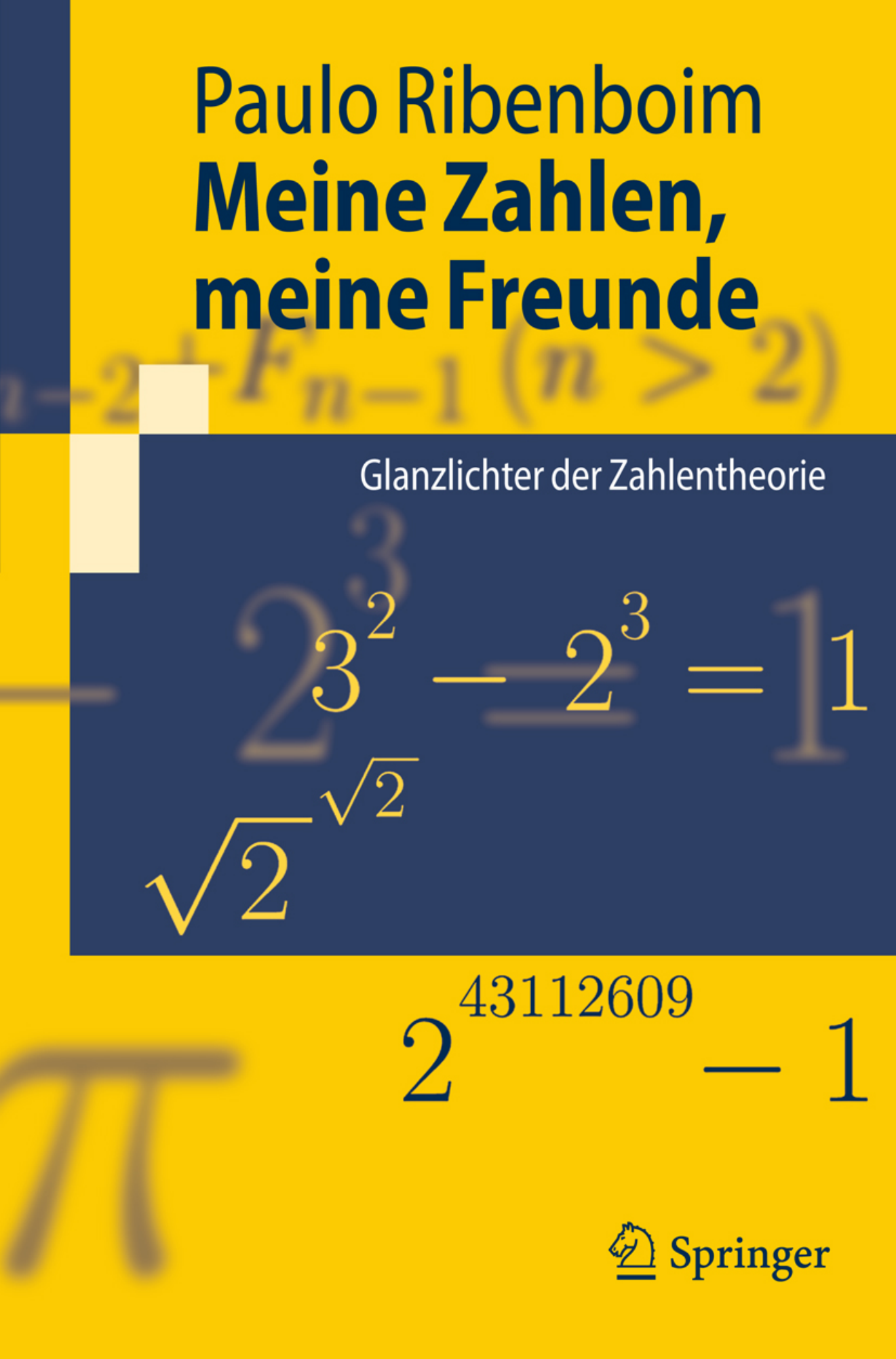
Paulo Ribenboim

Meine Zahlen, meine Freunde

Glanzlichter der Zahlentheorie



Springer

Springer-Lehrbuch

Paulo Ribenboim

Meine Zahlen, meine Freunde

Glanzlichter der Zahlentheorie

Springer

Prof. Dr. Paulo Ribenboim
Department of Mathematics and Statistics
Queen´s University
Kingston, Ontario K7L 3N6
Kanada

Übersetzer:
Dr. Jörg Richstein

ISBN 978-3-540-87955-8 e-ISBN 978-3-540-87957-2

DOI 10.1007/978-3-540-87957-2

Springer-Lehrbuch ISSN 0937-7433

Bibliografische Information der Deutschen Nationalbibliothek
Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über http://dnb.d-nb.de abrufbar.

Mathematics Subject Classification (2000): 11-06, 11Axx

Einbandgestaltung: WMX Design GmbH, Heidelberg

Gedruckt auf säurefreiem Papier

9 8 7 6 5 4 3 2 1

springer.de

Vorwort

Liebe Freunde der Zahlen:

Dieses Buch ist für Sie bestimmt. Es soll Ihnen ein exquisites intellektuelles Vergnügen bieten, das zu erfahren nur relativ wenige glückliche Menschen in der Lage sind.

Mögen diese Abhandlungen Ihre Wissbegier anregen und Sie zur Lektüre von Büchern und Artikeln verleiten, in denen die technischen Feinheiten der einzelnen Themen besprochen werden.

Ich muss Sie jedoch warnen. Die behandelten Probleme sind zwar einfach zu formulieren, aber größtenteils sehr schwierig. Viele sind immer noch ungelöst. Sie werden sehen, auf welche Weisen Mathematiker versucht haben, diese Probleme anzugreifen.

Gehirne in Betrieb! Geben Sie aber nicht mir die Schuld an Ihren schlaflosen Nächten (ich habe schon meine eigenen).

Einige der Kapitel entstanden im Laufe der Jahre aus meinen üblichen Abschweifungen.

Aus anderen könnten ganze Bücher werden, was aber vermutlich nie geschehen wird.

An der Vielfältigkeit der Themen lassen sich die vielen Gestalten erkennen, die die Zahlen annehmen, um ihren Reiz auszuüben und die Wendigkeit des Geistes abzuverlangen. Ihres Geistes, lieber Leser, der schon darauf bedacht ist, dieses Vorwort zu verlassen.

Gehen Sie nun zu Seite 1 (oder 127?).

Kingston, Ontario, Kanada — *Paulo Ribenboim*
Januar 2009

Inhaltsverzeichnis

1

Die Fibonacci-Zahlen und das Nordpolarmeer

Einleitung

Es gibt tatsächlich keinen besonderen Zusammenhang zwischen den Fibonacci-Zahlen und dem Nordpolarmeer. Aber ich dachte mir, dass der Titel vielleicht Ihre Neugier auf das Kapitel wecken würde. Sie werden enttäuscht sein, wenn Sie etwas über das Nordpolarmeer erfahren wollten, denn mein Thema werden die Fibonacci-Zahlen und ähnliche Folgen sein.

Wie Eisberge im Nordpolarmeer sind die Fibonacci-Zahlen nur der sichtbare Teil einer Theorie, die viel tiefer reicht: Die Theorie der linear rekurrenten Folgen.

Die sogenannten Fibonacci-Zahlen tauchten in der Lösung eines Problems auf, das Fibonacci (auch bekannt als Leonardo Pisano) in seinem Buch *Liber Abaci* (1202) vorstellte, es ging dabei um Vermehrungsmuster bei Kaninchen.

Die erste bedeutsame Arbeit zum Thema ist der wegweisende Artikel von Lucas aus dem Jahr 1878. Später erschienen die klassischen Beiträge von Bang (1886) und Zsigmondy (1892) über Primfaktoren spezieller Folgen von Binomialzahlen. Carmichael (1913) veröffentlichte einen weiteren fundamentalen Artikel, worin er frühere Ergebnisse auf Spezialfälle von Lucas-Folgen ausdehnte. Von dem was folgte, möchte ich vor allem die Arbeit von Lehmer erwähnen, die in Anwendungen in der Theorie der Primzahltests zu vielerlei Entwicklungen führte.

Der Themenbereich ist sehr umfassend und ich werde hier nur bestimmte Aspekte davon behandeln.

Wenn sich Ihr Interesse im Grunde auf die Fibonacci- und Lucas-Zahlen beschränkt, so empfehle ich Ihnen die Lektüre der Büchlein von Vorob'ev (1963), Hoggatt (1969), und Jarden (1958).

1 Grundlegende Definitionen

A Lucas-Folgen

Es seien P, Q ganze Zahlen ungleich 0, $D = P^2 - 4Q$ sei die *Diskriminante*, wobei $D \neq 0$ vorausgesetzt werde (um ausgeartete Fälle auszuschließen).

Betrachte das Polynom $X^2 - PX + Q$, bezeichnet als das *charakteristische Polynom*, mit Nullstellen

$$\alpha = \frac{P + \sqrt{D}}{2} \quad \text{und} \quad \beta = \frac{P - \sqrt{D}}{2}.$$

Folglich ist $\alpha \neq \beta$, $\alpha + \beta = P$, $\alpha \cdot \beta = Q$ und $(\alpha - \beta)^2 = D$.

Für jedes $n \geq 0$ seien $U_n = U_n(P, Q)$ und $V_n = V_n(P, Q)$ nun wie folgt definiert:

$$\begin{aligned} U_0{=}0\,,\ U_1{=}1\ ,\ U_n{=}P \cdot U_{n-1} - Q \cdot U_{n-2} \ (\text{für } n \geq 2),\\ V_0{=}2\,,\ V_1{=}P\,,\ V_n{=}P \cdot V_{n-1} - Q \cdot V_{n-2} \ (\text{für } n \geq 2). \end{aligned}$$

Die Folgen $U = (U_n(P, Q))_{n\geq 0}$ und $V = (V_n(P, Q))_{n\geq 0}$ nennt man die (erste und zweite) *Lucas-Folge mit Parametern* (P, Q). Die Folge $(V_n(P, Q))_{n\geq 0}$ wird auch als *begleitende* Folge mit Parametern (P, Q) bezeichnet.

Die folgenden Potenzreihenentwicklungen lassen sich für beliebiges (P, Q) leicht nachweisen:

$$\frac{X}{1 - PX + QX^2} = \sum_{n=0}^{\infty} U_n X^n \qquad \text{und}$$

$$\frac{2 - PX}{1 - PX + QX^2} = \sum_{n=0}^{\infty} V_n X^n.$$

Die Lucas-Folgen sind Beispiele von algorithmisch erzeugten Zahlenfolgen.

Die zum $n$ten Schritt (oder zum Zeitpunkt n) gehörenden Zahlen sind $U_n(P, Q)$ bzw. $V_n(P, Q)$. In diesem Fall ist der Algorithmus eine lineare Rekurrenz mit zwei Parametern. Sobald die Parameter und die Startwerte gegeben sind, ist die gesamte Folge, das heißt sind alle zukünftigen Werte bestimmt. Aber auch zwei beliebige, aufeinanderfolgende Werte bestimmen bei gegebenen Parametern alle zukünftigen und vorangegangenen Folgenglieder vollständig.

B Spezielle Lucas-Folgen

Ich werde wiederholt spezielle Lucas-Folgen untersuchen, sei es aufgrund ihrer historischen Bedeutung oder um ihrer selbst willen. Dies sind die Folgen der Fibonacci-Zahlen, der Lucas-Zahlen, der Pell-Zahlen sowie weiterer Zahlenfolgen, die mit Binomialzahlen verbunden sind.
(a) Es sei $P = 1$, $Q = -1$, also $D = 5$. Die Zahlen $U_n = U_n(1, -1)$ heißen *Fibonacci-Zahlen*, während man die Zahlen $V_n = V_n(1, -1)$ die *Lucas-Zahlen* nennt. Hier die ersten Glieder der Folgen:

Fibonacci-Zahlen : 0, 1, 2, 3, 5, 8, 13, 21, 34, 55, 89, 144, ...
Lucas-Zahlen : 2, 1, 3, 4, 7, 11, 18, 29, 47, 76, 123, 99, 322, ...

(b) Es sei $P = 2$, $Q = -1$, also $D = 8$. Die Zahlen $U_n = U_n(2, -1)$ und $V_n = V_n(2, -1)$ sind die *Pell-Zahlen* und die *begleitenden Pell-Zahlen*. Hier die ersten Folgenglieder:

$U_n(2, -1)$: 0, 1, 2, 5, 12, 29, 70, 169, ...
$V_n(2, -1)$: 2, 2, 6, 14, 34, 82, 198, 478, ...

(c) Es seien a, b ganze Zahlen mit $a > b \geq 1$. Sei $P = a + b$, $Q = ab$, also $D = (a - b)^2$. Für jedes $n \geq 0$ sei $U_n = \frac{a^n - b^n}{a-b}$ und $V_n = a^n + b^n$. Es ist nun nicht schwierig nachzuprüfen, dass $U_0 = 0$, $U_1 = 1$, $V_0 = 2$, $V_1 = a + b = P$ und dass $(U_n)_{n\geq 0}$, $(V_n)_{n\geq 0}$ die ersten und zweiten Lucas-Folgen mit Parametern P, Q sind.

Insbesondere erhält man für $b = 1$ die Folge der Zahlen $U_n = \frac{a^n - 1}{a-1}$, $V_n = a^n + 1$; die Parameter sind nun $P = a + 1$, $Q = a$. Schließlich ergibt sich, falls auch $a = 2$ gewählt wird, die Folge $U_n = 2^n - 1$, $V_n = 2^n + 1$ mit Parametern $P = 3$, $Q = 2$.

C Verallgemeinerungen

An dieser Stelle ist es angebracht, auf Erweiterungen des Begriffs der Lucas-Folgen hinzuweisen, auch wenn diese hier nicht behandelt werden. Derartige Verallgemeinerungen sind in vier Richtungen möglich, nämlich durch Veränderung der Startwerte, durch Mischen der beiden Lucas-Folgen, durch Verzicht auf die Ganzzahligkeit der Folgenglieder oder indem man mehr als zwei Parameter zulässt.

Obwohl viele Ergebnisse über Lucas-Folgen erfolgreich auf diese allgemeineren Folgen übertragen wurden und sich interessante Anwendungen fanden, habe ich mich der Klarheit wegen dazu entschlossen, mich auf die Lucas-Folgen zu beschränken.

(a) Es seien wie zuvor P, Q ganze Zahlen. Seien T_0, T_1 beliebige ganze Zahlen mit der Einschränkung, dass T_0 oder T_1 ungleich 0 ist (um den Trivialfall auszuschließen). Sei

$$W_0 = PT_0 + 2T_1 \quad \text{und} \quad W_1 = 2QT_0 + PT_1,$$

sowie

$$\begin{aligned} T_n &= P \cdot T_{n-1} - Q \cdot T_{n-2} \qquad \text{und} \\ W_n &= P \cdot W_{n-1} - Q \cdot W_{n-2} \qquad (\text{für } n \geq 2). \end{aligned}$$

Die Folgen $(T_n(P,Q))_{n\geq 0}$ und $W_n(P,Q))_{n\geq 0}$ sind die (ersten und zweiten) *linear rekurrenten Folgen* mit Parametern (P,Q) und *zugehörig zum Paar* (T_0,T_1). Die Lucas-Folgen sind spezielle, normierte linear rekurrente Folgen mit den gegebenen Parametern; sie sind zugehörig zum Paar $(0,1)$.

(b) Lehmer (1930) untersuchte diese Folgen: Seien P, Q ganze Zahlen ungleich 0 und α, β die Nullstellen des Polynoms $X^2 - \sqrt{P} \cdot X + Q$. Definiere

$$L_n(P,Q) = \begin{cases} \frac{\alpha^n - \beta^n}{\alpha - \beta} \text{ falls } n \text{ ungerade,} \\ \frac{\alpha^n - \beta^n}{\alpha^2 - \beta^2} \text{ falls } n \text{ gerade.} \end{cases}$$

$L = (L_n(P,Q))_{n\geq 0}$ ist die *Lehmer-Folge* mit Parametern P, Q. Ihre Glieder sind ganze Zahlen. Die Lehmer-Folgen wurden zunächst von Lehmer und später von Schinzel und Stewart im Rahmen verschiedener Arbeiten über Lucas-Folgen untersucht. Die entsprechenden Artikel sind in den Literaturangaben verzeichnet.

(c) Sei $\mathcal{R}$ ein nicht notwendigerweise mit $\mathbb{Z}$ identischer Integritätsbereich. Sei P, $Q \in \mathcal{R}$, P, $Q \neq 0$ derart, dass $D = P^2 - 4Q \neq 0$. Die Folgen $(U_n(P,Q))_{n\geq 0}$, $(V_n(P,Q))_{n\geq 0}$ von Elementen aus $\mathcal{R}$ lassen sich analog dem Fall $\mathcal{R} = \mathbb{Z}$ definieren.

Bemerkenswerte Fälle ergeben sich, wenn $\mathcal{R}$ der Ring der ganzen Zahlen eines Zahlkörpers ist (z.B. einem quadratischen Zahlkörper), oder wenn $\mathcal{R} = \mathbb{Z}[x]$ (oder ein anderer Polynomring), oder auch wenn es sich bei $\mathcal{R}$ um einen endlichen Körper handelt. Für letzteren Fall siehe Selmer (1966).

(d) Es seien ganze Zahlen P_0, P_1, …, P_{k-1} (mit $k \geq 1$) gegeben, die gewissen Einschränkungen unterliegen mögen, um Trivialfälle auszuschließen. Seien S_0, S_1, …, S_{k-1} ganze Zahlen. Definiere für $n \geq k$:

$$S_n = P_0 \cdot S_{n-1} - P_1 \cdot S_{n-2} + P_2 \cdot S_{n-3} - \ldots + (-1)^{k-1} P_{k-1} \cdot S_{n-k}.$$

Dann heißt $(S_n)_{n\geq 0}$ *linear rekurrente Folge der Ordnung k mit Parametern* P_0, P_1, …, P_{k-1} *und Startwerten* S_0, S_1, …, S_{k-1}. Der Fall $k = 2$ war oben zu sehen. Für $k = 1$ erhält man die geometrische Reihe $(S_0 \cdot P_0^n)_{n\geq 0}$.

Es besteht ein großes Interesse an der Theorie der linear rekurrenten Folgen mit einer Ordnung größer als zwei und viele Fragen sind noch offen.

2 Grundlegende Eigenschaften

Die Zahlen der Lucas-Folgen besitzen vielerlei Eigenschaften, die die Gesetzmäßigkeit ihrer Erzeugung widerspiegeln.

A Binets Formeln

Binet (1843) gab die folgenden Ausdrücke unter Verwendung der Nullstellen α, β des Polynoms $X^2 - PX + Q$ an:

2.1. Binets Formeln:

$$U_n = \frac{\alpha^n - \beta^n}{\alpha - \beta},$$
$$V_n = \alpha^n + \beta^n.$$

Der Beweis ist natürlich sehr einfach. Man beachte, dass nach Binets Formeln gilt

$$U_n(-P, Q) = (-1)^{n-1} U_n(P, Q) \qquad \text{sowie}$$
$$V_n(-P, Q) = (-1)^n V_n(P, Q).$$

Es wird daher für die meisten der folgenden Betrachtungen $P \geq 1$ angenommen.

B Entartete Lucas-Folgen

Sei (P, Q) derart, dass der Quotient $\eta = \alpha/\beta$ der Nullstellen von $X^2 - Px + Q$ eine Einheitswurzel ist. Dann nennt man die Folgen $U(P, Q)$, $V(P, Q)$ *entartet*.

Ich werde nun alle entarteten Folgen beschreiben.

Da

$$\eta + \eta^{-1} = \frac{\alpha}{\beta} + \frac{\beta}{\alpha} = \frac{P^2 - 2Q}{Q}$$

eine ganze algebraische Zahl und rational ist, muss es sich um eine ganze Zahl handeln.

Aus $|\frac{\alpha}{\beta} + \frac{\beta}{\alpha}| \leq 2$ folgt $P^2 - 2Q = 0, \pm Q, \pm 2Q$, hieraus $P^2 = Q, 2Q, 3Q, 4Q$. Falls $\mathrm{ggT}(P, Q) = 1$, dann ist $(P, Q) = (1, 1), (-1, 1), (2, 1)$ oder $(-2, 1)$ und die Folgen sind

$$\begin{array}{lrrrrrrrrrrr}
U(1,1) & : & 0, & 1, & 1, & 0, & -1, & -1, & 0, & 1, & 1, & 0, & \ldots \\
U(-1,1) & : & 0, & 1, & -1, & 0, & 1, & -1, & 0, & \ldots & & & \\
V(1,1) & : & 2, & 1, & -1, & -2, & -1, & 1, & 2, & 1, & -1, & -2, & \ldots \\
V(-1,1) & : & 2, & -1, & -1, & 2, & -1, & -1, & 2, & \ldots & & & \\
U(2,1) & : & 0, & 1, & 2, & 3, & 4, & 5, & 6, & 7, & \ldots & & \\
U(-2,1) & : & 0, & 1, & -2, & 3, & -4, & 5, & -6, & 7, & \ldots & & \\
V(2,1) & : & 2, & 2, & 2, & 2, & 2, & 2, & 2, & 2, & \ldots & & \\
V(-2,1) & : & 2, & -2, & 2, & -2, & 2, & -2, & 2, & -2, & \ldots & &
\end{array}$$

Es ergibt sich im Falle einer entarteten Folge, dass $D = 0$ oder $D = -3$.

C Wachstum und numerische Berechnungen

Ich werde zunächst Ergebnisse über das Wachstum der Folge $U(P, Q)$ angeben.

2.2. Wenn die Folgen $U(P, Q)$, $V(P, Q)$ nicht entartet sind, dann wachsen $|U_n|$, $|V_n|$ mit n gegen Unendlich.

Dies folgt aus einem Resultat von Mahler (1935) über das Wachstum der Koeffizienten von Taylorreihen. Mahler zeigte zudem

2.3. Falls $Q \geq 2$, $\mathrm{ggT}(P, Q) = 1$, $D < 0$, dann gilt für jedes $\varepsilon > 0$ bei genügend großem n

$$|U_n| \geq |\beta^n|^{1-\varepsilon}.$$

Die Berechnungen von U_n, V_n lassen sich wie folgt durchführen. Sei

$$M = \begin{pmatrix} P & -Q \\ 1 & 0 \end{pmatrix}.$$

Dann gilt für $n \geq 1$,

$$\begin{pmatrix} U_n \\ U_{n-1} \end{pmatrix} = M^{n-1} \begin{pmatrix} 1 \\ 0 \end{pmatrix}$$

und

$$\begin{pmatrix} V_n \\ V_{n-1} \end{pmatrix} = M^{n-1} \begin{pmatrix} 2 \\ P \end{pmatrix}.$$

Die schnellste Methode zur Ermittlung der Potenz M^k der Matrix M ist die sukzessive Berechnung der Potenzen M, M^2, M^4, …, M^{2^e}, wobei $2^e \leq k < 2^{e+1}$; dies erfolgt durch sukzessives Quadrieren der Matrizen. Wenn weiter die 2-adische Entwicklung von k durch $k = k_0 + k_1 \times 2 + k_2 \times 2^2 + \ldots + k_e \times 2^e$ gegeben ist, wobei $k_i = 0$ oder 1, dann folgt $M^k = M^{k_0} \times (M^2)^{k_1} \times \ldots \times (M^{2^e})^{k_e}$.

Man beachte, dass die einzig überhaupt auftretenden Faktoren diejenigen sind, wo $k_i = 1$.

Binets Formeln erlauben in manchen Fällen auch die schnelle Berechnung von U_n und V_n.

Wenn $D \geq 5$ und $|\beta| < 1$, dann

$$\left| U_n - \frac{\alpha^n}{\sqrt{D}} \right| < \frac{1}{2} \quad \text{(für } n \geq 1\text{)},$$

und $|V_n - \alpha^n| < \frac{1}{2}$ (für n derart, dass $n \cdot (-\log|\beta|) > \log 2$). Somit ist cU_n die nächstgelegene ganze Zahl zu $\frac{\alpha^n}{\sqrt{D}}$, und V_n diejenige zu α^n. Dies gilt insbesondere für Fibonacci- und Lucas-Zahlen, für die $D = 5$, $\alpha = (1 + \sqrt{5})/2 = 1{,}616\ldots$, (die Goldene Zahl), $\beta = (1 - \sqrt{5})/2 = -0{,}616\ldots$.

Es folgt, dass die Fibonacci-Zahl U_n und die Lucas-Zahl V_n etwa $n/5$ Ziffern besitzen.

D Algebraische Beziehungen

Die Zahlen der Lucas-Folgen besitzen vielerlei Eigenschaften. Ein Blick in die Ausgaben von *The Fibonacci Quarterly* hinterlässt den Eindruck, dass der Fantasie der Mathematiker beim Bestreben, neue Formen dieser Gleichungen und Formeln hervorzubringen, keine Grenzen gesetzt sind. Mithin gibt es Ausdrücke, die nur die Zahlen U_n enthalten, während andere auf die Zahlen V_n beschränkt sind, wohingegen in wieder anderen U_n und V_n kombiniert sind. Es gibt Formeln für U_{m+n}, U_{m-n}, V_{m+n}, V_{m-n} (bezüglich U_m, U_n, V_m, V_n); dies sind die Additions- und Subtraktionsformeln.

Es gibt auch Formeln für U_{kn}, V_{kn} und U_{n^k}, V_{n^k}, U_n^k, cV_n^k (wobei $k \geq 1$) und viele mehr.

Ich werde eine kleine Anzahl von Formeln auswählen, die ich für am meisten nützlich erachte. Ihre Beweise sind fast immer sehr einfache Übungsaufgaben, entweder durch Anwendung von Binets Formeln oder durch Induktion.

Es ist zweckdienlich, die Lucas-Folgen in derartiger Weise auf negative Indizes zu erweitern, dass dieselbe Rekursion (mit den gegebenen Parametern P, Q) immer noch gilt.

2.4. Erweiterung auf negative Indizes:

$$U_{-n} = -\frac{1}{Q^n} U_n, \quad V_{-n} = \frac{1}{Q^n} V_n \quad (\text{für } n \geq 1).$$

2.5. U_n und V_n lassen sich durch P und Q ausdrücken. Zum Beispiel ist

$$\begin{aligned} U_n = P^{n-1} - \binom{n-2}{1} P^{n-3}Q + \binom{n-3}{2} P^{n-5}Q^2 + \dots \\ +(-1)^k \binom{n-1-k}{k} P^{n-1-2k}Q^k + \dots + (\text{letzter Summand}) \end{aligned}$$

wobei

$$(\text{letzter Summand}) = \begin{cases} (-1)^{\frac{n}{2}-1} \binom{\frac{n}{2}}{\frac{n}{2}-1} P Q^{\frac{n}{2}-1} & \text{für } n \text{ gerade,} \\ (-1)^{\frac{n-1}{2}} Q^{\frac{n-1}{2}} & \text{für } n \text{ ungerade.} \end{cases}$$

Somit ist $U_n = f_n(P, Q)$, wobei $f_n(X, Y) \in \mathbb{Z}[X, Y]$. Die Funktion f_n ist isobar mit Gewicht $n-1$, wobei X das Gewicht 1 und Y das Gewicht 2 hat.

In ähnlicher Weise gilt $V_n = g_n(P, Q)$, wobei $g_n \in \mathbb{Z}[X, Y]$. Die Funktion g_n ist isobar mit Gewicht n, wobei X das Gewicht 1 und Y das Gewicht 2 hat.

2.6. Quadratische Beziehungen:

$$V_n^2 - DU_n^2 = 4Q^n$$

für jedes $n \in \mathbb{Z}$.

Dies lässt sich auch in dieser Form ausdrücken:

$$U_{n+1}^2 - PU_{n+1}U_n + QU_n^2 = Q^n.$$

2.7. Umrechnungsformeln:

$$\begin{aligned} DU_n &= V_{n+1} - QV_{n-1}, \\ V_n &= U_{n+1} - QU_{n-1}, \end{aligned}$$

für jedes $n \in \mathbb{Z}$.

2.8. Addition von Indizes:

$$\begin{aligned} U_{m+n} &= U_m V_n - Q^n U_{m-n}, \\ V_{m+n} &= V_m V_n - Q^n V_{m-n} = DU_m U_n + Q^n V_{m-n}, \end{aligned}$$

für jedes m, $n \in \mathbb{Z}$.

Andere Formeln der gleichen Art sind:

$$\begin{aligned} 2U_{m+n} &= U_m V_n + U_n V_m, \\ 2Q^n U_{m-n} &= U_m V_n - U_n V_m, \end{aligned}$$

für jedes m, $n \in \mathbb{Z}$.

2.9. Multiplikation von Indizes:

$$\begin{aligned} U_{2n} &= U_n V_n, \\ V_{2n} &= V_n^2 - 2Q^n, \\ U_{3n} &= U_n(V_n^2 - Q^n) = U_n(DU_n^2 + 3Q^n), \\ V_{3n} &= V_n(V_n^2 - 3Q^n), \end{aligned}$$

für jedes $n \in \mathbb{Z}$.

Es ist für den allgemeinen Fall $k \geq 3$ möglich, Formeln für U_{kn} und V_{kn} durch Induktion über k zu gewinnen. Ich werde allerdings davon absehen, diese explizit anzugeben.

E Teilbarkeitseigenschaften

2.10. Sei $U_m \neq 1$. Dann wird U_n von U_m genau dann geteilt, wenn $m \mid n$.
Sei $V_m \neq 1$. Dann wird V_n von V_m genau dann geteilt, wenn $m \mid n$ und n/m ungerade ist.

Für die folgenden Eigenschaften sei vorausgesetzt, dass $\mathrm{ggT}(P, Q) = 1$.

2.11. $\mathrm{ggT}(U_m, U_n) = U_d$, wobei $d = \mathrm{ggT}(m, n)$.

2.12.

$$\mathrm{ggT}(V_m, V_n) = \begin{cases} V_d & \text{falls } \frac{m}{d} \text{ und } \frac{n}{d} \text{ ungerade sind,} \\ 1 \text{ oder } 2 & \text{sonst,} \end{cases}$$

wobei $d = \mathrm{ggT}(m, n)$.

2.13.

$$\mathrm{ggT}(U_m, V_n) = \begin{cases} V_d & \text{falls } \frac{m}{d} \text{ gerade und } \frac{n}{d} \text{ ungerade ist,} \\ 1 \text{ oder } 2 & \text{sonst,} \end{cases}$$

wobei $d = \mathrm{ggT}(m, n)$.

2.14. Wenn $n \geq 1$, dann $\mathrm{ggT}(U_n, Q) = 1$ und $\mathrm{ggT}(V_n, Q) = 1$.

3 Primteiler von Lucas-Folgen

Die klassischen Resultate über Primteiler von Termen der Lucas-Folgen gehen auf Euler (für Zahlen $\frac{a^n - b^n}{a-b}$), Lucas (für Fibonacci- und Lucas-Zahlen) und Carmichael (für andere Lucas-Folgen) zurück.

A Die Mengen $\mathcal{P}(U)$, $\mathcal{P}(V)$ und der Rang des Erscheinens

Es bezeichne $\mathcal{P}$ die Menge der Primzahlen. Gegeben seien die Lucas-Folgen $U = (U_n(P, Q))_{n \geq 0}$, $V = (V_n(P, Q))_{n \geq 0}$. Dann seien

$$\mathcal{P}(U) = \{p \in \mathcal{P} \mid \exists n \geq 1 \text{ derart, dass } U_n \neq 0 \text{ und } p \mid U_n\},$$
$$\mathcal{P}(V) = \{p \in \mathcal{P} \mid \exists n \geq 1 \text{ derart, dass } V_n \neq 0 \text{ und } p \mid V_n\}.$$

Für entartete U, V sind $\mathcal{P}(U)$, $\mathcal{P}(V)$ leicht zu bestimmen.

Es wird daher im Folgenden angenommen, dass U, V nicht-entartet sind und somit gilt $U_n(P, Q) \neq 0$, $V_n(P, Q) \neq 0$ für alle $n \geq 1$.

Man beachte, dass wenn p eine Primzahl ist, die sowohl P als auch Q teilt, dann gilt $p \mid U_n(P, Q)$, $p \mid V_n(P, Q)$ für alle $n \geq 2$. Für die nun folgenden Betrachtungen ist es daher unproblematisch anzunehmen, dass $\mathrm{ggT}(P, Q) = 1$. Somit gehört (P, Q) zur Menge

$$\mathcal{S} = \{(P, Q) \mid P \geq 1,\ \mathrm{ggT}(P, Q) = 1,\ P^2 \neq Q,\ 2Q,\ 3Q,\ 4Q\}.$$

Für jede Primzahl p definiere

$$\rho_U(p) = \begin{cases} n & \text{falls } n \text{ der kleinste positive Index mit } p \mid U_n \text{ ist,} \\ \infty & \text{falls } p \nmid U_n \text{ für jedes } n > 0, \end{cases}$$

$$\rho_V(p) = \begin{cases} n & \text{falls } n \text{ der kleinste positive Index mit } p \mid V_n \text{ ist,} \\ \infty & \text{falls } p \nmid V_n \text{ für jedes } n > 0. \end{cases}$$

Wir nennen $\rho_U(n)$ (bzw. $\rho_V(p)$)) den *Rang des Erscheinens* von p in der Lucas-Folge U (bzw. V).

Ich werde nun zunächst die Bestimmung der geraden Zahlen in den Lucas-Folgen untersuchen.

3.1. Es sei $n \geq 0$. Dann:

$$U_n \text{ gerade} \iff \begin{cases} P \text{ gerade} & Q \text{ ungerade, } n \text{ gerade,} \\ & \text{oder} \\ P \text{ ungerade} & Q \text{ ungerade, } 3 \mid n, \end{cases}$$

und

$$V_n \text{ gerade} \iff \begin{cases} P \text{ gerade} & Q \text{ ungerade, } n \geq 0, \\ & \text{oder} \\ P \text{ ungerade} & Q \text{ ungerade, } 3 \mid n. \end{cases}$$

Spezialfälle. Für die Folgen der Fibonacci- und Lucas-Zahlen ($P = 1$, $Q = -1$) erhält man:
U_n ist genau dann gerade, wenn $3 \mid n$,
V_n ist genau dann gerade, wenn $3 \mid n$.
Für die Folge der Zahlen $U_n = \frac{a^n - b^n}{a-b}$, $V_n = a^n + b^n$, mit $a > b \geq 1$, $\mathrm{ggT}(a, b) = 1$, $p = a + b$, $q = ab$ erhält man:
Falls a, b ungerade sind, dann ist U_n genau dann gerade, wenn n gerade ist, während V_n für jedes n gerade ist.
Falls a, b eine unterschiedliche Parität aufweisen, dann sind U_n, V_n immer ungerade (für $n \geq 1$).

Mit den oben eingeführten Bezeichnungsweisen lässt sich das Resultat **(3.1)** in folgender Weise neu formulieren:

3.2. $2 \in \mathcal{P}(U)$ genau dann, wenn Q ungerade ist

$$\rho_U(2) = \begin{cases} 2 & \text{wenn } P \text{ gerade}, \quad Q \text{ ungerade}, \\ 3 & \text{wenn } P \text{ ungerade}, Q \text{ ungerade}, \\ \infty & \text{wenn } P \text{ ungerade}, Q \text{ gerade}, \end{cases}$$

$2 \in \mathcal{P}(V)$ genau dann, wenn Q ungerade ist

$$\rho_V(2) = \begin{cases} 1 & \text{wenn } P \text{ gerade}, \quad Q \text{ ungerade}, \\ 3 & \text{wenn } P \text{ ungerade}, Q \text{ ungerade}, \\ \infty & \text{wenn } P \text{ ungerade}, Q \text{ gerade}. \end{cases}$$

Falls Q ungerade ist, gilt darüber hinaus, dass $2 \mid U_n$ (bzw. $2 \mid V_n$) genau dann, wenn $\rho_U(2) \mid n$ (bzw. $\rho_V(2) \mid n$).

Die letzte Aussage lässt sich auf ungerade Primzahlen erweitern:

3.3. Es sei p eine ungerade Primzahl.
Wenn $p \in \mathcal{P}(U)$, dann $p \mid U_n$ genau dann, wenn $\rho_U(p) \mid n$.
Wenn $p \in \mathcal{P}(V)$, dann $p \mid V_n$ genau dann, wenn $\rho_V(p) \mid n$ und $\frac{n}{\rho_V(p)}$ ungerade ist.

Ich betrachte nun ungerade Primzahlen p und werde angeben, wann $p \in \mathcal{P}(U)$.

3.4. Es sei p eine ungerade Primzahl.
Wenn $p \nmid P$ und $p \mid Q$, dann $p \nmid U_n$ für jedes $n \geq 1$.
Wenn $p \mid P$ und $p \nmid Q$, dann $p \mid U_n$ genau dann, wenn n gerade ist.
Wenn $p \nmid PQ$ und $p \mid D$, dann $p \mid U_n$ genau dann, wenn $p \mid n$.
Wenn $p \nmid PQD$, dann ist p Teiler von $U_{\psi_D}(p)$, wobei $\psi_D(p) = p - (\frac{D}{p})$ und $(\frac{D}{p})$ das Legendre-Symbol bezeichnet.

Folglich ist

$$\mathcal{P}(U) = \{p \in \mathcal{P} \mid p \nmid Q\},$$

und $\mathcal{P}(U)$ eine unendliche Menge.

Die Aussage für den Fall $p \nmid PQD$ ist interessanter, die anderen sind sehr einfach zu erhalten.

Das Ergebnis lässt sich mithilfe des Rangs des Erscheinens ausdrücken:

3.5. Sei p eine ungerade Primzahl.
Wenn $p \nmid P$, $p \mid Q$, dann $\rho_U(p) = \infty$.
Wenn $p \mid P$, $p \nmid Q$, dann $\rho_U(p) = 2$.
Wenn $p \nmid PQ$, $p \mid D$, dann $\rho_U(p) = p$.
Wenn $p \nmid PQD$, dann $\rho_U(p) \mid \Psi_D(p)$.

Spezialfälle. Für die Folge der Fibonacci-Zahlen ($P = 1$, $Q = -1$), $D = 5$ und $5 \mid U_n$ genau dann, wenn $5 \mid n$.
Wenn p eine ungerade Primzahl ist und $p \neq 5$, dann $p \mid U_{p-(\frac{5}{p})}$, also $\rho_U(p) \mid (p - (\frac{5}{p}))$. Wegen $U_3 = 2$ folgt $\mathcal{P}(U) = \mathcal{P}$.

Es sei $a > b \geq 1$, $\mathrm{ggT}(a, b)$, $P = a + b$, $Q = ab$, $U_n = \frac{a^n - b^n}{a-b}$.
Wenn p Teiler von a oder b ist, aber nicht beide teilt, dann gilt $p \nmid U_n$ für jedes $n \geq 1$.
Wenn $p \nmid ab$, $p \mid a + b$, so gilt $p \mid U_n$ genau dann, wenn n gerade ist.
Wenn $p \nmid ab(a+b)$, aber $p \mid a-b$, so gilt $p \mid U_n$ genau dann, wenn $p \mid n$.
Wenn $p \nmid ab(a + b)(a - b)$, dann $p \mid U_{p-1}$. (Man beachte, dass $D = (a - b)^2$).
Somit, $\mathcal{P}(U) = \{p \mid p \nmid ab\}$.

Nimmt man $b = 1$ und gilt $p \nmid a$, dann $p \mid U_{p-1}$, daher $p \mid a^{p-1} - 1$ (dies ist der kleine Satz von Fermat, der hier als Spezialfall der letzten Aussage von **(3.4)** auftaucht); dies gilt für $p \mid (a + 1)(a - 1)$ trivialerweise.

Das Ergebnis **(3.4)** wird durch das sogenannte *Gesetz der Wiederholung* vervollständigt, das zuerst von Lucas in Bezug auf die Fibonacci-Zahlen entdeckt wurde:

3.6. Es sei p^e (mit $e \geq 1$) die maximale Potenz von p, die U_n teilt. Sei $f \geq 1$, $p \nmid k$. Dann ist p^{e+f} Teiler von U_{nkp^f}. Darüberhinaus gilt für $p \nmid Q$, $p^e \neq 2$, dass p^{e+f} die maximale Potenz von p ist, die U_{nkp^e} teilt.

Wie oben gesehen ist Fermats kleiner Satz ein Spezialfall der Aussage, dass ein primes p, das PQD nicht teilt, Teiler von $U_{\Psi_D(p)}$ ist. Ich werde nun zeigen, wie man Eulers klassischen Satz neu deuten kann.

Für die Nullstellen α, β des charakteristischen Polynoms $X^2 - PX + Q$ definiere das Symbol

$$\left(\frac{\alpha, \beta}{2}\right) = \begin{cases} 1 & \text{wenn } Q \text{ gerade ist,} \\ 0 & \text{wenn } Q \text{ ungerade und } P \text{ gerade ist,} \\ -1 & \text{wenn } Q \text{ und } P \text{ beide ungerade sind,} \end{cases}$$

und für jede ungerade Primzahl p

$$\left(\frac{\alpha, \beta}{p}\right) = \begin{cases} \left(\frac{D}{p}\right) & \text{wenn } p \nmid D, \\ 0 & \text{wenn } p \mid D. \end{cases}$$

Es sei $\Psi_{\alpha,\beta}(p) = p - (\frac{\alpha,\beta}{p})$ für jedes prime p. Unter Verwendung der früheren Bezeichnung ist nun $\Psi_{\alpha,\beta}(p) = \Psi_D(p)$, wenn p ungerade ist und $p \nmid D$.

Definiere für $n = \prod_p p^e$ die *verallgemeinerte Eulersche Funktion*

$$\Psi_{\alpha,\beta}(n) = n \prod_r \frac{\Psi_{\alpha,\beta}(p)}{p},$$

also $\Psi_{\alpha,\beta}(p^e) = p^{e-1}\Psi_{\alpha,\beta}(p)$ für jede Primzahl p und $e \geq 1$. Definiere zudem die *Carmichael-Funktion* $\lambda_{\alpha,\beta}(n) = \mathrm{kgV}\{\Psi_{\alpha,\beta}(p^e)\}$. Somit ist $\lambda_{\alpha,\beta}(n)$ Teiler von $\Psi_{\alpha,\beta}(n)$.

Für den Spezialfall wenn $\alpha = a$, $\beta = 1$ und a eine ganze Zahl ist, ergibt sich $\Psi_{a,1}(p) = p - 1$ für jede Primzahl p, die a nicht teilt. Für $\mathrm{ggT}(a, n) = 1$ folgt daher $\Psi_{a,1}(n) = \varphi(n)$, wobei φ die klassische Eulersche Funktion bezeichnet.

Die Verallgemeinerung von Eulers Satz durch Carmichael sieht folgendermaßen aus:

3.7. n teilt $U_{\lambda_{\alpha,\beta}(n)}$ und somit auch $U_{\Psi_{\alpha,\beta}(n)}$.

Es ist interessant, einmal den Quotienten $\frac{\Psi_D(p)}{\rho_U(p)}$ zu betrachten. Jarden (1958) zeigte, dass für die Folge der Fibonacci-Zahlen gilt:

$$\sup\left\{\frac{p - (\frac{5}{p})}{\rho_U(D)}\right\} = \infty$$

(mit p gegen ∞). Kiss (1978) verallgemeinerte dies zu:

3.8. (a) Für jede Lucas-Folge $U_n(P, Q)$,

$$\sup\left\{\frac{\Psi_D(p)}{\rho_U(p)}\right\} = \infty.$$

(b) Es gibt $C > 0$ (abhängig von P, Q) derart, dass

$$\frac{\Psi_D(p)}{\rho_U(p)} < C\frac{p}{\log p}.$$

Ich werde mich nun der begleitenden Lucas-Folge $V = (V_n(P, Q))_{n\geq 0}$ zuwenden und die Menge der Primzahlen $\mathcal{P}(V)$ untersuchen. Es ist nicht bekannt, wie man die Menge $\mathcal{P}(V)$ unter Verwendung nur endlich vieler Kongruenzen beschreiben kann. Ich werde partielle Kongruenzbedingungen angeben und diese durch Ergebnisse über Dichtheit ergänzen.

Aufgrund von $U_{2n} = U_n V_n$ folgt, dass $\mathcal{P}(V) \subseteq \mathcal{P}(U)$. Es wurde bereits gesagt, dass $2 = \mathcal{P}(V)$ genau dann gilt, wenn Q ungerade ist.

3.9. Es sei p eine ungerade Primzahl.
Wenn $p \nmid P$, $p \mid Q$, dann $p \nmid V_n$ für alle $n \geq 1$.
Wenn $p \mid P$, $p \nmid Q$, so ist $p \mid V_n$ genau dann, wenn n ungerade ist.
Wenn $p \nmid PQ$, $p \mid D$, dann $p \nmid V_n$ für alle $n \geq 1$.
Wenn $p \nmid PQD$, so ist $p \mid V_{\frac{1}{2}\Psi_D(p)}$ genau dann, wenn $(\frac{Q}{P}) = -1$.
Wenn $p \nmid PQD$ und $(\frac{Q}{p}) = 1$, $(\frac{D}{p}) = -(\frac{-1}{p})$, dann $p \nmid V_n$ für alle $n \geq 1$.

Obiges Resultat hat zur Folge, dass $\mathcal{P}(V)$ eine unendliche Menge ist.[1] Man kann die letzten beiden Aussagen weiter verfeinern; eine vollständige Bestimmung von $\mathcal{P}(V)$ ist jedoch nicht bekannt.

Hinsichtlich des Ranges des Erscheinens lässt sich **(3.9)** folgendermaßen umformulieren:

3.10. Sei p eine ungerade Primzahl.
Wenn $p \mid P$, $p \nmid Q$, dann $\rho_V(p) = 1$.
Wenn $p \nmid P$, $p \mid Q$, dann $\rho_V(p) = \infty$.
Wenn $p \nmid PQ$, $p \mid D$, dann $\rho_V(p) = \infty$.
Wenn $p \nmid PQD$, $(\frac{Q}{p}) = -1$, dann ist $\rho_V(p)$ Teiler von $\frac{1}{2}\Psi_D(p)$.
Wenn $p \nmid PQD$, $(\frac{Q}{p}) = 1$, $(\frac{D}{p}) = -(\frac{-1}{p})$, dann $\rho_V(p) = \infty$.

Die folgende Vermutung wurde bisher noch nicht allgemein bewiesen, sie ist jedoch für Spezialfälle verifiziert, die weiter unten aufgeführt sind:

Vermutung. Für jede begleitende Lucas-Folge V existiert der Grenzwert

$$\delta(V) = \lim \frac{\pi_V(x)}{\pi(x)}$$

und ist echt größer als 0.

Dabei ist $\pi(x) = \#\{p \in \mathcal{P} \mid p \leq x\}$ und $\pi_V(x) = \#\{p \in \mathcal{P}(V) \mid p \leq x\}$. Der Grenzwert $\delta(V)$ ist die *Dichte* der Menge der Primteiler von V unter allen Primzahlen.

Spezialfälle. Es sei $(P, Q) = (1, -1)$, also V die Folge der Lucas-Zahlen. In diesem Fall lassen sich die obigen Ergebnisse in gewisser Weise vervollständigen.

[1] Dies wurde durch WARD (1954) auf alle binären linear rekurrenten Folgen ausgedehnt

Genauer:
Wenn $p \equiv 3, 7, 11, 19 \pmod{20}$, dann $p \in \mathcal{P}(V)$.
Wenn $p \equiv 13, 17 \pmod{20}$, dann $p \notin \mathcal{P}(V)$.
Wenn $p \equiv 1, 9 \pmod{20}$, dann kann es passieren, dass $p \in \mathcal{P}(V)$ oder $p \notin \mathcal{P}(V)$.

Jarden (1958) zeigte, dass es unendlich viele Primzahlen $p \equiv 1 \pmod{20}$ in $\mathcal{P}(V)$ gibt und auch, dass unendlich viele Primzahlen $p \equiv 1 \pmod{20}$ nicht in $\mathcal{P}(V)$ liegen. Weitere Resultate erzielte Ward (1961), der zum Schluss kam, dass es keine endliche Menge von Kongruenzen gibt, aufgrund derer entschieden werden könnte, ob eine beliebige Primzahl p in $\mathcal{P}(V)$ enthalten ist oder nicht.

Angeregt durch eine Methode von Hasse (1966) und die Analyse von Ward (1961) zeigte Lagarias (1985), dass für die Folge der Lucas-Zahlen die Dichte $\delta(V)$ gleich $2/3$ ist.

Brauer (1960) und Hasse (1966) untersuchten ein Problem von Sierpiński: Bestimme die Primzahlen p, für die 2 eine gerade Ordnung modulo p hat, oder gleichbedeutend, bestimme die Primzahlen p, die die Zahlen $2^n + 1 = V_n(3, 2)$ teilen. Hasse zeigte, dass $\delta(V(3, 2)) = 17/24$. Lagarias wies darauf hin, dass Hasses Beweis auch die folgende Aussage beinhaltet: Wenn $a \geq 3$ quadratfrei ist, dann gilt $\delta(V(a + 1, a)) = 2/3$; siehe auch einen anderen Artikel von Hasse (1965).

Laxton (1969) betrachtete für jedes $a \geq 2$ die Menge $\mathcal{W}(a)$ aller binären linear rekurrenten Folgen W mit $W_1 \neq W_0$, $W_1 \neq aW_0$ und für $n \geq 2$, $W_n = (a + 1)W_{n-1} - aW_{n-2}$. Diese Menge beinhaltet die Lucas-Folgen $U(a + 1, a)$, $V(a + 1, a)$. Für jedes prime p sei

$$e_p(a) = \begin{cases} 0 & \text{wenn } p \mid a, \\ \text{Ordnung von } a \bmod b & \text{wenn } p \nmid a. \end{cases}$$

Laxton gab eine heuristische Erklärung für folgenden Effekt an: Wenn der Grenzwert

$$\frac{1}{\pi(x)} \sum_{p \leq x} \frac{e_p(a)}{p - 1}$$

für x gegen ∞ existiert, dann ist für jedes $W \in \mathcal{W}(a)$ dieser der zu erwartetende (oder durchschnittliche) Wert der Dichte der Primzahlen in $\mathcal{P}(\mathcal{W})$ (d.h., die Menge der Primzahlen, die irgendein W_n teilen).

Stephens (1976) verwendete eine Methode von Hooley (1967), der unter der Voraussetzung einer Verallgemeinerung der Riemannschen Vermutung Artins Vermutung bewiesen hatte, dass 2 eine Primi-

tivwurzel modulo p für unendlich viele Primzahlen p ist. Sei $a \geq 2$ keine echte Potenz. Angenommen, die verallgemeinerte Riemannsche Vermutung gelte für die Dedekindsche ζ-Funktion aller Körper $\mathbb{Q}(a^{1/n}, \zeta_k)$, wobei ζ_k eine primitive $k$te Einheitswurzel ist. Dann ist für jedes $x \geq 2$

$$\sum_{p \leq x} \frac{e_p(a)}{p-1} = c(a)\frac{x}{\log x} + \mathrm{O}\left(\frac{x \log\log x}{(\log x)^2}\right);$$

nach dem Primzahlsatz existiert der oben betrachtete Grenzwert und ist gleich $c(a)$. Stephens wertete $c(a)$ aus. Es sei

$$C = \prod_p \left(1 - \frac{p}{p^3 - 1}\right),$$

sowie $a = a_1 \cdot (a_2)^2$ mit quadratfreiem a_1. Sei weiter r die Anzahl der verschiedenen Primfaktoren von a_1 und f definiert durch

$$f = \begin{cases} -\frac{2}{5} & \text{wenn } a_1 \equiv 1 \pmod 4, \\ -\frac{1}{64} & \text{wenn } a_1 \equiv 2 \pmod 4, \\ -\frac{1}{20} & \text{wenn } a_1 \equiv 3 \pmod 4. \end{cases}$$

Dann gilt

$$c(a) = C\left[1 - (-1)^r f \prod_{\substack{q \mid a_1 \\ q \text{ prim}}} \frac{q}{q^3 - q - 1}\right].$$

Stephens zeigte auch, dass obige Abschätzung auch ohne die Annahme der Riemannschen Vermutung im Durchschnitt richtig ist. Genauer: Sei $a \geq 2$ (wie zuvor), $e > 1$ und $x \geq 1$. Dann gibt es $c_1 > 0$ derart, dass wenn $N > \exp\{c_1(\log x)^{\frac{1}{2}}\}$, dann

$$\sum_{x \leq N} \sum_{p \leq x} \frac{e_p(a)}{p-1} = C\int_1^x \frac{dt}{t} + \mathrm{O}\left(\frac{x}{(\log x)^e}\right).$$

B Primitive Faktoren von Lucas-Folgen

Es sei p eine Primzahl. Wenn $\rho_U(p) = n$ (bzw. $\rho_V(p) = n$), dann nennt man p einen *primitiven Faktor* von $U_n(P,Q)$ (bzw. $V_n(P,Q)$). Es bezeichne $\mathrm{Prim}(U_n)$ die Menge der primitiven Faktoren von U_n, und

analog $\mathrm{Prim}(V_n)$ die Menge der primitiven Faktoren von V_n. Sei $U_n = U_n^* \cdot U_n'$, $V_n = V_n^* \cdot V_n'$, wobei $\mathrm{ggT}(U_n^*, U_n') = 1$, $\mathrm{ggT}(V_n^*, V_n^1) = 1$ und $p \mid U_n^*$ (bzw. $p \mid V_n^*$) genau dann, wenn p ein primitiver Faktor von U_n (bzw. V_n) ist. U_n^*, (bzw. V_n^*) heißt *primitiver Teil* von U_n (bzw. V_n). Aus $U_{2n} = U_n \cdot V_n$ folgt, dass $U_{2n}^* \mid V_n^*$ und somit, $\mathrm{Prim}(U_{2n}) \subseteq \mathrm{Prim}(V_n^*)$. Es ist nicht ausgeschlossen, dass $U_n^* = 1$ (bzw. $V_n^* = 1$); ich werde diese Frage behandeln.

Existenz primitiver Faktoren

Das Studium der primitiven Faktoren von Lucas-Folgen geht auf Bang und Zsigmondy im Zusammenhang mit speziellen Lucas-Folgen zurück (siehe unten). Der erste Hauptsatz stammt von Carmichael (1913):

3.11. Es sei $(P, Q) \in \mathcal{S}$ und $D > 0$.

1. Wenn $n \neq 1, 2, 6$, dann gilt $\mathrm{Prim}(U_n) \neq \varnothing$, mit der einzigen Ausnahme $(P, Q) = (1, -1)$, $n = 12$ (was zur Fibonacci-Zahl $U_{12} = 144$ führt).
   Desweiteren ist $\mathrm{Prim}(U_n) \neq \varnothing$, wenn D ein Quadrat ist und $n \neq 1$, mit der einzigen Ausnahme $(P, Q) = (3, 2)$, $n = 6$ (was die Zahl $2^6 - 1 = 63$ ergibt).
2. Wenn $n \neq 1, 3$, dann gilt $\mathrm{Prim}(V_n) \neq \varnothing$, mit der einzigen Ausnahme $(P, Q) = (1, -1)$, $n = 6$ (was die Lucas-Zahl $V_6 = 18$ ergibt).
   Darüberhinaus ist $\mathrm{Prim}(V_n) \neq \varnothing$, wenn D ein Quadrat ist und $n \neq 1$, mit der einzigen Ausnahme $(P, Q) = (3, 2)$, $n = 3$ (was zur Zahl $2^3 + 1 = 9$ führt).

In seinem Artikel bewies Carmichael zudem, dass wenn p kein Teiler von D ist und $p \in \mathrm{Prim}(U_n)$, dann $p \equiv \pm 1 \pmod{n}$, während wenn $p \in \mathrm{Prim}(V_n)$, so $p \equiv \pm 1 \pmod{2n}$.

Das Resultat von Carmichael wurde von Lekkerkerker (1953) erweitert:

> Auch ohne die Annahme $\mathrm{ggT}(P, Q) = 1$ gibt es für $D > 0$ nur endlich viele n derart, dass $U_n(P, Q)$ (bzw. $V_n(P, Q)$) keinen primitiven Faktor hat.

Durst (1961) bewies:

3.12. Sei $(P, Q) \in \mathcal{S}$ und $D > 0$. Dann hat $U_6(P, Q)$ genau dann keinen primitiven Faktor, wenn eine der folgenden Bedingungen erfüllt ist:

1. $P = 2^{t+1} - 3r$, $Q = (2^t - r)(2^t - 3r)$, wobei $t \geq 1$, $2^{t+1} > 3r$ und r ungerade und positiv ist.
2. $P = 3^s k$, $Q = 3^{2s-1}k^2 - 2^t$, wobei $s \geq 1$, $t \geq 0$, $k \equiv \pm 1 \pmod 6$ und $3^{2s-1}k^2 < 2^{t+2}$.

Somit gibt es unendlich viele Paare (P, Q), für die $U_6(P, Q)$ keinen primitiven Faktor besitzt. DURST betrachtete auch solche Parameterpaare (P, Q), bei denen $\mathrm{ggT}(P, Q)$ größer als 1 sein kann.

3.13. Es sei I eine endliche Menge ganzer Zahlen mit $1 \in I$. Dann gibt es unendlich viele Paare (P, Q) mit $P \geq 1$, $P \neq Q$, $2Q$, $3Q$, $4Q$, $P^2 - 4Q > 0$ derart, dass $\mathrm{Prim}(U(P, Q)) = I$.

Für $D < 0$ gilt obige Aussage nicht mehr ohne Weiteres. Zum Beispiel wird für $(P, Q) = (1, 2)$ und $n = 1, 2, 3, 5, 8, 12, 13, 18$, $\mathrm{Prim}(U_n) = \varnothing$.

Im Jahr 1962 untersuchte SCHINZEL den Fall $D < 0$. Die folgende Aussage ist ein Korollar eines allgemeineren Resultats, zu dem er 1974 gelangte.

3.14. Es gibt $n_0 > 0$ derart, dass $U_n(P, Q)$, $V_n(P, Q)$ für alle $n \geq n_0$, $(P, Q) \in \mathcal{S}$ einen primitiven Faktor haben.

Der Beweis verwendet BAKERs untere Schranken für Linearformen in Logarithmen; n_0 ist effektiv berechenbar. Es ist dabei wichtig zu betonen, dass n_0 unabhängig von den Parametern ist. STEWART (1977A) zeigte, dass $n_0 \leq e^{452}4^{67}$. STEWART bewies auch, dass es für $n > 4$, $n \neq 6$ nur endlich viele, im Prinzip explizit bestimmbare Lucas-Folgen $U(P, Q)$, $V(P, Q)$ der angegebenen Art gibt, so dass $U_n(P, Q)$ (bzw. $V_n(P, Q)$) keinen primitiven Faktor besitzt.

VOUTIER (1995) verwendete eine von TZANAKIS (1989) entwickelte Methode, um Thues Gleichungen zu lösen und bestimmte für jedes n, $4 < n \leq 30$, $n \neq 6$, die endliche Menge von Parametern $(P, Q) \in \mathcal{S}$, für die $U_r(P, Q)$ keinen primitiven Faktor hat.

Das nächste Ergebnis von GYÖRY (1981) betrifft Elemente von Lucas-Folgen, die Primfaktoren einer gegebenen Menge besitzen. Es sei E eine endliche Menge von Primzahlen. $E^\times$ bezeichne die Menge aller natürlichen Zahlen, deren Primfaktoren aus E stammen.

3.15. Sei $s > 1$ und $E = \{p \text{ prim} \mid p \leq s\}$. Es gibt effektiv berechenbare $c_1 = c_1(s) > 0$, $c_2 = c_2(s) > 0$ derart, dass wenn $(P, Q) \in \mathcal{S}$, $4 < n$, und $U_n(P, Q) \in E^\times$, dann

$$n \leq \max\{s+1,\, e^{452} \cdot 2^{67}\},$$

und $\max\{P, |Q|\} \leq c_1$ sowie $|U_n(P,Q)| \leq c_2$.

Im Jahr 1982 gab GYÖRY einen Wert für die Konstanten an. Ein interessantes Korollar ist das folgende:

3.16. Sei $s > 1$ und $E = \{p \text{ prim} \mid p \leq s\}$. Es gibt ein effektiv berechenbares $c_3 = c_3(s) > 0$ derart, dass wenn $a > b \geq 1$ ganze Zahlen mit $\mathrm{ggT}(a,b) = 1$ sind und wenn $3 < n$, $\frac{a^n - b^n}{a-b} = m \in E^{\times}$, dann gilt $n < s$ und $\max\{a, m\} < c_3$.

Spezialfälle. Der folgende, sehr nützliche Satz wurde von ZSIGMONDY (1892) bewiesen; der Fall $a = 2$, $b = 1$ war bereits vorher von BANG (1886) betrachtet worden. ZSIGMONDYs Satz wurde des Öfteren wiederentdeckt (BIRKHOFF (1904), CARMICHAEL (1913), KANOLD (1950), ARTIN (1955), und LÜNEBURG (1981), der einen einfacheren Beweis angab). Ein leicht zugänglicher Beweis findet sich in RIBENBOIM (1994).

Sei $a > b \geq 1$, $\mathrm{ggT}(a,b) = 1$. Betrachte die Folge der Binomialzahlen

$$(a^n - b^n)_{n \geq 0}.$$

Falls $P = a + b$, $Q = ab$, so $a^n - b^n = U_n(P,Q) \cdot (a-b)$. Die Primzahl p nennt man *primitiven Faktor* von $a^n - b^n$, wenn $p \mid a^n - b^n$ aber $p \nmid a^m - b^m$ für alle m, $1 \leq m < n$. Es bezeichne $\mathrm{Prim}(a^n - b^n)$ die Menge aller primitiven Faktoren von $a^n - b^n$. Es ist offensichtlich, dass für $n > 1$ gilt, $\mathrm{Prim}(a^n - b^n) = \mathrm{Prim}(U_n(P,Q)) \setminus \{p \mid p \text{ teilt } a - b\}$.

3.17. Sei $a > b \geq 1$, $\mathrm{ggT}(a,b) = 1$.

1. Für jedes $n > 1$ hat die Binomialzahl $a^n - b^n$ einen primitiven Faktor, ausgenommen in den folgenden Fällen:
   $a = 2$, $b = 1$, $n = 6$ (dies führt zu $2^6 - 1 = 63$),
   a, b sind ungerade, $a + b$ ist eine Zweierpotenz, $n = 2$.
   Darüberhinaus hat jeder primitive Faktor von $a^n - b^n$ die Form $kn + 1$.
2. Für jedes $n > 1$ hat die Binomialzahl $a^n + b^n$ einen primitiven Faktor, ausgenommen den Fall $a = 2$, $b = 1$, $n = 3$ (dies ergibt $2^3 + 1 = 9$).

Die Anzahl primitiver Faktoren

Ich betrachte nun den primitiven Teil von Gliedern der Lucas-Folgen und untersuche die Anzahl der verschiedenen Primfaktoren von U_n^*, V_n^*. Die folgende Frage ist ungeklärt: Gibt es zu $(P,Q) \in \mathcal{S}$ unendlich viele $n \geq 1$ derart, dass $\#(\mathrm{Prim}(U_n)) = 1$, bzw. $\#(\mathrm{Prim}(V_n)) = 1$, d.h. U_n^* (bzw. V_n^*) ist eine Primzahlpotenz? Diese Frage ist vermutlich sehr schwer zu beantworten. Im nächsten Unterabschnitt (c) wird ein ähnliches Problem angesprochen.

Ich werde nun Bedingungen angeben, die zur Folge haben, dass

$$\#(\mathrm{Prim}(U_n)) \geq 2 \quad \text{und} \quad \#(\mathrm{Prim}(V_n)) \geq 2.$$

Für irgendeine ganze Zahl c ungleich 0 bezeichne $k(c)$ den *quadratfreien Kern* von c, d.h. c geteilt durch seinen größten quadratischen Faktor. Für $(P,Q) \in \mathcal{S}$ sei $M = \max\{P^2 - 4Q, P^2\}$, $\kappa = \kappa(P,Q) = k(MQ)$ und definiere

$$\eta = \eta(P,Q) = \begin{cases} 1 & \text{wenn } \kappa \equiv 1 \pmod 4, \\ 2 & \text{wenn } \kappa \equiv 2 \text{ oder } 3 \pmod 4. \end{cases}$$

Schinzel (1963a) zeigte (siehe auch Rotkiewicz (1962) für den Fall $Q > 0$ und $D > 0$):

3.18. Es gibt effektiv berechenbare endliche Teilmengen $\mathcal{M}_0$, $\mathcal{N}_0$ von $\mathcal{S}$ sowie für jedes $(P,Q) \in \mathcal{S}$ eine effektiv berechenbare ganze Zahl $n_0(P,Q) > 0$ derart, dass mit $(P,Q) \in \mathcal{S}$, $\eta \neq 1, 2, 3, 4, 6$ und $\frac{n}{\eta\kappa}$ ungerade gilt $\#(\mathrm{Prim}(U_n(P,Q))) \geq 2$. Dabei gibt es folgende Ausnahmen:

1. $D = P^2 - 4Q > 0$:

$$n = \eta \cdot |\kappa| \ \text{ und } \ (P,Q) \in \mathcal{M}_0\,;$$
$$n = 3 \cdot \eta \cdot |\kappa| \ \text{ und } \ (P,Q) \in \mathcal{N}_0\,;$$
$$(n,P,Q) = (2D,1,-2),\ (2D,3,2)$$

2. $D = P^2 - 4Q < 0$:

$$(n,P,Q) \text{ mit } n \leq n_0(P,Q).$$

Somit gibt es für jedes $(P,Q) \in \mathcal{S}$ unendlich viele n mit der Eigenschaft, dass $\#(\mathrm{Prim}(U_n(P,Q))) \geq 2$. Schinzel gab Mengen $\mathcal{M}$, $\mathcal{N}$ mit jeweils enthaltenen Ausnahmemengen $\mathcal{M}_0$, $\mathcal{N}_0$ an, die später in einer allerdings unveröffentlichten Berechnung von Brillhart und Selfridge vollständig bestimmt wurden. An späterer Stelle werde ich auf das folgende Korollar zurückgreifen:

3.19. Sei $(P,Q) \in \mathcal{S}$ mit Q ein Quadrat und $D > 0$. Wenn $n > 3$, dann

$$\#(\mathrm{Prim}(U_n(P,Q))) \geq 2,$$

mit der Ausnahme $(n,P,Q) = (5,3,1)$.

Somit ist insbesondere $U_n(P,Q)$ keine Primzahl, wenn $n > 3$ und Q ein Quadrat ist, es sei denn $(n,P,Q) = (5,3,1)$.

Wegen $\mathrm{Prim}(U_n(P,Q)) \subseteq \mathrm{Prim}(V_n(P,Q))$ ist es einfach, aus **(3.16)** Bedingungen abzuleiten, die $\#(\mathrm{Prim}(V_n(P,Q))) \geq 2$ zur Folge haben; insbesondere gibt es für jedes $(P,Q) \in \mathcal{S}$ unendlich viele solcher Indizes n.

Diese Ergebnisse wurden in nachfolgenden Arbeiten von Schinzel (1963), (1968) verschärft, diese gehen aber zu sehr ins Detail, um sie hier vorzustellen. Es ist zweckmäßiger, Folgendes zu betrachten:

Spezialfälle. Seien $a > b \geq 1$ teilerfremde Zahlen und $P = a + b$, $Q = ab$, also $U_n(P,Q) = \frac{a^n - b^n}{a-b}$, $V_n(P,Q) = a^n + b^n$. Selbst für diese speziellen Folgen ist nicht bekannt, ob es unendlich viele n derart gibt, dass $\#\,\mathrm{Prim}(U_n(P,Q)) = 1$, bzw. $\#\,\mathrm{Prim}(V_n(P,Q)) = 1$.

Schinzel (1962b) bewies den folgenden Satz, der einen Spezialfall von **(3.16)** darstellt. Sei $\kappa = k(a,b)$,

$$\eta = \begin{cases} 1 & \text{wenn } \kappa \equiv 1 \pmod 4, \\ 2 & \text{wenn } \kappa \equiv 2 \text{ oder } 3 \pmod 4. \end{cases}$$

3.20. Unter obigen Voraussetzungen:

1. Wenn $n > 20$ und $\frac{n}{\eta\kappa}$ eine ungerade ganze Zahl ist, dann gilt $\#\,\mathrm{Prim}(\frac{a^n-b^n}{a-b}) \geq 2$.
2. Wenn $n > 10$ und κ gerade sowie $\frac{n}{\kappa}$ eine ungerade ganze Zahl ist, dann gilt $\#\,\mathrm{Prim}(a^n + b^n) \geq 2$.

Somit existieren unendlich viele n derart, dass $\#\,\mathrm{Prim}(\frac{a^n-b^n}{a-b}) \geq 2$ bzw. $\#\,\mathrm{Prim}(a^n + b^n) \geq 2$. Schinzel zeigte auch:

3.21. Unter obigen Voraussetzungen: Wenn $\kappa = c^h$, wobei $h \geq 2$ wenn $k(c)$ ungerade und $h \geq 3$ wenn $k(c)$ gerade ist, dann gibt es unendlich viele n derart, dass $\#\,\mathrm{Prim}(\frac{a^n-b^n}{a-b}) \geq 3$.

Für beliebige (a,b) mit $a > b \geq 1$, $\mathrm{ggT}(a,b) = 1$ ist jedoch nicht bekannt, ob es unendlich viele n mit $\#\,\mathrm{Prim}(\frac{a^n-b^n}{a-b}) \geq 3$ gibt.

Potenzteiler des primitiven Teils

Man weiß nichts darüber, wann der primitive Teil von Potenzen geteilt wird, außer dass es selten passiert. Um den Schwierigkeitsgrad der Frage einschätzen zu können, bietet es sich an, sofort den sehr speziellen Fall $(P, Q) = (3, 2)$, also $U_n = 2^n - 1$, $V_n = 2^n + 1$ zu betrachten. Man erinnere sich, dass wenn $n = q$ prim ist, $U_q = 2^q - 1$ eine *Mersenne-Zahl* genannt wird, gewöhnlich mit $M_q = U_q = 2^q - 1$ bezeichnet. Darüberhinaus nennt man im Falle $n = 2^m$ die Zahl $V_{2^m} = 2^{2^m} + 1$ eine *Fermat-Zahl*, hier ist die Bezeichnung $F_m = V_{2^m} = 2^{2^m} + 1$ gebräuchlich.

Die folgenden Tatsachen lassen sich leicht zeigen: $\mathrm{ggT}(M_q, M_p) = 1$ wenn $p \neq q$, und $\mathrm{ggT}(F_m, F_n) = 1$ wenn $m \neq n$. Es folgt, dass M_q, F_m mit ihren primitiven Teilen übereinstimmen.

Eine natürliche Zahl, die ein Produkt von echten Potenzen ist, nennt man eine *quadratvolle Zahl*.

Ich gebe jetzt einige miteinander verwandte Aussagen an, von denen allerdings keine je nachgewiesen werden konnte.

(M) Es gibt unendlich viele Primzahlen p derart, dass M_p quadratfrei ist.
(M′) Es gibt unendlich viele Primzahlen p derart, dass M_p nicht quadratvoll ist.
(F) Es gibt unendlich viele n derart, dass F_n quadratfrei ist.
(F′) Es gibt unendlich viele n derart, dass F_n nicht quadratvoll ist.
(B) Es gibt unendlich viele n derart, dass der primitive Teil von $2^n - 1$ quadratfrei ist.
(B′) Es gibt unendlich viele n derart, dass der primitive Teil von $2^n - 1$ nicht quadratvoll ist.
(C) Es gibt unendlich viel n derart, dass der primitive Teil von $2^n + 1$ quadratfrei ist.
(C′) Es gibt unendlich viele n derart, dass der primitive Teil von $2^n + 1$ nicht quadratvoll ist.

Diese und weitere, ähnliche Aussagen werden in Kapitel 9 behandelt. Dort wird auch erklärt, warum ein Beweis einer jeden der obigen Vermutungen wohl sehr schwierig sein wird.

Der größte Primfaktor von Gliedern von Lucas-Folgen

Das Problem der Abschätzung der Größe des größten Primfaktors von Gliedern der Lucas-Folgen war Gegenstand vieler interessanter Arbeiten.

Für eine natürliche Zahl n bezeichne $P[n]$ den größten Primfaktor und $\nu(n)$ die Anzahl der verschiedenen Primfaktoren von n. Die Anzahl $q(n)$ der verschiedenen quadratfreien Faktoren von n ist somit $q(n) = 2^{\nu(n)}$. Es gab auch Arbeiten darüber, die Größe $Q[n]$ des größten quadratfreien Faktors von n abzuschätzen, darauf soll aber hier nicht eingegangen werden.

Für $n \geq 1$ bezeichne $\Phi_n(X, Y) \in \mathbb{Z}[X, Y]$ das $n$te homogenisierte Kreisteilungspolynom

$$\Phi_n(X, Y) = \prod_{\substack{\mathrm{ggT}(i,n)=1 \\ 1 \leq i \leq n}} (X - \zeta^i Y),$$

wobei ζ eine primitive $n$te Einheitswurzel ist; somit hat $\Phi_n(X, Y)$ den Grad $\varphi(n)$ (die Eulersche φ-Funktion).

Wenn P, Q ganze Zahlen ungleich 0 sind, $D = P^2 - 4Q \neq 0$ und α, β die Nullstellen von $X^2 - PX + Q$ sind, dann ist $\Phi_n(\alpha, \beta) \in \mathbb{Z}$ (für $n \geq 2$) und $\alpha^n - \beta^n = \prod_{d|n} \Phi_d(\alpha, \beta)$.

Es folgt leicht, dass

$$P\left[\frac{\alpha^n - \beta^n}{\alpha - \beta}\right] \geq P[\Phi_n(\alpha, \beta)],$$
$$P[\alpha^n - \beta^n] \geq P[\Phi_n(\alpha, \beta)],$$
$$P[\alpha^n + \beta^n] \geq P[\Phi_{2n}(\alpha, \beta)].$$

Es genügt daher, untere Abschätzungen für $P\,[\Phi_n(\alpha, \beta)]$ zu finden.

Das erste Ergebnis stammt von Zsigmondy (1892) und wiederum von Birkhoff (1904): *Wenn a, b teilerfremde ganze Zahlen sind und $a > b \geq 1$, dann gilt $P[a^n - b^n] \geq n+1$ und $P[a^n + b^n] \geq 2n+1$ (mit der Ausnahme $2^3 + 1 = 9$).* Schinzel ergänzte dazu (1962): *Wenn ab ein Quadrat oder das Zweifache eines Quadrats ist, dann ist $P[a^n - b^n] \geq 2n + 1$, ausgenommen im Fall $a = 2$, $b = 1$ und $n = 4$, 6, 12.*

In seiner Arbeit über primitive Faktoren von Lucas-Folgen mit $D > 0$ zeigte Carmichael (1913), dass wenn $n > 12$, dann $P[U_n] \geq n - 1$ und $P[V_n] \geq 2n - 1$. Erdös (1965) vermutete:

$$\lim_{n \to \infty} \frac{P[2^n - 1]}{n} = \infty.$$

Dieses Problem und damit verwandte, nach wie vor offene Fragen waren Gegenstand ausführlicher Untersuchungen von Stewart (siehe Stewart (1975, 1977b); Shorey (1981); Stewart (1982, 1985)).

Mehrere der Ergebnisse, die ich nun vorstelle, betreffen den größten Primfaktor für den Fall, dass der Index n Element einer Menge mit asymptotischer Dichte 1 ist.

Eine Teilmenge S von $\mathbb{N}$ hat die asymptotische Dichte γ, $0 \le \gamma \le 1$, wobei

$$\lim_{N\to\infty} \frac{\#\{n \in S \mid n \le N\}}{N} = \gamma.$$

Beispielsweise hat die Menge $\mathcal{P}$ der Primzahlen die asymptotische Dichte 0.

Die Verknüpfung des Primzahlsatzes mit der Tatsache, dass jeder primitive Faktor von $\Phi_n(a,b)$ die Form $hn+1$ hat ergibt:

3.22. Es gibt eine Menge T mit asymptotischer Dichte 1 derart, dass

$$\lim_{\substack{n\to\infty \\ n\in T}} \frac{P[\Phi(a,b)]}{n} = \infty.$$

Insbesondere gilt $\lim_{n\to\infty, n\in T} \frac{P[2^n-1]}{n} = \infty$, wobei T eine Menge mit asymptotischer Dichte 1 ist. Obiges Resultat wurde präzisiert und auf Folgen mit beliebiger Diskriminante $D \neq 0$ ausgedehnt. Sei $0 \le \kappa \le 1/\log 2$. Definiere die Menge

$$\mathcal{N}_\kappa = \{n \in \mathbb{N} \mid n \text{ hat höchstens } \kappa \log\log n \text{ verschiedene Primfaktoren}\}.$$

Zum Beispiel gilt $\mathcal{P} \subset \mathcal{N}_\kappa$ für jedes κ wie oben. Ein klassisches Resultat (siehe das Buch von Hardy und Wright (1938)) ist das Folgende: Wenn $0 \le \kappa \le 1/\log 2$, dann hat $\mathcal{N}_\kappa$ die asymptotische Dichte 1.

Mit anderen Worten, „die meisten“ natürlichen Zahlen haben „wenige“ verschiedene Primfaktoren.

Das folgende Ergebnis stammt von Stewart (1977b) für reelle α, β und von Shorey (1981) für beliebige α, β.

3.23. Es sei κ, α, β wie oben. Wenn $n \in \mathcal{N}_\kappa$, $n \ge 3$, dann

$$P[\Phi_n(\alpha,\beta)] \ge C\varphi(n)\frac{\log n}{q(n)},$$

wobei $C \ge 0$ eine effektiv berechenbare Zahl ist, die nur von α, β und κ abhängt.

Man erinnere sich, dass $q(n) = 2^{\nu(n)}$ und $\nu(n) \le \kappa \log\log n$. Es folgt mit geeigneten Konstanten $C_1 > 0$ und $C_2 > 0$, dass

$$P[\Phi_n(\alpha,\beta)] > C_1 \frac{n \log n}{2^{\nu(n)} \log(1+\nu(n))}$$

und

$$P[\Phi_n(\alpha,\beta)] > C_2 \frac{n \log n^{1-\kappa \log 2}}{\log\log\log n}.$$

Insbesondere gelten die obigen Abschätzungen für $n \in \mathcal{N}_\kappa$, $n > 3$ und jede Lucas-Folge $U_n(P,Q)$, $V_n(P,Q)$ sowie $\alpha^n - \beta^n$.

Da $\nu(p) = 1$ für jede Primzahl p, folgt

$$P[a^p - b^p] \geq Cp \log p,$$
$$P[a^p + b^p] \geq Cp \log p$$

(mit geeignetem $C > 0$). Insbesondere ergibt sich für die Mersenne-Zahlen $M_p = 2^p - 1$,

$$P[2^p - 1] \geq Cp \log p,$$

und für die Fermat-Zahl $F_m = 2^{2^m} + 1$,

$$P[2^{2^m} + 1] \geq Cm \times 2^m,$$

diese Abschätzung lässt sich allerdings auch auf direkte Weise gewinnen, worauf D. Knayswick hinwies.

Stewart konnte noch schärfere, ins Technische gehende Ausdrücke für untere Schranken von $P[\Phi_n(\alpha,\beta)]$ angeben und er vermutete, dass

$$P[\Phi(\alpha,\beta)] > C[\varphi(n)]^2$$

für reelle α, β und jedes $n > 3$ erfüllt ist, wobei $C > 0$ eine effektiv berechenbare Zahl ist (abhängig von α, β). Dies gilt dann, wenn n quadratfrei ist.

Unter Verwendung einer verfeinerten Form von Bakers unteren Schranken für Linearformen in Logarithmen (wie von Waldschmidt (1980) angegeben), bewies Stewart (1982) das folgende Resultat, das für alle $n > C_0$ gilt (eine absolute Konstante):

3.24. Für jedes $(P,Q) \in \mathcal{S}$ gibt es eine effektiv berechenbare Zahl $C_1 = C_1(P,Q) > 0$ derart, dass wenn $n > C_0$, dann sind $P[U_n]$ und $P[V_n]$ nach unten beschränkt durch

$$\max\left\{ n-1, C_1 \frac{n \log n}{q(n)^{\frac{4}{3}}} \right\}.$$

Der folgende Satz hat zwar keine weitere Auswirkung, gibt aber schärfere Schranken für Mengen mit asymptotischer Dichte 1 an (Stewart (1982)):

3.25. Sei $f : \mathbb{N} \to \mathbb{R}_{>0}$ eine beliebige Funktion mit $\lim f(n) = 0$. Für jedes $(P, Q) \in \mathcal{S}$ gibt es eine Menge $T \subseteq \mathbb{N}$ mit asymptotischer Dichte 1 derart, dass für $n \in T$ gilt

$$P[U_n] \geq f(n) \frac{n(\log n)^2}{\log \log n}.$$

Stewart studierte neben den Lucas-Folgen auch andere linear rekurrente Folgen und gab Resultate für Folgen mit einer Ordnung höher als 2 an, die hier jedoch nicht behandelt werden sollen. Eine umfangreiche Untersuchung ist in Stewart (1985) zu finden.

Ein interessantes Ergebnis in diesem Zusammenhang war bereits früher von Mahler (1966) erzielt worden:

3.26. Sei $Q \geq 2$, $D = P^2 - 4Q < 0$ und E eine endliche Menge von Primzahlen. Es bezeichne $E^{\times}[U_n]$ den größten Faktor von U_n, wobei die Primfaktoren sämtlich Element von E seien. Für $0 < \epsilon < \frac{1}{2}$ gibt es $n_0 > 1$ derart, dass wenn $n > n_0$, so $\left| \frac{U_n}{E^{\times}[U_n]} \right| > Q^{(1/2-\epsilon)n}$. Insbesondere gilt $\lim P[U_n] = \infty$.

Der Beweis verwendet p-adische Methoden.

4 Primzahlen in Lucas-Folgen

Es seien U, V die Lucas-Folgen mit Parametern $(P, Q) \in S$.

Die wichtigsten Fragen im Zusammenhang mit Primzahlen in Lucas-Folgen sind die folgenden:

1. Gibt es $n > 1$ derart, dass $U_n(P, Q)$ bzw. $V_n(P, Q)$ eine Primzahl ist?
2. Gibt es unendlich viele $n > 1$ derart, dass $U_n(P, Q)$ bzw. $V_n(P, Q)$ prim ist?

Ich werde die verschiedenen Möglichkeiten besprechen und angeben, was man über die wichtigsten Spezialfälle weiß.

Das folgende Beispiel zeigt eine Lucas-Folge mit nur einem Primzahlglied, nämlich U_2:
$U(3, 1)$: 0 1 3 8 21 55 144 377 987 ...

Dies wurde im Anschluss an **(3.19)** angemerkt. Auf gleiche Weise erhält man mit ungeraden a und b und $a > b \geq 1$ sowie $P = a + b$, $Q = ab$, dass $V_n(P, Q) = a^n + b^n$ für jedes $n \geq 1$ gerade ist und somit keine Primzahl sein kann.

Durch Anwendung von CARMICHAELs Satz **(3.11)** über die Existenz primitiver Faktoren gewinnt man einfach:

4.1. Wenn $D > 0$ und $U_n(P, Q)$ prim ist, dann ist $n = 2$, 4 oder n ist eine ungerade Primzahl. Wenn $V_n(P, Q)$ prim ist, dann ist n entweder auch prim oder eine Zweierpotenz.

Dieser Satz gilt nicht für $D < 0$, wie dieses Beispiel zeigt:

Sei $(P, Q) = (1, 2)$, also $D = -7$ und

$$U(1,2)\colon\ 0\ 1\ 1\ -1\ -3\ -1\ 5\ 7\ -3\ -17\ -11\ 23\ 45\ -1\ -91\ -89\ \ldots$$

In diesem Beispiel sind $U_6, U_8, U_9, U_{10}, U_{15}, \ldots$ sämtlich Primzahlen.

Genauso sind beispielsweise in $V(1, 2)$ die Glieder $|V_9|$ und $|V_{10}|$ prim.

Spezialfälle. In ihrem Artikel von 1999 geben DUBNER und KELLER alle Indizes $n < 50\,000$ an, für die die Fibonacci-Zahl U_n bzw. die Lucas-Zahl V_n Primzahlen sind: U_n ist prim für $n = 3$, 4, 5, 7, 11, 13, 17, 23, 29, 43, 47, 83, 131, 137, 359, 431, 433, 449, 509, 569, 571, $2971^{(W)}$, $4723^{(M)}$, $5387^{(M)}$, $9311^{(DK)}$ [W: entdeckt von H. C. WILLIAMS; M: entdeckt von F. MORAIN; DK: entdeckt von H. DUBNER und W. KELLER].

Darüber hinaus ist U_n im Bereich $n < 50\,000$ für $n = 9677$, 14431, 25561, 30757, 35999, 37511 eine *Quasiprimzahl*[2] (und für kein anderes $n < 50\,000$). Dies bedeutet, dass diese Zahlen Zerlegbarkeitstest widerstanden.

