# Prima Zahlen? – Primzahlen!

*Teilnehmer:*

| | |
|---|---|
| Yu Shi Li | Andreas-Oberschule, Berlin |
| Felix Fichte | Heinrich-Hertz-Oberschule, Berlin |
| Tuyet Mai Hoang Thi | Heinrich-Hertz-Oberschule, Berlin |
| Harry Bober | Herder-Oberschule, Berlin |
| Vincent Hitzler | Immanuel-Kant-Oberschule, Berlin |
| Julius Range | Käthe-Kollwitz-Oberschule, Berlin |
| David Schmidt | Städtisches Stiftsgymnasium, Xanten |

*Gruppenleiter:*

| | |
|---|---|
| Jürg Kramer | Humboldt-Universität zu Berlin<br>Mitglied im DFG-Forschungszentrum MATHEON<br>„Mathematik für Schlüsseltechnologien“ |
| Anna v. Pippich | Humboldt-Universität zu Berlin<br>Mitglied im DFG-Forschungszentrum MATHEON<br>„Mathematik für Schlüsseltechnologien“ |

Primzahlen bilden sozusagen die Atome der (multiplikativen) Zahlenwelt: Eine Primzahl lässt sich außer durch die Zahl 1 und sich selbst durch keine weitere Zahl teilen, und alle ganzen Zahlen lassen sich eindeutig als Produkt von Primzahlen darstellen. Diese Eigenschaften zeichnen die Primzahlen aus und es stellen sich ganz natürlich folgende Fragen:

(a) Wieviele Primzahlen gibt es?

(b) Wie kann man Primzahlen erkennen?

(c) Gibt es eine einfache Formel für alle Primzahlen?

(d) Wie sind die Primzahlen unter den natürlichen Zahlen verteilt?

(e) Können wir die Primzahlen bis zu einer gewissen Stelle mit Hilfe einer einfachen Formel abzählen?

Zur Diskussion und Beantwortung dieser und weiterer Fragen werden wir unterschiedlichste Methoden kennenlernen und sehen, warum Primzahlen auch heute noch eines der geheimnisvollsten und faszinierendsten Objekte der Mathematik sind. Dabei werden wir insbesondere den Zusammenhang zur bis heute unbewiesenen Riemannschen Vermutung, einem der Milleniumsprobleme, studieren. Schließlich wollen wir auch den praktischen Nutzen von Primzahlen, z.B. für die Kryptographie, kennenlernen.

# 1 Der Fundamentalsatz der Arithmetik

**Definition 1.1.** Eine natürliche Zahl $p > 1$ heißt *Primzahl*, wenn $p$ keine nichttrivialen Teiler hat, d.h. $p$ besitzt nur die Teiler 1 und $p$. Die Menge der Primzahlen bezeichnen wir im folgenden mit

$$\mathbb{P} := \{p \in \mathbb{N} \mid p \text{ ist Primzahl}\}.$$

**Lemma 1.1.** *Jede natürliche Zahl $a > 1$ besitzt mindestens einen Primteiler $p \in \mathbb{P}$, d.h. es existiert eine Primzahl $p$ mit $p \mid a$.*

*Beweis.* Zu diesem $a$ betrachten wir die Menge

$$\mathcal{T}(a) := \{b \in \mathbb{N} \mid b > 1 \text{ mit } b \mid a\}.$$

Da $a$ sich selbst teilt und nach Voraussetzung $a > 1$ gilt, muss $a \in \mathcal{T}(a)$ gelten. Wir wissen also, dass $\mathcal{T}(a)$ eine nicht-leere und nach unten beschränkte Menge ist. Somit existiert ein kleinstes Element $p \in \mathcal{T}(a)$.

Wir wollen zeigen, dass $p$ eine Primzahl ist. Dazu nehmen wir das Gegenteil an, d.h. wir nehmen an, dass $p$ einen von sich selbst und von 1 verschiedenen Teiler $q$ mit $1 < q < p$ besitzt. Da $q|p$ und $p|a$ gilt, folgt, dass $q$ auch $a$ teilt und somit in der Menge $\mathcal{T}(a)$ liegt.

