Kapitel 3
Primzahlen

Wie wir aus dem ersten Kapitel wissen, sind Primzahlen die Grundbausteine für die multiplikative Struktur der ganzen Zahlen, und aus Kapitel zwei wissen wir, daß sie auch wichtige Anwendungen außerhalb der Zahlentheorie haben. Es lohnt sich also auf jeden Fall, sie etwas genauer zu untersuchen.

§1: Die Verteilung der Primzahlen

Als erstes stellt sich die Frage, wie viele Primzahlen es gibt. Die Antwort finden wir schon in EUKLIDs Elementen; der dort gegebene Beweis dürfte immer noch der einfachste sein: Es gibt unendlich viele Primzahlen, denn gäbe es nur endlich viele Primzahlen $p_1, \ldots, p_n$, so könnten wir deren Produkt P bilden und die Primzerlegung von $P+1$ betrachten. Da P durch alle p_i teilbar ist, ist $P+1$ durch kein p_i teilbar, im Widerspruch zur Existenz der Primfaktorzerlegung. Somit muß es noch weitere, also unendlich viele Primzahlen geben.

Um nicht ganz auf dem Stand von vor rund zweieinhalb Jahrtausenden stehen zu bleiben, wollen wir uns noch einen zweiten, auf EULER zurückgehenden Beweis ansehen.

Dazu betrachten wir für eine reelle Zahl $s > 1$ die unendliche Reihe

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

Als erstes müssen wir uns überlegen, daß diese Reihe konvergiert. Da alle Summanden positiv sind, müssen wir dafür nur zeigen, daß es eine

gemeinsame obere Schranke für alle Teilsummen gibt. Da die Funktion $x \mapsto 1/x^s$ für $x > 0$ monoton fallend ist, haben wir für $n-1 \le x \le n$ die Abschätzung $1/n^s \le 1/x^s$, d.h.

$$\sum_{n=1}^{N} \frac{1}{n^s} = 1 + \sum_{n=2}^{N} \frac{1}{n^s} \le 1 + \int_1^N \frac{dx}{x^s}$$

$$< 1 + \int_1^\infty \frac{dx}{x^s} = 1 + \frac{1}{s-1} = \frac{s}{s-1}\,.$$

Somit ist $\zeta(s)$ für alle $s > 1$ wohldefiniert.

Einen Zusammenhang mit Primzahlen liefert der folgende

Satz: *a)* Für $s > 1$ ist $\zeta(s) = \prod_{p \text{ prim}} \frac{1}{1 - \frac{1}{p^s}}$.

b) Für alle $N \in \mathbb{N}$ und alle reellen $s > 0$ ist $\sum_{n=1}^{N} \frac{1}{n^s} \le \prod_{\substack{p \le N \\ p \text{ prim}}} \frac{1}{1 - \frac{1}{p^s}}$.

Beweis: Wir beginnen mit *b)*. Für $N = 1$ steht hier die triviale Formel $1 \le 1$; sei also $N \ge 2$, und seien $p_1, \ldots, p_r$ die sämtlichen Primzahlen kleiner oder gleich N. Nach der Summenformel für die geometrische Reihe ist

$$\frac{1}{1 - \frac{1}{p_k^s}} = \sum_{\ell=0}^{\infty} \frac{1}{p_k^{\ell s}}\,,$$

und das Produkt der rechtsstehenden Reihen über $k = 1$ bis r ist wegen der Eindeutigkeit der Primzerlegung die Summe über alle jene $1/n^s$, für die n keinen Primteiler größer N hat. Darunter sind insbesondere alle $n \le N$, womit *b)* bewiesen wäre.

Die Differenz zwischen $\zeta(s)$ und dem Produkt auf der rechten Seite von *b)* ist gleich der Summe über alle $1/n^s$, für die n mindestens einen Primteiler größer N haben. Diese Summe ist natürlich höchstens gleich der Summe aller $1/n^s$ mit $n > N$, und die geht wegen der Konvergenz von $\zeta(s)$ gegen null für $N \to \infty$. Damit ist auch *a)* bewiesen. ∎

Auch daraus folgt, daß es unendlich viele Primzahlen gibt: Gäbe es nämlich nur endlich viele, so stünde auf der rechten Seite von *b)* für jedes hinreichend große N das Produkt über die *sämtlichen* Primzahlen. Da es nur endlich viele Faktoren hat, wäre es auch für $s = 1$ endlich, und damit müßte

$$\sum_{n=1}^{\infty} \frac{1}{n}$$

kleiner oder gleich dieser Zahl sein, im Widerspruch zur Divergenz der harmonischen Reihe.

Verglichen mit dem Beweis aus EUKLIDs Elementen ist EULERs Methode erheblich komplizierter. Um trotzdem ihre Existenzberechtigung zu haben, sollte sie uns daher auch mehr Informationen liefern. In welchem Maße sie dies tatsächlich leistet, geht wahrscheinlich sogar noch deutlich über alles hinaus, was EULER seinerzeit träumen konnte.

Zunächst einmal können wir Teil *b)* für $s = 1$ zu einer quantitativen Abschätzung bezüglich der Anzahl $\pi(N)$ der Primzahlen kleiner oder gleich N umformulieren: Wie oben im Konvergenzbeweis für $\zeta(s)$ können wir aus der Monotonie der Funktion $x \mapsto 1/x$ folgern, daß für alle $N \in \mathbb{N}$ gilt

$$\log(N+1) = \int_1^{N+1} \frac{dx}{x} < \sum_{n=1}^{N} \frac{1}{n} < 1 + \int_1^{N} \frac{dx}{x} = 1 + \log N\,.$$

Zur Abschätzung der linken Seite beachten wir einfach, daß der Faktoren $1/(1-1/p)$ für $p = 2$ gleich zwei ist, ansonsten aber kleiner. Somit ist

$$\log(N+1) < \sum_{n=1}^{N} \frac{1}{n} \leq \prod_{\substack{p \leq N \\ p \text{ prim}}} \frac{1}{1-\frac{1}{p}} \leq 2^{\pi(N)}$$

und damit

$$\pi(N) \geq \frac{\log\log(N+1)}{\log 2}\,.$$

Wie wir bald sehen werden, ist das allerdings eine sehr schwache Abschätzung.

EULERs Methode erlaubt uns auch, die Dichte der Primzahlen zu vergleichen mit der Dichte beispielsweise der Quadratzahlen: Wie wir oben gesehen haben, konvergiert $\zeta(s)$ für alle $s > 1$, insbesondere also konvergiert die Summe $\zeta(2)$ der inversen Quadratzahlen. EULER konnte mit seiner Methode zeigen, daß die Summe der inversen Primzahlen *divergiert*, so daß die Primzahlen zumindest in diesem Sinne dichter liegen als die Quadratzahlen und alle anderen Potenzen mit (reellem) Exponenten $x > 1$.

Zum Beweis fehlt uns nur noch eine Analysis I Übungsaufgabe: Wir wollen uns überlegen, daß für alle $0 \leq x \leq \frac{1}{2}$ gilt $(1 - x) \geq 4^{-x}$. An den Intervallenden stimmen beide Funktionen überein, und $1 - x$ ist eine lineare Funktion. Es reicht daher, wenn wir zeigen, daß 4^{-x} eine konvexe Funktion ist, daß also ihre zweite Ableitung überall im Intervall positiv ist. Das ist aber klar, denn die ist einfach $\log(4)^2 \cdot 4^{-x}$. Für jede Primzahl p ist daher

$$1 - \frac{1}{p} \geq 4^{-1/p} \quad \text{und} \quad \frac{1}{1 - \frac{1}{p}} \leq 4^{1/p} .$$

Zusammen mit der vorigen Abschätzung folgt

$$\log(N + 1) < \prod_{\substack{p \leq N \\ p \text{ prim}}} \frac{1}{1 - \frac{1}{p}} \leq \prod_{\substack{p \leq N \\ p \text{ prim}}} 4^{1/p} = 4^{\sum \frac{1}{p}} ,$$

wobei die Summe im Exponenten über alle Primzahlen $p \leq N$ geht. Da $\log(N + 1)$ für $N \to \infty$ gegen unendlich geht, muß somit auch die Summe der inversen Primzahlen divergieren.

Mit diesen Bemerkungen fängt allerdings die Nützlichkeit der Funktion $\zeta(s)$ für das Verständnis der Funktion $\pi(N)$ gerade erst an: Ein Jahrhundert nach EULER erkannte RIEMANN, daß die Funktion $\zeta(s)$ ihre wahre Nützlichkeit für das Studium von $\pi(N)$ erst zeigt, wenn man sie auch für komplexe Argumente s betrachtet. Jeder, der sich ein bißchen mit Funktionen einer komplexer Veränderlichen auskennt, kann leicht zeigen, daß $\zeta(s)$ auch für komplexe Zahlen mit Realteil größer ein konvergiert: Der Imaginärteil des Exponenten führt schließlich nur zu einem Faktor vom Betrag eins.

RIEMANNs wesentliche Erkenntnis war, daß sich $\zeta(s)$ fortsetzen läßt zu einer analytischen Funktion auf der gesamten Menge der komplexen Zahlen mit Ausnahme der Eins (wo die ζ-Funktion wegen der Divergenz der harmonischen Reihe keinen endlichen Wert haben kann).

GEORG FRIEDRICH BERNHARD RIEMANN (1826-1866) war Sohn eines lutherischen Pastors und schrieb sich 1946 auf Anraten seines Vaters an der Universität Göttingen für das Studium der Theologie ein. Schon bald wechselte an die Philosophische Fakultät, um dort unter anderem bei GAUSS Mathematikvorlesungen zu hören. Nach Promotion 1851 und Habilitation 1854 erhielt er dort 1857 einen Lehrstuhl. Trotz seines frühen Todes initiierte er grundlegende auch noch heute fundamentale Entwicklungen in der Geometrie, der Zahlentheorie und über abelsche Funktionen. Wie sein Nachlaß zeigte, stützte er seine 1859 aufgestellte Vermutung über die Nullstellen der ζ-Funktion auf umfangreiche Rechnungen.

Für Leser, die nicht mit dem Konzept der analytischen Fortsetzung vertraut sind, möchte ich ausdrücklich darauf hinweisen, daß dies selbstverständlich nicht bedeutet, daß die definierende Summe der ζ-Funktion für reelle Zahlen kleiner eins oder komplexe Zahlen mit Realteil kleiner oder gleich eins konvergiert: Analytische Fortsetzung besteht darin, daß eine differenzierbare Funktion (die im Komplexen automatisch beliebig oft differenzierbar ist und um jeden Punkt in eine TAYLOR-Reihe entwickelt werden kann) via TAYLOR-Reihen über ihren eigentlichen Definitionsbereich hinweg ausgedehnt wird. Man kann beispielsweise zeigen, das $\zeta(-1) = -\frac{1}{12}$ ist. Setzt man $s = -1$ in die für $s > 1$ gültige Reihe ein, erhält man die Summe aller natürlicher Zahlen, die selbstverständlich nicht gleich $-\frac{1}{12}$ ist, sondern divergiert. Entsprechend hat $\zeta(s)$ Nullstellen bei allen geraden negativen Zahlen, obwohl auch hier die entsprechenden Reihen divergieren. Diese Nullstellen bezeichnet man als die sogenannten *trivialen* Nullstellen der ζ-Funktion, da sie sich sofort aus einer bei der Konstruktion der analytischen Fortsetzung zu beweisenden Funktionalgleichung ablesen lassen. Für die Primzahlverteilung spielen vor allem die übrigen, die sogenannten nichttrivialen Nullstellen, eine große Rolle.

Wie wir gerade gesehen haben, liegen die Primzahlen zumindest in einem gewissen Sinne dichter als die Quadratzahlen. Zur Einstimmung auf das Problem der Primzahlverteilung wollen wir uns kurz mit der (deutlich einfacheren) Verteilung der Quadratzahlen beschäftigen.

Die Folge der Abstände zwischen zwei aufeinanderfolgenden Quadratzahlen ist einfach die Folge der ungeraden Zahlen, denn

$$(n+1)^2 - n^2 = 2n + 1\,.$$

Zwei aufeinanderfolgende Quadratzahlen $Q < Q'$ haben daher die Differenz $Q' - Q = 2\sqrt{Q} + 1$.