Für $n \leq 50\,000$ ist V_n für $n = 2$, 4, 5, 7, 8, 11, 13, 16, 17, 19, 31, 37, 41, 47, 53, 61, 71, 79, 113, 313, 353, $503^{(W)}$, $613^{(W)}$, $617^{(W)}$, $863^{(W)}$, $1097^{(DK)}$, $1361^{(DK)}$, $4787^{(DK)}$, $4793^{(DK)}$, $5851^{(DK)}$, $7741^{(DK)}$, $10691^{(DK)}$, $14449^{(DK)}$ als prim nachgewiesen [W: entdeckt von H. C. WILLIAMS; DK: entdeckt von H. DUBNER und W. KELLER].

Darüber hinaus ist V_n für $n = 8467$, 12251, 13963, 19469, 35449, 36779, 44507 (und für kein anderes $n \leq 50\,000$) quasiprim.

Aufgrund der Größe der Primzahlkandidaten ist es notwendig, ein Primzahlzertifikat zu erstellen.

[2] Engl.: *probable prime*

Der Artikel von Dubner und Keller erhält noch viele weitere Faktorisierungen; es handelt sich um eine Fortsetzung vorangegangener Arbeiten vieler anderer Mathematiker; hier seien vor allem erwähnt: Jarden (1958), Brillharts Ausgabe von Jardens Buch (1973) und der Artikel von Brillhart (1988), der vollständige Faktorisierungen von U_n (für $n \leq 1000$) und V_n (für $n \leq 500$) enthält.

Die zu $a = 2$, $b = 1$ gehörigen Lucas-Folgen sind $U_n = 2^n - 1$ und $V_n = 2^n + 1$.

Wenn nun U_n eine Primzahl ist, so gilt dies schon für $n = q$ und $M_q = U_q = 2^q - 1$ ist eine Mersenne-Primzahl. Wenn V_n eine Primzahl ist, dann gilt $n = 2^m$ und $F_m = 2^{2^m} + 1$ ist eine Fermat-Primzahl.

Bisher sind nur 46 Mersenne-Primzahlen bekannt, die größte davon $M_{43112609}$, die 2008 als Primzahl nachgewiesen wurde; es handelt sich um eine Zahl mit über 10 Millionen Ziffern. Demgegenüber ist die größte bekannte Fermat-Primzahl F_4. Eine detaillierte Diskussion über Mersenne- und Fermat-Zahlen findet sich in meinem Buch *Die Welt der Primzahlen* (2006) .

Man glaubt, dass es unendlich viele Mersenne-Primzahlen gibt. Im Falle der Fermat-Primzahlen sind die vorhandenen Information nicht ausreichend, um irgendeine Vermutung zu belegen.

5 Potenzen und quadratvolle Zahlen in Lucas-Folgen

In diesem Abschnitt werde ich mich den folgenden Fragen zuwenden. Es seien U, V die Lucas-Folgen mit Parametern $(P, Q) \in \mathcal{S}$. Betrachte für $k \geq 1$, $h \geq 2$ die Menge

$$\mathcal{C}_{U,k,h} = \{U_n \mid U_n = kx^h, \text{ mit } |x| \geq 2\}.$$

Sei $\mathcal{C}_{U,k} = \bigcup_{h \geq 2} \mathcal{C}_{U,k,h}$, also besteht $\mathcal{C}_{U,k}$ aus allen U_n der Form $U_n = kx^h$ für ein $|x| \geq 2$ und $h \geq 2$. Im Fall $k = 1$ erhält man die Menge aller U_n, die echte Potenzen sind.

In gleicher Weise sei

$$\mathcal{C}^*_{U,k} = \{U_n \mid U_n = kt, \text{ wobei } t \text{ eine quadratvolle Zahl ist}\}.$$

Für $k = 1$ ergibt sich die Menge aller U_n, die quadratvolle Zahlen sind.

Analoges sei für die Mengen $\mathcal{C}_{V,k,h}$ und $\mathcal{C}_{V,k}*$ in Verbindung mit der Folge V definiert.

Die wesentliche Frage ist es herauszufinden, ob und wann obige Mengen leer, endlich oder unendlich sind, und sie wenn möglich genau zu bestimmen.

Ein verwandtes Problem betrifft die Quadratklassen in den Folgen U, V.

U_n, U_m heißen *quadrat-äquivalent*, wenn es ganze Zahlen a, $b \neq 0$ derart gibt, dass $U_m a^2 = U_n b^2$, oder gleichbedeutend, wenn $U_m U_n$ ein Quadrat ist. Dies ist offensichtlich eine Äquivalenzrelation auf der Menge $\{U_n \mid n \geq 1\}$, ihre Klassen nennt man *Quadratklassen der Folge* U. Wenn U_n, U_m sich in derselben Quadratklasse befinden und wenn $d = \mathrm{ggT}(U_n, U_m)$, dann gilt $U_m = dx^2$, $U_n = dy^2$, und umgekehrt.

Die Quadratklassen der Folge V sind in gleicher Weise definiert.

In Bezug auf die Quadratklassen sind die Probleme dieselben: zu bestimmen, ob es nichttriviale Quadratklassen gibt, d.h. solche, die mehr als ein Element haben; danach herauszufinden, ob es nur endlich viele nichttriviale Quadratklassen gibt, ob eine Quadratklasse endlich ist, und wenn möglich die Quadratklassen genau zu bestimmen.

Für $k \geq 1$ bedeute die Bezeichnung $k\square$ eine Zahl der Form kx^2 mit $x \geq 2$; d.h. $\square$ bezeichnet ein Quadrat größer als 1.

Die ersten Ergebnisse zu diesen Fragen waren die Bestimmungen quadratischer Fibonacci- und Lucas-Zahlen. Dies gelang mit ziemlich einfachen, aber raffinierten Argumenten. In meiner Darstellung ziehe ich es vor, zunächst die Hauptsätze anzugeben, anstatt dem Weg ihrer Entwicklung zu folgen.

A Hauptsätze für Potenzen

Der Hauptsatz von Shorey (1981, 1983) (gültig für alle nichtdegenerierten binären rekurrenten Folgen) wurde bewiesen durch scharfe untere Schranken für Linearformen in Logarithmen von Baker (1973) und einer p-adischen Version von van der Poorten (1977), unterstützt durch ein weiteres Resultat von Kotov (1976).

Man könnte auch ein Ergebnis von Shorey (1977) verwenden, worauf Pethö hinwies.

5.1. Sei $(P, Q) \in \mathcal{S}$, $k \geq 1$. Es gibt eine effektiv berechenbare Zahl $C = C(P, Q, k) > 0$ derart, dass wenn $n \geq 1$, $|x| \geq 2$, $h \geq 2$ und $U_n = kx^h$, dann n, $|x|$, $h < C$. Eine ähnliche Aussage gilt für die Folge V.

Insbesondere gibt es in einer gegebenen Lucas-Folge nur endlich viele Potenzen.

STEWARTs Artikel (1980) enthält auch das folgende Resultat, worauf MIGNOTTE und WALDSCHMIDT hinwiesen. Für $h \geq 2$, $n \geq 1$ bezeichne $[n]^h$ die $h$te Potenz, die n am nächsten kommt.

5.2. Wenn $Q = \pm 1$, dann

$$\lim_{n\to\infty} |U_n - [U_r]^h| = \infty.$$

Dies erhält man durch den Nachweis, dass es für jedes d eine effektiv berechenbare Zahl $C = C(P, d) > 0$ derart gibt, dass für $U_n = x^h + d$ mit $|x| \geq 1$, $h \geq 2$ gilt n, $|x|$, $h < C$.

Die obigen, allgemeinen Aussagen reichen nicht aus, um alle Folgenglieder U_n der Form kx^h zu bestimmen, da die angegebenen Schranken zu groß sind.

PETHÖ (1982) gab die folgende Erweiterung von **(5.1)** an (gültig für alle nicht-entarteten binären rekurrenten Folgen):

5.3. Sei E eine endliche Menge von Primzahlen und $E^\times$ die Menge aller Zahlen, deren sämtliche Primfaktoren aus E stammen. Dann gibt es zu $(P, Q) \in \mathcal{S}$ eine effektiv berechenbare, nur von P, Q und E abhängige Zahl $C > 0$ derart, dass wenn $n \geq 1$, $|x| \geq 2$, $h \geq 2$, $k \in E^\times$ und $U_n = kx^h$, dann n, $|x|$, h, $k \geq C$. Für die Folge V gilt ein analoges Resultat.

B Genaue Bestimmung bei speziellen Folgen

Ich werde nun spezielle Folgen untersuchen, und zwar diejenigen mit Parametern $(1, -1)$ (die Fibonacci- und Lucas-Zahlen), die mit Parametern $(2, -1)$ (die Pell-Zahlen) sowie für $a > 1$ solche mit Parametern $(a + 1, a)$, dabei insbesondere den Fall $(3, 2)$.

Die zu untersuchenden Fragen betreffen Quadrate, doppelte Quadrate, andere Vielfache von Quadraten, Quadratklassen, Kuben sowie höhere Potenzen.

Die Ergebnisse sind in einer Tabelle zusammengefasst (siehe Seite 37).

Quadrate

Die einzigen Quadrate in der Folge der Fibonacci-Zahlen sind $U_1 = U_2 = 1$ und $U_{12} = 144$. Dieses Ergebnis erzielten unabhängig voneinander COHN und WYLER im Jahr 1964.

Das einzige Quadrat in der Folge der Lucas-Zahlen ist $V_3 = 4$, dies bewies Cohn (1964a).

Einer der Beweise verwendet nur Teilbarkeitseigenschaften und algebraische Identitäten die Fibonacci- und Lucas-Zahlen betreffend. Einem anderen Beweis liegt die Lösung der Gleichungen $X^2 - 5Y^4 = \pm 4$, $X^4 - 5Y^2 = \pm 4$ zugrunde.

Im Fall der Parameter $(P, Q) = (2, -1)$, der zur Folge der Pell-Zahlen führt, lässt sich einfach zeigen, dass V_n nie ein Quadrat sein kann. Das einzige quadratische U_n (mit $n > 1$) ist $U_7 = 169$. Der Beweis folgt aus einer Untersuchung der Gleichung $X^2 - 2Y^4 = -1$, die Gegenstand eines langen Artikels von Ljunggren (1942c) ist. Robbins berichtete in (1984) von diesem Ergebnis. Es wurde später unter Verwendung einer Methode zur diophantischen Approximation unter Zuhilfenahme von Computerberechnungen von Pethö (1991) wiederentdeckt.

Sei $a \geq 2$, $P = a+1$ und $Q = a$. Nagell (1921a) (und Ljunggren (1942c), der die Arbeit abgeschlossen hat) bewies: Wenn $\frac{a^n-1}{a-1}$ ein Quadrat ist und $n > 1$, dann $(a, n) = (3, 5)$ oder $(7, 4)$.

Ko (1960, 1964) zeigte: Wenn $a^n + 1$ ein Quadrat ist, dann gilt $(a, n) = (2, 3)$. Dieses Ergebnis beantwortete ein Problem, das lange Zeit bestanden hatte.

Ein kurzer Beweis von Kos Satz geht auf Chein (1976) zurück; einen weiteren fand Rotkiewicz (1983), dieser erforderte die Berechnung von Jacobi-Symbolen.

Detaillierte Beweise der obigen Sätze finden sich in meinem Buch *Catalan's Conjecture* (1994).

Der Spezialfall mit Parametern $(3, 2)$ erzeugt die Zahlen $U_n = 2^n - 1$, $V_n = 2^n + 1$ und es ist leicht nachzuvollziehen, dass $2^n - 1 = \square$ nur für $n = 1$, und $2^n + 1 = \square$ nur für $n = 3$ gelten kann.

Doppelte Quadrate

Cohn (1964b) bewies für Fibonacci-Zahlen U_n und Lucas-Zahlen V_n:

Wenn $U_n = 2\square$, dann $n = 3$ oder 6, was zu $U_3 = 2$, $U_6 = 8$ führt.

Wenn $V_n = 2\square$, dann $n = 0$ oder 6, mit $V_0 = 2$, $V_6 = 18$.

Ich konnte in der Literatur nichts über die Bestimmung derjenigen Pell-Zahlen $U_n(2, -1)$, $V_n(2, -1)$, $\frac{a^n-1}{a-1}$, $a^n + 1$ finden, die doppelte Quadrate sind (abgesehen von den trivialen Fällen).

Quadratklassen

Cohn (1972) bestimmte die Quadratklassen von Fibonacci- und Lucas-Zahlen (sowie weiterer, allgemeinerer Folgen). In (1989a) habe ich eine andere Methode verwendet, um dieses Problem zu lösen:

> Die Quadratklassen der Fibonacci-Zahlen bestehen alle aus einer Zahl, ausgenommen die Fälle $\{U_1, U_2, U_{12}\}$ und $\{U_3, U_6\}$.
>
> Die Quadratklassen der Lucas-Zahlen bestehen alle aus einer Zahl, ausgenommen $\{V_1, V_3\}$, $\{V_0, V_6\}$.

Die Quadratklassen der Folgen von Pell-Zahlen sind noch nicht bestimmt worden.

In Bezug auf die Quadratklassen der Folgen $U_n = \frac{a^n-1}{a-1}$, $V_n = a^n+1$ $(n \geq 1)$ sei auf Ribenboim (1989b) verwiesen.

> Die Quadratklassen der Folge U bestehen alle nur aus einer Zahl. Wenn a gerade ist, sind auch die Quadratklassen von V auf ein Element beschränkt. Darüber hinaus gibt es eine effektiv berechenbare Zahl $C > 0$ derart, dass wenn
>
> $$(a^n + 1)(a^m + 1) = \square$$
>
> mit $m \neq n$ und ungeradem a, dann a, m, $n < C$. Es gibt also nur endlich viele nichttriviale Quadratklassen, die zudem alle endlich sind.

Zahlen der Form $k\square$ mit $k \geq 3$

Sei $k \geq 3$ ohne Einschränkung der Allgemeinheit als quadratfrei angenommen. Oft wird für k eine ungerade Primzahl gewählt.

Ich habe einige Artikel erwähnt, die sich mit speziellen Lucas-Folgen mit Folgengliedern der Form $k\square$ befassen. Es ist in diesem Zusammenhang unvermeidbar, unvollständig zu sein und ich möchte mich bei allen Autoren entschuldigen, deren Arbeit ich nicht erwähnt habe.

Zu Fibonacci-Zahlen bzw. Lucas-Zahlen der Form $p\square$ (mit einer ungeraden Primzahl p) gibt es Arbeiten von Steiner (1980), Robbins (1983a) und Goldman (1988).

Steiner zeigte, dass aus $U_n = 3\square$ folgt $n = 4$. Robbins bewies: Falls $U_n = p\square$ mit einer Primzahl p und $p \equiv 3 \pmod 4$ oder $3 < p < 10000$, dann ist $p = 3001$.

Goldman zeigte, dass wenn $p = 3, 7, 47$ oder 2207 und die Lucas-Zahl $V_n = p\square$, dann $V_n = p$; man beachte, dass dann $n = 2^e$ (mit $e = 1, 2, 3, 4$).

Auch im Falle der Folge $\frac{a^n-1}{a-1}$, $(n \geq 0,\ a \geq 2)$ gibt es ein Teilergebnis von Rotkiewicz (1983): Wenn $a \equiv 0$ oder 3 (mod 4) und $n > 1$, n ungerade, dann $\frac{a^n-1}{a-1} \neq n\square$. Dieses Resultat wurde durch die Berechnung von Jacobi-Symbolen erzielt.

Kuben

London und Finkelstein (1969) zeigten, dass die einzigen Fibonacci-Kuben $U_1 = U_2 = 1$ und $U_6 = 8$ sind, wohingegen die einzige kubische Lucas-Zahl $V_1 = 1$ ist. Der Beweis von London und Finkelstein benötigt die Lösung der kubischen diophantischen Gleichung $x^2 \pm 100 = y^3$ unter bestimmten Bedingungen. Dies Resultat erzielten Lagarias (1981), sowie Pethö (1983) mit einem andersartigen Beweis unter Verwendung von Waldschmidts Form (1980) der unteren Schranke für Linearformen in Logarithmen und anschließenden Computerberechnungen. Pethö erzielte zudem Ergebnisse über Fibonacci-Zahlen der Form px^3 und p^2x^3. In Bezug auf Pell-Zahlen zeigte Pethö (1991), dass für $n > 1$ der Term $U_n(2, -1)$ nie eine Kubikzahl sein kann.

Nagell (1920, 1921b) (von Ljunggren (1942a, 1943) ergänzt) zeigte, dass wenn $\frac{a^n-1}{a-1}$ eine Kubikzahl ist und $n = 3$, dann $a = 18$; darüber hinaus gilt mit $n > 3$, dass $n \not\equiv -1$ (mod 6), was nur ein Teilergebnis darstellt.

Die Arbeit von Nagell und Ljunggren zeigte auch, dass $a^n + 1$ nur in den Trivialfällen kubisch sein kann.

Diese Aussagen sind für die Fälle $2^n - 1$, $2^n + 1$ natürlich selbstverständlich, sie können keine Kubikzahlen sein. Dies ist in Gérono (1870) erwähnt.

Höhere Potenzen

Ein natürliches Problem war es festzustellen, ob es unter den Fibonacci- und Lucas-Zahlen irgendwelche höheren Potenzen als Kuben (und verschieden von 1) gibt. Keine einzige wurde jemals experimentell gefunden und das Problem war auf alle Fälle schwierig.

In (1978) und (1983b) zeigte Robbins: Es sei $q \geq 5$ prim und n der kleinste Index derart, dass die Fibonacci-Zahl U_n eine $q$te Potenz ist. Dann ist n selbst prim.

Wenn also p ein Primteiler von U_n ist, dann gilt $n = \rho_U(p)$, aber auch $p^q \mid U_n$, und es schien, dass die elementare Methode von Robbins nicht ausreichen würde, um das Problem zu lösen.

Ein meisterhafter Artikel, in dem die Expertise der Autoren Bugeaud, Mignotte und Siksek (2006) zusammentrifft, enthält die Lösung des Problems: Die einzigen nichttrivialen Potenzen unter den Fibonacci-Zahlen sind 8 und 144 und die einzige nichttriviale Potenz unter den Lucas-Zahlen ist die 4.

Pethö (1991) bewies, dass eine Pell-Zahl $U_n(2,-1)$ (mit $n > 1$) keine Potenz höher als ein Quadrat sein kann.

Der bereits erwähnten Arbeit von Nagell und Ljunggren ist zu entnehmen: Wenn $\frac{a^n-1}{a-1} = y^m$ mit $m > 3$, $n \geq 3$, dann $n \neq 3$. Darüber hinaus folgt aus Nagell (1920) und Ljunggren (1943), dass notwendigerweise 3 und 4 keine Teiler von n sind wenn $m > 3$ (was nur ein Teilergebnis ist).

Inkeri teilte mir Folgendes mit: Wenn $\frac{a^n-1}{a-1}$ eine $p$te Potenz ist (mit $a > 1$, $n > 1$ und p prim), dann gilt für den p-adischen Wert $v_p(a) \neq 1$ (der Beweis findet sich in meinem Buch *Catalan's Conjecture* (1994), Seite 120).

Das Problem herauszufinden, ob a^n+1 oder auch analog a^n-1 gleich einer höheren Potenz sein kann, läuft auf die Bestimmung aller aufeinander folgenden Potenzen von ganzen Zahlen hinaus. Catalan (1844) vermutete, dass 8 und 9 die einzigen aufeinander folgenden Potenzen sind. Das Problem war noch offen, als ich mein bereits erwähntes Buch *Catalan's Conjecture* schrieb, das sich ausschließlich mit dieser Frage beschäftigte. Zu jener Zeit hatte Tijdeman (1976) unter geschickter Verwendung von Bakers unteren Schranken für Linearformen in Logarithmen bereits gezeigt:

5.4. Es gibt eine effektiv berechenbare Zahl $C > 0$ derart, dass wenn $a^n + 1 = b^m$ mit $a, b \geq 1$, $m \geq 2$, dann $a, b, m, n < C$.

Langevin (1976) berechnete eine obere Schranke für C:

$$C < e^{e^{e^{e^{730}}}},$$

eine Grenze, die das Vorstellbare überschreitet.

Mignotte unternahm mit seinen Mitarbeitern große Anstrengungen, um die von Langevin gefundene Schranke zu verkleinern. Es verblieb aber noch ein großes Intervall, das vielleicht immer noch aufeinanderfolgende Potenzen enthalten könnte.

Der vollständige Beweis Catalans Vermutung gelang Mihăilescu im Jahr 2004 und beruht auf tiefliegenden Eigenschaften von Zahlkörpern in Verbindung mit Catalans Gleichung.

Wie bei Fermats letztem Satz oder auch höheren Potenzen unter Fibonacci-Zahlen waren außergewöhnliche Anstrengungen erforderlich, um zu zeigen, dass es die berüchtigten Zahlen nicht gab.

Im krassen Gegensatz zur allgemeinen Vermutung Catalans ist es für die speziellen Folgen von Zahlen $2^n - 1$, $2^n + 1$ einfach zu beweisen, dass sie keine höheren Potenzen sein können (mit Ausnahme der 1). Dies zeigte Gérono (1870).

Repunit-Zahlen

Man nennt eine Zahl eine *Repunit-Zahl*, wenn ihre Dezimaldarstellung ausschließlich aus Einsen besteht. Solche Zahlen haben die Form

$$\frac{10^n - 1}{10 - 1} = U_n(11, 10).$$

Eine von 1 verschiedene Repunit-Zahl ist weder ein Quadrat noch eine fünfte Potenz. Dies folgt aus dem bereits erwähnten Resultat von Inkeri. Einen unabhängigen Beweis fand Bond (siehe auch mein Buch *Catalan's Conjecture* (1994), Seite 120).

Inkeri (1972) zeigte, dass eine Repunit-Zahl (verschieden von 1) keine Kubikzahl sein kann. Ein weiterer Beweis stammt von Rotkiewicz (1981) (siehe *Catalan's Conjecture*, Seiten 119, 120).

Die Frage nach der Bestimmung von Potenzen unter Repunit-Zahlen ist inzwischen vollständig gelöst — nur die triviale Repunit-Zahl 1 ist eine Potenz. Dieses Resultat findet sich in einem Abdruck von Bugeaud (1999). Der Beweis benutzt Schranken in Linearformen in zwei p-adischen Logarithmen sowie intensive modulare Berechnungen zur Lösung von Thue-Gleichungen.

Zusammenfassung

Es ist vielleicht eine gute Idee, die verschiedenen bis jetzt angesprochenen Ergebnisse über spezielle Lucas-Folgen in einer Tabelle zusammen zu fassen.

Ein Ausrufezeichen (!) deutet an, dass das Problem gelöst ist; ein Fragezeichen (?) bedeutet, dass das Problem noch völlig ungelöst ist

oder dass ich nichts in der Literatur darüber finden konnte. Die Bezeichnung (!?) sagt aus, dass nur Teilergebnisse erzielt werden konnten und immer noch Fälle zu klären sind.

Folge	Fibonacci	Lucas	$U_n(2,-1)$	$V_n(2,-1)$	$U_n(3,2)$	$V_n(3,2)$	$\frac{a^n-1}{a-1}$ $(a>2)$	a^n+1 $(a>2)$
$\square$	! Cohn Wyler	! Cohn	! Ljungren	! Ljungren	! trivial	! Frénicle de Bessy	! Nagell Ljungren	! Ko
$2\square$	! Cohn	! Cohn	?	?	! trivial	! trivial	?	?
Quadratklassen	! Cohn Ribenboim	! Cohn Ribenboim	?	?	! trivial	! trivial	! Ribenboim	!? Ribenboim
Kuben	! London und Finkelstein	! London und Finkelstein	! Pethö	?	! Gérono	! Gérono	!? Nagell Ljungren	! Nagell Ljungren
Höhere Potenzen	! Bugeaud, Mignotte, Siksek				! Gérono	! Gérono	!? Nagell	! Mihăilescu

C Einheitliche Bestimmung von Vielfachen, Quadraten und Quadratklassen für bestimmte Familien von Lucas-Folgen

Eine interessante und in gewisser Hinsicht unerwartete Tatsache bei der Bestimmung von Quadraten, doppelten Quadraten und Quadratklassen ist es, dass bestimmte unendliche Familien von Lucas-Folgen auf einmal betrachtet werden können und so einheitliche Ergebnisse entstehen.

In einer Reihe von Veröffentlichungen verband Cohn (1966, 1967, 1968, 1972) dieses Problem mit der Lösung biquadratischer Gleichungen. Er erzielte dabei Resultate für alle (nicht-entarteten) Folgen mit Parametern $(P, \pm 1)$ und ungeradem $P \geq 1$.

Wie in Kürze ersichtlich wird, gelten einige Ergebnisse auch für bestimmte unendliche (wenn auch dünne) Mengen gerader Parameter P.

McDaniel und ich haben eine neue Methode entwickelt, die die Berechnung von Jacobi-Symbolen beinhaltet und die auf Parameter (P, Q) mit ungeraden P, Q, $P \geq 1$, $\mathrm{ggT}(P, Q) = 1$ und $D > 0$ anwendbar ist.

Die Ergebnisse wurden in unserem Artikel von (1992) angekündigt, detaillierte Beweise finden sich in McDaniel (1996).

Quadrate und doppelte Quadrate

Die nun folgenden Resultate stammen von McDaniel und Ribenboim.

Es wird angenommen, dass $P \geq 1$, P und Q ungerade sind mit $\mathrm{ggT}(P, Q) = 1$ und $D = P^2 - 4Q > 0$.

5.5. 1. Wenn $U_n = \square$, dann $n = 1, 2, 3, 6$ oder 12.
2. $U_2 = \square$ genau dann, wenn $P = \square$.
3. $U_3 = \square$ genau dann, wenn $P^2 - Q = \square$.
4. $U_6 = \square$ genau dann, wenn $P = 3\square$, $P^2 - Q = 2\square$, $P^2 - 3Q = 6\square$.
5. $U_{12} = \square$ genau dann, wenn $P = \square$, $P^2 - Q = 2\square$, $P^2 - 2Q = 3\square$, $P^2 - 3Q = \square$ und $(P^2 - 2Q)^2 - 3Q^2 = 6\square$.

Die Bestimmung aller zulässigen (P, Q) mit $U_3(P, Q) = \square$ ist offensichtlich und es gibt natürlich unendlich viele solcher Paare (P, Q).

5.6. Die Menge aller zulässigen Parameter (P, Q) mit $U_6(P, Q) = \square$ ist durch die Menge $\{(s, t) \mid \mathrm{ggT}(s, t) = 1,\ s \text{ gerade},\ t \text{ ungerade},\ st \equiv 1 \pmod 3\}$ parametrisierbar, indem man setzt

$$P = \frac{(s^2 - t^2)^2}{3}, \quad Q = (a^2 - b^2)^2 - \frac{8(a^2 + b^2 + ab)^2}{q}$$

mit

$$a = \frac{2(s^2 + t^2 + st)}{3}, \quad b = \frac{s^2 + t^2 + st}{3},$$

und drei weiteren analogen Formen für P, Q (die hier der Kürze wegen nicht aufgelistet sind). Insbesondere gibt es unendlich viele (P, Q) mit $U_6(P, Q) = \square$.

$(P, Q) = (1, -1)$ ist das einzige bekannte Paar mit $U_{12}(P, Q) = \square$. Es ist nicht bekannt, ob das System von Gleichungen in **(5.5)** Teil 5. eine weitere nichttriviale Lösung zulässt.

5.7. 1. Wenn $U_n = 2\square$, dann $n = 3$ oder 6.
2. $U_3 = 2\square$ genau dann, wenn $P^2 - Q = 2\square$.
3. $U_6 = 2\square$ genau dann, wenn $P = \square$, $P^2 - Q = 2\square$ und $P^2 - 3Q = \square$.

Die Menge der zulässigen Parameter (P, Q) mit $U_3(P, Q) = 2\square$ ist offensichtlich unendlich und leicht parametrisierbar.

Die Menge der zulässigen (P, Q) mit $U_6(P, Q) = 2\square$ ist nicht vollständig bekannt. Die Teilmenge aller $(1, Q)$ mit $U_6(1, Q) = 2\square$ lässt sich jedoch parametrisieren und als unendlich groß nachweisen.

Bezüglich V ist Folgendes bekannt:

5.8. 1. Wenn $V_n = \square$, dann $n = 1$, 3 oder 5.
2. $V_3 = \square$ genau dann, wenn $P = \square$.
3. $V_3 = \square$ genau dann, wenn sowohl P als auch $P^2 - 3Q$ Quadrate sind oder wenn sowohl P als auch $P^2 - 3Q$ die Form $3\square$ haben.
4. $V_5 = \square$ genau dann, wenn $P = 5\square$ und $P^4 - 5P^2Q + 5Q^2 = 5\square$.

5.9. Die Menge aller zulässigen (P, Q) mit $V_3(P, Q) = \square$ ist unendlich und folgendermaßen parametrisierbar:

Erster Typ: $P = s^2$, $Q = \frac{s^4 - t^2}{3}$ mit ungeradem s, t gerade, 3 kein Teiler von st, $\mathrm{ggT}(s, t) = 1$ und $s^2 < 2t$;

Zweiter Typ: $P = 3s^2$, $Q = 3s^4 - t^2$ mit ungeradem s, t gerade, 3 teilt s, $\mathrm{ggT}(s, t) = 1$ und $\sqrt{3}s^2 < 2t$.

5.10. Die Menge aller zulässigen (P, Q) mit $V_5(P, Q) = \square$ ist unendlich und folgendermaßen parametrisierbar:

Erster Typ: $P = 5s^2t^2$, $Q = -\frac{s^8 - 50s^4t^4 + 125t^8}{4}$ mit s, t ungerade, 5 kein Teiler von s, $\mathrm{ggT}(s, t) = 1$ und $|s| > \left[\frac{25 + 5\sqrt{5}}{2}\right]^{\frac{1}{4}} t$.

Zweiter Typ: $P = s^2t^2$, $Q = -\frac{5(s^8 - 10s^4t^4 + 5t^8)}{4}$ mit s, t ungerade, 5 kein Teiler von s, $\mathrm{ggT}(s, t) = 1$ und $|s| > \left[\frac{49 + \sqrt{1901}}{10}\right]^{\frac{1}{4}} t$.

5.11. 1. Wenn $V_n = 2\square$, dann $n = 3$ oder 6.
2. $V_3 = 2\square$ genau dann, wenn entweder $P = \square$, $P^2 - 3Q = 2\square$ oder $p = 3\square$, $P^2 - 3Q = 6\square$.
3. $V_6 = 2\square$ genau dann, wenn $P^2 - 2Q = 3\square$ und $(P^2 - 2Q)^2 - 3Q^2 = 6\square$.

5.12. Die Menge aller zulässigen (P, Q) mit $V_6(P, Q) = 2\square$ ist unendlich und folgendermaßen parametrisierbar: $P = s^2$, $Q = 3s^4 - 2t^2$ mit s ungerade, $\mathrm{ggT}(s, t) = 1$, 3 kein Teiler von s und $\sqrt{6}s^2 < 4t$.

Auf meine Anfrage hin bestimmte J. Top die Paare (P, Q) mit $V_6(P, Q) = 2\square$ (siehe den bereits erwähnten Artikel von McDaniel und Ribenboim):

5.13. Die zulässigen (P, Q) mit $V_6(P, Q) = 2\square$ korrespondieren mit den rationalen Punkten einer bestimmten elliptischen Kurve, wobei die Gruppe der rationalen Punkte isomorph zu $(\mathbb{Z}/2) \times \mathbb{Z}$ ist. Diese Punkte führen zu unendlich vielen Paaren zulässiger Parameter. $(P, Q) = (1, -1)$ korrespondiert zu den Punkten mit Ordnung 2; $(5, -1)$ korrespondiert zum Generator der Untergruppe unendlicher Ordnung.

Weitere Lösungen lassen sich durch das Gruppengesetz berechnen, d.h. mit der klassischen Sehnen- und Tangentenmethode. Somit sind

$$(P, Q) = (29, -4801), (4009, 3593279), (58585, -529351744321), \ldots$$

auch mögliche Parameter.

Der Umgang mit dem Fall, dass P oder Q gerade sind, ist ungleich schwieriger. Die ersten bekannten Ergebnisse stammen von Cohn (1972).

5.14. Sei $Q = -1$ und $P = V_m(A, -1)$ mit A ungerade, $m \equiv 3 \pmod 6$.

1. Wenn $U_n(P, -1) = \square$, dann $n = 1$ oder $n = 2$ und $P = 4$ oder 36.
2. Wenn $U_n(P, -1) = 2\square$, dann $n = 4$, $P = 4$.
3. Wenn $V_n(P, -1) = \square$, dann $n = 1$, $P = 4$ oder 36.
4. Wenn $U_n(P, -1) = 2\square$, dann $n = 2$ und $P = 4$ oder 140.

5.15. Sei $Q = 1$ und $P = V_m(A, 1)$ mit A ungerade und $3|m$.

1. Wenn $U_n(P, 1) = \square$, dann $n = 1$.
2. Wenn $U_n(P, 1) = 2\square$, dann $n = 2$ und $P = 18$ oder 19602.
3. $V_n(P, 1) = \square$ ist unmöglich.
4. Wenn $V_n(P, 1) = 2\square$, dann $n = 1$ und $P = 18$ oder 19602.

Man beachte, dass es unendlich viele gerade $P = V_m(A, -1)$ mit ungeradem A und $m \equiv 3 \pmod 6$ gibt, diese Menge jedoch dünn ist.

So sind zum Beispiel 4, 36, 76, 140, 364, 756, 1364, 2236, 3420, 4964 für $P < 6000$ die einzigen Möglichkeiten. Eine analoge Bemerkung gilt für die Zahlen $P = V_n(A, 1)$ mit ungeradem A, wenn 3 Teiler von m ist.

Im Jahr 1983 veröffentlichte ROTKIEWICZ das folgende bemerkenswerte Teilresultat:

5.16. Wenn P gerade ist, $Q \equiv 1 \pmod 4$, $\mathrm{ggT}(P, Q) = 1$ und wenn $U_n(P, Q) = \square$, dann ist n entweder ein ungerades Quadrat oder n ist eine gerade Zahl, die keine Zweierpotenz ist und deren größter Primfaktor die Diskriminante D teilt.

McDaniel und Ribenboim (1998b) verwendeten das Resultat von ROTKIEWICZ, um zu zeigen:

5.17. Sei P positiv und gerade, $Q \equiv 1 \pmod 4$ mit $D = P^2 - 4Q > 0$, $\mathrm{ggT}(P, Q) = 1$ und sei $U_n(P, Q) = \square$. Dann ist n ein Quadrat oder das Zweifache eines ungeraden Quadrats; alle Primfaktoren von n teilen D; wenn $p^t > 2$ ein Primzahlpotenzteiler von n ist, dann gilt für $1 \leq u < t$, dass $U_{p^u} = p\square$ wenn u gerade ist, und $U_{p^U} = p\square$ wenn u ungerade ist. Wenn n gerade ist und $U_n = \square$, dann gilt zudem $p = \square$ oder $p = 2\square$.

Quadratklassen

In (1992) bewiesen MCDANIEL und ich gemeinsam den folgenden Satz:

5.18. Sei $(P, Q) \in \mathcal{S}$. Dann gibt es für jedes $n > 0$ eine effektiv berechenbare ganze und von P, Q und n abhängige Zahl $C_n > 0$ derart, dass wenn $n < m$ und $U_n(P, Q)U_m(P, Q) = \square$ oder $V_n(P, Q)V_m(P, Q) = \square$, dann $M < C_n$.

Insbesondere sind alle Quadratklassen in den Folgen U, V endlich.

Für $(P, 1)$, $(P, -1)$ mit ungeradem P verwendete COHN (1972) seine Ergebnisse über bestimmte biquadratische Gleichungen vom Typ $X^4 - DY^2 = \pm 4, \pm 1$ und $X^2 - DY^4 = \pm 4, \pm -1$, um Aussagen über Quadratklassen zu gewinnen:

5.19. Sei $P \geq 1$ ungerade.

1. Wenn $1 \leq n < m$ und $U_n(P,-1)U_m(P,-1) = \square$, dann
   $n = 1, \quad m = 2, \quad P = \square, \quad$ oder
   $n = 1, \quad m = 12, \quad P = 1, \quad$ oder
   $n = 3, \quad m = 6, \quad P = 1, \quad$ oder
   $n = 3, \quad m = 6, \quad P = 3.$
2. Wenn $P \geq 3$, $1 \leq n \leq m$ und $U_n(P,1)U_m(P,1) = \square$, dann
   $n = 1, \quad m = 6, \quad P = 3, \quad$ oder
   $n = 1, \quad m = 2, \quad P = \square.$

5.20. Sei $P \geq 1$ ungerade.

1. Wenn $0 \leq n < m$ und $V_n(P,1)V_m(P,1) = \square$, dann
   $n = 0, \quad m = 6, \quad P = 1, \quad$ oder
   $n = 1, \quad m = 3, \quad P = 1, \quad$ oder
   $n = 0, \quad m = 6, \quad P = 5.$
2. Wenn $P \geq 3$, $0 \leq n < m$, und $V_n(P,1)V_m(P,1) = \square$, dann
   $n = 0$, $m = 3$, $P = 3$ oder 27.

Ein sehr spezieller Fall konnte später von André-Jeannin (1992) mit einer direkteren Methode behandelt werden.

Den folgenden Satz bewies McDaniel (1998a):

5.21. Sei $P > 0$, $Q \neq 0$, $\mathrm{ggT}(P,Q) = 1$ und $D = P^2 - 4Q > 0$. Angenommen, P, Q sind ungerade.

1. (a) Wenn $1 < m < n$ und $U_m U_n = \square$, dann $(m,n) \in \{(2,3),(2,12),(3,6),(5,10)\}$ oder $n = 3m$,
   (b) Wenn $1 < m$, $U_m U_{3m} = \square$, dann ist m ungerade, $3 \nmid m$, $Q \equiv 1 \pmod 4$, $\left(\frac{-Q}{P}\right) = +1$ und $P < |Q+1|$.
   (c) Für gegebenes P und $m > 1$ gibt es eine effektiv berechenbare Konstante $C > 0$ derart, dass wenn Q wie oben und wenn $U_m U_{3m} = \square$, dann $|Q| < C$.
   (d) Für P, Q wie oben gibt es ein effektiv berechenbares $C > 0$ derart, dass wenn $m > 1$ und $U_m U_{3m} = \square$, dann $m < C$.
2. (a) Wenn $1 < m < n$ und $V_m V_n = \square$, dann $n = 3m$.
   (b) Wenn $1 < m$ und $V_m V_{3m} = \square$, dann ist m ungerade, $3 \nmid m$, $Q \equiv 3 \pmod 4$, $3 \nmid P$, $\left(\frac{-3Q}{P}\right) = +1$ und $P < |\frac{Q}{k} + k|$, wobei $k = \sqrt[5]{0{,}6} \approx 0{,}9$.

(c) Für gegebenes $m > 1$ und P gibt es ein effektiv berechenbares $C > 0$ derart, dass wenn $Q \neq 0$ wie oben und wenn $V_m V_{3m} = \square$, dann $|Q| < C$.
(d) Für P, Q wie oben gibt es ein effektiv berechenbares $C > 0$ derart, dass wenn $1 < m$ und $V_m V_{3m} = \square$, dann $m < C$.

Vielfache von Quadraten

Es gibt nur wenige systematische Untersuchungen, diese stammen hauptsächlich von Cohn (1972).

Sei $k \geq 3$ eine ungerade quadratfreie Zahl und $P \geq 1$ ungerade. Cohn untersuchte die Gleichungen $U_n(P, -1) = k\square$, $U_n(P, -1) = 2k\square$, konnte aber keine vollständigen Ergebnisse erzielen.

Es gibt sicher einen kleinsten Index $r > 0$ derart, dass k Teiler von $U_r(P, -1)$ ist. Da die Quadratklassen in diesen Fall wie bereits gesagt aus höchstens zwei Zahlen bestehen, gibt es auch nur höchstens zwei Indizes n derart, dass $U_n(P, -1) = k\square$ bzw. $2k\square$.

5.22. Unter obigen Annahmen und Bezeichnungsweisen:

1. Wenn $r \not\equiv 0 \pmod 3$ und $U_n = k\square$, dann $n = r$, während $U_n = 2k\square$ unmöglich ist.
2. Für $r \equiv 3 \pmod 6$ ist $U_n(P, -1) = k\square$ unmöglich, man fand jedoch keine Lösung $U_n(P, -1) = 2k\square$ für diesen Fall.
3. Wenn $n \equiv 0 \pmod 6$, und wenn der 2-adische Wert $v_2(r)$ gerade ist, dann ist $U_n(P, -1) = 2k\square$ unmöglich; wenn $v_2(r)$ ungerade ist, dann ist $U_n(P, -1) = k\square$ unmöglich, es sei denn $P = 5$, $n = 12$, $k = 455$. Die anderen Fälle sind offen.

Cohn gab auch an, wie man für den Fall $P \geq 3$ die Gleichungen $U_n(P, 1) = k\square$ bzw. $2k\square$ in ähnlicher Weise behandeln kann und zu Teilresultaten gelangt.

D Quadratvolle Zahlen in Lucas-Folgen

Sei $(P, Q) \in \mathcal{S}$ und U bzw. V die Lucas-Folgen mit Parametern (P, Q). Wenn U_n eine quadratvolle Zahl ist und p ein primitiver Faktor von U_n, dann ist p^2 Teiler von U_n. Dies legt nahe, dass die Menge aller Indizes n, für die U_n quadratvoll ist, endlich sein sollte. Eine analoge Bemerkung trifft auf die Folge V zu.

Für die Fibonacci- und Lucas-Zahlen ist ein Beweis für diese Tatsache bekannt, dieser basiert auf Massers Vermutung.

Massers Vermutung (1985), die man auch (ABC)-Vermutung nennt, ist die folgende (siehe auch Oesterlé (1988)):

Es sei $\epsilon > 0$ gegeben und es seien a, b, c positive ganze Zahlen mit $\mathrm{ggT}(a, b) = 1$, $a + b = c$ sowie $g = \prod_{p|abc} p$. Dann gibt es eine positive Zahl $C(\epsilon)$ derart, dass $c < C(\epsilon)g^{1+\epsilon}$. Ein Beweis der (ABC)-Vermutung stellt für die Mathematiker eine große Herausforderung dar. Eine viel schwächere Form der quälenden (ABC)-Vermutung konnte Stewart (1986) beweisen. Elkies (1991) zeigte, dass die (ABC)-Vermutung den berühmten Satz von Faltings zur Folge hat (der die Vermutung von Mordell beweist). Es ist auch bekannt, dass aus der (ABC)-Vermutung folgt, dass es höchstens endlich viele ganze Zahlen $n \geq 3$, x, y, $z \neq 0$ mit $x^n + y^n = z^n$ geben kann, was nur knapp an einem Beweis von Fermats letztem Satz vorbeigeht.

G. Walsh machte mich auf Folgendes aufmerksam:

5.23. Wenn Massers Vermutung wahr ist, dann gibt es für eine gegebene quadratfreie Zahl $k \geq 1$ nur endlich viele Indizes n derart, dass die Fibonacci-Zahl U_n oder die Lucas-Zahl V_n die Form kt hat, wobei t eine quadratvolle Zahl ist.

Der Beweis ist kurz und einfach.

Für eine Zahl $N = \prod_{i=1}^{r} p_i^{e_i}$ (wobei $p_1, \ldots, p_r$ verschiedene Primfaktoren sind und $e_1, \ldots, e_r \geq 1$), ist der *quadratvolle Teil* von N nach Definition

$$w(N) = \prod_{e_i > 1} p_i^{e_i}.$$

Somit ist N genau dann quadratvoll, wenn $N = w(N)$.

Im Jahr 1999 bewiesen Ribenboim und Walsh unter der Annahme der Richtigkeit der (ABC)-Vermutung:

5.24. Seien U, V Lucas-Folgen mit positiver Diskriminante. Für jedes $\epsilon > 0$ sind die Mengen $\{n \mid w(U_n) > U_n^{\epsilon}\}$ und $\{n \mid w(V_n) > V_n^{\epsilon}\}$ endlich. Insbesondere hat jede der Folgen U, V nur endlich viele Terme, die quadratvolle Zahlen sind.

Bemerkenswerte Spezialfälle ergeben sich, wenn man $P = 1, Q = -1$ wählt (Fibonacci- und Lucas-Zahlen), $P = 2$, $Q = -1$ (Pell-Zahlen), $P = 3$, $Q = 2$ und allgemeiner $P = a + 1$ $Q = a$ (wobei $a > 1$). Insbesondere folgt aus der (ABC)-Vermutung, dass es nur endlich viele quadratvolle Mersenne-Zahlen M_q und Fermat-Zahlen F_m gibt.

Literaturverzeichnis

1202 Leonardo Pisano (Fibonacci). *Liber Abbaci (^{2}1228).* Tipografia delle Scienze Matematiche e Fisiche, Rome, Ausgabe von 1857. B. Boncompagni, Herausgeber.

1657 Frénicle de Bessy. Solutio duorum problematum circa numeros cubos et quadratos. Bibliothèque Nationale de Paris.

1843 J. P. M. Binet. Mémoire sur l'intrégation des équations linéaires aux différences finies, d'un ordre quelconque, á coefficients variables. *C. R. Acad. Sci. Paris*, 17:559–567.

1844 E. Catalan. Note extraite d'une lettre addressée á l'éditeur. *J. reine u. angew. Math.*, 27:192.

1870 G. C. Gérono. Note sur la résolution en nombres entiers et positifs de l'équation $x^m = y^n + 1$. *Nouv. Ann. de Math. (2)*, 9: 469–471 und 10:204–206 (1871).

1878 E. Lucas. Théorie des fonctions numériques simplement périodiques. *Amer. J. of Math.*, 1:184–240 und 289–321.

1886 A. S. Bang. Taltheoretiske Untersogelser. *Tidskrift Math., Ser. 5*, 4:70–80 und 130–137.

1892 K. Zsigmondy. Zur Theorie der Potenzreste. *Monatsh. f. Math.*, 3:265–284.

1904 G. D. Birkhoff und H. S. Vandiver. On the integral divisors of $a^n - b^n$. *Ann. Math. (2)*, 5:173–180.

1909 A. Wieferich. Zum letzten Fermatschen Theorem. *J. reine u. angew. Math.*, 136:293–302.

1913 R. D. Carmichael. On the numerical factors of arithmetic forms $\alpha^n \pm \beta^n$. *Ann. of Math. (2)*, 15:30–70.

1920 T. Nagell. Note sur l'équation indéterminée $\frac{x^n-1}{x-1} = y^q$. *Norsk Mat. Tidsskr.*, 2:75–78.

1921 T. Nagell. Des équations indéterminées $x^2 + x + 1 = y^n$ et $x^2 + x + 1 = 3y^n$. *Norsk Mat. Forenings Skrifter, Ser. I*, 1921, Nr. 2, 14 Seiten.

1921 T. Nagell. Sur l'équation indéterminée $\frac{x^n-1}{x-1} = y^2$. *Norsk Mat. Forenings Skrifter, Ser. I*, 1921, Nr. 3, 17 Seiten.

1930 D. H Lehmer. An extended theory of Lucas' functions. *Ann. of Math.*, 31:419–448.

1935 K. Mahler. Eine arithmetische Eigenschaft der Taylor-Koeffizienten rationaler Funktionen. *Nederl. Akad. Wetensch. Amsterdam Proc.*, 38:50–60.

1938 G. H. Hardy und E. M. Wright. *An Introduction to the Theory of Numbers.* Clarendon Press, Oxford, 5. Ausgabe (1979).

1942 W. Ljunggren. Einige Bemerkungen über die Darstellung ganzer Zahlen durch binäre kubische Formen mit positiver Diskriminante. *Acta Math.*, 75:1–21.

1942 W. Ljunggren. Über die Gleichung $x^4 - Dy^2 = 1$. *Arch. Math. Naturvid.*, 45(5):61–70.

1942 W. Ljunggren. Zur Theorie der Gleichung $x^2 + 1 = Dy^4$. *Avh. Norsk Vid. Akad. Oslo.*, 1(5):1–27.

1943 W. Ljunggren. New propositions about the indeterminate equation $\frac{x^n-1}{x-1} = y^q$. *Norsk Mat. Tidsskr.*, 25:17–20.

1950 H.-J. Kanold. Sätze über Kreisteilungspolynome und ihre Anwendungen auf einige zahlentheoretische Probleme. *J. reine u. angew. Math.*, 187:355–366.

1953 C. G. Lekkerkerker. Prime factors of elements of certain sequences of integers. *Nederl. Akad. Wetensch. Proc. (A)*, 56:265–280.

1954 M. Ward. Prime divisors of second order recurring sequences. *Duke Math. J.*, 21:607–614.

1955 E. Artin. The order of the linear group. *Comm. Pure Appl. Math.*, 8:335–365.

1955 M. Ward. The intrinsic divisors of Lehmer numbers. *Ann. of Math. (2)*, 62:230–236.

1958 D. Jarden. *Recurring Sequences.* Riveon Lematematike, Jerusalem. ^{3}1973, revised und enlarged by J. Brillhart, Fibonacci Assoc., San Jose, CA.

1960 A. A. Brauer. Note on a number theoretical paper of Sierpiński. *Proc. Amer. Math. Soc.*, 11:406–409.

1960 Chao Ko. On the Diophantine equation $x^2 = y^n + 1$. *Acta Sci. Natur. Univ. Szechuan*, 2:57–64.

1961 L. K. Durst. Exceptional real Lucas sequences. *Pacific J. Math.*, 11:489–494.

1961 M. Ward. The prime divisors of Fibonacci numbers. *Pacific J. Math.*, 11:379–389.

1962 A. Rotkiewicz. On Lucas numbers with two intrinsic prime divisors. *Bull. Acad. Polon. Sci. Sér. Sci. Math. Astron. Phys.*, 10: 229–232.

1962 A. Schinzel. The intrinsic divisions of Lehmer numbers in the case of negative discriminant. *Ark. Math.*, 4:413–416.

1962 A. Schinzel. On primitive prime factors of $a^n - b^n$. *Proc. Cambridge Phil. Soc.*, 58:555–562.

1963 A. Schinzel. On primitive prime factors of Lehmer numbers, I. *Acta Arith.*, 8:213–223.

1963 A. Schinzel. On primitive prime factors of Lehmer numbers, II. *Acta Arith.*, 8:251–257.

1963 N. N. Vorob'ev. *The Fibonacci Numbers.* D. C. Heath, Boston.

1964 J. H. E. Cohn. On square Fibonacci numbers. *J. London Math.Soc.*, 39:537–540.

1964 J. H. E. Cohn. Square Fibonacci numbers etc. *Fibonacci Q.*, 2:109–113.

1964 Chao Ko. On the Diophantine equation $x^2 = y^n + 1$. *Scientia Sinica (Notes)*, 14:457–460.

1964 O. Wyler. Squares in the Fibonacci series. *Amer. Math. Monthly*, 7:220–222.

1965 J. H. E. Cohn. Lucas and Fibonacci numbers and some Diophantine equations. *Proc. Glasgow Math. Assoc.*, 7:24–28.

1965 P. Erdös. Some recent advances and current problems in number theory. In *Lectures on Modern Mathematics, Vol. III*, herausgegeben von T. L. Saaty, 169–244. Wiley, New York.

1965 H. Hasse. Über die Dichte der Primzahlen p, für die eine vorgegebene ganzrationale Zahl $a \neq 0$ von durch eine vorgegebene Primzahl $l \neq 2$ teilbarer bzw. unteilbarer Ordnung mod p ist. *Math. Annalen*, 162:74–76.

1966 J. H. E. Cohn. Eight Diophantine equations. *Proc. London Math. Soc. (3)*, 16:153–166 und 17:381.

1966 H. Hasse. Über die Dichte der Primzahlen p, für die eine vorgegebene ganzrationale Zahl $a \neq 0$ von gerader bzw. ungerader Ordnung mod p ist. *Math. Annalen*, 168:19–23.

1966 K. Mahler. A remark on recursive sequences. *J. Math. Sci.*, 1:12–17.

1966 E. Selmer. *Linear Recurrences over Finite Fields.* Lectures Notes, Department of Mathematics, University of Bergen.

1967 J. H. E. Cohn. Five Diophantine equations. *Math. Scand.*, 21: 61–70.

1967 C. Hooley. On Artin's conjecture. *J. reine u. angew. Math.*, 225:209–220.

1968 J. H. E. Cohn. Some quartic Diophantine equations. *Pacific J. Math.*, 26:233–243.

1968 L. P. Postnikova und A. Schinzel. Primitive divisors of the expression $a^n - b^n$. *Math. USSR-Sb.*, 4:153–159.

1968 A. Schinzel. On primitive prime factors of Lehmer numbers, III. *Acta Arith.*, 15:49–70.

1969 V. E. Hoggatt. *Fibonacci and Lucas Numbers.* Houghton-Mifflin, Boston.

1969 R. R. Laxton. On groups of linear recurrences, I. *Duke Math. J.*, 36:721–736.

1969 H. London und R. Finkelstein (alias R. Steiner). On Fibonacci and Lucas numbers which are perfect powers. *Fibonacci Q.*, 7:476-481 und 487.

1972 J. H. E. Cohn. Squares in some recurrence sequences. *Pacific J. Math.*, 41:631–646.

1972 K. Inkeri. On the Diophantic equation $a\frac{x^n-1}{x-1} = y^m$. *Acta Arith.*, 21:299–311.

1973 A. Baker. A sharpening for the bounds of linear forms in logarithms, II. *Acta Arith.*, 24:33–36.

1973 H. London und R. Finkelstein (alias R. Steiner). *Mordell's Equation* $y^2 - k = x^3$. Bowling Green State University Press, Bowling Green, OH.

1974 A. Schinzel. Primitive divisions of the expression $A^n - B^n$ in algebraic number fields. *J. reine u. angew. Math.*, 268/269:27–33.

1975 A. Baker. *Transcendental Number Theory.* Cambridge Univ. Press, Cambridge.

1975 C. L. Stewart. The greatest prime factor of $a^n - b^n$. *Acta Arith.*, 26:427–433.

1976 E. Z. Chein. A note on the equation $x^2 = y^n + 1$. *Proc. Amer. Math. Soc.*, 56:83–84.

1976 S. V. Kotov. Über die maximale Norm der Idealteiler des Polynoms $\alpha x^m + \beta y^n$ mit den algebraischen Koeffizenten. *Acta Arith.*, 31:210–230.

1976 M. Langevin. Quelques applications des nouveaux résultats de van der Poorten. *Sém. Delange-Pisot-Poitou,* 17^e *année*, 1976, Nr. G12, 1–11.

1976 P. J. Stephens. Prime divisors of second order linear recurrences, I. and II. *J. Nb. Th.*, 8:313–332 und 333–345.

1976 R. Tijdeman. On the equation of Catalan. *Acta Arith.*, 29: 197–209.

1977 A. Baker. The theory of linear forms in logarithms. In *Transcendence Theory: Advances and Applications (Proceedings of a conference held in Cambridge 1976)*, herausgegeben von A. Baker und D. W. Masser, 1–27. Academic Press, New York.

1977 T. N. Shorey, A. J. van der Porten, R. Tijdeman und A. Schinzel. Applications of the Gel'fond-Baker method to Diophantine equations. In *Transcendence theory: Advances and Applications*, herausgegeben von A. Baker und D. W. Masser, 59–77. Academic Press, New York.

1977 C. L. Stewart. On divisors of Fermat, Fibonacci, Lucas and Lehmer numbers. *Proc. London Math. Soc.*, 35:425–447.

1977 C. L. Stewart. Primitive divisors of Lucas and Lehmer numbers. In *Trancendence Theory: Advances and Applications*, herausgegeben von A. Baker und D. W. Masser, 79–92. Academic Press, New York.

1977 A. J. van der Poorten. Linear forms in logarithms in p-adic case. In *Transcendence Theory: Advances and Applications*, herausgegeben von A. Baker und D. W. Masser, 29–57. Academic Press, New York.

1978 P. Kiss und B. M. Phong. On a function concerning second order recurrences. *Ann. Univ. Sci. Budapest. Eötvös Sect Math.*, 21: 119–122.

1978 N. Robbins. On Fibonacci numbers which are powers. *Fibonacci Q.*, 16:515–517.

1980 R. Steiner. On Fibonacci numbers of the form $v^2 + 1$. In *A Collection of Manuscripts Related to the Fibonacci Sequence*, herausgegeben von W. E. Hogatt und M. Bicknell-Johnson, 208–210. The Fibonacci Association, Santa Clara.

1980 C. L. Stewart. On some Diophantine equations and related recurrence sequences. In *Séminaire de Théorie des Nombres Paris 1980/81 (Séminare Delange-Pisot-Poitou), Progress in Math.,* 22:317–321 (1982). Birkhäuser, Boston.

1980 M. Waldschmidt. A lower bound for linear forms in logarithms. *Acta Arith.*, 37:257–283.

1981 K. Györy, P. Kiss und A. Schinzel. On Lucas and Lehmer sequences and their applications to Diophantine equations. *Colloq. Math.*, 45:75–80.

1981 J. C. Lagarias und D. P. Weissel. Fibonacci and Lucas cubes. *Fibonacci Q.*, 19:39–43.

1981 H. Lüneburg. Ein einfacher Beweis für den Satz von Zsigdmondy über primitive Primteiler von $A^n - B^n$. In *Geometries and Groups,* Lect. Notes in Math., 893:219–222, herausgegeben von M. Aigner und D. Jungnickel. Springer-Verlag, New York.

1981 T. N. Shorey und C. L. Stewart. On divisors of Fermat, Fibonacci, Lucas and Lehmer numbers, II. *J. London Math. Soc.*, 23:17–23.

1982 K. Györy. On some arithmetical properties of Lucas and Lehmer numbers. *Acta Arith.*, 40:369–373.

1982 A. Pethö. Perfect powers in second order linear recurrences. *J. Nb. Th.*, 15:5–13.

1982 C. L. Stewart. On divisors of terms of linear recurrence sequences. *J. reine u. angew. Math.*, 333:12–31.

1983 A. Pethö. Full cubes in the Fibonacci sequence. *Publ. Math. Debrecen*, 30:117–127.

1983 N. Robbins. On Fibonacci numbers of the form px^2, where p is a prime. *Fibonacci Q.*, 21:266–271.

1983 N. Robbins. On Fibonacci numbers which are powers, II. *Fibonacci Q.*, 21:215–218.

1983 A. Rotkiewicz. Applications of Jacobi symbol to Lehmer's numbers. *Acta Arith.*, 42:163–187.

1983 T. N. Shorey und C. L. Stewart. On the Diophantine equation $ax^{2t} + bx^t y + cy^2 = 1$ and pure powers in recurrence sequences. *Math. Scand.*, 52:24–36.

1984 N. Robbins. On Pell numbers of the form px^2, where p is prime. *Fibonacci Q. (4)*, 22:340–348.

1985 J. C. Lagarias. The set of primes dividing the Lucas numbers has density 2/3. *Pacific J. Math.*, 118:19–23.

1985 D. W. Masser. Open problems. In *Proceedings Symposium Analytic Number Theory*, herausgegeben von W. W. L. Chen, London. Imperial College.

1985 C. L. Stewart. On the greatest prime factor of terms of a linear recurrence sequence. *Rocky Mountain J. Math.*, 15:599–608.

1986 T. N. Shorey und R. Tijdeman. *Exponential Diophantine Equations.* Cambridge University Press, Cambridge.

1986 C. L. Stewart und R. Tijdeman. On the Oesterlé-Masser conjecture. *Monatshefte Math.*, 102:251–257.

1987 A. Rotkiewicz. Note on the Diophantine equation $1 + x + x^2 + \ldots + x^m = y^m$. *Elem. of Math.*, 42:76.

1988 J. Brillhart, P. L. Montgomery, und R. D. Silverman. Tables of Fibonacci and Lucas factorizations. *Math. of Comp.*, 50: 251–260.

1988 M. Goldman. Lucas numbers of the form px^2, where $p = 3$, 7, 47 or 2207. *C. R. Math. Rep. Acad. Sci. Canada*, 10:139–141.

1988 J. Oesterlé. Nouvelles approches du "théorème" de Fermat. Séminaire Bourbaki, 40ème anée, 1987/8, Nr. 694, *Astérisque*, 161–162, 165–186.

1989 P. Ribenboim. Square-classes of Fibonacci numbers and Lucas numbers. *Portug. Math.*, 46:159–175.

1989 P. Ribenboim. Square-classes of $\frac{a^n-1}{a-1}$ and $a^n + 1$. *J. Sichuan Univ. Nat. Sci. Ed.*, 26:196–199. Sonderausgabe.

1989 N. Tzanakis und B. M. M. de Weger. On the practical solution of the Thue equation. *J. Nb. Th.*, 31:99–132.

1991 W. D. Elkies. *ABC* implies Mordell. *Internat. Math. Res. Notices (Duke Math. J.)*, 7:99–109.

1991 A. Pethö. The Pell sequence contains only trivial perfect powers. In *Colloquia on Sets, Graphs and Numbers, Soc. Math., János Bolyai*, 561–568. North-Holland, Amsterdam.

1991 P. Ribenboim. *The Little Book of Big Primes.* Springer-Verlag, NY.

1991 P. Ribenboim und W. L McDaniel. Square-classes of Lucas sequences. *Portug. Math.*, 48:469–473.

1992 R. André-Jeannin. On the equations $U_n = U_q x^2$, where q is odd and $V_n = V_q x^2$, where q is even. *Fibonacci Q.*, 30:133–135.

1992 W. L. McDaniel und P. Ribenboim. Squares and double squares in Lucas sequences. *C. R. Math. Rep. Acad. Sci. Canada*, 14:104–108.

1996 W. L. McDaniel und P. Ribenboim. The Square Terms in Lucas Sequences. *J. Nb. Th.*, 58: 104–123.

1994 P. Ribenboim. *Catalan's Conjecture.* Academic Press, Boston.

1995 P. M. Voutier. Primitive divisors of Lucas and Lehmer sequences. *Math. of Comp.*, 64:869–888.

1998 W. L. McDaniel und P. Ribenboim. Square classes in Lucas sequences having odd parameters. *J. Nb. Th.*, 73:14–23.

1998 W. L. McDaniel und P. Ribenboim. Squares in Lucas sequences having one even parameter. *Colloq. Math.*, 78:29–34.

1999 Y. Bugeaud und M. Mignotte. On integers with identical digits. Vorabdruck.

1999 H. Dubner und W. Keller. New Fibonacci and Lucas primes. *Math. of Comp.*, 68:417–427.

1999 P. Ribenboim. Números primos, Mistérios e Récordes. Instituto de Matématica Puru e Aplicado, Rio de Janeiro.

1999 P. Ribenboim und P. G. Walsh. The *ABC* conjecture and the powerful part of terms in binary recurring sequences. *J. Nb. Th.*, 74:134–147.

2006 P. Ribenboim. *Die Welt der Primzahlen.* Springer-Verlag, Heidelberg.

2004 P. Mihăilescu. Primary cyclotomic units and a proof of Catalan's conjecture. *J. reine u. angew. Math.*, 572:167–195.

2006 Y. Bugeaud, M. Mignotte und S. Siksek. Classical and modular approaches to exponential Diophantine equations. *Ann. Math.*, 163:969-1018

2

Darstellung reeller Zahlen mit Hilfe von Fibonacci-Zahlen

Unser Ziel ist die Herleitung einer neuen Darstellung der positiven reellen Zahlen als Summen von Reihen, die Fibonacci-Zahlen enthalten. Wir werden sehen, dass sich dies durch eine einfache Anwendung eines alten Satzes von KAKEYA (1941) bewerkstelligen lässt. Das Kapitel schließt mit einem Ergebnis von LANDAU (1899), in dem ein Zusammenhang der Summe $\sum_{n=1}^{\infty} \frac{1}{F_n}$ mit Werten von Theta-Reihen hergestellt wird. Es lohnt sich, dieses heute eher schwer zugängliche Resultat von LANDAU einmal zu Tage zu fördern.

1. Sei $(s_i)_{i\geq 1}$ eine Folge positiver reeller Zahlen mit $s_1 > s_2 > s_3 > \cdots$ und $\lim_{i\to\infty} s_i = 0$. Sei $S = \sum_{i=1}^{\infty} s_i \leq \infty$.

Wir bezeichnen $x > 0$ als durch die Folge $(s_i)_{i\geq 1}$ darstellbar, wenn $x = \sum_{j=1}^{\infty} s_{i_j}$ (wobei $i_1 < i_2 < i_3 < \cdots$). Zwangsläufig gilt dann $x \leq S$.

Das erste Ergebnis geht auf KAKEYA zurück. Der Vollständigkeit halber fügen wir einen Beweis an:

Proposition 1. *Die folgenden Aussagen sind äquivalent:*

(1) *Jedes x, $0 < x \leq S$, ist durch die Folge $(s_i)_{i\geq 1}$, $x = \sum_{j=1}^{\infty} s_{i_j}$ darstellbar, wobei i_1 der kleinste Index ist, für den $s_{i_1} < x$ gilt.*
(2) *Jedes x, $0 < x \leq S$, ist durch die Folge $(s_i)_{i\geq 1}$ darstellbar.*
(3) *Für jedes $n \geq 1$ gilt $s_n \leq \sum_{i=n+1}^{\infty} s_i$.*

Beweis. (1) $\Rightarrow$ (2) Folgt trivialerweise.

(2) $\Rightarrow$ (3) Falls es ein $n \geq 1$ mit $s_n > \sum_{i=n+1}^{\infty} s_i$ gibt, so sei x derart, dass $s_n > x > \sum_{i=n+1}^{\infty} s_i$ gilt. Nach Annahme ist $x = \sum_{j=1}^{\infty} s_{i_j}$ mit $i_1 < i_2 < \ldots$. Aus $s_n > x > s_{i_1}$ folgt $n < i_1$ und daher $x = \sum_{j=1}^{\infty} s_{i_j} \leq \sum_{k=n+1}^{\infty} s_k$, was nicht sein kann.

(3) $\Rightarrow$ (1) Wegen $\lim_{i\to\infty} s_i = 0$ gibt es einen kleinsten Index i_1 derart, dass $s_{i_1} < x$. Gleichermaßen existiert ein kleinster Index i_2 mit $i_1 < i_2$ und $s_{i_2} < x - s_{i_1}$.

Allgemeiner bezeichne i_n für jedes $n \geq 1$ den kleinsten Index, für den $i_{n-1} < i_n$ und $s_{i_n} < x - \sum_{j=1}^{n-1} s_{i_j}$ gilt. Es folgt $x \geq \sum_{j=1}^{\infty} s_{i_j}$.

Angenommen $x > \sum_{j=1}^{\infty} s_{i_j}$. Wir stellen fest, dass es ein N mit folgender Eigenschaft geben muss: Wenn $m \geq N$, dann $s_{i_m} < x - \sum_{j=1}^{m} s_{i_j}$. Denn ansonsten existierten unendlich viele Indizes $n_1 < n_2 < n_3 < \cdots$ derart, dass $s_{i_{n_k}} \geq x - \sum_{j=1}^{n_k} s_{i_j}$. Im Grenzfall ergäbe sich

$$0 = \lim_{k\to\infty} s_{i_{n_k}} \geq x - \sum_{j=1}^{\infty} s_{i_j} > 0,$$

und dies ist ein Widerspruch.

Wir wählen nun das minimale N mit obiger Eigenschaft und zeigen: Für jedes $m \geq N$ gilt $i_m + 1 = i_{m+1}$. Denn

$$s_{i_m+1} < s_{i_m} < x - \sum_{j=1}^{m} s_{i_j},$$

also folgt aus der Definition der Folge der Indizes tatsächlich $i_m + 1 = i_{m+1}$. Daher

$$\{i_N, i_N + 1, i_N + 2, \dots\} = \{i_N, i_{N+1}, i_{N+2}, \dots\}.$$

Als Nächstes zeigen wir, dass $i_N = 1$. Falls $i_N > 1$, so betrachten wir den Index $i_N - 1$ und nach Annahme (3),

$$s_{i_N-1} \leq \sum_{k=i_N}^{\infty} s_k = \sum_{j=N}^{\infty} s_{i_j} < x - \sum_{j=1}^{N-1} s_{i_j}.$$

Wir haben $i_{N-1} \leq i_N - 1 < i_N$. Aber $i_{N-1} < i_N - 1$ ist unmöglich, da i_N als kleinster Index definiert war, der $i_{N-1} < i_N$ und $s_{i_N} < x - \sum_{j=1}^{N-1} s_{i_j}$ erfüllt. Somit gilt $i_{N-1} = i_N - 1$, d.h. $s_{i_{N-1}} < x - \sum_{j=1}^{N-1} s_{i_j}$, und dies stellt einen Widerspruch zur Wahl von N als minimal bezüglich obiger Eigenschaft dar.

Daher ist $i_N = 1$ und $x > \sum_{j=1}^{\infty} s_{i_j} = \sum_{i=1}^{\infty} s_i = S$, was der Annahme widerspricht. □

Wir wollen an dieser Stelle anmerken: Wenn obige Bedingungen für die Folge $(s_i)_{i\geq 1}$ erfüllt sind und wenn gilt $m \geq 0$, dann ist jedes x mit $0 < x < S = \sum_{i=m+1}^{\infty} s_i$ durch die Folge $(s_i)_{i\geq m+1}$ darstellbar. Dabei ist i_1 der kleinste Index derart, dass $m+1 \leq i_1$ und $s_{i_1} < x$.

Tatsächlich ist Bedingung (3) für $(s_i)_{i\geq 1}$ erfüllt und daher auch für $(s_i)_{i\geq m+1}$. Wegen $0 < x < S$ folgt die Anmerkung aus der Proposition.

Proposition 1 wurde verallgemeinert (siehe z.B. FRIDY (1966)). Wir untersuchen nun die Frage einer eindeutigen Darstellung (dies wurde von BROWN (1971) verallgemeinert).

Proposition 2. *Unter Beibehaltung obiger Bezeichnungen sind die folgenden Aussagen äquivalent:*

(2′) *Jedes* x, $0 < x < S$ *besitzt eine eindeutige Darstellung* $x = \sum_{j=1}^{\infty} s_{i_j}$.
(3′) *Für jedes* $n \geq 1$ *gilt* $s_n = \sum_{i=n+1}^{\infty} s_i$.
(4′) *Für jedes* $n \geq 1$ *gilt* $s_n = \frac{1}{2^{n-1}} s_1$ *(und daher* $S = 2s_1$*).*

Beweis. (2′) ⇒ (3′) Angenommen es gibt ein $n \geq 1$ derart, dass $s_n \neq \sum_{i=n+1}^{\infty} s_i$. Da aus (2′) Bedingung (2) und damit auch (3) folgt, gilt $s_n < \sum_{i=n+1}^{\infty} s_i$. Es sei x derart, dass $s_n < x < \sum_{i=n+1}^{\infty} s_i$ erfüllt ist. Nach obiger Anmerkung lässt sich x durch die Folge $\{s_i\}_{i\geq n+1}$ darstellen, d.h. $x = \sum_{j=1, k_j \geq n+1}^{\infty} s_{k_j}$. Andererseits zieht (2′) Bedingung (2) und daher auch (1) nach sich und somit besitzt x eine Darstellung $x = \sum_{j=1}^{\infty} s_{i_j}$, wobei i_1 der kleinste Index mit $s_{i_1} < x$ ist. Aus $s_n < x$ folgt $i_1 \leq n$, und somit hätte x im Widerspruch zur Annahme zwei verschiedene Darstellungen.

(3′) ⇒ (4′) Es ist $s_n = s_{n+1} + \sum_{i=n+2}^{\infty} s_i = 2s_{n+1}$ für jedes $n \geq 1$ und daher $s_n = \frac{1}{2^{n-1}} s_1$ für jedes $n \geq 1$.

(4′) ⇒ (2′) Angenommen es gibt ein x mit $0 < x < S$ und zwei verschiedenen Darstellungen

$$x = \sum_{j=1}^{\infty} s_{i_j} = \sum_{j=1}^{\infty} s_{k_j}.$$

Sei j_0 der kleinste Index mit $i_{j_0} \neq k_{j_0}$, z.B. $i_{j_0} < k_{j_0}$. Dann

$$\sum_{j=j_0}^{\infty} s_{i_j} = \sum_{j=j_0}^{\infty} s_{k_j} \leq \sum_{n=i_{j_0}+1}^{\infty} s_n.$$

Nach Voraussetzung und Division durch s_1 erhalten wir

$$\sum_{n=i_{j_0}}^{\infty} \frac{1}{2^n} \geq \sum_{j=j_0}^{\infty} 2^{1-k_j} = \sum_{j=j_0}^{\infty} 2^{1-i_j} = 2^{1-i_{j_0}} + \sum_{j=j_0+1}^{\infty} 2^{1-i_j}$$
$$= \sum_{n=i_{j_0}}^{\infty} 2^{-n} + \sum_{j=j_0+1}^{\infty} 2^{1-i_j},$$

und somit $\sum_{j=j_0+1}^{\infty} 2^{1-i_j} \leq 0$, was nicht sein kann. □

Für praktische Anwendungen sei noch angemerkt: Wenn $s_n \leq 2s_{n+1}$ für jedes $n \geq 1$ gilt, dann ist Bedingung (3) erfüllt.

Tatsächlich ist

$$\sum_{i=n+1}^{\infty} s_i \leq 2 \sum_{i=n+1}^{\infty} s_{i+1} = 2 \sum_{i=n+2}^{\infty} s_i,$$

daher

$$s_{n+1} \leq \sum_{i=n+2}^{\infty} s_i$$

und $s_n \leq 2s_{n+1} \leq \sum_{i=n+1}^{\infty} s_i$.

2. Wir geben nun mehrere Methoden zur Darstellung reeller Zahlen an.

Zunächst die dyadische Darstellung, die man natürlich auch leicht direkt gewinnen kann:

Korollar 1. *Jede reelle Zahl x, $0 < x < 1$, lässt sich in eindeutiger Weise in der Form $x = \sum_{j=1}^{\infty} \frac{1}{2^{n_j}}$ schreiben (mit $1 \leq n_1 < n_2 < n_3 < \cdots$).*

Beweis. Dies wurde in Proposition 2 gezeigt, man wähle $s_1 = \frac{1}{2}$. □

Korollar 2. *Jede positive reelle Zahl x lässt sich in der Form $x = \sum_{j=1}^{\infty} \frac{1}{n_j}$ schreiben (mit $n_1 < n_2 < n_3 < \cdots$).*

Beweis. Wir betrachten die monoton fallende Folge $(1/n)_{n\geq 1}$ mit Grenzwert 0. Es gilt $\sum_{n=1}^{\infty} \frac{1}{n} = \infty$ und $\frac{1}{n} \leq \frac{2}{n+1}$ für jedes $n \geq 1$. Daher lässt sich nach KAKEYAs Satz und obiger Anmerkung jedes $x > 0$ in der angegebenen Weise darstellen. □

Korollar 3. *Jede positive reelle Zahl x lässt sich in der Form $x = \sum_{j=1}^{\infty} \frac{1}{p_{i_j}}$ schreiben (dabei ist $p_1 < p_2 < p_3 < \cdots$ die aufsteigende Folge der Primzahlen).*

Beweis. Wir betrachten die monoton fallende Folge $(1/p_i)_{i\geq 1}$ mit Grenzwert 0. EULER bewies $\sum_{i=1}^{\infty} \frac{1}{p_i} = \infty$. Nach dem Satz von Tschebyscheff (Beweis von Bertrands „Postulat“) gibt es in jedem Intervall $(n, 2n)$ eine Primzahl, daher gilt $p_{i+1} < 2p_i$ und $\frac{1}{p_i} < \frac{2}{p_{i+1}}$ für jedes $i \geq 1$. Damit ist nach Kakeyas Satz und obiger Anmerkung gezeigt, dass jedes $x > 0$ wie angegeben darstellbar ist. □

3. Wir werden nun reelle Zahlen mit Hilfe von Fibonacci-Zahlen darstellen und dabei erste Eigenschaften solcher Zahlen angeben.

Die ersten beiden Fibonacci-Zahlen sind $F_1 = F_2 = 1$. Für jedes weitere $n \geq 3$ ist F_n durch die rekurrente Folge $F_n = F_{n-1} + F_{n-2}$ definiert.

Somit beginnt die Folge der Fibonacci-Zahlen mit

$$1, 1, 2, 3, 5, 8, 13, 21, 34, 55, 89, 144, \ldots.$$

Im folgenden Lemma geben wir die Fibonacci-Zahlen in einer geschlossenen Form an. Diese geht auf BINET (1843) zurück.

Es sei $\alpha = \frac{\sqrt{5}+1}{2}$ (die Goldene Zahl) und $\beta = -\frac{\sqrt{5}-1}{2}$. Damit gilt $\alpha + \beta = 1$, $\alpha\beta = -1$ und α, β sind die Lösungen von $X^2 - X - 1 = 0$, wobei $-1 < \beta < 0 < 1 < \alpha$.

Lemma 1. *Für jedes $n \geq 1$ ist $F_n = \frac{\alpha^n - \beta^n}{\sqrt{5}}$ und $\frac{\alpha^{n-1}}{\sqrt{5}} < F_n < \frac{\alpha^{n+1}}{\sqrt{5}}$.*

Beweis. Wir betrachten die Folge der Zahlen $G_n = \frac{\alpha^n - \beta^n}{\sqrt{5}}$ für $n \geq 1$. Dann $G_1 = G_2 = 1$ und darüber hinaus,

$$\begin{aligned} G_{n-1} + G_{n-2} &= \frac{\alpha^{n-1} - \beta^{n-1}}{\sqrt{5}} + \frac{\alpha^{n-2} - \beta^{n-2}}{\sqrt{5}} \\ &= \frac{\alpha^{n-2}(\alpha+1) - \beta^{n-2}(\beta+1)}{\sqrt{5}} = \frac{\alpha^n - \beta^n}{\sqrt{5}} \\ &= G_n \end{aligned}$$

da $\alpha^2 = \alpha + 1$ und $\beta^2 = \beta + 1$. Das heißt, die Folge $(G_n)_{n\geq 1}$ fällt mit der Folge der Fibonacci-Zahlen zusammen.

Nun beweisen wir die Abschätzungen.

Wenn $n \geq 1$, dann

$$(-\beta)^n = \frac{1}{\alpha^n} < \alpha^{n-1} = -\alpha^n\beta = \alpha^n(\alpha - 1) = \alpha^{n+1} - \alpha^n,$$

also

$$F_n = \frac{\alpha^n - \beta^n}{\sqrt{5}} \leq \frac{\alpha^n + (-\beta)^n}{\sqrt{5}} < \frac{\alpha^{n+1}}{\sqrt{5}}.$$

In ähnlicher Weise gilt für $n \geq 2$

$$(-\beta)^n = \frac{1}{\alpha^n} < \alpha^{n-2} = -\alpha^{n-1}\beta = \alpha^{n-1}(\alpha - 1) = \alpha^n - \alpha^{n-1},$$

und so

$$F_n = \frac{\alpha^n - \beta^n}{\sqrt{5}} \geq \frac{\alpha^n - (-\beta)^n}{\sqrt{5}} > \frac{\alpha^{n-1}}{\sqrt{5}};$$

was auch für den Fall $n = 1$ richtig ist. □

Für jedes $m \geq 1$ sei nun $I_m = \sum_{n=1}^{\infty} \frac{1}{F_n^{1/m}}$.

Lemma 2. *Für jedes $m \geq 1$ gilt $I_m < \infty$, $I_1 < I_2 < I_3 < \cdots$, und $\lim_{m\to\infty} I_m = \infty$.*

Beweis. Es ist

$$I_m < \sum_{n=1}^{\infty} \left(\frac{\sqrt{5}}{\alpha^{n-1}}\right)^{1/m} = (\sqrt{5})^{1/m} \sum_{n=1}^{\infty} \left(\frac{1}{\alpha^{1/m}}\right)^{n-1} = \frac{(\sqrt{5})^{1/m}\alpha^{1/m}}{\alpha^{1/m} - 1},$$

unter Beachtung, dass $\frac{1}{\alpha^{1/m}} < 1$.

Als Nächstes gelangen wir zu

$$I_{m-1} = \sum_{n=1}^{\infty} \frac{1}{F_n^{1/m-1}} < \sum_{n=1}^{\infty} \frac{1}{F_n^{1/m}} = I_m.$$

Schließlich,

$$I_m = \sum_{n=1}^{\infty} \frac{1}{F_n^{1/m}} > \sum_{n=1}^{\infty} \left(\frac{\sqrt{5}}{\alpha^{n+1}}\right)^{1/m} = \frac{(\sqrt{5})^{1/m}}{\alpha^{1/m}} \times \frac{1}{\alpha^{1/m} - 1};$$

und damit $\lim_{m\to\infty} I_m = \infty$. □

Proposition 3. *Für jede positive reelle Zahl x gibt es ein eindeutiges $m \geq 1$ derart, dass $x = \sum_{j=1}^{\infty} \frac{1}{F_{i_j}^{1/m}}$, aber x nicht die Form $\sum_{j=1}^{\infty} \frac{1}{F_{i_j}^{1/(m-1)}}$ hat.*

Beweis. Zunächst bemerken wir, dass jede der Folgen $(1/F_n^{1/m})_{n\geq 1}$ monoton fallend ist und den Grenzwert 0 hat. Nach obigem Lemma gibt es $m \geq 1$ derart, dass $I_{m-1} < x \leq I_m$ (mit $I_0 = 0$).

Wir stellen fest, dass

$$\frac{1}{F_n} \leq \frac{2}{F_{n+1}} \leq \frac{2^m}{F_{n+1}} \quad \text{für } m \geq 1,$$

da $F_{n+1} = F_n + F_{n-1} < 2F_n$. Nach Proposition 1 und einer früheren Anmerkung ist x wie angegeben darstellbar. Die zweite Aussage folgt schließlich aus $x > I_{m-1} = \sum_{i=1}^{\infty} \frac{1}{F_i^{1/m-1}}$. □

Die Zahl $I_1 = \sum_{n=1}^{\infty} \frac{1}{F_n}$ scheint ziemlich rätselhaft zu sein. Wie wir gesehen haben, ist $\sqrt{5} < I_1 < \sqrt{5}\frac{\alpha}{\alpha-1}$.

4. Im Jahre 1899 gab LANDAU einen Ausdruck für I_1 in Form von Lambert- und Jacobi-Theta-Reihen an. Die Lambert-Reihen sind definiert durch $L(x) = \sum_{n=1}^{\infty} \frac{x^n}{1-x^n}$; sie sind konvergent für $0 < x < 1$, wie man mit Hilfe des Quotientenkriteriums leicht verifizieren kann.

Jacobi-Theta-Reihen sind von entscheidender Bedeutung (z.B. in der Theorie der elliptischen Funktionen) und folgendermaßen definiert: Für $0 < |q| < 1$ und $z \in C$,

$$\begin{aligned}
\theta_1(z,q) &= i \sum_{n=-\infty}^{\infty} (-1)^n q^{\left(n-\frac{1}{2}\right)^2} e^{(2n-1)\pi iz} \\
&= 2q^{1/4} \sin \pi z - 2q^{9/4} \sin 3\pi z + 2q^{25/4} \sin 5\pi z - \cdots \\
\theta_2(z,q) &= \sum_{n=-\infty}^{\infty} q^{\left(n+\frac{1}{2}\right)^2} e^{(2n-1)\pi iz} \\
&= 2q^{1/4} \cos \pi iz + 2q^{9/4} \cos 3\pi z + 2q^{25/4} \cos 5\pi z + \cdots \\
\theta_3(z,q) &= \sum_{n=-\infty}^{\infty} q^{n^2} e^{2n\pi iz} \\
&= 1 + 2q \cos 2\pi z + 2q^4 \cos 4\pi z + 2q^9 \cos 6\pi z + \cdots \\
\theta_4(z,q) &= \sum_{n=-\infty}^{\infty} (-1)^n q^{n^2} e^{2n\pi iz} \\
&= 1 - 2q \cos 2\pi z + 2q^4 \cos 4\pi z - 2q^9 \cos 6\pi z + \cdots
\end{aligned}$$

Insbesondere,

$$\begin{aligned}\theta_1(0,q) &= 0\\ \theta_2(0,q) &= 2q^{1/4}+2q^{9/4}+2q^{25/4}+\cdots\\ \theta_3(0,q) &= 1+2q+2q^4+2q^9+\cdots\\ \theta_4(0,q) &= 1-2q+2q^4-2q^9+\cdots\end{aligned}$$

Wir kommen nun zum Beweis von LANDAUs Satz:

Proposition 4.

$$\sum_{n=1}^{\infty}\frac{1}{F_{2n}} = \sqrt{5}\left[L\left(\frac{3-\sqrt{5}}{2}\right)-L\left(\frac{7-3\sqrt{5}}{2}\right)\right]. \tag{1}$$

$$\begin{aligned}\sum_{n=0}^{\infty}\frac{1}{F_{2n-1}} &= -\sqrt{5}(1+2\beta^4+2\beta^{16}+2\beta^{36}+\cdots)(\beta+\beta^9+\beta^{25}+\cdots)\\ &= -\frac{\sqrt{5}}{2}[\theta_3(0,\beta)-\theta_2(0,\beta^4)]\theta_2(0,\beta^4).\end{aligned} \tag{2}$$

Beweis. (1) Es ist

$$\frac{1}{F_n} = \frac{\sqrt{5}}{\alpha^n-\beta^n} = \frac{\sqrt{5}}{\frac{(-1)^n}{\beta^n}-\beta^n} = \frac{\sqrt{5}\beta^n}{(-1)^n-\beta^{2n}},$$

so dass

$$\begin{aligned}\frac{1}{\sqrt{5}}\sum_{n=1}^{\infty}\frac{1}{F_{2n}} &= \sum_{n=1}^{\infty}\frac{\beta^{2n}}{1-\beta^{4n}} = \sum_{n=1}^{\infty}\sum_{k=0}^{\infty}\beta^{(4k+2)n} = \sum_{k=0}^{\infty}\sum_{n=1}^{\infty}\beta^{(4k+2)n}\\ &= \sum_{k=0}^{\infty}\frac{\beta^{4k+2}}{1-\beta^{4k+2}} = \frac{\beta^2}{1-\beta^2}+\frac{\beta^6}{1-\beta^6}+\frac{\beta^{10}}{1-\beta^{10}}+\cdots.\end{aligned}$$

Wegen $|\beta|<1$ folgt

$$\begin{aligned}\sum_{n=1}^{\infty}\frac{1}{F_{2n}} &= \sqrt{5}\left[L(\beta^2)-L(\beta^4)\right]\\ &= \sqrt{5}\left[L\left(\frac{3-\sqrt{5}}{2}\right)-L\left(\frac{7-3\sqrt{5}}{2}\right)\right].\end{aligned}$$

(2) Hier ist

$$\begin{aligned}\frac{1}{\sqrt{5}}\sum_{n=0}^{\infty}\frac{1}{F_{2n-1}} &= -\sum_{n=0}^{\infty}\frac{\beta^{2n+1}}{1+\beta^{4n+2}}\\ &= -\sum_{n=0}^{\infty}\beta^{2n+1}(1-\beta^{4n+2}+\beta^{8n+4}+\cdots)\\ &= (-\beta+\beta^3-\beta^5+\beta^7-\beta^9+\cdots)\\ &\quad +(-\beta^3+\beta^9-\beta^{15}+\beta^{21}-\cdots)\\ &\quad +(-\beta^5+\beta^{15}-\beta^{25}+\beta^{35}-\cdots)\\ &\quad +(-\beta^7+\beta^{21}-\beta^{35}+\beta^{49}-\cdots)+\cdots .\end{aligned}$$

Wir müssen jetzt den Koeffizienten von β^m bestimmen (für ungerades m). Dabei sei angemerkt, dass aufgrund der absoluten Konvergenz der Reihe die Summanden umgeordnet werden dürfen.