Damit wäre $q$ ein kleineres Element der Menge $\mathcal{T}(a)$. Dies steht aber im Widerspruch zur Wahl von $p$. Somit gilt $p \in \mathbb{P}$. □

**Satz 1.2.** *Jede Zahl $a \in \mathbb{N}$, $a > 0$, lässt sich eindeutig schreiben als*

$$a = p_1^{a_1} \cdot \ldots \cdot p_r^{a_r},$$

*wobei $p_1, \ldots, p_r$ paarweise verschiedene Primzahlen sind und $a_1, \ldots, a_r \in \mathbb{N}_{>0}$ gilt; das leere Produkt wird hierbei als 1 definiert.*

*Beweis. Existenz:*
Der Beweis der Existenz der Primfaktorzerlegung von $a$ lässt sich sehr einfach mit Hilfe von Lemma 1.1 induktiv beweisen.

*Eindeutigkeit:*
Induktionsanfang: Die Behauptung ist für $a = 1$ offensichtlich richtig.
Induktionsannahme: Wir nehmen an, dass die Eindeutigkeit der Primfaktorzerlegung für alle $a' \in \mathbb{N}$ mit $1 \leq a' < a$ gilt.
Induktionsbehauptung: Wir haben die Eindeutigkeit der Primfaktorzerlegung für $a$ zu zeigen.
Induktionsbeweis (indirekter Beweis): Im Gegensatz zur Behauptung nehmen wir

an, dass $a$ zwei verschiedene Primfaktorzerlegungen besitzt, d.h. wir haben die beiden Primfaktorzerlegungen

$$\begin{aligned} a &= p_1^{a_1} \cdot p_2^{a_2} \cdot \ldots \cdot p_r^{a_r} = p_1 \cdot b \qquad \text{mit} \quad b = p_1^{a_1-1} \cdot p_2^{a_2} \cdot \ldots \cdot p_r^{a_r}, \\ a &= q_1^{b_1} \cdot q_2^{b_2} \cdot \ldots \cdot q_s^{b_s} = q_1 \cdot c \qquad \text{mit} \quad c = q_1^{b_1-1} \cdot q_2^{b_2} \cdot \ldots \cdot q_s^{b_s}. \end{aligned}$$

Ohne Beschränkung der Allgemeinheit können wir annehmen, dass

$$p_1 \notin \{q_1, \ldots, q_s\} \quad \text{und} \quad p_1 < q_1 \tag{1.1}$$

gilt. Hieraus ergibt sich die Ungleichung

$$a = q_1 \cdot c > p_1 \cdot c,$$

woraus folgt, dass ein $a' \in \mathbb{N}$ existiert mit der Eigenschaft

$$a' = a - p_1 \cdot c = \begin{cases} p_1 \cdot (b - c), \\ (q_1 - p_1) \cdot c, \end{cases}$$

wobei $a'$, $b-c$, $q_1 - p_1$, $c$ natürliche Zahlen kleiner als $a$ sind, welche nach Induktionsannahme eindeutige Primfaktorzerlegungen besitzen.

Wegen $a' = p_1 \cdot (b - c) = (q_1 - p_1) \cdot c$ kommt $p_1$ in der eindeutig bestimmten Primfaktorzerlegung von $(q_1 - p_1) \cdot c$ vor. Aufgrund der Eindeutigkeit der Primfaktorzerlegung erhalten wir somit

$$p_1 \,|\, (q_1 - p_1) \quad \text{oder} \quad p_1 \,|\, c.$$

Aufgrund von (1.1) und der Eindeutigkeit der Primfaktorzerlegung von $c$ kann $p_1$ die Zahl $c$ aber nicht teilen. Somit gilt

$$p_1 \,|\, (q_1 - p_1),$$

woraus unmittelbar $p_1 \,|\, q_1$ folgt. Dies ist aber wegen $1 < p_1 < q_1$ für die Primzahl $q_1$ nicht möglich. Damit haben wir einen Widerspruch, d.h. unsere Annahme der Existenz zweier verschiedener Primfaktorzerlegungen für $a$ ist falsch.