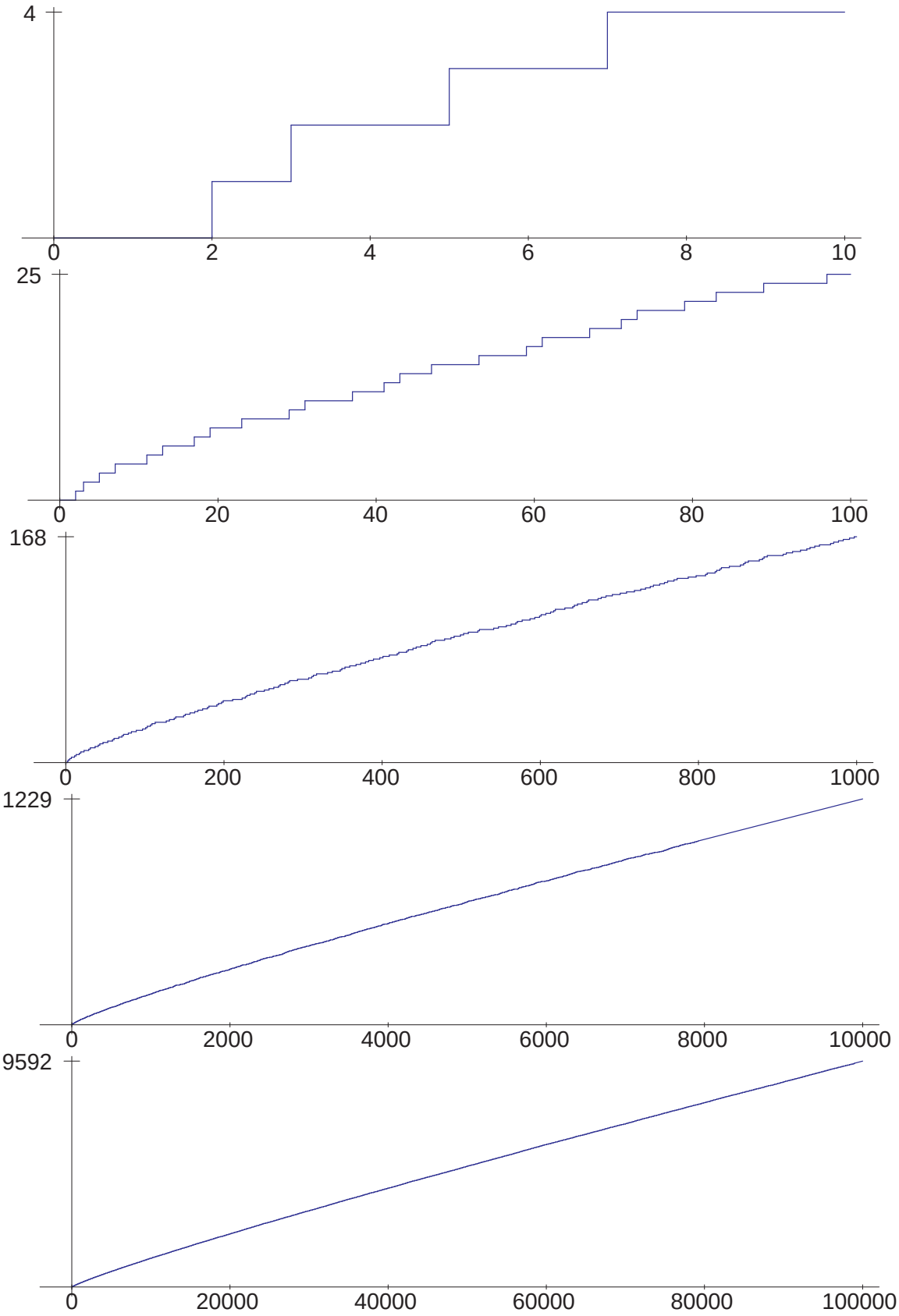
Bei den Primzahlen ist die Situation leider sehr viel unübersichtlicher: EULER meinte sogar, die Verteilung der Primzahlen sei ein Geheimnis, das der menschliche Verstand nie erfassen werde. Der kleinstmögliche Abstand zwischen zwei verschiedenen Primzahlen ist offensichtlich eins, der Abstand zwischen zwei und drei. Er kommt nur an dieser einen Stelle vor, denn außer der Zwei sind schließlich alle Primzahlen ungerade.

Der Abstand zwei ist schon deutlich häufiger: Zwei ist beispielsweise der Abstand zwischen drei und fünf, aber auch der zwischen den Primzahlen $10^{100} + 35737$ und $10^{100} + 35739$. Seit langer Zeit wird vermutet, daß es unendlich viele solcher *Primzahlzwillinge* gibt; experimentelle Untersuchungen deuten sogar darauf hin, daß ihre Dichte für Zahlen der Größenordnung n bei ungefähr $1 : (\log n)^2$ liegen sollte, aber bislang konnte noch niemand auch nur beweisen, daß es unendlich viele gibt.

Eine obere Grenze für den Abstand zwischen zwei aufeinanderfolgenden Primzahlen gibt es genauso wenig wie bei den Quadratzahlen: Ist $n \geq 2$ und $2 \leq i \leq n$, so ist die Zahl $n! + i$ durch i teilbar und somit keine Primzahl. Der Abstand zwischen der größten Primzahl kleiner oder gleich $n! + 1$ und ihrem Nachfolger ist somit mindestens n.

Um einen ersten Eindruck von der Verteilung der Primzahlen zu bekommen, betrachten wir den Graphen der Funktion

$$\pi\colon \begin{cases} \mathbb{R}_{>0} \to \mathbb{N}_0 \\ \quad x \mapsto \text{Anzahl der Primzahlen} \leq x \end{cases}.$$


4
0
2
4
6
8
10
25
0
20
40
60
80
100
168
0
200
400
600
800
1000
1229
0
2000
4000
6000
8000
10000
9592
0
20000
40000
60000
80000
100000

Die Abbildungen auf der vorigen Seite zeigen ihn für die Intervalle von null bis 10^i für $i = 1, \ldots, 5$. Wie man sieht, werden die Graphen immer glatter, und bei den beiden letzten Bilder könnte man glauben, es handle sich um den Graphen einer differenzierbaren Funktion; daher auch die Schreibweise $\pi(x)$ statt – wie bisher – $\pi(N)$.

Auf den ersten Blick sieht diese Funktion fast linear aus.; sieht man sich allerdings die Zahlenwerte genauer an, so sieht man schnell, daß $\pi(x)$ etwas langsamer wächst als eine lineare Funktion; die Funktion $x/\log x$ ist eine deutlich bessere Approximation. In der Tat können wir auch mit unseren sehr elementaren Mitteln eine entsprechende Aussage beweisen:

Satz: Es gibt Konstanten $c_1, c_2 > 0$, so daß gilt:

$$c_1 \frac{x}{\log x} < \pi(x) < c_2 \frac{x}{\log x} .$$

Beweis: Wir betrachten die neue Funktion

$$\vartheta(x) = \sum_{p \le x} \log p ,$$

wobei ein Summationsindex p hier wie stets in diesem Beweis bedeuten soll, daß wir über alle *Primzahlen* mit der jeweils angegebenen Eigenschaft summieren.

Dann ist einerseits

$$\pi(x) = \sum_{p \le x} \frac{\log p}{\log p} \ge \sum_{p \le x} \frac{\log p}{\log x} = \frac{\vartheta(x)}{\log x} ,$$

andererseits ist

$$\begin{aligned} \vartheta(x) = \sum_{p \le x} \log p &\ge \sum_{\sqrt{x} < p \le x} \log p > \log\left(\sqrt{x}\right)\left(\pi(x) - \pi\left(\sqrt{x}\right)\right) \\ &= \frac{1}{2} \log(x)\left(\pi(x) - \pi\left(\sqrt{x}\right)\right) \end{aligned}$$

und damit auch $\pi(x) < \dfrac{2\vartheta(x)}{\log x} + \pi\left(\sqrt{x}\right) < \dfrac{2\vartheta(x)}{\log x} + \sqrt{x}$. Wenn wir also zeigen können

1. Es gibt Konstanten $c_1, c_3 > 0$, so daß $c_1 x < \vartheta(x) < c_3 x$
2. $\displaystyle\sum_{p \le x} \frac{\log p}{p} = \log x + O(1)$,

dann folgt die Behauptung des Satzes.

Zum Beweis der ersten Aussage betrachten wir die Primzerlegung

$$n! = \prod_{p \le n} p^{e_p}$$

von $n!$. Unter den natürlichen Zahlen bis n sind $\left[\frac{n}{p}\right]$ durch p teilbar, $\left[\frac{n}{p^2}\right]$ durch p^2, *usw.;* daher ist

$$e_p = \sum_{k \ge 1} \left[\frac{n}{p^k}\right] \quad \text{und} \quad \log n! = \sum_{p \le n} e_p \log p = \sum_{p \le n} \sum_{k \ge 1} \left[\frac{n}{p^k}\right] \log p\,.$$

Die Summanden mit $k > 1$ liefern dabei nur einen kleinen Beitrag:

$$\sum_{p \le n} \sum_{k \ge 2} \left[\frac{n}{p^k}\right] \log p \le \sum_{p \le n} \left(\log p \cdot \sum_{k \ge 2} \frac{n}{p^k} \right) = n \sum_{p \le n} \frac{\log p}{p(p-1)}$$

nach der Summenformel für die geometrische Reihe:

$$\sum_{k \ge 2} \frac{1}{p^k} = \frac{1}{p^2} \cdot \frac{1}{1 - \frac{1}{p}} = \frac{1}{p^2 - p} = \frac{1}{p(p-1)}\,.$$

Zur weiteren Abschätzung ersetzen wir die Summe über alle Primzahlen kleiner oder gleich n durch die Summe über alle Zahlen bis n und beachten, daß für reellen $x \ge 2$ gilt $\log x < \sqrt{x}$, also

$$\frac{\log x}{x(x-1)} < \frac{\sqrt{x}}{x^2} = \frac{1}{x^{3/2}}:$$

$$\sum_{p \le n} \frac{\log p}{p(p-1)} \le \sum_{i=2}^{n} \frac{\log i}{i(i-1)} \le \sum_{i=2}^{n} \frac{1}{i^{3/2}}\,.$$

Da $\sum_{i=1}^{\infty} \frac{1}{i^s}$ für alle $s > 1$ konvergiert, konvergiert die rechts stehende Summe für $n \to \infty$ gegen einen endlichen Wert (ungefähr 1,612375), ist also $O(1)$, und damit ist $\sum_{k \ge 2} \frac{1}{p^k} = O(n)$. Setzen wir dies in die

Formel für $\log n!$ ein, erhalten wir nach allen bislang bewiesenen Abschätzungen, daß

$$\log n! = \sum_{p\le n} \left[\frac{n}{p}\right] \log p + O(n)\,.$$

Dies können wir vergleichen mit der STIRLINGschen Formel

$$\log n! = n\log n - n + O(\log n)\,,$$

deren Beweis für Leser, die ihn noch nicht kennen, im Anhang zu diesem Paragraphen skizziert ist. Kombinieren wir dies mit der gerade bewiesenen Formel, ist also

$$\sum_{p\le n} \left[\frac{n}{p}\right] \log p = n\log n + O(n)\,. \qquad (*)$$

Damit ist

$$\begin{aligned}\sum_{p\le 2n} \left(\left[\frac{2n}{p}\right] - 2\left[\frac{n}{p}\right]\right) \log p &= 2n\log 2n - 2n\log n + O(2n)\\ &= 2n\log 2 + O(n) = O(n)\,.\end{aligned}$$

Hier ist $\left[\frac{2n}{p}\right] - 2\left[\frac{n}{p}\right]$ stets entweder null oder eins; speziell für die Primzahlen p mit $n < p < 2n$ ist $\left[\frac{n}{p}\right] = 0$ und $\left[\frac{2n}{p}\right] = 1$. Somit ist

$$\vartheta(2n) - \vartheta(n) = \sum_{n<p<2n} \log p \le \sum_{p\le 2n} \left(\left[\frac{2n}{p}\right] - 2\left[\frac{n}{p}\right]\right) \log p = O(n)\,.$$

Die Formel $\vartheta(2n) - \vartheta(n) = O(n)$ bleibt gültig, wenn wir n durch eine reelle Zahl x ersetzen; somit ist

$$\vartheta(x) = \sum_{i=0}^{\infty} \left(\vartheta\left(\frac{x}{2^i}\right) - \vartheta\left(\frac{x}{2^{i+1}}\right)\right) = O\left(\sum_{i=0}^{\infty} \frac{x}{2^i}\right) = O(x)\,,$$

womit die obere Schranke für $\vartheta(x)$ bewiesen wäre.

Bevor wir uns der unteren Schranke zuwenden, beweisen wir zunächst die zweite Aussage. Natürlich ist $\frac{n}{p} = \left[\frac{n}{p}\right] + O(1)$, also ist nach $(*)$

$$\begin{aligned}\sum_{p\le n} \frac{n}{p} \log p &= \sum_{p\le n} \left[\frac{n}{p}\right] \log p + O\left(\sum_{p\le n} \log p\right)\\ &= n\log n + O(n) + O\big(\vartheta(n)\big) = n\log n + O(n)\,,\end{aligned}$$

denn wie wir gerade gesehen haben ist $\vartheta(n) = O(n)$. Kürzen wir die obige Formel durch n, erhalten wir die gewünschte Aussage

$$\sum_{p\le n} \frac{\log p}{p} = \log n + O(1)\,,$$

die natürlich auch dann gilt, wenn wir n durch eine reelle Zahl x ersetzen: Der Term $O(1)$ schluckt alle dabei auftretenden zusätzlichen Fehler.

Für $0 < \alpha < 1$ ist daher

$$\sum_{\alpha x<p\le x} \frac{\log p}{p} = \log x - \log \alpha x + O(1) = \log \frac{1}{\alpha} + O(1)\,,$$

wobei der Fehlerterm $O(1)$ nicht von α abhängt.

Da $\log \frac{1}{\alpha}$ für $\alpha \to 0$ gegen ∞ geht, ist für hinreichend kleine Werte von α und $x > c/\alpha$ für irgendein $c > 2$ beispielsweise

$$\sum_{\alpha x<p\le x} \frac{\log p}{p} > 10\,,$$

und für solche Werte von α und c ist dann

$$10 < \sum_{\alpha x<p\le x} \frac{\log p}{p} < \frac{1}{\alpha x} \sum_{\alpha x<p\le x} \log p \le \frac{\vartheta(x)}{\alpha x}\,.$$

Somit ist $10\alpha x < \vartheta(x)$, womit auch die untere Schranke aus der ersten Behauptung bewiesen wäre und damit der gesamte Satz. ∎

Der bewiesene Satz ist nur ein schwacher Abglanz dessen, was über die Funktion $\pi(x)$ bekannt ist. Zum Abschluß des Kapitels seien kurz einige der wichtigsten bekannten und vermuteten Eigenschaften von $\pi(x)$ zusammengestellt. Diese knappe Übersicht folgt im wesentlichen dem Artikel *Primzahlsatz* aus

> DAVID WELLS: Prime Numbers – The Most Mysterious Figures in Math, *Wiley,* 2005,

einer Zusammenstellung im Lexikonformat von interessanten Tatsachen und auch bloßen Kuriosa aus dem Umkreis der Primzahlen.

