# 3

# Gibt es primzahldefinierende Funktionen?

Die Untersuchung von Primzahlen wirft die Frage auf, ob es nicht einfach berechenbare Funktionen $f(n)$ gibt, die für alle natürlichen Zahlen $n$ definiert sind und einige oder alle Primzahlen produzieren.

Beispielsweise sollte eine der folgenden Bedingungen erfüllt sein:

(a) $f(n) = p_n$ (die $n$-te Primzahl) für alle $n \geq 1$;

(b) $f(n)$ ist immer prim und wenn $n \neq m$, dann $f(n) \neq f(m)$;

(c) der positive Wertebereich der Funktion ist identisch mit der Menge der Primzahlen.

Offensichtlich ist Bedingung (a) schärfer als (b) und als (c).

Die bisher erzielten Resultate sind eher enttäuschend, außer einigen, die in Bezug auf (c) von theoretischem Interesse sind.

## I Funktionen mit der Eigenschaft (a)

In ihrem berühmten Buch fragten Hardy & Wright:

(1) Gibt es eine Formel für die $n$-te Primzahl?

(2) Gibt es für eine Primzahl eine Formel, die sich aus den vorangegangenen Primzahlen aufbaut?

P. Ribenboim, *Die Welt der Primzahlen*, 2. Aufl., Springer-Lehrbuch,
DOI 10.1007/978-3-642-18079-8_3, © Springer-Verlag Berlin Heidelberg 2011

Hinter Frage (1) verbirgt sich die Absicht, anhand von berechenbaren und möglichst herkömmlichen Funktionen einen geschlossenen Ausdruck für die $n$-te Primzahl $p_n$ zu finden. Dieses Problem ist eng damit verbunden, die *Primzahlfunktion* auf vernünftige Weise auszudrücken.

Für jede reelle Zahl $x > 0$ bezeichne $\pi(x)$ die Anzahl der Primzahlen $p$ mit $p \leq x$.

Dies ist die traditionell übliche Bezeichnung für eine der wichtigsten Funktionen der Primzahltheorie. Auf sie wird in Kapitel 4 näher eingegangen. Obwohl die Zahl $\pi = 3{,}14159265\ldots$ und die Funktion $\pi(x)$ in der Formel unten gleichzeitig vorkommen, besteht keine Verwechslungsgefahr.

Ich werde zunächst eine Formel für $\pi(m)$ angeben, die auf Willans (1964) zurückgeht. Sie beruht auf dem klassischen Satz von Wilson, der in Kapitel 2 bewiesen wurde.

Für jede ganze Zahl $j \geq 1$ sei

$$F(j) = \left[\cos^2 \pi \frac{(j-1)! + 1}{j}\right],$$

wobei $[x]$ die eindeutig bestimmte ganze Zahl $n$ darstellt, so dass die reelle Zahl $x$ die Ungleichung $n \leq x < n + 1$ erfüllt.

Für jede ganze Zahl $j > 1$ wird $F(j) = 1$, wenn $j$ eine Primzahl ist, ansonsten $F(j) = 0$. Zudem gilt $F(1) = 1$.

Somit ist

$$\pi(m) = -1 + \sum_{j=1}^{m} F(j).$$

Willans drückte $\pi(m)$ auch so aus:

$$\pi(m) = \sum_{j=2}^{m} H(j) \quad \text{für } m = 2, 3, \ldots,$$

wobei

$$H(j) = \frac{\sin^2 \pi \dfrac{\big((j-1)!\big)^2}{j}}{\sin^2 \dfrac{\pi}{j}}.$$

Mináč gab alternativ den folgenden, unveröffentlichten Ausdruck an, der weder Sinus noch Kosinus enthält:

$$\pi(m) = \sum_{j=2}^{m} \left[\frac{(j-1)! + 1}{j} - \left[\frac{(j-1)!}{j}\right]\right].$$

**Beweis.** Der Beweis von Minácˇs Formel ist recht einfach. Da er nirgendwo sonst veröffentlicht ist, wird er hier gezeigt.

Zunächst eine Bemerkung: Wenn $n \neq 4$ keine Primzahl ist, dann wird $(n-1)!$ von $n$ geteilt. Denn $n$ ist entweder gleich einem Produkt $n = ab$ mit $2 \leq a, b \leq n-1$ und $a \neq b$, oder $n = p^2 \neq 4$. Im ersten Fall teilt $n$ die Fakultät $(n-1)!$; im zweiten Fall gilt $2 < p \leq n-1 = p^2-1$, also $2p \leq p^2 - 1$, und $n$ teilt $2p^2 = p \times 2p$, das wiederum Teiler von $(n-1)!$ ist.

Für jedes prime $j$ gilt nach dem Satz von Wilson, dass $(j-1)!+1 = kj$ (wobei $k$ eine ganze Zahl ist), also

$$\left[\frac{(j-1)!+1}{j} - \left[\frac{(j-1)!}{j}\right]\right] = \left[k - \left[k - \frac{1}{j}\right]\right] = 1.$$

Falls $j$ keine Primzahl ist und $j \geq 6$, dann folgt aus obiger Bemerkung, dass $(j-1)! = kj$ (mit einer ganzen Zahl $k$). Daher

$$\left[\frac{(j-1)!+1}{j} - \left[\frac{(j-1)!}{j}\right]\right] = \left[k + \frac{1}{j} - k\right] = 0.$$

Schließlich, wenn $j = 4$, dann

$$\left[\frac{3!+1}{4} - \left[\frac{3!}{4}\right]\right] = 0.$$

Dies genügt für den Beweis der Formel für $\pi(m)$. □

Unter Verwendung der obigen Bezeichnung gab Willans die folgende Formel für die $n$-te Primzahl an:

$$p_n = 1 + \sum_{m=1}^{2^n} \left[\left[\frac{n}{\sum_{j=1}^{m} F(j)}\right]^{1/n}\right]$$

oder durch die Primzahlfunktion ausgedrückt,

$$p_n = 1 + \sum_{m=1}^{2^n} \left[\left[\frac{n}{1+\pi(m)}\right]^{1/n}\right].$$

Das verwandte Problem, eine Primzahl $q$ durch die unmittelbar vorangegangene Primzahl $p$ auszudrücken, löste Willans so:

$$q = 1 + p + F'(p+1) + F'(p+1)F'(p+2) + \cdots + \prod_{j=1}^{p} F'(p+j),$$

wobei $F'(j) = 1 - F(j)$ und $F(j)$ wie oben definiert ist.

Eine andere Formel für die kleinste Primzahl, die direkt auf ein $m \geq 2$ folgt, fand Ernvall unter Verwendung von Bertrands Postulat (noch als Student, 1975 veröffentlicht): Es sei

$$d = \mathrm{ggT}((m!)^{m!} - 1, (2m)!),$$

sowie

$$t = \frac{d^d}{\mathrm{ggT}(d^d, d!)},$$

und $a$ sei die eindeutig bestimmte ganze Zahl, für die $d^a$ Teiler von $t$ ist, aber $t$ nicht von $d^{a+1}$ geteilt wird. Dann ist die kleinste auf $m$ folgende Primzahl

$$p = \frac{d}{\mathrm{ggT}(t/d^a, d)}\,.$$

Wenn man $m = p_{n-1}$ wählt, ergibt dies eine Formel für $p_n$.

Ungeachtet der Tatsache, dass diese Formeln keinen praktischen Wert besitzen, neige ich dazu zu denken, dass sie für Logiker durchaus relevant sind, um sich klarzumachen, wie verschiedene Bereiche der Arithmetik aus unterschiedlichen Axiomatisierungen oder Teilen von Peanos Arithmetik ableitbar sind.

Gandhi fand 1971 eine Formel für die $n$-te Primzahl $p_n$. Um sie zu erläutern, benötige ich eine der wichtigsten arithmetischen Funktionen, die *Möbius-Funktion*. Sie ist wie folgt definiert:

$$\begin{cases} \mu(1) = 1, \\ \mu(n) = (-1)^r, \text{ falls } n \text{ das Produkt } r \text{ verschiedener Primzahlen ist}, \\ \mu(n) = 0, \text{ falls } n \text{ vom Quadrat einer Primzahl geteilt wird.} \end{cases}$$

Es sei $P_{n-1} = p_1 p_2 \cdots p_{n-1}$. Gandhi zeigte:

$$p_n = \left[1 - \frac{1}{\log 2} \log\left(-\frac{1}{2} + \sum_{d|P_{n-1}} \frac{\mu(d)}{2^d - 1}\right)\right],$$

oder äquivalent dazu: $p_n$ ist die einzige ganze Zahl mit

$$1 < 2^{p_n}\left(-\frac{1}{2} + \sum_{d|P_{n-1}} \frac{\mu(d)}{2^d - 1}\right) < 2.$$

Der folgende einfache Beweis stammt von Vanden Eynden aus dem Jahre 1972.