Damit haben wir die Eindeutigkeit der Primfaktorzerlegung natürlicher Zahlen mit vollständiger Induktion bewiesen. □

# 2 Fermatsche Primzahlen

**Definition 2.1.** Eine Primzahl der Form $p = 2^n + 1$ ($n \in \mathbb{N}$) heißt *Fermatsche Primzahl*.

**Lemma 2.1.** *Sei $n \in \mathbb{N}$. Dann gilt die Folgerung*

$$2^n + 1 = \textit{Primzahl} \Longrightarrow n = 2^m \textit{ mit einem } m \in \mathbb{N}.$$

*Beweis.* Angenommen, $n$ ist keine Zweierpotenz, dann besitzt $n$ einen ungeraden Teiler $r \in \mathbb{N}$, $r > 1$, d.h. es gilt

$$n = r \cdot n'$$

mit einem $n' \in \mathbb{N}$, $0 < n' < n$. Mit $a := 2^{n'}$ berechnen wir

$$\begin{aligned}
&(a+1) \cdot (a^{r-1} - a^{r-2} + - \ldots + a^2 - a + 1) = \\
&(a^r - a^{r-1} + - \ldots + a^3 - a^2 + a) + (a^{r-1} - a^{r-2} + - \ldots + a^2 - a + 1) = \\
&a^r + 1 = 2^{n' \cdot r} + 1 = 2^n + 1.
\end{aligned}$$

Wegen $0 < n' < n$ folgt $1 < a + 1 = 2^{n'} + 1 < n$ und damit ist $2^{n'} + 1$ ein echter Teiler von $2^n + 1$, d.h. $2^n + 1$ ist keine Primzahl. □

*Bemerkung.* Die Umkehrung von Lemma 2.1 ist falsch, denn es gilt zwar:

$$\begin{array}{lrcrcll}
m = 0: & 2^{2^0} + 1 & = & 2^1 + 1 & = & 3, & \text{Primzahl,} \\
m = 1: & 2^{2^1} + 1 & = & 2^2 + 1 & = & 5, & \text{Primzahl,} \\
m = 2: & 2^{2^2} + 1 & = & 2^4 + 1 & = & 17, & \text{Primzahl,} \\
m = 3: & 2^{2^3} + 1 & = & 2^8 + 1 & = & 257, & \text{Primzahl,} \\
m = 4: & 2^{2^4} + 1 & = & 2^{16} + 1 & = & 65\,537, & \text{Primzahl.}
\end{array}$$

Allerdings ist bereits die Zahl $2^{2^5} + 1 = 4\,294\,967\,297$ keine Primzahl mehr, da sie den nicht-trivialen Teiler 641 besitzt. Die Zahlen 3, 5, 7, 257 und 65 537 sind die einzigen bis heute bekannten Fermatschen Primzahlen und es ist eine noch unbewiesene Vermutung der Zahlentheorie, dass es außer diesen ersten fünf keine weiteren Fermatschen Primzahlen gibt.

**Lemma 2.2.** *Die Zahlen $F_m := 2^{2^m} + 1$ ($m \in \mathbb{N}$) sind paarweise teilerfremd.*

*Beweis.* Durch Induktion über $m$ zeigen wir zunächst, dass

$$F_m - 2 = F_0 \cdot F_1 \cdot \ldots \cdot F_{m-1} \tag{2.1}$$

gilt. Der Induktionsanfang für $m = 1$ ist wegen $F_1 - 2 = (2^{2^1} + 1) - 2 = 3 = F_0$ richtig. Wir nehmen nun an, dass (2.1) für ein $m \in \mathbb{N}$ erfüllt ist. Wir haben zu zeigen, dass dann auch $F_{m+1} - 2 = F_0 \cdot F_1 \cdot \ldots \cdot F_{m-1} \cdot F_m$ gilt. Mit unserer Induktionsannahme berechnen wir

$$\begin{aligned}
&F_0 \cdot F_1 \cdot \ldots \cdot F_{m-1} \cdot F_m = (F_m - 2) \cdot F_m = F_m^2 - 2 \cdot F_m = \\
&(2^{2^m} + 1)^2 - 2 \cdot (2^{2^m} + 1) = 2^{2^m \cdot 2} - 1 = (2^{2^{m+1}} + 1) - 2 = F_{m+1} - 2,
\end{aligned}$$

was die Behauptung beweist. Damit haben wir (2.1) per Induktion bewiesen.