GAUSS kam 1792, im Alter von 15 Jahren also, durch seine Experimente zur Vermutung, daß $\pi(x)$ ungefähr gleich dem sogenannten *Integrallogarithmus* von x sein sollte:

$$\pi(x) \approx \mathrm{Li}(x) \underset{\text{def}}{=} \int_2^x \frac{d\xi}{\log \xi} \,.$$

Auch LEGENDRE versuchte, $\pi(x)$ anhand experimenteller Daten anzunähern. Er stellte dazu eine Liste aller Primzahlen bis 400 000 zusammen, das sind immerhin 33 860 Stück, und suchte eine glatte Kurve, die den Graphen von π möglichst gut annähert. In seinem 1798 erschienenen Buch *Essai sur la théorie des nombres* gab er sein Ergebnis an als

$$\pi(x) \approx \frac{x}{\log x - 1{,}08366} \,.$$

Über ein halbes Jahrhundert später gab es den ersten Beweis einer Aussage: PAFNUTIJ L'VOVIČ ČEBYŠĒV (1821–1894), in der Numerik meist bekannt in der Schreibweise Tschebytscheff, zeigte 1851: *Falls*

$$\lim_{x\to\infty} \frac{\pi(x)}{x/\log x}$$

existiert, dann muß er den Wert eins haben.

1852 bewies er dann ein deutlich schärferes Resultat: Für *hinreichend große* Werte von x ist

$$c_1 \cdot \frac{x}{\log x} < \pi(x) < c_2 \cdot \frac{x}{\log x} \quad \text{mit} \quad c_1 \approx 0{,}92 \;\text{ und }\; c_2 \approx 1{,}105 \,.$$

1896 schließlich zeigten der französische Mathematiker JACQUES SALOMON HADAMARD (1865–1963) und sein belgischer Kollege CHARLES JEAN GUSTAVE NICOLAS BARON DE LA VALLÉE POUSSIN (1866–1962) unabhängig voneinander die Aussage, die heute als **Primzahlsatz** bekannt ist:

$$\pi(x) \sim \frac{x}{\log x} \,.$$

Dies bedeutet nun freilich nicht, daß damit die Formeln von GAUSS und von LEGENDRE überflüssig wären: Die Tatsache, daß der Quotient zweier

Funktionen asymptotisch gleich eins ist, erlaubt schließlich immer noch beträchtliche Unterschiede zwischen den beiden Funktionen: Nur der *relative* Fehler muß gegen null gehen.

Offensichtlich ist für jedes $a \in \mathbb{R}$

$$\lim_{x\to\infty} \frac{x/\log x}{x/(\log x - a)} = \lim_{x\to\infty} \frac{\log x - a}{\log x} = 1 - \lim_{x\to\infty} \frac{a}{\log x} = 1\,,$$

und es ist auch nicht schwer zu zeigen, daß

$$\lim_{x\to\infty} \frac{x/\log x}{\mathrm{Li}(x)} = 1$$

ist. Nach dem Primzahlsatz ist daher auch für jedes $a \in \mathbb{R}$

$$\pi(x) \sim \frac{x}{\log x - a} \quad \text{und} \quad \pi(x) \sim \mathrm{Li}(x)\,.$$

Wie DE LA VALLÉE POUSSIN zeigte, liefert der Wert $a = 1$ unter allen reellen Zahlen a die beste Approximation an $\pi(x)$, aber $\mathrm{Li}(x)$ liefert eine noch bessere Approximation. Für kleine Werte von x sieht man das auch in der folgenden Tabelle, in der alle reellen Zahlen zur nächsten ganzen Zahl gerundet sind. Wie kaum anders zu erwarten, liefert LEGENDRES Formel für 10^4 und 10^5 die besten Werte:

n	$\pi(n)$	$\frac{n}{\log n}$	$\frac{n}{\log n-1}$	$\frac{n}{\log n-1{,}08366}$	$\mathrm{Li}(n)$
10^3	168	145	169	172	178
10^4	1 229	1 086	1 218	1 231	1 246
10^5	9 592	8 686	9 512	9 588	9 630
10^6	78 489	72 382	78 030	78 534	78 628
10^7	664 579	620 420	661 459	665 138	664 918
10^8	5 761 455	5 428 681	5 740 304	5 769 341	5 762 209
10^9	50 847 478	48 254 942	50 701 542	50 917 519	50 849 235

Wenn wir genaue Aussagen über $\pi(x)$ machen wollen, sollten wir also etwas über die Differenz $\mathrm{Li}(x) - \pi(x)$ wissen. Hier kommen wir in das Reich der offenen Fragen, und nach derzeitigem Verständnis hängt alles ab von der oben erwähnten RIEMANNschen Zetafunktion. Nach einer berühmten Vermutung von RIEMANN haben alle nichttrivialen Nullstellen von $\zeta(s)$ den Realteil ein halb. Falls dies stimmt, ist

$$\pi(x) = \mathrm{Li}(x) + O(\sqrt{x}\log x)\,.$$

Die RIEMANNsche Vermutung ist eines der wichtigsten ungelösten Probleme der heutigen Mathematik; sie war 1900 eines der HILBERTschen Probleme und ist auch eines der sieben *Millennium problems,* für deren Lösung das CLAY Mathematics Institute in Cambridge, Mass. 2000 einen Preis von jeweils einer Million Dollar ausgesetzt hat; für Einzelheiten siehe `http://www.claymath.org/millennium/` .

Anhang: Die Eulersche Summenformel und die Stirlingsche Formel

Die EULERsche Summenformel erlaubt es, eine endliche Summe auf ein Integral zurückzuführen und dadurch in vielen Fällen erst rechnerisch handhabbar zu machen. Wir betrachten eine reellwertige differenzierbare Funktion f, deren Definitionsbereich das Intervall $[1,\, n]$ enthält.

Für eine reelle Zahl x bezeichnen wir weiterhin mit $[x]$ die größte ganze Zahl kleiner oder gleich x; außerdem führen wir noch die Bezeichnung $\{x\} \underset{\text{def}}{=} x - [x]$ ein für den gebrochenen Anteil von x. Für eine ganze Zahl k ist somit $\{x\} = x - k$ für alle x aus dem Intervall $[k,\, k+1)$.

Partielle Integration führt auf die Gleichung

$$\int_k^{k+1} \left(\{x\} - \tfrac{1}{2}\right) f'(x)\,dx = \left(x - k - \tfrac{1}{2}\right) f(x) \Big|_k^{k+1} - \int_k^{k+1} f(x)\,dx$$

$$= \frac{f(k+1) + f(k)}{2} - \int_k^{k+1} f(x)\,dx\,.$$

Addition aller solcher Gleichungen von $k = 1$ bis $k = n - 1$ liefert

$$\int_1^n \left(\{x\} - \tfrac{1}{2}\right) f'(x)\,dx = \frac{f(1)}{2} + \sum_{k=2}^{n-1} f(k) + \frac{f(n)}{2} - \int_1^n f(x)\,dx\,,$$

womit man die Summe der $f(k)$ berechnen kann:

Satz (EULERsche Summenformel): Für eine differenzierbare Funktion $f\colon D \to \mathbb{R}$, deren Definitionsbereich das Intervall $[1,\, n]$ umfaßt,

ist

$$\sum_{k=1}^{n} f(k) = \int_1^n f(x)\,dx + \frac{f(1)+f(n)}{2} + \int_1^n \left(\{x\} - \tfrac{1}{2}\right) f'(x)\,dx\,.$$

■

Für die Abschätzung von $n!$ interessiert uns speziell der Fall, daß $f(x) = \log x$ der natürliche Logarithmus ist; hier wird die EULERsche Summenformel zu

$$\begin{aligned}\log n! &= \int_1^n \log x\,dx + \frac{\log n}{2} + \int_1^n \frac{\{x\} - \frac{1}{2}}{x}\,dx \\ &= x(\log x - 1)\Big|_1^n + \frac{\log n}{2} + \int_1^n \frac{\{x\} - \frac{1}{2}}{x}\,dx \\ &= n(\log n - 1) + 1 + \frac{\log n}{2} + \int_1^n \frac{\{x\} - \frac{1}{2}}{x}\,dx\,.\end{aligned}$$

In dieser Formel stört noch das rechte Integral; dieses können wir wie folgt abschätzen: Für eine natürliche Zahl k ist

$$\int_k^{k+1} \frac{\{x\} - \frac{1}{2}}{x}\,dx = \int_{-\frac{1}{2}}^{\frac{1}{2}} \frac{x}{k + \frac{1}{2} + x}\,dx$$

$$= \int_0^{\frac{1}{2}} \left(\frac{x}{k + \frac{1}{2} + x} - \frac{x}{k + \frac{1}{2} - x} \right) dx = \int_0^{\frac{1}{2}} \frac{-2x^2}{\left(k + \frac{1}{2}\right)^2 - x^2}\,dx\,.$$

Im Intervall von 0 bis $\frac{1}{2}$ ist der Integrand monoton fallend, d.h.

$$0 \geq \frac{-2x^2}{\left(k + \frac{1}{2}\right)^2 - x^2} \geq \frac{-\frac{1}{2}}{\left(k + \frac{1}{2}\right)^2 - \frac{1}{4}} = \frac{-2}{(2k+1)^2 - 1} \geq -\frac{1}{2k^2}\,,$$

und damit ist

$$0 \geq \int_k^{k+1} \frac{\{x\} - \frac{1}{2}}{x}\, dx = \int_0^{\frac{1}{2}} \frac{-2x^2}{\left(k + \frac{1}{2}\right)^2 - x^2}\, dx \geq -\frac{1}{4k^2}\,,$$

denn wir können das Integral abschätzen durch das Produkt aus der Länge des Integrationsintervalls und dem Minimum des Integranden. Summation von $k = 1$ bis $n - 1$ schließlich gibt die Abschätzung

$$0 \geq \int_1^n \frac{\{x\} - \frac{1}{2}}{x}\, dx \geq -\sum_{k=1}^{n-1} \frac{1}{4k^2} > -\frac{1}{4} \sum_{k=1}^{\infty} \frac{1}{k^2}$$

für das störende Integral aus der obigen Formel. Da die Summe rechts konvergiert, konvergiert auch das Integral für $n \to \infty$ gegen einen Grenzwert I. Somit ist

$$\log n! = n(\log n - 1) + \frac{\log n}{2} + I + 1 + o(1)\,,$$

also folgt insbesondere die Abschätzung

$$\log n! = n \log n + O(n)\,,$$

die wir im Beweis des Satzes über $\pi(n)$ verwendet haben.

§2: Das Sieb des Eratosthenes

Das klassische Verfahren zur Bestimmung aller Primzahlen unterhalb einer bestimmten Schranke geht zurück auf ERATOSTHENES im dritten vorchristlichen Jahrhundert. Es funktioniert folgendermaßen:

Um alle Primzahlen kleiner oder gleich einer Zahl N zu finden, schreibe man zunächst die Zahlen von eins bis N in eine Reihe.

Eins ist nach Definition keine Primzahl – für griechische Mathematiker wie EUKLID war die Eins nicht einmal eine Zahl. Also streichen wir die Eins durch. Die Zwei ist prim, aber ihre echten Vielfachen sind natürlich keine Primzahlen, werden also durchgestrichen. Dazu müssen wir nicht von jeder Zahl nachprüfen, ob sie durch zwei teilbar ist, sondern wir streichen einfach nach der Zwei jede zweite Zahl aus der Liste durch.

Die erste nichtdurchgestrichene Zahl der Liste ist dann die Drei. Sie muß eine Primzahl sein, denn hätte sie einen von eins verschiedenen kleineren Teiler, könnte das nur die Zwei sein, und alle Vielfachen von zwei (außer der Zwei selbst) sind bereits durchgestrichen.

Auch die echten Vielfachen der Drei sind keine Primzahlen, werden also durchgestrichen. Auch dazu streichen wir wieder einfach jede dritte Zahl aus der Liste durch, unabhängig davon, ob sie bereits durchgestrichen ist oder nicht. (Alle durch sechs teilbaren Zahlen sind offensichtlich schon durchgestrichen.)

Genauso geht es weiter mit der Fünf *usw.;* nach jedem Durchgang durch die Liste muß offenbar die erste noch nicht durchgestrichene Zahl eine Primzahl sein, denn alle Vielfache von kleineren Primzahlen sind bereits durchgestrichen, und wenn eine Zahl überhaupt einen echten Teiler hat, dann ist sie natürlich auch durch eine echt kleinere Primzahl teilbar.

Wie lange müssen wir dieses Verfahren durchführen? Wenn eine Zahl x Produkt zweier echt kleinerer Faktoren u, v ist, können u und v nicht beide größer sein als $\sqrt{x}$: Sonst wäre schließlich $x = uv$ größer als x. Also ist einer der beiden Teiler u, v kleiner oder gleich $\sqrt{x}$, so daß x mindestens einen Teiler hat, dessen Quadrat kleiner oder gleich x ist. Damit ist eine zusammengesetzte Zahl x durch mindestens eine Primzahl p teilbar mit $p^2 \leq x$.