Falls m ungerade ist und m von d geteilt wird, dann taucht β^m in der Zeile beginnend mit $-\beta^{m/d}$ auf. Das Vorzeichen ist

$$\begin{cases}+ & \text{wenn } d\equiv 3 \pmod 4,\\ - & \text{wenn } d\equiv 1 \pmod 4.\end{cases}$$

Der Koeffizient ϵ_m von β^m ist daher $\epsilon_m=\delta_3(m)-\delta_1(m)$, wobei

$$\begin{aligned}\delta_1(m) &= \#\{d \mid 1\le d\le m,\ d\mid m \text{ und } d\equiv 1 \pmod 4\},\\ \delta_3(m) &= \#\{d \mid 1\le d\le m,\ d\mid m \text{ und } d\equiv 3 \pmod 4\}.\end{aligned}$$

Ein wohlbekanntes Resultat von Jacobi (siehe Hardy & Wrights Buch, Seite 241) bringt die Differenz $\delta_1(m)-\delta_3(m)$ mit der Zahl $r(m)=r_2(m)$ der Darstellungen von m als Summe zweier Quadrate in Zusammenhang. Genauer: Es sei $r(m)$ die Anzahl der Paare (s,t) der ganzen Zahlen (inklusive der Null und den negativen Zahlen) derart, dass $m=s^2+t^2$. Jacobi zeigte, dass

$$r(m)=4[\delta_1(m)-\delta_3(m)].$$

Es folgt, dass die Anzahl $r'(m)$ der Paare (s,t) von ganzen Zahlen mit $s>t\ge 0$ und $m=s^2+t^2$ gegeben ist durch

$$r'(m)=\begin{cases}\frac{r(m)}{8} & \text{wenn } m \text{ kein Quadrat ist,}\\ \frac{r(m)-4}{8}1+=\frac{r(m)+4}{8} & \text{wenn } m \text{ ein Quadrat ist;}\end{cases}$$

(der erste Summand entspricht dabei der Darstellung von m als Summe zweier Quadrate ungleich 0).

Daher,

$$\epsilon_m = -\frac{r(m)}{4} = \begin{cases} -2r'(m) & \text{wenn } m \text{ kein Quadrat ist,} \\ -(2r'(m)-1) & \text{wenn } m \text{ ein Quadrat ist.} \end{cases}$$

Da m ungerade ist folgt, dass $s \not\equiv t \pmod 2$ und so

$$\begin{aligned} \frac{1}{\sqrt{5}} \sum_{n=0}^{\infty} \frac{1}{F_{2n+1}} &= \sum_{\substack{m=1 \\ m \text{ ungerade}}}^{\infty} \epsilon_m \beta^m \\ &= -2(1+\beta^4+\beta^{16}+\beta^{36}+\cdots)(\beta+\beta^9+\beta^{25}+\cdots) \\ &\quad +(\beta+\beta^9+\beta^{25}+\cdots) \\ &= -(1+2\beta^4+2\beta^{16}+2\beta^{36}+\cdots)(\beta+\beta^9+\beta^{25}+\cdots). \end{aligned}$$

Somit

$$\sum_{n=0}^{\infty} \frac{1}{F_{2n+1}} = -\sqrt{5}(1+2\beta^4+2\beta^{16}+2\beta^{36}+\cdots)(\beta+\beta^9+\beta^{25}+\cdots).$$

Wir können diese Formel nun mittels Jacobi-Theta-Reihen ausdrücken:

$$\begin{aligned} 1+2\beta^4+2\beta^{16}+2\beta^{36}+\cdots &= (1+2\beta+2\beta^4+2\beta^9+2\beta^{16}+\cdots \\ -(2\beta+2\beta^9+2\beta^{25}+\cdots) &= \theta_3(0,\beta)-\theta_2(0,\beta^4), \end{aligned}$$

also

$$\sum_{n=0}^{\infty} \frac{1}{F_{2n+1}} = -\frac{\sqrt{5}}{2}\left[\theta_3(0,\beta)-\theta_2(0,\beta^4)\right]\theta_2(0,\beta^4).$$

□

Eine Formel von Almqvist (1983), die mir freundlicherweise mitgeteilt wurde, verwendet ausschließlich Theta-Reihen um I_1 auszudrücken:

$$I_1 = \frac{\sqrt{5}}{4}\left\{\left[\theta_2\left(0,-\frac{1}{\beta^2}\right)\right]^2 + \frac{1}{\pi}\int_0^1 \left(\frac{d}{dx}\log\theta_4\left(x,-\frac{1}{\beta^2}\right)\right)\cot \pi x\, dx\right\}.$$

Die folgende Frage blieb lange Zeit unbeantwortet: Ist $I_1 = \sum_{n=1}^{\infty} \frac{1}{F_n}$ irrational? Die Antwort lautet Ja—dies bewies André-Jeannin im Jahr 1989 mittels einer Methode, die an diejenige erinnert, die Apéry für den Beweis der Irrationalität von $\zeta(3) = \sum_{n=1}^{\infty} \frac{1}{n^3}$ verwendete.

Carlitz (1971) betrachtete ferner die folgenden Zahlen:

$$S_k = \sum_{n=1}^{\infty} \frac{1}{F_n F_{n+1} \dots F_{n+k}},$$

wobei $S_0 = \sum_{n=1}^{\infty} \frac{1}{F_n} = I_1$.

Offensichtlich sind diese Reihen sämtlich konvergent. Carlitz zeigte, dass $S_3, S_7, S_{11}, \dots \in \mathbb{Q}(\sqrt{5})$, während $S_{4k} = r_k + r'_k S_0$ für $k \geq 1$ und $r_k, r'_k \in \mathbb{Q}$.

Man könnte sich fragen: Sind alle Zahlen S_0, S_1, S_2 algebraisch unabhängig?

Literaturverzeichnis

1899 E. Landau. Sur la série des inverses de nombres de Fibonacci. *Bull. Soc. Math. France 27*, 298–300.

1941 S. Kakeya. On the partial sums of an infinite series. *Science Reports Tôhoku Imp. Univ. (1)*, 3:159–163.

1960 G. Sansone und J. Gerretsen. *Lectures on the Theory of Functions of a Complex Variable, Vol. I.* P. Noordhoff, Groningen.

1966 J. A. Fridy. Generalized bases for the real numbers. *Fibonacci Q.*, 4:193–201.

1971 J. L. Brown. On generalized bases for real numbers. *Fibonacci Q.*, 9:477–496.

1971 L. Carlitz. Reduction formulas for Fibonacci summations. *Fibonacci Q.*, 9:449–466 und 510.

1987 J. M. Borwein und P. B. Borwein. *Pi and the AGM.* John Wiley & Sons, New York.

1989 R. André-Jeannin. Irrationalité de la somme des inverses de certaines suites récurrentes. *C. R. Acad. Sci. Paris, Sér. I*, 308: 539–541.

3

Primzahlrekorde

Die Primzahltheorie lässt sich grob in vier Untersuchungsbereiche einteilen: Wieviele Primzahlen gibt es? Wie kann man sie generieren? Wie kann man sie erkennen? Wie sind die Primzahlen unter den natürlichen Zahlen verteilt? Bei der Beantwortung dieser Fragen treten Berechnungen auf, die nur für Zahlen bis zu einer gewissen Größe durchführbar sind. In diesem Kapitel sind die größten bisher erreichten Werte erfasst — die Primzahlrekorde.

Alle Welt liebt Rekorde. Sie faszinieren uns und lassen unsere Fantasie blühen. Das berühmte *Guinness Buch der Rekorde*, das bereits in erstaunlicher Anzahl von Ausgaben erschien, enthält viele bemerkenswerte und interessante Begebenheiten und Tatsachen. Wussten Sie zum Beispiel, dass die längste ununterbrochene Fahrt mit dem Fahrrad von Carlos Vieira aus Leiria/Portugal unternommen wurde? Zwischen dem 8. und 16. Juni 1983 radelte er 191 Stunden nonstop und legte dabei eine Strecke von 2407 Kilometern zurück. Oder wussten Sie, dass der größte Stein, der jemals aus einem Menschen herausoperiert wurde, 6,29 Kilogramm wog? Die Patientin war eine 80-jährige Frau aus London, die Operation fand im Jahr 1952 statt. Etwas das unserem Interesse hier näherliegt: Hideaki Tomoyoki, geboren im Jahr 1932 in Yokohama, zitierte 40 000 Ziffern von π aus dem Gedächtnis. Eine heldenhafte Tat, die 17 Stunden und 20 Minuten Zeit erforderte, eingerechnet der Pausen, die sich auf 4 Stunden aufsummierten. Allerdings stößt man beim Blättern im *Guinness Buch* nur auf sehr wenige wissenschaftliche Rekorde, und noch seltener auf Rekorde über Zahlen.

Vor einiger Zeit schrieb ich das Buch *The New Book of Prime Number Records* (RIBENBOIM (1996)[1]), in dem ich von den großen Leistungen der Mathematiker in diesem von Guinness so vernachlässigten Gebiet berichte. Es lohnt sich einmal zu erzählen, wie es zu diesem Buch kam. Von meiner Universität darauf angesprochen, einen Kolloquiumsvortrag für Studierende im Grundstudium zu halten, begann ich mit der Suche nach einem Thema, das zugleich verständlich und interessant ist. Mir kam die Idee, über *Primzahlrekorde* zu sprechen, da das Thema Rekorde schon im Zusammenhang mit Sport bei Studenten sehr beliebt ist. Das Interesse der Studenten übertraf dann meine Erwartungen so sehr, dass ich mich dazu entschloss, eine Monografie über den Vortrag zu verfassen. Beim Schreiben erfuhr ich von so vielen neuen Rekorden, dass der kurze Text, den ich eigentlich verfassen wollte, immer länger wurde. Durch die Hilfe von Kollegen, die mich mit vielen wertvollen Hinweisen versorgten gelang es mir schließlich, diese Arbeit zu vollenden.

Ich muss zugeben, dass ich bei der Vorbereitung zu diesem Vortrag nicht viel über die Sätze zu Primzahlen und Primzahlrekorden wusste (tatsächlich wusste ich sehr wenig!) Die Gegebenheiten erschienen mir zwar interessant, aber doch zusammenhangslos. Es sah so aus, als handelte es sich um isolierte Sätze über Primzahlen und es war nicht ersichtlich, wie daraus eine zusammenhängende Theorie entstehen könnte. Wenn man aber ein Buch schreiben möchte, besteht die erste Aufgabe darin, das Sachgebiet zu einem schlüssigen Ganzen zu formen.

Die wissenschaftliche Methode könnte man als zweistufigen Prozess betrachten: zunächst Beobachtung und Experiment — *Analyse*; dann die Formulierung von Regeln, Theoremen und systematischen Beziehungen der Gegebenheiten — *Synthese*. In dieser Weise spezifiziert bestand meine Aufgabe darin, eine Synthese dessen darzustellen, was über Primzahlen bekannt war und dabei einen Schwerpunkt auf Rekorde zu legen. Jegliche Originalität meiner Arbeit liegt zweifelsohne in der systematischen Untersuchung des Zusammenspiels zwischen Theorie und Berechnung. Dieses Unterfangen benötigt keine Rechtfertigung, wenn man beachtet welche Rolle die Primzahlen in der Zahlentheorie spielen. Schließlich besagt der Fundamentalsatz der Arithmetik, dass sich jede natürliche Zahl $N > 1$ in eindeutiger Weise (bis auf die Reihenfolge der Faktoren) als Produkt von Primzahlen darstellen lässt. Primzah-

[1] siehe auch *Die Welt der Primzahlen* (RIBENBOIM (2006))

len bilden somit das Fundament, auf dem die Struktur der Arithmetik aufgebaut ist.

Wie ging ich nun bei der Ordnung der Theorie der Primzahlen vor? Ich begann damit, vier direkte, eindeutige Fragen zu stellen:

1. Wieviele Primzahlen gibt es?
2. Wie kann man Primzahlen generieren?
3. Wie kann man feststellen, ob eine gegebene Zahl prim ist?
4. Wo befinden sich die Primzahlen?

Die Primzahltheorie entfaltet sich in natürlicher Weise aus diesen vier Fragen, wie ich im Folgenden zeigen werde.

Wieviele Primzahlen gibt es?

Bekanntlich bewies Euklid in seinen *Elemente*n, dass es unendlich viele Primzahlen gibt, er ging dabei wie folgt vor: Angenommen es gäbe nur endlich viele Primzahlen. Dann sei p die größte unter ihnen und P das Produkt aller Primzahlen kleiner oder gleich p; betrachte nun die Zahl P plus 1:

$$P + 1 = \big(\prod_{q \le p} q\big) + 1.$$

Es gibt nun zwei Fälle: Entweder (a) $P + 1$ ist prim oder (b) $P + 1$ ist nicht prim. Im Falle (a) wäre $P + 1$ aber eine Primzahl größer als p. Um wenn (b) wahr wäre, kann keine der Primzahlen $q \le p$ ein Teiler von $P + 1$ sein, die Primfaktoren von $P + 1$ wären also alle größer als p. In beiden Fällen führt die Annahme, dass es eine größte Primzahl p gibt zu einem Widerspruch. Dies zeigt, dass es unendlich viele Primzahlen geben muss.

Aus diesem indirekten Beweis lässt sich kein Verfahren ableiten, um Primzahlen zu erzeugen, aber er wirft sofort eine Frage auf: Gibt es unendlich viele Primzahlen p derart, dass die zugehörige Zahl $P + 1$ auch prim ist? Es gibt viele Mathematiker, die Berechnungen zu diesem Problem angestellt haben.

Rekord. $p = 392113$ *ist die größte bekannte Primzahl für die auch* $P + 1$ *prim ist;* $P + 1$ *besteht aus* 169966 *Ziffern. Dies wurde im September 2001 von* D. Heuer *ermittelt.*

Es gibt viele weitere Beweise (wenn auch nicht unendlich viele) für die Existenz unendlich vieler Primzahlen und jeder enthüllt einen weiteren interessanten Aspekt der Menge aller Primzahlen. EULER zeigte, dass die Reihe der Kehrwerte der Primzahlen divergent ist:

$$\sum \frac{1}{p} = \infty.$$

Auch dies zeigt wieder, dass es nicht nur endlich viele Primzahlen geben kann. EULERs Beweis kann man in vielen Büchern über elementare Zahlentheorie oder reeller Analysis finden, so etwa in Hardy und Wright (1979). Er gestattet eine interessante Schlussfolgerung: Für jedes beliebig kleine $\epsilon > 0$ ist

$$\sum_{n=1}^{\infty} \frac{1}{n^{1-\epsilon}} < \infty.$$

Das heißt, die Primzahlen liegen dichter zusammen bzw. sind nicht so weit verstreut wie Zahlen der Form $n^{1-\epsilon}$. Beispielsweise sind Primzahlen sich näher als die Quadrate n^2, für die EULER zeigte

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

Ein weiterer, einfacher und eleganter Beweis dafür, dass es unendlich viele Primzahlen gibt, wurde von GOLDBACH angegeben. Es reicht offensichtlich, eine unendliche Folge $F_0, F_1, F_2, F_3, \ldots$ paarweise teilerfremder Zahlen zu finden (d.h. keine zwei besitzen einen gemeinsamen Faktor außer der 1); da jedes F_n mindestens einen Primfaktor hat, muss es dann auch unendlich viele Primzahlen geben. Es ist leicht zu zeigen, dass die Folge der Fermat-Zahlen $F_n = 2^{2^n}+1$ diese Eigenschaft besitzt. Offensichtlich sind weder F_n noch F_{n+k} $(k > 0)$ durch 2 teilbar; und wenn p ein ungerader Primteiler von F_n ist, dann gilt $2^{2^n} \equiv -1 \pmod{p}$ und so $2^{2^{n-k}} = (2^{2^n})^{2^k} \equiv 1 \pmod{p}$. Daher $F_{n+k} \equiv 2 \pmod{p}$, und aus $p > 2$ folgt, dass p kein Teiler von F_{n+k} ist. Ich werde auf die Fermat-Zahlen im Anschluss an den nächsten Abschnitt noch näher eingehen.

Die Erzeugung von Primzahlen

Das Problem ist, eine „gute“ Funktion $f : \mathbb{N} \to \{Primzahlen\}$ zu finden. Diese Funktion sollte so einfach wie möglich zu berechnen sein und sich

durch bereits gut bekannte Funktionen ausdrücken lassen. Man könnte der Funktion weitere Eigenschaften abverlangen, so etwa:

Bedingung (a). $f(n)$ ist gleich der $n$ten Primzahl; dies läuft auf eine „Formel“ für die $n$te Primzahl hinaus.

Bedingung (b). Für $m \neq n$, $f(m) \neq f(n)$; dies bedeutet, dass die Funktion verschiedene Primzahlen generiert, nicht aber notwendigerweise alle.

Man kann auch versuchen, eine für ganz $\mathbb{N}$ definierte Funktion f mit ganzzahligen (nicht notwendigerweise positiven) Werten zu finden, die Folgendes erfüllt:

Bedingung (c). Die Menge der Primzahlen stimmt mit der Menge der positiven Werte der Funktion überein. Dies ist eine viel schwächere Bedingung, die man auf unerwartete Weisen erfüllen kann, wie ich später zeige.

Wir wollen mit der Diskussion von Primzahlformeln beginnen. Es gibt viele davon! Tatsächlich haben viele von uns in jungen Jahren eine Formel für die $n$te Primzahl gesucht — und oftmals mit Erfolg. Unglücklicherweise hatten diese Formeln eines gemeinsam: Sie drücken die $n$te Primzahl durch schwer zu berechnende Funktionen der vorangegangenen Primzahlen aus. Folglich sind diese Formeln ungeeignet, um Eigenschaften der Primzahlen aus ihnen abzuleiten. Ich möchte zur Veranschaulichung trotzdem einmal eine solche Formel angeben, die man 1971 fand. Ich werde dies zu Ehren ihres Entdeckers J. M. Gandhi tun, ein Mathematiker, der auch an Fermats letztem Satz arbeitete.

Um die Angabe der Formel zu erleichtern, werde ich zunächst die Möbius-Funktion $\mu : \mathbb{N} \to \mathbb{Z}$ einführen:

$$\mu(n) = \begin{cases} 1 & \text{wenn } n = 1, \\ (-1)^r & \text{wenn } n \text{ quadratfrei und das Produkt von } r \text{ verschiedenen Primfaktoren ist,} \\ 0 & \text{sonst.} \end{cases}$$

Wenn nun $p_1, p_2, p_3, \ldots$ die Folge der Primzahlen in aufsteigender Reihenfolge ist, setze $P_{n-1} = p_1 p_2 \ldots p_{n-1}$; dann ist Gandhis Formel:

$$p_n = \left[1 - \log_2 \left(-\frac{1}{2} + \sum_{d, P_{n-1}} \frac{\mu(d)}{2^d - 1} \right) \right].$$

Hier bezeichnet $\log_2$ den Logarithmus zur Basis 2 und $[x]$ die größte ganze Zahl, die kleiner oder gleich der reellen Zahl x ist.

Man sieht wie schwierig es ist, p_n mithilfe von Gandhis Formel zu berechnen!

Ich werde nun die Konstruktion einer Formel zur Primzahlerzeugung skizzieren. E. M. Wright und G. H. Hardy zeigten in ihrem berühmten Buch (Hardy und Wright (1979)), dass wenn $\omega = 1{,}9287800\ldots$ und

$$f(n) = \left\lceil 2^{2^{\cdot^{\cdot^{2^{\omega}}}}} \right\rceil \qquad \text{(mit } n \text{ Zweien)},$$

dann ist $f(n)$ für alle n prim. Es ergibt sich $f(1) = 3$, $f(2) = 13$ und $f(3) = 16381$. Der Wert $f(4)$ ist bereits sehr schwierig zu berechnen, er hat fast 5000 Stellen. Der genaue Wert von ω erfordert die Kenntnis der Primzahlen, diese Formel ist daher letztendlich uninteressant.

Existieren wirklich einfache Funktionen, die Primzahlen erzeugen? Derartige Polynome kann es nicht geben, was auf das folgende Resultat zurückzuführen ist:

Für jedes $f \in \mathbb{Z}[X_1, \ldots, X_m]$ gibt es unendlich viele m-Tupel ganzer Zahlen $(n_1, \ldots, n_m)$, für die $|f(n_1, \ldots, n_m)|$ eine zerlegbare Zahl ist.

Viele weitere Ergebnisse ähnlicher Art sind bekannt.

Aber gibt es vielleicht Polynome in nur *einer* Unbestimmten, für die viele aufeinander folgende Werte Primzahlen ergeben? Genauer: Sei q eine Primzahl Finde ein Polynom mit Grad 1, d.h. ein Polynom der Form $f_q(X) = dX + q$, dessen Werte an den Stellen $0, 1, \ldots, q-1$ sämtlich prim sind. Dann generiert f_q eine Folge von q Primzahlen in arithmetischer Folge mit Differenz d und Initialwert q.

Für kleine Werte von q ist es einfach, f_q zu finden:

q	d	Werte bei $0, 1, \ldots, q-1$					
2	1	2	3				
3	2	3	5	7			
5	6	5	11	17	23	29	
7	150	7	157	307	…	…	907

Es ist allerdings nicht klar ob man beweisen kann, dass dies für alle Primzahlen q möglich ist.

Im Jahr 1986 ermittelte G. Löh für zwei weitere Primzahlen die kleinsten Werte von d:

$$\text{Für } q = 11, \quad d = 1\,536\,160\,080.$$
$$\text{Für } q = 13, \quad d = 9\,918\,821\,194\,590.$$

Rekord. *Für $q = 17$ errechnete* P. Carmody *im November 2001 den Wert* $d = 41976\,20478\,99923\,32560$

Man kann auch das verwandte Problem untersuchen, die längste Folge von Primzahlen in arithmetischer Folge zu finden.

Rekord. *Die längste bekannte Kette von Primzahlen in arithmetischer Folge fanden* R. Chermoni *und* J. Wroblewski *im Mai 2008. Sie besteht aus* 25 *Termen und beginnt mit* $a = 6\,17105\,49128\,32631$*, die Differenz beträgt* $d = 8173\,76580\,82080$.

Euler entdeckte quadratische Polynome mit vielen Primzahlwerten. Ihm fiel auf, dass wenn q gleich einer der Primzahlen 2, 3, 5, 11, 17 oder 41 ist, dann sind die Werte $f_q(0), f_q(1), \ldots, f_q(q-2)$ des Polynoms $f_q(X) = X^2 + X + q$ sämtlich prim. (Offensichtlich ist $f_q(q-1) = q^2$ nicht prim, also ist diese Folge von zusammenhängenden Primzahlwerten die beste, die man sich erhoffen kann.) Für $q = 41$ ergeben sich diese 40 Primzahlen: $41, 43, 47, 53, \ldots, 1447, 1523, 1601$.

Die nächste Frage ist naheliegend: Gibt es Primzahlen $q > 41$, für die die ersten $q - 1$ Werte von Eulers quadratischem Polynom alle prim sind? Wenn es unendlich viele solcher Primzahlen q gäbe, könnte man beliebig lange Folgen von Primzahlen erzeugen! Allerdings sagt der folgende Satz, dass dies nicht sein kann:

Satz. *Sei q eine Primzahl. Die Zahlen $f_q(0), f_q(1), \ldots, f_q(q-2)$ sind genau dann sämtlich Primzahlen, wenn der imaginär-quadratische Zahlkörper $\mathbb{Q}(\sqrt{1-4q})$ die Klassenzahl 1 hat* (G. Rabinowitsch, 1912).

(Ein quadratischer Zahlkörper K hat Klassenzahl 1, wenn jede algebraische ganze Zahl in K sich als Produkt von Primzahlen in K ausdrücken lässt und wenn sich zwei derartige Darstellungen nur durch einen Einheitsfaktor unterscheiden, d.h. durch eine algebraische ganze Zahl, die ein Teiler von 1 in K ist.)

Satz. *Sei q eine Primzahl. Ein imaginär-quadratischer Zahlkörper $\mathbb{Q}(\sqrt{1-4q})$ hat Klassenzahl 1 genau dann, wenn $4q-1 = 7, 11, 19, 43, 67$ oder 163, d.h. $q = 2, 3, 5, 11, 17$ oder 41.*

Die imaginär-quadratischen Zahlkörper mit Klassenzahl 1 wurden im Jahre 1966 unabhängig voneinander von A. Baker und H. M. Stark bestimmt, zweifelsfrei in Anlehnung an eine frühere Arbeit von Heegner aus dem Jahr 1952.

Somit wurde der folgende, unschlagbare Rekord erreicht:

Rekord. *$q = 41$ ist die größte Primzahl, für die die Werte $f_q(0)$, $f_q(1), \ldots, f_q(q-2)$ des Polynoms $f_q(X) = X^2 + X + q$ alle prim sind.*

Es ist dabei wichtig zu erwähnen, dass hinter der Lösung dieses eher harmlos aussehenden Problems eine ziemlich komplizierte Theorie steckt. Details finden sich in Kapitel 5.

Ich werde mich nun solchen Polynomen zuwenden, deren positiver Wertebereich mit der Menge der Primzahlen übereinstimmt. Die erstaunliche Tatsache, dass derartige Polynome existieren, wurde 1971 von Yu. V. Matijasevič in Verbindung mit Hilberts zehntem Problem entdeckt. Hier die Rekorde, aufgelistet in Abhängigkeit der Anzahl der Unbekannten n und des Grades d des Polynoms:

Rekorde.

n	d	Jahr
21	21	1971 Yu. V. Matijasevič *(nicht explizit angegeben)*
26	25	1976 J. P. Jones, D. Salo, H. Wada, D. Wiens
42	5	1976 Jones et al. *(nicht explizit angegeben): Kleinstes d*
10	$\sim 1{,}6 \times 10^{48}$	1978 Yu. V. Matijasevič *(nicht explizit angegeben): Kleinstes n*

Es ist unbekannt, ob 10 und 5 die Minimalwerte für n bzw. d sind.

Das Erkennen von Primzahlen

Ist es zu einer gegebenen natürlichen Zahl N möglich, in einer endlichen Anzahl von Rechenschritten herauszufinden, ob N eine Primzahl ist? Ja! Es reicht dazu, N durch jede Primzahl d mit $d^2 < N$ zu teilen. Wenn der Rest jedesmal ungleich Null ist, dann ist N prim. Das Problem der Methode ist, dass sie für große N eine sehr große Anzahl von Rechenschritten erfordert. Die Schwierigkeit besteht also darin, einen Algorithmus A zu finden, bei dem die Anzahl der Berechnungsschritte durch eine Funktion f_A in der Zahl der Ziffern von N beschränkt ist, wobei $f_A(N)$ nicht zu schnell mit N wachse. Beispielsweise sollte $f_A(N)$ eine Polynomfunktion der Anzahl der binären Ziffern von N sein, diese ist $1 + [\log_2(N)]$. Im Wesentlichen ist diese Zahl proportional zum natürlichen Logarithmus $\log N$, da $\log_2(N) = \log N / \log 2$.

Das Problem konnte erst im Jahre 2002 von M. Agrawal, N. Kayal und N. Saxena gelöst werden (siehe auch ihr Artikel von 2004). Die Komplexität ihres Algorithmus konnte inzwischen bis auf

$O(\log^{6+\varepsilon} n)$ verbessert werden. Die Suche hatte zu verschiedensten Arten von Primzahltests geführt. Je nach Sichtweise lassen sich diese folgendermaßen klassifizieren:

$$\begin{cases}\text{Algorithmen für beliebige Zahlen}\\ \text{Algorithmen für Zahlen spezieller Form}\end{cases}$$

$$\begin{cases}\text{Algorithmen die nicht auf Vermutungen basieren}\\ \text{Algorithmen denen Vermutungen zugrunde liegen}\end{cases}$$

$$\begin{cases}\text{Deterministische Algorithmen}\\ \text{Probabilistische Algorithmen}\end{cases}$$

Zur Erläuterung dieser Begriffe zeige ich einige Beispiele.

Ein auf beliebige Zahlen anwendbarer Algorithmus stammt von G. L. Miller (1976). Seine Komplexität lässt sich nur mithilfe der verallgemeinerten Riemannschen Vermutung abschätzen. Unter Annahme dieser Vermutung gilt für Millers Algorithmus die Abschätzung $f_A(N) \leq C(\log N)^5$ mit einer positiven Konstante C. Damit handelt es sich um einen Algorithmus, dessen polynomielles Wachstum unsicher ist. Im Gegensatz dazu besitzt der Algorithmus von L. M. Adleman, C. Pomerance und R. S. Rumely (1983) eine völlig sichere Komplexitätsabschätzung: Die Anzahl der Berechnungsschritte als Funktion der binären Ziffern von N ist durch $(\log N)^{C \log\log\log N}$ beschränkt, dabei ist C eine Konstante. Die Komplexität ist daher in der Praxis nicht weit davon entfernt, polynomiell zu sein, zudem kann dieser Algorithmus auf beliebiges N angewendet werden.

Diese Algorithmen sind beide deterministisch, im Gegensatz zu denjenigen, die ich nun beschreiben werde. Zunächst muss ich die sogenannten Pseudoprimzahlen einführen. Sei $a > 1$ eine ganze Zahl. Für jede Primzahl p die a nicht teilt, besagt Fermats kleiner Satz, dass $a^{p-1} \equiv 1 \pmod{p}$. Es ist aber für eine Zahl $N > 1$ mit $a^{N-1} \equiv 1 \pmod{N}$ durchaus möglich, zerlegbar zu sein — in diesem Fall nennen wir N eine *Pseudoprimzahl zur Basis a*. Zum Beispiel ist 341 die kleinste Pseudoprimzahl zur Basis 2. Jede Basis a besitzt unendlich viele Pseudoprimzahlen. Einige unter diesen erfüllen eine zusätzliche Kongruenzbedingung, man nennt sie dann *starke Pseudoprimzahlen zur Basis a*; von ihnen gibt es wiederum unendlich viele.

Ein Algorithmus heißt *probabilistischer Primzahltest*, wenn seine Anwendung auf eine Zahl N entweder dazu führt, dass N zerlegbar ist oder dazu, dass N mit hoher Wahrscheinlichkeit eine Primzahl ist. Zu Tests dieser Art gehören die von R. Baillie und S. S. Wagstaff

(1980) sowie M. O. Rabin (1980). Bei diesen Tests werden gewisse „Belege“ überprüft. Sei $k > 1$ (zum Beispiel $k = 30$) und seien $a_1 = 2, a_2 = 3, \ldots, a_k$ Primzahlen, die als Belege dienen werden. Sollte ein Beleg der Bedingung $a_j^{N-1} \equiv 1 \pmod{N}$ nicht genügen, dann ist N sicher zerlegbar. Wenn die Kongruenz für jeden Beleg a_j gültig ist (das heißt, wenn N Pseudoprimzahl zur Basis a_j für alle $j = 1, 2, \ldots, k$ ist), dann ist N mit hoher Wahrscheinlichkeit eine Primzahl.

Rabins Test verläuft ähnlich, verwendet aber Kongruenzen, die noch einschränkender sind und damit eine höhere Wahrscheinlichkeit zur Folge haben. Der Test führt zum Ergebnis, dass N entweder sicher zerlegbar ist oder aber mit einer Wahrscheinlichkeit von $1-(1/4^k)$ prim. Für $k = 30$ gibt der Test nur in einem von 10^{18} Fällen ein falsches Resultat für N aus. Diese probabilistischen Verfahren lassen sich offensichtlich sehr einfach anwenden.

Ich wende mich nun Primzahltests zu, die auf Zahlen der Form $N \pm 1$ anwendbar sind, wobei viele wenn nicht gar alle der Primfaktoren von N bekannt sind. Die Tests für $N + 1$ hängen von einer schwachen Umkehrung von Fermats letztem Satz ab, die auf Pepin zurückgeht, während die Verfahren für $N - 1$ Lucas-Folgen verwenden.

Im Jahre 1877 zeigte Pepin, dass die Fermat-Zahlen $F_n = 2^{2^n} + 1$ genau dann prim sind, wenn $3^{(F_n-1)/2} \equiv -1 \pmod{F_n}$. Die Suche nach Primzahlen unter den Fermat-Zahlen F_n hat zu einigen Rekorden geführt.

Rekord. *Die größte bekannte Fermat-Primzahl ist* $F_4 = 65537$.

Rekord. F_{11} *ist die größte vollständig faktorisierte Fermat-Zahl (*R. P. Brent *und* F. Morain*,* 1988*)*

Rekord. $F_{2478782}$ *ist die größte als zerlegbar bekannte Fermat-Zahl; sie hat den Faktor* $3 \times 2^{2478785} + 1$ *(*J.B. Cosgrave et. al. 2003*).*

Rekord. F_{33} *ist die kleinste Fermat-Zahl, von der man nicht weiß, ob sie zerlegbar oder eine Primzahl ist.*

Für die Mersenne-Zahlen $M_q = 2^q - 1$ mit einer Primzahl q verwendet man den Lucas-Test (1878): Sei $S_0 = 4, S_{k+1} = S_k^2 - 2$ für $k \geq 0$. Dann ist M_q genau dann prim, wenn M_q Teiler von S_{q-2} ist. Dieser Test ermöglicht es, sehr große Primzahlen zu entdecken.

Rekord. *Bis heute fand man* 46 *Mersenne-Primzahlen. Die größte bekannte Mersenne-Primzahl, zugleich auch die größte bekannte Primzahl überhaupt, ist* M_q *mit* $q = 43\,112\,609$ *(man könnte einfach nachrechnen, dass diese Zahl über* 10 *Millionen Stellen hat). Sie wurde im August 2008 von* E. Smith *gefunden. Die nächstkleinere Mersenne-Primzahl ist* M_q *mit* $q = 37\,156\,667$ *und wurde nur zwei Wochen später von Hans-Michael Elvenich entdeckt.*

Die Suche nach neuen Primzahlen erfuhr einen deutlichen Schub, als G. Woltman einen – man könnte fast sagen, Club gründete, genauer ein echt kooperatives Forschungsprogramm ins Leben rief: „The Great Internet Mersenne Prime Search“ (GIMPS). Es mobilisierte Tausende von Computern rund um die Welt, auf diese Weise konnten die 10 größten bekannten Mersenne-Primzahlen gefunden werden. Der implementierte Algorithmus ist eine Modifikation eines Verfahrens von R. E. Crandall und hat bei der Suche eine wesentliche Rolle gespielt.

Rekord. *Die größte bekannte zerlegbare Mersenne-Zahl ist* M_q *mit* $q = 137211941292195 \times 2^{171960} - 1$ (Z. Járai, G. Farkas, T. Csajbok und J. Kasza, Mai 2006).

Vom Jahr 1876 an, als E. Lucas bewies, dass M_{127} prim ist, bis zum Jahr 1989 hielt den Titel „größte Primzahl“ immer eine Mersenne-Primzahl. Dies ist seit 1992 auch wieder wahr, in den drei Jahren davor aber regierte ein anderer Champion: $391581 \times 2^{216193} - 1$.

Rekord. *Die größte heute bekannte (Nicht-Mersenne-) Primzahl ist* $19249 \times 2^{13018586} + 1$ *mit* 3 918 990 *Ziffern, entdeckt im Jahr* 2007 *von* K. Agafonov *et. al.*

Die Verteilung der Primzahlen

An dieser Stelle ist uns Folgendes bekannt:

1. Es gibt unendlich viele Primzahlen.
2. Es ist keine halbwegs einfache Formel für die Primzahlen bekannt.
3. Man kann feststellen, ob eine gegebene Zahl prim ist, sofern sie nicht zu groß ist.

Was lässt sich über die Verteilung der Primzahlen unter den natürlichen Zahlen sagen? Ich hatte dazu bereits an früherer Stelle einen Hinweis gegeben, der im Zusammenhang mit EULERs Beweis der Existenz unendlich vieler Primzahlen stand: Die Primzahlen liegen enger beieinander als beispielsweise die Quadrate. Eine einfache Methode, die Verteilung der Primzahlen zu studieren besteht darin, ihre Anzahl bis zu einer bestimmten Grenze zu bestimmen. Für jedes reelle $x > 0$ setze $\pi(x) = \#\{\text{Primzahlen } p \mid p \leq x\}$. Es ist also π die Zählfunktion für Primzahlen. Um einen Eindruck des Verhaltens von π zu erlangen, vergleichen wir sie mit einfacheren Funktionen. Diese Vorgehensweise führt zu Aussagen asymptotischer Natur.

Im Alter von nur 15 Jahren vermutete C. F. GAUSS aufgrund seiner Untersuchungen zu Primzahltabellen, dass

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

Das heißt, der Grenzwert des Quotienten

$$\frac{\pi(x)}{x/\log x},$$

für $x \to \infty$ existiert und ist gleich 1. Eine äquivalente Formulierung ist

$$\pi(x) \sim \int_1^x \frac{dt}{\log t}.$$

Die Funktion auf der rechten Seite nennt man den Integrallogarithmus, er wird mit *Li* bezeichnet. GAUSS' Behauptung wurde im Jahr 1896 von J. HADAMARD und C. DE LA VALLÉE POUSSIN bewiesen; zuvor hatte P. L. TSCHEBYSCHEFF gezeigt, dass wenn der Grenzwert existiert, dieser gleich 1 sein muss.

Der Satz zählt zu den wichtigsten Ergebnissen der Primzahltheorie, aus diesem Grund nennt man ihn üblicherweise den *Primzahlsatz*. Allerdings gibt er offensichtlich keinen Hinweis auf den genauen Wert von $\pi(x)$. Für diesen Zweck gibt es die berühmte Formel, die D. F. E. MEISSEL im Jahr 1871 fand. Darin wird der exakte Wert von $\pi(x)$ durch die Werte $\pi(y)$ für alle $y \leq x^{2/3}$ und Primzahlen $p \leq x^{1/2}$ ausgedrückt.

Rekord. *Der größte genau berechnete Wert $\pi(N)$ ist $\pi(4 \times 10^{22}) = 783\,964\,159\,847\,056\,303\,858$. Dieser Wert wurde innerhalb eines von* X. GOURDON *geleiteten verteilten Rechenprojekts bestimmt.*

Die Differenzen

$$\left|\pi(x) - \frac{x}{\log x}\right| \qquad \text{und} \qquad |\pi(x) - Li(x)|$$

sind nicht beschränkt, wenn $x \to \infty$. Die möglichst genaue Auswertung dieser Fehlerterme ist für Anwendungen des Primzahlsatzes von enormer Bedeutung. Auf Grundlage von Tabellen wurde zunächst vermutet und später bewiesen (J. B. Rosser und L. Schoenfeld, 1962), dass $x/\log x \leq \pi(x)$, sobald $x \geq 17$. Die ist insofern bemerkenswert, da im Gegensatz dazu die Differenz $Li(x) - \pi(x)$ unendlich oft das Vorzeichen wechselt, wie J. E. Littlewood (1914) zeigte. Im Jahr 1933 bewies S. Skewes, dass die Differenz $Li(x) - \pi(x)$ für ein x_0 mit $x_0 \leq e^{e^{e^{7,7}}}$ negativ wird. Tatsächlich erfolgt dieser Vorzeichenwechsel viel früher:

Rekord. *Das kleinste x_0, für das $Li(x) < \pi(x)$ muss kleiner als* $6{,}69 \times 10^{370}$ *sein* (H. J. J. te Riele, 1987).

Die wichtigste Funktion beim Studium der Verteilung der Primzahlen ist die Riemannsche *Zetafunktion*: Für jede komplexe Zahl s mit $\mathrm{Re}(s) > 1$ ist die Reihe $\sum_{n=1}^{\infty} 1/n^s$ absolut konvergent; sie ist zudem gleichmäßig konvergent in jeder Halbebene $\{s \mid \mathrm{Re}(s) > 1+\epsilon\}$ für jedes $\epsilon > 0$. Die so definierte Funktion ζ lässt sich zu einer meromorphen Funktion über die ganze komplexe Ebene mit einem einzigen Pol fortsetzen. Dieser Pol liegt im Punkt $s = 1$ und hat die Ordnung 1 und Residuum 1. Es war das Studium der Eigenschaften dieser Funktion, das schließlich zum Beweis des Primzahlsatzes führte. Wie man leicht mithilfe der von ζ erfüllten Funktionalgleichung zeigen kann, besitzt ζ die Nullstellen $-2, -4, -6, \ldots$. Alle anderen Nullstellen von ζ sind komplexe Zahlen $\sigma + it$ (t reell) mit $0 < \sigma < 1$.

Die bis heute unbewiesene *Riemannsche Vermutung* besagt: Die nichttrivialen Nullstellen der Riemannschen Zetafunktion liegen alle auf der *kritischen Geraden* $\frac{1}{2} + it$ (t reell). Ohne allzusehr ins Detail gehen zu wollen möchte ich nur anmerken, dass man viele Sätze über die Verteilung der Primzahlen beweisen könnte, wenn man die Richtigkeit der Riemannschen Vermutung voraussetzt. Es ist daher von grundlegender Bedeutung, die nichttrivialen Nullstellen von ζ zu bestimmen. Aufgrund von Symmetrieeigenschaften reicht es, die Nullstellen mit $t > 0$ zu suchen, die man als Folge $\sigma_n + it_n$ mit $t_n \leq t_{n+1}$ auflisten kann. Im Falle $t_n = t_{n+1}$ müssen wir fordern, dass $\sigma_n < \sigma_{n+1}$. (Es muss zunächst gezeigt werden, dass es nur endlich viele Nullstellen von ζ für jeden Wert von t geben kann.)

Rekord. *Die Riemannsche Vermutung ist für die ersten 10 Billionen Nullstellen verifiziert. Der betreffende Imaginärteil erstreckt sich dabei bis etwa* $2,446 \times 10^{12}$*. Die Berechnungen führte* X. Gourdon *durch (Oktober 2004).*

Rekord. *Im Jahr* 1974 *zeigte* N. Levinson*, dass mindestens ein Drittel der Nullstellen der Riemannschen Zetafunktion auf der kritischen Geraden liegt. Dieses Resultat verbesserte* J. B. Conrey *(1989), er konnte* $1/3$ *durch* $2/5$ *ersetzen.*

Die vorangegangenen Betrachtungen bezogen sich auf das asymptotische Verhalten der Funktionen π und ζ, was sehr nützlich ist, wenn es um die Abschätzung der Fehlerterme geht. Man könnte sagen, es ging um die Bestimmung von π „im Unendlichen“. Ich wende mich nun dem *lokalen* Verhalten von π zu — der Abschätzung der Lücken zwischen den Primzahlen. Hierbei ist die wesentliche Frage: Wenn man die $n$te Primzahl p_n kennt, wo wird man die folgende Primzahl p_{n+1} finden? Man beschäftigt sich also mit der Folge der Differenzen $d_n = p_{n+1} - p_n$. Es ist leicht zu sehen, dass $\limsup d_n = \infty$, das heißt, es gibt beliebig lange Blöcke aufeinander folgender zerlegbarer Zahlen. Hier ist einer: Für jedes N sind die N aufeinander folgenden Zahlen

$$(N+1)!+2, (N+1)!+3, \ldots, (N+1)!+(N+1)$$

sämtlich zerlegbar. Manche Mathematiker haben Spaß daran gefunden, die größten Blöcke aufeinander folgender zerlegbarer Zahlen zwischen relativ kleinen Primzahlen zu finden — die größte Lücke zwischen solchen Primzahlen.

Rekord. *Die größte Lücke zwischen aufeinander folgenden Primzahlen, die explizit bestimmt wurde, besteht aus* 337445 *zerlegbaren Zahlen, die auf eine 7996-stellige Primzahl folgen. Entdeckt hatten die Lücke* T. Alm *und* J.K. Andersen *im Oktober* 2004*, die Bestätigung der Primalität der sie einschließenden Primzahlen erfolgte durch* F. Morain *ein halbes Jahr später.*

Die Frage nach großen Lücken zwischen nicht zu großen Primzahlen lässt sich weiter präzisieren. Man betrachte die Folge d_n/p_n der relativen Lücken. Bereits 1845 stellte J. Bertrand aufgrund von Untersuchungen an Primzahltabellen die Behauptung auf, dass es zwischen p_n und $2p_n$ für jedes $n \geq 1$ eine Primzahl gibt. Es war Tschebyscheff,

der dies erstmals bewies. Man kann die Aussage auch so schreiben: $p_{n+1} < 2p_n$ oder besser noch, $d_n/p_n < 1$. Dieses wenn auch amüsante Resultat ist schwächer als das, was sich aus dem Primzahlsatz ableiten lässt:

$$\lim_{n\to\infty} \frac{d_n}{p_n} = 0.$$

Die Untersuchung von Lücken zwischen Primzahlen führte zu folgender Vermutung: Für jedes $\epsilon > 0$ gilt die Ungleichung $p_{n+1} < p_n + p_n^{1/2+\epsilon}$ für alle genügend großen n.

Rekord. *Als letzter Eintrag einer langen Liste markiert die Arbeit von* R. C. Baker, G. Harman *und* J. Pintz *aus dem Jahr 2001 den aktuellen Rekord:* $p_{n+1} < p_n + p_n^{0{,}525}$.

Was lässt sich über den limes inferior der Differenzenfolge d_n aussagen? Zwei Primzahlen p und p' $(p < p')$ heißen *Primzahlzwillinge*, wenn $p' - p = 2$. Es ist immer noch nicht bekannt, ob es unendlich viele Primzahlzwillinge gibt, d.h. ob $\liminf d_n = 2$. Die Frage ist heikel. Im Jahr 1919 zeigte V. Brun, dass für die Summe über die Kehrwerte von Primzahlzwillingen gilt

$$\sum \left(\frac{1}{p} + \frac{1}{p+2} \right) = B < \infty.$$

Es folgt, dass falls es wie erwartet unendlich viele Primzahlzwillinge gibt, diese sehr dünn gesät sind. Der Wert der Brunschen Konstante B wurde wiederholt berechnet und präzisiert, die letzte Rechnung von 2002 von P. Sebah und P. Demichel ergab $B \approx 1{,}902160583104$.

Rekord. *Das größte heute bekannte Paar von Primzahlzwillingen ist* $2003663613 \times 2^{195000} \pm 1$ *mit 58711 Ziffern, entdeckt innerhalb des verteilten Rechenprojekts* PrimeGrid *im Jahr* 2007.

Fazit

Damit diese Präsentation nicht allzu lang wird, musste ich viele faszinierende Fragen überspringen, so zum Beispiel das Verhalten von Primzahlen in arithmetischen Folgen, ganz zu schweigen von der Goldbachschen Vermutung. Glücklicherweise sind diese und viele weitere in meinem Buch von 2006 ausführlich besprochen und warten nur darauf,

gelesen zu werden! Ich werde diesen Abschnitt mit zwei Kuriositäten beschließen, um diese in Ihr Repertoire einzubringen.

Eine *Repunit-Zahl* ist eine ganze Zahl der Form $R_n = 111\ldots1$ mit n Ziffern gleich 1. Es ist unbekannt, ob unendlich viele prime Repunit-Zahlen existieren, aber es gibt den folgenden Rekord.

Rekord. H. C. Williams *und* H. Dubner *zeigten im Jahr* 1986*, dass* R_{1031} *eine Primzahl ist.*

Es sind nur vier weitere prime Repunit-Zahlen bekannt: R_2, R_{19}, R_{23}, und R_{317}.

Ich führe zum Schluss noch einen bemerkenswerten Rekord an — wenn Sie aber wissen wollen warum und wie er gefunden wurde, müssen Sie D. Broadhurst fragen.

Rekord. *Die größte bekannte Primzahl, deren Ziffern alle prim sind, ist die 82000-stellige Zahl*

$$(10^{40950}+1)\times(10^{20055}+1)\times(10^{10374}+1)\times (10^{4955}+1)\times(10^{2507}+1)\times(10^{1261}+1)\times M+1,$$

wobei

$$M = 3\times R_{1898} + 555531001\times 10^{940} - R_{958}$$

und die R_n *Repunit-Zahlen sind. Gefunden wurde diese Zahl von D. Broadhurst unter Mitwirkung von P. Carmody, G. Childers und weiteren (Oktober 2003).*

Die Betrachtung und das Studium der Primzahlen ist eine gleichermaßen fruchtbare wie unterhaltsame Betätigung. Mathematikern bereiten sie sehr viel Vergnügen und das alleine rechtfertigt den Arbeitsaufwand. Man gelangt schnell dazu, die Primzahlen als Freunde anzusehen — Freunde, die einem Probleme bringen!

Literaturverzeichnis

1979 G. H. Hardy und E. M. Wright. *An Introduction to the Theory of Numbers.* Clarendon Press, Oxford, 5. Ausgabe.

1988 P. Ribenboim. Eulers berühmtes primzahlerzeugendes Polynom und die Klassenzahl imaginär-quadratischer Zahlkörper. Siehe dieses Buch, Kapitel 5.

1991 P. Ribenboim. *The Little Book of Big Primes.* Springer New York 1991.

1996 P. Ribenboim. *The New Book of Prime Number Records.* Springer New York 1996.

2004 M. Agrawal, N. Kayal und N. Saxena Primes is in P. *Ann. Math.*, 160:781–793.

2006 P. Ribenboim. *Die Welt der Primzahlen.* Springer Berlin Heidelberg 2006.

4

Primzahlverkauf

Ich bin ein hohes Tier in einer Fabrik, die Primzahlen produziert.

Und ich werde Ihnen von einem interessanten Dialog mit einem Käufer berichten, der aus einem fremden Land kommt.

Der Dialog

—**Käufer**: Ich möchte gerne einige Primzahlen kaufen.

—**Ich** (großzügig): Ich kann Ihnen viele Primzahlen kostenlos geben: 2, 3, 5, 7, 11, 13, 17, 19, ...

—**Käufer** (mein großzügiges Angebot unterbrechend): Vielen Dank, aber ich möchte Primzahlen mit 100 Stellen. Haben Sie solche zu verkaufen?

—**Ich**: In dieser Fabrik können wir Primzahlen produzieren, die so groß sind wie Sie möchten. Es gibt da eine alte Methode von Euklid, von der Sie vielleicht gehört haben. Angenommen, wir haben n Primzahlen, sagen wir $p_1, p_2, \ldots, p_n$. Wir multiplizieren sie und addieren 1 und erhalten so die Zahl $N = p_1 p_2 \ldots p_n + 1$. Nun ist N entweder selbst eine Primzahl oder aber wir nehmen irgendeinen Primfaktor von N, falls N nicht prim ist. In dieser Weise kann man einfach sehen, dass wir eine Primzahl gewinnen, die nicht unter denen war, die wir vermischt haben. Nennen wir sie p_{n+1}. Wenn wir nun $p_1, p_2, \ldots, p_n, p_{n+1}$ wie erwähnt vermischen, erhalten wir eine weitere Primzahl p_{n+2}. Durch Wiederholung dieser Prozedur kann man soviele Primzahlen erzeugen wie man möchte und so auch welche die mindestens 100 Stellen haben.

—**Käufer**: Es war sehr nett von Ihnen, mir diese Prozedur zu erläutern. Selbst in meiner fernen Heimat hatte ich davon gehört. Man

kann so tatsächlich Primzahlen gewinnen, die beliebig lang sein können. Ich möchte jedoch welche, die ganz genau 100 Stellen haben, nicht mehr, nicht weniger. Haben Sie solche?

—**Ich**: Ja. Vor langer Zeit — zu Beginn des vorletzten Jahrhunderts — bemerkte BERTRAND, dass es zwischen jeder Zahl $N > 1$ und dem Doppelten $2N$, mindestens eine Primzahl gibt. Diese experimentelle Beobachtung wurde durch einen strengen Beweis von TSCHEBYSCHEFF bestätigt. Man kann also auf diese Weise Primzahlen p_1, p_2, p_3 erhalten, wobei

$$\begin{aligned} 10^{99} < p_1 &< 2 \times 10^{99} \\ 2 \times 10^{99} < p_2 &< 4 \times 10^{99} \\ 4 \times 10^{99} < p_3 &< 8 \times 10^{99}. \end{aligned}$$

—**Käufer**: Das heißt, dass Sie garantiert 3 Primzahlen mit 100 Stellen haben, vielleicht ein paar mehr. Aber ich will viele Primzahlen mit 100 Stellen kaufen. Wieviele könnten Sie herstellen?

—**Ich**: Ich habe nie gezählt, wieviele Primzahlen mit 100 Stellen man letzten Endes produzieren könnte. Man sagte mir, dass meine Kollegen in anderen Fabriken die Anzahl aller Primzahlen bis 10^{22} gezählt hätten. Die Anzahl der Primzahlen bis N wird normalerweise mit $\pi(N)$ bezeichnet. Die erwähnte Zählung ergab damit:

$$\begin{aligned} \pi(10^8) &= 5\,761\,455 \\ \pi(10^9) &= 50\,847\,534 \\ \pi(10^{12}) &= 37\,607\,912\,018 \\ \pi(10^{17}) &= 2\,625\,557\,157\,654\,233 \\ \pi(10^{18}) &= 24\,739\,954\,287\,740\,860 \\ \pi(10^{20}) &= 2\,220\,819\,602\,560\,918\,840 \\ \pi(10^{22}) &= 201\,467\,286\,689\,315\,906\,290. \end{aligned}$$

Und obwohl noch in keiner Fabrik alle Primzahlen bis 10^{22} erzeugt wurden, ist die Zählung von $\pi(10^{22})$ genau.

—**Käufer** (ein wenig verwundert): Wenn ich das richtig verstehe, wissen Sie nicht, wieviele Primzahlen einer bestimmten Größe es gibt. Wie können Sie aber dann Ihre Fabrik betreiben und die Auslieferung Ihrer Ware garantieren?

—**Ich**: Ihr Land verkauft doch Öl, oder nicht? Und Sie können zwar ziemlich genau abschätzen, wieviel Öl sich in geringer Tiefe befindet,

aber Sie können nicht genau messen, wieviel sich insgesamt unter der Erde befindet. Bei uns ist es genau dasselbe.

Gauss, einer der führenden Wissenschaftler entdeckte, dass

$$\pi(N) \sim \frac{N}{\log N}$$

für große Werte von N. Dies wurde erst vor etwas über einem Jahrhundert durch Beweise von Hadamard und de la Vallée Poussin bestätigt.

—**Käufer**: Meinen Sie, dass $\pi(N)$ ungefähr gleich $N/\log N$ ist, abgesehen von einem kleinen Fehler?

—**Ich**: Ja. Um genau zu sein geht der relative Fehler, also der Absolutwert der Differenz $|\pi(N) - N/\log N|$ geteilt durch $\pi(N)$ gegen 0, wenn N gegen Unendlich läuft.

—**Käufer**: Also können Sie wegen des Fehlers bei Ihrer Abschätzung nicht sehr präzise sein. Es sei denn, Sie schätzen den Fehler ab.

—**Ich**: Richtig (der Käufer ist nicht dumm ...). Tschebyscheff zeigte vor dem Beweis des Primzahlsatzes, dass für großes N gilt

$$0{,}9\frac{N}{\log N} < \pi(N) < 1{,}1\frac{N}{\log N}.$$

Um die Primzahlen mit 100 Stellen zu zählen:

$$\begin{aligned} 0{,}9\frac{10^{99}}{99\log 10} &< \pi(10^{99}) < 1{,}1\frac{10^{99}}{990\log 10} \\ 0{,}9\frac{10^{100}}{100\log 10} &< \pi(10^{100}) < 1{,}1\frac{10^{100}}{100\log 10}. \end{aligned}$$

Es ist einfach, die Differenz $\pi(10^{100}) - \pi(10^{99})$ abzuschätzen, die die Anzahl der Primzahlen mit genau 100 Stellen angibt:

$$3{,}42 \times 10^{97} < \pi(10^{100}) - \pi(10^{99}) < 4{,}38 \times 10^{97}.$$

—**Käufer**: Sie sind reich! Ich glaube Sie haben mehr Primzahlen als wir Öl. Aber ich frage mich, wie Ihre Fabrik Primzahlen mit 100 Stellen erzeugt. Ich habe eine Idee, allerdings weiß ich nicht, wie effizient meine Methode wäre.

1. Schreibe alle Zahlen mit 100 Stellen auf.
2. Streiche nach und nach alle Vielfachen von 2, von 3, von 5, ..., von jeder Primzahl p kleiner als 10^{99}. Dazu finde man das erste Vielfache von p, streiche dann jede $p$te Zahl.

Was übrig bleibt sind die Primzahlen zwischen 10^{99} und 10^{100}, das heißt die Primzahlen mit genau 100 Stellen.

—**Ich**: Diese Prozedur ist richtig und wurde bereits von ERATOSTHENES entdeckt (im dritten Jahrhundert v. Chr.) In Wirklichkeit könnten Sie sogar aufhören, wenn Sie alle Vielfachen aller Primzahlen kleiner als 10^{50} gestrichen haben.

Allerdings ist diese Produktionsmethode zu langsam. Was erklärt, warum die Archäologen niemals eine Primzahlfabrik unter den griechischen Ruinen entdeckten, sondern nur Tempel für Apollo, Statuen von Aphrodite (seit den Römern als Venus bekannt) und weiteren hässlichen Zeugnissen eines hohen Grades an Dekadenz.

Sogar mit Computern ist dieser Prozess zu langsam für eine praktische Anwendung. Man stelle sich einen Computer vor, der 10^6 Ziffern pro Sekunde schreibt.

- Es gibt $10^{100} - 10^{99} = 10^{99} \times 9$ Zahlen mit 100 Stellen.
- Diese Zahlen haben zusammen $10^{101} \times 9$ Ziffern.
- Man benötigt $10^{95} \times 9$ Sekunden, um diese Zahlen aufzuschreiben, das sind ungefähr $1{,}5 \times 10^{94}$ Minuten oder 25×10^{92} Stunden, also mehr als 10^{91} Tage, das heißt in der Größenordnung von 3×10^{88} Jahren und das sind 3×10^{86} Jahrhunderte!

Und nach dem Aufschreiben der Zahlen (falls es überhaupt noch ein Danach gibt ...) ist noch viel mehr zu erledigen!

Bevor sich der Käufer beschwert, füge ich hinzu:

—**Ich**: Es gibt Möglichkeiten, das Verfahren zu beschleunigen, aber selbst dann ist die Methode immer noch zu langsam. Statt zu versuchen, alle Primzahlen mit 100 Stellen aufzulisten, verwendet unsere Fabrik schnelle Algorithmen zur Erzeugung so vieler Primzahlen wie benötigt werden, um unsere Aufträge zu erfüllen.

—**Käufer**: Ich bin begeistert. Ich wusste nie, wie wichtig es ist, schnelle Verfahren zu haben. Können Sie mir etwas über die Vorgehensweise sagen, die Sie in Ihrer Fabrik verwenden? Ich bin sehr interessiert. [Ja, dieser Käufer war zu neugierig. An dieser Stelle war ich davon überzeugt, dass er ein Spion war.]

—**Ich**: Wenn Sie einen Mercedes kaufen, fragen Sie nicht, wie er gebaut wurde. Sie wählen Ihre Lieblingsfarbe, Rosa, Lila oder Grün mit orangenen Punkten, Sie fahren ihn und sind glücklich, weil alle anderen neidisch auf Sie sind.

Unsere Fabrik wird die Primzahlen ausliefern, die Sie bestellt haben und wir sind sogar besser als Mercedes. Wir geben eine lebenslange Garantie. Auf Wiedersehen, der Herr.

Nach dem Dialog

Ich hoffe, dass Sie nach dem Dialog mit dem Spion-Käufer neugierig darauf geworden sind, die schnelle Prozedur kennenzulernen die wir verwenden, um große Primzahlen zu erzeugen. Ich werde Ihnen einige meiner meistgehüteten Geheimnisse verraten. In unserer Fabrik gibt es zwei Hauptbereiche.

1) Produktion von Primzahlen
2) Qualitätskontrolle.

Produktion von Primzahlen

Einige der Grundlagen unserer Produktionsmethoden wurde vor langer Zeit von Pocklington (1914/16) entdeckt. Ich werde den Satz in einer für unsere spezielle Situation der Primzahlproduktion angepassten Form vorstellen und beweisen. Dann werde ich erläutern, wie man ihn anwenden kann, um in verblüffend kurzer Zeit Primzahlen mit der gewünschten Länge zu gewinnen.

Kriterium von Pocklington. *Sei p eine ungerade Primzahl, k eine natürliche Zahl derart, dass p kein Teiler von k ist und $1 \leq k < 2(p+1)$ gilt. Sei ferner $N = 2kp+1$. Dann sind die folgenden Aussagen gleichwertig:*

1) N ist eine Primzahl.
2) Es gibt eine natürliche Zahl a, $2 \leq a < N$ derart, dass

$$a^{kp} \equiv -1 \pmod{N}$$

und

$$\mathrm{ggT}(a^k + 1, N) = 1.$$

Beweis. (1) $\Rightarrow$ (2) Angenommen N ist eine Primzahl. Bekanntlich gibt es dann eine ganze Zahl a, $1 < a < N$ derart, dass $a^{N-1} \equiv 1 \pmod{N}$, aber $a^m \not\equiv 1 \pmod{N}$ für $1 < m < N-1$; eine solche Zahl a nennt man *Primitivwurzel modulo* N. Also $a^{2kp} \equiv 1 \pmod{N}$, jedoch $a^{kp} \not\equiv 1 \pmod{N}$; somit $a^{kp} \equiv -1 \pmod{N}$. Zudem ist $a^k \not\equiv -1 \pmod{N}$, sonst wäre $a^{2k} \equiv 1 \pmod{N}$, was nicht der Fall ist; also ist $\mathrm{ggT}(a^k + 1, N) = 1$.

(2) $\Rightarrow$ (1) Um zu zeigen, dass N eine Primzahl ist, werden wir beweisen: Wenn q irgendein Primteiler von N ist, dann gilt $\sqrt{N} < q$. Es folgt, dass N keine zwei (gleiche oder verschiedene) Primfaktoren haben kann, also ist N eine Primzahl.

Sei also q irgendein Primfaktor von N. Dann ist $a^{kp} \equiv -1 \pmod{q}$ und $a^{2kp} \equiv 1 \pmod{q}$. Somit ist $\mathrm{ggT}(a, q) = 1$. Sei e die Ordnung von a modulo q, also ist e nach Fermats kleinem Satz Teiler von $q-1$. Gleichermaßen ist e Teiler von $2kp = N-1$, da $a^{2kp} \equiv 1 \pmod{q}$. Man beachte, dass $a^k \not\equiv 1 \pmod{q}$, sonst wäre $a^{kp} \equiv 1 \pmod{q}$; aus $a^{kp} \equiv -1 \pmod{q}$ folgte $q = 2$ und N wäre gerade, was falsch ist.

Aus $\mathrm{ggT}(a^k+1, N) = 1$ ergibt sich $a^k \not\equiv -1 \pmod{q}$. Somit $a^{2k} \not\equiv 1 \pmod{q}$, daher $e \nmid 2k = (N-1)/p$. Aber $e \mid N-1$, also ist $(N-1)/e$ eine ganze Zahl, demzufolge gilt $p \nmid (N-1)/e$. Da $N-1 = e((N-1)/e)$ und $p \mid N-1$, folgt $p \mid e$, somit $p \mid q-1$. Auch gilt $2 \mid q-1$, daher $2p \mid q-1$, so dass $2p \le q-1$ und $2p+1 \le q$. Es folgt, dass $N = 2kp+1 < 2 \times 2(p+1)p+1 = 4p^2+4p+1 = (2p+1)^2 \le q^2$, demzufolge $\sqrt{N} < q$. Dies schließt den Beweis ab. □

Das Kriterium von Pocklington wird auf die folgende Weise angewendet, um Primzahlen der erforderlichen Größe zu produzieren, hier beispielhaft mit 100 Stellen.

Erster Schritt: Wähle zum Beispiel eine Primzahl p_1 mit $d_1 = 5$ Stellen. Finde $k_1 < 2(p_1+1)$ derart, dass $p_2 = 2k_1p_1 + 1$ genau $d_2 = 2d_1 = 10$ Stellen oder $d_2 = 2d_1 - 1 = 9$ Stellen hat und es $a_1 < p_2$ gibt, das die Bedingungen $a_1^{k_1p_1} \equiv -1 \pmod{p_2}$ und $\mathrm{ggT}(a_1^{k_1} + 1, p_2) = 1$ erfüllt. Nach Pocklingtons Kriterium ist p_2 eine Primzahl.

Anschließende Schritte: Wiederhole dieselbe Prozedur beginnend mit der Primzahl p_2 um die Primzahl p_3 zu erhalten, usw.... Um eine Primzahl mit 100 Stellen zu erzeugen, muss der Prozess fünf Male wiederholt werden. Im letzten Schritt sollte man k_5 so wählen, dass $2k_5p_5 + 1$ genau 100 Stellen hat.

Durchführbarkeit des Algorithmus

Wenn p und k mit $1 \leq k < 2(p+1)$ gegeben sind, wobei k kein Vielfaches von p sei und wenn $N = 2kp + 1$ eine Primzahl ist, dann besitzt N eine Primitivwurzel. Es würde zuviele technische Details erfordern, um die folgenden Resultate genau zu erläutern. Manche von ihnen sind Experten bekannt, andere noch unveröffentlicht. Es folgt aus einer verallgemeinerten Form der Riemannsche Vermutung, dass wenn x eine große positive reelle Zahl ist und die positive ganze Zahl a kein Quadrat ist, dann konvergiert das Verhältnis

$$\frac{\#\{\text{Primzahlen } q \leq x \text{ so dass } a \text{ eine Primitivwurzel modulo } q \text{ ist}\}}{\#\{\text{Primzahlen } q \leq x\}}.$$

Wenn a prim ist, dann ist der Grenzwert größer oder gleich Artins Konstante

$$\prod_{q \text{ prim}} \left(1 - \frac{1}{q(q-1)}\right) \approx 0{,}37.$$

Genauer ist für zwei gegebene positive ganze Zahlen a, b, die keine Quadrate sind und eine große Primzahl q die Wahrscheinlichkeit viel höher, dass a oder b eine Primitivwurzel modulo q ist. Wenn man $a = 2$, $b = 3$ wählt, ist sie mindestens 58%. Die entsprechende Wahrscheinlichkeit wächst erheblich, wenn man drei positive ganze Zahlen a, b, c wählt, die keine Quadrate sind.

Dies legt die folgende Vorgehensweise nahe. Gegeben sei eine Primzahl p. Wähle k, das nicht Vielfaches von p ist, mit $1 \leq k < 2(p+1)$. Für primes $N = 2kp+1$ ist es sehr wahrscheinlich, dass $2, 3$ oder 5 eine Primitivwurzel modulo N ist. Falls dies nicht zutrifft, ist es angebracht, eine andere Zahl k' wie k zu wählen und zu prüfen, ob $N' = 2k'p + 1$ eine Primzahl ist.

Die Frage ist: Wie sind die Chancen, ein k derart zu finden, dass N eine Primzahl ist? Ich werde diesen Punkt nun erörtern.

1. Als Spezialfall von Dirichlets berühmten Satz (siehe Ribenboim (2006), Ribenboim (1991)) folgt, dass es für gegebenes p unendlich viele ganze Zahlen $k \geq 1$ derart gibt, dass $2kp + 1$ eine Primzahl ist. Dies lässt sich auf elementare Weise zeigen.
2. Wie klein kann k sein, so dass $2kp + 1$ prim ist? Ein spezieller Fall eines tiefliegenden Satzes von Linnik besagt:
   Für jede genügend große Zahl p gibt es in der arithmetischen Folge

mit erstem Term 1 und Differenz $2p$ eine Primzahl $p_1 = 2kp + 1$, die $p_1 \leq (2p)^L$ erfüllt; dabei ist L eine positive Konstante (die unabhängig von p ist) (siehe Ribenboim (2006)).

3. Vor einiger Zeit zeigte HEATH-BROWN, dass $L \leq 5{,}5$.
4. POCKLINGTONs Kriterium erfordert das Auffinden von $k < 2(p+1)$ derart, dass $p_1 = 2kp + 1$ eine Primzahl ist. Dies impliziert, dass $p_1 < (2p+1)^2$. Es gibt bisher keinen Satz der garantiert, dass solch kleine Werte von k zu einer Primzahl führen.
5. Eine neuere Arbeit von BOMBIERI, FRIEDLANDER, und IWANIEC behandelt Primzahlen p, für die kleine Primzahlen $p_1 = 2kp + 1$ existieren. Ihre Resultate, die Aussagen im Mittel beinhalten, deuten darauf hin, dass es für einen erheblichen Anteil der Primzahlen p eine kleine Primzahl $p_1 = 2kp + 1$ gibt.

Die oben angesprochenen Probleme sind überaus schwierig. In der Praxis können wir die Betrachtungen ignorieren und mit wenigen Versuchen einen geeigneten Wert von k finden.

Zeitliche Abschätzung zur Erzeugung einer 100-stelligen Primzahl

Die Zeit, die der Lauf eines Algorithmus' praktisch benötigt, hängt von der Geschwindigkeit des Computers und von der Anzahl der Bit-Operationen ab (d.h. Ziffern-Operationen).

Als Basis für diese Diskussion sei angenommen, dass der Computer 10^6 Bit-Operationen pro Sekunde erledigen kann. Wenn wir eine obere Schranke für die Anzahl der Bit-Operationen angeben können, ergibt die Division dieser durch 10^6 eine obere Schranke für die Anzahl der benötigten Sekunden.

Ein genauerer Blick auf die Prozedur zeigt, dass sie aus der wiederholten Anwendung der folgenden Operationen auf natürlichen Zahlen besteht: Multiplikation ab modulo n, Exponentiation a^b modulo n, Berechnung des größten gemeinsamen Teilers.

Es ist wohlbekannt (siehe LeVeque (1975), Mignotte (1991)) und nicht schwer zu zeigen, dass es für jede der obigen Operationen eine Konstante $C > 0$ und eine ganze Zahl $e \geq 1$ derart gibt, dass die Zahl der Bit-Operationen, die die Berechnung erfordert, maximal gleich Cd^e beträgt, wobei d die größte der beteiligten Zahlen ist. Die Kombination dieser Abschätzungen ergibt eine obere Schranke derselben Form Cd^e *für die Methode* ($C > 0, e \geq 1$ und d Maximum der beteiligten Zahlen).

Es ist nicht meine Absicht, explizite Werte für C und e anzugeben, wenn p, k und a gegeben sind. Lassen Sie mich nur sagen, dass C, e eher klein sind, so dass der Algorithmus sehr schnell abläuft. Ich möchte betonen, dass diese Abschätzung den Aufwand der Berechnungen von k und a nicht beinhaltet.

Obige Diskussion offenbart, dass es noch Vieles gibt, das berücksichtigt werden muss, um die Primzahlerzeugung und Machbarkeit des Algorithmus zu verstehen. Diese Aufgabe delegieren wir an die Forschungs- und Entwicklungsabteilung unserer Firma. Ich bewundere unsere Kollegen aus der Forschungsabteilung, die mit den tiefen Geheimnissen der Primzahlen konfrontiert sind.

Bevor ich zu einer schnellen Vorstellung unserer Abteilung für Qualitätskontrolle komme, möchte ich gerne ein paar kurze Kommentare der vorangegangenen Betrachtungen abgeben. Sie betreffen die Komplexität des Algorithmus.

Man sagt, ein Algorithmus A auf den natürlichen Zahlen läuft in *Polynomialzeit*, wenn es positive Zahlen C, e (in Abhängigkeit des Algorithmus) derart gibt, dass die Anzahl der Bit-Operationen (oder äquivalent, der Zeit), die benötigt wird, um den Algorithmus auf Zahlen mit maximal d Ziffern anzuwenden, höchstens Cd^e beträgt.

Ein Algorithmus, der nicht in Polynomialzeit läuft, ist ganz sicher zu teuer, um ihn zu implementieren und wird von unserer Fabrik abgelehnt. Eine wesentliche Aufgabe der Forschung ist es, Algorithmen zu finden, die in Polynomialzeit laufen. Unser Algorithmus zur Produktion von Primzahlen gegebener Größe läuft praktisch in Polynomialzeit, obwohl dies noch nicht durch einen Beweis belegt werden konnte.

Qualitätskontrolle

Die Qualitätskontrolle unserer Firma wacht darüber, ob die zum Verkauf stehenden Primzahlen auch wirklich Primzahlen sind. Wenn man POCKLINGTONs Methode verwendet, muss man sich nur Sorgen darüber machen, dass kein dummer Rechenfehler passierte, da sie ansonsten automatisch zu Primzahlen führt. Für den Fall, dass andere Verfahren zur Anwendung kommen, wie ich in Kürze aufzeigen werde, muss man einen Kontrollmechanismus haben. Die Abteilung zur Qualitätssicherung befasst sich auch mit Fragen zur Beratung. Eine große Zahl N wird mit der Frage vorgestellt: Ist N eine Primzahl?

Somit beschäftigt sich unsere Qualitätskontrollabteilung auch mit Primzahltests. Da dies ein einträgliches Geschäft ist, gibt es inzwischen viele zur Verfügung stehende Verfahrung zur Prüfung auf Primalität. Ich möchte diese kurz durch folgende vier Sichtweisen klassifizieren:

1. Tests für beliebige Zahlen.
   Tests für Zahlen spezieller Form, so wie $F_n = 2^{2^n} + 1$ (Fermat-Zahlen), $M_p = 2^p - 1$, (p prim, Mersenne-Zahlen), etc. ...
2. Tests die auf Sätzen beruhen.
   Tests, die sich auf Formen der Riemannschen Vermutung über die Nullstellen der Zetafunktion gründen, oder auf heuristischen Aussagen basieren.
3. Deterministische Tests.
4. Probabilistische oder Monte Carlo-Tests.

Ein deterministischer Test auf eine Zahl N angewandt wird bescheinigen, ob N eine Primzahl oder aber zerlegbar ist. Monte Carlo-Methoden auf N angewandt sagen aus, dass N entweder zerlegbar oder mit hoher Wahrscheinlichkeit prim ist.

Bevor ich fortfahre möchte ich sagen, dass es lange Zeit ein großes Problem war, die folgende Frage zu beantworten: Gibt es einen nicht auf Vermutungen basierenden, deterministischen Primzahltest für beliebige Zahlen, der in Polynomialzeit läuft? Erst im August 2002 konnte diese Frage positiv beantwortet werden, als M. Agrawal, N. Kayal und N. Saxena ein derartiges Verfahren veröffentlichten (siehe auch ihr Artikel von 2004).

Schon der Versuch, alle Methoden und Algorithmen, die für Primzahltests verwendet werden für Sie zu beschreiben wäre langwierig und komplex. Ich werde mich daher nur auf den starken Pseudoprimzahltest beschränken, dieser ist vom Monte Carlo-Typus.

Pseudoprimzahlen

Sei N eine Primzahl und a derart, dass $1 < a < N$. Nach Fermats kleinem Satz gilt dann $a^{N-1} \equiv 1 \pmod{N}$.

Die Umkehrung dessen ist jedoch nicht allgemein wahr. Das kleinste Beispiel ist $N = 341 = 11 \times 31$ mit $a = 2$, $2^{340} \equiv 1 \pmod{341}$.

Man nennt die Zahl N eine *Pseudoprimzahl zur Basis* a, wenn $\mathrm{ggT}(a, N) = 1$, N zerlegbar ist und $a^{N-1} \equiv 1 \pmod{N}$ gilt. Für jedes $a \geq 2$ gibt es unendlich viele Pseudoprimzahlen zur Basis a.

Man beachte nun, dass für jede ungerade Primzahl N folgende Eigenschaft erfüllt ist:

> Für jedes a, $2 \leq a < N$ mit $\mathrm{ggT}(a, N) = 1$, schreibe $N-1$ in der Form $N - 1 = 2^s d$ (wobei $1 \leq s$, d ungerade). Dann ist entweder $a^d \equiv 1 \pmod{N}$ oder es gibt r, $0 \leq r < s$ derart, dass $a^{2^r d} \equiv -1 \pmod{N}$. (∗)

Wiederum gilt die Umkehrung nicht, wie das Beispiel $N = 2047 = 23 \times 89$ mit $a = 2$ zeigt.

Die Zahl N nennt man eine *starke Pseudoprimzahl zur Basis* a, wenn $\mathrm{ggT}(a, N) = 1$, N zerlegbar ist und Bedingung (∗) erfüllt ist.

Der starke Pseudoprimzahltest

Die wesentlichen Schritte beim starken Pseudoprimzahltest für eine Zahl N sind die folgenden:

1. Wähle $k > 1$ Zahlen a, $2 \leq a < N$ derart, dass $\mathrm{ggT}(a, N) = 1$. Dies lässt sich durch Probedivision leicht erreichen und benötigt keine Kenntnis der Primfaktoren von N. Falls $\mathrm{ggT}(a, N) > 1$ für ein a mit $1 < a < N$, dann ist N zerlegbar.
2. Prüfe für jede gewählte Basis a, ob Bedingung (∗) erfüllt ist.

Wenn es ein a gibt, für das (∗) nicht erfüllt ist, dann ist N zerlegbar. Somit ist für ein primes N die Bedingung (∗) für alle Basen a erfüllt. Das Ereignis, dass (∗) für verschiedene Basen erfüllt ist, kann man als unabhängig ansehen, sofern die Wahl der Basen zufällig erfolgte.

Rabin bewies (siehe Ribenboim (2006)): Es sei N zerlegbar. Dann ist die Anzahl der Basen a, für die N eine starke Pseudoprimzahl zur Basis a ist, kleiner als $\frac{1}{4}(N-1)$. Damit ist für zerlegbares N die Wahrscheinlichkeit, dass (∗) für k Basen erfüllt ist, höchstens gleich $1/4^k$. Also ist die Aussage, dass N eine Primzahl ist, wenn (∗) für k verschiedene Basen erfüllt ist, nur in einem von 4^k Fällen falsch; zum Beispiel würde dies für $k = 30$ nur einmal in 10^{18} Fällen passieren.

Der starke Pseudoprimzahltest läuft in Polynomialzeit und ist auf jede Zahl anwendbar.

Unter der Voraussetzung einer verallgemeinerten Form der Riemannschen Vermutung zeigte Miller (siehe Ribenboim (2006)): Wenn N zerlegbar ist, dann gibt es eine Basis a mit $\mathrm{ggT}(a, N) = 1$ und $a < (\log N)^{2+\varepsilon}$ derart, dass (∗) nicht erfüllt ist.

Eine neue Produktionsmethode

Wir können RABINs Test verwenden, um Zahlen mit 100 Stellen zu produzieren und sie mit einer nur sehr geringen Fehlerwahrscheinlichkeit als Primzahlen zu zertifizieren.

1. Wähle eine Zahl N mit 100 Stellen. Bevor man mit der harten Arbeit beginnt, ist es ein Leichtes, durch Probedivision bis z.B. 1000 herauszufinden, ob N kleine Faktoren besitzt. Falls dies nicht der Fall ist, behalte N, ansonsten wähle N' und verfahre in gleicher Weise.
2. Verwende 30 kleine, zu N teilerfremde Zahlen a als Basen um zu verifizieren, ob Bedingung $(*)$ erfüllt ist. Verwerfe N falls für irgendeine Basis a Bedingung $(*)$ nicht gilt und wiederhole den Prozess mit einer anderen Zahl N'. Falls $(*)$ für alle a erfüllt ist, können wir nach Rabins Berechnung N als Primzahl deklarieren; wenn wir dies tun, liegen wir nur in höchstens einer von 10^{18} Zahlen falsch. Wieviel Pech muss man haben, um gleich zweimal hintereinander zerlegbare Zahlen zu wählen? Nach den bereits erwähnten Ungleichungen von TSCHEBYSCHEFF ist der Anteil der 100-stelligen Primzahlen, die prim sind, nicht kleiner als $\frac{3{,}42}{9\times 10^2} \approx \frac{1}{260}$ und nicht größer als $\frac{4{,}38}{9\times 10^2} \approx \frac{1}{205}$. Nicht intelligente Angestellte, die gerade Zahlen wählen oder solche, die durch $3, 5, \ldots$ oder kleine Primzahlen (sagen wir bis 1000) teilbar sind, werden mit Sicherheit gefeuert. Die Chance eine Primzahl auszuwählen wächst, und es ist durchaus vernünftig, Rabins Methode zur Primzahlproduktion zu verwenden.

Wir können die Zahl N sogar mit einer „Geld-zurück-Garantie“ als Primzahl verkaufen, da die Wahrscheinlichkeit, dass wir eine zerlegbare Zahl als Primzahl verkaufen, nur einmal in 1 000 000 000 000 000 000 Fällen passiert! Dies ist eine bessere Garantie als irgendjemand sonst bei egal welchem Handel geben kann. Wir sind sicher, dass unsere Firma nicht bankrott geht und sie weiterhin in großzügiger Weise meine Reisen finanziert, um für unsere Produkte zu werben — einhergehend mit üppigen Dinners und feinsten Weinen, um unsere Kunden davon zu überzeugen, dass Primzahlen zu einer Lebensart geworden sind.

Anhang

Hier ist ein Beispiel einer Primzahl mit 100 Stellen, berechnet von L. Roberts, unter Verwendung der Methode von Pocklington.

$p_1 = 2333$ $k_1 = 2001$ $a_1 = 2$
$p_2 = 9336667$ $k_2 = 9336705$ $a_2 = 3$
$p_3 = 174347410924471$ $k_3 = 174347410924479$ $a_3 = 2$
$p_4 = 607940393921354891483080512 19$
$k_4 = 607940393921354891483080512 56$ $a_4 = 3$
$p_5 = 739183045122504318980574950295193587260702667372985056 2129$
$k_5 = 500000000000000000000000000000000000000137$ $a_5 = 2$
$p_6 = 739183045122504318980574950295193587260905203527348622 396300677536380883042909432530860197905402334 7$

Literaturverzeichnis

1914 H. C. Pocklington. The determination of the prime or composite nature of large numbers by Fermat's theorem. *Proc. Cambridge Phil. Soc.*, 18:29–30.

1975 W. J. LeVeque, Herausgeber. *Studies in Number Theory.* Math. Assoc. of America, Washington.

1979 D. A. Plaisted. Fast verification, testing and generation of large primes. *Theor. Comp. Sci.*, 9:1–16.

1991 M. Mignotte. *Mathematics for Computer Algebra.* Springer-Verlag, New York.

1991 P. Ribenboim. *The Little Book of Big Primes.* Springer-Verlag, New York.

1996 P. Ribenboim. *The New Book of Prime Number Records.* Springer-Verlag, New York.

2004 M. Agrawal, N. Kayal und N. Saxena Primes is in P. *Ann. Math.*, 160:781–793.

2006 P. Ribenboim. *Die Welt der Primzahlen.* Springer-Verlag, Heidelberg.

5

Eulers berühmtes primzahlerzeugendes Polynom und die Klassenzahl imaginär-quadratischer Zahlkörper[1]

Einführung

Kann ein nicht-konstantes Polynom mit ganzzahligen Koeffizienten ausschließlich Primzahlwerte annehmen?

