Zahlentheorie

Thomas Peters
Thomas' Mathe-Seiten
www.mathe-seiten.de

30. September 2012

Dieser Artikel beginnt mit dem Abstecken der verschiedenen Zahlbereiche. Einem Kapitel über die Dichtheit der rationalen und reellen Zahlen schließt sich ein Kapitel über Irrationalitätsbeweise an, das Grundzüge der Analysis benutzt und auch übersprungen werden kann. Einfache algebraische Strukturen werden verwendet, um die Zahlbereiche zu erweitern. Dann werden natürliche und ganze Zahlen genauer untersucht. Als wichtiges zahlentheoretisches Hilfmittel wird die Moduloarithmetik vorgestellt. Mit ihrer Hilfe werden Primzahltests, Faktorisierungsverfahren und Quadratzahlen untersucht. Anschließend werden Grundbegriffe der abstrakten Algebra eingeführt. Darauf folgt ein Kapitel über Betrands Postulat für Unerschrockene. Den Abschluss bildet ein Streifzug durch die Zahlentheorie.

Inhaltsverzeichnis

Abbildungsverzeichnis **6**

1 Kleine Zahlenkunde **7**
1.1 Natürliche Zahlen . . . 7
1.2 Ganze Zahlen . . . 7
1.3 Rationale Zahlen . . . 8
1.4 Reelle Zahlen . . . 8
1.4.1 Algebraische Zahlen . . . 8
1.4.2 Transzendente Zahlen . . . 9
1.4.3 Die reellen Zahlen als Körper . . . 9

2 Rationale vs. reelle Zahlen **10**

3 Irrationalitätsbeweise **12**
3.1 Polynomwurzeln . . . 12
3.2 Die Irrationalität von e . . . 13
3.3 Das Niven-Polynom . . . 14
3.4 Potenzen von e . . . 14
3.5 Die Irrationalität von π . . . 16
3.6 Aussichten . . . 16
3.7 Die Liouville'sche Konstante . . . 17

4 Erweiterungen der reellen Zahlen **19**
4.1 Komplexe Zahlen . . . 19
4.2 Quaternionen . . . 20
4.3 Oktaven . . . 20
4.4 Allgemeine Ergebnisse . . . 21
4.4.1 Distributivgesetz . . . 21
4.4.2 Konjugationen . . . 22
4.4.3 Multiplikativ inverses Element . . . 23
4.4.4 Kommutativität, Assoziativität und das Ende der Divisionsalgebren 23
4.5 Hyperkomplexe Zahlen . . . 25

5 Teiler und Vielfache **26**
5.1 Vorbetrachtungen . . . 26
5.2 Teiler . . . 27
5.3 Vielfache . . . 30

5.4 Primzahlen . . . 30
5.5 Teilbarkeitsregeln . . . 33
5.5.1 Teilbar durch $2, 4, 5, 8, 10^n$ . . . 33
5.5.2 Teilbar durch $2^n, 5^n$ . . . 33
5.5.3 Teilbar durch $3, 9$ . . . 34
5.5.4 Teilbar durch 6 . . . 34
5.5.5 Teilbar durch 7 . . . 34
5.5.6 Teilbar durch 11 . . . 35
5.5.7 Teilbar durch 13 . . . 36
5.5.8 Teilbarkeitsregeln in Aktion . . . 36
5.5.9 Aufgaben . . . 37

6 Moduloarithmetik **38**
6.1 Restklassen . . . 38
6.2 Rechenregeln für Restklassen . . . 39
6.2.1 Addition . . . 39
6.2.2 Multiplikation . . . 40
6.2.3 Anmerkungen . . . 41
6.3 Multiplikationstabellen . . . 42
6.4 Anwendungen . . . 43
6.5 Der Chinesische Restsatz . . . 44

7 Primzahltests **47**
7.1 Das Sieb des Eratosthenes . . . 47
7.2 Der Satz von Wilson . . . 47
7.3 Der kleine Satz von Fermat . . . 48
7.4 Der Satz von Euler . . . 49
7.5 Die RSA-Verschlüsselung . . . 51
7.6 Der Satz von Pocklington . . . 53

8 Faktorisierungsverfahren **54**
8.1 Probedivision . . . 54
8.2 Das Verfahren von Fermat . . . 54

9 Quadratzahlen **56**
9.1 Vorbetrachtungen . . . 56
9.2 Quadratische Reste . . . 57
9.3 Pythagoräische Tripel . . . 57
9.4 Summen von Quadraten . . . 59

10 Ein bisschen Algebra **61**
10.1 Gruppen . . . 61
10.2 Ringe . . . 63
10.3 Integritätsringe . . . 64

10.4 Körper 67

11 Bertrands Postulat **69**

12 Ein Streifzug durch die Zahlentheorie **73**
12.1 Die σ-Funktion und perfekte Zahlen 73
12.2 Die Chance, zwei teilerfremde Zahlen zu ziehen 75
12.3 Sätze über Teilbarkeit 75
12.4 Über die Häufigkeit von Ziffern 76
12.5 Beatty-Folgen 77
12.6 Alternativen zu Euklids Beweis 77
12.7 Primzahlen und die Riemann'sche Zetafunktion 79
12.8 Kaprekar-Konstanten 82

Index **84**

Abbildungsverzeichnis

4.1 Die Fano-Ebene. 21

1 Kleine Zahlenkunde

Bevor wir in das weite Feld der Zahlentheorie einsteigen, müssen wir uns zwangsläufig erst einmal damit befassen, was wir unter Zahlen verstehen wollen. Dabei wird sich zeigen, dass wir die Zahlbereiche immer weiter ausweiten müssen, um bestimmte Gleichungen lösen zu können. So beschreiten wir hier den Weg von den natürlichen bis zu den reellen Zahlen. Die Zahlbereiche ab den komplexen Zahlen werden später behandelt.

1.1 Natürliche Zahlen

Die *natürlichen Zahlen* können durch verschiedene Axiomensysteme eingeführt werden. Am intuitivsten sind wohl die *Peano-Axiome*:

1. 1 ist eine Zahl.
2. Jede Zahl n hat genau einen Nachfolger n'.
3. 1 ist nicht Nachfolger einer Zahl.
4. Jede Zahl ist Nachfolger höchstens einer Zahl.
5. Von allen Mengen, die die Zahl 1 und mit der Zahl n auch deren Nachfolger n' enthalten, ist die Menge $\mathbb{N}$ der natürlichen Zahlen die kleinste. (Prinzip der *vollständigen Induktion*).

Hier bedeutet „Zahl“ stets „natürliche Zahl“, denn etwas anderes haben wir ja noch nicht definiert. Durch Hinzunahme der Null entsteht die Menge $\mathbb{N}_0 = \mathbb{N} \cup \{0\}$.

1.2 Ganze Zahlen

Um Gleichungen der Form $x = a - b$ mit $a, b \in \mathbb{N}_0$ mit $b > a$ lösen zu können, führt man die negativen ganzen Zahlen $\mathbb{Z}^-$ ein. Sie entstehen durch Spiegelung des Zahlenstrahls am Nullpunkt. Die natürlichen Zahlen bilden die Menge $\mathbb{Z}^+ = \mathbb{N}$ (die positiven ganzen Zahlen). Insgesant ist die Menge der *ganzen Zahlen* $\mathbb{Z} = \mathbb{Z}^- \cup \{0\} \cup \mathbb{Z}^+$.

1.3 Rationale Zahlen

Die Menge der ganzen Zahlen ist bezüglich der Addition und Subtraktion abgeschlossen. Das heißt, sind a und b zwei ganze Zahlen, so ist $a+b$ sowie $a-b$ wieder eine ganze Zahl. Das gleiche gilt für die Multiplikation. Bei der Division treten allerdings Probleme auf. Denn ist $|a|$ kein Vielfaches von $|b|$, so ist a/b keine ganze Zahl. Zur Lösung definieren wir die Menge $\mathbb{Q}$ der *rationalen Zahlen*: $\mathbb{Q} = \{a/b \,|\, a, b \in \mathbb{Z}, b \neq 0\}$.

1.4 Reelle Zahlen

Die rationalen Zahlen bilden die Menge der endlichen oder periodischen Dezimalbrüche. Aber was ist mit den unendlichen nicht-periodischen Dezimalbrüchen? Beispielsweise kann man die positive Lösung der Gleichung $x^2 = 2$ durch eine Intervallschachtelung rationaler Zahlen beliebig annähern, aber man wird nie zu einem Ende kommen oder eine Periode finden.

Wir beweisen nun, dass unser Beispiel $\sqrt{2}$ irrational ist. Dazu führen wir einen Widerspruchsbeweis. Angenommen, $\sqrt{2}$ wäre rational, dann gäbe es teilerfremde $p, q \in \mathbb{Z}, q \neq 0$ so, dass $(p/q)^2 = 2$. Daraus folgt $p^2 = 2 \cdot q^2$, d. h., 2 ist Teiler von p. Ersetzen wir p durch $2p'$, so erhalten wir $q^2 = (2p')^2/2 = 2 \cdot p'^2$, was bedeutet, dass 2 auch Teiler von q ist. Da aber p und q teilerfremd sein sollten, haben wir einen Widerspruch hergeleitet. Also ist $\sqrt{2}$ irrational. □

Ein anderes einfaches Beispiel ist die Zahl, die die Gleichung $2^x = 3$ bzw. $x = \log_2 3$ erfüllt. Wäre x rational, dann wäre $x = p/q$ und $2^{p/q} = 3$, was auf $2^p = 3^q$ führt. Das widerspricht aber dem *Fundamentalsatz der Arithmetik*[1]. □

Die *reellen Zahlen* $\mathbb{R}$ setzen sich also aus den rationalen und den *irrationalen* Zahlen $\mathbb{R}\backslash\mathbb{Q}$ zusammen. Über die genauen Verhältnisse dieser Zusammensetzung werden wir später mehr erfahren. Ebenfalls später werden wir Verfahren kennenlernen, um irrationalen Zahlen zu „konstruieren“. Die irrationalen Zahlen selber lassen sich noch in die *algebraischen* und in die *transzendenten* Zahlen unterteilen.

1.4.1 Algebraische Zahlen

Eine Zahl x heißt algebraisch, wenn sie die Lösung eines Polynoms mit ganzzahligen Koeffizienten ist, d. h.

$$a_n x^n + a_{n-1} x^{n-1} + \ldots a_1 x + a_0 = 0 \qquad \text{mit } a_i \in \mathbb{Z}, a_n \neq 0$$

erfüllt. Wenn n der kleinstmögliche Grad des Polynoms ist, heißt x algebraisch vom Grad n. Die rationalen Zahlen sind also algebraisch vom Grad 1 (die einzigen algebraischen Zahlen, die nicht irrational sind), Quadratwurzeln aus Zahlen, die keine Quadratzahlen

[1] Satz von der eindeutigen Primfaktorzerlegung

sind, sind somit vom Grad 2. Die Summe, die Differenz, das Produkt und der Quotient zweier algebraischer Zahlen ist wieder algebraisch.

Die Menge der algebraischen Zahlen ist abzählbar, da sowohl die Koeffizienten der Polynome als auch der Grad der Polynome selbst abzählbar sind. Wir wissen aber, dass die Menge der reellen Zahlen überabzählbar ist. Die Lösung dieses Problems sind die transzendenten Zahlen.

1.4.2 Transzendente Zahlen

Eine reelle Zahl, die nicht algebraisch ist, heißt transzendent. Es gibt also „wesentlich mehr“ transzendente als algebraische Zahlen. Schließlich ist die Summe aus einer transzendenten und einer algebraischen Zahl transzendent.

1.4.3 Die reellen Zahlen als Körper

Die reellen Zahlen bilden eine algebraische Struktur, die man *Körper* nennt. Dieser Körper hat folgende Eigenschaften:

- Bezüglich der Addition gilt:
  - $x + y = y + x$ für alle $x, y \in \mathbb{R}$ (Kommutativgesetz)
  - $x + (y + z) = (x + y) + z$ für alle $x, y, z \in \mathbb{R}$ (Assoziativgesetz)
  - $0 + x = x + 0 = x$ für alle $x \in \mathbb{R}$ (Existenz des neutralen Elements)
  - $x + (-x) = (-x) + x = 0$ für alle $x \in \mathbb{R}$ (Existenz des inversen Elements)
- Bezüglich der Multiplikation gilt:
  - $x \cdot y = y \cdot x$ für alle $x, y \in \mathbb{R}$ (Kommutativgesetz)
  - $x \cdot (y \cdot z) = (x \cdot y) \cdot z$ für alle $x, y, z \in \mathbb{R}$ (Assoziativgesetz)
  - $1 \cdot x = x \cdot 1 = x$ für alle $x \in \mathbb{R}$ (Existenz des neutralen Elements)
  - $x \cdot 1/x = 1/x \cdot x = 1$ für alle $x \in \mathbb{R}\backslash\{0\}$ (Existenz des inversen Elements)
- Distributivgesetze:
  - $x \cdot (y + z) = x \cdot y + x \cdot z$ für alle $x, y, z \in \mathbb{R}$
  - $(x + y) \cdot z = x \cdot z + y \cdot z$ für alle $x, y, z \in \mathbb{R}$

2 Rationale vs. reelle Zahlen

Es gibt unendlich viele rationale Zahlen. Es gibt auch unendlich viele irrationale Zahlen. Es gibt aber nicht gleich viele rationale wie irrationale Zahlen. In einem gewissen Sinn gibt es „unendlich viel mehr“ irrationale Zahlen. Betrachtet man die Verteilung der reellen Zahlen auf der Zahlengeraden, so könnte man naiv annehmen, dass auf „viele“ irrationale Zahlen eine rationale Zahl kommt, dass die rationalen Zahlen praktisch „dünn“ verteilt sind.

Tatsächlich ist das Gegenteil der Fall. Die rationalen wie die irrationalen Zahlen liegen auf der Zahlengeraden *dicht*. Das bedeutet, dass man zwischen zwei beliebig weit voneinander entfernten Punkten auf der Zahlengeraden unendlich viele rationale wie irrationale Zahlen findet.

Um das zu zeigen, reicht es aus zu beweisen, dass man zwischen zwei Punkten eine rationale bzw. irrationale Zahl findet. Denn dann liegt wieder eine Zahl zwischen dieser und einer der beiden anderen usw. Also impliziert die Existenz einer einzigen Zahl die Existenz von unendlich vielen. Um die Dichtheit der rationalen und irrationalen Zahlen zu zeigen, beweisen wir also die folgenden vier Sätze:

1. Zwischen zwei beliebigen rationalen Zahlen liegt mindestens eine rationale Zahl.
2. Zwischen zwei beliebigen rationalen Zahlen liegt mindestens eine irrationale Zahl.
3. Zwischen zwei beliebigen irrationalen Zahlen liegt mindestens eine rationale Zahl.
4. Zwischen zwei beliebigen irrationalen Zahlen liegt mindestens eine irrationale Zahl.

Beweise: Seien a und b zwei rationale (bzw. irrationale) Zahlen und $a < b$,

1. so ist $c = (a + b)/2$ rational und es gilt $a < c < b$. □
2. so unterscheiden sich a und b ab der n-ten Dezimalstelle. a) b enthält ab der n-ten Stelle nicht nur Nullen. Dann sei c die Zahl, die man erhält, wenn man von b ab der n-ten Stelle die Dezimalziffern abschneidet. Ferner hat b ab der m-ten Stelle $(m > n)$ die erste von Null verschiedene Ziffer. Dann hänge man an c noch $m - n$ Nullen an und dann eine beliebige Reihe von Zufallsziffern. Vorausgesetzt, diese Reihe ist nicht periodisch, so ist c irrational. b) b enthält ab der n-ten Stelle nur Nullen. Dann bilde man solange $b' = (a + b)/2$, bis das Verfahren a) für a und b' angewendet werden kann. □
3. so unterscheiden sich a und b ab der n-ten Dezimalstelle. Dann sei c die Zahl, die man erhält, wenn man von b ab der n-ten Stelle die Dezimalziffern abschneidet. Es ist $a < c < b$, und da c eine endliche Dezimalzahl ist, ist c rational. □

4. siehe 2., wobei die Unterscheidung a) und b) weggelassen werden kann. □

Man könnte auch noch mit denselben Verfahren zeigen, dass zwischen einer rationalen und einer irrationalen Zahl beliebig viele rationale und irrationale Zahlen liegen. Damit haben wir die Dichtheit der rationalen und reellen Zahlen auf dem Zahlenstrahl bewiesen.

Was wir hieraus gelernt haben ist, dass sich rationale und irrationale Zahlen weniger durch ihre Häufigkeit auf dem Zahlenstrahl unterscheiden, als vielmehr durch ihre „Komplexität“. Denn da rationale Zahlen Lösungen der Gleichung $a \cdot x - b = 0$ sind mit $a, b \in \mathbb{Z}$ (das sind abzählbar unendlich viele), kann ihre „Komplexität“ als kleiner angesehen werden als die der transzendenten (irrationalen) Zahlen, für die keine Polynomgleichung existiert.

3 Irrationalitätsbeweise

Im Einführungskapitel haben wir bereits zwei elementare Irrationalitätsbeweise kennen gelernt. Hier werden wir allgemeinere Regeln aufstellen, um die Irrationalität einer Zahl festzustellen. Außerdem geben wir hier die wichtigen Beweise für die Irrationalität der Euler'schen Zahl e sowie der Kreiszahl π. Transzendenz ist im Allgemeinen schwerer nachzuweisen als Irrationalität, deshalb werden wir hier nur einen exemplarischen Beweis anführen. Die Transzendenz von e und π gehört sicher zu den wichtigsten Ergebnissen der Zahlentheorie; letztere lieferte die endgültige Begründung für die Unmöglichkeit der Quadratur des Kreises.

3.1 Polynomwurzeln

Sei $P(x)$ ein Polynom n-ten Grades

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

mit $a_n, \ldots, a_o \in \mathbb{Z}$ und $a_n \neq 0$. Sei nun der gekürzte Bruch p/q Wurzel von P, dann teilt p das Absolutglied a_0 und q teilt a_n.

Beweis: Wenn p/q Wurzel von P ist, dann ist $q^n \cdot P(p/q) = 0$ und somit

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

Also teilt p das Produkt $a_0 \cdot q^n$, aber da p und q teilerfremd sind, teilt p die Zahl a_0. Aus dem gleichen Grund teilt q nun a_n. □

Anwendungen:

- Die Wurzeln des unitären Polynoms ($a_n = 1$) sind entweder ganze Zahlen oder irrational.
  Beweis: Da q den Koeffizienten $a_n = 1$ teilen muss, ist $q = \pm 1$. □
- Die Wurzeln von $x^n - a_0 = 0$ mit $n > 1$ und a_0 prim sind irrational.
  Beweis: q müsste 1 teilen, also $q = \pm 1$. p müsste die Primzahl a_0 teilen, also $p = 1$ oder $p = a_0$. Beide Möglichkeiten erfüllen die Gleichung nicht. □

  U. a. sind also $\sqrt{2}$, $\sqrt{3}$, $\sqrt{5}$, ... irrational.

Wir haben somit ein allgemeines Kriterium gefunden, um herauszufinden, ob ein gegebener Wurzelterm irrational ist oder nicht.
Beispiel: Prüfe, ob $\sqrt[3]{6}$ irrational ist!

$$x = \sqrt[3]{6} \iff x^3 - 6 = 0.$$

Wir finden $q = \pm 1$, $p = 1, 2, 3, 6$. Wir erhalten keine Lösung der Gleichung, also ist x irrational.

3.2 Die Irrationalität von e

Die Irrationalität von e ist der Schlüssel zur Irrationlität von gewissen Potenzen von e und Logarithmen. Wir betrachten hier gleich zwei Beweise, die sich in ihrer Vorgehensweise unterscheiden.

Beweis 1: Wir betrachten nicht e, sondern dessen Kehrwert 1/e. Wenn 1/e irrational ist, muss auch e irrational sein. Für 1/e existiert die Reihenentwicklung

$$\frac{1}{\mathrm{e}} = \sum_{i=0}^{\infty} \frac{(-1)^i}{i!}$$

oder ausgeschrieben $1/\mathrm{e} = 1/0! - 1/1! + 1/2! - 1/3! + \cdots$
Sei $S(k)$ die k-te Partialsumme dieser Reihe, so ist $S(k) - S(k-1) = \pm 1/k!$. Bilden wir eine Tabelle aus sukzessiven Partialsummen, so können wir den Wert von 1/e immer genauer eingrenzen. Wenn man die Werte jeder Zeile auf einen gemeinsamen Nenner bringt, erhält man:

$$\begin{aligned} 2/6 < \ & 1/\mathrm{e} \ < 3/6 \\ 8/24 < \ & 1/\mathrm{e} \ < 9/24 \\ 44/120 < \ & 1/\mathrm{e} \ < 45/120 \\ 264/720 < \ & 1/\mathrm{e} \ < 265/720 \\ & \cdots \end{aligned}$$

Wobei die Zähler immer um 1 differieren und die Nenner gleich $k!$ sind. Der ersten Zeile entnehmen wir, dass der Nenner von $1/\mathrm{e} = p/q$ kein Teiler von 6 sein kann. Ansonsten könnte man 1/e nämlich als $m/6$ schreiben, aber es existiert kein m zwischen 2 und 3 Genauso kann q kein Teiler von 24, 120, 720 usw. sein. Die Tabelle enthält aber alle Nenner $k!$, und jedes m ist Teiler von $k!$ für alle $m \leq k$. Folglich kann 1/e und somit e nicht rational sein. □

Beweis 2: Diesmal benutzen wir gleich die Reihenentwicklung von e

$$\mathrm{e} = \sum_{i=0}^{\infty} \frac{1}{i!}$$

oder ausgeschrieben $\mathrm{e} = 1/0! + 1/1! + 1/2! + 1/3! + \cdots$
Sei nun $\mathrm{e} = p/q$ mit $q > 1$, dann ist

$$q! \left(\mathrm{e} - 1 - \frac{1}{1!} - \frac{1}{2!} - \ldots - \frac{1}{q!} \right) = q! \left(\frac{1}{(q+1)!} + \frac{1}{(q+2)!} + \ldots \right)$$

eine ganze Zahl größer Null. Eine Abschätzung für die rechte Seite ergibt jedoch

$$\frac{1}{q+1} + \frac{1}{(q+1)(q+2)} + \cdots < \frac{1}{2} + \frac{1}{2^2} + \cdots = 1,$$

was ein Widerspruch ist. □

3.3 Das Niven-Polynom

An dieser Stelle brauchen wir einen kleinen Einschub, um zu weiteren Erkenntnissen zu gelangen. Im Folgenden werden wir unter $N_n(x)$ ein ganz bestimmtes Polynom verstehen, das definiert ist als

$$N_n(x) = \frac{x^n(1-x)^n}{n!} = \frac{1}{n!}\sum_{i=n}^{2n}(-1)^{i-n}\binom{n}{i-n}x^i.$$

Man kann unmittelbar ablesen, dass $N_n(x) = 0$ für $x = 0$ und $x = 1$. Allgemein ist

$$N_n(x) = N_n(1-x).$$

Daher haben wir für jedes n bei $x = 1/2$ einen Extrempunkt. Ferner gilt die Ungleichung

$$0 < N_n(x) < \frac{1}{n!} \quad \text{für}\, 0 < x < 1.$$

An den Nullstellen gilt

$$N_n^{(m)}(0) = N_n^{(m)}(1) = 0 \quad \text{für}\, m < n \,\text{und}\, m > 2n$$

sowie

$$N_n^{(m)}(0) = N_n^{(m)}(1) = \frac{m!}{n!} \cdot a_m \quad \text{für}\, n \le m \le 2n,$$

wobei a_m der Koeffizient von x^m und mit $^{(m)}$ die m-te Ableitung gemeint ist. Außerdem ist

$$N_n^{(2n+k)}(x) = 0 \quad \text{für}\, k > 0.$$

Wichtig für uns ist die Erkenntnis, dass $N_n(x)$ und seine Ableitungen an $x = 0$ und $x = 1$ nur ganzzahlige Werte annehmen.

3.4 Potenzen von e

Für jedes $a \in \mathbb{Z}^+$ ist e^a irrational.

Der Beweis ist etwas kompliziert; wir brauchen einige Vorbetrachtungen, um die nachfolgende Rechnung zu verstehen. Zunächst definieren wir die Funktion

$$I(x) = a^{2n}N_n(x) - a^{2n-1}N_n'(x) + \cdots - aN_n^{(2n-1)}(x) + N_n^{(2n)}(x)$$

mit $I(0), I(1) \in \mathbb{Z}$ und berechnen

$$aI(x) = a^{2n+1}N_n(x) - a^{2n}N_n'(x) + \cdots - a^2 N_n^{(2n-1)}(x) + aN_n^{(2n)}(x)$$

sowie

$$I'(x) = a^{2n}N_n'(x) - a^{2n-1}N_n''(x) + \cdots - aN_n^{(2n)}(x) + N_n^{(2n+1)}(x).$$

Für die Summe dieser Ausdrücke, also $aI(x) + I'(x)$ ergibt sich

$$a^{2n+1}N_n(x) + N_n^{(2n+1)}(x) = a^{2n+1}N_n(x).$$

Wir nehmen nun an, $\mathrm{e}^a = p/q$ und betrachten den Ausdruck

$$q(\mathrm{e}^{ax}I(x))' = q(a\mathrm{e}^{ax}I(x) + \mathrm{e}^{ax}I'(x)) = q\mathrm{e}^{ax}(aI(x) + I'(x)) = q\mathrm{e}^{ax}a^{2n+1}N_n(x).$$

Daher können wir schreiben

$$qa^{2n+1}\int_0^1 \mathrm{e}^{ax}N_n(x)\,\mathrm{d}x = q\left[\mathrm{e}^{ax}I(x)\right]_0^1 = q[\mathrm{e}^a I(1) - I(0)] = pI(1) - qI(0).$$

Daher muss das Integral eine ganze Zahl sein. Wir haben aber für $N_n(x)$ die Ungleichung $0 < N_n(x) < 1/n!$, die man für hinreichend große n durch Multiplikation mit $qa^{2n+1}\mathrm{e}^{ax}$ und Integration über $[0;1]$ umformen kann zu

$$0 < qa^{2n+1}\int_0^1 \mathrm{e}^{ax}N_n(x)\,\mathrm{d}x < \frac{qa^{2n}(\mathrm{e}^a - 1)}{n!} < 1,$$

was ein Widerspruch ist. □

Anwendungen:

- Wenn e^a irrational ist, ist auch $1/\mathrm{e}^a = \mathrm{e}^{-a}$ irrational. Das Ergebnis kann also auf $\mathbb{Z}^-$ ausgedehnt werden.
- Für jedes $p/q \in \mathbb{Q}\backslash\{0\}$ ist $\mathrm{e}^{p/q}$ irrational.
  Beweis: Wäre $\mathrm{e}^{p/q}$ rational, dann wäre auch $(\mathrm{e}^{p/q})^q = \mathrm{e}^p$ rational — Widerspruch!□
- Für jedes $p/q \in \mathbb{Q}^+\backslash\{1\}$ ist $\ln(p/q)$ irrational.
  Beweis: Angenommen, $\ln(p/q) = a/b$, dann folgt $p/q = \mathrm{e}^{a/b}$ — Widerspruch! □
- Somit sind also e, e^2, $\sqrt{\mathrm{e}}$, $\mathrm{e}^{-3/9}$, ... irrational.

3.5 Die Irrationalität von π

Anstatt zu beweisen, dass die Zahl π irrational ist, zeigen wir das stärkere Ergebnis π^2 ist irrational. Das impliziert die Irrationalität von π (ansonsten wäre das Quadrat einer rationalen Zahl irrational).