Aus der Beziehung (2.1) folgt, dass die Zahl $F_n$ für $n \in \mathbb{N}$ mit $n < m$ ein Teiler von $F_m - 2$ ist. Angenommen, eine Primzahl $p$ teilt nun sowohl $F_n$ als auch $F_m$, dann muss $p$ auch die Zahl $F_m - (F_m - 2) = 2$ teilen, woraus sofort $p = 2$ folgt. Dies ist aber ein Widerspruch, da $F_n$ ungerade und damit nicht durch 2 teilbar ist. Damit haben wir bewiesen, dass $F_n$ teilerfremd zu $F_m$ ist. □

**Satz 2.3.** *Es gibt unendlich viele Primzahlen.*

*Beweis von Goldbach.* Für $m \in \mathbb{N}$ betrachten wir die unendliche Folge

$$1 < F_0 < F_1 < \ldots < F_m < F_{m+1} < \ldots,$$

wobei $F_m := 2^{2^m} + 1$. Nach Lemma 1.1 besitzt jede Zahl $F_m$ mindestens einen Primteiler und nach Lemma 2.2 sind die Zahlen $F_m$ paarweise teilerfremd. Falls nun also $p_0$ eine Primzahl ist, die $F_0$ teilt, und $p_1$ eine Primzahl, die $F_1$ teilt, und so weiter, dann sind alle

$$p_0, p_1, \ldots, p_m, p_{m+1}, \ldots$$

verschieden, d.h. es gibt unendlich viele Primzahlen. □

# 3 Mersennesche Primzahlen

**Definition 3.1.** Eine Primzahl der Form $p = 2^n - 1$ ($n \in \mathbb{N}$) heißt *Mersennesche Primzahl*.

**Lemma 3.1.** *Sei $n \in \mathbb{N}$. Dann gilt die Folgerung*

$$2^n - 1 = \textit{Primzahl} \Rightarrow n = \textit{Primzahl}.$$

*Beweis.* Angenommen, $n$ ist keine Primzahl. Dann besitzt $n$ zwei echte Teiler, d.h. es gilt $n = a \cdot b$ mit $a, b \in \mathbb{N}$ und $1 < a, b < n$. Wir berechnen

$$\begin{aligned}
&(2^a - 1) \cdot (2^{(b-1)a} + 2^{(b-2)a} + 2^{(b-3)a} + \ldots + 2^a + 1) = \\
&(2^{a+(b-1)a} + 2^{a+(b-2)a} + 2^{a+(b-3)a} + \ldots + 2^{2a} + 2^a) + \\
&(-2^{(b-1)a} - 2^{(b-2)a} - 2^{(b-3)a} - \ldots - 2^a - 1) = \\
&2^{a+(b-1)a} - 1 = 2^{ab} - 1 = 2^n - 1.
\end{aligned}$$

Wegen $1 < a < n$ folgt $1 < 2^a - 1 < 2^n - 1$ und damit ist $2^a - 1$ ein echter Teiler von $2^n + 1$, d.h. $2^n + 1$ ist keine Primzahl. □

*Bemerkung.* Die Umkehrung von Lemma 3.1 ist falsch: für die ersten vier Primzahlen $n = 2, 3, 5, 7$ sind zwar $2^2-1 = 3$, $2^3-1 = 7$, $2^5-1 = 31$, $2^7-1 = 127$ auch Primzahlen, allerdings ist bereits für $n = 11$ die Zahl $2^{11}-1 = 2047 = 23 \cdot 89$ keine Primzahl mehr. Es ist ein noch ungelöstes Problem der Zahlentheorie, ob es unendlich viele Mersennsche Primzahlen gibt. Die derzeit größte bekannte Primzahl ist auch eine Mersennsche Primzahl, nämlich

$$2^{43\,112\,609} - 1,$$

eine Zahl mit 12 978 189 Stellen.

# 4 Die Riemannsche Zetafunktion

Um den Primzahlen weiter auf die Schliche zu kommen, haben wir die sogenannte Riemannsche Zetafunktion

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

für $s \in \mathbb{R}$ betrachtet.

**Satz 4.1.** *Die Reihe $\zeta(s)$ konvergiert für $s > 1$.*

*Beweis.* Die behauptete Konvergenz für $s > 1$ lässt sich beispielsweise einfach mit Hilfe des Cauchyschen Vergleichskriteriums beweisen. □

Durch die Eulersche Produktentwicklung kann man die Riemannsche Zetafunktion mit den Primzahlen in Verbindung bringen.

