

Eric Müller

## Vollständige Induktion

Nach GIUSEPPE PEANO (1858 - 1932) kann man die Menge  $N$  der natürlichen Zahlen durch folgende Axiome definieren [1]:

1. 1 ist eine natürliche Zahl.
2. Zu jeder natürlichen Zahl  $n$  gibt es genau eine weitere, ihren Nachfolger  $n' = n+1$ .
3. Stets ist  $n' \neq 1$ .
4. Aus  $n' = m'$  folgt  $n = m$ .
5. Ist  $M$  eine Menge natürlicher Zahlen mit den Eigenschaften:
  - a) 1 gehört zu  $M$ ,
  - b) wenn  $n$  zu  $M$  gehört, so gehört auch  $n+1$  zu  $M$ ,
 dann umfasst  $M$  alle natürlichen Zahlen.

Auf dem fünften Axiom beruht das Verfahren der vollständigen Induktion, mit der man Aussagen und Formeln für alle natürlichen Zahlen beweisen kann. Es eignet sich besonders für solche Aussagen, die man leichter für eine gegebene natürliche Zahl beweisen kann, wenn man bereits die Gültigkeit für kleinere Zahlen, insbesondere die nächstkleinere Zahl, voraussetzen kann. Insbesondere eignet sich die vollständige Induktion zum Beweis von Eigenschaften rekursiv definierter Folgen.

Das Grundprinzip sieht folgendermaßen aus:

1. Man beweist die Aussage/Formel für die Zahl 1 (**Induktionsanfang** oder **Verankerung**).
2. Man nimmt an, die Aussage/Formel gelte bereits für eine natürliche Zahl  $n$  (**Induktionsannahme**).
3. Man folgert die Gültigkeit für die nächste natürliche Zahl  $n+1$  (**Induktionsschritt**).

Die Erfüllungsmenge der Aussage/Formel genügt dann sämtlichen Bedingungen des fünften Axioms von PEANO, ist also bereits  $N$ , so dass die Aussage/Formel für alle natürlichen Zahlen gilt.

Anschaulich kann man sich eine Folge dicht hintereinander senkrecht stehender Dominosteine vorstellen; stößt man den ersten Stein an, wirft er den nächsten mit um, dieser wieder den nächsten, so dass schließlich alle Steine umgefallen sind. Dem Induktionsanfang entspricht das Anstoßen des ersten Steines, und für den „Induktionsschritt“ ist es notwendig, dass die Steine so dicht hintereinander stehen, dass ein Stein im Fallen den nächsten umwerfen kann.

*Aufgabe:*

Zeige, dass für alle natürlichen Zahlen  $n$  folgende Formel gilt:

$$1^2 + 2^2 + \dots + n^2 = \frac{1}{6} n(n+1)(2n+1)$$

*Lösung:*

Beweis mit vollständiger Induktion nach  $n$ :

- Induktionsanfang: Für  $n=1$  hat die linke Seite den Wert 1, die rechte ist gleich

$$\frac{1}{6} \cdot 1 \cdot 2 \cdot 3 = 1.$$

- Induktionsannahme: Die Formel gelte für  $n = k$ .
- Induktionsschritt: Gültigkeit der Formel für  $k+1$ :

$$\begin{aligned} 1^2 + 2^2 + \dots + k^2 + (k+1)^2 &= \\ \frac{k(k+1)(2k+1)}{6} + (k+1)^2 &= \frac{k(k+1)(2k+1) + 6(k+1)^2}{6} = \\ = \frac{(k+1)(k(2k+1) + 6(k+1))}{6} &= \frac{(k+1)(2k^2 + k + 6k + 6)}{6} = \frac{(k+1)(k+2)(2k+3)}{6} \end{aligned}$$

Die Formel gilt also auch für  $k+1$ .

*Aufgabe:*

Die Folge  $\{a_n\}$  sei definiert durch  $a_1 = 2$ ,  $a_{n+1} = 3a_n - 2$  für alle natürlichen  $n$ . Zeige, dass für alle  $n$  gilt:  $a_n = 3^{n-1} + 1$ .

*Lösung:*

*Beweis mit vollständiger Induktion nach  $n$ :*

- Induktionsanfang: Für  $n = 1$  gilt  $a_1 = 2 = 3^0 + 1$
- Induktionsannahme: Die Formel gelte für  $n = k$ .
- Induktionsschritt: Dann gilt:  $a_{k+1} = 3a_k - 2 = 3(3^{k-1} + 1) - 2 = 3^k + 1 = 3^{(k+1)-1} + 1$

Der Induktionsanfang muss aber nicht unbedingt an der Stelle 1 erfolgen. Kann man den Induktionsanfang für eine natürliche (oder ganze) Zahl  $k_0$  zeigen und den Induktionsschritt von  $n$  auf  $n+1$  für alle  $n \geq k_0$  durchführen, so gilt die Aussage/Formel für alle natürlichen (oder ganzen) Zahlen größer oder gleich  $k_0$ .

*Aufgabe:*

Für welche natürlichen  $n$  gilt  $2^n > n^2$ ?

*Lösung:*

Untersuchung mit vollständiger Induktion;

- der Induktionsanfang ist offenbar möglich für  $n = 1$ .
- Induktionsannahme: Die Ungleichung gelte für  $n = k$ .
- Zum Induktionsschritt:

Dann ist  $2^{k+1} \geq 2 \cdot 2^k > 2k^2$ . Wäre letzteres größer oder gleich  $(k+1)^2$ , würde der Induktionsschritt funktionieren. Es ist

$$2k^2 \geq (k+1)^2 \Leftrightarrow 2k^2 \geq k^2 + 2k + 1 \Leftrightarrow k^2 - 2k + 1 \geq 2 \Leftrightarrow (k-1)^2 \geq 2.$$

Dies ist also erst möglich für  $k > 3$ . Somit passt obiger Induktionsanfang nicht zum Induktionsschritt, man muss also neu verankern. Für die Werte 2, 3 und 4 gilt die Ungleichung nicht, aber für  $n = 5$  ist  $2^5 = 32 > 25 = 5^2$ ; dies passt zum Induktionsschritt, der für  $n \geq 5$  möglich ist. Die Ungleichung stimmt also für  $n = 1$  und  $n \geq 5$ .

Kann man eine Aussage/Formel für die Zahl  $k_0$  zeigen und folgt aus der Gültigkeit für eine Zahl  $n$  die für die Zahl  $n+2$ , so gilt die Aussage/Formel für alle geraden bzw. ungeraden Zahlen der Form  $k_0 + 2l$  mit  $l \in \mathbb{N}_0$  (Hierbei steht  $\mathbb{N}_0$  für  $\mathbb{N} \cup \{0\}$ ). Man kann diesen Fall natürlich auch durch eine Parametertransformation in den Ausgangsfall überführen.

*Aufgabe:*

Für alle geraden  $n \in \mathbb{N}$  ist  $n(n+2)$  ein Vielfaches von 8.

*Lösung:*

Beweis mit vollständiger Induktion:

- Induktionsanfang für  $n=2$ :  $2(2+2)=8$ .
- Induktionsannahme: Für gerades  $n=k$  sei  $n(n+2)$  Vielfaches von 8.
- Induktionsschritt: Die Aussage gilt für  $k+2$ . Es ist  
 $(k+2)(k+4) = k^2 + 6k + 8 = k(k+2) + 4k + 8 = k(k+2) + 4(k+2)$ .  
 Da  $k$  gerade ist, ist auch  $k+2$  gerade, also  $4(k+2)$  durch 8 teilbar.  
 Da  $k(k+2)$  nach Induktionsvoraussetzung durch 8 teilbar ist, ist es auch die Summe  $(k+2)(k+4)$ .