ERATOSTHENES (Ερατοσθένες) wurde 276 v.Chr. in Cyrene im heutigen Libyen geboren, wo er zunächst von Schülern des Stoikers ZENO ausgebildet wurde. Danach studierte er noch einige Jahre in Athen, bis ihn 245 der Pharao PTOLEMAIOS III als Tutor seines Sohns nach Alexandrien holte. 240 wurde er dort Bibliothekar der berühmten Bibliothek im Museion.
Heute ist er außer durch sein Sieb vor allem durch seine Bestimmung des Erdumfangs bekannt. Er berechnete aber auch die Abstände der Erde von Sonne und Mond und entwickelte einen Kalender, der Schaltjahre enthielt. 194 starb er in Alexandrien, nach einigen Überlieferungen, indem er sich, nachdem er blind geworden war, zu Tode hungerte.

Für das Sieb des ERATOSTHENES, angewandt auf die Zahlen von eins

bis N heißt das, daß wir aufhören können, sobald die erste nicht-durchgestrichene Zahl p ein Quadrat $p^2 > N$ hat; dann können wir sicher sein, daß jede zusammengesetzte Zahl $x \leq N$ bereits einen kleineren Primteiler als p hat und somit bereits durchgestrichen ist. Die noch nicht durchgestrichenen Zahlen in der Liste sind also Primzahlen.

Damit lassen sich leicht von Hand alle Primzahlen bis hundert finden, mit etwas Fleiß auch die bis Tausend, aber sicher nicht die hundertstelligen.

Trotzdem kann uns ERATOSTHENES helfen, zumindest zu zeigen, daß gewissen Zahlen nicht prim sind: Wenn wir Primzahlen in einem Intervall $[a,\ b]$ suchen, d.h. also Primzahlen p mit

$$a \leq p \leq b\,,$$

so können wir ERATOSTHENES auf dieses Intervall fast genauso anwenden wie gerade eben auf das Intervall $[1,\ N]$:

Wir gehen aus von einer Liste $p_1, \ldots, p_r$ der ersten Primzahlen; dabei wählen wir r so, daß die Chancen auf nicht durch p_r teilbare Zahlen im Intervall $[a,\ b]$ noch einigermaßen realistisch sind, d.h. wir gehen bis zu einer Primzahl p_r, die ungefähr in der Größenordnung der Intervallänge $b - a$ liegt.

Nun können wir mit jeder der Primzahlen p_i sieben wie im klassischen Fall; wir müssen nur wissen, wo wir anfangen sollen.

Dazu berechnen wir für jedes p_i den Divisionsrest $r_i = a \bmod p_i$. Dann ist $a - r_i$ durch p_i teilbar, liegt allerdings nicht im Intervall $[a,\ b]$. Die erste Zahl, die wir streichen müssen, ist also $a - r_i + p_i$, und von da an streichen wir einfach, ohne noch einmal dividieren zu müssen, wie gehabt jede p_i-te Zahl durch.

Was nach r Durchgängen noch übrig bleibt, sind genau die Zahlen aus $[a,\ b]$, die durch keine der Primzahlen p_i teilbar sind. Sie können zwar noch größere Primteiler haben, aber wichtig ist, daß wir mit minimalem Aufwand für den Großteil aller Zahlen aus $[a,\ b]$ gesehen haben, daß sie keine Primzahlen sind. Für den Rest brauchen wir andere Verfahren, aber die sind allesamt erheblich aufwendiger als ERATOSTHENES, so daß sich diese erste Reduktion auf jeden Fall lohnt.

§3: Fermat-Test und Fermat-Zahlen

Nach dem kleinen Satz von FERMAT gilt für jede Primzahl p und jede nicht durch p teilbare Zahl a die Formel $a^{p-1} \equiv 1 \bmod p$. Im Umkehrschluß folgt sofort:

Falls für eine natürliche Zahl $1 \le a \le p-1$ *gilt* $a^{p-1} \not\equiv 1 \bmod p$, *kann* p *keine Primzahl sein.*

Beispiel: Ist $p = 129$ eine Primzahl? Falls ja, ist nach dem kleinen Satz von FERMAT $2^{128} \equiv 1 \bmod 129$. Tatsächlich ist aber

$$2^7 = 128 \equiv -1 \bmod 129\,,$$

also hat die Zwei in $(\mathbb{Z}/129)^\times$ die Ordnung 14. Da 14 kein Teiler von 128 ist, kann $2^{128} \bmod 129$ nicht eins sein. (Wegen $128 \equiv 2 \bmod 14$ ist $2^{128} \equiv 2^2 = 4 \bmod 129$.) Somit ist 129 keine Primzahl.

Dieses Ergebnis hätten wir natürlich auch durch Probedivisionen leicht gefunden: Da 129 die Quersumme 12 hat, ist die Zahl durch drei teilbar; ihre Primzerlegung ist $129 = 3 \cdot 43$.

Keine Kopfrechenaufgabe ist die Frage, ob $F_{20} = 2^{2^{20}} + 1$ eine Primzahl ist. Falls ja, wäre nach dem kleinen Satz von FERMAT insbesondere

$$3^{F_{20}-1} = 1 \bmod F_{20}, \quad \text{also} \quad 3^{(F_{20}-1)/2} \equiv \pm 1 \bmod F_{20}\,.$$

Nachrechnen zeigt, daß dies nicht der Fall ist, allerdings ist das „Nachrechnen“ bei dieser 315 653-stelligen Zahl natürlich keine Übungsaufgabe für Taschenrechner: 1988 brauchte eine Cray X-MP dazu 82 Stunden, der damals schnellste Supercomputer Cray-2 immerhin noch zehn; siehe

JEFF YOUNG, DUNCAN A. BUELL: The Twentieth Fermat Number is Composite, *Math. Comp.* **50** (1988), 261–263.

Damit war gezeigt, daß F_{20} keine Primzahl ist. (Die anscheinend etwas weltabgewandt lebenden Autoren meinten, dies sei die aufwendigste bis dahin produzierte 1-Bit-Information.)

Umgekehrt können wir leider nicht folgern, daß p eine Primzahl ist, wenn für ein $a \in \mathbb{N}$ mit $1 < a < p-1$ gilt $a^{p-1} \equiv 1 \bmod p$. So ist

beispielsweise $18^{322} \equiv 1 \bmod 323$, aber $323 = 17 \cdot 19$ ist zusammengesetzt. Immerhin gibt es nicht viele $a \leq 323$ mit $a^{322} \equiv 1 \bmod 323$: Die einzigen Möglichkeiten sind $a = \pm 1$ und $a = \pm 18$.

Es kann nicht vorkommen, daß für eine zusammengesetzte Zahl n und alle $1 \leq a \leq n$ gilt $a^{n-1} \equiv 1 \bmod n$, denn ist p ein Primteiler von n, so ist für jedes Vielfache a von p natürlich auch a^{n-1} durch p teilbar, kann also nicht kongruent eins modulo des Vielfachen n von p sein. Zumindest für die a mit ggT$(a, n) > 1$ kann die Gleichung also nicht erfüllt sein.

Bei großen Zahlen n mit nur wenigen Primfaktoren ist die Chance, ein solches a zu erwischen, recht klein; wenn dies die einzigen Gegenbeispiele sind, wird uns der FERMAT-Test also fast immer in die Irre führen.

Definition: Eine natürliche Zahl n heißt CARMICHAEL-Zahl, wenn sie keine Primzahl ist, aber trotzdem für jede natürliche Zahl a mit ggT$(a, n) = 1$ gilt: $a^{n-1} \equiv 1 \bmod n$.

ROBERT DANIEL CARMICHAEL (1879–1967) war ein amerikanischer Mathematiker, der unter anderem Bücher über die Relativitätstheorie, über Zahlentheorie, über Analysis und über Gruppentheorie veröffentlichte. Ab 1915 lehrte er an der University of Illinois. Er zeigte 1910, daß 561 die gerade definierte Eigenschaft hat und publizierte auch später noch eine Reihe von Arbeiten über solche Zahlen.

Satz: Eine natürliche Zahl n ist genau dann eine CARMICHAEL-Zahl, wenn sie das Produkt von mindestens drei paarweise verschiedenen ungeraden Primzahlen ist, wobei für jeden Primfaktor p auch $p - 1$ Teiler von $n - 1$ ist.

Beweis: Sei zunächst $n = \prod p_i$ ein Produkt paarweise verschiedener Primzahlen, für die $p_i - 1$ Teiler von $n - 1$ ist. Nach dem chinesischen Restesatz ist dann $(\mathbb{Z}/N)^\times \cong \prod (\mathbb{Z}/p_i)^\times$. In der Gruppe $(\mathbb{Z}/p_i)^\times$ ist die Ordnung eines jeden Elements ein Teiler von $p_i - 1$ und damit von $n - 1$; also ist auch in $(\mathbb{Z}/n)^\times$ die Ordnung eines jeden Elements Teiler von $n - 1$. Damit gilt für jedes zu n teilerfremde $a \in \mathbb{Z}$ die Kongruenz $a^{n-1} \equiv 1 \bmod n$, d.h. n ist eine CARMICHAEL-Zahl.

Umgekehrt sei n eine CARMICHAEL-Zahl. Dann ist n ungerade, denn für gerade Zahlen n ist $(n-1)^{n-1} \equiv (-1)^{n-1} = -1 \bmod n$.

Als nächstes wollen wir uns überlegen, daß n Produkt verschiedener Primzahlen sein muß: Angenommen, in der Primzerlegung von n tritt eine Primzahl p mehrfach auf, d.h. $n = p^e q$ mit einer zu p teilerfremden Zahl q. Nach dem binomischen Lehrsatz gilt

$$(p+1)^{p^{e-1}} = \sum_{k=0}^{p^{e-1}} \binom{p^{e-1}}{k} p^k \,,$$

und für alle $k \neq 0$ ist

$$\begin{aligned}\binom{p^{e-1}}{k} p^k &= \frac{p^{e-1}(p^{e-1}-1)\cdots(p^{e-1}-k+1)}{k!} p^k \\ &= p^{e-1} \cdot \frac{p^{e-1}}{1} \cdot \frac{p^{e-1}-2}{2} \cdots \frac{p^{e-1}-(k-1)}{k-1} \cdot \frac{p^k}{k} \,.\end{aligned}$$

In jedem der Brüche $(p^{e-1}-\ell)/\ell$ kommt p in Zähler und Nenner mit der gleichen Potenz vor, denn $\ell < p^{e-1}$ und $p^{e-1} - \ell \equiv -\ell \bmod p^{e-1}$. Im letzten Bruch p^k/k steht p im Zähler offensichtlich mit einer höheren Potenz als im Nenner; insgesamt ist der Ausdruck also mindestens durch p^e teilbar. Somit ist $(1+p)^{p^{e-1}} \equiv 1 \bmod p^e$; in $(\mathbb{Z}/p^e)^\times$ gibt es daher Elemente, deren Ordnung ein Vielfaches von p ist. Da nach dem chinesischen Restesatz $(\mathbb{Z}/n)^\times \cong (\mathbb{Z}/p^e)^\times \times (\mathbb{Z}/q)^\times$ ist, gibt es dann auch in $(\mathbb{Z}/n)^\times$ ein solches Element a. Da $n-1$ nicht durch p teilbar ist, ist n kein Vielfaches dieser Ordnung, so daß a^{n-1} modulo n nicht eins sein kann. Damit ist n keine CARMICHAEL-Zahl; eine CARMICHAEL-Zahl muß also Produkt verschiedener Primzahlen sein.

Für jeden Primteiler p von n muß $p-1$ ein Teiler von $n-1$ sein, denn nach dem chinesischen Restesatz ist $(\mathbb{Z}/n)^\times$ das Produkt der Gruppen $(\mathbb{Z}/p)^\times$, es gibt also in $(\mathbb{Z}/n)^\times$ eine primitive Wurzel a modulo p. Da $a^{n-1} \equiv 1 \bmod n$ und damit insbesondere modulo p ist, muß $n-1$ ein Vielfaches der Ordnung $p-1$ von a modulo p sein.

Schließlich müssen wir uns noch überlegen, daß n ein Produkt von mindestens drei Primzahlen ist: Da n nach Definition keine Primzahl

ist, wäre $n = pq$ sonst das Produkt zweier Primzahlen. Wie wir gerade gesehen haben, müßte

$$n - 1 = pq - 1 = (p-1)q + (q-1) = p(q-1) + (p-1)$$

sowohl durch $p-1$ als auch durch $q-1$ teilbar sein, also müßten $p-1$ und $q-1$ durcheinander teilbar sein, d.h. $p = q$, was wir bereits ausgeschlossen haben.

■

Als Beispiel können wir ein Produkt $n = (6t+1)(12t+1)(18t+1)$ mit drei primen Faktoren betrachten, z.B.

$$1729 = 7 \times 13 \times 19 \quad \text{für } t = 1 \quad \text{oder} \quad 294409 = 37 \times 73 \times 109$$

für $t = 6$. Hier ist $n - 1 = 1296t^3 + 396t^2 + 36t = 36t \cdot (36t^2 + 11t + 1)$ offensichtlich durch $6t, 12t$ und $18t$ teilbar, n ist also eine CARMICHAEL-Zahl.

Natürlich muß nicht jede CARMICHAEL-Zahl von dieser Form sein; die kleinste CARMICHAEL-Zahl beispielsweise ist $561 = 3 \cdot 11 \cdot 17$ und hat keinen einzigen Primfaktor kongruent eins modulo sechs.

Eine größte CARMICHAEL-Zahl gibt es nicht, denn nach

W.R. ALFORD, ANDREW GRANVILLE, CARL POMERANCE: There are infinitely many Carmichael numbers, *Ann. Math*, **140** (1994), 703–722

gibt es unendlich viele. Konkret zeigen sie, daß die Anzahl der CARMICHAEL-Zahlen kleiner oder gleich x für große Zahlen x mindestens gleich $x^{2/7}$ ist. Die tatsächliche Anzahl dürfte wohl deutlich größer sein, ist aber immer noch sehr viel kleiner als die der Primzahlen.

