Kapitel 6

# Ganze Zahlen, Teiler und Primzahlen

6

# 6

# 6 Ganze Zahlen, Teiler und Primzahlen

In diesem Kapitel behandeln wir die Eigenschaften ganzer Zahlen. Dieser Bereich der Mathematik wird *Zahlentheorie* genannt und ist ein wahrhaft ehrwürdiges Gebiet: Die Wurzeln reichen ungefähr 2500 Jahre zurück, bis zum Anbeginn der griechischen Mathematik. Man könnte meinen, nach 2500 Jahren der Forschung sei im Wesentlichen alles bekannt. Wir werden jedoch sehen, dass dies nicht der Fall ist: Es gibt sehr einfache, naheliegende Fragen, die wir nicht beantworten können und es gibt andere einfache, natürliche Fragen, für die erst innerhalb der letzten paar Jahre eine Antwort gefunden werden konnte!

## 6.1 Teilbarkeit ganzer Zahlen



Wir beginnen mit einigen grundsätzlichen Bezeichnungen bezüglich ganzer Zahlen. Seien $a$ und $b$ zwei ganze Zahlen. Wir sagen $a$ *teilt* $b$ oder $a$ *ist ein Teiler von* $b$ oder $b$ *ist ein Vielfaches von* $a$ (diese Bezeichnungen bedeuten dasselbe), wenn eine ganze Zahl $m$ existiert, so dass $b = am$ gilt. Wir schreiben dafür $a \mid b$. Ist $a$ kein Teiler von $b$, dann schreiben wir $a \nmid b$. Falls $a \neq 0$ gilt, dann bedeutet $a \mid b$, dass der Bruch $b/a$ eine ganze Zahl ist.
Wenn $a \nmid b$ und $a > 0$ gilt, dann können wir $b$ immer noch durch $a$ teilen, allerdings mit Rest. Der Rest $r$ bei der Division $b \div a$ ist eine ganze Zahl, die $0 \leq r < a$ erfüllt. Ist $q$ der Quotient einer Division mit Rest, dann haben wir

$$b = aq + r.$$

Eine Division mit Rest auf diese Weise zu betrachten, wird sich noch als sehr nützlich erweisen.
Sie haben diese Bezeichnungen möglicherweise schon früher einmal gesehen. Die folgenden Übungsaufgaben sollen Ihnen bei der Überprüfung helfen, ob Sie sich noch genügend daran erinnern.

---

**Übung 6.1.1** Überprüfen Sie (mit Hilfe der Definition), dass für jede ganze Zahl $a$ gilt: $1 \mid a$, $-1 \mid a$, $a \mid a$ und $-a \mid a$.

---

**Übung 6.1.2** Was bedeutet es für $a$, umgangssprachlich ausgedrückt, wenn (a) $2 \mid a$, (b) $2 \nmid a$ und (c) $0 \mid a$?

---

**Übung 6.1.3** Beweisen Sie,
(a) falls $a \mid b$ und $b \mid c$, dann gilt $a \mid c$,
(b) falls $a \mid b$ und $a \mid c$, dann gilt $a \mid b + c$ und $a \mid b - c$,
(c) falls $a, b > 0$ und $a \mid b$, dann gilt $a \leq b$,

(d)falls $a \mid b$ und $b \mid a$, dann gilt entweder $a = b$ oder $a = (-b)$.

---

**Übung 6.1.4** Sei $r$ der Rest bei der Division $b \div a$. Angenommen, es gilt $c \mid a$ und $c \mid b$. Beweisen Sie, dass $c \mid r$ gilt.

---

**Übung 6.1.5** Angenommen, es gilt $a \mid b$ und $a, b > 0$. Sei $r$ der Rest bei der Division $c \div a$ und sei $s$ der Rest bei der Division $c \div b$. Wie lautet der Rest bei der Division $s \div a$?

---

**Übung 6.1.6** Beweisen Sie, dass
(a)für jede ganze Zahl $a$ gilt: $a - 1 \mid a^2 - 1$,
(b)allgemeiner, für jede ganze Zahl $a$ und jede positive ganze Zahl $n$ gilt:

$$a - 1 \mid a^n - 1.$$

6.2

## 6.2 Primzahlen und ihre Geschichte

Eine ganze Zahl $p > 1$ wird *Primzahl* genannt, falls sie durch keine andere ganze Zahl, außer $1, -1, p$ und $-p$ teilbar ist. Man kann dies auch so ausdrücken: Eine Primzahl ist eine ganze Zahl $p > 1$, die sich nicht als Produkt zweier kleinerer natürlicher Zahlen schreiben läßt. Eine ganze Zahl $n > 1$, die keine Primzahl ist, wird *zusammengesetzt* genannt (die Zahl 1 wird weder als Primzahl noch als zusammengesetzte Zahl angesehen). Demnach sind $2, 3, 5, 7, 11$ Primzahlen, während $4 = 2 \cdot 2$, $6 = 2 \cdot 3$, $8 = 2 \cdot 4$, $9 = 3 \cdot 3$, $10 = 2 \cdot 5$ keine Primzahlen sind. Tabelle 6.1 zeigt alle Primzahlen bis 500.
Primzahlen faszinieren die Menschen seit jeher. Ihre Folge scheint sehr unregelmäßig zu sein, aber bei näherer Betrachtung erhält man den Eindruck, als gäbe es doch eine Menge versteckter Strukturen. Die alten Griechen wußten bereits, dass es unendlich viele solcher Zahlen gibt. (Sie wußten es nicht nur, sie haben es bewiesen!)
Es war nicht einfach, weitere Fakten über Primzahlen zu beweisen. Ihre Folge ist einigermaßen gleichmäßig, weißt jedoch Lücken und Ballungsgebiete auf (siehe Bild 6.2). Wie groß sind diese Lücken? Gibt es eine Primzahl mit einer beliebig vorgegebenen Anzahl von Stellen? Die Antwort auf diese Frage wird für uns wichtig werden, wenn wir uns mit Kryptographie beschäftigen. Die Antwort lautet übrigens „ja“ . Diese Tatsache konnte allerdings erst Mitte des neunzehnten Jahrhunderts bewiesen werden und eine Menge ähnlicher Fragen sind selbst bis heute unbeantwortet.
Mit der Verbreitung der Computer kam auch für die Theorie der Primzahlen ein neuer Entwicklungsschub. Wie erkennt man, ob eine natürliche Zahl $n$ eine Primzahl ist? Selbstverständlich ist das ein endliches Problem (man kann alle kleineren natürlichen

1, ***2***, ***3***, 4, ***5***, 6, ***7***, 8, 9, 10, ***11***, 12, ***13***, 14, 15, 16, ***17***, 18, ***19***, 20, 21, 22, ***23***, 24, 25, 26, 27, 28, ***29***, 30, ***31***, 32, 33, 34, 35, 36, ***37***, 38, 39, 40, ***41***, 42, ***43***, 44, 45, 46, ***47***, 48, 49, 50, 51, 52, ***53***, 54, 55, 56, 57, 58, ***59***, 60, ***61***, 62, 63, 64, 65, 66, ***67***, 68, 69, 70, ***71***, 72, ***73***, 74, 75, 76, 77, 78, ***79***, 80, 81, 82, ***83***, 84, 85, 86, 87, 88, ***89***, 90, 91, 92, 93, 94, 95, 96, ***97***, 98, 99, 100, ***101***, 102, ***103***, 104, 105, 106, ***107***, 108, ***109***, 110, 111, 112, ***113***, 114, 115, 116, 117, 118, 119, 120, 121, 122, 123, 124, 125, 126, ***127***, 128, 129, 130, ***131***, 132, 133, 134, 135, 136, ***137***, 138, ***139***, 140, 141, 142, 143, 144, 145, 146, 147, 148, ***149***, 150, ***151***, 152, 153, 154, 155, 156, ***157***, 158, 159, 160, 161, 162, ***163***, 164, 165, 166, 167, 168, 169, 170, 171, 172, ***173***, 174, 175, 176, 177, 178, ***179***, 180, ***181***, 182, 183, 184, 185, 186, 187, 188, 189, 190, ***191***, 192, ***193***, 194, 195, 196, ***197***, 198, ***199***, 200, 201, 202, 203, 204, 205, 206, 207, 208, 209, 210, ***211***, 212, 213, 214, 215, 216, 217, 218, 219, 220, 221, 222, ***223***, 224, 225, 226, ***227***, 228, ***229***, 230, 231, 232, 233, 234, 235, 236, 237, 238, ***239***, 240, ***241***, 242, 243, 244, 245, 246, 247, 248, 249, 250, ***251***, 252, 253, 254, 255, 256, ***257***, 258, 259, 260, 261, 262, ***263***, 264, 265, 266, 267, 268, ***269***, 270, ***271***, 272, 273, 274, 275, 276, ***277***, 278, 279, 280, ***281***, 282, ***283***, 284, 285, 286, 287, 288, 289, 290, 291, 292, ***293***, 294, 295, 296, 297, 298, 299, 300, 301, 302, 303, 304, 305, 306, ***307***, 308, 309, 310, ***311***, 312, ***313***, 314, 315, 316, ***317***, 318, 319, 320, 321, 322, 323, 324, 325, 326, 327, 328, 329, 330, ***331***, 332, 333, 334, 335, 336, ***337***, 338, 339, 340, 341, 342, 343, 344, 345, 346, ***347***, 348, ***349***, 350, 351, 352, ***353***, 354, 355, 356, 357, 358, ***359***, 360, 361, 362, 363, 364, 365, 366, ***367***, 368, 369, 370, 371, 372, ***373***, 374, 375, 376, 377, 378, ***379***, 380, 381, 382, ***383***, 384, 385, 386, 387, 388, ***389***, 390, 391, 392, 393, 394, 395, 396, ***397***, 398, 399, 400, ***401***, 402, 403, 404, 405, 406, 407, 408, ***409***, 410, 411, 412, 413, 414, 415, 416, 417, 418, ***419***, 420, ***421***, 422, 423, 424, 425, 426, 427, 428, 429, 430, ***431***, 432, ***433***, 434, 435, 436, 437, 438, ***439***, 440, 441, 442, ***443***, 444, 445, 446, 447, 448, ***449***, 450, 451, 452, 453, 454, 455, 456, ***457***, 458, 459, 460, ***461***, 462, ***463***, 464, 465, 466, ***467***, 468, 469, 470, 471, 472, 473, 474, 475, 476, 477, 478, ***479***, 480, 481, 482, 483, 484, 485, 486, ***487***, 488, 489, 490, ***491***, 492, 493, 494, 495, 496, 497, 498, ***499***, 500

**Abbildung 6.1.** Die Primzahlen bis 500.

Zahlen ansehen und prüfen, ob sich ein echter Teiler von $n$ darunter befindet), aber solch einfache Vorgehensweisen werden ausgesprochen aufwendig und unpraktisch, sobald die Anzahl der Stellen mehr als etwa 20 beträgt.

Sehr viel effizientere Algorithmen (Computerprogramme) zur Untersuchung, ob eine gegebene Zahl eine Primzahl ist, gibt es erst seit 25 Jahren. Später werden wir noch einen Eindruck von diesen Methoden bekommen. Mit Hilfe dieser Methoden kann jetzt ziemlich leicht festgestellt werden, ob eine Zahl mit 1000 Stellen eine Primzahl ist oder nicht.

Ist eine ganze Zahl, größer als 1, selbst keine Primzahl, dann kann sie als Produkt von Primzahlen geschrieben werden: Wir können sie als Produkt zweier kleinerer natürlicher Zahlen schreiben. Ist eine dieser Zahlen keine Primzahl, so schreiben wir sie


**Abbildung 6.2.** Ein Strich-Diagramm der Primzahlen bis 1000.

als Produkt zweier kleinerer natürlicher Zahlen, etc.. Früher oder später haben wir nur noch Primzahlen. Die alten Griechen kannten (und bewiesen!) bereits eine schöne Eigenschaft dieser Darstellungsform, nämlich ihre *Eindeutigkeit*. Das bedeutet, es gibt keine weitere Möglichkeit, eine natürliche Zahl $n$ als Produkt von Primzahlen aufzuschreiben (natürlich ausgenommen, wir multiplizieren die Primzahlen in einer anderen Reihenfolge). Es bedarf einiger Raffinesse, dies zu beweisen (wie wir im nächsten Abschnitt sehen werden) und zu erkennen, dass ein solches Resultat wichtig ist, war schon eine große Leistung. All das ist jedoch bereits mehr als 2000 Jahre her!
Es ist wirklich überraschend, dass bis heute noch kein effizienter Weg bekannt ist, solche Zerlegungen zu *finden*. Selbstverständlich können unter Einsatz von leistungsstarken Supercomputern und gewaltigen parallelen Systemen Zerlegungen ziemlich großer Zahlen durch rohe Gewalt gefunden werden. Der derzeitige Rekord liegt bei rund 140 Stellen und die Schwierigkeit wächst sehr rasch (exponentiell) mit der Anzahl der Stellen. Die Primfaktorzerlegung einer gegebenen 400-stelligen Zahl mit einer der heute bekannten Methoden zu finden, liegt weit jenseits der Möglichkeiten, welche die Computer in absehbarer Zukunft bieten können.

6.3

## 6.3 Primfaktorzerlegung

Wie wir gesehen haben, kann jede natürliche Zahl, die größer als 1 und nicht selbst schon eine Primzahl ist, als Produkt von Primzahlen dargestellt werden. Wir können sogar sagen, *jede* natürliche Zahl kann als Produkt von Primzahlen geschrieben werden: Primzahlen kann man als „Produkt mit einem Faktor“ ansehen und wenn man möchte, kann man die Zahl 1 als „leeres Produkt“ betrachten. Behalten wir dies im Sinn, so können wir folgenden bereits angekündigten Satz, der manchmal auch als „Fundamentalsatz der Arithmetik“ bezeichnet wird, angeben und beweisen:

6.3.1 **Satz 6.3.1** Jede natürliche Zahl läßt sich als Produkt von Primzahlen darstellen, wobei diese Faktorisierung bis auf die Reihenfolge der Primfaktoren eindeutig ist.

**Beweis 6** Wir beweisen diesen Satz mit Hilfe einer Art der Induktion, die manchmal auch als das Argument des „kleinsten Verbrechers“ bezeichnet wird. Es ist ein indirekter Beweis: Wir nehmen an, die Behauptung sei falsch und nutzen diese Annahme, um einen Widerspruch abzuleiten.
Nehmen wir also an, es gibt eine natürliche Zahl mit zwei verschiedenen Primfaktorzerlegungen. Eine solche Zahl bezeichnen wir als „Verbrecher“ . Es gibt möglicherweise viele Verbrecher. Wir betrachten den *kleinsten* Verbrecher $n$. Ein Verbrecher zu sein bedeutet, mindestens zwei verschiedene Primfaktorzerlegungen zu besitzen:

$$n = p_1 \cdot p_2 \cdots p_m = q_1 \cdot q_2 \cdots q_k \,.$$

Wir können voraussetzen, dass $p_1$ die kleinste in diesen Faktorisierungen vorkommende Primzahl ist. (Falls notwendig, können wir die linke und rechte Seite vertauschen, so dass die kleinste Primzahl beider Faktorisierungen auf der linken Seite erscheint. Danach verändern wir die Reihenfolge der Faktoren auf der linken Seite, so dass der kleinste Faktor ganz vorne steht. In der Mathematik sprechen wir üblicherweise davon, dass wir „ohne Beschränkung der Allgemeinheit“ $p_1$ als kleinste Primzahl voraussetzen können.) Wir werden nun einen kleineren Verbrecher erzeugen, was dann zu einem Widerspruch führt, da wir annahmen, dass $n$ der kleinste war.
Die Zahl $p_1$ kann unter den Faktoren $q_i$ nicht vorkommen, denn sonst könnten wir beide Seiten durch $p_1$ teilen und einen kleineren Verbrecher erhalten.
Wir teilen jedes $q_i$ durch $p_1$ mit Rest: $q_i = p_1 a_i + r_i$, wobei $0 \leq r_i < p_1$. Wir wissen, dass $r_i \neq 0$ gilt, denn eine Primzahl kann kein Teiler einer anderen Primzahl sein.
Sei $n' = r_1 r_2 \cdots r_k$. Wir zeigen, dass $n'$ ein kleinerer Verbrecher ist. Trivialerweise gilt $r_i < p_1 < q_i$ und somit $n' = r_1 r_2 \cdots r_k < q_1 q_2 \cdots q_k = n$. Wir zeigen, dass $n'$ ebenfalls zwei verschiedene Primfaktorzerlegungen besitzt. Eine davon kann mit Hilfe der Definition von $n' = r_1 r_2 \cdots r_k$ erhalten werden. Die Faktoren müssen hier keine Primzahlen sein, aber wir können sie jeweils in Primfaktoren zerlegen, so dass wir schließlich eine Primfaktorzerlegung von $n'$ erhalten.
Um eine weitere Zerlegung zu bekommen, stellen wir wie folgt fest, dass $p_1 \mid n'$ gilt. Wir können die Definition von $n'$ in folgender Form schreiben:

$$n' = (q_1 - a_1 p_1)(q_2 - a_2 p_1) \cdots (q_k - a_k p_1).$$

Nachdem wir die Klammern aufgelöst haben, sehen wir, dass jeder Term durch $p_1$ teilbar ist. (Einer der Terme ist $q_1 q_2 \cdots q_k$. Dieser entspricht $n$ und ist daher durch $p_1$ teilbar. Alle anderen Terme enthalten $p_1$ als Faktor.) Nun teilen wir $n'$ durch $p_1$ und anschließend faktorisieren wir $n'/p_1$, um letztlich eine Faktorisierung von $n'$ zu erhalten.