**Beweis.** Der Einfachheit halber sei $Q = P_{n-1}$, $p_n = p$ und

$$S = \sum_{d|Q} \frac{\mu(d)}{2^d - 1}\,.$$

Somit ist

$$(2^Q - 1)S = \sum_{d|Q} \mu(d) \frac{2^Q - 1}{2^d - 1} = \sum_{d|Q} \mu(d)\big(1 + 2^d + 2^{2d} + \cdots + 2^{Q-d}\big).$$

Für $0 \le t < Q$ taucht der Term $\mu(d)2^t$ genau dann auf, wenn $\mathrm{ggT}(t, Q)$ von $d$ geteilt wird. Also ist der Koeffizient von $2^t$ in der letzten Summe gleich $\sum_{d|\mathrm{ggT}(t,Q)} \mu(d)$, insbesondere $\sum_{d|Q} \mu(d)$ für $t = 0$.

Es ist jedoch einfach zu zeigen (und wohl bekannt), dass für jedes $m \ge 1$ gilt:

$$\sum_{d|m} \mu(d) = \begin{cases} 1 & \text{wenn } m = 1, \\ 0 & \text{wenn } m > 1. \end{cases}$$

Es bezeichne nun $\sum'_{0<t<Q}$ die Summe über alle $t$ mit $0 < t < Q$ und $\mathrm{ggT}(t, Q) = 1$. Damit erhält man $(2^Q - 1)S = \sum'_{0<t<Q} 2^t$; der größte Index $t$ in dieser Summation ist $t = Q - 1$. Es folgt, dass

$$2(2^Q - 1)\left(-\frac{1}{2} + S\right) = -(2^Q - 1) + \sum_{0<t<Q}{}' 2^{t+1} = 1 + \sum_{0<t<Q-1}{}' 2^{t+1}.$$

Wenn $2 \le j < p_n = p$, dann gibt es eine Primzahl $q$ derart, dass $q < p_n = p$ (also $q \mid Q$) und $q \mid Q - j$. Daher erfüllt jeder Index $t$ in obiger Summe $0 < t \le Q - p$. Somit ist

$$\frac{2^{Q-p+1}}{2 \times 2^Q} < -\frac{1}{2} + S = \frac{1 + \sum_{0<t\le Q-p}{}' 2^{t+1}}{2(2^Q - 1)} < \frac{2^{Q-p+2}}{2 \times 2^Q}\,,$$

wobei die Ungleichungen leicht zu erhalten sind.

Nach Multiplikation mit $2^p$ ergibt sich daraus

$$1 < 2^p \left(-\frac{1}{2} + S\right) < 2. \qquad \square$$

Golomb fand 1974 einen anderen, sehr aufschlussreichen Beweis. Seine Beschreibung erfolgt aus der Sicht des Eratosthenes-Siebs (siehe Kapitel 2, Abschnitt I), angewendet auf die Binärdarstellung von 1.

Jeder positiven Zahl $n$ sei eine Wahrscheinlichkeit oder ein Gewicht $W(n) = 2^{-n}$ zugewiesen. Offensichtlich gilt $\sum_{n=1}^{\infty} W(n) = 1$.

Mit dieser Zuordnung ergibt sich für die Wahrscheinlichkeit, dass eine zufällig gewählte Zahl ein Vielfaches einer gegebenen Zahl $d \geq 1$ ist, der Wert

$$M(d) = \sum_{n=1}^{\infty} W(nd) = \sum_{n=1}^{\infty} 2^{-nd} = \frac{1}{2^d - 1}.$$

Wie man leicht nachprüfen kann, beträgt die Wahrscheinlichkeit, dass eine zufällig gewählte Zahl zu einer vorgegebenen Zahl $m \geq 1$ teilerfremd ist,

$$\begin{aligned} R(m) &= 1 - \sum_{p|m} M(p) + \sum_{pp'|m} M(pp') - \sum_{pp'p''|m} M(pp'p'') + \cdots \\ &= \sum_{d|m} \mu(d) M(d) = \sum_{d|m} \frac{\mu(d)}{2^d - 1}. \end{aligned}$$

Wie zuvor sei $Q = p_1 p_2 \cdots p_{n-1}$, somit ist

$$R(Q) = \sum_{d|Q} \frac{\mu(d)}{2^d - 1}.$$

Andererseits kann man mit obiger Zuordnung $R(Q)$ direkt durch

$$R(Q) = \sum_{\mathrm{ggT}(m,Q)=1} W(m) = \frac{1}{2} + \frac{1}{2^{p_n}} + \frac{1}{2^{p_{n+1}}} + \alpha,$$

angeben, wobei $\alpha$ die Summe der Kehrwerte einiger höherer Potenzen von 2 ist. Somit ist

$$R(Q) - \frac{1}{2} = \sum_{d|Q} \frac{\mu(d)}{2^d - 1} - \frac{1}{2} = \frac{1}{2^{p_n}} + \frac{1}{2^{p_{n+1}}} + \alpha,$$

und daher

$$2^{p_n} \left( \sum_{d|Q} \frac{\mu(d)}{2^d - 1} - \frac{1}{2} \right) = 1 + \theta_n,$$

wobei $0 < \theta_n < 1$. Also ist $p_n$ die einzige ganze Zahl $m$, die

$$1 < 2^m \left( \sum_{d|Q} \frac{\mu(d)}{2^d - 1} - \frac{1}{2} \right) < 2$$

erfüllt, und dies ist einfach eine andere Darstellung von Gandhis Formel. Man beachte, dass $0 < \theta_n < \frac{1}{2}$, da $p_{n+1} \geq p_n + 2$.

In Binärschreibweise wird all dies leichter erkennbar. Sei nun $W(n) = 0{,}000\ldots1$ (mit der Ziffer 1 an der $n$-ten Stelle), also $\sum_{n=1}^{\infty} W(n) = 0{,}1111\ldots = 1$.

Für die geraden Zahlen ergibt sich

$$\sum_{n=1}^{\infty} W(2n) = 0{,}010101\ldots = \frac{1}{2^2-1} = \frac{1}{3}.$$

Durch Bildung der Differenz erhält man mit $P_1 = p_1 = 2$:

$$R(P_1) = \sum_{2|n} W(n) = 0{,}101010\ldots = 1 - \frac{1}{3}.$$

Subtraktion der Vielfachen von 3 und die korrigierende Addition der zweifach abgezogenen Vielfachen von 6 führt zu

$$Q(3) = 0{,}001001001\ldots = \frac{1}{2^3-1} = \frac{1}{7},$$
$$Q(6) = 0{,}000001000001\ldots = \frac{1}{2^6-1} = \frac{1}{63},$$

und mit $P_2 = p_1 p_2 = 6$,

$$R(P_2) = R(P_1) - Q(3) + Q(6) = 0{,}1000101000101000\ldots$$
$$= 1 - \frac{1}{3} - \frac{1}{7} + \frac{1}{63}.$$

In derselben Weise fortfahrend,

$$R(P_{n-1}) = 0{,}100\ldots0100\ldots0100\ldots = \frac{1}{2} + \frac{1}{2^{p_n}} + \frac{1}{2^{p_{n+1}}} + \alpha$$

und $$R(P_{n-1}) - \frac{1}{2} = 0{,}000\ldots010\ldots,$$

wobei die Ziffer 1 an Position $p_n$ auftritt.

## II Funktionen mit der Eigenschaft (b)

Im Jahre 1947 bewies Mills, dass es eine reelle Zahl $\theta > 0$ mit der Eigenschaft gibt, dass $[\theta^{c^n}]$ für jede natürliche Zahl $n$ eine Primzahl

ist. Weitere Untersuchungen ergaben, dass es für jedes $c > 2{,}106$ überabzählbar unendlich viele reelle Zahlen $\theta$ derart gibt, dass $[\theta^{c^n}]$ für jedes natürliche $n$ prim ist. Den kleinsten Wert von $\theta$ für den von Mills gewählten Fall $c = 3$ nennt man *Mills' Konstante*, die dazugehörigen Primzahlen $[\theta^{3^n}]$ die *Mills-Primzahlen*.

Unter Annahme der Riemannschen Vermutung (siehe Kapitel 4, Abschnitt I) ist es möglich, Mills' Konstante explizit zu bestimmen. Caldwell & Cheng (2005) berechneten die Konstante $\theta = 1{,}3063778838\ldots$ auf 6850 Stellen und ermittelten die Mills-Primzahlen $[\theta^{3^n}]$ für $n = 1, 2, \ldots, 10$. Die Zahl $[\theta^{3^{10}}]$ selber hat 6854 Ziffern.

Die voraussichtlich nächsten Zahlen der Folge wurden von P. Carmody als Quasiprimzahlen mit 20562 und 61684 Ziffern ermittelt. Mittlerweile konnte $[\theta^{3^{11}}]$ als Primzahl bestätigt werden; siehe den Rekord für das vernetzte ECPP-Verfahren in Kapitel 2, Abschnitt XI, B, wo auch eine formelmäßige Darstellung dieser Zahl zu finden ist.

In ähnlicher Weise ergibt

$$g(n) = \left\lfloor 2^{2^{2^{\cdot^{\cdot^{2^{\omega}}}}}} \right\rfloor$$

(eine Kette aus $n$ Exponenten) für jedes $n \geq 1$ eine Primzahl; hier bezeichnet $\omega$ eine Zahl, die etwa $1{,}9287800\ldots$ beträgt (siehe Wright, 1951).

