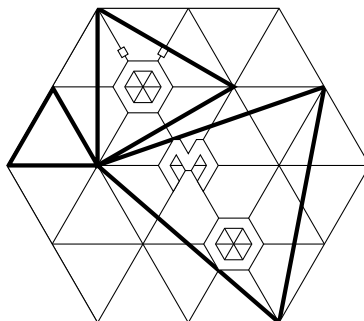
# Zahlentheorie für den Regionalwettbewerb für Fortgeschrittene der Österreichischen Mathematik-Olympiade

Clemens Heuberger\*

Version September 2019

## Inhaltsverzeichnis

<b>1</b>	<b>Zifferndarstellungen in anderen Basen</b>	<b>3</b>
<b>2</b>	<b>„Aufeinanderfolgende Quadrate“</b>	<b>3</b>
<b>3</b>	<b>Vertiefung Teilbarkeit</b>	<b>3</b>
<b>4</b>	<b>Elementare quadratische diophantische Gleichungen in zwei Variablen</b>	<b>4</b>
<b>5</b>	<b>Vertiefung Kongruenzen</b>	<b>6</b>
5.1	Division von Kongruenzen . . . . .	6
5.2	Periodizität von Potenzen modulo $m$ . . . . .	6
5.3	Kleiner Satz von Fermat . . . . .	7
<b>A</b>	<b>Lösungen</b>	<b>8</b>



---

\* Clemens Heuberger, Institut für Mathematik, Alpen-Adria-Universität Klagenfurt, Universitätsstraße 65–67, 9020 Klagenfurt am Wörthersee, [clemens.heuberger@aau.at](mailto:clemens.heuberger@aau.at).



# 1 Zifferndarstellungen in anderen Basen

**Satz 1.1.** Sei  $b \geq 2$ . Dann besitzt jede positive ganze Zahl  $n$  eine eindeutige Zifferndarstellung

$$n = a_\ell b^\ell + \dots + a_1 b^1 + a_0$$

zur Basis  $b$  mit  $a_j \in \{0, \dots, b-1\}$  und  $a_\ell \neq 0$ . Wir schreiben

$$n = (a_\ell a_{\ell-1} \dots a_1 a_0)_b.$$

Im Fall  $b = 2$  spricht man auch von der Binärdarstellung von  $n$ .

# 2 „Aufeinanderfolgende Quadrate“

Diese Methode, um zu zeigen, dass eine diophantische Gleichung unlösbar ist (bzw. um deren Lösungen zu beschränken), beruht auf dem folgenden einfachen Satz.

**Satz 2.1.** Seien  $b$  und  $x$  ganze Zahlen mit  $b^2 < x < (b+1)^2$ . Dann ist  $x$  kein vollständiges Quadrat.

Dieser Satz stellt eine Möglichkeit dar, folgende Aufgabe zu lösen.

**Beispiel 2.2** (LWA 2014/1, Walther Janous). Man bestimme alle Lösungen der Gleichung

$$a^2 = b \cdot (b+7)$$

mit ganzen Zahlen  $a \geq 0$  und  $b \geq 0$ .

# 3 Vertiefung Teilbarkeit

Der folgende Satz gibt beispielhaft einige Anwendungen der eindeutigen Primfaktordarstellung an.

**Satz 3.1.** Seien  $a$ ,  $b$  und  $c$  ganze Zahlen und  $p$  eine Primzahl.

1. Wenn  $\text{ggT}(a, b) = 1$  und  $ab = c^2$ , so sind auch  $a$  und  $b$  vollständige Quadrate.
2. Wenn  $p \mid a^2$ , dann gilt auch  $p^2 \mid a^2$ .
3. Es gilt  $a^3 \mid (3a)!$ .
4. Für  $1 \leq a \leq p-1$  ist der Binomialkoeffizient  $\binom{p}{a}$  durch  $p$  teilbar.

**Beispiel 3.2** (LWA 2014/1, Walther Janous). Man bestimme alle Lösungen der Gleichung

$$a^2 = b \cdot (b+7)$$

mit ganzen Zahlen  $a \geq 0$  und  $b \geq 0$ .