Der Beweis läuft ähnlich wie beim Beweis der Irrationalität von e. Wir nehmen an $\pi^2 = p/q$ und definieren die Funktion

$$J(x) = q^n(\pi^{2n}N_n(x) - \pi^{2n-2}N_n^{(2)}(x) + \pi^{2n-4}N_n^{(4)} - \cdots - \pi^2 N_n^{(2n-2)}(x) + N_n^{(2n)}(x))$$

und wissen, dass $J(0), J(1) \in \mathbb{Z}$. Wir bestimmen

$$J'(x) = q^n(\pi^{2n}N_n'(x) - \pi^{2n-2}N_n^{(3)}(x) + \pi^{2n-4}N_n^{(5)} - \cdots - \pi^2 N_n^{(2n-1)}(x) + N_n^{(2n+1)}(x))$$

$$J^{(2)}(x) = q^n(\pi^{2n}N_n^{(2)}(x) - \pi^{2n-2}N_n^{(4)}(x) + \pi^{2n-4}N_n^{(6)} - \cdots - \pi^2 N_n^{(2n)}(x) + N_n^{(2n+2)}(x)).$$

Jetzt kommen wir zur eigentlichen Rechnung:

$$\begin{aligned}(J'(x)\sin\pi x - J(x)\,\pi\cos\pi x)' &= J^{(2)}(x)\sin\pi x + J'(x)\,\pi\cos\pi x \\ &\quad -J'(x)\,\pi\cos\pi x + J(x)\,\pi^2\sin\pi x \\ &= (J^{(2)}(x) + \pi^2\,J(x))\sin\pi x \\ &= \pi^{2n+2}q^n N_n(x)\sin\pi x \\ &= \pi^2 p^n N_n(x)\sin\pi x\end{aligned}$$

Daher haben wir

$$\pi p^n \int_0^1 N_n(x)\sin\pi x\,\mathrm{d}x = \frac{1}{\pi}\left[J'(x)\sin\pi x - J(x)\,\pi\cos\pi x\right]_0^1 = J(0) + J(1).$$

Also ist das Integral eine ganze Zahl. Wir finden aber für hinreichend große n mit der Ungleichung für $N_n(x)$ mittels Multiplikation mit $\pi p^n \sin\pi x$ und Integration über $[0;1]$

$$0 < \pi p^n \int_0^1 N_n(x)\sin\pi x\,\mathrm{d}x < \frac{2p^n}{n!} < 1,$$

was ein Widerspruch ist. □

3.6 Aussichten

Ebenso wie man beweisen kann, dass die Zahl π^2 irrational ist, kann man auch zeigen, dass die Zahl $\pi^{p/q}$ mit $p/q \in \mathbb{Q}\backslash\{0\}$ irrational ist. Zu den Logarithmen wäre noch zu ergänzen, dass auch $\log_a b$ mit $a, b \in \mathbb{Z}^+\backslash\{1\}$ irrational ist (wenn es nicht aus $\mathbb{N}$ ist).

Man kann aber auch allgemeinere Überlegungen anstellen: Kann z. B. eine irrationale Zahl zu einer irrationalen Potenz erhoben rational sein? (Die Antwort ist ja — das

wissen wir z. B. aus unserer Untersuchung der e-Funktion. Da $e^{p/q}$ irrational ist, muss die Lösung der Gleichung $e^x = n$ irrational sein. Der folgende Beweis ist jedoch weitaus einfacher.) Dazu machen wir folgende Überlegung:

$\sqrt{2}$ ist eine irrationale Zahl. Wenn $\sqrt{2}^{\sqrt{2}}$ rational wäre, hätten wir eine Lösung gefunden. Wenn $\sqrt{2}^{\sqrt{2}}$ nicht rational ist, nehmen wir $\left(\sqrt{2}^{\sqrt{2}}\right)^{\sqrt{2}}$, was nun auf jeden Fall rational ist. Das Faszinierende an diesem Beweis ist, dass es überhaupt keine Rolle spielt, ob $\sqrt{2}^{\sqrt{2}}$ nun irrational ist oder nicht [1].

Der Beweis der Irrationalität ist jedoch eine heikle Sache. So ist immer noch nicht klar, ob eine so bekannte Zahl wir die Euler-Mascheroni-Konstante γ irrational ist.

3.7 Die Liouville'sche Konstante

Zum Schluss werden wir noch einen Transzendenzbeweis führen. Es ist bemerkenswert, dass die transzendenten Zahlen den algebraischen zahlenmäßig weit überlegen sind, es aber dennoch extrem schwer fällt, eine solche explizit anzugeben. Um hier überhaupt einen Transzendenzbeweis führen zu können, müssen wir einen wichtigen Satz von Liouville benutzen.

Eine Zahl x heißt durch rationale Zahlen *schlecht approximierbar*, wenn x für alle Zahlen $p/q \in \mathbb{Q}$ der Ungleichung

$$\left| x - \frac{p}{q} \right| > \frac{\epsilon}{q^\mu}$$

mit festem $\epsilon > 0$ und $\mu > 0$ genügt. Der Satz von Liouville besagt nun, dass alle algebraischen Zahlen vom Grad $n > 1$ schlecht approximierbar sind, wobei dann $\mu = n$ ist. Es müssen also alle irrationalen Zahlen, die nicht schlecht approximierbar sind, transzendent sein.

Betrachten wir den Ausdruck

$$L = \sum_{i=0}^{\infty} a_i 10^{-i!}$$

mit $a_i \in \{1; 2; \ldots; 9\}$. Für $a_i = 1$ für jedes i ergibt sich die *Liouville'sche Konstante*, eine der esten Zahlen, deren Transzendenz bewiesen wurde. Sie besitzt eine 1 an jeder Dezimalstelle, die gleich $i!$ ist, und ansonsten nur Nullen. Wir betrachten jedoch die allgemeinere Zahl

$$L = 0{,}a_1 a_2 000 a_3 0000 \cdots,$$

wobei die Abstände zwischen den a_i immer länger werden. Sei nun L_k die Zahl, die man erhält, wenn man nur die ersten k-Terme von L berücksichtigt. Dann haben wir die

[1] Tatsächlich besagt das *Gelfond-Schneider-Theorem*, dass wenn x und y Wurzeln eines Polynoms sind und $x \neq 0$ und $x \neq 1$ und y irrational ist, muss x^y transzendent sein. $\sqrt{2}^{\sqrt{2}}$ ist also irrational.

Ungleichung

$$|L - L_k| < \frac{10}{10^{(k+1)!}}.$$

Wir werden nun zeigen, dass L nicht algebraisch sein kann. Dazu setzen wir

$$L_k = \frac{p}{q} = \frac{p}{10^{k!}}.$$

Nun muss es ein $\epsilon > 0$ geben, so dass

$$|L - L_k| > \frac{\epsilon}{10^{nk!}}$$

erfüllt ist. Die beiden Ungleichungen kann man kombinieren zu

$$\frac{\epsilon}{10^{nk!}} < |L - L_k| < \frac{10}{10^{(k+1)!}},$$

was umgeformt werden kann zu

$$\frac{10}{\epsilon} > \frac{10^{(k+1)!}}{10^{nk!}} = \frac{\left(10^{k!}\right)^{k+1}}{\left(10^{k!}\right)^{n}} = \left(10^{k!}\right)^{k+1-n},$$

was nicht stimmen kann, denn der Ausdruck rechts geht mit $k \to \infty$ gegen unendlich.□

4 Erweiterungen der reellen Zahlen

Der Körper der reellen Zahlen ist bezüglich der Operationen Addition, Subtraktion, Multiplikation und Division abgeschlossen. Dennoch gibt es algebraische Gleichungen (z. B. $x^2 = -1$), die keine reelle Lösung besitzen. Um diese Gleichungen lösen zu können, führt man den Körper der *komplexen* Zahlen ein. Dieser Körper ist nun algebraisch abgeschlossen, d. h. jede algebraische Gleichung mit komplexen Koeffizienten ist in ihm lösbar. Genauer gesagt besagt der *Fundamentalsatz der Algebra*, dass ein Polynom n-ten Grades genau n (nicht notwendigerweise verschiedene) Lösungen hat. Danach besteht vom Standpunkt der Lösbarkeit von Gleichungen kein weiterer Grund, den Zahlbereich weiter zu vergrößern. Bestimmte Rechnungen lassen sich aber im Kontext höherer Divisionsalgebren[1] vereinfachen und besser formulieren. Wir folgen hier der *Cayley-Dickson-Konstruktion*, um diese Divisionsalgebren zu konstruieren.

Im Rahmen der komplexen Zahlen finden sich wundersame Verbindungen zwischen Funktionen, die im Reellen nichts miteinander zu tun zu haben scheinen. Das bekannteste Beispiel für so eine Beziehung ist wohl die *Euler'sche Gleichung* $\mathrm{e}^{\mathrm{i}x} = \cos x + \mathrm{i}\sin x$. Darüberhinaus ist die Theorie der komplexen Funktionen von ausgesprochener mathematischer (insbesondere geometrischer) Schönheit. Davon können wir hier aber nicht reden, wir werden uns ausschließlich auf die komplexen Zahlen als Zahlbereich konzentrieren.

4.1 Komplexe Zahlen

Eine komplexe Zahl ist nichts weiter als ein Paar reeller Zahlen (a, b). Die Addition zweier komplexer Zahlen erfolgt komponentenweise, also $(a, b) + (a, c) = (a + c, b + d)$. Die Multiplikation ist $(a, b) \cdot (c, d) = (ac - bd, da + bc)$. Daraus folgt unmittelbar $(0, 1)^2 = (-1, 0)$, womit unser eingangs erwähntes Problem gelöst wäre (wobei wir insgeheim vorausgesetzt haben, dass wir die reellen Zahlen mit den komplexen Zahlen der Form $(a, 0)$ identifizieren). Diese Zahl taufen wir *imaginäre Einheit* und nennen sie i, also $\mathrm{i}^2 = (0, 1)^2 = -1$. Eine komplexe Zahl kann also auch in der Form $a + \mathrm{i}b$ geschrieben werden. Die Zahl $(a, -b)$ nennen wir zu (a, b) *komplex konjugiert* und schreiben $\overline{(a, b)} = (a, -b)$.

[1] Die genau Definition des Begriffs *Divisionsalgebra* würde uns leider zu lange aufhalten, da wir die algebraischen Grundlagen nicht haben. Wir benötigen hier vor allem die Nullteilerfreiheit, d. h. dass aus $x \cdot y = 0$ stets $x = 0$ oder $y = 0$ folgt.

4.2 Quaternionen

Wir verstehen unter einem *Quaternion* ein Paar komplexer Zahlen (a, b). Die Addition erfolgt wieder komponentenweise, aber die Multiplikation ist $(a, b)\cdot(c, d) = (ac-\overline{d}b, da+b\overline{c})$. Dies ist dieselbe Formel wie bei den komplexen Zahlen mit Ausnahme der Konjugationen. Tatsächlich hätten wir bei den komplexen Zahlen ebenfalls Konjugationen verwenden können, denn die zu einer reellen Zahl Konjugierte ist die Zahl selber. Die zu einem Quaternion (a, b) konjugierte Zahl soll $(\overline{a}, -b)$ sein, was wieder mit der Definition für komplexe Zahlen identisch ist.

Spezielle Quaternionen sind $1 = ((1, 0), (0, 0))$, $\mathrm{i} = ((0, 1), (0, 0))$, $\mathrm{j} = ((0, 0), (1, 0))$ und $\mathrm{k} = ((0, 0), (0, 1))$. j und k sind zusätzliche imaginäre Einheiten, deren Quadrat ebenfalls -1 ist, wie eine Rechnung zeigt.

Aus diesen Definitionen kann man Regeln zur Multiplikation der Einheiten herleiten. Diese lauten:

$$\mathrm{ij} = \mathrm{k}, \mathrm{ik} = -\mathrm{j}$$

$$\mathrm{ji} = -\mathrm{k}, \mathrm{jk} = \mathrm{i}$$

$$\mathrm{ki} = \mathrm{j}, \mathrm{kj} = -\mathrm{i}$$

$$\mathrm{ii} = \mathrm{jj} = \mathrm{kk} = -1$$

$$\mathrm{ijk} = -1$$

Als Beispiel beweisen wir $\mathrm{ji} = -\mathrm{k}$. Dazu berechnen wir

$$\begin{aligned}\mathrm{ji} &= ((0, 0), (1, 0)) \cdot ((0, 1), (0, 0)) \\ &= ((0, 0) \cdot (0, 1)) - (0, 0) \cdot (1, 0), (0, 0) \cdot (0, 0) + (1, 0) \cdot (0, -1)) \\ &= ((0, 0), (0, -1)) \\ &= -\mathrm{k}.\end{aligned}$$

□

4.3 Oktaven

Bildet man ein Paar von Quaternionen, so entstehen die *Cayley-Zahlen* oder *Oktaven*. Die Muktiplikations- und die Konjugationsregel ist mit denen für die Quaternionen definierten identisch. So wie komplexe Zahlen und Quaternionen können auch Oktaven als Linearkombination der imaginären Einheiten geschrieben werden. Um das Ganze übersichtlich zu halten, benennt man sie um in e_1 bis e_7. Wie bei den Quaternionen ist $e_i^2 = -1$, und sie sind bezüglich der Multiplikation *antikommutativ*, d. h. $e_i \cdot e_k = -e_k \cdot e_i$. Wie man die imaginären Einheiten im Einzelnen zu multiplizieren hat, liest man am Besten an der *Fano-Ebene* ab. Die Fano-Ebene ist ein Gebilde aus der projektiven Geometrie, das uns als Schaubild dienen soll.

Wir multiplizieren die Einheiten, indem wir einfach den Pfeilen folgen. Man erhält also z. B. $e_7 \cdot e_2 = e_5$, $e_6 \cdot e_4 = e_2$ oder $e_2 \cdot e_3 = e_1$. Außerdem erkennen wir die Übereinstimmung mit den Rechenregeln für Quaternionen.

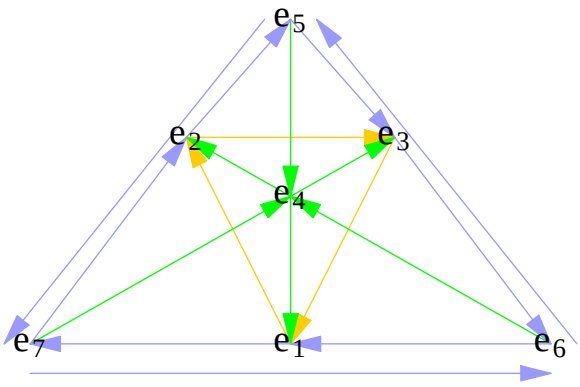

Abbildung 4.1: Die Fano-Ebene.

Allen vier Zahlbereichen (reelle Zahlen, komplexe Zahlen, Quaternionen und Oktaven) ist gemeinsam, dass zu einer Zahl ein multiplikativ inverses Element existiert. Ebenso waren alle Zahlbreiche Divisionsalgebren. Führt man einen weiteren Konstruktionsschritt durch und bildet ein Paar von Oktaven, so ist dies nicht mehr der Fall. Und es geht noch weiter: Waren die reellen und komplexen Zahlen kommutativ bezüglich der Multiplikation, so sind es die Quaternionen nicht mehr. Die Oktaven schließlich sind nicht mal mehr assoziativ bezüglich der Multiplikation. Es macht also algebraisch wenig Sinn, das Konstruktionsverfahren fortzusetzen.

4.4 Allgemeine Ergebnisse

Wir werden jetzt ein paar allgemeine Eigenschaften dieser Zahlbereiche besprechen. Um die Notation zu erleichtern, werden wir von 2^n-ionen sprechen. 2^0-ionen sind die reellen Zahlen, 2^1-ionen komplexe Zahlen, 2^2-ionen Quaternionen und 2^3-ionen Oktaven. Das Verfahren, das sich bei diesen Beweisen anbietet, ist die vollständige Induktion. Es werdeh hier eckige Gruppierungsklammern „[ ]“ verwendet, um sie von den Paarklammern „( )“ optisch abzusetzen und die Formeln lesbarer zu machen.

4.4.1 Distributivgesetz

Bevor wir uns spezielleren Eigenschaften widmen, müssen wir zuerst die Grundlagen schaffen, um unsere Rechnungen durchführen zu können. Wir werden später sehen, dass weder Kommutativgesetz noch Assoziativgesetz für alle 2^n-ionen gelten. Das Distributivgesetz gilt jedoch immer.

Wir setzen es für reelle Zahlen als gegeben voraus. Der Induktionsschritt für 2^{n+1}-ionen folgt.

- Multiplikation von links:

$$\begin{aligned}(a,b)\cdot[(c,d)+(e,f)] &= (a,b)\cdot(c+e,d+f)\\ &= (a[c+e]-\overline{d+f}b,[d+f]a+b\overline{c+e})\end{aligned}$$

Laut Induktionsvoraussetzung ist das[2]

$$(ac + ae - \overline{d}b - \overline{f}b, da + fa + b\overline{c} + b\overline{e}).$$

Den Term kann man wieder als Summe schreiben:

$$(ac - \overline{d}b, da + b\overline{c}) + (ae - \overline{f}b, fa + b\overline{e}) = (a, b) \cdot (c, d) + (a, b) \cdot (e, f). \qquad \square$$

- Multiplikation von rechts:

$$\begin{aligned}[(a, b) + (c, d)] \cdot (e, f) &= (a + c, b + d) \cdot (e, f) \\ &= ([a + c]e - \overline{f}[b + d], f[a + c] + [b + d]\overline{e})\end{aligned}$$

Wieder ist das nach Induktionsvoraussetzung gleich

$$(ae + ce - \overline{f}b - \overline{f}d, fa + fc + b\overline{e} + d\overline{e}),$$

was in eine Summe zerlegt werden kann

$$(ae - \overline{f}b, fa + b\overline{e}) + (ce - \overline{f}d, fc + d\overline{e}) = (a, b) \cdot (e, f) + (c, d) \cdot (e, f). \qquad \square$$

4.4.2 Konjugationen

Das nächste Ergebnis, das wir später brauchen werden, ist $\overline{\overline{x}} = x$. In Worten: Die Konjugation der zu einem 2^n-ion Konjugierten ist wieder die Zahl selber. Diese Gleichung gilt natürlich für die komplexen Zahlen, aber wir werden es allgemein beweisen. Für ein 2^{n+1}-ion gilt $\overline{\overline{(a, b)}} = \overline{(\overline{a}, -b)} = (\overline{\overline{a}}, -[-b])$. Dies ist nach Induktionsvoraussetzung gleich (a, b). $\square$

Weitere Eigenschaften komplexer Zahlen sind $\overline{x + y} = \overline{x} + \overline{y}$ und $\overline{xy} = \overline{y}\,\overline{x}$.

Beweis der Summenregel:

$$\overline{(a, b) + (c, d)} = \overline{(a + c, b + d)} = (\overline{a + c}, -[b + d]).$$

Laut Induktionsvoraussetzung ist dies

$$(\overline{a} + \overline{c}, -b + -d) = (\overline{a}, -b) + (\overline{c}, -d) = \overline{(a, b)} + \overline{(c, d)}. \qquad \square$$

[2] Die Umformung der Konjugation einer Summe kann hier angewendet werden, da unten der Beweis ohne das Distributivgesetz geführt wird.

Beweis der Produktregel:

$$\overline{(a,b)\cdot(c,d)} = \overline{(ac-\overline{d}b, da+b\overline{c})} = (\overline{ac-\overline{d}b}, -[da+b\overline{c}]).$$

Aus der Induktionsvoraussetzung folgt die Gleichheit zu

$$(\overline{c}\,\overline{a}-\overline{b}d, -da+-b\overline{c}) = (\overline{c}\,\overline{a}-\overline{-b}[-d], -da+[-b]\overline{c}).$$

Durch die Minuszeichen können wir das schreiben als

$$(\overline{c},-d)\cdot(\overline{a},-b) = \overline{(c,d)}\cdot\overline{(a,b)}. \qquad \square$$

Es ist bekannt, dass die Summe und das Produkt aus einer komplexen Zahl und ihrer Konjugierten reell ist. Überraschenderweise gilt dies für alle hier erzeugten Zahlbereiche.

Der Induktionsanfang ist trivial: Sowohl die Summe als auch das Produkt aus reellen Zahlen ist reell. Die Konjugation eines 2^{n+1}-ions (a,b) ist $(\overline{a},-b)$. Daher ist die Summe aus $(a,b)+(\overline{a},-b) = (a+\overline{a},0)$ sowie das Produkt $(a,b)\cdot(\overline{a},-b) = (a\overline{a}-\overline{-b}b, [-b]a + ba) = (a\overline{a}+\overline{b}b, 0)$ und $(\overline{a},-b)\cdot(a,b) = (\overline{a}a-\overline{b}[-b], b\overline{a}+[-b]\overline{a}) = (\overline{a}a+\overline{b}b, 0)$. Laut Induktionsvoraussetzung sind $a+\overline{a}$, $a\overline{a}$, $\overline{a}a$ und $\overline{b}b$ reell, womit der Beweis erbracht wäre. $\square$

Nebenbei haben wir bewiesen, dass das Produkt $x\overline{x}$ und $\overline{x}x$ nicht nur reell, sondern auch positiv ist für $x \neq 0$[3].

4.4.3 Multiplikativ inverses Element

Aufgrund der obigen Ergbenisse können wir nun das multiplikativ inverse Element jedes 2^n-ions angeben. Da $x\overline{x}$ für $x \neq 0$ immer reell und positiv ist, ist $\overline{x}/[x\overline{x}]$ zu jedem x multiplikativ invers.

4.4.4 Kommutativität, Assoziativität und das Ende der Divisionsalgebren

Wir haben bereits erwähnt, dass die 2^4-ionen keine Divisionsalgebra mehr sind. Darüberhinaus haben wir gesehen, dass die 2^n-ionen mit wachsendem n der Reihe nach Kommutativität und Assoziativität verlieren. Diesen Prozess werden wir uns nun genauer ansehen.

Um zu sehen, warum die 2^4-ionen keine Divisionsalgebra mehr sind, werden wir versuchen, allgemein zu beweisen, dass 2^n-ionen immer eine Divisionsalgebra sind. Angenommen,

$$(a,b)\cdot(c,d) = (ac-\overline{d}b, da+b\overline{c}) = (0,0) = 0.$$

[3]Im Realteil steht nämlich die Summe zweier positiver Zahlen.

Dann muss gelten $ac - \overline{d}b = 0$ und $da + b\overline{c} = 0$. Wir multiplizieren die erste Gleichung mit $\overline{c}$, die zweite Gleichung mit $\overline{d}$: $[ac]\overline{c} - [\overline{d}b]\overline{c} = 0$ sowie $\overline{d}[da] + \overline{d}[b\overline{c}] = 0$. Die Summe dieser Gleichungen ist

$$[ac]\overline{c} - [\overline{d}b]\overline{c} + \overline{d}[b\overline{c}] + \overline{d}[da] = 0.$$

Wenn nun die 2^{n-1}-ionen assoziativ wären, würden sich die beiden mittleren Summanden herauskürzen und man erhielte $a[c\overline{c}]+[\overline{d}d]a = 0$. Da sowohl $c\overline{c}$ als auch $\overline{d}d$ reell sind, kann man das Kommutativgesetz anwenden und man erhält $c\overline{c} + \overline{d}d = 0$ (woraus $c = 0$ und $d = 0$ folgt) oder $a = 0$ (woraus $b = 0$ folgt). Da die Oktaven aber nicht assoziativ sind, kann man diese Umformung nicht machen, und es liegt ein starker Hinweis vor, dass die 2^4-ionen keine Divisionsalgebra sind. Die Oktaven sind dagegen eine Divisionsalgebra, da die Quaternionen assoziativ sind.

Was uns zur nächsten Frage führt: Wieso sind die Oktaven nicht assoziativ? Dazu werden wir wieder allgemein beweisen, dass alle 2^n-ionen assoziativ sind:

$$\begin{aligned}
[(a,b)\cdot(c,d)]\cdot(e,f) =& (ac - \overline{d}b, da + b\overline{c})\cdot(e,f)\\
=& ([ac - \overline{d}b]e - \overline{f}[da + b\overline{c}], f[ac - \overline{d}b] + [da + b\overline{c}]\overline{e})\\
=& ([ac]e - [\overline{d}b]e - \overline{f}[da] - \overline{f}[b\overline{c}],\\
& f[ac] - f[\overline{d}b] + [da]\overline{e} + [b\overline{c}]\overline{e})\\
(a,b)\cdot[(c,d)\cdot(e,f)] =& (a,b)\cdot(ce - \overline{f}d, fc + d\overline{e})\\
=& (a[ce - \overline{f}d] - \overline{fc + d\overline{e}}\,b, [fc + d\overline{e}]a + b\,\overline{ce - \overline{f}d})\\
=& (a[ce] - a[\overline{f}d] - [\overline{c}\,\overline{f}]b - [e\overline{d}]b,\\
& [fc]a + [d\overline{e}]a + b[\overline{e}\,\overline{c}] - b[\overline{d}f])
\end{aligned}$$

Die beiden Ausdrücke sind unter der Bedingung gleich, dass die 2^{n-1}-ionen assoziativ und kommutativ sind. Die Oktaven sind also nicht assoziativ, weil die Quaternionen nicht kommutativ sind. Die Quaternionen sind assoziativ, weil die komplexen Zahlen kommutativ sind.

Was uns zur nächsten Frage führt: Wieso sind die Quaternionen nicht kommutativ?

$$\begin{aligned}
(a,b)\cdot(c,d) &= (ac - \overline{d}b, da + b\overline{c})\\
(c,d)\cdot(a,b) &= (ca - \overline{b}d, bc + d\overline{a})
\end{aligned}$$

Diese Terme sind genau dann gleich, wenn die 2^{n-1}-ionen kommutativ und gleich ihrer Konjugierten sind. Die Quaternionen sind also nicht kommutativ, weil die komplexen Zahlen nicht gleich ihren komplex Konjugierten sind. Und die komplexen Zahlen sind kommutativ, weil die reellen Zahlen mit ihren Konjugierten identisch sind.

Was uns zur nächsten Frage führt: Wieso sind die komplexen Zahlen nicht gleich ihren Konjugierten? $\overline{(a,b)} = (\overline{a}, -b)$. Dies ist genau dann gleich (a,b), wenn die 2^{n-1}-ionen gleich ihren Konjugierten sind und $b = -b$ oder $2b = 0$ ist. In der Sprache der Algebra sagt man, die 2^{n-1}-ionen müssen die Charakteristik 2 haben. Da die reellen Zahlen aber offenbar nicht die Charakteristik 2 haben, sind die komplexen Zahlen ungleich ihren Konjugierten, sind die Quaternionen nicht kommutativ, sind die Oktaven nicht assoziativ

und sind die 2^4-ionen keine Divisionsalgebra. (Letzteres haben wir nicht streng bewiesen.) Wenn wir nun noch zeigen können, dass ein 2^n-ion keine Divisionsalgebra sein kann, wenn es das 2^{n-1}-ion nicht ist, haben wir bewiesen, dass es nur vier Divisionsalgebren in unserem Schema gibt.
$(x, 0) \cdot (y, 0) = (xy, 0) = (0, 0) = 0$. Dies ist nur dann der Fall, wenn $xy = 0$ ist. □

Zum Abschluss sei noch bemerkt: Selbst wenn wir mit einer Algebra der Charakteristik 2 starten und die Cayley-Dickson-Konstruktion anwenden, werden wir keine unendliche Folge von Divisionsalgebren erhalten.

4.5 Hyperkomplexe Zahlen

Quaternionen wurden von Hamilton eingeführt, um eine Verallgemeinerung der komplexen Zahlen zu schaffen. Wir haben schon bermekt, dass dabei das Kommutativgesetz verloren geht. Aber es gibt noch eine andere Verallgemeinerung der komplexen Zahlen, die *hyperkomplexen Zahlen*, in der das Kommutativgesetz gilt. Sie wurden ebenfalls von Hamilton untersucht. Er entdeckte, dass in diesem Zahlbereich dafür eine andere wichtige Eigenschaft feht, und zwar die Existenz eines multiplikativ inversen Elements für jede hyperkomplexe Zahl.

Die Multiplikationsregeln für hyperkomplexe Zahlen sind:

$$\mathrm{ij} = \mathrm{k}, \mathrm{ik} = -\mathrm{j}$$

$$\mathrm{ji} = \mathrm{k}, \mathrm{jk} = -\mathrm{i}$$

$$\mathrm{ki} = -\mathrm{j}, \mathrm{kj} = -\mathrm{i}$$

$$\mathrm{ii} = \mathrm{jj} = -\mathrm{kk} = -1$$

$$\mathrm{ijk} = 1$$

Man beachte die Erhaltung der Kommutativität, z. B. $\mathrm{ij} = \mathrm{ji} = \mathrm{k}$.

5 Teiler und Vielfache

Nachdem wir uns bis jetzt vornehmlich mit reellen Zahlen beschäftigt haben, werden wir nun etwas *elementare Zahlentheorie* betreiben. Sie ist elementar in dem Sinne, dass keine Methoden aus der Analysis verwendet werden. Der neue Zahlenbereich, den wir nun betrachten werden, ist also die Menge der ganzen Zahlen $\mathbb{Z}$. Im weiteren Text ist, soweit nicht anders vermerkt, mit „Zahl“ stets „ganze Zahl“gemeint.