Aufgrund der Tatsache, dass sowohl $\theta$ als auch $\omega$ nur annäherungsweise bekannt sind und die resultierenden Zahlen sehr schnell anwachsen, sind diese Formeln nur Kuriositäten. So ist $g(1) = 3$, $g(2) = 13$, $g(3) = 16381$, und hier hat bereits $g(4)$ mehr als 5000 Stellen. In der Literatur finden sich viele weitere, ähnliche Formeln, die aber genauso nutzlos sind; siehe Dudley (1969).

An dieser Stelle mag man sich fragen: Warum versucht man es anstelle dieser seltsamen Funktionen, welche Exponenten und die Gauß-Klammer enthalten, nicht mit irgendeinem Polynom mit ganzzahligen Koeffizienten? Der nächste Abschnitt wird diesem Thema gewidmet sein.

## III Primzahlerzeugende Polynome

Es folgt die Antwort auf die Frage am Ende des vorangegangenen Abschnitts:

*Für jedes nicht-konstante Polynom $f(X)$ mit ganzzahligen Koeffizienten in einer Unbekannten gibt es unendlich viele ganze Zahlen $n$, für die $|f(n)|$ keine Primzahl ist.*

**Beweis.** Man kann annehmen, dass es eine ganze Zahl $n_0 \geq 0$ gibt, so dass $|f(n_0)| = p$ eine Primzahl ist. Da das Polynom nicht konstant ist, folgt $\lim_{x\to\infty} |f(x)| = \infty$. Also gibt es $n_1 > n_0$, so dass für $n \geq n_1$, $|f(n)| > p$. Für jedes $h$ mit $n_0 + ph \geq n_1$ wird $f(n_0 + ph) = f(n_0)$ + (Vielfaches von $p$) = (Vielfaches von $p$). Da $|f(n_0 + ph)| > p$, muss $|f(n_0 + ph)|$ zerlegbar sein. □

Der obige Satz stammt aus einem Brief von Goldbach an Euler vom 28. September 1743.

Da es kein ganzzahliges Polynom in einer Unbekannten gibt, das für unseren Zweck tauglich ist, stellt sich die Frage, ob vielleicht ein Polynom in mehreren Unbekannten geeignet sein könnte. Wie der folgende Satz deutlich macht, ist dies erneut ausgeschlossen:

*Wenn $f(X_1, X_2, \ldots, X_m)$ ein Polynom mit komplexwertigen Koeffizienten in $m$ Unbekannten ist, so dass die Werte $|f(n_1, n_2, \ldots, n_m)|$ für frei wählbare natürliche Zahlen $n_1, n_2, \ldots, n_m$ Primzahlen sind, dann muss $f$ konstant sein.*

Obwohl der Funktionswert nichtkonstanter Polynome $f(X)$ mit ganzzahligen Koeffizienten für unendlich viele natürliche Zahlen (dem Betrage nach) zerlegbar ist, entdeckte Euler im Jahre 1772 ein Polynom $f(X)$, das eine lange Reihe von Primzahlen erzeugt.

Hier ist Eulers berühmtes Beispiel, welches er Bernoulli in einem Brief mitteilte: $f(X) = X^2 + X + 41$. Für $k = 0, 1, 2, 3, \ldots, 39$ sind sämtliche Werte Primzahlen, und zwar 41, 43, 47, 53, 61, 71, 83, 97, 113, 131, 151, 173, 197, 223, 251, 281, 313, 347, 383, 421, 461, 503, 547, 593, 641, 691, 743, 797, 853, 911, 971, 1033, 1097, 1163, 1231, 1301, 1373, 1447, 1523, 1601. Der Wert für $k = 40$ ist $1681 = 41^2$.

Dieses Beispiel begründete neue Entwicklungen:

(1) Auf einigermaßen systematische Weise lineare, quadratische oder höhergradige Polynome $f(X)$ zu finden, so dass für möglichst großes $k > 0$ alle $|f(0)|, |f(1)|, \ldots, |f(k)|$ Primzahlen sind.

(2) Polynome zu bestimmen, die betragsmäßig so viele Primzahlwerte wie möglich annehmen (nicht notwendigerweise für aufeinander folgende Argumente).

Ich werde zuerst lineare Polynome betrachten. Der Fall der quadratischen Polynome ist eng mit der Arithmetik quadratischer Zahlkörper verbunden. Es bietet sich daher an, diesem Thema einen eigenen Unterabschnitt zu widmen. Über Polynome höheren Grades ist sehr wenig bekannt; siehe Kapitel 6, Abschnitt II.

## A Primzahlwerte linearer Polynome

Es sei $f(X) = dX + q$ mit $d > 1$, $q > 1$, $\mathrm{ggT}(d, q) = 1$. Mit $f(0)$ ist auch $q$ eine Primzahl. Ferner ist $f(q)$ nicht prim. Daher kann es für lineare Polynome höchstens $q$ aufeinander folgende Argumente geben, die Primzahlwerte liefern. Dies führt zu folgendem offenen Problem: Ist die Aussage richtig, dass es für jede Primzahl $q$ eine ganze Zahl $d \geq 1$ gibt, so dass $q$, $d + q$, $2d + q, \ldots, (q - 1)d + q$ Primzahlen sind? Zum Beispiel ergibt

$q = 3$, $d = 2$ die Primzahlen 3, 5, 7;

$q = 5$, $d = 6$ die Primzahlen 5, 11, 17, 23, 29;

$q = 7$, $d = 150$ die Primzahlen 7, 157, 307, 457, 607, 757, 907.

Diese Frage ist so schwierig, dass ich nicht an einen Beweis in näherer Zukunft glaube. Lagrange hat gezeigt, dass falls ein solches $d$ existiert, es ein Vielfaches von $\prod_{p<q} p$ sein muss.

G. Löh entdeckte 1986 für $q = 11$ den kleinstmöglichen Wert $d = 1536160080$ und für $q = 13$ das kleinste $d = 9918821194590$.

### Rekord

Das kleinste $d$ für $q = 17$ wurde im November 2001 von P. Carmody gefunden und beträgt $d = 341976204789992332560$. Ein weiteres, beeindruckendes Rechenkunststück!

Ich werde mich diesen und anderen Fragen über Primzahlen in arithmetischen Folgen in Kapitel 4, Abschnitt V zuwenden.

## B Über quadratische Zahlkörper

Um die Probleme im Fall der quadratischen Polynome zu verstehen, ist es sinnvoll, zunächst die notwendigen Grundlagen über quadratische Zahlkörper zusammenzustellen. Da dieses Thema in einer Vielzahl von Büchern über Zahlentheorie behandelt wird, ist es nicht notwendig, einen speziellen Literaturhinweis zu geben. Die klassische Theorie der

binären quadratischen Formen, die Gauß in seinem berühmten Meisterwerk *Disquisitiones Arithmeticae* (1801) entwickelte, ist ebenso in vielen modernen Büchern zu finden, so etwa in Flath (1989) und in einem langen Kapitel meines eigenen Buches *My Numbers, My Friends* (2000, deutsche Übersetzung 2009). An dieser Stelle soll nur erwähnt werden, was später benötigt wird.

Es sei $d \neq 0, 1$ eine positive oder negative quadratfreie Zahl. Die zugehörige (fundamentale) *Diskriminante* ist

$$\Delta = \begin{cases} d & \text{falls} \quad d \equiv 1 \pmod 4, \\ 4d & \text{falls} \quad d \equiv 2 \text{ oder } 3 \pmod 4. \end{cases}$$

Dann ist $\mathbb{Q}(\sqrt{d}) = \mathbb{Q}(\sqrt{\Delta})$ der zugehörige quadratische Zahlkörper. Er besteht aus allen Zahlen $r + s\sqrt{d}$, wobei $r, s \in \mathbb{Q}$. Im Falle $d > 0$ sind die Zahlen $r + s\sqrt{d}$ reell und man spricht von einem *reell-quadratischen Zahlkörper*. Wenn $d < 0$, heißt $\mathbb{Q}(\sqrt{d})$ *imaginär-quadratischer Zahlkörper*.

Jedes Element $\alpha$ von $\mathbb{Q}(\sqrt{d})$ ist eine Wurzel eines Polynoms $f(X) \in \mathbb{Q}[X]$. $f(X)$ hat den Grad 2, wenn $\alpha$ nicht in $\mathbb{Q}$ liegt, und natürlich den Grad 1 für $\alpha \in \mathbb{Q}$, wobei der Leitkoeffizient gleich 1 ist. Wenn jeder Koeffizient von $f(X)$ in $\mathbb{Z}$ liegt, nennt man $\alpha$ eine *ganze algebraische Zahl* von $\mathbb{Q}(\sqrt{d})$. Die Menge $A$ der ganzen algebraischen Zahlen bildet einen Unterring von $\mathbb{Q}(\sqrt{d})$. Die Elemente von $A$ lassen sich einfach charakterisieren:

> Wenn $d \equiv 1 \pmod 4$, dann haben die Elemente von $A$ die Form $(m + n\sqrt{d})/2$, wobei $m, n$ in $\mathbb{Z}$ liegen und die gleiche Parität haben.
>
> Wenn $d \equiv 2$ oder $3 \pmod 4$, dann haben die Elemente von $A$ die Form $m + n\sqrt{d}$, wobei $m, n$ in $\mathbb{Z}$ liegen.