Nein! Aufgrund von Folgendem:

Satz. *Wenn $f(X) \in \mathbb{Z}[X]$ mit Grad > 0, dann gibt es unendlich viele natürliche Zahlen n derart, dass $f(n)$ zerlegbar ist.*

Beweis. Die Aussage ist wahr, wenn $f(n)$ für jedes $n \geq 1$ zerlegbar ist. Angenommen, es gäbe ein $n_0 \geq 1$, das zu einem primen $f(n_0) = p$ führt. Da $\lim_{n\to\infty} |f(n)| = \infty$, gibt es $n_0 \geq 1$ derart, dass wenn $n \geq n_1$, dann $|f(n)| > p$. Nehme irgendein h mit $n_0 + ph \geq n_1$. Dann $|f(n_0+ph)| > p$, aber $f(n_0 + ph) = f(n_0) + (\text{Vielfaches von } p) = \text{Vielfaches von } p$, also ist $|f(n_0 + ph)|$ zerlegbar. □

Muss andererseits ein nicht-konstantes Polynom $f(X) \in \mathbb{Z}[X]$ immer mindestens einen Primzahlwert annehmen?

Die Frage ist von Interesse, wenn $f(X)$ irreduzibel und primitiv ist (das heißt, der größte gemeinsame Teiler seiner Koeffizienten ist gleich 1) und es darüberhinaus keine Primzahl p gibt, die alle Werte $f(n)$ teilt (für beliebige ganze Zahlen n).

[1] Dies ist die Niederschrift einer Vorlesung an der Universität von Rom am 8. Mai 1986. Die Originalvorlage verschwand, als mein Gepäck in Toronto (!) gestohlen wurde; ich hatte jedoch eine Kopie an meinen Freund Paolo Maroscia geschickt, dessen Gepäck in Rom nicht gestohlen wurde (!) und der so freundlich war, mich einen Blick in seine Kopie werfen zu lassen. Es ist gut, Freunde zu haben.

Bunjakowski und später Schinzel und Sierpiński (1958) vermuteten, dass jedes Polynom $f(X) \in \mathbb{Z}[X]$, das obigen Bedingungen genügt, mindestens einen Primzahlwert annimmt. Dies konnte nie für beliebige Polynome bewiesen werden. Für die speziellen Polynome $f(X) = aX+b$ mit $\mathrm{ggT}(a, b) = 1$ stimmt die Aussage — dies ist nichts Anderes als der berühmte Satz von Dirichlet: Jede arithmetische Folge

$$\{a + kb \mid k = 0, 1, 2, \dots\} \quad \text{mit} \quad \mathrm{ggT}(a, b) = 1,$$

enthält unendlich viele Primzahlen.

In meinem Buch *Die Welt der Primzahlen* (2006) weise ich auf viele erstaunliche Konsequenzen aus der Hypothese von Bunjakowski hin, die Schinzel und Sierpiński ableiteten. Aber das ist nicht Gegenstand dieses Kapitels.

Ungeachtet des Satzes und dessen, was ich gerade sagte, ist es für viele Polynome leicht zu verifizieren, dass sie Primzahlwerte annehmen und es ist denkbar, dass dies für viele aufeinander folgende ganze Zahlen geschieht. Zum Beispiel hat Eulers berühmtes Polynom $f(X) = X^2 + X + 41$ die Eigenschaft, dass $f(n)$ für $n = 0, 1, \dots, 39$ prim ist (40 aufeinanderfolgende Primzahlwerte):

> 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.

Allerdings ist $f(40) = 40^2 + 40 + 41 = 40 \times 41 + 41 = 41^2$.

Man beachte, dass wenn $n > 0$, dann $(-n)^2 + (-n) + 41 = (n - 1)^2 + (n - 1) + 41$, also wird $X^2 + X + 41$ auch prim für die Zahlen

$$n = -40, -39, \dots, -2, -1.$$

Welche anderen Polynome haben obige Eigenschaft?

Einige dieser Polynome kann man einfach aus $X^2 + X + c$ gewinnen, indem man X durch $X - a$ ersetzt, wobei $a \geq 1$. Zum Beispiel $(X - a)^2 + (X - a) + 41 = X^2 - (2a - 1)X + (a^2 - a + 41)$; wählt man $a = 1$, dann ergibt sich $X^2 - X + 41$, das prime Werte für jede Zahl n, $-39 \leq n \leq 40$ ergibt, während die Wahl von $a = 40$ zu $X^2 - 79X + 1601$ führt, das für jede Zahl n, $0 \leq n \leq 79$ Primzahlwerte annimmt. Dies sind aber die gleichen Werte die auch $X^2 + X + 41$ erzeugt, zweifach genommen. Zusammenfassend scheint es interessant,

die Aufmerksamkeit auf Polynome der Form X^2+X+c und ihre Werte bei aufeinanderfolgenden ganzen Zahlen $n = 0, 1, \ldots$ zu konzentrieren. Wenn der Wert an der Stelle 0 gleich einer Primzahl q ist, dann ist $c = q$. Da $(q-1)^2 + (q-1) + q = q^2$, kann $X^2 + X + q$ bestenfalls für $0, 1, 2, \ldots, q-2$ Primzahlwerte ergeben (so wie bei $q = 41$). Zum Beispiel ist $f(n)$ für $f(X) = X^2 + X + q$ und $q = 2, 3, 5, 11, 17, 41$, für alle Argumente $n = 0, 1, \ldots, q-2$ prim. Für $q = 7, 13, 19, 23, 29, 31, 37$ ist dies jedoch nicht wahr, wie man leicht nachprüfen kann.

Gibt es ein $q > 41$ derart, dass X^2+X+q für $n = 0, 1, \ldots q-2$ prim ist? Gibt es unendlich oder nur endlich viele solcher Primzahlen q? Falls es nur endlich viele sind, welches ist das größtmögliche q?

Dasselbe Problem sollte man sich für Polynome ersten Grades $f(X) = aX + b$ mit $a, b \geq 1$ stellen. Wenn $f(0)$ gleich einer Primzahl q ist, so $b = q$. Dann ist $f(q) = aq + q = (a+1)q$ zerlegbar. Somit kann $aX + q$ bestenfalls für X gleich $0, 1, \ldots, q-1$ prime Werte annehmen.

Kann man derartige Polynome finden? Äquivalent ausgedrückt, kann man arithmetische Folgen mit q Primzahlen finden, von denen die erste Zahl mit q übereinstimmt?

Für kleine Werte von q ist dies nicht schwer.

Falls $q = 3$, wähle: 3, 5, 7, also $f(X) = 2X + 3$.

Falls $q = 5$, wähle: 5, 11, 17, 23, 29, also $f(X) = 6X + 5$.

Falls $q = 7$, wähle: 7, 157, 307, 457, 607, 757, 907, also $f(X) = 150X + 7$.

Vor einiger Zeit informierte mich Keller darüber, dass für $q = 11, 13$ die kleinsten derartigen arithmetischen Folgen durch die Polynome $f(X) = d_{11}X + 11$, bzw. $f(X) = d_{13}X + 13$ gegeben werden, dabei ist

$$d_{11} = 1536160080 = 2 \times 3 \times 5 \times 7 \times 7315048,$$
$$d_{13} = 9918821194590 = 2 \times 3 \times 5 \times 7 \times 11 \times 4293861989;$$

diese Bestimmung erforderte eine nicht zu unterschätzende Rechenzeit, die Berechnung führten Keller und Löh durch. Inzwischen ist auch der Wert von d_{17} bekannt, gefunden hat ihn P. Carmody im Jahr 2001:

$$d_{17} = 341976204789992332560.$$

Man weiß nicht, ob es für jede Primzahl q eine arithmetische Folge von q Primzahlen gibt, von denen die erste Zahl q selbst ist. Schon

das Problem, beliebig lange arithmetische Folgen zu finden, die ausschließlich aus Primzahlen bestehen (ohne Einschränkung des Initialwerts oder der Differenz) war lange Zeit offen und konnte erst im Jahr 2004 von B. Green und T. Tao gelöst werden (siehe auch ihren Artikel von 2008). Ihr Beweis war nicht konstruktiv, die längste bekannte derartige Folge besteht aus 25 Primzahlen und wurde von R. Chermoni und J. Wroblewski im Mai 2008 gefunden.

Die Bestimmung aller Polynome $f(X) = X^2 + X + q$, die prime $f(n)$ für $n = 0, 1, \ldots, q-2$ ergeben, ist eng mit der Theorie imaginärquadratischer Zahlkörper verbunden. Um diesen Zusammenhang verstehen zu können, werde ich nun die dazu notwendigen Hauptresultate vorstellen.

1 Quadratische Erweiterungen

Es sei d eine ganze Zahl, jedoch kein Quadrat und $K = \mathbb{Q}(\sqrt{d})$ der Körper aller Elemente $\alpha = a + b\sqrt{d}$, wobei $a, b \in \mathbb{Q}$. Ohne Einschränkung der Allgemeinheit kann man annehmen, dass d quadratfrei ist, somit $d \not\equiv 0 \pmod 4$. Die Körpererweiterung $K|\mathbb{Q}$ ist quadratisch, das heißt, K bildet einen Vektorraum der Dimension 2 über $\mathbb{Q}$.

Umgekehrt gilt, dass wenn K eine quadratische Körpererweiterung von $\mathbb{Q}$ ist, es notwendigerweise die Form $K = \mathbb{Q}(\sqrt{d})$ haben muss, wobei d eine quadratfreie Zahl ist.

Wenn $d > 0$, dann ist K ein Teilkörper des Körpers $\mathbb{R}$ der reellen Zahlen: man nennt ihn einen *reellen quadratischen Zahlkörper*.

Wenn $d < 0$, dann ist K kein Teilkörper von $\mathbb{R}$ und man nennt K einen *imaginär-quadratischen Zahlkörper*.

Wenn $\alpha = a + b\sqrt{d} \in K$ mit $a, b \in \mathbb{Q}$, dann ist das komplex konjugierte Element $\alpha' = a - b\sqrt{d}$. Offensichtlich gilt $\alpha = \alpha'$ genau dann, wenn $\alpha \in \mathbb{Q}$.

Die Norm von α ist $N(\alpha) = \alpha\alpha' = a^2 - db^2 \in \mathbb{Q}$. Es ist klar, dass $N(\alpha) \neq 0$ genau dann, wenn $\alpha \neq 0$. Falls $\alpha, \beta \in K$, dann $N(\alpha\beta) = N(\alpha)N(\beta)$; insbesondere ist $N(\alpha) = \alpha^2$, falls $\alpha \in \mathbb{Q}$.

Die Spur von α ist $\mathrm{Sp}(\alpha) = \alpha + \alpha' = 2\alpha \in \mathbb{Q}$. Wenn $\alpha, \beta \in K$, dann $\mathrm{Sp}(\alpha + \beta) = \mathrm{Sp}(\alpha) + \mathrm{Sp}(\beta)$; insbesondere gilt für $\alpha \in \mathbb{Q}$, dass $\mathrm{Sp}(\alpha) = 2\alpha$.

Es ist offensichtlich, dass α, α' die Nullstellen der quadratischen Gleichung $X^2 - \mathrm{Sp}(\alpha)X + N(\alpha) = 0$ sind.

2 Ganzheitsringe

Sei $K = \mathbb{Q}(\sqrt{d})$, wobei d eine quadratfreie Zahl ist.

Das Element $\alpha \in K$ ist eine algebraische ganze Zahl, wenn es ganze Zahlen $m, n \in \mathbb{Z}$ derart gibt, dass $\alpha^2 + m\alpha + n = 0$.

Sei A die Menge aller algebraischen ganzen Zahlen von K. Die Menge A ist ein Unterring von K, dem Körper der Brüche von A, und es ist $A \cap \mathbb{Q} = \mathbb{Z}$. Wenn $\alpha \in A$, dann ist das Konjugierte α' ein Element von A. Offensichtlich gilt $\alpha \in A$ genau dann, wenn sowohl $N(\alpha)$ als auch $\mathrm{Sp}(\alpha)$ in $\mathbb{Z}$ liegen.

Hier ein Kriterium für die Bestimmung, ob das Element $\alpha = a + b\sqrt{d} (a, b \in \mathbb{Q})$ eine algebraische ganze Zahl ist: $\alpha \in A$ genau dann, wenn

$$\begin{cases} 2a = u \in \mathbb{Z}, & 2b = v \in \mathbb{Z} \\ u^2 - dv^2 \equiv 0 \pmod 4. \end{cases}$$

Mithilfe dieses Kriteriums lässt sich zeigen:

Wenn $d \equiv 2$ oder $3 \pmod 4$, dann $A = \{a + b\sqrt{d} \mid a, b \in \mathbb{Z}\}$.

Wenn $d \equiv 1 \pmod 4$, so $A = \{\frac{1}{2}(a+b\sqrt{d}) \mid a, b \in \mathbb{Z}, a \equiv b \pmod 2\}$.

Wenn $\alpha_1, \alpha_2 \in A$ die Eigenschaft haben, dass jedes Element $\alpha \in A$ auf eindeutige Weise die Form $\alpha = m_1\alpha_1 + m_2\alpha_2$ mit $m_1, m_2 \in \mathbb{Z}$ hat, dann nennt man $\{\alpha_1, \alpha_2\}$ eine *Ganzheitsbasis* von A. Mit anderen Worten, $A = \mathbb{Z}\alpha_1 \oplus \mathbb{Z}\alpha_2$.

Wenn $d \equiv 2$ oder $3 \pmod 4$, dann ist $\{1, \sqrt{d}\}$ eine Ganzheitsbasis von A.

Wenn $d \equiv 1 \pmod 4$, dann ist $\left\{1, \frac{1+\sqrt{d}}{2}\right\}$ eine Ganzheitsbasis von A.

3 Diskriminanten

Sei $\{\alpha_1, \alpha_2\}$ eine Ganzheitsbasis. Dann ist

$$D = D_k = \det \begin{pmatrix} \mathrm{Sp}(\alpha_1^2) & \mathrm{Sp}(\alpha_1\alpha_2) \\ \mathrm{Sp}(\alpha_1\alpha_2) & \mathrm{Sp}(\alpha_2^2) \end{pmatrix}$$

unabhängig von der Wahl der Ganzheitsbasis. Man nennt D die *Diskriminante* von K. D ist eine ganze Zahl ungleich Null.

Wenn $d \equiv 2$ oder $3 \pmod 4$, dann

$$D = \det \begin{pmatrix} \mathrm{Sp}(2) & \mathrm{Sp}(\sqrt{d}) \\ \mathrm{Sp}(\sqrt{d}) & \mathrm{Sp}(d) \end{pmatrix} = \det \begin{pmatrix} 2 & 0 \\ 0 & 2d \end{pmatrix},$$

also $D = 4d$.

Falls $d \equiv 1 \pmod 4$, dann

$$D = \det \begin{pmatrix} \mathrm{Sp}(1) & \mathrm{Sp}\left(\frac{1+\sqrt{d}}{2}\right) \\ \mathrm{Sp}\left(\frac{1+\sqrt{d}}{2}\right) & \mathrm{Sp}\left(\frac{1+\sqrt{d}}{2}\right)^2 \end{pmatrix} = \det \begin{pmatrix} 2 & 1 \\ 0 & \frac{1+d}{2} \end{pmatrix},$$

also $D = d$.

Jede Diskriminante D ist kongruent zu 0 oder 1 (mod 4).

In Form der Diskriminanten,

$$A = \{(a + b\sqrt{D})/2 \mid a, b \in \mathbb{Z}, a^2 \equiv Db^2 \pmod 4\}.$$

4 Zerlegung von Primzahlen

Sei $K = \mathbb{Q}(\sqrt{d})$ mit einer quadratfreien ganzen Zahl d und sei A der Ganzheitsring von K.

Das Ideal $P \neq 0$ von A ist ein Primideal, wenn der Restklassenring A/P keine Nullteiler hat.

Wenn P ein Primideal ist, dann gibt es eine eindeutige Primzahl p derart, dass $P \cap \mathbb{Z} = \mathbb{Z}p$ oder äquivalent, dass $P \supseteq Ap$.

Wenn I, J Ideale von A ungleich dem Nullideal sind, dann nennt man I einen Teiler von J, wenn es ein Ideal I_1 von A gibt mit $I \cdot I_1 = J$.

Das Primideal P das die Primzahl p enthält, teilt das Ideal Ap.

Wenn I ein vom Nullideal verschiedenes Ideal von A ist, dann ist der Restklassenring A/I endlich. Die Norm von I ist $N(I) = \#(A/I)$.

A Eigenschaften der Norm

Wenn I, J Ideale ungleich Null sind, dann ist $N(I, J) = N(I)N(J)$. Wenn I Teiler von J ist, dann ist $N(I)$ Teiler von $N(J)$.

Wenn $\alpha \in A$, $\alpha \neq 0$, dann $N(A\alpha) = |N(\alpha)|$ (Absolutwert der Norm von α). Insbesondere, wenn $a \in \mathbb{Z}$, dann $N(Aa) = a^2$.
Wenn das Primideal P Teiler von Ap ist, dann ist $N(P)$ gleich p oder p^2.

Jedes vom Nullideal verschiedene Ideal I ist in eindeutiger Weise das Produkt von Primideal-Potenzen:

$$I = \prod_{i=1}^{n} P_i^{e_i}.$$

Wenn I, J Ideale ungleich Null sind und wenn $I \supseteq J$, dann ist I Teiler von J.

Jedes Ideal $I \neq 0$ lässt sich durch zwei Elemente generieren, von denen sich eines aus $\mathbb{Z}$ wählen lässt; wenn $I \cap \mathbb{Z} = \mathbb{Z}n$, dann $I = An + A\alpha$ für ein $\alpha \in A$. In diesem Fall wird die Bezeichnungsweise $I = (n, \alpha)$ verwendet.

Betrachte nun den Spezialfall, wenn p eine Primzahl ist. Dann ist Ap von einem der folgenden Typen:

$$\begin{cases} Ap = P^2, & \text{wobei } P \text{ ein Primideal ist: } p \text{ ist in } K \text{ verzweigt.} \\ Ap = P, & \text{wobei } P \text{ ein Primideal ist: } p \text{ ist in } K \text{ unbeteiligt.} \\ Ap = P_1 P_2, & \text{wobei } P_1, P_2 \text{ verschiedene Primideale sind: } p \text{ ist} \\ & \text{in } K \text{ zerfallen.} \end{cases}$$

Man beachte auch, dass wenn $Ap = I \cdot J$, wobei I und J irgendwelche nicht notwendigerweise verschiedenen Ideale ungleich A sind, dann muss es sich bei I und J um Primideale handeln.

Ich werde nun aufzeigen, wann eine Primzahl p sich verzweigt, unbeteiligt ist oder zerfällt und zudem Generatoren für die Primideale von A angeben. Es gibt zwei Fälle: $p \neq 2$ und $p = 2$.

Es bezeichne $\left(\frac{d}{p}\right)$ das Legendre-Symbol, also

$$\left(\frac{d}{p}\right) = \begin{cases} 0 & \text{wenn } p \text{ Teiler von } d \text{ ist,} \\ +1 & \text{wenn } d \text{ ein Quadrat modulo } p \text{ ist,} \\ -1 & \text{wenn } d \text{ kein Quadrat modulo } p \text{ ist.} \end{cases}$$

Sei $p \neq 2$.

1) Wenn p Teiler von d ist, dann $Ap = (p, \sqrt{d})^2$.
2) Wenn p kein Teiler von d ist und es kein $a \in \mathbb{Z}$ derart gibt, dass gilt $d \equiv a^2 \pmod{p}$, dann ist Ap ein Primideal.
3) Wenn p kein Teiler von d ist und es $a \in \mathbb{Z}$ derart gibt, dass $d \equiv a^2 \pmod{p}$, dann $Ap = (p, a + \sqrt{d})(p, a - \sqrt{d})$.

Daher,

1) p ist verzweigt genau dann, wenn $\left(\frac{d}{p}\right) = 0$.
2) p ist unbeteiligt genau dann, wenn $\left(\frac{d}{p}\right) = -1$.
3) p ist zerfallen genau dann, wenn $\left(\frac{d}{p}\right) = +1$.

Beweis. Der Beweis teilt sich in verschiedene Abschnitte auf. (a) Wenn $\left(\frac{d}{p}\right) = -1$, dann ist Ap ein Primideal.

Ansonsten ist $Ap = P \cdot P'$ oder P^2 mit $P \cap \mathbb{Z} = \mathbb{Z}p$. Sei $\alpha \in A$ derart, dass $P = (p, \alpha) \supseteq A\alpha$, also $P \mid A\alpha$, somit ist p Teiler von $N(P)$, das wiederum $N(A\alpha) = |N(\alpha)|$ teilt. Wenn $p \mid \alpha$, dann $\frac{\alpha}{p} \in A$ und $P = Ap \cdot \left(1, \frac{\alpha}{p}\right) = Ap$, was nicht sein kann. Also $p \nmid \alpha$. Dann,

$$\begin{cases} d \equiv 2 \text{ oder } 3 \pmod 4 \\ d \equiv 1 \pmod 4 \end{cases} \Rightarrow \begin{cases} \alpha = a + b\sqrt{d}, & \text{mit } a, b \in \mathbb{Z} \\ \alpha = \frac{a+b\sqrt{d}}{2}, & \text{mit } a, b \in \mathbb{Z},\ a \equiv b \pmod 2 \end{cases}$$
$$\Rightarrow \begin{cases} N(\alpha) = a - db^2 \\ N(\alpha) = \frac{a^2 - db^2}{4} \end{cases}$$
$$\Rightarrow p \text{ teilt } a^2 - db^2,$$

daher $a^2 \equiv db^2 \pmod p$, und so $p \nmid b$ (ansonsten $p \mid a$ und $p \mid \alpha$, was nicht sein kann).

Sei b' dergestalt, dass $bb' \equiv 1 \pmod p$, also $(ab')^2 \equiv d \pmod p$, damit entweder $p \mid d$ oder $\left(\frac{d}{p}\right) = +1$, was einen Widerspruch bedeutet.

(b) Wenn $\left(\frac{d}{p}\right) = 0$, dann $Ap = (p, \sqrt{d})^2$.

Sei $P = (p, \sqrt{d})$, also

$$P^2 = (p^2, p\sqrt{d}, d) = Ap\left(p, \sqrt{d}, \frac{d}{p}\right)$$

da $\frac{d}{p} \in \mathbb{Z}$. Aber d ist quadratfrei, also $\text{ggT}\left(p, \frac{d}{p}\right) = 1$, somit $P^2 = Ap$, und daraus folgt, dass P ein Primideal ist.

(c) Wenn $\left(\frac{d}{p}\right) = -1$, dann $Ap = (p, a + \sqrt{d})(p, a - \sqrt{d})$, wobei $1 \le a \le p - 1$ und $a^2 \equiv d \pmod p$.

Denn es gilt

$$\begin{aligned}(p, a + \sqrt{d})(p, a - \sqrt{d}) &= (p^2, pa + p\sqrt{d}, pa - p\sqrt{d}, a^2 - d) \\ &= Ap\left(p, a + \sqrt{d}, a - \sqrt{d}, \frac{a^2 - d}{p}\right) \\ &= Ap\left(p, a + \sqrt{d}, a - \sqrt{d}, 2a, \frac{a^2 - d}{p}\right) \\ &= Ap,\end{aligned}$$

da $\text{ggT}(p, 2a) = 1$. Wenn eines der Ideale $(p, a + \sqrt{d})$, $(p, a - \sqrt{d})$ gleich A ist, so würde dies auch für das andere gelten, was nicht sein kann.

Also sind $(p, a+\sqrt{d})$, $(p, a-\sqrt{d})$ Primideale. Sie sind verschieden: Wenn $(p, a+\sqrt{d}) = (p, a-\sqrt{d})$ wäre, dann sind sie gleich ihrer Summe

$$(p, a+\sqrt{d}, a-\sqrt{d}) = (p, a+\sqrt{d}, a-\sqrt{d}, 2a) = A,$$

was nicht sein kann.

Schließlich gilt, dass diese drei Fälle ausschließend und vollständig sind, so dass die Umkehraussagen ebenso gelten. □

Bemerkung. Wenn $d \equiv 1 \pmod 4$ und $d \equiv a^2 \pmod p$, dann

$$(p, a+\sqrt{d}) = (p, l(a-1)+\omega),$$

wobei $\omega = \frac{1+\sqrt{d}}{2}$ und $2l \equiv 1 \pmod p$. Damit gibt es, wenn $\left(\frac{d}{p}\right) \neq -1$, ein $b \in \mathbb{Z}$, $0 \leq b \leq p-1$ derart, dass p Teiler von $N(b+\omega)$ ist. Darüberhinaus ist $d \equiv 1 \pmod p$, falls $b = p-1$.

Es ist $a+\sqrt{d} = a-1+2\omega$. Wenn $2l \equiv 1 \pmod p$, dann

$$(p, a+\sqrt{d}) = (p, (a-1)+2\omega) = (p, l(a-1)+\omega).$$

Wenn $\left(\frac{d}{p}\right) \neq -1$, dann gibt es ein Primideal P, das Ap teilt, wobei

$$P = (p, a+\sqrt{d}), \quad 0 \leq a \leq p-1.$$

Also $P = (p, b+\omega)$ mit $0 \leq b \leq p-1$ und $b \equiv l(a-1) \pmod p$.

Aus $P \supseteq A(b+\omega)$ folgt, dass p Teiler von $N(P)$ ist, welches $N(b+w)$ teilt. Schließlich, falls $N(p-1+\omega) = N\left(\frac{2p-1+\sqrt{d}}{2}\right) = \frac{(2p-1)^2-d}{4}$ von p geteilt wird, ist p Teiler von $\frac{1-d}{4}$, also $d \equiv 1 \pmod p$.

Sei $p = 2$.

Wenn $d \equiv 2 \pmod 4$, dann $A2 = (2, \sqrt{d})^2$.

Wenn $d \equiv 3 \pmod 4$, dann $A2 = (2, 1+\sqrt{d})^2$.

Wenn $d \equiv 1 \pmod 8$, dann $A2 = (2, \omega)(2, \omega')$.

Wenn $d \equiv 5 \pmod 8$, dann ist $A2$ ein Primideal.

Daher,

(1) 2 ist verzweigt genau dann, wenn $d \equiv 2$ oder $3 \pmod 4$.

(2) 2 ist unbeteiligt genau dann, wenn $d \equiv 5 \pmod 8$.

(3) 2 ist zerfallen genau dann, wenn $d \equiv 1 \pmod 8$.

Beweis. Der Beweis teilt sich in verschiedene Abschnitte auf.

(a) Wenn $d \equiv 5 \pmod 8$, dann ist $A2$ ein Primideal.

Ansonsten gilt $A2 = P \cdot P'$ oder P^2, mit $P \cap \mathbb{Z} = \mathbb{Z}2$. Dann gibt es $\alpha \in A$ derart, dass $P = (2, \alpha) \supseteq A\alpha$, somit ist P Teiler von $A\alpha$ und 2 teilt $N(P)$, das Teiler von $N(\alpha)$ ist.

Wenn $2 \mid a$, dann $P = A2\left(l, \frac{\alpha}{2}\right) = A2$, was nicht sein kann. Daher

$$2 \nmid \alpha = \frac{a + b\sqrt{d}}{2}, \quad \text{mit } a \equiv b \pmod 2,$$

also $N(\alpha) = \frac{a^2 - db^2}{4}$. Da $2 \mid N(\alpha)$: 8 teilt $a^2 - db^2 \equiv a^2 - 5b^2 \equiv a^2 + 3b^2 \pmod 8$.

Wenn a, b ungerade sind, dann $a^2 \equiv b^2 \equiv 1 \pmod 8$, also $a^2 + 3b^2 = 4 \pmod 8$, was nicht sein kann. Also sind a, b gerade, $a = 2a'$, $b = 2b'$, und $\alpha = a' + b'\sqrt{d}$. 2 teilt $N(\alpha) = (a')^2 - d(b')^2$.

Da d ungerade ist folgt, dass a', b' beide gerade oder beide ungerade sind. Wenn a', b' gerade sind, dann wird α von 2 geteilt, was nicht sein kann. Wenn a', b' beide ungerade sind, dann $\alpha = a' + b'\sqrt{d} =$ (Vielfaches von 2) $+ 1 + \sqrt{d} =$ (Vielfaches von 2) $+ 2\omega =$ (Vielfaches von 2), was nicht sein kann.

(b) Wenn $d \equiv 1 \pmod 8$, dann $A2 = (2, \omega)(2, \omega')$.

Tatsächlich,

$$(2, \omega)(2, \omega') = \left(4, 2\omega, 2\omega', \frac{1-d}{4}\right) = A2\left(2, \omega, \omega', \frac{1-d}{8}\right) = A2,$$

da $\omega + \omega' = 1$.

Auch ist $(2, \omega) \neq (2, \omega')$, da ansonsten diese Ideale gleich ihrer Summe $(2, \omega, \omega') = A$ wären, weil $\omega + \omega' = 1$.

(c) Wenn $d \equiv 2$ oder $3 \pmod 4$, dann $A2 = (2, \sqrt{d})^2$, bzw. $(2, 1 + \sqrt{d})^2$.

Zunächst sei $d = 4e + 2$; dann

$$(2, \sqrt{d})^2 = (4, 2\sqrt{d}, d) = A2(2, \sqrt{d}, 2e + 1) = A2,$$

also ist $(2, \sqrt{d})$ ein Primideal.

Nun sei $d = 4e + 3$; dann

$$\begin{aligned}
(2, 1 + \sqrt{d})^2 &= (4, 2 + 2\sqrt{d}, 1 + d + 2\sqrt{d}) \\
&= (4, 2 + 2\sqrt{d}, 4(e+1) + 2\sqrt{d}) \\
&= A2(2, 1 + \sqrt{d}, 2(e+1) + \sqrt{d}) \\
&= A2(2, 2e + 1, 1 + \sqrt{d}, 2(e+1) + \sqrt{d}) \\
&= A2,
\end{aligned}$$

und somit ist $(2, 1 + \sqrt{d})$ ein Primideal.

Wieder gilt, dass diese drei Fälle ausschließend und vollständig sind, so dass die Umkehraussagen ebenso gelten. □

5 Einheiten

Das Element $\alpha \in A$ ist eine Einheit, wenn es $\beta \in A$ derart gibt, dass $\alpha\beta = 1$. Die Menge U der Einheiten bildet mit der Multiplikation eine Gruppe. Es folgt eine Beschreibung der Gruppe von Einheiten für die verschiedenen Fälle. Zunächst sei $d < 0$.

Sei $d \neq -1, -3$; dann $U = \{\pm 1\}$.

Sei $d = -1$; dann $U = \{\pm 1, \pm i\}$, mit $i = \sqrt{-1}$.

Sei $d = -3$; dann $U = \{\pm 1, \pm\rho, \pm\rho^2\}$, mit $\rho^3 = 1$, $\rho \neq 1$, d.h. $\rho = \frac{-1+\sqrt{-3}}{2}$.

Sei $d > 0$. Dann ist die Gruppe der Einheiten gleich dem Produkt $U = \{\pm 1\} \times C$, wobei C eine zyklische, multiplikative Gruppe ist. Daher ist $C = \{\epsilon^n \mid n \in \mathbb{Z}\}$, wobei ϵ die kleinste Einheit mit $\epsilon > 1$ ist. Das Element ϵ nennt man die *Fundamentaleinheit*.

6 Die Klassenzahl

Die Theorie der quadratischen Zahlkörper hat seine Wurzeln im Studium der binären quadratischen Formen $aX^2 + bXY + cY^2$ (wobei a, b, c ganze Zahlen sind und $ac \neq 0$). Die Diskriminante der Form ist nach Definition $D = b^2 - 4ac$. Man beachte, dass $D \equiv 0$ oder $1 \pmod 4$; sei $d = D/4$ bzw. $d = D$.

Man sagt, eine ganze Zahl m wird durch die Form repräsentiert, wenn es ganze Zahlen x, y derart gibt, dass $m = ax^2 + bxy + cy^2$.

Wenn eine Form $a'(X')^2 + b'X'Y + c'(Y')^2$ sich durch einen linearen Tausch der Variablen aus obiger Form ergibt,

$$\begin{cases} X = hX' + kY' \\ Y = mX' + nY' \end{cases}$$

wobei h, k, m, n ganze Zahlen sind und die Determinante $hn - km = 1$ ist, dann stellen die zwei Formen dieselben ganzen Zahlen dar. In diesem Sinne liegt es nahe, solche Formen als äquivalent anzusehen. Offensichtlich haben äquivalente Formen dieselbe Diskriminante.

In seinem Werk *Disquisitiones Arithmeticae* klassifizierte Gauss die binären quadratischen Formen mit gegebener Diskriminante D. Gauss definierte eine Operation zur Komposition zwischen Äquivalenzklassen von Formen einer gegebenen Diskriminante. Die Klassen bilden unter dieser Operation eine Gruppe. Gauss zeigte, dass es für eine gegebene Diskriminante D nur endlich viele Äquivalenzklassen binärer quadratischer Formen gibt.

Die Theorie wurde später neu interpretiert, indem jede Form $aX^2 + bXY + cY^2$ der Diskriminanten D dem Ideal I von $\mathbb{Q}(\sqrt{d}) = \mathbb{Q}(\sqrt{D})$ generiert durch a und $\frac{-b+\sqrt{D}}{2}$ zugeordnet wurde. Definiere zwei nicht-Null-Ideale I, I' als äquivalent, wenn es ein Element $\alpha \in \mathbb{Q}(\sqrt{d})$ ungleich Null derart gibt, dass $I = A\alpha \cdot I'$. Dann korrespondieren äquivalente binäre quadratische Formen mit äquivalenten Idealen und die Komposition der Äquivalenzklassen von Formen entspricht der Multiplikation von Äquivalenzklassen von Idealen. Somit hat $\mathbb{Q}(\sqrt{d})$ endlich viele Idealklassen. Es bezeichne $h = h(d)$ die Anzahl der Idealklassen oder die Klassenzahl des Körpers $\mathbb{Q}(\sqrt{d})$.

Es ist die Klassenzahl $h(d)$ genau dann gleich 1, wenn jedes Ideal von $\mathbb{Q}(\sqrt{d})$ ein Hauptideal ist.

Gauss vermutete, dass es für jedes $h \geq 1$ nur endlich viele imaginärquadratische Zahlkörper $\mathbb{Q}(\sqrt{d})$ (mit $d < 0$) mit Klassenzahl h gibt. Ich werde bald mehr über diese Vermutung berichten.

Ich werde nun beschreiben, wie man die Klassenzahl der quadratischen Zahlkörper $\mathbb{Q}(\sqrt{D})$ berechnen kann. Definiere die reelle Zahl θ wie folgt:

$$\theta = \begin{cases} \frac{1}{2}\sqrt{D} & \text{wenn } D > 0, \\ \frac{2}{\pi}\sqrt{-D} & \text{wenn } D < 0. \end{cases}$$

Ein nicht-Null-Ideal I von A heißt *normalisiert*, wenn $N(I) \leq [\theta]$ (die größte ganze Zahl kleiner oder gleich θ). Man nennt das Ideal I *primitiv*, wenn es keine Primzahl p derart gibt, dass Ap Teiler von I ist.

Sei $\mathcal{N}$ die Menge normalisierter primitiver Ideale von A.

Wenn $I \in \mathcal{N}$ und wenn p eine verzweigte Primzahl ist, dann gilt $p^2 \nmid N(I)$. Wenn p eine unbeteiligte Primzahl ist, dann ist $p \nmid N(I)$. Somit

$$N(I) = \prod_{r \text{ verzweigt}} r \times \prod_{p \text{ zerfallen}} p^{e(p)}.$$

Man kann zeigen, dass jede Klasse von Idealen ein primitives normalisiertes Ideal enthält. Aus der Tatsache, dass es für jedes $m \geq 1$ höchstens endlich viele Ideale I von A mit $N(I) = m$ gibt folgt einmal mehr, dass die Anzahl der Idealklassen endlich ist.

Man beachte, dass wenn $\mathcal{N}$ nur aus dem Einheitsideal $A = A \cdot 1$ besteht, dann ist $h = 1$. Also folgt $h = 1$, wenn jede Primzahl p mit $p \leq [\theta]$ unbeteiligt ist. Tatsächlich, wenn $I \in \mathcal{N}$, dann $N(I) = 1$, also ist I das Einheitsideal, folglich ist $h = 1$.

Es bezeichne $N(\mathcal{N})$ die Menge der ganzen Zahlen $N(I)$, für die $I \in \mathcal{N}$.

Um entscheiden zu können, ob die Ideale I, $J \in \mathcal{N}$ äquivalent sind, muss man herausfinden, welche ganzen Zahlen $m \in N(\mathcal{N})$ die Form $m = N(A\alpha)$ haben.

Sei $m \geq 1$ und

$$\alpha = \begin{cases} u + v\sqrt{d} & \text{wenn } d \equiv 2 \text{ oder } 3 \pmod 4, \text{ mit } u, v \in \mathbb{Z}, \\ \frac{u+v\sqrt{d}}{2} & \text{wenn } d \equiv 1 \pmod 4, \text{ mit } u, v \in \mathbb{Z},\ u \equiv v \pmod 2. \end{cases}$$

Es folgt nun, dass $A\alpha$ genau dann ein primitives Ideal mit $N(A\alpha) = m$ ist, wenn

$$\begin{cases} m = |u^2 - dv^2| & \operatorname{ggT}(u, v) = 1 \quad \text{wenn } d \equiv 2 \text{ oder } 3 \pmod 4, \\ m = \frac{|u^2-dv^2|}{4} & \operatorname{ggT}\left(\frac{u-v}{2}, v\right) = 1 \quad \text{wenn } d \equiv 1 \pmod 4. \end{cases}$$

(dies nennt man die *primitive Darstellung* von m).

Beweis. Sei $d \equiv 2$ oder $3 \pmod 4$, $m = N(A\alpha) = |u^2 - dv^2|$, also $\operatorname{ggT}(u, v) = 1$, da $A\alpha$ primitiv ist.

Sei $d \equiv 1 \pmod 4$, $m = N(A\alpha) = \frac{|u^2-dv^2|}{4}$, somit gilt, dass wenn p Teiler von $\frac{u-v}{2}$ ist und p zudem v teilt, dann teilt p auch $\alpha = \frac{u-v}{2} - v\left(\frac{1+\sqrt{d}}{2}\right)$, was im Widerspruch zur Annahme steht.

Umgekehrt sei $d \equiv 2$ oder $3 \pmod 4$, also $N(A\alpha) = m$: Wenn p Teiler von $A\alpha$ ist, dann folgt aus der Tatsache, dass $\{1, \sqrt{d}\}$ eine Integralbasis ist, dass $p \mid u$ und $p \mid v$, was nicht sein kann.

Sei $d \equiv 1 \pmod 4$, also $N(A\alpha) = m$. Falls p Teiler von $A\alpha$ ist folgt aus der Tatsache, dass

$$\alpha = \frac{u-v}{2} + v\left(\frac{1+\sqrt{d}}{2}\right) \quad \text{und} \quad \left\{1, \frac{1+\sqrt{d}}{2}\right\}$$

eine Integralbasis ist, dass p auch $\frac{u-v}{2}$ und v teilt, was nicht sein kann. □

A Berechnung der Klassenzahl

Sei $d > 0$, also $\theta = \frac{1}{2}\sqrt{D}$.

$[\theta] = 1$.

Aus $1 \leq \frac{1}{2}\sqrt{D} < 2$ folgt, dass $4 \leq D < 16$ mit $D \equiv 0$ oder $1 \pmod 4$, somit $D \in \{4, 5, 8, 9, 12, 13\}$ und daher $d \in \{5, 2, 3, 13\}$.

Nun ist $N(\mathcal{N}) = \{1\}$, damit besteht $\mathcal{N}$ nur aus dem Einheitsideal und daher $h = 1$.

$[\theta] = 2$.

Aus $2 \leq \frac{1}{2}\sqrt{D} < 3$ erhält man, dass $16 \leq D < 36$ mit $D \equiv 0$ oder $1 \pmod 4$, somit $D \in \{16, 17, 20, 21, 24, 25, 28, 29, 32, 33\}$ und daher $d \in \{17, 21, 6, 7, 29, 33\}$.

Nun ist $N(\mathcal{N}) = \{1, 2\}$.

Nehme zum Beispiel $d = 17$. Da $17 \equiv 1 \pmod 8$ ergibt sich $A^2 = P \cdot P'$, $N(P) = N(P') = 2$, $2 = \frac{1}{4}|3^2 - 17 \times 1^2|$, und $\mathrm{ggT}\left(\frac{3-17}{2}, 17\right) = 1$, daher

$$P = A\alpha, \quad \alpha = \frac{3 + \sqrt{17}}{2},$$
$$P' = A\alpha, \quad \alpha' = \frac{3 - \sqrt{17}}{2}.$$

Somit ist die Klassenzahl h gleich 1.

Sei $d = 21$. Aus $21 \equiv 5 \pmod 8$ folgt, dass $A2$ ein Primideal ist, 2 ist unbeteiligt, somit ist $h = 1$.

Sei $d = 6$, dann ist 2 Teiler von $24 = D$, also ist 2 verzweigt, $A2 = P^2$, und $2 = |2^2 - 6 \times 1^2|$, $\mathrm{ggT}(2, 1) = 1$, somit $P = A\alpha$ mit $\alpha = 2 + \sqrt{6}$. Also $h = 1$.

$[\theta] = 3$.

Aus $3 \leq \frac{1}{2}\sqrt{D} < 4$ folgt $36 \leq D < 64$ mit $D \equiv 0$ oder $1 \pmod 4$, daher

$$D \in \{36, 37, 40, 41, 44, 45, 48, 49, 52, 53, 56, 57, 60, 61\}$$

und somit

$$d \in \{37, 10, 41, 11, 53, 14, 57, 15, 61\}.$$

Nun ist $N(\mathcal{N}) = \{1, 2, 3\}$.

Nehme zum Beispiel $d = 10$. Die 2 ist verzweigt, da sie $40 = D$ teilt, und $A2 = R^2$. Da $\left(\frac{10}{3}\right) = \left(\frac{1}{3}\right) = 1$, ist 3 zerfallen, $A3 = P \cdot P'$. Die Ideale R, P, P' sind primitiv.

2 hat keine primitive Darstellung: Wenn $2 = |u^2 - 10v^2|$, dann $u^2 = 10v^2 \pm 2 \equiv \pm 2 \pmod{10}$, was unmöglich ist.

3 hat keine primitive Darstellung: Wenn $3 = |u^2 - 10v^2|$, dann $u^2 = 10v^2 \pm 3 \equiv \pm 3 \pmod{10}$, was unmöglich ist.

Somit sind R, P, P' keine Hauptideale. Die Ideale RP, RP' sind primitiv. Zudem gilt

$$\begin{aligned} -2 \times 3 = -6 = 2^2 - 10 \times 1^2, \quad & \operatorname{ggT}(2,1) = 1, \\ 2 \times 3 = N(RP) = N(RP'), & \end{aligned}$$

daher sind RP, RP' Hauptideale. Schließlich folgt $h' = 2$.

Sei $d < 0$, also $\theta = \frac{2}{\pi}\sqrt{-D}$.

$[\theta] = 1$.

Aus $1 \le \frac{2}{\pi}\sqrt{-D} < 2$ folgt $\frac{\pi^2}{4} \le |D| < \pi^2$ und damit $|D| \equiv 0$ oder $3 \pmod 4$, daher $|D| \in \{3, 4, 7, 8\}$ und folglich $d \in \{-3, -1, -7, -2\}$. Nun ist $N(\mathcal{N}) = 1$, somit besteht $\mathcal{N}$ nur aus dem Einheitsideal, also $h = 1$.

$[\theta] = 2$.

Aus $2 \le \frac{2}{\pi}\sqrt{-D} < 3$ folgt $\pi^2 \le |D| < \frac{9}{4}\pi^2$ und $|D| \equiv 0$ oder $3 \pmod 4$, daher $|D| \in \{11, 12, 15, 16, 19, 20\}$ und so $d \in \{-11, -15, -19, -5\}$.

Nehme zum Beispiel $d = -11$. Wegen $-11 \equiv 5 \pmod 8$ ist 2 unbeteiligt, und somit $h = 1$.

Sei $d = -5$. Da $D = -20$ von 2 geteilt wird, ist 2 verzweigt, $A2 = P^2$.

2 hat keine primitive Darstellung: Wenn $2 = |u^2 + 5v^2|$, dann $u^2 = -5v^2 + 2 \equiv 2 \pmod 5$, was unmöglich ist. Zudem gilt $-5 \equiv 3 \pmod 4$. Also ist P kein Hauptideal und $h = 2$.

Sei $d = -15$. Aus $-15 \equiv 1 \pmod 8$ folgt $A2 = P \cdot P'$.

2 hat keine primitive Darstellung: Wenn

$$2 = \frac{|u^2 + 15v^2|}{4}, \quad \text{mit} \quad \operatorname{ggT}\left(\frac{u - v}{2}, v\right) = 1,$$

dann $u^2 + 15v^2 = 8$, also $u^2 \equiv 3 \pmod 5$, was unmöglich ist. Auch ist $-15 \equiv 1 \pmod 4$. Da P, P' keine Hauptideale sind, folgt $h = 2$.

Sei $d = -19$. Wegen $-19 \equiv 5 \pmod 8$ ist 2 unbeteiligt, daher $h = 1$.

$[\theta] = 3$.

Aus $3 \leq \frac{2}{\pi}\sqrt{-D} < 4$ folgt $\frac{9\pi^2}{4} \leq |D| < 4\pi^2$ und $|D| \equiv 0$ oder $3 \pmod 4$, somit

$$|D| \in \{23, 24, 27, 28, 31, 32, 35, 36, 39\},$$

und daher

$$d \in \{-23, -6, -31, -35, -39\}.$$

Nehme $d = -31$. Aus $-31 \equiv 1 \pmod 8$ folgt $A2 = P \cdot P'$. Da $-31 \equiv 1 \pmod 8$ ist $A2 = P \cdot P'$. Und aus $\left(\frac{-31}{3}\right) = \left(\frac{-1}{3}\right)\left(\frac{1}{3}\right) = -1$ ergibt sich, dass $A3$ ein Primideal ist.

2 hat keine primitive Darstellung: Wenn

$$2 = \frac{|u^2 + 31v^2|}{4}, \quad \text{mit} \quad \text{ggT}\left(u - v\frac{u-v}{2}, v\right) = 1,$$

dann $8 = u^2 + 31v^2$, was unmöglich ist. Wegen $-31 \equiv 1 \pmod 4$ sind P, P' keine Hauptideale. Wenn P, P' äquivalent sind, dann $P = P'.A\alpha$, also $P^2 = P \cdot P' \cdot A\alpha = A(2\alpha)$, somit $4 = N(P^2) = 4N(A\alpha)$ und daher $N(A\alpha) = 1$, also $A\alpha = A$ und $P = P'$, was nicht sein kann. Daraus folgt $h = 3$.

Diese Beispiele sollen genügen um zu erläutern, wie man die Klassenzahl zumindest für Diskriminanten mit kleinem Absolutwert berechnen kann. Es gibt kompliziertere Methoden, mithilfe derer man die Klassenzahl sogar für große Werte von $|d|$ effizient berechnen kann. Diese Algorithmen sind in den Büchern von Buell (1989) und Cohen (1993) beschrieben, in denen natürlich auch reell-quadratische Zahlkörper behandelt werden.

B Bestimmung aller quadratischen Zahlkörper mit Klassenzahl 1

Sei $d > 0$.

Man vermutet, dass es unendlich viele $d > 0$ derart gibt, dass $\mathbb{Q}(\sqrt{d})$ die Klassenzahl 1 hat. Es wird wohl schwierig nachzuweisen sein, aber man glaubt, dass die Vermutung stimmt.

Zum Beispiel gibt es 142 Körper $\mathbb{Q}(\sqrt{d})$ mit $2 \leq d < 500$, die die Klassenzahl 1 haben.

Sei $d < 0$.

Wir hatten gesehen, dass wenn $\mathcal{N}$ nur aus dem Einheitsideal besteht, dann ist $h = 1$. Umgekehrt gilt:

Wenn $d < 0$ und $h = 1$, dann $\mathcal{N} = \{A\}$.

Beweis. Für $|D| \leq 7$ stimmt die Behauptung. Sei $|D| > 7$, $I \in \mathcal{N}$ und $I \neq A$, so dass es ein Primideal P gibt, das I teilt. Dann ist $N(P) = p$ oder p^2, wobei p eine Primzahl ist. Wenn $N(P) = p^2$, dann ist p unbeteiligt und $Ap = P$ teilt I, also wäre I nicht primitiv, was ein Widerspruch ist. Wenn $N(P) = p$, dann $p \leq N(I) \leq [\theta] \leq \frac{2}{\pi}\sqrt{|D|}$, da P Teiler von I ist. Falls p eine primitive Darstellung hat:

Wenn $d \equiv 2$ oder $3 \pmod 4$, dann $d = \frac{D}{4}$, also $p = u^2 - dv^2$, somit $v \neq 0$ und daher $\frac{2}{\pi}\sqrt{|D|} \geq p \geq |d| = \frac{|D|}{4}$, also $7 \geq \frac{64}{\pi^2} \geq |D|$, was nicht sein kann.

Wenn $d \equiv 1 \pmod 4$, dann $d = D$, also $p = \frac{u^2 - dv^2}{4}$, damit $v \neq 0$ und so $\frac{2}{\pi}\sqrt{|D|} \geq p \geq \frac{|d|}{4} = \frac{|D|}{4}$, und wieder $7 \geq D$, was nicht sein kann.

Folglich ist P kein Hauptideal und $h \neq 1$, was der Annahme widerspricht. □

Gauss entwickelte eine Geschlechtertheorie und bewies:

Wenn $d < 0$ und wenn t die Anzahl der verschiedenen Primfaktoren von D ist, dann ist 2^{t-1} Teiler der Klassenzahl von $\mathbb{Q}(\sqrt{d})$.

Es folgt, dass wenn $h = 1$, dann $D = -4$, -8 oder $-p$, wobei p eine Primzahl ist, $p \equiv 3 \pmod 4$, damit $d = -1$, -2 oder $-p$.

Aus dieser Betrachtung ergibt sich:

Wenn $D = -3, -4, -7, -8$, dann $h = 1$.

Wenn $D \neq -3, -4, -7, -8$ und $D = -p$, $p \equiv 3 \pmod 4$, dann $h = 1$ genau dann, wenn $\mathcal{N} = \{A\}$, und dies ist gleichbedeutend mit den folgenden Bedingungen:

2 ist unbeteiligt in $\mathbb{Q}(\sqrt{-p})$ und wenn q irgendeine ungerade Primzahl ist mit $q \leq [\theta]$, dann $\left(\frac{-p}{q}\right) = -1$, d.h. q ist unbeteiligt in $\mathbb{Q}(\sqrt{-p})$.

Dieses Kriterium wird bei der Bestimmung aller $D < 0$, $|D| \leq 200$ verwendet, für die $h = 1$.

$[\theta] = 1$.

Dies ergibt die Diskriminanten $D = -3, -4, -7, -8$.

$[\theta] = 2$.

Nun ist $-20 \leq D \leq -11$ mit $D = p$, $p \equiv 3 \pmod 4$, also $D = -11$ oder -19.

Wegen $-11 \equiv 5 \pmod 8$ ist 2 unbeteiligt, also ist $h = 1$ wenn $D = -11$.

Genauso folgt, dass wegen $-19 \equiv 5 \pmod 8$ die 2 unbeteiligt ist, also ist $h = 1$ wenn $D = -19$.

$[\theta] = 3$.

Nun ist $-39 \leq D \leq -23$ mit $D = -p$, $p \equiv 3 \pmod 4$, also $D = -23$ oder -31. Aber $-23 \not\equiv 5 \pmod 8$, $-31 \not\equiv 5 \pmod 8$, also sind die Klassenzahlen von $\mathbb{Q}(\sqrt{-23})$ und von $\mathbb{Q}(\sqrt{-31})$ nicht 1.

$[\theta] = 4$.

Nun ist $-59 \leq D \leq -40$, $D = -p$, $p \equiv 3 \pmod 4$, also $D = -43$, -47, -59. Wegen $-43 \equiv 5 \pmod 8$ und $\left(\frac{-43}{3}\right) = -1$ hat $\mathbb{Q}(\sqrt{-43})$ die Klassenzahl 1. Aus $-47 \not\equiv 5 \pmod 8$ und $\left(\frac{-59}{3}\right) = 1$ folgt, dass 3 nicht unbeteiligt ist. Also sind die Klassenzahlen von $\mathbb{Q}(\sqrt{-47})$ und von $\mathbb{Q}(\sqrt{-59})$ nicht gleich 1.

Dieselbe Berechnung führt zu:

$[\theta] = 5$: $D = -67$ mit Klassenzahl 1.
$[\theta] = 6$: keine Diskriminante.
$[\theta] = 7$: keine Diskriminante.
$[\theta] = 8$: $D = -163$ mit Klassenzahl 1.

Diesen Prozess könnte man über 200 hinaus fortsetzen, dies führt aber zu keiner weiteren Diskriminante für die die Klassenzahl 1 wird. Natürlich kann man daraus nicht entscheiden, ob es irgendeine weitere solche Diskriminante gibt oder ob es nur endlich viele imaginärquadratische Zahlkörper mit Klassenzahl 1 gibt.

In einem klassischen Artikel zeigten Heilbronn und Linfoot im Jahr 1934 mit analytischen Methoden, dass es neben den obigen Beispielen höchstens einen weiteren Wert von $d < 0$ derart gibt, dass $\mathbb{Q}(\sqrt{d})$ die Klassenzahl 1 hat. Lehmer zeigte, dass wenn es eine solche Diskriminante d überhaupt gibt, dann muss $|d| > 5 \times 10^9$ gelten. Im Jahr 1952 bewies Heegner, dass es kein weiteres d geben kann, allerdings war sein Beweis unklar, wenn nicht sogar lückenhaft. Baker kam im Jahr 1966 mit seiner Methode absoluter unterer Schranken

von Linearformen dreier Logarithmen zum selben Schluss; dies ist auch in seinem Artikel von 1971 erwähnt. Etwa zur gleichen Zeit bewies Stark ohne Kenntnis von Heegners Arbeit, aber mit ähnlichen Ideen bezüglich elliptischer modularer Funktionen, dass kein weiterer Wert für d möglich ist. So waren also alle imaginär-quadratischen Zahlkörper mit Klassenzahl 1 bestimmt. Es war in gewisser Hinsicht ernüchternd, als es Deuring 1968 gelang, Heegners Beweis klarzustellen. Die dabei verwendeten technischen Details übersteigen den Rahmen dieses Abschnitts bei Weitem.

An dieser Stelle sollte gesagt werden, dass auch Gauss' Vermutung im positiven Sinne gelöst worden war. Dank der Arbeit von Hecke, Deuring, Mordell und Heilbronn konnte festgestellt werden, dass wenn $d < 0$ und $|d|$ gegen Unendlich geht, dies auch für die Klassenzahl von $\mathbb{Q}(\sqrt{d})$ gilt. Damit gibt es für jede ganze Zahl $h \geq 1$ nur endlich viele Körper $\mathbb{Q}(\sqrt{d})$ mit $d < 0$, die die Klassenzahl h haben.

Die Bestimmung aller imaginär-quadratischen Zahlkörper mit Klassenzahl 2 wurde von Baker, Stark und Weinberger erreicht.

Eine explizite Abschätzung der Anzahl der imaginär-quadratischen Zahlkörper mit einer gegebenen Klassenzahl konnte durch die Bemühungen von Siegel, Goldfeld und Gross und Zagier erzielt werden. Zu diesem Punkt empfehle ich die Lektüre des Artikels von Goldfeld (1985).

7 Der Hauptsatz

Satz. *Sei q eine Primzahl und $f_q(X) = X^2 + X + q$. Die folgenden Bedingungen sind äquivalent:*

(1) $q = 2, 3, 5, 11, 17, 41$.

(2) $f_q(n)$ ist eine Primzahl für $n = 0, 1, \ldots, q-2$.

(3) $\mathbb{Q}(\sqrt{1-4q})$ hat die Klassenzahl 1.

Beweis. Die Folgerung (1) $\Rightarrow$ (2) ist eine einfache Verifikation.

Die Äquivalenz der Aussagen (2) und (3) wurde erstmals von Rabinowitsch im Jahr 1912 gezeigt. Im Jahr 1936 bewies Lehmer ein weiteres Mal (2) $\Rightarrow$ (3). (3) $\Rightarrow$ (2) wurde erneut von Szekeres (1974) und von Ayoub und Chowla (1981) nachgewiesen, letzterer gab den einfachsten Beweis an. Der Beweis von (3) $\Rightarrow$ (1) folgt aus der vollständigen Bestimmung aller imaginär-quadratischen Zahlkörper mit Klassenzahl 1. Da dieser Beweis tiefliegende Resultate erfordert, werde ich auch den Beweis von (3) $\Rightarrow$ (2) angeben.

(2) $\Rightarrow$ (3) Sei $d = 1 - 4q < 0$, also $d \equiv 1 \pmod 4$. Wenn $q = 2$ oder 3, dann $d = -7$ oder -11 und $\mathbb{Q}(\sqrt{d})$ hat Klassenzahl 1, wie bereits gesehen. Nehme nun an, dass $q \geq 5$. Es genügt zu zeigen, dass jede Primzahl $p \leq \frac{2}{\pi}\sqrt{|d|}$ unbeteiligt in $\mathbb{Q}(\sqrt{d})$ ist.

Sei zunächst $p = 2$; aus $q = 2t-1$ folgt $d = 1-4q = 1-4(2t-1) = 5 \pmod 8$, also ist 2 unbeteiligt in $\mathbb{Q}(\sqrt{d})$.

Sei nun $p \neq 2$, $p \leq \frac{2}{\pi}\sqrt{|d|} < \sqrt{|d|}$ und angenommen, p sei nicht unbeteiligt. Dann $\left(\frac{d}{p}\right) \neq -1$ und es gibt wie erwähnt $b \in \mathbb{Z}$, $0 \leq b \leq p-1$ derart, dass p Teiler von $N(b+\omega)$ ist, wobei $\omega = \frac{1+\sqrt{d}}{2}$, d.h., p teilt

$$\begin{aligned}(b+\omega)(b+\omega') &= b^2 + b(\omega+\omega') + \omega\omega' \\ &= b^2 + b + \frac{1-d}{4} \\ &= b^2 + b + q = f_q(b).\end{aligned}$$

Man beachte auch, dass $b \neq p-1$, ansonsten wäre wie gezeigt p Teiler von $1-d = 4q$, damit $p = q < \sqrt{|d|} = \sqrt{|1-4q|}$, also $q^2 < 4q-1$ und daher $q = 2$ oder 3 im Widerspruch zur Annahme.

Nach Annahme ist $f_q(b)$ also eine Primzahl, somit $\sqrt{4q-1} > p = f_q(b) \geq f_q(0) = q$ und wiederum $q = 2$ oder 3, ein weiterer Widerspruch.

Dies zeigt, dass jede Primzahl p kleiner als $\frac{2}{\pi}\sqrt{|d|}$ unbeteiligt ist, daher $h = 1$.

(3) $\Rightarrow$ (1) Wenn $\mathbb{Q}(\sqrt{1-4q})$ die Klassenzahl 1 hat, dann $d = 1 - 4q = -7, -11, -19, -43, -67, -163$, somit $q = 2, 3, 5, 11, 17, 41$. □

Wie ich bereits andeutete, ist der Beweis damit vollständig, aber es bleibt interessant, sich den Beweis von (3) $\Rightarrow$ (2) anzusehen.

Beweis. Angenommen $d = 1 - 4q$ und die Klassenzahl von $\mathbb{Q}(\sqrt{-d})$ ist 1. Dann ist entweder $d = -1, -2, -3, -7$ oder $d < -7$, also $d = -p$ mit $p \equiv 3 \pmod 4$ und $q > 2$.

Wie bereits erwähnt ist 2 unbeteiligt in $\mathbb{Q}(\sqrt{-p})$, also $p \equiv 3 \pmod 8$. Als Nächstes zeige ich, dass gilt $\left(\frac{l}{p}\right) = -1$, wenn l irgendeine ungerade Primzahl mit $l < q$ ist. Tatsächlich zerfällt l in $\mathbb{Q}(\sqrt{-p})$, wenn $\left(\frac{l}{p}\right) = 1$. Aber $h = 1$, also gibt es eine algebraische ganze Zahl $\alpha = \frac{a+b\sqrt{-p}}{2}$ derart, dass $Al = A\alpha \cdot A\alpha'$.

Dann

$$l^2 = N(Al) = N(A\alpha) \cdot N(A\alpha') = N(A\alpha)^2 = N(\alpha)^2,$$

also $l = N(\alpha) = \frac{a^2+b^2p}{4}$. Daher $p + 1 = 4q > 4l = a^2 + b^2p$, somit $1 > a^2 + (b^2 - 1)p$ und notwendigerweise $a^2 = 0$, $b^2 = 1$ also $4l = p$, was nicht sein kann.

Nehme nun an, dass es ein m mit $0 \leq m \leq q - 2$ derart gibt, dass $f_q(m) = m^2 + m + q$ nicht prim ist. Dann gibt es eine Primzahl l mit $l^2 \leq m^2 + m + q$ und $m^2 + m + q = al$, wobei $a \geq 1$. Da $m^2 + m + q$ ungerade ist folgt $l \neq 2$. Zudem

$$4l^2 \leq (2m + 1)^2 + p < \left(\frac{p-1}{2}\right)^2 + p = \left(\frac{p+1}{2}\right)^2,$$

und so $l < (p+1)/4 = q$. Wie gezeigt worden war ist $\left(\frac{l}{p}\right) = -1$. Jedoch

$$4al = (2m + 1)^2 + 4q - 1 = (2m + 1)^2 + p,$$

daher ist $-p$ ein Quadrat modulo l, also folgt nach dem Gaußschen Reziprozitätsgesetz

$$1 = \left(\frac{-p}{l}\right) = \left(\frac{-1}{l}\right)\left(\frac{p}{l}\right) = (-1)^{\frac{l-1}{2}}\left(\frac{l}{p}\right)(-1)^{\frac{l-1}{2}\times\frac{p-1}{2}} = \left(\frac{l}{p}\right),$$

und dies kann nicht sein. □

Literaturverzeichnis

1912 G. Rabinowitsch. Eindeutigkeit der Zerlegung in Primzahlfaktoren in quadratischen Zahlkörper. 418–421.

1936 D. H. Lehmer. On the function $x^2 + x + A$. *Sphinx*, 6:212–214.

1958 A. Schinzel und W. Sierpiński. Sur certaines hypothèses concernant les nombres premiers. Remarques. *Acta Arith.*, 4:185–208 und 5:259 (1959).

1961 A. Schinzel. Remarks on the paper "Sur certaines hypothèses concernant les nombres premiers". *Acta Arith.*, 7:1–8.

1962 H. Cohn. *Advanced Number Theory.* Dover, New York.

1966 Z. I. Borevich und I. R. Shafarevich. *Number Theory.* Academic Press, New York.

1972 P. Ribenboim. *Algebraic Numbers.* Wiley-Interscience, New York.

1974 G. Szekeres. On the number of divisors of $x^2 + x + A$. *J. Nb. Th.*, 6:434–442.

1981 R. G. Ayoub und S. Chowla. On Euler's polynomial. *J. Nb. Th.*, 13:443–445.

1985 D. M. Goldfeld. Gauss's class number problem for imaginary quadratic fields. *Bull. Amer. Math. Soc.*, 13:23–37.

1989 D. A. Buell. *Binary Quadratic Forms.* Springer-Verlag, New York.

1993 H. Cohen. *A Course in Computational Algebraic Number Theory.* Springer-Verlag, Berlin.

1995 P. A. Pritchard, A. Moran und A. Thyssen. Twenty-two primes in arithmetic progression. *Math. of Comp.*, 64:1337–1339.

1996 P. Ribenboim. *The New Book of Prime Number Records.* Springer-Verlag, New York.

2008 B. Green und T. Tao. The primes contain arbitrarily long arithmetic progressions. *Ann. Math.*, 167:481–547.

6

Gauß und das Klassenzahlproblem

1 Einführung

Die Theorie der binären quadratischen Formen gehört zu den großen Errungenschaften von Gauss in der Zahlentheorie.

Einige der von Gauss formulierten Vermutungen sind noch heute Gegenstand umfangreicher Forschung. Dieser Text[1] enthält auch eine kurze Beschreibung der wichtisten Ergebnisse der jüngeren Vergangenheit bezüglich der Vermutungen von Gauss über die Klassenzahl.

2 Höhepunkte im Leben von Gauß

Carl Friedrich Gauß wurde im Jahre 1777 in Braunschweig geboren und starb 1855 in Göttingen.

Er war ein frühreifes Kind, wie die folgende, berühmte Anekdote belegt.

Als im Alter von acht Jahren die Schüler seiner Klasse den Lehrer geärgert hatten, bekamen sie die folgende Aufgabe: Addiert alle Zahlen von 1 bis 100:

$$1 + 2 + 3 + \cdots + 100.$$

Der Lehrer dachte, dass er nun eine lange Ruhepause hätte. Darin hatte er sich allerdings getäuscht, denn der junge Gauss hatte die Antwort bereits parat: 5050. Überrascht fragte der Lehrer, wie er denn so schnell die Antwort gefunden hatte. Woraufhin das Kind erklärte:

[1] Dies ist eine erweiterte Version einer Vorlesung im Rahmen des Ersten Gauß-Symposiums in Guarujá, Brasilien im Juli 1989.

„Ich stellte mir die Zahlen von 1 bis 100 in einer Zeile aufgeschrieben vor und dann noch einmal die gleichen Zahlen in einer zweiten Zeile, allerdings rückwärts notiert:

$$\begin{array}{cccccccc} 1 & 2 & 3 & \dots & 98 & 99 & 100 \\ 100 & 99 & 98 & \dots & 3 & 2 & 1 \end{array}$$

Mir fiel auf, dass die zwei Zahlen sich in jeder Spalte auf 101 summierten. Es gibt 100 Spalten, was insgesamt 10100 ergibt, wobei ich aber jede Zahl zweimal gezählt habe, d.h. die fragliche Summe ist gleich der Hälfte von 10100, d.h. 5050."

Ich kann nicht beschwören, dass sich die Geschichte genauso zugetragen hat wie ich sie gerade erzählte, aber wie die Italiener sagen: „*se non è vero, è ben trovato*".

Der junge Gauss gab noch viele weitere Beispiele seiner überragenden Intelligenz. Er war in allen Disziplinen exzellent, insbesondere in klassischen Sprachen und Mathematik.

Im Alter von elf Jahren kam Gauss auf das Gymnasium. Seine Talente wurden bereits im Jahr 1792 erkannt, als er im Alter von 15 Jahren ein Stipendium des Herzogs von Braunschweig erhielt, das es ihm erlaubte, seine Studien ohne finanzielle Sorgen fortzusetzen.

Gauss rechnete mit großer Begeisterung. Zum Beispiel berechnete er sowohl Primzahltabellen (als er noch sehr jung war) als auch quadratische Reste, Primitivwurzeln modulo Primzahlen, Inverse von Primzahlen auf viele Stellen genau usw. ...

Die Ergebnisse seiner Berechnungen dienten als Grundlage für Vermutungen und Aussagen, die er später während seiner ganzen Karriere oftmals mit großem Erfolg zu beweisen versuchte.

Gauss schrieb sich an der Universität von Göttingen ein, wo er von einer umfangreichen Bibliothek profitieren konnte. Dort studierte er Bernoullis *Ars Conjectandi*, Newtons *Principia* sowie die Werke von Euler, Lagrange und Legendre.

Gauss mathematisches Interesse war weitläufig, er interessierte sich zudem für Astronomie, Erdvermessung und Physik.

Die folgende kurze Tabelle einiger früher mathematischer Entdeckungen von Gauss deutet an, welche bemerkenswerten Leistungen er vollbracht hatte und sein ganzes Leben hindurch vollbringen würde.

Alter	Jahr	
18	1795	Reihenentwicklung für das arithmetisch-geometrische Mittel. Die Methode kleinster Quadrate. Vermutung: Der Primzahlsatz. Nicht-euklidische Geometrie.
19	1796	Quadratisches Reziprozitätsgesetz. Bestimmung der mit Zirkel und Lineal konstruierbaren regulären Polygone (darunter auch das 17-Eck).
20	1797	Der Fundamentalsatz der Algebra.
22	1799	Zusammenhang zwischen arithmetisch-geometrischem Mittel und der Länge der Lemniskate.
23	1800	Doppelt-periodische Funktionen.
24	1801	Veröffentlichung der *Disquisitiones Arithmeticae*

In seinem Werk *Disquisitiones Arithmeticae* (Gauss (1801)), das einen in viele Sprachen übersetzten Meilenstein der Zahlentheorie darstellt, präsentiert Gauss in geordneter Weise seine Entdeckungen der vorangegangenen Jahre, die die Werke seiner Vorgänger Fermat, Euler, Lagrange und Legendre klären und vervollständigen.

Das Buch enthält: Die Theorie der Kongruenzen (mit der sehr erfreulichen Einführung der Bezeichnungsweise $a \equiv b \pmod{n}$); unbestimmte lineare Gleichungen; binäre quadratische Formen; unbestimmte quadratische Gleichungen; Kreisteilung; und die Konstruktion regulärer Polygone mit Lineal und Zirkel.

Als Gauss noch jung war, wendete er seine Aufmerksamkeit anderen Bereichen der Mathematik sowie der Astronomie und der Physik zu. Da es in diesem Kapitel aber um binäre quadratische Formen geht, werde ich davon absehen, auf Gauss' Beiträge zu den anderen Themen einzugehen. Eine sehr aufschlussreiche Studie über Gauss findet sich in Kaufmann-Bühler (1981), wo auch andere Aspekte seiner Arbeit betrachtet werden. Es lohnt sich auch, einmal einen Blick in Gauss' Tagebuch (siehe Gauß' Werke (1870)) und den Kommentar von Gray (1984) zu werfen.

3 Kurzer geschichtlicher Hintergrund

Eine der berühmtesten Entdeckungen von Fermat bezieht sich auf die Darstellung der Primzahlen als Summe von Quadraten.

Sei p eine Primzahl. Dann ist $p = x^2 + y^2$ (mit ganzen Zahlen x, y) genau dann, wenn $p = 2$ oder $p \equiv 1 \pmod{4}$. In diesem Fall ist die Darstellung von p eindeutig (mit $0 < x < y$ wenn $p \neq 2$). Mithilfe des

Legendre-Symbols lässt sich die Bedingung wie folgt darstellen: $p = 2$ oder $(-1/p) = +1$.

Auf die gleiche Weise ist $p = x^2 + 2y^2$ (mit ganzen Zahlen x, y) genau dann, wenn $p = 2$ oder $p \equiv 1$ oder $3 \pmod 8$; äquivalent, $p = 2$ oder $(-2/p) = +1$. Wieder ist die Darstellung eindeutig (mit $0 < x, y$).

Ebenso gilt $p = x^2 + 3y^2$ (mit ganzen Zahlen x, y) genau dann, wenn $p = 3$ oder $p \equiv 1 \pmod 3$, oder äquivalent, $p = 3$ oder $(-3/p) = +1$. Auch hier ist die Darstellung eindeutig (mit $0 < x, y$).

Gleichwohl war Euler bekannt, dass die Bedingung $p = 5$ oder $p \equiv 1, 3, 7$ oder $9 \pmod{20}$ oder äquivalent $p = 5$ oder $(-5/p) = +1$ ausdrückt, dass die Primzahl p die Form $p = x^2 + 5y^2$ oder $p = 2x^2 + 2xy + 3y^2$ hat (mit ganzen Zahlen x, y). Genau genommen vermutete Euler, dass $p = x^2 + 5y^2$ genau dann gilt, wenn $p = 5$ oder $p \equiv 1$ oder $9 \pmod{20}$. Der Beweis der Vermutung ist mit der Geschlechtertheorie verbunden.

Lagrange und Legendre untersuchten das allgemeinere Problem: Gegeben seien ganze Zahlen a, b, c. Wie lässt sich die ganze Zahl m in der Form

$$m = ax^2 + bxy + cy^2$$

darstellen, wobei x, y ganze Zahlen sind?

In seinem Werk *Disquisitiones Arithmeticae* legte Gauss in systematischer und detaillierter Weise die Resultate von Euler, Legendre und Lagrange dar und entwickelte die Theorie weit über das hinaus, was seine Vorgänger geleistet hatten.

Die geschichtliche Entwicklung der faszinierenden Theorie der binären quadratischen Formen ist in den Büchern von Weil (1984) und Edwards (1977) ausführlich beschrieben.

4 Binäre quadratische Formen

Eine *binäre quadratische Form* (oder einfach, eine Form) ist ein homogenes Polynom vom Grad 2 in zwei Unbekannten

$$Q = aX^2 + bXY + cY^2,$$

mit Koeffizienten a, b, $c \in \mathbb{Z}$.

Eine einfachere Bezeichnungsweise ist $Q = \langle a, b, c \rangle$.

Gauss hatte gute Gründe dafür, innerhalb seiner Theorie nur solche Formen zu betrachten, bei denen b gerade ist; traditionellerweise

ist diese Einschränkung auch heute noch in einigen Darstellungen der Theorie zu finden. Die Ergebnisse des von EISENSTEIN betrachteten allgemeineren Falls kann auf einfache Weise mit denen von GAUSS für die Formen $\langle a, b, c\rangle$ mit geradem b in Zusammenhang gebracht werden.

Die Form $Q = \langle a, b, c\rangle$ heißt *einfach*, wenn $\mathrm{ggT}(a, b, c) = 1$.

Wenn $\langle a, b, c\rangle$ irgendeine Form ist und $d = \mathrm{ggT}(a, b, c)$, dann ist die Form $\langle \frac{a}{d}, \frac{b}{d}, \frac{c}{d}\rangle$ einfach. Dies gestattet es uns, von beliebigen Formen zu einfachen zu gelangen.

Die *Diskriminante* von $Q = \langle a, b, c\rangle$ ist $D = D(Q) = b^2 - 4ac$. Die Diskriminante wird auch mit $\mathrm{Diskr}(Q)$ bezeichnet.

Eine ganze Zahl D ist Diskriminante irgendeiner Form genau dann, wenn $D \equiv 0$ oder $1 \pmod 4$. Tatsächlich erfüllt eine Diskriminante eine der obigen Kongruenzen. Umgekehrt sei

$$P = \begin{cases} \langle 1, 0, \frac{-D}{4}\rangle, \text{ wenn } D \equiv 0 \pmod 4, \\ \langle 1, 1, \frac{-D+1}{4}\rangle, \text{ wenn } D \equiv 1 \pmod 4. \end{cases}$$

Dann hat P die Diskriminante D und heißt die *Hauptform* der Diskriminante D.

Wenn $D = D(Q)$ ein Quadrat ist, dann

$$aQ = \left[aX - \frac{-b + \sqrt{D}}{2}Y\right]\left[aX - \frac{-b - \sqrt{D}}{2}Y\right],$$

also ist es das Produkt von Linearfaktoren mit ganzzahligen Koeffizienten. Dieser Fall ist entartet und daher wird von nun an vorausgesetzt, dass die Diskriminante kein Quadrat ist. Somit $ac \neq 0$.

Eine ganze Zahl m ist ein *Wert* von Q oder ist durch Q *dargestellt*, wenn es ganze Zahlen x, y derart gibt, dass $m = Q(x, y) = ax^2 + bxy + cy^2$; jede solche Relation nennt man *Darstellung* von m durch Q. Wenn darüberhinaus $\mathrm{ggT}(x, y) = 1$, dann spricht man von *einfachen Werten* und *einfachen Darstellungen*.

Die Menge der Werte von Q ist

$$\{\text{Werte von } Q\} = \{mt^2 \mid m \text{ ist ein einfacher Wert von } Q \text{ und } t \in \mathbb{Z}\}.$$

Die Formen sind wie folgt klassifiziert:

$$\begin{aligned} &\textit{definite Formen}, \text{ wenn } D < 0; \\ &\textit{indefinite Formen}, \text{ wenn } D > 0. \end{aligned}$$

Wenn die Form Q indefinit ist, dann nimmt sie offensichtlich sowohl positive als auch negative Werte an.

Es ist offensichtlich, dass wenn $Q = \langle a, b, c\rangle$ und $D = b^2 - 4ac < 0$ gilt, die folgenden Bedingungen äquivalent sind:

1. $a > 0$;
2. $c > 0$;
3. $Q(x, y) > 0$ für alle ganzen Zahlen x, y ungleich 0.

In diesem Fall nennt man Q *positiv definit*, wenn $a > 0$ und *negativ definit*, wenn $a < 0$.

Da positive definite Formen $\langle a, b, c\rangle$ mit negativen definiten Formen $\langle -a, -b, -c\rangle$ korrespondieren genügt es, positive definite Formen zu untersuchen. Somit werden alle Formen mit negativer Diskriminante wenn nicht abweichend angegeben zu positiven definiten Formen.

Die folgende Bezeichnung wird an späterer Stelle nützlich sein.

Es ist passend, $\bar{Q} = \langle a, -b, c\rangle$ als *konjugierte* Form von $Q = \langle a, b, c\rangle$ zu bezeichnen. Natürliche haben Q und $\bar{Q}$ dieselbe Diskriminante und Q ist positiv definit genau dann, wenn dies auch für $\bar{Q}$ gilt.

Die Nullstellen der Form $Q = \langle a, b, c\rangle$ sind

$$\omega = \frac{-b + \sqrt{D}}{2a} \quad \text{(die } \textit{erste Nullstelle}\text{) und}$$
$$\eta = \frac{-b - \sqrt{D}}{2a} \quad \text{(die } \textit{zweite Nullstelle}\text{).}$$

Wir werden die folgende Bezeichnung verwenden.

Für irgendeine Diskriminante D bezeichne $\mathcal{Q}_D$ die Menge aller Formen, wenn $D > 0$ (bzw. alle positiven definiten Formen, wenn $D < 0$); in gleicher Weise sei $\mathrm{Prim}(\mathcal{Q}_D)$ die Teilmenge von $\mathcal{Q}_D$, die aus einfachen Formen besteht.

Sei

$$\mathcal{Q} = \bigcup\{\mathcal{Q}_D \mid D \equiv 0 \text{ oder } 1 \pmod 4\} \quad \text{und}$$
$$\mathrm{Prim}(\mathcal{Q}) = \bigcup\{\mathrm{Prim}(\mathcal{Q}_D) \mid D \equiv 0 \text{ oder } 1 \pmod 4\}.$$

Sei $D \equiv 0$ oder $1 \pmod 4$. Man nennt D eine Fundamentaldiskriminante, wenn jede Form mit Diskriminante D einfach ist.

Es ist leicht einzusehen, dass dies genau dann passiert, wenn gilt

1. immer dann, wenn $D \equiv 1 \pmod 4$, ist D quadratfrei,
2. immer dann, wenn $D \equiv 0 \pmod 4$, ist $D = 4D'$ mit D' quadratfrei und $D' \equiv 2$ oder $3 \pmod 4$.

Damit haben die Fundamentaldiskriminanten die Form

$$D = \pm q_1 q_2 \cdots q_r \quad \text{oder} \quad D = \pm 4 q_2 \cdots q_r \quad \text{oder} \quad D = \pm 8 q_2 \cdots q_r,$$

wobei $q_1, q_2, \ldots, q_r$ verschiedene ungerade Primzahlen sind.

Andererseits ist nicht jede Diskriminante D fundamental, wenn sie eine der beiden obigen Formen hat, betrachte z.B. $D = -4 \times 3$.

Jede Diskriminante D ist eindeutig darstellbar durch $D_0 f^2$, wobei D_0 eine Fundamentaldiskriminante ist und $f \geq 1$. D_0 nennt man *Fundamentaldiskriminante zugehörig zur Diskriminante* D.

Die folgende Bijektion lässt sich leicht gewinnen:

$$\mathcal{Q}_D \longrightarrow \bigcup_{e|f} \mathrm{Prim}(\mathcal{Q}_{D/e^2}).$$

Insbesondere gilt $\mathcal{Q}_D = \mathrm{Prim}(\mathcal{Q}_D)$, wenn $D = D_0$ eine Fundamentaldiskriminante ist.

5 Die Hauptprobleme

Die Theorie der binären quadratischen Formen beschäftigt sich mit den folgenden Problemen:

Problem 1. Gegeben seien ganze Zahlen m und D, $D \equiv 0$ oder $1 \pmod 4$. Gibt es eine einfache Darstellung von m durch eine Form mit Diskriminante D?

Im positiven Falle betrachte die nächsten Probleme:

Problem 2. Zähle alle diejenigen Formen $Q \in \mathcal{Q}_D$ auf, für die m eine einfache Darstellung durch Q besitzt.

Problem 3. Bestimme für jedes $Q \in \mathcal{Q}_D$, für das m eine einfache Darstellung durch Q besitzt, alle diese Darstellungen.

Um die Probleme zu lösen ist es erforderlich, die Äquivalenz von Formen zu untersuchen.

6 Äquivalenz von Formen

Es bezeichne $\mathrm{GL}_2(\mathbb{Z})$ die *lineare Gruppe vom Rang 2 über* $\mathbb{Z}$; diese besteht aus allen Matrizen

$$A = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$$

mit α, β, γ, $\delta \in \mathbb{Z}$ und $\alpha\delta - \beta\gamma = \pm 1$.

Sei $\mathrm{SL}_2(\mathbb{Z})$ die Menge all derer Matrizen $A \in \mathrm{GL}_2(\mathbb{Z})$, für die gilt $\alpha\delta - \beta\gamma = 1$. Dies ist eine normale Untergruppe von $\mathrm{GL}_2(\mathbb{Z})$ mit Index 2, man nennt sie die *spezielle lineare Gruppe vom Rang* 2 *über* $\mathbb{Z}$.

Die Gruppe $\mathrm{GL}_2(\mathbb{Z})$ operiert auf der Menge $\mathcal{Q}$ der Formen in folgender Weise. Wenn $A = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \in \mathrm{GL}_2(\mathbb{Z})$, dann sei $T_A : \mathcal{Q} \to \mathcal{Q}$ die wie folgt definierte Abbildung.

Wenn $Q = \langle a, b, c\rangle$, $Q' = \langle a', b', c'\rangle$, dann

$$T_A(\langle a, b, c\rangle) = \langle a', b', c'\rangle$$

wobei

$$(*) \begin{cases} a' = a\alpha^2 + b\alpha\gamma + c\gamma^2 = Q(\alpha, \gamma), \\ b' = 2a\alpha\beta + b(\alpha\delta + \beta\gamma) + 2c\gamma\delta, \\ c' = a\beta^2 + b\beta\delta + c\delta^2 = Q(\beta, \delta). \end{cases}$$

Somit,

$$Q'(X, Y) = Q(\alpha X + \beta Y, \gamma X + \delta Y).$$

Es ist leicht zu erkennen, dass wenn A, $A' \in \mathrm{GL}_2(\mathbb{Z})$, dann $T_{AA'}(Q) = T'_A(T_A(Q))$. Q ist eine einfache Form genau dann, wenn $T_A(Q)$ eine einfache Form ist.

Die Abbildung T_A ist die Identität genau dann, wenn $A = \pm I$, wobei

$$I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

die Einheitsmatrix ist.

Die Formen Q, Q' nennt man *äquivalent*, wenn es $A \in \mathrm{GL}_2(\mathbb{Z})$ derart gibt, dass $Q' = T_A(Q)$. Diese Tatsache wird durch $Q \sim Q'$ bezeichnet und es ist leicht nachzuvollziehen, dass es sich dabei um eine Äquivalenzrelation handelt.

Die Formen Q, Q' sind *echt äquivalent*, wenn es $A \in \mathrm{SL}_2(\mathbb{Z})$ derart gibt, dass $Q' = T_A(Q)$; die Notation hier ist $Q \approx Q'$, und wiederum

handelt es sich dabei um eine Äquivalenzrelation. Die echte Äquivalenzklasse von $Q = \langle a, b, c\rangle$ sei mit $\mathbb{Q} = \langle a, b, c\rangle$ bezeichnet.

Offensichtlich folgt aus $Q \approx Q'$ auch $Q \sim Q'$.

Jede Äquivalenzklasse ist entweder die Vereinigung zweier echter Äquivalenzklassen oder einfach eine echte Äquivalenzklasse. Zum Beispiel ist für jede ganze Zahl $a \neq 0$ jede Form, die äquivalent zu $\langle a, 0, a\rangle$ ist, auch echt äquivalent zu $\langle a, 0, a\rangle$.

Man kann leicht erkennen, dass Q, Q' im Falle $Q \sim Q'$ dieselbe Menge von Werten haben; somit ist eine ganze Zahl genau dann durch Q dargestellt, wenn sie durch Q' dargestellt wird. Ebenso haben Q und Q' dieselbe Menge einfacher Werte.

Darüberhinaus gilt für $Q \sim Q'$, dass $\mathrm{Diskr}(Q) = \mathrm{Diskr}(Q')$.

Für $D \equiv 0, 1 \pmod 4$ bezeichne $\mathrm{Cl}_+(\mathcal{Q}_D)$ die Menge der echten Äquivalenzklassen von Formen mit Diskriminante D und $\mathrm{Cl}_+(\mathrm{Prim}\,\mathcal{Q}_D)$ die Teilmenge der echten Äquivalenzklassen von einfachen Formen. Die ähnlichen Bezeichnungsweisen $\mathrm{Cl}(\mathcal{Q}_D)$, $\mathrm{Cl}(\mathrm{Prim}\,\mathcal{Q}_D)$ werden für Mengen von Äquivalenzklassen verwendet.