Es ist auch erlaubt, dass man zum Beweis der Induktionsbehauptung zwei (oder auch mehrere) vorangegangene Werte benutzt, zum Beispiel also die Aussage/Formel für  $n+1$  mit Hilfe der Gültigkeit der Aussage für  $n$  und  $n-1$  beweist. Dazu muss man aber auch den Induktionsanfang für eine entsprechende Anzahl aufeinanderfolgender Zahlen durchführen. In das Grundschema lässt sich dieser Fall dadurch bringen, dass man als neue von  $n$  abhängige Aussage setzt: „Die ursprüngliche Aussage gilt für die Werte  $n$  und  $n+1$ “. Die neue Induktionsvoraussetzung lautet dann, dass die ursprüngliche Aussage für die Werte  $k$  und  $k+1$  gilt, und zu zeigen ist die neue Induktionsbehauptung, dass die ursprüngliche Aussage/Formel für die Werte  $k+1$  und  $k+2$  gilt. Die Gültigkeit für den Wert  $k+1$  ist aber aus der Induktionsvoraussetzung bereits klar. Analog läuft dies ab, wenn man mehr als zwei vorangegangene Werte benötigt.

*Aufgabe:*

Die Folge  $\{a_n\}$  sei definiert durch  $a_0 = 2$ ,  $a_1 = 5$  und  $a_{n+1} = 5a_n - 6a_{n-1}$  für  $n \in \mathbb{N}$ .  
 Zeige: Für alle  $n \in \mathbb{N}_0$  gilt  $a_n = 2^n + 3^n$ .

*Lösung:*

Beweis mit vollständiger Induktion nach  $n$ :

- Induktionsanfang für  $n=0$  und  $n=1$ :  $a_0 = 2 = 2^0 + 3^0$ ,  $a_1 = 5 = 2^1 + 3^1$ .
- Induktionsannahme: Die Formel gelte für  $n=k$  und  $n=k+1$ , wobei  $k \in \mathbb{N}_0$ .
- Induktionsschritt: Die Formel ist richtig für  $k+2$ :  
 $a_{k+2} = 5a_{k+1} - 6a_k = 5(2^{k+1} + 3^{k+1}) - 6(2^k + 3^k) = 2^{k+2} + 3^{k+2}$

*Aufgabe:*

Es sei  $x$  eine von 0 verschiedene reelle Zahl, für die  $x+1/x$  ganzzahlig ist. Zeige, dass dann auch  $x^n + 1/x^n$  für alle  $n \in \mathbb{N}_0$  ganzzahlig ist.

*Lösung:*

Beweis mit vollständiger Induktion nach  $n$ :

- Induktionsanfang für  $n=1$  ist klar und für  $n=0$  möglich wegen  $x^0 + 1/x^0 = 1 + 1 = 2$ .
- Induktionsannahme: Die Aussage gelte für  $n=k$  und  $n=k-1$  mit  $k \in \mathbb{N}$ .
- Induktionsschritt: Dann ist  
 $x^{k+1} + 1/x^{k+1} = (x^k + 1/x^k)(x + 1/x) - (x^{k-1} + 1/x^{k-1})$ .  
 Da auf der rechten Seite ganze Zahlen stehen, ist auch die linke Seite ganzzahlig.

Es ist auch möglich, die Aussage/Formel für eine Zahl  $k_0$  zu beweisen und für die Induktionsbehauptung für  $m+1$  die Gültigkeit der Aussage/Formel für alle Zahlen von  $k_0$  bis einschließlich  $m$  vorauszusetzen (denn dafür hat man die Gültigkeit ja bereits gezeigt).

Auf den Standardfall kann man dies dadurch zurückführen, dass man als neue von  $n$  abhängige Aussage setzt, dass die ursprüngliche Aussage für alle Zahlen von  $k_0$  bis einschließlich  $k_0 + n - 1$  gilt.

*Aufgabe:*

Jedes (nicht notwendig konvexe) Vieleck lässt sich in Dreiecke zerlegen.

*Lösung:*

Beweis mit vollständiger Induktion nach der Eckenzahl  $n$  des Vielecks.

- Induktionsanfang: Für  $n=3$  ist die Aussage offenbar erfüllt.
- Induktionsannahme: Die Aussage gelte für alle Vielecke mit  $n \leq k$  Ecken.
- Induktionsschritt: Gegeben sei ein  $(k+1)$ -Eck. Gelingt es, zwei nicht an derselben Kante liegende Ecken durch eine ganz im Vieleck liegende Strecke miteinander zu verbinden, wird das  $(k+1)$ -Eck in zwei Vielecke mit je höchstens  $k$  Ecken aufgeteilt, die sich nach Induktionsvoraussetzung in Dreiecke zerlegen lassen, somit auch das Ausgangsvieleck. Zu zeigen ist also nur noch die Existenz einer derartigen Sehne. Ist das  $(k+1)$ -Eck konvex, liegt die Verbindungsstrecke zweier Ecken nach Definition immer im Vieleck. Ist das  $(k+1)$ -Eck nicht konvex, gibt es mindestens eine Ecke  $E$  mit einem überstumpfen Innenwinkel. Ein von  $E$  ausgehender Strahl in das Feld dieses Innenwinkels schneidet den Rand des Vielecks erstmals wieder in einer Kante oder Ecke. Im letzteren Fall ist man fertig; im ersteren Fall kann man den Strahl in mindestens einer Richtung soweit im Winkelfeld drehen, dass eine Ecke erreicht wird (entweder eine Begrenzungsecke dieser Kante oder eine andere hineinragende Ecke), weil jede Kante nur unter einem höchstens stumpfen Winkel von einem nicht von einem nicht auf ihr liegenden Punkt zu sehen ist.

## Polynome

### 1. Bezeichnungen

Es seien  $n$  eine nicht negative ganze Zahl,  $a_0, a_1, a_2, \dots, a_n$  Zahlen aus  $Z, Q$  oder  $R$  und  $X$  eine Variable. Dann heißt ein Ausdruck

$$P(X) = a_n X^n + a_{n-1} X^{n-1} + \dots + a_1 X + a_0$$

oder kurz **P Polynom**, die Zahlen  $a_0, a_1, \dots, a_n$  heißen **Koeffizienten**,  $a_n$  heißt **Leitkoeffizient**,  $a_0$  heißt **konstanter Term**. Ist  $a_1 = 1$ , so heißt das Polynom **normiert**. Gilt  $a_n \neq 0$ , so ist  $n$  der **Grad** des Polynoms und wird mit  $\deg P$  bezeichnet.

Außerdem habe das **Nullpolynom**  $P(X) \equiv 0$  Grad Null. Die Polynome vom Grad 0 heißen **konstant**, solche vom Grad 1 **linear**, vom Grad 2 **quadratisch**, vom Grad 3 **kubisch**.

Kein Polynom sind Ausdrücke wie  $2+1/X$  oder unendliche Reihen wie  $1 + X + X^2 + X^3 + \dots$

Eine wichtige Eigenschaft von Polynomen ist (ohne Beweis):

**Satz:**

Zwei Polynome sind genau dann gleich, wenn sie gleichen Grad und gleiche Koeffizienten haben.