Für große Zahlen p wird es zunehmend unwahrscheinlich, daß sie auch nur für ein a den FERMAT-Test bestehen, ohne Primzahl zu sein. Rechnungen von

SU HEE KIM, CARL POMERANCE: The probability that a Random Probable Prime is Composite, *Math. Comp.* **53** (1989), 721–741

geben folgende obere Schranke für die Wahrscheinlichkeit ε, daß eine zufällig gewählte Zahl p der angegebenen Größenordnung den FERMAT-Test mit einem vorgegebenen a besteht und trotzdem keine Primzahl ist:

$p \approx 10^{60}$	10^{70}	10^{80}	10^{90}	10^{100}
$\varepsilon \leq 7{,}16 \cdot 10^{-2}$	$2{,}87 \cdot 10^{-3}$	$8{,}46 \cdot 10^{-5}$	$1{,}70 \cdot 10^{-6}$	$2{,}77 \cdot 10^{-8}$
$p \approx 10^{120}$	10^{140}	10^{160}	10^{180}	10^{200}
$\varepsilon \leq 5{,}28 \cdot 10^{-12}$	$1{,}08 \cdot 10^{-15}$	$1{,}81 \cdot 10^{-19}$	$2{,}76 \cdot 10^{-23}$	$3{,}85 \cdot 10^{-27}$
$p \approx 10^{300}$	10^{400}	10^{500}	10^{600}	10^{700}
$\varepsilon \leq 5{,}8 \cdot 10^{-29}$	$5{,}7 \cdot 10^{-42}$	$2{,}3 \cdot 10^{-55}$	$1{,}7 \cdot 10^{-68}$	$1{,}8 \cdot 10^{-82}$
$p \approx 10^{800}$	10^{900}	10^{1000}	10^{2000}	10^{3000}
$\varepsilon \leq 5{,}4 \cdot 10^{-96}$	$1{,}0 \cdot 10^{-109}$	$1{,}2 \cdot 10^{-123}$	$8{,}6 \cdot 10^{-262}$	$3{,}8 \cdot 10^{-397}$

(Sie geben natürlich auch eine allgemeine Formel an, jedoch ist diese zu grausam zum Abtippen.)

Wenn wir RSA-Moduln von 2048 Bit konstruieren wollen, brauchen wir etwa dreihundertstellige Primzahlen; hier liegt die Irrtumswahrscheinlichkeit bei einem einzigen FERMAT-Test also bei höchstens $5{,}8 \cdot 10^{-29}$. Wenn das zu hoch ist, kann man mit mehreren zufällig gewählten Basen testen und dadurch dir Fehlerwahrscheinlichkeit deutlich verringern – auch wenn es wohl gewagt wäre, zwei solche Tests als unabhängig anzunehmen.

Die Bundesnetzagentur empfiehlt, bei probabilistischen Primzahltests für die Erzeugung von RSA-Moduln eine Irrtumswahrscheinlichkeit von höchsten $2^{-100} \approx 7{,}89 \cdot 10^{-31}$ zuzulassen. Da die Wahrscheinlichkeiten in obiger Tabelle obere Schranken sind, könnte das vielleicht schon mit einem Test erreicht sein; besser sind auf jeden Fall mehrere oder, noch besser, ein Test, der wirklich *beweisen* kann, daß eine Zahl prim ist.

Einige Leute reden bei Zahlen, die einen FERMAT-Test bestanden haben, von „wahrscheinlichen Primzahlen“. Das ist natürlich Unsinn: Eine Zahl ist entweder *sicher* prim oder *sicher* zusammengesetzt; für Wahrscheinlichkeiten gibt es hier keinen Spielraum. Besser ist der ebenfalls gelegentlich zu hörende Ausdruck „industrial grade primes“, also „Industrieprimzahlen“, der ausdrücken soll, daß wir zwar nicht *bewiesen* haben, daß die Zahl wirklich prim ist, daß sie aber für (manche) „industrielle Anwendungen“ gut genug ist.

Zumindest grundsätzlich läßt sich der FERMAT-Test auch ausbauen zu

einem echten Primzahltest; die einfachste Art ist die folgende sehr schwache Version eines Satzes von POCKLINGTON:

Satz: Ist für zwei natürliche Zahlen p, a zwar $a^{p-1} \equiv 1 \bmod p$, aber für jeden Primteiler q von $p-1$ gilt $a^{(p-1)/q} \not\equiv 1 \bmod p$, so ist p eine Primzahl.

Beweis: Offensichtlich muß dann die Ordnung von a in $(\mathbb{Z}/p\mathbb{Z})^\times$ gleich $p-1$ sein. Wie wir aus Kapitel 1, §8 wissen, hat $(\mathbb{Z}/p\mathbb{Z})^\times$ die Ordnung $\varphi(p)$, und für jede zusammengesetzte Zahl folgt aus der dort angegebenen Formel leicht, daß $\varphi(p) < p-1$ ist. Also muß p prim sein. ∎

HENRY CABOURN POCKLINGTON (1870–1952) wurde im englischenn Exeter geboren; er studierte an dem College, aus 1904 die University of Leeds wurde. Damals wurden Studenten dort auf Examen in London vorbereitet; POCKLINGTON erhielt 1889 Bachelorgrade sowohl in Experimentalphysik als auch in Mathematik und erhielt anschließend verschiedene Stipendien des St. John's College in Cambdridge, zunächst als Student, dann als *fellow*. 1896 erhielt er den Doktorgrad der Universität London. Als seine Stipendien 1900 ausliefen, wurde er Physiklehrer an einer Schule in Leeds und blieb dies auch bis zu seiner Pensionierung 1926, obwohl er mehrfach Angebote von Universitäten bekam und 1907 sogar *fellow* der *Royal Society* wurde. Zwischen 1895 und 1940 publizierte er rund vierzig Arbeiten, zunächst hauptsächlich aus dem Gebiet der Physik und Astronomie, ab 1910 aber vor allem aus der Mathematik,

Der Nachteil des gerade bewiesenen Satzes ist, daß wir alle Primteiler von $p-1$ kennen müssen; wenn wir Primzahlen mit mehreren hundert Dezimalstellen suchen, ist das meist keine sehr realistische Annahme. Für Zahlen spezieller Bauart kann dieser Test jedoch sehr nützlich sein: Wenn wir von einer Zahl n mit wenigen, uns bekannten Primteilern ausgehen, läßt sich so testen, ob $n+1$ eine Primzahl ist.

Die einfachsten Kandidaten für n sind Primzahlpotenzen $n = p^r$; für eine ungerade Primzahl p ist allerdings $n+1$ gerade und somit keine Primzahl. Auf den Fall $p = 2$ werden wir gleich zurückkommen.

Bei kleinen geraden Zahlen b mit wenigen Primfaktoren gibt es gelegentlich Chancen, daß $b^r + 1$ eine Primzahl ist, allerdings kommt auch das nur selten vor. Ein Beispiel wäre etwa

$$p = 24^4 + 1 = 331\,777\,.$$

Hier hat $p - 1 = 24^4$ nur 2 und 3 als Primteiler, wir müssen also eine Zahl a finden, so daß

$$a^{p-1} \equiv 1 \bmod p, \quad a^{(p-1)/2} \not\equiv 1 \bmod p \quad \text{und} \quad a^{(p-1)/3} \not\equiv 1 \bmod p$$

ist. Dazu berechnen wir am besten zunächst $x = a^{(p-1)/6} \bmod p$, sodann $y = a^{(p-1)/3} \bmod p = x^2 \bmod p$ und $z = a^{(p-1)/2} \bmod p = x^3 \bmod p$. Wenn p eine Primzahl ist, muß offensichtlich $z \equiv -1 \bmod p$ sein, und wenn dies gilt, ist auch $a^{(p-1)} \equiv 1 \bmod p$.

Für $a = 2$ erhalten wir $x = 92553, y = 239223$ und $z = 1$; das beweist nichts. Für $a = 3$ ist sogar bereits $x = 1$, aber für $a = 5$ wird $x = 92554$, $y = 92553$ und $z = 331776 \equiv -1 \bmod p$. Dies *beweist*, daß p eine Primzahl ist.

Als nächstes wollen wir uns überlegen, wann $n = 2^r + 1$ prim sein kann. Für ungerade r ist n durch drei teilbar, denn $2^r \equiv (-1)^r \equiv -1 \bmod 3$; für $r > 1$ kann n dann also nicht prim sein. Auch wenn r nur durch eine ungerade Zahl $u > 1$ teilbar ist, kann $2^r + 1$ nicht prim sein, denn ist $r = uv$, so ist $2^r = (2^v)^u \equiv (-1)^u \equiv -1 \bmod 2^v + 1$, so daß $2^v + 1$ ein nichttrivialer Teiler ist. Die einzigen Kandidaten für Primzahlen sind daher die Zahlen

$$F_n = 2^{2^n} + 1 ,$$

bei denen der Exponent r eine Zweierpotenz ist. Sie heißen FERMAT-Zahlen, weil FERMAT zwischen 1630 und 1640 in mehreren Briefen, unter anderem an PASCAL und an MERSENNE, die Vermutung äußerte, diese Zahlen seien allesamt prim.

Für $F_0 = 3, F_1 = 5, F_2 = 17$ sieht man das mit bloßem Auge und mit auch $F_3 = 257$ gibt es keine nennenswerten Schwierigkeiten. Für größere Werte von n können wir den obigen Test anwenden; da 2 der einzige Primteiler von $F_n - 1$ ist, wird er hier einfach einfach zur folgenden Aussage:

Lemma: F_n ist genau dann eine Primzahl, wenn es ein a gibt mit

$$a^{(F_n-1)/2} \equiv -1 \bmod F_n .$$

■

Für $F_4 = 2^{16} + 1 = 65\,537$ ist $(F_n - 1)/2 = 2^{15}$, wir müssen also ein a finden, so daß $a^{2^{15}} \equiv -1 \bmod F_4$ ist. Für $a = 2$ bekommen wir nach 15 Quadrierungen das nutzlose Ergebnis eins, für $a = 3$ aber die gewünschte -1. Damit ist F_4 als Primzahl erkannt – was auch FERMAT wußte.

Für $F_5 = 2^{32} + 1 = 429\,4967\,297$ müssen wir $a^{2^{31}} \bmod F_5$ berechnen, brauchen also schon 31 Quadrierungen. Für $a = 2$ erhalten wir wieder die nutzlose Eins, für $a = 3$ aber das Ergebnis 10 324 303, das sich offenbar auch modulo F_5 deutlich von ± 1 unterscheidet. Somit ist F_5 *keine* Primzahl und FERMATs obige Vermutung ist widerlegt. Sie ist übrigens die einzige seiner vielen Vermutungen, die sich als falsch erwies.

Der erste, der erkannte, daß F_5 zusammengesetzt ist, war EULER, den GOLDBACH in Sankt Petersburg auf FERMATs Vermutung aufmerksam gemacht hatte. Nachdem EULERs Beweisversuche erfolglos blieben, fand er 1732 schließlich die Faktorisierung $F_5 = 641 \cdot 6\,700\,417$. Obwohl EULER viel rechnete, fand er diese Faktorisierung natürlich nicht durch systematisches Ausprobieren aller Primzahlen bis zur Quadratwurzel von F_5: dafür hätte er im schlimmsten Fall immerhin durch 6542 Primzahlen dividieren müssen!

Stattdessen benutzte EULER den kleinen Satz von FERMAT, um zunächst Aussagen über mögliche Teiler von FERMAT-Zahlen zu bekommen. Er fand

Lemma: Jeder Primteiler p von F_n ist kongruent eins modulo 2^{n+1}.

Beweis: Ist $2^{2^n} \equiv -1 \bmod F_n$, so ist erst recht $2^{2^n} \equiv -1 \bmod p$, also $2^{2^{n+1}} \equiv 1 \bmod p$. Die Ordnung der Zwei in $\mathbb{F}_p^\times$ ist somit ein Teiler von 2^{n+1}, also eine Zweierpotenz. Wäre diese kleiner als 2^{n+1}, wäre sie ein Teiler von 2^n, so daß $2^{2^n} \equiv +1 \bmod p$ sein müßte. Somit ist 2^{n+1} die genaue Ordnung. Diese muß aber nach dem Satz von LAGRANGE ein Teiler der Gruppenordnung sein, d.h. 2^{n+1} teilt $p-1$, was die Behauptung beweist. ∎

Somit wußte EULER, daß jeder Primteiler von F_5 die Form $p = 64k + 1$ haben muß; Primzahlen dieser Form gibt es nur 209 unterhalb von 2^{15},

was das Problem schon viel handhabbarer erscheinen läßt. Dazu kam, daß er Glück hatte: Schon für $k = 10$ bekam er einen Teiler. Nach 193, 257, 449 und 577 ist 641 bereits die fünfte Primzahl dieser Form!

Tatsächlich aber machte er sich trotzdem zuviel Arbeit, denn wie der französische Mathematiker EDOUARD LUCAS (1842–1891) fand, gilt sogar

Lemma: Für $n \geq 3$ ist jeder Primteiler p von F_n kongruent eins modulo 2^{n+2}.

