

Zahlentheorie

Einleitung

Ihren mystischen Nimbus haben die natürlichen Zahlen nach und nach verloren; aber niemals ist das Interesse von Mathematikern und Laien an den Gesetzen der Zahlenwelt schwächer geworden. Es mag sein, daß EUKLID's Ruhm auf der geometrischen Deduktion seiner „Elemente“ beruht; bis heute haben die „Elemente“ jedenfalls den Unterricht in der Geometrie entscheidend beeinflusst. Und doch war EUKLID's Geometrie im wesentlichen eine Zusammenstellung älterer Ergebnisse, während seine Beiträge zur Zahlentheorie anscheinend originelle Leistungen waren. DIOPHANT von Alexandria (etwa 275 n. Chr.) hat später die Zahlentheorie wesentlich weiter entwickelt. PIERRE DE FERMAT (1601–1665), ein Jurist aus Toulouse und einer der größten Mathematiker der neueren Zeit, begründete die moderne Zahlentheorie. EULER (1707–1783), vielleicht der erfindungsreichste Mathematiker überhaupt, hat die Zahlentheorie durch viele Arbeiten und Beiträge bereichert. Große Namen in den Annalen der Mathematik – LEGENDRE, RIEMANN, DIRICHLET – können dieser Liste hinzugefügt werden. GAUSS (1777 bis 1855), der hervorragendste und vielseitigste Mathematiker der Neuzeit, hat seine Begeisterung für die Zahlentheorie in die Worte gefaßt: „Die Mathematik ist die Königin der Wissenschaften, und die Zahlentheorie ist die Königin der Mathematik.“

§ 1. Die Primzahlen

1. Grundtatsachen

Die meisten Aussagen der Zahlentheorie, wie überhaupt der ganzen Mathematik, betreffen nicht einzelne Objekte – die Zahl 5 oder die Zahl 32 – sondern ganze Klassen von Objekten, charakterisiert durch eine gemeinsame Eigenschaft, wie die Klasse der geraden Zahlen

$2, 4, 6, 8, \dots$

oder die Klasse aller durch 3 teilbaren Zahlen

$3, 6, 9, 12, \dots$

oder die Klasse aller Quadrate ganzer Zahlen

$1, 4, 9, 16, \dots$

und so weiter.

Von grundlegender Bedeutung in der Zahlentheorie ist die Klasse der *Primzahlen*. Die meisten positiven ganzen Zahlen können in kleinere Faktoren zerlegt werden: $10 = 2 \cdot 5$, $111 = 3 \cdot 37$, $144 = 3 \cdot 3 \cdot 2 \cdot 2 \cdot 2 \cdot 2$ usw. Zahlen, die sich

nicht zerlegen lassen, heißen Primzahlen. Genauer ausgedrückt ist *eine Primzahl eine ganze Zahl p größer als 1, die keine anderen Faktoren enthält als sich selbst und eins*. (Eine Zahl a heißt ein *Faktor* oder *Teiler* einer Zahl b , wenn es eine Zahl c gibt, so daß $b = ac$.) Die Zahlen 2, 3, 5, 7, 11, 13, 17, . . . sind Primzahlen, während z. B. 12 keine ist, da $12 = 3 \cdot 4$. Die große Bedeutung der Klasse der Primzahlen beruht darauf, daß *jede* positive ganze Zahl ($\neq 1$) als *Produkt von Primzahlen* darstellbar ist: Wenn eine Zahl nicht selbst eine Primzahl ist, kann sie schrittweise in Faktoren zerlegt werden, bis alle Faktoren Primzahlen sind; so ist z. B. $360 = 3 \cdot 120 = 3 \cdot 30 \cdot 4 = 3 \cdot 3 \cdot 10 \cdot 2 \cdot 2 = 3 \cdot 3 \cdot 5 \cdot 2 \cdot 2 \cdot 2 = 2^3 \cdot 3^2 \cdot 5$. Eine positive ganze, von 1 verschiedene Zahl, die keine Primzahl ist, bezeichnet man als *zerlegbar* oder *zusammengesetzt*.

Eine der ersten Fragen über die Primzahlen ist, ob es nur eine endliche Anzahl verschiedener Primzahlen gibt, oder ob die Menge der Primzahlen unendlich viele Elemente enthält, wie die Menge aller natürlichen Zahlen, von der sie ein Teil ist. Die Antwort lautet: *Es gibt unendlich viele Primzahlen*.

Der Beweis für die Unendlichkeit der Menge der Primzahlen, den EUKLID gibt, wird immer ein Musterbild mathematischer Schlußweise bleiben. Er verfährt nach der „indirekten Methode“. Wir machen zunächst versuchsweise die Annahme, daß der Satz falsch ist. Das bedeutet, daß es nur endlich viele Primzahlen gibt, vielleicht sehr viele — etwa eine Billion — aber jedenfalls eine bestimmte endliche Anzahl n . Mit Hilfe der Indexschreibweise können wir diese Primzahlen mit p_1, p_2, \dots, p_n bezeichnen. Jede andere Zahl wird dann zerlegbar sein und muß durch mindestens eine der Zahlen p_1, p_2, \dots, p_n teilbar sein. Wir werden jetzt einen Widerspruch aufzeigen, indem wir eine Zahl A angeben, die von sämtlichen Primzahlen p_1, p_2, \dots, p_n verschieden ist, weil sie größer ist als jede von ihnen, und die doch durch keine von ihnen teilbar ist. Diese Zahl ist

$$A = p_1 p_2 \dots p_n + 1,$$

d. h. um eins größer als das Produkt der Zahlen, von denen wir angenommen hatten, daß sie die sämtlichen Primzahlen wären. A ist größer als jede der Primzahlen und muß daher zerlegbar sein. Aber bei Division durch p_1 oder durch p_2 oder durch irgendein p läßt A immer den Rest 1, daher hat A keine der Zahlen p als Teiler. Unsere ursprüngliche Annahme, daß es nur eine endliche Anzahl von Primzahlen gäbe, führt zu einem Widerspruch, also ist die Annahme unsinnig, und daher muß ihr Gegenteil zutreffen.

Obwohl dieser Beweis indirekt ist, kann er leicht so abgeändert werden, daß er wenigstens im Prinzip eine Methode zur Herstellung einer unendlichen Folge von Primzahlen liefert. Beginnen wir mit irgendeiner Primzahl, z. B. $p_1 = 2$, und nehmen wir an, daß wir n Primzahlen p_1, p_2, \dots, p_n kennen, so bemerken wir (wie oben), daß $p_1 p_2 \dots p_n + 1$ entweder selbst eine Primzahl ist oder einen Primfaktor haben muß, der von den bereits bekannten verschieden ist. Da dieser Faktor immer durch einfaches Probieren gefunden werden kann, so sind wir sicher, daß wir jedenfalls eine neue Primzahl p_{n+1} finden können. Fahren wir in derselben Weise fort, so sehen wir, daß die Folge der konstruierbaren Primzahlen niemals abbricht.

Übung: Man führe diese Konstruktion durch, indem man mit $p_1 = 2, p_2 = 3$ beginnt und 5 weitere Primzahlen bestimmt.

Wenn eine Zahl als Produkt von Primzahlen dargestellt ist, so können wir diese Primfaktoren in beliebiger Reihenfolge anordnen. Ein wenig Probieren läßt keinen Zweifel, daß, abgesehen von dieser Willkür in der Anordnung, die Zerlegung einer

Zahl N in Primfaktoren eindeutig ist: *Jede ganze Zahl N größer als 1 kann nur auf eine einzige Art als Produkt von Primzahlen geschrieben werden.* Diese Behauptung erscheint auf den ersten Blick so naheliegend, daß man geneigt ist, sie für selbstverständlich zu halten. Aber sie ist keineswegs eine Trivialität; der Beweis erfordert, obwohl er durchaus elementar ist, einen gewissen Scharfsinn. Der klassische Beweis, den EUKLID für diesen „Fundamentalsatz der Arithmetik“ gibt, stützt sich auf ein Verfahren oder „Algorithmus“ zur Auffindung des größten gemeinsamen Teilers zweier Zahlen. Dies wird auf S. 35 f. erörtert werden. Hier wollen wir statt dessen einen Beweis jüngerer Datums bringen, der etwas kürzer und vielleicht etwas raffinierter ist als der euklidische. Er ist ein typisches Beispiel eines indirekten Beweises. Wir werden annehmen, daß es eine natürliche Zahl gibt, die auf zwei wesentlich verschiedene Weisen in Primzahlen zerlegt werden kann, und aus dieser Annahme werden wir einen Widerspruch herleiten. Dieser Widerspruch wird zeigen, daß die Annahme der Existenz einer Zahl mit zwei wesentlich verschiedenen Primzahlzerlegungen unhaltbar ist, und daß folglich die Primzahlzerlegung jeder Zahl eindeutig ist.

*Wenn es eine positive ganze Zahl gibt, die in zwei wesentlich verschiedene Produkte von Primzahlen zerlegt werden kann, dann muß es eine *kleinste* solche Zahl m geben (siehe S. 15). Für diese gilt

$$(1) \quad m = p_1 p_2 \cdots p_r = q_1 q_2 \cdots q_s,$$

worin die p und q Primzahlen sind. Wenn wir die Reihenfolge der p und q nötigenfalls abändern, dürfen wir annehmen, daß

$$p_1 \leq p_2 \leq \cdots \leq p_r, \quad q_1 \leq q_2 \leq \cdots \leq q_s.$$

Nun kann p_1 nicht gleich q_1 sein; denn wenn das der Fall wäre, könnten wir von beiden Seiten der Gleichung (1) den ersten Faktor wegheben und erhielten zwei wesentlich verschiedene Primzahlzerlegungen einer positiven ganzen Zahl kleiner als m ; dies wäre ein Widerspruch dagegen, daß wir m als die *kleinste* Zahl dieser Eigenschaft gewählt hatten. Daher ist entweder $p_1 < q_1$ oder $q_1 < p_1$. Nehmen wir an, es sei $p_1 < q_1$. (Wenn $q_1 < p_1$, brauchen wir nur die Buchstaben p und q im folgenden zu vertauschen.) Wir bilden die ganze Zahl

$$(2) \quad m' = m - p_1 q_2 q_3 \cdots q_s.$$

Indem wir für m die beiden Ausdrücke der Gleichung (1) einsetzen, können wir m' in den folgenden beiden Formen schreiben:

$$(3) \quad m' = (p_1 p_2 \cdots p_r) - (p_1 q_2 \cdots q_s) = p_1 (p_2 p_3 \cdots p_r - q_2 q_3 \cdots q_s),$$

$$(4) \quad m' = (q_1 q_2 \cdots q_s) - (p_1 q_2 \cdots q_s) = (q_1 - p_1) (q_2 q_3 \cdots q_s).$$

Da $p_1 < q_1$, so folgt aus (4), daß m' eine positive ganze Zahl ist, während m' wegen (2) kleiner als m sein muß. Folglich muß die Primzahlzerlegung von m' , abgesehen von der Reihenfolge der Faktoren, *eindeutig* sein. Aber aus (3) ergibt sich, daß p_1 ein Faktor von m' ist, daher muß nach (4) p_1 entweder ein Teiler von $q_1 - p_1$ oder von $q_2 q_3 \cdots q_s$ sein. (Dies ergibt sich aus der angenommenen Eindeutigkeit der Zerlegung von m' , siehe die Überlegung im nächsten Absatz.) Das letzte ist unmöglich, da alle q größer sind als p_1 . Folglich muß p_1 ein Teiler von $q_1 - p_1$ sein, so daß es eine ganze Zahl h geben muß, für die

$$q_1 - p_1 = p_1 \cdot h \quad \text{oder} \quad q_1 = p_1 (h + 1).$$

Aber hiernach müßte p_1 ein Teiler von q_1 sein, im Widerspruch zu der Tatsache, daß q_1 eine Primzahl ist. Dieser Widerspruch zeigt, daß unsere ursprüngliche Annahme unhaltbar ist, und damit ist der Fundamentalsatz der Arithmetik bewiesen.