Sind diese beiden Faktorisierungen denn tatsächlich unterschiedlich? Ja! Die Primzahl $p_1$ kommt nur in der zweiten vor. In der ersten kann sie nicht auftreten, da jeder Primfaktor kleiner als $p_1$ ist.
Folglich haben wir einen kleineren Verbrecher gefunden. Da wir annahmen, $n$ sei der kleinste Verbrecher, stellt dies einen Widerspruch dar. Die einzige Möglichkeit, diesen Widerspruch aufzulösen, besteht in der Folgerung, dass es keine Verbrecher gibt. Unsere „indirekte Annahme“ war falsch. Keine natürliche Zahl kann zwei verschiedene Primfaktorzerlegungen besitzen. □

---

**Übung 6.3.1** Lesen Sie die folgende Argumentation mit dem „kleinsten Verbrecher“ sorgfältig durch:

> BEHAUPTUNG: *Jede negative ganze Zahl ist ungerade.*
>
> BEWEIS: Nehmen wir umgekehrt an, dass es negative ganze Zahlen gibt, die gerade sind. Wir nennen diese Zahlen Verbrecher. Sei $n$ ein kleinster Verbrecher. Wir betrachten die Zahl $2n$. Sie ist kleiner als $n$ (man beachte, dass $n$ negativ ist!) und somit ein kleinerer Verbrecher. Da wir annahmen, dass $n$ der kleinste Verbrecher ist, stellt dies einen Widerspruch dar.

Diese Behauptung ist offensichtlich falsch. Wo liegt der Fehler im Beweis?

Als Anwendung des Satzes 6.3.1 beweisen wir eine Tatsache, die bereits den Pythagoräern (Schüler des großen griechischen Mathematikers und Philosophen Pythagoras) im sechsten Jahrhundert V. CHR. bekannt war.

---

6.3.2 **Satz 6.3.2** Die Zahl $\sqrt{2}$ ist irrational.

(Eine reelle Zahl ist *irrational*, wenn sie sich nicht als Bruch zweier ganzer Zahlen darstellen läßt. Für die Pythagoräer stellte sich folgende Frage in der Geometrie: Sie wollten wissen, ob die Diagonale eines Quadrats mit seiner Seite „meßbar“ ist, ob es also eine Strecke gibt, die in beiden ganzzahlig oft enthalten ist. Der obige Satz beantwortet diese Frage mit „nein“ , was einen erheblichen Tumult in den Reihen der Pythagoräer ausgelöst hat.)

---

**Beweis 7** Wir geben wiederum einen indirekten Beweis an: Wir nehmen an, $\sqrt{2}$ ist eine rationale Zahl und erhalten einen Widerspruch. Diese indirekte Annahme bedeutet, dass $\sqrt{2}$ als Quotient zweier positiver ganzer Zahlen dargestellt werden kann: $\sqrt{2} = a/b$. Durch beidseitiges Quadrieren und Umordnen erhalten wir $2b^2 = a^2$.
Wir betrachten nun die Primfaktorzerlegung beider Seiten und dabei insbesondere die Primzahl 2 auf beiden Seiten. Nehmen wir an, dass 2 in der Primfaktorzerlegung von $a$

genau $m$ mal vorkommt, während sie $n$ mal in der Primfaktorzerlegung von $b$ auftritt. Dann kommt sie $2m$ mal in der Primfaktorzerlegung von $a^2$ vor. Andererseits tritt sie $2n$ mal bei der Primfaktorzerlegung von $b^2$ auf und folglich $2n+1$ mal bei der Primfaktorzerlegung von $2b^2$. Da $2b^2 = a^2$ gilt und die Primfaktorzerlegung eindeutig ist, muss $2n+1 = 2m$ sein. Dies ist jedoch unmöglich, da $2n+1$ ungerade ist, während $2m$ eine gerade Zahl ist. Dieser Widerspruch zeigt, dass $\sqrt{2}$ irrational sein muss. □

**Übung 6.3.2** Gibt es irgendeine gerade Primzahl?

**Übung 6.3.3**

(a) Beweisen Sie: Wenn $p$ eine Primzahl ist, $a$ und $b$ gerade Zahlen sind und $p \mid ab$, dann gilt entweder $p \mid a$ oder $p \mid b$ (oder beides).

(b) Angenommen, $a$ und $b$ sind gerade Zahlen und $a \mid b$. Nehmen wir außerdem an, $p$ ist eine Primzahl und $p \mid b$, aber $p \nmid a$. Beweisen Sie, dass $p$ ein Teiler des Bruchs $b/a$ ist.

**Übung 6.3.4** Zeigen Sie, dass die Primfaktorzerlegung einer Zahl $n$ höchstens $\log_2 n$ Faktoren enthält.

**Übung 6.3.5** Sei $p$ eine Primzahl und $1 \leq a \leq p-1$. Wir betrachten die Zahlen $a, 2a, 3a, \ldots, (p-1)a$ und teilen jede davon durch $p$. Wir erhalten die Reste $r_1, r_2, \ldots, r_{p-1}$. Beweisen Sie, dass jede ganze Zahl von 1 bis $p-1$ *genau einmal* unter diesen Resten vorkommt.
[Hinweis: Beweisen Sie zuerst, dass kein Rest zweimal auftreten kann.]

**Übung 6.3.6** Beweisen Sie: Ist $p$ eine Primzahl, dann ist $\sqrt{p}$ irrational. Zeigen Sie etwas allgemeiner, dass $\sqrt{n}$ irrational ist, falls $n$ eine nicht-quadratische ganze Zahl ist.

**Übung 6.3.7** Versuchen Sie, einen noch allgemeineren Satz über die Irrationalität der Zahlen $\sqrt[k]{n}$ zu formulieren und zu beweisen.

## 6.4 Über die Menge der Primzahlen

6.4

Der folgende Satz war bereits Euclid im dritten Jahrhundert v. Chr. bekannt.

**Satz 6.4.1** Es gibt unendlich viele Primzahlen. 6.4.1

**Beweis 8** Wir müssen zeigen, dass es zu jeder natürlichen Zahl $n$ eine Primzahl gibt, die größer als $n$ ist. Um dies zu erreichen, betrachten wir die Zahl $n! + 1$ und davon einen beliebigen Primteiler $p$. Wir zeigen, dass $p > n$ gilt. Dazu verwenden wir abermals einen indirekten Beweis, indem wir $p \leq n$ annehmen und einen Widerspruch herleiten. Falls $p \leq n$, dann gilt $p \mid n!$, da $p$ dann eine der ganzen Zahlen ist, deren Produkt $n!$ bildet. Wir wissen außerdem, dass $p \mid n! + 1$ gilt und $p$ somit ein Teiler der Differenz $(n! + 1) - n! = 1$ sein muss. Dies ist jedoch unmöglich und folglich muss $p$ größer als $n$ sein. □

Betrachten wir viele verschiedene Diagramme und Tabellen von Primzahlen, so erhalten wir hauptsächlich einen Eindruck ihrer starken Unregelmäßigkeit. In Bild 6.2 wird beispielsweise jede Primzahl bis 1000 durch einen Balken dargestellt. Es treten große „Lücken“ zwischen Primzahlen auf, aber es gibt auch welche, die sehr dicht beisammen liegen. Wir können zeigen, dass die Lücken immer größer werden, um so größer die betrachteten Zahlen werden. Es gibt irgendwo einen String mit 100 aufeinander folgenden zusammengesetzten Zahlen. An anderer Stelle (sehr viel weiter weg) gibt es einen String mit 1000 aufeinander folgenden zusammengesetzten Zahlen, etc.. Wir geben dies in folgender mathematischer Ausdrucksweise an:

**6.4.2** **Satz 6.4.2** Zu jeder natürlichen Zahl $k$ existieren $k$ aufeinander folgende zusammengesetzte Zahlen.

**Beweis 9** Wir können diesen Satz mit einer Argumentation beweisen, die derjenigen des Beweises von Satz 6.4.1 recht ähnlich ist. Sei $n = k+1$. Wir betrachten die Zahlen

$$n! + 2,\ n! + 3,\ \ldots,\ n! + n.$$

Kann eine dieser Zahlen eine Primzahl sein? Die Antwort lautet „nein“ : Die erste Zahl ist gerade, da $n!$ und 2 beide gerade sind. Die zweite Zahl ist durch 3 teilbar, da $n!$ und 3 beide durch 3 ($n > 2$ vorausgesetzt) teilbar sind. Allgemein ist $n! + i$ für alle $i = 2, 3, \ldots, n$ durch $i$ teilbar. Diese Zahlen können daher keine Primzahlen sein und wir haben $n - 1 = k$ aufeinander folgende zusammengesetzte Zahlen gefunden. □

Was können wir zur entgegengesetzten Frage sagen, nämlich Primzahlen zu finden, die sehr dicht beisammen liegen. Alle Primzahlen mit Ausnahme der 2 sind ungerade, daher beträgt die Differenz zwischen zwei Primzahlen mindestens zwei, ausgenommen bei 2 und 3. Zwei Primzahlen, deren Differenz 2 beträgt, werden *Primzahlzwillinge* genannt. Somit sind $(3, 5)$, $(5, 7)$, $(11, 13)$, $(17, 19)$ Primzahlzwillinge. Betrachten wir die Tabelle der Primzahlen bis 500, so finden wir eine Menge Primzahlzwillin-

ge. Umfangreiche Berechnungen zeigen, dass es Primzahlzwillinge mit hunderten von Stellen gibt. Trotzdem ist bisher nicht bekannt, ob es unendlich viele Primzahlzwillinge gibt! (Sehr wahrscheinlich gibt es unendlich viele. Aber trotz der Bemühungen vieler Mathematiker in mehr als 2000 Jahren konnte bisher noch kein Beweis dafür erbracht werden!)
Eine andere Möglichkeit, Satz 6.4.2 umzudrehen, besteht in der Frage nach der möglichen Größe der Lücken in Relation zu ihrer Lage auf der Zahlengeraden. Könnte es passieren, dass es überhaupt keine Primzahl mit beispielsweise 100 Stellen gibt? Dies ist wiederum eine sehr schwierige Frage, aber wir wissen deren Antwort. (Nein, das kann nicht passieren.)

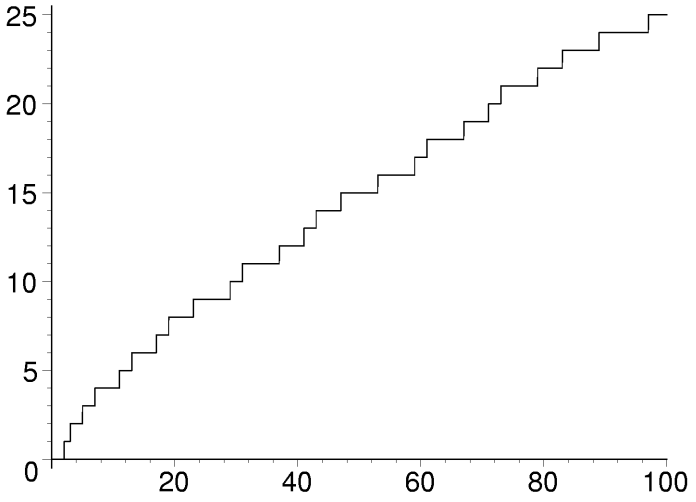


**Abbildung 6.3.** Der Graph von $\pi(n)$ von 1 bis 100.

Eine der wichtigsten Fragen zu den Primzahlen lautet: Wie viele Primzahlen gibt es bis zu einer vorgegebenen Zahl $n$? Wir bezeichnen die Anzahl der Primzahlen bis $n$ mit $\pi(n)$. Bild 6.3 stellt den Graph dieser Funktion im Bereich von 1 bis 100 dar und Bild 6.4 zeigt den Bereich von 1 bis 2000. Wir sehen, dass die Funktion einigermaßen sanft wächst und ihre Steigung nur langsam etwas abnimmt. Es ist sicherlich unmöglich, eine exakte Formel für $\pi(n)$ zu erhalten. Um 1900 wurde ein sehr wichtiges Ergebnis durch Hadamard und de la Vallée Poussin bewiesen. Es wird als *Primzahlsatz* bezeichnet.

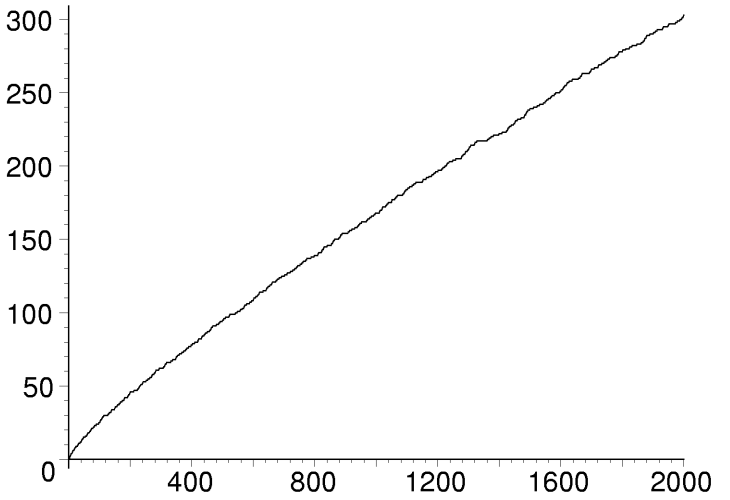


**Abbildung 6.4.** Der Graph von $\pi(n)$ von 1 bis 2000.

**6.4.3** **Satz 6.4.3 (Der Primzahlsatz)** Sei die Anzahl der Primzahlen unter $1, 2, \ldots, n$ mit $\pi(n)$ bezeichnet, dann gilt

$$\pi(n) \sim \frac{n}{\ln n}.$$

($\ln n$ meint hier den „natürlichen Logarithmus“ , d.h. den Logarithmus zur Basis $e = 2,718281\ldots$. Man sollte sich darüber im Klaren sein, dass diese Notation bedeutet, der Quotient

$$\pi(n) \Big/ \frac{n}{\ln n}$$

nähert sich beliebig dicht der 1, wenn $n$ entsprechend groß wird.)

Der Beweis des Primzahlsatzes ist sehr schwierig. Die Tatsache, dass die Anzahl der Primzahlen bis $n$ ungefähr $n/\ln n$ entspricht, wurde auf empirischem Weg bereits im achtzehnten Jahrhundert festgestellt. Allerdings dauerte es mehr als 100 Jahre, bevor er 1896 durch Hadamard und de la Vallée Poussin bewiesen wurde.
Um den Nutzen dieses Satzes zu demonstrieren, beschäftigen wir uns mit der Beantwortung der in der Einleitung gestellten Frage: Wie viele Primzahlen mit (sagen wir) 200 Stellen gibt es? Wir erhalten die Antwort durch Subtraktion der Anzahl der Primzahlen bis $10^{199}$ von der Anzahl der Primzahlen bis $10^{200}$. Nach dem Primzahlsatz

beträgt diese Anzahl ungefähr

$$\frac{10^{200}}{200\ln 10} - \frac{10^{199}}{199\ln 10} \approx 1,95 \cdot 10^{197}.$$

Das sind eine Menge Primzahlen! Verglichen mit der Gesamtzahl aller natürlichen 200-stelligen Zahlen, von denen wir wissen, dass es $10^{200} - 10^{199} = 9 \cdot 10^{199}$ gibt, erhalten wir

$$\frac{9 \cdot 10^{199}}{1,95 \cdot 10^{197}} \approx 460.$$

Unter den 200-stelligen natürlichen Zahlen ist demnach jede 460. Zahl eine Primzahl.