## 2. Operationen mit Polynomen

Man kann Polynome addieren, subtrahieren und multiplizieren:

$$(\sqrt{8}X + 2) + (5X^2 + 4) = 5X^2 + \sqrt{8}X + 6, \quad (X + 2)(X - 1) = X^2 + X - 2$$

Daneben gibt es noch eine Polynomdivision, die wie die Division ganzer Zahlen nicht immer ohne Rest abläuft, genauer gesagt, sind P und Q Polynome, wobei  $Q(X) \neq 0$ , gibt es Polynome S und R mit

$$P(X) = S(X)Q(X) + R(X),$$

wobei R das Nullpolynom ist oder einen Grad kleiner als deg Q hat. Zur praktischen Ausführung der Polynomdivision:

$$(X^4 + X^2 + 2) : (X^2 + X + 1) = X^2 - X + 1 + \frac{1}{X^2 + X + 1}$$

$$\begin{array}{r} X^4 + X^3 + X^2 \\ -X^3 \phantom{+ X^2} - X \\ \hline X^2 + X + 2 \\ -X^2 - X - 1 \\ \hline 1 \end{array}$$

## 3. Nullstellen von Polynomen

Setzt man in  $P(X)$  für die Variable X eine Zahl z ein, erhält man den Wert  $P(z)$  des Polynoms an der Stelle z. Ist insbesondere  $P(z) = 0$ , heißt z **Nullstelle** von P.

**Satz:**

Ist z eine Nullstelle von P, so enthält P den Faktor  $X - z$ .

*Beweis:*

Polynomdivision:  $P(X) = S(X)(X-z) + R(X)$ . Der Rest  $R(X)$  ist das Nullpolynom oder hat Grad kleiner als linear Polynom  $\deg(X-z)$ , ist also konstant. Setze z für X ein. Dann folgt  $R(z)=0$ ; R ist also das Nullpolynom.

Im allgemeinen ist es sehr schwierig, die Nullstellen eines Polynoms zu bestimmen. Allgemeine Lösungsformeln dafür gibt es nach GALOIS nur bis zum Grad 4, aber sie sind nur bis zum Grad 2 im Reellen handhabbar. Nicht jedes Polynom mit reellen Koeffizienten hat auch reelle Nullstellen, z. B. das Polynom  $X^2 + 1$  lässt sich nicht als Produkt linearer Polynome mit reellen Koeffizienten schreiben. Es gelten aber folgende Aussagen, die hier ohne Beweis angegeben werden:

**Satz:**

Es sei  $P$  ein Polynom mit reellen Koeffizienten. Gibt es zwei reelle Zahlen  $a$  und  $b$  mit  $a < b$ , so dass  $P(a)$  und  $P(b)$  verschiedene Vorzeichen haben, liegt im Intervall  $[a;b]$  mindestens eine Nullstelle von  $P$ .

**Satz:**

Jedes Polynom mit reellen Koeffizienten und ungeradem Grad hat mindestens eine reelle Nullstelle.

**Satz:**

Jedes Polynom mit reellen Koeffizienten lässt sich als Produkt linearer und quadratischer Polynome mit reellen Koeffizienten schreiben, wobei man es so einrichten kann, dass nur die quadratischen Polynome keine reellen Nullstellen haben.

Es gibt jedoch einige Sonderfälle, in denen Nullstellen auch von Polynomen vom Grad größer als 2 im Reellen berechnet werden können:

**Rationale Nullstellen von Polynomen mit ganzzahligen Koeffizienten****Satz:**

Es sei  $P(X) = a_n X^n + a_{n-1} X^{n-1} + \dots + a_1 X + a_0$  mit  $a_0 \neq 0$  ein Polynom mit ganzzahligen Koeffizienten mit rationaler Nullstelle  $p/q$ , wobei  $p, q$  ganze Zahlen sind und  $p$  und  $q$  teilerfremd. Dann wird  $a_0$  von  $p$  und  $a_n$  von  $q$  geteilt; insbesondere sind alle rationalen Nullstellen normierter Polynome mit ganzzahligen Koeffizienten ganzzahlig und teilen  $a_0$ .

*Beweis:*

$p/q$  ist eine Nullstelle, also

$$0 = a_n \frac{p^n}{q^n} + a_{n-1} \frac{p^{n-1}}{q^{n-1}} + \dots + a_1 \frac{p}{q} + a_0 \quad \Big| \cdot q^n$$

$$0 = a_n p^n + a_{n-1} p^{n-1} q + \dots + a_1 p q^{n-1} + a_0 q^n.$$

Somit ist  $p$  als Faktor in den ersten  $n$  Summanden enthalten und teilt damit auch  $a_0 q^n$ . Da  $p$  und  $q$  teilerfremd sind, teilt  $p$  auch  $a_0$ . Analog folgt, dass  $q$  den Koeffizienten  $a_n$  teilt.

**Beispiel:**

Das Polynom  $P(X) = X^3 - 5X^2 + X + 1$  hat keine rationalen Nullstellen, da  $P(1) = -2$  und  $P(-1) = -6$ .

Nullstellen von Polynomen mit ganzzahligen Koeffizienten lassen sich noch durch folgenden Satz ausschließen, der aber noch viele weitere Anwendungen hat:

**Satz:**

Es sei  $P$  ein Polynom mit ganzzahligen Koeffizienten, und  $a$  und  $b$  zwei verschiedene ganze Zahlen. Dann teilt  $a - b$  die Zahl  $P(a) - P(b)$ .

*Beweis:*

Für alle  $x, y$  aus  $\mathbb{R}$  und alle natürlichen Zahlen  $k$  gilt die Identität

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

Hiermit kann man aus  $P(a) - P(b)$  den Faktor  $a - b$  ausklammern.

**Beispiel:**

Es sei  $P$  ein Polynom mit ganzzahligen Koeffizienten und  $P(0) = 770$  sowie  $P(2) = 910$ . Zeige, dass 5 und 9 keine Nullstellen von  $P$  sein können.

*Lösung:*

Nach obigem Satz teilt  $5 - 2$  die Zahl  $P(5) - P(2)$ . Wäre 5 eine Nullstelle, folgte, dass 3 die Zahl  $-910$  teilt. Das ist ein Widerspruch. Außerdem müsste  $9 - 0$  die Zahl  $P(9) - P(0)$  teilen, wenn 9 eine Nullstelle wäre. Aber 9 teilt nicht  $-770$  (letzte Aussage folgt auch aus dem ersten Satz).

**Reziproke Polynome**

Ein Polynom  $P(X) = a_n X^n + a_{n-1} X^{n-1} + \dots + a_1 X + a_0$  heißt **reziprok**, wenn  $a_k = a_{n-k}$  für alle  $k = 0, 1, \dots, n$  gilt.