Ein wichtiges Corollar des Fundamentalsatzes ist das folgende: *Wenn eine Primzahl der Teiler eines Produktes ab ist, so muß p ein Teiler entweder von a oder von b sein.* Denn wenn p weder ein Teiler von a noch von b wäre, so würde das Produkt der Primzahlzerlegungen von a und b eine Primzahlzerlegung des Produkts ab ergeben, die p nicht enthielte. Da andererseits p nach Voraussetzung ein Faktor von ab ist, so existiert eine ganze Zahl t von der Art, daß

$$ab = pt.$$

Daher würde das Produkt von p mit einer Primfaktorzerlegung von t eine Primfaktorzerlegung der Zahl ab ergeben, in der p enthalten ist, im Widerspruch zu der Tatsache, daß ab nur eine einzige Primzahlzerlegung besitzt.

Beispiele: Wenn man festgestellt hat, daß 13 ein Faktor von 2652 ist, und daß $2652 = 6 \cdot 442$, so kann man schließen, daß 13 ein Faktor von 442 ist. Andererseits ist 6 ein Faktor von 240 und $240 = 15 \cdot 16$, aber 6 ist weder ein Faktor von 15 noch von 16. Dies zeigt, daß die Voraussetzung, daß p eine Primzahl ist, wesentlich ist.

Übung. Um alle Teiler einer beliebigen Zahl a zu finden, brauchen wir nur a in ein Produkt

$$a = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdots p_r^{\alpha_r}$$

zu zerlegen, worin die p verschiedene Primzahlen sind, die jede zu einer gewissen Potenz erhoben sind. Sämtliche Teiler von a sind die Zahlen

$$b = p_1^{\beta_1} \cdot p_2^{\beta_2} \cdots p_r^{\beta_r},$$

worin die β beliebige ganze Zahlen ≥ 0 sind, die die Ungleichungen

$$0 \leq \beta_1 \leq \alpha_1, 0 \leq \beta_2 \leq \alpha_2, \dots, 0 \leq \beta_r \leq \alpha_r$$

erfüllen. Man beweise diese Behauptung. Dementsprechend zeige man, daß die Anzahl der verschiedenen Teiler von a (einschließlich der Teiler a und 1) durch das Produkt

$$(\alpha_1 + 1)(\alpha_2 + 1) \cdots (\alpha_r + 1)$$

gegeben ist. Zum Beispiel hat

$$144 = 2^4 \cdot 3^2$$

$5 \cdot 3$ Teiler. Diese sind 1, 2, 4, 8, 16, 3, 6, 12, 24, 48, 9, 18, 36, 72, 144.

2. Die Verteilung der Primzahlen

Eine Tabelle aller Primzahlen bis zu einer gegebenen natürlichen Zahl N kann man herstellen, indem man der Reihe nach alle Zahlen bis N hinschreibt, dann diejenigen wegstreicht, die Vielfache von 2 sind, dann von den übrigen alle, die Vielfache von 3 sind, und so weiter, bis alle zerlegbaren Zahlen ausgeschieden sind. Dieses Verfahren, das „Sieb des Eratosthenes“ genannt, fängt in seinen Maschen alle Primzahlen bis zu N . Vollständige Tabellen der Primzahlen bis etwa 10000000 sind im Laufe der Zeit mit Hilfe einer verfeinerten Methode zusammengestellt worden; sie liefern uns eine ungeheure Menge empirischer Angaben über Verteilung und Eigenschaften der Primzahlen. Auf Grund dieser Tabellen lassen sich viele plausible Vermutungen aufstellen (als ob die Zahlentheorie eine Experimentalwissenschaft wäre), die häufig sehr schwierig zu beweisen sind.

a) *Formeln zur Konstruktion von Primzahlen*

Man hat versucht, einfache arithmetische Formeln zu finden, die lauter Primzahlen, wenn auch nicht alle Primzahlen liefern. FERMAT sprach die berühmte Vermutung (aber nicht die ausdrückliche Behauptung) aus, daß alle Zahlen der Form

$$F(n) = 2^{2^n} + 1$$

Primzahlen seien. Tatsächlich erhalten wir für $n = 1, 2, 3, 4$

$$F(1) = 2^2 + 1 = 5,$$

$$F(2) = 2^{2^2} + 1 = 2^4 + 1 = 17,$$

$$F(3) = 2^{2^3} + 1 = 2^8 + 1 = 257,$$

$$F(4) = 2^{2^4} + 1 = 2^{16} + 1 = 65537,$$

also stets Primzahlen. Aber im Jahre 1732 entdeckte EULER die Faktorzerlegung $2^{2^5} + 1 = 641 \cdot 6700417$, also ist $F(5)$ keine Primzahl. Später wurden noch mehr von diesen „Fermatschen Zahlen“ als zerlegbar erkannt, wobei in jedem Fall tiefere zahlentheoretische Methoden erforderlich waren, da die Schwierigkeiten des direkten Ausprobierens unüberwindlich sind. Bis heute ist noch nicht einmal bewiesen, daß irgendeine der Zahlen $F(n)$ für $n > 4$ eine Primzahl ist.

Ein anderer merkwürdiger und einfacher Ausdruck, der viele Primzahlen liefert, ist

$$f(n) = n^2 - n + 41.$$

Für $n = 1, 2, 3, \dots, 40$ sind die $f(n)$ Primzahlen, aber für $n = 41$ erhalten wir $f(n) = 41^2$, eine Zahl, die keine Primzahl ist.

Der Ausdruck

$$n^2 - 79n + 1601$$

liefert Primzahlen für alle n bis 79, versagt aber für $n = 80$. Im ganzen hat es sich als erfolgloses Bemühen erwiesen, nach Ausdrücken einfacher Art zu suchen, die nur Primzahlen liefern. Noch weniger aussichtsreich ist der Versuch, eine algebraische Formel zu finden, die *sämtliche* Primzahlen liefert.

b) *Primzahlen in arithmetischen Folgen*

Während es einfach zu beweisen war, daß in der Folge aller natürlichen Zahlen 1, 2, 3, 4, ... unendlich viele Primzahlen vorkommen, bereiten Folgen wie 1, 4, 7, 10, 13, ... oder 3, 7, 11, 15, 19, ... oder, allgemeiner, beliebige arithmetische Folgen $a, a + d, a + 2d, \dots, a + nd, \dots$, worin a und d keinen gemeinsamen Teiler haben, erhebliche Schwierigkeiten. Alle Beobachtungen wiesen auf die Tatsache hin, daß es *in jeder solchen Folge unendlich viele Primzahlen* gibt, ebenso wie in der einfachsten, 1, 2, 3, ... Der Beweis dieses allgemeinen Satzes war eine der berühmten Leistungen von LEJEUNE-DIRICHLET (1805–1859), einem der großen Meister seiner Generation. Sein Erfolg beruhte auf einer genialen Anwendung der höheren Analysis. Noch heute, nach hundert Jahren, zählt DIRICHLET'S Arbeit über diesen Gegenstand zu den hervorragenden Leistungen der Mathematik. Es ist bisher nicht gelungen, seinen Beweis so zu vereinfachen, daß er denen zugänglich ist, die nicht in der Technik der Infinitesimalrechnung und Funktionentheorie bewandert sind.

Während wir hier den Beweis für DIRICHLETs allgemeines Theorem nicht darstellen können, ist es leicht, für gewisse *spezielle* arithmetische Folgen, z. B. $4n + 3$ und $6n + 5$, den einfachen euklidischen Beweis abzuwandeln. Um die erste dieser beiden Folgen zu behandeln, bemerken wir, daß jede Primzahl größer als 2 ungerade ist (da sie sonst durch 2 teilbar wäre) und daher die Form $4n + 1$ oder $4n + 3$ hat, mit einer geeigneten ganzen Zahl n . Ferner ist das Produkt zweier Zahlen der Form $4n + 1$ wieder von dieser Form, da

$$(4a + 1)(4b + 1) = 16ab + 4a + 4b + 1 = 4(4ab + a + b) + 1.$$

Nun nehmen wir an, es gäbe nur eine endliche Anzahl von Primzahlen $p_1, p_2, p_3, \dots, p_n$ von der Form $4n + 3$, und betrachten die Zahl

$$N = 4(p_1 p_2 \dots p_n) - 1 = 4(p_1 \dots p_n - 1) + 3.$$

Entweder ist N selbst eine Primzahl, oder es kann in ein Produkt von Primzahlen zerlegt werden, unter denen p_1, p_2, \dots, p_n nicht vorkommen können, da diese, wenn N durch sie geteilt wird, den Rest -1 geben. Ferner können nicht alle Faktoren von N von der Form $4n + 1$ sein; denn N selbst ist nicht von dieser Form, und wie wir gesehen haben, ist jedes Produkt von Zahlen der Form $4n + 1$ wieder von dieser Form. Daher muß mindestens ein Primfaktor von der Form $4n + 3$ sein, und dies ist unmöglich, da keine von den Zahlen p_1, p_2, \dots, p_n , von denen wir annahmen, daß sie *alle* Primzahlen der Form $4n + 3$ darstellten, ein Faktor von N sein kann. Also führt die Annahme, daß die Anzahl der Primzahlen der Form $4n + 3$ endlich sei, zu einem Widerspruch, und folglich muß die Anzahl dieser Primzahlen unendlich sein.

Übung. Man beweise den entsprechenden Satz für die Folge $6n + 5$.

c) Der Primzahlsatz

Auf der Suche nach einem Gesetz über die Verteilung der Primzahlen wurde der entscheidende Schritt getan, als man die erfolglosen Versuche aufgab, eine einfache mathematische Formel zu finden, die *alle* Primzahlen oder die genaue Anzahl der Primzahlen unter den ersten n ganzen Zahlen angibt, und sich stattdessen mit einer Auskunft über die *durchschnittliche* Verteilung der Primzahlen unter den natürlichen Zahlen begnügte.

Für eine beliebige natürliche Zahl n möge A_n die Anzahl der Primzahlen unter den Zahlen $1, 2, 3, \dots, n$ bezeichnen. Wenn wir in einer Liste der ersten ganzen Zahlen alle Primzahlen unterstreichen:

$$1 \quad 2 \quad 3 \quad 4 \quad 5 \quad 6 \quad 7 \quad 8 \quad 9 \quad 10 \quad \underline{11} \quad 12 \quad \underline{13} \quad 14 \quad 15 \quad 16 \quad \underline{17} \quad 18 \quad \underline{19} \dots,$$

so können wir die ersten Werte von A_n feststellen:

$$A_1 = 0, \quad A_2 = 1, \quad A_3 = 2, \quad A_4 = 2, \quad A_5 = A_6 = 3, \quad A_7 = A_8 = A_9 = A_{10} = 4,$$

$$A_{11} = A_{12} = 5, \quad A_{13} = A_{14} = A_{15} = A_{16} = 6, \quad A_{17} = A_{18} = 7, \quad A_{19} = 8, \text{ usw.}$$

Wenn wir jetzt eine beliebige Folge von Werten n nehmen, die unbegrenzt zunimmt, sagen wir

$$n = 10, 10^2, 10^3, 10^4, \dots,$$

dann werden die zugehörigen Werte von A_n ,

$$A_{10}, A_{10^2}, A_{10^3}, A_{10^4}, \dots,$$

ebenfalls unbegrenzt zunehmen (allerdings langsamer). Da, wie wir wissen, unendlich viele Primzahlen existieren, müssen die Werte von A_n für wachsendes n früher oder später jede endliche Zahl überschreiten. Die „Dichte“ der Primzahlen unter den ersten n ganzen Zahlen wird durch den Quotienten $\frac{A_n}{n}$ gegeben, und aus einer Primzahlentabelle kann man die Werte von $\frac{A_n}{n}$ empirisch für einige große Werte von n entnehmen.

n	A_n/n
10^3	0,168
10^6	0,078498
10^9	0,050847478
...