(Warnung: Diese Argumentation ist ungenau. Wir haben im Primzahlsatz nämlich nur behauptet, $\pi(n)$ liegt dicht bei $n/\ln n$, falls $n$ hinreichend groß ist. Es ist möglich, genauere Angaben hinsichtlich der Größe von $n$ zu machen, damit der Fehler geringer als zum Beispiel ein Prozent ausfällt. Dies führt jedoch zu noch schwierigeren Fragen, die selbst bis heute noch nicht vollständig beantwortet sind.)

Es gibt eine Menge weiterer einfacher Beobachtungen, die man bei der Betrachtung von Primzahltafeln machen kann. Sie neigen jedoch dazu, sich sehr schwer beweisen zu lassen und die meisten sind selbst bis heute noch unbewiesen - in manchen Fällen sogar nach 2500-jährigen Bemühungen. Das Problem der Primzahlzwillinge haben wir bereits erwähnt. Ein weiteres berühmtes ungelöstes Problem ist die *Goldbachsche Vermutung*. Diese besagt, *jede gerade natürliche Zahl, größer als 2, kann als Summe zweier Primzahlen dargestellt werden.* Goldbach hat außerdem auch noch eine Vermutung zu ungeraden Zahlen aufgestellt: *Jede natürliche Zahl, größer als 5, kann als Summe dreier Primzahlen dargestellt werden.* Diese zweite Vermutung wurde von Vinogradov in den dreißiger Jahren des 20. Jahrhunderts mit Hilfe sehr tiefgehender Methoden im Wesentlichen bewiesen. Wir sagten „im Wesentlichen“ , da der Beweis nur für sehr große Zahlen funktioniert und es möglicherweise endlich viele Ausnahmen gibt.
Nehmen wir an, wir haben eine ganze Zahl $n$ und möchten wissen, wie bald wir nach $n$ auf jeden Fall eine Primzahl finden. Wie groß oder klein ist zum Beispiel die erste Primzahl, die mindestens 100 Stellen besitzt? In unserem Beweis zur Unendlichkeit der Primzahlen wird gezeigt, dass es zu jedem $n$ eine Primzahl zwischen $n$ und $n! + 1$ gibt. Dies ist eine sehr schwache Aussage. Sie besagt zum Beispiel, dass es eine Primzahl zwischen 10 und $10! + 1 = 3.628.801$ gibt. Dabei ist die nächste Primzahl selbstverständlich 11. Der russische Mathematiker P.L. Chebyshev bewies Mitte des neunzehnten Jahrhunderts, dass zwischen $n$ und $2n$ immer eine Primzahl liegt. Inzwischen wurde bewiesen, dass es zwischen zwei aufeinander folgenden Kubikzahlen immer eine Primzahl gibt (z.B. zwischen $10^3 = 1000$ und $11^3 = 1331$). Ein weiteres altes, berühmtes, bisher jedoch ungelöstes Problem besteht in der Frage, ob es zwischen zwei aufeinander folgenden Quadratzahlen immer eine

Primzahl gibt. (Versuchen Sie es: Sie werden in der Tat sehr viele Primzahlen finden. Wir finden zum Beispiel zwischen $100 = 10^2$ und $121 = 11^2$ die Primzahlen 101, 103, 107, 109, 113. Zwischen $100^2 = 10.000$ und $101^2 = 10.201$ finden wir 10.007, 10.009, 10.037, 10.039, 10.061, 10.067, 10.069, 10.079, 10.091, 10.093, 10.099, 10.103, 10.111, 10.133, 10.139, 10.141, 10.151, 10.159, 10.163, 10.169, 10.177, 10.181, 10.193.)

**Übung 6.4.1** Zeigen Sie, dass unter allen $k$-stelligen Zahlen ungefähr jede $2, 3k.$ Zahl eine Primzahl ist.

6.5

## 6.5 Fermats „kleiner“ Satz

**Abbildung 6.5.** Pierre de Fermat

Primzahlen sind wichtig, da wir aus ihnen alle positiven ganzen Zahlen bilden können. Es zeigt sich jedoch, dass sie auch eine Menge weiterer, oft überraschender Eigenschaften besitzen. Eine davon wurde durch den französischen Mathematiker Pierre de Fermat (1601–1655) entdeckt. Sie wird heute der „kleine“ Satz von Fermat genannt.

6.5.1 **Satz 6.5.1:** *Satz von Fermat* Ist $p$ eine Primzahl und $a$ eine ganze Zahl, dann gilt $p \mid a^p - a$.

Bevor wir diesen Satz beweisen, möchten wir noch erwähnen, dass er häufig auch in folgender Form angegeben wird: *Ist $p$ eine Primzahl und $a$ eine ganze, nicht durch $p$*

*teilbare Zahl, dann gilt*

$$p \mid a^{p-1} - 1. \tag{37}$$

Die Tatsache, dass diese beiden Behauptungen äquivalent sind (im Sinne von: Wenn wir wissen, dass eine der Behauptungen wahr ist, können wir die andere leicht beweisen.), wird dem Leser als Übungsaufgabe 6.10.20 überlassen.
Zum Beweis von Fermats Satz benötigen wir ein Lemma, in dem eine weitere Teilbarkeitseigenschaft von Primzahlen (die aber leichter zu beweisen ist) angegeben wird:

**Lemma 6.5.1** Ist $p$ eine Primzahl und $0 < k < p$, dann gilt $p \mid \binom{p}{k}$. **6.5.1**

**Beweis 10** Wir wissen nach Satz 1.8.1, dass

$$\binom{p}{k} = \frac{p(p-1)\cdots(p-k+1)}{k(k-1)\cdots 1}$$

gilt. Der Zähler wird hier von $p$ geteilt, nicht jedoch der Nenner, da alle Faktoren des Nenners kleiner als $p$ sind und wir durch Übungsaufgabe 6.3.3(a) wissen, dass eine Primzahl $p$, die keinen der Faktoren teilt, auch das ganze Produkt nicht teilt. Es folgt daher (siehe Übungsaufgabe 6.3.3(b)), dass $p$ ein Teiler von $\binom{p}{k}$ ist. □

**Beweis 11:** *(von Satz 6.5.1)* Wir können nun Fermats Satz durch Induktion nach $a$ beweisen. Es reicht aus, die Behauptung für nicht-negative $a$ zu zeigen, da $(-a)^p - (-a) = -(a^p - a)$ für ungerade Primzahlen $p$ gilt und die Aussage für $p = 2$ sowieso klar ist.
Die Behauptung gilt trivialerweise, falls $a = 0$. Es sei nun $a > 0$ und wir schreiben $a = b + 1$. Dann gilt

$$\begin{aligned} a^p - a &= (b+1)^p - (b+1) \\ &= b^p + \binom{p}{1} b^{p-1} + \cdots + \binom{p}{p-1} b + 1 - b - 1 \\ &= (b^p - b) + \binom{p}{1} b^{p-1} + \cdots + \binom{p}{p-1} b. \end{aligned}$$

Der Ausdruck $(b^p - b)$ ist hier nach Induktionsvoraussetzung durch $p$ teilbar, während die anderen Terme nach Lemma 6.5.1 durch $p$ teilbar sind. Es folgt, dass $a^p - a$ ebenfalls durch $p$ teilbar ist, was die Induktion vervollständigt. □

Wir machen nun einen kurzen Ausflug in die Geschichte der Mathematik. Fermat ist besonders wegen seines „letzten“ Satzes bekannt. Dieser besteht aus folgender Aussage:

*Ist $n > 2$, dann ist die Summe der $n$-ten Potenzen zweier natürlicher Zahlen niemals die $n$-te Potenz einer natürlichen Zahl.*

(Die Voraussetzung $n > 2$ ist unumgänglich: Es gibt Beispiele, bei denen die Summe zweier Quadratzahlen eine dritte Quadratzahl ergibt. Zum Beispiel $3^2 + 4^2 = 5^2$ oder $5^2 + 12^2 = 13^2$. Es gibt sogar unendlich viele solcher Tripel aus Quadratzahlen, siehe Übungsaufgabe 6.6.7.)
Fermat behauptete in einer Notiz, dass er seinen Satz bewiesen hätte, schrieb den Beweis dafür jedoch niemals nieder. Die Aussage seines Satzes war das wohl berühmteste ungelöste Problem in der Mathematik bis es 1995 schließlich von Andrew Wiles (bei einem Teil mit Hilfe von Robert Taylor) bewiesen wurde.

---

**Übung 6.5.1** Zeigen Sie anhand von Beispielen, dass weder die Behauptung in Lemma 6.5.1, noch Fermats „kleiner“ Satz gültig bleiben, wenn wir die Voraussetzung, dass $p$ eine Primzahl ist, fallen lassen.

---

**Übung 6.5.2** Wir betrachten ein reguläres $p$-Gon und alle $k$-Teilmengen seiner Eckenmenge für ein festgelegtes $k$ ($1 \leq k \leq p-1$). Diese $k$-Teilmengen werden alle in eine Anzahl von Schubfächern getan: Wir geben zwei $k$-Teilmengen in dasselbe Schubfach, wenn sie durch Rotation ineinander überführt werden können. Somit gehören zum Beispiel alle $k$-Teilmengen, die aus $k$ aufeinander folgenden Ecken bestehen, in dasselbe Schubfach.

(a) Beweisen Sie: Ist $p$ eine Primzahl, dann wird jedes Schubfach genau $p$ dieser gedrehten Kopien enthalten.

(b) Zeigen Sie anhand eines Beispiels, dass (a) nicht gültig bleibt, wenn wir die Voraussetzung, dass $p$ eine Primzahl ist, fallen lassen.

(c) Verwenden Sie (a), um einen neuen Beweis von Lemma 6.5.1 anzugeben.

---

**Übung 6.5.3** Man stelle sich zur Basis $a$ geschriebene Zahlen vor, die höchstens $p$ Stellen enthalten. Zwei Zahlen sollen in ein Schubfach getan werden, wenn sie durch einen zyklischen Shift auseinander hervorgehen. Wie viele werden in jeder Klasse sein? Geben Sie auf diese Weise einen neuen Beweis für Fermats Satz an.

---

**Übung 6.5.4** Geben Sie einen dritten auf Übungsaufgabe 6.3.5 gestützten Beweis für Fermats „kleinen“ Satz an.
[Hinweis: Betrachten Sie das Produkt $a(2a)(3a)\cdots((p-1)a)$.]

## 6.6 Der euklidische Algorithmus



Bisher haben wir mehrere Bezeichnungen und Ergebnisse bezüglich ganzer Zahlen behandelt. Nun wenden wir uns der Frage zu, wie wir Berechnungen hinsichtlich dieser Ergebnisse durchführen können. Wie entscheiden wir, ob eine gegebene Zahl eine Primzahl ist oder nicht? Wie bestimmen wir die Primfaktorzerlegung einer Zahl?
Wir können dabei die Grundrechenarten – Addition, Subtraktion, Multiplikation, Division mit Rest – effektiv nutzen. Dies werden wir hier jedoch nicht behandeln.
Der Schlüssel zu etwas weitergehender algorithmischer Zahlentheorie ist ein Algorithmus, der den *größten gemeinsamen Teiler* zweier natürlicher Zahlen $a$ und $b$ berechnet. Dieser ist definiert als die größte natürliche Zahl, die sowohl ein Teiler von $a$ als auch von $b$ ist. (Da 1 immer ein gemeinsamer Teiler ist und kein Teiler größer als die beiden Zahlen sein kann, ergibt diese Definition durchaus einen Sinn: Mindestens ein gemeinsamer Teiler ist immer vorhanden und in der Menge der gemeinsamen Teiler muss ein größtes Element vorhanden sein.) Der größte gemeinsame Teiler von $a$ und $b$ wird mit $\mathrm{ggT}(a,b)$ bezeichnet. Also gilt

$$\mathrm{ggT}(1,6)=1, \qquad \mathrm{ggT}(2,6)=2, \qquad \mathrm{ggT}(3,6)=3,$$

$$\mathrm{ggT}(4,6)=2, \qquad \mathrm{ggT}(5,6)=1, \qquad \mathrm{ggT}(6,6)=6.$$

Wir bezeichnen zwei ganze Zahlen als *teilerfremd*, wenn ihr größter gemeinsamer Teiler 1 ist. Es wird sich als nützlich erweisen, $\mathrm{ggT}(a,0)=a$ für alle $a\geq 0$ zu definieren.
Recht ähnlich geartet ist der Begriff des *kleinsten gemeinsamen Vielfachen* zweier natürlicher Zahlen. Es handelt sich dabei um die kleinste natürliche Zahl, die ein Vielfaches beider Zahlen ist. Sie wird als $\mathrm{kgV}(a,b)$ bezeichnet. Es gilt zum Beispiel

$$\mathrm{kgV}(1,6)=6, \qquad \mathrm{kgV}(2,6)=6, \qquad \mathrm{kgV}(3,6)=6,$$

$$\mathrm{kgV}(4,6)=12, \qquad \mathrm{kgV}(5,6)=30, \qquad \mathrm{kgV}(6,6)=6.$$

Der größte gemeinsame Teiler zweier natürlicher Zahlen kann recht einfach mit Hilfe ihrer Primfaktorzerlegungen ermittelt werden: Man betrachte die gemeinsamen Primfaktoren, potenziere jeden mit dem kleineren der beiden Exponenten und berechne das Produkt dieser Primzahlpotenzen. Es gilt zum Beispiel $900=2^2\cdot 3^2\cdot 5^2$ und $54=2\cdot 3^3$ und somit $\mathrm{ggT}(900,54)=2\cdot 3^2=18$.
Das Problem dieser Methode besteht darin, dass die Bestimmung der Primfaktorzerlegung bei großen Zahlen sehr schwierig wird. Der Algorithmus, den wir in diesem Abschnitt behandeln werden, wird den größten gemeinsamen Teiler zweier natürlicher Zahlen sehr viel schneller ermitteln, ohne die jeweilige Primfaktorzerlegung vorher zu bestimmen. Dieser Algorithmus ist ein wichtiger Bestandteil fast aller Algorithmen, die Berechnungen mit ganzen Zahlen mit sich bringen. (Und, wie wir schon anhand

des Namens erkennen können, geht er auf den großen griechischen Mathematiker Euklid zurück!)

---

**Übung 6.6.1** Zeigen Sie:
Sind $a$ und $b$ natürliche Zahlen mit $a \mid b$, dann gilt $\mathrm{ggT}(a,b) = a$.

---

**Übung 6.6.2**
(a)Beweisen Sie $\mathrm{ggT}(a,b) = \mathrm{ggT}(a, b-a)$.
(b)Sei $r$ der Rest beim Teilen von $b$ durch $a$, dann gilt $\mathrm{ggT}(a,b) = \mathrm{ggT}(a,r)$.

---

**Übung 6.6.3** Beweisen Sie:
(a)Ist $a$ gerade und $b$ ungerade, dann gilt $\mathrm{ggT}(a,b) = \mathrm{ggT}(a/2, b)$.
(b)Sind $a$ und $b$ beide gerade, dann gilt $\mathrm{ggT}(a,b) = 2\mathrm{ggT}(a/2, b/2)$.

---

**Übung 6.6.4** Wie kann man das kleinste gemeinsame Vielfache zweier ganzer Zahlen ausdrücken, wenn die Primfaktorzerlegung beider Zahlen bekannt ist?

---

**Übung 6.6.5** Angenommen, es sind zwei ganze Zahlen gegeben, wobei die Primfaktorzerlegung einer dieser Zahlen bekannt ist. Man beschreibe eine Möglichkeit, den größten gemeinsamen Teiler dieser beiden Zahlen zu berechnen.

---

**Übung 6.6.6** Beweisen Sie, dass für zwei beliebige ganze Zahlen $a$ und $b$ gilt:

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

---

**Übung 6.6.7** Drei natürliche Zahlen $a$, $b$ und $c$ bilden ein *pythagoreisches Zahlentripel*, falls $a^2 + b^2 = c^2$ gilt.
(a)Man wähle drei natürliche Zahlen $x$, $y$ und $z$ und es sei $a = 2xyz$, $b = \left(x^2 - y^2\right)z$, $c = \left(x^2 + y^2\right)z$. Prüfen Sie, ob $(a,b,c)$ ein pythagoreisches Zahlentripel ist.
(b)Zeigen Sie, dass alle pythagoreischen Zahlentripel auf diese Art entstehen: Sind $a, b, c$ natürliche Zahlen, für die $a^2 + b^2 = c^2$ gilt, dann gibt es andere natürliche Zahlen $x$, $y$ und $z$, so dass $a$, $b$ und $c$ durch die oben angegebenen Formeln ausgedrückt werden können.
[Hinweis: Zeigen Sie zuerst, dass sich das Problem auf den Fall reduzieren läßt, bei dem $\mathrm{ggT}(a,b,c) = 1$ gilt und $a$ gerade, sowie $b$ und $c$ ungerade sind. Anschließend schreibe man $a^2 = (b-c)(b+c)$ und nutze dies, um festzustellen, dass $(b+c)/2$ und $(b-c)/2$ Quadratzahlen sind.]