**Satz 4.2.** *Für $s \in \mathbb{R}$ mit $s > 1$ besteht die Produktentwicklung*

$$\zeta(s) = \prod_{p \in \mathbb{P}} \frac{1}{1 - p^{-s}}.$$

*Beweis.* Mit Hilfe der Summationsformel einer geometrischen Reihe

$$\sum_{n=0}^{\infty} q^n = \frac{1}{1-q} \quad (|q| < 1)$$

lassen sich die Faktoren der rechten Seite der behaupteten Produktentwicklung für $s > 1$ wie folgt umformen

$$\frac{1}{1 - p^{-s}} = \sum_{m=0}^{\infty} p^{-ms}.$$

Durch Einsetzen dieser Formel erhalten wir für die rechte Seite

$$\prod_{p\in\mathbb{P}} \frac{1}{1-p^{-s}} = \prod_{p\in\mathbb{P}} \sum_{m=0}^{\infty} p^{-ms} = \prod_{p\in\mathbb{P}} \left(1 + \frac{1}{p^s} + \frac{1}{p^{2s}} + \frac{1}{p^{3s}} + \dots\right) =$$
$$\left(1 + \frac{1}{2^s} + \frac{1}{2^{2s}} + \dots\right)\left(1 + \frac{1}{3^s} + \frac{1}{3^{2s}} + \dots\right)\left(1 + \frac{1}{5^s} + \frac{1}{5^{2s}} + \dots\right)\cdot\dots$$

Nach Ausmultiplizieren ergeben sich Terme der Form

$$\frac{1}{(p_1^{a_1}\cdot\ldots\cdot p_r^{a_r})^s},$$

wobei $p_1,\dots,p_r \in \mathbb{P}$ und $a_1,\dots,a_r \in \mathbb{N}_{>0}$ gilt. Nach dem Fundamentalsatz der Arithmetik wissen wir nun aber, dass dabei alle natürlichen Zahlen erfasst werden, d.h. wir haben die Gleichheit

$$\prod_{p\in\mathbb{P}} \frac{1}{1-p^{-s}} = \sum_{n=1}^{\infty} \frac{1}{n^s}$$

gezeigt, was die Behauptung ist. □

*Bemerkung.* An dieser Stelle sei auf die beiden folgenden Tatsachen hingewiesen:

1. Die Produktentwicklung ist äquivalent zum Fundamentalsatz (Satz 1.2).
2. Da $\zeta(1)$ divergent ist, folgt mit der Produktentwicklung, dass es unendlich viele Primzahlen gibt. Dies ist also ein alternativer Beweis von Satz 2.3.

Um einzuschätzen, welche Werte die Riemannsche Zetafunktion annimmt, haben wir $\zeta(2)$ berechnet (Basler Problem).

**Satz 4.3.** *Es gilt*

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

*Beweis.* Wir verweisen hier auf den sehr elementaren Beweis 11 aus [1]. □

# 5 Die Primzahlfunktion

Wir beginnen mit folgendem Zitat:

> Don Zagier (1975): Es gibt zwei Tatsachen über die Verteilung von Primzahlen: Die eine ist, daß die Primzahlen, trotz ihrer einfachen Definition und Rolle als Bausteine der natürlichen Zahlen, zu den willkürlichsten, widerspenstigsten Objekten gehören, die der Mathematiker überhaupt studiert. Sie wachsen wie Unkraut unter den natürlichen Zahlen, scheinbar keinem anderen Gesetz als dem Zufall unterworfen, und kein Mensch kann voraussagen, wo wieder eine sprießen wird, noch einer Zahl ansehen, ob sie prim ist oder nicht. Die andere Tatsache ist viel verblüffender, denn sie sagt just das Gegenteil, daß die Primzahlen die ungeheuerste Regelmäßigkeit aufzeigen, dass sie durchaus Gesetzen unterworfen sind und diesen mit fast peinlicher Genauigkeit gehorchen.

In diesem Abschnitt wollen wir untersuchen, wo die Primzahlen liegen. Dabei stellen wir einerseits fest, dass wir für beliebiges $k \in \mathbb{N}_{>0}$ eine Primzahllücke der Länge $k$ finden können: Ist nämlich $N$ das Produkt aller Primzahlen, welche kleiner oder gleich $k+1$ sind, so sind die $k$ Zahlen

$$N+2, N+3, \ldots, N+k, N+k+1$$

*keine* Primzahlen.