- Es sei  $P(X) = a_n X^n + a_{n-1} X^{n-1} + \dots + a_1 X + a_0$  reziprokes Polynom von ungeradem Grad  $n$ . Dann ist  $-1$  Nullstelle von  $P$ , denn es gilt  $P(-1) = -a_n + a_{n-1} - \dots - a_1 + a_0 = 0$ . Man kann also  $P(X) = (X + 1)S(X)$  schreiben, wobei  $S$  reziprokes Polynom von geradem Grad ist.
- Nun sei  $P(X) = a_n X^n + a_{n-1} X^{n-1} + \dots + a_1 X + a_0$  reziprokes Polynom von geradem Grad  $n = 2k$ . Wegen  $a_0 = a_n \neq 0$  kann  $P$  nicht die Nullstelle 0 haben. Es sei  $x$  Nullstelle. Dann ist

$$\begin{aligned} a_{2k} X^{2k} + a_{2k-1} X^{2k-1} + \dots + a_1 X + a_0 &= 0 & | :x^k \\ a_{2k} X^k + a_{2k-1} X^{k-1} + \dots + a_1 X^{1-k} + a_0 X^{-k} &= 0 \end{aligned}$$

Letztere Gleichung kann man wegen  $a_{2k-m} = a_m$  für  $m = 0, 1, \dots, 2k$  weiter zusammenfassen:

$$a_0(x^k + 1/x^k) + a_1(x^{k-1} + 1/x^{k-1}) + \dots + a_{k-1}(x + 1/x) + a_k = 0$$

Zur Umformung der letzten Gleichung setzt man zunächst  $s_m = x^m + 1/x^m$  für  $m \in \mathbb{N}_0$ . Man kann leicht folgende Beziehungen nachrechnen:

$$s_0 = 2, \quad s_1 = x + 1/x, \quad s_{m+1} = (x + 1/x)s_m - s_{m-1} \quad \text{für } m \in \mathbb{N}_0.$$

Damit kann man  $s_m$  für alle  $m \in \mathbb{N}_0$  in der Form

$$s_m = (x + 1/x)^m + b_{m-1}(x + 1/x)^{m-1} + \dots + b_1(x + 1/x) + b_0$$

mit ganzzahligen Koeffizienten  $b_0, b_1, \dots, b_{m-1}$  schreiben, wie man leicht mit vollständiger Induktion zeigen kann. Setzt man noch  $u = x + 1/x$ , kann man die Nullstellenbestimmung von  $P$  auf die Ermittlung der Nullstellen  $u$  eines Polynoms vom Grad  $k$  zurückführen.

**Beispiel:**

Bestimme die Nullstellen des Polynoms  $X^5 + 3X^4 - 20X^3 - 20X^2 + 3X + 1$ .

*Lösung:*

Das reziproke Polynom ungeraden Grades hat Nullstelle  $-1$ . Nach Herausdividieren des Faktors  $X + 1$  bleibt das Polynom  $X^4 + 2X^3 - 22X^2 + 2X + 1$ . Für eine Nullstelle  $z$  gilt also

$$z^2 + 1/z^2 + 2(2 + 1/z) - 22 = 0 \Leftrightarrow (z + 1/z)^2 + 2(z + 1/z) - 24 = 0$$

Setze  $u = z + 1/z$ . Dann ist  $u^2 + 2u - 24 = (u + 6)(u - 4) = 0$ , also  $u = 4$  oder  $u = -6$ .

Durch Auflösen der quadratischen Gleichungen  $z^2 - uz + 1 = 0$  erhält man schließlich als Nullstellen:  $-2 + \sqrt{3}$ ,  $-2 - \sqrt{3}$ ,  $3 + \sqrt{8}$ ,  $3 - \sqrt{8}$ ,  $-1$ .

#### 4. Satz von Vietà

Es sei  $P(X) = X^n + b_{n-1}X^{n-1} + \dots + b_1X + b_0$  normiertes Polynom vom Grad  $n$  mit Nullstellen  $x_1, \dots, x_n$ . Nach Teil 3 enthält  $P$  die Faktoren  $X - x_1, \dots, X - x_n$ . Teilt man  $P$  durch diese Faktoren, bleibt das konstante Polynom mit Wert 1 übrig, da  $P$  und  $(X - x_1)\dots(X - x_n)$  beide normiert sind und selben Grad haben. Somit besitzt  $P$  auch die Form

$$P(X) = (X - x_1)\dots(X - x_n).$$

Durch Ausmultiplizieren ergibt sich daraus (Satz von Vietà):

$$b_{n-1} = -x_1 - x_2 - \dots - x_n$$

$$b_{n-2} = x_1x_2 + x_1x_3 + \dots + x_1x_n + \dots + x_2x_n + \dots + x_{n-1}x_n$$

$$b_{n-3} = -(x_1x_2x_3 + x_1x_2x_4 + \dots + x_{n-2}x_{n-1}x_n)$$

.

.

$$b_n = (-1)^n x_1 x_2 \dots x_n$$

Die Ausdrücke auf den rechten Seiten (nach Weglassen des eventuellen Vorfaktors  $-1$ ) heißen auch elementarsymmetrische Funktionen oder elementarsymmetrische Polynome. Sie haben zunächst die Eigenschaft, dass ihr Wert unverändert bleibt, wenn man die Variablen beliebig vertauscht (permutiert). Darüber hinaus lässt sich sogar jeder durch Addition, Multiplikation und Skalarmultiplikation aus  $x_1, \dots, x_n$  entstandene Ausdruck, der bei Permutation von  $x_1, \dots, x_n$  in sich übergeht, mit diesen elementarsymmetrischen Funktionen darstellen:

*Aufgabe:*

Das Polynom  $X^3 - aX^2 + bX - c$  habe die Nullstellen  $x_1, x_2$  und  $x_3$ . Bestimme ein normiertes Polynom dritten Grades mit den Nullstellen  $x_1x_2, x_1x_3$  und  $x_2x_3$ .

*Lösung:*

Nach Satz von VIETÀ ist zunächst

$$a = x_1 + x_2 + x_3, \quad b = x_1x_2 + x_1x_3 + x_2x_3, \quad c = x_1x_2x_3.$$

Gesuchtes Polynom sei  $X^3 - \alpha X^2 + \beta X - \gamma$ , wobei

$$\alpha = x_1x_2 + x_1x_3 + x_2x_3 = b$$

$$\beta = (x_1x_2)(x_1x_3) + (x_1x_2)(x_2x_3) + (x_1x_3)(x_2x_3) = (x_1 + x_2 + x_3)x_1x_2x_3 = ac$$

$$\gamma = (x_1x_2)(x_1x_3)(x_2x_3) = c^2.$$

Das gesuchte Polynom lautet also  $X^3 - bX^2 + acX - c^2$ .

*Aufgabe:*

Das Polynom  $3X^2 + aX - 2$  ( $a$  reeller Parameter) hat die Nullstellen  $x_1$  und  $x_2$  mit  $6x_1 + x_2 = 0$ . Für welche Werte von  $a$  ist dies möglich?

*Lösung:*

Normierung des Ausgangspolynoms:  $X^2 + \frac{a}{3}X - \frac{2}{3}$ . Nach Satz von VIETÀ gilt  $\frac{a}{3} = -x_1 - x_2$ ,

außerdem gilt nach Voraussetzung  $x_2 = -6x_1$ , woraus sich  $a = 15x_1$  ergibt. Somit ist  $\frac{a}{15}$  eine

Nullstelle des Ausgangspolynoms:

$$\left(\frac{a}{15}\right)^2 + \frac{a}{3} \cdot \frac{a}{15} - \frac{2}{3} = 0.$$

Diese quadratische Gleichung hat die Lösungen 5 und -5.