5.1 Vorbetrachtungen

Beginnen wir mit den denkbar einfachsten Eigenschaften ganzer Zahlen: Ist $a \in \mathbb{Z}$, so gilt entweder $a < 0, a = 0$ oder $a > 0$. Dabei gelten folgende Bezeichnungen:

- $a < 0$: a heißt *negativ*
- $a \leq 0$: a heißt *nichtpositiv*
- $a = 0$: a heißt *Null*
- $a \geq 0$: a heißt *nichtnegativ*
- $a > 0$: a heißt *positiv*

Eine weitere unmittelbare Möglichkeit, die ganzen Zahlen in zwei Mengen zu unterteilen, ist die Unterscheidung zwischen *geraden* und *ungeraden* Zahlen. Ist $a \in \mathbb{Z}$ gerade, so ist $a = 2k$ mit $k \in \mathbb{Z}$, wogegen ein ungerades a als $a = 2k - 1$ dargestellt wird. Alle geraden Zahlen sind durch 2 teilbar, alle ungeraden nicht.

Wir erhalten die Menge der geraden Zahlen

$$\mathbb{G} = \{\, a \mid\ a = 2k, k \in \mathbb{Z} \,\}$$

und die Menge der ungeraden Zahlen

$$\mathbb{U} = \{\, a \mid\ a = 2k - 1, k \in \mathbb{Z} \,\}.$$

Die Eigenschaft der ganzen Zahlen, entweder gerade oder ungerade zu sein, bezeichnet man als *Parität*.

Wir untersuchen nun, wie gerade und ungerade Zahlen bei den Operationen Addition und Multiplikation zusammenwirken. Seien $g, h \in \mathbb{G}$ und $u, v \in \mathbb{U}$, so erhalten wir

$$\begin{aligned} g + h &= (2k) + (2l) = 2(k + l) \\ u + v &= (2k - 1) + (2l - 1) = 2(k + l - 1) \\ g + u &= (2k) + (2l - 1) = 2(k + l) - 1 \end{aligned}$$

Die Summe zweier Zahlen gleicher Parität ist also immer gerade, wogegen die Summe zweier Zahlen verschiedener Parität immer ungerade ist.

$$g \cdot h = (2k) \cdot (2l) = 4kl = 2(2kl)$$
$$u \cdot v = (2k-1) \cdot (2l-1) = 4kl - 2k - 2l + 1 = 2(2kl - k - l + 1) - 1$$
$$g \cdot u = (2k) \cdot (2l-1) = 4kl - 2k = 2(2kl - k)$$

Hier ergibt sich keine Ausgewogenheit zwischen geraden und ungeraden Zahlen: Das Produkt zweier Zahlen ist nur dann ungerade, wenn beide Faktoren ungerade sind.

5.2 Teiler

Die Zahl $b \in \mathbb{Z}$ teilt $a \in \mathbb{Z}$, wenn es ein $c \in \mathbb{Z}$ gibt mit $a = bc$. Man schreibt $b|a$, und b heißt *Teiler* von a. Die Menge aller Teiler von a ist $\{\, b \in \mathbb{Z} \mid b|a \,\}$.

Da $a|a$ und $1|a$ immer gilt, nennt man a und 1 auch *triviale Teiler* von a. Teiler, die keine trivialen Teiler sind, heißen *echt*.

Eng verbunden mit dem Begriff des Teilers ist der Begriff des Rests: Sind $a, b \in \mathbb{Z}$, $b > 0$, dann gibt es ein $r \in \mathbb{Z}$, $r < b$ mit $b|(a - r)$.
Beweis: Sei $C = \{\, c \in \mathbb{Z} \mid cb \leq a \,\}$ und $d = \max(C)$.[1] Dann ist

$$bd + b > a \geq bd \iff 0 \leq a - bd < b.$$

Mit $r = a - bd$ ist der Satz bewiesen. □

Es heißt r der *Rest* von a modulo b, geschrieben $a = r \bmod b$.

Für Teiler gelten die folgenden Rechenregeln:

- $a|b$ und $a|c \Rightarrow a|(b \pm c)$
  Beweis: $a|b \iff b = pa$, $a|c \iff c = qa : b \pm c = pa \pm qa = (p \pm q)a$ □
- $a|b$ und $a|c \Rightarrow a|(b \cdot c)$
  Beweis: $a|b \iff b = pa$, $a|c \iff c = qa : b \cdot c = pa \cdot qa = (p \cdot q \cdot a)a$ □
- $a|b$ und $b|c \Rightarrow a|c$
  Beweis: $a|b \iff b = pa$, $b|c \iff c = qb : c = q \cdot (pa) = (qp) \cdot a$ □
- $a|b$ und $b|a \Rightarrow a = \pm b$
  Beweis: $a|b \iff b = pa$, $b|a \iff a = qb$
  $a = q \cdot (pa) = (qb) \cdot a \Rightarrow qp = 1 \Rightarrow p = \pm 1$ □

In den obigen Sätzen war a manchmal sowohl Teiler von b als auch von c. Daher nennt man a auch *gemeinsamen Teiler* von b und c. Genauer: Seien $a \in \mathbb{N}$, $b, c \in \mathbb{Z}$. Dann heißt a gemeinsamer Teiler von b und c, wenn $a|b$ und $a|c$ gilt. Haben zwei Zahlen außer ± 1

[1] Dieses Maxiumum existiert, da C eine endliche nichtleere Teilmenge von $\mathbb{Z}$ ist.

keinen gemeinsamen Teiler, so heißen sie *teilerfremd* oder *relativ prim*. Der maximale gemeinsame Teiler von b und c heißt *größter gemeinsamer Teiler* und wird mit $\mathrm{ggT}(b, c)$ bezeichnet.

Für den ggT gelten offenbar folgende Beziehungen:

- $\mathrm{ggT}(a, b) = \mathrm{ggT}(b, a)$
- $\mathrm{ggT}(a, b) = \mathrm{ggT}(-a, b)$
- $\mathrm{ggT}(a, 0) = |a|$

Außerdem haben wir die Sätze:

- $\mathrm{ggT}(a, b) = \mathrm{ggT}(a - b, b)$ für $a > b$
  Beweis: Sei $c = \mathrm{ggT}(a, b)$. Da $c|a$ und $c|b$ folgt $c|(a - b)$. Dann folgt aus $a > b$, dass $c \geq \max\left(\left\{d \in \mathbb{Z} \,\middle|\, d|(a-b)\right\}\right)$. Außerdem ist $c \leq \max\left(\left\{d \in \mathbb{Z} \,\middle|\, d|b\right\}\right)$. Aus Kombination der Ungleichungen folgt $c = \mathrm{ggT}(a - b, b)$. Die Umkehrung erhält man genauso. □
- $\mathrm{ggT}(a, b) = \mathrm{ggT}(a, b - a)$ für $a < b$
  Beweis: Sei $c = \mathrm{ggT}(a, b)$. Da $c|a$ und $c|b$ folgt $c|(b - a)$. Dann folgt aus $b > a$, dass $c \geq \max\left(\left\{d \in \mathbb{Z} \,\middle|\, d|(b-a)\right\}\right)$. Außerdem ist $c \leq \max\left(\left\{d \in \mathbb{Z} \,\middle|\, d|a\right\}\right)$. Aus Kombination der Ungleichungen folgt $c = \mathrm{ggT}(a, b - a)$. Die Umkehrung erhält man genauso. □
- $\mathrm{ggT}(a, b) = \mathrm{ggT}(b, a \bmod b)$ für $b \neq 0$
  Dieser Satz ist die Grundlage für den *Euklidischen Algorithmus*, mit dem man den ggT zweier beliebiger Zahlen bestimmen kann. Er wird unten bewiesen. □

Bei den Beweisen wurde von der Tatsache Gebrauch gemacht, dass jede endliche nichtleere Teilmenge der natürlichen Zahlen ein maximales Element hat.

Wir bestimmen nun den ggT zweier beliebiger $a, b \in \mathbb{Z}$. Aufgrund der obigen Sätze können wir annehmen, dass $a, b > 0$ und $a > b$ gilt. Dann funktioniert der Euklidische Algorithmus wie folgt:

$$a = q_0 b + r_0, \qquad 0 \leq r_0 < b,\ q_0 \in \mathbb{N}_0$$

Setze $r_{-1} = b$ und betrachte

$$b = q_1 r_0 + r_1, \qquad 0 \leq r_1 < r_0$$

und weiter

$$r_0 = q_2 r_1 + r_2, \qquad 0 \leq r_2 < r_1$$

oder allgemein

$$r_n = q_{n+2} r_{n+1} + r_{n+2}, \quad 0 \leq r_{n+2} < r_{n+1}.$$

Die Folge (r_n) ist eine nichtnegative Zahlenfolge und streng monoton fallend. Der Abbruch erfolgt also bei $r_i = 0$, und das Ergebnis ist $\mathrm{ggT}(a, b) = r_{i-1}$.
Beweis: Es gilt $r_{i-1}|a$, denn aus $r_n = q_{n+2}r_{n+1} + r_{n+2}$ folgt, dass ein gemeinsamer Teiler von r_{n+1} und r_{n+2} auch r_n teilt. Also teilt r_{i-1} alle vorhergehenden Reste und auch a. Andersherum muss ein gemeinsamer Teiler von a auch b und r_0 teilen. Zusammenfassung: Der Rest r_{i-1} ist gemeinsamer Teiler von a und b und jeder gemeinsame Teiler teilt r_{i-1}. Dann ist $r_{i-1} = \mathrm{ggT}(a, b)$. □

Dabei haben wir verwendet, dass alle gemeinsamen Teiler von a und b auch $\mathrm{ggT}(a, b)$ teilen. Das wiederum lässt sich leicht mit der *Primfaktorzerlegung* von $\mathrm{ggT}(a, b)$ verstehen. Denn existierte ein gemeinsamer Teiler von a und b, der kein Teiler von $c = \mathrm{ggT}(a, b)$ ist, dann gäbe es mindestens einen Primfaktor d von a und b, der in c (zumindest in dieser Potenz) nicht vorkommt. Das widerspricht aber der Tatsache, dass c der größte gemeinsame Teiler von a und b ist, denn $(d \cdot c)|a$ und $(d \cdot c)|b$ aber $d \cdot c \geq \mathrm{ggT}(a, b)$. □

Die Funktionsweise des Algorithmus versteht man am Besten an einem Beispiel. Wir bestimmen den ggT von $a = 45$ und $b = 12$:

$$\begin{aligned} 45 &= 3 \cdot 12 + 9 \\ 12 &= 1 \cdot 9 + 3 \\ 9 &= 3 \cdot 3 + 0 \end{aligned}$$

Das Ergebnis ist also $\mathrm{ggT}(45, 12) = 3$.

Mit Hilfe des Euklidischen Algorithmus kann man zeigen, dass $c = \mathrm{ggT}(a, b)$ die kleinste positive Zahl ist, so dass $c = xa + yb$ mit $x, y \in \mathbb{Z}$ geschrieben werden kann.
Beweis: Aus dem ersten Schritt des Algorithmus entnehmen wir, dass

$$\begin{aligned} r_0 &= a - q_0 b \quad \text{sowie} \\ r_1 &= b - q_1 r_0 = b - q_1(a - q_0 b) = -q_1 a + (1 + q_0 q_1)b, \end{aligned}$$

womit die Existenz einer solchen Darstellung für die ersten Schritte bewiesen ist. Allgemein gelte die Induktionsvoraussetzung $r_n = x_n a + y_n b$ und $r_{n+1} = x_{n+1} a + y_{n+1} b$. Dann ist der Induktionsschritt

$$\begin{aligned} r_{n+2} &= r_n - q_{n+2} r_{n+1} = x_n a + y_n b - q_{n+2}(x_{n+1} a + y_{n+1} b) \\ &= (x_n - q_{n+2} x_{n+1})a + (y_n - q_{n+2} y_{n+1})b, \end{aligned}$$

womit die Existenz für jedes n und vor allem für den $\mathrm{ggT}(a, b)$ bewiesen ist.
Umgekehrt wird jede Zahl der Form $d = x'a + y'b$ von gemeinsamen Teilern von a und b geteilt, also auch von c. Sollte c nicht die kleinste solche Zahl sein, so muss $d < c$ gelten. Es teilt c aber d, daher muss c die kleinste solche Zahl sein. □

Die folgenden Aussagen sind also äquivalent:

- $c = \mathrm{ggT}(a, b)$.
- c ist gemeinsamer Teiler von a und b, und jeder gemeinsame Teiler von a und b teilt c.
- c ist die kleinste positive Zahl, die als $c = xa + yb$ geschrieben werden kann.

5.3 Vielfache

Analog zum Begriff des Teilers ist der Begriff des *Vielfachen*: Die Zahl $a \in \mathbb{Z}$ heißt das Vielfache von $b \in \mathbb{Z}$, wenn b Teiler von a ist. Die Menge der Vielfachen von b bezeichnet man auch als $b \cdot \mathbb{Z}$.

Weiter heißt a *gemeinsames Vielfaches* von $b, c \in \mathbb{Z}$, wenn $b|a$ und $c|a$ gilt. Das *kleinste gemeinsame Vielfache* $\mathrm{kgV}(a, b)$ ist das kleinste positive gemeinsame Vielfache von a und b.

Interessanterweise gilt die Beziehung

$$\mathrm{ggT}(a, b) \cdot \mathrm{kgV}(a, b) = a \cdot b.$$

Sie kann mit Hilfe der *Primfaktorzerlegung* bewiesen werden.

$$\begin{aligned} a &= p_1^{k_1} p_2^{k_2} \cdots p_n^{k_n} \\ b &= p_1^{l_1} p_2^{l_2} \cdots p_n^{l_n} \end{aligned}$$

Hierbei sind die p_i Primzahlen und n das Maximum der Anzahl der Primfaktoren von a und b. Die $k_i, l_i \in \mathbb{N}_0$ geben an, wie oft der Primfaktor in a bzw. b vorkommt. D. h. das Produkt durchläuft alle Primzahlen bis p_n, und falls eine Primzahl kein Faktor sein sollte, ist sein Exponent 0. Dann ist

$$\begin{aligned} \mathrm{ggT}(a, b) &= p_1^{m_1} p_2^{m_2} \ldots p_n^{m_n} \\ \mathrm{kgV}(a, b) &= p_1^{M_1} p_2^{M_2} \ldots p_n^{M_n} \end{aligned}$$

mit $m_i = \min(k_i, l_i)$ und $M_i = \max(k_i, l_i)$. Damit ist

$$\begin{aligned} & \mathrm{ggT}(a, b) \cdot \mathrm{kgV}(a, b) = a \cdot b \\ \iff & p_1^{m_1} p_2^{m_2} \ldots p_n^{m_n} \cdot p_1^{M_1} p_2^{M_2} \ldots p_n^{M_n} = p_1^{k_1} p_2^{k_2} \ldots p_n^{k_n} \cdot p_1^{l_1} p_2^{l_2} \ldots p_n^{l_n} \\ \iff & p_1^{m_1+M_1} p_2^{m_2+M_2} \ldots p_n^{m_n+M_n} = p_1^{k_1+l_1} p_2^{k_2+l_2} \ldots p_n^{k_n+l_n}. \end{aligned}$$

Für die Addition der Minima und Maxima auf der linken Seite gibt es drei Möglichkeiten ($k_i < l_1, k_i = l_i$ und $k_i > l_i$). In jedem der drei Fälle ist $m_i + M_i = k_i + l_i$, womit der Satz bewiesen ist. □

Damit erhalten wir ein einfaches Verfahren, um das kgV zweier teilerfremder Zahlen zu berechnen: Man muss sie nur multiplizieren.

5.4 Primzahlen

Eine Zahl $a \in \mathbb{N}$, die genau zwei verschiedene positive Teiler hat, bezeichnet man als *Primzahl*. Die Menge aller Primzahlen sei $\mathbb{P}$. Eine Zahl $a \in \mathbb{N}\backslash\{1\}$, die keine Primzahl

ist, heißt *zusammengesetzt*[2]. Eine Zahl, die Teiler einer Zahl und gleichzeitig prim ist, heißt *Primteiler*.

Das Studium der Primzahlen macht einen Großteil der Zahlentheorie aus. Wir kommen später auf ein paar interessante Sätze über Primzahlen zu sprechen. Hier werden wir jedoch zunächst den *Fundamentalsatz der Arithmetik*, den *Satz von der eindeutigen Primfaktorzerlegung*, herleiten, um die Grundlage für weitere Untersuchungen (und einige vorangegangene) zu schaffen.

Zunächst stellen wir fest: Jede zusammengesetzte Zahl $a \in \mathbb{N}$ enthält einen Teiler $b \in \mathbb{N}$ mit $1 < b \leq \sqrt{a}$.
Beweis: $a = b \cdot c$, $1 < b, c < a$ und $b \leq c$
$\Rightarrow b^2 \leq bc = a \Rightarrow b \leq \sqrt{a}$ □

Wollten wir also im primitiver Weise einen *Primzahltest* auf a durchführen, so könnten wir aufhören, wenn wir bis zur *multiplikativen Mitte* $\sqrt{a}$ keinen echten Teiler gefunden haben.

Die offensichtlichste Frage über Primzahlen ist: Wie viele Primzahlen gibt es? Die bekannte Antwort: unendlich viele.
Beweis: Angenommen, es gäbe eine größte Primzahl p. Dann betrachten wir die Zahl

$$a = 2 \cdot 3 \cdot 5 \cdots p + 1.$$

Nun gibt es zwei Möglichkeiten, a ist prim oder ist es nicht. Im ersten Fall haben wir bereits einen Widerspruch. Betrachten wir daher den zweiten Fall: a ist durch keine Primzahl der Produkts teilbar, da immer ein Rest von 1 bei Division übrigbleibt. Daher muss, wenn a zusammengesetzt ist, der Primteiler größer als p sein, was auch ein Widerspruch ist. □

Außerdem zeigt dieser Beweis, dass zwei aufeinanderfolgende Zahlen keinen gemeinsamen Teiler haben können. Denn wenn sie keinen gemeinsamen Primteiler haben, dann erst recht keinen gemeinsamen zusammengesetzten Teiler.

Wenn man sich die Liste der Primzahlen anschaut, fällt auf, dass der *Primzahlabstand* immer größer wird. Tatsächlich kann der Abstand zwischen zwei Primzahlen beliebig groß werden.
Beweis: Wir betrachten die Folge

$$a! + 2, a! + 3, a! + 4, \cdots, a! + a.$$

Keine dieser Zahlen kann eine Primzahl sein, denn die erste ist durch 2 teilbar, die zweite durch 3, ... und die letzte durch a. □

[2]Dabei erhält die Zahl 1 die Sonderrolle, weder prim noch zusammengesetzt zu sein.

Jetzt werden wir uns näher mit den Eigenschaften von Primteilern beschäftigen. Dazu zeigen wir zuerst, dass jede zusammengesetzte Zahl mindestens einen Primteiler hat. Genauer: Für jede Zahl $a \geq 2$ ist ihr kleinster positiver von 1 verschiedener Teiler eine Primzahl.
Beweis: Sei $B = \{ b \in \mathbb{N} \mid b|a, b \neq 1 \}$. Wegen $a \in B$ ist B nicht leer. Da jede nichtleere Teimenge von $\mathbb{N}$ ein kleinstes Element besitzt, existiert $c = \min(B)$. Wegen $c|a$ gilt für jeden positiven Teiler d von c mit $d \neq 1$ stets $d|a$. Wegen der Minimalitätseigenschaft von c folgt $d = c$. Also ist c prim. □

Eine Zahl $p \in \mathbb{N}\backslash\{1\}$ ist genau dann eine Primzahl, wenn aus $p|(nm)$ stets $p|n$ oder $p|m$ folgt.
Beweis. Sei p prim, und es gelte $p|(nm)$. Falls $p|n$ sind wir fertig. Falls nicht $p|n$, so ist $\mathrm{ggT}(p, n) = 1$. Dann gibt es zwei Zahlen $a, b \in \mathbb{Z}$ mit $1 = ap + bn$. Daraus folgt $m = apm + bnm$. Da p beide Summanden teilt, teilt p auch m.
Andersherum sei p nicht prim, dann kann $p|(nm)$ und $p|n$ oder $p|m$ nicht für alle n, m gelten. Denn sei $p = a' \cdot b'$ mit $a', b' \in \mathbb{N}$, $0 < a', b' < p$, so gilt $p|(a'b')$, aber weder $p|a'$ noch $p|b'$. □

Wichtige Folge: Teilt eine Primzahl ein Produkt, so teilt sie mindestens einen der Faktoren.

Nun haben wir genug Rüstzeug gesammelt, um den Fundamentalsatz der Arithmetik zu beweisen. Er besagt: Jede Zahl $a \in \mathbb{N}\backslash\{1\}$ ist eindeutig in ein Produkt von Primfaktoren zerlegbar.
Beweis: Wir wissen bereits, dass a mindestens einen Primteiler hat. Diesen spalten wir ab und betrachten den Quotienten aus a und diesem Primteiler. Dieser ist entweder selbst prim oder besitzt mindestens einen Primteiler, den wir wieder abspalten usw. Es folgt die Existenz einer Zerlegung von a in Primfaktoren.
Nun beweisen wir die Eindeutigkeit: Die Zerlegung der 2 ist offensichtlich eindeutig. Nun sei die Eindeutigkeit der Zerlegung bis n bewiesen und wir betrachten den Fall $a = n+1$,

$$a = p_1 p_2 \cdots p_i.$$

Angenommen, sie wäre nicht eindeutig, dann gäbe es eine weitere Zerlegung

$$a = q_1 q_2 \cdots q_j.$$

Da p_1 nun a teilt, teilt p_1 auch das zweite Produkt und damit mindestens einen der Faktoren. Da alle diese Faktoren prim sind, ist $p_1 = q_k$ für irgendein k. Dann betrachten wir den Quotient des zweiten Produkts mit p_1 und erhalten ein Produkt mit n Faktoren, dessen Eindeutigkeit die Induktionsvoraussetzung ist. □

Dass die Eindeutigkeit der Primfaktorzerlegung keineswegs eine Selbstverständlichkeit ist, werden wir später feststellen, wenn wir andere algebraische Strukturen als $\mathbb{Z}$ untersuchen.

Normalerweise fasst man bei der Primfaktorzerlegung gleiche Primzahlen zu einer Potenz zusammen. Dann lassen sich auf einfache Weise sämtliche Teiler von a hinschreiben. Ist nämlich

$$a = p_1^{a_1} p_2^{a_2} \cdots p_i^{a_i},$$

so haben alle Teiler $b|a$ die Form

$$b = p_1^{b_1} p_2^{b_2} \cdots p_i^{b_i}$$

mit $0 \leq b_i \leq a_i$.

5.5 Teilbarkeitsregeln

Spätestens, wenn es an die Bruchrechnung geht, muss jeder Schüler gewisse Teilbarkeitsregeln lernen. Einige davon sind unmittelbar einsichtig, andere entziehen sich einem elementaren Verständnis. Daher sind hier einige Teilbarkeitsregeln und ihre Begründung aufgeführt. Der Einfachheit halber rechnen wir hier immer im *Dezimalsystem*.

5.5.1 Teilbar durch $2, 4, 5, 8, 10^n$

- Eine Zahl ist genau dann durch 2 teilbar, wenn ihre letzte Ziffer gerade oder 0 ist.
- Eine Zahl ist genau dann durch 4 teilbar, wenn ihre letzten 2 Ziffern durch 4 teilbar sind.
- Eine Zahl ist genau dann durch 5 teilbar, wenn ihre letzte Ziffer eine 0 oder eine 5 ist.
- Eine Zahl ist genau dann durch 10^n teilbar, wenn sie auf n Nullen endet.

Diese Regeln erklären sich wohl von selbst. Wenden wir uns nach diesem Vorgeplänkel nun den wirklich interessanten Fällen zu.

5.5.2 Teilbar durch $2^n, 5^n$

Eine Zahl ist genau dann durch 2^n (bzw. 5^n) teilbar, wenn ihre letzten n Ziffern durch 2^n (bzw. 5^n) teilbar sind.
Beweis: Die Zahl lässt sich darstellen als

$$\cdots + a_4 \cdot 10^4 + a_3 \cdot 10^3 + a_2 \cdot 10^2 + a_1 \cdot 10^1 + a_0 \cdot 10^0,$$

wobei die a_k Zahlen von 0 bis 9 sein können. Die Zahl $\cdots + a_n \cdot 10^n$ ist auf jeden Fall durch 2^n (bzw. 5^n) teilbar, da sich 10^n schreiben lässt als $(2 \cdot 5)^n = 2^n \cdot 5^n$. Die Teilbarkeit hängt somit nur noch von den Ziffern a_{n-1} bis a_0 ab. □

5.5.3 Teilbar durch $3, 9$

Eine Zahl ist genau dann durch 3 (bzw. 9) teilbar, wenn ihre *Quersumme* durch 3 (bzw. 9) teilbar ist.
Beweis: Machen wir zunächst eine kleine Umformung:

$$\begin{aligned} & 10^i - 1 = (10-1) \cdot (10^{i-1} + \cdots + 10 + 1) \\ \Rightarrow \quad & 10^i = 9 \cdot (10^{i-1} + \cdots + 10 + 1) + 1 = 9 \cdot b_i + 1, \end{aligned}$$

wobei b_i als Abkürzung für die Klammer fungiert. Damit können wir unsere Zahl umschreiben zu

$$\begin{aligned} & a_n \cdot 10^n + a_{n-1} \cdot 10^{n-1} + \cdots + a_1 \cdot 10 + a_0 \\ =& a_n \cdot (9 \cdot b_n + 1) + a_{n-1} \cdot (9 \cdot b_{n-1} + 1) + \cdots + a_1 \cdot (9 \cdot b_1 + 1) + a_0 \\ =& 9 \cdot (a_n \cdot b_n + a_{n-1} \cdot b_{n-1} + \cdots + a_1 \cdot b_1) + a_n + a_{n-1} + \cdots + a_0. \end{aligned}$$

Der erste Teil ist mit Sicherheit durch 3 (bzw. 9) teilbar. Die Teilbarkeit hängt somit nur noch von der Summe der Ziffern ab. □

Übrigens kann man diese Quersummentests *rekursiv* durchführen. Ist eine Quersumme immer noch zu groß, so kann man deren Quersumme bilden usw.

5.5.4 Teilbar durch 6

Eine Zahl ist genau dann durch 6 teilbar, wenn sie gerade und ihre Quersumme durch 3 teilbar ist. Der Beweis bleibt dem gewillten Leser als Übung überlassen...

5.5.5 Teilbar durch 7

Eine Zahl ist genau dann durch 7 teilbar, wenn ihre *alternierende Quersumme* durch 7 teilbar ist. Bei der Bildung der alternierenden Quersumme sind die Ziffern von rechts in 3er-Gruppen anzuordnen.
Beispiel: $123471023473 = 123.471.023.473$
alternierenden Quersumme: $473 - 23 + 471 - 123 = 798$.
$798 = 7 \cdot 114 \Rightarrow 123471023473 = 0 \bmod 7$

Beweis: Zunächst brauchen wir zwei Hilfssätze, die zunächst über vollständige Induktion bewiesen werden müssen.