Es ist eine grundlegende Tatsache, dass es im Allgemeinen für eine gegebene Diskriminante mehr als eine Äquivalenzklasse einfacher Formen gibt.

So sind zum Beispiel die Formen $\langle 1, 0, 5\rangle$, $\langle 2, 2, 3\rangle$ einfach mit Diskriminante -20. Sie können aber nicht äquivalent sein, da 5 ein Wert der ersten, aber nicht der zweiten Form ist, wie man leicht verifizieren kann, wenn man beachtet, dass $2x^2 + 2xy + 3y^2 \not\equiv 1 \pmod 4$ für alle ganzen Zahlen x, y gilt.

7 Bedingte Lösung der Hauptprobleme

Lösung von Problem 1. Gegeben seien m und D mit $D \equiv 0$ oder $1 \pmod 4$. Dann existiert eine einfache Darstellung von m durch eine Form mit Diskriminante D genau dann, wenn es ein n derart gibt, dass $D \equiv n^2 \pmod{4m}$.

Der Beweis ist nicht schwierig. Man beachte zunächst das Folgende:

Wenn m eine einfache Darstellung durch $Q \in \mathcal{Q}_D$ hat, dann gibt es $n \in \mathbb{Z}$ derart, dass $D \equiv n^2 \pmod{4m}$ und $Q \sim \langle m, n, l\rangle$ mit $l = \frac{n^2-D}{4m}$.

Tatsächlich gibt es ganze Zahlen α, γ mit $\mathrm{ggT}(\alpha, \gamma) = 1$ und $m = Q(\alpha, \gamma)$. Seien β, δ ganze Zahlen mit $\alpha\delta - \beta\gamma = 1$ und sei $A = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$; sei $Q' = T_A(Q)$, also $Q' = \langle m, n, l\rangle \in \mathcal{Q}_D$ (für gewisse n, l); damit $D = n^2 - 4ml$ und so $D \equiv n^2 \pmod{4m}$ und $l = \frac{n^2-D}{4m}$.

Umgekehrt gebe es n mit $D \equiv n^2 \pmod{4m}$. Sei $l = \frac{n^2-D}{4m}$, also $\langle m, n, l\rangle \in \mathcal{Q}_D$ und m besitzt eine einfache Darstellung durch $\langle m, n, l\rangle$.

Beispielsweise sei $m = 4$, $D = 17$. Dann besitzt 4 eine einfache Darstellung durch die Form $\langle 4, 1, -1\rangle$, welche die Diskriminante $D = 17$ hat.

Lösung von Problem 2. Angenommen $n_1, \ldots, n_k$ seien die ganzen Zahlen mit $1 \leq n_i \leq 2m$ und $D \equiv n_i^2 \pmod{4m}$. Dann besitzt m eine einfache Darstellung durch die Form $Q \in \mathcal{Q}_D$ genau dann, wenn $Q \approx \langle m, n, l\rangle$, wobei $n \equiv n_i \pmod{2m}$ für irgendein i, und $l = \frac{n^2-D}{4m}$.

Die eine Richtung ist klar. Umgekehrt gilt wie schon bei der Lösung von Problem 1: Wenn m eine einfache Darstellung durch $Q \in \mathcal{Q}_D$ hat, dann gibt es ein n derart, dass $D \equiv n^2 \pmod{4m}$ und $Q \approx \langle m, n, l\rangle$, wobei $l = \frac{n^2-D}{4m}$. Wenn $n \equiv n' \pmod{2m}$ mit $1 \leq n' \leq 2m$, dann $D \equiv n^2 \equiv n'^2 \pmod{4m}$, also $n' = n_i$ (für irgendein i).

Hieraus ergibt sich eine Prozedur zum Finden der Formen Q, die eine einfache Darstellung von m liefern (sobald Problem 4 gelöst ist).

Zum Beispiel hat 4 eine einfache Darstellung durch eine Form Q mit Diskriminante 17 genau dann, wenn Q echt äquivalent zu einer der Formen $\langle 4, 1, -1\rangle$, $\langle 4, 7, 2\rangle$ ist.

Lösung von Problem 3. Sei $m = Q(\alpha, \gamma)$ mit $\mathrm{ggT}(a, \gamma) = 1$ eine einfache Darstellung von m durch die Form Q. Dann gibt es eindeutig bestimmte ganze Zahlen β, δ derart, dass $A = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$ und $T_A(Q) = \langle m, n, l\rangle$ mit $D \equiv n^2 \pmod{4m}$, $1 \leq n \leq 2m$, $l = \frac{n^2-D}{4m}$. Dies ist nicht schwer nachzuweisen. Man bedenke, dass wenn β_0, δ_0 dergestalt sind, dass $\alpha\delta_0 - \gamma\beta_0 = 1$, dann sind alle möglichen Paare ganzer Zahlen (β, δ) mit $\alpha\delta - \beta\gamma = 1$ gegeben durch

$$\begin{cases} \beta = \beta_0 + k\alpha \\ \delta = \delta_0 + k\gamma \end{cases} \qquad \text{für beliebiges } k \in \mathbb{Z}.$$

Es ist möglich, k eindeutig so zu wählen, dass

$$n = 2a\alpha\beta + b(\alpha\delta + \beta\gamma) + 2c\gamma\delta$$

wobei $1 \leq n < 2m$ und $D \equiv n^2 \pmod{4m}$.

Die Darstellung $m = Q(\alpha, \gamma)$ nennt man zu n gehörig, wenn n wie oben bestimmt ist. Umgekehrt entspricht sie für jedes n mit $1 \leq n < 2m$, $D \equiv n^2 \pmod{4m}$ und $Q \approx \langle m, n, l\rangle$ zum Beispiel folgender Darstellung: Wenn $T_A(Q) = \langle m, n, l\rangle$ mit $A = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$,

dann $m = T_A(Q)(1,0) = Q(\alpha,\gamma)$. Offensichtlich gehört diese Darstellung zu n.

Es bleibt noch, alle einfachen Darstellungen zu bestimmen, die zum selben Wert n gehören. Es seien $m = Q(\alpha,\gamma) = Q(\alpha',\gamma')$ einfache Darstellungen. Wenn (β,δ), (β',δ') die eindeutig bestimmten Paare ganzer Zahlen derart sind, dass gilt $A = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$, $A' = \begin{pmatrix} \alpha' & \beta' \\ \gamma' & \delta' \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$ mit $T_A(Q) = \langle m,n,l\rangle$, $T_{A'}(Q) = \langle m,n',l'\rangle$ und $1 \le n,\ n' < 2m$, $l = \frac{n^2-D}{4m}$, $l' = \frac{n'^2-D}{4m}$, dann $n = n'$ genau dann, wenn es $B \in \mathrm{SL}_2(\mathbb{Z})$ mit $A' = BA$ und $T_B(Q) = Q$ gibt.

Die Aufzählung aller möglichen einfachen Darstellungen von m durch Q erfordert also die Lösung der folgenden Probleme:

Problem 1. Es seien Q, Q' Formen einer gegebenen Diskriminante. Entscheide, ob Q und Q' äquivalent sind (bzw. echt äquivalent) oder ob dies nicht der Fall ist.

Genauer gesagt ist es erforderlich, einen Algorithmus für dieses Problem zu finden.

Problem 2. Bestimme für jede Form Q die Menge

$$\{B \in \mathrm{SL}_2(\mathbb{Z}) \mid T_B(Q) = Q\}.$$

Diese Menge, die offensichtlich eine Untergruppe von $\mathrm{SL}_2(\mathbb{Z})$ ist, nennt man die *Automorphe* von Q. Es ist genau genommen der Stabilisator von Q bei der Operation von $\mathrm{SL}_2(\mathbb{Z})$ auf der Menge der Formen.

Man beachte, dass wenn $Q \approx Q'$ und wenn $A_0 \in \mathrm{SL}_2(\mathbb{Z})$ die Eigenschaft hat, dass $T_{A_0}(Q) = Q'$, dann ist $\{A \in \mathrm{SL}_2(\mathbb{Z}) \mid T_A(Q) = Q'\} = \{BA_0 \mid B \text{ in der Automorphen von } Q\}$.

Wenn $T_B(Q) = Q$, dann ist in der Tat $T_{BA_0}(Q) = Q'$. Umgekehrt, wenn $T_A(Q) = Q'$, dann $T_{AA_0^{-1}}(Q) = Q$, also ist $AA_0^{-1} = B$ in der Automorphen von Q und $A = BA_0$.

8 Echte Äquivalenzklassen definiter Formen

Sei $D < 0$, $D \equiv 0$ oder $1 \pmod 4$.

Die wesentliche Idee in dieser Untersuchung echter Äquivalenzklassen positiver definiter Formen ist es, in geeigneter Weise speziell reduzierte Formen zu wählen, wie ich es nun zeigen werde.

Lemma 1. *Wenn $Q \in \mathcal{Q}_D$, dann gibt es $\langle a,b,c\rangle$ derart, dass $Q \approx \langle a,b,c\rangle$ und $|b| \le a \le c$.*

Beweis. Sei $Q = \langle m,n,l\rangle$, sei $\epsilon = \pm 1$ derart, dass $\epsilon n = |n|$. Wenn

$$A = \begin{pmatrix} 1 & -\epsilon \\ 0 & 1 \end{pmatrix} \quad \text{und} \quad b = \begin{pmatrix} 1 & 0 \\ -\epsilon & 1 \end{pmatrix},$$

dann

$$T_A(Q) = \langle m, n - 2\epsilon m, m + l - |n|\rangle = \langle m', n', l'\rangle,$$
$$T_B(Q) = \langle m + l - |n|, n - 2\epsilon l, l\rangle = \langle m', n', l'\rangle.$$

Wenn $|n| > m$, dann gilt in $T_A(Q)$, $m' + l' < m + l$.
Wenn $|n| > l$, dann gilt in $T_B(Q)$, $m' + l' < m + l$.
Durch Wiederholen dieser Vorgehensweise erreicht man eine Form $\langle a,b,c\rangle$ mit $|b| \le a$, $|b| \le c$ in derselben Klasse.
Wenn $a \le c$, dann stoppe. Falls $c < a$, setze $C = \left(\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right)$, dann $T_C(\langle a,b,c\rangle) = \langle c,-b,a\rangle$. □

Es ist wichtig zu beachten, dass wenn $Q \approx \langle a,b,c\rangle$ mit $|b| \le a \le c$, dann

$$a = \inf\{Q(\alpha,\beta) \mid \alpha,\beta \text{ ganze Zahlen}, Q(\alpha,\beta) \neq 0\},$$
$$ac = \inf\{Q(\alpha,\beta)Q(\gamma,\delta) \mid \alpha,\beta,\gamma,\delta \text{ ganze Zahlen}, \alpha\delta - \beta\gamma \neq 0\}.$$

Also sind a, c und somit auch $|b|$ eindeutig durch Q bestimmt. Es folgt, dass wenn $\langle a,b,c\rangle \approx \langle a',b',c'\rangle$ mit $|b| \le a \le c$ und $|b'| \le a' \le c'$, dann $a = a'$, $c = c'$, $b = \pm b'$. Darüberhinaus gilt in dieser Situation $\langle a,b,c\rangle \approx \langle a,-b,c\rangle$ genau dann, wenn $a = |b|$ oder $a = c$ oder $b = 0$.
Durch Kombination dieser Aussagen erhält man das folgende Hauptresultat:
Wenn $Q \in \mathcal{Q}_D$, dann gibt es eine eindeutig bestimmte Form $\langle a,b,c\rangle \in \mathcal{Q}_D$ derart, dass $Q \approx \langle a,b,c\rangle$ und

$$\text{(Rot)} \quad \begin{cases} |b| \le a \le c \\ \text{wenn } |b| = a \text{ oder } c = a, \text{ dann } b \ge 0. \end{cases}$$

Die Formen, die obiger Bedingung (Rot) genügen, nennt man die *reduzierten positiv definiten Formen* mit Diskriminante D.
Es sollte nicht unerwähnt bleiben, dass für $Q, Q' \in \mathcal{Q}_D$ die folgenden Bedingungen äquivalent sind.

(1) $Q \approx Q'$ oder $Q \approx \bar{Q}'$ ($\bar{Q}'$ bezeichnet die konjugierte Form von Q')
(2) $Q \sim Q'$
(3) {Werte von Q} = {Werte von Q'}.

Die einzige nicht-triviale Implikation ist (3) $\Rightarrow$ (1). Seien $Q_0 = \langle a, b, c\rangle$, $Q_0' = \langle a', b', c'\rangle$ reduzierte Formen dergestalt, dass $Q \approx Q_0$, $Q' \approx Q_0'$, also haben Q_0, Q_0' dieselben Mengen von Werten. Nach der Charakterisierung von a, c, a', c' als Infima von Werten folgt, dass $a = a'$, $c = c'$, und da diese Formen dieselbe Diskriminante haben, gilt $|b| = |b'|$. Somit $Q \approx Q'$ oder $Q \approx \bar{Q}'$.

Man sollte erwähnen, dass Schinzel (1980) zeigte, dass es Formen Q, Q' mit verschiedenen Diskriminanten, aber derselben Menge von Werten gibt, zum Beispiel $Q = \langle 1, 0, 3\rangle$ und $Q' = \langle 1, 1, 1\rangle$.

Numerisches Beispiel der Reduzierung einer definiten Form

Sei $\langle 2, 5, 4\rangle \in Q_{-7}$. Dann

$$\langle 2, 5, 4\rangle \approx \langle 2, 1, 1\rangle \approx \langle 1, -1, 2\rangle \approx \langle 1, 1, 2\rangle.$$

Es ist leicht einzusehen, dass wenn $\langle a, b, c\rangle \in \mathcal{Q}_D$ eine reduzierte Form ist, dann gilt

$$\begin{cases} 0 \le |b| \le \sqrt{\frac{|D|}{3}}, \\ b^2 \equiv D \pmod 4, \\ a \text{ teilt } \frac{b^2-D}{4}, \\ |b| \le a \le \frac{b^2-D}{4a}. \end{cases}$$

Somit ist die Anzahl reduzierter Formen endlich und gleich der Anzahl der echten Äquivalenzklassen; es folgt auch, dass die Anzahl der Äquivalenzklassen endlich ist.

Es wird sich als nützlich erweisen, die folgenden Notationen einzuführen.

Sei

$\tilde{h}(D)$ = Anzahl der Äquivalenzklassen von $\mathcal{Q}_D$,
$h(D)$ = Anzahl der Äquivalenzklassen von $\mathrm{Prim}(\mathcal{Q}_D)$,
$\tilde{h}_+(D)$ = Anzahl der echten Äquivalenzklassen von $\mathcal{Q}_D$,
$h_+(D)$ = Anzahl der echten Äquivalenzklassen von $\mathrm{Prim}(\mathcal{Q}_D)$.

Die folgenden Ungleichungen sind trivial: $h(D) \le \tilde{h}(D)$, $h_+(D) \le \tilde{h}_+(D)$ und $h(D) \le h_+(D) \le 2h(D)$, $\tilde{h}(D) \le \tilde{h}_+(D) \le 2\tilde{h}(D)$. Wie Beispiele zeigen werden, können obige Zahlen durchaus verschieden sein.

Anhand der Bijektion aus §4 lässt sich einfach zeigen, dass wenn $D = D_0 f^2$, wobei D_0 die Fundamentaldiskriminante zugehörig zu D ist, dann ist

$$\tilde{h}(D) = \sum_{e|f} h\left(\frac{D}{e^2}\right),$$
$$\tilde{h}_+(D) = \sum_{e|f} h_+\left(\frac{D}{e^2}\right);$$

zudem gilt, wenn D eine Fundamentaldiskriminante ist, dass

$$\tilde{h}(D) = h(D) \quad \text{und} \quad \tilde{h}_+(D) = h_+(D).$$

Angesichts der vorangegangenen Betrachtungen lässt sich eine Formel für die Zahl $\tilde{h}_+(D)$ leicht angeben.

Setze

$$n(a,b) = \begin{cases} 1 & \text{wenn } b = 0, \\ 1 & \text{wenn } b = a, \\ 1 & \text{wenn } a = \sqrt{\frac{b^2-D}{4}}, \\ 2 & \text{sonst.} \end{cases}$$

Dann ist $\tilde{h}_+(D) = \sum_{b\in\mathcal{B}} \sum_{a\in\mathcal{A}_b} n(a,b)$, wobei

$$\mathcal{B} = \{b \mid 0 \le b < \sqrt{\frac{|D|}{3}}, b \equiv D \pmod 2\}$$
$$\mathcal{A}_b = \{a \mid a \text{ teilt } \tfrac{b^2-D}{4} \text{ und } b \le a \le \sqrt{\tfrac{b^2-D}{4}}\}$$

Diese Formel lässt sich für kleines $|D|$ leicht verwenden.

Zahlenbeispiel

Um $h_+(-303)$ zu berechnen und alle reduzierten Formen mit Diskriminante $D = -303$ zu bestimmen:

$b \in \mathcal{B}$ genau dann, wenn b ungerade ist und $0 < b < 10$ gilt, somit $\mathcal{B} = \{1, 3, 5, 7, 9\}$.

Es ist leicht nachvollziehbar, dass $\mathcal{A}_1 = \{1, 2, 4\}$, $\mathcal{A}_3 = \{3, 6\}$, $\mathcal{A}_5 = 0$, $\mathcal{A}_7 = \{8\}$ und $\mathcal{A}_9 = 0$.

Gemäß der Definition von $n(a,b)$,

$$\begin{aligned}\tilde{h}_+(-303) &= n(1,1)+n(1,2)+n(1,4)+n(3,3)+n(3,6)+n(7,8)\\ &= 1+2+2+1+2+2=10.\end{aligned}$$

Da -303 eine Fundamentaldiskriminante ist, ergibt sich $h_+(-303) = \tilde{h}_+(-303) = 10$.

Hier die explizite Bestimmung der reduzierten Formen mit Diskriminante -303:

b	$\frac{b^2-D}{4}$	a	b
±1	76	1 2 4 ~~19~~ ~~38~~ ~~76~~	76 38 19 ~~4~~ ~~2~~ ~~1~~
±3	78	3 6 ~~13~~ ~~26~~ ~~39~~ ~~78~~	26 13 6 3 2 1
±5	82	~~41~~ ~~82~~	~~2~~ ~~1~~
±7	88	8 ~~11~~ ~~22~~ ~~44~~ ~~88~~	11 ~~8~~ ~~4~~ ~~2~~ ~~1~~
±9	96	~~12~~ ~~16~~ ~~32~~ ~~48~~ ~~96~~	~~8~~ ~~6~~ ~~3~~ ~~2~~ ~~1~~

Die reduzierten Formen sind demnach
$\langle 1,1,76\rangle$, $\langle 2,1,38\rangle$, $\langle 4,1,19\rangle$, $\langle 1,-1,76\rangle$, $\langle 2,-1,38\rangle$, $\langle 4,-1,19\rangle$, $\langle 3,3,26\rangle$, $\langle 6,3,13\rangle$, $\langle 6,-3,13\rangle$, $\langle 8,7,11\rangle$ und $\langle 8,-7,11\rangle$.

Daraus folgt, dass $\tilde{h}(-303) = h(-303) = 6$.

Noch ein Zahlenbeispiel

Wenn $D = -72 = 9\times(-8)$, dann ist die zugehörige Fundamentaldiskriminante $D_0 = -8$.

Dieselbe Methode führt zu

$$\begin{aligned}h(-72) &= h_+(-72) = 2,\\ h(-8) &= h_+(-8) = 1.\end{aligned}$$

Also $\tilde{h}(-72) = \tilde{h}_+(-72) = 3$, mit den reduzierten Formen $\langle 1,0,18\rangle$, $\langle 2,0,9\rangle$ und $\langle 3,0,6\rangle$ (letztere nicht einfach).

9 Echte Äquivalenzklassen indefiniter Formen

Sei $D > 0$ (kein Quadrat).

Man nennt die Form $Q = \langle a,b,c\rangle \in \mathcal{Q}_D$ eine *reduzierte indefinite Form* mit Diskriminante D, wenn die folgenden Bedingungen erfüllt sind:

$$\text{(Rot)}\qquad \begin{cases} 0 < b < \sqrt{D},\\ \sqrt{D} - b < 2|a| < \sqrt{D} + b.\end{cases}$$

Es folgt (wie leicht zu sehen ist), dass

$ac < 0$, $|a| < \sqrt{D}$, $|c| < \sqrt{D}$ und auch $\sqrt{D} - b < 2|c| < \sqrt{D} + b$.

Zudem ist $\langle a, b, c\rangle$ eine reduzierte Form, wenn $|a| \le |c|$ und $\sqrt{D} - 2|a| < b < \sqrt{D}$.

Hier der einfache Algorithmus, um die reduzierten Formen in $\mathcal{Q}_D$ aufzuzählen.

Für jede ganze Zahl b, $0 < b < \sqrt{D}$, für die 4 Teiler von $D - b^2$ ist, faktorisiere die ganze Zahl $(D - b^2)/4$ auf alle möglichen Weisen.

Für jede Faktorisierung $(D - b^2)/4 = ac$ mit a, $c > 0$, prüfe, wann die Bedingungen

$$(*)\ \begin{cases} \sqrt{D} - b < 2a < \sqrt{D} + b \\ \sqrt{D} - b < 2c < \sqrt{D} + b \end{cases}$$

erfüllt sind. Wenn nicht, verwerfe die Faktorisierung. Wenn $(*)$ erfüllt ist, dann sind die Formen $\langle a, b, -c\rangle$, $\langle -a, b, c\rangle$, $\langle c, b, -a\rangle$, $\langle -c, b, a\rangle$ reduziert mit Diskriminante D; man beachte, dass es im Fall $a = c$ nur zwei verschiedene Formen gibt.

Zahlenbeispiel

Die reduzierten Formen mit Diskriminante $D = 52$ müssen ein gerades b mit $0 < b < 52$ haben, damit ist 4 ein Teiler von $52 - b^2$; somit $b = 2$, 4 oder 6. Wenn $b = 2$, dann $-ac = \frac{52-4}{4} = 12$; darüberhinaus $\sqrt{52} - 2 < 2|a|$, $2|c| < \sqrt{52} + 2$, also $(a, c) = (\pm 3, \mp 4)$, $(\pm 4, \mp 3)$. Wenn $b = 4$, dann $-ac = \frac{52-16}{4} = 9$; weiter $\sqrt{82} - 4 < 2|a|$, $2|c| < \sqrt{52} + 4$, also $(a, c) = (\pm 3, \mp 3)$. Für $b = 6$ ist $ac < 0$, $ac = \frac{52-36}{4} = 4$; weiter $\sqrt{52} - 6 < 2|a|$, $2|c| < \sqrt{52} + 6$, also $(a, c) = (\pm 1, \mp 4)$, $(\pm 2, \mp 2)$, $(\pm 4, \mp 1)$.

Somit sind die reduzierten Formen $\langle \pm 3, 2, \mp 4\rangle$, $\langle \pm 4, 2, \mp 3\rangle$, $\langle \pm 1, 6, \mp 4\rangle$, $\langle \pm 2, 6, \mp 2\rangle$ und $\langle \pm 4, 6, \mp 1\rangle$.

Lemma 1. *Jedes $Q \in \mathcal{Q}_D$ ist äquivalent zu einer reduzierten Form.*

Beweis. Sei $Q = \langle m, n, l\rangle$. Wir werden zeigen, dass es $\langle a, b, c\rangle \approx Q$ derart gibt, dass $|a| \le |c|$, $\sqrt{D} - 2|a| < b < \sqrt{D}$; nach einer vorangegangenen Anmerkung ist $\langle a, b, c\rangle$ dann eine reduzierte Form.

Sei $\lambda = [\sqrt{D}]$ und betrachte die Menge der $2|l|$ ganzen Zahlen $\{\lambda + 1 - 2|l|, \lambda + 2 - 2|l|, \ldots, \lambda\}$. Dann gibt es ein eindeutiges n', $\lambda + 1 - 2|l| \le n' \le \lambda$ mit $n \equiv -n' \pmod{2|l|}$.

Sei

$$\delta = -\frac{n+n'}{2|l|} \quad \text{und} \quad A = \begin{pmatrix} 0 & 1 \\ -1 & \delta \end{pmatrix}.$$

Dann $T_A\langle m,n,l\rangle = \langle l,n',l'\rangle$ mit $l' = m + n\delta + l\delta^2$ und $\sqrt{D} - 2|l| < n' < \sqrt{D}$.

Wiederhole dies, solange $|l| > |l'|$. Da nicht ewig $|l| > |l'| > |l''| > \cdots$ gelten kann, gelangt man zu einer Form $\langle a,b,c\rangle \approx Q$, mit $|c| \le |a|$ und $\sqrt{D} - 2|a| < b < \sqrt{D}$, die Form ist reduziert. □

Numerisches Beispiel der Reduktion einer indefiniten Form

Sei $\langle 76,58,11\rangle \in \mathcal{Q}_{20}$. Dann

$$\langle 76,58,11\rangle \approx \langle 11,-14,4\rangle \approx \langle 4,-2,-1\rangle \approx \langle -1,4,5\rangle.$$

Man kann zeigen, dass es nur endlich viele Formen $\langle a,b,c\rangle \in \mathcal{Q}_D$ mit $ac < 0$ gibt. Also gibt es nur endlich viele reduzierte Formen und man kann schließen:

Die Anzahl der echten Äquivalenzklassen indefiniter Formen mit Diskriminante D ist endlich. Damit ist auch die Anzahl der echten Äquivalenzklassen von $\mathrm{Prim}(\mathcal{Q}_D)$ endlich, und so auch die Anzahl der Äquivalenzklassen von $\mathcal{Q}_D$ und von $\mathrm{Prim}(\mathcal{Q}_D)$.

Wie im Falle der positiven definiten Formen wird die folgende Bezeichnungsweise Verwendung finden:

$\tilde{h}_+(D)$, $h_+(D)$ für die Anzahl echter Äquivalenzklassen von $\mathcal{Q}_D$ bzw. $\mathrm{Prim}(\mathcal{Q}_D)$;

$\tilde{h}(D)$, $h(D)$ für die Anzahl der Äquivalenzklassen von $\mathcal{Q}_D$, $\mathrm{Prim}(\mathcal{Q}_D)$.

Wiederum sind die folgenden Ungleichungen trivial:

$$h_+(D) \le \tilde{h}_+(D), \quad h(D) \le \tilde{h}(D),$$

$$h(D) \le h_+(D) \le 2h(D), \quad \tilde{h}(D) \le \tilde{h}_+(D) \le 2\tilde{h}(D).$$

Wenn $D = D_0 f^2$, wobei D_0 eine Fundamentaldiskriminante ist, dann

$$\tilde{h}(D) = \sum_{e|f} h\left(\frac{D}{e^2}\right) \quad \text{und} \quad \tilde{h}_+(D) = \sum_{e|f} h_+\left(\frac{D}{e^2}\right).$$

Somit ist $\tilde{h}_+(D) = h_+(D)$ und $\tilde{h}(D) = h(D)$, wenn D eine Fundamentaldiskriminante ist. Wie man anhand von Beispielen belegen kann, können $h(D)$, $h_+(D)$ (bzw. $\tilde{h}(D)$, $\tilde{h}_+(D)$) durchaus verschieden sein.

Es ist wesentlich, den Fall zweier echt äquivalenter reduzierter Formen zu untersuchen.

Sei $\mathcal{R}_D$ die Menge reduzierter Formen in $\mathcal{Q}_D$.

Wenn $Q = \langle a, b, c\rangle \in \mathcal{R}_D$, dann gibt es eine eindeutig bestimmte echt äquivalente Form $Q' = \langle c, b', c'\rangle \in \mathcal{R}_D$ mit $2c \mid b + b'$, sowie eine eindeutige äquivalente Form $Q'' = \langle a'', b'', a\rangle \in \mathcal{R}_D$ mit $2a \mid b + b''$. Die Form Q' nennt man *rechtsadjazent* und die Form Q'' *linksadjazent* zu Q. Notwendigerweise ist $2|c|$ Teiler von $b + b'$ und $2|a|$ teilt $b + b''$. Sei $Q' = p(Q)$, $Q'' = \lambda(Q)$; dann ist $Q = \lambda(Q')$, $Q = \rho(Q'')$. Man beachte, dass $\rho(Q) = T_A(Q)$, wobei

$$A = \begin{pmatrix} 0 & 1 \\ -1 & \delta \end{pmatrix},$$

und δ eindeutig ist. Die eigentliche Bestimmung von δ wird an späterer Stelle erfolgen, aber es sollte bereits auf $a\delta > 0$ hingewiesen werden.

Da $\mathcal{R}_D$ endlich ist, gibt es für jedes $Q \in \mathcal{R}_D$ Indizes $i < i + k$ derart, dass wenn $Q_1 = \rho(Q)$, $Q_2 = \rho(Q_1)$, ... gilt $Q_i = Q_{i+k}$; aber $Q_{i-1} = \lambda(Q_i) = \lambda(Q_{i+k}) = Q_{i+k-1}$, ..., und dies ergibt $Q = Q_k$. Sei $k \geq 1$ minimal. Dann nennt man die Menge $\{Q = Q_0, Q_1, \ldots, Q_k\}$ die *Periode* von Q. Offensichtlich ist diese Menge auch die Periode eines jeden $Q_i (1 \leq i \leq k)$. Somit ist $\mathcal{R}_D$ in Perioden partitioniert; Formen in derselben Periode sind offenbar echt äquivalent. Die Umkehrung ist ein Hauptresultat der Theorie:

Wenn $Q, Q' \in \mathcal{R}_D$ und $Q \approx Q'$, dann sind Q, Q' in derselben Periode. Somit ist $\tilde{h}_+(D)$ gleich der Anzahl der Perioden und in gleicher Weise ist $h_+(D)$ die Anzahl der Perioden einfacher reduzierter Formen.

Es ist nicht schwer nachzuvollziehen, dass die Anzahl der Formen in jeder Periode gerade sein muss.

Es gibt eine interessante Verbindung zwischen Perioden und Kettenbruchentwicklungen.

Die Tatsache, dass die Form $\langle a, b, c\rangle$ reduziert ist, kann man auch durch die Nullstellen ω, η der Form ausdrücken. Es ist nämlich $\langle a, b, c\rangle$ reduziert genau dann, wenn $|w| > 1$, $|\eta| < 1$ und $\omega\eta < 0$.

Es sei $\{Q = Q_0, Q_1, \ldots, Q_{2r-1}\}$ die Periode der reduzierten Form Q. Sei weiter $\rho(Q_i) = T_{A_i}(Q_i) = Q_{i+1}$, wobei $A_i = \begin{pmatrix} 0 & 1 \\ -1 & \delta_i \end{pmatrix}$. Seien ω_i, η_i die Nullstellen der Form Q_i. Dann

$$|\omega_i| = \frac{1}{|\delta_i| + |\omega_{i+1}|} \quad \text{für } i = 0, 1, \ldots, 2r-1 \text{ und } |\omega_r| = |\omega_0|.$$

Somit

$$|\omega| = [\overline{|\delta_0|, |\delta_1|, \ldots, |\delta_{r-1}|}],$$

das heißt $|\delta_0|, |\delta_1|, \ldots, |\delta_{r-1}|$ sind die Teilquotienten in der einfachen Kettenbruchentwicklung der quadratischen irrationalen Zahl ω; diese Entwicklung ist periodisch.

Es gilt zudem, dass wenn $Q = \langle a, b, c\rangle$ eine Form mit Diskriminante $D > 0$ ist und $\left|\frac{-b+\sqrt{D}}{2a}\right|$ eine einfache periodische Kettenbruchentwicklung mit Periode r und Teilquotienten $|\delta_0|, |\delta_1|, \ldots, |\delta_{r-1}|$, dann ist Q eine reduzierte Form. Ihre Periode hat $2r$ Elemente wenn r ungerade ist, r Elemente für gerades r und sie ist gleich $\{Q = Q_0, Q_1, \ldots, Q_{2r-1}\}$ mit

$$Q_{i+1} = T_{A_i}(Q_i), \quad A_i = \begin{pmatrix} 0 & 1 \\ -1 & \delta_i \end{pmatrix}, \quad A_{i+r} = \begin{pmatrix} 0 & 1 \\ -1 & -\delta_i \end{pmatrix},$$

für $0 \le i \le r-1$; wenn $Q_i = \langle a_i, b_i, c_i\rangle$, dann $a_i\delta_i > 0$ (für $i = 0, 1, \ldots, r-1$).

Zahlenbeispiel

Für kleine Werte von $D > 0$ ist es leicht, $\tilde{h}_+(D)$, $h_+(D)$ zu berechnen. Zum Beispiel ist für $D = 68$ (keine Fundamentaldiskriminante) $\sqrt{D} = 2\sqrt{17} = 8{,}24\ldots$.

Bestimmung der reduzierten Formen mit Diskriminante 68: Da 4 Teiler von $D - b^2$ ist und $0 < b < \sqrt{D}$ folgt $b = 2, 4, 6, 8$. Zudem $\sqrt{D} - b < 2|a| < \sqrt{D} + b$. Daraus ergeben sich die Möglichkeiten:

b	$\sqrt{D} - b$	$\sqrt{D} + b$	$\lvert ac\rvert$	$\lvert a\rvert$	$\lvert c\rvert$
2	6,24	10,24	16	4	4
4	4,24	12,24	13	–	–
6	2,24	14,24	8	2	4
				4	2
8	0,24	16,24	1	1	1

Damit besteht $\mathcal{R}_{68}$ aus den 8 Formen

$$\langle \pm 4, 2, \mp 4\rangle, \quad \langle \pm 2, 6, \mp 4\rangle, \quad \langle \pm 4, 6, \mp 2\rangle, \quad \langle \pm 1, 8, \mp 1\rangle.$$

Berechnung der Periode von $\langle 4, 2, -4\rangle$: ihre erste Nullstelle ist $\omega = \frac{\sqrt{17}-1}{4}$, die die folgende Kettenbruchentwicklung hat: $\omega = [\overline{1, 3, 1}]$.

Für $0 \le i \le 5$ sei $A_i = \begin{pmatrix} 0 & 1 \\ -1 & -\delta_i \end{pmatrix}$ mit $\delta_0 = 1$, $\delta_1 = -3$, $\delta_2 = 1$, $\delta_3 = -1$, $\delta_4 = 3$, $\delta_5 = -1$. Sei $Q_{i+1} = T_{A_i}(Q_i)$ (für $i = 0, 1, \ldots, 5$); dann besteht die Periode von $\langle 4, 2, -4\rangle$ aus dieser Form sowie den Formen $\langle -4, 6, 2\rangle$, $\langle 2, 6, -4\rangle$, $\langle -4, 2, 4\rangle$, $\langle 4, 6, -2\rangle$ und $\langle -2, 6, 4\rangle$.

Die andere Periode ist $\{\langle 1, 8, -1\rangle, \langle -1, 8, 1\rangle\}$. Somit $\tilde{h}_+(68) = 2$, während $h_+(68) = 1$. Desweiteren, $\tilde{h}(68) = 2$, $h(68) = 1$.

A Ein weiteres Zahlenbeispiel

Sei $D = 76 = 4 \times 19$ (dies ist eine Fundamentaldiskriminante). Die reduzierten Formen sind $\langle \pm 3, 4, \mp 5\rangle$, $\langle \pm 5, 4, \mp 3\rangle$, $\langle \pm 2, 6, \mp 5\rangle$, $\langle \pm 5, 6, \mp 2\rangle$, $\langle \pm 1, 8, \mp 3\rangle$ und $\langle \pm 3, 8, \mp 1\rangle$.

Zur Berechnung der Periode von $\langle 3, 4, -5\rangle$: Ihre erste Nullstelle ist $\omega = \frac{-2+\sqrt{19}}{3}$. Die einfache Kettenbruchentwicklung von ω ist $\omega = \overline{[1, 3, 1, 2, 8, 2]}$ und die Periode von $\langle 3, 4, -5\rangle$ ist $\{\langle 3, 4, -5\rangle, \langle -5, 6, 2\rangle, \langle 2, 6, -5\rangle, \langle -5, 4, 3\rangle, \langle 3, 8, -1\rangle, \langle -1, 8, 3\rangle\}$.

Es gibt eine weitere Periode bestehend aus den anderen sechs reduzierten Formen. Somit ist $h_+(76) = 2$, während $h(76) = 1$.

10 Die Automorphe einer einfachen Form

Man erinnere sich, dass die Automorphe einer Form $Q = \langle a, b, c\rangle$ aus all denjenigen $A \in \mathrm{SL}_2(\mathbb{Z})$ besteht, für die $T_A(Q) = Q$ gilt.

Die Beschreibung der Automorphen erfordert die vorausgehende Untersuchung des Verhaltens der Nullstellen von Q unter der Operation irgendeines $A \in \mathrm{GL}_2(\mathbb{Z})$.

Sei also $Q = \langle a, b, c\rangle$ mit Nullstellen ω, η; sei $A \in \mathrm{GL}_2(\mathbb{Z})$ und $Q' = T_A(Q)$ habe die Nullstellen ω', η'.

Wenn $\zeta \in \{\omega', \eta'\}$, dann

$$(\gamma\zeta' + \delta)^2 Q\left(\frac{\alpha\zeta' + \beta}{\gamma\zeta' + \delta}, 1\right) = Q(\alpha\zeta' + \beta, \gamma\zeta' + \delta) = Q'(\zeta', 1) = 0;$$

wegen $\gamma\zeta' + \delta \neq 0$ ist $\frac{\alpha\zeta'+\beta}{\gamma\zeta'+\delta}$ eine Nullstelle von Q.

Eine einfache Berechnung zeigt, dass wenn $A \in \mathrm{SL}_2(\mathbb{Z})$, dann

$$\frac{\alpha\omega' + \beta}{\gamma\omega' + \beta} = \omega \quad \text{und} \quad \frac{\alpha\eta' + \beta}{\gamma\eta' + \delta} = \eta,$$

während wenn $A \notin \mathrm{SL}_2(\mathbb{Z})$, dann korrespondiert ω' mit η und η' mit ω.

Wenn sich $A \in \mathrm{SL}_2(\mathbb{Z})$ in der Automorphen der einfachen Form $Q = \langle a, b, c\rangle$ befindet, dann folgt aus $T_A(Q) = Q$, dass $\omega = \frac{\alpha\omega+\beta}{\gamma\omega+\delta}$, somit

$$\gamma\omega^2 + (\delta - \alpha)\omega - \beta = 0.$$

Es gilt aber auch

$$a\omega^2 + b\omega + c = 0,$$

und da $\mathrm{ggT}(a, b, c) = 1$, muss es eine ganze Zahl $u \neq 0$ derart geben, dass $\gamma = au$, $\delta - \alpha = bu$, $-\beta = cu$. Sei $t = \delta + \alpha$; dann $t \equiv bu \pmod 2$, $\alpha = \frac{t-bu}{2}$, $\delta = \frac{t+bu}{2}$. Aus $\alpha\delta - \beta\gamma = 1$ folgt, dass $\frac{t^2-b^2u^2}{4} + acu^2 = 1$ und schließlich $t^2 - Du^2 = 4$.

Diese Berechung deutet auf eine Beschreibung der Automorphen von $Q = \langle a, b, c\rangle$ hin:

A ist in der Automorphen von Q genau dann, wenn es ganze Zahlen t, u derart gibt, dass

$$\begin{cases} t^2 - Du^2 = 4 \\ \alpha = \frac{t-bu}{2} \\ \beta = -cu \\ \gamma = au \\ \delta = \frac{t+bu}{2}. \end{cases}$$

Damit gibt es eine eins-zu-eins-Beziehung zwischen Automorphen von Q und den ganzzahligen Lösungen der Gleichung

$$T^2 - DU^2 = 4.$$

Für $D < 0$ besitzt diese Gleichung nur die Lösungen

$$(t, u) = \begin{cases} (\pm 2, 0) & \text{wenn } D \neq -4, -3, \\ (\pm 2, 0), (\pm 1, \pm 1) & \text{wenn } D = -3, \\ (\pm 2, 0), (0, \pm 1) & \text{wenn } D = -4. \end{cases}$$

Also ist im Falle $D < 0$ die Anzahl der Elemente in der Automorphen von Q

$$w = \begin{cases} 2 & \text{wenn } D \neq -3, -4, \\ 6 & \text{wenn } D = -3, \\ 4 & \text{wenn } D = -4. \end{cases}$$

Für den Fall $D > 0$ bewies Lagrange, was bereits Fermat wusste: Es gibt unendlich viele Paare (t, u) ganzer Zahlen mit $t^2 - Du^2 = 4$.

Für (t_1, u_1) mit $t_1, u_1 > 0$ und minimalem $t_1 + u_1\sqrt{D}$ sind alle Lösungen (t, u) durch die Relationen gegeben:

$$\frac{t + u\sqrt{D}}{2} = \left(\frac{t_1 + u_1\sqrt{D}}{2}\right)^n \qquad \text{für } n = 0, \pm 1, \pm 2, \ldots .$$

Damit ist für $D > 0$ die Automorphe von Q unendlich.

LAGRANGE gab auch einen Algorithmus an, der es mithilfe von Kettenbrüchen ermöglicht, t_1 und u_1 zu bestimmen; dies ist sicher wohlbekannt.

Zahlenbeispiel

Bestimmung aller einfachen Darstellungen von $m = 17$ durch die Form $Q = \langle 2, 6, 5\rangle$ mit Diskriminante -4.

Man beachte zunächst, dass -4 quadratischer Rest modulo 68 ist, da -1 quadratischer Rest modulo 17 ist. Die ganzen Zahlen $n = 4, 13$ sind die einzigen Lösungen von $-1 \equiv n^2 \pmod{17}$, $1 \le n < 17$, also sind 8, 26 die einzigen ganzen Zahlen n mit $-4 \equiv n^2 \pmod{68}$, $1 \le n < 34$.

Um zu ermitteln, ob es eine einfache Darstellung von 17 durch Q zugehörig zu 8 gibt, muss man verifizieren, dass $Q \approx \langle 17, 8, 1\rangle$. Aber $h(-4) = 1$, also sind Q, $\langle 17, 8, 1\rangle$ notwendigerweise äquivalent zur einzigen reduzierten Form $\langle 1, 0, 1\rangle$ mit Diskriminante -4. Die Reduktion wird folgendermaßen durchgeführt:

$$\langle 2,6,5\rangle \xrightarrow[\left(\begin{smallmatrix}1 & -1\\ 0 & 1\end{smallmatrix}\right)]{\approx} \langle 2,2,1\rangle \xrightarrow[\left(\begin{smallmatrix}1 & 0\\ -1 & 1\end{smallmatrix}\right)]{\approx} \langle 1,0,1\rangle,$$

$$\langle 17,8,1\rangle \xrightarrow[\left(\begin{smallmatrix}1 & 0\\ -1 & 1\end{smallmatrix}\right)]{\approx} \langle 10,6,1\rangle \xrightarrow[\left(\begin{smallmatrix}1 & 0\\ -1 & 1\end{smallmatrix}\right)]{\approx} \langle 5,4,1\rangle$$

$$\langle 5,4,1\rangle \xrightarrow[\left(\begin{smallmatrix}1 & 0\\ -1 & 1\end{smallmatrix}\right)]{\approx} \langle 2,2,1\rangle \xrightarrow[\left(\begin{smallmatrix}1 & 0\\ -1 & 1\end{smallmatrix}\right)]{\approx} \langle 1,0,1\rangle$$

Sei

$$\begin{aligned} A &= \begin{pmatrix}1 & -1\\ 0 & 1\end{pmatrix}\begin{pmatrix}1 & 0\\ -1 & 1\end{pmatrix}\begin{pmatrix}1 & 0\\ 1 & 1\end{pmatrix}\begin{pmatrix}1 & 0\\ 1 & 1\end{pmatrix}\begin{pmatrix}1 & 0\\ 1 & 1\end{pmatrix}\begin{pmatrix}1 & 0\\ 1 & 1\end{pmatrix} \\ &= \begin{pmatrix}-2 & -1\\ 3 & 1\end{pmatrix} \end{aligned}$$

Dann,

$$T_A(\langle 2,6,5\rangle) = \langle 17,8,1\rangle.$$

Die Automorphen von $Q = \langle 2,6,5\rangle$ bestehen aus den Matrizen

$$\begin{pmatrix} \pm 1 & 0 \\ 0 & \pm 1 \end{pmatrix} \quad \text{und} \quad \begin{pmatrix} \mp 3 & \mp 5 \\ \pm 2 & \pm 3 \end{pmatrix}.$$

Alle einfachen Darstellungen erhält man aus den Matrizen BA, wobei B in der Automorphen von Q liegt:

$$\begin{pmatrix} \mp 2 & \mp 1 \\ \pm 3 & \pm 1 \end{pmatrix} \quad \text{und} \quad \begin{pmatrix} \mp 9 & \mp 2 \\ \pm 5 & \pm 1 \end{pmatrix}.$$

Damit ergeben sich die vier Darstellungen:

$$17 = Q(\mp 2, \pm 3) = Q(\mp 9, \pm 5).$$

Eine ähnliche Berechnung führt zu den einfachen Darstellungen von 17 durch Q, die zu 26 gehören:

$$T_{A'}(\langle 2,6,5\rangle) = \langle 17,26,10\rangle, \quad \text{wobei } A' = \begin{pmatrix} 7 & 5 \\ -3 & -2 \end{pmatrix}.$$

Die Matrizen BA' mit B in der Automorphen von Q sind

$$\begin{pmatrix} \pm 7 & \pm 5 \\ \mp 3 & \mp 2 \end{pmatrix} \quad \text{und} \quad \begin{pmatrix} \mp 6 & \mp 5 \\ \pm 5 & \pm 4 \end{pmatrix};$$

dies ergibt die vier Darstellungen:

$$17 = Q(\pm 7, \mp 3) = Q(\mp 6, \pm 5).$$

Der klassische Fall, der sich auf die Form $Q = \langle 1,0,1\rangle$ bezieht, wurde von FERMAT untersucht und wird in direkter Weise in einführenden Büchern behandelt. Die Ergebnisse von FERMAT lassen sich aber auch als Spezialfall von GAUSS' Theorie erzielen:

Eine ganze Zahl $m \geq 1$ besitzt eine einfache Darstellung als Summe zweier Quadrate genau dann, wenn $m = m_1 m_2^2$ mit $\mathrm{ggT}(m_1, m_2) = 1$ und wenn die Primteiler von m_1 entweder gleich 2 oder Primzahlen $p \equiv 1 \pmod 4$ sind. In diesem Fall ist die Anzahl der einfachen Darstellungen von m als Summe zweier Quadrate gleich

$$\rho(m) = 4(d_1(m) - d_3(m)),$$

wobei

$$d_1(m) = \#\{d > 0 \mid d \equiv 1 \pmod 4, d \mid m\},$$
$$d_3(m) = \#\{d > 0 \mid d \equiv 3 \pmod 4, d \mid m\}.$$

Um zu dieser Aussage zu gelangen, muss man im Wesentlichen die folgenden Punkte betrachten:

m ist Summe zweier Quadrate genau dann, wenn m durch eine Form mit Diskriminante -4 darstellbar ist, da $h_+(-4) = 1$. Dies passiert genau dann, wenn $-4 \equiv n^2 \pmod{4m}$ für irgendein n oder äquivalent, wenn -1 quadratischer Rest modulo m ist. Eine einfache Berechnung mit dem Jacobi-Symbol führt zur angegebenen Bedingung für m.

Jedes n mit $1 \leq n < 2m$ und $-4 \equiv n^2 \pmod{4m}$ entspricht $\omega = 4$ einfachen Darstellungen von m als Summe zweier Quadrate. Aus der Theorie der Kongruenzen ist die Anzahl der Lösungen n wie oben gleich $\sum_{k|m} \left(\frac{-1}{k}\right) = d_1(m) - d_3(m)$. Damit ist die Anzahl der einfachen Darstellungen tatsächlich $4(d_1(m) - d_3(m))$.

11 Komposition von echten Äquivalenzklassen einfacher Formen

Einer der wichtigsten und tiefliegendsten Beiträge von Gauss im Studium binärer quadratischer Formen ist die Theorie der Komposition. Die Idee war bereits von Legendre für einen Spezialfall umrissen worden.

Sei D irgendeine Diskriminante. Gauss definierte eine binäre Operation in der Menge $\mathrm{Cl}_+(\mathrm{Prim}(\mathcal{Q}_D))$ echter Äquivalenzklassen von einfachen Formen mit Diskriminante D. Wie sich zeigt, besitzt diese als *Komposition* bezeichnete Operation einige nette Eigenschaften.

Die Theorie wird hier in einer auf Dirichlet zurückgehenden einfachen Form vorgestellt.

Seien $Q = \langle a, b, c\rangle$, $Q' = \langle a', b', c'\rangle$ einfache Formen mit Diskriminante D. Die neue Form $Q'' = \langle a'', b'', c''\rangle$ ist wie folgt definiert.

Sei $\delta = \mathrm{ggT}\left(a, a', \frac{b+b'}{2}\right)$ und seien u, v, w irgendwelche ganzen Zahlen mit

$$au + a'v + \frac{b + b'}{2}w = \delta.$$

Man beachte, dass es unendlich viele Möglichkeiten zur Wahl von u, v, w gibt.

Definiere

$$\begin{cases} a'' = \frac{aa'}{\delta^2}, \\ b'' = \frac{1}{\delta}\left[aub' + a'vb + \frac{bb'+D}{2}w\right], \\ c'' = \frac{(b'')^2 - D}{4a''}. \end{cases}$$

Dann ist auch $Q'' = \langle a'', b'', c'' \rangle$ eine einfache Form mit Diskriminante D, abhängig von der Wahl von u, v, w—was durch die Bezeichnung $Q'' = Q''_{(u,v,w)}$ angedeutet ist. Man kann zeigen, dass wenn auch u_1, v_1, w_1 ganze Zahlen sind, die $au_1 + av_1 + \frac{b+b'}{2}w_1 = \delta$ erfüllen, dann ist die Form $Q''_{(u_1,v_1,w_1)}$ echt äquivalent zu $Q''_{(u,v,w)}$, obwohl verschieden von ihr.

Dem Paar einfacher Formen Q, Q' kann man somit die echte Äquivalenzklasse $\mathbf{Q}''_{(u,v,w)}$ von $Q''_{u,v,w)}$ zuordnen. Wenn $Q \approx Q_1$ und $Q' \approx Q'_1$ und wenn Q'', Q''_1 wie oben aus Q, Q' bzw. Q_1, Q'_1 hervorgehen, dann gilt auch $Q'' \approx Q''_1$. Dies erlaubt es uns, eine Operation der *Komposition* echter Äquivalenzklassen von einfachen Formen mit Diskriminante D zu definieren:

$$\mathbf{Q} * \mathbf{Q}' = \mathbf{Q}'',$$

wobei Q'' wie oben definiert ist (mit irgendwelchen u, v, w).

Gauss zeigte, dass wenn Q, Q', $Q'' \in \mathrm{Prim}(\mathcal{Q}_D)$ und wenn gilt $\mathbf{Q} * \mathbf{Q}' = \mathbf{Q}''$, dann gibt es für alle ganzen Zahlen x, y, x', y' ganze Zahlen x'' und y'', die Linearkombinationen von xx', xy', yx', yy' mit Koeffizienten aus $\mathbb{Z}$ sind, so dass gilt $Q''(x'', y'') = Q(x, y)Q'(x', y')$.

Der Beweis dieser wichtigen Eigenschaft der Komposition ist ziemlich kompliziert und ich werde ihn nun andeuten.

Zunächst lässt sich zeigen, dass es für je zwei beliebige Klassen $\mathbf{Q}$, $\mathbf{Q}'$ einfacher Formen möglich ist, einfache Formen $Q_1 \approx Q$, $Q'_1 \approx Q'$ so zu wählen, dass gilt

$$Q_1 = \langle a, b, a'c \rangle$$

$$Q'_1 = \langle a', b, ac \rangle$$

mit a, $a' \geq 1$, $\mathrm{ggT}(a, a') = 1$.

Seien u, v derart, dass gilt $au + a'v = 1$, sei $w = 0$ und betrachte die einfache Form Q''_1, die aus Q_1, Q'_1 und $(u, v, 0)$ wie in der Definition der Komposition gezeigt hervorgehe. Eine einfache Rechnung ergibt $Q''_1 = \langle aa', b, c \rangle$, und $\mathbf{Q}''_1 = \mathbf{Q}_1 * \mathbf{Q}_1 = \mathbf{Q} * \mathbf{Q}'$.

Dann kann man zeigen, dass $Q_1(x, y) \cdot Q'_1(x', y') = Q''_1(x'', y'')$, wobei

$$\begin{cases} x'' = xx' - cyy', \\ y'' = axy' + a'yx' + byy'. \end{cases}$$

Dies genügt, um die Aussage zu beweisen.

Die Komposition von echten Äquivalenzklassen einfacher Formen genügt dem Assoziativ- und dem Kommutativgesetz. Für die echte Äquivalenzklasse $\mathbf{P}$ der Hauptform P gilt, dass $\mathbf{Q} * \mathbf{P} = \mathbf{Q}$ für jede Klasse $\mathbf{Q}$. Die Klasse $\mathbf{P}$ nennt man *Hauptklasse*. Schließlich gibt es für jede Klasse $\mathbf{Q}$ eine notwendigerweise eindeutige Klasse $\mathbf{Q}'$ derart, dass $\mathbf{Q} * \mathbf{Q}' = \mathbf{P}$; die Klasse $\mathbf{Q}'$ ist die *Inverse von* $\mathbf{Q}$ unter der Komposition.

Damit ist $\mathrm{Cl}_+(\mathrm{Prim}(\mathcal{Q}_D))$ eine endliche abelsche Gruppe unter der Operation der Komposition—eine Tatsache, die von Gauss entdeckt wurde, auch wenn er es in anderen Worten ausdrückte.

Das Inverse der Klasse $\langle a, b, c\rangle$ ist $\langle a, -b, c\rangle$; dies ist die Klasse der zugehörigen Formen.

Eine Klasse, die gleich ihrer Inversen ist, nennt man eine *zweideutige Klasse*. Diese sind genau die Elemente der Ordnung 1 oder 2 in der Gruppe der Klassen einfacher Formen unter der Operation der Komposition. Man kann leicht zeigen, dass wenn $\langle a, b, c\rangle$ dergestalt ist, dass a Teiler von b ist, dann gilt $\langle a, b, c\rangle \approx \langle a, -b, c\rangle$, somit ist die Klasse $\langle a, b, c\rangle$ zweideutig.

Zahlenbeispiel

Wenn $D = -20$ und $P = \langle 1, 0, 5\rangle$, $Q = \langle 2, 2, 3\rangle$, dann ist $\mathbf{Q} * \mathbf{Q} = \mathbf{P}$, wie man leicht verifizieren kann.

Der Struktursatz für endliche abelsche Gruppen besagt, dass die Gruppe unter Komposition $\mathrm{Cl}_+(\mathrm{Prim}(\mathcal{Q}_D))$ in eindeutiger Weise (bis auf Isomorphie) das direkte Produkt primärer zyklischer Gruppen ist.

Die Struktur von $\mathrm{Cl}_+(\mathrm{Prim}(\mathcal{Q}_D))$ wird in §13 untersucht werden.

12 Die Geschlechtertheorie

Die Geschlechtertheorie wurde für den Versuch entwickelt, in einfacher Weise solche Primzahlen zu charakterisieren, die sich durch eine Form mit einer Fundamentaldiskriminanten darstellen lassen.

Genauer sei D eine Diskriminante und p eine Primzahl die $2D$ nicht teilt. Angenommen p lasse sich durch eine einfache Form mit Diskriminante D darstellen; mit anderen Worten, D ist quadratischer Rest

$4p$, also $\left(\frac{D}{p}\right) = +1$. Das Problem ist, durch Berechnung der Werte von p bei bestimmten quadratischen Charakteren zugehörig zu D zu entscheiden, welche einfachen Formen mit Diskriminante D die Primzahl p darstellen.

Wie wir sehen werden, gelangt die Geschlechtertheorie nicht ganz an ihr Ziel.

Wie in Abschnitt §3 bemerkt, ist für $D = -4$ und $Q = X^2 + Y^2$ die Primzahl p genau dann Summe zweier Quadrate, wenn $p = 2$ oder $p \equiv 1 \pmod 4$. In gleicher Weise gilt für $D = -12$, $Q = X^2 + 3Y^2$, dass p genau dann durch Q dargestellt wird, wenn $p = 3$ oder $p \equiv 1 \pmod 3$.

Allerdings war an früherer Stelle bemerkt worden, dass im Falle $D = -20$ die Klassenzahl $h_+(-20) = 2$ ist und dass es zwei reduzierte Formen mit Diskriminante -20 gibt, die nicht echt äquivalent sind, nämlich

$$Q_1 = X^2 + 5Y^2 \quad \text{und} \quad Q_2 = 2X^2 + 2XY + 3Y^2.$$

Jetzt:

$p = 5$ wird durch Q_1 dargestellt;

wenn $p \equiv 11, 13, 17, 19 \pmod{20}$, d.h. $\left(\frac{-5}{p}\right) = -1$, dann wird p weder durch Q_1 noch durch Q_2 dargestellt;

wenn $p \equiv 1, 3, 7, 9 \pmod{20}$, d.h. $\left(\frac{-5}{p}\right) = +1$, dann wird p durch Q_1 oder Q_2 dargestellt.

Es verbleibt zu entscheiden, welche der beiden Q_1 oder Q_2 eine gegebene Primzahl p des letzten Typs darstellt.

Dasselbe Problem tritt auch bei anderen Diskriminanten D auf für die $h_+(D) > 1$, und die Geschlechtertheorie unternimmt einen ernsthaften Versuch, dies zu lösen.

Sei D irgendeine Diskriminante (nicht notwendigerweise fundamental). Seien $q_1, \ldots, q_r$, $(r \geq 0)$ die verschiedenen ungeraden Primzahlen, die den quadratfreien Kern von D teilen. Die Nummerierung sei so, dass $q_1 \equiv \cdots \equiv q_s \equiv 1 \pmod 4$ und $q_{s+1} \equiv \cdots \equiv q_r \equiv -1 \pmod 4$ mit $0 \leq s \leq r$.

Für jedes m, für das q_i kein Teiler von m ist, sei $\chi_i(m) = \left(\frac{m}{q_i}\right)$ $(i = 1, \ldots, r)$, somit ist χ_i ein Charakter modulo q_i.

Für jede ungerade ganze Zahl m sei

$$\delta(m) = (-1)^{(m-1)/2} \quad \text{und} \quad \eta(m) = (-1)^{(m^2-1)/8}.$$

Wiederum ist δ ein Charakter modulo 4 und η ein Charakter modulo 8.

Jedem Typ von Diskriminante wird nun unter Beachtung folgender Regeln eine Menge von Charakteren zugeordnet:

Diskriminante	Zugeordnete Charaktere	$(\#, \#')$
$D \equiv 1 \pmod 4$	$\chi_1, \ldots, \chi_r$	(r, r)
$D = 4D'$, $D' \equiv 1 \pmod 4$	$\chi_1, \ldots, \chi_r$	$(r, r+1)$
$D = 4D'$, $D' \equiv 3 \pmod 4$	$\chi_1, \ldots, \chi_r$, δ	$(r+1, r+1)$
$D = 4D'$, $D' \equiv 2 \pmod 8$	$\chi_1, \ldots, \chi_r$, η	$(r+1, r+1)$
$D = 4D'$, $D' \equiv 6 \pmod 8$	$\chi_1, \ldots, \chi_r$, $\delta\eta$	$(r+1, r+1)$
$D = 4D'$, $D' = 4E^2 q_1 \cdots q_r$	$\chi_1, \ldots, \chi_s$, $\chi_{s+1}\delta, \ldots, \chi_r\delta$	$(r, r+1)$
$D = 4D'$, $D' = 8E^2 q_1 \cdots q_r$	$\chi_1, \ldots, \chi_s$, $\chi_{s+1}\delta, \ldots, \chi_r\delta$, η	$(r+1, r+1)$

$(\#, \#') = $ *(Anzahl zugeordneter Charaktere, Anzahl der Primteiler von D)*

Es ist praktisch, die Menge aller zugeordneten Charaktere jeweils mit Θ und ihre Mächtigkeit durch t zu bezeichnen.

Nach dem quadratischen Reziprozitätsgesetz gilt für $\mathrm{ggT}(m, 2D) = 1$

$$\prod_{\theta \in \Theta} \theta(m) = \left(\frac{D}{m}\right).$$

Man kann die folgenden Aussagen beweisen. Wenn $\mathrm{ggT}(m, 2D) = 1$ und m irgendein Wert von $Q \in \mathrm{Prim}(\mathcal{Q}_D)$ ist, dann $\left(\frac{D}{m}\right) = 1$. Wenn $\mathrm{ggT}(m', 2D) = 1$ und m' irgendein anderer Wert von Q ist, dann $\theta(m) = \theta(m')$ für jeden zugeordneten Charakter θ.

Dies gestattet es uns, $\theta(Q) = \theta(m)$ für jede ganze Zahl m und jeden zugeordneten Charakter θ zu definieren, wenn m durch Q dargestellt wird und wenn gilt $\mathrm{ggT}(m, 2D) = 1$.

Es folgt für $Q \approx Q'$ sofort, dass $\theta(Q) = \theta(Q')$ für jeden zugeordneten Charakter θ gilt, was es für jede echte Äquivalenzklasse und jeden zugeordneten Charakter θ erlaubt, $\theta(\mathbf{Q}) = \theta(Q)$ zu definieren.

Sei $\{+1, -1\}^t$ die multiplikative Gruppe von t-Tupeln ganzer Zahlen $+1$ oder -1 und definiere die Abbildung

$$\Xi : \mathrm{Cl}_+(\mathrm{Prim}(\mathcal{Q}_D)) \longrightarrow \{+1, -1\}^t$$

durch

$$\Xi(\mathbf{Q}) = (\theta(\mathbf{Q}))_{\theta \in \Theta}.$$

Es ist leicht zu zeigen, dass die Abbildung Ξ unter der Komposition ein Homomorphismus der Gruppe $\mathrm{Cl}_+(\mathrm{Prim}(\mathcal{Q}_D))$ in $\{+1, -1\}^t$ ist.

Man beachte, dass $\prod_{\theta\in\Theta}\theta(\mathbf{Q}) = 1$.

Es lässt sich zeigen, dass das Bild von Ξ die Menge aller $\sigma = (\sigma_1, \ldots, \sigma_t)$ mit $\sigma_i \in \{+1, -1\}$ ist, wobei $\prod_{i=1}^{t}\sigma_i = 1$. Die Bildmenge hat somit 2^{t-1} Elemente.

Für jedes σ im Bild von Ξ nennt man das Urbild

$$\Xi^{-1}(\sigma) = \{\mathbf{Q} \mid \Xi(\mathbf{Q}) = \sigma\},$$

von σ das *Geschlecht* von $\mathrm{Cl}_+(\mathrm{Prim}(\mathcal{Q}_D))$ mit generischem Charakter σ.

Das Geschlecht mit generischem Charakter $\sigma_1 = \{+1, \ldots, +1\}$ heißt das Hauptgeschlecht, es ist eine Untergruppe von $\mathrm{Cl}_+(\mathrm{Prim}(\mathcal{Q}_D))$. Jedes Geschlecht ist eine Nebenklasse des Hauptgeschlechts.

Es wird an einigen Stellen die folgende Bezeichnung verwendet werden: $[\mathbf{Q}]$ ist das Geschlecht der Klasse $\mathbf{Q}$.

Die Anzahl der Geschlechter ist $g(D) = 2^{t-1}$ und die Anzahl der Klassen in jedem Geschlecht ist $f(D) = \frac{h_+(D)}{2^{t-1}}$; insbesondere ist 2^{t-1} Teiler von $h_+(D)$.

Man beachte, dass wenn D eine Fundamentaldiskriminante ist, dann ist t gleich der Anzahl der verschiedenen Primfaktoren von D (einschließlich der 2, wenn D gerade ist).

Gauss bewies den folgenden wichtigen Satz, den man den Verdopplungssatz nennt:

Das Hauptgeschlecht besteht aus den Quadraten (unter Komposition) der echten Äquivalenzklassen einfacher Formen.

Aus obigen Betrachtungen lässt sich das folgende Kriterium gewinnen. Sei p eine Primzahl die $2D$ nicht teilt und sei $\mathcal{G}$ ein Geschlecht echter Äquivalenzklassen einfacher Formen mit Diskriminante D, sagen wir

$$\mathcal{G} = \{\mathbf{Q}_1, \ldots, \mathbf{Q}_k\}.$$

Dann wird p genau dann durch eine Form Q dargestellt, die zu einer der Klassen $Q_i \in \mathcal{G}(1 \le i \le k)$ gehört, wenn $(\theta(p))_{\theta\in\Theta} = \Xi(\mathbf{Q}_i)$.

Man beachte, dass wenn das Geschlecht mehr als eine echte Äquivalenzklasse hat, obiges Kriterium keine Auskunft darüber gibt, welche Form p unter denjenigen darstellt, deren Äquivalenzklasse im Geschlecht liegt.

Um noch einmal auf das Beispiel mit Diskriminante $D = -20$ mit den zwei Klassen $\mathbf{Q}_1 = \langle 1, 0, 5\rangle$ (der Hauptklasse) und $\mathbf{Q}_2 = \langle 2, 2, 3\rangle$ zurück zu kommen; man beachte, dass es $g(-20) = 2$ Geschlechter gibt, also sind $\mathbf{Q}_1$, $\mathbf{Q}_2$ in verschiedenen Geschlechtern.

Wenn p eine ungerade Primzahl ist mit $p \neq 5$, dann wird p genau dann durch Q_1 dargestellt, wenn $\left(\frac{p}{5}\right) = 1$ und $(-1)^{(p-1)/2} = 1$, also $p \equiv 1 \pmod 4$ und $p \equiv \pm 1 \pmod 5$, oder äquivalent, $p \equiv 1$ oder $9 \pmod{20}$.

In gleicher Weise gilt, dass p genau dann durch Q_2 dargestellt wird, wenn

$$(-1)^{(p-1)/2} = \chi_1(Q_2) = \chi_1(3) = (-1)^{(3-1)/2} = -1,$$

und

$$\left(\frac{p}{5}\right) = \chi_2(p) = \chi_2(Q_2) = \chi_2(2) = \left(\frac{2}{5}\right) = -1.$$

Somit $p \equiv 3 \pmod 4$ und $p \equiv \pm 2 \pmod 5$, oder äquivalent, $p \equiv 3, 7 \pmod{20}$.

Man beachte, dass die Geschlechtertheorie die Vermutung von Euler bezüglich der Form $X^2 + 5Y^2$ beweist.

Die Anwendung der Geschlechtertheorie ist im Falle, dass es mehr als eine Form in jedem Geschlecht gibt, nicht so aufschlussreich.

Zahlenbeispiel

Sei $D = -56 = -8 \times 7$.

Die Anzahl der Geschlechter ist 2.

Die reduzierten Formen sind $P = \langle 1, 0, 14\rangle$, $Q_1 = \langle 3, 2, 5\rangle$, $Q_2 = \langle 2, 0, 7\rangle$, $Q_3 = \langle 3, -2, 5\rangle$.

Eine einfache Rechnung zeigt, dass $\mathrm{Cl}_+(\mathrm{Prim}(\mathcal{Q}_{-56}))$ eine zyklische Gruppe mit $\mathbf{Q}_1^2 = \mathbf{Q}_2$, $\mathbf{Q}_1^3 = \mathbf{Q}_3$, $\mathbf{Q}_1^4 = \mathbf{P}$ ist.

Das Hauptgeschlecht ist $\{\mathbf{P}, \mathbf{Q}_2\}$ und das nicht-Hauptgeschlecht $\{\mathbf{Q}_1, \mathbf{Q}_3\}$; dies hat den generischen Charakter $\{-1, -1\}$. Daraus folgt, dass eine Primzahl $p \neq 2, 7$ durch P oder Q_2 genau dann dargestellt wird, wenn $\chi_1(p) = (-1)^{(P^2-1)/2} = 1$, d.h. $\left(\frac{2}{p}\right) = 1$ und $\left(\frac{p}{7}\right) = 1$; durch eine einfache Berechnung ergibt sich $p \equiv 1, 9, 15, 23, 25$ oder $39 \pmod{56}$. Aber es lässt sich keine Bedingung ableiten, dass p durch P dargestellt wird (bzw. durch Q_2).

In gleicher Weise gilt für $p \neq 2, 7$, dass p genau dann durch Q_1 oder durch Q_3 dargestellt wird, wenn $p \equiv 3, 5, 13, 19, 27, 45 \pmod{56}$.

Wie weiter unter erklärt wird, entwickelte sich aus der Arbeit von Euler über die „numeri idonei“ (auch „geeignete Zahlen“ genannt) und der Arbeit von Gauss Interesse für Fundamentaldiskriminanten mit $D < 0$, deren Hauptgeschlecht nur aus der Hauptklasse besteht.

Hier eine Liste der 65 bekannten Fundamentaldiskriminanten $D < 0$ für die gilt, dass das Hauptgeschlecht nur aus der Hauptklasse besteht:

$h_+(D)$	$-D$
1	3 4 7 8 11 19 43 67 163
2	15 20 24 35 40 51 52 88 91 115 123 148 187 232 235 267 403 427
4	84 120 132 168 195 228 280 312 340 372 408 435 483 520 532 555 595 627 708 715 760 795 1012 1435
8	420 660 840 1092 1155 1320 1380 1428 1540 1848 1995 3003 3315
16	5460

Bis heute sind keine weiteren solchen Fundamentaldiskriminanten bekannt! (Siehe §18 für eine genauere Diskussion diesbezüglich.)

Es sind zudem die folgenden 36 nicht-Fundamentaldiskriminanten mit nur aus der Hauptklasse bestehendem Hauptgeschlecht bekannt:

$$\begin{aligned}-D = {} & 3\times 2^2, 3\times 3^2, 3\times 4^2, 3\times 5^2, 3\times 7^2, 3\times 8^2, 4\times 2^2, 4\times 3^2,\\ & 4\times 4^2, 4\times 5^2, 7\times 2^2, 7\times 4^2, 7\times 8^2, 8\times 2^2, 8\times 3^2, 8\times 6^2,\\ & 11\times 3^2, 15\times 2^2, 15\times 4^2, 15\times 8^2, 20\times 3^2, 24\times 2^2, 35\times 3^2,\\ & 40\times 2^2, 88\times 2^2, 120\times 2^2, 168\times 2^2, 232\times 2^2,\\ & 280\times 2^2, 312\times 2^2, 408\times 2^2, 520\times 2^2, 760\times 2^2,\\ & 840\times 2^2, 1320\times 2^2, 1848\times 2^2.\end{aligned}$$

Aufgrund der Geschlechtertheorie ist es für jede der obigen Diskriminanten mithilfe der aufgezeigten Methode möglich zu zeigen, ob sich eine ungerade Primzahl durch eine der einfachen Formen mit dieser Diskriminante darstellen lässt oder nicht.

Es gibt eine interessante, von Gauss entdeckte Verbindung zwischen negativen Diskriminanten mit einer Klasse in jedem Geschlecht und Eulers geeigneten Zahlen, die definiert wurden, um große Primzahlen zu finden.

Die Definition geeigneter Zahlen bezieht sich auf ungerade ganze Zahlen $m \geq 1$ mit folgenden Eigenschaften:

(i) wenn x, y, x', y' nicht-negative ganze Zahlen derart sind, dass $x^2 + ny^2 = x'^2 + n(y')^2$, dann ist $(x', y') = (x, y)$ oder (y, x);

(ii) wenn x, y nicht-negative ganze Zahlen derart sind, dass $m = x^2 + ny^2$, dann ist $\mathrm{ggT}(x, y) = 1$.

Die ganze Zahl $n \geq 1$ ist eine *geeignete Zahl*, wenn sie die folgende Eigenschaft besitzt: Jede ungerade ganze Zahl $m \geq 1$, die zu n teilerfremd ist und obigen Bedingungen (i) und (ii) genügt, ist eine Primzahl.

Gauss zeigte:

Sei $n \geq 1$ eine ganze Zahl. Dann besteht das Hauptgeschlecht der Fundamentaldiskriminanten $D = -4n$ genau dann aus nur aus einer Klasse, wenn n eine geeignete Zahl ist.

Somit sind die 65 bekannten geeigneten Zahlen: 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.

Weitere Informationen über geeignete Zahlen finden sich in Frei (1985, 1984); Steinig (1966).

Es gibt noch weitere Möglichkeiten, um zu zeigen, dass zwei Formen zum selben Geschlecht gehören. Um diese Bedingungen ausdrücken zu können, wird der Begriff der Äquivalenz folgendermaßen erweitert.

Sei R einer der folgenden Ringe:

(1) $R = \mathbb{Z}_{(n)}$ (der Ring der rationalen Zahlen mit einem zu n teilerfremden Nenner);

(2) $R = \mathbb{Z}_p$ (der Ring der p-adischen ganzen Zahlen, mit einer Primzahl p);

(3) $R = \mathbb{Z}/m\mathbb{Z}$ (der Ring der Restklassen modulo $m \geq 2$).

In jedem Fall sei $\lambda : \mathbb{Z} \to R$ der natürliche Ringhomomorphismus; in den Fällen (1), (2) ist λ die Einbettung und in Fall (3) die Restabbildung. Für $Q = \langle a, b, c\rangle$ sei $\lambda Q = \langle \lambda(a), \lambda(b), \lambda(c)\rangle = \lambda(a)X^2 + \lambda(b)XY + \lambda(c)Y^2$ die zugehörige binär-quadratische Form über dem Ring R. Somit lassen sich in den Fällen (1) und (2) Q und λQ bestimmen.

Die Formen $Q = \langle a, b, c\rangle$, $Q' = \langle a', b', c'\rangle$ nennt man *R-äquivalent*, wenn es $A = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \in \mathrm{GL}_2(R)$ derart gibt, dass $\lambda Q' = T_A(\lambda Q)$. In den Fällen (1), (2) bedeutet dies (gemäß kanonischer Einbettung), dass Bedingungen $(*)$ von §6 erfüllt sind. Im Fall (3) werden diese Gleichheiten zu Kongruenzen modulo m. Die Bezeichnung ist $Q \sim Q'$ (über R).

In ähnlicher Weise nennt man $\rho \in R$ einen *Wert* von Q, wenn es α, $\gamma \in R$ derart gibt, dass $(\lambda Q)(\alpha, \gamma) = \rho$. Zum Beispiel ist $r \pmod m \in \mathbb{Z}/m\mathbb{Z}$ ein Wert von Q, wenn es ganze Zahlen x, y mit $Q(x, y) \equiv r \pmod m$ gibt.

Jede der folgenden äquivalenten Bedingungen charakterisiert den Fall, dass zwei Formen Q, $Q' \in \mathcal{Q}_D$ im selben Geschlecht sind:

(i) Q, Q' haben für alle $m \geq 2$ dieselbe Menge von Werten in jedem $\mathbb{Z}/m\mathbb{Z}$;

(ii) $Q \sim Q'$ (über $\mathbb{Z}/m\mathbb{Z}$) für alle $m \geq 2$;

(iii) $Q \sim Q'$ (über $\mathbb{Z}_p$) für alle Primzahlen p;

(iv) $Q \sim Q'$ (über $\mathbb{Z}_{(n)}$) für jedes $n \geq 2$.

Diese Ergebnisse sind die Eckpfeiler einer umfassenden Theorie quadratischer Formen, die an dieser Stelle nicht entwickelt werden soll.

13 Die Struktur der Gruppe von echten Äquivalenzklassen einfacher Formen

Sei D irgendeine Diskriminante.

Man rufe sich in Erinnerung, dass $\mathrm{Cl}_+(\mathrm{Prim}(\mathcal{Q}_D))$ eine endliche abelsche Gruppe ist. Als solche ist sie das direkte Produkt ihrer p-Sylow-Untergruppen S_p für jeden Primteiler p von $h_+(D)$. Jede nichttriviale p-Sylow-Untergruppe ist wiederum das direkte Produkt von $k(p) \geq 1$ zyklischer p-Gruppen. Die eindeutig definierte ganze Zahl $k(p)$ nennt man den *p-Rang* der Gruppe $\mathrm{Cl}_+(\mathrm{Prim}(\mathcal{Q}_D))$.

Betrachte zunächst die Primzahl $p = 2$. Die 2-Sylow-Untergruppe S_2 enthält die Untergruppe $\mathcal{A}$ der zweideutigen Klassen (die Klassen mit einer die 2 teilenden Ordnung).

Gauss zeigte, dass die Ordnung von $\mathcal{A}$ gleich der Anzahl $g(D) = 2^{t-1}$ der Geschlechter ist (t bezeichnet die Anzahl der zugeordneten Charaktere von D, diese ist gleich der Anzahl der Primteiler von D, wenn D eine Fundamentaldiskriminante ist). Eine klare und detaillierte Darstellung seines Beweises findet sich zum Beispiel im Buch von Flath (1989).

Die einzige zweideutige Klasse ist die Hauptklasse genau dann, wenn $D = p$ oder $4p$, wobei p eine ungerade Primzahl ist mit $p \equiv 1 \pmod 4$.

Man kann leicht nachvollziehen, dass wenn ein nicht-Hauptgeschlecht eine zweideutige Klasse $\mathbf{Q}$ enthält, dann gibt es eine Bijektion zwischen der Menge $\mathcal{A} \cap [\mathbf{P}]$ zweideutiger Klassen im Hauptgeschlecht und der Menge $\mathcal{A} \cap [\mathbf{Q}]$.

Das Hauptgeschlecht $[\mathbf{P}]$ kann zyklisch sein oder auch nicht. Wenn es zyklisch ist und eine gerade Ordnung hat, dann hat $\mathcal{A} \cap [\mathbf{P}]$ nur zwei Klassen, und so hat jedes Geschlecht entweder keine zweideutige Klasse oder genau zwei zweideutige Klassen—dies passiert für genau die Hälfte

aller Geschlechter. Wenn allerdings **P** die einzige zweideutige Klasse in $\mathcal{A} \cap [\mathbf{P}]$ ist, dann hat jedes Geschlecht genau eine zweideutige Klasse.

Wenn das Hauptgeschlecht nicht zyklisch ist, sei $e(D)$ das Maximum der Ordnungen seiner Klassen; also $e(D) < f(D)$ (die Ordnung des Hauptgeschlechts) und tatsächlich ist $e(D)$ ein Teiler von $f(D)$.

Gauss nannte D eine *reguläre* Diskriminante, wenn das Hauptgeschlecht zyklisch ist; ansonsten heißt D *irregulär* und $f(D)/e(D)$ ist ihr *Irregularitätsindex*.

Wenn zum Beispiel das Hauptgeschlecht 3 oder mehr zweideutige Klassen enthält, dann ist D irregulär und der Irregularitätsindex ist gerade. Wenn die Anzahl der zweideutigen Klassen im Hauptgeschlecht gleich 1 oder 2 ist, dann ist $f(D)/e(D)$ ungerade (aber nicht notwendigerweise gleich 1).

In Artikel 306 der *Disquisitiones Arithmeticae* gibt Gauss unendlich viele negative Diskriminanten mit einem durch 3 teilbaren Irregularitätsindex an, diese sind

$$\begin{aligned} D &= -(216k + 27), \quad \text{mit } k \geq 1, \\ D &= -(1000k + 75), \quad \text{mit } k \geq 1, \\ &\text{usw.}\ldots. \end{aligned}$$

Er notierte auch die folgenden Beispiele:

$-D = 576, 580, 820, 884, 900$, mit Irregularitätsindex 2,
$-D = 243, 307, 339, 459, 675, 755, 891, 974$, mit Irregularitätsindex 3.

Gauss gab nur ein Beispiel einer irregulären positiven Diskriminanten an: $D = 3026$; sie hat den Irregularitätsindex 2.

Sei nun p eine ungerade Primzahl. Gauss hat nichts über den p-Rang der Klassengruppe ausgesagt. Ich werde auf diesen Punkt im Abschnitt §20 zurückkommen.

14 Berechnungen und Vermutungen

Gauss stellte viele Berechnungen zu den Formen $\langle a, 2b, c\rangle$, an, auf die er seine Aufmerksamkeit konzentriert hatte. Allerdings lassen sich seine Resultate auch für beliebige Formen verwenden.

Für Fundamentaldiskriminanten $-3000 < D < 0$ ermittelte er:

$h_+(D) = 1$ genau dann, wenn $-D = 3, 4, 7, 8, 11, 19, 43, 67, 163$ (dies sind 9 Werte);

$h_+(D) = 2$ genau dann, wenn $-D$ aus einer Menge von 18 Werten stammt, von denen der größte 427 ist;

$h_+(D) = 3$ genau dann, wenn $-D$ aus einer Menge von 16 Werten stammt, von denen der größte 907 ist; usw. ...

Aufgrund seiner Berechnungen vermutete Gauss (siehe *Disquisitiones Arithmeticae*, Artikel 303):

Hypothese 1. Es gibt nur 9 Fundamentaldiskriminanten $D < 0$ derart, dass $h_+(D) = 1$.

Hypothese 2. Für jedes $n \geq 2$ gibt es nur endlich viele Fundamentaldiskriminanten $D < 0$ derart, dass $h_+(D) = n$. Insbesondere gibt es für $n = 2$ nur 18 Werte, für $n = 3$ nur 16 Werte, usw. ...

Um genau zu sein, wird die Vermutung dann bewiesen sein, wenn man einen Algorithmus finden kann, der es ermöglicht, alle Diskriminanten $D < 0$ zu finden, für die gilt $h_+(D) = n$.

Bezüglich echter Äquivalenzklassen indefiniter Formen mit Fundamentaldiskriminante $D > 0$ vermutet man allgemein Folgendes (siehe auch *Disquisitiones Arithmeticae*, Artikel 304):

Hypothese 3. Es gibt unendlich viele Fundamentaldiskriminanten $D > 0$ derart, dass $h_+(D) = 1$.

In Zusammenhang mit der Anzahl der Klassen im Hauptgeschlecht vermutete Gauss (Artikel 303):

Hypothese 4. Für jede ganze Zahl $m \geq 1$ gibt es nur endlich viele Diskriminanten $D < 0$ derart, dass die Anzahl der Klassen im Hauptgeschlecht von D gleich m ist.

Dies kann man auch folgendermaßen ausdrücken:

$$\lim_{|D| \to \infty} f(D) = \infty$$

($f(D)$ ist die Anzahl der Klassen im Hauptgeschlecht von D).

Gauss fiel durch Rechnungen an Zahlenbeispielen auf, dass die Anzahl der positiven Diskriminanten D mit $f(D) = 1$ bei wachsendem D

immer seltener werden. Er vermutete, dass es unendlich viele solcher Diskriminanten gibt und warf das Problem auf, das Verhalten von

$$\frac{\{\#\{D \mid 1 \leq D \leq N, f(D) = 1\}}{N}$$

für $N \to \infty$ zu studieren.

Wir werden sehen, dass die Vermutungen 1, 2 und 4 inzwischen bewiesen sind, nur noch Vermutung 3 ist nach wie vor offen.

15 Die Zeit nach Gauß

Die ergiebige Theorie, die Gauss entwickelt und im Alter von nur 24 Jahren in den *Disquisitiones Arithmeticae* veröffentlicht hatte, war von nachhaltiger Bedeutung. Ihre Darstellung erforderte den ganzen Abschnitt V des Buches und füllte über 250 Seiten. Gauss' Text enthält viele Zahlenbeispiele und Algorithmen, verdeutlicht und ergänzt die früheren Ergebnisse von Fermat, Euler, Legendre und besonders von Lagrange. Ich habe hier nur einige wenige Aspekte seiner Untersuchungen berührt.

In der Zeit nach der Veröffentlichung von Gauss' Theorie folgte die analytische Arbeit Dirichlets zur Berechnung der Anzahl von echten Äquivalenzklassen einfacher Formen einer gegebenen Diskriminante und später die von Klein entwickelte geometrische Theorie über Formen.

Darüber hinaus erschien Dedekinds weitreichende Interpretation. Um eine durchschaubare Erläuterung der Komposition von echten Äquivalenzklassen einfacher Formen bereitzustellen, begründete Dedekind eine Verbindung zwischen Formen und Idealen in quadratischen Zahlkörpern; siehe Dedekinds Ergänzungen zu Dirichlets *Vorlesungen über Zahlentheorie*.

16 Formen im Vergleich zu Idealen in quadratischen Zahlkörpern

Um den Zusammenhang zwischen Formen und Idealen in quadratischen Zahlkörpern zu erläutern, beginne ich damit, einige Tatsachen in Erinnerung zu rufen.

Sei $d \neq 0, 1$ eine quadratfreie ganze Zahl und sei $K = \mathbf{Q}(\sqrt{d})$ der zugehörige quadratische Zahlkörper, der aus den Elementen $\alpha = x + y\sqrt{d}$ besteht, wobei $x, y \in \mathbf{Q}$.

Die *Diskriminante* von K ist definiert als

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

Also ist D_K eine Fundamentaldiskriminante.

Dadurch sind Bijektionen zwischen der Menge der quadratfreien Zahlen $d \neq 0$, 1, der Menge quadratischer Zahlkörper und der Menge von Fundamentaldiskriminanten definiert.