**Beispiel 3.3.** Man bestimme alle Lösungen der Gleichung

$$x^3 - y^3 = 19$$

in ganzen Zahlen  $x$  und  $y$ .

## 4 Elementare quadratische diophantische Gleichungen in zwei Variablen

Das folgende Beispiel soll aufzeigen, welcher Typ von Gleichungen und Umformungen in diesem Abschnitt behandelt werden.

**Beispiel 4.1.** Man bestimme alle natürlichen Zahlen  $x$  und  $y$  mit

$$9x^2 - 6xy - 15y^2 - 12x - 28y = 29.$$

*Lösung 1.* Wir fassen zunächst derart zu einem vollständigen Quadrat zusammen, dass alle Vorkommissen von  $x$  in einem Quadrat zusammengefasst werden. Es geht also darum, die Terme  $9x^2$ ,  $-6xy$  sowie  $-12x$  zu behandeln. Glücklicherweise ist  $9 = 3^2$  und 3 sowohl in  $-6xy$  als auch in  $-12x$  enthalten, sodass wir direkt zusammenfassen können:

$$9x^2 - 6xy - 12x = (3x - y - 2)^2 - y^2 - 4 - 4y.$$

Wir setzen  $3x - y - 2 = a$  und erhalten damit aus der ursprünglichen Gleichung

$$a^2 - 16y^2 - 32y = 33.$$

Wir fassen neuerlich zu einem vollständigen Quadrat zusammen:

$$16y^2 + 32y = 16(y + 1)^2 - 16$$

Wir erhalten deshalb mit der Substitution  $b = y + 1$  die Gleichung

$$a^2 - 16b^2 = 17.$$

Glücklicherweise ist 16 ein vollständiges Quadrat, wir können damit die linke Seite faktorisieren:

$$(a - 4b)(a + 4b) = 17.$$

Da  $b = y + 1$  und  $y \geq 0$ , ist  $b \geq 1$ , somit gilt  $a - 4b < a + 4b$ . Weiters ist 17 eine Primzahl, wir können damit 17 nur als Produkt  $17 = 1 \cdot 17$  oder  $17 = (-1)(-17)$  schreiben.

Im ersten Fall erhalten wir

$$\begin{aligned} a - 4b &= 1 \\ a + 4b &= 17 \end{aligned}$$

und nach Addition der beiden Gleichungen  $2a = 18$ , also  $a = 9$  und damit aus der ersten Gleichung  $b = 2$ . Es ergibt sich  $y + 1 = b = 2$  und damit  $y = 1$  und  $3x - y - 2 = a = 9$  und damit  $3x = 12$  und  $x = 4$ . Wir haben somit das Lösungspaar  $(x, y) = (4, 1)$  erhalten.

Im zweiten Fall erhalten wir

$$\begin{aligned} a - 4b &= -17 \\ a + 4b &= -1, \end{aligned}$$

$2a = -18$ ,  $a = -9$  und daraus  $b = 2$  und  $y = 1$ . Es ergibt sich  $3x - y - 2 = -9$  und daraus  $3x = -6$ , Widerspruch zu  $x \geq 0$ .

Wir haben damit genau eine Lösung  $(x, y) = (4, 1)$  erhalten.  $\square$

*Lösung 2.* Alternativ kann man die ursprüngliche Gleichung als quadratische Gleichung

$$9x^2 + (-6y - 12)x + (-15y^2 - 28y - 29) = 0$$

in  $x$  sehen und diese über die Lösungsformel lösen:

$$\begin{aligned} x &= \frac{-(-6y - 12) \pm \sqrt{(-6y - 12)^2 - 4 \cdot 9 \cdot (-15y^2 - 28y - 29)}}{18} \\ &= \frac{6y + 12 \pm \sqrt{36(y^2 + 4y + 4 + 15y^2 + 28y + 29)}}{18} = \frac{y + 2 \pm \sqrt{16y^2 + 32y + 33}}{3}. \end{aligned} \quad (1)$$

Da  $x$  eine ganze Zahl ist, ist  $16y^2 + 32y + 33$  ein vollständiges Quadrat, also

$$16y^2 + 32y + 33 = a^2$$

für eine natürliche Zahl  $a$ .