Nun wenden wir uns dem euklidischen Algorithmus zu. Er basiert auf zwei einfachen Tatsachen, die uns bereits durch die Übungsaufgaben 6.6.1 und 6.6.2 bekannt sind.
Angenommen, es sind zwei natürliche Zahlen $a$ und $b$ gegeben und wir möchten ihren größten gemeinsamen Teiler finden. Wir tun folgendes:

1. Ist $a > b$, dann vertausche $a$ und $b$.
2. Ist $a > 0$, dann teile $b$ durch $a$, um einen Rest $r$ zu erhalten. Ersetze $b$ durch $r$ und kehre zu 1. zurück.
3. Oder (falls $a = 0$), dann ist $b$ der ggT und man beende den Vorgang.

Führen wir den Algorithmus durch, insbesondere per Hand, dann gibt es keinen Grund, $a$ und $b$ zu vertauschen, wenn $a < b$ ist: Wir teilen einfach die größere durch die kleinere Zahl (mit Rest) und ersetzen die größere durch den Rest, falls dieser ungleich 0 ist. Nun führen wir einige Beispiele durch.

$$\begin{aligned}
\mathrm{ggT}(300, 18) &= \mathrm{ggT}(12, 18) = \mathrm{ggT}(12, 6) = 6.\\
\mathrm{ggT}(101, 100) &= \mathrm{ggT}(1, 100) = 1.\\
\mathrm{ggT}(89, 55) &= \mathrm{ggT}(34, 55) = \mathrm{ggT}(34, 21) = \mathrm{ggT}(13, 21) = \mathrm{ggT}(13, 8)\\
&= \mathrm{ggT}(5, 8) = \mathrm{ggT}(5, 3) = \mathrm{ggT}(2, 3) = \mathrm{ggT}(2, 1) = 1.
\end{aligned}$$

Man kann in jedem der Fälle nachprüfen, dass das Ergebnis tatsächlich der größte gemeinsame Teiler ist (indem man die Primfaktorzerlegung der Zahlen verwendet).
Das erste, worüber wir uns bei der Beschreibung eines Algorithmus Gedanken machen müssen, ist die Frage, ob er überhaupt irgendwann abbricht. Warum ist der euklidische Algorithmus endlich? Das ist einfach: Die Zahlen steigen niemals an, denn eine von ihnen wird jedesmal kleiner, wenn Schritt 2 ausgeführt wird und der Rest ist nichtnegativ. Der ganze Prozess kann also nicht unendlich lange andauern.
Dann müssen wir uns natürlich vergewissern, dass der Algorithmus auch das Gewünschte liefert. Das ist zweifellos der Fall: In Schritt 1 (Vertauschen der Zahlen) wird der größte gemeinsame Teiler selbstverständlich nicht verändert. Schritt 2 (Ersetzen der größeren Zahl durch den Rest bei der Division) ändert nach Übungsaufgabe 6.6.2(b) den größten gemeinsamen Teiler ebenfalls nicht. Und wenn wir in Schritt 3 anhalten, ist die ermittelte Zahl nach Übungsaufgabe 6.6.1 in der Tat der größte gemeinsame Teiler der beiden aktuellen Zahlen.
Man sollte sich bei der Entwicklung eines Algorithmus auch noch eine dritte etwas subtilere Frage stellen: Wie lange dauert der Prozess? Wie viele Schritte werden vor dem Abbruch ausgeführt? Die Argumentation, mit der wir gezeigt haben, dass der Prozess endlich ist, liefert uns auch eine Schranke für dessen Dauer: Da bei jeder Ausführung der aus Schritt 1 und 2 bestehenden Schleife eine der beiden Zahlen kleiner wird, hält der Prozess auf jeden Fall nach weniger als $a+b$ Wiederholungen an. Das ist allerdings wirklich keine gute Schranke: Wenn wir den euklidischen Algorithmus bei zwei 100-stelligen Zahlen anwenden, dann besagt die Schranke von $a+b$, dass er nicht

länger als $2 \cdot 10^{100}$ Schritte dauert. Dies ist eine astronomisch hohe Zahl und damit unbrauchbar. Glücklicherweise ist dies jedoch nur eine obere Schranke, zumal die pessimistischste. Unsere angeführten Beispiele scheinen zu zeigen, dass der Algorithmus sehr viel schneller abbricht.
Die Beispiele lassen allerdings auch erkennen, dass diese Frage ziemlich heikel ist. Wir sehen, dass die Länge des euklidischen Algorithmus in Abhängigkeit der behandelten Zahlen ziemlich schwanken kann. Einige Beobachtungen, die man bei der Betrachtung der Beispiele machen kann, kommen auch in den folgenden Übungsaufgaben vor.

**Übung 6.6.8** Zeigen Sie, dass der euklidische Algorithmus für beliebig große natürliche Zahlen in zwei Schritten beendet sein kann, selbst wenn ihr ggT gleich 1 ist.

**Übung 6.6.9** Beschreiben Sie den auf zwei aufeinander folgende Fibonacci Zahlen angewendeten euklidischen Algorithmus. Nutzen Sie diese Beschreibung, um zu zeigen, dass der euklidische Algorithmus beliebig viele Schritte haben kann.

Was *können* wir über die Dauer des euklidischen Algorithmus aussagen? Der Schlüssel zur Antwort liegt in folgendem Lemma:

6.6.1 **Lemma 6.6.1** Während der Ausführung des euklidischen Algorithmus fällt das Produkt der zwei aktuellen Zahlen bei jeder Iteration um mindestens den Faktor 2.

**Beweis 12** Um dies einzusehen, betrachten wir den Schritt, bei dem das Paar $(a, b)$ ($a < b$) durch das Paar $(r, a)$ ersetzt wird (man entsinne sich, $r$ ist der Rest bei der Division von $b$ durch $a$). Dann haben wir $r < a$ und $a + r \leq b$. Infolgedessen gilt $b \geq a + r > 2r$ und somit $ar < \frac{1}{2}ab$, wie behauptet wurde. □

Nehmen wir an, dass wir den euklidischen Algorithmus bei zwei Zahlen $a$ und $b$ anwenden und $k$ Schritte davon ausführen. Das Produkt der zwei nach $k$ Schritten aktuellen Zahlen beträgt nach Lemma 6.6.1 höchstens $ab/2^k$. Da dies eine natürliche Zahl und damit mindestens 1 ist, erhalten wir

$$ab \geq 2^k,$$

und daher

$$k \leq \log_2(ab) = \log_2 a + \log_2 b.$$

Dadurch haben wir folgendes bewiesen:

**Satz 6.6.1** Die Anzahl der Schritte des auf zwei natürliche Zahlen angewendeten euklidischen Algorithmus beträgt höchstens $\log_2 a + \log_2 b$. **6.6.1**

In der oberen Schranke für die Anzahl der Schritte haben wir die Summe der Zahlen durch die Summe der Logarithmen dieser Zahlen ersetzt. Dies stellt eine erhebliche Verbesserung dar. Zum Beispiel beträgt die Anzahl der Iterationsschritte bei der Berechnung des größten gemeinsamen Teilers zweier 300-stelliger Zahlen weniger als $2\log_2 10^{300} = 600\log_2 10 < 2000$. Erheblich weniger als $2 \cdot 10^{300}$, unsere erste naive Abschätzung! Bemerkenswert ist die Tatsache, dass $\log_2 a$ kleiner als die Anzahl der Bits von $a$ ist (wenn $a$ zur Basis 2 geschrieben ist). Wir können daher feststellen, dass der euklidische Algorithmus nicht mehr Iterationsschritte benötigt als die Anzahl der Bits, die beim Aufschreiben der Zahlen zur Basis 2 erforderlich sind.
Der obige Satz liefert uns lediglich eine obere Schranke für die Anzahl der Iterationsschritte, die der euklidische Algorithmus benötigt. Wir können Glück haben und es geht viel schneller. Wenn wir den euklidischen Algorithmus zum Beispiel auf zwei aufeinander folgende Zahlen anwenden, braucht er lediglich einen einzigen Schritt. Es kann jedoch auch passieren, dass nicht viel weniger Schritte benötigt werden als die durch die obere Schranke gegebene Anzahl. Falls Sie Übungsaufgabe 6.6.9 gelöst haben, konnten Sie feststellen, dass der euklidische Algorithmus $k-1$ Schritte braucht, wenn man ihn auf zwei aufeinander folgende Fibonacci Zahlen $F_k$ und $F_{k+1}$ anwendet. Andererseits liefert das obige Lemma die Schranke

$$\log_2 F_k + \log_2 F_{k+1} \approx \log_2 \left( \frac{1}{\sqrt{5}} \left( \frac{1+\sqrt{5}}{2} \right)^k \right) + \log_2 \left( \frac{1}{\sqrt{5}} \left( \frac{1+\sqrt{5}}{2} \right)^{k+1} \right)$$

$$= -\log_2 5 + (2k+1)\log_2 \left( \frac{1+\sqrt{5}}{2} \right) \approx 1,388k - 1,628,$$

und wir haben die Anzahl der Schritte daher lediglich um einen Faktor von ungefähr 1,388 oder weniger als 40% überschätzt.
Fibonacci Zahlen liefern nicht nur gute Beispiele großer Zahlen, anhand derer wir die Arbeitsweise des euklidischen Algorithmus betrachten können, sondern sie sind auch sehr hilfreich, um eine noch bessere Schranke für die Anzahl der Iterationsschritte zu ermitteln. Wir geben das Ergebnis in Form einer Übungsaufgabe an. Sie beinhaltet in gewissem Sinne die Aussage, dass der euklidische Algorithmus bei zwei aufeinander folgenden Fibonacci Zahlen am längsten braucht.

**Übung 6.6.10** Angenommen, es gilt $a < b$ und der auf $a$ und $b$ angewendete euklidische Algorithmus benötigt $k$ Schritte. Beweisen Sie, dass $a \geq F_k$ und $b \geq F_{k+1}$.

**Übung 6.6.11** Man betrachte folgende Version des euklidischen Algorithmus, um $\mathrm{ggT}(a, b)$ zu berechnen: (1) Falls nötig, vertausche die Zahlen, um $a \leq b$ zu erhalten; (2) Falls $a = 0$, dann gebe die Zahl $b$ zurück; (3) Falls $a \neq 0$, dann ersetze $b$ durch $b - a$ und gehe zu (1).

(a) Führen Sie diesen Algorithmus aus, um $\mathrm{ggT}(19, 2)$ zu berechnen.

(b) Zeigen Sie, dass dieser modifizierte euklidische Algorithmus immer mit dem korrekten Ergebnis endet.

(c) Wie lange braucht dieser Algorithmus im schlimmsten Fall, wenn er auf zwei 100-stellige ganze Zahlen angewandt wird?

**Übung 6.6.12** Man betrachte folgende Version des euklidischen Algorithmus, um $\mathrm{ggT}(a, b)$ zu berechnen. Beginnen Sie damit, die größte Potenz von 2 zu berechnen, die sowohl $a$ als auch $b$ teilt. Ist dies $2^r$, dann teilen Sie $a$ und $b$ durch $2^r$. Nach diesen „Vorarbeiten“ tun sie folgendes:

(1) Falls nötig, vertausche die Zahlen, um $a \leq b$ zu erhalten.

(2) Falls $a \neq 0$, dann bestimme die Paritäten von $a$ und $b$. Ist $a$ gerade und $b$ ungerade, dann ersetze $a$ durch $a/2$; sind sowohl $a$ als auch $b$ ungerade, dann ersetze $b$ durch $b - a$; in jedem Fall gehe zu (1) zurück.

(3) Falls $a = 0$, dann gebe die Zahl $2^r b$ als ggT zurück.

Nun kommen die Übungsaufgaben:

(a) Führen Sie diesen Algorithmus aus, um $\mathrm{ggT}(19, 2)$ zu berechnen.

(b) Es scheint, als hätten wir in Schritt (2) den Fall ignoriert, bei dem sowohl $a$ als auch $b$ gerade sind. Zeigen sie, dass dies niemals auftritt.

(c) Zeigen Sie, dass dieser modifizierte euklidische Algorithmus immer mit dem korrekten Ergebnis endet.

(d) Zeigen Sie, dass dieser Algorithmus nicht mehr als 1500 Iterationen benötigt, wenn er auf zwei 100-stellige ganze Zahlen angewandt wird.

Der euklidische Algorithmus liefert viel mehr als nur den größten gemeinsamen Teiler zweier Zahlen. Die wichtigste Beobachtung besteht darin, dass alle Zahlen, die wir bei der Ausführung des euklidischen Algorithmus zur Berechnung des größten gemeinsamen Teilers zweier natürlicher Zahlen $a$ und $b$ produzieren, als Summe eines ganzzahligen Vielfachen von $a$ und eines ganzzahligen Vielfachen von $b$ dargestellt werden können.

Als Beispiel betrachten wir noch einmal die Berechnung von $\mathrm{ggT}(300, 18)$:

$$\mathrm{ggT}(300, 18) = \mathrm{ggT}(12, 18) = \mathrm{ggT}(12, 6) = 6.$$

Die Zahl 12 wurde hier als Rest bei der Division $300 \div 18$ erhalten. Das bedeutet, wir erhielten sie, indem wir von 300 das größte Vielfache von 18, welches kleiner als 300

ist, subtrahierten: $12 = 300 - 16 \cdot 18$. Wir beschreiben dies in folgender Form:

$$\mathrm{ggT}(300, 18) = \mathrm{ggT}(300 - 16 \cdot 18, 18).$$

Als nächstes subtrahierten wir 12 von 18 und erhielten 6. Dies können wir unter Beibehaltung der Form (Vielfaches von 300)-(Vielfaches von 18) tun:

$$\mathrm{ggT}(300 - 16 \cdot 18, 18) = \mathrm{ggT}(300 - 16 \cdot 18, 17 \cdot 18 - 300).$$

Es folgt somit, dass der ggT, nämlich 6, diese Form besitzt:

$$6 = 17 \cdot 18 - 300.$$

Wir beweisen nun formal, dass alle durch den euklidischen Algorithmus zur Berechnung von $\mathrm{ggT}(a, b)$ produzierten Zahlen als Summe eines ganzzahligen Vielfachen von $a$ und eines ganzzahligen Vielfachen von $b$ dargestellt werden können. Nehmen wir an, dies gilt für zwei der produzierten aufeinander folgenden Zahlen, so dass die eine $a' = am + bn$ und die andere $b' = ak + bl$ ist, wobei $m, n, k, l$ ganze Zahlen (nicht notwendigerweise positiv) sind. Dann berechnen wir im nächsten Schritt den Rest von (sagen wir) $b'$ modulo $a'$, was

$$a' - qb' = (am + bn) - q(ak + bl) = a(m - qk) + b(n - ql)$$

ist und daher wieder die richtige Form besitzt.
Wir erhalten insbesondere folgenden Satz:

**Satz 6.6.2** Sei $d = \mathrm{ggT}(a, b)$. Dann läßt sich $d$ in der Form **6.6.2**

$$d = am + bn,$$

darstellen, wobei $m$ und $n$ ganze Zahlen sind.

Ebenso wie bei dem oben angeführten Beispiel können wir die Darstellungsform $am + bn$ der ganzen Zahlen während der Berechnung beibehalten. Dies zeigt, dass der im obigen Satz angegebene Ausdruck für $d$ nicht nur existiert, sondern auch leicht zu berechnen ist.

## 6.7 Kongruenzen **6.7**

Die Notation gehört nicht zur reinen, logischen Struktur der Mathematik: Wir könnten die Menge der reellen Zahlen mit $\mathbf{V}$ bezeichnen oder die Addition durch # und die Bedeutung der mathematischen Ergebnisse wäre trotzdem dieselbe. Eine gute Notation kann jedoch wundervoll suggestiv sein und zu einem echten begrifflichen Durchbruch

führen. Einer dieser wichtigen Schritte war getan, als Carl Friedrich Gauss feststellte, dass der Ausdruck „$a$ und $b$ besitzen bei der Division durch $m$ denselben Rest“ sehr häufig verwendet wird und sich diese Relation recht ähnlich zur Gleichheit verhält. Er führte dafür eine Bezeichnung ein, die *Kongruenz*.