Beweis: Wir gehen genauso vor wie EULER, suchen aber ein Element von $\mathbb{F}_p^\times$, dessen Ordnung 2^{n+2} ist. Ein solches Element haben wir gefunden, wenn wir in $\mathbb{F}_p^\times$ ein x finden mit $x^2 = 2$. Wegen der Beziehung

$$\left(2^{2^{n-1}} + 1\right)^2 = 2^{2^n} + 1 + 2^{2^{n-1}+1} \equiv 2^{2^{n-1}+1} \bmod F_n$$

haben wir zunächst eine Zahl y gefunden mit $y^2 \equiv 2^u \bmod F_n$, wobei $u = 2^{n-1} + 1$ eine ungerade Zahl ist. Mit dem erweiterten EUKLIDischen Algorithmus können wir daher ganze Zahlen v, w finden mit $uv+2w = 1$. Damit ist auch

$$2 = 2^{uv+2w} = (2^u)^v \cdot (2^w)^2 = y^{2v} \cdot 2^{2w} = (y^v \cdot 2^w)^2$$

ein Quadrat in $\mathbb{F}_p^\times$.

∎

Mit dieser Verschärfung seines Lemmas hätte sich EULER auf Primzahlen der Form $128k + 1$ beschränken können und hätte bereits im zweiten Anlauf (nach einem vergeblichen Versuch mit 257) seinen Faktor gefunden.

Auch wenn er nie etwas darüber publiziert hat, hätte er auch beweisen können und bewies vielleicht auch, daß sein Kofaktor $q = 6\,700\,417$ ebenfalls eine Primzahl ist: Da jeder Primteiler p von q insbesondere auch F_5 teilt, muß $p \equiv 1 \bmod 128$ sein, und wenn es einen echten Teiler gibt, gibt es auch einen der kleiner ist als $\sqrt{q} \approx 2588{,}5$. Es gibt nur zwanzig Zahlen der Form $128k + 1$ unterhalb von $\sqrt{q}$, und nur fünf davon sind prim: Neben den bereits bekannten Kandidaten 257 und 641 sind das noch 769, 1153 und 1409. Fünf einfache Divisionen mit Rest

zeigen, daß q durch keine dieser Zahlen teilbar ist; somit haben wir bewiesen, daß auch q prim sein muß.

Die Suche nach FERMAT-Primzahlen sowie nach Faktoren von FERMAT-Zahlen beschäftigt auch heute noch eine ganze Reihe von Mathematikern; die jeweils neuesten Ergebnisse sind zum Beispiel auf den Webseiten von `www.fermatsearch.org` zu finden. Unter anderem ist bewiesen, daß F_n für $5 \leq n \leq 32$ sowie viele andere Werte von n zusammengesetzt ist; oft sind auch zumindest einige Faktoren bekannt. FERMATsche Primzahlen mit $n > 4$ wurden bislang keine gefunden, allerdings ist auch noch nicht bewiesen, daß es unendlich viele FERMAT-Zahlen gibt, die *keine* Primzahlen sind.

Der oben angegebene Beweis von LUCAS zeigt übrigens auch, warum wir beim Primzahltest für F_4 mit der Basis zwei keinen Erfolg hatten: Da 2 modulo F_4 ein Quadrat ist, *muß* die Potenz mit Exponent $(F_4 - 1)/2$ gleich eins sein, denn sie ist schließlich die $(F_4 - 1)$-te Potenz der Wurzel aus 2. Aus diesem Grund wurde bei der Überprüfung von F_{20} nicht mit $a = 2$ gearbeitet, obwohl dies rechnerisch sehr viel effizienter gewesen wäre. Wie wir im Kapitel über quadratische Reste sehen werden, konnten sich die Autoren *vor* Beginn ihrer Rechnung leicht davon überzeugen, daß drei modulo F_{20} *keine* Quadratzahl ist; der Aufwand für die Entscheidung, ob eine Zahl a Quadrat modulo F_{20} ist, erfordert einen Aufwand, der ungefähr dem für die Anwendung des EUKLIDischen Algerithmus auf a und F_{20} entspricht, im Falle $a = 3$ also nicht viel mehr als die Berechnung von F_{20} mod 3, was man im Kopf als $(-1)^{2^{20}} + 1 = 2$ berechnen kann.

Kehren wir zurück zu Primzahltests für allgemeine Zahlen n, Wenn wir $n - 1$ zumindest teilweise faktorisieren können, hilft gelegentlich der folgende Satz:

Satz: Angenommen $n = uv$ ist das Produkt zweier teilerfremder Zahlens $u < v$, und wir kennen die Primzerlegung $v = \prod q_i^{e_i}$ von v. Falls es ein $a \in \mathbb{N}$ gibt, so daß $a^{n-1} \equiv 1 \bmod n$ und

$$\text{ggT}\left(a^{(n-1)/q_i} - 1, n\right) = 1 \qquad \text{für alle } i\,,$$

ist n eine Primzahl.

Beweis: Angenommen, p sei ein echter Primteiler von n, und a erfülle die angegebenen Bedingungen. Die Ordnung der Restklasse von a in $(\mathbb{Z}/p)^\times$ sei r; sie ist natürlich ein Teiler von $p-1$.

Da $a^{n-1} \equiv 1 \bmod n$ und damit erst recht modulo des Teilers p, ist r auch Teiler von $n-1$; da $a^{(n-1)/q_i} - 1$ aber teilerfremd zu n ist, ist $a^{(n-1)/q_i}$ nicht kongruent eins modulo p; die Ordnung r teilt also keine der Zahlen $(n-1)/q_i$. Somit teilt r zwar das volle Produkt $u \prod q_i^{e_i}$, nicht aber das Produkt, in dem auch nur ein Exponent e_i erniedrigt wurde. Somit ist r für jedes i ein Vielfaches von $q_i^{e_i}$ und damit auch ein Vielfaches von v. Da r ein Teiler von $p-1$ ist, folgt insbesondere daß $v < p$ sein muß. Nun ist aber $n = uv$ und $u < v$, d.h. $v > \sqrt{n}$. Damit haben wir gezeugt, daß jeder echte Primteiler von n größer als $\sqrt{n}$ sein muß. Da dies unmöglich ist, gibt es keine echten Primteiler, d.h. n ist eine Primzahl. ∎

§4: Der Test von Miller und Rabin

Der Test von MILLER und RABIN ist eine etwas strengere Version des Tests von FERMAT: Um zu testen, ob p eine Primzahl sein kann, schreiben wir $p-1$ zunächst als Produkt $2^n u$ einer Zweierpotenz und einer ungeraden Zahl; sodann berechnen wir $a^u \bmod p$. Falls wir das Ergebnis eins erhalten, ist erst recht $a^{p-1} \equiv 1 \bmod p$, und wir können nicht folgern, daß p zusammengesetzt ist.

Andernfalls quadrieren wir das Ergebnis bis zu n-mal modulo p. Falls dabei nie eine Eins erscheint, folgt nach FERMAT, daß p zusammengesetzt ist. Falls vor der ersten Eins eine von -1 (*bzw.* $p-1$) verschiedene Zahl erscheint, folgt das auch, denn im Körper $\mathbb{F}_p$ hat die Eins nur die beiden Quadratwurzeln ± 1. In allen anderen Fällen erfahren wir nicht mehr als bei FERMAT.

Algorithmisch funktioniert der Test also folgendermaßen:

Schritt 0: Wähle ein zufälliges a, schreibe $p - 1 = 2^n u$ mit einer ungeraden Zahl u und berechne $b = a^u \bmod p$. Falls dies gleich Eins ist, endet der Algorithmus und wir konnten nicht zeigen, daß p eine zusammengesetzte Zahl ist; sie kann prim sein.

Schritt $i, 1 \leq i \leq n$**:** Falls $b \equiv -1 \bmod p$, endet der Algorithmus und wir können nicht ausschließen, daß p prim ist. Falls $b = 1$ ist (was frühestens im zweiten Schritt der Fall sein kann), ist p zusammengesetzt und der Algorithmus endet. Andernfalls wird b durch $b^2 \bmod p$ ersetzt und es geht weiter mit Schritt $i + 1$.

Schritt $n + 1$**:** Der Algorithmus endet mit dem Ergebnis, daß p zusammengesetzt ist.

Beispiel: Ist 247 eine Primzahl? Wir wählen $a = 77$, und da $77^{246} \bmod 247 = 1$ ist, können wir mit FERMAT nicht ausschließen, daß 247 prim ist. Da aber $77^{123} \bmod 247 = 77$ ist, sagt uns der Algorithmus von MILLER und RABIN im zweiten Schritt, wenn wir $77^2 \equiv 1 \bmod 247$ betrachten, daß die Zahl zusammengesetzt sein muß.

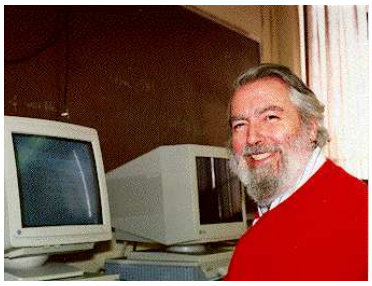
Hätten wir allerdings mit $a = 87$ gearbeitet, hätten wir im nullten Schritt $87^{123} \equiv 1 \bmod 247$ berechnet und hätten $247 = 13 \cdot 19$ nicht als zusammengesetzt erkannt.

GARY L. MILLER entwickelte diesen Test 1975 im Rahmen seiner Dissertation (in Informatik) an der Universität von Berkeley. Dabei ging es ihm nicht um einen probabilistischen Test, sondern um einen Test, der immer die richtige Antwort liefert. Er konnte zeigen, daß dies hier beim Test von hinreichend vielen geeigneten Basen der Fall ist **vorausgesetzt** die bis heute immer noch offene verallgemeinerte RIEMANN-Vermutung ist richtig. Er lehrte später zunächst einige Jahre an der University of Waterloo, inzwischen an der Carnegie Mellon University. Seine späteren Arbeiten stammen hauptsächlich aus dem Gebiet der rechnerischen Geometrie. www.cs.cmu.edu/∼glmiller

MICHAEL O. RABIN wurde 1931 in Breslau geboren. Die Familie wanderte nach Israel aus, wo er an der hebräischen Universität von Jerusalem Mathematik studierte. Nach seinem Diplom 1953 ging er nach Princeton, wo er 1957 promovierte. Seit 1958 lehrt er an der hebräischen Universität, wo er unter anderem auch Dekan der mathematischen Fakultät und Rektor war. Seit 1983 ist er zusätzlich Inhaber des THOMAS J. WATSON-Lehrstuhls für Informatik an der Harvard University. Seine Forschungen, für die er u.a. 1976 den TURING-

Preis erhielt, beschäftigen sich mit der Komplexität mathematischer Operationen und der Sicherheit von Informationssystemen. Seine home page in Harvard ist zu finden unter `www.seas.harvard.edu/directory/Rabin` .

Anscheinend wurde der Test von MILLER und RABIN bereits 1974, also vor MILLERs Veröffentlichung, von SELFRIDGE verwendet; daher sieht man gelegentlich auch die korrektere Bezeichnung *Test von* MILLER, RABIN *und* SELFRIDGE.



Der amerikanische Mathematiker JOHN L. SELFRIDGE promovierte 1958 an der University of California in Los Angelos. Bis zu seiner Emeritierung lehrte er an der Northern Illinois University. Seine Arbeiten befassen sich vor allem mit der analytischen sowie der konstruktiven Zahlentheorie. Vierzehn davon schrieb er mit PAUL ERDŐS. `math.niu.edu/faculty/index.php?cmd=detail&id=91`

§5: Der Test von Agrawal, Kayal und Saxena

Im August 2002 stellten MANINDRA AGRAWAL, NEERAJ KAYAL und NITIN SAXENA, zwei Bachelor-Studenten am Indian Institute of Technology in Kanpur und ihr Professor, einen Primzahltest vor, der ebenfalls auf dem kleinen Satz von FERMAT beruht, aber (natürlich auf Kosten eines erheblich größeren Aufwands) immer die richtige Antwort liefert; er ist inzwischen erschienen in

> MANINDRA AGRAWAL, NEERAJ KAYAL, NITIN SAXENA: PRIMES is in P, *Annals of Mathematics* **160** (2004), 781-793.

Selbstverständlich war dies nicht der erste Primzahltest, der deutlich schneller als Probedivisionen zeigt, ob eine gegebene Zahl prim ist oder nicht; es ist auch bei weitem nicht der schnellste solche Test. Er hat aber gegenüber anderen solchen Tests zwei Besonderheiten:

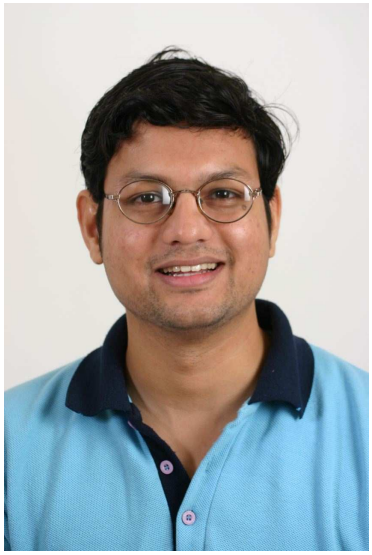
1. Zu seinem Verständnis ist – nach einigen in der letzten Zeit gefundenen Vereinfachungen – nur elementare Zahlentheorie notwendig.
2. Es ist der bislang einzige Test, von dem man beweisen kann, daß seine Laufzeit für n-stellige Zahlen durch ein Polynom in n begrenzt werden kann.