Wir sehen nun diese Gleichung als quadratische Gleichung in  $y$ , lösen sie mit der quadratischen Lösungsformel und erhalten

$$y = \frac{-32 \pm \sqrt{(32)^2 - 4 \cdot 16 \cdot (33 - a^2)}}{32} = \frac{-32 \pm \sqrt{64(16 - 33 + a^2)}}{32} = \frac{-4 \pm \sqrt{a^2 - 17}}{4}.$$

Da  $y$  eine ganze Zahl ist, ist  $a^2 - 17$  ein vollständiges Quadrat, es gibt somit eine natürliche Zahl  $c$  mit  $a^2 - 17 = c^2$ . Wir schreiben diese Gleichung als

$$(a - c)(a + c) = a^2 - c^2 = 17$$

um. Da  $a$  und  $c$  natürliche Zahlen sind und 17 eine Primzahl ist, sind  $a + c \geq 0$  und  $a + c \geq a - c$ , somit folgen  $a + c = 17$  und  $a - c = 1$ , somit  $2a = 18$ ,  $a = 9$  und  $c = 8$ .

Wir erhalten

$$y = \frac{-4 \pm 8}{4}$$

und damit wegen  $y \geq 0$  den Wert  $y = 1$ . Aus (1) folgt dann

$$x = \frac{3 \pm 9}{3}$$

und damit wegen  $x \geq 0$  der Wert  $x = 4$ .

Somit haben wir das Lösungspaar  $(x, y) = (4, 1)$  erhalten.  $\square$

Analog kann man jede quadratische diophantische Gleichung in zwei Unbekannten

$$ax^2 + bxy + cy^2 + dx + ey + f = 0 \quad (2)$$

mit bekannten ganzzahligen  $a, \dots, e$  und  $f$  und Unbekannten  $x$  und  $y$  umformen. Man erhält schließlich die Gleichung

$$X^2 + AY^2 = B \quad (3)$$

oder die Gleichung

$$X^2 + CY = B \quad (4)$$

für passende ganze Zahlen  $A, B$  und  $C$ .

Die Gleichung (4) ist äquivalent zur Kongruenz  $X^2 \equiv B \pmod{C}$ , damit gibt es entweder keine Lösung oder endlich viele Lösungen modulo  $C$ .

Wenn  $A > 0$ , so ist die Gleichung (3) offensichtlich nur für  $B \geq 0$  lösbar. In diesem Fall gibt es endlich viele Lösungen, weil  $|Y|$  durch  $\sqrt{B/A}$  beschränkt ist.

Wenn  $A < 0$  und  $A = -E^2$  für eine ganze Zahl  $E$  ist, so kann die linke Seite von (3) faktorisiert werden. Man erhält aus der Primfaktorzerlegung von  $B$  endlich viele Lösungen.

Wenn schließlich  $A = -D$  für eine positive ganze Zahl  $D$  ist, die kein Quadrat ist, so nennt man die Gleichung *Pellsche Gleichung*. Diese gehört aber nicht zum Curriculum eines Regionalwettbewerbs.

**Beispiel 4.2** (LWA 2014/1, Walther Janous). Man bestimme alle Lösungen der Gleichung

$$a^2 = b \cdot (b + 7)$$

mit ganzen Zahlen  $a \geq 0$  und  $b \geq 0$ .

Manche dieser Methoden lassen sich auch auf mehr als zwei Variablen verallgemeinern:

**Beispiel 4.3.** Man bestimme alle ganzen Zahlen  $x, y$  und  $z$  mit  $x^2 + y^2 + z^2 = 10$ .

## 5 Vertiefung Kongruenzen

### 5.1 Division von Kongruenzen

Bekanntlich darf man Kongruenzen addieren, subtrahieren und multiplizieren. Hier soll geklärt werden, wie mit der Division von Kongruenzen umzugehen ist.