*Aufgabe:*

Löse das folgende Gleichungssystem:

$$x + y + z = 0, \quad x^2 + y^2 + z^2 = 2, \quad x^3 + y^3 + z^3 = 0.$$

*Lösung:*

Wir bezeichnen die elementarsymmetrischen Funktionen mit

$$\sigma_1 = x + y + z,$$

$$\sigma_2 = xy + yz + zx,$$

$$\sigma_3 = xyz.$$

Durch Vergleichen der Grade der Polynome ergeben sich folgende Ansätze:

$$x^2 + y^2 + z^2 = k\sigma_1^2 + l\sigma_2$$

$$x^3 + y^3 + z^3 = m\sigma_1^3 + n\sigma_1\sigma_2 + \sigma_3.$$

Durch Einsetzen verschiedener Werte für  $x$ ,  $y$  und  $z$  erhält man  $k = m = 1$ ,  $l = -2$ ,  $n = -3$ ,  $p = 3$ . Somit lautet das Gleichungssystem umgeschrieben auf  $\sigma_1$ ,  $\sigma_2$  und  $\sigma_3$ :

$$\sigma_1 = 0, \quad \sigma_1^2 - 2\sigma_2 = 2, \quad \sigma_1^3 - 3\sigma_1\sigma_2 + \sigma_3 = 0.$$

Daraus folgt  $\sigma_1 = 0$ ,  $\sigma_2 = -1$  und  $\sigma_3 = 0$ . Berücksichtigt man die Bedeutungen der elementarsymmetrischen Funktionen im Satz von VIETÀ, so müssen  $x$ ,  $y$  und  $z$  Nullstellen des Polynoms  $Y^3 - \sigma_1 Y^2 + \sigma_2 Y - \sigma_3 = Y^3 - Y = Y(Y+1)(Y-1)$  sein. Daher gibt es für  $(x;y;z)$  die Möglichkeiten  $(-1; 0; 1)$ ,  $(-1;1; 0)$ ,  $(0; -1; 1)$ ,  $(1; -1; 0)$ ,  $(0; 1; -1)$  und  $(1; 0; -1)$ .

## 5. Weitere Aufgaben

Zum Themenbereich der Polynome kamen in den letzten Jahren u. a. folgende Aufgaben in der deutschen Mathematikolympiade vor:

1. Berechnen Sie die Zahl

$$123456785 \cdot 123456787 \cdot 123456788 \cdot 123456796 - \\ - 123456782 \cdot 123456790 \cdot 123456791 \cdot 123456793,$$

ohne die Zahlenwerte der beiden Produkte einzeln zu berechnen (34. Olympiade, 3. Stufe, Klasse 10, Aufgabe 2).

2. Für jede ganze Zahl  $n$  mit  $n \geq 0$  sei  $f_n$  die durch

$$f_n(x) = x^3 + (n+3)x^2 + 2nx - \frac{n}{n+1}$$

für alle reellen  $x$  definierte Funktion. Man ermittle alle diejenigen ganzen Zahlen  $n \geq 0$ , für die gilt: Alle Nullstellen von  $f_n$  liegen in einem Intervall der Länge 3 (33. Olympiade, 3. Stufe, Klasse 11 - 13, Aufgabe 3B).

## Zur elementaren Zahlentheorie

### 1. Grundlagen

Es seien  $a, b \in \mathbb{Z}$  und  $a \neq 0$ . Schreibe  $a \mid b$ , in Worten „a teilt b“, wenn es eine ganze Zahl  $n$  gibt mit  $b = an$ .

Es seien  $a, b, c \in \mathbb{Z}$  und  $c \neq 0$ . Schreibe  $a \equiv b \pmod{c}$ , in Worten „a kongruent b modulo c“, wenn  $c \mid a-b$ .

Hierfür gelten folgende Regeln (hierin seien  $a, b, c, d \in \mathbb{Z}$  und  $a$  und  $b$  nicht null).

1.  $a \mid b$  und  $b \mid c \Rightarrow a \mid c$ ,  $a \mid c$  und  $a \mid d \Rightarrow a \mid c+d$  und  $a \mid c-d$ .
2. Gilt  $a \mid cd$  und sind  $a$  und  $c$  teilerfremd, folgt  $a \mid d$ .
3. Aus  $a \mid c$  folgt  $c \equiv 0 \pmod{a}$ .
4. Ist  $d$  der Rest von  $c$  bei Division durch  $a$ , so ist  $c \equiv d \pmod{a}$ .
5. Sind  $c'$  und  $d'$  Zahlen mit  $c \equiv c' \pmod{a}$  und  $d \equiv d' \pmod{a}$ , folgt  
 $c+d \equiv c'+d' \pmod{a}$ ,  $c-d \equiv c'-d' \pmod{a}$  und  $cd \equiv c'd' \pmod{a}$ .  
 Letztere Gleichung gilt wegen  $cd - c'd' = c(d-d') + (c-c')d'$  und da  $d-d'$  und  $c-c'$  durch  $a$  teilbar sind.
6. Ist  $P$  ein Polynom mit ganzzahligen Koeffizienten, folgt  $P(c) \equiv P(c') \pmod{a}$ .

#### Beispiel:

Es gilt  $10 \equiv -2 \pmod{4}$  und  $10000001 \equiv 1 \pmod{2}$ , aber nicht  $-5 \equiv -10 \pmod{6}$ .

#### Aufgabe:

Eine Gleichung  $a = b$  kann nicht erfüllt sein, wenn man eine natürliche Zahl  $n$  finden kann, für die *nicht* gilt:  $a \equiv b \pmod{n}$ .

#### Beweis:

Denn aus  $a = b$  folgt für alle  $n \in \mathbb{N}$ :  $a \equiv b \pmod{n}$ .

Das Problem ist hierbei meist, eine geeignete Zahl  $n$  zu finden, um die Ungleichheit zu zeigen. Kommen z. B.  $k$ -te Potenzen für einen festen Wert von  $k$  vor, ist es oft günstig, die Gleichung modulo  $k^2$  oder  $2k^2$  zu betrachten.

#### Aufgabe:

8007 ist keine Summe von 3 Quadratzahlen.

#### Lösung:

Untersuche die Gleichung  $x^2 + y^2 + z^2 = 8007$  modulo 8. Wegen  $(n+8)^2 \equiv n^2 \pmod{8}$  und  $(8-n)^2 \equiv n^2 \pmod{8}$  braucht man nur die Fälle  $n \in \{0;1;2;3;4\}$  zu untersuchen, um alle auftretenden Reste herauszufinden. Hierfür ergibt sich:

$n$	0	1	2	3	4
$n^2 \pmod{8}$	0	1	4	1	0

Nun hat 8007 den Rest 7 bei Division durch 8, und es gibt keine Möglichkeit, durch Addition dreier Reste mit Werten 0, 1 und 4 den Rest 7 zu erhalten. Daher ist die Gleichung modulo 8 unmöglich.

*Aufgabe:*

Für kein  $n \in \mathbb{N}$  gilt  $100 \mid 9^n + 1$ .

*Lösung:*

Es ist sogar  $4 \mid 9^n + 1$  für alle  $n \in \mathbb{N}$  falsch, denn wegen  $9 \equiv 1 \pmod{4}$  ist  $9^n + 1 \equiv 1^n + 1 \equiv 2 \pmod{4}$ , also  $9^n + 1$  nicht durch 4 teilbar.