Satz 1: $10^{6i} - 1 = 0 \bmod 7 \quad (i > 0)$
Induktionsanfang: $10^6 - 1 = 0 \bmod 7$ (w)
Induktionsschritt: $10^{6(i+1)} - 1 = 10^{6i} \cdot 10^6 - 1$
$= (10^{6i} - 1) \cdot (10^6 - 1) + (10^{6i} - 1) + 10^6 - 1$ □

Satz 2: $10^{6i-3}+1=0 \bmod 7 \quad (i>0)$
Induktionsanfang: $10^3+1=0 \bmod 7$ (w)
Induktionsschritt: $10^{6(i+1)-3}+1=10^{6i+3}+1=10^{6i-3}\cdot 10^6+1$
$=(10^{6i-3}+1)\cdot(10^6-1)+10^{6i-3}+1-(10^6-1)$ □

Nun zum eigentlichen Beweis. Wir schreiben unsere Zahl

$$\begin{aligned}
&\cdots a_{11}a_{10}a_9.a_8a_7a_6.a_5a_4a_3.a_2a_1a_0\\
=&10^0\cdot(a_2a_1a_0)+10^{6-3}\cdot(a_5a_4a_3)+10^6\cdot(a_8a_7a_6)+10^{12-3}\cdot(a_{11}a_{10}a_9)+\cdots\\
=&(10^0-1)\cdot(a_2a_1a_0)+(a_2a_1a_0)\\
&+(10^{6-3}+1)\cdot(a_5a_4a_3)-(a_5a_4a_3)\\
&+(10^6-1)\cdot(a_8a_7a_6)+(a_8a_7a_6)\\
&+(10^{12-3}+1)\cdot(a_{11}a_{10}a_9)-(a_{11}a_{10}a_9)+\cdots.
\end{aligned}$$ □

5.5.6 Teilbar durch 11

Eine Zahl ist genau dann teilbar durch 11, wenn ihre (echte) alternierende Quersumme durch 11 teilbar ist.
Beispiel: 1353
alternierende Quersumme: $3-5+3-1=0 \Rightarrow 1353=0 \bmod 11$
Beweis: Zum Beweis zunächst wieder zwei Hilfssätze:

Satz 1: $10^{2i+1}+1=0 \bmod 11$
Indukionssanfang: $10^1+1=0 \bmod 11$ (w)
Induktionsschritt: $10^{2(i+1)+1}+1=10^{2i+3}+1=10^{2i+1}\cdot 100+1$
$=(10^{2i+1}+1)\cdot 100-100+1=(10^{2i+1}+1)\cdot 100-99$ □

Satz 2: $10^{2i}-1=0 \bmod 11$
Induktionssanfang: $10^2-1=0 \bmod 11$ (w)
Induktionsschritt: $10^{2(i+1)}-1=10^{2i+2}-1=10^{2i}\cdot 100-1$
$=(10^{2i}-1)\cdot 100+100-1=(10^{2i}-1)\cdot 100+99$ □

Wir können also schreiben

$$\begin{aligned}
10^{2i+1}=&11\cdot b_{2i+1}-1\\
10^{2i}=&11\cdot b_{2i}+1,
\end{aligned}$$

wobei die b_k lediglich eine Abkürzung für die Teiler mit 11 sind.

Nun zum Beweis der Teilbarkeitsregel:

$$a_n\cdot 10^n+a_{n-1}\cdot 10^{n-1}+\cdots+a_1\cdot 10+a_0$$

Es sei n gerade (der Beweis für n ungerade verläuft analog). Dann kann man schreiben

$$\begin{aligned}
&a_{2k}\cdot 10^{2k}+a_{2k-1}\cdot 10^{2k-1}+\cdots+a_1\cdot 10+a_0\\
=&a_{2k}\cdot(11\cdot b_{2k}+1)+a_{2k-1}\cdot(11\cdot b_{2k+1}-1)+\cdots+a_1(11\cdots b_1-1)+a_0\\
=&11\cdot(a_{2k}\cdot b_{2k}+a_{2k-1}\cdot b_{2k+1}+\cdots+a_1\cdot b_1)+a_{2k}-a_{2k-1}+\cdots-a_1+a_0.
\end{aligned}$$ □

5.5.7 Teilbar durch 13

Eine Zahl ist genau dann durch 13 teilbar, wenn ihre alternierende Quersumme (aus 3er-Gruppen) durch 13 teilbar ist. Das Verfahren ist also identisch mit dem Testen der Teilbarkeit durch 7.
Beweis: Zum Beweis brauchen wir nur die Hilfssätze umzuformulieren, denn der eigentliche Beweis bleibt ja gleich.

Satz 1: $10^{6i} - 1 = 0 \bmod 13 \quad (i > 0)$
Induktionsanfang: $10^6 - 1 = 0 \bmod 13$ (w)
Induktionsschritt: $10^{6(i+1)} - 1 = 10^{6i} \cdot 10^6 - 1$
$= (10^{6i} - 1) \cdot (10^6 - 1) + (10^{6i} - 1) + 10^6 - 1$ □

Satz 2: $10^{6i-3} + 1 = 0 \bmod 13 \quad (i > 0)$
Induktionsanfang: $10^3 + 1 = 0 \bmod 13$ (w)
Induktionsschritt: $10^{6(i+1)-3} + 1 = 10^{6i+3} + 1 = 10^{6i-3} \cdot 10^6 + 1$
$= (10^{6i-3} + 1) \cdot (10^6 - 1) + 10^{6i-3} + 1 - (10^6 - 1)$ □

5.5.8 Teilbarkeitsregeln in Aktion

- Problem 1: Eine Zahl besteht aus 81 Einsen. Zeige, dass sie durch 81 teilbar ist!
- Problem 2: Bei der Zahl $21! = 5109094x171709440000$ ist die Ziffer x verlorengangen. Finde x!
- Lösung zu Problem 1:

$$\begin{aligned} x =& 111 \cdots 111 \quad (81 \text{ Einsen}) \\ =& 10^{80} + 10^{79} + \cdots + 10^1 + 1 \\ =& (10^{80} - 1 + 1) + (10^{79} - 1 + 1) + \cdots + (10^1 - 1 + 1) + (1 - 1 + 1) \end{aligned}$$

  $10^{80} - 1$ ist eine Zahl, die aus 80 Neunen besteht, $10^{79} - 1$ besteht aus 79 Neunen usw. 9 wird faktorisiert:

$$x = 9 \cdot (11 \cdots 11 + 11 \cdots 11 + \cdots + 111 + 11 + 1) + 81$$

  Es reicht nun aus zu zeigen, dass die Zahl in der Klammer durch 9 teilbar ist: Quersumme der Klammer:

$$80 + 79 + \cdots + 3 + 2 + 1 = \frac{81 \cdot 80}{2}$$ □

- Lösung zu Problem 2: Zu Eigenschaften der *Fakultät* siehe den entsprechenden Artikel.

$$21! = 1 \cdot 2 \cdot 3 \cdots 20 \cdot 21$$

  Da $6! = 1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 \cdot 6$ ist jede Fakultät $n!$ mit $n > 5$ durch 9 teilbar, also auch 21!. Summe der obigen Ziffern ist 61. Daraus folgt $x = 2$. □

5.5.9 Aufgaben

1. Zeige, dass $1010101\cdots0101$ (81 Einsen und 80 Nullen) durch 81 teilbar ist!
2. Sei x eine Zahl, die aus 81 Einsen und n Nullen ($n \geq 0$) zwischen jedem Paar Einsen besteht. Zeige, dass x durch 81 teilbar ist!
3. Welche Ziffern der untersuchten Zahl 21! hätten mit dem oben angegebenen Verfahren nicht wiederhergestellt werden können?

6 Moduloarithmetik

Die *Moduloarithmetik* ist für die elementare Zahlentheorie eines der wichtigsten Hilfsmittel. Ihre Prinzipien sind für das Verständnis der folgenden Seiten wesentlich. Außerdem ermöglicht es die Moduloarithmetik in einfacher Weise, die Konstruktion algebraischer Strukturen aufzuzeigen, die uns zunächst merkwürdig erscheinen. Dabei werden sich die abstrakten Rechnungen als höchst nützlich herausstellen.

6.1 Restklassen

Wir haben die Schreibweise $a = r \bmod b$ schon verwendet. Dabei bezeichnete r den Rest, der bei der Division von a durch b bleibt. Man sagt auch, *a ist kongruent zu r modulo b.* Wir betrachten nun einige Besonderheiten, die auftreten, wenn der Divisor eine Primzahl ist.

Ist $p \in \mathbb{P}$ und $a, b \in \mathbb{Z}$, so ist der Rest von $(a + b) \bmod p$ gleich der Summe der Reste von $a \bmod p$ und $b \bmod p$.

Beweis: $a = cp + r_a$, $b = dp + r_b$ mit $0 \leq r_a + r_b$

$$a + b = (cp + r_a) + (dp + r_b) = (c + d)p + r_a + r_b$$

Falls $r_a + r_b < p$, so sind wir fertig. Sonst ist

$$a + b = (c + d + 1)p + (r_a + r_b - p) \text{ mit } 0 \leq r_a + r_b - p < p.$$

Im ersten Fall ist $(a + b) = (r_a + r_b) \bmod p$, im zweiten Fall auch:

$$(a + b) = (r_a + r_b - p) \bmod p = (r_a + r_b) \bmod p.$$

Also gilt allgemein

$$(a + b) = (a \bmod p + b \bmod p) \bmod p. \qquad \square$$

Ist $p \in \mathbb{P}$ und $a, b \in \mathbb{Z}$, so ist der Rest von $(a \cdot b) \bmod p$ gleich dem Produkt der Reste von $a \bmod p$ und $b \bmod p$.

Beweis:

$$(a \cdot b) = (cp + r_a) \cdot (dp + r_b) = (dc)p^2 + (r_a d + r_b c)p + r_a r_b$$

Da die ersten beiden Summanden durch p teilbar sind, ist $(a \cdot b) \bmod p$ durch $r_a r_b$ gegeben:

$$(a \cdot b) = (a \bmod p) \cdot (b \bmod p) \bmod p. \qquad \square$$

Diese beiden Ergebnisse führen uns dazu, uns die Reste der ganzen Zahlen $\bmod p$ genauer anzusehen. Wir definieren: Sei $p \in \mathbb{P}$ und $k \in \mathbb{N}_0$ mit $0 \leq k < p$. Dann heißt die Menge aller ganzen Zahlen, die bei Division durch p den Rest k haben, die *Restklasse* k *modulo* p und schreiben

$$C_k^p = \{\, a \in \mathbb{Z} \mid a = k \bmod p \,\}.$$

Für jede Primzahl p gibt es genau p Restklassen, und jede ganze Zahl $a \in \mathbb{Z}$ liegt in genau einer Restklasse $\bmod p$. Diese eindeutig bestimmte Restklasse, die a enthält, wird mit $[a]_p$ bezeichnet. Ist $b \in [a]_p$, so heißt a auch *Repräsentant* von b. Die Menge der Restklassen $\{\, [a]_p \mid a \in \mathbb{Z} \,\}$ wird mit $\mathbb{Z}/p\mathbb{Z}$ oder $\mathbb{Z}_p$ bezeichnet.

Wir untersuchen nun, welche Eigenschaften zwei Zahlen $a, b \in \mathbb{Z}$ haben, die in derselben Restklasse liegen.
Ist a Repräsentant von b, so ist p Teiler von $a - b$.

Beweis: $a = cp + r$, $b = dp + r$

$$a - b = cp + r - (dp - r) = cp - dp = (c - d)p \qquad \square$$

Ist $b \in [a]_p$, so ist $a \in [b]_p$.

Beweis:

$$b \in [a]_p \iff a - b = 0 \bmod p \iff a \in [b]_p \qquad \square$$

6.2 Rechenregeln für Restklassen

Restklassen sind Mengen, und mit Mengen lässt sich bekanntlich nicht wie mit Zahlen rechnen. Man kann aber ihre Elemente, die ganzen Zahlen, dazu benutzen, Rechenregeln für Restklassen zu definieren.

6.2.1 Addition

Sind $a, b \in [0]_p$, so ist auch $a + b \in [0]_p$.

Beweis: $a = cp$, $b = dp$

$$a + b = cp + dp = (c + d)p \qquad \square$$

Die Restklasse $[a' + b']_p$ ist unabhängig von der Wahl von $a' \in [a]_p$ und $b' \in [b]_p$ eindeutig bestimmt.

Beweis: Seien $a', a'' \in [a]_p$ und $b', b'' \in [b]_p$. Dann soll gelten

$$[a' + b']_p = [a'' + b'']_p.$$

Das gilt genau dann, wenn

$$(a' + b') - (a'' + b'') = 0 \bmod p \iff (a' - a'') + (b' - b'') = 0 \bmod p.$$

Da a', a'' bzw. b', b'' in derselben Restklasse liegen, liegt ihre Differenz in $[0]_p$. Da also beide Summanden in $[0]_p$ liegen, liegt auch ihre Summe in $[0]_p$. $\square$

Wir wissen nun also, dass eine Operation auf Restklassen möglich ist, die der Addition zweier ganzer Zahlen analog ist. Das Ergebnis dieser Addition ist unabhängig von der Wahl der Elemente der Restklassen, die man benötigt, um die Operation anzugeben. Somit können wir die *Summe von Restklassen* definieren als

$$[a]_p + [b]_p = [a + b]_p.$$

Obwohl diese Addition von Restklassen prinzipiell nicht mit der Addition von Zahlen verglichen werden kann, so erhalten wir doch uns vertraute Gesetze:

- Assoziativgesetz: $([a]_p + [b]_p) + [c]_p = [a]_p + ([b]_p + [c]_p)$
- Kommutativgesetz: $[a]_p + [b]_p = [b]_p + [a]_p$
- Existenz des neutralen Elements: $[0]_p + [a]_p = [a]_p$
- Existenz des inversen Elements: $[a]_p + [p - a]_p = [0]_p$

Diese Gesetze folgen direkt aus der Tatsache, dass die Addition von Restklassen durch die Addition ihrer Elemente, den ganzen Zahlen, definiert ist, für die diese Gesetze gelten.

6.2.2 Multiplikation

Sind $a \in [1]_p$ und $b \in [k]_p$, so ist $a \cdot b \in [k]_p$.

Beweis: $a = cp + 1$, $b = dp + k$

$$a \cdot b = (cp + 1) \cdot (dp + k) = (cd)p^2 + (ck + d)p + k$$

Da die ersten beiden Summanden durch p teilbar sind, folgt $a \cdot b = k \bmod p$. □

Die Restklasse $[a' \cdot b']_p$ ist unabhängig von der Wahl von $a' \in [a]_p$ und $b' \in [b]_p$ eindeutig definiert.

Beweis: Seien $a', a'' \in [a]_p$ und $b', b'' \in [b]_p$. Dann muss gelten:

$$[a' \cdot b']_p = [a'' \cdot b'']_p$$

Also: $a'b' - a''b'' = 0 \bmod p$:

$$a'b' - a''b'' = a'b' - a'b'' + a'b'' - a''b'' = a'(b' - b'') + b''(a' - a'') \bmod p$$

Da $p|(b' - b'')$ und $p|(a' - a'')$ ist die Summe in $[0]_p$. □

Jetzt können wir ähnlich wie oben bei der Addition zweier Restklassen definieren, was das *Produkt zweier Restkassen* sein soll:

$$[a]_p \cdot [b]_p = [a \cdot b]_p.$$

Aus den gleichen Gründen wie oben finden wir auch hier die uns vertrauten Regeln:

- Assoziativgesetz: $([a]_p \cdot [b]_p) \cdot [c]_p = [a]_p \cdot ([b]_p \cdot [c]_p)$
- Kommutativgesetz: $[a]_p \cdot [b]_p = [b]_p \cdot [a]_p$
- Existenz des neutralen Elements: $[a]_p \cdot [1]_p = [a]_p$
- Distributivgesetz: $[a]_p \cdot ([b]_p + [c]_p) = [a]_p \cdot [b]_p + [a]_p \cdot [c]_p$

Die einzige Schwierigkeit bereitet die Existenz des multiplikativ inversen Elements. Sie kann folgendermaßen behoben werden:

Sei $p \in \mathbb{P}$ mit $1 < k < p$, dann ist $\mathrm{ggT}(k, p) = 1$ bzw. es existieren $a, b \in \mathbb{Z}$ mit $ak + bp = 1$. Dabei muss entweder $a < 0$ und $b > 0$ gelten oder $a > 0$ und $b < 0$.

$$a < 0 : ak = -1 \bmod p \Rightarrow (ak)^2 = 1 \bmod p \Rightarrow [a^2 k]_p \cdot [k]_p = [1]_p$$
$$a > 0 : ak = 1 \bmod p \Rightarrow [a]_p \cdot [k]_p = [1]_p \qquad \square$$

Da sich für jedes k stets ein $a < 0$ und ein $a > 0$ finden lässt, ist es nur eine Frage der Konvention, das multiplikativ inverse Element auch eindeutig zu machen.

6.2.3 Anmerkungen

Da $a = a + p \bmod p$ genügt es, sich für die Zwecke der Restklassenarithmetik auf die a mit $0 \leq a < p$ zu beschränken. Man sagt, sie bilden ein vollständiges *Repräsentantensystem*.

Restklassen lassen sich nicht nur für Primzahlen definieren, sondern für beliebige ganze Zahlen p. Falls p aber zusammengesetzt ist, existieren sog. *Nullteiler*, d. h. Reste, deren Produkt 0 modulo p ist, von denen selbst aber keiner 0 ist.
Genauer: a ist Nullteiler genau dann, wenn $a \cdot b = 0 \bmod p$ und $0 < a,\ b < p$.
Beispiel: $2 \cdot 3 = 0 \bmod 6$ aber $2 \neq 0 \bmod 6$ und $3 \neq 0 \bmod 6$
Ist p eine Primzahl, so können keine Nullteiler auftreten.

Beweis: Es sei $a \cdot b = 0 \bmod p$ mit p prim, $0 \leq a, b < p$.
$p|(a \cdot b) \Rightarrow p|a$ oder $p|b$.
Dann muss gelten $a = 0$ oder $b = 0$. $\square$

Da wir uns auf $0 \leq a < p$ beschränkt haben, sind die Vielfachen von p keine Nullteiler, und es ist ja auch $[p]_p = [0]_p$, d. h. $p = 0 \bmod p$. Mehr über Nullteiler werden wir später erfahren.

Ein weiterer Grund, warum wir hier nur Restklassen für $p \in \mathbb{P}$ betrachten ist der, dass nur dann eine Division definierbar ist. (Voraussetzung ist auf jeden Fall, dass wir nur unser Repräsentantensystem betrachten.)
Beispiel:

$$[3]_6 \cdot [1]_6 = [3]_6 \cdot [3]_6 = [3]_6$$
$$[3]_6 \cdot [0]_6 = [3]_6 \cdot [2]_6 = [3]_6 \cdot [4]_6 = [0]_6$$

$[3]_6/[3]_6$ ist also nicht eindeutig $[1]_6$, wie wir es erwarten würden. Bei Primzahlen kann dieses Problem nicht auftreten, da (wie wir gleich sehen werden) in jeder Zeile einer Multiplikationstabelle ein Rest nur einmal vorkommen kann.

6.3 Multiplikationstabellen

Nun werfen wir einen Blick auf die folgende Tabelle. Sie ist eine Multiplikationstabelle modulo 23, wobei der Eintrag in der a-ten Spalte, b-ten Zeile $a \cdot b \bmod 23$ entspricht.

0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	0
0	2	4	6	8	10	12	14	16	18	20	22	1	3	5	7	9	11	13	15	17	19	21	0
0	3	6	9	12	15	18	21	1	4	7	10	13	16	19	22	2	5	8	11	14	17	20	0
0	4	8	12	16	20	1	5	9	13	17	21	2	6	10	14	18	22	3	7	11	15	19	0
0	5	10	15	20	2	7	12	17	22	4	9	14	19	1	6	11	16	21	3	8	13	18	0
0	6	12	18	1	7	13	19	2	8	14	20	3	9	15	21	4	10	16	22	5	11	17	0
0	7	14	21	5	12	19	3	10	17	1	8	15	22	6	13	20	4	11	18	2	9	16	0
0	8	16	1	9	17	2	10	18	3	11	19	4	12	20	5	13	21	6	14	22	7	15	0
0	9	18	4	13	22	8	17	3	12	21	7	16	2	11	20	6	15	1	10	19	5	14	0
0	10	20	7	17	4	14	1	11	21	8	18	5	15	2	12	22	9	19	6	16	3	13	0
0	11	22	10	21	9	20	8	19	7	18	6	17	5	16	4	15	3	14	2	13	1	12	0
0	12	1	13	2	14	3	15	4	16	5	17	6	18	7	19	8	20	9	21	10	22	11	0
0	13	3	16	6	19	9	22	12	2	15	5	18	8	21	11	1	14	4	17	7	20	10	0
0	14	5	19	10	1	15	6	20	11	2	16	7	21	12	3	17	8	22	13	4	18	9	0
0	15	7	22	14	6	21	13	5	20	12	4	19	11	3	18	10	2	17	9	1	16	8	0
0	16	9	2	18	11	4	20	13	6	22	15	8	1	17	10	3	19	12	5	21	14	7	0
0	17	11	5	22	16	10	4	21	15	9	3	20	14	8	2	19	13	7	1	18	12	6	0
0	18	13	8	3	21	16	11	6	1	19	14	9	4	22	17	12	7	2	20	15	10	5	0
0	19	15	11	7	3	22	18	14	10	6	2	21	17	13	9	5	1	20	16	12	8	4	0
0	20	17	14	11	8	5	2	22	19	16	13	10	7	4	1	21	18	15	12	9	6	3	0
0	21	19	17	15	13	11	9	7	5	3	1	22	20	18	16	14	12	10	8	6	4	2	0
0	22	21	20	19	18	17	16	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	0
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0

Die Variablen laufen also von 0 bis 23, dabei ist die vertikale Achse umgedreht. Unter den Diagonalen verstehen wir die Einträge (a, a) und $(a, p-a)$. Offenbar gibt es in dieser Tabelle Muster, die wir nun zu erklären versuchen. Obwohl wir hier nur die Tabelle für $p = 23$ betrachten, gilt das ab jetzt Gesagte für beliebiges (primes) p.

Zunächst einmal stellen wir fest, dass der Tabelleneintrag mit den Koordinaten $(a, b) = a \cdot b \bmod p$ oder anders formuliert der Repräsentant $k \in [a \cdot b]_p$ mit $0 \leq k < p$ ist. Wir können also unsere neu gewonnene Restklassenarithmetik anwenden.

In der obigen Tabelle gibt es zwei Sorten von Mustern: 1. Spiegelsymmetrien an den Diagonalen und 2. kreisförmige Muster um den Mittelpunkt. Zuerst zu den Spiegelsymmetrien: Wir wissen, dass die Restklassenmultiplikation kommutativ ist. Daher ist $(a, b) = (b, a)$, was die Symmetrie zu der Diagonalen von links oben nach rechts unten erklärt. Die Symmetrie entlang der anderen Geraden besagt, dass $(a, b) = (p - a, p - b)$ ist. Das bestätigt die Rechnung:

$$[p - a]_p \cdot [p - b]_p = [p^2 - (a + b)p + ab]_p = [ab]_p.$$

Beide Symmetrien zusammen besorgen noch die Beziehung $(a, b) = (p - b, p - a)$. So ist also der Eintrag $[ab]_p$ an insgesamt vier Stellen in der Tabelle zu finden.

Nun zu den Kreismustern: Diese Muster entstehen dadurch, dass sich die einstelligen Tabelleneinträge von den zweistelligen optisch abheben. Diese Muster sind in den Multiplikationstabellen um so besser zu erkennen, je größer p ist. Hier ist p noch relativ klein,

daher sind die genauen Kurven schwer auszumachen. Der erste Kreisbogen taucht dann auf, wenn die Ergebnisse der Multiplikation erstmals zweistellig werden. Daher bezeichnet $ab = 10$ den ersten Bogen. Das ist die Gleichung einer Hyperbel! Wie haben es also keineswegs mit Kreisen zu tun. Der zweite Bogen entsteht, wenn die Produkte wieder einstellig werden, also bei $ab = p$. Die nächsten Bögen sind entsprechend $ab = p+10$ und $ab = 2p$. Aus den Spiegelsymmetrien folgt, dass auch für die anderen drei Ecken ähnliche Überlegungen gelten. Daher erscheinen die Hyperbelbögen als Kreise. Es ist interessant herauszufinden, wieviele Hyperbeln das Bild enthält.

Nun schauen wir uns die Zeilen und Spalten einzeln an. Da p prim ist, sind sämtliche Restklassen nullteilerfrei, daher befinden sich die Nullen in der Tabelle genau an den Stellen, an denen einer der Faktoren 0 oder p ist, also an den Rändern. Darüberhinaus sind alle Zeilen (Spalten), die einem $b > 0$ ($a > 0$) entsprechen, das zu p teilerfremd ist (in unserem Beispiel sind das alle), Permutationen der ersten Zeile (Spalte). (Beachte: Die Nummerierung beginnt mit Null.) Dazu reicht es zu zeigen, dass jeder Rest nur einmal pro Zeile (Spalte) auftreten kann.

Beweis: Sei b teilerfremd zu p und $a_1, a_2 \in \mathbb{N}_0$ mit $0 \leq a_1, a_2 < p$ und $a_1 > a_2$.
Angenommen, es sei

$$ba_1 = ba_2 \bmod p \Rightarrow b(a_1 - a_2) = 0 \bmod p \Rightarrow a_1 - a_2 = 0 \bmod p.$$

Also ist eine Zahl $0 < a_1 - a_2 < p$ teilbar durch p. Widerspruch! □

Eine besondere Zeile (Spalte) ist offenbar die erste, denn dort tauchen alle Zahlen a mit $0 \leq a < p$ der Reihe nach auf. Das ist auch klar: $b \cdot 1 = b \bmod p$ für alle b.

6.4 Anwendungen

Wir kommen nun zur ersten „richtigen“ Anwendung der Moduloarithmetik (abgesehen von den Teilbarkeitsregeln). Es handelt sich um die wohlbekannte *Neunerprobe*. Sie funktioniert folgendermaßen: Führt man eine Operation (Addition oder Multiplikation) auf zwei Zahlen durch, so muss die gleiche Operation folgendermaßen auf die Neunerreste angewendet werden:
Beispiel: $12345 + 98765 = 111110$
Probe:
$(12345 \bmod 9 + 98765 \bmod 9) \bmod 9 = (6 + 8) \bmod 9 = 14 \bmod 9 = 5 = 111110 \bmod 9$
Beispiel: $12345 \cdot 98765 = 1219253925$
Probe:
$(12345 \bmod 9 \cdot 98765 \bmod 9) \bmod 9 = (6 \cdot 8) \bmod 9 = 48 \bmod 9 = 3 = 1219253925 \bmod 9$
So lassen sich Fehler relativ leicht feststellen. Allerdings kann man so nicht alle Fehler aufdecken (nämlich genau die nicht, die das Ergebnis um ein Vielfaches von 9 ändern).

Wenn nun a in $[a]_9$ liegt und b in $[b]_9$, so muss $a + b \in [a + b]_9$ und $a \cdot b \in [a \cdot b]_9$ sein. Das ist alles, was die Neunerprobe überprüft. Dabei erleichtert es die Rechnung ernorm, dass der Rest modulo 9 genau der Quersumme entspricht ($10^k = 1 \bmod 9$):

$$a = a_0 + 10a_1 + \ldots + 10^k a_k = a_0 + a_1 + \ldots + a_k \bmod 9.$$

Als weitere einfache Anwendung der Moduloarithmetik seien die ISBNs (International Standard Book Numbers) erwähnt, mit denen seit 1969 sämtliche gedruckte Bücher versehen werden. Eine typische ISBN ist z. B. 3-499-60883-9.

Der erste Ziffernblock identifiziert dabei das Land, der zweite den Verlag, und der dritte die Buchnummer des Verlages. Die letzte Ziffer ist eine Kontrollziffer $k \in \{0; 1; \ldots; 9; X\}$, wobei X für 10 steht. Wird nun eine ISBN angegeben, so kann man folgendermaßen Tippfehler aufdecken: a_i seien die 9 Ziffern der ISBN. Dann ergibt sich die Kontrollziffer k als

$$k = a_1 + 2a_2 + 3a_3 + \ldots + 9a_9 \bmod 11.$$

Beipiel: $9 = 3 + 2 \cdot 4 + 3 \cdot 9 + 4 \cdot 9 + 5 \cdot 6 + 6 \cdot 0 + 7 \cdot 8 + 8 \cdot 8 + 9 \cdot 3 \bmod 11$
In 80% aller Buchbestellungen sind Schreibfehler Einzelfehler, d. h. nur eine Ziffer wurde falsch angegeben. Bei weiteren 10% werden zwei Ziffern miteinander vertauscht. Beide Fehlertypen können durch diese Probe aufgedeckt werden:
Einzelfehler: $a_i \mapsto a_i + e_i$

$$\Delta k = ie_i \neq 0 \bmod 11$$

Vertauschung: $a_i \leftrightarrow a_j$

$$\Delta k = ja_i + ia_j - ia_i - ja_j = (j - i)(a_i - a_j) \neq 0 \bmod 11$$

In beiden Fällen liegt eine Abweichung von der Kontrollziffer vor; die Neunerprobe hätte Vertauschungsfehler nicht aufgedeckt.