**Satz 5.1.** Seien  $a, b, c$  und  $m$  ganze Zahlen.

1. Wenn  $\text{ggT}(c, m) = 1$ , so sind  $ac \equiv bc \pmod{m}$  und  $a \equiv b \pmod{m}$  äquivalent.
2. Wenn  $c \neq 0$ , so sind  $ac \equiv bc \pmod{mc}$  und  $a \equiv b \pmod{m}$  äquivalent.
3. Wenn  $c \neq 0$ , so sind  $ac \equiv bc \pmod{m}$  und  $a \equiv b \pmod{m'}$  mit  $m' = m/\text{ggT}(m, c)$  äquivalent.

*Beweis.* 1. Da  $\text{ggT}(m, c) = 1$ , sind die folgenden Aussagen äquivalent:

$$ac \equiv bc \pmod{m} \iff m \mid c(a - b) \iff m \mid (a - b) \iff a \equiv b \pmod{m}.$$

2. Für  $c \neq 0$  sind die folgenden Aussagen äquivalent:

$$ac \equiv bc \pmod{mc} \iff mc \mid c(a - b) \iff m \mid (a - b) \iff a \equiv b \pmod{m}.$$

3. Für  $c \neq 0$  setzen wir  $d = \text{ggT}(c, m)$  sowie  $c = dc'$  und  $m = dm'$ . Dann ist  $\text{ggT}(c', m') = 1$ . Es gilt

$$\begin{aligned} ac \equiv bc \pmod{m} &\iff adc' \equiv bdc' \pmod{dm'} \iff ac' \equiv bc' \pmod{m'} \\ &\iff a \equiv b \pmod{m'}, \end{aligned}$$

wobei nacheinander der zweite und der erste Punkt verwendet wurden. □

### 5.2 Periodizität von Potenzen modulo $m$

Wir betrachten hier eine positive ganze Zahl  $m$  und für eine ganze Zahl  $a$  die Folge der Potenzen  $a^n$  modulo  $m$ .

Als Beispiel betrachten wir  $m = 12$  und  $a \in \{3, 5\}$ .

$n$	0	1	2	3	4	...
$3^n \pmod{12}$	1	3	9	3	9	...
$5^n \pmod{12}$	1	5	1	5	1	...

Wir sehen hier, dass  $3^n \pmod{12}$  gemischt periodisch mit Vorperiodenlänge 1 und Periodenlänge 2 ist, wohingegen  $5^n$  rein periodisch mit Periodenlänge 2 ist.

Dass dies ein allgemeines Phänomen ist, lehrt der folgende Satz.

**Satz 5.2.** Seien  $a \in \mathbb{Z}$  und  $m$  eine positive ganze Zahl.

1. Die Folge  $(a^n)_{n \in \mathbb{N}}$  ist periodisch modulo  $m$ , d.h., es gibt ein  $N \in \mathbb{N}$  und ein  $\ell > 0$ , sodass

$$a^{n+\ell} \equiv a^n \pmod{m}$$

für alle  $n \geq N$  gilt.

2. Falls  $\text{ggT}(a, m) = 1$ , so ist die Folge rein periodisch, d.h. es gibt ein  $\ell > 0$ , sodass

$$a^{n+\ell} \equiv a^n \pmod{m}$$

für alle  $n \in \mathbb{N}$  gilt (das entspricht  $N = 0$  in obiger Notation).

*Beweis.* 1. Da es nur endlich viele Reste modulo  $m$  gibt, muss es ein  $\ell > 0$  und ein  $N \geq 0$  geben, sodass

$$a^{N+\ell} \equiv a^N \pmod{m} \tag{5}$$

gilt. Für alle  $n \geq N$  gilt dann (durch Multiplikation mit  $a^{n-N}$ ), dass  $a^{n+\ell} \equiv a^n \pmod{m}$ .