Für jedes $n \geq 1$ und $\alpha_1, \alpha_2, \ldots, \alpha_n$ aus $\mathbb{Q}(\sqrt{d})$ heißt die Menge aller Elemente der Form $\sum_{i=1}^{n} \gamma_i \alpha_i$, wobei $\gamma_1, \gamma_2, \ldots, \gamma_n$ in $A$ liegen, das von $\alpha_1, \alpha_2, \ldots, \alpha_n$ erzeugte *gebrochene Ideal*. Wenn $I$ ein gebrochenes Ideal ist, dann gilt $I + I \subseteq I$ und $AI \subseteq I$. Unter den gebrochenen Idealen befindet sich für jedes $\alpha$ aus $\mathbb{Q}(\sqrt{d})$ das *gebrochene Hauptideal* $A\alpha$. Das Produkt $IJ$ zweier gebrochener Ideale ist nach Definition das gebrochene Ideal, das aus der Menge aller endlichen Summen $\sum_{i=1}^{n} \alpha_i \beta_i$ besteht, wobei $\alpha_i$ aus $I$ und $\beta_i$ aus $J$ für alle $i = 1, 2, \ldots, n$ und alle $n \geq 0$. Unter dieser Multiplikation bilden die gebrochenen Ideale ungleich dem Nullideal eine abelsche Gruppe, und die vom Nullideal verschiedenen, gebrochenen Hauptideale sind eine Untergruppe davon.

Gauß bewies (in anderen Worten gleicher Bedeutung), dass der Quotient aus der Gruppe der nicht-verschwindenden gebrochenen Ideale und der Untergruppe der vom Nullideal verschiedenen gebrochenen Hauptideale eine endliche abelsche Gruppe ist. Diese Gruppe wird mit $\mathrm{Cl}_d$ (oder auch mit $\mathrm{Cl}_\Delta$) bezeichnet und heißt *Klassengruppe* von $\mathbb{Q}(\sqrt{d})$ (oder auch von $\Delta$). Die Anzahl der Elemente dieser Gruppe ist $h_d$ (oder auch $h_\Delta$), und man nennt sie *Klassenzahl* von $\mathbb{Q}(\sqrt{d})$ (oder auch von $\Delta$). Eine Klassenzahl gleich 1 ist gleichbedeutend damit, dass jedes gebrochene Ideal ein Hauptideal ist.

Wenn $\alpha, \beta$ in $\mathbb{Q}(\sqrt{d})$ liegen, dann *teilt* $\alpha$ nach Definition $\beta$, falls es ein $\gamma$ in $A$ gibt, so dass $\alpha\gamma = \beta$. Elemente von $A$, welche die 1 teilen, heißen *Einheiten* von $A$. Ein von Null verschiedenes Element $\pi \in A$, das keine Einheit ist, wird *algebraische Primzahl* genannt, falls die folgende Bedingung erfüllt ist: Wenn $\alpha, \beta$ in $A$ liegen und $\alpha\beta = \pi$, dann ist $\alpha$ oder $\beta$ eine Einheit.

Es stellt sich heraus, dass $h_d = 1$ genau dann erfüllt ist, wenn der Fundamentalsatz in $\mathbb{Q}(\sqrt{d})$ gilt: Jede ganze algebraische Zahl ungleich Null lässt sich in eindeutiger Weise (bis auf Einheiten und Reihenfolge der Faktoren) als Produkt von algebraischen Primzahlen darstellen.

Der *Exponent* $e_d$ der Klassengruppe $\mathrm{Cl}_d$ ist definiert als das Maximum der Ordnungen der Klassen in der Gruppe $\mathrm{Cl}_d$. Dann wird $e_d$ von allen Ordnungen der Klassen geteilt. Offensichtlich gilt $e_d = 1$ genau dann, wenn $h_d = 1$. Des Weiteren ist $e_d$ eine Zweierpotenz genau dann, wenn dies auch auf $h_d$ zutrifft.

Die von Gauß entwickelte Geschlechtertheorie binärer quadratischer Formen führt zu einem präziseren Ergebnis: Es sei

$$h_d^* = \begin{cases} h_d & \text{falls} \quad d < 0, \\ 2h_d & \text{falls} \quad d > 0. \end{cases}$$

Sei $N + 1$ die Anzahl der verschiedenen Primfaktoren von $\Delta$. Gauß zeigte, dass $2^N$ die Zahl $h_d^*$ teilt. Ferner ist $h_d = 2^N$, falls $d < 0$ und $e_d = 1$ oder 2.

Es folgt $N = 0$, wenn $h_d = 1$, so dass $d = -1, -2$ oder $d = -p$, wobei $p$ eine Primzahl ist, die $p \equiv 3 \pmod 4$ erfüllt. Wenn $h_d = 2$, dann $N = 1$. Für $d$ gibt es nun drei mögliche Typen:

(I) $d = -2p$, wobei $p$ eine beliebige ungerade Primzahl ist;

(II) $d = -p$, wobei $p$ prim ist und $p \equiv 1 \pmod 4$ gilt;

(III) $d = -pq$, wobei $p < q$ Primzahlen sind, die $pq \equiv 3 \pmod 4$ erfüllen.

Die binären quadratischen Formen mit gegebener Diskriminante bilden zudem eine endliche abelsche Gruppe (unter der Komposition von Formen); diese Gruppe steht in eindeutiger Weise in Zusammenhang mit der Gruppe $\mathrm{Cl}_\Delta$, was hier nicht weiter erklärt wird. Die Formen lassen sich in Geschlechter einteilen, wobei jedes Geschlecht eine bestimmte Anzahl von Klassen enthält. Aus der Geschlechtertheorie folgt, dass die folgenden beiden Aussagen für $d < 0$ äquivalent sind:

(1) Die Klassengruppe binärer quadratischer Formen mit Diskriminante $d$ hat den Exponenten 1 oder 2.

(2) Jedes Geschlecht der Klassengruppe binärer quadratischer Formen mit Gruppendiskriminante $d$ besteht nur aus einer Klasse.

Diese letzte Eigenschaft erlaubt eine Interpretation hinsichtlich Eulers „numeri idonei“, die nun beschrieben werden soll.

Es sei $n \geq 1$ und $E(n)$ die Menge der ungeraden natürlichen Zahlen $q$, so dass es mindestens ein Paar ganzer Zahlen $(x, y)$ mit $x \geq 0$, $y \geq 0$, $q = x^2 + ny^2$ und $\mathrm{ggT}(x, ny) = 1$ gibt. Die Zahl $n$ heißt *numerus idoneus* (oder auch *geeignete Zahl*), wenn $E(n)$ keine zerlegbare Zahl enthält. Beispielsweise folgt aus Fermats Studien über Zahlen der Form $x^2 + y^2$, dass $n = 1$ ein numerus idoneus ist. Gauß bewies, dass mit $d < 0$ der Exponent $e_d$ genau dann die Werte 1 oder 2 annimmt, wenn es sich bei $-d$ um ein numerus idoneus handelt. Euler gab die folgenden 65 numeri idonei an:

> 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 12, 13, 15, 16, 18, 21, 22, 24, 25, 28, 30, 33, 37, 40, 42, 45, 48, 57, 58, 60, 70, 72, 78, 85, 88, 93, 102, 105, 112, 120, 130, 133, 165, 168, 177, 190, 210, 232, 240, 253, 273, 280, 312, 330, 345, 357, 385, 408, 462, 520,760, 840, 1320, 1365, 1848.

Die vollständige Bestimmung aller numeri idonei ist nach wie vor ein offenes Problem. Es konnte gezeigt werden, dass neben den oben aufgeführten Zahlen höchstens noch eine weitere existieren kann. Man glaubt jedoch, dass es keine weitere mehr gibt und die Liste somit komplett ist.

Ich werde mich nun dem Problem der Bestimmung von imaginärquadratischen Zahlkörpern $\mathbb{Q}(\sqrt{d})$ mit vorgegebenem $h_d$ zuwenden.

**(1)** Gauß zeigte, dass $h_d = 1$ für $d = -1, -2, -3, -7, -11, -19, -43, -67, -163$; er vermutete zudem in Artikel 303, dass dies die einzig möglichen ganzen Zahlen $d < 0$ sind, für die $\mathbb{Q}(\sqrt{d})$ den Wert

$h_d = 1$ hat. (Um die Wahrheit zu sagen, bezog sich Gauß nicht auf imaginär-quadratische Zahlkörper, sondern vielmehr auf negative Diskriminanten, die nur eine Klasse binärer quadratischer Formen haben.)

In einem klassischen Artikel bewiesen Heilbronn & Linfoot 1934, dass es höchstens eine weitere ganze Zahl $d < 0$ geben kann, für die $\mathbb{Q}(\sqrt{d})$ die Klassenzahl 1 hat. Lehmer (1933) zeigte, dass wenn es ein solches $d$ gibt, sein Absolutwert sehr groß sein muss: $|d| > 5 \times 10^9$. Im Jahre 1952 bewies Heegner, dass kein solches $d$ existiert, allerdings waren einige Schritte im Beweis unklar, wenn nicht gar falsch.