Der Quotient A_n/n kann als Wahrscheinlichkeit dafür aufgefaßt werden, daß eine aufs Geratewohl aus den ersten n ganzen Zahlen herausgegriffene Zahl eine Primzahl ist, da es n Möglichkeiten der Wahl gibt und darunter A_n Primzahlen sind.

Im Einzelnen ist die Verteilung der Primzahlen unter den natürlichen Zahlen außerordentlich unregelmäßig. Aber diese Unregelmäßigkeit „im Kleinen“ verschwindet, wenn wir unsere Aufmerksamkeit der durchschnittlichen Verteilung der Primzahlen, wie sie durch das Verhältnis $\frac{A_n}{n}$ gegeben wird, zuwenden. Das einfache Gesetz, dem dieses Verhältnis gehorcht, ist eine der merkwürdigsten Entdeckungen der Mathematik. Um den *Primzahlsatz* zu formulieren, müssen wir den „natürlichen Logarithmus“ einer Zahl n definieren. Hierzu wählen wir zwei zueinander senkrechte Achsen in einer Ebene und betrachten die Gesamtheit aller Punkte in der Ebene, für die das Produkt ihrer Abstände x und y von den beiden Achsen gleich 1 ist. Dies ist eine gleichseitige Hyperbel, mit der Gleichung $xy = 1$. Wir definieren nun $\ln n$ als diejenige Fläche in Fig. 5, die begrenzt wird von der Hyperbel, der x -Achse und den beiden Vertikalen $x = 1$ und $x = n$. (Eine eingehendere Besprechung des Logarithmus findet sich in Kap. VIII.) Auf Grund einer empirischen Untersuchung von Primzahlentabellen bemerkte GAUSS, daß das Verhältnis

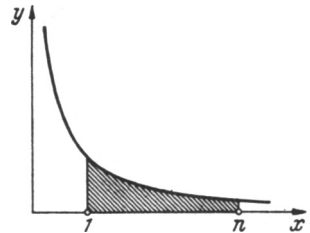


Fig. 5. Die Fläche des schraffierten Gebiets unter der Hyperbel definiert $\ln n$

$\frac{A_n}{n}$ angenähert gleich $1/\ln n$ ist, und daß die Annäherung sich mit wachsendem n zu verbessern scheint. Die Güte der Annäherung ist durch das Verhältnis $\frac{A_n/n}{1/\ln n}$ gegeben, dessen Werte für $n = 1000, 1000000$ und 1000000000 in der folgenden Tabelle angegeben sind.

n	A_n/n	$1/\ln n$	$\frac{A_n/n}{1/\ln n}$
10^3	0,168	0,145	1,159
10^6	0,078498	0,072382	1,084
10^9	0,050847478	0,048254942	1,053
...

Auf Grund solcher empirischer Feststellungen sprach GAUSS die Vermutung aus, daß das Verhältnis A_n/n der Größe $1/\ln n$ „asymptotisch gleich“ ist. Dies bedeutet; wenn wir eine Folge von immer größeren Werten n nehmen, sagen wir wie oben

$$n = 10, 10^2, 10^3, 10^4, \dots,$$

dann nähert sich das Verhältnis von A_n/n zu $1/\ln n$,

$$\frac{A_n/n}{1/\ln n},$$

berechnet für diese aufeinanderfolgenden Werte von n , immer mehr dem Wert 1, d. h. die Differenz zwischen dem Wert dieses Verhältnisses und 1 kann beliebig klein gemacht werden, wenn wir genügend große Werte von n wählen. Diese Behauptung wird symbolisch durch das Zeichen \sim dargestellt:

$$\frac{A_n}{n} \sim \frac{1}{\ln n} \text{ bedeutet } \frac{A_n/n}{1/\ln n} \text{ strebt gegen } 1, \text{ wenn } n \text{ zunimmt.}$$

Das Zeichen \sim kann natürlich nicht durch das gewöhnliche Gleichheitszeichen $=$ ersetzt werden, wie aus der Tatsache hervorgeht, daß A_n immer eine ganze Zahl ist, während dies für $n/\ln n$ nicht zutrifft.

Daß das durchschnittliche Verhalten der Primzahlverteilung durch die Logarithmusfunktion beschrieben werden kann, ist eine sehr merkwürdige Entdeckung; denn es ist erstaunlich, daß zwei mathematische Begriffe, die scheinbar gar nichts miteinander zu tun haben, in Wirklichkeit so eng miteinander verknüpft sind.

Obwohl die Formulierung der Gaußschen Vermutung einfach zu verstehen ist, ging ein strenger Beweis weit über die Leistungsfähigkeit der mathematischen Wissenschaft zu GAUSS' Zeiten hinaus. Um diesen Satz, in dem nur ganz elementare Begriffe auftreten, zu beweisen, benötigt man die stärksten Methoden der modernen Mathematik. Es dauerte fast hundert Jahre, ehe die Analysis so weit entwickelt war, daß HADAMARD (1896) in Paris und DE LA VALLÉE POUSSIN (1896) in Löwen einen vollständigen Beweis des Primzahlsatzes geben konnten. Vereinfachungen und wichtige Abänderungen wurden von v. MANGOLDT und LANDAU angegeben. Lange vor HADAMARD hatte RIEMANN (1826–1866) entscheidende Pionierarbeit geleistet in einer berühmten Arbeit, in der er gleichsam die Strategie für den Angriff auf das Problem entwarf. Der amerikanische Mathematiker NORBERT WIENER hat jetzt den Beweis so umgestaltet, daß die Benutzung komplexer Zahlen bei einem wichtigen Schritt des Gedankengangs vermieden wird. Aber der Beweis des Primzahlsatzes ist noch immer keine leichte Angelegenheit. Wir werden auf diesen Gegenstand noch auf S. 369ff. zurückkommen.

d) Zwei ungelöste Probleme, die Primzahlen betreffen

Während das Problem der durchschnittlichen Primzahlverteilung befriedigend gelöst worden ist, gibt es noch viele Vermutungen, die durch alle empirischen Feststellungen gestützt werden, aber bis heute noch nicht bewiesen werden konnten.

Eine davon ist die berühmte Goldbachsche Vermutung. GOLDBACH (1690 bis 1764) hat nur durch dieses Problem, das er 1742 in einem Brief an EULER aufstellte, in der Geschichte der Mathematik Bedeutung erlangt. Er bemerkte, daß

jede von ihm untersuchte gerade Zahl (außer 2, die selbst eine Primzahl ist) als Summe zweier Primzahlen dargestellt werden kann. Zum Beispiel:

$4 = 2 + 2$, $6 = 3 + 3$, $8 = 5 + 3$, $10 = 5 + 5$, $12 = 5 + 7$, $14 = 7 + 7$,
 $16 = 13 + 3$, $18 = 11 + 7$, $20 = 13 + 7$, \dots , $48 = 29 + 19$, \dots , $100 = 97 + 3$
 usw.

GOLDBACH fragte EULER, ob er beweisen könnte, daß dies für alle geraden Zahlen zutrifft, oder ob er ein Gegenbeispiel angeben könnte? EULER gab niemals eine Antwort, auch ist sonst bisher kein Beweis oder Gegenbeispiel gefunden worden. Die empirischen Ergebnisse zugunsten der Behauptung, daß jede gerade Zahl so dargestellt werden kann, sind durchaus überzeugend, wie jeder bestätigen kann, der eine Anzahl von Beispielen prüft. Der Grund für die Schwierigkeit ist, daß Primzahlen durch *Multiplikation* definiert sind, während es sich bei diesem Problem um *Additionen* handelt. Ganz allgemein ist es schwierig, Zusammenhänge zwischen den multiplikativen und additiven Eigenschaften der ganzen Zahlen aufzufinden.

Bis vor kurzem schien ein Beweis der Goldbachschen Vermutung vollkommen unangreifbar. Heute scheint die Lösung nicht mehr gänzlich hoffnungslos zu sein. 1931 wurde, völlig unerwartet und zum größten Erstaunen der Fachleute, von einem bis dahin unbekannten jungen russischen Mathematiker, SCHNIRELMANN (1905–1938), ein bedeutender Erfolg errungen. SCHNIRELMANN bewies, daß *jede positive ganze Zahl als Summe von nicht mehr als 300000 Primzahlen dargestellt werden kann*. Obwohl dieses Ergebnis im Vergleich zu dem ursprünglichen Ziel, die Goldbachsche Vermutung zu beweisen, beinahe komisch anmutet, so ist es jedenfalls der erste Schritt in dieser Richtung. Der Beweis ist ein direkter, konstruktiver, obwohl er keinerlei praktische Methode angibt, um die Zerlegung einer beliebigen Zahl in eine Summe von Primzahlen zu finden. Etwas später gelang es dem russischen Mathematiker VINOGRADOFF mit Hilfe von Methoden, die von HARDY, LITTLEWOOD und ihrem indischen Mitarbeiter RAMANUJAN stammen, die Zahl der Summanden von 300000 auf 4 herabzudrücken. VINOGRADOFFs großartige Leistung kommt der Lösung des Goldbachschen Problems schon sehr viel näher. Es besteht aber ein prinzipieller Unterschied zwischen SCHNIRELMANNs und VINOGRADOFFs Ergebnis, noch bedeutsamer vielleicht als der Unterschied von 300000 und 4. VINOGRADOFFs Satz ist nur für alle „hinreichend großen“ Zahlen bewiesen, genauer gesagt, VINOGRADOFF bewies, daß es eine Zahl N gibt, derart, daß jede Zahl $n > N$ als Summe von höchstens 4 Primzahlen dargestellt werden kann. VINOGRADOFFs Beweis erlaubt nicht, N abzuschätzen; im Gegensatz zu SCHNIRELMANNs Satz ist er wesentlich indirekt und nicht konstruktiv. Was VINOGRADOFF wirklich bewiesen hat, ist, daß die Annahme, es gäbe unendlich viele ganze Zahlen, die nicht in höchstens 4 Primzahlsummanden zerlegt werden können, zu einem Widerspruch führt. Hier haben wir ein gutes Beispiel des tiefliegenden Unterschieds zwischen den beiden Beweistypen, dem direkten und dem indirekten.

Zum Schluß sei noch ein anderes ungelöstes Problem über Primzahlen erwähnt, welches mindestens ebenso reizvoll ist wie die Goldbachsche Vermutung, welches aber noch weiter von einer befriedigenden Antwort entfernt zu sein scheint. Es ist auffallend, daß in den Tabellen der Primzahlen immer wieder Paare p und $p + 2$ vorkommen, die sich nur um zwei unterscheiden, z. B. 3 und 5, 11 und 13, 29 und 31 usw. Die sich aufdrängende Vermutung ist nun, daß es unendlich viele solcher

Paare gibt. — Obwohl kaum ein Zweifel an der Richtigkeit der Vermutung besteht, ist bisher noch kein entscheidender Fortschritt in der Richtung auf einen Beweis gelungen.

§ 2. Kongruenzen

1. Grundbegriffe

Überall, wo die Frage nach der Teilbarkeit ganzer Zahlen durch eine bestimmte ganze Zahl d auftritt, dient der Begriff und die Bezeichnung „Kongruenz“ (auf GAUSS zurückgehend) zur Klärung und Vereinfachung der Überlegungen.