2. Da  $\text{ggT}(a, m) = 1$ , gilt auch  $\text{ggT}(a^N, m) = 1$  und wir dürfen  $a^N$  aus (5) kürzen. Somit gilt  $a^\ell \equiv a^0 = 1 \pmod{m}$ . Durch Multiplikation mit  $a^n$  erhalten wir das gewünschte Resultat.  $\square$

**Beispiel 5.3.** Man bestimme die Einerziffer von  $2^{3^{2015}}$ .

### 5.3 Kleiner Satz von Fermat

Satz (5) zeigt, dass es für  $\text{ggT}(a, m)$  ein  $\ell > 0$  gibt, sodass  $a^\ell \equiv a^0 = 1 \pmod{m}$  gilt, macht aber keinerlei Aussage über dieses  $\ell$ . Wir zeigen nun, dass im Fall eines Primzahlmoduls mehr ausgesagt werden kann.

**Satz 5.4** (Fermat). *Seien  $p$  eine Primzahl und  $a$  eine nicht durch  $p$  teilbare ganze Zahl. Dann gilt*

$$a^{p-1} \equiv 1 \pmod{p}. \tag{6}$$

*Beweis.* Wir betrachten die Zahlen  $1a, 2a, 3a, \dots, (p-1)a$ . Diese sind zu  $p$  teilerfremd, weil  $\text{ggT}(a, p) = 1$  nach Voraussetzung und  $\text{ggT}(j, p) = 1$  für  $1 \leq j \leq p-1$  gilt. Weiters sind die genannten Zahlen paarweise inkongruent modulo  $p$ : gälte nämlich  $ja \equiv ka \pmod{p}$  für gewisse  $0 < j < k < p$ , so wäre  $j \equiv k \pmod{p}$  nach Satz 5.1, ein Widerspruch zum gewählten Bereich von  $j$  und  $k$ .

Da nun die  $p-1$  Zahlen  $1a, 2a, \dots, (p-1)a$  paarweise inkongruent modulo  $p$  und zu  $p$  teilerfremd sind, müssen sie alle Reste modulo  $p$  außer 0 durchlaufen.

Multipliziert man alle diese Zahlen zusammen, so erhält man

$$(1a)(2a)(3a)\dots((p-1)a) \equiv 1 \cdot 2 \cdot 3 \dots (p-1) \pmod{p},$$

weil ja links und rechts die gleichen Reste modulo  $p$  (lediglich in unterschiedlicher Reihenfolge) stehen.

Wir fassen die Faktoren  $a$  auf der linken Seite zusammen und erhalten

$$a^{p-1}(1 \cdot 2 \cdot 3 \dots (p-1)) \equiv 1 \cdot 2 \cdot 3 \dots (p-1) \pmod{p}.$$

Da  $1 \cdot 2 \cdot 3 \dots (p-1)$  zu  $p$  teilerfremd ist, dürfen wir dieses Produkt nach Satz 5.1 kürzen und erhalten wie gefordert

$$a^{p-1} \equiv 1 \pmod{p}. \tag{6}$$

$\square$

Multipliziert man (6) mit  $a$ , erhält man folgende Folgerung, die offensichtlich auch für  $a \equiv 0 \pmod{p}$  gilt.

**Korollar 5.5.** Seien  $p$  eine Primzahl und  $a \in \mathbb{Z}$ , so gilt

$$a^p \equiv a \pmod{p}. \quad (7)$$

Tatsächlich ist diese Folgerung äquivalent zur Aussage des kleinen Satzes von Fermat, da für  $p \nmid a$  der Faktor  $a$  auch wieder gekürzt werden darf.

Wir geben einen unabhängigen Beweis des Korollars (und damit des kleinen Satzes von Fermat).

*Beweis 2 von Korollar 5.5.* Wir beweisen das Korollar durch Induktion nach  $a$ .

Für  $a = 0$  ist  $0^p \equiv 0 \pmod{p}$  zu zeigen, was jedenfalls wahr ist.