## 2. Satz von EULER-FERMAT

Es seien  $a$  und  $c$  teilerfremde natürliche Zahlen, außerdem  $n \in \mathbb{N}$ . Will man den Rest von  $a^n$  bei Division durch  $c$  bestimmen und ist  $n$  recht groß, so ist es nützlich, einen Exponenten  $m$  zu kennen mit  $a^m \equiv 1 \pmod{c}$ , denn für  $n > m$  ist dann  $a^n \equiv a^m a^{n-m} \equiv a^{n-m} \pmod{c}$ . Auf diese Weise kann man den Exponenten von  $a$  oft stark verkleinern und sich die Aufgabe erleichtern. Nehmen wir einmal an, es gebe einen kleinsten natürlichen Exponenten  $m$  mit  $a^m \equiv 1 \pmod{c}$ . Dann sind alle natürlichen Exponenten  $k$  mit  $a^k \equiv 1 \pmod{c}$  Vielfache von  $m$ , denn wenn man  $k$  mit Rest durch  $m$  dividiert, erhält man  $k = tm + r$ ,  $r < m$ , also ist dann

$$1 \equiv a^k \equiv a^{tm+r} \equiv (a^m)^t a^r \equiv a^r \pmod{c}.$$

Da  $m$  die kleinste natürliche Zahl ist mit  $a^m \equiv 1 \pmod{c}$ , kann dies also nur gelten für  $r = 0$ . Mit dem Satz von EULER-FERMAT kann man ziemlich leicht ein für viele Anwendungen genügend kleines Vielfaches von  $m$  erhalten. Hierzu muss zunächst noch die sogenannte EULERSche  $\phi$ -Funktion eingeführt werden:

**Definition:**

Für gegebenes  $n \in \mathbb{N}$  sei  $\phi$  die Anzahl der zu  $n$  teilerfremden Zahlen  $c$  mit  $1 \leq c \leq n$ .

**Beispiel:**

$\phi(6) = 2$  (nämlich die Zahlen 1 und 5).

**Satz:**

Ist  $p$  Primzahl, so gilt  $\phi(p) = p - 1$ .

*Beweis:*

Die  $p - 1$  Zahlen  $1, 1, \dots, p-1$  sind zu  $p$  teilerfremd.

### Allgemeine Bestimmung der Funktionswerte

Es sei  $n = p_1^{a_1} p_2^{a_2} \dots p_r^{a_r}$  die Zerlegung der natürlichen Zahl  $n$  in Primfaktoren, wobei die Faktoren  $p_1, \dots, p_r$  Primzahlen sind und  $a_1, \dots, a_r$  natürliche Zahlen. Bestimme  $\phi(n)$ , ausgehend von der Menge  $\{1; 2; \dots; n\}$  mit  $n$  Elementen. Alle Vielfachen von  $p_1$  sind nicht teilerfremd zu  $n$ , dies schließt genau  $1/p_1$  Zahlen aus. Alle Vielfachen von  $p_2$  sind auch nicht teilerfremd zu  $n$ ,

müssen also auch ausgeschlossen werden usw. Hierbei sind offenbar einige Zahlen zuviel ausgeschlossen worden, nämlich z. B. die Vielfachen von  $p_1 p_2$  einmal zu viel; sie müssen also wieder eingerechnet werden, also  $\frac{n}{p_1 p_2}$  Zahlen, ebenso die Vielfachen der anderen Produkte

zweier Primfaktoren. Die Vielfachen der Produkte dreier Primfaktoren sind zunächst dreimal ausgeschlossen, dann wieder dreimal eingerechnet worden, müssen also nochmals ausgeschlossen werden usw. Schließlich erhält man

$$\begin{aligned}\phi(n) &= n - \frac{n}{p_1} - \dots - \frac{n}{p_r} + \frac{n}{p_1 p_2} + \frac{n}{p_1 p_3} + \dots + \frac{n}{p_{r-1} p_r} - \frac{n}{p_1 p_2 p_3} - \dots + \frac{(-1)^r n}{p_1 p_2 \dots p_r} = \\ &= n \left(1 - \frac{1}{p_1}\right) \left(1 - \frac{1}{p_2}\right) \dots \left(1 - \frac{1}{p_r}\right)\end{aligned}$$

*Beispiel:*

$$\phi(6) = 6 \left(1 - \frac{1}{2}\right) \left(1 - \frac{1}{3}\right) = 2; \text{ ist } p \text{ Primzahl, folgt } \phi(p) = p \left(1 - \frac{1}{p}\right) = p - 1.$$

### Satz von EULER - FERMAT

Es seien  $a$  und  $c$  teilerfremde natürliche Zahlen. Dann gilt  $a^{\phi(c)} \equiv 1 \pmod{c}$ .

*Beweis*

Es seien  $d_1, \dots, d_{\phi(c)}$  die zu  $c$  teilerfremden Zahlen in  $\{1, \dots, c\}$ . Dann sind auch die Zahlen  $ad_1, \dots, ad_{\phi(c)}$  teilerfremd zu  $c$  und haben paarweise verschiedene Reste bei Division durch  $c$ ; denn sind  $k$  und  $m$  Indices mit  $ad_k \equiv ad_m \pmod{c}$ , folgt  $c | a(d_k - d_m)$  und  $c | d_k - d_m$  und  $d_k = d_m$ , da  $a$  und  $c$  teilerfremd sind. Daher haben auch  $ad_1, \dots, ad_{\phi(c)}$  alle möglichen Reste bei Division durch  $c$ , die bei zu  $c$  teilerfremden Zahlen auftreten können, somit ist

$$\begin{aligned}d_1 \dots d_{\phi(c)} &\equiv ad_1 \dots ad_{\phi(c)} \pmod{c} \Rightarrow \\ d_1 \dots d_{\phi(c)} &\equiv a^{\phi(c)} d_1 \dots d_{\phi(c)} \pmod{c} \Rightarrow \\ c &| (a^{\phi(c)} - 1) d_1 \dots d_{\phi(c)} \Rightarrow \\ c &| (a^{\phi(c)} - 1) \Rightarrow \\ a^{\phi(c)} &\equiv 1 \pmod{c}.\end{aligned}$$

**Beispiel:**

Welchen Rest hat  $15337^{15338}$  bei Division durch 6?

*Lösung:*

15337 ist teilerfremd zu 6, also ist  $15337^{\phi(6)} \equiv 1 \pmod{6}$ . Wegen  $\phi(6) = 2$  ist  $15337^2 \equiv 1 \pmod{6}$ , also auch  $15337^{15338} \equiv 1 \pmod{6}$ .

*Aufgabe:*

Zeige  $7 | 2222^{5555} + 5555^{2222}$ .

*Lösung:*

Es ist  $2222 \equiv 3 \pmod{7}$ ,  $5555 \equiv 4 \pmod{7}$ , weiter ist  $\phi(7) = 6$ ,  $2222 \equiv 2 \pmod{6}$  und  $5555 \equiv 5 \pmod{6}$ . Damit folgt

$$2222^{5555} + 5555^{2222} \equiv 3^{5555} + 4^{2222} \equiv 3^5 + 4^2 \equiv 259 \equiv 0 \pmod{7}$$

### 3. Euklidischer Algorithmus

Zur Bestimmung des größten gemeinsamen Teilers zweier nicht negativer ganzer Zahlen zerlegt man oft diese in Primfaktoren und sieht nach, welche Faktoren bei beiden Zahlen vorkommen. Man kann den größten gemeinsamen Teiler aber auch ohne Primfaktorzerlegung bestimmen. Sind  $a$ ,  $s$  und  $b$  nicht negative ganze Zahlen mit  $sb \leq a$  und ist  $t$  gemeinsamer Teiler von  $a$  und  $b$ , so teilt  $t$  auch  $a - sb$  und  $b$  und umgekehrt, d. h. die größten gemeinsamen Teiler bleiben unverändert. Durch fortgesetzte Anwendung dieser Reduktion kann man den allgemeinen Fall auf den Fall, dass eine Zahl die Null ist, zurückführen. Der größte gemeinsame Teiler von  $a$  und  $0$  ist aber offenbar  $a$  für  $a \in \mathbb{N}$ .

#### Beispiel

Es ist  $\text{ggT}(525; 231) = \text{ggT}(63; 231) = \text{ggT}(231; 63) = \text{ggT}(42; 63) = \text{ggT}(63; 42) = \text{ggT}(21; 42) = \text{ggT}(21; 0) = 21$ .