Um diesen Begriff einzuführen, wollen wir die Reste untersuchen, die bei der Division der ganzen Zahlen durch 5 übrigbleiben. Wir haben

$$\begin{array}{lll}
 0 = 0 \cdot 5 + 0 & 7 = 1 \cdot 5 + 2 & -1 = -1 \cdot 5 + 4 \\
 1 = 0 \cdot 5 + 1 & 8 = 1 \cdot 5 + 3 & -2 = -1 \cdot 5 + 3 \\
 2 = 0 \cdot 5 + 2 & 9 = 1 \cdot 5 + 4 & -3 = -1 \cdot 5 + 2 \\
 3 = 0 \cdot 5 + 3 & 10 = 2 \cdot 5 + 0 & -4 = -1 \cdot 5 + 1 \\
 4 = 0 \cdot 5 + 4 & 11 = 2 \cdot 5 + 1 & -5 = -1 \cdot 5 + 0 \\
 5 = 1 \cdot 5 + 0 & 12 = 2 \cdot 5 + 2 & -6 = -2 \cdot 5 + 4 \\
 6 = 1 \cdot 5 + 1 & \text{usw.} & \text{usw.}
 \end{array}$$

Wir bemerken, daß der Rest, der bleibt, wenn eine beliebige ganze Zahl durch 5 geteilt wird, stets eine der fünf Zahlen 0, 1, 2, 3, 4 ist. Wir sagen, daß zwei ganze Zahlen a und b „kongruent modulo 5“ sind, wenn sie bei Division durch 5 *denselben Rest* lassen. So sind 2, 7, 12, 17, 22, . . . , -3 , -8 , -13 , -18 , . . . alle kongruent modulo 5, da sie den Rest 2 lassen. Allgemein ausgedrückt sagen wir, daß zwei ganze Zahlen a und b *kongruent modulo d* sind, wobei d eine bestimmte ganze Zahl ist, wenn es eine ganze Zahl n gibt, derart, daß $a - b = nd$. Zum Beispiel sind 27 und 15 kongruent modulo 4, weil

$$27 = 6 \cdot 4 + 3, \quad 15 = 3 \cdot 4 + 3.$$

Der Begriff der Kongruenz ist so nützlich, daß es wünschenswert ist, dafür eine kurze Schreibweise zu haben. Wir schreiben

$$a \equiv b \pmod{d},$$

um auszudrücken, daß a und b kongruent modulo d sind. Wenn über den Modul kein Zweifel besteht, kann man auch das „mod d “ der Formel weglassen. (Wenn a nicht kongruent b modulo d ist, schreiben wir $a \not\equiv b \pmod{d}$).

Kongruenzen kommen im Alltagsleben häufig vor. Zum Beispiel geben die Zeiger einer Uhr die Stunde modulo 12 an, und der Kilometerzähler im Auto zeigt die insgesamt zurückgelegten Kilometer modulo 100000.

Ehe wir mit der Erörterung der Kongruenzen im einzelnen beginnen, sollte sich der Leser klar machen, daß die folgenden Aussagen alle einander äquivalent sind:

1. a ist kongruent b modulo d .
2. $a = b + nd$ für eine gewisse ganze Zahl n .
3. d ist ein Teiler von $a - b$.

Der Nutzen der Gaußschen Kongruenzschreibweise liegt darin, daß die Kongruenz in bezug auf einen bestimmten Modul viele der formalen Eigenschaften

der gewöhnlichen Gleichheit hat. Die wichtigsten formalen Eigenschaften der Gleichheits-Beziehung $a = b$ sind die folgenden:

- 1) Es ist immer $a = a$.
- 2) Wenn $a = b$, dann ist auch $b = a$.
- 3) Wenn $a = b$ und $b = c$, dann ist $a = c$.

Ferner: wenn $a = a'$ und $b = b'$, dann ist

- 4) $a + b = a' + b'$.
- 5) $a - b = a' - b'$.
- 6) $ab = a'b'$.

Diese Eigenschaften bleiben erhalten, wenn die Beziehung $a = b$ durch $a \equiv b \pmod{d}$ ersetzt wird. So ist

- 1') immer $a \equiv a \pmod{d}$,
- 2') wenn $a \equiv b \pmod{d}$, dann auch $b \equiv a \pmod{d}$,
- 3') wenn $a \equiv b \pmod{d}$ und $b \equiv c \pmod{d}$, dann auch $a \equiv c \pmod{d}$.

Die triviale Nachprüfung dieser Tatsachen bleibe dem Leser überlassen.

Ferner: wenn $a \equiv a' \pmod{d}$ und $b \equiv b' \pmod{d}$, dann ist

- 4') $a + b \equiv a' + b' \pmod{d}$,
- 5') $a - b \equiv a' - b' \pmod{d}$,
- 6') $ab \equiv a'b' \pmod{d}$.

Es können also *Kongruenzen in bezug auf denselben Modul addiert, subtrahiert und multipliziert werden*. Um diese drei Aussagen zu beweisen, brauchen wir nur folgendes zu bemerken: Wenn

$$a = a' + rd, \quad b = b' + sd,$$

dann ist

$$\begin{aligned} a + b &= a' + b' + (r + s)d, \\ a - b &= a' - b' + (r - s)d, \\ ab &= a'b' + (a's + b'r + rsd)d, \end{aligned}$$

woraus die gewünschten Eigenschaften folgen.

Der Begriff der Kongruenz erlaubt eine anschauliche geometrische Deutung. Wenn wir die ganzen Zahlen geometrisch darzustellen wünschen, wählen wir gewöhnlich eine Strecke der Länge 1 und erweitern sie durch Vielfache derselben Länge nach beiden Seiten. Auf diese Weise finden wir für jede ganze Zahl einen entsprechenden Punkt auf der Geraden wie in Fig. 6. Wenn wir es dagegen mit den

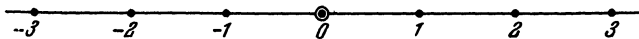


Fig. 6. Geometrische Darstellung der ganzen Zahlen

ganzen Zahlen modulo d zu tun haben, so werden zwei beliebige kongruente Zahlen als dieselbe Zahl angesehen, da es nur auf ihr Verhalten bei Division durch d ankommt und sie denselben Rest lassen. Um dies geometrisch zu veranschaulichen, wählen wir einen Kreis, der in d gleiche Teile geteilt ist. Jede ganze Zahl läßt bei Division durch d als Rest eine der d Zahlen $0, 1, 2, \dots, d-1$, die in gleichen Abständen auf dem Umfang des Kreises angeordnet werden. Jede ganze Zahl ist

einer dieser Zahlen kongruent modulo d und wird daher geometrisch durch einen dieser Punkte dargestellt. Fig. 7 ist für den Fall $d = 6$ gezeichnet. Das Zifferblatt einer Uhr ist ein weiteres Beispiel aus dem täglichen Leben.

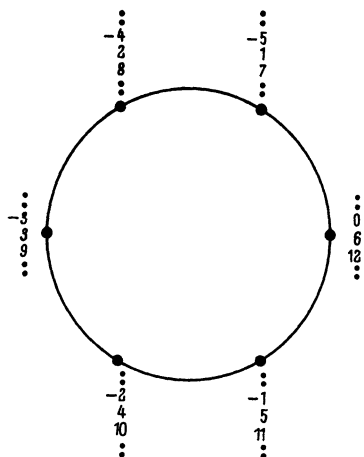


Fig. 7. Geometrische Darstellung der ganzen Zahlen modulo 6

Als Beispiel für die Anwendung der multiplikativen Eigenschaft 6') der Kongruenzen können wir die Reste bestimmen, die bei der Division aufeinanderfolgender Zehnerpotenzen durch eine gegebene Zahl bleiben. Zum Beispiel ist

$$10 \equiv -1 \pmod{11},$$

da $10 = -1 + 11$. Multiplizieren wir diese Kongruenz wiederholt mit sich selbst, so ergibt sich

$$10^2 \equiv (-1)(-1) = 1 \pmod{11},$$

$$10^3 \equiv -1 \pmod{11},$$

$$10^4 \equiv 1 \pmod{11} \text{ usw.}$$

Hieraus läßt sich zeigen, daß eine beliebige natürliche Zahl

$$z = a_0 + a_1 \cdot 10 + a_2 \cdot 10^2 + \cdots + a_n \cdot 10^n,$$

im Dezimalsystem ausgedrückt, bei Division durch 11 denselben Rest läßt wie die Summe ihrer Ziffern mit abwechselndem Vorzeichen genommen,

$$t = a_0 - a_1 + a_2 - a_3 + \cdots.$$

Denn wir können schreiben

$$z - t = a_1 \cdot 11 + a_2(10^2 - 1) + a_3(10^3 + 1) + a_4(10^4 - 1) + \cdots.$$

Da alle Zahlen 11 , $10^2 - 1$, $10^3 + 1$, ... kongruent $0 \pmod{11}$ sind, gilt dies von $z - t$ ebenfalls, und daher läßt z bei Division durch 11 denselben Rest wie t . Insbesondere folgt, daß eine Zahl dann und nur dann durch 11 teilbar ist (d. h. den Rest 0 läßt), wenn die Summe ihrer Ziffern mit abwechselndem Vorzeichen durch 11 teilbar ist. Zum Beispiel: da $3 - 1 + 6 - 2 + 8 - 1 + 9 = 22$, ist die Zahl $z = 3162819$ durch 11 teilbar. Noch einfacher ist es, ein Kennzeichen für die Teilbarkeit durch 3 oder 9 zu finden, da $10 \equiv 1 \pmod{3}$ oder 9 und daher $10^n \equiv 1 \pmod{3}$ oder 9 für jedes n . Daraus folgt, daß eine Zahl z dann und nur dann durch 3 oder 9 teilbar ist, wenn die Summe ihrer Ziffern — die sogenannte Quersumme —

$$s = a_0 + a_1 + a_2 + \cdots + a_n$$

ebenfalls durch 3 bzw. durch 9 teilbar ist.

Für Kongruenzen modulo 7 haben wir

$$10 \equiv 3, 10^2 \equiv 2, 10^3 \equiv -1, 10^4 \equiv -3, 10^5 \equiv -2, 10^6 \equiv 1.$$

Diese Reste wiederholen sich dann beim Weitergehen. Daher ist z dann und nur dann durch 7 teilbar, wenn der Ausdruck

$$r = a_0 + 3a_1 + 2a_2 - a_3 - 3a_4 - 2a_5 + a_6 + 3a_7 + \cdots$$

durch 7 teilbar ist.

Übung: Man suche ein ähnliches Kennzeichen für die Teilbarkeit durch 13.

Beim Addieren oder Multiplizieren von Kongruenzen mit Bezug auf einen festen Modul, etwa $d = 5$, können wir verhindern, daß die auftretenden Zahlen zu groß werden, wenn wir jede Zahl a immer durch diejenige aus der Menge

$$0, 1, 2, 3, 4$$

ersetzen, zu der sie kongruent ist. Um also Summen und Produkte von ganzen Zahlen modulo 5 zu berechnen, brauchen wir nur die folgenden Tabellen für die Addition und die Multiplikation zu benutzen.