Baker erzielte 1966 mit seiner Methode expliziter unterer Schranken für Linearformen von drei Logarithmen dasselbe Ergebnis; dies ist auch in seinem Artikel von 1971 erwähnt. Ohne Kenntnis von Heegners Ergebnissen bewies Stark (1967) etwa zur gleichen Zeit mit Hilfe ähnlicher Ideen, jedoch elliptische modulare Funktionen betreffend, dass es keine weitere Zahl $d$ mit der geforderten Eigenschaft gibt. Damit waren alle imaginär-quadratischen Zahlkörper mit $h_d = 1$ bestimmt.

Man könnte es als Ernüchterung ansehen, als es Deuring 1968 gelang, Heegners Beweis zu entwirren, und Stark (1969) zudem bewies, dass Gelfond & Linnik 1949 den zu dieser Zeit bereits bekannten Satz über die lineare Unabhängigkeit von nur zwei Logarithmen hätten verwenden können, um zum selben Resultat zu gelangen. Die in diesen Beweisen enthaltenen technischen Details liegen außerhalb des Rahmens dieses Buchs.

**(2)** Mit Hilfe seiner Methode unterer Schranken für Linearformen in Logarithmen bewies Baker (1971), dass sich alle imaginär-quadratischen Zahlkörper mit Klassenzahl $h_d = 2$ effektiv bestimmen lassen, er gab allerdings keine explizite Schranke für die Diskriminante an. Im selben Band derselben Zeitschrift berechnete Stark, dass wenn $h_d = 2$, dann $|d| < 10^{1100}$. Montgomery & Weinberger zeigten 1974, dass $h_d$ für $10^{12} \leq |d| \leq 10^{1200}$ nicht gleich 2 sein kann. Zuvor hatte Lehmer verifiziert, dass $h_d = 2$ im Bereich von $10^6 \leq |d| \leq 10^{12}$ nicht auftritt.

Zusammenfassend lässt sich sagen: Wenn $d < 0$ und $h_d = 2$, dann ist $d = -5, -6, -10, -13, -15, -22, -35, -37, -51, -58, -91, -115, -123, -187, -235, -267, -403, -427$. Alles in allem 18 Diskriminanten.

Die Bestimmung aller $d < 0$ mit $e_d = 2$ ist noch unvollständig. Weinberger ermittelte 1973 eine explizite obere Schranke für alle $|d|$ mit $e_d = 2$.

**(3)** Hinsichtlich beliebiger Werte von $h_d$ vermutete Gauß, dass es für jedes $n \geq 1$ höchstens endlich viele Körper $\mathbb{Q}(\sqrt{d})$ mit $d < 0$ gibt, für die $h_d = n$ ist. Diese Vermutung über die Klassenzahl von imaginär-quadratischen Zahlkörpern wurde von Gross & Zagier (1983, 1986) bewiesen. Der Beweis setzte die vorherige bahnbrechende Arbeit von Goldfeld (1977) voraus und folgt aus diesem genaueren Ergebnis:

*Für jedes $\varepsilon > 0$ gibt es ein effektiv berechenbares $C = C(\varepsilon) > 0$, so dass für alle $d < 0$, $h_d > C(\log |d|)^{1-\varepsilon}$.*

Das Studium der Klassenzahl reell-quadratischer Zahlkörper ist komplizierter. Es sei an dieser Stelle nur die Vermutung von Gauß erwähnt, dass es unendlich viele reell-quadratische Zahlkörper mit Klassenzahl $h_d = 1$ gibt. Es wäre eine Glanzleistung, diese Vermutung zu beweisen.

## C Primzahlerzeugende quadratische Polynome

Ein quadratisches Polynom $f(X) = aX^2+bX+c$ (mit $a \geq 1, c \geq 1$), für das es ein $l > 2$ derart gibt, dass $f(0), f(1), \ldots, f(l-1)$ sämtlich Primzahlen sind, nennt man *primzahlerzeugendes Polynom*. Wie zu Beginn dieses Abschnitts erwähnt, ist $l$ beschränkt; den maximal möglichen Wert von $l$ nennt man *primzahlerzeugende Länge* von $f(X)$.

In diesem Unterabschnitt werden wir sehen, dass es einen überraschenden Zusammenhang zwischen primzahlerzeugenden Polynomen und Klassenzahlen quadratischer Körper gibt. Es gibt jedoch noch eine weitere Verbindung völlig anderer Art, die sich auf die Primzahlmehrlingsvermutung bezieht. Dies wird in Kapitel 4, Abschnitt IV gezeigt.

Wir betrachten die Polynome $f_q(X) = X^2 + X + q$, wobei $q$ eine Primzahl ist. Man beachte, dass $f_q(q-1) = q^2$. Rabinowitsch bewies 1912 die Äquivalenz folgender Aussagen:

(1) $f_q(X)$ besitzt eine primzahlerzeugende Länge von $q - 1$.

(2) Der imaginär-quadratische Zahlkörper $\mathbb{Q}(\sqrt{1-4q})$ hat Klassenzahl 1.

Im selben Jahr zeigte Frobenius, dass (1) aus (2) folgt. Lehmer bewies 1936 ein weiteres Mal, dass (2) Folge von (1) ist. In jüngerer Zeit gelangten Szekeres (1974) und Ayoub & Chowla (1981) wiederum zur Implikation (2) $\Rightarrow$ (1). Eine detaillierte Diskussion dieses Ergebnisses findet sich in Cohns Buch (1962) oder auch in meinem eigenen Artikel (1988), wo sämtliche Rechnungen und Beweise ausführlich und fast von Grund auf dargestellt sind.

Die vollständige Bestimmung aller imaginär-quadratischer Zahlkörper mit Klassenzahl 1 liefert die möglichen Werte von $q$. Tatsächlich sind unter den neun unter (1) aufgelisteten Werten von $d$ alle außer $-1$ und $-2$ kongruent zu 1 modulo 4, für die verbleibenden ergibt $(1-d)/4$ mit Ausnahme von $d=-3$ eine Primzahl $q$. Die so gewonnenen Primzahlen sind $q=2,\,3,\,5,\,11,\,17,\,41$. Nur für genau diese hat das Polynom $f_q(X)$ eine primzahlerzeugende Länge von $q-1$. Daraus ergibt sich folgender Rekord, der niemals übertroffen werden wird.

### Rekord

Das bestmögliche Resultat für Polynome des Typs $X^2+X+q$ ist bereits das von Euler: $q=41$ ist die größte Primzahl derart, dass das Polynom für $k=0,1,\ldots,q-2$ Primzahlwerte annimmt.

Es gibt eine Vielzahl quadratischer Polynome mit einer großen primzahlerzeugenden Länge. Legendre erwähnte, dass die Polynome $2X^2+q$ für $q=3,\,5,\,11,\,29$ die maximal mögliche primzahlerzeugende Länge $q$ besitzen. A. Lévy stellte 1914 fest, dass $3X^2+3X+23$ eine primzahlerzeugende Länge von 22 hat. Van der Pol & Speziali bemerkten 1951, dass die primzahlerzeugende Länge von $6X^2+6X+31$ gleich 29 ist. Diese Beispiele veranschaulichen bereits das nun folgende Ergebnis.

Gemäß der drei möglichen Typen imaginär-quadratischer Zahlkörper mit Klassenzahl 2 sei

$$f_{\mathrm{I}}(X)=2X^2+p,\ \text{falls } p \text{ eine ungerade Primzahl ist;}$$

$$f_{\mathrm{II}}(X)=2X^2+2X+(p+1)/2,\ \text{falls } p \text{ eine Primzahl ist und } p\equiv 1 \pmod 4;$$

$$f_{\mathrm{III}}(X)=pX^2+pX+(p+q)/4,\ \text{falls } p<q \text{ Primzahlen sind und } pq\equiv 3 \pmod 4.$$

Man beachte, dass $f_{\mathrm{I}}(p)$, $f_{\mathrm{II}}((p-1)/2)$ und $f_{\mathrm{III}}((p+q)/4-1)$ zerlegbar sind. Das folgende Resultat geht in dieser Form auf Louboutin (1991) zurück; siehe auch Frobenius (1912) und Hendy (1974).

(I) $h_{-2p}=2$ genau dann, wenn $f_{\mathrm{I}}(X)$ eine primzahlerzeugende Länge gleich $p$ hat;

(II) $h_{-p}=2$ genau dann, wenn $f_{\mathrm{II}}(X)$ eine primzahlerzeugende Länge von $(p-1)/2$ hat;

(III) $h_{-pq} = 2$ genau dann, wenn $f_{\mathrm{III}}(X)$ eine primzahlerzeugende Länge von $(p+q)/4 - 1$ hat.

Durch Vergleich mit der Liste derjenigen $d < 0$, für die $h_d = 2$ ist, ergibt sich in den drei Fällen:

(I) $p = 3,\ 5,\ 11,\ 29$;

(II) $p = 5,\ 13,\ 37$;

(III) $(p,q) = (3,5),\ (3,17),\ (3,41),\ (3,89),\ (5,7),\ (5,23),\ (5,47),\ (7,13),\ (7,61),\ (11,17),\ (13,31)$.

Im selben Artikel von 1991 gelangt Louboutin zu den folgenden Charakterisierungen von Körpern mit negativer Diskriminante und Klassenzahl 4. Es sei $2 < q < p$, wobei $p$, $q$ Primzahlen sind. Dann ist

(1) $h_{-2pq} = 4$ genau dann, wenn $2qk^2 + p$ für alle $k = 0,\ 1, \ldots, p-1$ prim ist.