Noch mehr Information erhält man mit folgendem erweiterten euklidischen Algorithmus:

	Kurzform
$525 = 1 \cdot 525 + 0 \cdot 231$	$525 \quad 1 \quad 0$
$231 = 0 \cdot 525 + 1 \cdot 231$	$231 \quad 0 \quad 1$
$63 = 1 \cdot 525 - 2 \cdot 231$	$63 \quad 1 \quad -2$
$42 = -3 \cdot 525 + 7 \cdot 231$	$42 \quad -3 \quad 7$
$21 = 4 \cdot 525 - 9 \cdot 231$	$21 \quad 4 \quad -9$
$0 = -11 \cdot 525 + 25 \cdot 231$	$0 \quad -11 \quad 25$

Fazit: Zu zwei Zahlen  $a$  und  $b$  kann man ganzzahlige Vielfache  $ka$  und  $mb$  bestimmen, so dass  $ka+mb = \text{ggT}(a; b)$ .

#### Satz:

Es seien  $a$ ,  $n$  teilerfremde natürliche Zahlen. Dann gibt es eine Zahl  $b \in \mathbb{Z}$  mit  $ab \equiv 1 \pmod{n}$ .

#### Beweis:

- Möglichkeit: Da  $a$  und  $n$  teilerfremd sind, gibt es ganzzahlige Vielfache  $kn$  und  $ma$  mit  $kn+ma = \text{ggT}(a; n) = 1$ . Dann ist aber  $ma \equiv 1 \pmod{n}$ . Setze also  $b = m$ .
- Möglichkeit: Nach Satz von EULER-FERMAT ist mit  $b = a^{\phi(n)-1}$  auch  $ab \equiv a^{\phi(n)} \equiv 1 \pmod{n}$ .

#### Aufgabe:

Bestimme die kleinste natürliche Zahl, die auf 1986 endet und durch 1987 teilbar ist.

#### Lösung:

Die Zahl hat die Darstellung  $10000x + 1986$  mit  $x \in \mathbb{N}_0$ . So ist  $1987 | 10000x + 1986$ , also gibt es ein  $n \in \mathbb{N}$  mit  $1987n = 10000x + 1986$  bzw.  $10000x - 1987(n-1) = 1$ . Mit dem erweiterten euklidischen Algorithmus erhält man  $x = 214$  und  $n = 1078$ . Die Zahl lautet 2141986.

## 4. Diophantische Gleichungen

Diophantische Gleichungen sind Gleichungen, bei denen die Variablen natürliche oder ganze Zahlen sind. Dadurch ergeben sich meist starke Einschränkungen für die Lösungen, so dass oft auch eine Gleichung für mehrere Variablen nur endlich viele Lösungen oder gar keine Lösungen hat, auch wenn dieselbe Gleichung für reelle Werte sehr viele Lösungen hat. Es gibt viele teils recht komplizierte Lösungsverfahren für Typen diophantischer Gleichungen, von denen hier nur die einfachsten vorgestellt werden. Auf die Methode, die Gleichung modulo gewisser Zahlen zu betrachten, um Lösungsmöglichkeiten einzuschränken, wird hier nicht weiter eingegangen. Das Verfahren mit konjugierten Zahlen steht in Teil 5.

### 1. Methode

Zwischen zwei aufeinanderfolgenden ganzen Zahlen, ganzen Quadratzahlen, ganzen Kubikzahlen usw. ist kein weitere ganze Zahl, ganze Quadratzahl, ganze Kubikzahl usw.

#### Beispiel:

$$\text{Finde alle } x, y \in \mathbb{N}_0 \text{ mit } x^3 + 8x^2 - 6x + 8 = y^3.$$

#### Lösung:

Es ist  $(x+3)^3 = x^3 + 9x^2 + 27x + 27 > x^3 + 8x^2 - 6x + 8 > x^3 + 6x^2 + 12x + 8 = (x+2)^3$ , sofern  $2x^2 - 18x > 0$  ist. Dies gilt für  $x > 9$ , d. h. für  $x > 9$  hat die Gleichung keine Lösung. Die Fälle  $x < 9$  kann man durchprobieren und erhält die Lösungen (0;2) und (9;11).

### 2. Methode:

Ist eine ganze Quadratzahl, Kubikzahl usw. Produkt teilerfremder Zahlen, so sind die Faktoren ebenfalls Quadratzahlen, Kubikzahlen usw.

#### Beispiel:

$$\text{Zeige, dass die Gleichung } x^3 + 3 = 4y(y+1) \text{ keine ganzzahligen Lösungen hat.}$$

#### Lösung:

Es ist  $x^3 = 4y^2 + 4y - 3 = (2y+3)(2y-1)$ . Die beiden Faktoren auf der rechten Seite sind ungerade und teilerfremd, denn jeder gemeinsamer Teiler ist auch gemeinsamer Teiler ihrer Differenz, nämlich 4. Es sei  $p$  ein Primfaktor von  $x$ . Da  $2y+3$  und  $2y-1$  teilerfremd sind, steckt  $p^3$  in genau einem der Faktoren. Daher sind  $2y+3$  und  $2y-1$  selbst Kubikzahlen:

$$2y + 3 = a^3, \quad 2y - 1 = b^3 \Rightarrow a^3 - b^3 = 4.$$

Letztere Gleichung hat keine Lösungen.

### 3. Methode („Rationale Parametrisierung von Kegelschnittsgleichungen“)

Gegeben sei eine rationale Zahl  $u \neq 0$ . Finde rationale Zahlen  $x$ , für die  $x^2 + u$  Quadrat einer rationalen Zahl ist. Dies ist offenbar möglich, wenn es rationale Zahlen  $a$  und  $b$  mit  $x = a - b$  und  $u = 4ab$  gibt, denn dann ist  $x^2 + u = (a+b)^2$ . Wegen  $u \neq 0$  sind auch  $a$  und  $b$  von Null verschieden. Somit ist  $b = \frac{u}{4a}$ , also  $x = a - \frac{u}{4a}$ .

Fazit: Für  $a \in \mathbb{Q} \setminus \{0\}$  und  $x = a - \frac{u}{4a}$  ist  $x^2 + u$  Quadrat einer rationalen Zahl. (Dies sind üb-

rigens auch alle Möglichkeiten, weil man  $a$  und  $b$  aus  $x = a - b$  und  $a + b = \sqrt{x^2 + u}$  zurückgewinnen kann und dann notwendig  $u = 4ab$  gilt).

*Aufgabe:*

Es gibt keine natürliche Zahl  $n > 1$ , für die  $n^2 - n$  Quadratzahl ist, aber unendlich viele rationale Zahlen  $q > 1$ , für die  $q^2 - q$  Quadratzahl ist.

*Lösung:*

a) Für alle  $n > 1$  ist  $n^2 > n^2 - n > (n-1)^2$ , also Ausschluss nach der ersten Methode.

c) Es ist  $q^2 - q = \left(q - \frac{1}{2}\right)^2 - \frac{1}{4}$ . Für rationales  $a$  ungleich 0 und  $q - \frac{1}{2} = a - \frac{1}{4 \cdot 4a}$  ist  $q^2 - q$  Quadratzahl. Für  $a > 1$  ist  $q = \frac{1}{2} + a + \frac{1}{16a} > 1$  Zahl der gewünschten Form.