$a + b$		$a \cdot b$	
$b \equiv 0$	1 2 3 4	$b \equiv 0$	1 2 3 4
$a \equiv 0$	0 1 2 3 4	$a \equiv 0$	0 0 0 0 0
1	1 2 3 4 0	1	0 1 2 3 4
2	2 3 4 0 1	2	0 2 4 1 3
3	3 4 0 1 2	3	0 3 1 4 2
4	4 0 1 2 3	4	0 4 3 2 1

Aus der zweiten Tabelle geht hervor, daß ein Produkt ab nur dann kongruent 0 (mod 5) ist, wenn a oder b kongruent 0 (mod 5) ist. Das deutet auf das allgemeine Gesetz

$$7) \quad ab \equiv 0 \pmod{d} \text{ nur, wenn } a \equiv 0 \text{ oder } b \equiv 0 \pmod{d}.$$

Dies ist eine Erweiterung des gewöhnlichen Gesetzes für ganze Zahlen, nach dem ab nur $= 0$ sein kann, wenn $a = 0$ oder $b = 0$. Das Gesetz (7) gilt dann und nur dann, wenn d eine Primzahl ist. Denn die Kongruenz

$$ab \equiv 0 \pmod{d}$$

bedeutet, daß d ein Teiler von ab ist; ist nun d eine Primzahl, dann wissen wir, daß sie nur dann Teiler des Produkts ab sein kann, wenn sie entweder Teiler von a oder von b ist, also nur, wenn

$$a \equiv 0 \pmod{d} \quad \text{oder} \quad b \equiv 0 \pmod{d}.$$

Wenn aber d keine Primzahl ist, dann können wir $d = r \cdot s$ setzen, worin r und s kleiner als d sind, so daß

$$r \not\equiv 0 \pmod{d}, \quad s \not\equiv 0 \pmod{d}$$

und trotzdem

$$rs = d \equiv 0 \pmod{d};$$

d. h. das Gesetz ist nicht gültig. Zum Beispiel ist $2 \not\equiv 0 \pmod{6}$ und $3 \not\equiv 0 \pmod{6}$, aber $2 \cdot 3 = 6 \equiv 0 \pmod{6}$.

Übung: Man zeige, daß die folgende *Kürzungsregel* für Kongruenzen in bezug auf einen Primzahlmodul gilt:

Wenn $ab \equiv ac$ und $a \not\equiv 0$, dann ist $b \equiv c$.

Übungen: 1. Welcher Zahl zwischen 0 und 6 (einschließlich) ist das Produkt $11 \cdot 18 \cdot 2322 \cdot 13 \cdot 19$ kongruent modulo 7?

2. Welcher Zahl zwischen 0 und 12 (einschließlich) ist $3 \cdot 7 \cdot 11 \cdot 17 \cdot 19 \cdot 23 \cdot 29 \cdot 113$ kongruent modulo 13?

3. Welcher Zahl zwischen 0 und 4 (einschließlich) ist die Summe $1 + 2 + 2^2 + \dots + 2^{19}$ kongruent modulo 5?

2. Der kleine Fermatsche Satz

Im 17. Jahrhundert entdeckte FERMAT, der Begründer der modernen Zahlentheorie, den wichtigen Satz: *Für eine beliebige Primzahl p , die nicht Teiler der ganzen Zahl a ist, gilt*

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

Das heißt, daß die $(p-1)$ te Potenz von a bei Division durch p den Rest 1 läßt.

Einige unserer früheren Rechnungen bestätigen diesen Satz; z. B. fanden wir, daß $10^6 \equiv 1 \pmod{7}$, $10^2 \equiv 1 \pmod{3}$ und $10^{10} \equiv 1 \pmod{11}$. Ebenso können wir zeigen, daß $2^{12} \equiv 1 \pmod{13}$ und $5^{10} \equiv 1 \pmod{11}$. Um die letzteren Kongruenzen nachzuprüfen, brauchen wir nicht diese hohen Potenzen wirklich auszurechnen, da wir uns die multiplikative Eigenschaft der Kongruenzen zunutze machen können:

$$\begin{array}{llll} 2^4 \equiv 16 \equiv 3 & \pmod{13}, & 5^2 \equiv 3 & \pmod{11}, \\ 2^8 \equiv 9 \equiv -4 & \pmod{13}, & 5^4 \equiv 9 \equiv -2 & \pmod{11}, \\ 2^{12} \equiv -4 \cdot 3 = -12 \equiv 1 & \pmod{13}. & 5^8 \equiv 4 & \pmod{11}, \\ & & 5^{10} \equiv 3 \cdot 4 = 12 \equiv 1 & \pmod{11}. \end{array}$$

Um den Fermatschen Satz zu beweisen, betrachten wir die Vielfachen von a

$$m_1 = a, \quad m_2 = 2a, \quad m_3 = 3a, \dots, m_{p-1} = (p-1)a.$$

Keine zwei dieser Zahlen können kongruent modulo p sein; denn dann wäre p ein Teiler von $m_r - m_s = (r-s)a$ für ein gewisses Paar von ganzen Zahlen r, s mit $1 \leq r < s \leq (p-1)$. Aber nach Satz (7) kann dies nicht sein, denn da $s-r$ kleiner als p ist, ist p kein Teiler von $s-r$, während nach Voraussetzung p kein Teiler von a ist. Auch kann keine der Zahlen kongruent 0 sein. Daher muß jede der Zahlen m_1, m_2, \dots, m_{p-1} genau einer entsprechenden unter den Zahlen $1, 2, 3, \dots, \dots, p-1$ kongruent sein. Daraus folgt

$$m_1 m_2 \cdots m_{p-1} = 1 \cdot 2 \cdot 3 \cdots (p-1) a^{p-1} \equiv 1 \cdot 2 \cdot 3 \cdots (p-1) \pmod{p},$$

oder, wenn wir K als Abkürzung für $1 \cdot 2 \cdot 3 \cdots (p-1)$ schreiben,

$$K(a^{p-1} - 1) \equiv 0 \pmod{p}.$$

Aber K ist nicht durch p teilbar, da keiner seiner Faktoren es ist, daher muß nach dem Satz (7) $a^{p-1} - 1$ durch p teilbar sein, d. h.

$$a^{p-1} - 1 \equiv 0 \pmod{p}.$$

Das ist der Fermatsche Satz.

Um den Satz nochmals zu kontrollieren, nehmen wir $p = 23$ und $a = 5$. Wir haben dann, immer modulo 23, $5^2 \equiv 2$, $5^4 \equiv 4$, $5^8 \equiv 16 \equiv -7$, $5^{16} \equiv 49 \equiv 3$, $5^{20} \equiv 12$, $5^{22} \equiv 24 \equiv 1$. Mit $a = 4$ anstelle von 5 erhalten wir, wiederum modulo 23, $4^2 \equiv -7$, $4^3 \equiv -28 \equiv -5$, $4^4 \equiv -20 \equiv 3$, $4^8 \equiv 9$, $4^{11} \equiv -45 \equiv 1$, $4^{22} \equiv 1$.

In dem oben angegebenen Beispiel mit $a = 4$, $p = 23$ und in anderen bemerken wir, daß nicht nur die $(p-1)$ te Potenz von a , sondern schon eine niedrigere Potenz kongruent 1 sein kann. Es gilt dann immer, daß die kleinste derartige Potenz, in diesem Fall 11, ein Teiler von $(p-1)$ ist. (Siehe die folgende Übung 3).

Übungen: 1. Man zeige durch ähnliche Rechnung, daß $2^8 \equiv 1 \pmod{17}$; $3^8 \equiv -1 \pmod{17}$; $3^{14} \equiv -1 \pmod{29}$; $2^{14} \equiv -1 \pmod{29}$; $4^{14} \equiv 1 \pmod{29}$; $5^{14} \equiv 1 \pmod{29}$.

2. Man bestätige den kleinen Fermatschen Satz für $p = 5, 7, 11, 17$ und 23 mit verschiedenen Werten von a .

3. Man beweise den allgemeinen Satz: Die kleinste positive ganze Zahl e , für die $a^e \equiv 1 \pmod{p}$, muß Teiler von $p - 1$ sein. Anleitung: Man teile $p - 1$ durch e , was

$$p - 1 = ke + r$$

ergibt, wobei $0 \leq r < e$, und benutze, daß $a^{p-1} \equiv a^e \equiv 1 \pmod{p}$.

3. Quadratische Reste

Betrachten wir die Beispiele zum Fermatschen Satz, so finden wir, daß nicht nur immer $a^{p-1} \equiv 1 \pmod{p}$ ist, sondern daß (wenn p eine von 2 verschiedene Primzahl, also ungerade und von der Form $2p' + 1$ ist) darüber hinaus für manche

Werte von a auch $a^{p'} \equiv a^{\frac{p-1}{2}} \equiv 1 \pmod{p}$ ist. Diese Tatsache regt zu interessanten Untersuchungen an. Wir können den Fermatschen Satz in folgender Form schreiben:

$$a^{p-1} - 1 = a^{2p'} - 1 = (a^{p'} - 1)(a^{p'} + 1) \equiv 0 \pmod{p}.$$

Da ein Produkt nur dann durch p teilbar ist, wenn einer der Faktoren es ist, so ergibt sich sofort, daß entweder $a^{p'} - 1$ oder $a^{p'} + 1$ durch p teilbar sein muß, so daß für jede Primzahl $p > 2$ und jede Zahl a , die nicht durch p teilbar ist, entweder

$$a^{\frac{p-1}{2}} \equiv 1 \quad \text{oder} \quad a^{\frac{p-1}{2}} \equiv -1 \pmod{p}.$$

Seit dem Beginn der modernen Zahlentheorie haben sich die Mathematiker bemüht herauszufinden, für welche Zahlen a der erste Fall vorliegt und für welche der zweite. Nehmen wir an, a sei modulo p kongruent dem Quadrat einer Zahl x ,

$$a \equiv x^2 \pmod{p}.$$

Dann ist $a^{\frac{p-1}{2}} \equiv x^{p-1}$, was nach dem Fermatschen Satz kongruent 1 modulo p ist. Eine Zahl $a (\not\equiv 0 \pmod{p})$, die modulo p einer Quadratzahl kongruent ist, heißt ein *quadratischer Rest* von p , während eine Zahl $b (\not\equiv 0 \pmod{p})$, die keiner Quadratzahl kongruent ist, ein *quadratischer Nichtrest* von p genannt wird. Wir

haben eben gesehen, daß jeder quadratische Rest von p die Kongruenz $a^{\frac{p-1}{2}} \equiv 1 \pmod{p}$ befriedigt. Ohne große Schwierigkeit läßt sich beweisen, daß für jeden

Nichtrest b die Kongruenz $b^{\frac{p-1}{2}} \equiv -1 \pmod{p}$ gilt. Darüber hinaus werden wir alsbald zeigen, daß es unter den Zahlen $1, 2, 3, \dots, p-1$ genau $\frac{p-1}{2}$ quadratische Reste und $\frac{p-1}{2}$ Nichtreste gibt.

Obwohl viele empirische Daten durch direkte Ausrechnung gesammelt werden konnten, war es nicht leicht, allgemeine Gesetze über die Verteilung der quadratischen Reste und Nichtreste zu entdecken. Eine erste tiefliegende Eigenschaft dieser Reste wurde von LEGENDRE (1752–1833) bemerkt und später von GAUSS das *quadratische Reziprozitätsgesetz* genannt. Dieses Gesetz betrifft das Verhalten von zwei verschiedenen Primzahlen p und q und sagt aus, daß q ein quadratischer Rest von p dann und nur dann ist, wenn p ein quadratischer Rest von q ist, vorausgesetzt, daß das Produkt $\frac{p-1}{2} \cdot \frac{q-1}{2}$ gerade ist. Ist dieses Produkt *ungerade*,

dann ist umgekehrt p ein Rest von q dann und nur dann, wenn q ein *Nichtrest* von p ist. Eine der Leistungen des jungen GAUSS war der erste strenge Beweis dieses merkwürdigen Gesetzes, das längere Zeit die Mathematiker herausgefordert hatte. GAUSS' erster Beweis war keineswegs einfach, und das Reziprozitätsgesetz ist selbst heute noch nicht allzu leicht zu begründen, obwohl eine ganze Anzahl verschiedener Beweise veröffentlicht worden ist. Seine wahre Bedeutung ist erst kürzlich im Zusammenhang mit der modernen Entwicklung der algebraischen Zahlentheorie erkannt worden.