6.5 Der Chinesische Restsatz

Es gibt einen großen Unterschied zwischen der uns bekannten Arithmetik und der Restklassenarithmetik. In diesem Fall sind nämlich die Grundrechenarten gewissermaßen periodisch! Das hat zur Folge, dass man für Gleichungen, in denen nur Reste betrachtet werden, prinzipiell keine eindeutige Lösung geben kann, sondern immer unendlich viele. Ein wichtiger Satz zum Lösen von Gleichungssystemen in der Moduloarithmetik (man spricht von *Kongruenzensystemen*) ist der *Chinesische Restsatz*.

Bevor wir den allgemeinen Fall betrachten zunächst ein Beispiel. Zu lösen sei das Kongruenzensystem

$$a = 1 \bmod 4 \qquad (1)$$
$$a = 2 \bmod 5 \qquad (2)$$
$$a = 3 \bmod 6 \qquad (3)$$

Gleichung (1) ist äquivalent zu $a = 4t + 1$ ($t \in \mathbb{Z}$). Einsetzen in (2) und (3):

$$\begin{aligned} 4t + 1 &= 2 \bmod 5 \\ 4t + 1 &= 3 \bmod 6 \end{aligned}$$

$$\begin{aligned} & 4t = 1 \bmod 5 \\ \iff \quad & 4t = 2 \bmod 6 \end{aligned}$$

$$\begin{aligned} & t = 4 \bmod 5 \qquad (4) \\ \iff \quad & t = 2 \bmod 6 \qquad (5) \end{aligned}$$

Aus Gleichung (4) erhalten wir wiederum $t = 5s + 4$ ($s \in \mathbb{Z}$), eingesetzt in (5):

$$\begin{aligned} & 5s + 4 = 2 \bmod 6 \\ \iff \quad & 5s = 4 \bmod 6 \\ \iff \quad & s = 2 \bmod 6 \end{aligned}$$

also $s = 6r + 2$ ($r \in \mathbb{Z}$). Insgesamt erhalten wir damit

$$a = 4(5(6r + 2) + 4) + 1 = 120r + 57$$

$$\iff a = 57 \bmod 120$$

Alle a mit $a \in [57]_{120}$ sind somit Lösungen dieses Kongruenzensystems.

Nun zum allgemeinen Fall. Betrachten wir zuerst ein System aus zwei Gleichungen. Seien b_1, b_2 teilerfremd. Dann hat das Kongruenzensystem

$$\begin{aligned} a &= r_1 \bmod b_1 \\ a &= r_2 \bmod b_2 \end{aligned}$$

eine eindeutige Lösung modulo $b_1 b_2$.

Beweis: Existenz: $a = r_1 \bmod b_1 \iff a = kb_1 + r_1$ ($k \in \mathbb{Z}$)
Dann muss gelten $kb_1 + r_1 = r_2 \bmod b_2$. Da $\mathrm{ggT}(b_1, b_2) = 1$ gibt es $x, y \in \mathbb{Z}$ so dass $1 = xb_1 + yb_2 \iff (r_2 - r_1) - (r_2 - r_1)xb_1 = (r_2 - r_1)yb_2 \iff kb_1 = r_2 - r_1 \bmod b_2$ mit $k = x(r_2 - r_1)$
Eindeutigkeit: Seien a, a' zwei Lösungen, also

$$\begin{aligned} a' = \quad a = \quad & r_1 \bmod b_1 \\ a' = \quad a = \quad & r_2 \bmod b_2 \end{aligned}$$

$$\iff a' = a \bmod b_1 \text{ und } a' = a \bmod b_2$$

Da $\mathrm{ggT}(b_1, b_2) = 1$ folgt $a' = a \bmod b_1 b_2$. □

Wir können nun von der Lösbarkeit eines Systems mit zwei Gleichungen auf die Lösbarkeit von Systemen mit beliebig vielen Gleichungen übergehen.
Sind die $b_1, b_2, \ldots, b_k$ paarweise teilerfremd [1], so besitzt das Kongruenzenystem

$$\begin{aligned} a &= r_1 \bmod b_1 \\ a &= r_2 \bmod b_2 \\ &\cdots \\ a &= r_k \bmod b_k \end{aligned}$$

Lösungen.

Beweis: Es sei $x = b_1 b_2 \ldots b_k$ und $y_i = x/b_i$ für $i = 1, 2, \ldots, k$. Dann sind x und y_i teilerfremd (insbesondere b_i und y_i), daher gibt es ein z_i mit $y_i z_i = 1 \bmod b_i$ $(i = 1, 2, \ldots, k)$. Die Zahl $y_1 z_1 r_1 + y_2 z_2 r_2 + \cdots + y_k z_k r_k$ ist dann eine Lösung. □

Zum Schluss werden wir noch betrachten, welche Werte die Lösungen eines solchen Kongruenzensystems annehmen können.
Die Lösungen des Kongruenzensystems

$$\begin{aligned} a &= r_1 \bmod b_1 \\ a &= r_2 \bmod b_2 \\ &\cdots \\ a &= r_k \bmod b_k \end{aligned}$$

sind, falls welche existieren, eindeutig modulo $e = \mathrm{kgV}(b_1, b_2, \ldots, b_k)$.

Beweis: Sind x_1 und x_2 zwei Lösungen, so gilt $x_1 = x_2 = r_i \bmod b_i$ für alle $i = 1, 2, \ldots, k$, also $b_i | (x_1 - x_2)$. Mit $e | (x_1 - x_2)$ findet man $x_1 = x_2 \bmod e$. Ist umgekehrt x_1 eine Lösung des Kongruenzensystems und $x_2 = x_1 \bmod e$, so ist $x_1 = x_2 = r_i \bmod b_i$ für $i = 1, 2, \ldots, k$. □

Wir erhalten damit den Chinesischen Restsatz: Sind die b_i eines Kongruenzensystems paarweise teilerfremd, so existiert eine Lösung, und diese ist eindeutig modulo $\mathrm{kgV}(b_1, b_2, \ldots, b_k)$.

[1] paarweise teilerfremd bedeutet, dass $\mathrm{ggT}(b_i, b_j) = 1$ für $i \neq j$

7 Primzahltests

Hier werden wir uns, wie der Titel vermuten lässt, mit der Frage beschäftigen, wie man einer Zahl ansehen kann, ob sie prim ist oder nicht. Überraschenderweise ist es dazu nicht notwendig, einen echten Teiler anzugeben, denn es gibt einige Beziehungen, die nur für Primzahlen gelten. Diese können als einfache *Primzahltests* verwendet werden. Als direkte Anwendung wird die RSA-Verschlüsselung besprochen. Abschließend wird auf die Frage eingegangen, wie man dafür Primzahlen gewinnen kann.

7.1 Das Sieb des Eratosthenes

Das *Sieb des Eratosthenes* ist eines der ältesten (und umständlichsten) Verfahren, um Primzahlen zu bestimmen. Dazu schreibt man sich alle zu testenden Zahlen beginnend mit 2 bis n auf. Dann geht man zur ersten Zahl (2) und streicht alle Vielfachen von ihr weg. Dann geht man zur nächsten Zahl der Liste (3) und streicht wiederum alle Vielfachen weg usw. Kommt man zur Primzahl p, so dass $p^2 > n$, so kann man aufhören und sicher sein, dass alle noch verbleibenden Zahlen Primzahlen sind.

Mit Hilfe dieser Überlegung kann man leicht Sätze finden wie: Alle Primzahlen $p > 3$ sind von der Form $6n \pm 1$.

Beweis: Alle $p \in \mathbb{P}$, $p > 3$ sind ungerade. Diese wären $6n+1$, $6n+3$ und $6n+5$. Da $3|(6n+3)$, bleiben noch die anderen beiden übrig. Mit $6n+5 = 6k-1$ für $k = n+1$ folgt die Behauptung. □

Hieraus ergibt sich insbesondere, dass es nur ein *Primzahltriplett* der Form n, $n+2$, $n+4$ gibt, und zwar 3, 5 und 7.

7.2 Der Satz von Wilson

Wir benutzen im Folgenden einige Ergebnisse der Restklassenarithmetik. Zunächst zeigen wir, dass es für jedes $p \in \mathbb{P}$ genau zwei zu sich selbst inverse Restklassen gibt, nämlich $[1]_p$ und $[p-1]_p$.

Beweis: $[a]_p$ sei zu sich selbst invers, also

$$a^2 = 1 \bmod p \iff a^2 = 1 + kp \quad (k \in \mathbb{Z})$$

Das heißt aber $(a-1)(a+1) = kp$ und damit $p|(a-1)$ oder $p|(a+1)$. Wegen $1 \leq a < p$ folgt $a = 1$ oder $a = p-1$. □

Der *Satz von Wilson* besagt nun, dass eine Zahl p genau dann prim ist, wenn $(p-1)! = -1 \bmod p$.

Beweis: Der Satz ist formuliert mit Hilfe der Restklassenarithmetik äquivalent zu $[(p-1)!]_p = [p-1]_p$, ausgeschrieben

$$[1]_p[2]_p[3]_p \cdots [p-1]_p = [p-1]_p.$$

Für den Fall $p = 2$ besteht das Produkt nur aus dem Faktor $[1]_2$ wie verlangt. Sei nun p prim und ungerade. Da das Produkt $p-3$ Faktoren hat, die nicht selbstinvers sind, muss sich jeder Faktor mit einem anderen (seinem Inversen) auslöschen. Die Anzahl dieser Faktoren ist gerade, daher bleibt kein Faktor übrig. Es bleiben die beiden selbstinversen Faktoren $[1]_p$ und $[p-1]_p$. □

So schön dieser Satz auch ist, so unbrauchbar ist er auch für die Praxis, denn das Berechnen der Fakultät großer Zahlen ist sehr aufwendig.

Interessanterweise gilt für zusammengesetzte Zahlen $n > 4$, dass $(n-1)! = 0 \bmod n$.

Beweis: Sei $n = ab$ mit $a, b > 1$ und $a \neq b$. Sowohl a als auch b tauchen als Faktoren in $(n-1)!$ auf. Daher folgt $n|(n-1)!$. Falls $a = b$, dann ist $n = a^2$ und $1 < a < 2a < a^2$, falls $n > 4$. □

7.3 Der kleine Satz von Fermat

Zunächst ein paar Vorbetrachtungen. Seien $a, n \in \mathbb{N}$, $a, n \geq 2$, dann gilt:

- Ist n zusammengesetzt, so ist auch $a^n - 1$ zusammengesetzt.
  Beweis: Sei $n = cd$ mit $c, d \geq 2$. Dann ist
  $$a^{cd} - 1 = (a^d - 1)(1 + a^d + a^{2d} + \cdots + a^{(c-1)d}).$$ □

- Ist $a \geq 3$, so ist $a^n - 1$ zusammengesetzt.
  Beweis: $a \geq 3 \iff a - 1 \geq 2$, also
  $$a^n - 1 = (a-1)(1 + a + a^2 + \cdots + a^{n-1}).$$ □

- Ist a ungerade, so ist $a^n + 1$ gerade, also nicht prim.
  Beweis: Sei $a = 2k + 1$, so ist
  $$a^n + 1 = (2k+1)^n + 1 = ((2k)^n + n(2k)^{n-1} + \cdots + n(2k) + 1) + 1,$$
  also gerade. □

- Ist n keine Zweierpotenz, so ist $a^n + 1$ nicht prim.
  Beweis: Ist n keine Zweierpotenz, so hat n mindestens einen ungeraden echten Teiler, also $n = c(2k+1)$ mit $c, k \in \mathbb{N}$.
  $$a^n + 1 = a^{c(2k+1)} + 1 = (a^c + 1)(a^{c(2k)} - a^{c(2k-1)} + \cdots - a^2 + 1)$$ □

Aus den ersten beiden Sätzen ergibt sich, dass eine Zahl der Form $a^n - 1$ nur dann prim sein kann, wenn $a = 2$ und p selbst prim ist. Zahlen dieser Form heißen *Mersenne'sche Zahlen*, Primzahlen dieser Form *Mersenne'sche Primzahlen*. Die letzten beiden Sätze führen zur Definition der *Fermat'schen Zahlen* $2^{2^n} + 1$. Primzahlen dieser Form heißen *Fermat'sche Primzahlen*. Man beachte, dass in beiden Fällen die Form notwendig, aber keineswegs hinreichend ist!

Ein wichtiger Satz über Potenzen ist der *kleine Satz von Fermat*: Sei $p \in \mathbb{P}$ und a kein Vielfaches von p. Dann gilt $a^{p-1} = 1 \bmod p$.

Beweis:

$$[(p-1)!]_p = [1]_p[2]_p[3]_p \dots [p-1]_p$$

Da $\mathrm{ggT}(a, p) = 1$ ist, folgt die Gleichheit zu

$$[a]_p[2a]_p[3a]_p \cdots [(p-1)a]_p = [a^{p-1}(p-1)!]_p.$$

Division durch $[(p-1)!]_p \neq [0]_p$ gibt die Behauptung. □

Der Satz von Fermat gibt im Gegensatz zum Satz von Wilson kein hinreichendes Kriterium für Primheit. Daher gibt es p, die keine Primzahlen sind, aber dennoch $a^{p-1} = 1 \bmod p$ erfüllen. Diese Zahlen sind relativ selten und heißen *pseudoprim zur Basis a* oder *Carmichael-Zahlen*.

7.4 Der Satz von Euler

Dieser Satz ist zwar eigentlich kein Primzahltest, aufgrund der Verwandtschaft zu Fermats kleinem Satz sei er hier jedoch trotzdem aufgeführt. Außerdem wird jetzt eine wichtige zahlentheoretische Funktion eingeführt.

Die *Euler'sche φ-Funktion* gibt die Anzahl der zu n teilerfremden Zahlen kleiner gleich n an, also die Anzahl der Elemente der Menge $\{\, 1 \leq a \leq n \mid \mathrm{ggT}(a, n) = 1 \,\}$. Wir werden jetzt ein paar Eigenschaften dieser Funktion untersuchen.

Zunächst stellen wir fest, dass für $p \in \mathbb{P}$ gilt $\varphi(p) = p - 1$. Darüberhinaus ist

$$\varphi(p^n) = p^n - p^{n-1} = p^{n-1}(p-1) = p^n \left(1 - \frac{1}{p}\right).$$

Beweis: Teiler von p^n sind genau die Vielfachen von p kleiner als p^n. Davon gibt es p^{n-1} Stück. Zieht man diese von der Gesamtheit der Zahlen kleiner gleich p^n ab, so ergibt sich die Behauptung. □

Seien m, n zwei teilerfremde Zahlen. Dann gilt $\varphi(m \cdot n) = \varphi(m) \cdot \varphi(n)$.
Beweis: Es gilt zu zeigen, dass alle zu $m \cdot n$ teilerfremden Zahlen umkehrbar eindeutig auf zu m und n teilerfremde Zahlen abgebildet werden können. Sei ein a mit $1 \leq a \leq m \cdot n$

teilerfremd zu $m \cdot n$. Ferner seien r_1 und r_2 die Reste bei der Division von a durch m bzw. n:

$$a = r_1 \bmod m$$
$$a = r_2 \bmod n$$

Es gilt $\mathrm{ggT}(r_1, m) = 1$ und $\mathrm{ggT}(r_2, n) = 1$. Sowohl r_1 als auch r_2 sind durch a eindeutig bestimmt. Umgekehrt seien r_1 und r_2 gegeben. Laut Chinesischem Restsatz gibt es dann ein eindeutig bestimmtes a, das das Gleichungssystem erfüllt. □

Wir haben damit eine Möglichkeit, $\varphi(n)$ über die Primfaktorzerlegung von n zu berechnen:
Sei $n = p_1^{n_1} p_2^{n_2} \cdots p_k^{n_k}$, dann ist

$$\varphi(n) = n \left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right) \cdots \left(1 - \frac{1}{p_k}\right).$$

Beweis:

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

□

Nun kommen wir zum *Satz von Euler*. Er kann aufgrund des bis hierher Gesagten als Verallgemeinerung des kleinen Satzes von Fermat gesehen werden (denn für primes p ist $\varphi(p) = p - 1$).

Seien a und n teilerfremd. Dann ist $a^{\varphi(n)} = 1 \bmod n$.
Beweis: Der Beweis erfolgt analog zum Beweis des Satzes von Fermat. Seien $[r_i]_n$ die Restklassen modulo n, deren Reste teilerfremd zu n sind. Dann betrachten wir das Produkt

$$[r_1]_n [r_2]_n \cdots [r_{\varphi(n)}]_n$$

Da a und n teilerfremd sind, ist dieses Produkt gleich

$$[ar_1]_n [ar_2]_n \cdots [ar_{\varphi(n)}]_n.$$

Mit anderen Worten:

$$ar_1 ar_2 \cdots ar_{\varphi(n)} = r_1 r_2 \cdots r_{\varphi(n)} \bmod n$$

$$\iff a^{\varphi(n)} = 1 \bmod n$$

□

7.5 Die RSA-Verschlüsselung

Man könnte meinen, dass die Zahlentheorie, in gewissem Sinne der „reinste“ Zweig der Mathematik, für Anwendungen „im Alltag“ so gut wie nutzlos ist. Interessanter Weise ist genau das Gegenteil der Fall. Heutzutage käme man ohne die modernen Methoden der Zahlentheorie überhaupt nicht mehr aus. Denn im Zuge der Entwicklung weltweiter Datennetze ist es immer wichtiger geworden, sensible Daten zu schützen, indem man sie *verschlüsselt*. Eines der verbreitetsten Verfahren dazu ist die *RSA-Verschlüsselung*, benannt nach den Entwicklern Rivest, Shamir und Adleman. Sie gilt als praktisch unknackbar.

Der Grund dafür ist der, dass man ein Produkt von zwei Primzahlen verwendet. Diese Primzahlen sind von enormer Größe, so dass das Faktorisieren dieses Produkts für alle gegenwärtig bekannten Algorithmen nicht in annehmbarem Zeitaufwand geleistet werden kann. Deshalb sucht man auch nach immer größeren Primzahlen.

RSA ist ein *asymmetrisches* Verfahren. Im Gegensatz zu *symmetrischen* Verfahren, wo Sender und Empfänger einen *gemeinsamen Schlüssel* haben, hat hier jeder einen *öffentlichen Schlüssel* und einen *privaten Schlüssel*. Das bedeutet, dass der Schlüssel, mit dem die Nachricht verschlüsselt wurde, mitgeliefert wird. Das ist aber nur die halbe Wahrheit: Dieser Schlüssel ist nämlich das eben erwähnte Produkt, und ohne die Kenntnis der Primzahlen ist dieser zum Entschlüsseln praktisch nutzlos. Doch das Austauschen der Schlüssel soll hier nicht weiter interessieren, wir werden das Verschlüsselungsverfahren untersuchen.

Bevor wir etwas verschlüsseln können, müssen wir erst etwas haben, dass man verschlüsseln kann. Das heißt, wir müssen sämtliche Daten in eine Zahl umwandeln, und zwar in eine ganze Zahl. Dazu gibt es prinzipiell unendlich viele Möglichkeiten: Will man z. B. reinen Text umwandeln, so kann man Zeichen für Zeichen in den ASCII-Code transformieren, man kann einen eigenen Code verwenden, man kann die Buchstaben erst gruppieren und dann transformieren usw. (Das Gruppieren soll verhindern, dass man anhand der Häufigkeitsverteilung bestimmter Buchstaben einzelne Codes „raten“ kann.) Das soll uns hier aber nicht weiter beschäftigen. Am Ende wird dann daraus z. B. durch einfaches Aneinanderhängen eine einzige Zahl gebildet.

Nehmen wir nun an, wir haben unsere Daten irgendwie transformiert und eine Zahl $x \in \mathbb{N}_0$ vorliegen. Diese soll in eine Zahl $y \in \mathbb{N}_0$ umgewandelt werden, und zwar so, dass man x aus y später wiederherstellen kann. Dazu benötigen wir zwei Primzahlen $p, q \in \mathbb{P}$, eine *Kodierzahl* $k \in \mathbb{N}$ sowie eine *Dekodierzahl* $d \in \mathbb{N}$. Und zwar wählen wir d so aus, dass

$$kd = 1 \bmod (p-1)(q-1)$$

gilt. Dabei sind p, q, d geheim, k und $m = pq$ werden mit y weitergegeben. Ein Empfänger, der p, q, d kennt, kann so ohne Probleme y wieder in x verwandeln. Kennt der Empfänger diese nicht, so hat er keine Chance. Das Verfahren funktioniert folgendermaßen:

Wir definieren die Kodierfunktion

$$K(x) = x^k \bmod m$$

und die Dekodierfunktion

$$D(y) = y^d \bmod m.$$

Dann wird $y = K(x)$ gebildet und weitergegeben. Anschließend wird $D(y)$ berechnet. Daraus kann man dann x wiedergewinnen ($(p-1)(q-1) = \varphi(m)$; $\mathrm{ggT}(x, m) = 1$):

$$\begin{aligned} D(K(x)) &= x^{kd} \bmod m \\ &= x^{l\cdot\varphi(m)+1} \bmod m \quad (l \in \mathbb{N}) \\ &= (x^{\varphi(m)})^l \cdot x \bmod m \\ &= x \bmod m \end{aligned}$$

Nun zu einem konkreten Beispiel. Wir verschlüsseln den Text

„THOMAS' MATHE-SEITEN".

Dazu konvertieren wir jedes Zeichen ins ASCII-Format und erhalten

$$84, 72, 79, 77, 65, 83, 39, 32, 77, 65, 84, 72, 69, 45, 83, 69, 73, 84, 69, 78.$$

Da diese Zahlen unnötig groß sind, „normieren" wir durch Subtraktion von 32:

$$52, 40, 47, 45, 33, 51, 7, 0, 45, 33, 52, 40, 37, 13, 51, 37, 41, 52, 37, 46$$

Als nächstes fassen wir die Buchstaben zu 2-er Gruppen zusammen:

$$(52, 40), (47, 45), (33, 51), (7, 0), (45, 33), (52, 40), (37, 13), (51, 37), (41, 52), (37, 46)$$

Dann hängen wir die Elemente der 2-er Gruppen aneinander:

$$5240, 4745, 3351, 700, 4533, 5240, 3713, 5137, 4152, 3746$$

Diese Zahlen werden jetzt einzeln verschlüsselt. Wir müssen nun darauf achten, dass m größer ist als die größte zu verschlüsselnde Zahl (ist in der Praxis natürlich immer der Fall), denn sonst liefert die Entschlüsselung einen falschen Wert. Deshalb wählen wir $p = 71$, $q = 83$. Dann ist $m = pq = 5893$ und $(p-1)(q-1) = 5740$. Jetzt müssen wir k und d so wählen, dass $kd = 1 \bmod 5740$. Für $k = 2013$ finden wir z. B. $d = 4377$.
Wir können jetzt für alle x_i den Ausdruck $K(x_i) = x_i^{2013} \bmod 5893$ bilden:

$$1942, 3748, 3383, 5174, 1946, 1942, 2354, 4478, 3221, 199$$

Das ist die Nachricht, die unser Empfänger erhalten wird. Mit seinem privaten Schlüssel kann er nun $D(y_i) = y_i^{4377} \bmod 5893$ berechnen:

$$5240, 4745, 3351, 700, 4533, 5240, 3713, 5137, 4152, 3746$$

Der Weg zurück zur Nachricht ist offensichtlich.

Übung: Auf die gleiche Weise wie oben wurde aus einem Text eine Zahlenfolge gebildet. Das Ergebnis ist

$$1516, 4379, 1615, 4061, 1347, 1447, 8555, 4883.$$

Der öffentliche Schlüssel ist $m = 8633$ und $k = 3013$. Wie lautet die Nachricht?

7.6 Der Satz von Pocklington

Es stellt sich nun natürlich die Frage, wie man auf möglichst effiziente Weise große Primzahlen, wie sie für die RSA-Verschlüsselung benötigt werden, erhalten kann. Effizient bedeutet dabei, dass die vermutlichen Primzahlen möglichst groß sein sollten, und der Aufwand, sie zu testen, möglichst klein. Ein solches Verfahren liefert der folgende Satz:

Sei $n \in \mathbb{N}$ und $s|(n-1)$ mit $s > \sqrt{n}$. Wenn es ein $a \in \mathbb{N}$ gibt, so dass $a^{n-1} = 1 \bmod n$ und $\mathrm{ggT}(a^{(n-1)/q} - 1, n) = 1$ für jeden Primteiler q von s ist, dann ist $n \in \mathbb{P}$.

Beweis: Angenommen, n sei zusammengesetzt. Dann existiert ein Primfaktor $p \leq \sqrt{n}$ von n. Sei $b = a^{(n-1)/s} \bmod n$. Dann ist

$$b^s = \left(a^{(n-1)/s}\right)^s = a^{n-1} = 1 \bmod n.$$

Daraus folgt, dass $b^s = 1 \bmod p$ ist. Für alle Primteiler q von s gilt aber $b^{s/q} \neq 1 \bmod p$, denn falls es ein solches q' mit $b^{s/q'} = 1 \bmod p$ gäbe, dann wäre p ein Teiler von

$$b^{s/q'} - 1 = a^{(n-1)/q'} - 1,$$

was der Voraussetzung $\mathrm{ggT}(a^{(n-1)/q} - 1, n) = 1$ widerspricht. Nach Fermats kleinem Satz ist nun $b^{p-1} = 1 \bmod p$. Daraus ergibt sich, dass $s|(p-1)$, was der Voraussetzung $s > \sqrt{n}$ widerspricht, denn $p \leq \sqrt{n}$. □

Die Schwierigkeit bei diesem Verfahren ist nun nicht mehr, n als Primzahl zu entlarven, sondern vielmehr ein passendes a zu finden, das $a^{n-1} = 1 \bmod n$ erfüllt und dann für dieses a $\mathrm{ggT}(a^{(n-1)/q} - 1, n) = 1$ für alle q zu testen.

8 Faktorisierungsverfahren

Im letzten Kapitel haben wir etwas über Primzahltests erfahren. Angenommen nun, wir haben verifiziert, dass eine gegebene Zahl nicht prim ist. Wie kommen wir dann an ihre Primfaktorzerlegung? Es ist eines der großen Probleme der modernen Zahlentheorie, dass man dieses simple Problem bis jetzt nur mit enormem Aufwand für große Zahlen lösen kann. Dabei genügt es offenbar, einen einzigen Faktor (nicht notwendig prim) zu finden, denn dann kann man die Faktorisierung rekursiv auf kleineren Zahlen aufbauen.

In diesem Kapitel werden einige einfache Verfahren vorgestellt. Da man über die Struktur der gegebenen Zahl i. A. nichts weiß, ist es wenig ratsam, nur ein Verfahren durchzuführen. In der Praxis wird man mehrere Verfahren parallel laufen lassen. Auf die zur Zeit effektivsten Verfahren mittels *Kettenbruchzerlegung*, *Elliptischer Kurven* (mit denen man auch Primzahltests durchführen kann) und *Quadratischen Siebverfahren* kann hier leider nicht eingegangen werden.

8.1 Probedivision

Wir gehen im Folgenden davon aus, dass n ungerade ist (sollte das nicht der Fall sein, so dividieren wir so lange durch 2, bis wir einen ungeraden Faktor erhalten). Dann kann man versuchen, ob n durch Teiler der Form

$$a_1 < a_2 < a_3 < \cdots < \sqrt{n}$$

teilbar ist. Es ist die geschickte Wahl der a_i, die dieser Verfahren erheblich effizienter macht: Als Teiler kommen nun nur noch ungerade Zahlen in Frage. Teilt man jedoch durch alle ungeraden Zahl kleiner $\sqrt{n}$, so führt man eine Reihe überflüssiger Divisionen aus. Ist n z. B. nicht durch 5 teilbar, so kann man sich die Division durch 15 schenken. Es wäre also am effektivsten, nur durch die ungeraden Primzahlen zu teilen. Dazu muss allerdings erst einmal eine Liste aller Primzahlen bis $\sqrt{n}$ generiert werden, was die Effektivität wieder senkt. Es gilt also eine Ausgewogenheit herzustellen zwischen einer einfach zu erzeugenden Liste und zu viel Redundanz.

Dieses Verfahren ist natürlich für große n mit großen Primfaktoren unbrauchbar. Es bietet sich höchstens als *Preprocessing* an, um kleinere Faktoren zu eliminieren.