**Abbildung 6.6.** Carl Friedrich Gauss (1777–1855)

Besitzen $a$ und $b$ bei der Division durch $m$ denselben Rest (wobei $a, b, m$ ganze Zahlen sind und $m > 0$ ist), dann schreiben wir

$$a \equiv b \pmod{m}$$

(man liest: $a$ ist kongruent $b$ modulo $m$). Äquivalent dazu kann man auch sagen: $m$ ist ein Teiler von $b - a$. Die Zahl $m$ wird als *Modul* der Kongruenzrelation bezeichnet. Die Notation legt nahe, dass wir diese Relation als Analogon zur Gleichheit ansehen wollen. Eine Menge Eigenschaften der Gleichheit sind tatsächlich auch für die Kongruenz gültig, zumindest wenn wir den Modul $m$ fest lassen. Wir haben
*Reflexivität*,

$$a \equiv a \pmod{m},$$

*Symmetrie*,

$$a \equiv b \pmod{m} \qquad \Longrightarrow \qquad b \equiv a \pmod{m},$$

und *Transitivität*,

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

Das ist trivial, wenn wir die Kongruenzrelation als Gleichheit betrachten, nämlich als Gleichheit der Reste beim Teilen durch $m$.

Wir können mit Kongruenzen ebenso wie mit Gleichungen rechnen. Haben wir zwei Kongruenzen mit demselben Modul

$$a \equiv b \pmod{m} \quad \text{und} \quad c \equiv d \pmod{m},$$

können wir sie addieren, subtrahieren und multiplizieren. Wir erhalten

$$a + c \equiv b + d \pmod{m}, \quad a - c \equiv b - d \pmod{m}, \quad ac \equiv bd \pmod{m}$$

(zur Division werden wir später kommen). Ein nützlicher Spezialfall der Multiplikationsregeln besteht darin, dass wir beide Seiten der Kongruenz mit derselben Zahl multiplizieren können: Falls $a \equiv b \pmod{m}$, dann gilt $ka \equiv kb \pmod{m}$ für alle ganzen Zahlen $k$.
Diese Eigenschaften müssen natürlich bewiesen werden. Nach Voraussetzung sind $a - b$ und $c - d$ durch $m$ teilbar. Um zu beweisen, dass die Kongruenzen addiert werden können, müssen wir zeigen, dass $(a + c) - (b + d)$ ebenfalls durch $m$ teilbar ist. Zu diesem Zweck schreiben wir dies in Form von $(a-b)+(c-d)$, was die Summe zweier durch $m$ teilbarer ganzer Zahlen ist und somit auch selbst durch $m$ geteilt werden kann. Sehr ähnlich läßt sich beweisen, dass Kongruenzen subtrahiert werden können. Die Multiplikation ist jedoch ein klein wenig schwieriger. Wir müssen zeigen, dass $ac-bd$ durch $m$ teilbar ist. Dazu schreiben wir dies in Form von

$$ac - bd = (a - b)c + b(c - d).$$

Hierbei sind $a - b$ und $c - d$ durch $m$ teilbar, folglich auch $(a - b)c$ und $b(c - d)$ und somit auch ihre Summe.
Die Kongruenzschreibweise ist sehr nützlich, um vielfältige Aussagen und Beweise über Teilbarkeit zu formulieren. Zum Beispiel kann Fermats Satz (Satz 6.5.1) wie folgt angegeben werden: Ist $p$ eine Primzahl, dann gilt

$$a^p \equiv a \pmod{p}.$$

---

**Übung 6.7.1** Wie lautet die größte ganze Zahl $m$, für die $12345 \equiv 54321 \pmod{m}$ gilt?

---

**Übung 6.7.2** Welche der folgenden „Regeln“ sind wahr?

(a) $a \equiv b \pmod{c} \;\Rightarrow\; a + x \equiv b + x \pmod{c + x}$;

(b) $a \equiv b \pmod{c} \;\Rightarrow\; ax \equiv bx \pmod{cx}$.

(c) $\left.\begin{array}{l} a \equiv b \pmod{c} \\ x \equiv y \pmod{z} \end{array}\right\} \;\Rightarrow\; a + x \equiv b + y \pmod{c + z}$;

(d) $\left.\begin{array}{l} a \equiv b \pmod{c} \\ x \equiv y \pmod{z} \end{array}\right\} \;\Rightarrow\; ax \equiv by \pmod{cz}$.

**Übung 6.7.3** Wie würden wir $a \equiv b \pmod 0$ definieren?

**Übung 6.7.4** (a) Finden Sie zwei ganze Zahlen $a$ und $b$, für die $2a \equiv 2b \pmod 6$ gilt, aber $a \not\equiv b \pmod 6$. (b) Zeigen Sie: Falls $c \neq 0$ und $ac \equiv bc \pmod{mc}$, dann gilt $a \equiv b \pmod m$.

**Übung 6.7.5** Sei $p$ eine Primzahl. Zeigen Sie: Falls $x, y, u, v$ ganze Zahlen sind, so dass $x \equiv y \pmod p$, $u, v > 0$ und $u \equiv y \pmod{p-1}$, dann gilt $x^u \equiv y^v \pmod p$.

6.8

## 6.8 Seltsame Zahlen

Was ist Donnerstag + Freitag?
Wenn Sie diese Frage nicht verstehen, dann fragen Sie ein Kind. Es wird Ihnen sagen, dass es Dienstag ist. (Es könnte Diskussionen darüber geben, ob die Woche mit Montag oder Sonntag beginnt. Aber selbst wenn wir meinen, sie beginnt mit Sonntag, können wir immer noch sagen, dass Sonntag der Tag 0 ist.)
Wir sollten nun keine Schwierigkeiten haben, herauszufinden, dass Mittwoch·Dienstag = Samstag, Donnerstag$^2$ = Dienstag, Montag − Samstag = Dienstag, etc. ist.
Auf diese Weise können wir Rechenoperationen mit den Tagen der Woche ausführen: Wir haben ein neues Zahlensystem eingeführt! In diesem System gibt es nur 7 Zahlen, die wir So, Mo, Di, Mi, Do, Fr und Sa nennen und wir können Addition, Subtraktion und Multiplikation mit ihnen ebenso wie mit Zahlen durchführen (wir könnten sie auch Glück, Freude, Pech, Zorn, Ärger, Furcht und Egon nennen. Worauf es ankommt, ist die Arbeitsweise der Rechenoperationen).
Nicht nur, dass wir diese Operationen definieren können, sie arbeiten auch noch ziemlich ähnlich wie Operationen mit ganzen Zahlen. Addition und Multiplikation sind kommutativ

$$\mathrm{Di} + \mathrm{Fr} = \mathrm{Fr} + \mathrm{Di}, \qquad \mathrm{Di} \cdot \mathrm{Fr} = \mathrm{Fr} \cdot \mathrm{Di},$$

und assoziativ

$$(\mathrm{Mo} + \mathrm{Mi}) + \mathrm{Fr} = \mathrm{Mo} + (\mathrm{Mi} + \mathrm{Fr}), \qquad (\mathrm{Mo} \cdot \mathrm{Mi}) \cdot \mathrm{Fr} = \mathrm{Mo} \cdot (\mathrm{Mi} \cdot \mathrm{Fr}),$$

und das Distributivgesetz gilt

$$(\mathrm{Mo} + \mathrm{Mi}) \cdot \mathrm{Fr} = (\mathrm{Mo} \cdot \mathrm{Fr}) + (\mathrm{Mi} \cdot \mathrm{Fr}).$$

Die Subtraktion ist zur Addition invers:

$$(\mathrm{Mo} + \mathrm{Mi}) - \mathrm{Mi} = \mathrm{Mo}.$$

Sonntag verhält sich wie 0:

$$\text{Mi} + \text{So} = \text{Mi}, \qquad \text{Mi} \cdot \text{So} = \text{So}$$

und Montag verhält sich wie 1:

$$\text{Mi} \cdot \text{Mo} = \text{Mi}.$$

All dies ist nichts Neues, wenn wir „Montag“ als 1, „Dienstag“ als 2, etc. betrachten und uns klarmachen, dass wir, da der 8. Tag wieder Montag ist, die Ergebnisse jeder Rechenoperation durch ihren Rest modulo 7 ersetzen müssen. Die obigen Identitäten drücken jeweils Kongruenzrelationen aus und folgen direkt aus den grundlegenden Eigenschaften der Kongruenzen.
Wie sieht es nun mit der Division aus? In einigen Fällen ist dies naheliegend. Was ist zum Beispiel Sa/Mi? Übersetzen wir dies in ganze Zahlen, so heißt es 6/3. Das ist gleich 2, entspricht also Di. Die Überprüfung ergibt: $\text{Di} \cdot \text{Mi} = \text{Sa}$.
Was ist jedoch Di/Mi? In unserem üblichen Zahlensystem wäre dies $2/3$, was keine ganze Zahl ist. Rationale Zahlen wurden so eingeführt, dass wir über das Ergebnis jeder Division sprechen können (ausgenommen, Divisionen durch 0). Müssen wir nun auch „Bruchteile von Wochentagen“ einführen?
Es stellt sich heraus, dass dieses neue Zahlensystem (mit nur 7 „Zahlen“ ) hübscher ist! Was bedeutet Di/Mi? Es ist eine „Zahl“ $X$, für die $X \cdot \text{Mi} = \text{Di}$ gilt. Es läßt sich leicht prüfen, dass $\text{Mi} \cdot \text{Mi} = \text{Di}$ ist. Damit haben wir $\text{Di}/\text{Mi} = \text{Mi}$ (oder zumindest scheint es einen Sinn zu ergeben, wenn wir dies sagen).
Dieses Beispiel zeigt, dass es für uns möglich sein kann, Divisionen durchzuführen, ohne neue „Zahlen“ (oder neue Wochentage) einführen zu müssen. Aber ist die Ausführung der Division immer möglich?
Betrachten wir eine andere Division, um zu sehen, wie das Ganze funktioniert: Mi/Fr. Diesmal versuchen wir *nicht* zu vermuten, was herauskommt. Stattdessen nennen wir das Ergebnis $X$ und zeigen, dass einer der Wochentage $X$ entsprechen muss.
Sei also $X = \text{Mi}/\text{Fr}$. Das bedeutet, dass $X \cdot \text{Fr} = \text{Mi}$ gilt. Für jeden Wochentag $X$ ist das Produkt $X \cdot \text{Fr}$ einer der Wochentage.
Die wichtigste Behauptung besteht darin, dass *für verschiedene Tage $X$ die Produkte $X \cdot \text{Fr}$ alle unterschiedlich sind.* Nehmen wir an, es gilt

$$X \cdot \text{Fr} = Y \cdot \text{Fr}.$$

Dann erhalten wir

$$(X - Y) \cdot \text{Fr} = \text{So} \tag{38}$$

(wir haben hier das Distributivgesetz und die Tatsache, dass sich Sonntag wie 0 verhält, verwendet). Das Produkt zweier Zahlen, die beide ungleich Null sind, ist wieder eine Zahl ungleich Null. Der Sonntag verhält sich auch in diesem Sinne analog zur 0, das

heisst, das Produkt zweier nicht-Sonntage ist ein nicht-Sonntag. (Überprüfen Sie dies!) Also erhalten wir $X - Y = \text{So}$ und daher $X = Y + \text{So} = Y$.
Die Tage $X \cdot \text{Fr}$ sind somit also alle verschieden. Es gibt sieben davon, daher muss jeder Wochentag in dieser Form auftreten. Insbesondere wird auch „Mi“ vorkommen. Diese Argumentation funktioniert bei jeder Division, ausgenommen, wir versuchen durch Sonntag zu teilen. Wir wissen bereits, dass sich der Sonntag wie 0 verhält, und daher ergibt die Multiplikation von Sonntag mit jeglichem anderen Tag wieder Sonntag. Wir können daher keinen anderen Tag durch Sonntag dividieren (und das Ergebnis von $\text{So}/\text{So}$ ist nicht wohldefiniert, es könnte jeder Tag sein).
Die in Abschnitt 6.7 eingeführten Kongruenzen ermöglichen oft eine angenehme Handhabung dieser seltsamen Zahlen. Wir können zum Beispiel (38) in Form von

$$(x - y) \cdot 5 \equiv 0 \pmod 7$$

schreiben (wobei $x$ und $y$ die den Tagen $X$ und $Y$ entsprechenden Zahlen sind), daher ist 7 ein Teiler von $(x - y)5$. Es sind jedoch weder 5 noch $x - y$ durch 7 teilbar ($x$ und $y$ sind zwei verschiedene nicht-negative ganze Zahlen, beide kleiner als 7). Dies ist ein Widerspruch, da 7 eine Primzahl ist. Auf diese Weise können wir, anstelle von Wochentagen, über die üblichen Zahlen sprechen. Der Preis dafür besteht in der Verwendung von Kongruenzen anstelle der Gleichheit.

---

**Übung 6.8.1** Bestimmen Sie Mi/Fr, Di/Fr, Mo/Di, Sa/Di.

---

Gibt es hier an der Zahl 7 irgendetwas besonderes? In einer Gesellschaft, in der die Woche aus 10, 13 oder 365 Tagen besteht, könnten wir Addition, Subtraktion und Multiplikation ebenso definieren.
Sei $m$ die Anzahl der Wochentage, was wir in mathematischer Sprache den Modulus nennen. Es wäre unpraktisch, für die Wochentage neue Namen einzuführen[1], also nennen wir sie einfach $\overline{0}, \overline{1}, \ldots, \overline{m-1}$. Die Striche über den Zahlen bedeuten, dass sich zum Beispiel $\overline{2}$ nicht nur auf Tag 2, sondern auch auf Tag $m + 2$, Tag $2m + 2$, etc. bezieht.
Die Addition ist durch $\overline{a} + \overline{b} = \overline{c}$ definiert, wobei $c$ der Rest von $a + b$ modulo $m$ ist. Die Multiplikation und Subtraktion sind in ähnlicher Art definiert. Auf diese Weise erhalten wir ein neues Zahlensystem: Es besteht lediglich aus $m$ Zahlen und die Grundrechenarten können darin durchgeführt werden. Diese Rechenoperationen genügen den grundlegenden Rechengesetzen, was ebenso wie im obigen Fall $m = 7$ folgt. Diese Art der Rechnung wird *modulare Arithmetik* genannt.
Was ist mit der Division? Wenn Sie den Beweis dafür, dass wir die Division mit $m = 7$ ausführen können, sorgfältig durchlesen, wird Ihnen auffallen, dass wir eine spezielle

[1] In vielen Sprachen sind die Namen der Wochentage von Zahlen abgeleitet.

Eigenschaft der 7 verwendet haben: Sie ist eine Primzahl! Es gibt tatsächlich einen grundlegenden Unterschied zwischen der modularen Arithmetik mit und ohne Primzahlmodul. Im Folgenden werden wir unsere Aufmerksamkeit auf den Fall beschränken, bei dem der Modul eine Primzahl ist. Um dies zu betonen, werden wir ihn mit $p$ bezeichnen. Dieses aus $\overline{0}, \overline{1}, \ldots, \overline{p-1}$ bestehende Zahlensystem wird zusammen mit den vier wie oben definierten Operationen ein *Primkörper* genannt.

**Der 2-elementige Körper.** Die kleinste Primzahl ist 2 und der einfachste Primkörper besteht aus lediglich 2 Elementen, $\overline{0}$ und $\overline{1}$. Die Additions- und Multiplikationstafeln dafür anzugeben, ist einfach:

| $+$ | $\overline{0}$ | $\overline{1}$ |
|---|---|---|
| $\overline{0}$ | $\overline{0}$ | $\overline{1}$ |
| $\overline{1}$ | $\overline{1}$ | $\overline{0}$ |

| $\cdot$ | $\overline{0}$ | $\overline{1}$ |
|---|---|---|
| $\overline{0}$ | $\overline{0}$ | $\overline{0}$ |
| $\overline{1}$ | $\overline{0}$ | $\overline{1}$ |

(Es gibt tatsächlich nur eine einzige Operation, die nicht aus den allgemeinen Eigenschaften von 0 und 1 folgt, nämlich $\overline{1}+\overline{1}=\overline{0}$. Es ist weder nötig die Subtraktionstafel anzugeben, da in diesem Körper $a+b=a-b$ für alle $a$ und $b$ gilt (überprüfen!), noch die Divisionstafel, da folgendes offensichtlich ist: Durch $\overline{0}$ können wir nicht teilen und die Division durch $\overline{1}$ bewirkt beim Dividenden keine Veränderung.)