Andererseits gibt es auch immer wieder Primzahlzwillinge, z.B. (3,5), (5,7), oder (11,13). Das derzeit grösste bekannte Paar von Primzahlen ist

$$(65\,516\,468\,355 \cdot 2^{333\,333} - 1, 65\,516\,468\,355 \cdot 2^{333\,333} + 1)$$

und es ist ein uraltes ungelöstes Problem, ob es unendliche viele Primzahlzwillinge gibt.

**Definition 5.1.** Für $x \in \mathbb{R}$ definieren wir die *Primzahlfunktion* durch

$$\pi(x) := \sharp\{p \in \mathbb{P} \mid p \leq x\},$$

d.h. $\pi(x)$ ist definiert als die Anzahl aller Primzahlen kleiner gleich $x$.

*Bemerkung.* Die Primzahlfunktion ist eine Treppenfunktion und springt stets um 1 bei jedem $x \in \mathbb{P}$.

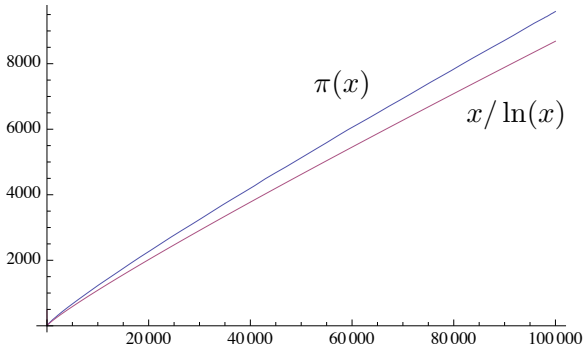
*Überlegung.* Man betrachte die ersten Zehnerpotenzen:

| $n$ | $\pi(n)$ | $n/\pi(n)$ |
|---:|---:|---:|
| 10 | 4 | 2.5 |
| 100 | 25 | 4.0 |
| 1 000 | 168 | 6.0 |
| 10 000 | 1 229 | 8.1 |
| 100 000 | 9 592 | 10.4 |
| 1 000 000 | 78 498 | 12.7 |
| 10 000 000 | 664 579 | 15.0 |

Man bemerkt, dass $n/\pi(n)$ immer um ungefähr 2.3 steigt, wenn wir zur nächsten Zehnerpotenz übergehen. Nun ist $2.3 \sim \ln(10)$ und wir vermuten die Beziehung

$$\frac{10n}{\pi(10n)} \sim \frac{n}{\pi(n)} + \ln(10)\,,$$
$$\text{d.h. } \frac{n}{\pi(n)} \sim \ln(n) \quad \text{bzw.} \quad \pi(n) \sim \frac{n}{\ln(n)}.$$

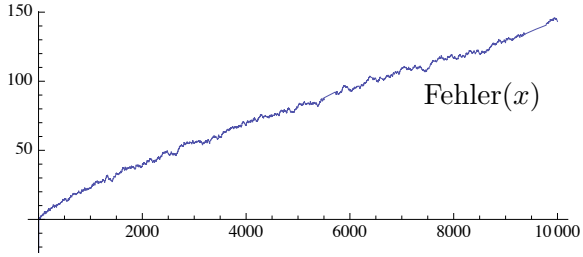
Sieht man sich die Kurven $\pi(x)$ und $x/\ln(x)$ unter einem „Makroskop“ an, so erkennt man tatsächlich eine erstaunliche Ähnlichkeit, die der folgende Satz, der sogenannte Primzahlsatz, präzisiert.




**Satz 5.1.** *(Primzahlsatz). Es gilt*

$$\pi(x) \sim \frac{x}{\ln(x)}, \qquad \textit{d.h.} \qquad \lim_{x\to\infty} \frac{\pi(x)}{x/\ln(x)} = 1.$$

*Beweis.* Der Primzahlsatz wurde 1896 von Hadamard und von de la Vallée Poussin bewiesen; ein elementarer Beweis wurde 1949 von Atle Selberg (siehe [4]), ein anderer von Paul Erdős gefunden. □




Wie groß der Fehler $\text{Fehler}(x) := \pi(x) - x/\ln(x)$ ist, ist ein Milleniumsproblem, die sogannte Riemannsche Vermutung.