Wir nehmen nun an, dass (7) für ein  $a \in \mathbb{N}$  gelte. Dann gilt nach dem binomischen Lehrsatz und Satz 3.1, dass

$$(a+1)^p \equiv \sum_{j=0}^p \binom{p}{j} a^j 1^{p-j} \equiv a^0 + a^p \equiv 1 + a \pmod{p},$$

weil ja  $\binom{p}{j}$  für alle bis auf den ersten und letzten Summanden modulo  $p$  wegfällt und  $a^p \equiv a \pmod{p}$  laut Induktionsannahme gilt. Damit gilt (7) auch für  $a+1$ .

Die Erweiterung auf  $a \in \mathbb{Z}$  folgt daraus, dass es bei der Aussage nur um Reste modulo  $p$  geht.  $\square$

## A Lösungen

*Lösung von Beispiel 2.2.* Für  $b \geq 10$  gilt

$$(b+3)^2 = b^2 + 6b + 9 < b^2 + 7b < b^2 + 8b + 16 = (b+4)^2,$$

somit kann  $b^2 + 7b$  kein Quadrat sein und die Gleichung  $a^2 = b(b+7)$  hat somit keine Lösungen  $b \geq 10$ .

Für  $b \in \{0, \dots, 9\}$  erhält man

$b$	0	1	2	3	4	5	6	7	8	9
$b(b+7)$	0	8	18	30	44	60	78	98	120	144
$a$	0	—	—	—	—	—	—	—	—	12

Die einzigen Lösungen sind damit  $(a, b) \in \{(0, 0), (12, 9)\}$ .  $\square$

*Lösung von Beispiel 3.2.* Sei  $d = \text{ggT}(b, b+7)$ . Da  $d \mid (b+7)$  und  $d \mid b$ , gilt auch  $d \mid ((b+7) - b) = 7$ , somit  $d = \text{ggT}(b, b+7) \in \{1, 7\}$ . Wir unterscheiden diese beiden Fälle.

1. Es gelte  $\text{ggT}(b, b+7) = 1$ . Dann folgt

$$\begin{aligned} b &= x^2, \\ b+7 &= y^2 \end{aligned}$$

für passende ganze Zahlen  $x$  und  $y$  mit  $0 \leq x < y$ . Es folgt

$$7 = y^2 - x^2 = (y-x)(y+x).$$

Da beide Faktoren der rechten Seite positiv sind und 7 eine Primzahl ist, folgt  $y-x=1$  und  $y+x=7$  und somit  $y=4$ ,  $x=3$ ,  $b=9$ ,  $b+7=16$  und  $a=xy=12$ .

2. Es gelte  $\text{ggT}(b, b+7) = 7$ . Dann folgt

$$\begin{aligned} b &= 7x^2, \\ b+7 &= 7y^2 \end{aligned}$$



für passende ganze Zahlen  $x$  und  $y$  mit  $0 \leq x < y$ . Es folgt

$$7 = 7y^2 - 7x^2 = 7(y-x)(y+x) \iff 1 = (y-x)(y+x).$$

Die einzige mögliche Faktorisierung ist  $y-x = y+x = 1$ , also  $x = 0$  und  $y = 1$ , woraus sich  $b = 0$  und  $a = 0$  ergeben.

Die einzigen beiden Lösungen  $(a, b)$  sind somit  $(0, 0)$  und  $(12, 9)$ .  $\square$

*Lösung von Beispiel 3.3.* Aus  $x^3 - y^3 = 19$  ergibt sich wegen der Monotonie der dritten Potenz sofort  $x > y$ .

Faktorisieren der linken Seite ergibt

$$(x-y)(x^2 + xy + y^2) = 19.$$

Da 19 eine Primzahl ist und  $x > y$ , folgt  $x-y \in \{1, 19\}$ .