Es ist unbequem all diese Querstriche über die Zahlen zu schreiben, daher werden wir sie häufig weglassen. Allerdings müssen wir dann vorsichtig sein, da wir wissen müssen, ob $1+1$ nun 2 oder 0 ist. Aus diesem Grund ändern wir das Additionszeichen und verwenden $\oplus$ für die Addition in einem 2-elementigen Körper. In dieser Notation sehen die Additions- und Multiplikationstafeln wie folgt aus:

| $\oplus$ | 0 | 1 |
|---|---|---|
| 0 | 0 | 1 |
| 1 | 1 | 0 |

| $\cdot$ | 0 | 1 |
|---|---|---|
| 0 | 0 | 0 |
| 1 | 0 | 1 |

(Für die Multiplikation müssen wir kein neues Symbol einführen, da die Multiplikationstafel für 0 und 1 in einem 2-elementigen Körper dieselbe wie bei den üblichen Zahlen ist.)
Dieser Körper ist sehr klein, aber auch sehr wichtig, da er in der Informatik, der Informationstheorie und der mathematischen Logik sehr häufig verwendet wird: Seine zwei Elemente können als „JA-NEIN“ , „WAHR-FALSCH“ , „SIGNAL-KEIN SIGNAL“ , etc. interpretiert werden.

---

**Übung 6.8.2** Die 0 bedeute „FALSCH“ und die 1 bedeute „WAHR“ . Seien $A$ und $B$ zwei Aussagen (die entweder wahr oder falsch sind). Formulieren Sie unter Verwendung der Operationen $\oplus$ und $\cdot$ die wahren Aussagen „nicht A“ , „$A$ oder $B$“ , „$A$ und $B$“ .

**Übung 6.8.3** Sei der Modul gleich 6. Zeigen Sie anhand eines Beispiels, dass die Division durch eine „Zahl“ ungleich Null nicht immer ausgeführt werden kann. Verallgemeinern Sie das Beispiel auf jeden zusammengesetzten Modul.

**Division in modularer Arithmetik.** Unser Beweis, dass die Division in modularer Arithmetik nur ausgeführt werden kann, falls der Modul eine Primzahl ist, war recht einfach. Er enthält jedoch keine Informationen darüber, wie man die Division durchführt. Würden wir wie oben vorgehen, um den Quotienten zu bestimmen, so würde dies bedeuten, dass wir alle Zahlen zwischen $0$ und $p-1$ betrachten müssten. Dies war für $p = 7$ in Ordnung. Für eine Primzahl wie $p = 234.527$ wäre es jedoch ziemlich langwierig (ganz zu schweigen von wirklich großen Primzahlen, wie sie in der Kryptographie und Computersicherheit Verwendung finden).
Wie können wir also beispielsweise $\overline{53}$ durch $\overline{2}$ modulo 234.527 teilen?
Wir können das Problem vereinfachen und nur die Division von $\overline{1}$ durch $\overline{2}$ modulo 234.527 betrachten. Haben wir $\overline{1}/\overline{2} = \overline{a}$, dann können wir $\overline{53}/\overline{2} = \overline{53} \cdot \overline{a}$ erhalten, wovon wir wissen, wie wir es zu berechnen haben.
An diesem Punkt können wir den Beweis anhand eines allgemeinen Falles noch besser erläutern. Seien ein Primzahlmodul $p$ und eine ganze Zahl $a$ ($1 \leq a \leq p-1$) gegeben und wir möchten eine ganze Zahl $x$ ($0 \leq x \leq p-1$) finden, so dass $\overline{ax} = \overline{1}$ gilt. Unter Verwendung der Kongruenzschreibweise aus Abschnitt 6.7 können wir dies wie folgt schreiben

$$ax \equiv 1 \pmod{p}.$$

Der Schlüssel zur Lösung dieses Problems ist der euklidischen Algorithmus. Wir bestimmen den größten gemeinsamen Teiler von $a$ und $p$. Da die Antwort offensichtlich ist, hört sich das eigentlich ziemlich albern an: $p$ ist eine Primzahl und $1 \leq a < p$. Somit können sie keinen größeren gemeinsamen Teiler als 1 besitzen und daher gilt $\mathrm{ggT}(p, a) = 1$. Erinnern wir uns, dass uns der euklidische Algorithmus aber noch mehr liefert: Er gibt uns den größten gemeinsamen Teiler in der Form $au + pv$, wobei $u$ und $v$ ganze Zahlen sind. Daher erhalten wir

$$au + pv = 1,$$

wodurch

$$au \equiv 1 \pmod{p}$$

impliziert wird. Damit sind wir schon fast fertig. Das einzige Problem besteht noch darin, dass die ganze Zahl $u$ nicht zwischen 1 und $p-1$ liegen muss. Ist jedoch $x$ der Rest von $u$ modulo $p$, dann erhalten wir durch Multiplikation der Kongruenz $x \equiv u \pmod{p}$ mit $a$ (wir erinnern uns an Abschnitt 6.7: Dies ist eine legale Rechen-

operation bei Kongruenzen.)

$$ax \equiv au \equiv 1 \pmod{p}.$$

Dies ist die Lösung unseres Problems, da $0 \leq x \leq p-1$ gilt.
Wir wenden diesen Algorithmus nun auf unser obiges Beispiel mit $a = 2$ und $p = 234.527$ an. Der euklidische Algorithmus ist in diesem Fall wirklich sehr einfach: Man teile $234.527$ mit Rest durch $2$. Der Rest ist bereits gleich 1. Daher erhalten wir

$$2 \cdot (-117.263) + 234.527 \cdot 1 = 1.$$

Der Rest von -117.263 modulo 234.527 ist 117.264, somit bekommen wir

$$\overline{1}/\overline{2} = \overline{117.264}.$$

---

**Übung 6.8.4** Berechnen Sie $\overline{1}/\overline{53}$ modulo 234.527.

Sobald wir wissen, wie die grundlegenden Rechenoperationen ausgeführt werden können, ist es möglich, schwierigere Aufgabenstellungen, wie zum Beispiel das Lösen linearer Gleichungen durchzuführen. Dafür besinnen wir uns darauf, was wir mit gewöhnlichen Zahlen machen würden. Veranschaulichen können wir dies anhand einiger Beispiele, bei denen wir die Kongruenzschreibweise zusammen mit den grundlegenden Eigenschaften aus Abschnitt 6.7 verwenden.

**Beispiel 1:** Wir betrachten eine lineare Gleichung, sagen wir

$$\overline{7}X + \overline{3} = \overline{0},$$

wobei der Modul 47 ist. (Man prüfe anhand der Tabelle, dass dies eine Primzahl ist!) Dies können wir als Kongruenz umschreiben:

$$7x + 3 \equiv 0 \pmod{47}.$$

Die zweite Form ist üblicher, daher werden wir damit weiterarbeiten.
Wir formen dies zu

$$7x \equiv -3 \pmod{47} \tag{39}$$

um, genau wie wir es mit einer Gleichung machen würden (wenn wir alle Zahlen positiv schreiben wollten, könnten wir $-3$ durch ihren Rest 44 modulo 47 ersetzen, aber dies ist je nach Geschmack freigestellt).
Als nächstes müssen wir den Kehrwert von 7 modulo $47$ bestimmen. Der euklidische Algorithmus ergibt

$$\mathrm{ggT}(7, 47) = \mathrm{ggT}(7, 5) = \mathrm{ggT}(2, 5) = \mathrm{ggT}(2, 1) = 1,$$

und mit der erweiterten Version erhalten wir

$$5 = 47 - 6 \cdot 7, \qquad 2 = 7 - 5 = 7 - (47 - 6 \cdot 7) = 7 \cdot 7 - 47,$$

$$1 = 5 - 2 \cdot 2 = (47 - 6 \cdot 7) - 2 \cdot (7 \cdot 7 - 47) = 3 \cdot 47 - 20 \cdot 7.$$

Dies zeigt, dass $(-20) \cdot 7 \equiv 1 \pmod{47}$ gilt. Der Kehrwert von 7 modulo 47 beträgt also $-20$ (was wir wiederum auch als 27 schreiben könnten).
Durch die Division beider Seiten von (39) durch 7, was der Multiplikation beider Seiten mit 27 entspricht, erhalten wir nun

$$x \equiv 13 \pmod{47}.$$

(Wir bekommen 13 entweder als Rest von $(-3)(-20)$ oder als Rest von $44 \cdot 27$ modulo 47, das Ergebnis ist dasselbe.)

**Beispiel 2:** Als nächstes lösen wir ein System aus zwei linearen Gleichungen mit zwei Variablen. Wir behandeln in diesem Beispiel etwas größere Zahlen, um zu zeigen, dass wir auch mit diesen zurecht kommen. Der Modulus sei $p = 127$ und wir betrachten die Gleichungen

$$\begin{aligned} \overline{12}X + \overline{31}Y &= \overline{2}, \\ \overline{2}X + \overline{89}Y &= \overline{23}. \end{aligned} \tag{40}$$

Wir können sie als folgende Kongruenzen beschreiben:

$$\begin{aligned} 12x + 31y &\equiv 2 \pmod{127}, \\ 2x + 89y &\equiv 23 \pmod{127}. \end{aligned}$$

**a) Eliminieren einer Variablen:** Wie würden wir dieses System lösen, wenn es gewöhnliche Gleichungen wären? Um $x$ zu eliminieren könnten wir die zweite Gleichung mit 6 multiplizieren und sie von der ersten abziehen. In diesem Primkörper können wir das ebenfalls tun und erhalten

$$(31 - 6 \cdot 89)y \equiv 2 - 6 \cdot 23 \pmod{127}$$

oder

$$(-503)y \equiv -136 \pmod{127}.$$

Wir können die negativen Zahlen durch ihre Reste modulo 127 ersetzen und bekommen

$$5y \equiv 118 \pmod{127}. \tag{41}$$

**b) Division:** Als nächstes möchten wir die Gleichung durch 5 dividieren. Nun folgt das, was wir vorhin besprochen haben: Wir müssen den euklidischen Algorithmus anwenden. Die Berechnung des größten gemeinsamen Teilers ist einfach:

$$\mathrm{ggT}(127,5) = \mathrm{ggT}(2,5) = \mathrm{ggT}(2,1) = 1.$$

Dies ergibt nichts Neues: Wir wußten schon vorher, dass der größte gemeinsame Teiler 1 sein würde. Um mehr zu erhalten, müssen wir an diese Berechnung eine andere anschließen, wobei jede Zahl als ganzzahlige Vielfache von 127 plus einer Vielfachen der Zahl 5 geschrieben wird:

$$\mathrm{ggT}(127,5) = \mathrm{ggT}(127-25\cdot 5,5) = \mathrm{ggT}(127-25\cdot 5,(-2)\cdot 127+51\cdot 5) = 1.$$

Dies ergibt

$$(-2)\cdot 127 + 51\cdot 5 = 1.$$

Daher gilt $5\cdot 51 \equiv 1 \pmod{127}$ und somit haben wir den „Kehrwert“ von 5 modulo 127 gefunden.
Anstatt Gleichung (40) durch fünf zu teilen, multiplizieren wir sie mit dem „Kehrwert“ 51, um

$$y \equiv 51\cdot 118 \pmod{127} \tag{42}$$

zu erhalten.

**c) Abschluß:** Berechnen wir die rechte Seite von (42) und bestimmen danach den Rest modulo 127, erhalten wir $y \equiv 49 \pmod{127}$. Mit anderen Worten ist $Y = \overline{49}$ die Lösung. Wir müssen nun diesen Wert wieder in eine der Originalgleichungen einsetzen, um $x$ zu bestimmen:

$$2x + 89\cdot 49 \equiv 23 \pmod{127}$$

und daher gilt

$$2x \equiv 23 - 89\cdot 49 \equiv 107 \pmod{127}.$$

Wir müssen also noch eine Division durchführen. In Analogie zu dem, was wir oben getan haben, erhalten wir

$$(-63)\cdot 2 + 127 = 1$$

und folglich

$$64\cdot 2 \equiv 1 \pmod{127}.$$

Wir können also, anstatt durch 2 zu teilen, mit 64 multiplizieren und bekommen

$$x \equiv 64\cdot 107 \pmod{127}.$$

Durch die Berechnung der rechten Seite und ihres Rests modulo 127 erhalten wir $x \equiv 117 \pmod{127}$ oder anders ausgedrückt $X = \overline{117}$. Wir haben (40) somit gelöst.

**Beispiel 3:** Wir sind sogar in der Lage, quadratische Gleichungen zu lösen, zum Beispiel

$$x^2 - 3x + 2 \equiv 0 \pmod{53}.$$

Wir können dies auch so schreiben:

$$(x-1)(x-2) \equiv 0 \pmod{53}.$$

Einer der Faktoren auf der linken Seite muß kongruent zu 0 modulo 53 sein, wobei entweder $x \equiv 1 \pmod{53}$ oder $x \equiv 2 \pmod{53}$ gilt.
Wir haben hier durch reines Hinsehen eine Möglichkeit gefunden, die linke Seite als Produkt darzustellen. Was passiert, wenn wir Gleichungen mit größeren Zahlen haben, wie zum Beispiel $x^2 + 134.517x + 105.536 \equiv 0 \pmod{234.527}$? Es ist zweifelhaft, ob es jemandem gelingt, hier eine Zerlegung zu erraten. In diesem Fall können wir versuchen, die schon aus der Schule bekannte Methode zur Lösung quadratischer Gleichungen anzuwenden. Sie funktioniert, allerdings ist einer ihrer Schritte ziemlich schwierig: das Ziehen von Quadratwurzeln. Es ist durchaus möglich, dies effizient zu tun, allerdings ist der Algorithmus zu kompliziert, um hier erläutert zu werden.

---

**Übung 6.8.5** Lösen Sie das Kongruenzsystem

$$\begin{aligned} 2x + 3y &\equiv 1 \pmod{11}, \\ x + 4y &\equiv 4 \pmod{11}. \end{aligned}$$

---

**Übung 6.8.6** Lösen Sie die „Kongruenzgleichungen“

$$\text{(a)}\ x^2 - 2x \equiv 0 \pmod{11}, \qquad \text{(b)}\ x^2 \equiv 4 \pmod{23}.$$

6.9

## 6.9 Zahlentheorie und Kombinatorik

Viele der von uns eingeführten kombinatorischen Hilfsmittel sind auch in der Zahlentheorie sehr nützlich. Induktion wird überall verwendet. Wir zeigen einige elegante Beweise, die auf dem *Taubenschlagprinzip* und auf der *Inklusions-Exklusions-Formel* basieren.

*Uns seien $n$ natürliche Zahlen gegeben: $a_1, a_2, \ldots, a_n$. Zeigen Sie, dass wir eine (nicht-leere) Teilmenge dieser Zahlen auswählen können, deren Summe durch $n$ teilbar ist.*

(Es ist möglich, dass diese Teilmenge alle $n$ Zahlen enthält.)

*Lösung:* Wir betrachten folgende $n$ Zahlen:

$$\begin{aligned} b_1 &= a_1, \\ b_2 &= a_1 + a_2, \\ b_3 &= a_1 + a_2 + a_3, \\ &\vdots \\ b_n &= a_1 + a_2 + a_3 + \cdots + a_n. \end{aligned}$$

Wir haben gefunden, was wir suchten, falls unter diesen $n$ Zahlen eine dabei ist, die durch $n$ teilbar ist. Ist keine dabei, dann teilen wir alle Zahlen $b_1, b_2, \ldots, b_n$ mit Rest durch $n$. Man schreibe diese Reste auf. Welche Zahlen erhalten wir? Es könnte jeweils $1, 2, \ldots$ oder $n-1$ sein. Wir haben jedoch eine Gesamtmenge von $n$ Zahlen! Nach dem Taubenschlagprinzip besitzen daher zwei der Zahlen $b_1, b_2, \ldots, b_n$ denselben Rest beim Teilen durch $n$. Sagen wir, diese beiden Zahlen sind $b_i$ und $b_j$ $(i < j)$, dann ist ihre Differenz $b_j - b_i$ durch $n$ teilbar. Es gilt jedoch

$$b_j - b_i = a_{i+1} + a_{i+2} + \cdots + a_j.$$

Wir haben somit eine bestimmte Teilmenge der Zahlen $a_1, a_2, \ldots, a_n$ gefunden, nämlich $a_{i+1}, a_{i+2}, \ldots, a_j$, deren Summe durch $n$ teilbar ist. Dies wollten wir zeigen.