(2) Sei $pq \equiv 1 \pmod 4$. Dann $h_{-pq} = 4$ genau dann, wenn $(pq+1)/2$ eine Primzahl ist und für $k = 0,\ 1, \ldots, (p+q)/2-2$, $k \neq (p-1)/2$, $2qk^2 + 2qk + (p+q)/2$ prim wird.

Mollin entwickelte eine umfassendere Theorie zur Verbindung von imaginär-quadratischen Zahlkörpern mit Exponent 2 und speziellen primzahlerzeugenden Polynomen. Es sei $d \neq 0, 1$ eine quadratfreie negative ganze Zahl und $\Delta$ die zugehörige fundamentale Diskriminante. Seien $2 \leq q_1 < q_2 < \cdots < q_{N+1} = p$ die verschiedenen Primfaktoren von $\Delta$ und $q = \prod_{i=1}^{N} q_i$. Definiere für jedes $m \geq 1$ mit $m \mid q$ das folgende Polynom:

$$f_{\Delta,m}(X) = \begin{cases} mX^2 - \dfrac{\Delta}{4m} & \text{wenn } \ 4m \mid \Delta, \\ mX^2 + mX + \dfrac{m^2 - \Delta}{4m} & \text{wenn } \ 4m \nmid \Delta \end{cases}$$

(man beachte im letzteren Fall, dass $4m$ Teiler von $m^2 - \Delta$ ist). Sei $B_{\Delta,m} = [|\Delta|/4m]$. Es wird nun die folgende Bezeichnung verwendet: wenn $n = \prod_{i=1}^{k} p_i^{e_i}$ (wobei $p_i$ die unterschiedlichen Primfaktoren sind), dann $\nu(n) = \sum_{i=1}^{k} e_i$. Sei

$$\Omega(f_{\Delta,m}(X)) = \max\left\{\nu(f_{\Delta,m}(k)) \mid k = 0, 1, \ldots, B_{\Delta,m} - 1\right\}.$$

Mollin bewies (siehe sein Buch von 1996 oder seinen Übersichtsartikel von 1997): Mit obigen Bezeichnungsweisen und unter der Annahme, dass $\Delta < -4$, sind die folgenden Bedingungen äquivalent:

(1) $e_d \leq 2$.

(2) $h_d = 2^N$ und für jeden Teiler $m$ von $q$, $1 \leq m$, $\Omega(f_{\Delta,m}(X)) + \nu(m) - 1 = N$.

(3) $h_d = 2^N$ und es existiert ein Teiler $m$ von $q$, $1 \leq m$, so dass $\Omega(f_{\Delta,m}(X)) + \nu(m) - 1 = N$.

Nach Wahl von $m = q$ folgt, dass $f_{\Delta,q}(k)$ für $k = 0, 1, \ldots, B_{\Delta,q} - 1$ eine Primzahl ist. Es ist leicht zu verifizieren, dass die an früherer Stelle erwähnten Resultate von Rabinowitsch und Louboutin Spezialfälle hiervon sind.

Sasaki bewies 1986: $h_d = 2$ gilt genau dann, wenn $\Omega(f_{\Delta,1}(X)) = 2$. Dieses Resultat lässt sich aus Mollins Satz (1996) ableiten.

Es ist abermals leicht nachzuvollziehen, dass sich das primzahlerzeugende Verhalten der früher erwähnten Polynome anhand von Mollins Satz erklären lässt: $d = -2 \times 29$, $\Delta = -8 \times 29$, $N = 1$; $-d$ ist ein numerus idoneus, also $e_d \leq 2$, $m = 2$, $\nu(m) = 1$, $B_{\Delta,m} = 29$, $f_{\Delta,m}(X) = 2X^2 + 29$, also $\Omega(2X^2 + 29) = 1$ und daher ist $f_{\Delta,m}(k)$ für $k = 0, 1, \ldots, 28$ eine Primzahl.

Hoffentlich gelingt es Ihnen, in gleicher Weise das Verhalten der Polynome $3X^2 + 3X + 23$ und $6X^2 + 6X + 31$ zu erklären.

Bis hierher wurde nur der Fall negativer Diskriminanten betrachtet, es gibt jedoch eine ähnliche Theorie für Polynome mit positiver Diskriminante. Siehe zum Beispiel Louboutin (1990), Mollin (1996, 1996a), sowie Sasaki (1986a).

Durch den Einsatz von Computern fand man weitere primzahlerzeugende quadratische Polynome, die nicht durch irgendeine Theorie begründet sind.

### Rekord

Das von R. Ruby 1990 entdeckte quadratische Polynom $f(X) = 36X^2 - 810X + 2753$ erzeugt die zur Zeit längste Reihe von Primzahlen für aufeinander folgende Argumente, in diesem Fall für $X = 0, 1, \ldots, 44$.

Die Polynome $103X^2 - 3945X + 34381$ (von R. Ruby) und $47X^2 - 1701X + 10181$ (von G. Fung) ergeben im Absolutwert jeweils 43 Primzahlen.

Dress & Landreau (2003) fanden Polynome höheren Grades: $f(X) = 66x^3 + 83x^2 - 13735x + 30139$, welches 46 aufeinander folgende Primzahlwerte $|f(k)|$ für $k = -26$ bis $k = 19$ ergibt, sowie das Polynom

$f(X) = 16x^4 + 28x^3 - 1685x^2 - 23807x + 110647$, das Primzahlen $|f(k)|$ für $k = -23$ bis $k = 22$ erzeugt.

Wenn man für Polynome $f(X)$ auch rationale Koeffizienten zulässt, so dass aber immer ganzzahlige Funktionswerte $f(k)$ entstehen, dann ist der Rekordhalter

$$f(X) = \frac{1}{72}X^6 - \frac{5}{24}X^5 - \frac{1493}{72}X^4 + \frac{1027}{8}X^3 + \frac{100471}{18}X^2 - \frac{11971}{6}X - 57347.$$

Für alle ganzen Zahlen $k$ von $k = -42$ bis $k = 15$ ist $|f(k)|$ eine Primzahl. Also ergeben 58 aufeinander folgende ganzzahlige Argumente 58 Primzahlen als Werte des Polynoms. Dieser Rekord wurde von Dress und Landreau in einer Pressemitteilung vom April 2010 bekannt gegeben. Er wird wohl nicht leicht zu übertreffen sein.

## D Der Wettlauf um Primzahlwerte und Primteiler

### Der Wettlauf um Primzahlwerte

Die folgende Untersuchung hat viele Amateurmathematiker angezogen. Es sei $f(X)$ ein nicht-konstantes Polynom mit ganzzahligen Koeffizienten sowie $N \geq 1$ und

$$\pi^*_{f(X)}(N) = \#\{n \mid 0 \leq n \leq N,\ |f(n)| \text{ ist eine Primzahl}\}.$$

Man beachte, dass es sich dabei nicht notwendigerweise um verschiedene Primzahlen handeln muss.

Das Problem besteht darin, für gegebenes $N$ (normalerweise groß) und $d \geq 1$ ein Polynom $f(X)$ vom Grade $d$ zu finden, so dass $\pi^*_{f(X)}(N)$ maximal wird. Wenn man möchte, kann man die Suche auch auf normierte Polynome (das heißt mit Leitkoeffizient 1) oder auch normierte Polynome speziellen Typs einschränken.

Es gibt viele heiß umkämpfte Rekorde.

#### Rekorde

A. Für $N = 1000$ ergibt das quadratische Polynom $f(X) = 2X^2 - 1584X + 98621$, gefunden vom Amateurmathematiker S.M. Williams (Brief vom Oktober 1993), die maximale Anzahl von Primzahlwerten, nämlich $\pi^*_{f(X)}(1000) = 706$. Frühere Rekorde, ebenfalls von Williams, waren

$$f_1(X) = 2X^2 - 1904X + 42403,$$
$$f_2(X) = 2X^2 - 1800X - 5749,$$

mit $\pi^*_{f_1(X)}(1000) = 693$ beziehungsweise $\pi^*_{f_2(X)}(1000) = 686$.

B. Für $N = 1000$ und ausschließlich quadratische normierte Polynome ist der derzeitige Champion

$$g(X) = (X - 499)^2 + (X - 499) + 27941,$$

mit $\pi^*_{g(X)}(1000) = 669$, von N. Boston persönlich übermittelt.

Man beachte, dass die Menge $\{h(k) \mid 0 \le k \le 1000\}$ für $h(X) = X^2 + X + 27941$ genau 600 verschiedene Primzahlen enthält. Dies könnte ein Rekord des abgewandelten Wettkampfs (bis $N = 1000$) von quadratischen Polynomen mit verschiedenen Primzahlwerten bedeuten.

Karst fand 1973 das Polynom $f(X) = 2X^2 - 199$, das 597 Primzahlwerte ergibt. Demgegenüber erzeugt Eulers Polynom $X^2 + X + 41$ 582 Primzahlwerte.

Das Rennen zwischen diesen beiden berühmten Polynomen wurde auf viel höhere Schranken für $N$ ausgeweitet. In einer Nachricht vom Dezember 1998 teilte S.S. Gupta (der das Rechnen liebt) die folgenden Ergebnisse mit:

$$\pi^*_{2X^2-199}(10^7) = 2381779,$$
$$\pi^*_{X^2+X+41}(10^7) = 2208197.$$

Angesichts einer Vermutung von Hardy und Littlewood werde ich dieser Frage für Polynome $f(X) = X^2 + X + A$ in Kapitel 6, Abschnitt IV erneut nachgehen.