8.2 Das Verfahren von Fermat

Sei $n = ab$. Dann setzen wir $x = (a + b)/2$ und $y = (a - b)/2$ (x und y sind ganzzahlig, da a und b ungerade sind). Dann kann man n nach

$$n = (x + y)(x - y) = x^2 - y^2$$

faktorisieren. Das Verfahren beginnt, indem man $x = [\sqrt{n}]$ setzt. (Wir suchen nun also Teiler in der Nähe der multiplikativen Mitte). Dann wird überprüft, ob $x^2 - n$ eine Quadratzahl ist. Wenn ja, kann man daraus a und b bestimmen. Wenn nicht, so inkrementiert man x. Man bricht ab, wenn ein Teiler gefunden wurde oder $x = (n+1)/2$ ist. Dann ist nämlich

$$\begin{aligned} & x^2 - n = y^2 \,\text{mit}\, y = (n-1)/2 \\ \Rightarrow \quad & x - y = 1 \,\text{und}\, x + y = n \\ \Rightarrow \quad & n \in \mathbb{P}. \end{aligned}$$

Der Trick hierbei ist, dass man nicht unbedingt die Wurzel ziehen muss, um festzustellen, ob k ein Quadrat ist. So kann k z. B. nur dann ein Quadrat sein, wenn $k \in [0]_8$, $k \in [1]_8$ oder $k \in [4]_8$ ist.
Beweis: Dazu betrachten wir einfach für ein k aus jeder Restklasse modulo 8, in welcher Restklasse k^2 liegt:

$$\begin{aligned} k \in [0]_8 &\Rightarrow k^2 \in [0]_8 \\ k \in [1]_8 &\Rightarrow k^2 \in [1]_8 \\ k \in [2]_8 &\Rightarrow k^2 \in [4]_8 \\ k \in [3]_8 &\Rightarrow k^2 \in [1]_8 \\ k \in [4]_8 &\Rightarrow k^2 \in [0]_8 \\ k \in [5]_8 &\Rightarrow k^2 \in [1]_8 \\ k \in [6]_8 &\Rightarrow k^2 \in [4]_8 \\ k \in [7]_8 &\Rightarrow k^2 \in [1]_8 \end{aligned}$$

□

Eine Variation dieses Verfahrens ist das folgende: Man wählt x und y so, dass $x^2 = y^2 \bmod n$ aber $x \neq \pm y \bmod n$ erfüllt ist. Dann ist $\text{ggT}(x+y, n)$ oder $\text{ggT}(x-y, n)$ ein Teiler von n.
Beweis: $n|(x^2 - y^2) \iff n|(x+y)(x-y)$. Da aber n weder $x+y$ noch $x-y$ teilt, folgt die Behauptung. □

Das Problem hierbei ist einfach, die x und y aufzuspüren.

9 Quadratzahlen

Ein wichtiger Teil der Zahlentheorie ist die Erforschung der Eigenschaften von Quadratzahlen. Das bekannteste Beispiel für eine Gleichung, in der Quadrate auftauchen, ist natürlich der *Satz des Pythagoras*, der hier eingehend untersucht wird. Als wichtiges Handwerkszeug werden die quadratischen Reste vorgestellt und als Anwendung bei den Summen aus Quadraten vorgeführt.

9.1 Vorbetrachtungen

Wir haben schon einige Eigenschaften von Quadratzahlen kennengelernt, ohne sie explizit aufzuschreiben. So impliziert die Irrationalität von $\sqrt{2}$ unmittelbar, dass der Quotient zweier Quadratzahlen niemlas 2 sein kann. Betrachtet man diesen Sachverhalt genauer, so stellt man leicht fest, dass der Quotient zweier Quadratzahlen nur wieder eine Quadratzahl sein kann (wenn er denn überhaupt eine natürliche Zahl ist).

Wir werden oft das einfache Ergebnis brauchen, dass das Quadrat einer geraden (ungeraden) Zahl wieder gerade (ungerade) ist.

Beweis: $(2n)^2 = 4n^2 = 2(2n)^2$
$(2n-1)^2 = 4n^2 - 4n + 1 = 2(2n^2 - 2n + 1) - 1$ □

Ebenso wichtig: Sind a und b teilerfremd und Quadrate, so ist auch ab ein Quadrat.

Beweis: Sei $a = p_1^{k_1} p_2^{k_2} \cdots p_m^{k_m}$ und $b = q_1^{l_1} q_2^{l_2} \cdots q_n^{l_n}$. Da a und b Quadrate sind, müssen sämtliche Primfaktoren zu einer geradzahligen Potenz erhoben sein. Wegen $\mathrm{ggT}(a,b) = 1$ ist $p_i \neq q_j$ für alle i, j. Also ist bei

$$ab = p_1^{k_1} p_2^{k_2} \cdots p_m^{k_m} q_1^{l_1} q_2^{l_2} \cdots q_n^{l_n}$$

jeder Exponent gerade. □

Über die Teiler von Quadraten lässt sich Folgendes sagen: Die Anzahl der echten Teiler von Quadratzahlen ist immer ungerade, die Anzahl der Teiler von Nicht-Quadratzahlen immer gerade.
Beweis: a habe die echten Teiler $b_0, b_1, \ldots b_k$, die mittels Index der Größe nach geordnet sind. Da $a/b_0 = b_k, a/b_1 = b_{k-1}$ oder allgemein $a/b_i = b_{k-i}$, erhält man immer $a = b_i b_{k-i}$. a ist also das Produkt der kleinsten mit dem größten Teiler, des zweitkleinsten mit dem zweitgrößten und so weiter. Es gibt nun genau dann ein b_i, so dass $b_i^2 = a$, wenn in der Mitte ein Teiler übrigbleibt, die Teileranzahl also ungerade ist. □

9.2 Quadratische Reste

Wir haben quadratische Reste schon benutzt, als wir uns das Faktorisierungsverfahren von Fermat angesehen haben. Hier wird nun die allgemeine Definition nachgeliefert:
a heißt *quadratischer Rest modulo* p genau dann, wenn a teilerfremd zu p ist und es ein x gibt mit $x^2 = a \bmod p$. Ansonsten heißt a *quadratischer Nichtrest*. Die Null ist also per Definition kein quadratischer Rest.
Beispiele:
quadratische Reste modulo 12:

x	0	1	2	3	4	5	6	7	8	9	10	11
x^2	0	1	4	9	4	1	0	1	4	9	4	1

quadratische Reste: $\{1\}$
quadratische Nichtreste: $\{0, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11\}$

quadratische Reste modulo 13:

x	0	1	2	3	4	5	6	7	8	9	10	11	12
x^2	0	1	4	9	3	12	10	10	12	3	9	4	1

quadratische Reste: $\{1, 3, 4, 9, 19, 12\}$
quadratische Nichtreste: $\{0, 2, 5, 6, 7, 8, 11\}$

Wegen $x^2 = (-x)^2$ erhält man bereits alle quadratischen Reste für $x \leq \varphi(p)/2$. Wie man sieht sind für den Fall, dass p prim ist, alle quadratischen Reste verschieden. Die Anzahl der quadratischen Reste ist also kleiner gleich $\varphi(p)/2$ für p zusammengesetzt und gleich $\varphi(p)/2$ für primes p.

Wie bereits gesehen, kann man mit Hilfe quadratischer Reste das Wurzelziehen überflüssig machen, um gewisse Zahlen als Quadrate auszuschließen. Jetzt soll noch eine andere Anwendung gezeigt werden. Und zwar kann man mit Hilfe quadratischer Reste ohne weiteres zeigen, dass die Gleichung $a^2 + b^2 = 4c + 3$ keine Lösung mit $a, b, c \in \mathbb{Z}$ hat.
Beweis: Wir betrachten die Restklasse modulo 4:

$$a^2 + b^2 = 4c + 3 \bmod 4 \iff a^2 + b^2 = 3 \bmod 4$$

a^2 und b^2 können aber nur gleich 0 oder 1 mod 4 sein, die Summe $a^2 + b^2$ demnach nur 0, 1 oder 2. Mit anderen Worten: Die Summe aus zwei quadratischen Resten modulo 4 kann niemals 3 ergeben. □

9.3 Pythagoräische Tripel

Rechtwinklige Dreiecke spielen in der Geometrie eine große Rolle. Der Satz des Pythagoras ist vielleicht der bekannteste mathematische Satz überhaupt. Daher war es schon immer interessant, solche rechtwinkligen Dreiecke zu untersuchen, bei denen die Seitenlängen ganze Zahlen sind.

$(x, y, z) \in \mathbb{N}^3$ heißt *pythagoräisches Tripel* genau dann, wenn $x^2 + y^2 = z^2$ ist. Wenn (x, y, z) ein solches Tripel ist, dann ist natürlich auch (dx, dy, dz) mit $d \in \mathbb{N}$ ein solches Tripel. Wir werden uns daher darauf beschränken, solche Tripel zu betrachten, bei denen $\mathrm{ggT}(x, y, z) = 1$ ist. Ein solches Tripel heißt *primitives pythagoräisches Tripel*. Dann sind die x, y, z aber auch paarweise teilerfremd.
Beweis: Angenommen beispielsweise, x und y hätten einen gemeinsamen Teiler größer 1. Dann hat aber wegen $x^2 + y^2 = z^2$ auch z diesen Teiler, was der Annahme widerspricht, das Tripel sei primitiv. □

Nun untersuchen wir die Paritäten. Es können nicht alle Zahlen gerade sein, denn dann wäre das Tripel nicht primitiv. Auch können wegen der paarweisen Teilerfremdheit nicht zwei Zahlen gerade sein. Es können aber auch nicht alle drei Zahlen ungerade sein. Bleibt die Möglichkeit, dass eine Zahl gerade ist und zwei ungerade sind.
Wir vermuten: x und y sind ungerade. Die Rechnung zeigt jedoch

$$z^2 = x^2 + y^2 = (2k-1)^2 + (2l-1)^2 = 4k^2 - 4k + 1 + 4l^2 - 4l + 1 = 4(k^2 + l^2 - k - l) + 2,$$

was nicht durch 4 teilbar ist. Widerspruch!
Es kann also nur x gerade und y ungerade sein oder umgekehrt. Im Folgenden bezeichne y immer die gerade Zahl. Dann ist

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

Da diese beiden Faktoren gerade sind, setzen wir $y = 2k, z - x = 2l$ und $z + x = 2m$. Aus der Primitivität des Tripels folgt, dass l und m teilerfremd und nicht beide selbst (un)gerade sind. Außerdem sieht man an der Produktdarstellung von y^2, dass l und m selbst wieder Quadrate sein müssen, also $l = p^2$ und $m = q^2$. Zusammenfassung:

$$y = 2pq, x = q^2 - p^2, z = p^2 + q^2$$

Sind umgekehrt p^2 und q^2 Quadrate verschiedener Parität mit $p < q$, dann erfüllt das obige Tripel $(q^2 - p^2, 2pq, p^2 + q^2)$ die pythagoräische Gleichung. Folge: Es gibt unendlich viele primitive pythagoräische Tripel.

Es gibt ein sehr einfaches Verfahren zu Generierung pythagoräischer Tripel: Man schreibt sätmliche Quadratzahlen und ihre Differenzen in eine Tabelle:

$$\begin{array}{ccccccccccc} 0 & & 1 & & 4 & & 9 & & 16 & & 25 & & \cdots \\ & 1 & & 3 & & 5 & & 7 & & 9 & & \cdots & \end{array}$$

In der zweiten Zeile stehen sämtliche ungeraden Zahlen. Ist eine davon ein Quadrat, also von der Form $(2k-1)^2$, so erhält man mit den beiden darüberstehenden Zahlen ein pythagoräisches Tripel:

$$\begin{array}{rcl} & (2k-1)^2 + n^2 & = (n+1)^2 \\ \iff & n^2 + 2n + 1 - n^2 & = 4k^2 - 4k + 1 \\ \iff & n & = 2k^2 - 2k \end{array}$$

Man erhält also ausgedrückt in Abhängigkeit von k:

$$(2k-1)^2 + (2k-2k)^2 = (2k^2-2k+1)^2$$

Man erkennt, dass sich für jedes ungerade x ein y und z finden lässt, so dass ein pythagoräisches Tripel gebildet wird. Diese Form findet somit alle pythagoräischen Tripel, nicht nur die primitiven.

Wir kommen nun auf die geometrische Interpretation.

$$x^2 + y^2 = z^2 \iff \left(\frac{x}{z}\right)^2 + \left(\frac{y}{z}\right)^2 = 1$$

Also entspricht jedem pythagoräischen Tripel ein *rationaler Punkt* auf dem Einheitskreis und umgekehrt (ein rationaler Punkt einer Kurve ist ein Punkt, dessen Koordinaten rational sind).
Sei $P = \{\, (x,y) \in \mathbb{Q}^2 \mid x^2+y^2 = 1, x, y > 0 \,\}$ die Menge aller rationalen Punkte auf dem Einheitskreis im 1. Quadranten. Wir betrachten die Schnittpunkte des Einheitskreises mit der Geraden $y = t(x+1)$, $0 < t < 1$ im 1. Quadranten:

$$\begin{aligned}
& 1 - x^2 && = t^2(x+1)^2 \\
\Rightarrow \quad & 1 - x^2 && = t^2x^2 + 2t^2x + t^2 \\
\Rightarrow \quad & (t^2+1)x^2 + 2t^2x + t^2 - 1 && = 0 \\
\Rightarrow \quad & x^2 + \frac{2t^2}{t^2+1}x + \frac{t^2-1}{t^2+1} && = 0
\end{aligned}$$

Die Lösung dieser Gleichung ist $x = \dfrac{1-t^2}{1+t^2}$ und damit $y = \dfrac{2t}{1+t^2}$. Für $t \in \mathbb{Q}$ ist (x,y) ein rationaler Punkt. Sei nun (x,y) ein rationaler Punkt ungleich $(-1,0)$, dann ist die Steigung t der Geraden eine rationale Zahl, $t = \dfrac{y}{x+1}$. Also ist

$$P = \left\{ \left(\frac{1-t^2}{1+t^2}, \frac{2t}{1+t^2}\right) \,\middle|\, t \in \mathbb{Q},\, 0 < t < 1 \right\}.$$

Damit haben wir eine vollständige Parametrisierung aller rationaler Punkte im 1. Quadranten, die wir durch Erweitern einem pythagoräischen Tripel zuordnen können.

9.4 Summen von Quadraten

Man kann sich nun die Frage stellen, wann eine natürliche Zahl als Summe von Quadraten darstellbar ist. Man findet z. B. leicht, dass $m \cdot n$ Summe von zwei Quadraten ist, wenn m und n selber Summe zweier Quadrate sind, denn

$$\begin{aligned}
m \cdot n =& (a^2+b^2)(c^2+d^2) \\
=& a^2c^2 + a^2d^2 + b^2c^2 + b^2d^2 \\
=& a^2c^2 + 2acbd + b^2d^2 + a^2d^2 - 2adbc + b^2c^2 \\
=& (ac+bd)^2 + (ad-bc)^2.
\end{aligned}$$

□

Auf ähnliche Weise sieht man, dass $m \cdot n$ Summe aus vier Quadraten ist, wenn m und n Summe von vier Quadraten sind.

Die folgenden Sätze können hier leider nicht bewiesen werden, da dazu ein intensiveres Studium der quadratischen Reste notwendig ist.

- $p \in \mathbb{P}$ ist genau dann Summe zweier Quadrate, wenn $p = 2$ oder $p = 1 \bmod 4$ ist.
- $n \in \mathbb{N}$ ist genau dann Summe zweier Quadrate, wenn in der Primfaktorzerlegung alle $p_i = 3 \bmod 4$ in gerader Potenz auftreten.
- Jede Zahl $n \in \mathbb{N}$ ist Summe von 4 Quadraten.

Zum Abschluss werden wir den Beweis führen, dass keine Zahl $n \in \mathbb{N}$ der Form $n = 4^a(8b + 7)$, $a, b \in \mathbb{N}_0$ als Summe von weniger als 4 Quadraten geschrieben werden kann.

Beweis: Nehmen wir das Gegenteil an, also $n = x_1^2 + x_2^2 + x_3^2$, $x_i \in \mathbb{N}_0$.

- Ist $a = 0$, so ist $8k + 7 = x_1^2 + x_2^2 + x_3^2$ ungerade. Wir unterscheiden dann:
  - alle x_i sind ungerade:
    Dann ist $x_i^2 = 1 \bmod 8$: $(2k - 1)^2 = 4k(k - 1) + 1$ und damit $x_1^2 + x_2^2 + x_3^2 = 3 \bmod 8$. Widerspruch!
  - x_1 und x_2 gerade, x_3 ungerade:
    Dann ist $x_1^2, x_2^2 = 0 \bmod 4$ und $x_3^2 = 1 \bmod 4$: $x_1^2 + x_2^2 + x_3^2 = 1 \bmod 4$. Widerspruch!
- Nun sei $a > 0$: Dann ist $x_1^2 + x_2^2 + x_3^2 = 4^a(8b + 7)$ gerade.
  - x_1 und x_2 ungerade, x_3 gerade:
    $x_1^2 + x_2^2 + x_3^2 = 2 \bmod 4$. Widerspruch!
  - Alle x_i gerade:
    Wir dividieren durch 4 und erhalten

    $$4^{a-1}(8b + 7) = \left(\frac{x_1}{2}\right)^2 + \left(\frac{x_2}{2}\right)^2 + \left(\frac{x_3}{2}\right)^2.$$

    Wiederholt man diese Division, so erhält man entweder den obigen Fall oder $a = 0$. In jedem Fall finden wir einen Widerspruch. □

10 Ein bisschen Algebra

Bis jetzt haben wir auf den sonst üblichen mathematischen Formalismus bei der Vermittlung elementarer Zahlentheorie verzichtet: den Formalismus der Algebra. Alle Ergebnisse der Zahlentheorie konnten bis jetzt ohne algebraisches Wissen verstanden und bewiesen werden. In diesem Kapitel werden wir sehen, dass die Algebra eine übergeordnete Struktur der Mathematik vorgibt, und wieso man zu Verallgemeinerungen strebt. Dabei werden wir auf algebraische Begriffe, auf die wir schon gestoßen sind, näher eingehen.

10.1 Gruppen

Eine *Gruppe* ist eine nichtleere Menge G zusammen mit einer Verknüpfung $+$, geschrieben als Paar $(G, +)$, die den folgenden Regeln genügt:

- Die Gruppe ist abgeschlossen: Sind $g_1, g_2 \in G$, so ist auch
$$g_1 + g_2 = g_3 \in G.$$
- Für je 3 Elemente $g_1, g_2, g_3 \in G$ gilt das Assoziativgesetz
$$(g_1 + g_2) + g_3 = g_1 + (g_2 + g_3).$$
- Es gibt es linksneutrales Element genannt 0, so dass für jedes $g \in G$ gilt
$$0 + g = g.$$
- Für jedes $g \in G$ gibt es ein linksinverses Element $(-g)$, so dass gilt
$$(-g) + g = 0.$$

Man beachte, dass die Menge G keineswegs eine Zahlenmenge sein muss, die Symbole $+$, $-$ und 0 sind also wirklich streng symbolisch zu sehen. Ein Beispiel für eine Gruppe, die nichts mit Zahlen zu tun hat, ist z. B. die Gruppe der Rotationen eines gleichseitigen Dreiecks um seinen Schwerpunkt. Die Addition entspricht dabei der Hintereinanderausführung von Rotationen, und die Menge enthalte die Rotationen um 0°, 120° und 240°. Das Minuszeichen bedeutet dann Drehung im negativen Drehsinn. Man überprüft leicht anhand der Bedingungen, dass es sich tatsächlich um eine Gruppe handelt.

Oft findet man in der Definition der Gruppe einfach „invers“ statt „linksinvers“ und „neutral“ statt „linksneutral“. Das liegt daran, dass in jeder algebraischen Struktur, die

den Bedingungen der Gruppe genügt, das linksinverse gleich dem rechtsinversen Element und das linksneutrale gleich dem rechtsneutralen Element ist. (Man überlege sich, dass es in einer Gruppe nur ein neutrales Element geben kann!) Das ist aber keineswegs von vornherein klar und bedarf eines Beweises, und zwar allein anhand der Eigenschaften einer Gruppe. Diese Beweise sind etwas sperrig, aber notwendig.

Beweis der ersten Aussage:

$$\begin{aligned} g + (-g) &= g + (0 + (-g)) \\ &= g + (((-g) + g) + (-g)) \\ &= g + ((-g) + (g + (-g))) \\ &= (g + (-g)) + (g + (-g)) \end{aligned}$$

Addition des Linksinversen zu $g + (-g)$:

$$\begin{aligned} 0 &= -(g + (-g)) + ((g + (-g)) + (g + (-g))) \\ &= (-(g + (-g)) + (g + (-g)) + (g + (-g)) \\ &= 0 + (g + (-g)) \\ &= g + (-g) \end{aligned}$$ □

Beweis der zweiten Aussage:

$$g + 0 = g + ((-g) + g) = (g + (-g)) + g = 0 + g$$ □

Außerdem gilt in jeder Gruppe $(-(-g)) = g$. Das folgt schon aus

$$g + (-g) = (-g) + g = 0,$$

wonach g das Inverse zu $-g$ ist. □

Diese Rechnungen sind so sperrig, weil die Kommutativität keine Eigenschaft einer Gruppe sein muss. Daher erweitern wir die Definition: Gilt für alle $g_1, g_2 \in G$ das Kommutativgesetz $g_1 + g_2 = g_2 + g_1$, so heißt die Gruppe *kommutativ* oder *abelsch*.
Beispiel: Bezüglich der Restklassenaddition ist $\mathbb{Z}/p\,\mathbb{Z}$ mit $p > 1 \in \mathbb{N}$ eine abelsche Gruppe.

Da das Pluszeichen für Gruppen rein symbolisch ist, kann man es durch ein anderes Symbol, z. B. das Malzeichen, ersetzen. Dann ändern sich die Bezeichnungen konventionsgemäß wie folgt: neutrales Element: 1, inverses Element: g^{-1}, Verknüpfung: $g_1 \cdot g_2$
Als Abkürzung der n-maligen Hintereinanderausführung der Vernküpfung mit dem gleichen Element der Menge schreibt man auch ng bzw. g^n. Man nennt eine Gruppe entsprechend ihrer Notation *additiv* bzw. *multiplikativ*.

10.2 Ringe

Nun untersuchen wir algebraische Strukturen mit mehreren Verknüpfungen. Um diese zu unterscheiden, bekommt eine Verknüpfung das feste Symbol $+$, die andere das feste Symbol $\cdot$.
Und zwar heißt das Tripel $(R, +, \cdot)$ ein *Ring*, wenn R eine Menge, $(R, +)$ eine kommutative Gruppe ist und die folgenden Bedingungen für alle $r_1, r_2, r_3 \in R$ erfüllt sind:

- Assoziativgesetz:
$$(r_1 \cdot r_2) \cdot r_3 = r_1 \cdot (r_2 \cdot r_3)$$
- Distributivgesetze:
$$\begin{aligned} r_1 \cdot (r_2 + r_3) &= r_1 \cdot r_2 + r_1 \cdot r_3 \\ (r_1 + r_2) \cdot r_3 &= r_1 \cdot r_3 + r_2 \cdot r_3 \end{aligned}$$

Die erste Verknüpfung nennen wir Addition, die zweite Multiplikation. Wir verwenden die Notationen für Gruppen. Ist die Multiplikation in R zusätzlich kommutativ, so handelt es sich um einen kommutativen Ring.

Offensichtliche Beipiele für (kommutative) Ringe sind die ganzen, rationalen, reellen, komplexen Zahlen und die sog. Restklassenringe $\mathbb{Z}/p\mathbb{Z}$. Hier zeigt sich die Nützlichkeit der Algebra: Sie bewahrt uns davor, das Rad ständig neu erfinden zu müssen. Denn haben wir z. B. einmal eine Eigenschaft von Ringen gefunden, so gilt sie überall, wo eine Ringstruktur vorhanden ist, und sie muss nicht für jeden Ring neu bewiesen werden. Darum betrachtet man in der Algebra die Dinge abstrakt, anstatt sich eine klare Vorstellung zu machen: Das bewahrt vor unnötiger Arbeit!

In jedem Ring gilt $(x, y \in R)$:

- $x \cdot 0 = 0 \cdot x = 0$
Beweis:
$$x \cdot 0 + x \cdot 0 = x \cdot (0 + 0) = x \cdot 0 = x \cdot 0 + 0 \Rightarrow x \cdot 0 = 0$$
$$0 \cdot x + 0 \cdot x = (0 + 0) \cdot x = 0 \cdot x = 0 \cdot x + 0 \Rightarrow 0 \cdot x = 0 \qquad \square$$

- $x \cdot (-y) = (-x) \cdot y = -(x \cdot y)$
Beweis:
$$x \cdot y + x \cdot (-y) = x \cdot (y + (-y)) = x \cdot 0 = 0 \Rightarrow x \cdot (-y) = -(x \cdot y)$$
$$x \cdot y + (-x) \cdot y = (x + (-x)) \cdot y = 0 \cdot y = 0 \Rightarrow (-x) \cdot y = -(x \cdot y) \qquad \square$$

- $(-x) \cdot (-y) = x \cdot y$
Beweis:
$$(-x) \cdot (-y) = -(x \cdot (-y)) = -((-x) \cdot y) = -(-(x \cdot y)) = x \cdot y \qquad \square$$

- $(-1) \cdot x = -x$
  Beweis:
  $$(-1) \cdot x = -(1 \cdot x) = -x \qquad \square$$

Wir überprüfen nun die Gültigkeit der binomischen Formeln in Ringen:

- $(x + y) \cdot (x + y) = x^2 + x \cdot y + y \cdot x + y^2$
- $(x - y) \cdot (x - y) = x^2 - x \cdot y - y \cdot x + y^2$
- $(x + y) \cdot (x - y) = x^2 - x \cdot y + y \cdot x - y^2$

Die binomischen Formeln gelten also nur dann allgemein, wenn der Ring kommutativ ist.

In Ringen gilt normalerweise nicht $x \cdot y = 0 \Rightarrow x = 0$ oder $y = 0$. Sind x und y ungleich 0 und gilt $x \cdot y = 0$, so heißen x und y *Nullteiler*.

10.3 Integritätsringe

Wir werden noch eine Weile bei den Ringen bleiben, um einige Eigenschaften der ganzen Zahlen in neuem Licht erscheinen zu lassen. So werden wir uns besonders mit der Primfaktorzerlegung in Ringen befassen und neue Zahlbereiche kennenlernen.

Man bezeichnet einen kommutativen Ring als *Integritätsring*, wenn er nullteilerfrei ist. Wir werden jetzt eine besimmte Sorte von Integritätsringen untersuchen, und zwar die Ringe

$$\mathbb{Z}[\sqrt{n}] = \{a + b\sqrt{n} \,|\, a, b \in \mathbb{Z}\}, n \in \mathbb{N}.$$

Hierbei soll n kein Quadrat sein, weil sonst $\mathbb{Z}[\sqrt{n}] = \mathbb{Z}$ wäre. Wir beschränken uns jedoch zunächst auf $n = 3$. Man überprüft leicht, dass $\mathbb{Z}[\sqrt{3}]$ sogar ein kommutativer Ring ist, mit neutralem Element der Addition 0 und neutralem Element der Multiplikation 1. Weniger offensichtlich ist, dass $\mathbb{Z}[\sqrt{3}]$ ein Integritätsring ist. Das soll nun bewiesen werden.