Für  $x-y = 19$  ergibt sich

$$\begin{aligned} 1 &= x^2 + xy + y^2 = (y+19)^2 + y(y+19) + y^2 = 3y^2 + 57y + 361 \\ &= 3\left(y + \frac{19}{2}\right)^2 + \frac{361}{4} \geq \frac{361}{4} > 1, \end{aligned}$$

ein Widerspruch.

Daher muss  $x-y = 1$  gelten. Es ergibt sich

$$19 = x^2 + xy + y^2 = (y+1)^2 + y(y+1) + y^2 = 3y^2 + 3y + 1,$$

was zu

$$y^2 + y - 6 = 0$$

äquivalent ist. Es ergeben sich  $y = -3$  und  $y = 2$  und daraus die Lösungspaare  $(x, y) \in \{(-2, -3), (3, 2)\}$ .  $\square$

*Lösung von Beispiel 4.2.* Löst man  $b^2 + 7b - a^2 = 0$  nach  $b$  auf, erhält man

$$b = -\frac{7}{2} \pm \frac{\sqrt{49 + 4a^2}}{2}$$

Daher muss  $49 + 4a^2$  eine Quadratzahl sein. Sei  $49 + 4a^2 = x^2$  für ein  $x > 0$ , dann gilt

$$49 = x^2 - 4a^2 = (x+2a) \cdot (x-2a).$$

Da  $x > 0$  und  $a \geq 0$ , ist auch  $x+2a > 0$  und damit auch  $x-2a = 49/(x+2a) > 0$ . Man kann 49 auf zwei Arten in positive Faktoren zerlegen ( $7 \cdot 7$  oder  $49 \cdot 1$ ). Außerdem gilt wegen  $a \geq 0$ , dass  $x+2a \geq x-2a$ . Im ersten Fall erhält man  $a = 0$ , im zweiten  $a = 12$ . Insgesamt erhält man die Lösungspaare  $(a, b) = (0, 0)$  bzw.  $(12, 9)$ .  $\square$

*Lösung von Beispiel 4.3.* Mit  $(x, y, z)$  ist auch  $(\pm x, \pm y, \pm z)$  (mit unabhängigen Vorzeichen) eine Lösung der gegebenen Gleichung. Weiters ist die Gleichung symmetrisch in  $x, y, z$ . Wir können daher ohne Beschränkung der Allgemeinheit  $0 \leq x \leq y \leq z$  voraussetzen.

Es ergibt sich

$$z^2 \leq 10 = x^2 + y^2 + z^2 \leq 3z^2,$$

woraus  $2 \leq z \leq 3$  folgt.

Im Fall  $z = 3$  ergibt sich  $x^2 + y^2 = 1$ , woraus sich sofort  $x = 0$  und  $y = 1$  ergeben.

Im Fall  $z = 2$  ergibt sich  $x^2 + y^2 = 6$ . Wir erhalten wie vorhin

$$y^2 \leq 6 = x^2 + y^2 \leq 2y^2$$

und damit  $2 \leq y \leq 2$ , also  $y = 2$  und  $x^2 = 2$ , ein Widerspruch.

Wir erhalten damit die Lösungstriple

$$(x, y, z) \in \{(0, \pm 1, \pm 3), (\pm 1, 0, \pm 3), (0, \pm 3, \pm 1), (\pm 1, \pm 3, 0), (\pm 3, 0, \pm 1), (\pm 3, \pm 1, 0)\},$$

wobei alle Vorzeichen unabhängig sind. □

*Lösung von Beispiel 5.3.* Wir betrachten  $2^k$  modulo 10:

$k$	0	1	2	3	4	5
$2^k \pmod{10}$	1	2	4	8	6	2

Die Zweierpotenzen sind daher modulo 10 gemischt periodisch mit Periodenlänge 4 und Vorperiodenlänge 1.

Wir müssen daher  $3^{2015}$  modulo 4 bestimmen. Da  $3 \equiv -1 \pmod{4}$ , ist  $3^{2015} \equiv -1 \pmod{4} \equiv 3 \pmod{4}$ . Daher gilt

$$2^{3^{2015}} \equiv 2^3 = 8 \pmod{10}.$$

□