Im Alter von 78 Jahren fand M.L. Greenwood – ohne Verwendung eines Computers – die Polynome

$$h_1(X) = -4X^2 + 381X - 8524,$$
$$h_2(X) = -2X^2 + 185X - 31819,$$

die 50 gerade Werte und 48 verschiedene ungerade Primzahlwerte annehmen, wenn $k$ die Zahlen $0, 1, \ldots, 99$ durchläuft. Der Profi Boston schloss sich dem Amateur Greenwood an, zusammen fanden beide 1995 mit Hilfe von Computern das Polynom $f(X) = 41X^2 - 4641X + 88007$. Für $k = 0, 1, \ldots, 99$ nimmt es 90 verschiedene Primzahlwerte $f(k)$ an.

Das Rennen um kubische Polynome mit $N = 500$ (vergleichbar mit dem 500-Meilen-Rennen von Indianapolis) wurde von Goetgheluck (1989) initiiert. Der Sieger ist

$$f(X) = 2X^3 - 489X^2 + 39847X - 1084553.$$

Dieses Polynom erzeugt für $k \leq 500$ genau 267 Primzahlen. Der Leitkoeffizient musste bei diesem Wettkampf gleich 1 oder 2 sein, daneben gab es weitere Einschränkungen bezüglich der Größe der Koeffizienten.

Ich werde in Kapitel 6, Abschnitt III das umgekehrte Phänomen betrachten, bei dem Polynome für alle $n = 0, 1, 2, \ldots$ bis zu einem hohen $N$ zerlegbare Werte annehmen.

**Der Wettlauf um kleinste Primfaktoren**

Für eine ganze Zahl $m$ ungleich 0 bezeichne $P_0[m]$ den kleinsten Primfaktor von $m$. Wenn $f(X) = aX^2 + bX + c$ ein Polynom mit ganzzahligen Koeffizienten ist und ferner $a \geq 1$, $c \neq 0$, sei

$$P_0[f(X)] = \min\{P_0[f(k)] \mid k = 0, 1, 2, \ldots\}.$$

Darüber hinaus sei für $N \geq 1$

$$q_N = \min\{P_0[f(k)] \mid k = 0, 1, 2, \ldots, N\}.$$

Wegen $q_1 \geq q_2 \geq \ldots$, gibt es ein $N$, so dass $q_N < N$. Dann gilt $P_0[f(X)] = q_N$, was die Berechnung von $P_0[f(X)]$ ermöglicht: Denn wenn $p$ eine Primzahl mit $p < q_N$ ist und $p \mid f(M)$ für ein $M > N$, schreibe $M = dp + r$ mit $0 \leq r < p < q_N < N$. Aus $f(M) \equiv f(r) \pmod{p}$ folgt $p \mid f(r)$, so dass $p \geq q_N$, was der Annahme widerspricht.

Nun sei $f_A(X) = X^2 + X + A$ für $A \geq 1$. Man hat gezeigt, dass es für jede Primzahl $q$ ein $A < q\#$ gibt, so dass $P_0[f_A(X)] = q$. Das Ziel ist nun, den größten Wert für $P_0[f_A(X)]$ zu finden. Nebenbei bemerkt ist $P_0[f_{41}(X)] = 41$.

Rekord

Wenn man $A$ als prim voraussetzt und zudem fordert, dass $A$ der kleinste Wert ist, der $P_0[f_A(X)] = q$ erfüllt, dann ist

$$P_0[X^2 + X + 33239521957671707] = 257.$$

Dies wurde von P. Carmody 2001 entdeckt. Vorangegangene Rekorde von L. Rodríguez Torres stammten aus den Jahren 1996 beziehungsweise 1995:

$$P_0[X^2 + X + 67374467] = 107,$$
$$P_0[X^2 + X + 32188691] = 71.$$

Der größte bekannte Wert von $P_0[f_A(X)]$ für den Fall, dass $A$ prim, aber nicht notwendigerweise minimal ist, wurde von M.J. Jacobson und H.C. Williams 2002 unter Verwendung eines speziellen elektronischen Zahlensiebes gefunden, das in ihrem Artikel (2003) beschrieben ist. Für die 57-stellige Primzahl $A = 605069291083802407422281785816166476624287786946587507887$ ermittelten sie $P_0[f_A(X)] = 373$.

Wenn die Bedingung, dass $A$ prim sein soll, auch noch fallen gelassen wird, erreichten sie $P_0[f_A(X)] = 401$ für die 68-stellige Zahl $A = 47392132545934368303439248393872932657758235983472584357825592740917$ (ein Produkt aus sechs Primzahlen). Der vorherige Rekord stammte von Lukes, Patterson & Williams (1995), die nach intensiven Berechnungen fanden, dass

$$P_0[X^2 + X + 2457080965043150051] = 281.$$

# IV Funktionen mit der Eigenschaft (c)

Wir erinnern uns daran, dass Bedingung (c) erfordert, dass die Menge der Primzahlen mit der Menge der positiven Werte einer Funktion zusammenfällt. Überraschenderweise ist dies möglich, und es wurde als Nebenprodukt bei der Untersuchung von Hilberts zehntem Problem entdeckt. Die Ideen kommen aus der Logik und die Ergebnisse sind recht außergewöhnlich, auch wenn es für sie bis heute keine unmittelbare praktische Anwendung gibt.

Bei der nun folgenden Beschreibung verzichte ich auf technische Details, um mich nicht allzu sehr von den Primzahlen zu entfernen. An dieser Stelle muss ich mathematische Strenge und Intuition gegeneinander abwägen. Dabei hoffe ich auf den guten Willen des Lesers, meine Ausführungen in keiner Weise falsch zu verstehen. Denen, die auf die nun folgenden Ergebnisse neugierig geworden sind, empfehle ich den hübschen Artikel von Davis (1973).

Hilberts zehntes Problem fragt nach ganzzahligen Lösungen $(x_1, \ldots, x_n)$ von diophantischen Gleichungen $P(X_1, \ldots, X_n) = 0$, wobei $P$ irgendein Polynom mit ganzzahligen Koeffizienten und einer beliebigen Anzahl von Unbestimmten ist. Genauer gesagt geht es darum, einen Algorithmus zu finden, der über eine beliebige diophantische Gleichung aussagen kann, ob sie eine ganzzahlige Lösung besitzt.

Ein Algorithmus sollte als ein Entscheidungsverfahren verstanden werden, welches als Computerprogramm implementiert werden kann und in endlich vielen aufeinander folgenden Schritten eine Antwort „ja“

oder „nein“ liefert – in einer Vorgehensweise, die von Mathematikern als zulässig erachtet wird.

Beim Studium der Mengen $S$ von $n$-Tupeln $(x_1, \ldots, x_n)$ ganzer Zahlen ist der zentrale Begriff der folgende: $S$ heißt *diophantische Menge*, wenn es ein Polynom mit ganzzahligen Koeffizienten in Unbestimmten $X_1, \ldots, X_n$, $Y_1, \ldots, Y_m$ $(m \geq 0)$ gibt, so dass $(x_1, \ldots, x_n) \in S$ genau dann gilt, wenn es positive ganze Zahlen $y_1, \ldots, y_m$ gibt, die

$$P(x_1, \ldots, x_n, y_1, \ldots, y_m) = 0$$

erfüllen.

Zunächst die trivialen Beispiele. Jede endliche Menge $S$ von $n$-Tupeln positiver ganzer Zahlen ist diophantisch. Denn wenn $S$ aus den $n$-Tupeln $\left(a_1^{(i)}, \ldots, a_n^{(i)}\right)$ besteht (wobei $i = 1, \ldots, k$ und $k \geq 1$), dann seien $Y_j^{(i)}$ $(i = 1, \ldots, k, j = 1, \ldots, n)$ verschiedene Unbestimmte und

$$P = \prod_{i=1}^{k} \left[(X_1 - Y_1^{(i)})^2 + \cdots + (X_n - Y_n^{(i)})^2\right].$$

Wenn man nun $Y_j^{(i)}$ gleich $a_j^{(i)}$ setzt (für alle $i, j$), ist $(x_1, \ldots, x_n) \in S$ genau dann, wenn $P\left(x_1, \ldots, x_n, a_1^{(1)}, \ldots, a_n^{(1)}, \ldots, a_1^{(k)}, \ldots, a_n^{(k)}\right) = 0$.

Noch ein Beispiel: die Menge $S$ aller positiver zerlegbarer Zahlen. In diesem Fall ist $x$ genau dann zerlegbar, wenn es positive ganze Zahlen $y$, $z$ gibt, für die $(x, y, z)$ eine Lösung von $X - (Y + 1)(Z + 1) = 0$ ist.