*Die Riemannsche Vermutung.* Es gilt die Abschätzung

$$\big|\text{Fehler}(x)\big| \le C \cdot \sqrt{x} \qquad (C = \text{Konstante}).$$

# 6 RSA - Primzahlen in der Kryptographie

RSA ist ein Verfahren zur Verschlüsselung und Signierung von beliebiger Information, welche sich mit Hilfe natürlicher Zahlen darstellen lässt. Das Verfahren wurde 1977 von Ronald L. **R**ivest, Adi **S**hamir und Leonard **A**dleman am MIT (Cambridge, USA) entwickelt. Die Sicherheit des Verfahrens basiert auf der Eigenschaft der natürlichen Zahlen, dass sich diese zwar eindeutig in Primfaktoren zerlegen lassen, diese Zerlegung aber bei sehr großen Zahlen (ca. 400-stellig) auch mit den größten Rechnern der Welt erst nach astronomisch langer Rechenzeit gefunden werden kann.

**Satz 6.1.** *(Division mit Rest). Es seien $a, b$ zwei ganze Zahlen mit $b \neq 0$. Dann existieren eindeutig bestimme ganze Zahlen $q, r$ mit $0 \leq r < |b|$, so dass*

$$a = q \cdot b + r$$

*gilt.*

*Beweis.* Siehe [2], S. 96. □

*Bemerkung.* Sind $a, b$ zwei ganze Zahlen mit $b \neq 0$, so bezeichnen wir im Folgenden den Rest $r$ von $a$ nach Division durch $b$ mit $R_b(a)$.

**Satz 6.2.** *(Euklidischer Algorithmus). Es seien $a, b$ zwei ganze Zahlen mit $b \neq 0$. Durch fortgesetzte Division mit Rest erhalten wir*

$$\begin{aligned}
a &= q_1 \cdot b + r_1 && \text{mit} \quad 0 < r_1 < |b|,\\
b &= q_2 \cdot r_1 + r_2 && \text{mit} \quad 0 < r_2 < r_1,\\
r_1 &= q_3 \cdot r_2 + r_3 && \text{mit} \quad 0 < r_3 < r_2,\\
&\vdots\\
r_{n-1} &= q_{n+1} \cdot r_n + r_{n+1} && \text{mit} \quad 0 < r_{n+1} < r_n,\\
r_n &= q_{n+2} \cdot r_{n+1}.
\end{aligned}$$

*Dann ist der letzte nicht verschwindende Rest $r_{n+1}$ gleich dem größten gemeinsamen Teiler $\mathrm{ggT}(a, b)$ von $a, b$.*

*Beweis.* Siehe [2], S. 143. □

*Bemerkung.* Rollt man den Euklidischen Algorithmus von hinten auf, so erkennt man, dass man in der Lage ist, zu vorgegebenen ganzen Zahlen $a, b$ ganze Zahlen $x, y$ zu berechnen, welche der Gleichung

$$x \cdot a + y \cdot b = \mathrm{ggT}(a, b)$$

genügen, d.h. der größte gemeinsame Teiler von $a, b$ kann als ganzzahlige Linearkombination von $a, b$ dargestellt werden.

**Satz 6.3.** *(Kleiner Satz von Fermat). Es seien $p$ eine Primzahl und $a$ eine zu $p$ teilerfremde ganze Zahl. Dann gilt*

$$a^{p-1} \equiv 1 \mod p \iff p|(a^{p-1}-1) \iff R_p(a^{p-1}) = 1.$$

*Beweis.* Man betrachte das Repräsentantensystem $\{1, \ldots, p-1\}$ der primen Restklassen modulo $p$. Indem wir diese Repräsentanten mit $a$ multiplizieren, erhalten wir ein anderes Repräsentantensystem derselben Restklassen modulo $p$. Damit erkennen wir die Gleichheit

$$(a \cdot 1) \cdot \ldots \cdot (a \cdot (p-1)) \equiv 1 \cdot \ldots \cdot (p-1) \mod p.$$

Nach Multiplikation mit dem multiplikativ-inversen Element des Produkts $1 \cdot \ldots \cdot (p-1) \mod p$, ergibt sich

$$a^{p-1} \equiv 1 \mod p,$$

wie behauptet. □

**Satz 6.4.** *(Satz von Euler). Es seien $p, q$ zwei verschiedene Primzahlen und $a$ eine zu $p, q$ teilerfremde ganze Zahl. Dann gilt*

$$a^{(p-1)(q-1)} \equiv 1 \mod pq \iff pq|(a^{(p-1)(q-1)}-1) \iff R_{pq}(a^{(p-1)(q-1)}) = 1.$$

*Beweis.* Der Beweis lässt sich relativ leicht mit Hilfe des Kleinen Satzes von Fermat herleiten. □

## Verschlüsselung

Um eine Information (z.B. einen Text) mit dem RSA-Verfahren zu verschlüsseln, geht man wie folgt vor; dabei wird die zu übermittelnde Nachricht mit ASCII in einen Block von Zahlen mit Blöcken der Länge $m_1, m_2, \ldots$ aufgeteilt, so dass gilt $m_i < n$ gilt.