## 5. Konjugierte Zahlen

Es seien  $a, b$  rationale Zahlen und  $d \in \mathbb{N}$ , wobei  $d$  keine Quadratzahl ist. Dann ist die Darstellung  $a + b\sqrt{d}$  eindeutig, denn für  $a + b\sqrt{d} = a' + b'\sqrt{d}$  mit  $a \neq a'$  ist auch  $b \neq b'$ , und für  $b \neq b'$  gilt  $a - a' = (b' - b)\sqrt{d}$ , also  $\sqrt{d} = \frac{a - a'}{b - b'}$  im Widerspruch zur Irrationalität von  $\sqrt{d}$ . Aus  $a + b\sqrt{d}$  erhält man also eindeutig  $a$  und  $b$ . Man kann also definieren:

**Definition:**

Die zu  $a + b\sqrt{d}$  **konjugierte Zahl** ist  $\overline{a + b\sqrt{d}} = a - b\sqrt{d}$ .

Man kann folgende Regeln nachrechnen:

**Satz:**

Für Zahlen  $x$  und  $y$  der oben angegebenen Form gilt  
 $\overline{\overline{x}} = x$ ,  $\overline{x + y} = \overline{x} + \overline{y}$ ,  $\overline{x - y} = \overline{x} - \overline{y}$ ,  $\overline{xy} = \overline{x} \cdot \overline{y}$ ,  $x + \overline{x} \in \mathbb{Q}$

Sind die beiden rationalen Koeffizienten sogar ganzzahlig, ist  $x + \overline{x}$  sogar eine gerade ganze Zahl.

*Aufgabe:*

Bestimme alle ganzzahligen/rationalen Lösungen von  $(a + b\sqrt{3})^4 + (c + d\sqrt{3})^4 = 1 + \sqrt{3}$

*Lösung:*

Wenn diese Gleichung gilt, dann ist auch die konjugierte Gleichung

$$(a - b\sqrt{3})^4 + (c - d\sqrt{3})^4 = 1 - \sqrt{3}$$

wahr. Hiervon ist aber die rechte Seite negativ, wogegen die linke Seite als Summe reeller vierter Potenzen nicht negativ sein kann. Somit hat die Gleichung keine rationalen Lösungen, also erst recht keine ganzzahligen.

*Aufgabe:*

Zeige, dass  $\left[ (5 + \sqrt{22})^{60} \right]$  ungerade ist (Hierbei bezeichnet  $[x]$  die größte ganze Zahl, die kleiner oder gleich der reellen Zahl  $x$  ist).

*Lösung:*

Nach der obigen Theorie ist  $(5 + \sqrt{22})^{60} + (5 - \sqrt{22})^{60}$  eine gerade ganze Zahl. Weiter ist  $0 < 5 - \sqrt{22} < 1$ , also auch  $0 < (5 - \sqrt{22})^{60} < 1$ , also

$\left[ (5 + \sqrt{22})^{60} \right] = (5 + \sqrt{22})^{60} + (5 - \sqrt{22})^{60} - 1$  ungerade, weil  $(5 + \sqrt{22})^{60} + (5 - \sqrt{22})^{60}$  gerade ist.

## 6. Weitere Aufgaben

Zum Themenbereich der elementaren Zahlentheorie kamen in den letzten Jahren u.a. folgende Aufgaben in der deutschen Mathematikolympiade vor:

1. Es seien  $a$  und  $b$  je eine der Ziffern 1, 2, 3, 4, 5, 6, 7, 8, 9. Ferner sei  $z$  diejenige natürliche Zahl, deren Zifferndarstellung im Dezimalsystem  $ababab$  lautet. Man beweise, dass jede so zu beschreibende Zahl  $z$  durch 481 teilbar ist. (35. Olympiade, 2. Stufe, Klasse 10, Aufgabe 3)
2. Man ermittle alle diejenigen Paare  $(x;y)$  positiver ganzer Zahlen  $x, y$ , welche die Gleichung  $10x^3 - (2y + 5)x^2 + (y-4)x + 76 = 0$  erfüllen.
3. Man ermittle für jede natürliche Zahl  $n$  die größte Zweierpotenz, die ein Teiler der Zahl  $\left[ (4 + \sqrt{18})^n \right]$  ist. (33. Olympiade, 3. Stufe, Klasse 11 - 13, Aufgabe 6)
4. Ermitteln Sie alle positiven Zahlen  $n$  mit der Eigenschaft, dass die drei Zahlen  $n+1$ ,  $n+10$  und  $n+55$  einen gemeinsamen Teiler größer als 1 haben. (33. Olympiade, 3. Stufe, Klasse 9, Aufgabe 5)
5. Ist  $m$  eine natürliche Zahl mit  $m \geq 2$ , so werde eine Zahlenfolge  $\{x_n\}$  für  $n = 0, 1, 2, \dots$  durch die Festsetzungen definiert, dass  $x_0 = 0$ ,  $x_1 = 1$  gelten soll und für  $n \geq 0$  jeweils  $x_{n+2}$  der Rest (mit  $0 \leq x_{n+2} < m$ ) sein soll, den  $x_{n+1} + x_n$  bei Division durch  $m$  lässt. Man untersuche, ob zu jeder natürlichen Zahl  $m \geq 2$  eine natürliche Zahl  $k \geq 1$  existiert, mit der die drei Gleichungen  $x_0 = x_k$ ,  $x_1 = x_{k+1}$  und  $x_2 = x_{k+2}$  gelten. (33. Olympiade, 3. Stufe, Klasse 11-13, Aufgabe 3A)
6. Für jede positive ganze Zahl  $n$  denke man sich nach folgender Vorschrift eine weitere Zahl  $n'$  gebildet:  
Aus der Zifferndarstellung von  $n$  im Dezimalsystem wird die erste Ziffer weggenommen und statt dessen hinter die letzte Ziffer angefügt. Dann sei  $n'$  die Zahl mit der entstandenen

Zifferndarstellung (Bei dieser Zifferndarstellung von  $n'$  wird auch die Möglichkeit einer Anfangsziffer Null zugelassen, wenn nämlich die zweite Ziffer von  $n$  eine Null war).

Untersuchen Sie, ob es durch 7 teilbare Zahlen  $n$  gibt, für die  $n' = n:7$  gilt. Ermitteln Sie, wenn es solche Zahlen gibt, die kleinste unter ihnen. (33. Olympiade, 3. Stufe, Klasse 10, Aufgabe 2)

7. Jemand findet die Angabe  $23! = 2585201673*8849*6640000$ .

Darin sind auch die zwei durch \* angedeuteten unleserlichen Ziffern. Er möchte diese Ziffern ermitteln, ohne die Multiplikationen vorzunehmen, die der Definition von  $23!$  entsprechen. Führen Sie eine solche Ermittlung durch und begründen Sie sie. Dabei darf verwendet werden, dass die angegebenen Ziffern korrekt sind (Hinweis: Für jede positive ganze Zahl  $n$  wird  $n!$  definiert als das Produkt aller positiven ganzen Zahlen von 1 bis  $n$ ).

33. Olympiade, 4. Stufe, Klasse 10, Aufgabe 4)

## Quellenhinweise

Die Ausführungen folgen teilweise den Skripten „Zur vollständigen Induktion an ungewöhnlichen Beispielen“ von Dr. Horst Sewerin sowie „Polynome“ und „Definitionen und Sätze aus der Zahlentheorie“ von Prof. Arthur Engel, die im Rahmen der Vorbereitung auf die Internationale Mathematikolympiade verwendet werden.

[1] Karl Strubecker, Einführung in die höhere Mathematik, Band 1, Oldenbourg-Verlag, München 1966

Anschrift des Autors:  
 Dr. Eric F. Müller  
 Alramstraße 6  
 81371 München