---

**Übung 6.9.1** Uns seien $n$ Zahlen aus der Menge $\{1, 2, \ldots, 2n-1\}$ gegeben. Zeigen Sie, dass man unter diesen $n$ Zahlen immer zwei finden kann, die teilerfremd zueinander sind.

Als sehr wichtige Anwendung der Inklusion–Exklusion beantworten wir folgende Frage: *Wie viele zu 1200 teilerfremde natürliche Zahlen gibt es, die kleiner als 1200 sind?* Wir kennen die Primfaktorzerlegung von 1200, nämlich $1200 = 2^4 \cdot 3 \cdot 5^2$. Daher wissen wir, dass genau die durch 2, 3 oder 5 teilbaren Zahlen einen gemeinsamen Faktor mit 1200 besitzen. Wir möchten also die Anzahl aller natürlichen Zahlen, die kleiner als 1200 und nicht durch 2, 3 oder 5 teilbar sind, bestimmen.
Man kann leicht berechnen, dass es bis 1200

$\frac{1200}{2}$ durch 2 teilbare Zahlen
(jede zweite Zahl ist gerade),

$\frac{1200}{3}$ durch 3 teilbare Zahlen und

$\frac{1200}{5}$ durch 5 teilbare Zahlen gibt.

Die sowohl durch 2 als auch durch 3 teilbaren Zahlen sind genau die durch 6 teilbaren Zahlen. Bis 1200 gibt es daher

$\frac{1200}{6}$ durch 2 und 3 teilbare Zahlen

und analog gibt es

$\frac{1200}{10}$ durch 2 und 5 teilbare Zahlen und

$\frac{1200}{15}$ durch 3 und 5 teilbare Zahlen.

Schließlich sind die Zahlen, die durch 2, 3 und 5 teilbar sind, genau diejenigen, welche durch 30 teilbar sind. Daher gibt es

$\frac{1200}{30}$ durch 2, 3 und 5 teilbare Zahlen.

Wir können nun mit diesen Daten die Inklusion–Exklusion nutzen, um die gesuchte Anzahl zu bestimmen:

$$1200 - \left(\frac{1200}{2} + \frac{1200}{3} + \frac{1200}{5}\right) + \frac{1200}{2\cdot 3} + \frac{1200}{2\cdot 5} + \frac{1200}{3\cdot 5} - \frac{1200}{2\cdot 3\cdot 5} = 320.$$

Wenn wir 1200 auf der linken Seite der obigen Gleichung ausklammern, dann kann das, was übrigbleibt, in eine nette Produktform umgewandelt werden (überprüfen Sie die Berechnungen!):

$$1200 \cdot \left(1 - \frac{1}{2} - \frac{1}{3} - \frac{1}{5} + \frac{1}{2\cdot 3} + \frac{1}{2\cdot 5} + \frac{1}{3\cdot 5} - \frac{1}{2\cdot 3\cdot 5}\right)$$

$$= 1200 \cdot \left(1 - \frac{1}{2}\right) \cdot \left(1 - \frac{1}{3}\right) \cdot \left(1 - \frac{1}{5}\right).$$

Sei $n$ eine natürliche Zahl. Wir bezeichnen die Anzahl der Zahlen, die teilerfremd zu $n$ und nicht größer als $n$ sind, mit $\phi(n)$. (Wir verwenden hier „nicht größer“ anstelle von „kleiner“ . Dies ist jedoch nur für $n = 1$ von Bedeutung, da dies der einzige Fall ist, bei dem eine Zahl teilerfremd zu sich selbst ist, also $\phi(1) = 1$ gilt.). Primzahlen besitzen selbstverständlich die meisten zu sich teilerfremden Zahlen: Ist $p$ eine Primzahl, dann wird jede kleinere natürliche Zahl in $\phi(p)$ mitgezählt, es gilt also $\phi(p) = p - 1$. Die Zahl $\phi(n)$ kann im Allgemeinen so, wie wir es in dem konkreten Fall oben getan haben, berechnet werden: *Sind $p_1, p_2, \ldots, p_r$ alles verschiedene Primfaktoren von $n$, dann gilt*

$$\phi(n) = n \cdot \left(1 - \frac{1}{p_1}\right) \cdot \left(1 - \frac{1}{p_2}\right) \cdots \left(1 - \frac{1}{p_r}\right). \tag{43}$$

Der Beweis folgt den obigen Berechnungen und wird als Übungsaufgabe 6.9.2 gestellt.

**Übung 6.9.2** Beweisen Sie (43).

**Übung 6.9.3** Sei $n$ eine natürliche Zahl. Wir berechnen $\phi(d)$ für jeden Teiler $d$ von $n$ und addiere diese Zahlen anschließend. Wie lautet die Summe? (Man experimentiere, formuliere eine Vermutung und beweise sie.)

**Übung 6.9.4** Wir addieren alle natürlichen Zahlen, die kleiner als $n$ und teilerfremd zu $n$ sind. Was erhalten wir?

**Übung 6.9.5** Beweisen Sie folgende Erweiterung von Fermats Satz: Ist $\mathrm{ggT}(a, b) = 1$, dann ist $a^{\phi(b)} - 1$ durch $b$ teilbar.
[Hinweis: Verallgemeinern Sie den Beweis für den Satz von Fermat aus Übungsaufgabe 6.5.4.]

## 6.10 Wie prüft man, ob eine Zahl eine Primzahl ist?

6.10

Ist 123.456 eine Primzahl? Natürlich nicht, denn sie ist gerade! Ist 1.234.567 eine Primzahl? Dies ist nicht so einfach zu beantworten. Aber wenn man gezwungen wird, kann man alle Zahlen $2, 3, 4, 5 \ldots$ ausprobieren, um zu sehen, ob es sich dabei um einen Teiler handelt. Besitzt man die Geduld, bis 127 zu kommen, ist man fertig: $1.234.567 = 127 \cdot 9721$.
Wie sieht es mit 1.234.577 aus? Man kann wieder versuchen einen Teiler zu finden, indem man jede Zahl $2, 3, 4, 5, \ldots$ betrachtet. Diesmal wird man jedoch keinen echten Teiler finden! Wenn man wirklich geduldig ist und bis zur Quadratwurzel von 1.234.577 weitermacht, die übrigens $1111,1 \ldots$ beträgt, dann weiß man immerhin, dass man keinen echten Teiler mehr finden wird (warum?).
Wie sieht es jedoch mit der Zahl

$$1.111.222.233.334.444.555.566.667.777.888.899.967$$

aus? Ist es eine Primzahl (sie ist eine), dann müssen wir alle Zahlen bis zu ihrer Quadratwurzel ausprobieren. Ihre Quadratwurzel ist größer als $10^{18}$, da die Zahl größer als $10^{36}$ ist. Mehr als $10^{18}$ Zahlen auszuprobieren, ist selbst für den leistungsfähigsten Computer der Welt ein hoffnungsloses Unterfangen.

**Der Fermat-Test.** Wie können wir feststellen, ob diese Zahl eine Primzahl ist? Nun, unser Computer sagt es uns. Aber woher weiß es der Computer? Einen Ansatz liefert uns der Satz von Fermat. Der kleinste nicht-triviale Fall besagt, *ist $p$ eine Primzahl, dann gilt $p \mid 2^p - 2$*. Nehmen wir an, $p$ ist ungerade (was lediglich den Fall $p = 2$ ausschließt), dann wissen wir, dass $p \mid 2^{p-1} - 1$ gilt.

Was passiert, wenn wir die Teilbarkeitsbedingung $n \mid 2^{n-1} - 1$ für zusammengesetzte Zahlen testen? Sie ist offensichtlich nicht erfüllt, falls $n$ gerade ist (keine gerade Zahl ist ein Teiler einer ungeraden Zahl). Also beschränken wir unsere Aufmerksamkeit auf ungerade Zahlen. Hier sind einige Ergebnisse:

$$9 \nmid 2^8 - 1 = 255, \qquad 15 \nmid 2^{14} - 1 = 16.383, \qquad 21 \nmid 2^{20} - 1 = 1.048.575,$$

$$25 \nmid 2^{24} - 1 = 16.777.215.$$

Dies suggeriert uns, es sei vielleicht möglich, anhand der Bedingung $n \mid 2^{n-1} - 1$ zu testen, ob eine Zahl eine Primzahl ist oder nicht. Das ist eine nette Idee, allerdings hat sie einige bedeutende Mängel.

**Wie man GROSSE Potenzen berechnet.** Es ist leicht, die Formel $2^{n-1} - 1$ aufzuschreiben. Aber es ist etwas ganz anderes, dies zu berechnen! Scheinbar müssen wir die 2 noch $n - 2$ mal mit 2 multiplizieren, um $2^{n-1}$ zu erhalten. Für eine 100-stellige Zahl $n$ bedeutet dies, es müssen ungefähr $10^{100}$ Schritte ausgeführt werden, was wir niemals durchführen können.
Wir können jedoch bei der Berechnung von $2^{n-1}$ auch ein wenig trickreicher vorgehen. Veranschaulichen wir dies am Beispiel $2^{24}$: Wir könnten mit $2^3 = 8$ beginnen, Quadrieren ergibt $2^6 = 64$. Erneutes Quadrieren ergibt $2^{12} = 4096$ und ein weiteres mal Quadrieren führt zu $2^{24} = 16.777.216$. Anstelle von 23 Multiplikationen brauchten wir nur 5.
Es scheint, als wenn dieser Trick nur deshalb funktionieren würde, weil 24 durch eine solch große Potenz von 2 teilbar ist und wir daher $2^{24}$, ausgehend von einer kleinen Zahl, durch wiederholtes Quadrieren bestimmen konnten. Wir zeigen nun, wie man einen ähnlichen Trick durchführen kann, wenn der Exponent eine weniger freundliche ganze Zahl, wie zum Beispiel 29, ist. Hier ist eine Möglichkeit $2^{29}$ zu berechnen:

$$2^2 = 4, \quad 2^3 = 8, \quad 2^6 = 64, \quad 2^7 = 128, \quad 2^{14} = 16.384,$$

$$2^{28} = 268.435.456, \quad 2^{29} = 536.870.912.$$

Es ist vielleicht das Beste, diese Sequenz rückwärts zu lesen: Müssen wir eine ungerade Potenz von 2 berechnen, dann erreichen wir dies, indem wir die vorhergehende Potenz mit 2 multiplizieren. Haben wir eine gerade Potenz zu berechnen, quadrieren wir eine geeignete kleinere Potenz.

---

**Übung 6.10.1** Zeigen Sie, dass $2^n$ mit weniger als $2k$ Multiplikationen berechnet werden kann, falls $n$ zur Basis 2 die Anzahl von $k$ Bits besitzt.

**Wie man GROSSE Zahlen vermeidet.** Wir haben gezeigt, wie man die erste Schwierigkeit bewältigt, aber die obigen Berechnungen offenbaren schon die zweite: Die Zahlen werden zu groß! Sagen wir, eine Zahl $n$ besitzt 100 Stellen, dann ist nicht nur $2^{n-1}$ selbst astronomisch groß, sondern schon die Anzahl der Stellen dieser Potenz ist astronomisch! Wir könnten sie niemals aufschreiben, geschweige denn prüfen, ob sie durch $n$ teilbar ist.

Der Ausweg besteht darin, sobald wir eine Zahl größer als $n$ haben, diese mit Rest durch $n$ zu teilen und dann nur noch mit diesem Rest der Division zu arbeiten. (Wir könnten auch sagen, wir arbeiten in modularer Arithmetik mit dem Modul $n$. Wir werden keine Divisionen ausführen müssen, daher braucht $n$ keine Primzahl zu sein.) Wollen wir beispielsweise prüfen, ob $25 \mid 2^{24}-1$ gilt, dann müssen wir $2^{24}$ berechnen. Wie oben beginnen wir mit der Berechnung von $2^3 = 8$. Danach Quadrieren wir, um $2^6 = 64$ zu erhalten. Nun wird dies unverzüglich durch den Rest der Division $64 \div 25$ ersetzt. Dieser beträgt 14. Dann berechnen wir $2^{12}$, indem wir $2^6$ quadrieren. Allerdings wird nun anstelle von 64 die 14 quadriert, um 196 zu erhalten, was wiederum durch den Rest bei der Division $196 \div 25$ ersetzt wird. Dieser beträgt 21. Schließlich erhalten wir $2^{24}$ durch das Quadrieren von $2^{12}$. Allerdings quadrieren wir stattdessen 21 und erhalten 441, was wir nun durch 25 teilen, um den Rest 16 zu erhalten. Da sich $16 - 1 = 15$ nicht durch 25 teilen läßt, folgt, dass 25 keine Primzahl ist.

Das hört sich, angesichts der Trivialität dieses Ergebnisses, nicht gerade nach einer eindrucksvollen Folgerung an, aber dies war ja auch nur zur Illustration gedacht. Wenn $n$ nun $k$ Bits zur Basis 2 hat, dann haben wir gesehen, dass es nur $2k$ Multiplikationen bedarf, um $2^n$ zu berechnen. Um die Zahlen dabei klein zu halten, müssen wir lediglich in jedem Schritt eine Division (mit Rest) ausführen. Wir müssen uns daher nie mit Zahlen beschäftigen, die größer als $n^2$ sind. Wenn $n$ nun 100 Stellen besitzt, dann hat $n^2$ davon 199 oder 200. Solche Zahlen von Hand zu multiplizieren macht nicht besonders viel Spass, aber mit einem Computer ist dies recht einfach.

**Pseudoprimzahlen.** Hier kommt die dritte Schwäche des auf Fermats Satz gründenden Primzahltests. Angenommen, wir führen den Test für eine Zahl $n$ aus. Schlägt er fehl (das bedeutet, $n$ ist kein Teiler von $2^{n-1}-1$), dann wissen wir natürlich, dass $n$ keine Primzahl ist. Aber angenommen, wir finden heraus, es gilt $n \mid 2^{n-1}-1$. Können wir daraus schließen, dass $n$ eine Primzahl ist? Mit Fermats Satz kann diese Schlussfolgerung sicherlich nicht begründet werden. Gibt es zusammengesetzte Zahlen $n$, für die $n \mid 2^{n-1}-1$ gilt? Unglücklicherweise lautet die Antwort „ja“ . Die kleinste dieser Zahlen ist $341 = 11 \cdot 31$. Sie ist keine Primzahl, aber es gilt

$$341 \mid 2^{340} - 1. \tag{44}$$

(Woher wissen wir ohne umfangreiche Berechnungen, dass diese Teilbarkeitsbeziehung gilt? Wir können Fermats Satz verwenden. Es reicht zu zeigen, dass sowohl 11 als auch 31 Teiler von $2^{340}-1$ sind, denn dann gilt dies auch für ihr Produkt. 11 und

31 sind unterschiedliche Primzahlen. Nach Fermats Satz gilt

$$11 \mid 2^{10} - 1.$$

Nun ziehen wir das Ergebnis von Übungsaufgabe 6.1.6 heran: Es impliziert

$$2^{10} - 1 \mid 2^{340} - 1.$$

Daher gilt

$$11 \mid 2^{340} - 1.$$

Für 31 brauchen wir Fermats Satz gar nicht, sondern nur wieder Übungsaufgabe 6.1.6:

$$31 = 2^5 - 1 \mid 2^{340} - 1.$$

Dies beweist (44).)
Solche Zahlen, die selbst keine Primzahlen sind, sich jedoch insofern wie Primzahlen verhalten, als der Satz von Fermat mit Basis $a = 2$ für sie zutrifft, werden *Pseudoprimzahlen* (falsche Primzahlen) genannt oder noch etwas präziser, Pseudoprimzahlen zur Basis 2. Obwohl solche Zahlen ziemlich selten sind (es gibt zwischen 1 und 10.000 lediglich 22 Pseudoprimzahlen zur Basis 2), zeigen sie, dass unser Primzahltest „falsche positive“ Ergebnisse liefern kann und daher (im mathematischen Sinne) überhaupt kein Primzahltest ist.
(Können wir es uns erlauben, hin und wieder einen Fehler zu machen, dann können wir auch mit dem einfachen Fermat-Test zur Basis 2 leben. Wenn das Schlimmste, was passieren kann, in einem abstürzenden Computerspiel besteht, dann können wir das riskieren. Hängt jedoch die Sicherheit einer Bank oder eines Landes davon ab, dass keine „falsche Primzahl“ verwendet wird, dann müssen wir noch etwas besseres finden.)
Eine Idee zu unserer Rettung besteht darin, dass wir noch gar nicht die volle Leistungsstärke des Satzes von Fermat verwendet haben:
Wir können nämlich auch $n \mid 3^n - 3$, $n \mid 5^n - 5$, etc. prüfen. Diese Tests können wir mit Hilfe derselben Tricks ausführen, wie wir oben beschrieben haben. Schon durch den ersten dieser Tests wird tatsächlich die „falsche Primzahl“ 341 ausgeschlossen: Sie ist kein Teiler von $3^{340} - 1$.
Die folgende Beobachtung sagt uns, dies funktioniert immer, zumindest wenn wir genügend Geduld besitzen:

*Eine natürliche Zahl $n > 1$ ist genau dann eine Primzahl, wenn sie für jede Basis $a = 1, 2, 3, \ldots, n - 1$ den Fermat-Test*

$$n \mid a^{n-1} - 1$$

*erfüllt.*

Der Satz von Fermat sagt uns, dass Primzahlen den Fermat-Test für jede Basis erfüllen. Andererseits, falls $n$ eine zusammengesetzte Zahl ist, gibt es Zahlen $a$, $1 \leq a \leq n-1$, die nicht teilerfremd zu $n$ sind. Mit keiner dieser Zahlen wird der Fermat-Test erfüllt: Ist $p$ ein gemeinsamer Primteiler von $a$ und $n$, dann ist $p$ auch ein Teiler von $a^{n-1}$ und kann daher kein Teiler von $a^{n-1}-1$ sein. Deshalb kann $n$ ebenfalls kein Teiler von $a^{n-1}-1$ sein.