Zuerst aber führen wir den Begriff der *Konjugation* ein, den wir von den komplexen Zahlen her kennen. Ist $x = a + b\sqrt{3}$, so ist $\overline{x} = a - b\sqrt{3}$. Dann hat man:

- $\overline{x + y} = \overline{x} + \overline{y}$
  Beweis:
  $$\begin{aligned} \overline{(a_1 + b_1\sqrt{3}) + (a_2 + b_2\sqrt{3})} &= (a_1 + a_2) - (b_1 + b_2)\sqrt{3} \\ &= \overline{a_1 + b_1\sqrt{3}} + \overline{a_2 + b_2\sqrt{3}} \end{aligned} \qquad \square$$

- $\overline{x \cdot y} = \overline{x} \cdot \overline{y}$
  Beweis:

$$\begin{aligned}\overline{(a_1 + b_1\sqrt{3}) \cdot (a_2 + b_2\sqrt{3})} &= \overline{(a_1a_2 + 3b_1b_2) + (a_1b_2 + a_2b_1)\sqrt{3}} \\ &= (a_1a_2 + 3b_1b_2) - (a_1b_2 + a_2b_1)\sqrt{3} \\ &= \overline{a_1 + b_1\sqrt{3}} \cdot \overline{a_2 + b_2\sqrt{3}}\end{aligned}$$

□

Nun definieren wir:

$$N(x) = x \cdot \overline{x} = (a + b\sqrt{3}) \cdot (a - b\sqrt{3}) = a^2 - 3b^2.$$

Man nennt N eine *Norm*. Klarerweise ist $N(x) = N(\overline{x})$. Da der Quotient zweier Quadrate niemals 3 sein kann, ist $N(x) \neq 0$ für $x \neq 0$.

$$N(x \cdot y) = (x \cdot y) \cdot \overline{(x \cdot y)} = x \cdot y \cdot \overline{x} \cdot \overline{y} = N(x) \cdot N(y)$$

Jetzt können wir zeigen, dass $\mathbb{Z}[\sqrt{3}]$ ein Integritätsring ist, dass also für alle $x, y \in \mathbb{Z}[\sqrt{3}]$ gilt: $x \cdot y = 0 \Rightarrow x = 0$ oder $y = 0$
Beweis: Sei $x \cdot y = 0$. Dann ist auch $N(x \cdot y) = 0$, oder anders $N(x) \cdot N(y) = 0$.
$\Rightarrow N(x) = 0$ oder $N(y) = 0 \Rightarrow x = 0$ oder $y = 0$ □

Wir untersuchen nun Quadrate in $\mathbb{Z}[\sqrt{3}]$:

$$(a + b\sqrt{3})^2 = (a^2 + 3b^2) + 2ab\sqrt{3}$$

Wir werden nun allgemein die Frage beantworten, wann $c + d\sqrt{3}$ ein Quadrat in $\mathbb{Z}[\sqrt{3}]$ ist. Man erhält $c = a^2 + 3b^2$ und $d = 2ab$. Wir können nun also unsere Erkenntnisse über Moduloarithmetik und quadratische Reste anwenden. In $\mathbb{Z}[\sqrt{3}]$ kommt aber eine neue Möglichkeit hinzu: Ist $c + d\sqrt{3}$ ein Quadrat, dann muss auch $c - d\sqrt{3}$, also die Konjugation, ein Quadrat sein!

$$(a - b\sqrt{3})^2 = (a^2 + 3b^2) - 2ab\sqrt{3} = c - d\sqrt{3}$$

Wenn also $c - d\sqrt{3} < 0$ ist, kann auch $c + d\sqrt{3}$ kein Quadrat sein! Damit finden wir eine notwendige Bedingung für Quadrate in $\mathbb{Z}[\sqrt{3}]$:

$$c - d\sqrt{3} \geq 0 \iff c \geq d\sqrt{3}$$

Nun werden wir wie angekündigt die Primfaktorzerlegung in $\mathbb{Z}[\sqrt{3}]$ untersuchen. Dabei müssen wir zunächst ein paar Begriffe, die wir von den ganzen Zahlen kennen, erweitern. Seien dazu $x, y, z \in \mathbb{Z}[\sqrt{3}]$:
$x \neq 0$ teilt y genau dann, wenn es ein z gibt mit $x \cdot z = y$.
x heißt *Einheit* genau dann, wenn x jedes y teilt.
x heißt prim, wenn es nur durch sich selbst und alle Einheiten teilbar ist. Die Einheiten selbst sollen nicht als prim angesehen werden.

Hier wird es interessant, denn die Anzahl der Einheiten von $\mathbb{Z}[\sqrt{3}]$ ist unendlich!

Beweis: Zunächst stellen wir fest, dass $x = 2 + \sqrt{3}$ eine Einheit ist:

$$\frac{a + b\sqrt{3}}{2 + \sqrt{3}} = \frac{(a + b\sqrt{3}) \cdot (2 - \sqrt{3})}{4 - 3} = (2a - 3b) + (2b - a)\sqrt{3},$$

was ein Element von $\mathbb{Z}[\sqrt{3}]$ ist. Ebenso ist natürlich $\overline{x}$ eine Einheit. Wenn x aber eine Einheit ist, dann ist auch x^n mit $n \in \mathbb{N}$ eine Einheit und $\overline{x}^n$. Da $\overline{x} = 1/x$ ist, ist x^n eine Einheit für alle $n \in \mathbb{Z}$. Da darüberhinaus alle Potenzen von x verschieden sind, haben wir unendlich viele Einheiten. □

Damit wird die Eindeutigkeit der Primfaktorzerlegung natürlich auf eine harte Probe gestellt. Überhaupt stellt sich die Frage, wie man überhaupt einer Zahl aus $\mathbb{Z}[\sqrt{3}]$ ansehen kann, ob sie eine Einheit ist. Dabei sind die folgenden Sätze behilflich.

- x ist Einheit genau dann, wenn x Teiler von 1 ist.
  Beweis: Die Einheit x sollte alle Zahlen aus $\mathbb{Z}[\sqrt{3}]$ teilen, also auch 1. Umgekehrt teilt 1 alle Zahlen aus $\mathbb{Z}[\sqrt{3}]$, also teilen auch alle Teiler von 1 alle anderen Zahlen.□

- x ist genau dann eine Einheit, wenn $N(x) = \pm 1$ ist.
  Beweis: Wenn $N(x) = \pm 1$ ist, dann ist entweder $x \cdot \overline{x} = 1$ oder $x \cdot (-\overline{x}) = 1$. In beiden Fällen gibt es ein y, so dass $x \cdot y = 1$ ist.
  Umgekehrte Richtung: Angenommen, $a = |N(x)| > 1$. Sei b teilerfremd zu a. Dann gibt es ein y, so dass $x \cdot y = b$ ist und damit $a|N(y)| = b$. Also ist a ein Teiler von b, Widerspruch! □

Nun zur Primfaktorzerlegung. Zunächst einmal stellen wir fest, dass aus $N(x \cdot y) = N(x) \cdot N(y)$ folgt, dass $N(x_1 x_2 \cdots x_n) = N(x_1)N(x_2) \cdots N(x_n)$ ist. Sei nun $x \in \mathbb{Z}[\sqrt{3}]$ nicht prim. Dann kann x geschrieben werden als $x = x_1 x_2$. Wenn x_1 und x_2 prim wären, wären wir fertig. Sind sie es nicht, dann benennen wir die Variablen um und zerlegen wir weiter: $x = x_1 x_2 x_3$. Alles was wir nun zeigen müssen ist, dass dieser Prozess nicht unendlich fortgesetzt werden kann. Daher berechnen wir $N(x) = N(x_1)N(x_2) \cdots N(x_n)$. Da $N(x)$ aber nur eine endliche Anzahl von Teilern hat, kann das Produkt auf der rechten Seite auch nur aus einer endlichen Anzahl von Faktoren bestehen. An dem Punkt, an dem kein weiterer Faktor mehr abgespalten werden kann, haben wir die vollständige Primfaktorzerlegung von x gefunden.
Aus der Eindeutigkeit der Primfaktorzerlegung von $N(x)$ folgt aber unglücklicherweise nicht auch die Eindeutigkeit der Primfaktorzerlegung von x. Denn es gibt mehrere x, so dass $N(x)$ denselben Wert hat. Diese ergeben sich aber sämtlich durch Mutliplikation mit einer Einheit. Deshalb ist, wenn $N(x)$ prim ist, auch x prim.

Da die Einheiten bei der Primfaktorzerlegung keine Rolle spielen, kann eine Zahl sehr verschieden aussehende Zerlegungen haben. Erst wenn alle Einheiten beseitigt sind, kann man diese Zerlegungen sinnvoll vergleichen. Der obige Satz, dass aus $N(x)$ prim folgt, dass x prim ist, ist leider nur hinreichend, aber keineswegs notwendig.

Gegenbeispiel: $x = 5$ ist prim in $\mathbb{Z}[\sqrt{3}]$.
Beweis: $N(5) = 25$. Hat 5 also zwei Teiler $x, y \in \mathbb{Z}[\sqrt{3}]$, die keine Einheiten sind, so gilt $N(5) = N(x)N(y)$. Also ist $N(x) = \pm 5$ und $N(y) = \pm 5$. Sei $x = a + b\sqrt{3}$. Dann ist

$$N(x) = a^2 - 3b^2 = \pm 5 \Rightarrow a^2 + 2b^2 = 0 \bmod 5$$

5 ist genau dann prim, wenn diese Gleichung keine ganzzahligen Lösungen hat. Jetzt kommen wir auf die quadratischen Reste zurück: Die quadratischen Reste modulo 5 sind 1 und 4. a^2 ist also gleich 0, 1 oder 4, $2b^2$ gleich 0, 2 oder 3. Die Summe ist nur dann 0, wenn a und b gleich 0 modulo 5 sind. Also gilt

$$5|a \text{ und } 5|b \Rightarrow 25|a^2 \text{ und } 25|b^2 \Rightarrow 25|(a^2 - 3b^2) \Rightarrow 25|N(x) \Rightarrow 25|5$$

Widerspruch! □

Nicht alle Integritätsringe $\mathbb{Z}[\sqrt{n}]$ besitzen eine eindeutige Primfaktorzerlegung. Man kann zeigen, dass für negative n nur die Zahlen der Integritätsringe mit $n = -1$ und $n = -2$ eindeutig in Primfaktoren zerlegbar sind. Der Fall $n = -1$ ergibt $\mathbb{Z}[i]$, die sog. *Gauß'schen Zahlen*, die praktisch eine Erweiterung der ganzen Zahlen auf die komplexe Ebene darstellen. Zum Abschluss betrachten wir eine Struktur, in der keine eindeutige Primfaktorzerlegung möglich ist.

Und zwar betrachten wir die Menge $V = \{\, 4n + 1 \mid n \in \mathbb{N}_0 \,\}$, welche bezüglich der Multiplikation ein *kommutatives Monoid* darstellt. Die Multiplikation ist innerhalb von V abgeschlossen:

$$(4n + 1)(4m + 1) = 16nm + 4n + 4m + 1 = 4(4nm + n + m) + 1,$$

was ein Element von V ist. Die Multiplikation ist assoziativ und kommutativ, und es gibt ein neutrales Element. Das macht ein kommutatives Monoid aus. Wir zeigen an einem Beispiel, dass die Darstellung von $x \in V$ als Produkt von unzerlegbaren Elementen in V nicht eindeutig ist: $441 = 21 \cdot 21 = 9 \cdot 49$.

10.4 Körper

Ein *Körper* ist ein kommutativer Ring, indem jedes von Null verschiedene Element ein multiplikativ Inverses besitzt.
Beispiel: Für p prim ist $\mathbb{Z}/p\,\mathbb{Z}$ ein Körper. Weitere bekannte Körper sind $\mathbb{Q}$, $\mathbb{R}$ und $\mathbb{C}$.

Man kann den Gedanken von $\mathbb{Z}[\sqrt{n}]$ auf rationale Zahlen erweitern:

$$\mathbb{Q}[\sqrt{n}] = \{a + b\sqrt{n} \,|\, a, b \in \mathbb{Q}\}$$

Man kann dann zeigen, dass $\mathbb{Q}[\sqrt{n}]$ ein Körper ist, und zwar ein sog. *quadratischer Zahlkörper*. Genauer gesagt ist es der kleinste Körper, der alle rationalen Zahlen und $\sqrt{n}$

enthält. Das Einzige, was problematisch erscheint, ist der Beweis der Abgeschlossenheit von $\mathbb{Q}[\sqrt{n}]$ bezüglich der Division. Daher sei er hier geführt:

$$\begin{aligned}\frac{a_1 + b_1\sqrt{n}}{a_2 + b_2\sqrt{n}} &= \frac{(a_1 + b_1\sqrt{n}) \cdot (a_2 - b_2\sqrt{n})}{a_2^2 - b_2^2 n} \\ &= \frac{(a_1 a_2 - b_1 b_2 n) + (a_2 b_1 - a_1 b_2)\sqrt{n}}{a_2^2 - b_2^2 n}\end{aligned}$$

□

Zum Abschluss führen wir noch die *Charakteristik* ein: Das kleinste n, so dass $n \cdot 1 = 0$ ist, heißt die Charakteristik des Körpers. Existiert kein solches n, so sagt man, die Charakteristik sei unendlich. Tatsächlich ist die Charakteristik eines Körpers entweder eine Primzahl oder unendlich.

11 Bertrands Postulat

Einer der einfachsten Sätze der Zahlentheorie ist der folgende: In jedem Intervall $[n; 2n]$ befindet sich mindestens eine Primzahl. Doch wie es mit den meisten vermeintlich einfachen Sätzen so ist — sie sind nur schwer zu beweisen. So gelang es Bertrand nicht, sein nach ihm benanntes Postulat zu verifizieren. Nach ihm versuchten sich mehrere Kollegen erfolgreich, dies zu tun. Wir folgen nun einem Beweis, der lediglich elementare Rechnungen verwendet. Man sollte sich durch die Länge des Beweises nicht abschrecken lassen!

Zuerst definieren wir die Funktion

$$\vartheta(x) = \sum_{\substack{p\in\mathbb{P}:\\ 0<p\leq x}} \ln p,$$

also die Summe der natürlichen Logarithmen aller Primzahlen kleiner gleich x. Dann gilt

$$\vartheta(x) < 2x \ln 2.$$

Beweis: Wir betrachten die Binomialkoeffizienten

$$M = \binom{2m+1}{m} = \frac{(2m+1)!}{m!(m+1)!}.$$

Sei $p \in \mathbb{P}$ und $m+1 < p \leq 2m+1$. Dann teilt p den Zähler von M, aber nicht den Nenner, also teilt p M. Dann teilt auch das Produkt dieser Primzahlen M und

$$\sum_{m+1<p\leq 2m+1} \ln p < \ln M$$

bzw.

$$\vartheta(2m+1) - \vartheta(m+1) < \ln M.$$

Andererseits sind auf der rechten Seite der Gleichung

$$(1+1)^{2m+1} = \binom{2m+1}{0} + \binom{2m+1}{1} + \cdots + \binom{2m+1}{2m+1}$$

zwei Terme gleich M, also

$$\begin{aligned} & 2M < 2^{2m+1} \\ \iff \quad & M < 2^{2m} \\ \iff & \ln M < 2m \ln 2 \end{aligned}$$

und damit

$$\vartheta(2m+1) - \vartheta(m+1) < 2m \ln 2.$$

Nun beweisen wir die Behauptung mittels vollständiger Induktion.
Induktionsanfang: $\vartheta(1) = 0 < 2\ln 2$ und $\vartheta(2) = \ln 2 < 4\ln 2$.
Induktionsschritt: Angenommen nun, der Satz ist wahr für $x < n$. Es muss gezeigt werden, dass er dann auch für $x = n$ gilt. Für gerades $n > 2$ ist $n \notin \mathbb{P}$ und deshalb

$$\vartheta(n) = \vartheta(n-1) < 2(n-1)\ln 2 < 2n\ln 2.$$

Ein ungerades n kann geschrieben werden als $n = 2m + 1$. Dann gilt

$$\begin{aligned} & \vartheta(2m+1) - \vartheta(m+1) < 2m\ln 2 \\ \iff \quad & \vartheta(2m+1) < \vartheta(m+1) + 2m\ln 2 \\ & < 2(m+1)\ln 2 + 2m\ln 2 \\ & = (4m+2)\ln 2 \\ & = 2n\ln 2. \end{aligned}$$

□

Als nächstes definieren wir $j(n,p)$ als die höchste Potenz von $p \in \mathbb{P}$, die $n!$ teilt. p taucht genau $[n/p]$-mal als Faktor von $n!$ auf. Genauso taucht $[n/p^2]$-mal p^2 als Faktor auf oder $[n/p^3]$-mal p^3 usw. Also ist die höchste Potenz von p, die $n!$ teilt

$$j(n,p) = \sum_{m \le \log_p n} \left[\frac{n}{p^m}\right].$$

Angenommen nun, Betrands Postulat wäre falsch, es gäbe also kein $p \in \mathbb{P}$ mit $n < p < 2n$ für irgendein n. Sei

$$N = \binom{2n}{n} = \frac{(2n)!}{(n!)^2}.$$

Nach unserer Annahme müssten alle Primzahlen, die N teilen kleiner gleich n sein. Wir finden also

$$N = \frac{(2n)!}{(n!)^2} = \frac{\prod\limits_{p \le 2n} p^{j(2n,p)}}{\prod\limits_{p \le n} p^{2j(n,p)}}.$$

Nun gibt es aber laut Annahme keine Primzahlen zwischen n und $2n$, daher kann das $p \le 2n$ im Zähler durch $p \le n$ ersetzt werden und wir erhalten

$$N = \prod_{p \le n} p^{j(2n,p) - 2j(n,p)}.$$

Sei im Weiteren $k(p) = j(2n,p) - 2j(n,p)$. Logarithmieren wir die obige Gleichung, so erhalten wir

$$\ln N = \sum_{p \le n} k(p)\ln p.$$

Dabei ist $k(p)$ eine Summe aus Termen der Form $[2x] - 2[x]$. Diese Terme sind entweder 0 ($[2x]$ gerade) oder 1 ($[2x]$ ungerade).

Jetzt zeigen wir, dass $k(p) = 0$ für $p > 2/3n$. Dann ist nämlich $2/3n < p \leq n$ bzw. $2 \leq 2n/p < 3$ und $[2n/p] = 2$, also $[2n/p] - 2[n/p] = 0$. Deshalb ist $p^2 > (4/9)n^2 > 2n$ ab $n > 4$. □

Als nächstes zeigen wir, dass die Terme mit $k(p) \geq 2$ vernachlässigbar sind. Für so einen Term ist $p^2 < 2n$ bzw. $p < \sqrt{2n}$, also ist die Anzahl solcher Terme höchstens $\sqrt{2n}$. $k(p)$ ist aber die Summe der Terme $[2n/p^m] - 2[n/p^m]$, was gleich 0 ist für $p^m > 2n$ bzw. $m > \log_p 2n$, also ist $\log_p 2n$ einer obere Schranke für $k(p)$. Mit $k(p) \ln p \leq \ln 2n$ erhalten wir

$$\sum_{k(p)\geq 2} k(p) \ln p \leq \sqrt{2n} \ln 2n.$$

Für die Terme mit $k(p) = 1$ haben wir dir obere Schranke

$$\sum_{p\leq 2/3n} \ln p = \vartheta\left(\frac{2}{3}n\right) < \frac{4}{3}n \ln 2,$$

wie oben bewiesen wurde.
Als Zusammenfassung unserer Ergebnisse ergibt sich

$$\ln N < \frac{4}{3}n \ln 2 + \sqrt{2n} \ln 2n.$$

Betrachten wir nun

$$(1+1)^{2n} = \binom{2n}{0} + \binom{2n}{1} + \cdots + \binom{2n}{2n},$$

so ist der größte dieser $2n+1$ Terme N. Also ist

$$2^{2n} < 2nN$$

oder

$$2n \ln 2 < \ln 2n + \ln N \leq \ln 2n + \frac{4}{3}n \ln 2 + \sqrt{2n} \ln 2n.$$

Für große Werte von n ist der dominierende Term $4/3n \ln 2$, was kleiner ist als $2n \ln 2$. Nun brauchen wir nur ein n zu finden, das diese Ungleichung verletzt, und der Widerspruchsbeweis ist vollständig. Nehmen wir $n \geq 2^9$, so ist

$$\ln 2n \geq \ln 2^{10} = 10 \ln 2.$$

Teilt man die obige Ungleichung durch $\ln 2$, so ergibt sich

$$\begin{aligned}
& 2^{10} < 10 + 2^{10}\frac{2}{3} + 2^5 10 \\
\iff \quad & 2^{10}\left(1 - \frac{2}{3}\right) < 10(2^5+1) \\
\iff \quad & 2^{10}\frac{1}{3} < 10(2^5+1) \\
\iff & 2^{10} < 30(2^5+1) < 31(2^5+1) = (2^5-1)(2^5+1) = 2^{10} - 1,
\end{aligned}$$

was ein Widerspruch ist! D. h. die Annahme, Bertrands Postulat wäre falsch und $n \geq 2^9$, führt zu einem Widerspruch. Bleibt nur noch, das Postulat für $n < 2^9 = 512$ zu beweisen. Dazu reicht diese Folge von Primzahlen aus, von denen jede etwas kleiner als das Doppelte ihres Vorgängers ist:

$$2, 3, 5, 7, 13, 23, 43, 83, 163, 317, 631$$

Damit ist Bertrands Postualt bewiesen.

12 Ein Streifzug durch die Zahlentheorie

Wir haben nun einen kleinen Einblick in die Welt der Zahlentheorie erhalten und werden dieses letzte Kapitel nutzen, auf einige Begriffe, denen wir begegnet sind, nochmal einzugehen, Querverbindungen zu schaffen und auch ein paar ganz neue Aspekte kennenzulernen.

12.1 Die σ-Funktion und perfekte Zahlen

Die σ-Funktion $\sigma(n)$ gibt die Summe aller positiven Teiler von n an:

$$\sigma(n) = \sum_{d|n} d$$

Hier sind ein paar Werte aufgeführt:

n	1	2	3	4	5	6	7	8	9	10
$\sigma(n)$	1	3	4	7	6	12	8	15	13	18

Laut Fundamentalsatz der Arithmetik kann man $\sigma(n)$ folgendermaßen berechnen:

$$\begin{aligned}
\sigma(n) &= \sum_{\substack{b_1,\ldots,b_i \\ 0\le b_k\le a_k}} p_1^{b_1}\cdots p_i^{b_i} \\
&= \sum_{\substack{b_2,\ldots,b_i \\ 0\le b_k\le a_k}} \left(\sum_{\substack{b_1 \\ 0\le b_k\le a_k}} p_1^{b_1} \right) \cdot p_2^{b_2}\cdots p_i^{b_i} \\
&= \frac{p_1^{a_1+1}-1}{p_1-1} \sum_{\substack{b_2,\ldots,b_i \\ 0\le b_k\le a_k}} p_2^{b_2}\cdots p_i^{b_i} \\
&= \frac{p_1^{a_1+1}-1}{p_1-1}\cdots\frac{p_i^{a_i+1}-1}{p_i-1}
\end{aligned}$$

Damit gilt für teilerfremde a, b stets $\sigma(a\cdot b) = \sigma(a)\cdot\sigma(b)$.

Eine Zahl heisst *perfekt* oder *vollkommen* genau dann, wenn $\sigma(n) = 2n$ ist, die Summe aller Teiler außer n selbst also wieder n ergibt. Der obigen Tabelle entnehmen wir, dass

die kleinste perfekte Zahl 6 ist. Bis heute ist unklar, ob es unendlich viele perfekte oder ungerade perfekte Zahlen gibt.

Es gibt einen interessanten Zusammenhang zwischen perfekten Zahlen und Mersenne'schen Primzahlen: Wenn $2^k - 1$ eine Primzahl ist, dann ist $2^{k-1}(2^k - 1)$ eine perfekte Zahl, und jede gerade perfekte Zahl hat diese Form.

Beweis: Angenommen, $p = 2^k - 1$ ist prim. Dann gilt es zu zeigen, dass $n = 2^{k-1}(2^k - 1)$ perfekt ist:

$$\sigma(n) = \sigma(2^{k-1}) \cdot \sigma(p) = (2^k - 1) \cdot (p + 1) = (2^k - 1) \cdot 2^k = 2n$$

Sei andersrum n eine gerade perfekte Zahl. Dann kann man n schreiben als $2^{k-1}m$, wobei m eine ungerade Zahl sein soll und $k \geq 2$.

$$\sigma(n) = \sigma(2^{k-1}m) = \sigma(2^{k-1}) \cdot \sigma(m) = (2^k - 1) \cdot \sigma(m)$$

Da n perfekt ist gilt

$$\sigma(n) = 2n = 2^k m.$$

Gleichsetzen gibt

$$2^k m = (2^k - 1) \cdot \sigma(m),$$

also teilt $2^k - 1$ $2^k m$, d. h. $2^k - 1$ teilt m. Dann kann man m schreiben als $m = (2^k - 1)l$. Einsetzen in obige Gleichung und Division durch $2^k - 1$ gibt

$$2^k l = \sigma(m).$$

Da m und l beide m teilen, folgt

$$2^k l = \sigma(m) \geq m + l = 2^k l \Rightarrow \sigma(m) = m + l.$$

Dann muss m prim sein, denn die einzigen Teiler von m sind m und $l = 1$. □

Eine andere Eigenschaft perfekter Zahlen ist die, dass die iterierte Quersumme jeder geraden perfekten Zahl (außer 6) 1 ergibt, z. B. $8128 \mapsto 19 \mapsto 10 \mapsto 1$.