Als Beispiel zur Erläuterung der Verteilung der quadratischen Reste wollen wir $p = 7$ wählen. Da

$$0^2 \equiv 0, \quad 1^2 \equiv 1, \quad 2^2 \equiv 4, \quad 3^2 \equiv 2, \quad 4^2 \equiv 2, \quad 5^2 \equiv 4, \quad 6^2 \equiv 1,$$

alle modulo 7, und da die weiteren Quadratzahlen nur dieselbe Folge von Zahlen wiederholen, sind die quadratischen Reste von 7 alle Zahlen, die kongruent 1, 2 und 4 sind, während die Nichtreste kongruent 3, 5 und 6 sind. Im allgemeinen Fall bestehen die quadratischen Reste von p aus den Zahlen, die kongruent $1^2, 2^2, \dots, (p-1)^2$ sind. Aber diese $p-1$ Quadrate sind paarweise kongruent, denn

$$x^2 \equiv (p-x)^2 \pmod{p} \quad (\text{z. B. } 2^2 \equiv 5^2 \pmod{7}),$$

weil $(p-x)^2 = p^2 - 2px + x^2 \equiv x^2 \pmod{p}$. Daher sind die Hälfte der Zahlen $1, 2, \dots, p-1$ quadratische Reste und die andere Hälfte sind quadratische Nichtreste.

Um das quadratische Reziprozitätsgesetz zu verdeutlichen, wollen wir $p = 5$, $q = 11$ wählen. Da $11 \equiv 1^2 \pmod{5}$, ist 11 ein quadratischer Rest von 5. Da das Produkt $\frac{5-1}{2} \cdot \frac{11-1}{2}$ gerade ist, sagt uns das Reziprozitätsgesetz, daß auch 5 ein quadratischer Rest von 11 ist. Wir bestätigen dies durch die Feststellung, daß $5 \equiv 4^2 \pmod{11}$. Wenn andererseits $p = 7$, $q = 11$ gewählt wird, so ist das Produkt $\frac{7-1}{2} \cdot \frac{11-1}{2}$ ungerade, und tatsächlich ist 11 ein Rest $\pmod{7}$, da $11 \equiv 2^2 \pmod{7}$, während 7 ein Nichtrest $\pmod{11}$ ist.

Übungen: 1. $6^2 = 36 \equiv 13 \pmod{23}$. Ist 23 ein quadratischer Rest $\pmod{13}$?

2. Wir haben gesehen, daß $x^2 \equiv (p-x)^2 \pmod{p}$. Man zeige, daß dies die *einzigsten* Kongruenzen zwischen den Zahlen $1^2, 2^2, 3^2, \dots, (p-1)^2$ sind.

§ 3. Pythagoreische Zahlen und großer Fermatscher Satz

Eine interessante Frage der Zahlentheorie hängt mit dem pythagoreischen Lehrsatz zusammen. Die Griechen wußten, daß ein Dreieck mit den Seiten 3, 4 und 5 rechtwinklig ist. Dies regte zu der Frage an, welche anderen rechtwinkligen Dreiecke Seiten haben, deren Längen ganze Vielfache einer Einheitslänge sind. Der Satz des PYTHAGORAS drückt sich algebraisch durch die Gleichung aus:

$$(1) \quad a^2 + b^2 = c^2,$$

in der a und b die Längen der Katheten eines rechtwinkligen Dreiecks sind und c die Länge der Hypotenuse ist. Das Problem, *alle* rechtwinkligen Dreiecke mit Seiten von ganzzahligen Längen zu finden, ist daher äquivalent mit dem Problem, alle ganzzahligen Lösungen a, b, c der Gleichung (1) zu finden. Jedes solche Zahlen-tripel wird ein *pythagoreisches Zahlentripel* genannt.

Das Problem, alle pythagoreischen Zahlentripel zu finden, läßt sich sehr einfach lösen. Wenn a, b und c ein pythagoreisches Zahlentripel bilden, so daß $a^2 + b^2 = c^2$, so wollen wir zur Abkürzung $a/c = x$, $b/c = y$ setzen. x und y sind rationale Zahlen mit der Eigenschaft $x^2 + y^2 = 1$. Wir haben dann $y^2 = (1-x)(1+x)$ oder $\frac{y}{(1+x)} = \frac{(1-x)}{y}$. Der gemeinsame Wert der beiden Seiten dieser Gleichung ist eine Zahl t , die sich als Quotient $\frac{u}{v}$ zweier ganzer Zahlen ausdrücken läßt. Wir können nun schreiben $y = t(1+x)$ und $1-x = ty$ oder

$$tx - y = -t, \quad x + ty = 1.$$

Aus diesen simultanen Gleichungen finden wir sofort

$$x = \frac{1-t^2}{1+t^2}, \quad y = \frac{2t}{1+t^2}.$$

Setzen wir für x, y, t ihre Werte ein, so haben wir

$$\frac{a}{c} = \frac{v^2 - u^2}{u^2 + v^2}, \quad \frac{b}{c} = \frac{2uv}{u^2 + v^2}.$$

Daher ist

$$\begin{aligned} a &= (v^2 - u^2)r, \\ (2) \quad b &= (2uv)r, \\ c &= (u^2 + v^2)r, \end{aligned}$$

mit einem gewissen Proportionalitätsfaktor r . Hieraus geht hervor: wenn (a, b, c) ein pythagoreisches Zahlentripel ist, müssen a, b und c den Zahlen $v^2 - u^2$, $2uv$ und $u^2 + v^2$ proportional sein. Umgekehrt ist leicht einzusehen, daß jedes Tripel (a, b, c) , das durch (2) definiert ist, ein pythagoreisches Tripel ist; denn aus (2) ergibt sich

$$\begin{aligned} a^2 &= (u^4 - 2u^2v^2 + v^4)r^2, \\ b^2 &= (4u^2v^2)r^2, \\ c^2 &= (u^4 + 2u^2v^2 + v^4)r^2, \end{aligned}$$

so daß $a^2 + b^2 = c^2$.

Dieses Ergebnis läßt sich noch etwas vereinfachen. Aus jedem pythagoreischen Zahlentripel (a, b, c) können wir durch Multiplikation mit beliebigen natürlichen Zahlen s unendlich viele andere pythagoreische Tripel (sa, sb, sc) ableiten. Aus $(3, 4, 5)$ erhalten wir $(6, 8, 10)$, $(9, 12, 15)$ usw. Solche Tripel sind nicht wesentlich verschieden, da sie ähnlichen rechtwinkligen Dreiecken entsprechen. Wir werden daher ein *primitives* pythagoreisches Zahlentripel als ein solches definieren, bei dem a, b und c keinen gemeinsamen Faktor enthalten. Es läßt sich dann zeigen, daß die Formeln

$$\begin{aligned} a &= v^2 - u^2, \\ b &= 2uv, \\ c &= u^2 + v^2 \end{aligned}$$

für beliebige positive ganze Zahlen u und v mit $v > u$, wenn u und v keinen gemeinsamen Teiler haben und nicht beide ungerade sind, sämtliche primitiven pythagoreischen Zahlentripel liefern.

*Übung: Man beweise die letzte Behauptung.

Als Beispiele für primitive pythagoreische Zahlentripel haben wir $u = 1$, $v = 2$: (3, 4, 5), $u = 2$, $v = 3$: (5, 12, 13), $u = 3$, $v = 4$: (7, 24, 25), . . . , $u = 7$, $v = 10$: (51, 140, 149), usw.

Dieses Ergebnis für pythagoreische Zahlen läßt natürlich die Frage entstehen, ob ganze Zahlen a, b, c gefunden werden können, für die $a^3 + b^3 = c^3$ oder $a^4 + b^4 = c^4$ ist, oder allgemeiner, ob für einen gegebenen positiven ganzen Exponenten $n > 2$ die Gleichung

$$(3) \quad a^n + b^n = c^n$$

mit positiven ganzen Zahlen a, b, c gelöst werden kann. Diese Frage führte zu einer in der Geschichte der Mathematik höchst bemerkenswerten Entwicklung: FERMAT hat viele wichtige zahlentheoretische Entdeckungen in Randbemerkungen in seinem Exemplar des Werkes von DIOPHANTUS, dem großen Zahlentheoretiker der Antike, niedergelegt. Er hat dort viele Sätze ausgesprochen, ohne sich mit deren Beweis aufzuhalten, und diese Sätze sind alle später bewiesen worden, mit einer wichtigen Ausnahme. Bei seinen Anmerkungen zu den pythagoreischen Zahlen schrieb FERMAT, daß die Gleichung (3) nicht in ganzen Zahlen lösbar sei, sobald n eine ganze Zahl > 2 ist; aber der elegante Beweis, den er hierfür gefunden habe, sei leider zu lang für den Rand, auf den er schreibe.

Diese allgemeine Behauptung FERMATs konnte bisher weder widerlegt noch bewiesen werden, obwohl sich viele der größten Mathematiker darum bemüht haben.* Der Satz ist allerdings für viele spezielle Werte von n bewiesen worden, insbesondere für alle $n < 619$, aber nicht für alle n , obgleich niemals ein Gegenbeispiel geliefert worden ist. Wenn der Satz selbst auch mathematisch kein überwältigendes Interesse bieten mag, so haben die Versuche, ihn zu beweisen, doch manche bedeutende zahlentheoretische Untersuchung veranlaßt. Das Problem hat auch in nichtmathematischen Kreisen viel Aufsehen erregt, zum Teil wegen eines Preises von 100000 Mark, der für denjenigen ausgesetzt wurde, der die erste Lösung des Problems liefern würde. Der Preis wurde von der Göttinger Akademie der Wissenschaften verwaltet, und bis zu seiner Entwertung durch die Inflation wurde jedes Jahr eine große Anzahl unrichtiger „Lösungen“ den Treuhändern eingesandt. Selbst ernstzunehmende Mathematiker täuschten sich zuweilen und übersandten oder veröffentlichten Beweise, die zusammenbrachen, nachdem irgendein oberflächlicher Fehler entdeckt worden war. Das allgemeine Interesse scheint seit der Geldentwertung etwas nachgelassen zu haben; doch von Zeit zu Zeit findet sich noch immer die sensationelle Mitteilung in der Presse, daß das Problem von einem bis dato unbekannten Genie gelöst worden sei.

§ 4. Der euklidische Algorithmus

1. Die allgemeine Theorie

Der Leser kennt die gewöhnliche Methode der Division einer ganzen Zahl durch eine andere und weiß, daß das Verfahren so lange weitergeführt werden kann, bis der Rest kleiner ist als der Divisor. Wenn z. B. $a = 648$ und $b = 7$ ist, so haben wir

* Anmerkung des Verlages: Der Satz von Fermat wurde im Oktober 1994 von Andrew Wiles bewiesen

den Quotienten $q = 92$ und einen Rest $r = 4$

$$648 : 7 = 92 \text{ Rest } 4 \quad 648 = 7 \cdot 92 + 4$$

$$\begin{array}{r} 63 \\ \hline 18 \\ 14 \\ \hline 4 \end{array}$$

Wir können dies als allgemeinen Satz aussprechen: *Wenn a eine beliebige ganze Zahl und b eine ganze Zahl größer als 0 ist, dann können wir stets eine ganze Zahl q finden, so daß*

$$(1) \quad a = bq + r,$$

wobei r eine ganze Zahl ist, die der Ungleichung $0 \leq r < b$ genügt.