MANINDRA AGRAWAL erhielt 1986 seinen BTech und 1991 seinen PhD in Informatik am Indian Institute of Technology in Kanpur, wo er – abgesehen von Gastaufenthalten in Madras, Ulm, Princeton und Singapur – seither als Professor lehrt. Seine Arbeiten befassen sich hauptsächlich mit der Komplexität von Schaltungen und von Algorithmen. Für die Arbeit mit KAYAL und SAXENA erhielt er gemeinsam mit diesen unter anderem den GÖDEL-Preis 2006 für die besten Zeitschriftenveröffentlichung auf dem Gebiet der Theoretischen Informatik.

http://www.cse.iitk.ac.in/users/manindra/

NEERAJ KAYAL wurde 1979 geboren. Er erhielt 2002 seinen BTech und 2006 seinen PhD bei MANINDRA AGRAWAL am Indian Institute of Technology in Kanpur. Neuere Arbeiten beschäftigen unter anderem sich mit der Komplexität des Isomorphieproblems bei endlichen Ringen sowie der Lösbarkeit von bivariaten Polynomgleichungen über endlichen Körpern. Nach einem kurzen Aufenthalt an der Rutgers University arbeitet er inzwischen bei Microsoft Research.

http://research.microsoft.com/en-us/people/neeraka/



NITIN SAXENA wurde 1981 geboren. Er erhielt 2002 seinen Bachelor of Technology und 2006 seinen PhD bei MANINDRA AGRAWAL am Indian Institute of Technology in Kanpur. Während der Arbeit an seiner Dissertation über die Anwendung von Ringhomomorphismen auf Fragen der Komplexitätstheorie besuchte er jeweils ein Jahr lang die Universitäten Princeton und Singapur, danach arbeitete er als Postdoc in der Gruppe *Quantum Computing and Advanced Systems Research* am Centrum voor Wiskunde en Informatica in Amsterdam. 2006–2012 war er *Bonn Junior Fellow* am HAUSDORFF CENTER der Universität Bonn, seit 2013 hat er eine Professur am Indian Institute of Technology in Kanpur. Sein Interesse gilt algorithmischen Verfahren der Algebra und Zahlentheorie sowie Fragen der Komplexitätstheorie.

http://www.cse.iitk.ac.in/users/nitin/

Für uns ist vor allem der erste Punkt wichtig; der zweite ist zwar ein für Komplexitätstheoretiker sehr interessantes Ergebnis, hat aber keinerlei praktische Bedeutung: Im Buch

> VICTOR SHOUP: A computational Introduction to Number Theory and Algebra, *Cambridge University Press*, ^{2}2008 (*Volltext* unter `http://shoup.net/ntb/`),

dem dieser Paragraph im wesentlichen folgt, argumentiert SHOUP, daß alternative Algorithmen, so man sich auf Zahlen von weniger als 2^{256} Bit beschränkt, durch eine vergleichbare Schranke abgeschätzt werden können, und natürlich sind die Zahlen, mit denen wir es üblicherweise zu tun haben, deutlich kleiner. In der Praxis sind die alternativen Algorithmen deutlich schneller.

(2^{256} liegt knapp über 10^{77}; derzeitige Schätzungen für die Anzahl der Nukleonen im Universum liegen bei etwa 10^{80}. Damit ist klar, daß kein Computer, der mit irgendeiner Art von heute bekannter Technologie arbeitet, je eine solche Zahl speichern kann, geschweige denn damit rechnen.)

Im folgenden wird es daher nur um eine mathematische Betrachtung des Algorithmus von AGRAWAL, KAYAL und SAXENA gehen; für einen (kurzen und elementaren) Beweis der Komplexitätsaussage sei beispielsweise auf das zitierte Buch von SHOUP verwiesen.

Die Grundidee des Algorithmus steckt im folgenden

Satz: $n > 1$ sei eine natürliche Zahl und $a \in \mathbb{N}$ sei dazu teilerfremd. n ist genau dann prim, wenn im Polynomring über $\mathbb{Z}/N$ gilt:

$$(X + a)^n = X^n + a\,.$$

Beweis: Nach dem binomischen Lehrsatz ist

$$(X + a)^n = X^n + a^n + \sum_{i=1}^{n-1} \binom{n}{i} a^i X^{n-i}\,.$$

Für eine Primzahl n gilt nach dem kleinen Satz von FERMAT in $\mathbb{Z}/n$ die Gleichung $a^n = a$. Außerdem ist für $1 \leq i \leq n-1$ der Binomialkoeffizient

$$\binom{n}{i} = \frac{n(n-1)\cdots(n-i+1)}{i!}$$

durch n teilbar, da n Faktor des Zählers, nicht aber des Nenners ist. Somit verschwinden in $\mathbb{Z}/n$ alle diese Binomialkoeffizienten, und die Gleichung aus dem Satz ist bewiesen.

Umgekehrt sei n eine zusammengesetzte Zahl und p ein Primteiler von n. Genauer sei $n = p^e m$ mit einer zu p teilerfremden Zahl m. Dann ist der Zähler von $\binom{n}{p}$ genau durch p^e teilbar, denn die Faktoren $(n-1), \ldots, (n-p+1)$ sind allesamt teilerfremd zu p, und der Nenner ist genau durch p teilbar. Somit ist $\binom{n}{p}$ zwar durch p^{e-1} teilbar, nicht aber durch p^e und damit erst recht nicht durch n. Wenn wir $(X+a)^n$ über $\mathbb{Z}/n$ ausmultiplizieren, kann daher der Summand $\binom{n}{p} a^p X^{n-p}$ nicht verschwinden, und damit kann die Gleichung aus dem Satz nicht gelten. ∎

In dieser Form führt der Satz allerdings noch nicht zu einem praktikablen Primzahltest: Das Ausmultiplizieren von $(X+a)^n$ führt schließlich auf $n+1$ Summanden, der Aufwand ist also proportional zu n und damit vergleichbar damit, daß wir für jede natürliche Zahl $1 < m < n$ nachprüfen, ob n ohne Rest durch m teilbar ist. Die wesentliche neue Idee von AGRAWAL, KAYAL und SAXENA besteht darin zu zeigen, daß es bereits reicht, Gleichungen der im Satz genannten Art modulo einem geeigneten Polynom $X^r - 1$ mit einem relativ kleinen Grad r nachzuprüfen.

Konkret geht ihr Algorithmus folgendermaßen vor:

n sei die zu testende natürliche Zahl und $\ell(n) = [\log_2 n] + 1$ die Anzahl ihrer Binärziffern.

1. Schritt: Stelle sicher, daß n keine Potenz einer anderen natürlichen Zahl ist.

Das läßt sich beispielsweise dadurch bewerkstelligen, daß man die Quadratwurzel, Kubikwurzel *usw.* von n soweit ausrechnet bis man

erkennt, daß es sich um keine natürliche Zahl handelt. Der ungünstigste Fall ist offenbar der, daß n eine Zweierpotenz sein könnte; man muß also bis zur $[\log_2 n]$-ten Wurzel gehen.

2. Schritt: Finde die kleinste natürliche Zahl $r > 1$ mit der Eigenschaft, daß entweder ggT$(n, r) > 1$ ist oder aber ggT$(n, r) = 1$ ist und n mod r in $(\mathbb{Z}/r)^\times$ eine größere Ordnung als $4\ell(n)^2$ hat.

Dies geschieht einfach dadurch, daß man die Zahlen $r = 2, 3, \ldots$ allesamt durchprobiert, bis zum ersten mal eine der beiden Bedingungen erfüllt ist. Die Bedingung über die Ordnung der Restklasse von n in $(\mathbb{Z}/r)^\times$ prüft man nach, indem man nacheinander ihre Potenzen ausrechnet, bis man entweder eine Eins gefunden hat oder aber der Exponent größer als $4\ell(n)^2$ ist.

3. Schritt: Falls $r = n$, ist n prim und der Algorithmus endet.

In der Tat: Dann haben wir für alle $r < n$ überprüft, daß ggT$(n, r) = 1$ ist. Wenn der Algorithmus etwas taugt, darf er natürlich höchstens für sehr kleine Werte von n mit diesem Schritt enden.

4. Schritt: Falls im zweiten Schritt ein r gefunden wurde, für das der ggT von n und r größer als eins ist, muß n zusammengesetzt sein und der Algorithmus endet.

Denn dann haben wir einen Teiler von n gefunden.

Andernfalls kennen wir nun eine zu n teilerfremde Zahl r, für die n mod r in $(\mathbb{Z}/r)^\times$ eine größere Ordnung als $4\ell(n)^2$ hat.

5. Schritt: Teste für $j = 1, \ldots, \ell \underset{\text{def}}{=} 2\ell(n)[\sqrt{r}] + 1$, ob über $\mathbb{Z}/n$

$$(X + j)^n \equiv X^n + j \bmod (X^r - 1)\,.$$

Sobald ein j gefunden wird, für das dies nicht erfüllt ist, endet der Algorithmus mit dem Ergebnis n *ist zusammengesetzt.*

Falls nämlich n eine Primzahl ist, stimmen $(X + j)^n$ und $X^n + j$ als Polynome mit Koeffizienten aus $\mathbb{Z}/n$ nach obigem Satz überein, sind also erst recht auch gleich modulo $(X^r - 1)$.

6. Schritt: Wenn alle Tests im fünften Schritt bestanden sind, ist n eine Primzahl.

Dies zu beweisen ist die Hauptarbeit dieses Paragraphen.

Nach den Kommentaren zu den einzelnen Schritten ist klar, daß der Algorithmus für eine Primzahl n stets das richtige Ergebnis liefert; wir müssen zeigen, daß er auch zusammengesetzte Zahlen stets erkennt.

Sei also n eine zusammengesetzte Zahl. Falls n Potenz einer anderen natürlichen Zahl ist, wird dies im ersten Schritt erkannt; wir können und werden im folgenden daher annehmen, daß dies nicht der Fall ist.

Das r aus dem zweiten Schritt ist auf jeden Fall echt kleiner als n, denn als zusammengesetzte Zahl hat n insbesondere einen Teiler $r < n$. Der Algorithmus kann daher nicht im dritten Schritt mit der Antwort „n ist prim“ enden. Falls er im vierten Schritt endet, lieferte der zweite Schritt einen Teiler von n, und wir erhalten die richtige Antwort „n ist zusammengesetzt“.

Für den Rest des Paragraphen können wir somit annehmen, daß der zweite Schritt auf ein r führte, für das ggT$(n, r) = 1$ ist. Wir müssen zeigen, daß einer der Tests im fünften Schritt scheitert, daß es also eine natürliche Zahl j gibt mit

$$1 \leq j \leq \ell \quad \text{und} \quad (X + j)^n \not\equiv X^n + j \bmod (X^r - 1) \text{ in } \mathbb{Z}/n[X]\,.$$

Wir nehmen an, das sei nicht der Fall, und betrachten einen Primteiler p von n. Dieser muß größer als r sein, denn sonst hätte der Algorithmus bereits mit dem vierten Schritt spätestens bei $r = p$ geendet.

Jede Kongruenz modulo n ist erst recht eine Kongruenz modulo p; wir können daher davon ausgehen, daß für alle j mit $1 \leq j \leq \ell$ gilt

$$(X + j)^n \equiv X^n + j \bmod (X^r - 1) \text{ in } \mathbb{F}_p[X]\,.$$

Wenn wir zum Faktorring $R = \mathbb{F}_p[X]/(X^r - 1)$ übergehen, ist dort also

$$(X + j)^n = X^n + j \quad \text{falls} \quad 1 \leq j \leq \ell\,.$$

Um diese seltsame Relation genauer zu untersuchen, betrachten wir für jede zu r teilerfremde natürliche Zahl k die Abbildung

$$\widehat{\sigma}_k\colon \begin{cases} \mathbb{F}_p[X] \to R \\ \qquad g \mapsto g(X^k) \bmod (X^r - 1) \end{cases},$$

die in jedem Polynom g die Variable X überall durch X^k ersetzt.

Lemma: $\widehat{\sigma}_k$ ist surjektiv und sein Kern besteht genau aus den Vielfachen des Polynoms $X^r - 1$.

Beweis: Wir betrachten $\widehat{\sigma}_k$ nur für Indizes k, die zu r teilerfremd sind. Zu jedem solchen Index gibt es daher ein k', so daß $kk' \equiv 1 \bmod r$ ist, und modulo $X^r - 1$ ist damit $X^{kk'} \equiv X$. Für ein beliebiges Polynom $g \in \mathbb{F}_p[X]$ und $h(X) = g(X^{k'})$ ist daher in R

$$\widehat{\sigma}_k(h) = h(X^k) = g(X^{kk'}) = g(X) = g\,,$$

die Abbildung ist also surjektiv.

Was ihren Kern betrifft, so enthält er auf jeden Fall $X^r - 1$ und alle seine Vielfachen, denn

$$\widehat{\sigma}_k(X^r - 1) = (X^{kr} - 1) \bmod (X^r - 1) = 1^k - 1 = 0\,,$$

da $X^r \equiv 1 \bmod (X^r - 1)$.

Umgekehrt sei g irgendein Polynom aus dem Kern von $\widehat{\sigma}_k$. Dann ist das Polynom $h(X) = g(X^k)$ modulo $X^r - 1$ gleich dem Nullpolynom, ist also ein Vielfaches von $X^r - 1$. Konkret sei $h = (X^r - 1)f$. Im Faktorring R ist dann

$$g(X) = g(X^{kk'}) = h(X^{k'}) = (X^{k'r} - 1)f(X^{k'}) = 0\,,$$

denn wegen $X^r = 1$ in R ist dort $X^{k'r} - 1 = 0$.

In $\mathbb{F}_p[X]$ muß $g(X)$ daher ein Vielfaches von $X^r - 1$ sein, und genau das war die Behauptung über den Kern von $\widehat{\sigma}_k$.