Beweis: Sei $Q(n)$ die Quersumme von n. Es wurde schon gezeigt, dass $Q(n) = n \bmod 9$. Damit reduziert sich der Beweis darauf zu zeigen, dass alle geraden perfekten Zahlen größer 6 kongruent zu 1 modulo 9 sind. Sei n eine gerade perfekte Zahl, dann ist $n = 2^{p-1}(2^p - 1)$ mit $p \in \mathbb{P}$. Dann ist p entweder 2, 3 oder kongruent zu 1 oder 5 modulo 6. Den Fall $p = 2$ dürfen wir ausschließen. Nun gilt aber $2^6 = 1 \bmod 9$, d. h. die Potenzen von 2 wiederholen sich mit der Periode 6 modulo 9. Jetzt müssen wir nur noch $2^{1-1}(2^1 - 1)$, $2^{3-1}(2^3 - 1)$ und $2^{5-1}(2^5 - 1)$ überprüfen, und sie sind alle gleich 1 modulo 9. □

12.2 Die Chance, zwei teilerfremde Zahlen zu ziehen

Machen wir einen kleinen Abstecher in die analytische Zahlentheorie: Wie groß ist die Wahrscheinlichkeit, dass zwei zufällig ausgewählte natürliche Zahlen teilerfremd sind? Seien $a, b, c \in \mathbb{N}$. Die Wahrscheinlichkeit, dass a ein Vielfaches von c ist, beträgt $1/c$, denn jede c-te Zahl ist ja ein Vielfaches von c. Ebenso ist die Wahrscheinlichkeit, dass b ein Vielfaches von c ist $1/c$. Dann ist die Wahrscheinlichkeit, dass sowohl a als auch b durch c teilbar sind, $1/c^2$. Sei nun $c = \mathrm{ggT}(a, b)$, so müssen a/c und b/c teilerfremd sein, was mit der gesuchten Wahrscheinlichkeit p eintritt. Die Wahrscheinlichkeit p_c, dass a und b Vielfache von c sowie a/c und b/c teilerfremd sind beträgt somit

$$p_c = p \cdot \frac{1}{c^2}.$$

Irgendeine natürliche Zahl wird mit Sicherheit $\mathrm{ggT}(a, b)$ sein, d. h.

$$\sum_{c=1}^{\infty} p_c = \sum_{c=1}^{\infty} p \cdot \frac{1}{c^2} = p \sum_{c=1}^{\infty} \frac{1}{c^2} = 1.$$

Nun haben wir im Artikel über Fourier-Reihen gezeigt, dass

$$\sum_{c=1}^{\infty} \frac{1}{c^2} = \frac{\pi^2}{6}.$$

Damit ergibt sich die gesuchte Wahrscheinlichkeit zu $p = 6/\pi^2 = 0{,}6079\ldots$

12.3 Sätze über Teilbarkeit

- Satz: Die Summe zweier Primzahlen größer 3 eines Primzahlzwillings ist stets durch 12 teilbar.
  Beweis: Seien $p, q \in \mathbb{P}$ diese Primzahlen, also $q = p + 2$ und $p < k < q$. Das ergibt in Abhängigkeit von k: $p = k - 1$, k, $q = k + 1$. Da p und q ungerade sind, muss k gerade sein. Ebenso muss von drei aufeinanderfolgenden Zahlen eine durch 3 teilbar sein. Da p und q dies nicht sind, bleibt nur noch k übrig. Darüberhinaus ist $p + q = (k - 1) + (k + 1) = 2k$. Da k wie gezeigt die Teiler 2 und 3 hat, folgt die Behauptung. □

- Satz: Für jede Primzahl $p > 3$ gilt $p^2 = 1 \bmod 24$.
  Beweis: Jede Primzahl größer 3 läßt sich schreiben als $12n \pm 7$ oder $12n \pm 11$ ($n \in \mathbb{N}_0$).
  $$(12n \pm 7)^2 = 144n^2 \pm 168n + 49 = 1 \bmod 24$$
  $$(12n \pm 11)^2 = 144n^2 \pm 264n + 121 = 1 \bmod 24$$ □

- Satz: Die Differenz aus einer Zahl und ihrem Ziffernsturz (d. h. die Ziffern in umgekehrter Reihenfolge) ist ein Vielfaches von 9.
  Beweis: Es gilt $Q(n) = n \bmod 9$. Da die Quersumme sich bei Permutation der Ziffern nicht ändert, haben wir als Differenz $Q(n) - Q(n) = 0 \bmod 9$. □

- Satz: Alle Primzahlen p teilen den Binomialkoeffizienten $\binom{p}{k}$ mit $0 < k < p$.
  Beweis:
  $$\binom{p}{k} = \frac{p!}{k!(p-k)!}$$
  Da p im Nenner nicht als Faktor auftaucht, kann p auch aus dem Produkt im Zähler nicht herausgekürzt werden. Folglich teilt p den Zähler des Bruchs, nicht aber den Nenner, also teilt p den Binomialkoeffizienten. □

- Satz: Es gibt zwei Potenzen von 3, deren Differenzen durch 123456789 teilbar sind.
  Beweis: Es gibt 123456789 Reste modulo 123456789. Betrachten wir die Folge
  $$1, 3, 3^2, \ldots, 3^{123456789},$$
  welche 123456790 Zahlen enthält. Nach dem Schubfachprinzip muss es dann zwei von ihnen geben, nennen wir sie 3^n und 3^m, $n > m$, die in der gleichen Restklasse modulo 123456789 liegen. Dann ist ihre Differenz $3^n - 3^m$ teilbar durch 123456789.□

  Ähnlich ist der folgende Satz: Es gibt eine Potenz von 3, die auf 001 endet.
  Beweis: Seien 3^n und 3^m zwei Zahlen, die den gleichen Rest modulo 1000 haben. $3^n - 3^m = 3^m(3^{n-m} - 1)$ ist teilbar durch 1000. Da 1000 und 3^m teilerfremd sind, muss 1000 $3^{n-m} - 1$ teilen. Dann endet 3^{n-m} auf 001. □

12.4 Über die Häufigkeit von Ziffern

Betrachten wir die Zahlen mit einer einzigen Ziffer $0, 1, 2, \ldots, 9$, so gibt es genau eine, in der eine gewisse Ziffer (z. B. 2 — die Ziffer 0 spielt natürlich eine Sonderrolle und wird nicht betrachtet) auftaucht. Unter allen Zahlen mit einer oder zwei Ziffern $0, 1, 2, \ldots, 99$ enthalten die Zahlen
$$2, 12, 20, 21, \ldots, 29, 32, 42, \ldots, 92$$
die Ziffer 2, das sind insgesamt 19 Stück. Unter den ein- bis dreistelligen Zahlen sind es dann $9 \cdot 19 + 100$ Zahlen mit der Ziffer 2. Wir kommen so zur Rekursionsformel für die Anzahl der Zahlen mit einer bestimmten Ziffer
$$Z_{n+1} = 9 \cdot Z_n + 10^n, \qquad Z_1 = 1.$$
Überlegen wir uns nun eine explizite Formel: Es gibt 10^n Möglichkeiten, eine (mindestens) n-stellige Zahl hinzuschreiben (beginnt die Zahl mit Nullen, hat sie ja weniger Ziffern). Wollen wir an der n-ten Stelle eine 2 vermeiden, so haben wir 9 Möglichkeiten, das macht also insgesamt 9^n Zahlen, in denen keine 2 auftaucht. Also gibt es insgesamt
$$Z_n = 10^n - 9^n$$

Zahlen, in denen mindestens eine 2 auftaucht. Man überzeugt sich leicht, dass diese Formel die Rekursionsgleichung erfüllt. Nun geht aber der Quotient

$$\frac{10^n - 9^n}{10^n} = 1 + \left(\frac{9}{10}\right)^n$$

mit $n \to \infty$ gegen 1, also enthalten fast alle großen Zahlen eine 2!

12.5 Beatty-Folgen

Sei r eine positive irrationale Zahl und $s = 1/r$. Dann definieren wir die Folgen $a_n = n(r+1)$ und $b_n = n(s+1)$ mit $n > 0$. Dann sind natürlich auch sämtliche Folgenglieder irrational. Interessanterweise gibt es für jedes $m \in \mathbb{N}$ genau ein Element aus $\{a_n\} \cup \{b_n\}$, das im Intervall $[m, m+1]$ liegt. Mit anderen Worten: Die ganzzahligen Anteile der beiden Folgen decken die gesamten natürlichen Zahlen ab!

Beweis: Sei m eine ganze Zahl. Es gibt $[m/(r+1)]$ Folgenglieder der ersten Folge, die kleiner als m sind. Ebenso gibt es $[m/(s+1)]$ Folgenglieder der zweiten Folge, die kleiner als m sind. Da keines der Folgenglieder beider Folgen eine ganze Zahl ist, gilt

$$\begin{aligned} \frac{m}{r+1} - 1 < &\left[\frac{m}{r+1}\right] < \frac{m}{r+1}, \\ \frac{m}{s+1} - 1 < &\left[\frac{m}{s+1}\right] < \frac{m}{s+1}. \end{aligned}$$

Außerdem berechnen wir

$$\frac{1}{r+1} + \frac{1}{s+1} = \frac{1}{r+1} + \frac{1}{\frac{1}{r}+1} = \frac{1}{r+1} + \frac{r}{r+1} = 1.$$

Daher ergibt die Summe der beiden oberen Gleichungen

$$m - 2 < \left[\frac{m}{r+1}\right] + \left[\frac{m}{s+1}\right] < m,$$

was auf

$$\left[\frac{m}{r+1}\right] + \left[\frac{m}{s+1}\right] = m - 1$$

hinausläuft. Durchläuft nun m alle natürlichen Zahlen, so wird immer genau ein Element der Vereinigungsmenge $\{a_n\} \cup \{b_n\}$ hinzugefügt. □

12.6 Alternativen zu Euklids Beweis

Euklids Beweis dafür, dass es unendlich viele Primzahlen gibt, ist ein Klassiker, der an Einfachheit kaum zu überbieten ist. Kürzer ist nur noch der folgende Beweis von Kummer:

Angenommen, es gäbe nur endlich viele Primzahlen. Dann bilde man deren Produkt $n = p_1 p_2 \cdots p_n$. Nach dem Fundamentalsatz der Arithmetik muss $n-1$ mindestens einen gemeinsamen Primteiler mit n haben, nennen wir ihn p_i. Dann muss p_i auch die Differenz $n-(n-1)=1$ teilen, was der Tatsache widerspricht, dass p_i prim ist. □

Eine andere Möglichkeit besteht in der Konstruktion einer unendlichen Folge paarweise teilerfremder Zahlen. Denn sind diese paarweise teilerfremd, so haben sie insbesondere keinen gemeinsamen Primteiler. Folglich sind die Primteiler aller Zahlen dieser Folge verschieden, es gibt nunmehr unendlich viele Primzahlen.

Der folgende Beweis von Goldbach benutzt zur Konstruktion einer solchen Folge die Fermat'schen Zahlen. Dazu stellen wir zunächst fest, dass die Fermat'schen Zahlen der Rekursionsgleichung

$$F_n = (F_{n-1}-1)^2 + 1$$

genügen. Nun behaupten wir: Keine zwei Fermat'schen Zahlen $F_n = 2^{2^n}+1$ $(n \geq 0)$ haben einen gemeinsamen Teiler.

Beweis: Wir zeigen, dass $F_n - 2 = F_0 F_1 \cdots F_{n-1}$ gilt.
Induktionsanfang: $F_0 = 3$, $F_1 = 5$: $F_1 - 2 = F_0$ (w)
Induktionsschritt:

$$\begin{aligned}
F_{n+1} - 2 &= (F_n - 1)^2 + 1 - 2 = F_n^2 - 2F_n \\
&= (F_0 F_1 \cdots F_{n-1} + 2)^2 - 2(F_0 F_1 \cdots F_{n-1} + 2) \\
&= F_0^2 F_1^2 \cdots F_{n-1}^2 + 4F_0 F_1 \cdots F_{n-1} + 4 - 2(F_0 F_1 \cdots F_{n-1} + 2) \\
&= F_0^2 F_1^2 \cdots F_{n-1}^2 + 2F_0 F_1 \cdots F_{n-1} \\
&= F_0 F_1 \cdots F_{n-1}(F_0 F_1 \cdots F_{n-1} + 2) \\
&= F_0 F_1 \cdots F_{n-1} F_n
\end{aligned}$$

Daraus folgt, dass $F_m | (F_n - 2)$ für alle $(m < n)$. Somit muss jedes $p \in \mathbb{P}$, das F_n und F_m teilt auch 2 teilen. Folglich ist $p = 2$. Da aber alle Fermat'schen Zahlen ungerade sind, haben wir einen Widerspruch! □

Übrigens ist nach Gauß ein n-Eck genau dann mit Zirkel und Lineal konstruierbar, wenn n eine Primzahl von der Form $2^{2^k}+1$ ist oder ein Produkt aus verschiedenen solcher Primzahlen und einer Potenz von 2 oder eine Potenz von 2.

Einen weiteren Beweisansatz liefert Dirichlets Satz: Sind a und b teilerfremd, so enthält $\{an+b \,|\, n \in \mathbb{N}\}$ unendlich viele Primzahlen. Wir werden diesen Satz für $a = 3$ und $b = 4$ beweisen.

Sämtliche natürliche Zahlen sind von der Form $4n$, $4n+1$, $4n+2$ oder $4n+3$. Die Zahlen $4n$ und $4n+2$ sind durch 2 teilbar, und können daher (abgesehen von der 2 selber) nicht prim sein. Für Zahlen der Form $4n+1$ gilt $(4n+1)(4m+1) = 16nm + 4n + 4m + 1 = 4(4nm + n + m) + 1$, das Produkt zweier Zahlen dieser Form ist also wieder von der gleichen Form. Nehmen wir nun an, es gäbe nur endlich viele Primzahlen $p_1, p_2, \ldots, p_l$ der Form $4n+3$. Sei $a = 4p_1 p_2 \cdots p_l + 3$. Da a selber von der Form $4n+3$ ist, können nicht alle Primfaktoren von a die Form $4n+1$ haben. Jedenfalls muss es einen Primfaktor geben, der verschieden von $p_1, p_2, \ldots, p_l$ ist. Widerspruch! □

Schließen wir diesen Beweisreigen ab, indem wir eine Überleitung zum nächsten Abschnitt schaffen. Sei $p \in \mathbb{P}$, so ist

$$\sum_{i=0}^{\infty} \frac{1}{p^i} = \frac{1}{1 - \frac{1}{p}}.$$

Für zwei $p_1, p_2 \in \mathbb{P}$ gilt dann

$$\sum_{i_1,i_2 \geq 0}^{\infty} \frac{1}{p_1^{i_1} \cdot p_2^{i_2}} = \sum_{i_1=0}^{\infty} \frac{1}{p_1^{i_1}} \cdot \sum_{i_2=0}^{\infty} \frac{1}{p_2^{i_2}} = \frac{1}{1 - \frac{1}{p_1}} \cdot \frac{1}{1 - \frac{1}{p_2}}.$$

Angenommen nun, es gäbe nur endlich viele, nämlich n, Primzahlen. Dann steht nach dem Fundamentalsatz der Arithmetik auf der linken Seite der Gleichung die *harmonische Reihe*

$$\sum_{m=1}^{\infty} \frac{1}{m} = \prod_{k=1}^{n} \frac{1}{1 - \frac{1}{p_k}}.$$

Wir wissen aber, dass die harmonische Reihe divergiert, daher steht der unendliche Wert links der Gleichung im Widerspruch zum endlichen auf der rechten Seite. □

12.7 Primzahlen und die Riemann'sche Zetafunktion

Mit dem letzten Beweis haben wir den Übergang zur *analytischen Zahlentheorie* beschritten. Schreibt man die letzte Zeile der Rechnung korrekt

$$\sum_{m=1}^{\infty} \frac{1}{m} = \prod_{k=1}^{\infty} \frac{1}{1 - \frac{1}{p_k}},$$

so folgt die Divergenz des Produkts auf der rechten Seite. Wir werden nun zeigen, dass auch die Summe

$$\sum_{i=1}^{\infty} \frac{1}{p_i}$$

divergiert. Dazu benutzen wir unsere Erkenntnis über das Produkt. Betrachten wir das Produkt für die ersten r Primzahlen. Ist das Produkt unbeschränkt, so gilt das auch für

$$\begin{aligned} \ln \prod_{k=1}^{r} \frac{1}{1 - \frac{1}{p_k}} &= \sum_{k=1}^{r} \ln \frac{1}{1 - \frac{1}{p_k}} \\ &= -\sum_{k=1}^{r} \ln 1 - \frac{1}{p_k}. \end{aligned}$$

Mit der Taylorentwicklung $-\ln(1-x) = \sum_{n=1}^{\infty} x^n/n$ wird daraus

$$= \sum_{k=1}^{r}\sum_{n=1}^{\infty}\frac{1}{np_k^n}$$
$$= \frac{1}{p_1}+\frac{1}{p_2}+\cdots+\frac{1}{p_r}+\sum_{k=1}^{r}\sum_{n=2}^{\infty}\frac{1}{np_k^n}.$$

Wenn wir nun ableiten können, dass der zweite Teil der Summe konvergent ist, so muss notwenigerweise die Summe der Kehrwerte der Primzahlen unbeschränkt sein:

$$\sum_{n=2}^{\infty}\frac{1}{n}\left(\frac{1}{p_k}\right)^n < \sum_{n=2}^{\infty}\left(\frac{1}{p_k}\right)^n = \frac{1}{p_k^2}\cdot\sum_{n=0}^{\infty}\frac{1}{p_k^n} = \frac{1}{p_k^2}\cdot\frac{1}{1-\dfrac{1}{p_k}} \le \frac{2}{p_k^2}$$

Damit ist

$$\sum_{k=1}^{r}\sum_{n=2}^{\infty}\frac{1}{np_k^n} < \sum_{k=1}^{r}\sum_{n=2}^{\infty}\left(\frac{1}{p_k}\right)^n < 2\sum_{m=1}^{\infty}\frac{1}{m^2}.$$ □

Interessanterweise ist die Summe der Kehrwerte der *Primzahlzwillinge* konvergent, und zwar konvergiert sie gegen die *Brun'sche Konstante*

$$B = \left(\frac{1}{3}+\frac{1}{5}\right)+\left(\frac{1}{5}+\frac{1}{7}\right)+\left(\frac{1}{11}+\frac{1}{13}\right)+\cdots = 1{,}90216058\ldots$$

Es gibt also in diesem Sinne wesentlich weniger Primzahlzwillinge als Primzahlen. Da man aber nicht weiß, ob B irrational ist, bleibt das Problem der Anzahl der Primzahlzwillinge weiterhin ungelöst.

Die wichtigste Funktion in der analytischen Zahlentheorie ist die *Riemann'sche Zetafunktion*

$$\zeta(s) = \sum_{n=1}^{\infty}\frac{1}{n^s}.$$

Es gilt nämlich

$$\zeta(s) = \prod_{i=1}^{\infty}\frac{1}{1-\dfrac{1}{p_i^s}}.$$

Beweis: Wir sahen schon, dass

$$\sum_{k=0}^{\infty}\frac{1}{p_i^k} = \frac{1}{1-\dfrac{1}{p_1}}.$$

Dann ist

$$\prod_{i=1}^{r}\frac{1}{1-\dfrac{1}{p_i^s}} = \prod_{i=1}^{r}\sum_{k=0}^{\infty}\left(\frac{1}{p_i^s}\right)^k = \sum_{k_1,k_2,\ldots,k_r}\frac{1}{(p_1^{k_1}p_2^{k_2}\ldots p_r^{k_r})^s}.$$

Auf der rechten Seite im Nenner stehen nun sämtliche Zahlen, die sich mit den ersten r Primzahlen darstellen lassen. Lässt man r gegen unendlich gehen, so folgt die Behauptung. □

Womit wir erneut die unendliche Anzahl der Primzahlen bewiesen hätten: Es folgt sofort, dass $\zeta(2) = \pi^2/6$ ist, also irrational. Würde das Produkt aber nur über eine endliche Reihe von Faktoren erstreckt, könnte das nicht sein. Widerspruch! □

In der analytischen Zahlentheorie wird die Zetafunktion aber nicht nur für natürliche, sondern auch für komplexe Werte betrachtet. Eines der größten Probleme der Mathematik in der heutigen Zeit ist die *Riemann'sche Vermutung*: Alle nichttrivialen Nullstellen (die trivialen liegen bei $\zeta(-2k), k \in \mathbb{N}$) liegen auf der *kritischen Geraden* $\mathrm{Re}(s) = 0{,}5$. Dabei ist bekannt, dass alle nichttrivialen Nullstellen im *kritischen Streifen* $0 \leq \mathrm{Re}(s) \leq 1$ liegen.

Für alle natürlichen geraden Werte existiert eine geschlossene Formel. Sie sind alle transzendent. Die ungeraden Werte machen mehr Schwierigkeiten. Da Apéry die Irrationalität von $\zeta(3)$ beweisen konnte, heisst diese Zahl nun *Apérys Konstante*.

Eine weitere wichtige Funktion $\pi(x)$ zählt die Anzahl der Primzahlen $p < x$. Für sie gilt der *Primzahlsatz*

$$\lim_{x\to\infty} \frac{\pi(x)}{\dfrac{x}{\ln x}} = 1,$$

d. h. $\pi(x) \approx x/\ln x$, wogegen die Approximation für x gegen unendlich immer besser wird. Leider kann der Primzahlsatz hier nicht bewiesen werden.

Doch wo wir gerade bei der analytischen Zahlentheorie sind, sollen hier noch ein paar Ergebnisse präsentiert werden, deren Thematik wir angeschnitten haben. Sei $P_H(n)$, $P_U(n)$ und $P_F(n)$ die Anzahl der pythagoräischen Dreiecke, deren Hypotenuse, Umfang bzw. Fläche n nicht überschreitet. Dann kommt man zu folgenden Ergebnissen:

$$\begin{aligned}
\lim_{n\to\infty} \frac{P_H(n)}{n} &= \frac{1}{2\pi} \\
\lim_{n\to\infty} \frac{P_U(n)}{n} &= \frac{\ln 2}{\pi^2} \\
\lim_{n\to\infty} \frac{P_F(n)}{\sqrt{n}} &= \frac{\Gamma^2\left(\frac{1}{4}\right)}{\sqrt{2\pi^5}}
\end{aligned}$$

Und auch über das Grenzverhalten der Euler'schen φ-Funktion lassen sich Aussagen machen:

$$\begin{aligned}
\limsup_{n\to\infty} \frac{\varphi(n)}{n} &= 1 \\
\liminf_{n\to\infty} \frac{\varphi(n)\ln\ln n}{n} &= e^{-\gamma}
\end{aligned}$$

Ein Ergebnis aus der elementaren Zahlentheorie ist das *Primzahlpolynom*: Ein Polynom in 26 Variablen, dessen positive Funktionswerte sämtlich Primzahlen sind!

12.8 Kaprekar-Konstanten

Normalerweise werden Eigenschaften von Zahlen, die sich auf ihre Darstellung in einem bestimmten Stellenwertsystem beziehen, nicht von der strengen Zahlentheorie untersucht. Da die Kaprekar-Konstanten aber in jedem Stellenwertsystem auftreten, sei hier eine Ausnahme gemacht.

Betrachten wir eine vierstellige Zahl, die keine Schnapszahl ist, z. B. 2314. Wir bilden nun diejenigen Permutationen ihrer Ziffern, die die größte und kleinste Zahl ergeben und bestimmen ihre Differenz: $4321 - 1234 = 3087$. Das gleiche Spiel wird mit 3087 wiederholt: $8730 - 0378 = 8352$. Und nochmal: $8532 - 2358 = 6174$. Doch nun passiert etwas Merkwürdiges: $7641 - 1467 = 6174$! Die Zahl 6174 ist also Fixpunkt dieser Iteration. Tatsächlich erhält man aus jeder vierstelligen Zahl, die keine Schnapszahl ist, durch diese Iteration die *Kaprekar-Konstante* 6174, und zwar nach höchstens sieben Schritten.

Beweisen lässt sich das am Einfachsten mit *brute force*: Man schreibt ein Computerprogramm, das alle vierstelligen Zahlen testet.

Wir werden dieses Problem nun etwas verallgemeinern: Gegeben sei eine n-stellige Zahl, deren Ziffern in absteigender Reihenfolge sortiert sind, von der eine andere n-stelligen Zahl mit den gleichen Ziffern in umgekehrter Reihenfolge abgezogen wird. Dann ist das Ergebnis eine weitere n-stellige Zahl (wenn man führende Nullen mit einbezieht). Die Differenzbildung ist dann abgeschlossen auf der Menge N der n-stelligen Zahlen. Dann ist der beschriebene *Kaprekar-Algorithmus* K eine Abbildung $K : N \mapsto N$. Formal ist dann die Iteration mit dem Startwert $x_0 \in N$

$$\begin{aligned} K(x_0) &\mapsto x_1 \\ K(x_1) &\mapsto x_2 \\ K(x_2) &\mapsto x_3 \\ &\dots \end{aligned}$$

wobei natürlich irgendwann einmal

$$K(x_n) \mapsto x_n$$

auftreten kann. x_n wird durch den Kaprekar-Algorithmus auf sich selbst abgebildet und heisst *Fixpunkt*. Das ist z. B. bei der Menge N_{10}^4 der vierstelligen Dezimalzahlen aufgetreten.

Ein anderes mögliches Verhalten ist das folgende:

$$\begin{aligned} &\dots \\ K(x_n) &\mapsto x_{n+1} \\ K(x_{n+1}) &\mapsto x_{n+2} \\ &\dots \\ K(x_{n+k}) &\mapsto x_n \end{aligned}$$

was bedeutet, dass ein Zyklus mit der Periode k aufgetreten ist. Man spricht dann von *Kaprekar-Zyklen*.

Man kann zeigen, dass jede Menge N aus n-stelligen Zahlen in jedem beliebigen Positionssystem mindestens einen solchen Zyklus besitzt. Die Menge N enthält nämlich nur endlich viele Zahlen, daher muss die Iteration zwangsläufig früher oder später auf eine schon vorgekommene Zahl zurückkommen. Die Menge N_{10}^5 der fünfstelligen Dezimalzahlen besitzt sogar drei Zyklen, nämlich

$$95553 \mapsto 99954$$

$$97641 \mapsto 98622 \mapsto 97533 \mapsto 96543$$

$$96642 \mapsto 97731 \mapsto 98532 \mapsto 97443$$

Iterationen mit Fixpunkt ergeben sich u. a. noch in den folgenden Systemen: N_{10}^3: 954, N_8^3: 522_{10}, N_{16}^3: 4200_{10}, N_2^5: 30_{10}.

Zum Abschluss dieses Abschnitts werden wir ein weiteres Phänomen dieser Art untersuchen. Betrachten wir irgendeine Zahl, z. B. 123456789, und zählen ihre geraden (4) und ungeraden (5) sowie die Gesamtzahl (9) der Ziffern und bilden daraus eine neue Zahl: 459. Nach nochmaliger Iteration erhalten wir 123. Und diese 123 erhält man aus jeder bliebigen Zahl!

Beweis: Sei f die Abbildung, die eine Iteration durchführt. Dann ist offensichtlich $f(n) < n$ für $n > 999$. Durch Wiederholung dieses Arguments kommt man dazu, dass es ausreicht, dreistellige Zahlen zu untersuchen. Bezeichne im Tupel (g, u, t) g die Anzahl der geraden, u die Anzahl der ungeraden und t die Totalzahl der Ziffern von n. Dann ist jede dreistellige Zahl von der Form $(0, 3, 3)$, $(1, 2, 3)$, $(2, 1, 3)$ oder $(3, 0, 3)$. Wendet man nun die Iteration einmal an, so erhält in jedem der vier Fälle $(1, 2, 3)$. □

Es gibt noch unzählige weitere Iterationen dieser Art, die auf einen Fixpunkt hinauslaufen. Erwähnt sei noch das *Collatz-Problem*, das zur Zeit wichtigste noch ungelöste Problem dieser Art. Die Iteration ist durch

$$f(n) = \begin{cases} \dfrac{n}{2} & n \text{ gerade} \\ 3n + 1 & n \text{ ungerade} \end{cases}$$

gegeben. Vermutlich enden alle Iteration für beliebiges n auf den Zyklus $4, 2, 1$, aber bewiesen ist das nicht.

Index

Algebra, 61
algebraische Abgeschlossenheit, 19
Antikommutativitätb, 20
Apérys Konstante, 81

Beatty-Folgen, 77
Bertrands Postulat, 69
Brun'sche Konstante, 80

Carmichael-Zahlen, 49
Cayley-Dickson-Konstruktion, 19
Cayley-Zahlen, 20
Chinesischer Restsatz, 44
Collatz-Problem, 83

Dichtheit, 10
Divisionsalgebra, 19

e, 13
Einheit, 65
Euklidischer Algorithmus, 28
Euler'sche Gleichung, 19
Euler'sche φ-Funktion, 49
Euler'sche φ-Funktion, 81
Euler'sche Zahl, *siehe* e

Faktorisierungsverfahren, 54
Fano-Ebene, 20
Fermat'sche
    Primzahlen, 49
    Zahlen, 49, 78
Fundamentalsatz der Algebra, 19
Fundamentalsatz der Arithmetik, 32, 73, 79

ggT, 28
Gruppen, 61
    abelsche, 62
    kommutative, 62

harmonische Reihe, 79

imaginäre Einheit, 19
Integritätsringe, 64

Körper, 9, 67
Kaprekar-Konstanten, 82
kgV, 30
Kongruenzensystem, 44
Kreiszahl, *siehe* π

Liouville'sche Konstante, 17

Mersenne'sche
    Primzahlen, 49
    Zahlen, 49
Moduloarithmetik, 38
Moduloarithmetk, 65
Multiplikationstabellen, 42
multiplikative Mitte, 31

Negativität, 26
Neunerprobe, 43
Nichtnegativität, 26
Nichtpositivität, 26
Nichtrest
    quadratischer, 57
Niven-Polynom, 14
Norm, 65
Null, 26
Nullteiler, 41, 64

Oktaven, 20

Parität, 26, 58
Peano-Axiome, 7

π, 16
Polynomwurzeln, 12
Positivität, 26
Primfaktorzerlegung, 29, 30
    in Integritätsringen, 65
Primteiler, 31
Primzahlabstand, 31
Primzahlen, 30, 38
Primzahlpolynom, 81
Primzahlsatz, 81
Primzahltest, 31, 47
Primzahltriplett, 47
Primzahlzwillinge, 80
Probedivision, 54
Pseudoprimzahlen, 49
pythagoräische Tripel, 57, 81

Quadratzahlen, 55, 56, 58
    Summen von, 59
Quaternionen, 20
Quersumme, 34
    alternierende, 34, 36
    iterierte, 74

rationale Punkte, 59
Repräsentant, 39
Repräsentantensystem, 41
Rest, 27
    quadratischer, 57, 65
Restklassen, 38, 55
    Rechenregeln, 39
Riemann'sche Zetafunktion, 79
Ringe, 63
RSA-Verschlüsselung, 51

Satz v. d. eindeutigen Primfaktorzerlegung, *siehe* Fundamentalsatz d. Arithmetik
Satz von Dirichlet, 78
Satz von Euler, 49
Satz von Fermat, 48
Satz von Pocklington, 53
Satz von Wilson, 47
Sieb des Eratosthenes, 47
σ-Funktion, 73

Teilbarkeitsregeln, 33
Teiler, 27
    echte, 27
    gemeinsame, 27
    triviale, 27

Verfahren von Fermat, 54
Vielfache, 30
vollständige Induktion, 7

Zahlen
    algebraische, 8
    ganze, 7, 26
    Gauß'sche, 67
    gerade, 26
    hyperkomplexe, 25
    irrationale, 8
    komplexe, 19
    natürliche, 7
    perfekte, 73
    rationale, 8
    reelle, 8
    schlecht approximierbare, 17
    teilerfremde, 28, 75
    transzendente, 9, 17
    ungerade, 26
    vollkommende, 73
    zusammengesetzte, 31