Die folgende Aussage von Putnam aus dem Jahre 1960 ist nicht schwer zu beweisen:

Eine Menge $S$ positiver ganzer Zahlen ist genau dann diophantisch, wenn ein Polynom $Q$ mit ganzzahligen Koeffizienten (in $m \geq 1$ Unbekannten) existiert, so dass

$$S = \{Q(x_1, \ldots, x_m) \geq 1 \mid x_1 \geq 1, \ldots, x_m \geq 1\}.$$

Der nächste Schritt innerhalb dieser Theorie besteht darin nachzuweisen, dass die Menge der Primzahlen diophantisch ist. Dazu ist es notwendig, die Definition der Primzahlen aus der Sicht der Theorie der diophantischen Mengen zu untersuchen.

Eine positive ganze Zahl $x$ ist genau dann eine Primzahl, wenn $x > 1$ und für beliebige ganze Zahlen $y$, $z$ mit $y \leq x$ und $z \leq x$ entweder $yz < x$ oder $yz > x$ oder $y = 1$ oder $z = 1$. Diese Definition der Primzahlen beinhaltet das beschränkt universell quantifizierte Vorkommen von $y$, $z$, nämlich $y \leq x$, $z \leq x$.

Eine andere Möglichkeit der Definition von Primzahlen ist die folgende. Die positive ganze Zahl $x$ ist genau dann eine Primzahl, wenn $x > 1$ und $\mathrm{ggT}((x-1)!, x) = 1$. Letztere Bedingung lässt sich folgendermaßen auf andere Weise ausdrücken: Es gibt positive ganze Zahlen $a$, $b$, so dass $a(x-1)! - bx = 1$. Wenn $a$ oder $b$ negativ sind, nehme man eine hinreichend große ganze Zahl $k$, so dass $a' = a + kx > 0$, $b' = b + k(x-1)! > 0$ und $a'(x-1)! - b'x = 1$.

Mit Hilfe der von Putnam, Davis, J. Robinson und Matijasevič entwickelten Theorie lässt sich unter Verwendung einer der obigen Charakterisierungen von Primzahlen der folgende, wichtige Satz beweisen:

*Die Menge der Primzahlen ist diophantisch.*

Eine Kombination dieser Resultate führt zum folgenden, erstaunlichen Satz:

*Es gibt ein Polynom mit ganzzahligen Koeffizienten, so dass die Menge der Primzahlen mit dem positiven Wertebereich des Polynoms zusammenfällt, wobei die Variablen die nichtnegativen ganzen Zahlen durchlaufen.*

Es sei bemerkt, dass dieses Polynom auch negative Werte annimmt und dass einige Primzahlen mehrfach als Wert des Polynoms auftreten können.

Matijasevič gab 1971 ein System algebraischer Relationen an, das zu einem solchen Polynom führt, ohne dass es dabei explizit erzeugt wird. Dieses Polynom in 24 Unbestimmten hatte den Grad 37. In der englischen Übersetzung seines Artikels konnte dies auf den Grad 21 und 21 Unbestimmte verbessert werden.

Jones, Sato, Wada & Wiens gaben 1976 ein Polynom mit dieser Eigenschaft explizit an (vom Grad 25, in 26 Unbestimmten $a, b, c, \ldots, z$):

$$
\begin{aligned}
(k+2)\big\{ & 1-[wz+h+j-q]^2-[(gk+2g+k+1)(h+j)+h-z]^2 \\
& -[2n+p+q+z-e]^2-[16(k+1)^3(k+2)(n+1)^2+1-f^2]^2 \\
& -[e^3(e+2)(a+1)^2+1-o^2]^2-[(a^2-1)y^2+1-x^2]^2 \\
& -[16r^2y^4(a^2-1)+1-u^2]^2-[((a+u^2(u^2-a))^2-1)(n+4dy)^2 \\
& +1-(x+cu)^2]^2-[n+l+v-y]^2 \\
& -[(a^2-1)l^2+1-m^2]^2-[ai+k+1-l-i]^2 \\
& -[p+l(a-n-1)+b(2an+2a-n^2-2n-2)-m]^2 \\
& -[q+y(a-p-1)+s(2ap+2a-p^2-2p-2)-x]^2 \\
& -[z+pl(a-p)+t(2ap-p^2-1)-pm]^2\big\}.
\end{aligned}
$$

Man ist natürlich dazu verleitet, die Anzahl der Unbestimmten, den Grad oder beides zu reduzieren. Allerdings bezahlt man dafür einen Preis. Wenn die Zahl $n$ der Unbestimmten reduziert wird, erhöht sich der Grad $d$, umgekehrt wächst $n$, wenn $d$ heruntergedrückt wird.

Dies wird in Tabelle 12 veranschaulicht, in der primzahldarstellende Polynome angegeben sind.

Tabelle 12. Polynome, die Primzahlen darstellen

| $n$ = Anzahl der Unbestimmten | $d$ = Grad | Autor | Jahr | Bemerkungen |
|---|---|---|---|---|
| 24 | 37 | Matijasevič | 1971 | Nicht explizit angegeben |
| 21 | 21 | Gleicher Autor | 1971 | |
| 26 | 25 | Jones, Sato, Wada & Wiens | 1976 | Erstes explizites Polynom |
| 42 | 5 | Gleiche Autoren | 1976 | Niedrigster Grad, nicht explizit angegeben |
| 12 | 13697 | Matijasevič | 1976 | |
| 10 | etwa $1{,}6 \times 10^{45}$ | Gleicher Autor | 1977 | Kleinste Anzahl von Unbestimmten, nicht explizit angegeben |

Die Anzahl der Variablen, die man mindestens benötigt, ist unbekannt (sie kann nicht gleich 2 sein). Allerdings konnte Jones zeigen, dass es ein primzahldarstellendes Polynom mit einem Grad von höchstens 5 gibt.

Die gleichen Methoden, die im Falle der Primzahlen zur Anwendung kamen, können auch für andere diophantische Mengen verwendet werden, sobald man die sie definierenden arithmetischen Eigenschaften vom gleichen Blickwinkel aus betrachtet.

Dies wurde von Jones ausgeführt. In einem Artikel von 1975 zeigte Jones, dass die Menge der Fibonacci-Zahlen identisch mit der Menge der positiven Werte eines Polynoms in 2 Unbestimmten vom Grad 5 mit nichtnegativen Argumenten ist:

$$2xy^4 + x^2y^3 - 2x^3y^2 - y^5 - x^4y + 2y.$$

Jones zeigte 1979, dass es für die Mengen der Mersenne-Primzahlen, der geraden vollkommenen Zahlen und der Fermat-Primzahlen in gleicher Weise ein entsprechendes Polynom in sieben Unbestimmten, allerdings höheren Grades gibt. Er gab für diese Mengen auch andere Polynome niedrigeren Grades an, die aber mehr Unbestimmte hatten.

Tabelle 13. Polynome, die verschiedene Mengen von Zahlen erzeugen

| Menge | Anzahl der Unbestimmten | Grad |
|---|---|---|
| Fibonacci-Zahlen | 2 | 5 |
| Mersenne-Primzahlen | 13 | 26 |
| | 7 | 914 |
| Gerade vollkommene Zahlen | 13 | 27 |
| | 7 | 915 |
| Fermat-Primzahlen | 14 | 25 |
| | 7 | 905 |

Durch eine Methode von Skolem (siehe sein Buch von 1938) lässt sich der Grad für die drei letzten Mengen auf 5 reduzieren, wobei sich dann die Anzahl der Variablen auf etwa 20 erhöht.

Für die Menge der Mersenne-Primzahlen sieht das Polynom vom Grad 26 in 13 Unbekannten so aus:

$$\begin{aligned} n\big\{&1-[4b+3-n]^2-b([2+hn^2-a]^2\\ &+[n^3d^3(nd+2)(h+1)^2+1-m^2]^2\\ &+[db+d+chn^2+g(4a-5)-kn]^2\\ &+[(a^2-1)c^2+1-k^2n^2]^2+[4(a^2-1)i^2c^4+1-f^2]^2\\ &+[(kn+lf)^2-((a+f^2(f^2-a))^2-1)(b+1+2jc)^2-1]^2)\big\}. \end{aligned}$$

Das Polynom vom Grad 27 in 13 Unbestimmten, das die geraden vollkommenen Zahlen liefert, ist das folgende:

$$\begin{aligned} (2b+2)n\big\{&1-[4b+3-n]^2-b([2+hn^2-a]^2\\ &+[n^3d^3(nd+2)(h+1)^2+1-m^2]^2\\ &+[db+d+chn^2+g(4a-5)-kn]^2\\ &+[(a^2-1)c^2+1-k^2n^2]^2+[4(a^2-1)i^2c^4+1-f^2]^2\\ &+[(kn+lf)^2-((a+f^2(f^2-a))^2-1)(b+1+2jc)^2-1]^2)\big\}. \end{aligned}$$

Die primen Fermat-Zahlen werden durch dieses Polynom vom Grad 25 in 14 Variablen erzeugt:

$$\begin{aligned} (6g+5)\big\{&1-[bh+(a-12)c+n(24a-145)-d]^2\\ &-[16b^3h^3(bh+1)(a+1)^2+1-m^2]^2\\ &-[3g+2-b]^2-[2be+e-bh-1]^2-[k+b-c]^2\\ &-[(a^2-1)c^2+1-d^2]^2-[4(a^2-1)i^2c^4+1-f^2]^2\\ &-[(d+lf)^2-((a+f^2(f^2-a))^2-1)(b+2jc)^2-1]^2\big\}. \end{aligned}$$