Dieser allgemeine Fermat-Test ist jedoch nicht effizient genug. Stellen wir uns vor, wir haben eine Zahl $n$ mit einigen hundert Stellen gegeben und wir möchten prüfen, ob es sich hierbei um eine Primzahl handelt oder nicht. Wir können den Fermat-Test zur Basis 2 durchführen. Angenommen, die Zahl erfüllt diesen Test, dann können wir ihn zur Basis 3 versuchen. Angenommen, sie erfüllt auch diesen Test, etc.. Wie lange müssen wir so fortfahren, bevor wir darauf schließen können, dass $n$ eine Primzahl oder eine zusammengesetzte Zahl ist? Wir sehen anhand der Argumentation, die den allgemeinen Fermat-Test rechtfertigt, dass wir nicht weiter als bis zur ersten Zahl, die einen gemeinsamen Teiler mit $n$ besitzt, gehen müssen. Man sieht leicht, dass die kleinste dieser Zahlen der kleinste Primteiler von $n$ ist. Gilt beispielsweise $n = pq$, wobei $p$ und $q$ unterschiedliche jeweils 100-stellige Primzahlen sind (also besitzt $n$ 199 oder 200 Stellen), dann müssen wir bis zum kleineren der beiden Werte von $p$ und $q$ jede Zahl ausprobieren. Das ergibt mehr als $10^{99}$ Versuche und ist damit hoffnungslos. (Außerdem können wir bei so einem Vorgehen auch gleich einfache Teilbarkeitstests durchführen und brauchen so etwas wie den Satz von Fermat gar nicht!)

Wir könnten anstelle von 2 auch mit irgendeiner anderen Basis $a$ beginnen und prüfen, ob Fermats Satz damit gilt. Es wäre zum Beispiel möglich, eine ganze Zahl $a$ mit $1 \leq a \leq n-1$ zufällig auszuwählen. Wir wissen, dass der Test nicht erfüllt ist, wenn $a$ nicht teilerfremd zu $n$ ist. Wenn $n$ keine Primzahl ist, haben wir dann auf diese Weise eine gute Chance dies herauszufinden? Das hängt von $n$ ab. Einige Werte von $n$ sind jedoch definitiv nicht gut. Nehmen wir zum Beispiel an, wir haben $n = pq$, wobei $p$ und $q$ unterschiedliche Primzahlen sind. Es ist einfach, alle Zahlen $a$ aufzulisten, die nicht teilerfremd zu $n$ sind: Dies sind die Vielfachen von $p$ ($p, 2p, \ldots, (q-1)p, qp$) und die Vielfachen von $q$ ($q, 2q, \ldots, (p-1)q, pq$). Die Gesamtzahl solcher Zahlen $a$ beträgt $q + p - 1$ (da $pq = n$ in beiden Listen vorkommt). Diese Zahl ist größer als $2 \cdot 10^{99}$, aber kleiner als $2 \cdot 10^{100}$. Somit beträgt die Wahrscheinlichkeit, eine dieser Zahlen bei einer zufälligen Wahl von $a$ zu treffen, weniger als

$$\frac{2 \cdot 10^{100}}{10^{199}} = 2 \cdot 10^{-99}.$$

Das zeigt, dass dieses Ereignis eine viel zu geringe Wahrscheinlichkeit besitzt, um jemals in der Praxis aufzutreten.

**Carmichael-Zahlen.** Unsere nächste Hoffnung besteht darin, dass der Fermat-Test für eine zusammengesetzte Zahl $n$ vielleicht viel eher als für ihren kleinsten Primteiler nicht erfüllt ist; oder aber, dass er bei einer zufälligen Wahl von $a$ für eine Menge

anderer Zahlen, neben den zu $n$ nicht teilerfremden, fehlschlägt. Dies ist unglücklicherweise nicht immer der Fall. Es gibt ganze Zahlen $n$, *Carmichael-Zahlen* genannt, die sogar noch schlimmer als Pseudoprimzahlen sind: Sie erfüllen den Fermat-Test für jede zu $n$ teilerfremde Basis $a$. Mit anderen Worten, es gilt

$$n \mid a^{n-1} - 1$$

für jedes $a$ mit $\mathrm{ggT}(n, a) = 1$. Die kleinste dieser Zahlen ist $n = 561$. Obwohl solche Zahlen sehr selten vorkommen, zeigen sie doch, dass der Fermat-Test nicht vollkommen zufrieden stellend ist.

**Der Miller–Rabin Test.** In den späten 70-er Jahren des 20. Jahrhunderts haben M. Rabin and G. Miller eine sehr einfache Möglichkeit gefunden, den Satz von Fermat ein bisschen zu verstärken und dadurch die durch die Carmichael-Zahlen verursachten Schwierigkeiten zu bewältigen. Wir veranschaulichen das Verfahren anhand des Beispiels $561$. Zum Faktorisieren der Zahl $a^{560} - 1$ verwenden wir ein wenig Schulmathematik, nämlich die Gleichung $x^2 - 1 = (x - 1)(x + 1)$:

$$\begin{aligned} a^{560} - 1 &= \big(a^{280} - 1\big)\big(a^{280} + 1\big) \\ &= \big(a^{140} - 1\big)\big(a^{140} + 1\big)\big(a^{280} + 1\big) \\ &= \big(a^{70} - 1\big)\big(a^{70} + 1\big)\big(a^{140} + 1\big)\big(a^{280} + 1\big) \\ &= \big(a^{35} - 1\big)\big(a^{35} + 1\big)\big(a^{70} + 1\big)\big(a^{140} + 1\big)\big(a^{280} + 1\big). \end{aligned}$$

Wir nehmen nun an, 561 wäre eine Primzahl. Sie müsste dann nach Fermats „kleinem“ Satz $a^{560} - 1$ für jeden Wert $1 \le a \le 560$ teilen. Teilt eine Primzahl ein Produkt, so teilt sie einen der Faktoren (Übungsaufgabe 6.3.3), daher muß mindestens eine der Relationen

$$561 \mid a^{35} - 1, \quad 561 \mid a^{35} + 1, \quad 561 \mid a^{70} + 1, \quad 561 \mid a^{140} + 1, \quad 561 \mid a^{280} + 1$$

gelten. Bereits für $a = 2$ ist jedoch keine dieser Relationen wahr.
Der Miller–Rabin Test basiert auf dieser Idee. Sei eine ungerade ganze Zahl $n > 1$ gegeben. Diese möchten wir testen, ob es sich um eine Primzahl handelt. Wir wählen eine ganze Zahl $a$ aus dem Bereich $0 \le a \le n - 1$ zufällig aus und betrachten $a^n - a$. Nun faktorisieren wir dies zu $a(a^{n-1} - 1)$ und fahren unter Verwendung der Gleichheit $x^2 - 1 = (x - 1)(x + 1)$ so lange wir können mit dem Faktorisieren fort. Anschließend testen wir, ob einer der Faktoren durch $n$ teilbar ist.
Schlägt der Test fehl, dann können wir sicher sein, dass $n$ keine Primzahl ist. Was passiert jedoch, wenn der Test erfolgreich verläuft? Unglücklicherweise kann dies, selbst wenn $n$ eine zusammengesetzte Zahl ist, auch passieren. Der springende Punkt dabei ist jedoch, dass *dieser Test mit einer Wahrscheinlichkeit, die unter $\frac{1}{2}$ liegt, ein falsches positives Ergebnis liefert* (man entsinne sich daran, dass wir $a$ zufällig gewählt hatten).

In der Hälfte der Fälle ein falsches Ergebnis zu erzielen, hört sich allerdings gar nicht gut an. Wir können das Experiment jedoch mehrmals wiederholen. Wenn wir es 10 mal wiederholen (jedes mal sei $a$ aufs Neue zufällig ausgewählt), dann beträgt die Wahrscheinlichkeit, ein falsches positives Ergebnis zu erhalten, weniger als $2^{-10} < 1/1000$ (da es für den Schluß '$n$ ist eine Primzahl', erforderlich ist, dass bei allen 10 Durchläufen unabhängig voneinander ein falsches positives Ergebnis erzielt wird). Wiederholen wir das Experiment 100 mal, dann sinkt die Wahrscheinlichkeit eines falschen positiven Ergebnisses auf unter $2^{-100} < 10^{-30}$, was astronomisch klein ist. Bei genügend häufiger Wiederholung liefert dieser Algorithmus demnach einen Primzahltest, dessen Fehlerwahrscheinlichkeit viel geringer als beispielsweise ein Hardwarefehler ist. Daher ist er für praktische Zwecke ziemlich geeignet. Er ist weit verbreitet und wird in Programmen, wie zum Beispiel Maple und Mathematica, sowie in der Kryptographie verwendet.

Angenommen, wir testen eine Zahl $n$ auf Primzahleigenschaften und finden heraus, dass sie zusammengesetzt ist. Wir würden dann auch gerne ihre Primfaktorzerlegung bestimmen. Es ist leicht einzusehen, dass wir anstatt nach einer Primfaktorzerlegung zu suchen auch weniger fordern können: Eine Zerlegung von $n$ in ein Produkt zweier kleinerer natürlicher Zahlen $n = ab$. Wenn wir eine Methode haben, solche Zerlegungen effizient zu bestimmen, dann können wir mit Primzahltests an $a$ und $b$ fortfahren. Handelt es sich bei ihnen um Primzahlen, dann haben wir die Primfaktorzerlegung von $n$ gefunden. Wenn (zum Beispiel) $a$ keine Primzahl ist, dann können wir unsere Methode zur Zerlegung von $a$ in ein Produkt zweier kleinerer natürlicher Zahlen anwenden, etc.. Da $n$ höchstens $\log_2 n$ Primfaktoren besitzt (Übungsaufgabe 6.3.4), müssen wir dies auch höchstens $\log_2 n$ mal wiederholen (was weniger als die Anzahl der Bits ist).
Unglücklicherweise (oder glücklicherweise, siehe Kapitel 15 über Kryptographie) ist jedoch keine effiziente Methode zur Zerlegung einer Zahl in ein Produkt zweier kleinerer ganzer Zahlen bekannt. Es wäre sehr wichtig, eine effiziente Methode zur Faktorisierung zu finden oder einen mathematischen Beweis zu erbringen, dass eine solche Methode nicht existiert. Wie die Antwort hier lauten wird, wissen wir jedoch nicht.

---

**Übung 6.10.2** Zeigen Sie, dass $561$ eine Carmicheal-Zahl ist. Genauer: Zeigen Sie, dass $561 \mid a^{561} - a$ für alle ganzen Zahlen $a$ gilt. [Hinweis: Da $561 = 3 \cdot 11 \cdot 17$ gilt, reicht es zu zeigen, dass $3 \mid a^{561} - a$, $11 \mid a^{561} - 1$ und $17 \mid a^{561} - a$. Beweisen Sie diese Relationen einzeln und verwenden Sie dazu die Methode des Beweises für $341 \mid 2^{340} - 1$.]

## Gemischte Übungsaufgaben

**Übung 6.10.3** Beweisen Sie, wenn $c \neq 0$ und $ac \mid bc$, dann gilt $a \mid b$.

**Übung 6.10.4** Beweisen Sie, wenn $a \mid b$ und $a \mid c$, dann gilt $a \mid b^2 + 3c + 2^b c$.

**Übung 6.10.5** Beweisen Sie, dass jede Primzahl, die größer als 3 ist, beim Teilen durch 6 den Rest 1 oder $-1$ besitzt.

**Übung 6.10.6** Sei $a > 1$ und $k, n > 0$. Beweisen Sie, dass $a^k - 1 \mid a^n - 1$ genau dann gilt, wenn $k \mid n$.

**Übung 6.10.7** Zeigen Sie: Ist $a > 3$, dann können $a$, $a + 2$ und $a + 4$ nicht alle Primzahlen sein. Kann es sich bei ihnen um Potenzen von Primzahlen handeln?

**Übung 6.10.8** Wie viele ganze Zahlen gibt es, die sich weder durch eine Primzahl, die größer als 20 ist, teilen lassen, noch durch das Quadrat einer Primzahl?

**Übung 6.10.9** Bestimmen Sie die Primfaktorzerlegung von (a) $\binom{20}{10}$ und (b) $20!$.

**Übung 6.10.10** Zeigen Sie, dass eine 30-stellige Zahl nicht mehr als 100 Primfaktoren besitzen kann.

**Übung 6.10.11** Zeigen Sie, dass eine 160-stellige Zahl eine Primzahlpotenz als Teiler besitzt, deren Wert mindestens 100 beträgt. Dies gilt nicht, wenn wir als Teiler eine Primzahl verlangen, die mindestens den Wert 100 hat.

**Übung 6.10.12** Bestimmen Sie die Anzahl der (positiven) Teiler von $n$, für $1 \leq n \leq 20$ (Beispiel: 6 besitzt 4 Teiler: 1, 2, 3, 6). Welche dieser Zahlen besitzt eine ungerade Anzahl von Teilern? Formulieren Sie eine Vermutung und beweisen Sie sie.

**Übung 6.10.13** Bestimmen Sie unter Verwendung des euklidischen Algorithmus den größten gemeinsamen Teiler von 100 und 254.

**Übung 6.10.14** Bestimmen Sie Paare ganzer Zahlen, für die der euklidische Algorithmus (a) 2 Schritte und (b) 6 Schritte dauert.

**Übung 6.10.15** Man entsinne sich an die in Übungsaufgabe 4.3.2 eingeführten Lucas Zahlen und beweise folgendes:
(a)$\mathrm{ggT}(F_{3k}, L_{3k}) = 2$,
(b)ist $n$ kein Vielfaches von 3, dann $\mathrm{ggT}(F_n, L_n) = 1$,
(c)$L_{6k} \equiv 2 \pmod 4$.

**Übung 6.10.16** Beweisen Sie, dass es zu jeder natürlichen Zahl $m$ eine Fibonacci Zahl gibt, die durch $m$ teilbar ist. (Nun, $F_0 = 0$ ist selbstverständlich durch jedes $m$ teilbar. Wir meinen eine größere.)

**Übung 6.10.17** Finden Sie zwei ganze Zahlen $x$ und $y$, so dass $25x + 41y = 1$ gilt.

**Übung 6.10.18** Finden Sie zwei ganze Zahlen $x$ und $y$, so dass gilt:

$$2x + y \equiv 4 \pmod{17},$$

$$5x - 5y \equiv 9 \pmod{17}.$$

**Übung 6.10.19** Beweisen Sie, dass $\sqrt[3]{5}$ irrational ist.

**Übung 6.10.20** Beweisen Sie, dass die beiden Formen des Satzes von Fermat, Satz 6.5.1 und (37) äquivalent sind.

**Übung 6.10.21** Zeigen Sie: Ist $p > 2$ ein Primzahlmodul, dann gilt

$$\frac{\overline{1}}{\overline{2}} = \overline{\frac{p+1}{2}}.$$

**Übung 6.10.22** Uns seien $n + 1$ Zahlen aus der Menge $\{1, 2, \ldots, 2n\}$ gegeben. Beweisen Sie, dass sich darunter zwei Zahlen befinden, bei denen die eine durch die andere teilbar ist.

**Übung 6.10.23** Wie lautet die Anzahl der natürlichen Zahlen, die nicht größer als 210 sind und sich nicht durch 2, 3 oder 7 teilen lassen?