∎

Da alle Vielfachen von $X^r - 1$ im Kern von $\widehat{\sigma}_k$ liegen, definiert $\widehat{\sigma}_k$ eine Abbildung σ_k von R nach R, die jedem Polynom g mod $(X^r - 1)$ aus R das Element $\widehat{\sigma}_k(g)$ zuordnet; nach dem gerade bewiesenen Lemma hängt dieses wirklich nur von der Restklasse g mod $(X^r - 1)$ ab. Außerdem zeigt das Lemma, daß σ_k sowohl surjektiv als auch injektiv ist, denn der Kern von $\widehat{\sigma}_k$ ist gleich dem Kern der Restklassenabbildung von $\mathbb{F}_p[X]$ nach R. Damit ist σ_k ein bijektiver Homomorphismus von R nach R, ein sogenannter *Automorphismus* von R. Wir haben damit für jede zu r teilerfremde natürliche Zahl k einen Automorphismus $\sigma_k\colon R \to R$, der jedem Polynom in X das entsprechende Polynom in X^k zuordnet. Da

wir in R rechnen, werden natürlich alle Polynome modulo $X^r - 1$ betrachtet.

Unmittelbar aus der Definition folgt, daß die verschiedenen Automorphismen σ_k miteinander kommutieren; genauer ist

$$\sigma_k \circ \sigma_{k'} = \sigma_{k'} \circ \sigma_k = \sigma_{kk'} ,$$

denn in allen drei Fällen wird im Endeffekt X durch $X^{kk'}$ ersetzt.

Speziell für das Element $X + j$ aus R ist $\sigma_k(X + j) = X^k + j$. Für $k = n$ und $j = 1, \ldots, \ell$ ist andererseits auch

$$\sigma_n(X + j) = (X + j)^n ,$$

denn für diese j wurde ja nach unserer Annahme der Test im fünften Schritt bestanden.

Wir wollen genauer untersuchen, wann die Gleichung $\sigma_k(f) = f^k$ erfüllt ist. Dazu definieren zwei Arten von Mengen:

$$\begin{array}{ll} C(f) = \left\{ k \in (\mathbb{Z}/r)^\times \;\middle|\; \sigma_k(f) = f^k \right\} & \text{für alle } f \in R \qquad \text{und} \\ D(k) = \left\{ f \in R \;\middle|\; \sigma_k(f) = f^k \right\} & \text{für alle } k \in (\mathbb{Z}/r)^\times \end{array}$$

Beide Mengen enthalten mit zwei Elementen auch deren Produkt, denn für zwei Elemente $k, k' \in C(f)$ ist

$$\sigma_{kk'}(f) = \sigma_k(f)\sigma_{k'}(f) = \sigma_k\big(\sigma_{k'}(f)\big) = \sigma_k(f^{k'}) = \sigma_k(f)^{k'} = f^{kk'} ,$$

und für $f, g \in D(k)$ ist

$$\sigma_k(fg) = \sigma_k(f)\sigma_k(g) = f^k g^k = (fg)^k .$$

Der Rest des Beweises besteht darin, daß wir die „Größe“ der Menge $D(n)$ auf zwei verschiedene Weisen abschätzen und daraus einen Widerspruch herleiten zur Annahme, daß n zusammengesetzt ist, aber trotzdem vom Algorithmus als Primzahl klassifiziert wird. Wir definieren zunächst zwei neue Zahlen:

- s sei die Ordnung der Restklasse von p in $(\mathbb{Z}/r)^\times$. Dann ist r ein Teiler von $p^s - 1$, denn $p^s \equiv 1 \bmod r$.

- t sei die Ordnung der von den Restklassen von p und n erzeugten Untergruppe von $(\mathbb{Z}/r)^\times$, d.h also die Ordnung der kleinsten Untergruppe, die beide Restklassen enthält. Da diese Untergruppe insbesondere die Restklasse von p und deren Potenzen enthält, ist t ein Vielfaches von s.

Als nächstes betrachten wir einen Körper K mit p^s Elementen. Einen solchen Körper kann man konstruieren, indem man den Vektorraum $\mathbb{F}_p^s$ identifiziert mit dem Vektorraum aller Polynome vom Grad kleiner s mit Koeffizienten aus $\mathbb{F}_p$ und dort eine Multiplikation einführt, die zwei Polynomen deren Produkt modulo einem festen irreduziblen Polynom vom Grad s über $\mathbb{F}_p$ zuordnet. Man kann zeigen (siehe Algebra-Vorlesung oder entsprechendes Lehrbuch), daß es für jedes s ein solches Polynom gibt, und daß zwei verschiedene irreduzible Polynome vom Grad s zu isomorphen Körpern führen.

Aus Kapitel 1 wissen wir, daß die multiplikative Gruppe jedes endlichen Körpers zyklisch ist; $K^\times$ ist also eine zyklische Gruppe der Ordnung $p^s - 1$. Diese Zahl ist, wie wir gerade gesehen haben, ein Vielfaches von r; somit gibt es in $K^\times$ (mindestens) ein Element ζ der Ordnung r. Für irgendein solches Element definieren wir einen Homomorphismus

$$\widehat{\tau}\colon \begin{cases} \mathbb{F}_p[X] \to K \\ \qquad g \mapsto g(\zeta) \end{cases} .$$

Da $\widehat{\tau}(X^r - 1) = \zeta^r - 1$ verschwindet, induziert $\widehat{\tau}$ einen Ringhomomorphismus $\tau\colon R \to K$. Die angekündigten Abschätzungen der „Größe“ von $D(n)$ beziehen sich auf die Mächtigkeit der Menge $S = \tau\big(D(n)\big)$:

Lemma: $S = \tau\big(D(n)\big)$ hat höchstens $n^{2[\sqrt{t}]}$ Elemente.

Beweis: Wir gehen davon aus, daß n weder eine Primzahl noch eine Primzahlpotenz ist; daher gibt es außer dem Primteiler p noch mindestens einen weiteren Primteiler q. Wenn wir (in $\mathbb{N}$) Potenzen der Form $n^u p^v$ und $n^{u'} p^{v'}$ mit $u, u', v, v' \in \mathbb{N}_0$ betrachten, sind diese daher genau dann gleich, wenn $(u, v) = (u', v')$ ist: Ist nämlich $u \neq u'$, so tritt g in der Primzerlegung der beiden Elemente mit verschiedenen Exponenten

auf, und ist $u = u'$, aber $v \neq v'$, so gilt entsprechendes für p. Daher hat die Menge

$$I = \left\{ n^u p^v \;\middle|\; 0 \leq u, v \leq [\sqrt{t}] \right\}$$

mindestens $\left([\sqrt{t}]+1\right)^2$ Elemente, und diese Zahl ist offensichtlich größer als t.

Nun war aber t definiert als die Ordnung der Untergruppe von $(\mathbb{Z}/r)^\times$, die von den Restklassen von n und von p erzeugt wird; daher muß es mindestens zwei Elemente

$$k = n^u p^v \quad \text{und} \quad k' = n^{u'} p^{v'}$$

aus I geben, die dieselbe Restklasse in $(\mathbb{Z}/r)^\times$ definieren, für die also gilt: $k \equiv k' \bmod r$. Da die Exponenten u, u', v, v' höchstens gleich $[\sqrt{t}]$ sind und p ein Teiler von n ist, können wir $n^{2[\sqrt{t}]}$ als (sehr grobe) obere Schranke für k und k' nehmen.

Nun sei $f \in R$ ein Element von $D(n)$. Nach Definition der Mengen $C(f)$ und $D(n)$ ist dann auch n ein Element von $C(f)$. Außerdem enthält $C(f)$ stets die Eins und nach dem kleinen Satz von FERMAT auch die Primzahl p, denn Potenzieren mit p ist über $\mathbb{F}_p$ ein Homomorphismus. Da mit zwei Elementen stets auch deren Produkt in $C(f)$ liegt, liegen daher die Restklassen modulo r aller Elemente von I in $C(f)$. Insbesondere sind daher k und k' Elemente von $C(f)$, d.h.

$$\sigma_k(f) = f^k \quad \text{und} \quad \sigma_{k'}(f) = f^{k'} .$$

Wegen $k \equiv k' \bmod r$ ist aber σ_k dieselbe Abbildung wie $\sigma_{k'}$; daher ist $f^k = f^{k'}$ für jedes $f \in D(n)$. Somit sind die Bilder $\tau(f)$ aller $f \in R$ Nullstellen des Polynoms $X^k - X^{k'}$. Dessen Grad ist das Maximum von k und k', und da $\tau(f)$ im Körper K liegt, gibt es höchstens so viele Nullstellen, wie der Grad angibt. Aufgrund der obigen Abschätzung für k und k' hat das Polynom daher höchstens $n^{2[\sqrt{t}]}$ Nullstellen, und damit kann auch S nicht mehr Elemente enthalten. ∎

Als untere Grenze für die Elementanzahl von S erhalten wir

Lemma: S enthält mindestens $2^{\min(t,\ell)} - 1$ Elemente.

Beweis: Wegen der bestandenen Tests in Schritt 5 liegt $\tau(X+j)$ in $D(n)$ für $j = 1, \ldots, \ell$. Da $p > r > t \geq m$ ist, sind die Zahlen von 1 bis m auch modulo p paarweise verschieden. Die Teilmenge

$$P = \Big\{ \prod_{j=1}^{m} (X+j)^{e_j} \;\Big|\; e_j \in \{0,1\} \text{ und } \sum_{j=1}^{m} e_j < m \Big\}$$

von $\mathbb{F}_p[X]$ enthält daher $2^m - 1$ Polynome.

Aus diesen Polynomen können wir Elemente von R *bzw.* K machen, indem wir für die Variable X die Restklasse $\eta = X \bmod (X^r - 1)$ *bzw.* das oben gewählte Element ζ der Ordnung r einsetzen; wir erhalten Teilmengen

$$P(\eta) = \big\{ f(\eta) \;\big|\; f \in P \big\} \subseteq R \quad \text{und} \quad P(\zeta) = \big\{ f(\zeta) \;\big|\; f \in P \big\} \subseteq K\,.$$

Da sowohl n als auch p in $D(n)$ liegen und mit zwei Elementen auch deren Produkt, liegt $P(\eta)$ in $D(n)$ und damit $\tau\big(P(\eta)\big) = P(\zeta)$ in S. Das Lemma ist daher bewiesen, sobald wir gezeigt haben, daß $P(\zeta)$ mindestens $2^m - 1$ Elemente enthält.

Falls dies nicht der Fall wäre, müßte es in P zwei verschiedene Polynome g und h geben, für die $g(\zeta) = h(\zeta)$ wäre. Wir müssen also zeigen, daß $g(\zeta) = h(\zeta)$ nur dann gelten kann, wenn $g = h$ ist.

Wie im vorigen Lemma folgt, da $1, p$ und n alle drei sowohl in $C\big(g(\eta)\big)$ als auch in $C\big(h(\eta)\big)$ liegen, daß alle natürlichen Zahlen k der Form $k = n^u p^v$ in diesen beiden Mengen liegen.

Da $g(\zeta) = h(\zeta)$, gilt für jedes solche k

$$\begin{aligned} 0 &= g(\zeta)^k - h(\zeta)^k = \tau\big(g(\eta)\big)^k - \tau\big(h(\eta)\big)^k = \tau\big(g(\eta)^k\big) - \tau\big(h(\eta)^k\big) \\ &= \tau\big(g(\eta^k)\big) - \tau\big(h(\eta^k)\big) = g(\zeta^k) - h(\zeta^k)\,. \end{aligned}$$

Da ζ in K die Ordnung r hat, hängt ζ^k nur von k mod r ab; die Anzahl verschiedener Restklassen der Form $n^u p^v$ modulo r hatten wir oben mit t bezeichnet. Somit hat die Differenz $g - h$ mindestens t Nullstellen. Andererseits sind aber g und h und damit auch ihre Differenz Polynome

vom Grad höchstens $t-1$, also muß $g-h$ das Nullpolynom sein, d.h. $g = h$. Somit enthält S mindestens $2^m - 1$ Elemente, wie behauptet. ∎

Zum Abschluß des Beweises, daß der Test von AGRAWAL, KAYAL und SAXENA stets die richtige Antwort liefert, müssen wir nun nur noch zeigen, daß die Schranken aus den beiden letzten Lemmata, die ja unter der Voraussetzung bewiesen wurde, daß eine zusammengesetzte Zahl als prim erkannt wird, einander widersprechen, daß also die untere Schranke größer ist als die obere:

Lemma: $2^{\min(t,\ell)} - 1 > n^{2[\sqrt{t}]}$.

Beweis: Da $\ell(n) > \log_2 n$, genügt es zu zeigen, daß

$$2^{\min(t,\ell)} - 1 > 2^{2\ell(n)[\sqrt{t}]}.$$

Da beide Exponenten natürliche Zahlen sind, genügt dazu wiederum, daß $\min(t,\ell) > 2\ell(n)[\sqrt{t}]$ ist, denn wenn sich die Exponenten um mindestens eins unterscheiden, ist die Differenz zwischen den Potenzen mindestens zwei. Wir müssen daher zeigen, daß sowohl t als auch ℓ größer sind als $2\ell(n)[\sqrt{t}]$.

Für $\ell = 2\ell(n)[\sqrt{r}] + 1$ ist das klar, da t die Ordnung einer Untergruppe von $(\mathbb{Z}/r)^\times$ bezeichnet und damit auf jeden Fall kleiner als r ist.

Die Ungleichung $t > 2\ell(n)[\sqrt{t}]$ ist sicherlich dann erfüllt, wenn sogar $t > 2\ell(n)\sqrt{t}$ ist, und dies wiederum ist äquivalent zur Ungleichung $t > 4\ell(n)^2$. Nun ist aber t die Ordnung jener Untergruppe von $(\mathbb{Z}/r)^\times$, die von den Restklassen von n und p erzeugt wird. Da wir im zweiten Schritt des Algorithmus sichergestellt haben, daß dort allein die Ordnung der Restklasse von n schon größer ist als $4\ell(n)^2$, ist auch die Ungleichung für t trivial. ∎

Damit ist die Korrektheit des Algorithmus vollständig bewiesen.