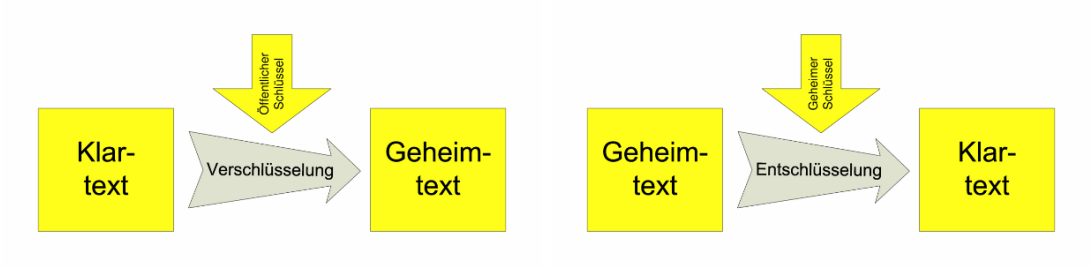
1. Man wähle zwei verschiedene Primzahlen $p, q \in \mathbb{P}$.
2. Man setze $n = p \cdot q$.
3. Man berechne $\varphi(n) = (p-1) \cdot (q-1)$.
4. Man wähle $c \in \mathbb{N}$ mit $1 < c < \varphi(n)$ und $\mathrm{ggT}(c, \varphi(n)) = 1$.
5. Man berechne $d \in \mathbb{N}$ mit $1 < d < \varphi(n)$ und $\varphi(n) \,|\, (c \cdot d - 1)$.
   (Mit Hilfe des Euklidischen Algorithmus' finden sich ganze Zahlen $d, y$, welche der Gleichung $c \cdot d + \varphi(n) \cdot y = 1$ genügen, was $\varphi(n) \,|\, (c \cdot d - 1)$ impliziert.)

6. Der öffentliche Schlüssel ist gegeben durch: $(c, n)$,
   der private Schlüssel ist gegeben durch: $(d, n)$.

7. Die Nachricht sei durch $m \in \mathbb{N}$ mit $\mathrm{ggT}(m, n) = 1$ gegeben.

8. Man verschlüssle die Nachricht durch $\overline{m} = R_n(m^c)$.

9. Das Entschlüsseln der Nachricht erfolgt durch $R_n(\overline{m}^d)$, da aufgrund des Satzes von Euler die Beziehung $m = R_n(\overline{m}^d)$ gilt.




## Signierung

Um eine Nachricht $M$ zu signieren, wird diese vom Sender mit dem eigenen privaten Schlüssel verschlüsselt. Zum Prüfen entschlüsselt der Empfänger die Nachricht mit dem öffentlichen Schlüssel des Senders und vergleicht diese mit der zusätzlich übermittelten unverschlüsselten Nachricht $M$. Wenn die beiden Informationen übereinstimmen, ist die Signatur gültig und der Empfänger kann sicher sein, dass derjenige, der das Dokument signiert hat, auch den privaten Schlüssel besitzt und dass niemand seit der Signierung das Dokument geändert hat.

# Literatur


[1] R. Chapman, *Evaluating* $\zeta(2)$, `http://www.uam.es/personal_pdi/ciencias/cillerue/Curso/zeta2.pdf`, 2003.

[2] J. Kramer, *Zahlen für Einsteiger. Elemente der Algebra und Aufbau der Zahlbereiche*, Vieweg+Teubner, 2008.

[3] P. Ribenboim, *Die Welt der Primzahlen. Geheimnisse und Rekorde*, Springer-Verlag, Berlin, 2011.

[4] A. Selberg, *An elementary proof of the prime-number theorem*, Ann. Math. **50**, Nr. 2, 1949, S. 305–313.