Sei

$$\omega = \begin{cases} \frac{1+\sqrt{d}}{2} & \text{wenn } d \equiv 1 \pmod 4, \\ \sqrt{d} & \text{wenn } d \equiv 2 \text{ oder } 3 \pmod 4. \end{cases}$$

Dann ist $\{1, \omega\}$ Basis des $\mathbf{Q}$-Vektorraums K, also lässt sich jedes Element α von K in eindeutiger Weise in der Form $\alpha = x + y\omega$ mit x, $y \in \mathbf{Q}$ schreiben.

Die *Konjugierte* von $\alpha = x + y\sqrt{d}$ $(x, y \in \mathbf{Q})$ ist $\bar{\alpha} = x - y\sqrt{d}$, die Norm von α gleich $N(\alpha) = \alpha\bar{\alpha} = x^2 - y^2 d \in \mathbf{Q}$. Insbesondere,

$$\bar{\omega} = \begin{cases} \frac{1-\sqrt{d}}{2} & \text{wenn } d \equiv 1 \pmod 4, \\ -\sqrt{d} & \text{wenn } d \equiv 2 \text{ oder } 3 \pmod 4, \end{cases}$$

und

$$N(\omega) = \begin{cases} \frac{1-d}{4} & \text{wenn } d \equiv 1 \pmod 4, \\ -d & \text{wenn } d \equiv 2 \text{ oder } 3 \pmod 4. \end{cases}$$

Wenn $\alpha \in K$ mittels der Basis $\{1, \omega\}$ ausgedrückt wird, so

$$N(x + y\omega) = \begin{cases} x^2 + xy + \frac{1-d}{4}y^2 & \text{wenn } d \equiv 1 \pmod 4, \\ x^2 - y^2 d & \text{wenn } d \equiv 2 \text{ oder } 3 \pmod 4. \end{cases}$$

Das Element $\alpha \in K$ nennt man eine *algebraische ganze Zahl*, wenn es die Nullstelle eines quadratischen normierten Polynoms $X^2 - aX + b \in \mathbb{Z}[X]$ ist. In diesem Fall ist $a = \alpha + \bar{\alpha}$ und $N(\alpha) = \alpha\bar{\alpha} = b \in \mathbb{Z}$.

Die Menge algebraischer ganzer Zahlen von K ist ein Unterring von K, der mit $\mathcal{O}_K$ bezeichnet wird. Offensichtlich ist $\mathbb{Z} \subset \mathcal{O}_K$, K ist der Körper der Quotienten von $\mathcal{O}_K$ und $\mathcal{O}_K = \mathbb{Z} \oplus \mathbb{Z}\omega$, also ist $\mathcal{O}_K$ ein freies $\mathbb{Z}$-Modul vom Rang 2.

Obiger Zusammenhang für Fundamentaldiskriminanten lässt sich auf alle möglichen Diskriminanten $D \equiv 0$ oder $1 \pmod 4$ erweitern; sie korrespondieren bijektiv mit Ordnungen in quadratischen Zahlkörpern, dies werde ich nun vorstellen.

Eine *Ordnung* von K ist ein Unterring $\mathcal{O}$ von K, der ein freies $\mathbb{Z}$-Modul vom Rang 2 ist. Somit gilt $\mathbb{Z} \subset \mathcal{O}$, K ist der Körper der Quotienten von $\mathcal{O}$ und es gibt zwei Elemente α, $\beta \in \mathcal{O}$ derart, dass sich jedes $\gamma \in \mathcal{O}$ auf eindeutige Weise in der Form $\gamma = x\alpha + y\beta$ mit x, $y \in \mathbb{Z}$ schreiben lässt. Dies wird durch $\mathcal{O} = \mathbb{Z}\alpha \oplus \mathbb{Z}\beta$ ausgedrückt.

Insbesondere ist der Ring algebraischer ganzer Zahlen $\mathcal{O}_K$ eine Ordnung von K.

Die *Diskriminante* irgendeines freien $\mathbb{Z}$-Moduls $\mathbb{Z}\alpha \oplus \mathbb{Z}\beta$ ist nach Definition gleich

$$\det \begin{pmatrix} \alpha & \beta \\ \bar{\alpha} & \bar{\beta} \end{pmatrix}^2 .$$

Sie ist unabhängig von der Wahl der Basis.

Die Diskriminante einer Ordnung $\mathcal{O}$ wird mit $\mathrm{Diskr}(\mathcal{O})$ bezeichnet und ist eine ganze Zahl kongruent zu 0 oder 1 modulo 4. Insbesondere ist die Diskriminante der Ordnung $\mathcal{O}_K$ aller algebraischen ganzen Zahlen von K $\mathrm{Diskr}(\mathcal{O}_K) = D_K$.

Die Diskriminante stellt eine Abbildung von der Menge der Ordnungen quadratischer Zahlkörper in die Menge ganzer Zahlen kongruent 0 oder 1 modulo 4 (die keine Quadrate sind) dar. Umgekehrt sei für den Fall $D \equiv 0$ oder $1 \pmod 4$ (D kein Quadrat) $D = f^2 D_0$, wobei $f \geq 1$ und D_0 eine Fundamentaldiskriminante ist. Sei K der quadratische Zahlkörper mit Diskriminante $D_K = D_0$. Dann ist $\mathcal{O}(D) = \mathbb{Z} \oplus \mathbb{Z}\frac{D+\sqrt{D}}{2}$ eine Ordnung von K mit $\mathrm{Diskr}(\mathcal{O}(D)) = D$; f nennt man *Leiter* der Ordnung $\mathcal{O}(D)$. Somit, $\mathcal{O}_K = \mathcal{O}(D_K)$.

Man beachte, dass

$$\mathcal{O}(D) = \left\{ \frac{x + y\sqrt{D}}{2} \mid x, y \in \mathbb{Z}, \quad x \equiv yD \pmod 2 \right\}.$$

Dies stellt eine Bijektion zwischen der Menge der Ordnungen quadratischer Zahlkörper und der Menge nichtquadratischer ganzer Zahlen kongruent 0 oder 1 modulo 4 dar.

Darüberhinaus, wenn $D = f^2 D_0$, $D' = e^2 D_0$ und e Teiler von f mit $e < f$ ist, so $\mathcal{O}(D) \subset \mathcal{O}(D')$. Insbesondere ist $\mathcal{O}_K$ die einzige maximale Ordnung im Körper K mit Diskriminante $D_K = D_0$.

Für jedes $D = f^2 D_K$ ist die additive Quotientengruppe $\mathcal{O}_K/\mathcal{O}(D)$ endlich und hat f Elemente.

Ein *gebrochenes Ideal* I der Ordnung $\mathcal{O} = \mathcal{O}(D)$ ist eine additive Untergruppe von K mit

(1) $\alpha I \subseteq I$ für jedes $\alpha \in \mathcal{O}$,
(2) es gibt ein Element $\delta \in \mathcal{O}$ ungleich Null mit $\delta I \subseteq \mathcal{O}$.

Jedes gebrochene Ideal I ungleich Null von $\mathcal{O}$ gestattet eine Basisdarstellung aus zwei Zahlen α, $\beta \in I$, d.h., $I = \mathbb{Z}\alpha \oplus \mathbb{Z}\beta$.

Für jedes $\alpha \in K$ ist die Menge $\mathcal{O}\alpha = \{\beta\alpha \mid \beta \in \mathcal{O}\}$ ein gebrochenes Ideal der Ordnung $\mathcal{O}$, genannt das durch α definierte *Hauptideal*. Insbesondere ist $\mathcal{O} = \mathcal{O}1$ das *Einheitsideal*, $0 = \mathcal{O}0$ das *Nullideal*.

Wenn I ein gebrochenes Ideal von $\mathcal{O}$ ist, dann gilt dies auch für das *Konjugierte* $\bar{I} = \{\bar{\alpha} \mid \alpha \in I\}$. Wenn I, J gebrochene Ideale $\mathcal{O}$ sind, so sei $I \cdot J = \{\sum_{i=1}^{n} \alpha_i \beta_i \mid \alpha_i \in I, \beta_i \in I, n \geq 1\}$. Dann ist $I \cdot J$ auch ein gebrochenes Ideal von $\mathcal{O}$. Die Multiplikation gebrochener Ideale ist eine assoziative und kommutative Operation mit Einheitsideal als Einheitselement. Zudem gilt $\mathcal{O}\alpha \cdot \mathcal{O}\beta = \mathcal{O}\alpha\beta$ für jedes $\alpha, \beta \in K$.

Das Produkt $I \cdot \bar{I}$ ist ein gebrochenes Hauptideal von $\mathbb{Z}$, erzeugt von einer eindeutig bestimmten positiven rationalen Zahl $l > 0$: $I \cdot \bar{I} = \mathcal{O}l$; nach Definition ist $N(I) = l$ die *Norm* von I. Offensichtlich ist $N(I \cdot J) = N(I)N(J)$ und $N(\mathcal{O}\alpha) = |N(\alpha)|$.

Wenn $\{\alpha, \beta\}$ irgendeine Basis von I ist, dann gilt $(\alpha\bar{\beta} - \bar{\alpha}\beta)^2 = N(I)^2 D$.

Ein gebrochenes Ideal I von $\mathcal{O} = \mathcal{O}(D)$ nennt man *invertierbar*, wenn es ein gebrochenes Ideal J derart gibt, dass $I \cdot J = \mathcal{O}$.

Die folgenden Aussagen über ein gebrochenes nicht-Nullideal I von $\mathcal{O}$ sind äquivalent:

(1) I ist invertierbar.
(2) $\mathcal{O} = \{\alpha \in K \mid \alpha I \subseteq I\}$.

Wenn $\mathrm{ggT}(N(I), f) = 1$, dann ist I invertierbar.

Insbesondere gilt im Falle $f = 1$, dass alle gebrochenen Nicht-Nullideale von $\mathcal{O}(D_K)$ invertierbar sind.

Wenn I, J invertierbare gebrochene Ideale von $\mathcal{O}$ sind und $I \subseteq J$, dann gibt es ein gebrochenes Ideal $J' \subseteq \mathcal{O}$ derart, dass $I = JJ'$ und somit ist $N(J)$ Teiler von $N(I)$. Insbesondere ist $N(J)$ für jedes $\alpha \in K$, $\alpha \neq 0$ für den Fall $\alpha \in J$ ein Teiler von $N(\alpha)$.

Es bezeichne $\mathcal{I} = \mathcal{I}(\mathcal{O}(D))$ die Menge aller invertierbaren gebrochenen Ideale von $\mathcal{O}(D)$; somit ist $\mathcal{I}$ eine multiplikative Gruppe, die die Untergruppen

$$\mathcal{P} = \mathcal{P}(\mathcal{O}(D)) = \{\mathcal{O}\alpha \mid \alpha \in K, \alpha \neq 0\}$$

und

$$\mathcal{P}_+ = \mathcal{P}_+(\mathcal{O}(D)) = \{\mathcal{O}\alpha \mid \alpha \in K, \alpha \neq 0, N(\alpha) > 0\}$$

enthält.

Die *Äquivalenz* von invertierbaren Idealen I, $J \in \mathcal{I}$ ist wie folgt definiert: $I \sim J$, wenn es ein $\alpha \in K$, $\alpha \neq 0$ derart gibt, dass $I = J \cdot \mathcal{O}\alpha$. Die Menge der Äquivalenzklassen invertierbarer Ideale von $\mathcal{O}$ wird mit $\mathrm{Cl}(\mathcal{O}(D))$ bezeichnet, die Äquivalenzklasse von I mit $\mathrm{cl}(I)$. Wenn $I \sim I'$ und $J \sim J'$, dann $I \cdot J \sim I' \cdot J'$. Dies gestattet es uns, die Operation $\mathrm{cl}(I) \cdot \mathrm{cl}(J) = \mathrm{cl}(I \cdot J)$ zu definieren.

Mit dieser Operation ausgestattet wird $\mathrm{Cl}(\mathcal{O}(D))$ zu einer Abelschen Gruppe, die isomorph zur Quotientengruppe $\mathcal{I}/\mathcal{P}$ ist.

Die *strikte Äquivalenz* invertierbarer Ideale I, $J \in \mathcal{I}$ ist wie folgt definiert: $I \approx J$, wenn es $\alpha \in K$ mit $N(\alpha) > 0$ derart gibt, dass $I = J \cdot \mathcal{O}\alpha$. Die Menge strikter Äquivalenzklassen invertierbarer Ideale von $\mathcal{O}$ wird mit $\mathrm{Cl}_+(\mathcal{O}(D))$ bezeichnet, die strikte Äquivalenzklasse von I mit $cl_+(I)$. Wieder gilt, dass wenn $I \approx I'$, $J \approx J'$, dann $I \cdot J \approx I' \cdot J'$, was es uns erlaubt, die Operation $\mathrm{cl}_+(I) \cdot \mathrm{cl}_+(J) = \mathrm{cl}_+(I \cdot J)$ einzuführen. Mit dieser Operation ist $\mathrm{Cl}_+(\mathcal{O}(D))$ eine Abelsche Gruppe isomorph zu $\mathcal{T}/\mathcal{P}_+$.

Die Abbildung $\mathrm{cl}_+(I) \mapsto \mathrm{cl}(I)$ von $\mathrm{Cl}_+(\mathcal{O})$ in $\mathrm{Cl}(\mathcal{O})$ ist ein surjektiver Homomorphismus mit einem Kern, der aus einem oder zwei Elementen besteht.

Im Gegensatz zur unendlichen Gruppe $\mathcal{T}(\mathcal{O}(D))$ ist die Gruppe $\mathrm{Cl}_+(\mathcal{O}(D))$ endlich, somit gilt dies auch für $\mathrm{Cl}(\mathcal{O}(D))$. Dieses wichtige Ergebnis bildet in Dedekinds Auslegung das Gegenstück zur Endlichkeit der Gruppe $\mathrm{Cl}_+(\mathrm{Prim}(D))$, was ich in Kürze erläutern werde.

Die Anzahl der Elemente in $\mathrm{Cl}(\mathcal{O}(D))$ wird mit $h(\mathcal{O}(D))$ bezeichnet und *Klassenzahl* der Ordnung $\mathcal{O}(D)$ genannt. Die Anzahl der Elemente von $\mathrm{Cl}_+(\mathcal{O}(D))$ nennt man die *strikte Klassenzahl* von $\mathcal{O}(D)$, bezeichnet mit $h_+(\mathcal{O}(D))$.

Mit obigem Homomorphismus, $h((\mathcal{O}(D)) \leq h_+((\mathcal{O}(D)) \leq 2h((\mathcal{O}(D))$. Der genaue Zusammenhang zwischen der Klassenzahl und der strikten Klassenzahl einer Ordnung wird noch präzisiert.

Die folgenden Aussagen über Ordnungen werden an späterer Stelle benötigt.

Ein Element $\alpha \in \mathcal{O} = \mathcal{O}(D)$ mit $\alpha^{-1} \in \mathcal{O}$ heißt eine *Einheit* von $\mathcal{O}$. Wenn $\alpha \in \mathcal{O}$ und es $k \geq 1$ gibt mit $\alpha^k = 1$, dann ist α eine Einheitswurzel und zudem eine Einheit. Die Menge $U = U(\mathcal{O}(D))$ der Einheiten von $\mathcal{O}$ bildet eine multiplikative Gruppe. Wenn α eine Einheit ist, so gilt dies auch für $\bar{\alpha}$ und $N(\alpha\bar{\alpha}) = \pm 1$.

Man betrachte die Situation im Fall maximaler Ordnung $\mathcal{O}(D_K)$.

Für $d < 0$ ist die Gruppe der Einheiten von $\mathcal{O}(D_K)$ endlich, so dass jede Einheit eine Einheitswurzel ist. Es bezeichne w die Anzahl der Einheiten. Dann

$$w = \begin{cases} 4 & \text{wenn } d = -1; \quad \text{die Einheiten sind } \pm 1, \pm\sqrt{-1} \\ 6 & \text{wenn } d = -3; \quad \text{die Einheiten sind } \pm 1, (\pm 1 \pm \sqrt{-3})/2 \\ 2 & \text{wenn } d \neq -1, -3; \quad \text{die Einheiten sind } \pm 1. \end{cases}$$

Wenn $D_K > 0$, dann gibt es eine eindeutige Einheit $\epsilon > 1$ derart, dass

$$U = \{\pm\epsilon^k \mid k \in \mathbb{Z}\}.$$

Die Einheit ϵ nennt man die *Fundamentaleinheit* von $\mathcal{O}(D_K)$. Die einzigen Einheitswurzeln sind ± 1.

Wegen $U(\mathcal{O}(D)) = U(\mathcal{O}(D_K)) \cap \mathcal{O}(D)$ ist $U(\mathcal{O}(D))$ für $D_K < 0$ endlich und besteht nur aus Einheitswurzeln. Wenn $D_K > 0$, dann gibt es ein kleinstes $t \geq 1$ derart, dass $\epsilon^t \in \mathcal{O}(D)$ und $U(\mathcal{O}(D)) = \{\pm\epsilon^{tk} \mid k \geq 1\}$; ϵ^t ist die Fundamentaleinheit von $\mathcal{O}(D)$.

Die Fundamentaleinheiten können eine Norm von 1 oder -1 haben, wobei beide Fälle auftreten.

Wenn $D_K \equiv 1 \pmod 4$, dann ist $D_K = d$ quadratfrei; die Fundamentaleinheit $\epsilon = \frac{x_1 + y_1\sqrt{d}}{2}$ (mit $x_1, y_1 \geq 1$, $x_1 \equiv y_1 \pmod 2$) ist derart, dass $x_1^2 - y_1^2 d = \pm 4$; darüberhinaus gilt für jedes Paar (x, y), $x, y \geq 1$ mit $x^2 - y^2 d = \pm 4$ notwendigerweise $x_1 + x + y_1\sqrt{d} < x + y\sqrt{d}$.

Wenn $D_K \equiv 0 \pmod 4$, dann $D_K = 4d$ mit $d \equiv 2, 3 \pmod 4$; die Fundamentaleinheit $\epsilon = x_1 + y_1\sqrt{d}$ (mit $x_1, y_1 \geq 1$) ist derart, dass $x_1^2 - y_1^2 d = \pm 1$ und $x_1 + y_1\sqrt{d} < x + y\sqrt{d}$, sobald $x, y \geq 1$, $x^2 - y^2 d = \pm 1$.

Diese Theorie wurde von LAGRANGE entwickelt.

Der Zusammenhang zwischen der Klassenzahl und der strikten Klassenzahl der Ordnung $\mathcal{O}(D)$ ist der Folgende:

(1) Wenn $D < 0$ oder $D > 0$ und die Fundamentaleinheit von $\mathcal{O}(D)$ die Norm -1 hat, dann $h_+(\mathcal{O}(D)) = h(\mathcal{O}(D))$.

(2) Wenn $D > 0$ und die Fundamentaleinheit die Norm 1 hat, dann $h_+(\mathcal{O}(D)) = 2h(\mathcal{O}(D))$.

Ich werde nun auf die wichtige Verbindung zwischen echten Äquivalenzklassen einfacher Formen und strikten Äquivalenzklassen invertierbarer gebrochener Ideale von Ordnungen eingehen.

Sei $D \equiv 0, 1 \pmod 4$ (D kein Quadrat), also $D = f^2 D_0$, wobei D_0 eine Fundamentaldiskriminante ist. Sei $K = \mathbf{Q}(\sqrt{D_0})$, die Diskriminante ist somit $D_K = D_0$. Sei $\mathcal{O} = \mathcal{O}(D)$ und sei $I \in \mathcal{I}(\mathcal{O})$, d.h. I ist ein invertierbares gebrochenes Ideal der Ordnung $\mathcal{O}$ verschieden vom Nullideal. Somit hat I die Basis $\{\alpha, \beta\}$, und damit

$$\det \begin{pmatrix} \alpha & \beta \\ \bar{\alpha} & \bar{\beta} \end{pmatrix} = \alpha\bar{\beta} - \bar{\alpha}\beta \neq 0.$$

Da $\frac{\alpha\bar{\beta} - \bar{\alpha}\beta}{\sqrt{d}}$ gleich seiner Konjugierten ist, handelt es sich um eine rationale Zahl. Damit ist entweder $\alpha\bar{\beta} - \bar{\alpha}\beta > 0$ oder $\beta\bar{\alpha} - \bar{\beta}\alpha > 0$. Es ist also möglich, ein Paar (α, β) derart zu wählen, dass $I = \mathbb{Z}\alpha \oplus \mathbb{Z}\beta$ und $\alpha\bar{\beta} - \bar{\alpha}\beta > 0$; (α, β) nennt man eine *positiv orientierte* Basis für I.

Da $\mathcal{O}\alpha \subseteq I$ und $\mathcal{O}\beta \subseteq I$ folgt, dass $N(I)$ Teiler von $N(\alpha)$ und $N(\beta)$ ist. Aber $N(I)^2$ teilt

$$(\alpha\bar{\beta} - \bar{\alpha}\beta)^2 = (\alpha\bar{\beta} + \bar{\alpha}\beta)^2 - 4N(\alpha)N(\beta),$$

also ist $N(I)$ Teiler von $\alpha\bar{\beta} + \bar{\alpha}\beta$.

Sei

$$Q = \left\langle \frac{N(\alpha)}{N(I)}, \frac{\alpha\bar{\beta} + \bar{\alpha}\beta}{N(I)}, \frac{N(\beta)}{N(I)} \right\rangle,$$

d.h. Q hat eine Diskriminante gleich D.

Man beachte, dass Q von der Wahl der positiv orientierten Basis $\{\alpha, \beta\}$ abhängt; dies wird durch die Schreibweise $Q = Q_{(\alpha,\beta)}$ gekennzeichnet. Wenn $\{\alpha', \beta'\}$ eine weitere positiv orientierte Basis von I ist, so kann man zeigen, dass $Q_{(\alpha,\beta)}$ und $Q_{(\alpha',\beta')}$ echt äquivalent sind. In gleicher Weise gilt, dass wenn die Ideale I, $I' \in \mathcal{I}$ strikt äquivalent sind, dann sind die zugehörigen Formen Q, Q' (unter Verwendung beliebiger positiv orientierter Basen von I, I') echt äquivalent. Dadurch wird eine Abbildung $\mathrm{cl}_+(I) \mapsto \mathbf{Q}$ von $\mathrm{Cl}_+(\mathcal{O}(D))$ auf $\mathrm{Cl}_+(\mathrm{Prim}(\mathcal{Q}_D))$ definiert.

Umgekehrt sei $Q = \langle a, b, c \rangle$ eine einfache Form mit Diskriminante $D = f^2 D_0$, wobei D_0 eine Fundamentaldiskriminante ist. Sei $K = \mathcal{Q}(\sqrt{D_0})$, also $D_K = D_0$.

Für $a > 0$ sei $I = \mathbb{Z}a \oplus \mathbb{Z}\left(\frac{b - \sqrt{D}}{2}\right)$.

Für $a < 0$ (also $D > 0$) sei $I = \mathbb{Z}a\sqrt{D} \oplus \mathbb{Z}\left(\frac{b-\sqrt{D}}{2}\right)\sqrt{D}$.

Es ist leicht zu sehen, dass in beiden Fällen I ein invertierbares gebrochenes Ideal der Ordnung $\mathcal{O}(D)$ ist.

Wiederum gilt, dass wenn $Q \approx Q'$, dann $I \approx I'$. Man beachte auch, dass wenn $a > 0$, dann ist die Basis $\left(a, \frac{b-\sqrt{D}}{2}\right)$ von I positiv orientiert (bzw. für $a < 0$ die Basis $\left(a\sqrt{D}, \frac{b-\sqrt{D}}{2}\sqrt{D}\right)$).

Damit wird eine Abbildung $\mathbf{Q} \mapsto \mathrm{cl}_+(I)$ von $\mathrm{Cl}_+(\mathcal{Q}_D)$ auf $\mathrm{Cl}_+(\mathcal{O}(D))$ definiert.

Wie man verifizieren kann, sind die beiden Abbildungen zueinander invers.

Darüberhinaus gilt, dass wenn $\mathbf{Q} * \mathbf{Q}' = \mathbf{Q}''$ (Komposition echter Äquivalenzklassen), dann erfüllen die zugehörigen strikten Klassen von Idealen $\mathrm{cl}_+(I) \cdot \mathrm{cl}_+(I') = \mathrm{cl}_+(I'')$.

Das heißt, die Gruppen (unter Komposition) $\mathrm{Cl}_+(\mathrm{Prim}(\mathcal{Q}_D))$ und $\mathrm{Cl}_+(\mathcal{O}(D))$ sind isomorph.

Insbesondere folgt auch, dass $h_+(D) = h_+(\mathcal{O}(D))$.

Man sollte an dieser Stelle beachten, dass es im Allgemeinen keinen Isomorphismus zwischen $\mathrm{Cl}(\mathrm{Prim}(\mathcal{Q}_D))$ und $\mathrm{Cl}(\mathcal{O}(D))$ gibt. Zum Beispiel wurde gezeigt, dass $h(-303) = 6$, $h_+(-303) = 10$, also $h(\mathcal{O}(-303)) = h_+(\mathcal{O}(-303) = 10$.

17 Dirichlets Klassenzahlformel

Unter Verwendung analytischer Methoden fand Dirichlet im Jahre 1839 eine Formel für die Anzahl von echten Äquivalenzklassen einfacher Formen einer gegebenen Diskriminante D.

Ich werde zunächst die Definition und die wichtigsten Eigenschaften des Kronecker-Symbols in Erinnerung rufen, das im Folgenden verwendet wird.

Sei $D \equiv 0$ oder $1 \pmod 4$, D kein Quadrat.

Das Kronecker-Symbol ist wie folgt definiert:

(1) $\left(\frac{D}{2}\right) = \begin{cases} 0 & \text{wenn } D \equiv 0 \pmod 4, \\ 1 & \text{wenn } D \equiv 1 \pmod 8, \\ -1 & \text{wenn } D \equiv 5 \pmod 8; \end{cases}$

(2) wenn p eine ungerade Primzahl ist, dann ist $\left(\frac{D}{p}\right)$ das Legendre-Symbol; insbesondere $\left(\frac{D}{p}\right) = 0$ wenn $p \mid D$;

(3) wenn $n = \prod_{i=1}^{r} p_i^{e_i}$ (mit p_i prim, $e_i \geq 1$), dann $\left(\frac{D}{n}\right) = \prod_{i=1}^{r} \left(\frac{D}{p_i}\right)^{e_i}$; insbesondere $\left(\frac{D}{1}\right) = 1$.

Die Berechnung des Kronecker-Symbols reduziert sich auf die Berechnung des Legendre-Symbols, was sich schnell mittels des Gaußschen Reziprozitätsgesetzes erreichen lässt.

Es ist auch notwendig, die wohlbekannte Tatsache zu verwenden, dass mit gegebenem m und D (wie oben) die Anzahl der ganzen Zahlen n mit $1 \leq n < 2m$ und $D \equiv n^2 \pmod{4m}$ gleich

$$\sum_{k|m,\, 1\leq k} \left(\frac{D}{k}\right)$$

ist.

Sei $D > 0$ und ϵ bezeichne die Fundamentaleinheit des reellquadratischen Zahlkörpers $\mathbf{Q}(\sqrt{D})$ zugehörig zu D. Sei $Q = \langle a, b, c\rangle \in \mathrm{Prim}(\mathcal{Q}_D)$. Die einfache Darstellung $m = Q(\alpha, \beta)$ nennt man eine *primäre Darstellung*, wenn

$$2a\alpha + (b - \sqrt{D})\beta > 0$$

und

$$1 \leq \left| \frac{2a\alpha + (b + \sqrt{D})\beta}{2a\alpha + (b - \sqrt{D})\beta} \right| \leq (\epsilon')^2$$

wobei

$$\epsilon' = \begin{cases} \epsilon & \text{wenn } N(\epsilon) = +1, \\ \epsilon^2 & \text{wenn } N(\epsilon) = -1. \end{cases}$$

Falls $D > 0$, definiere $w = 1$.

Für $D < 0$ bietet es sich an, jede einfache Darstellung als primär zu bezeichnen, w war für $D < 0$ bereits als Anzahl der Einheitswurzeln des quadratischen Zahlkörpers $\mathbf{Q}(\sqrt{D})$ definiert worden.

Dann ist für beliebiges $Q \in \mathrm{Prim}(\mathcal{Q}_D)$ die Anzahl der einfachen primären Darstellungen von $m \geq 1$ durch Q und zugehörig zu n (wobei $1 \leq n < 2m$, $D \equiv n^2 \pmod{4m}$) gleich 0 oder w.

Sei $Q \in \mathrm{Prim}(\mathcal{Q}_D)$, $m \geq 1$ und $\psi(m, Q)$ die Anzahl der einfachen primären Darstellungen von m durch Q.

Sei $\{Q_1, \ldots, Q_{h_+(D)}\}$ eine Menge von $h_+(D)$ paarweise nicht-echter äquivalenter einfacher Formen mit Diskriminante D.

Sei $\psi(m) = \sum_{i=1}^{h_+(D)} \psi(m, Q_i)$.

Dann gilt $\psi(m) = w \sum_{k|m} \left(\frac{D}{k}\right)$; diese Gleichheit reflektiert die Tatsache, dass jede einfache Darstellung zu einem n mit $1 \leq n < 2m$ und $D \equiv n^2 \pmod{4m}$ gehört.

Für jedes $Q \in \mathrm{Prim}(\mathcal{Q}_D)$ und reelles $t > 1$ sei

$$\Psi(t, Q) = \sum_{\substack{1 \leq m \leq t \\ \mathrm{ggT}(m,D)=1}} \psi(m, Q).$$

Der Grenzwert des Durchschnitts von $\Psi(t, Q)$ existiert und lässt sich ausrechnen:

$$\lim_{t\to\infty} \frac{1}{t}\Psi(t, Q) = \begin{cases} \frac{2\pi}{\sqrt{|D|}} \cdot \frac{\phi(|D|)}{|D|} & \text{wenn } D < 0, \\ \frac{\log \epsilon'}{\sqrt{D}} \cdot \frac{\phi(D)}{D} & \text{wenn } D > 0. \end{cases}$$

Dieser Durchschnitt ist unabhängig von der Wahl von Q.

Die Klassenzahl $h_+(D)$ taucht in folgender Weise auf:

$$\begin{aligned} \sum_{i=1}^{h_+(D)} \Psi(t, Q_i) &= \sum_{\substack{1 \leq m \leq t \\ \mathrm{ggT}(m,D)=1}} \sum_{i=1}^{h_+(D)} \psi(m, Q_i) \\ &= \sum_{\substack{1 \leq m \leq t \\ \mathrm{ggT}(m,D)=1}} \psi(m) \\ &= w \sum_{\substack{1 \leq m \leq t \\ \mathrm{ggT}(m,D)=1}} \sum_{k|m} \left(\frac{D}{k}\right). \end{aligned}$$

Nach Teilen durch t und Grenzübergang von t gegen Unendlich ergibt sich für die linke Seite

$$h_+(D) \cdot C_D \cdot \frac{\phi(|D|)}{|D|},$$

wobei

$$C_D = \begin{cases} \frac{2\pi}{\sqrt{|D|}} & \text{wenn } D < 0, \\ \frac{\log \epsilon'}{\sqrt{D}} & \text{wenn } D > 0. \end{cases}$$

Die Berechnung der rechten Seite ist weniger offensichtlich. Für Details seien die vorzüglichen Bücher von Hua (1982) oder Borevich und Shafarevich (1966) zur Lektüre empfohlen.

Auf jeden Fall ist

$$\lim_{t\to\infty}\frac{1}{t}\left[w\sum_{\substack{1\le m\le t\\ \mathrm{ggT}(m,D)=1}}\sum_{k|m}\left(\frac{D}{k}\right)\right]=w\frac{\psi(|D|)}{|D|}L(D),$$

wobei

$$L(D)=\sum_{k=1}^{\infty}\frac{1}{k}\left(\frac{D}{k}\right).$$

Man beachte, dass wenn es sich bei der Abbildung $n\mapsto\chi(n)=(D/n)$ um einen modularen Charakter handelt, dann ist $L(D)$ nichts anderes als $L(1|\chi)$, dem Wert der L-Reihe von χ bei $s=1$:

$$L(s|\chi)=\sum_{n=1}^{\infty}\frac{\chi(n)}{n^s}\quad\text{(konvergent für }\mathrm{Re}(s)>1).$$

Diese Reihe $L(D)$ konvergiert und es folgt, dass

$$h_+(D)=\frac{w}{C_D}L(D)=\begin{cases}\frac{w\sqrt{|D|}}{2\pi}L(D) & \text{wenn } D<0,\\ \frac{\sqrt{D}}{\log\epsilon'}L(D) & \text{wenn } D>0.\end{cases}$$

Die Berechnung von $L(D)$ ist schwierig. Für Fundamentaldiskriminanten D ergibt sich (siehe Hua (1982)):

$$L(D)=\begin{cases}-\frac{\pi}{|D|^{3/2}}\sum_{k=1}^{|D|-1}\left(\frac{D}{k}\right)k & \text{wenn } D<0,\\ -\frac{1}{\sqrt{D}}\sum_{k=1}^{D-1}\left(\frac{D}{k}\right)\log\sin\frac{k\pi}{D} & \text{wenn } D>0,\end{cases}$$

und schließlich folgt Dirichlets Formel für die strikte Klassenzahl (für Fundamentaldiskriminanten):

$$h_+(D)=\begin{cases}-\frac{w}{2|D|}\sum_{k=1}^{|D|-1}\left(\frac{D}{k}\right)k & \text{wenn } D<0,\\ -\frac{1}{\log\epsilon'}\sum_{k=1}^{D-1}\left(\frac{D}{k}\right)\log\sin\frac{k\pi}{D} & \text{wenn } D>0.\end{cases}$$

Unter Beachtung der Beziehung zwischen der Fundamentaleinheit und ϵ' sowie zwischen $h_+(D)$ und $h(D)$ lässt sich die Formel für die Klassenzahl $h(D)$ wie folgt anders schreiben:

$$h(D)=\begin{cases}-\frac{w}{2|D|}\sum_{k=1}^{|D|-1}\left(\frac{D}{k}\right)k & \text{wenn } D<0,\\ -\frac{1}{2\log\epsilon}\sum_{k=1}^{D-1}\left(\frac{D}{k}\right)\log\sin\frac{k\pi}{D} & \text{wenn } D>0.\end{cases}$$

Allgemeiner gilt für $D = f^2 D_0$ mit einer Fundamentaldiskriminanten D_0,

$$L(D) = \prod_{p|f} \frac{1 - \left(\frac{D_0}{p}\right)}{p} L(D_0),$$

und dieser Wert führt sofort zu den Formeln für $h_+(D)$ und $h(D)$ für beliebige Diskriminanten.

Ein anderer Ausdruck für $h(D)$ für den Fall einer Fundamentaldiskriminanten D mit $D < -4$ ist der Folgende:

$$h(D) = \frac{1}{2 - \left(\frac{D}{2}\right)} \sum_{\substack{1 \le k < |D|/2 \\ \mathrm{ggT}(k,D)=1}} \left(\frac{D}{k}\right).$$

Daraus ergibt sich für eine Primzahl p mit $p \equiv 3 \pmod 4$ und $p \neq 3$, dass

$$h(-p) = \begin{cases} R - N & \text{wenn } p \equiv 7 \pmod 8, \\ \frac{1}{3}(R - N) & \text{wenn } p \equiv 3 \pmod 8, \end{cases}$$

wobei

$$R = \#\{k \mid 1 \le k < \frac{P}{2}, \left(\frac{k}{p}\right) - 1\},$$
$$N = \#\{k \mid 1 \le k < \frac{P}{2}, \left(\frac{k}{p}\right) = -1\}.$$

Beispielsweise

$$h(-43) = \frac{1}{3}(R - N) = \frac{1}{3}(12 - 9) = 1.$$

Eine interessante Bemerkung findet sich in Artikel 303 der *Disquisitiones Arithmeticae*, wo Gauss erwähnt, dass für $D > 0$ das Produkt $h(D) \log \epsilon$ eine ähnliche Rolle wie $h_+(D)$ für $D < 0$ spielt. Diese Tatsache taucht später bei Siegel (1936) erneut auf und deutet auf die wesentliche Bedeutung der L-Reihe des Charakters χ hin.

18 Lösung des Klassenzahlproblems für definite Formen

Obwohl es die Klassenzahlformel tatsächlich erlaubt, $h(D)$ zu berechnen (siehe Buells Tabellen mit $h(D)$-Werten (Buell (1976) und Buell (1987)) für $|D| < 25 \times 10^6$), kann man keine Rückschlüsse

auf das Wachstum von $h(D)$ ziehen. Die Formel ist damit nicht hinreichend, um über die Richtigkeit der Vermutungen von GAUSS (siehe §14) zu entscheiden. Die Fragen sind viel schwieriger.

Die zwei exzellenten Artikel von GOLDFELD (1985) und OESTERLÉ (1988) seien zur Lektüre dringend empfohlen. Sie enthalten eine hervorragende Beschreibung des bisher Geleisteten zur Lösung des Problems der echten Äquivalenzklassen positiv definiter Formen mit Fundamentaldiskriminante, bzw. äquivalent, für imaginär-quadratische Zahlkörper.

Ich werde mich unverhohlen dieser zuverlässigen Quellen bedienen—was bleibt den Autoren nach meinem Ausdruck tiefer Anerkennung, als mir zu verzeihen?

Vor der Betrachtung der Frage im Allgemeinen lohnt es darauf hinzuweisen, dass es LANDAU bereits im Jahr 1903 gelungen war, einen Spezialfall zu lösen:

Wenn D irgendeine durch 4 teilbare Fundamentaldiskriminante ist, dann gilt $h(-D) = 1$ genau dann, wenn $-D = 4$ oder 8.

Es ist nicht schwierig, Abschätzungen für obere Schranken von $L(D) = L(1|\chi)$ anzugeben. Wenn $D \leq -5$, so $L(D) \leq \log|D|$ und daher

$$h(D) < \frac{\sqrt{D}\log|D|}{\pi}.$$

Zur Lösung des Klassenzahlproblems ist es wesentlich, untere Schranken für $h(D)$ zu bestimmen.

Man betrachte die Zetafunktion des Körpers $K = \mathbf{Q}(\sqrt{D})$:

$$\zeta_K(s) = \sum \frac{1}{N(I)^s} (\text{Summation über alle Nicht-Null-Ideale } I \text{ von } \mathcal{O}),$$

wobei $N(I)$ die Norm des Ideals I bezeichnet. Diese Reihe ist für $\mathrm{Re}(s) > 1$ absolut konvergent.

Wenn $K = \mathbf{Q}$, dann ist $\zeta_{\mathbf{Q}}(s)$ die Riemannsche Zetafunktion

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s} \quad (\text{für } \mathrm{Re}(s) > 1).$$

Klassische Berechnungen ergeben

$$\zeta_K(s) = \zeta(s)L(s|\chi) \quad (\text{für } \mathrm{Re}(s) > 1),$$

mit $\chi(n) = \left(\frac{D}{n}\right)$ für jedes $n \geq 1$.

Die Riemannsche Vermutung besagt, dass alle nicht-reellen Nullstellen $\sigma + it$ von $\zeta(s)$ den Realteil $\sigma = 1/2$ haben.

Im vorliegenden Kontext bedeutet die verallgemeinerte Riemannsche Vermutung die analoge Aussage für die L-Reihen $L(s|\chi)$.

Jeder weiß, dass sowohl die Riemannsche Vermutung als auch die Verallgemeinerung, so plausibel sie auch erscheinen mögen, immer noch unbewiesen sind. Es ist in der analytischen Zahlentheorie gängige Praxis, Folgerungen aus der Vermutung abzuleiten—so wie es im 19. Jahrhundert im Falle der nicht-euklidischen Geometrie geschah.

Hecke (siehe Landau (1913)) bewies unter der Annahme einer schwächeren Form der verallgemeinerten Riemannschen Vermutung für die L-Reihen des Charakters χ, dass es eine Konstante $c > 0$ derart gibt, dass

$$h(D) \geq \frac{1}{c} \cdot \frac{\sqrt{|D|}}{\log |D|}.$$

Daraus folgt, dass $\lim_{D\to-\infty} h(D) = \infty$, und wenn zudem $h(D) = 1$, dann

$$c \geq \frac{\sqrt{|D|}}{\log |D|},$$

und somit

$$|D| \leq (c \log |D|)^2.$$

Was konnte bewiesen werden, ohne sich auf die Richtigkeit der verallgemeinerten Riemannschen Vermutung zu verlassen?

Deuring (1933) zeigte:

Angenommen die klassische Riemannsche Vermutung ist falsch. Dann gibt es nur endlich viele Diskriminanten $D < 0$ mit $h(D) = 1$.

Kurz darauf bewies Mordell unter derselben Annahme, dass $\lim_{D\to-\infty} h(D) = \infty$.

Im selben Jahr folgerte Heilbronn (1934a): Wenn die verallgemeinerte Riemannsche Vermutung nicht zutrifft, so $\lim_{D\to-\infty} h(D) = \infty$.

Wie Goldfeld sagt: „Dies ist der erste bekannte Fall, bei dem ein Beweis zunächst die Wahrheit und dann die Unwahrheit der verallgemeinerten Riemannsche Vermutung voraussetzt und in beiden Fällen die richtige Antwort gibt!“

Siegel (1936) zeigte auf eine andere Weise, dass

$$\log h(D) \sim \log \sqrt{|D|} \quad \text{(asymptotisch mit } D \to -\infty);$$

insbesondere $\lim_{D\to-\infty} h(D) = \infty$.

Obige Beweise lieferten keine Schranke für die Diskriminanten $D < 0$ derart, dass $h(D)$ kleiner als ein gegebener Wert bleibt.

Ein verfeinerter Beweis von Heilbronn und Linfoot (1934b) führte zum Schluss, dass es außer den bereits erwähnten Diskriminanten $D < 0$ mit $h(D) = 1$ ($|D| = 3, 4, 7, 8, 11, 19, 43, 67, 163$) höchstens eine weitere gibt.

Es verging eine ziemlich lange Zeit, bis man diese zusätzliche zehnte Diskriminante ausschließen konnte; die Geschichte ist sehr interessant.

Heegner (1952)—der als Gymnasiallehrer eigentlich ein Outsider war—veröffentlichte einen Artikel, der die Existenz der zusätzlichen zehnten Diskriminante ausschloss. Heegners Beweis, der die Theorie modularer Formen verwendete, wurde als falsch eingestuft; tatsächlich fanden sich Fehler darin und zudem gab es undurchsichtige Passagen.

Baker (1966) wendete seine Methode der effektiven unteren Schranken linearer Formen dreier Logarithmen erfolgreich an und zeigte, dass die zusätzliche Diskriminante nicht existiert.

Stark (1967) gab einen weiteren Beweis an, ähnlich dem vom Heegner. Noch ein anderer stammt von Siegel (1968).

Eine Nachprüfung von Heegners Beweis durch Deuring (1968) genügte, um ihn wieder auf soliden Boden zu stellen. Stark (1969) machte die ganze Angelegenheit noch peinlicher, als er zeigte, wie man den Satz unter Verwendung effektiver unterer Schranken einer linearen Form von zwei Logarithmen beweisen konnte—und dies war bereits vollständig dadurch möglich, in dem man Transzendenz-Ergebnisse von Gel'fond und Linnik, anwendete, die bereits 1949 bekannt waren.

Der Weg hin zur Behandlung der imaginär-quadratischen Zahlkörper mit Klassenzahl 2 war nun gebahnt. Unter Verwendung effektiver unterer Schranken von Logarithmen zeigten Baker (1971) und Stark (1971) unabhängig voneinander, dass $h(D) = 2$ genau dann, wenn

$$|D| = 5, 6, 10, 13, 15, 22, 35, 37, 51, 58, 91, 115, 123, 187, 235, 267, 403, 427.$$

Es blieb noch ein weiter Weg hin zur Entscheidung über den Status der Vermutungen von Gauss über die Klassenzahl von imaginär-quadratischen Zahlkörpern. Es war wesentlich, effektive untere Schranken für die Klassenzahl zu finden. Der Weg hin zu diesem Ziel war kompliziert und erforderte die Theorie modularer Formen und elliptischer Funktionen.

Die Krönung der Arbeiten von Goldfeld (1977) und Gross und Zagier (1986) ergab (im Jahr 1983) die folgende effektive untere Schranke für $h(D)$:

Für jedes $\delta > 0$ gibt es eine effektiv berechenbare Zahl $C = C(\epsilon) > 0$ derart, dass

$$h(D) > C(\log |D|)^{1-\epsilon}.$$

Dies genügt, um zu folgern, dass es für jede gegebene Zahl n eine effektive, von n abhängige Schranke $B(n)$ derart gibt, dass wenn $h(D) = n$, dann $|D| \leq B(n)$. Somit sind Gauss' Klassenzahl-Vermutungen für definite Formen wahr.

Explizite Berechnungen von Oesterlé (1983) ergaben die unteren Schranken:

$$h(D) > \frac{1}{55}(\log |D|) \prod_{p|D,\, p\neq 2} \left(1 - \frac{[2\sqrt{p}]}{p+1}\right).$$

Diese Schranke gilt für Diskriminanten, die teilerfremd zu 5077 sind.

Diese und ähnliche Abschätzungen erlaubten die Bestimmung aller Körper mit Klassenzahl 3 (es gibt 16 solcher Körper, für diese ist $D \leq 907$), mit Klassenzahl 4 (es gibt 54 solcher Körper, für diese gilt $D < 1555$), weitere Ergebnisse in dieser Richtung werden folgen.

Dieselbe Methode wie von Heilbronn erlaubte es Chowla, eine (nicht-effektive) untere Schranke für die Anzahl der Klassen im Hauptgeschlecht irgendeiner Diskriminante $D < 0$ anzugeben. Man erinnere sich, dass diese Zahl gleich $h(D)/g(D)$ ist, wobei $g(D)$ die Anzahl der Geschlechter ist.

Chowla (1934) zeigte, dass

$$\lim_{|D|\to\infty} \frac{h(D)}{g(D)} = \infty.$$

Insbesondere gibt es für $n \geq 1$ nur endlich viele Diskriminanten $D < 0$ derart, dass die Anzahl der Klassen im Hauptgeschlecht n beträgt. Hieraus ergibt sich eine — wenn auch nicht-effektive — Lösung von Gauss' vierter Vermutung (siehe §14).

Weitere Arbeiten von Chowla und Briggs (1954) und Weinberger (1973a) führten zu folgendem interessanten Schluss:

Abgesehen von den bekannten, in §12 aufgelisteten Diskriminanten mit nur einer Klasse im Hauptgeschlecht gibt es höchstens ein weiteres D, wobei $|D| > 10^{60}$. Ob es eine solche Diskriminante gibt oder

nicht ist immer noch unbekannt. Die Existenz ist jedoch ausgeschlossen, sobald eine passende schwache Vermutung über die Nullstellen der zugehörigen L-Reihen bewiesen ist; siehe Chowla und Briggs (1954) und Grosswald (1963).

19 Das Klassenzahlproblem für indefinite Formen

Man erinnere sich, dass Gauss aufgrund numerischer Berechnungen vermutet hatte, dass es unendlich viele Fundamentaldiskriminanten $D > 0$ derart geben müsste, dass $h(D) = 1$, oder äquivalent, dass es unendlich viele reell-quadratische Zahlkörper mit Klassenzahl 1 gibt.

Das Problem ist eng verbunden mit der Größe der Fundamentaleinheit ϵ_D. Tatsächlich zeigte Siegel im Jahr 1936:

$$\log(h(D)\log\epsilon_D) \sim \log\sqrt{D} \quad \text{(asymptotisch mit } D \to \infty).$$

Umfassende Berechnungen der Klassenzahl von Wada (1981), Mollin und Williams (1992) und später von Jacobson (1998) stützen die Vermutung. Allerdings scheint der Beweis kompliziert und sehr schwierig zu sein.

Ich möchte auf einige Fortschritte und verwandte Untersuchungen zum Problem hinweisen.

Zunächst gibt es sehr interessante heuristische Betrachtungen von Cohen und Lenstra (1984) (oder Cohen (1993)) die die Automorphismusgruppe der Klassengruppe betreffen und zum Schluss führen, dass der Anteil von reell-quadratischen Zahlkörpern mit Klassenzahl 1 etwa gleich 75,466% betragen sollte. Dies kommt dem in Tabellen beobachteten Verhältnis tatsächlich sehr nahe. Ich werde auf diese sehr weitreichenden Vermutungen im nächsten Abschnitt zurückkommen.

Ein sehr interessanter Begriff, der von Lachaud (1986, 1987) untersucht wurde, ist das *Kaliber* einer Fundamentaldiskriminanten D, bzw. des zugehörigen Körpers $K = \mathbf{Q}(\sqrt{D})$. Nach Definition ist das Kaliber $k(D)$ die Anzahl der reduzierten einfachen Formen unter echter Äquivalenz. Man beachte, dass wenn $D < 0$, dann gilt $k(D) = h(D)$, aber wenn $D > 0$, dann ist im Allgemeinen $k(D) > h(D)$, wieviel größer hängt von der Periode der Nullstellen zugehörig zu den reduzierten Formen ab.

Für jede Klasse $\mathbf{Q}$ reduzierter Formen sei mit $m(\mathbf{Q})$ die Anzahl der Formen in ihrer Periode bezeichnet.

Dann

$$m(\mathbf{Q}) \log \alpha \leq \log \epsilon'_D < m(\mathbf{Q}) \log \sqrt{D},$$

wobei

$$\epsilon'_D = \begin{cases} \epsilon_D & \text{wenn } N(\epsilon_D) = +1, \\ \epsilon_D^2 & \text{wenn } N(\epsilon_D) = -1. \end{cases}$$

ϵ_D ist die Fundamentaleinheit und $\alpha = (1 + \sqrt{5})/2$ die Goldene Zahl. Dann

$$k(D) \log \alpha \leq h_+(D) \log \epsilon'_D < k(D) \log \sqrt{D},$$

und dies lässt sich auch schreiben als

$$k(D) \log \alpha \leq h(D) \log \epsilon_D < k(D) \log \sqrt{D}.$$

Aus Siegels Resultat,

$$\log(h(D) \log \epsilon_D) \sim \log \sqrt{D},$$

und es folgt, dass

$$\log k(D) \sim \log \sqrt{D}.$$

Somit gibt es für jedes $n \geq 1$ nur endlich viele reell-quadratische Zahlkörper $K = \mathbf{Q}(\sqrt{D})$ mit $k(D) \leq n$.

Dies ist das Analogon des Resultats für die Klassenzahl von imaginär-quadratischen Zahlkörpern, aber genau das Gegenteil dessen, was man für die Klassenzahl von reell-quadratischen Zahlkörpern erwartet hatte.

Als Konsequenz ergibt sich, dass für jedes $n \geq 1$ und $m \geq 1$ die Menge $\{D > 0 \mid D$ ist eine Fundamentaldiskriminante, $h(D) \leq n$ und das Maximum $m(D)$ der Längen der Perioden der reduzierten Formen mit Diskriminante D ist höchstens $m\}$ endlich ist — da für jedes solche D gilt $k(D) \leq mn$. Siehe Sasaki (1986).

Insbesondere gibt es für jedes $m \geq 1$ nur endlich viele Fundamentaldiskriminanten $D > 0$ mit $h(D) = 1$, und die Perioden der reduzierten Formen haben höchstens eine Länge von m. Die vorangegangenen Aussagen liefern allerdings keine effektiven Schranken.

Wie üblich ist es mithilfe einer schwächeren Form der verallgemeinerten Riemannschen Vermutung über die L-Reihen des Charakters χ von D möglich, effektive Ergebnisse zu erzielen, nämlich

$$h(D) \log \epsilon_D < 4{,}23 k(D).$$

Unter derselben Voraussetzung zeigte LACHAUD, dass die einzigen reell-quadratischen Zahlkörper $\mathbf{Q}(\sqrt{D})$ mit Kaliber 1 die sieben Körper $\mathbf{Q}(\sqrt{D})$ mit $D = 2, 5, 13, 29, 53, 173, 293$ sind. Darüberhinaus bewies SASAKI, dass wenn zudem gilt $m(D) = 1$, dann ist $D = 2$.

Andere Ergebnisse gehen in die folgende Richtung: Wenn $D > 0$ eine Fundamentaldiskriminante einer gegebenen „Prägung“ ist, dann gibt es nur endlich viele reell-quadratische Zahlkörper $\mathbf{Q}(\sqrt{D})$ mit Klassenzahl 1.

So hatten Chowla und Friedlander (1976) vermutet, dass wenn p eine Primzahl mit $p = m^2 + 1$ ist und $\mathbf{Q}(\sqrt{p})$ die Klassenzahl 1 hat, dann ist $p = 2, 5, 17, 37, 101, 197, 677$. Analog gilt, dass wenn p eine Primzahl mit $p = m^2 + 4$ ist und $\mathbf{Q}(\sqrt{p})$ die Klassenzahl 1 hat, dann ist $p = 5, 13, 29, 173, 293$.

Dies wurde unter Annahme der verallgemeinerten Riemannschen Vermutung unabhängig voneinander von LACHAUD (1987) und von Mollin und Williams (1988) bewiesen.

Ich möchte noch auf ein weiteres Resultat derselben Art hinweisen, das von Mollin und Williams (1989) bewiesen wurde:

Eine quadratfreie positive ganze Zahl $d = n^2 + r$, wobei r Teiler von $4n$ ist, bezeichnet man als zum *erweiterten Richaud-Degert Typus* gehörend.

Es gibt 43 (und möglicherweise 44) ganze Zahlen d vom erweiterten Richaud-Degert-Typus, deren entsprechender Zahlkörper $\mathbf{Q}(\sqrt{d})$ die Klassenzahl 1 hat; die vollständige Liste ist:

$$\begin{aligned} d = {} & 2, 3, 5, 6, 7, 11, 13, 14, 17, 21, 23, 29, 33, 37, 38, 47, 53, 62, 69, 77, \\ & 83, 93, 101, 141, 167, 173, 197, 213, 227, 237, 293, 398, 413, 437, \\ & 453, 573, 677, 717, 1077, 1133, 1253, 1293, 1757 \\ & \text{und möglicherweise ein weiterer Wert.} \end{aligned}$$

Sei nun $d > 0$ mit $d \neq 1$ eine quadratfreie ganze Zahl und wie zuvor

$$\omega = \begin{cases} \sqrt{d} & \text{wenn } d \equiv 2 \text{ oder } 3 \pmod 4, \\ \frac{1+\sqrt{d}}{2} & \text{wenn } d \equiv 1 \pmod 4. \end{cases}$$

Bezeichne mit k die Länge der Periode der Kettenbruchentwicklung von ω.

Mollin und Williams (1989) haben sämtliche der endlich vielen reell-quadratischen Zahlkörper $K = \mathbf{Q}(\sqrt{d})$ mit Klassenzahl 1 oder 2 explizit bestimmt (mit möglicherweise einer Ausnahme), wobei für die Länge k

der Periode von ω gilt $k \leq 24$. Diesmal waren nicht alle der ganzen Zahlen d vom erweiterten Richaud-Degert Typus.

Für eine einheitliche Darstellung der bisher erzielten Resultate von MOLLIN und WILLIAMS sei dem Leser deren Artikel Mollin und Williams (1990) und das Buch *Quadratics* von Mollin (1996) empfohlen.

Es wurden und werden wohl noch viele Teilergebnisse zum Problem erzielt, bevor ein echtes Verständnis den richtigen Zugang dazu öffnet.

20 Weitere Fragen und Vermutungen

Das Studium der Vermutungen von §14 führte zu weiteren, umfassenden und tiefen Problemen, die alle miteinander verbunden und wahrscheinlich sehr schwierig sind. Obwohl es momentan meines Wissens nach keine Methode gibt, um diese Fragen auch nur ansatzweise erfolgreich in Angriff zu nehmen, denke ich, dass es sich lohnt, sie einmal explizit zu nennen.

Problem 1. Ist jede natürliche Zahl gleich der Klassenzahl irgendeines quadratischen Zahlkörpers mit negativer bzw. positiver Diskriminante D?

Die folgende Frage ist eng damit verbunden und noch schwieriger:

Problem 2. Ist jede endliche abelsche Gruppe G isomorph zur Klassengruppe eines quadratischen Zahlkörpers mit Diskriminante $D < 0$ bzw. $D > 0$? Wenn ja, gibt es unendlich viele Zahlkörper $\mathbf{Q}(\sqrt{D})$ mit $D > 0$ derart, dass die Klassengruppe von $\mathbf{Q}(\sqrt{D})$ isomorph zu G ist?

Boyd und Kisilevsky (1972) zeigten, dass es nur endlich viele imaginär-quadratische Zahlkörper mit einer Klassengruppe gibt, die isomorph zum Produkt von zyklischen Gruppen der Ordnung 3 ist; sie bewiesen unter der Annahme der verallgemeinerten Riemannschen Vermutung das entsprechende Resultat für Klassengruppen, die isomorph zum Produkt von zyklischen Gruppen mit Ordnungen $n > 3$ sind.

Das nächste Problem bezieht sich auf den p-Rang $r_p(D)$ (mit einer Primzahl p) der Klassengruppe des quadratischen Zahlkörpers mit Diskriminante D.

Problem 3. Sei $p \geq 3$. Ist jede natürliche Zahl gleich dem p-Rang $r_p(D)$ für irgendeine negative bzw. positive Diskriminante D? Falls ja, gibt es unendlich viele Diskriminanten D derart, dass $r_3(D)$ größer oder gleich einer gegebenen natürlichen Zahl n ist?

Craig (1977) zeigte, dass es unendlich viele negative Diskriminanten D derart gibt, dass $r_3(D) \geq 4$.

Lässt sich das Folgende wenigstens entscheiden?

Problem 4. Ist $\sup\{r_p(D) : |D| \geq 1\} = \infty$? (für $D < 0$ bzw. $D > 0$).

In diesem Zusammenhang ist es wichtig zu lernen, wie man Diskriminanten bestimmen kann, für die der p-Rang wahrscheinlich groß ist.

Es wäre zudem von großer Bedeutung, Abschätzungen für den p-Rang zu gewinnen. Vielleicht ist dies für negative Diskriminanten möglich.

In Bezug auf diese Frage möchte ich berichten, dass für jedes $n \leq 6$ Diskriminanten $D < 0$ bekannt sind, für die der 3-Rang gleich n ist. Auch kennt man für jedes $n \leq 4$ Diskriminanten $D < 0$ mit einem 5-Rang von n .

Quer (1987) zeigte, dass

$$r_3(-408368221541174183) = 6,$$

und Schoof (1983) berechnete

$$r_5(-258559351511807) = 4;$$

siehe auch Llorente und Quer (1988).

Es ist nicht nötig, sich mit dem 2-Rang zu befassen, da aus der Geschlechtertheorie folgt, dass wenn D eine Fundamentaldiskriminante mit r verschiedenen Primfaktoren ist, dann ist der 2-Rang $r_2(D) = r - 1$, da die Anzahl der zweideutigen Klassen 2^{r-1} beträgt.

An dieser Stelle seien einige Ergebnisse über die Teilbarkeit der Klassenzahl erwähnt, die jedoch nicht stark genug sind, um eines der obigen Probleme zu lösen.

Nagell (1929) zeigte, dass es für jedes $n > 1$ unendlich viele imaginär-quadratische Zahlkörper $\mathbf{Q}(\sqrt{D})$ mit $D < 0$ derart gibt, dass die Klassenzahl durch n teilbar ist.

Dieser Satz wurde von Humbert (1939) und Ankeny und Chowla (1955) wiederentdeckt. Im Jahre 1986 erweiterte Mollin das Ergebnis mit einem einfacheren Beweis (siehe Mollin (1986)).

Ähnliches zeigte für reell-quadratische Zahlkörper zunächst Honda (1968), nämlich dass es unendlich viele reell-quadratische Zahlkörper mit einer durch 3 teilbaren Klassenzahl gibt. Im Jahre 1970 bewies

Yamamoto (1970) sowie Weinberger (1973b): Für jedes $n > 1$ gibt es unendlich viele reell-quadratische Zahlkörper mit einer durch n teilbaren Klassenzahl.

Ich kehre nun zu den heuristischen Argumenten von Cohen und Lenstra (1984) zurück; siehe auch das Buch von Cohen (1993). Aus den Tabellen von Klassengruppen für negative Diskriminanten ist ersichtlich (siehe Buell (1976, 1987), Saito und Wada (1988a,b)), dass die 3-Sylow-Untergruppe achtmal häufiger isomorph zu C_9 ist als zu $C_3 \times C_3$ (hier bezeichnet C_n die multiplikative zyklische Gruppe der Ordnung n). Dies ist genau das Verhältnis

$$\frac{\#\operatorname{Aut}(C_9)}{\#\operatorname{Aut}(C_3 \times C_3)}.$$

Diese und ähnliche Tatsachen legen nahe, die Wahrscheinlichkeiten des Auftretens einer Art von p-Sylow-Untergruppe danach zu berechnen, indem man die Gruppen G mit Gewichten $1/\#\operatorname{Aut}(G)$ versieht. Mithilfe dieser einfachen Idee gelangten Cohen und Lenstra zu Wahrscheinlichkeiten, die erstaunlich nahe bei den beobachteten Werten liegen.

Sei zunächst $D < 0$.

Die Wahrscheinlichkeit, dass der ungerade Teil der Klassengruppe eine zyklische Gruppe ist, beträgt

$$\frac{\zeta(2)\zeta(3)}{\zeta(6)C_\infty \prod_{i=1}^{\infty}(1-\frac{1}{2^i})} = 97{,}757\%$$

wobei

$$C_\infty = \prod_{n=2}^{\infty} \zeta(n) = 2{,}2948\ldots.$$

Für eine ungerade Primzahl p ist die Wahrscheinlichkeit, dass die Klassenzahl durch p teilbar ist, gleich

$$l(p) = 1 - \prod_{i=1}^{\infty}\left(1 - \frac{1}{p_i}\right) = \frac{1}{p} + \frac{1}{p^2} - \frac{1}{p^5} - \frac{1}{p^7} + \frac{1}{p^{12}} + \frac{1}{p^{15}} + \cdots.$$

Genauer,

$$\begin{aligned} l(3) &\simeq 44\%, \\ l(5) &\simeq 24\%, \\ l(7) &\simeq 16\%, \text{ usw}\ldots. \end{aligned}$$

Wenn p eine ungerade Primzahl ist, beträgt die Wahrscheinlichkeit, dass der p-Rang der Klassengruppe gleich $n \geq 1$ ist,

$$t_p(n) = \frac{\prod_{i=1}^{\infty}\left(1-\frac{1}{p^i}\right)}{p^{n^2}\prod_{j=1}^{n}\left(1-\frac{1}{p^j}\right)^2}.$$

Die Wahrscheinlichkeit, dass die p-Sylow-Untergruppe ($p > 2$) der Klassengruppe gleich einer gegebenen Gruppe ist:

$$\begin{aligned}
&S_3 = C_9 && : 9{,}33\% \\
&S_3 = C_3 \times C_3 && : 1{,}17\% \\
&S_3 = C_3 \times C_3 \times C_3 && : 0{,}005\% \\
&S_3 = C_3 \times C_3 \times C_3 \times C_3 && : 2{,}3 \times 10^{-8}\% \\
&S_5 = C_{25} && : 3{,}80\% \\
&S_5 = C_5 \times C_5 && : 0{,}16\%, \text{ usw.}\ldots.
\end{aligned}$$

Sei nun $D > 0$.

Die Wahrscheinlichkeit, dass die Ordnung des ungeraden Teils der Klassengruppe gleich ist zu n, sei mit $u(n)$ bezeichnet. Damit

$$\begin{aligned}
u(1) &= 75{,}5\% \\
u(3) &= 12{,}6\% \\
u(5) &= 3{,}8\% \\
u(7) &= 1{,}8\% \\
u(9) &= 1{,}6\%, \text{ usw}\ldots.
\end{aligned}$$

$u(n)$ ist auch die Wahrscheinlichkeit, dass die Klassenzahl von $\mathbf{Q}(\sqrt{p})$ (mit einer Primzahl p) gleich n ist.

Die Wahrscheinlichkeit, dass das ungerade prime p die Klassenzahl teilt, beträgt

$$1 - \prod_{k=2}^{\infty}\left(1-\frac{1}{p^k}\right).$$

Die Wahrscheinlichkeit, dass der p-Rang der Klassengruppe gleich $n \geq 1$ ist:

$$t'_p(n) = \frac{\prod_{i=1}^{\infty}\left(1-\frac{1}{p^i}\right)}{p^{n(n+1)}\prod_{j=1}^{n}\left(1-\frac{1}{p^j}\right)\prod_{j=1}^{n+1}\left(1-\frac{1}{p^j}\right)},$$

usw.....

Die obigen heuristischen Ergebnisse legen natürlich nahe, was die Antworten auf die zu Beginn dieses Abschnitts erwähnten Probleme sein *sollten*.

Der Leser möge vielleicht den Artikel von Jacobson (1998) hinzuziehen. Dieser enthält Tabellen, die umfassende Berechnungen für $D < 10^9$ erforderten. Die numerischen Resultate bestätigen die verblüffenden Vermutungen von Cohen und Lenstra und enthalten Listen von Diskriminanten, für die die Klassengruppe nicht-zyklische p-Sylow-Untergruppen (für alle $p \leq 23$) enthält, usw.

21 Viele unbehandelte Themen

Diese erweiterte Version meiner Vorlesung ist bereits viel länger geworden als ursprünglich beabsichtigt. Trotzdem konnten viele ebenso wichtige Themen nicht angesprochen werden. Darunter die geometrische Theorie quadratischer Formen wie von Klein entwickelt, die zu einer engen Verbindung zu modularen Formen führt; siehe auch den Übersichtsartikel von Serre (1985).

Das Problem der Darstellung ganzer Zahlen durch quadratische Formen kann man nicht vollständig mit den hier vorgestellten Methoden lösen, wenn es mehr als eine Klasse im Hauptgeschlecht gibt. Es lässt sich jedoch mithilfe der Klassenkörpertheorie behandeln, genauer mit dem Hilbert-Symbol. Diese Vorgehensweise ist im Buch von Cox (1989) sehr gut dargestellt.

Shanks bediente sich der Klassengruppe und sogar ihres Unterbaus, um zu raffinierten Algorithmen zur Faktorisierung und zu Primzahltests zu gelangen; siehe hierzu Shanks (1969, 1976, 1989).

Literaturverzeichnis

1801 C. F. Gauss. *Disquisitiones Arithmeticae.* G. Fleischer, Leipzig.

1870 C. F. Gauss. *Werke.* Königl. Ges. d. Wiss., Göttingen.

1892 P. Bachmann. *Zahlentheorie, Band I und II.* B. G. Teubner, Leipzig.

1907 J. Sommer. *Vorlesungen über Zahlentheorie.* B. G. Teubner, Leipzig.

1913 E. Landau. Über die Klassenzahl imaginär-quadratischer Zahlkörper. *Göttinger Nachr.*, 285–295.

1929 T. Nagell. Über die Klassenzahl imaginär-quadratischer Zahlkörper. *Abh. Math. Sem. Univ. Hamburg*, 1:140–150.

1933 M. Deuring. Imaginäre quadratische Zahlkörper mit der Klassenzahl 1. *Math. Z.*, 37:405–415.

1934 S. Chowla. An extension of Heilbronn's class-number theorem. *Quart. J. Math. Oxford*, 5:304–307.

1934 H. Heilbronn. On the class number of imaginary quadratic fields. *Quart. J. Math. Oxford*, 5(2):150–160.

1934 H. Heilbronn und E. H. Linfoot. On the imaginary quadratic corpora of class number one. *Quart. J. Math. Oxford*, 5(2):293–301.

1936 C. L. Siegel. Über die Classenzahl quadratischer Zahlkörper. *Acta Arith.*, 1:83–86. Nachdruck in *Gesammelte Abhandlungen, Vol. I*, 406–409. Springer-Verlag, Berlin, 1966.

1939 P. Humbert. Sur les nombres de classes de certains corps quadratiques. *Comm. Math. Helvetici*, 12:233–245 und 13:67 (1940).

1952 K. Heegner. Diophantische Analysis und Modulfunktionen. *Math. Z.*, 56:227–253.

1954 S. Chowla und W. E. Briggs. On discriminants of binary quadratic forms with a single class in each genus. *Can. J. Math.*, 6: 463–470.

1955 N. C. Ankeny und S. Chowla. On the divisibility of the class number of quadratic fields. *Pacific J. Math.*, 5:321–324.

1961 G. B. Mathews. *Theory of Numbers.* Nachdruck von Chelsea Publ. Co., Bronx, NY.

1962 H. Cohn. *Advanced Number Theory.* Dover, New York.

1963 E. Grosswald. Negative discriminants of binary quadratic forms with one class in each genus. *Acta Arith.*, 8:295–306.

1966 A. Baker. Linear forms in the logarithms of algebraic numbers. *Mathematika*, 13:204–216.

1966 Z. I. Borevich und I. R. Shafarevich. *Number Theory.* Academic Press, New York.

1966 J. Steinig. On Euler's idoneal numbers. *Elem. of Math.*, 21: 73–96.

1967 H. M. Stark. A complete determination of the complex quadratic fields of class number one. *Michigan Math. J.*, 14:1–27.

1968 M. Deuring. Imaginäre-quadratische Zahlkörper mit der Klassenzahl Eins. *Invent. Math.*, 5:169–179.

1968 T. Honda. On real quadratic fields whose class numbers are multiples of 3. *J. reine u. angew. Math.*, 233:101–102.

1968 P. G. Lejeune-Dirichlet. *Vorlesungen über Zahlentheorie (mit Zusätzen versehen von R. Dedekind).* Chelsea Publ. Co., New York. Nachdruck. Erste Ausgabe 1863.

1968 C. L. Siegel. Zum Beweise des Starkschen Satz. *Invent. Math.*, 5:180–191.

1969 D. Shanks. Class number, a theory of factorization, and genera. In *1969 Number Theory Institute (Proc. Sympos. Pure Math., Vol. XX, State Univ. New York, Stony Brook, N.Y., 1969)*, 415–440, Providence, R.I. Amer. Math. Soc.

1969 H. M. Stark. On the "gap" in a theorem of Heegner. *J. Nb. Th.*, 1:16–27.

1970 B. A. Venkov. *Elementary Number Theory.* Wolters-Noordhoff Publishing, Gröningen. Übersetzt aus dem Russischen und überarbeitet von H. Alderson.

1970 Y. Yamamoto. On unramified Galois extensions of quadratic number fields. *Osaka J. Math.*, 7:57–76.

1971 A. Baker. Imaginary quadratic fields with class number 2. *Ann. of Math. (2)*, 94:139–152.

1971 H. M. Stark. A transcendence theorem for class number problems. *Ann. Math. (2)*, 94:153–173.

1972 D. W. Boyd und H. Kisilevsky. On the exponent of the ideal class groups of complex quadratic fields. *Proc. Amer. Math. Soc.*, 31:433–436.

1973 P. J. Weinberger. Exponents of the class groups of complex quadratic fields. *Acta Arith.*, 22:117–124.

1973 P. J. Weinberger. Real quadratic fields with class numbers divisible by n. *J. Nb. Th.*, 5:237–241.

1975 A. Baker. *Transcendental Number Theory.* Cambridge Univ. Press, Cambridge.

1976 D. A. Buell. Class groups of quadratic fields. *Math. of Comp.*, 30:610–623.

1976 S. Chowla und J. B. Friedlander. Some remarks on L-functions and class numbers. *Acta Arith.*, 28:414–417.

1976 D. Shanks. A survey of quadratic, cubic and quartic algebraic number fields (from a computational point of view). In *Proceedings of the Seventh Southeastern Conference on Combinatorics, Graph Theory, and Computing (Louisiana State Univ., Baton Rouge, LA)*, 15–40. Utilitas Math., Winnipeg, Manitoba.

1977 M. Craig. A construction for irregular discriminants. *Osaka J. Math.*, 14:365–402.

1977 H. M. Edwards. *Fermat's Last Theorem: A Genetic Introduction to Algebraic Number Theory.* Springer-Verlag, New York.

1977 D. M. Goldfeld. *The conjectures of Birch and Swinnerton-Dyer and the class numbers of quadratic fields.* Astérisque 41–42, 219–227.

1980 H. Davenport. *Multiplicative Number Theory.* Springer-Verlag, New York, 2. Ausgabe.

1980 A. Schinzel. On the relation between two conjectures on polynomials. *Acta Arith.*, 38:285–322.

1981 W. Kaufmann-Bühler. *Gauss: A Biographical Study.* Springer-Verlag, Berlin-Heidelberg-New York.

1981 H. Wada. A table of ideal class numbers of real quadratic fields. *Sophia Kokyoroku in Mathematics.* Number 10.

1981 D. B. Zagier. *Zetafunktionen und quadratische Körper.* Springer-Verlag, Berlin.

1982 L. K. Hua. *Introduction to Number Theory.* Springer-Verlag, Berlin.

1983 B. Gross und D. B. Zagier. Points de Heegner et dérivées de fonctions *L. C. R. Acad. Sci. Paris*, 297:85–87.

1983 J. Oesterlé. Nombres de classes des corps quadratiques imaginaires. *Séminaire Bourbaki, exp. 631.*

1983 R. J. Schoof. Class groups of complex quadratic fields. *Math. of Comp.*, 41:295–302.

1984 H. Cohen und H. W. Lenstra, Jr. Heuristics on class groups of number fields. In *Number Theory, Noordwijkerhout 1983, Lect. Notes in Math., 1068*, 33–62. Springer-Verlag, Berlin.

1984 G. Frei. Les nombres convenables de Leonhard Euler. *Sém. Th. des Nombres), Besançon, (1983–84).* 58 Seiten.

1984 J. J. Gray. A commentary on Gauss's mathematical diary, 1796–1814, with an English translation. *Expo. Math.*, 2:97–130.

1984 A. Weil. *Number theory, an Approach through History, from Hammurapi to Legendre.* Birkhäuser, Boston.

1984 D. B. Zagier. L-series of elliptic curves, the Birch-Swinnerton-Dyer conjecture, and the class number problem of Gauss. *Notices Amer. Math. Soc.*, 31(7):739–743.

1985 G. Frei. Leonhard Euler's convenient numbers. *Math. Intelligencer*, 7(3):55–58, 64.

1985 D. M. Goldfeld. Gauss's class number problem for imaginary quadratic fields. *Bull. Amer. Math. Soc.*, 13:23–37.

1985 J. P. Serre. $\Delta = b^2 - 4ac$. *Mathematical Medley*, 13(1):1–10. Siehe auch den Anhang in Flath (1989).

1986 B. Gross und D. B. Zagier. Heegner points and derivatives of L-series. *Invent. Math.*, 84:225–320.

1986 G. Lachaud. Sur les corps quadratiques réels principaux. In *Séminaire de Théorie des Nombres, Paris 1984–85. Progress in Math. #63*, 165–175. Birkhäuser Boston, Boston, MA.

1986 R. A. Mollin. On class numbers of quadratic extensions of algebraic number fields. *Proc. Japan Acad., Ser. A*, 62:33–36.

1986 R. Sasaki. A characterization of certain real quadratic fields. *Proc. Japan Acad. Ser. A Math. Sci.*, 62:97–100.

1987 J. M. Borwein und P. B. Borwein. *Pi and the AGM.* John Wiley & Sons, New York.

1987 D. A. Buell. Class groups of quadratic fields, II. *Math. of Comp.*, 48:85–93.

1987 G. Lachaud. On real quadratic fields. *Bull. Amer. Math. Soc.*, 17:307–311.

1987 J. Quer. Corps quadratiques de 3-rang 6 et courbes elliptiques de rang 12. *C. R. Acad. Sci. Paris*, 305(6):215–218.

1988 P. Llorente und J. Quer. On the 3-Sylow subgroup of the class group of quadratic fields. *Math. of Comp.*, 50:321–333.

1988 R. A. Mollin und H. C. Williams. A conjecture of S. Chowla via the generalized Riemann hypothesis. *Proc. Amer. Math. Soc.*, 102:794–796.

1988 J. Oesterlé. Le problème de Gauss sur le nombres de classes. *L'Enseign. Math.,* 2^e *série*, 34:43–67.

1988 M. Saito und H. Wada. A table of ideal class groups of imaginary quadratic fields. *Sophia Kokyoroku in Mathematics.* Number 28.

1988 M. Saito und H. Wada. Tables of ideal class groups of real quadratic fields. *Proc. Japan Acad., Ser. A*, 64:347–349.

1989 D. A. Buell. *Binary Quadratic Forms.* Springer-Verlag, New York.

1989 D. A. Cox. *Primes of the Form* $x^2 + ny^2$. Wiley-Interscience, New York.

1989 D. E. Flath. *Introduction to Number Theory.* Wiley, New York.

1989 R. A. Mollin und H. C. Williams. Real quadratic fields of class number one and continued fraction period less than six. *C. R. Math. Reports Acad. Sci. Canada*, 11:51–56.

1989 D. Shanks. On Gauss and composition, I and II. In *Proc. Conf. Canadian Nb. Th. Assoc., Banff*, herausgegeben von R. A. Mollin, 163–204. Kluwer Acad. Publ., Dordrecht.

1990 R. A. Mollin und H. C. Williams. Class number problems for real quadratic fields. In *Number Theory and Cryptography (Sydney, 1989)*, 177–195. Cambridge Univ. Press, Cambridge. In London Math. Soc. Lecture Notes Ser., 154.

1992 R. A. Mollin und H. C. Williams. Computation of the class number of a real quadratic field. *Utilitas Math.*, 41:259–308.

1993 H. Cohen. *A Course in Computational Algebraic Number Theory.* Springer-Verlag, Berlin.

1996 R. A. Mollin. *Quadratics.* CRC Press, Boca Raton, FL.

1998 M. J. Jacobson, Jr. Experimental results on class groups of real quadratic fields (extended abstract). In *Algorithmic Number Theory (Portland, OR, 1998)*, 463–474. Springer-Verlag, Berlin.

7

Aufeinanderfolgende Potenzen

1 Einführung

(a) Wenn man die Folge der Quadrate und Kuben ganzer Zahlen in aufsteigender Reihenfolge aufschreibt

$$4\ 8\ 9\ 16\ 25\ 27\ 36\ 49\ 64\ 81\ 100\ldots,$$

also

$$z_1 < z_2 < z_3 < z_4 < \cdots < z_n < z_{n+1} < \cdots,$$

dann kann man sich viele Fragen stellen. Zum Beispiel:

(I) Gibt es aufeinanderfolgende ganze Zahlen in dieser Folge? Natürlich: 8 und 9. Gibt es weitere? Wieviele? Nur endlich viele?

Wenn wir eine Liste von Quadraten und Kuben bis 1 000 000 absuchen, finden sich keine weiteren Beispiele. Ist dies allgemeingültig? Oder werden vielleicht zufällig weitere Quadrate und Kuben aufeinanderfolgende Zahlen sein?

Wenn man mithilfe eines Computers die Suche fortführt scheint es, als ob die Differenzen größer werden (aber nicht monoton), d.h. Quadrate und Kuben tauchen immer seltener auf. Allerdings sollten wir aus dieser experimentellen Beobachtung nicht schließen, dass es keine weiteren zusammenhängenden Quadrate und Kuben außer der 8 und 9 gibt.

Betrachte die folgende Situation, in der Zahlen trotz der abnehmenden Häufigkeit ihres Auftretens immer noch zu einer bestimmten Darstellung dienen können. Unter den Zahlen bis 10 000 gibt es nur 100

Quadrate, also $\frac{1}{100}$; bis 1 000 000 gibt es nur 1 000 Quadrate, also $\frac{1}{1000}$; bis 100 000 000 gibt es nur 10 000 Quadrate, also $\frac{1}{10000}$; usw. Die Quadrate werden also immer seltener. Trotzdem zeigte LAGRANGE, dass sich jede natürliche Zahl als Summe von (höchstens) *vier* Quadraten darstellen lässt.

Somit besetzen die Quadrate trotz ihrer immer größer werdenden Seltenheit „strategische Positionen", um als Summe von vier Quadraten jede natürliche Zahl ersetzen zu können.

Dies sollte nur erwähnt sein, um vor falschen Schlussfolgerungen zu bewahren.

Eine zweite Frage ist die folgende:

(II) Gegeben sei k ($k \geq 2$). Für wieviele Indizes n ist $z_{n+1} - z_n \leq k$ zutreffend? Nur endlich viele?

Wir könnten auch andere Folgen betrachten, die Potenzen beinhalten:

(b) Die Folge $z_1 < z_2 < z_3 < \cdots$ aller echten Potenzen ganzer Zahlen: Quadrate, Kuben, fünfte Potenzen, siebte Potenzen, usw.

(c) Für $a, b \geq 2$, $a \neq b$ könnten wir die Folge $z_1 < z_2 < z_3 < \cdots$ aller Potenzen von a oder b in Betracht ziehen.

Zum Beispiel ergibt sich für $a = 2$, $b = 3$:

$$4\ 5\ 9\ 16\ 27\ 32\ 64\ 81\ 128\ 243\ 256 \ldots .$$

(d) Für $E = \{p_1, \ldots, p_r\}$ mit $r \geq 2$ und Primzahlen p_i sei S die Menge aller natürlichen Zahlen, deren Primfaktoren in E liegen:

$$S\colon z_1 < z_2 < z_3 < \cdots .$$

Die Folge (c) ist natürlich eine Teilfolge einer Folge vom Typ (d).

Für jede der Folgen (b), (c), (d) könnten wir uns die Fragen (I) und (II) stellen. Für Folge (b) aller Potenzen könnten wir uns zudem die Frage stellen (die im Fall der anderen Folgen (a), (c), (d) uninteressant ist):

(III) Gibt es drei oder mehr aufeinanderfolgende natürliche Zahlen, die Potenzen sind? Wieviele? Keine? Endlich viele?

Bevor wir fortfahren sollten wir überlegen, ob diese Fragen vielleicht einfach nur kurios sind. Wir könnten uns GAUSS' Sicht der Dinge vor

Augen führen: „Jeder Dummkopf kann Fragen über Zahlen stellen, die sogar tausend weise Menschen nicht lösen können."

Handelt es sich bei den gestellten Fragen um diese Sorte? Nein! Da sie Potenzen (und somit Multiplikation in einer besonderen Form) sowie Differenzen beinhalten, wird die additive und multiplikative Struktur der ganzen Zahlen kombiniert. Etwas wie das lange ungelöste berühmte Problem von FERMAT: Kann die Summe zweier $n$ter Potenzen wieder eine $n$te Potenz sein, wenn $n > 2$?

Wie sich zeigen wird, trägt das Studium derartiger Fragen in substantieller Weise zum Wissen über die ganzen Zahlen bei, was die Untersuchungen mehr als rechtfertigt.

2 Geschichte

Unsere Aufarbeitung des Problems wird sich in gewisser Weise an der historischen Entwicklung orientieren. Wir werden diesen Abschnitt also kurz halten und nur einige Punkte unterstreichen.

(1) In DICKSONs wertvoller *History of the Theory of Numbers, Volume II*, findet sich, dass das Problem erstmals in einer Frage von PHILIPPE DE VITRY auftaucht: Kann $3^m \pm 1$ eine Zweierpotenz sein? Dies wurde von LEVI BEN GERSON (alias LEO HEBRACUS) beantwortet, der von 1288 bis 1344 in Spanien lebte. Er zeigte, dass wenn $3^m \pm 1 = 2^n$, dann $m = 2$, $n = 3$, d.h. die Zahlen sind 9 und 8.

(2) Im Jahr 1657 äußerte FERMAT in den „Deuxieme Deli aux Mathematiciens" (Brief an FRÉNICLE DE BESSY): Wenn p eine ungerade Primzahl ist und $n \geq 2$, dann ist $p^n + 1$ kein Quadrat; gleichermaßen gilt für $n \geq 4$, dass $2^n + 1$ kein Quadrat sein kann.

Ein Beweis, der von FRÉNICLE veröffentlicht worden war, wurde 1943 von HOFMANN entdeckt.

(3) Mit der Methode des unendlichen Abstiegs, die auf FERMAT zurückgeht, konnte EULER 1738 zeigen, dass wenn die Differenz zwischen einem Quadrat und einem Kubus ± 1 beträgt, dann handelt es sich bei den Zahlen um 9 und 8.

(4) Im Jahr 1844 fragt CATALAN in einem Brief an CRELLE (veröffentlicht in Volume I von CRELLEs Journal), nach einem Beweis dafür, dass die einzigen aufeinanderfolgenden Potenzen 8 und 9 sind. Diese Vermutung heißt heute „Catalans Vermutung". Mit anderen Worten stellte er die Behauptung auf, dass die Gleichung $X^U - Y^V = 1$ in vier Unbekannten, von denen zwei im Exponenten liegen, in natürlichen Zahlen

größer als 1 als einzige Lösung $x = 3$, $u = 2$, $y = 2$, $v = 3$ besitzt. Die einzigen Ergebnisse von CATALAN zu dieser Gleichung sind einfache Beobachtungen, die in seiner *Mélanges Mathematiques, XV*, viel später im Jahre 1885 veröffentlicht sind. Unter den verschiedenen Behauptungen von CATALAN findet sich ohne Beweis auch, dass wenn $x^y - y^x = 1$, dann $x = 2$, $y = 3$—dabei ist der Beweis eine ziemlich einfach Übungsaufgabe. Für eine Biographie von CATALAN, siehe JONGMANS (1996).