Um diese Behauptung zu beweisen, ohne das Verfahren der ausführlichen Division zu benutzen, brauchen wir nur zu bemerken, daß eine beliebige ganze Zahl a entweder selbst ein Vielfaches von b ist,

$$a = bq,$$

oder zwischen zwei aufeinanderfolgenden Vielfachen von b liegt,

$$bq < a < b(q+1) = bq + b.$$

Im ersten Fall gilt die Gleichung (1) mit $r = 0$. Im zweiten Fall haben wir nach der linken Ungleichung

$$a - bq = r > 0$$

und nach der rechten Ungleichung

$$a - bq = r < b,$$

so daß $0 < r < b$, wie in (1) verlangt.

Aus dieser einfachen Tatsache werden wir mannigfache wichtige Folgerungen ableiten, z. B. ein Verfahren zur Bestimmung des größten gemeinsamen Teilers von zwei ganzen Zahlen.

Es seien a und b zwei ganze Zahlen, die nicht beide Null sind, und wir betrachten die Menge aller positiven ganzen Zahlen, die sowohl Teiler von a als auch von b sind. Diese Menge ist sicherlich endlich; denn wenn z. B. $a \neq 0$ ist, dann kann keine Zahl, die absolut genommen größer als a ist, Teiler von a sein, d. h. a hat nur endlich viele Teiler. Also kann es auch nur eine endliche Anzahl von gemeinsamen Teilern von a und b geben, und d möge der größte sein. Die ganze Zahl d heißt der *größte gemeinsame Teiler* von a und b und wird $d = (a, b)$ geschrieben. So finden wir für $a = 8$ und $b = 12$ durch Probieren $(8, 12) = 4$, während wir für $a = 5$ und $b = 9$ nur $(5, 9) = 1$ finden. Wenn a und b groß sind, z. B. $a = 1804$ und $b = 328$, so wäre der Versuch, (a, b) durch Probieren zu finden, recht mühselig. Eine kurze und sichere Methode liefert der *euklidische Algorithmus*. (Ein Algorithmus ist eine systematische Rechenmethode.) Er beruht auf der Tatsache, daß aus jeder Beziehung der Form

$$(2) \quad a = bq + r$$

geschlossen werden kann, daß

$$(3) \quad (a, b) = (b, r).$$

Denn jede Zahl u , die sowohl in a wie in b enthalten ist,

$$a = su, \quad b = tu,$$

muß auch in r enthalten sein, da $r = a - bq = su - qtu = (s - qt)u$, und umgekehrt muß jede Zahl v , die in b und r enthalten ist,

$$b = s'v, \quad r = t'v,$$

auch in a enthalten sein, da $a = bq + r = s'vq + t'v = (s'q + t')v$. Demnach ist *jeder* gemeinsame Teiler von a und b zugleich ein gemeinsamer Teiler von b und r und umgekehrt. Wenn daher die Menge *aller* gemeinsamen Teiler von a und b mit der Menge aller gemeinsamen Teiler von b und r identisch ist, dann muß auch der *größte* gemeinsame Teiler von a und b dem größten gemeinsamen Teiler von b und r gleich sein, womit (3) bewiesen ist. Der Nutzen dieser Beziehung wird sich sogleich ergeben.

Kehren wir zur Frage nach dem größten gemeinsamen Teiler von 1804 und 328 zurück. Durch gewöhnliche Division

$$\begin{array}{r} 1804 : 328 = 5 \quad \text{Rest } 164 \\ \underline{1640} \\ 164 \end{array}$$

finden wir

$$1804 = 5 \cdot 328 + 164.$$

Also können wir nach (3) schließen, daß

$$(1804, 328) = (328, 164).$$

Man beachte, daß die Aufgabe, $(1804, 328)$ zu finden, ersetzt worden ist durch eine Aufgabe mit kleineren Zahlen. Wir können das Verfahren fortsetzen. Wegen

$$\begin{array}{r} 328 : 164 = 2 \\ \underline{328} \\ 0, \end{array}$$

oder $328 = 2 \cdot 164 + 0$ haben wir $(328, 164) = (164, 0) = 164$. Also ist $(1804, 328) = (328, 164) = (164, 0) = 164$, womit das gewünschte Ergebnis gefunden ist.

Dieses Verfahren zur Bestimmung des größten gemeinsamen Teilers zweier Zahlen wird in geometrischer Form in EUKLID's *Elementen* angegeben. Für beliebige ganze Zahlen a und b , die nicht beide 0 sind, kann es arithmetisch in folgender Form beschrieben werden.

Wir können voraussetzen, daß $b > 0$ ist. Dann erhalten wir durch wiederholte Division:

$$\begin{array}{ll} a = bq_1 + r_1 & (0 < r_1 < b) \\ b = r_1q_2 + r_2 & (0 < r_2 < r_1) \\ (4) \quad r_1 = r_2q_3 + r_3 & (0 < r_3 < r_2) \\ r_2 = r_3q_4 + r_4 & (0 < r_4 < r_3) \\ \dots\dots\dots & \dots\dots\dots \end{array}$$

solange die Reste r_1, r_2, r_3, \dots nicht 0 sind. Aus den Ungleichungen rechts ersehen wir, daß die aufeinanderfolgenden Reste eine dauernd abnehmende Folge von positiven Zahlen bilden:

$$(5) \quad b > r_1 > r_2 > r_3 > r_4 > \dots > 0.$$

Also muß nach höchstens b Schritten (oft viel früher, da der Unterschied zwischen

zwei aufeinanderfolgenden Resten meist größer als 1 ist) der Rest 0 auftreten:

$$r_{n-2} = r_{n-1}q_n + r_n$$

$$r_{n-1} = r_n q_{n+1} + 0.$$

Wenn dies geschieht, wissen wir, daß

$$(a, b) = r_n;$$

mit anderen Worten, (a, b) ist der letzte positive Rest in der Folge (5). Das folgt aus der wiederholten Anwendung der Gleichung (3) auf die Gleichungen (4), denn aus den aufeinanderfolgenden Zeilen (4) ergibt sich

$$(a, b) = (b, r_1); \quad (b, r_1) = (r_1, r_2); \quad (r_1, r_2) = (r_2, r_3);$$

$$(r_2, r_3) = (r_3, r_4); \dots; (r_{n-1}, r_n) = (r_n, 0) = r_n.$$

Übung: Man bestimme mit dem euklidischen Algorithmus den größten gemeinsamen Teiler von (a) 187 und 77, (b) 105 und 385, (c) 245 und 193.

Eine äußerst wichtige Eigenschaft von (a, b) kann aus den Gleichungen (4) abgeleitet werden. Wenn $d = (a, b)$, dann können positive oder negative ganze Zahlen k und l gefunden werden, so daß

$$(6) \quad d = ka + lb.$$

Um das einzusehen, betrachten wir die Folge (5) der aufeinanderfolgenden Reste. Aus der ersten Gleichung von (4) folgt

$$r_1 = a - q_1 b,$$

so daß r_1 in der Form $k_1 a + l_1 b$ geschrieben werden kann (in diesem Fall ist $k_1 = 1$, $l_1 = -q_1$). Aus der nächsten Gleichung folgt

$$r_2 = b - q_2 r_1 = b - q_2 (k_1 a + l_1 b) = (-q_2 k_1) a + (1 - q_2 l_1) b = k_2 a + l_2 b.$$

Offenbar kann dieses Verfahren für die folgenden Reste r_3, r_4, \dots fortgesetzt werden, bis wir zu der Darstellung kommen:

$$r_n = ka + lb,$$

wie zu beweisen war.

Als Beispiel betrachten wir den euklidischen Algorithmus für (61, 24); der größte gemeinsame Teiler ist 1, und die gesuchte Darstellung für 1 kann aus den Gleichungen

$$\begin{aligned} 61 &= 2 \cdot 24 + 13, & 24 &= 1 \cdot 13 + 11, & 13 &= 1 \cdot 11 + 2, \\ 11 &= 5 \cdot 2 + 1, & 2 &= 2 \cdot 1 + 0 \end{aligned} \quad \text{gefunden werden.}$$

Aus der ersten dieser Gleichungen erhalten wir

$$13 = 61 - 2 \cdot 24,$$

aus der zweiten

$$11 = 24 - 13 = 24 - (61 - 2 \cdot 24) = -61 + 3 \cdot 24,$$

aus der dritten

$$2 = 13 - 11 = (61 - 2 \cdot 24) - (-61 + 3 \cdot 24) = 2 \cdot 61 - 5 \cdot 24$$

und aus der vierten

$$1 = 11 - 5 \cdot 2 = (-61 + 3 \cdot 24) - 5(2 \cdot 61 - 5 \cdot 24) = -11 \cdot 61 + 28 \cdot 24.$$

2. Anwendung auf den Fundamentalsatz der Arithmetik

Die Tatsache, daß $d = (a, b)$ immer in der Form $d = ka + lb$ geschrieben werden kann, läßt sich benutzen, um einen Beweis des Fundamentalsatzes der Arithmetik zu geben, der unabhängig von dem auf S. 19 gegebenen Beweis ist. Wir werden zuerst als Lemma das Corollar von S. 20 beweisen, und dann werden wir aus dem Lemma den Fundamentalsatz ableiten, indem wir also die Reihenfolge der Beweise umkehren.

Lemma: Wenn eine Primzahl p Teiler eines Produkts ab ist, dann muß p Teiler von a oder von b sein.

Wenn eine Primzahl p nicht Teiler der ganzen Zahl a ist, dann ist $(a, p) = 1$, da die einzigen Teiler von p die Zahlen p und 1 sind. Daher können wir ganze Zahlen k und l finden, so daß

$$1 = ka + lp.$$

Multiplizieren wir beide Seiten dieser Gleichung mit b , so erhalten wir

$$b = kab + lpb.$$

Wenn nun p ein Teiler von ab ist, so können wir schreiben

$$ab = pr,$$

so daß

$$b = kpr + lpb = p(kr + lb),$$

woraus klar wird, daß p ein Teiler von b ist. Wir haben also gezeigt: wenn p Teiler von ab , aber nicht von a ist, muß p notwendig Teiler von b sein, so daß auf jeden Fall die Primzahl p entweder Teiler von a oder von b ist, wenn sie Teiler von ab ist.

Die Verallgemeinerung für Produkte von mehr als zwei ganzen Zahlen ergibt sich sofort. Wenn zum Beispiel p Teiler von abc ist, so können wir durch zweimalige Anwendung des Lemmas zeigen, daß p Teiler von mindestens einer der Zahlen a , b , c sein muß. Denn wenn p weder Teiler von a noch von b , noch von c ist, so kann es nicht Teiler von ab sein und daher auch nicht von $(ab)c = abc$.

Übung: Soll diese Beweisführung auf Produkte einer beliebigen Anzahl n von ganzen Zahlen ausgedehnt werden, so muß explizit oder implizit das Prinzip der mathematischen Induktion angewandt werden. Man führe dies im einzelnen aus.