(5) In der Folgezeit wurden viele Spezialfälle von Potenzen mit kleinen Exponenten betrachtet, darunter von LEBESGUE (1850) sowie im letzten Jahrhundert NAGELL, OBLÁTH, S. SELBERG, CHAO KO, et al.

(6) Es folgte eine Reihe von Ergebnissen, die natürliche Zahlen x, y als Lösung von $x^m - y^n = 1$ Teilbarkeitsbedingungen auferlegten. Die wichtigsten Resultate in diesem Zusammenhang beziehen sich auf Exponenten m, n, die ungerade Primzahlen sind. Sie stammen von CASSELS, INKERI und HYYRÖ.

(7) In einer anderen Richtung gab es viele Resultate zu Abschätzungen über Anzahl und Größe möglicher aufeinanderfolgender Potenzen. Die wichtigsten Beiträge diesbezüglich kamen zunächst von HYYRÖ und vor allem von TIJDEMAN, der schlagkräftige Methoden aus der Theorie der diophantischen Approximation und BAKERs Abschätzungen über Linearformen von Logarithmen verwendete.

Die bereits bekannten Tatsachen und Methoden erlaubten die Bestimmung von Zahlen A, B mit $1 < A < B$ derart, dass wenn $x^m - y^n = 1$ mit $x, y, m, n > 2$, die beiden Potenzen im Intervall zwischen A und B liegen. Umfangreiche Berechnungen wurden angestellt, um die untere Schranke A zu vergrößern sowie die obere Schranke B zu verkleinern, um schließlich zu einer Überschneidung $B < A$ zu gelangen. Trotz aller Bemühungen verblieb ein großes Intervall, innerhalb dessen aufeinanderfolgende Potenzen liegen konnten.

(8) Schließlich kündigte MIHĂILESCU 2002 den Beweis von Catalans Vermutung an (veröffentlicht 2004). Nach einer tiefschürfenden Untersuchung der arithmetischen Eigenschaften von Kreisteilungskörpern ermöglichten die neuen Fakten in Kombination mit dem, was bekannt war, eine endgültige Lösung des Problems von Catalan.

Wir werden auf alle diese Punkte detailliert eingehen.

3 Spezialfälle

Wenn nicht anders angegeben, handelt es sich bei den in den Gleichungen auftretenden Zahlen um natürliche Zahlen.

Es ist günstig, wenn wir mit Levi ben Gersons Resultat beginnen; der hier angegebene Beweis stammt von M. Langevin, ein weiterer wurde von Franklin (1923) veröffentlicht.

3.1. Wenn $m, n \geq 2$ und $3^m - 2^n = \pm 1$, dann $m = 2$, $n = 3$. Somit sind in der Folge der Potenzen von 2 oder 3 die einzigen aufeinanderfolgenden ganzen Zahlen die 8 und 9.

Beweis. Wenn $2^n - 3^m = 1$ wäre, dann folgte $2^n \equiv 1 \pmod 3$, also ist n gerade und $n = 2n'$. Weiter $3^m = 2^{2n'} - 1 = (2^{n'} - 1)(2^{n'} + 1)$ und so $2^{n'} - 1 = 3^{m'}$, $2^{n'} + 1 = 3^{m-m'}$ mit $0 \leq m' < m - m'$. Subtraktion ergibt $2 = 3^{m'}(3^{m-2m'} - 1)$, daher $m' = 0$, $n' = 1$, $n = 2$, $m = 1$, im Widerspruch zur Voraussetzung.

Wenn $3^m - 2^n = 1$, dann kann $n = 2$ nicht sein, also $n \geq 3$ und daher $3^m \equiv 1 \pmod 8$. Somit ist m gerade, $m = 2m'$. Dann $2^n = 3^{2m'} - 1 = (3^{m'} - 1)(3^{m'} + 1)$, also $3^{m'} - 1 = 2^{n'}$, $3^{m'} + 1 = 2^{n-n'}$ mit $0 \leq n' < n - n'$. Subtraktion ergibt $2 = 2^{n'}(2^{n-2n'} - 1)$, also $n' = 1$, $n = 2n' + 1 = 3$ und $m = 2$. □

Die folgende Beobachtung ist ziemlich offensichtlich: Wenn $m, n \geq 2$ und wenn es für die Gleichung $X^m - Y^n = 1$ Lösungen in natürlichen Zahlen gibt und wenn p, q Primzahlen mit $p \mid m$, $q \mid n$ sind, dann gibt es auch natürliche Zahlen, die die Gleichung $X^p - Y^q = 1$ lösen. Es liegt also nahe, die Gleichung $X^p - Y^q = 1$ zu untersuchen, wobei p, q verschiedene Primzahlen sind.

Euler bewies im Jahre 1738 das folgende elementare Lemma:

Lemma 1. *Seien p, q Primzahlen und $x, y \geq 2$ derart, dass gilt $x^p - y^q = 1$. Wenn p ungerade ist, dann*

$$\begin{aligned} x - 1 &= a^q && \text{mit } y = aa',\ p \nmid aa', \\ \tfrac{x^p - 1}{x - 1} &= (a')^q && \operatorname{ggT}(a, a') = 1, \end{aligned}$$

oder

$$\begin{aligned} x - 1 &= p^{q-1}a^q && \text{mit } y = paa',\ p \nmid a', \\ \tfrac{x^{p-1}}{x - 1} &= p(a')^q && \operatorname{ggT}(a, a') = 1. \end{aligned}$$

In gleicher Weise gilt für ungerades q, dass

$$\begin{aligned} y+1 &= b^p \qquad \textit{mit } x = bb',\ q \nmid bb', \\ \tfrac{y^q+1}{y+1} &= (b')^p \qquad \mathrm{ggT}(b,b') = 1, \end{aligned}$$

oder

$$\begin{aligned} y+1 &= q^{p-1}b^p \qquad \textit{mit } x = qbb',\ q \nmid b', \\ \tfrac{y^q+1}{y+1} &= q(b')^p \qquad \mathrm{ggT}(b,b') = 1. \end{aligned}$$

Beweis. Der Beweis ist ziemlich einfach, wir werden ihn daher hier angeben. Es ist

$$y^q = x^p - 1 = (x-1)\frac{x^p-1}{x-1}.$$

Aber $\mathrm{ggT}\left(x-1, \frac{x^p-1}{x-1}\right) = 1$ oder p, da

$$\begin{aligned} \frac{x^p-1}{x-1} &= \frac{[(x-1)+1]^p - 1}{x-1} \\ &= (x-1)^{p-1} + \binom{p}{1}(x-1)^{p-2} + \cdots + \binom{p}{p-2}(x-1) + p. \end{aligned}$$

Zudem ist der fragliche größte gemeinsame Teiler genau dann gleich p, wenn $p \mid y$.

Als Nächstes stellen wir fest, dass $p^2 \nmid \frac{x^p-1}{x-1}$. Tatsächlich gilt wenn $p \mid \frac{x^p-1}{x-1}$, dass $p \mid x-1$; aber p^2 teilt jeden Summanden $(x-1)^{p-1}, \ldots, \binom{p}{p-2}(x-1)$, also kann p^2 nicht $\frac{x^p-1}{x-1}$ teilen. Wir haben damit die erste Aussage bezüglich $x-1$ und $\frac{x^p-1}{x-1}$ bewiesen. Der Beweis der zweiten Aussage verläuft ähnlich. □

Mithilfe derselben Methode bewies Euler:

Lemma 2. *Wenn q eine ungerade Primzahl ist mit $x, y \geq 2$ und $x^2 - y^q = 1$, dann gilt*

$$\begin{aligned} x-1 &= 2a^q \\ x+1 &= 2^{q-1}(a')^q \end{aligned}$$

oder

$$\begin{cases} x+1 = 2a^q \\ x-1 = 2^{q-1}(a')^q \end{cases}$$

wobei $a, a' \geq 1$, a ungerade ist und $\mathrm{ggT}(a,a') = 1$.

Unter Verwendung der Methode des unendlichen Abstiegs zeigte EULER:

3.2. Wenn $x, y \geq 1$ und $x^2 - y^3 = \pm 1$, dann $x = 3$, $y = 2$. In der Folge der Quadrate und Kuben sind 8 und 9 also die einzigen aufeinanderfolgenden ganzen Zahlen.

EULER hatte eigentlich gezeigt, dass die einzigen Lösungen der Gleichung $X^2 - Y^3 = \pm 1$ in positiven rationalen Zahlen $x = 3$, $y = 2$ sind; sein Beweis ist ziemlich trickreich.

Wir wollen an dieser Stelle auch anmerken, dass EULER die Methode des unendlichen Abstiegs verwendet hatte um zu zeigen, dass Fermats Gleichung $X^3 + Y^3 = Z^3$ nur triviale ganzzahlige Lösungen besitzt.

Im Jahr 1921 schlug NAGELL einen anderen Beweis vor, der zu einem früheren Resultat von LEGENDRE (1830, Band II, Seite 9) führt: Die Gleichung $X^3 + Y^3 = 2Z^3$ besitzt nur die Lösungen $x = y = z$ oder $x = -y$, $z = 0$ in ganzen Zahlen. LEGENDRES Beweis nutzte auch den unendlichen Abstieg. BACHMANN gab 1919 einen inkorrekten Beweis von LEGENDRES Resultat ohne die Methode des Abstiegs an.

Ein weiterer Weg zum Beweis von EULERS Ergebnis ohne die Methode des Abstiegs verwendet die Zahlen im kubischen Körper $K = \mathbb{Q}(\sqrt[3]{2})$. Aus

$$\mp 1 = u^3 - 2v^3 = (u - \sqrt[3]{2}v)(u^2 + \sqrt[3]{2}uv + \sqrt[3]{4}v^2)$$

folgt, dass $u - \sqrt[3]{2}v$ eine Einheit des Körpers K ist. Bekanntlich (siehe LEVEQUES Buch, Band II, Seiten 108–109) ist $u - \sqrt[3]{2}v$ bis auf das Vorzeichen eine Potenz der Fundamentaleinheit $-1 + \sqrt[3]{2}$:

$$u - \sqrt[3]{2}v = \pm(-1 + \sqrt[3]{2})^n.$$

Dann beweist man, dass n nicht negativ sein kann und $n \neq 2$. Schließlich zeigt man, dass n nicht größer als 2 sein kann, in dem man die Koeffizienten der beiden Seiten vergleicht und Kongruenzen modulo 3 betrachtet.

Also $u - \sqrt[3]{2}v = \pm(-1 + \sqrt[3]{2})$, was zu $x = 3$, $y = 2$ führt.

Nachdem $X^2 - Y^3 = \pm 1$ von EULER abgehandelt worden war, folgten als Nächstes die Gleichungen $X^2 - Y^m = \pm 1$ (mit $n \geq 5$).

Es geschah überraschenderweise, dass eine der Gleichungen ziemlich leicht zu behandeln war, während es bis zur Lösung der anderen noch 120 Jahre dauerte!

Welches ist die Leichte? Hier ist die Antwort. LEBESGUE verwendete ganze Gaußsche Zahlen, um 1850 zu zeigen:

3.3. Die Gleichung $X^m - Y^2 = 1$ besitzt nur triviale Lösungen in natürlichen Zahlen.

Beweis. Wir geben wieder nur einen Abriss des Beweises und überlassen die Details dem Leser. Wenn $x, y \geq 2$ und $x^m = y^2 + 1 = (y + i)(y - i)$, dann ist x ungerade, y muss gerade sein und es gibt ganze Zahlen u, v derart, dass

$$y + i = (u + iv)^m i^s \quad (\text{mit } 0 \leq s \leq 3);$$

somit

$$y - i = (u - iv)^m (-i)^s.$$

Also $x = u^2 + v^2$ und da x ungerade ist, muss u oder v gerade sein. Nach Subtraktion erhalten wir $2i = [(u+iv)^m - (u-iv)^m(-1)^s]i^s$ und dies führt zu

$$1 - \binom{m}{2} w^2 + \binom{m}{4} w^4 - \cdots \pm mw^{m-1} = \pm 1, \quad \text{wobei } w = u,$$

$v = \pm 1$ (wenn s gerade ist), oder $w = v$, $u = \pm 1$ (wenn s ungerade ist); also ist w gerade. Das Vorzeichen $-$ würde implizieren, dass w^2 Teiler von 2 wäre, was unmöglich ist. Das Vorzeichen $+$ ist ebenfalls unmöglich, was man dadurch erkennt, dass man die 2-adischen Werte der Summanden in obiger Relation betrachtet. □

Wir werden die Untersuchung der schwierigeren Gleichung $X^2 - Y^m = 1$ zurückstellen.

Die nächsten Gleichungen in der Reihe sind $X^3 - Y^m = \pm 1$, diese wurden von NAGELL im Jahr 1921 untersucht. Er zeigte zunächst:

3.4. (a) Wenn $m \geq 2$ keine Dreierpotenz ist, dann sind die einzigen Lösungen ungleich Null von $X^2 + X + 1 = Y^m$ das Paar $(-1, 1)$ für ungerades m, und $(-1, \pm 1)$, wenn m gerade ist.

(b) Wenn $m > 2$, dann sind $x = 1$ und $x = -2$ die einzigen Lösungen ungleich Null von $X^2 + X + 1 = 3Y^m$.

Zudem gibt es für $m = 2$ die Lösungen

$$\pm \frac{\sqrt{3}}{4}[(2 + \sqrt{3})^{2n+1} - (2 - \sqrt{3})^{2n+1}] - \frac{1}{2}$$

für $n = 0, 1, \ldots$.

Der Beweis ist sehr viel länger, also sei nur erwähnt, dass NAGELL im Fall (a) in $\mathbb{Q}(\omega) = \mathbb{Q}(\sqrt{-3})$ operierte, wobei $\omega = \frac{-1+\sqrt{-3}}{2}$ eine dritte Wurzel von 1 ist. Es führte ihn zu den Gleichungen $X \pm \omega = (Z - \omega)^q$ mit einer Primzahl $q > 3$ und den einzigen Lösungen $x = \pm 1, 0$. Für (b) und $m = 2$ arbeitete NAGELL im Körper $\mathbb{Q}(\sqrt{3})$, der die Fundamentaleinheit $2 + \sqrt{3}$ besitzt. Der Fall $4 \mid m$ führte ihn zur Gleichung $U^4 + V^4 = W^2$, die nach FERMAT nur triviale Lösungen besitzt. Im Falle einer Dreierpotenz m gelangte NAGELL zur Gleichung $X^3 + Y^3 = Z^3$. Für alle anderen Werte von m verwendete er den Körper $\mathbb{Q}(\omega)$.

Es war für NAGELL nun ein Leichtes zu zeigen:

3.5. Die Gleichungen $X^3 \pm 1 = Y^m$ (wobei m keine Zweierpotenz ist) haben nur triviale Lösungen in ganzen Zahlen.

Beweis. Wir können annehmen, dass es sich bei $m = q$ um eine Primzahl $q > 3$ handelt. Wenn x, y die Gleichung $y^q = x^3 \pm 1 = (x^2 \mp x + 1)(x \pm 1)$ erfüllen, dann ist $x^2 \mp x + 1 = a^q$ oder $3a^q$, mit einer ganzen Zahl a. Die Ersetzung von x durch $-x$ (im Falle negativen Vorzeichens) ergibt $x^2 + x + 1 = a^q$ oder $3a^q$, was zum Ergebnis führt. □

LJUNGGREN (1942, 1943) untersuchte die Gleichung $\frac{x^n-1}{x-1} = y^m$ und vervollständigte NAGELLS Resultat **(3.4)**(a) von oben und zeigte, dass dies auch gilt, wenn m eine Dreierpotenz ist.

Wir kehren nun zur Gleichung $X^2 - Y^n = 1$ (mit $n > 3$) zurück, die vielen Angriffen standhielt, bis sie schließlich gelöst wurde. Wie wir sehen werden, war die Lösung elementar, wenn auch sicher nicht einfach. Wir werden an dieser Stelle einige Teilresultate vorstellen. Und obwohl sie inzwischen vollkommen überflüssig sind, ist es sehr aufschlussreich zu sehen, auf welche Weisen die Mathematiker versuchten, die Gleichung zu lösen und wie die Verbindung zu anderen interessanten Problemen aussieht.

Wie bereits erwähnt, wurde die Gleichung erstmals in FERMATS „second définux mathématiciens“ von 1657 erwähnt. Wir geben FRÉNICLES Resultat an:

3.6. Wenn p eine ungerade Primzahl ist und $n \geq 2$, dann ist $p^n + 1$ kein Quadrat. Wenn $n \geq 4$, dann ist $2^n + 1$ kein Quadrat.

Beweis. Wenn $p^n = x^2 - 1 = (x + 1)(x - 1)$ mit $p \neq 2$, dann $\mathrm{ggT}(x + 1, x - 1) = 1$,

also

$$x + 1 = p^a$$
$$x - 1 = p^b$$

Daher $x - 1 = 1$, $x + 1 = p^n$ und somit $p^n = 3$, $n \geq 2$, was unmöglich ist.

Der Beweis der zweiten Behauptung verläuft ähnlich. □

Die schwächere Aussage, dass für jede ganze Zahl y die Zahl $y^n + 1$ keine vierte Potenz ist, wurde von S. SELBERG im Jahre 1932 bewiesen. Sein Beweis beruft sich auf ein älteres Resultat von STØRMER (1899), das im Zusammenhang mit der schnellen Berechnung der Dezimalbruchentwicklung von π steht.

Wir wollen diese unerwartete Verbindung erläutern und beginnen mit einem kurzen geschichtlichen Rückblick zur Berechnung von π.

Mithilfe der Methode der In- und Umkreis-Polygone fand ARCHIMEDES etwa um 250 B.C. die Abschätzung

$$3{,}1408 = \frac{223}{71} < \pi < \frac{22}{7} = 3{,}1428.$$

Im XIIten Jahrhundert berechnete FIBONACCI (LEONARDO DI PISA) π ungefähr zu $\frac{864}{275} = 3{,}1418$. ADRIANUS METIUS (1571–1635) schätzte

$$3{,}14150 = \frac{333}{106} < \pi < \frac{355}{113} = 3{,}14159.$$

Im XVIten Jahrhundert drückte F. VIÈTE (1540–1603) π durch ein unendliches Produkt aus:

$$\pi = \frac{2}{\sqrt{\frac{1}{2}}\sqrt{\frac{1}{2}+\frac{1}{2}\sqrt{\frac{1}{2}}}\sqrt{\frac{1}{2}+\frac{1}{2}\sqrt{\frac{1}{2}+\frac{1}{2}\sqrt{\frac{1}{2}}}}\cdots}$$

und dies ergab

$$3{,}1415926535 < \pi < 3{,}1415926537.$$

A. VAN ROOMAN berechnete π im Jahre 1593 auf 15 Dezimalstellen. LUDOLPH VAN CEULEN widmete sein Leben der Berechnung von π; zunächst errechnete er 1596 20 Dezimalen mithilfe eines Polygons mit 60×2^{29} Seiten! Nach seinem Tod veröffentlichte seine Frau im Jahr 1615

Ludolphs berechneten Wert von π, dieser besaß 32 korrekte Dezimalstellen. Seine Zeitgenossen waren so beeindruckt von dieser akribischen Arbeit, dass deutsche Autoren bis vor einiger Zeit die Zahl π als die Ludolph-Zahl bezeichneten.

Im XVIIten Jahrhundert tauchten unendliche Reihen und Produkte sowie Kettenbrüche auf: Die Reihe für den Arkussinus von I. Newton (1642–1727) im Jahr 1676; die Kettenbruchentwicklung für $\pi/4$ von Lord W. Brouncker (1620–1684) von 1658:

$$\frac{\pi}{4} = \frac{1}{1+}\frac{1^2}{2+}\frac{3^2}{2+}\frac{5^2}{2+}\cdots;$$

das unendliche Produkt für $\pi/2$ von J. Wallis (1616–1703) im Jahr 1655:

$$\frac{\pi}{2} = \frac{2}{1}\cdot\frac{2}{3}\cdot\frac{4}{3}\cdot\frac{4}{5}\cdot\frac{6}{5}\cdot\frac{6}{7}\cdot\frac{8}{7}\cdot\frac{8}{9}\cdot\cdots;$$

die Potenzreihe für die Arkustangens-Funktion von J. Gregory (1638–1675) aus dem Jahr 1671 und unabhängig davon die alternierende Reihe für $\pi/4$ von G. W. Leibniz (1646–1716) von 1674:

$$\frac{\pi}{4} = \arctan 1 = 1 - \frac{1}{3} + \frac{1}{5} - \frac{1}{7} + \cdots.$$

Im Jahr 1699 verwendete A. Sharp (1651–1742) die Reihe für den Arkustangens mit $\lambda = \frac{1}{\sqrt{3}}$, und berechnete π bis auf 72 Dezimalen—welch ein Unterschied zu den lebenslangen Anstrengungen, die die Polygonmethode erforderte.

Im Jahr 1737 (veröffentlicht 1744) berechnete Euler π auf 127 Dezimalen. Allerdings waren die Ausdrücke, die er 1755 entdeckte viel interessanter: Gerade Potenzen von π ausgedrückt durch Summen der Inversen gerader Potenzen der natürlichen Zahlen (Werte der ζ-Funktion):

$$\frac{\pi^2}{6} = \zeta(2) = \sum_{n=1}^{\infty}\frac{1}{n^2}$$
$$\frac{\pi^4}{90} = \zeta(4) = \sum_{n=1}^{\infty}\frac{1}{n^4}$$
$$\frac{\pi^6}{945} = \zeta(6) = \sum_{n=1}^{\infty}\frac{1}{n^6}.$$

Obige Formeln sind eher von theoretischem Interesse als für Berechnungen geeignet, allerdings werden wir hier nicht weiter auf die-

sen Punkt eingehen. EULER (veröffentlicht 1783) fand auch die folgende Verallgemeinerung von VIÈTES unendlichem Produkt für π. Wenn nämlich $0 < \theta < 180°$, dann ist

$$\theta = \frac{\sin\theta}{\cos\left(\frac{\theta}{2}\right)\cos\left(\frac{\theta}{2^2}\right)\cos\left(\frac{\theta}{2^3}\right)\cdots};$$

dies führt mit $\theta = 90°$ zu Viètes Formel.

Die Reihe für $\pi/4$ konvergiert zu langsam. Es ist allerdings möglich, die Konvergenz durch Verwendung der Summationsformel zu beschleunigen. Und zwar durch $\tan(x+y) = \frac{\tan x + \tan y}{1 - \tan x \tan y}$, setze $x = \arctan u$, $y = \arctan v$, dann $\arctan u + \arctan v = \arctan \frac{u+v}{1-uv}$.

Wenn man u, v derart wählt, dass $\frac{u+v}{1-uv} = 1$, dann ist $\pi/4 = \arctan u + \arctan v$.

Sei zum Beispiel $u = \frac{1}{2}$, also $v = \frac{1}{3}$, somit $(*)$ $\pi/4 = \arctan\frac{1}{2} + \arctan\frac{1}{3}$ (Formel von HUTTON, 1776); d.h.,

$$\frac{\pi}{4} = \left[\frac{1}{2} - \frac{1}{3}\left(\frac{1}{2}\right)^3 + \frac{1}{5}\left(\frac{1}{2}\right)^5 - \cdots\right] + \left[\frac{1}{3} - \frac{1}{3}\left(\frac{1}{3}\right)^3 + \frac{1}{5}\left(\frac{1}{3}\right)^5 - \cdots\right].$$

Diese Reihe konvergiert immer noch zu langsam. Um die Konvergenz zu verbessern, bestimmen wir v derart, dass

$$\frac{1}{2} = \frac{\frac{1}{3} + v}{1 - \frac{v}{3}},$$

also $v = \frac{1}{7}$, und in gleicher Weise v, dass gilt

$$\frac{1}{3} = \frac{\frac{1}{5} + v}{1 - \frac{v}{5}},$$

also $v = \frac{1}{8}$. Damit,

$$\arctan\frac{1}{2} = \arctan\frac{1}{3} + \arctan\frac{1}{7},$$
$$\arctan\frac{1}{3} = \arctan\frac{1}{5} + \arctan\frac{1}{8}.$$

Es folgt, dass

$$\frac{\pi}{4} = 2\arctan\frac{1}{2} - \arctan\frac{1}{7} \qquad (*)$$

und

$$\begin{aligned}\frac{\pi}{4} &= 2\arctan\frac{1}{3} + \arctan\frac{1}{7} \qquad (*)\\ &= 2\arctan\frac{1}{5} + \arctan\frac{1}{7} + 2\arctan\frac{1}{8}.\end{aligned}$$

Die erste Gleichung in dieser Formel stammt von HUTTON aus dem Jahr 1776 und EULER aus 1779, während die zweite Form G. VON VEGA (1756–1802) und dem Jahr 1794 zugeschrieben wird.

Beginnend mit $u = \frac{120}{119}$ wird $v = -\frac{1}{239}$, damit

$$\pi/4 = \arctan\frac{120}{119} - \arctan\frac{1}{119} = 4\arctan\frac{1}{5} - \arctan\frac{1}{239} \qquad (*)$$

was J. MACHINs (1680–1752) Formel ist.

Die Reihen in obigen Formeln konvergieren viel schneller und erlauben es, π auf viele Stellen genau zu berechnen: J. MACHIN (1706) mit 100 Stellen, F. DE LAGNY (1719) mit 127 Stellen und G. VON VEGA (1789) mit 136 Stellen.

Dieselbe Methode verwendete auch der Wunderrechner Z. DAHSE, Autor einer umfangreichen Primzahltabelle. Im Jahr 1844 berechnete DAHSE in zwei Monaten π auf 200 Stellen. Der Astronom T. CLAUSEN kam 1847 auf 248 Stellen. Spätere Bemühungen im vorletzten Jahrhundert stammen unter anderem von W. RUTHERFORD 1853 mit 400 Stellen, RICHTER 1855 mit 500 Stellen und W. SHANKS, der im Jahr 1873 707 Stellen erreichte (von denen allerdings „nur“ 527 Stellen korrekt waren, wie man später herausfand).

Nach dem Aufkommen von Computern wurde π 1962 von D. SHANKS und J. W. WRENCH unter Verwendung der Formel

$$\frac{\pi}{4} = 6\arctan\frac{1}{8} + 2\arctan\frac{1}{57} + \arctan\frac{1}{239}.$$

bis auf 100 000 Stellen berechnet. Diese Berechnungen wurden von J. GUILLOUD und M. BOUYER erweitert, die π 1974 bis auf eine Million Stellen genau berechneten und dabei GAUSS' Formel

$$\frac{\pi}{64} = \frac{3}{4}\arctan\frac{1}{18} + \frac{1}{2}\arctan\frac{1}{57} - \frac{5}{16}\arctan\frac{1}{239}.$$

verwendeten.

Zur Geschichte der Berechnung von π bis zum Jahr 1960 sei auf den Artikel von WRENCH (1960) verwiesen. Besonders auch auf die Spezialausgabe der Zeitschrift *Petit Archiméde* (1980) über π, die sehr gut dokumentiert und interessant zu lesen ist.

Einen explosionsartigen Fortschritt erlebte die Berechnung der Stellen von π mit der Implementierung des alten arithmetisch-geometrischen Mittels von GAUSS wie von den Brüdern BORWEIN vorgeschlagen. Dies wird ihrem sehr anregenden Buch *Pi and the AGM* (1987) beschrieben; siehe auch den Artikel von Bailey, Borwein, Borwein und Plouffe (1997) . Im Jahr 1997 gaben Y. KANADA und D. TAKAHASHI bekannt, dass sie 50 Milliarden Stellen von π berechnet hatten, die ich aber nicht gesehen habe. Genug? Nicht für KANADA, der im November 2002 zusammen mit einem zehnköpfigen Team 1 241 100 000 000 Stellen erreichte.

3,
14159 26535 89793 23846 26433 83279 50288 41971 69399 37510
58209 74944 59230 78164 06286 20899 86280 34825 34211 70679
82148 08651 32823 06647 09384 46095 50582 23172 53594 08128
48111 74502 84102 70193 85211 05559 64462 29489 54930 38196
44288 10975 66593 34461 28475 64823 37867 83165 27120 19091

45648 56692 34603 48610 45432 66482 13393 60726 02491 41273
72458 70066 06315 58817 48815 20920 96282 92540 91715 36436
78925 90360 01133 05305 48820 46652 13841 46951 94151 16094
33057 27036 57595 91953 09218 61173 81932 61179 31051 18548
07446 23799 62749 56735 18857 52724 89122 79381 83011 94912

98336 73362 44065 66430 86021 39494 63952 24737 19070 21798
60943 70277 05392 17176 29317 67523 84674 81846 76694 05132
00056 81271 45263 56082 77857 71342 75778 96091 73637 17872
14684 40901 22495 34301 46549 58537 10507 92279 68925 89235
42019 95611 21290 21960 86403 44181 59813 62977 47713 09960

51870 72113 49999 99837 29780 49951 05973 17328 16096 31859
50244 59455 34690 83026 42522 30825 33446 85035 26193 11881
71010 00313 78387 52886 58753 32083 81420 61717 76691 47303
59825 34904 28755 46873 11595 62863 88235 37875 93751 95778
18577 80532 17122 68066 13001 92787 66111 95909 21642 ...

Pour en savoir plus... tournez cette carte

Man fragt sich, welche Information von Interesse man wenn überhaupt aus solch umfangreichen Berechnungen gewinnen kann? Einen Eintrag in *Das Guinness Buch der Rekorde*? Gibt es etwas im Zusammenhang mit Atomkraft, das durch spezielle Muster in den Dezimalstellen von π ans Tageslicht käme? Tatsächlich schlug J. VON NEUMANN im Juni des Jahres 1949 vor, mit der ENIAC viele Stellen von π und e zu bestimmen und die Verteilung der Dezimalziffern statistisch zu untersuchen. Es zeigte sich, dass in der Tat jede Ziffer und jede kurze Folge von Ziffern wie 40533 unter den Stellen von π vorkommt. Beispielsweise taucht die Folge 0123456789 beginnend bei der 17 387 594 880ten Ziffer nach dem Dezimalpunkt auf. Dies ist natürlich nur eine experimentelle Beobachtung und stellt keinen Beweis für die „Normalität“ von π dar.

Wie oben gesehen kamen bei der Berechnung von π Formeln wie die mit $(*)$ markierten zur Anwendung. Diesbezüglich fragte D. GRAVÉ aus St. Petersburg, welche der Formeln

$$m \arctan \frac{1}{x} + n \arctan \frac{1}{y} = k\frac{\pi}{4}$$

wahr sind, wobei m, n, k, x, y ganze Zahlen ungleich Null sind und k, x, $y \geq 1$.

Dieses mit der schnellen Berechnung von π in Zusammenhang stehende Problem lieferte eine Verbindung mit der Gleichung $X^4 - 1 = Y^n$ dar, die von S. SELBERG untersucht wurde.

Im Jahre 1897 löste STØRMER GRAVÉs Problem; er gab 1899 noch einen einfacheren Beweis an. Setze $(a_1 + ib_1) \cdots (a_n + ib_n) = re^{i\phi}$ (a_j, b_j, ϕ reell und r reell und positiv), dann $\phi = \arctan \frac{b_1}{a_1} + \cdots + \arctan \frac{b_n}{a_n}$. Damit gilt $\arctan \frac{b_1}{a_1} + \cdots + \arctan \frac{b_n}{a_n} = s\pi$ (wobei s eine ganze Zahl ist) genau dann, wenn $(a_1 + ib_1) \cdots (a_n + ib_n)$ eine reelle Zahl ist. Insbesondere, $m \arctan \frac{1}{x} + n \arctan \frac{1}{y} = k\frac{\pi}{4}$ genau dann, wenn $(1 - i)^k (x + i)^m (y + i)^n$ reell ist. Dies führt zur ganzzahligen Lösung der Gleichungen $1 + X^2 = Y^n$ oder $1 + X^2 = 2Y^n$ (wobei $n \geq 3$, n ungerade sind). Wie wir in **(3.3)** gesehen haben, besitzt die erste der beiden Gleichungen nur triviale Lösungen. Was die zweite anbelangt, so zeigte STØRMER:

3.7. Wenn n keine Zweierpotenz ist und $n > 1$, dann sind $x = \pm 1$ die einzigen Lösungen von $1 + X^2 = 2Y^n$.

Übrigens war die Gleichung $1 + X^2 = 2Y^4$ von LAGRANGE (1777) mit der Methode des unendlichen Abstiegs gelöst worden, die einzigen Lösungen in natürlichen Zahlen sind $x = 239$, $y = 13$ (sowie die trivialen Lösungen $x = 1$, $y = 1$).

Unter Verwendung von **(3.7)** zeigte STØRMER, dass die einzigen Lösungen für GRAVÉs Problem die bereits mit $(*)$ markierten Ausdrücke sind. So waren irgendwie zufällig die Arkustangens-Formeln von Bedeutung bereits gefunden worden.

Nach dieser Bemerkung am Rande kehren wir zu SELBERGs Resultat zurück.

3.8. Wenn $n \geq 2$, dann besitzt die Gleichung $X^4 - Y^n = 1$ nur triviale Lösungen.

Beweis. Dies ist für gerades n leicht einzusehen, wie nehmen also an, dass n ungerade ist. Wenn y ungerade ist, dann $y^n = x^4 - 1 = (x^2 + 1)(x^2 - 1)$, somit gibt es natürliche Zahlen a, b derart, dass

$$x^2 + 1 = a^n$$
$$x^2 - 1 = b^n.$$

Durch Subtraktion gelangen wir leicht zu einem Widerspruch. Wenn y gerade ist, dann

$$x^2 + 1 = 2a^n$$
$$x^2 - 1 = 2^{n-1}b^n$$

(mit ganzen Zahlen a, b). Nach STØRMERs Resultat, $x^2 = 1$, $y = 0$, also eine triviale Lösung. □

Die nächsten Entwicklungsschritte beim Studium der Gleichung $X^2 - Y^n = 1$ waren unfruchtbare Versuche, falsche Richtungen und Streifzüge. Es ist allerdings interessant, diese Teilresultate einmal zu erwähnen, da einige der Methoden für andere Exponenten zur Anwendung kamen.

Im Jahr 1934 zeigte NAGELL, dass wenn $X^2 - Y^q = 1$ (mit einer Primzahl $q > 3$) eine nichttriviale Lösung besitzt, dann gilt $q \equiv 1 \pmod 8$. Darüber hinaus gibt es höchstens endlich viele Lösungen, was aus einem allgemeinen Satz von THUE folgt, der im letzten Abschnitt dieses Kapitels behandelt werden wird. In den Jahren 1940/1941 zeigte OBLÁTH, der durch die Sätze von WIEFERICH und MIRIMANOFF über Fermats Gleichung $X^p + Y^p = Z^p$ inspiriert war, dass wenn $X^2 - Y^q = 1$ eine nichttriviale Lösung besitzt, dann ist

$$2^{q-1} \equiv 1 \pmod{q^2} \quad \text{und} \quad 3^{q-1} \equiv 1 \pmod{q^2}.$$

Bekanntlich (und wie wir an späterer Stelle noch besprechen werden) sind obige Kongruenzen sehr selten erfüllt.

Inkeri und Hyyrö (1961) zeigten, dass wenn $x^2 - y^q = 1$, dann $q^2 \mid x$, $q^3 \mid y + 1$; ferner verbesserten sie Abschätzungen von OBLÁTH (1941, 1954) und zeigten, dass

$$x > 2^{q(q-2)} > 10^{3\times 10^9} \quad \text{und} \quad y > 4^{q-2} > 10^{6\times 10^5}.$$

Schließlich zeigte CHAO KO in zwei Arbeiten von 1960 und 1964, dass $X^2 - Y^n = 1$ für $n > 3$ keine Lösung in positiven ganzen Zahlen besitzt.

Der Beweis wurde später von CHEIN (1976) vereinfacht. Er basiert auf elementaren, obgleich nichttrivialen Ergebnissen. Das erste betrifft die Gleichung $X^2 - DY^2 = 1$ mit $D > 0$, D kein Quadrat.

Im Jahr 1657 merkte FERMAT in einem Brief an FRÉNICLE an, dass diese Gleichung unendlich viele ganzzahlige Lösungen besitzt, er gab aber wie üblich keinen Beweis an. Für die Geschichte dieser wichtigen

Gleichung siehe DICKSONS, *History of the Theory of Numbers, Band II* (1920) sowie HEATHS *Diophantus of Alexandria* (1885).

EULER trug ebenfalls zur Theorie dieser Gleichung bei, auch wenn er sie fälschlicherweise PELL zuschrieb, obwohl sie richtigerweise Fermats Gleichung genannt werden müsste—noch eine Gleichung von Fermat!

LAGRANGE benutzte die Theorie der Kettenbrüche um zu zeigen, dass die Gleichung tatsächlich unendlich viele Lösungen in ganzen Zahlen besitzt. Er wendete seine Methode auch beim Beweis seines berühmten Satzes an, dass die reellen Nullstellen quadratischer Gleichungen periodische, reguläre Kettenbruchentwicklungen haben und umgekehrt.

Hier eine kurze Zusammenfassung einiger der wichtigeren Eigenschaften der Lösungen von $X^2 - DY^2 = 1$ ($D > 0$, D kein Quadrat):

(a) Neben den trivialen Lösungen $x = \pm 1$, $y = 0$ gibt es unendlich viele Lösungen; weiterhin existiert eine Lösung (x_1, y_1) mit $y_1 > 0$, y_1 kleinstmöglich.

(b) Für jede ganze Zahl $n \neq 0$ seien x_n, y_n positive ganze Zahlen definiert durch $x_n + y_n\sqrt{D} = (x_1 + y_1\sqrt{D})^n$; dann ist $x_n^2 - Dy_n^2 = 1$.

(c) Umgekehrt, wenn x, y positive ganze Zahlen derart sind, dass $x^2 - Dy^2 = 1$, dann gibt es eine ganze Zahl $n \neq 0$ mit $x = x_n$, $y = y_n$.

(d) Wenn D quadratfrei ist, dann entsprechen die Lösungen den Einheiten $x + y\sqrt{D}$ von $\mathbb{Q}(\sqrt{D})$, die eine Norm von 1 haben. (Wenn $D \equiv 1 \pmod 4$, dann entsprechen die Einheiten $\frac{x+y\sqrt{D}}{2}$ mit $x \equiv y \equiv 1 \pmod 2$ und Norm 1 den Lösungen der Gleichung $X^2 - DY^2 = 4$).

Die Einheit $x_1 + y_1\sqrt{D}$ ist die *Fundamentaleinheit* von $\mathbb{Q}(\sqrt{D})$.

STØRMER bewies 1897 (und auf einfachere Weise 1908) das folgende interessante Lemma:

Wenn (x_n, y_n) eine Lösung von $X^2 - DY^2 = 1$ mit $n > 1$ ist, dann gibt es eine Primzahl die y_n, aber nicht D teilt.

STØRMER bewies ein ähnliches Resultat für die Gleichung $X^2 - DY^2 = -1$; dies war ein wenig einfacher.

Basierend auf STØRMERS Ergebnis bewies NAGELL im Jahr 1921 und erneut 1924 das folgende Teilbarkeitskriterium:

Wenn $x^2 - y^q = 1$ ($q > 3$ prim), dann $2 \mid y$ und $q \mid x$. (Wie wir sehen werden, wurde dies später von CASSELS verallgemeinert).

CHAO KOS Beweis des folgenden Ergebnisses erschien in zwei Etappen (1960, 1964) und ist inzwischen durch einen eleganten Beweis von CHEIN (1976) ersetzt worden:

3.9. Die Gleichung $X^2 - Y^q = 1$ besitzt keine Lösung in ganzen Zahlen ungleich Null.

Cheins zweiseitiger Beweis erschien im *American Mathematical Monthly.*

4 Teilbarkeitseigenschaften

Der Leitgedanke für die Aussagen in diesem Abschnitt ist es anzunehmen, dass es ganze Zahlen x, y ungleich Null gibt, die $x^p - y^q = 1$ erfüllen und Teilbarkeitsbedingungen abzuleiten, die von x, y, p, q erfüllt sein müssen. Diese Bedingungen sollten so einschränkend sein, dass sie die Existenz von Lösungen ausschließen. Beispielsweise zeigte Gerono 1870/71:

4.1. Wenn q eine Primzahl ist und $q^m - y^n = 1$ mit $m, n \geq 2$, dann $q = 3$, $y = 2$. In gleicher Weise folgt, dass wenn p eine Primzahl ist und wenn $x^m - p^n = 1$ mit $m, n \geq 2$ gilt, dann $p = 2$, $x = 3$.

Dies wurde wieder und wieder bewiesen, zum Beispiel von Catalan (1885), Carmichael (1909), Cassels (1953) und Rotkiewicz (1960).

Obláth gab im Jahr 1941 eine kleine Erweiterung bezüglich des Typs der Primfaktoren von x, y unter der Annahme von $x^m - y^n = 1$ an (mit $m, n \geq 2$). Siehe auch Hampel (1960).

Das bei Weitem wichtigste Resultat zu Teilbarkeitsbedingungen hypothetischer Lösungen stammt von Cassels (1960). Es ist sehr leicht anzugeben und auf den ersten Blick schwer zu erkennen, dass es eine solch wichtige Rolle für das Studium von Catalans Gleichung spielt.

4.2. Wenn p, q ungerade Primzahlen sind und $x, y \geq 2$ mit $x^p - y^q = 1$, dann gilt $p \mid y$, $q \mid x$.

Der Beweis verwendet Eulers Lemmata 1 und 2 und schwierige Abschätzungen, bleibt aber strikt elementar und beruft sich nicht auf hochkarätige Sätze. Es ist unmöglich, eine verständliche Skizze des Beweises in kleinem Rahmen anzugeben.

Ein unmittelbares Korollar ist die Lösung von Problem (III) der Einleitung durch Mąkowski (1962), was unabhängig auch Hyyrö (1963) zeigte.

4.3. Drei aufeinanderfolgende ganze Zahlen können keine echte Potenzen sein.

Beweis. Angenommen, die Aussage sei falsch. Dann haben wir $x^l - y^p = 1$, $y^p - z^q = 1$, wobei x, y, z natürliche Zahlen sind und die Exponenten l, p, q ohne Einschränkung der Allgemeinheit als prim angenommen werden können. Nach Cassels' Satz gilt $p \mid x$, $p \mid z$, also $p \mid x^l - z^q = 2$. Damit $x^l - y^2 = 1$, was nach LEBESGUEs Resultat **(3.3)** unmöglich ist. □

Als Nebenbemerkung werden wir nun Cassels' Satz auf Teilbarkeitseigenschaften von FERMAT- und FERENTINOU-NICOLACOPOULOU-Zahlen anwenden.

Die *nte Fermat-Zahl* ist $F_n = 2^{2^n} + 1$ $(n \geq 0)$, also $F_0 = 3$, $F_1 = 5$, $F_2 = 17$, $F_3 = 257$, $F_4 = 65537$. F_5 hat ungefähr 10 Ziffern, usw.

FERMAT äußerte, dass er glaube beweisen zu können und formulierte dies auch als Problem (Brief vom 18. Oktober 1640), dass alle Fermat-Zahlen Primzahlen sind, was für F_n mit $n \leq 4$ stimmt: Für F_5 und größere Fermat-Zahlen gelang es FERMAT nicht, die notwendigen Berechnungen durchzuführen, weil es ihm an umfangreichen Primzahltabellen mangelte.

Allerdings zeigte EULER:

Wenn p eine Primzahl ist und $p \mid F_n$, dann $p = 2^{n+2}k + 1$ (für irgendeine ganze Zahl k).

Aufgrund dieses Kriteriums war es für $n = 5$ ausreichend, die Primzahlen kongruent zu 1 modulo 128 zu prüfen. In dieser Weise leitete EULER im Jahr 1732 her, dass

$$F_5 = 641 \times 6700417.$$

Wir sehen also, dass FERMAT falsch lag! Aber es war nicht nur ein Zufall. Tatsächlich sind alle bis heute untersuchten Fermat-Zahlen zerlegbar—und genauer quadratfrei.

Eine interessante Verbindung mit den sogenannten Fermatquotienten zur Basis 2 entdeckten ROTKIEWICZ (1965) und Warren und Bray (1967):

$$q_p(2) = \frac{2^{p-1} - 1}{p}.$$

Nämlich: Wenn $p \mid F_n$, dann gilt $p^2 \mid F_n$ genau dann, wenn $(2^{p-1} - 1)/p \equiv 0 \pmod{p}$, d.h., $2^{p-1} \equiv 1 \pmod{p^2}$.

Letztere Kongruenz ist sehr selten erfüllt, wie wir bereits angemerkt hatten. Für $p < 2{,}5 \times 10^{15}$ erhalten wir $2^{p-1} \not\equiv 1 \pmod{p^2}$ außer für $p = 1093, 3511$.

Schinzel und Sierpiński vermuteten 1958, dass es unendlich viele quadratfreie Fermat-Zahlen gibt. Dies ist viel schwächer als die Vermutung von Eisenstein (1844), dass es unendlich viele prime Fermat-Zahlen gibt. Wenn Schinzels Vermutung stimmt, dann folgt aus der Tatsache, dass die Fermat-Zahlen paarweise teilerfremd sind, dass es unendlich viele Primzahlen p mit $2^{p-1} \not\equiv 1 \pmod{p^2}$ gibt. Und umgekehrt folgt aus einem berühmten Satz von Wieferich (siehe mein Buch von 1979), dass es unendlich viele Primzahlen p derart gibt, dass der *erste Fall* von Fermats letztem Satz für den Exponenten p wahr ist, d.h.:

„Es gibt keine ganzen Zahlen x, y, z, die keine Vielfachen von p sind und die $x^p + y^p = z^p$ erfüllen".

Obwohl Fermats letzter Satz von Wiles im Jahre 1994 bewiesen wurde, ist die obige Verbindung mit einem Spezialfall von Fermats Satz immer noch verblüffend. Tiefgründige Gewässer!

Wir führen nun die Zahlen von Ferentinou-Nicolacopoulou (1963) ein. Für $a \geq 2$, $n \geq 0$ sei

$$F_{a,n} = a^{a^n} + 1.$$

Das folgende Ergebnis ist ein einfaches Korollar von Cassels' Satz (Ribenboim (1979b)):

4.4. $F_{a,n}$ ist keine echte Potenz.

Beweis. Wenn $F_{a,n}$ eine echte Potenz wäre, könnten wir für eine Primzahl p schreiben $a^{a^n} + 1 = m^p$. Wenn q eine Primzahl ist, die a teilt, setze $a^n = qa'$, damit $m^p - (a^{a'})^q = 1$ und so $q \mid m$, was unmöglich ist. □

Insbesondere kann F_n keine echte Potenz sein; dieser Spezialfall benötigt nur Lebesgues Satz.

Eine weitere Konsequenz (Ribenboim (1979b)) ist die folgende Tatsache, die eine leichte Verbesserung von **(4.1)** darstellt:

4.5. Wenn $x^p - y^q = 1$ mit $p, q > 3$, dann haben x, y mindestens zwei ungerade Primfaktoren. Wir konzentrieren uns nun auf eine Verschärfung von Cassels' Satz von Hyyrö und Inkeri

Wenn p, q Primzahlen sind und $x^p - y^q = 1$, so folgt aus den vorangegangenen Resultaten, dass $p, q > 3$ und $p \mid y$, $q \mid x$.

Dann wird aus EULERs Lemma 1:

$$\begin{aligned} x-1 &= p^{q-1}a^q \\ \frac{x^p-1}{x-1} &= pu^p \quad \text{mit} \quad p \nmid u, y = pau, \\ y+1 &= q^{p-1}b^p \\ \frac{y^q+1}{y+1} &= qv^p \quad \text{mit} \quad q \nmid v, x = qbv. \end{aligned}$$

HYYRÖ zeigte 1964:

4.6. Unter Verwendung obiger Bezeichnungen:

$$\begin{array}{l} a = qa_0 - 1, \quad b = pb_0 + 1 \quad (\text{mit } a_0 \geq 1,\, b_0 \geq 1) \\ x \equiv 1 - p^{q-1} \pmod{q^2}, \quad y \equiv -1 + q^{p-1} \pmod{p^2}; \end{array}$$

somit gilt $q^2 \mid x$ genau dann, wenn $p^{q-1} \equiv \pmod{q^2}$, und $p^2 \mid y$ genau dann, wenn $q^{p-1} \equiv 1 \pmod{p^2}$.

Damit ist insbesondere $a \geq q-1$, $b \geq p+1$. Im Hinblick auf spätere Abschätzungen von x, y zeigte HYYRÖ auch:

4.7. Wenn $m > 3$ zerlegbar ist und $x^m - y^q = 1$ (wobei q eine Primzahl ist mit $q > 3$), und wenn p irgendeine Primzahl ist die m teilt, dann gilt $p^{q-1} \equiv 1 \pmod{q^2}$ und auch $q^2 \mid x$.

Das nächste Resultat von INKERI ist insofern sehr interessant, da es eine Verbindung mit der Klassenzahl von imaginär-quadratischen Zahlkörpern herstellt. Es verwendet auch eine altes Ergebnis von GAUSS über Kreisteilungspolynome.

In seinen *Disquisitiones Arithmeticae*, Artikel 357 (1801), zeigte GAUSS:

Wenn p eine ungerade Primzahl ist, dann gibt es Polynome $F, G \in \mathbb{Z}[X]$ derart, dass

$$4\frac{X^p-1}{X-1} = F(X)^2 - (-1)^{\frac{p-1}{2}} pG(X)^2.$$

Übrigens verwendete GAUSS diese Aussage bei der Bestimmung des Vorzeichens der Gaußschen Summe:

$$\tau = \sum_{j=1}^{p-1} \left(\frac{j}{p}\right) \zeta^j = \begin{cases} \sqrt{p} & \text{wenn } p \equiv 1 \pmod 4, \\ i\sqrt{p} & \text{wenn } p \equiv 3 \pmod 4. \end{cases}$$

Es dauerte vier Jahre, bis GAUSS die Lösung dieses Problems gefunden hatte. Erst 1805, als plötzlich, „Wie der Blitz einschlägt, hat sich das Räthsel gelöst“ (wie er später in einem Brief an einen Freund, den Astronomen OLBERS schrieb).

Für eine ungerade Primzahl p bezeichne $H(-p)$ die Klassenzahl des imaginär-quadratischen Zahlkörpers $\mathbb{Q}(\sqrt{-p})$.

GUT zeigte 1963, dass $H(-p) < \frac{p}{4}$ und diese Ungleichung verwendete INKERI. Es bedeutet im Grunde, dass $H(-p)$ nicht schnell wächst, wie zuvor von SIEGEL (1936) gezeigt worden war:

$$\log H(-p) \sim \log \sqrt{p}.$$

Hier INKERIs Ergebnis (1964):

4.8. Mit derselben Notation, wenn $x^p - y^q = 1$, dann:

(a) Wenn $p \equiv 3 \pmod 4$ und $q \nmid H(-p)$, dann $q^2 \mid x$, $y \equiv -1 \pmod{q^{2p-1}}$, $p^{q-1} \equiv 1 \pmod{q^2}$.

(b) Wenn $p \equiv q \equiv 3 \pmod 4$, $p > q > 3$ und $q \nmid H(-p)$, dann $q^2 \mid x$, $p^2 \mid y$, $x \equiv 1 \pmod{p^{2q-1}}$, $y \equiv -1 \pmod{q^{2p-1}}$, $p^{q-1} \equiv 1 \pmod{q^2}$ und $q^{p-1} \equiv 1 \pmod{p^2}$.

INKERI verwendete diese Teilbarkeitsbedingungen und Kongruenzen zusammen mit RIESELs Tabellen (1964) für die Reste von p^{q-1} modulo q^2 und q^{p-1} modulo p^2 um zum Beispiel zu zeigen: Unter den 946 Paaren von Primzahlen (p, q) mit $p \neq q$, $5 \leq p$, $q \leq 199$ gibt es 718 Paare, für die die Gleichung $X^p - Y^q = 1$ nur die triviale Lösung besitzt.

Diese Arbeit wurde später in zwei Artikeln von INKERI in den Jahren 1990 und 1991 fortgesetzt (eine zusammen mit AALTONEN verfasst). Unter den vielen Kriterien in diesen Arbeiten greifen wir uns die folgenden heraus:

4.9. Seien p, q verschiedene ungerade Primzahlen. Angenommen, dass es natürliche Zahlen x, y derart gibt, dass $x^p - y^q = 1$. Dann

(i) Wenn q kein Teiler von h_p ist (der Klassenzahl des Kreisteilungskörpers der $p$ten Einheitswurzeln), dann $q^2 \mid x$ und $p^{q-1} \equiv 1 \pmod{q^2}$.

(ii) Wenn p kein Teiler von h_q ist (der Klassenzahl des Kreisteilungskörpers der $q$ten Einheitswurzeln), dann $p^2 \mid y$ und $q^{p-1} \equiv 1 \pmod{p^2}$.

Dieses Kriterium eignet sich für Berechnungen und wurde verwendet, um für viele Paare verschiedener ungerader Primzahlen (p, q) zu

zeigen, dass die Gleichung $x^p - y^q = 1$ keine Lösung in positiven ganzen Zahlen besitzt. Beispielsweise gelang es INKERI auf diese Weise zu zeigen, dass $x^5 - y^7 = \pm 1$ keine Lösung in positiven ganzen Zahlen hat.

Ein Ergebnis anderen Typs bezüglich der Lösungen (x, y) von $x^m - y^n = 1$ mit $|x - y| = 1$ erzielte HAMPEL im Jahr 1956. Allgemeiner zeigte ROTKIEWICZ durch einen sehr leichten und eleganten Beweis im selben Jahr:

4.10. Wenn $a \geq 1$ eine ganze Zahl ist und wenn $\mathrm{ggT}(x, y) = 1$, $|x-y| = a$ und $x^m - y^n = a^n$, dann $x = 3$, $y = 2$, $m = 2$, $n = 3$, $a = 1$.

Der Beweis basiert auf einem Satz von BANG (1886) und ZSIGMONDY (1892), siehe Birkhoff und Vandiver (1904):

Wenn $a > b \geq 1$ mit $\mathrm{ggT}(a, b) = 1$, dann gibt es für jedes $n > 1$ eine Primzahl p derart, dass $p \mid a^n - b^n$, aber $p \nmid a^m - b^m$ für alle m, $1 \leq m < n$ (außer wenn $a = 2$, $b = 1$, $n = 6$ oder $n = 2$, a, b ungerade sind und $a + b$ eine Zweierpotenz ist).

5 Abschätzungen

In diesem Abschnitt wollen wir annehmen, dass Catalans Gleichung nichttriviale Lösungen besitzt. Absicht wird es sein, Abschätzungen für die Größe und Anzahl der hypothetischen Lösungen zu geben.

Zunächst suchen wir für gegebene verschiedene ganze Zahlen $a, b \geq 2$ nach natürlichen Zahlen u, v, die die Gleichung $a^U - b^V = 1$ lösen.

Danach betrachten wir feste Exponenten $m, n \geq 2$ und prüfen die möglichen Lösungen der Gleichung $X^m - Y^n = 1$.

Schließlich werden wir Lösungen der exponentiellen diophantischen Gleichung $X^U - Y^V = 1$ in natürlichen Zahlen untersuchen.

A Die Gleichung $a^U - b^V = 1$

LEVEQUE bewies im Jahr 1952 das folgende Resultat, das sich auch als einfache Konsequenz von HAMPELs Resultat gewinnen ließe (siehe **(4.9)**):

5.1. Für $a, b \geq 2$ besitzt $a^U - b^V = 1$ höchstens eine Lösung in natürlichen Zahlen u, v, außer $a = 3$, $b = 2$ mit den zwei Lösungen $u = v = 1$ und $u = 2$, $v = 3$.

Ein in gewisser Hinsicht interessantes Korollar betrifft die Summen aufeinanderfolgender Potenzen ganzer Zahlen:

$$S_1(n) = \sum_{j=1}^{n} j = \frac{n(n+1)}{2}$$
$$S_2(n) = \sum_{j=1}^{n} j^2 = \frac{n(n+1)(2n+l)}{6}$$
$$S_3(n) = \sum_{j=1}^{n} j^3 = \frac{n^2(n+1)^2}{4}, \quad \text{usw.}\ldots.$$

Allgemeiner wird $S_k(n) = \sum_{j=1}^{n} j^k$ durch ein Polynom des Grades $k+1$ gegeben, mit Koeffizienten, deren Nenner $k+1$ teilt und durch die Bernoulli-Zahlen ausgedrückt werden können—die allerdings im Übrigen für den momentanen Zweck irrelevant sind. Wie oben gesehen, ist $S_3(n) = [S_1(n)]^2$ für jedes $n \geq 1$.

Das Korollar aus LeVeques Resultat ist das folgende:

5.2. Wenn $t \geq 1$ und $u, v \geq 2$ die Eigenschaft haben, dass für jedes $n \geq 1$ gilt $S_v(n) = [S_1(n)]^u$, dann $v = 3$, $t = 1$, $u = 2$.

Dies gilt nur, weil die einzige Lösung von $2^V + 1 = (2^T - 1)^U$ in natürlichen Zahlen $t = 1$, $u = 2$, $v = 3$ ist.

Es sei hier noch erwähnt, dass Thue bereits im Jahre 1908 das folgende Resultat erzielt hatte:

Wenn $E = \{p_1, \ldots, p_r\}$, wobei $r \geq 2$ und jedes p_i eine Primzahl ist, und wenn S die Menge der natürlichen Zahlen ist, deren Primfaktoren alle aus E stammen, dann gibt es für jedes $k \geq 2$ höchstens endlich viele ganze Zahlen $z, z' \in S$ mit $z - z' = k$. Insbesondere hat für $a, b \geq 2$, $k \geq 1$ die Gleichung $a^U - b^V = k$ höchstens endlich viele Lösungen in ganzen Zahlen u, v. Dies wurde erneut von Pólya im Jahr 1918 gezeigt. Im Jahr 1931 gab Pillai eine quantitative Form dieses Satzes an, die eine obere Schranke für die Anzahl der Lösungen in natürlichen Zahlen der Ungleichung $0 < a^u - b^v \leq k$ beinhaltete (wobei $\frac{\log b}{\log a}$ irrational ist). Später im Jahr 1936 zeigte Herschfeld, dass $2^U - 3^V = 1$ höchstens eine Lösung für jedes hinreichend große k besitzt; Pillai erweiterte dieses Resultat 1936 auf beliebige Basen $a, b \geq 2$.

Cassels gab 1953 einen Algorithmus an, um die Lösung von $a^U - b^V = 1$ zu berechnen, falls es eine solche gibt. Er gab auf diese Weise einen neuen Beweis von LeVeques Resultat an.

5.3. Sei $a, b \geq 2$ und A (bzw. B) das Produkt der verschiedenen ungeraden Primteiler von a (bzw. b). Wenn $u, v \geq 2$ die Gleichung $a^u - b^v = 1$ erfüllen, dann:

(a) entweder $a = 3$, $b = 2$, $u = 2$, $v = 3$ oder

(b) u, v sind die kleinsten natürlichen Zahlen derart, dass $a^u \equiv 1 \pmod{B}$ und $b^v \equiv -1 \pmod{A}$.

Wir müssen daher also nur diese Werte u, v als mögliche Lösungen in Betracht ziehen.

B Die Gleichung $X^m - Y^n = 1$

Unsere Absicht ist es nun, Aussagen über die Anzahl und die Größe von Lösungen dieser Gleichung zu treffen. Den Beweis, dass diese Gleichung nur endlich viele Lösungen hat, kann man auf folgende Weisen führen:

(a) indem man zeigt, dass die Existenz unendlich vieler Lösungen zu einem Widerspruch führt;

(b) indem man explizit eine ganze Zahl $N \geq 1$ bestimmt, so dass die Anzahl der Lösungen höchstens gleich N sein kann;

(c) durch Bestimmung einer ganzen Zahl $C \geq 1$ mit der Eigenschaft, dass jede Lösung (x, y) die Bedingungen $x \leq C$, $y \leq C$ erfüllt. Durch Testen aller möglichen natürlichen Zahlen bis C ist es dann möglich, alle Lösungen zu finden.

Im Fall (a) gibt es keinen Hinweis darauf, wieviele Lösungen es gibt oder wie groß sie sind.

Im Fall (b) gibt es keinen Hinweis darauf, wie groß die Lösungen sind; man kann daher selbst wenn $N - 1$ Lösungen bekannt sind, nichts darüber aussagen, ob es noch eine weitere Lösung gibt oder wie groß diese ist.

Der Fall (c) schließlich ist der zufriedenstellendste. Wenn die durch die Methode des Beweises gefundene Konstante C allerdings viel zu groß ist—wie es häufig der Fall ist—dann ist es unmöglich, alle Lösungen zu finden.

Unser erstes Resultat ist eine einfache Konsequenz eines mächtigen klassischen Satzes, der auf Siegel (1929) zurückgeht und auf Ideen von Thue zu diophantischer Approximation basiert.

Es ist nützlich, die folgende etwas detailliertere Form von Siegels Satz zu verwenden, so wie von Inkeri und Hyyrö (1964b) angegeben (siehe auch den maßgeblichen Artikel von LeVeque (1964)):

Sei $m, n \geq 2$ mit $\max\{m, n\} \geq 3$. $f(X) \in \mathbb{Z}[X]$ habe den Grad n und es sei angenommen, dass alle Nullstellen einfach sind. Wenn a eine ganze Zahl ungleich Null ist, dann hat die Gleichung $f(X) = aY^m$ höchstens endlich viele Lösungen.

Insbesondere:

5.4. Für jede natürliche Zahl k hat die Gleichung $X^m - Y^n = k$ höchstens endlich viele Lösungen.

Dieses Resultat kann man auch als Konsquenz des folgenden interessanten Satzes von Mahler (1953) beweisen:

Wenn a, b ganze Zahlen ungleich Null sind, $x, y \geq 1$, $\mathrm{ggT}(x, y) = 1$, $m \geq 2$, $n \geq 3$, dann geht der größte Primfaktor der Zahl $ax^m - by^n$ gegen Unendlich, wenn $\max\{x, y\}$ gegen Unendlich geht.

Insbesondere gilt für hinreichend große x, y, dass $x^m - y^n$ nicht gleich k sein kann.

Ein elementarerer Beweis eines Spezialfalles von **(5.3)**, der auf Hyyrö (1964) zurückgeht, resultiert aus einer Anwendung eines Satzes von Davenport und Roth (1955) über diophantische Approximation. Ohne die verwendete Methode genauer zu beschreiben, geben wir Hyyrös Resultat an:

5.5. Die Anzahl der Lösungen von $X^m - Y^n = 1$ beträgt höchstens $e^{631m^2n^2}$.

Diese obere Grenze ist ziemlich groß, vor allem angesichts der Vermutung, dass es keine Lösungen gibt!

Darüberhinaus zeigte Hyyrö:

5.6. Wenn p, q Primzahlen sind, $x, y \geq 2$ und $x^p - y^q = 1$, dann gilt $x, y > 10^{11}$.

Die Lösungen können also nicht zu klein sein. Ferner gilt für den Fall, dass einer der Exponenten zerlegbar ist:

5.7. Wenn $x^m - y^n = 1$ und m zerlegbar ist, dann $x > 10^{84}$, wohingegen für zerlegbares n gilt, dass $y > 10^{84}$.

Es ist noch schlimmer (oder besser?) wenn m, n beide zerlegbar sind:

5.8. Wenn $x^m - y^n = 1$ und m, n zerlegbar sind, dann x^m, $y^n > 10^{10^9}$.

Hyyrö gab auch einen Algorithmus zum Finden der Lösungen (wenn es welche gibt) von $X^p - Y^q = 1$ an, wobei p, q Primzahlen sind. Er beinhaltet reguläre Kettenbruchentwicklungen. Für eine positive reelle Zahl α definieren wir sukzessive die ganzen Zahlen c_0, c_1, c_2, ..., und die positive reellen Zahlen α_1, α_2, ... durch die Relationen

$$\begin{aligned}
\alpha &= c_0 + \frac{1}{\alpha_1} \quad \text{wobei } c_0 = [\alpha], \text{ also } \alpha_1 > 1,\\
\alpha_1 &= c_1 + \frac{1}{\alpha_2} \quad \text{wobei } c_1 = [\alpha_1], \text{ also } \alpha_2 > 1,\\
\alpha_2 &= c_2 + \frac{1}{\alpha_3} \quad \text{wobei } c_2 = [\alpha_2], \text{ also } \alpha_3 > 1,
\end{aligned}$$

usw. Somit

$$\alpha = c_0 + \cfrac{1}{c_1 + \cfrac{1}{c_2 + \cfrac{1}{c_3 + \cdots \; \cfrac{1}{+\cfrac{}{c_n}+\cdots}}}}$$

und wir schreiben

$$\alpha = [c_0, c_1, c_2, \ldots, c_n, \ldots].$$

Obigen Bruch nennt man den *regulären Kettenbruch von* α. Wir definieren zudem

$$\begin{aligned}
A_0 &= c_0 \qquad A_1 = c_0 c_1 + 1\\
B_0 &= 1 \qquad B_1 = c_1,
\end{aligned}$$

und für $2 \le i \le n$,

$$\begin{aligned}
A_i &= c_i A_{i-1} + A_{i-2},\\
B_i &= c_i B_{i-1} + B_{i-2}.
\end{aligned}$$

Insbesondere, $B_0 \le B_1 < B_2 < B_3 < \cdots$.

Die Brüche A_i/B_i nennt man die *Konvergenten* von α, und $A_i/B_i = [c_0, c_1, \ldots, c_i]$ für jedes $i \ge 0$.

Wir rufen einige grundlegende Eigenschaften in Erinnerung:
(a) für jedes $i \geq 0$ gilt $\mathrm{ggT}(A_i, B_i) = 1$,
(b) $A_i/B_i \leq \alpha$ genau dann, wenn i gerade ist.
LAGRANGE zeigte im Jahr 1798:
(c) Für jedes $i \geq 0$,

$$\frac{1}{B_i(B_i + B_{i+1})} < \left|\alpha - \frac{A_i}{B_i}\right| < \frac{1}{B_i^2}.$$

(d) Wenn a, b ganze Zahlen ungleich Null sind mit $b \geq 1$, $\mathrm{ggT}(a, b) = 1$ und $\left|\alpha - \frac{a}{b}\right| < \frac{1}{2b^2}$, dann gibt es $i \geq 0$ derart, dass $a = A_i$, $b = B_i$.
Dies ist HYYRÖs Resultat:

5.9. Es seien p, q verschiedene ungerade Primzahlen. Wenn es ganze Zahlen $x, y \geq 2$ derart gibt, dass $x^p - y^q = 1$, so kann man sie durch den folgenden Algorithmus finden.
Sei

$$\alpha = \frac{q^{\frac{p-1}{p}}}{p^{\frac{q-1}{q}}};$$

betrachte die reguläre Kettenbruchentwicklung:

$$\alpha = [c_0, c_1, c_2, \dots].$$

Seien A_i/B_i die Konvergenten. Dann hat jede Lösung die Form

$$x = p^{q-1}A_i^q + (-1)^i, \quad y = q^{p-1}B_i^p - (-1)^i,$$

wobei $i \geq 0$ irgendein Index ist mit:
(i) $A_i > 1$, $B_i > 1$,
(ii) $A_i \equiv (-1)^{i+1} \pmod q$, $B_i \equiv (-1)^i \pmod p$,
(iii) $A_i \equiv (-1)^{i\frac{q^{p-1}-1}{p}} \pmod p$, $B_i \equiv (-1)^{i+1\frac{p^{q-1}-1}{q}} \pmod q$,
(iv) $c_{i+1} \geq (-1)^{i+1}A_i^{r-2}$, $c_{i+1} \geq (-1)^i B_i^{r-2}$, wobei $r = \min\{p, q\}$.

Dieser Algorithmus zeigt nicht an, ob es eine nichttriviale Lösung gibt. Falls es aber eine solche gibt, so wird er sie schließlich finden.

In seinem Artikel erzielt HYYRÖ weitere Ergebnisse zu Catalans Gleichung, die aus seiner Untersuchung der exponentiell-diophantischen Gleichung $X^n - d^U Y^n = \pm 1$ resultieren, wobei $n \geq 5$, $d \geq 2$ gegebene ganze Zahlen sind.

Nachdem gezeigt war, dass diese Gleichung höchstens eine ganzzahlige Lösung u, x, y mit $0 \leq u < n$, $x \geq 2$, $y \geq 1$ haben kann, konnte er beweisen:

5.10. Wenn p, q ungerade Primzahlen sind, wobei $m > 2$, $e \geq q$ und p^e Teiler von m ist, dann besitzt $X^m - Y^q = \pm 1$ keine Lösungen in ganzen Zahlen $x \geq 2$, $y \geq 1$.

5.11. Wenn $n \geq 5$, $a \geq 2$ ganzzahlig sind, dann haben die exponentiell-diophantischen Gleichungen $a^U - Y^n = \pm 1$ höchstens endlich viele Lösungen in ganzen Zahlen.

5.12. Für $a \geq 2$ haben die exponentiell-diophantischen Gleichungen $a^U - Y^V = \pm 1$ höchstens $(a+1)^\nu$ ganzzahlige Lösungen, wobei ν die Anzahl der verschiedenen Primfaktoren von a sind.

C Die Gleichung $X^U - Y^V = 1$

Die bisherigen Ergebnisse reichen nicht aus um zu schließen, dass die exponentiell-diophantische Gleichung mit vier Unbekannten $X^U - Y^V = 1$ nur endlich viele Lösungen besitzt. Tatsächlich ist dies wahr und wurde erstmalig von Tijdeman im Jahr 1976 unter Verwendung von Bakers Abschätzungen für Linearformen in Logarithmen gezeigt.

Baker wendete seine Abschätzungen an, um effektive Schranken für Lösungen verschiedener Typen von diophantischen Gleichungen anzugeben (siehe zum Beispiel sein Buch von 1975): diese Resultate stellen eine maßgebliche Verbesserung gegenüber den früheren qualitativen Aussagen von Thue, Siegel und Roth dar.

5.13. Wenn $m, n \geq 3$, $x, y \geq 1$ und $x^m - y^n = 1$, dann

$$\max\{x, y\} < \exp\exp\{(5n)^{10} m^{10m}\}$$

und

$$\max\{x, y\} < \exp\exp\{(5m)^{10} n^{10n}\}.$$

Tijdeman zeigte:

5.14. Es gibt eine effektiv berechenbare Zahl $C > 0$ derart, dass wenn x, y, m, n natürliche Zahlen sind mit $m, n \geq 2$ und $x^m - y^n = 1$, dann $\max\{x, y, m, n\} < C$.

Tijdemans Resultat könnte man als „Erledigung“ des Problems ansehen. Tatsächlich ist mit diesem Satz gezeigt, dass das Problem entscheidbar ist. Es ist nun „nur noch“ eine Frage, alle 4-Tupel natürlicher Zahlen kleiner als C zu probieren. An dieser Stelle bedeutet „nur noch“ allerdings zuviel, da die für C ermittelten Werte zu groß sind.

Tatsächlich war der aus TIJDEMANs Satz gewonnene und im Jahr 1996 von LANGEVIN berechnete Wert

$$C < \exp\exp\exp\exp\{730\}.$$

Haben Sie jemals versucht, eine solche Zahl abzuschätzen? Aus wievielen Ziffern besteht sie? Wenn man C mit Zahlen vergleicht, die in der Astronomie vorkommen, sollte der Wert von C noch nicht einmal astronomisch genannt werden. Aber um die Wahrheit zu sagen hat C kein Recht so groß zu sein—die abgeschätzte Größe von C drückt nur unsere Unkenntnis aus.

Der Satz von TIJDEMAN hatte eine nicht zu unterschätzende Rechenaktivität zur Folge, die dazu verwendet wurde, die Menge von Paaren (p, q) von Primzahlexponenten (p, q) zu vergrößern, für die $x^p - y^q = 1$ als unmöglich gezeigt werden kann, sobald $|x|$, $|y| > 1$. Die Berechnungen verlangten nach einer Verfeinerung der Kriterien. Die Suche nach kleineren unteren Schranken für die Exponenten erforderten schärfere Schranken für Linearformen in Logarithmen. Es war technisch schwierig, derartige Schranken zu erlangen.

Der Leser möge die Artikel von Bennett, Blass, Glass, Meronk und Steiner (1997) und Laurent, Mignotte und Nesterenko (1995) zu Rate ziehen. Kurz nachdem TIJDEMAN seinen Satz bewiesen hatte, zeigte Langevin (1976), dass wenn $x^m - y^n = 1$ mit m, n, x, $y > 1$, dann ist $\max\{m, n\} < 10^{110}$.

O'Neil (1995) zeigte, dass für prime Exponenten p und q gilt $\max\{p, q\} < 3{,}18 \times 10^{17}$ und p oder q sind kleiner als $2{,}6 \times 10^{12}$.

MIGNOTTE teilte mit, dass es ihm gelungen ist zu zeigen, dass wenn $p < q$, dann $p < 7{,}15 \times 10^{11}$ und $q < 7{,}78 \times 10^{16}$.

Auf der anderen Seite wurden untere Schranken für die möglichen Exponenten unter der Verwendung von Kriterien hergeleitet, die eine Verbesserung der schon in **(4.8)** und und **(4.9)** beschriebenen bahnbrechenden Resultate von INKERI darstellen; wie in diesen Abschnitten geschildert, erforderte es das letztere Kriterium für den Fall $p \equiv 1 \pmod 4$ festzustellen, ob q die Klassenzahl h_p des Kreisteilungskörpers $\mathbb{Q}(\zeta_p)$ teilt. Es sei erwähnt, dass h_p bis heute nur für $p < 71$ berechnet worden ist. Die Klassenzahl ist das Produkt der Faktoren $h_p = h_p^- h_p^+$, wobei h_p^+ die Klassenzahl des reellen Unterkörpers $\mathbb{Q}(\zeta_p + \zeta_p^{-1})$ ist — und dieser Faktor ist derjenige, der so schwer zu berechnen ist.

Einiges an Rechenaufwand konnte durch das folgende Kriterium von MIGNOTTE und ROY (1993) eingespart werden.

5.15. Sei $p-1=2^d s$ mit einer ungeraden ganzen Zahl s. Sei K' der Unterkörper von $\mathbb{Q}(\zeta_p)$ mit Grad 2^d, und sei h' seine Klassenzahl. Wenn $x^p - y^q = 1$ mit Primzahlen p, q und $|x|, |y| > 1$ sowie $p \equiv 1 \pmod 4$, dann ist q Teiler von h' oder $p^{q-1} \equiv 1 \pmod{q^2}$.

Im Jahr 1994 gab SCHWARZ ein Kriterium an, das nur den leichter berechenbaren Faktor h_p^- beinhaltete und dadurch eine substantielle Erweiterung der Berechnungen ermöglichte:

5.16. Unter Verwendung der vorangegangenen Bezeichnungen teilt entweder $p^{q-1} \equiv 1 \pmod{q^2}$ oder q den ersten Faktor h_p^- der Klassenzahl von K'.

BUGEAUD und HANROT leiteten 1999 weitere notwendige Bedingungen für den größten Exponenten her:

5.17. Wenn $p < q$, dann teilt q den Faktor h_p^- der Klassenzahl h_p von $\mathbb{Q}(\zeta_p)$.

Im Jahr 1999 gab MIHĂILESCU ein neues Kriterium an, das unabhängig von den Werten der Klassenzahlen war.

5.18. Unter Verwendung der vorangegangenen Bezeichnungen gilt sowohl $p^{q-1} \equiv 1 \pmod{q^2}$ als auch $q^{p-1} \equiv 1 \pmod{p^2}$.

Mithilfe dieses Kriteriums wurde der Rechenaufwand drastisch reduziert. In der Zwischenzeit hat MIGNOTTE verschiedene Artikel mit neuen Rechentricks und abgekürzten Verfahren sowie der Behandlung spezieller Paare von Exponenten veröffentlicht. Als Konsequenz daraus folgte, dass $p, q > 10^7$. J. GRANTHAM teilte mit, dass er die untere Schranke auf $p, q > 3 \times 10^8$ erhöht hat. MIGNOTTE fügte im Jahr 2000 eine weitere Bedingung hinzu, die die Exponenten erfüllen müssen.

5.19. Wenn $x^m - y^n = 1$ mit $m, n > 2$ und $x, y > 1$, dann sind m und n Primzahlen.

6 Der Beweis von Catalans Vermutung

Die Situation im Jahr 2000 war die, dass wenn $x^p - y^p = 1$ gilt, dann müssen $p^2|y, q^2|x$, $p^{q-1} \equiv 1 \pmod{q^2}$, $q^{p-1} \equiv 1 \pmod{p^2}$ (die Wieferich-Kongruenzen) sowie weitere Teilbarkeitsbedingungen und

Schranken erfüllt sein, die an früherer Stelle erwähnt wurden. Trotz aller gesammelter Information wurde MIHĂILESCU klar, dass ein gründliches Studium der Arithmetik der Kreisteilungskörper $\mathbb{Q}(\zeta_p)$ und $\mathbb{Q}(\zeta_q)$ unvermeidbar war. Dies war nicht überraschend, da sich die Bedingungen $\frac{x^p-1}{x-1} = pa^q$ und $\frac{y^q+1}{y+1} = qb^p$ zu $N(\frac{x-\zeta_p}{1-\zeta_p}) = a^q$ (Norm in der Erweiterung $\mathbb{Q}(\zeta_p)|\mathbb{Q}$) bzw. $N(\frac{y+\zeta_q}{1+\zeta_q}) = b^p$ (Norm in der Erweiterung $\mathbb{Q}(\zeta_q)|\mathbb{Q}$) übersetzen.

MIHĂILESCU gab im Jahr 2002 bekannt, dass er einen Beweis von Catalans Vermutung gefunden habe. Der Artikel erschien 2004. Eine in gewisser Hinsicht einfachere Version des Beweises wurde von Y. BILU gegen Ende 2002 vorgelegt. Eine Erklärung des eigentlichen Beweises erfordert Konzepte, die weit über das hinausgehen, was hier darzustellen möglich ist. Die theoretische Untersuchung von MIHĂILESCU lieferte ein weiteres Beispiel dafür, wie intelligentes Denken überschwängliche Berechnungen übertreffen kann.

7 Abschließende Kommentare und Anwendungen

Ein einfaches Korollar des Resultats **(5.3)** ist das folgende: Seien $m, n \geq 2$ verschiedene ganze Zahlen und $z_1 < z_2 < z_3 < \cdots$ die Folge derjenigen natürlichen Zahlen, die entweder eine $m$te oder eine $n$te Potenz einer natürlichen Zahl sind. Dann gilt $\lim_{i\to\infty}(z_{i+1} - z_i) = \infty$.

Für $n = 2$ geht obiges Ergebnis auf Landau und Ostrowski (1920) zurück, für beliebige m, n wurde es explizit von INKERI und HYYRÖ im Jahr 1964 formuliert.

Die Haupt-*Vermutung* in Bezug auf Potenzen, die man wohl PILLAI (1936) oder LANDAU zuschreiben könnte, ist die folgende:

Wenn $k \geq 2$, dann gibt es höchstens endlich viele Quadrupel natürlicher Zahlen x, y, m, n mit $m \geq 2$, $n \geq 2$ derart, dass $x^m - y^n = k$.

Diese Vermutung könnte man äquivalent folgendermaßen formulieren:

Wenn $z_1 < z_2 < z_3 < \cdots$ die Folge von Potenzen natürlicher Zahlen ist, dann gilt $\lim_{i\to\infty}(z_{i+1} - z_i) = \infty$.

Wir betrachten nun die Folge von Potenzen gegebener verschiedener Zahlen $a, b \geq 2$ oder allgemeiner, die Folge S von natürlichen Zahlen, deren Primfaktoren sämtlich aus der Menge von Primzahlen $E = \{p_1, \ldots, p_r\}$, $r \geq 2$ stammen.

Wir schreiben

$$S : z_1 < z_2 < z_3 < \cdots ,$$

S ist also Folge (d) der Einleitung.

Im Jahr 1897 zeigte STØRMER, dass

$$\liminf_{i\to\infty}(z_{i+1}-z_i)\geq 2,$$

mit anderen Worten, die Gleichung $X-Y=1$ besitzt nur endlich viele Lösungen für $x,y\in S$.

STØRMER gab eine konstruktive Methode an, um alle Lösungen zu finden; siehe auch den Artikel von LEHMER (1964). THUEs Ergebnis von 1918, das nach **(5.1)** erschien, allerdings nicht konstruktiv ist, ist das folgende:

$$\lim_{i\to\infty}(z_{i+1}-z_i)=\infty.$$

Im Jahr 1965 bewies ERDÖS, dass es für jedes $\epsilon>0$ ein i_0 derart gibt, dass wenn $i\geq i_0$, dann

$$\frac{z_{i+1}-z_i}{z_i}>\frac{1}{z_i^{\epsilon}}.$$

In den Jahren 1973 und 1974 zeigte TIJDEMAN, dass dieses Ergebnis in gewisser Hinsicht das bestmögliche ist. Tatsächlich gibt es effektiv berechenbare und nur von der Folge S abhängige Konstanten C, C' und ein i_0, dass für $i\geq i_0$

$$\frac{1}{(\log z_i)^{C'}}\geq\frac{z_{i+1}-z_i}{z_i}\geq\frac{1}{(\log z_i)^{C}}.$$

Weitere Resultate in derselben Richtung, die den gegenwärtigen Stand des Wissens darstellen, sind die folgenden:

Sei E die Menge der Primzahlen kleiner als N und S die Folge aller Zahlen, deren Primfaktoren sämtlich kleiner als N sind.

Sei $\tau>0$. Dann gibt es eine effektiv berechenbare Konstante C, die nur von N und τ abhängt, so dass wenn m,n,x,y alle größer sind als 1 und wenn $\mathrm{ggT}(ax^m,k)\leq\tau$ sowie $|a|$, $|b|$, $|k|\in S$ und

$$ax^m-by^n=k,$$

dann $\max\{|a|,|b|,|k|,m,n,x,y\}<C$.

In ähnlicher Weise:

Sei $\tau>0$, $m\geq 2$. Dann gibt es eine effektiv berechenbare Konstante C, die nur von N, τ und m abhängt, so dass wenn $n\geq 2$, $x\geq 2$, $y\geq 2$, $mn\geq 5$, wenn $\mathrm{ggT}(ax^m,k)\leq\tau$, $|a|$, $|b|$, $|k|\in S$ und $ax^m-by^n=k$, dann $\max\{|a|,|b|,|k|,n,x,y\}<C$.

Weitere Resultate mit ähnlicher Aussage finden sich in der wichtigen Monographie von Shorey und Tijdeman (1986).

Literaturverzeichnis

1288 Levi ben Gerson. Siehe Dickson, L. E., *History of the Theory of Numbers*, Vol II, p. 731. Carnegie Institution, Washington, 1920. Nachdruck von Chelsea Publ. Co., New York, 1971.

1640 P. Fermat. Lettre à Mersenne (Mai, 1640). In *Oeuvres, Vol. II*, 194–195. Gauthier-Villars, Paris, 1894.

1657 P. Fermat. Lettre à Frénicle (Février, 1657). In *Oeuvres, Vol. II*, 333–335. Gauthier-Villars, Paris, 1894.

1657 Frénicle de Bessy. Solutio duorum problematum circa numeros cubos et quadratos. Bibliothèque Nationale de Paris.

1732 L. Euler. Observationes de theoremate quodam Fermatiano aliisque ad numeros primos spectantibus. *Comm. Acad. Sci. Petrop.*, 6, 1732/3 (1738):103–107. Nachdruck in *Opera Omnia*, Ser. I, Vol. II. Comm. Arithm., I, 1–5. B. G. Teubner, Leipzig, 1915.

1737 L. Euler. De variis modis circuli quadraturam numeros primos exprimendi. *Comm. Acad. Sci. Petrop.*, 9, 1737 (1744):222–236. Nachdruck in *Opera Omnia*, Ser. I. Vol. XIV. Comm. Arithm., I, 245–259. B. G. Teubner, Leipzig. 1924.

1738 L. Euler. Theorematum quorundam arithmeticorum demonstrationes. *Comm. Acad. Sci. Petrop.*, 10, 1738 (1747):125–146. Nachdruck in *Opera Omnia*, Ser. I, Vol. II, Comm. Arithm., I, 38–58. B. G. Teubner, Leipzig. 1915.

1755 L. Euler. *Institutiones Calculi Differentialis.* Partis Posterioris (Caput V). Imp. Acad. Sci., St. Petersburg. Nachdruck in *Opera Omnia*, Ser. I, Vol. X, 321–328. B. G. Teubner, Leipzig, 1913.

1777 J. L. Lagrange. Sur quelques problèmes de l'analyse de Diophante. *Nouveaux Mém. Acad. Sci. Belles Lettres, Berlin.* Nachdruck in *Oeuvres*, Vol. IV, publiées par les soins de M. J.-A. Serret, 377–398, Gauthier-Villars, Paris. 1869.

1783 L. Euler. Variae observationnes circa angulos in progressione geometrica progredientes. *Opuscula Analytica, I*, 1783:345–352. Nachdruck in *Opera Omnia*, Ser. I, Vol. XV. 498–508. B. G. Teubner, Leipzig, 1927.

1798 J. L. Lagrange. Addition aux "Eléments d'Algèbre" d'Euler—Analyse Indéterminée. Nachdruck in *Oeuvres*, Vol. VII, publiées par les soins de M. J.-A. Serret, 3–180. Gauthier-Villars, Paris, 1877.