Aus diesem Ergebnis folgt der Fundamentalsatz der Arithmetik. Nehmen wir an, es seien zwei verschiedene Zerlegungen einer positiven ganzen Zahl N in Primzahlen gegeben:

$$N = p_1 p_2 \cdots p_r = q_1 q_2 \cdots q_s.$$

Da p_1 Teiler der linken Seite dieser Gleichung ist, muß es auch Teiler der rechten sein und daher nach der obigen Übung auch Teiler eines der Faktoren q_k . Aber q_k ist eine Primzahl, daher muß p_1 gleich diesem q_k sein. Nachdem man diese beiden gleichen Faktoren gestrichen hat, folgt in derselben Weise, daß p_2 Teiler eines der übrigen Faktoren q_i und daher ihm gleich sein muß. Man streicht p_2 und q_i und verfährt ebenso mit den p_3, \dots, p_r . Am Ende dieses Vorgangs sind alle p gestrichen, so daß nur 1 auf der linken Seite bleibt. Kein q kann auf der rechten Seite übrig sein, da alle q größer als eins sind. Also sind die p und q paarweise einander gleich, und das bedeutet, daß die beiden Zerlegungen, allenfalls abgesehen von der Reihenfolge, identisch waren.

3. EULERS φ -Funktion. Nochmals kleiner Fermatscher Satz

Zwei ganze Zahlen heißen *relativ prim*, wenn ihr größter gemeinsamer Teiler 1 ist:

$$(a, b) = 1.$$

Zum Beispiel sind 24 und 35 relativ prim, während 12 und 18 es nicht sind. *Wenn a und b relativ prim sind, so kann man immer mit geeignet gewählten positiven oder negativen ganzen Zahlen k und l schreiben:*

$$ka + lb = 1.$$

Das folgt aus der auf S. 37 besprochenen Eigenschaft von (a, b) .

Übung: Man beweise den Satz: *Wenn eine ganze Zahl r Teiler eines Produkts ab und relativ prim zu a ist, dann muß r Teiler von b sein.* (Anleitung: Wenn r relativ prim zu a ist, dann gibt es ganze Zahlen k und l , so daß

$$kr + la = 1.$$

Man multipliziere beide Seiten dieser Gleichung mit b .) Dieser Satz umfaßt das Lemma auf Seite 38 als speziellen Fall, da eine Primzahl dann und nur dann relativ prim zu einer ganzen Zahl a ist, wenn p nicht Teiler von a ist.

Für eine beliebige positive ganze Zahl n möge $\varphi(n)$ die Anzahl der ganzen Zahlen von 1 bis n bezeichnen, die relativ prim zu n sind. Diese Funktion $\varphi(n)$, die von EULER zuerst eingeführt wurde, ist eine „zahlentheoretische Funktion“ von großer Bedeutung. Die Werte von $\varphi(n)$ für die ersten Werte von n lassen sich leicht bestimmen:

$\varphi(1) = 1$	da 1 relativ prim zu 1 ist,
$\varphi(2) = 1$	da 1 relativ prim zu 2 ist,
$\varphi(3) = 2$	da 1 und 2 relativ prim zu 3 sind,
$\varphi(4) = 2$	da 1 und 3 relativ prim zu 4 sind,
$\varphi(5) = 4$	da 1, 2, 3, 4 relativ prim zu 5 sind,
$\varphi(6) = 2$	da 1 und 5 relativ prim zu 6 sind,
$\varphi(7) = 6$	da 1, 2, 3, 4, 5, 6 relativ prim zu 7 sind,
$\varphi(8) = 4$	da 1, 3, 5, 7 relativ prim zu 8 sind,
$\varphi(9) = 6$	da 1, 2, 4, 5, 7, 8 relativ prim zu 9 sind,
$\varphi(10) = 4$	da 1, 3, 7, 9 relativ prim zu 10 sind,
usw.	

Wir stellen fest, daß $\varphi(p) = p - 1$, wenn p eine Primzahl ist; denn eine Primzahl hat keinen anderen Teiler als sich selbst und 1 und ist daher relativ prim zu allen ganzen Zahlen 1, 2, 3, ..., $(p - 1)$. Wenn n die Primzahlzerlegung

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_r^{\alpha_r},$$

hat, in der die p lauter verschiedene Primzahlen, jede zu einer gewissen Potenz erhoben, bedeuten, dann ist

$$\varphi(n) = n \left(1 - \frac{1}{p_1}\right) \cdot \left(1 - \frac{1}{p_2}\right) \cdot \dots \cdot \left(1 - \frac{1}{p_r}\right).$$

Wegen $12 = 2^2 \cdot 3$ gilt z. B.

$$\varphi(12) = 12 \left(1 - \frac{1}{2}\right) \left(1 - \frac{1}{3}\right) = 12 \left(\frac{1}{2}\right) \left(\frac{2}{3}\right) = 4,$$

wie es sein muß. Der Beweis ist nicht schwer, soll hier aber fortgelassen werden.

**Übung:* Unter Benutzung der Eulerschen φ -Funktion soll der kleine Fermatsche Satz von S. 30 verallgemeinert werden. Der allgemeinere Satz behauptet: *Wenn n eine beliebige ganze Zahl ist und a relativ prim zu n , dann ist*

$$a^{\varphi(n)} \equiv 1 \pmod{n}.$$

4. Kettenbrüche. Diophantische Gleichungen

Der euklidische Algorithmus zur Bestimmung des größten gemeinsamen Teilers zweier Zahlen führt unmittelbar zu einer Methode für die Darstellung des Quotienten zweier ganzer Zahlen in Form eines zusammengesetzten Bruchs.

Wendet man den euklidischen Algorithmus z. B. auf die Zahlen 840 und 611 an, so liefert er die Gleichungen

$$\begin{aligned} 840 &= 1 \cdot 611 + 229, & 611 &= 2 \cdot 229 + 153, \\ 229 &= 1 \cdot 153 + 76, & 153 &= 2 \cdot 76 + 1, \end{aligned}$$

aus denen folgt, daß $(840, 611) = 1$. Aus diesen Gleichungen können wir die folgenden Ausdrücke ableiten:

$$\begin{aligned} \frac{840}{611} &= 1 + \frac{229}{611} = 1 + \frac{1}{611/229}, \\ \frac{611}{229} &= 2 + \frac{153}{229} = 2 + \frac{1}{229/153}, \\ \frac{229}{153} &= 1 + \frac{76}{153} = 1 + \frac{1}{153/76}, \\ \frac{153}{76} &= 2 + \frac{1}{76}. \end{aligned}$$

Durch Zusammenfassung dieser Gleichungen erhalten wir die Entwicklung der rationalen Zahl $\frac{840}{611}$ in der Form

$$\frac{840}{611} = 1 + \frac{1}{2 + \frac{1}{1 + \frac{1}{2 + \frac{1}{76}}}}.$$

Ein Ausdruck der Form

$$(7) \quad a = a_0 + \frac{1}{a_1 + \frac{1}{a_2 + \frac{1}{\ddots + \frac{1}{a_n}}}},$$

worin $a_0, a_1, a_2, \dots, a_n$ positive ganze Zahlen sind, heißt ein *Kettenbruch*. Der euklidische Algorithmus liefert uns eine Methode, um jede positive rationale Zahl in dieser Form auszudrücken.

Übung: Man stelle die Kettenbruchentwicklung von

$$\frac{2}{5}, \frac{43}{30}, \frac{169}{70}$$

auf.

*Kettenbrüche sind von großer Bedeutung in dem Zweig der höheren Arithmetik, der diophantische Analysis genannt wird. Eine *diophantische Gleichung* ist eine algebraische Gleichung in einer oder mehreren Unbekannten mit ganzzahligen Koeffizienten, für die ganzzahlige Lösungen gesucht werden. Solche Gleichungen können entweder gar keine, eine end-

liche oder eine unendliche Anzahl von Lösungen haben. Der einfachste Fall ist der der *linearen* diophantischen Gleichung mit zwei Unbekannten

$$(8) \quad ax + by = c,$$

worin a , b und c gegebene ganze Zahlen sind und ganzzahlige Lösungen x , y gesucht werden. Die vollständige Lösung einer Gleichung dieser Form kann mit dem euklidischen Algorithmus gefunden werden.

Zunächst findet man mit dem euklidischen Algorithmus $d = (a, b)$; dann ist bei geeigneter Wahl von k und l

$$(9) \quad ak + bl = d.$$

Daher hat die Gleichung (8) für den Fall $c = d$ die spezielle Lösung $x = k$, $y = l$. Allgemeiner, falls c ein Vielfaches von d ist,

$$c = d \cdot q,$$

gilt nach (9)

$$a(kq) + b(lq) = dq = c,$$

so daß (8) die spezielle Lösung $x = x^* = kq$, $y = y^* = lq$ hat. Wenn umgekehrt (8) irgendeine Lösung x , y für ein gegebenes c hat, dann muß c ein Vielfaches von $d = (a, b)$ sein; denn d ist Teiler von a und b und muß daher auch Teiler von c sein. Wir haben somit bewiesen, daß die Gleichung (8) dann und nur dann eine Lösung hat, wenn c ein Vielfaches von (a, b) ist.

Wir wollen nun die übrigen Lösungen von (8) bestimmen. Wenn $x = x'$, $y = y'$ eine andere Lösung als die oben mittels des euklidischen Algorithmus gefundene Lösung $x = x^*$, $y = y^*$ ist, dann muß offenbar $x = x' - x^*$, $y = y' - y^*$ eine Lösung der „homogenen“ Gleichung

$$(10) \quad ax + by = 0$$

sein. Aus

$$ax' + by' = c \quad \text{und} \quad ax^* + by^* = c$$

erhält man nämlich durch Subtraktion der zweiten Gleichung von der ersten

$$a(x' - x^*) + b(y' - y^*) = 0.$$

Nun ist die allgemeine Lösung der Gleichung (10) $x = rb/(a, b)$, $y = -ra/(a, b)$, worin r eine beliebige ganze Zahl ist. (Wir überlassen den Beweis dem Leser als Übungsaufgabe. Anleitung: Man teile durch (a, b) und benutze die Übung auf S. 39.) Hieraus folgt sofort:

$$x = x^* + rb/(a, b), \quad y = y^* - ra/(a, b).$$

Wir fassen zusammen: Die lineare diophantische Gleichung $ax + by = c$, worin a , b , c ganze Zahlen sind, hat dann und nur dann eine ganzzahlige Lösung, wenn c ein Vielfaches von (a, b) ist. In diesem Fall kann eine spezielle Lösung $x = x^*$, $y = y^*$ mit dem euklidischen Algorithmus gefunden werden, und die allgemeine Lösung hat die Form

$$x = x^* + rb/(a, b), \quad y = y^* - ra/(a, b),$$

worin r eine beliebige ganze Zahl ist.

Beispiele: Die Gleichung $3x + 6y = 22$ hat keine ganzzahlige Lösung, da $(3, 6) = 3$ und 3 nicht Teiler von 22 sind.

Die Gleichung $7x + 11y = 13$ hat die spezielle Lösung $x = -39$, $y = 26$, die man auf folgende Weise findet:

$$\begin{aligned} 11 &= 1 \cdot 7 + 4, & 7 &= 1 \cdot 4 + 3, & 4 &= 1 \cdot 3 + 1, & (7, 11) &= 1. \\ 1 &= 4 - 3 = 4 - (7 - 4) = 2 \cdot 4 - 7 = 2(11 - 7) - 7 = 2 \cdot 11 - 3 \cdot 7. \end{aligned}$$

Daher ist

$$\begin{aligned} 7 \cdot (-3) + 11(2) &= 1, \\ 7 \cdot (-39) + 11(26) &= 13. \end{aligned}$$

Die sämtlichen Lösungen sind dann gegeben durch

$$x = -39 + r \cdot 11, \quad y = 26 - r \cdot 7,$$

worin r eine beliebige ganze Zahl ist.

Übung: Man löse die diophantischen Gleichungen

$$a) \ 3x - 4y = 29, \quad b) \ 11x + 12y = 58, \quad c) \ 153x - 34y = 51.$$

Was ist Mathematik?

Courant, R.; Robbins, H.

2001, XXII, 399 S., Softcover

ISBN: 978-3-642-13700-6