1801 C. F. Gauss. *Disquisitiones Arithmeticae.* G. Fleischer, Leipzig.

1830 A. M. Legendre. *Théorie des Nombres, Vol. II, (3 édition).* Firmin Didot, Paris. Nachdruck von A. Blanchard, Paris, 1955.

1844 E. Catalan. Note extraite d'une lettre addressée á l'éditeur. *J. reine u. angew. Math.*, 27:192.

1844 Z. Dase. Der Kreis-Umfang für den Durchmesser 1 auf 200 Decimalstellen berechnet. *J. reine u. angew. Math.*, 27:198.

1844 F. G. Eisenstein. Aufgaben und Lehrsätze. *J. reine u. angew. Math.*, 27:86–88. Nachdruck in *Mathematische Werke*, Vol. I, 111-113, Chelsea, New York. 1975.

1850 V. A. Lebesgue. Sur l'impossibilité en nombres entiers de l'équation $x^m = y^2 + 1$. *Nouv. Ann. de Math.*, 9:178–181.

1870 G. C. Gérono. Note sur la résolution en nombres entiers et positifs de l'équation $x^m = y^n + 1$. *Nouv. Ann. de Math. (2)*, 9: 469–471 und 10:204–206 (1871).

1885 E. Catalan. Quelques théorémes empiriques (Mélanges Mathématiques, XV). *Mém. Soc. Royale Sci. de Liége, Sér. 2*, 12: 42–43.

1885 T. L. Heath. *Diophantus of Alexandria. A Study in the History of Greek Algebra.* Cambridge Univ. Press, Cambridge. Nachdruck von Dover. New York. 1964.

1886 A. S. Bang. Taltheoretiske Untersogelser. *Tidskrift Math., Ser. 5*, 4:70–80 und 130–137.

1892 K. Zsigmondy. Zur Theorie der Potenzreste. *Monatsh. f. Math.*, 3:265–284.

1897 C. Størmer. Quelques théorèmes sur l'équation de Pell $x^2 - Dy^2 = \pm 1$ et leurs applications. *Christiania Videnskabens Selskabs Skrifter, Math. Nat. Kl.*, 1897, Nr. 2, 48 Seiten.

1899 C. Størmer. Solution complète en nombres entiers de l'équation $m \arctang \frac{1}{x} + n \arctang \frac{1}{y} = k\frac{\pi}{4}$. *Bull. Soc. Math. France*, 27:160–170.

1904 G. D. Birkhoff und H. S. Vandiver. On the integral divisors of $a^n - b^n$. *Ann. Math. (2)*, 5:173–180.

1908 A. Thue. Om en general i store hele tal ulösbar ligning. *Christiania Videnskabens Selskabs Skrifter, Math. Nat. Kl.*, 1908, Nr. 7, 15 Seiten. Nachdruck in *Selected Matheinealcal Papers*, 219-231. Universitetsforlaget, Oslo, 1982.

1908 C. Størmer. Solution d'un problème curicux qu'on rencontre dans la théorie élémentaire des logarithmes. *Nyt Tidskrift f. Mat. (Copenhagen) B*, 19:1–7.

1909 R. D. Carmichael. Problem 155 (aufgestellt und gelöst von R. D. Carmichael). *Amer. Math. Monthly*, 16:38–39.

1918 G. Pólya. Zur arithmetischen Untersuchung der Polynome. *Math. Z.*, 1:143–148.

1919 P. Bachmann. *Das Fermatproblem in seiner bisherigen Entwicklung.* W. De Gruyter, Berlin. Nachdruck von Springer-Verlag, Berlin, 1976.

1920 L. E. Dickson. *History of the Theory of Numbers, Vol. II.* Carnegie Institution, Washington. Nachdruck von Chelsea Publ. Co. New York, 1971.

1920 E. Landau und A. Ostrowski. On the diophantine equation $ay^2 + by + c = dx^n$. *Proc. London Math. Soc., (2)*, 19:276–280.

1921 T. Nagell. Des équations indéterminées $x^2 + x + 1 = y^n$ et $x^2 + x + 1 = 3y^n$. *Norsk Mat. Forenings Skrifter, Ser. I*, 1921, Nr. 2, 14 Seiten.

1921 T. Nagell. Sur l'équation indéterminée $\frac{x^n-1}{x-1} = y^2$. *Norsk Mat. Forenings Skrifter, Ser. I*, 1921, Nr. 3, 17 Seiten.

1923 P. Franklin. Problem 2927. *Amer. Math. Monthly*, 30:81.

1924 T. Nagell. Über die rationale Punkte auf einigen kubischen Kurven. *Tôhoku Math. J.*, 24:48–53.

1929 C. L. Siegel. Über einige Anwendungen diophantischer Approximation. *Abhandl. Preuss. Akad. d. Wiss., Nr. I.* Nachdruck in *Gesammelte Abhandlungen, Vol. 1*, 209–266. Springer-Verlag, Berlin, 1966.

1931 S. S. Pillai. On the inequality "$0 < a^x - b^y \leq n$". *J. Indian Math. Soc.*, 19:1–11.

1932 S. Selberg. Sur l'impossibilité de l'équation indéterminée $z^p + 1 = y^2$. *Norsk Mat. Tidsskrift*, 14:79–80.

1934 T. Nagell. Sur une équation diophantienne à deux indéterminées. *Det Kongel. Norske Vidensk. Selskab Forhandliger, Trondhejm*, 1934, Nr. 38, 136–139.

1936 A. Herschfeld. The equation $2^x - 3^y = d$. *Bull. Amer. Math. Soc.*, 42:231–234.

1936 S. S. Pillai. On $a^x - b^y = c$. *J. Indian Math. Soc., (New Series)*, 2:119–122.

1936 C. L. Siegel. Über die Classenzahl quadratischer Zahlkörper. *Acta Arith.*, 1:83–86. Nachdruck in *Gesammelte Abhandlungen, Vol. I*, 406–409. Springer-Verlag, Berlin, 1966.

1940 R. Obláth. Az $x^2 - 1$ Számokól. (On the numbers $x^2 - 1$). *Mat. és Fiz. Lapok*, 47:58–77.

1941 R. Obláth. Sobre ecuaciones diofánticas imposibles de la forma $x^m + 1 = y^n$. (On impossible Diophantine equations of the form $x^m + 1 = y^n$). *Rev. Mat. Hisp.-Amer. IV*, 1:122–140.

1942 W. Ljunggren. Einige Bemerkungen über die Darstellung ganzer Zahlen durch binäre kubische Formen mit positiver Diskriminante. *Acta Math.*, 75:1–21.

1943 J. E. Hofmann. Neues über Fermats zahlentheoretische Herausforderungen von 1657. *Abhandl. d. Preussischen Akad. d. Wiss.*, 1943, Nr. 9, 52 Seiten.

1943 W. Ljunggren. New propositions about the indeterminate equation $\frac{x^n-1}{x-1} = y^q$. *Norsk Mat. Tidsskr.*, 25:17–20.

1952 W. J. LeVeque. On the equation $a^x - b^y = 1$. *Amer. J. of Math.*, 74:325–331.

1953 J. W. S. Cassels. On the equation $a^x - b^y = 1$. *Amer. J. of Math.*, 75:159–162.

1953 K. Mahler. On the greatest prime factor of $ax^m + by^n$. *Nieuw Arch. Wisk. (3)*, 1:113–122.

1954 R. Obláth. Über die Gleichung $x^m + 1 = y^n$. *Ann. Polon. Math.*, 1:73–76.

1955 H. Davenport und K. F. Roth. Rational approximations to algebraic numbers. *Mathematika*, 2:160–167.

1956 R. Hampel. On the solution in natural numbers of the equation $x^m - y^n = 1$. *Ann. Polon. Math.*, 3:1–4.

1956 W. J. LeVeque. *Topics in Number Theory. Vol. II.* Addison-Wesley, Reading, Mass.

1956 A. Rotkiewicz. Sur l'équation $x^z - y^t = a^t$ où $|x - y| = a$. *Ann. Polon. Math.*, 3:7–8.

1958 A. Schinzel und W. Sierpiński. Sur certaines hypothèses concernant les nombres premiers. Remarques. *Acta Arith.*, 4:185–208 und 5:259 (1959).

1960 J. W. S. Cassels. On the equation $a^x - b^y = 1$. II. *Proc. Cambridge Phil. Soc.*, 56:97–103.

1960 R. Hampel. O zagadnieniu Catalana (On the problem of Catalan). *Roczniki Polskiego Towarzystwa Matematycznego, Ser. I, Prace Matematyczne*, 4:11–19.

1960 Chao Ko. On the Diophantine equation $x^2 = y^n + 1$. *Acta Sci. Natur. Univ. Szechuan*, 2:57–64.

1960 A. Rotkiewicz. Sur le problème de Catalan. *Elem. d. Math.*, 15:121–124.

1960 J. W. Wrench. The evolution of extended decimal approximations to π. *Math. Teacher*, 53:644–650.

1961 K. Inkeri und S. Hyyrö. On the congruence $3^{p-1} \equiv 1 \pmod{p^2}$ and the diophantine equation $x^2 - 1 = y^p$. *Ann. Univ. Turku. Ser. AI*, 1961, Nr. 50, 2 Seiten.

1962 A. Mąkowski. Three consecutive integers cannot be powers. *Colloq. Math.*, 9:297.

1963 J. Ferentinou-Nicolacopoulou. Une propriété des diviseurs du nombre $r^{r^m} + 1$. Applications au dernier théorème de Fermat. *Bull. Soc. Math. Grèce, Sér. 4*, (1):121–126.

1963 M. Gut. Abschätzungen für die Klassenzahlen der quadratischen Körper. *Acta Arith.*, 8:113–122.

1963 S. Hyyrö. On the Catalan problem (in Finnish). *Arkhimedes*, 1963, Nr. 1, 53–54. Siehe Math. Reviews, 28, 1964, #62.

1964 S. Hyyrö. Über die Gleichung $ax^n - by^n = c$ und das Catalansche Problem. *Annales Acad. Sci. Fennicae, Ser. AI*, 1964(355):50 Seiten.

1964 K. Inkeri. On Catalan's problem. *Acta Arith.*, 9:285–290.

1964 K. Inkeri und S. Hyyrö. Über die Anzahl der Lösungen einiger diophantischer Gleichungen. *Ann. Univ. Turku. Ser. AI*, 1964, Nr. 78, 7 Seiten.

1964 Chao Ko. On the Diophantine equation $x^2 = y^n + 1$. *Scientia Sinica (Notes)*, 14:457–460.

1964 W. J. LeVeque. On the equation $y^m = f(x)$. *Acta Arith.*, 9: 209–219.

1964 D. H. Lehmer. On a problem of Størmer. *Illinois J. Math.*, 8:57–79.

1964 H. Riesel. Note on the congruence $a^{p-1} \equiv 1 \pmod{p^2}$. *Math. of Comp.*, 18:149–150.

1965 P. Erdös. Some recent advances and current problems in number theory. In *Lectures on Modern Mathematics, Vol. III*, herausgegeben von T. L. Saaty, 169–244. Wiley, New York.

1965 A. Rotkiewicz. Sur les nombres de Mersenne dépourvus de diviseurs carrés et sur les nombres naturels n tels que $n^2 \mid 2^n - 2$. *Matematicky Vesnik, Beograd, (2)*, 17:78–80.

1967 L. J. Warren und H. Bray. On the square-freeness of Fermat and Mersenne numbers. *Pacific J. Math.*, 22:563–564.

1973 R. Tijdeman. On integers with many small prime factors. *Compositio Math.*, 26:319–330.

1974 R. Tijdeman. On the maximal distance between integers composed of small primes. *Compositio Math.*, 28:159–162.

1975 A. Baker. *Transcendental Number Theory.* Cambridge Univ. Press, London.

1976 E. Z. Chein. A note on the equation $x^2 = y^n + 1$. *Proc. Amer. Math. Soc.*, 56:83–84.

1976 M. Langevin. Quelques applications des nouveaux résultats de van der Poorten. *Sém. Delange-Pisot-Poitou,* 17^e *année*, 1976, Nr. G12, 1–11.

1976 R. Tijdeman. On the equation of Catalan. *Acta Arith.*, 29: 197–209.

1979 P. Ribenboim. *13 Lectures on Fermat's Last Theorem.* Springer-Verlag, New York. Zweite Ausgabe mit einem neuen Nachwort, 1995.

1979 P. Ribenboim. On the square factors of the numbers of Fermat and Ferentinou-Nicolacopoulou. *Bull. Soc. Math. Grèce (N.S.)*, 20: 81–92.

1980 _____. *Numéro Spécial π, Supplément au "Petit Archimède", Nos. 64-65.* 289 Seiten. 61 Rue St. Fuscien. 80000, Amiens (France).

1986 T. N. Shorey und R. Tijdeman. *Exponential Diophantine Equations.* Cambridge University Press, Cambridge.

1990 K. Inkeri. On Catalan's conjecture. *J. Nb. Th.*, 34:142–152.

1991 M. Aaltonen und K. Inkeri. Catalan's equation $x^p - y^q = 1$ and related congruences. *Math. of Comp.*, 56:359–370.

1993 M. Mignotte. Un critère élémentaire pour l'équation de Catalan. *C. R. Math. Rep. Acad. Sci. Canada*, 15:199–200.

1994 P. Ribenboim. *Catalan's Conjecture.* Academic Press, Boston.

1995 M. Laurent, M. Mignotte und Y. Nesterenko. Formes linéaires en deux logarithmes et déterminants d'interpolation. *J. Nb. Th.*, 55:285–321.

1995 M. Mignotte. A criterion on Catalan's equation. *J. Nb. Th.*, 52:280–283.

1995 M. Mignotte und Y. Roy. Catalan's equation has no new solution with either exponent less than 10651. *Experiment. Math.*, 4:259–268.

1995 W. O'Neil. Improved upper bounds on the exponents in Catalan's equation. Manuscript.

1995 W. Schwarz. A note on Catalan's equation. *Acta Arith.*, 72: 277–279.

1996 F. Jongmans. *Eugène Catalan.* Soc. Belge Prof. Math. Expr. Française, Mons.

1996 M. Mignotte. Sur l'équation $x^p - y^q = 1$ lorsque $p \equiv 5 \bmod 8$. *C. R. Math. Rep. Acad. Sci. Canada*, 18:228–232.

1997 D. H. Bailey, J. M. Borwein, P. B. Borwein und S. Plouffe. The quest for pi. *Math. Intelligencer*, 19(1):50–57.

1997 C. D. Bennett, J. Blass, A. M. W. Glass, D. B. Meronk und R. P. Steiner. Linear forms in the logarithms of three positive rational numbers. *J. Théor. Nombres Bordeaux*, 9:97–136.

1997 M. Mignotte und Y. Roy. Minorations pour l'équation de Catalan. *C. R. Acad. Sci. Paris, Sér. I*, 324:377–380.

1999 M. Mignotte. Une remarque sur l'équation de Catalan. In *Number Theory in Progress, Vol. 1 (Zakopane-Kościelisko, 1997)*, 337–340. de Gruyter, Berlin.

1999 P. Mihăilescu. A class number free criterion for Catalan's conjecture. Manuscript, Zurich, (veröffentlicht 2003).

2001 M. Mignotte. Catalan's equation just before 2000. Proceedings of the Symposium in memory of Kustaa Inkeri, Turku 1999, 247–254. de Gruyter, Berlin 2001.

2003 Y. Bila. Catalan's conjecture (after P. Mihăilescu) Seminar Bourbaki 909 55^e année, Paris, 2002-2003.

2004 P. Mihăilescu. Primary cyclotomic units and a proof of Catalan's conjecture. *J. reine u. angew. Math.*, 572:167–195.

8

1093

1093! Falls Sie sich wundern sollten, worum es in diesem Kapitel geht, so möchte ich sofort erwähnen, dass es nicht von der Qualität der Weine des Jahrgangs 1093 handelt. Tatsächlich gibt es keinerlei Aufzeichnungen für solch ferne Zeiten. Erst 1855 begann ein auserlesenes Grüppchen von Weinexperten in Bordeaux damit, die feinsten Weingüter in der Region zu klassifizieren, ausgezeichnet wurden die herausragenden Châteaux Lafitte, Margaux, Latour und Haut-Brion als Premiers Crus in Médoc sowie Chateau Yquem in Sauternes als Premier Grand Cru. Ganz zu schweigen von den fabelhaften Weinen aus dem Burgund ... (siehe Fadiman (1981)). Allerdings geht es hier ja gar nicht um Weine.

Genau genommen kam mir die Idee zu diesem Kapitel nach einer Diskussion mit F. Le Lionnais in Paris. Er war ein Wissenschaftsautor mit einer scharfsinnigen Neugierde. Kurz nach dem Krieg gab er im Jahr 1946 ein Buch namens *Les Grands Courants de la Pensée Mathématique* heraus, das Beiträge solch bedeutender Mathematiker wie André Weil und einigen weiteren Mitgliedern der Bourbaki-Gruppe enthält. Der Artikel „L'Avenir des Mathématiques" von Weil ist sehr lesenswert und gibt eine Übersicht über das, was in mehr als fünfzig Jahren geschah. Das Buch wurde ins Englische übersetzt und ist immer noch verfügbar. Ich bekam kurz nach dem Erscheinen Kenntnis davon und war immer darauf aus, Le Lionnais zu treffen.

So war es mir eine große Freude, als ich ihm im Jahre 1976 auf einem Seminar über Mathematikgeschichte vorgestellt wurde. Während der Unterhaltung bekam ich mit, dass er an einem Buch über besondere Zahlen wie 2, 7, π, e, usw. ... arbeitete. Er fragte mich, ob ich irgendwelche Zahlen mit interessanten Eigenschaften kennen würde, die im

Buch einen Platz finden könnten.[1] Ich suchte und entschied mich für „1093“, worüber er bis dahin noch nichts gehört hatte.

Meine Absicht ist es, Ihnen zu erzählen, warum ich 1093 für eine interessante Zahl halte. (Später war ich froh, dass Le Lionnais 1093 in sein Buch über außergewöhnliche Zahlen aufgenommen hatte.) Natürlich könnte man sagen, dass *jede* natürliche Zahl außergewöhnlich ist. Falls nicht, so gäbe es eine kleinste Zahl N die nicht außergewöhnlich ist—und aufgrund dieser Eigenschaft wäre N natürlich außergewöhnlich ....

Nun, ... 1093 ist die kleinste Primzahl p, die die Kongruenz

$$2^{p-1} \equiv 1 \pmod{p^2} \tag{8.1}$$

erfüllt.

Es gilt also

$$2^{1092} \equiv 1 \pmod{1093^2}.$$

Dies wurde von Meissner (1913) entdeckt, der die Rechnung explizit durchführte. Nach Fermats kleinem Satz gilt

$$2^{p-1} \equiv 1 \pmod{p}, \tag{8.2}$$

aber es gibt im Allgemeinen keinen Grund zu erwarten, dass die stärkere Kongruenz (8.1) erfüllt ist.

In Band III von Landau (1927), findet sich der folgende Beweis von (8.1) für $p = 1093$:

$$3^7 = 2187 = 2p + 1,$$

also ergibt sich durch Quadrieren

$$3^{14} \equiv 4p + 1 \pmod{p^2}. \tag{8.3}$$

Andererseits,

$$\begin{aligned} 2^{14} &= 16384 = 15p - 11, \quad \text{also} \\ 2^{28} &= -330p + 121 \pmod{p^2}, \end{aligned}$$

damit

$$3^2 \times 2^{28} \equiv -1876p - 4 \pmod{p^2},$$

[1] Das Buch ist später erschienen: F. Le Lionnais *Les Nombres Remarquables*, Hermann Editeurs, Paris, 1983.

teilen durch 4,

$$3^2 \times 2^{26} \equiv -469p - 1 \pmod{p^2}.$$

In die 7te Potenz erheben:

$$3^{14} \times 2^{182} \equiv -4p - 1 \pmod{p^2}$$

unter Berücksichtigung von (8.3),

$$2^{182} \equiv -1 \pmod{p^2}.$$

Schließlich ergibt Potenzieren in die 6te Potenz,

$$2^{1092} \equiv 1 \pmod{p^2}.$$

Da die Kongruenz (8.1) im Allgemeinen nicht gilt, muss jeder Beweis dafür, dass sie im Fall $p = 1093$ gilt, quasi aus dem Stehgreif erfolgen.

Beeger (1922) fand, dass auch 3511 die Kongruenz (8.1) erfüllt. Man bedenke, dass er seine Rechnungen im Jahr 1921 durchführte, also bevor es Computer gab. Welch eine Hartnäckigkeit! Vor allem wenn man bedenkt, dass unbekannt war, ob es ein weiteres $p > 1093$ gibt.

Die Suche wurde inzwischen von P. Carlisle, R. Crandall und M. Rodenkirch bis $2{,}5\times10^{15}$ fortgesetzt (siehe auch Crandall, Dilcher und Pomerance (1997) sowie Knauer und Richstein (2005)), ohne dass eine weitere Primzahl gefunden werden konnte, die (8.1) erfüllt.

Das ist alles schön und gut, aber warum interessiert sich irgendjemand für die Kongruenz (8.1)?

Es war Abel, der im dritten Band von Crelles Journal (1828) fragte, ob es möglich sei, dass

$$a^{p-1} \equiv 1 \pmod{p^m} \tag{8.4}$$

erfüllt ist, wobei $m \geq 2$ und p eine Primzahl ist, die a nicht teilt.

Jacobi, der äußerst kompetent in numerischer Berechnung war, gab verschiedene Beispiele von (8.4) an:

$$\begin{aligned} 3^{10} &\equiv 1 \pmod{11^2}, \\ 7^4 &\equiv 1 \pmod{5^2}, \\ 31^6 &\equiv 1 \pmod{7^2}, \end{aligned}$$

und mit $m = 3$,

$$19^6 \equiv 1 \pmod{7^3}.$$

Aber das Problem ist nicht Beispiele zu finden, sondern die Frage zu beantworten:

Gibt es unendlich viele Primzahlen p derart, dass gilt $2^{p-1} \equiv 1 \pmod{p^2}$?

Um dieser Frage nachzugehen, formuliere ich sie mittels des Fermat-Quotienten neu. Wenn $a \geq 2$ und p eine Primzahl ist, die a nicht teilt, dann ist

$$q_p(a) = \frac{a^{p-1} - 1}{p} \tag{8.5}$$

eine ganze Zahl (nach Fermats kleinem Satz) und heißt der *Fermat-Quotient* mit Basis a und Exponent p. Somit ist $q_p(a) \equiv 0 \pmod{p}$ genau dann, wenn $a^{p-1} \equiv 1 \pmod{p^2}$.

Dies führt zum Rest modulo p von $q_p(a)$ und man trifft unmittelbar auf viele interessante Ergebnisse, die den Fermat-Quotienten mit interessanten arithmetischen Größen verbinden. Ich möchte dies anhand einiger Beispiele illustrieren.

Der Rest modulo p von $q_p(a)$ verhält sich wie ein Logarithmus. Diese Tatsache bemerkte Eisenstein im Jahr 1850:

$$q_p(ab) \equiv q_p(a) + q_p(b) \pmod{p}. \tag{8.6}$$

A Bestimmung des Restes von $q_p(a)$

Das erste schriftlich nachgewiesene Ergebnis stammt von Sylvester (1861a), der die schöne Kongruenz bewies:

$$\begin{aligned} q_p(2) &\equiv \frac{1}{2}\left(1 + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{\frac{p-1}{2}}\right) \\ &\equiv 1 + \frac{1}{3} + \cdots + \frac{1}{p-1} \pmod{p}. \end{aligned} \tag{8.7}$$

Und allgemeiner für beliebige Basen a:

$$q_p(a) = \sum_{j=1}^{p-1} \frac{a_j}{j} \pmod{p} \tag{8.8}$$

wobei $0 \leq a_j \leq p-1$ und $pa_j + j \equiv 0 \pmod{a}$.

Im Jahr 1910 zeigte Mirimanoff: Wenn $p = 2^r \pm 1$ eine Primzahl ist, so gilt $q_p(2) \equiv \mp 1/r \not\equiv 0 \pmod{p}$.

Später fand JOHNSON (1977) ein nützliches Hilfsmittel zur Bestimmung des Fermat-Quotienten. Wenn r die kleinste ganze Zahl mit $a^r \equiv \pm 1 \pmod{p}$ ist, dann folgt mit $a^r \equiv \pm 1 + tp$, dass

$$q_p(a) \equiv \mp \frac{t}{r} \pmod{p}. \tag{8.9}$$

B Identitäten und Kongruenzen für den Fermat-Quotienten

Der erste substantielle Artikel über Fermat-Quotienten stammt von LERCH (1905) und ist heute fast vergessen. Es ist mir eine Freude, Sie auf seine schönen Resultate aufmerksam zu machen.

Er zeigte zunächst, dass

$$\sum_{j=1}^{p-1} q_p(j) \equiv W(p) \pmod{p} \tag{8.10}$$

wobei $W(p)$ den Wilson-Quotient bezeichnet. Dieser ist in ähnlicher Weise definiert wie der Fermat-Quotient. Und zwar besagt Wilsons Satz, dass

$$(p-1)! \equiv -1 \pmod{p}, \tag{8.11}$$

somit ist der Quotient

$$W(p) = \frac{(p-1)! + 1}{p} \tag{8.12}$$

eine ganze Zahl, den man den *Wilson-Quotient* von p nennt. Bevor ich zu Fermat-Quotienten zurückkehre, lassen Sie mich nur erwähnen, dass die Bestimmung des Restes von $W(p)$ modulo p genauso interessant ist wie das entsprechende Problem für den Fermat-Quotienten. Insbesondere nennt man im Falle $W(p) \equiv 0 \pmod{p}$ die Primzahl p eine *Wilson-Primzahl*. Zum Beispiel sieht man leicht, dass es sich bei $p = 5, 13$ um Wilson-Primzahlen handelt. Die Suche nach neuen Wilson-Primzahlen enthüllte nur eine weitere (GOLDBERG): $p = 563$, bis 10^9 (P. CARLISLE, R. CRANDALL und M. RODENKIRCH, siehe auch Crandall, Dilcher und Pomerance (1997)). Die Frage, ob es unendlich viele Wilson-Primzahlen gibt, scheint sehr schwierig zu sein.

VANDIVER sagte dazu im Jahr 1955:

> Diese Frage scheint mir von solch besonderer Beschaffenheit zu sein, dass wenn ich irgendwann nach meinem Tod wiederauferstehen sollte und mir irgendein Mathematiker erzählte, dass sie endgültig gelöst ist, ich sofort wieder tot umfallen würde.

Lassen Sie mich nun zur Bestimmung des Restes des Wilson-Quotienten zurückkehren.

LERCH zeigte, dass

$$W(p) = B_{2(p-1)} - B_{p-1} \pmod{p}. \tag{8.13}$$

Dabei bezeichnet B_n die $n$te Bernoulli-Zahl, definiert durch

$$\frac{x}{e^x - 1} = \sum_{n=0}^{\infty} B_n \frac{x^n}{n!}. \tag{8.14}$$

So ist $B_0 = 1$, $B_1 = -1/2$ und $B_n = 0$ für jedes ungerade $n > 1$. Die Bernoulli-Zahlen erfüllen die Rekursionsgleichung:

$$\binom{n+1}{1} B_n + \binom{n+1}{2} B_{n-1} + \binom{n+1}{3} B_{n-2} + \cdots + \binom{n+1}{n} B_1 + 1 = 0. \tag{8.15}$$

Dies lässt sich symbolisch schreiben als

$$(B+1)^{n+1} - B^{n+1} = 0. \tag{8.16}$$

(Fasse B als Unbestimmte auf und ersetze nach Berechnung des Polynoms auf der linken Seite B^k durch B_k.)

Eine wichtige Eigenschaft der Bernoulli-Zahlen, die von EULER entdeckt wurde, verknüpft diese Zahlen mit der Riemannschen Zetafunktion ζ:

$$B_{2n} = (-1)^{n-1} \frac{2(2n)!}{(2\pi)^{2n}} \zeta(2n) \quad (\text{für } n \geq 1) \tag{8.17}$$

wobei

$$\zeta(s) = \sum_{j=1}^{\infty} \frac{1}{j^s}, \quad s \text{ komplex, } \mathrm{Re}(s) > 1. \tag{8.18}$$

Unter Verwendung der Funktionalgleichung für die Riemannsche Zetafunktion folgt

$$\zeta(1-n) = -\frac{B_n}{n} \quad (\text{für } n \geq 2) \tag{8.19}$$

und auch $\zeta(0) = -\frac{1}{2}$.

Zurück zu Lerchs Formel (8.10). Der Punkt ist der folgende: Da Fermat-Quotienten in gewisser Hinsicht schwer berechenbar sind, liegt es nahe, ihre Summe über alle Restklassen in Beziehung zu Ausdrücken von p zu bringen.

Dies geschah auch für gewichtete Summen. In einem Brief an Hensel bewiesen Friedmann und Tamarkine im Jahre 1909: Wenn $1 \leq n \leq p-1$, dann

$$\sum_{j=1}^{p-1} j^n q_p(j) \equiv (-1)^{[n/2]} \frac{B_n}{n} \pmod{p}. \tag{8.20}$$

Aus (8.19) folgt, dass wenn $2 \leq n \leq p-1$, dann

$$\sum_{j=1}^{p-1} j^n q_p(j) \equiv (-1)^{[(n-2)/2]} \zeta(1-n) \pmod{p} \tag{8.21}$$

sowie

$$\sum_{j=1}^{p-1} j q_p(j) \equiv -\frac{1}{2} = \zeta(0) \pmod{p}.$$

Lerch brachte den Fermat-Quotienten auch in Verbindung mit dem *Legendre-Quotient*

$$\lambda_p(j) = \frac{j^{\frac{p-1}{2}} - \left(\frac{j}{p}\right)}{p}. \tag{8.22}$$

Man erinnere sich, dass wenn $p \nmid j$ und $\left(\frac{j}{p}\right)$ das Legendre-Symbol bezeichnet, so gilt

$$\left(\frac{j}{p}\right) \equiv j^{\frac{p-1}{2}} \pmod{p}, \tag{8.23}$$

also ist $\lambda_p(j)$ eine ganze Zahl.

Lerch bewies

$$q_p(j) \equiv 2 \left(\frac{j}{p}\right) \lambda_p(j) \pmod{p}. \tag{8.24}$$

Ein weiterer schöner Zusammenhang betrifft die Verteilung quadratischer Reste und die Klassenzahl quadratischer Zahlkörper.

Es bezeichne $H(a)$ die Klassenzahl des quadratischen Zahlkörpers $\mathbb{Q}(\sqrt{a})$ (wobei a eine quadratfreie Zahl ist).

DIRICHLET bewies die berühmte Formel für $p \equiv 3 \pmod 4$, $p \neq 3$:

$$H(-p) = -\frac{1}{p}\sum_{j=1}^{p-1}\left(\frac{j}{p}\right) j = \frac{\rho - \rho'}{2 - \left(\frac{2}{p}\right)} \tag{8.25}$$

wobei

$\rho =$ Anzahl der quadratischen Reste zwischen 0 und $p/2$,

$\rho' =$ Anzahl der nicht-quadratischen Reste zwischen 0 und $p/2$.

Man weiß, dass $\rho > \rho'$ wenn $p \equiv 3 \pmod 4$. Dies ist ein schwieriger Satz. Die einzigen bis heute bekannten Beweise erfordern trotz der rein arithmetischen Natur die Analysis.

FRIEDMANN und TAMARKINE stellten fest, dass

$$\rho - \rho' \equiv \left[2 - \left(\frac{2}{p}\right)\right] 2B_{\frac{p+1}{2}} \pmod p \tag{8.26}$$

was zu

$$H(-p) \equiv 2B_{\frac{p+1}{2}} \pmod p. \tag{8.27}$$

führt.

LERCH zeigte

$$\sum \left(\frac{j}{p}\right) j q_p(j) \equiv \begin{cases} 0 & \text{wenn } p \equiv 1 \pmod 4, \\ H(-p) & \text{wenn } p \equiv 3 \pmod 4. \end{cases} \tag{8.28}$$

Lassen Sie mich nun zu einem Satz kommen, der das Interesse an Fermat-Quotienten entfachte und neue Forschungsgebiete eröffnet hat.

Die folgenden Resultate sind von historischer Bedeutung. Das Interesse an ihnen ging durch den Beweis von Fermats letztem Satz durch WILES nicht verloren, da die Methoden sich auch auf ähnliche diophantische Gleichungen wie zum Beispiel Catalans Gleichung

$$X^m - Y^n = 1 \tag{8.29}$$

anwenden lassen.

Im Jahre 1909 bewies WIEFERICH: Angenommen es gäbe ganze Zahlen x, y, z, die keine Vielfachen der ungeraden Primzahl p sind und die $x^p + y^p + z^p = 0$ erfüllen (d.h., der *erste* Fall von Fermats letztem Satz ist für p falsch). Dann gilt

$$2^{p-1} \equiv 1 \pmod{p^2}.$$

Damit ist nach dem, was ich zu Beginn dieses Kapitels gesagt hatte, der erste Fall von Fermats letztem Satz für jeden primen Exponenten $p < 2{,}5 \times 10^{15}$ wahr, außer möglicherweise für $p = 1093$ und 3511.

Der Beweis von WIEFERICH war sehr schwierig und technischer Natur. Er basierte auf dem folgenden, tiefschürfenden Resultat von KUMMER: Falls der erste Fall von Fermats letztem Satz (=*FLS*) für den Exponent p nicht wahr sein sollte und gilt $x^p + y^p + z^p = 0$ mit p, das xyz nicht teilt, dann

$$\left[\frac{d^{2s}\log(x + e^v y)}{dv^{2s}}\right] \times B_{2s} \equiv 0 \pmod{p} \tag{8.30}$$

für $2s = 2, 4, \ldots, p-3$ (und ähnlichen Kongruenzen für die Paare (y, x), (y, z), (z, y), (x, z), (z, x)).

Darüberhinaus verwendete WIEFERICH komplizierte Kongruenzen, die von den Bernoulli-Zahlen erfüllt sind. FURTWÄNGLER fand im Jahr 1912 einen anderen Beweis des Satzes von Wieferich, der Klassenkörpertheorie verwendete—eine weitere Bestätigung für die Stärke der Klassenkörpertheorie. Der Satz von Wieferich war der erste einer Reihe von Kriterien, die die Fermat-Quotienten beinhalteten.

MIRIMANOFF zeigte im Jahre 1910:

Wenn der erste Fall von *FLS* für den Exponenten p nicht wahr ist, dann gilt $q_p(3) \equiv 0 \pmod{p}$.

Da $p = 1093$, 3511 obige Kongruenz nicht erfüllen, folgt daraus die Richtigkeit des ersten Falles für alle Primzahlen kleiner als $2{,}5 \times 10^{15}$.

Diese Arbeit wurde von FROBENIUS, VANDIVER, POLLACZEK, ROSSER sowie in jüngerer Zeit von GRANVILLE und MONAGAN fortgesetzt. Mithilfe der Methode konnte bewiesen werden, dass wenn der erste Fall für p nicht gilt, dann ist

$$q_p(\ell) \equiv 0 \pmod{p} \quad \text{für Primzahlen } \ell,\ \ell \leq 89. \tag{8.31}$$

Ein erwähnenswertes Korollar ist das folgende, das auf SPUNAR zurückgeht:

Sei p eine ungerade Primzahl, die die folgende Eigenschaft (P89) erfüllt:

> Es gibt k, das nicht Vielfaches von p ist und für das gilt $kp = a \pm b$, wobei alle Primfaktoren von a, b höchstens gleich 89 sind.

Dann stimmt der erste Fall von *FLS* für den Exponenten p.

Der Beweis ist so einfach, dass ich ihn an dieser Stelle angebe.

Wenn der erste Fall für den Exponenten p nicht stimmt, dann folgt für jedes prime ℓ, $\ell \leq 89$ nach Formel (8.31), dass $\ell^{p-1} \equiv 1 \pmod{p^2}$. Also $a^{p-1} \equiv 1 \pmod{p^2}$ und $b^{p-1} \equiv 1 \pmod{p^2}$. Daher, $a^p \equiv a \pmod{p^2}$ und $b^p \equiv b \pmod{p^2}$. Aber $a = \mp b + kp$ und so $a^p \equiv \mp b^p \pmod{p^2}$. Aus $kp = a \pm b \equiv a^p \pm b^p \equiv 0 \pmod{p^2}$ folgt, dass p Teiler von k ist, was der Voraussetzung widerspricht.

In diesem Zusammenhang gibt es das folgende offene Problem:

Gibt es unendlich viele Primzahlen p mit Eigenschaft (P89)?

Puccioni zeigte im Jahre 1968: Wenn obige Menge endlich ist, dann ist für jede Primzahl ℓ, $\ell \leq 89$, $\ell \not\equiv 1 \pmod 8$ die Menge $M_\ell - \{p \mid \ell^{p-1} \equiv 1 \pmod{p^2}\}$ unendlich.

Unglücklicherweise bedeutet dieser Satz möglicherweise nichts, da die beiden fraglichen Mengen, so dünn sie auch sein mögen, immer noch unendlich groß sein können.

Hier eine Folgerung aus Spunars Resultat, die bereits Mirimanoff fand:

Der erste Fall von *FLS* gilt für alle primen Exponenten p der Form $p = 2^m \pm 1$.

Es ist ein Leichtes zu zeigen, dass:

Wenn $2^m + 1$ eine Primzahl ist, so $m = 2^n$ $(n \geq 0)$. Die Zahlen

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

wurden erstmalig von Fermat untersucht und heißen daher Fermat-Zahlen.

In ähnlicher Weise gilt, dass wenn $2^m - 1$ eine Primzahl ist, dann muss $m = p$ prim sein. Die Zahlen

$$M_p = 2^p - 1 \quad (p \text{ prim})$$

heißen Mersenne-Zahlen.

Fermat glaubte, dass alle Fermat-Zahlen prim seien. Und tatsächlich,

$$F_1 = 5, \quad F_2 = 17, \quad F_2 = 257, \quad F_4 = 65537.$$

F_5 ist erheblich größer und hat etwa 10 Stellen.

Euler bewies 1747 das folgende Kriterium: Wenn p Teiler von F_n $(n \geq 2)$ ist, so ist $p = 2^{n+1}k + 1$ (mit $k \geq 1$).

Er wandte dieses Kriterium auf F_5 an und fand den Teiler 641, also ist F_5 keine Primzahl.

Dies kann man auch auf die folgende Weise erkennen:

$$\begin{aligned} 641 &= 2^4 + 5^4 = 5 \times 2^7 + 1, \\ 2^{32} &= 2^4 \times 2^{28} = (641 - 5^4) \times 2^{28} \\ &= 641 \times 2^{28} - (5 \times 2^7)^4 \\ &= 641 \times 2^{28} - (641 - 1)^4 \equiv -1 \pmod{641}. \end{aligned}$$

Also teilt 641 die Zahl $2^{32} - 1 = F_5$.

Das Studium der Fermat- und Mersenne-Zahlen führte zur Entdeckung der ersten Primzahltests für große Zahlen.

Das erste Kriterium entwickelte LUCAS in Form einer Umkehrung von Fermats kleinem Satz:

Sei $n \geq 3$ ungerade und angenommen, es gebe a mit $1 < a < n$ derart, dass

$$a^{p-1} \equiv 1 \pmod{n},$$

und für Primteiler q von $n - 1$ gelte

$$a^{\frac{n-1}{q}} \not\equiv -1 \pmod{n}.$$

Dann ist n eine Primzahl.

Auf einem solchen Kriterium basierend zeigte PEPIN:

Die Fermat-Zahl F_n ist genau dann prim, wenn

$$3^{\frac{F_n-1}{2}} \equiv -1 \pmod{F_n}.$$

Es wurde intensiv nach Fermat-Primzahlen gesucht. Nach meiner Information, die allerdings schon wieder überholt sein kann, ist die größte als zerlegbar nachgewiesene Fermat-Zahl $F_{2478785}$. Es sind normalerweise umfangreiche Berechnungen notwendig, um eine Fermat-Zahl als zerlegbar nachzuweisen.

Entgegen FERMATs Glauben sind die einzigen bisher bekannten Fermat-Primzahlen die, die er selbst schon kannte!

Die folgenden Vermutungen sind schwächer als FERMATs ursprüngliche Aussage:

(a) EISENSTEIN (1844): Es gibt unendlich viele Fermat-Primzahlen;

(b) SCHINZEL (1963): Es gibt unendlich viele Fermat-Zahlen, die quadratfrei sind (d.h. Produkte verschiedener Primzahlen).

Für die Mersenne-Zahlen gab EULER den ersten Test für Faktoren an: Wenn p eine Primzahl ist mit $p > 3$, $p \equiv 3 \pmod 4$, dann teilt $2p + 1$ die Mersenne-Zahl M_p genau dann, wenn $2p + 1$ prim ist.

Auf diese Weise fand EULER heraus: 23 ist Teiler von M_{11}; ...; 503 ist Teiler von M_{251}, usw. ....

Das Problem ist die Bestimmung von Primzahlen p, für die $2p+1$ wieder prim ist. Solche Primzahlen nennt man zu Recht *Sophie Germain Primzahlen*. Sie war die erste, die diese Zahlen um 1820 untersuchte und bewies dabei den folgenden, wundervollen Satz, der von vollkommen neuer Natur war:

Wenn p und $2p+1$ Primzahlen sind, dann ist der erste Fall von *FLS* für den Exponenten p wahr.

Eine offene Frage ist: Gibt es unendlich viele Sophie Germain Primzahlen?

Man vergleiche diese Frage mit der folgenden (dem Primzahlzwillingsproblem):

Gibt es unendlich viele Primzahlen p derart, dass $p+2$ auch prim ist?

In beiden Fällen sind es lineare Polynome $2X+1$ bzw. $X+2$, und die Frage ist, ob sie unendlich oft Primzahlwerte für Primzahlargumente annehmen.

Lassen Sie mich nun einen sehr effizienten Primzahltest für Fermat- und Mersenne-Zahlen beschreiben, der im Jahr 1878 von LUCAS entwickelt wurde. Er verwendet linear-rekurrente Folgen zweiter Ordnung und genauer, Fibonacci- und Lucas-Zahlen.

Im dreizehnten Jahrhundert betrachtete FIBONACCI die Folge der Zahlen $F_0 = 0$, $F_1 = 1$, $F_2 = 1$, $F_3 = 2$, $F_4 = 3$, $F_5 = 5$, $F_6 = 8$, ..., und allgemeiner

$$F_n = F_{n-1} + F_{n-2}.$$

(Ich hoffe, es gibt an dieser Stelle keine Verwechslungen mit Fermat-Zahlen.)

Die Fibonacci-Zahlen haben eine Fülle an arithmetischen Eigenschaften. Bücher wurden über sie geschrieben und eine vierteljährlich erscheinende Zeitschrift widmet sich ihrer.

Eine begleitende Folge ist die der Lucas-Zahlen: $L_0 = 2$, $L_1 = 1$, $L_2 = 3$, $L_3 = 4$, $L_4 = 7$, $L_5 = 11$, ... und $L_n = L_{n-1} + L_{n-2}$ für $n \geq 2$.

Allgemeiner seien Zahlen U_0, U_1 und α, $\beta \in \mathbb{Q}$ gegeben und sei

$$U_n = \alpha U_{n-1} - \beta U_{n-2}. \tag{8.32}$$

Die Gleichung $X_2 - \alpha X + \beta = 0$ hat die Nullstellen

$$a = \frac{\alpha + \sqrt{\alpha^2 - 4\beta}}{2}, \quad b = \frac{\alpha - \sqrt{\alpha^2 - 4\beta}}{2},$$

also

$$\alpha = a + b, \beta = ab$$

und

$$U_n = (a+b)U_{n-1} - abU_{n-2}. \tag{8.33}$$

Für die Fibonacci- und Lucas-Zahlen ist $\alpha = 1$, $\beta = -1$, also

$$a = \frac{1+\sqrt{5}}{2} \text{ (der „Goldene Schnitt“)}, \quad b = \frac{1-\sqrt{5}}{2}.$$

Binets Formel ergibt

$$U_n = \frac{a^n - b^n}{a-b}. \tag{8.34}$$

Die Begleitfolge ist

$$V_n = a^n + b^n. \tag{8.35}$$

Setze

$$W_n = \frac{V_{2^{n-1}}}{Q^{2^{n-2}}} \quad (\text{für } n \geq 2), \tag{8.36}$$

somit,

$$W_1 = \frac{\alpha^2 - 2\beta}{\beta}, \quad W_{n+1} = W_n^2 - 2. \tag{8.37}$$

Durch geeignete Wahl von α, β gewann LUCAS die praktische „Testsequenz“:

Für $p \equiv 1 \pmod 4$ sei $W_2 = -4$, $W_{n+1} = W_n^2 - 2$, was zur Folge $-4, 14, 194, \ldots$ führt.

Sein Kriterium:

$M_p = 2^p - 1$ ist eine Primzahl genau dann, wenn M_p Teiler von W_p ist.

Für $p \equiv 3 \pmod 4$, $p > 3$, sei $W_2 = -3$, $W_{n+1} = W_n^2 - 2$, somit erhält man die Folge $-3, 7, 47, \ldots$.

Sein Kriterium in diesem Fall ist wiederum: $M_p = 2^p - 1$ ist eine Primzahl genau dann, wenn M_p Teiler von W_p ist.

Diese Methode wird heute verwendet, um Mersenne-Zahlen auf ihre Primalität hin zu prüfen.

Im Jahre 1644 war MERSENNE bekannt, dass M_p für $p = 2, 3, 5, 7, 13, 17, 19, 31$ eine Mersenne-Primzahl ist.

Im Jahre 1878 zeigte LUCAS, dass dies auch für $p = 61, 89, 107$ und 127 der Fall ist.

Mithilfe von Computern gewann man bis heute die Kenntnis von 46 Mersenne-Primzahlen, wobei die größten beiden $M_{43112609}$ mit 12978189 Stellen und $M_{37156667}$ mit 11185272 Stellen sind.

Schinzel vermutete Folgendes:

Es gibt unendlich viele quadratfreie Mersenne-Zahlen. Bis heute wurde keine Fermat- oder Mersenne-Zahl mit einem quadratischen Faktor gefunden.

Im Jahr 1965 nahm sich Rotkiewicz der obigen Vermutung an und bewies:

Wenn Schinzels Vermutung über Mersenne-Zahlen wahr ist, dann gibt es unendlich viele Primzahlen p derart, dass

$$2^{p-1} \not\equiv 1 \pmod{p^2}.$$

Übrigens machte Rotkiewicz vom folgenden interessanten (und vielfach wiederentdeckten) Satz von Zsigmondy (1892) Gebrauch:

Wenn $n \neq 6$, $n \geq 3$, $a \geq 2$, dann gibt es eine Primzahl p derart, dass die Ordnung von a modulo p gleich n ist. Äquivalent dazu gibt es eine Primzahl p derart, dass p Teiler von $a^n - 1$ ist, aber p die Zahlen $a^m - 1$ für $m < n$ nicht teilt.

Dieser Satz wurde entdeckt von Zsigmondy (davor von Bang für $a = 2$), Birkhoff und Vandiver, Dickson, Carmichael, Kanold, Artin, Hering, Lüneburg, Pomerance, und ... von wem noch? Ich würde es gerne wissen.

Aus dem Satz von Rotkiewicz folgt, dass es eine ziemlich überraschende und ich möchte sogar sagen tiefe Verbindung zwischen solch unterschiedlichen Bereichen wie Fermats letztem Satz, der Kongruenz $2^{p-1} \equiv 1 \pmod{p^2}$ und der Faktorisierung von Mersenne-Zahlen gibt. Aber ich bin vom Thema abgeschweift.

Es gibt einen heuristischen Grund zu glauben, dass es unendlich viele Primzahlen p mit $2^{p-1} \equiv 1 \pmod{p^2}$ gibt. Das Argument verläuft wie folgt. Da nichts Gegenteiliges bekannt ist, kann man (heuristisch) annehmen, dass für jede Primzahl p die Wahrscheinlichkeit, dass $\frac{2^{p-1}-1}{p} \equiv 0 \pmod{p}$ erfüllt ist, gerade $\frac{1}{p}$ beträgt, da es p Restklassen modulo p gibt. Wenn x irgendeine reelle Zahl ist, dann sollte die Anzahl der Primzahlen $p \leq x$ mit $2^{p-1} \equiv 1 \pmod{p^2}$ gleich

$$\sum_{p \leq x} \frac{1}{p} = \log\log x + \text{Fehlerterm}$$

sein.

Also gäbe es unendlich viele p, die obige Kongruenz erfüllen. Dieses Argument lässt sich jedoch nicht streng führen. Aus den Berechnungen ergibt sich abgesehen von den zwei Ausnahmen, dass $2^{p-1} \not\equiv 1 \pmod{p^2}$, also sollte man erwarten, dass es unendlich viele Primzahlen p geben sollte, die $2^{p-1} \not\equiv 1 \pmod{p^2}$ genügen. Dies ist noch nicht bewiesen, folgt aber aus der wichtigen und interessanten (ABC)-Vermutung von Masser und Oesterlé:

Für jedes $\varepsilon > 0$ gibt es eine reelle Zahl $K(\varepsilon) > 0$ derart, dass für beliebige positive ganze Zahlen A, B und C mit $\mathrm{ggT}(A, B, C) = 1$ und $A + B = C$ gilt

$$C \leq K(\varepsilon) r^{1+\varepsilon}$$

wobei r (das *Radikal* von ABC) das Produkt der verschiedenen Primfaktoren von ABC ist.

Wenn zum Beispiel $\varepsilon = \frac{1}{2}$ und $A = 2^m$, $B = 3^n$ (mit m und n groß) sowie $C = A^m + B^n$, dann folgt aus $C < K(\frac{1}{2}) r^{3/2}$ und $r = 6 \prod_{p|C} p$, dass C ein großes Radikal haben muss.

Silverman (1988) bewies:

Wenn die (ABC)-Vermutung wahr ist, dann gibt es unendlich viele Primzahlen p mit $2^{p-1} \not\equiv 1 \pmod{p^2}$.

Es wäre von größter Wichtigkeit, diese Vermutung zu beweisen.

Und die Zahl 1093 ist tatsächlich interessant....

Literaturverzeichnis

1828 N. H. Abel. Aufgabe von Herrn N. H. Abel zu Christiania (in Norwegian). *J. reine u. angew. Math.*, 3:212.

1828 C. G. J. Jacobi. Beantwortung der aufgabe S. 212 dieses Bandes: "Kann $\alpha^{m-1} - 1$ wenn μ eine Primzahl und α eine ganze Zahl und kliener als μ und größer als 1 ist, durch $\mu\mu$ theilbar sein?". *J. reine u. angew. Math.*, 3:301–303.

1844 F. G. Eisenstein. Aufgaben. *J. reine u. angew. Math.*, 27:87. (Nachdruck in *Mathematische Werke*, Vol. 1. No. 3, Chelsea, New York. 1975).

1850 F. G. Eisenstein. Eine neue Gattung zahlentheoretischer Funktionen, welche von zwei Elementen abhangen und durch gewisse lineare Funktionalgleichungen definiert werden. *ber. über verhandl. der königl. Preuß. Akad. d. Wiss. zu Berlin*, 36–42. Nachdruck in *Mathematische Werke*, Vol. 2. 705–712, Chelsea, New York, 1975.

1861 J. J. Sylvester. Note relative aux communications faites dans les séances du 28 Janvier et 4 Février 1861. *C. R. Acad. Sci. Paris*, 52:307–308. Nachdruck in *Math. Papers*, Vol. 2: 234–235; und *Corrigenda*, 241, Cambridge University Press, 1908.

1861 J. J. Sylvester. Sur une propriété des nombres premiers qui se rattache au théorème de Fermat. *C. R. Acad. Sci. Paris*, 52: 161–163. Nachdruck in *Math. Papers*, Vol. 2: 229–231, Cambridge University Press, 1908.

1876 E. Lucas. Sur la recherche des grands nombres premiers. *Congrès de l'Assoc. Française pour l'Avancement des Sciences*, Clermont-Ferrand 5:61–68.

1877 T. Pepin. Sur la formule $2^{2^n}+1$. *C. R. Acad. Sci. Paris*, 85: 329–331.

1878 E. Lucas. Théorie des fonctions numériques simplement périodiques. *Amer. J. of Math.*, 1:184–240 und 289–321.

1905 M. Lerch. Zur Theorie der Fermatschen Quotienten $a^{p-1} - 1/p \equiv q(a)$. *Math. Annalen*, 60:471–490.

1909 A. Friedmann und J. Tamarkine. Quelques formules concernant la théorie de la fonction $\{x\}$ et des nombres de Bernoulli. *J. reine u. angew. Math.*, 135:146–156.

1910 D. Mirimanoff. Sur le dernier théorème de Fermat. *C. R. Acad. Sci. Paris*, 150:204–206.

1913 W. Meissner. Über die Teilbarkeit von $2^n - 2$ durch das Quadrat der Primzahl $p = 1093$. *Sitzungsber. Akad. d. Wiss., Berlin*, 51:663–667.

1914 H. S. Vandiver. Extension of the criterion of Wieferich and Mirimanoff in connection with Fermat's last theorem. *J. reine u. angew. Math.*, 144:314–318.

1922 N. G. W. H. Beeger. On a new case of the congruence $2^{p-1} \equiv 1 \pmod{p^2}$. *Messenger of Math.*, 51:149–150.

1927 E. Landau. *Vorlesungen über Zahlentheorie, Vol. 3.* S. Hirzel, Leipzig. Nachdruck von Chelsea, New York, 1969.

1946 F. Le Lionnais. *Les Grands Courants de la Pensée Mathématique.* A. Blanchard, Paris.

1953 K. Goldberg. A table of Wilson quotients and the third Wilson prime. *J. London Math. Soc.*, 28:252–256.

1955 H. S. Vandiver. Divisibility problems in number theory. *Scripta Math.*, 21:15–19.

1963 A. Schinzel. Remarque au travail de W. Sierpiński sur les nombres $a^{2^n}+1$. *Colloq. Math.*, 10:137–138.

1963 W. Sierpiński. Sur les nombres composés de la forme $a^{2^n}+1$. *Colloq. Math.*, 10:133–135.

1965 A. Rotkiewicz. Sur les nombres de Mersenne dépourvus de diviseurs carrés et sur les nombres naturels n tels que $n^2 \mid 2^n-2$. *Matematicky Vesnik, Beograd, (2)*, 17:78–80.

1968 S. Puccioni. Un teorema per una resoluzione parziale del famoso teorema di Fermat. *Archimede*, 20:219–220.

1969 R. K. Guy. The primes 1093 and 3511. *Math. Student*, 35: 204–206 (1969).

1977 W. Johnson. On the non-vanishing of Fermat quotients (mod p). *J. reine u. angew. Math.*, 292:196–200.

1981 C. Fadiman und S. Aaron. *The Joys of Wine.* Galahad Books, New York.

1988 J. H. Silverman. Wieferich's criterion and the *abc*-conjecture. *J. Nb. Th.*, 30:226–237.

1996 P. Ribenboim. *The New Book of Prime Number Records.* Springer-Verlag, New York.

1997 R. E. Crandall, K. Dilcher und C. Pomerance. A search for Wieferich and Wilson primes. *Math. Comp.*, 66:433–449.

2005 J. Knauer und J. Richstein. The continuing search for Wieferich primes. *Math. Comp.*, 74:1559–1563.

9

Machtlos gegenüber Mächtigkeit

Ich habe diese Vorlesung viele Male in vielen Ländern gehalten. Und können Sie sich vorstellen, wer sie besuchte?

Politikwissenschaftler! Drittweltländer treffen auf die Weltmächte? Und der machtlose Paulo erzählt, wie sie sich wehren oder selbst zur Weltmacht werden ....

Nein, ich bin nur ein Mathematiker, der nicht weiß, wie man die vielen Probleme lösen soll, die mit denjenigen mächtigen ganzen Zahlen zu tun haben, die sich aus Potenzen zusammensetzen: den sogenannten *machtvollen* oder auch *potenten* Zahlen.

Meine Absicht ist es, verschiedene solcher Probleme vorzustellen, in einigen Fällen bis hin zu Vermutungen darüber, was wohl zutrifft.

Es werden die folgenden Bezeichnungsweisen zur Verwendung kommen. Für eine endliche Menge S bezeichne $\#S$ die Anzahl der Elemente von S. Wenn S eine Menge positiver ganzer Zahlen ist und $x \geq 1$, so sei $S(x) = \{s \in S \mid s \leq x\}$.

Die ganzen Zahlen der Form a^n, wobei $|a| > 1$, $n > 1$, nennt man Potenzen. Die Zahl 1 ist demnach keine Potenz.

1 Potente Zahlen

Der erste Artikel über potente Zahlen stammt von Erdös (1935); die englische Bezeichnung „powerful number“ wird jedoch später Golomb (1970) zugeschrieben.

Sei $k \geq 2$. Die natürliche Zahl $n \geq 1$ nennt man eine *k-potente Zahl*, wenn die folgende Eigenschaft erfüllt ist: Wenn eine Primzahl p die Zahl n teilt, so ist auch p^k Teiler von n.

Mit anderen Worten sind die k-potenten Zahlen genau die ganzen Zahlen, die man in der Form $a_0^k a_1^{k+1} \cdots a_{k-1}^{2k-1}$ schreiben kann (wobei $a_0, \ldots, a_{k-1}$ nicht notwendigerweise teilerfremde positive ganze Zahlen sind). Eine 2-potente Zahl nennt man auch eine *quadratvolle* Zahl, eine 3-potente auch *kubikvoll*. Insbesondere sind quadratvolle Zahlen solche, die die Form $a_0^2 a_1^3$ mit $a_0, a_1 \geq 1$ haben. Man beachte, dass 1 eine potente Zahl ist. Ich werde die Menge der k-potenten Zahlen mit W_k bezeichnen.

Die Hauptprobleme im Zusammenhang mit potenten Zahlen sind folgender Art:

1. Verteilung von potenten Zahlen.
2. Additive Probleme.
3. Differenzprobleme.

A Verteilung potenter Zahlen

Die Absicht ist es, die Anzahl der Elemente der Menge

$$W_k(x) = \{n \in W_k \mid 1 \leq n \leq x\} \tag{9.1}$$

zu bestimmen, wobei $x \geq 1$, $k \geq 2$.

Bereits im Jahr 1935 gaben Erdös und Szekeres das erste Resultat über $W_2(x)$ an:

$$\#W_2(x) = \frac{\zeta(\frac{3}{2})}{\zeta(3)} x^{1/2} + O(x^{1/3}) \quad \text{wenn } x \to \infty, \tag{9.2}$$

wobei $\zeta(s)$ die Riemannsche Zetafunktion ist; siehe auch Bateman (1954) und Golomb (1970).

Zur Beschreibung weiterer Resultate führe ich die Zetafunktion in Verbindung mit der Folge der k-potenten Zahlen ein. Sei

$$j_k(n) = \begin{cases} 1 & \text{wenn } n \;\; k\text{-potent ist,} \\ 0 & \text{sonst.} \end{cases}$$

Die Reihe $\sum_{n=1}^{\infty} \frac{j_k(n)}{n^s}$ konvergiert für $\mathrm{Re}(s) > \frac{1}{k}$ und definiert dort eine Funktion $F_k(s)$. Diese Funktion erlaubt die für $\mathrm{Re}(s) > \frac{1}{k}$ gültige Eulersche Produktdarstellung

$$F_k(s) = \prod_p \left(1 + \frac{\frac{1}{p^{ks}}}{1 - \frac{1}{p^s}}\right) = \prod_p \left(1 + \frac{1}{p^{(k-1)s}(p^s - 1)}\right). \tag{9.3}$$

Mithilfe wohlbekannter Methoden zeigten Ivić und Shiu 1982:

1.1. $\#W_k(x) = \gamma_{0,k}x^{\frac{1}{k}} + \gamma_{1,k}x^{\frac{1}{k+1}} + \cdots + \gamma_{k-1,k}x^{\frac{1}{2k-1}} + \Delta_k(x)$, wobei $\gamma_{i,k}$ das Residuum von $\frac{1}{k+i}$ an $\frac{F_k(s)}{s}$ ist.

Genauer,

$$\gamma_{i,k} = C_{k+i,k}\frac{\Phi_k(\frac{1}{k+i})}{\zeta(\frac{2k+2}{k+i})}, \tag{9.4}$$

wobei

$$C_{k+i,k} = \prod_{\substack{j=k \\ j\neq k+i}}^{2k-1} \zeta\left(\frac{j}{k+i}\right), \tag{9.5}$$

sowie $\Phi_2(s) = 1$, und wenn $k > 2$, dann hat $\Phi_k(s)$ eine Dirichletreihe mit Abszisse absoluter Konvergenz $\frac{1}{2k+3}$ und Fehlerterm $\Delta_k(x)$.

Erdös und Szekeres hatten diesen Fehlerterm bereits untersucht und zeigten, dass

$$\Delta_k(x) = O(x^{\frac{1}{k+1}}) \quad \text{wenn } x \to \infty. \tag{9.6}$$

Mittlerweile sind bessere Abschätzungen für den Fehlerterm bekannt. Sei

$$\rho_k = \inf\{\rho > 0 \mid \Delta_k(x) = O(x^\rho)\}.$$

Bateman und Grosswald zeigten im Jahr 1958, dass $\rho_2 \leq \frac{1}{6}$ und $\rho_3 \leq \frac{7}{46}$.

Schärfere Resultate stammen von Ivić und Shiu:

$$\begin{array}{lll} \rho_2 \leq 0{,}128 < \frac{1}{6}, & \rho_3 \leq 0{,}128 < \frac{7}{46}, & \rho_4 \leq 0{,}1189, \\ \rho_5 \leq \frac{1}{10}, & \rho_6 \leq \frac{1}{12}, & \rho_7 \leq \frac{1}{14}, \quad \text{usw.} \end{array}$$

Ich verweise in diesem Zusammenhang auch auf die Arbeit von Krätzel (1972).

Es wird vermutet, dass für jedes $k \geq 3$,

$$\Delta_k(x) = O(x^{\frac{1}{2k}}) \quad \text{für } x \to \infty. \tag{9.7}$$

Genauer, wenn man $k = 2$ wählt:

$$\#W_2(x) = \frac{\zeta(\frac{3}{2})}{\zeta(3)}x^{\frac{1}{2}} + \frac{\zeta(\frac{2}{3})}{\zeta(2)}x^{\frac{1}{3}} + \Delta_2(x), \tag{9.8}$$

mit $\Delta_2(x) = O(x^{\frac{1}{6}})$, für $x \to \infty$.

B Additive Probleme

Für $h \geq 2$, $k \geq 2$ werde ich die folgende Bezeichnungen verwenden:

$$\sum hW_k = \{\sum_{i=1}^{h} n_i \mid \text{jedes } n_i \in W_k \cup \{0\}\},$$
$$\sum hW_k(x) = \{n \in \sum hW_k \mid n \leq x\} \quad (\text{für } x \geq 1).$$

Bei den additiven Probleme geht es um den Vergleich der Mengen $\sum hW_k$ mit der Menge der natürlichen Zahlen, der Verteilung der Mengen und ähnliche Fragen.

Die Verteilung von $\sum 2W_2$ hat Erdös im Jahr 1975 behandelt:

1.2.

$$\#\sum 2W_2(x) = o\left(\frac{x}{(\log x)^{\alpha}}\right) \quad (\text{für } x \to \infty), \text{ wobei } 0 < \alpha < \tfrac{1}{2}.$$

Insbesondere ist $\#\sum 2W_2(x) = o(x)$, also gibt es unendlich viele natürliche Zahlen, die nicht Summe zweier quadratvoller Zahlen sind.

Odoni zeigte im Jahr 1981, dass es keine Konstante $C > 0$ derart gibt, dass

$$\#\sum 2W_2(x) \sim \frac{Cx}{(\log x)^{1/2}} \quad (\text{für } x \to \infty).$$

Das folgende Resultat war von Erdös und Ivić in den 1970er Jahren vermutet worden, bewiesen wurde es von Heath-Brown (1988):

1.3. Es gibt eine effektiv berechenbare Zahl n_0 mit der Eigenschaft, dass jedes $n \geq n_0$ gleich der Summe von höchstens drei quadratvollen Zahlen ist.

Die einzig bekannten Ausnahmen bis 32000 sind 7, 15, 23, 87, 111, und 119. Mollin und Walsh vermuteten im Jahr 1986, dass es keine weiteren Ausnahmen gibt.

Das folgende Problem bezüglich kubikvoller Zahlen ist immer noch offen:

Gibt es unendlich viele natürliche Zahlen, die nicht Summe dreier kubikvoller Zahlen sind? Wahrscheinlich lautet die Antwort Ja.

C Differenzprobleme

Probleme dieser Art sind die folgenden:

Problem D1. Gegeben sei $k \geq 2$, Bestimme welche Zahlen N die Form $N = n_1 - n_2$ haben, wobei $n_1, n_2 \in W_k$. Einen solchen Ausdruck für N nennt man eine *Darstellung als Differenz von k-potenten Zahlen*, oder einfach eine k-potente Darstellung. Für $k = 2$ werde ich einfach quadratvolle Darstellung schreiben. Falls $\mathrm{ggT}(n_1, n_2) = 1$, so heißt die Darstellung *primitiv*; falls n_1 oder n_2 eine Potenz oder gleich 1 ist, nennt man die Darstellung *degeneriert*.

Problem D2. Gegeben sei $k \geq 2$, $N \geq 1$. Bestimme die Menge oder nur die Anzahl der Darstellungen (primitiv oder nicht, degeneriert oder nicht) von N als Differenz von k-potenten Zahlen.

Das folgende Problem ist von derselben Art:

Problem D3. Gegeben seien ganze Zahlen $N_1, N_2 \geq 1$. Bestimme ob es k-potente Zahlen n_1, n_2, n_3 derart gibt, dass

$$n_2 - n_1 = N_1 \quad \text{und} \quad n_3 - n_2 = N_2.$$

Untersuche in diesem Fall die möglichen Tripel.

Man könnte sich ähnliche Probleme mit verschiedenen vorgegebenen Differenzen N_1, $N_2, \ldots, N_r \geq 1$ vorstellen, aber wie wir sehen werden, ist Problem D3 in seiner einfachsten Form ungelöst und sicher sehr schwierig.

Ich werde mit der Diskussion der Probleme D1 und D2 beginnen. Die erste Bemerkung, die auf Mahler zurückgeht zeigt, dass diese Fragen in engem Zusammenhang mit den Gleichungen $X^2 - DY^2 = C$ stehen.

Mahler sagte: Da die Gleichung $X^2 - 8Y^2 = 1$ unendlich viele Lösungen in ganzen Zahlen (x, y) besitzt und da die Zahl $8y^2$ quadratvoll ist, gestattet die 1 unendlich viele degenerierte (primitive) quadratvolle Darstellungen.

Im Jahr 1976 zeigte Walker, dass 1 auch eine unendliche Anzahl von nicht-degenerierten (primitiven) Darstellungen besitzt.

Im Jahr 1981 zeigte Sentance, dass 2 unendlich viele primitive degenerierte quadratvolle Darstellungen besitzt, darunter die kleinste:

$$2 = 27 - 25 = 70227 - 70225 = 189750627 - 189750625.$$

In jüngerer Zeit erschienen fast gleichzeitig und unabhängig voneinander frühere Arbeiten zusammenfassende Artikel von McDaniel, Mollin und Walsh, und Vanden Eynden. Es wurde gezeigt, dass:

1.4. Jede natürliche Zahl besitzt sowohl unendlich viele primitive degenerierte wie auch nicht-degenerierte quadratvolle Darstellungen.

Darüberhinaus gibt es einen Algorithmus, um solche Darstellungen zu bestimmen. Eine Zusammenfassung der obigen Resultate findet sich auch in Mollin (1987).

Erdös fragte, ob sich aufeinanderfolgende quadratvolle Zahlen auch anders als durch Lösungen geeigneter Gleichungen $EX^2 - DY^2 = 1$ finden lassen.

Bezüglich der Verteilung von Paaren aufeinanderfolgender quadratvoller Zahlen gibt es mehrere Vermutungen von Erdös (1976).

Erste* Erdös Vermutung:
[1]$\#\{n \mid n \text{ und } n+1 \text{ sind quadratvoll, } n \leq x\} < (\log x)^c$, *wobei* $c > 0$ *eine Konstante ist.*

Es ist bisher noch nicht einmal bewiesen, dass $c' x^{\frac{1}{3}}$ eine obere Schranke ist (mit einer Konstanten $c' > 0$).

Zweite Erdös Vermutung:
Es gibt keine zwei aufeinanderfolgenden kubikvollen Zahlen.

Es ist interessant zu erwähnen, dass die einzigen bekannten Beispiele aufeinanderfolgender ganzer Zahlen, von denen eine quadratvoll und die andere kubikvoll ist, $(8, 9)$ und $(12167, 12168)$ sind.

Eine verwandte Vermutung ist die folgende:

Dritte Erdös Vermutung:
Sei $a_1 < a_2 < a_3 < \cdots$ *die Folge kubikvoller Zahlen. Es gibt Konstanten* $c > 0$, $c' > 0$ *derart, dass für jedes genügend große* m *gilt,*

$$a_{m+1} - a_m > c m^{c'}.$$

Insbesondere,

$$\lim_{m \to \infty} (a_{m+1} - a_m) = \infty.$$

[1] Keiner vermag zu sagen, was Erdös' erste Vermutung war — ich würde mich nicht wundern, wenn es sein erster sinnvoller Satz als Kind war....

Vierte Erdös Vermutung:
Es gibt unendlich viele kubikvolle Zahlen, die die Summe zweier kubikvoller Zahlen sind.

Ich betrachte nun Problem D3 in seiner einfachsten Form, die sich auf drei aufeinanderfolgende quadratvolle Zahlen bezieht.

Mit seinem großartigen Verständnis und Tiefblick vermutete Erdös:

Fünfte Erdös Vermutung:
Es gibt keine drei aufeinanderfolgenden quadratvollen Zahlen.

Dies geht über die von Makowski (1962) und unabhängig von Hyyrö (1963) bewiesene Tatsache hinaus, dass es keine drei aufeinanderfolgenden Potenzen gibt.

Von diesen Vermutungen wurde nur die vierte nachgewiesen. Im Jahr 1995 bewies Nitaj, dass es unendlich viele kubikvolle Zahlen gibt, die eine Darstellung als Summe $x + y$ besitzen, wobei x ein Kubus und y eine kubikvolle Zahl ist. Im Jahr 1998 zeigte Cohn genauer, dass es unendlich viele kubikvolle Zahlen mit einer Summendarstellung $x + y$ derart gibt, dass x und y beides nicht-kubische kubikvolle Zahlen sind.

An späterer Stelle in diesem Kapitel werde ich noch auf die zweite, dritte und fünfte Vermutung zurückkommen. Es handelt sich dabei um schwierige Probleme und Berechnungen können höchstens dazu dienen, drei aufeinanderfolgende quadratvolle Zahlen zu finden—sofern sie existieren. Aber wann sollte man die Berechnung abbrechen, da ja keine Schranke bekannt ist?

Es ist völlig unerwartet und verblüffend, dass die Existenz dreier aufeinanderfolgender quadratvoller Zahlen mit Fermats letztem Satz in Verbindung steht. Ich werde später noch darauf eingehen.

2 Potenzen

Ich werde nun untersuchen, ob eine Summe zweier oder mehr Potenzen wieder eine Potenz sein kann und falls ja, wie oft. Ein schwierigeres Problem ist es, wenn gefordert wird, dass die Exponenten dieser Potenzen dieselben sein sollen.

A Pythagoreische Dreiecke und Fermats Problem

Es ist wohlbekannt, dass es unendlich viele primitive Pythagoreische Dreiecke ganzer Zahlen (x, y, z) gibt mit $0 < x, y, z$, $\mathrm{ggT}(x, y) = 1$, y gerade und $x^2 + y^2 = z^2$.

Die Gesamtheit dieser Tripel ist wie folgt parametrisiert:

$$\begin{aligned} x &= a^2 - b^2 \\ y &= 2ab \\ z &= a^2 + b^2 \end{aligned}$$

wobei $1 \leq b < a$ mit $\mathrm{ggT}(a, b) = 1$.

In diesem Zusammenhang ist das folgende Problem noch offen: Gibt es unendlich viele Pythagoreische Dreiecke (x, y, z) derart, dass x und y Primzahlen sind? Diese Frage wurde unter der Annahme untersucht, dass die Vermutung von Bunjakowski (1857) wahr ist, die sehr überzeugend ist.

Ein irreduzibles Polynom $f \in \mathbb{Z}[X]$ heißt *stark primitiv*, wenn es keine Primzahl p derart gibt, dass p für jede ganze Zahl k Teiler von $f(k)$ ist. Insbesondere ist der größte gemeinsame Teiler der Koeffizienten von f gleich 1.

Die Vermutung von Bunjakowski ist die folgende:

Wenn $f \in \mathbb{Z}[X]$ ein irreduzibles stark primitives Polynom ist, dann gibt es unendlich viele ganze Zahlen n derart, dass $|f(n)|$ eine Primzahl ist.

Man beachte, dass wenn $f(X)$ den Grad 1 hat, dann ist $f(X) = aX + b$ mit $\mathrm{ggT}(a, b) = 1$ und die obige Vermutung ist wahr—dies ist der Satz von Dirichlet über Primzahlen in arithmetischen Folgen.

Im Jahr 1958 formulierten Schinzel und Sierpiński diese und weitere Vermutungen neu und leiteten viele Konsequenzen aus ihnen ab. Insbesondere zeigten sie:

2.1. Angenommen die Vermutung von Bunjakowski stimmt. Seien a, b, c und d ganze Zahlen mit $a > 0$, $d > 0$, $b^2 - 4ac \neq 0$. Angenommen es gibt ganze Zahlen x_0, y_0 derart, dass $ax_0^2 + bx_0 + c = dy_0$. Dann existieren unendlich viele Paare (p, q) von Primzahlen mit $ap^2 + bp + c = dq$.

Es ist nun ein Leichtes zu zeigen:

2.2. Jede positive rationale Zahl $a/b \neq 1$ ($a > 0$, $b > 0$, $\mathrm{ggT}(a, b) = 1$) lässt sich auf unendlich viele Weisen in der Form $\frac{a}{b} = \frac{p^2-1}{q-1}$ schreiben, wobei p und q Primzahlen sind.

Beweis. Tatsächlich besitzt die Gleichung $bX^2 - (b - a) = aY$ die Lösung $(x_0, y_0) = (1, 1)$. Man beachte, dass wenn $b > 0$, $a > 0$, so

$4b(b-a) \neq 0$. Nach (2.1) gibt es unendlich viele Paare (p, q) von Primzahlen derart, dass $bp^2 - (b-a) = aq$, somit

$$\frac{a}{b} = \frac{p^2-1}{q-1}.$$

□

Anwendung von (2.2) mit der rationalen Zahl 2 ergibt:

2.3. Falls die Vermutung von BUNJAKOWSKI wahr ist, dann gibt es unendlich viele Pythagoreische Dreiecke (a, b, c) wobei a und c Primzahlen sind.

Beweis. Nach (2.2) gibt es unendlich viele Paare (p, q) von Primzahlen p, q derart, dass $2 = \frac{p^2-1}{q-1}$. Damit $p^2 = 2q-1$. Demzufolge $p^2+(q-1)^2 = q^2$, also ist $(p, q-1, q)$ ein Pythagoreisches Dreieck. □

Natürlich besteht die Schwierigkeit darin, die Vermutung von BUNJAKOWSKI zu beweisen. Für die Konsequenzen aus dieser Vermutung siehe auch mein Buch von 1996.

Ich wende mich nun Fermats letztem Satz zu. Für $n > 2$ bewies WILES im Jahr 1995, dass wenn $a^n + b^n = c^n$, dann $abc = 0$. Dies war die lang ersehnte Lösung von Fermats Problem. Von den zahllosen Teilresultaten, die vor dem kompletten Beweis durch WILES erzielt worden waren, möchte ich nur zwei erwähnen, die in den Zusammenhang passen.

Man sagte traditionellerweise, dass *der erste Fall von Fermats letztem Satz für den Primzahlexponenten p wahr ist*, wenn es keine ganzen Zahlen a, b und c (keine Vielfachen von p) derart gibt, dass $a^p+b^p = c^p$.

Im Jahr 1909 bewies WIEFERICH

2.4. Falls p eine ungerade Primzahl ist mit

$$2^{p-1} \not\equiv 1 \pmod{p^2}, \tag{9.9}$$

dann ist der erste Fall von Fermats letztem Satz für p wahr.

Wie in meinem Buch *13 Lectures on Fermat's Last Theorem* (1979, zweite Ausgabe 1995) erwähnt, trifft der erste Fall von Fermats letztem Satz für p zu, wenn es eine Primzahl $l \leq 89$ derart gibt, dass

$$l^{p-1} \not\equiv 1 \pmod{p^2} \tag{9.10}$$

(siehe insbesondere Granville (1988)).

Im Jahr 1985 bewiesen ADLEMAN, HEATH-BROWN und FOUVRY:

2.5. Es gibt unendlich viele prime Exponenten p, für die der erste Fall von Fermats letztem Satz zutrifft.

Die Methode des Beweises ließ allerdings keine Möglichkeit der expliziten Bestimmung irgendeines dieser Primzahlexponenten p zu.

B Varianten von Fermats Problem

Es ist einfach, Varianten von Fermats Problem zu formulieren.

Das verdrehte Fermat-Problem

Seien ganze Zahlen A, B, $C > 0$, $\mathrm{ggT}(A, B, C) = 1$ gegeben; sei $n \geq 3$. Das Problem ist es, alle ganzzahligen Lösungen der Gleichung

$$AX^n + BY^n = CZ^n \tag{9.11}$$

zu bestimmen. Für $n > 3$ hat die Kurve mit der obigen Gleichung ein Geschlecht größer als 1, so dass es nach dem mächtigen Satz von Faltings (1983) (Beweis von Mordells Vermutung) nur endlich viele Lösungen, d.h. Tripel (x, y, z) paarweise teilerfremder ganzer Zahlen gibt, die die gegebenen Gleichungen erfüllen. Oftmals haben derartige Gleichungen leicht zu findende und endlich viele triviale Lösungen.

Für jedes $N > 1$ bezeichne $S(N)$ die Menge aller Exponenten $n \leq N$, für die die Gleichung (9.11) nur die Triviallösungen besitzt.

Es wurde gezeigt (siehe Granville (1985b), Heath-Brown (1985)), dass:

2.6.

$$\lim_{N\to\infty} \frac{\#S(N)}{N} = 1.$$

In Worten: Für „fast alle“ Exponenten n haben die verdrehten Fermat-Gleichungen (für jedes Tripel (A, B, C)) nur triviale Lösungen.

Gleichwohl gibt es zur Zeit kein Kriterium das verrät, ob die verdrehte Fermat-Gleichung für beliebige A, B, C und n nur triviale Lösungen besitzt. Es gibt auch keinen Satz, der eine obere Schranke für die Größe der ganzen Zahlen x, y, z angibt, die Lösungen für die verdrehte Fermat-Gleichung sein könnten.

Hausaufgaben

In einem Artikel von 1999, den ich mit *Homework* betitelte (und der meine Kollegen dazu bringen sollte, hart zu arbeiten, jetzt wo ich im Ruhestand bin), stellte ich folgende Vermutung auf:

2.7. Sei $d \geq 1$. Dann gibt es eine natürliche Zahl $n_0(d)$ derart, dass wenn K irgendein Zahlkörper vom Grad höchstens gleich d ist und wenn gilt $n \geq n_0(d)$, dann hat die Gleichung $X^n + Y^n = Z^n$ höchstens die trivialen Lösungen in K.

An dieser Stelle bedeutet eine triviale Lösung in K irgendein Tripel (x, y, z) mit x, y, $z \in K$ und $xyz = 0$, sowie wenn K eine primitive sechste Einheitswurzel besitzt, jedes Tripel $(a, a\zeta^2, a\zeta)$ oder Permutationen davon, wobei a irgendein Element aus K ungleich Null ist. (Im Falle, dass ein solches Tripel eine Lösung ist, so $n \equiv \pm 1 \pmod 6$.)

Für $d = 1$ und wenn man $n_0(1) = 3$ wählt, ist obige Vermutung nichts Anderes als Fermats letzter Satz, der ja inzwischen bewiesen ist. Man vermutet auch, dass $n_0(2) = 5$. In diesem Zusammenhang möchte ich anmerken: Es gibt unendlich viele quadratische Zahlkörper $\mathbb{Q}(\sqrt{D})$ (D kein Quadrat) derart, dass $X^3 + Y^3 = Z^3$ nichttriviale Lösungen in $\mathbb{Q}(\sqrt{D})$ besitzt.

Die biquadratische Gleichung $X^4 + Y^4 = Z^4$ besitzt genau dann nichttriviale Lösungen in $\mathbb{Q}(\sqrt{D})$, wenn $D = -7$; mehr über diese Resultate finden sich in Ribenboim (1979). Für $p = 5$, 7, 11 hat die Gleichung $X^p + Y^p = Z^p$ nur triviale Lösungen in jedem quadratischen Zahlkörper (siehe Gross und Röhrlich (1978)). Es ist nichts weiter bekannt, wenn $p > 11$.

Hier ein anderes, aber verwandtes Problem:

Sei $n \geq 3$. Wie groß kann d sein, so dass es nur endlich viele Körper K mit einem Grad von höchstens d derart gibt, dass $X^n + Y^n = Z^n$ nur eine nichttriviale Lösung in K besitzt?

C Die Vermutung von Euler

Euler bewies, dass ein Kubus (verschieden von Null) keine Summe zweier Kuben (verschieden von Null) sein kann.

Im Jahr 1769 vermutete Euler für jedes $k > 3$: *Eine von Null verschiedene kte Potenz kann keine Summe von $k - 1$ kten Potenzen ungleich Null sein.*

Allerdings gaben LANDER und PARKIN im Jahr 1966 für $k = 5$ ein Gegenbeispiel an:

$$144^5 = 27^5 + 84^5 + 110^5 + 133^5.$$

Dieses war durch Computersuche gefunden worden und ist, soweit ich weiß, das einzige Beispiel für 5te Potenzen.

Im Jahr 1988 gab ELKIES eine parametrisierte unendliche Familie von Tripeln teilerfremder 4ter Potenzen an, deren Summe eine 4te Potenz ergibt. Das kleinste Beispiel war

$$20615673^4 = 2682440^4 + 15365639^4 + 18796760^4.$$

Diese Beispiele wurden durch die arithmetische Theorie elliptischer Kurven gewonnen.

Es ist denkbar, dass es für jedes $k > 5$ Gegenbeispiele zu Eulers Vermutung gibt.

Ich möchte gerne ein Problem formulieren. Sei $k \geq 3$ und definiere $v(k)$ als das Minimum der ganzen Zahlen $m > 1$ derart, dass es eine $k$te Potenz gibt, die die Summe von m natürlichen Zahlen ist, die $k$te Potenzen oder 1 sind. Nach Fermats letztem Satz gilt $v(k) > 2$. Das Problem ist die Bestimmung von $v(k)$. Da $3^3+4^3+5^3 = 6^3$ ist $v(3) = 3$.

Aus ELKIES' Beispiel folgt $v(4) = 3$. Nach LANDER und PARKINs Beispiel ist $v(5) \leq 4$. Es ist nicht bekannt, ob es eine 5te Potenz gibt, die die Summe dreier 5ter Potenzen ist.

Offensichtlich gilt $v(k) \leq 2^k$, da 2^k Summe von 2^k ganzen Zahlen alle gleich 1 ist. Es gibt keinerlei experimentelle Ergebnisse, die auch nur irgendeine Vermutung über $v(k)$ unterstützen würden. Gleichbedeutend ist nichts über die Existenz von rationalen Punkten in Hyperebenen $\sum_{i=1}^{n} x_i^k = 1$ bekannt. Dies ist ein weiteres Beispiel für die Wahl der Überschrift dieses Kapitels.

D Die Gleichung $AX^l + BY^m = CZ^n$

Seien A, B, C teilerfremde ganze Zahlen ungleich Null und seien l, m, $n \geq 2$. Je nach diesen Exponenten zeigt die Gleichung

$$AX^l + BY^m = CZ^n \tag{9.12}$$

ein sehr unterschiedliches Verhalten. Es gibt drei Möglichkeiten:

$$\frac{1}{l} + \frac{1}{m} + \frac{1}{n} \quad \begin{cases} < 1 & hyperbolischer Fall, \\ = 1 & Euklidischer Fall, \\ > 1 & spherischer Fall. \end{cases}$$

Der hyperbolische Fall

Dieser Fall wurde von Darmon und Granville im Jahr 1995 untersucht. Unter Verwendung von Faltings Satz zeigten sie

2.8. Wenn $\frac{1}{l}+\frac{1}{m}+\frac{1}{n}<1$, dann besitzt die Gleichung (9.12) nur endlich viele Lösungen in teilerfremden ganzen Zahlen (x,y,z) ungleich Null.

Der Fall $A=B=C=1$ war Objekt genauerer Untersuchungen. Es sind nur zehn solcher Lösungen bekannt (im hyperbolischen Fall):

$$\begin{aligned}
1^l+2^3&=3^2,\\
2^5+7^2&=3^4,\\
7^3+13^2&=2^9,\\
2^7+17^3&=71^2,\\
3^5+11^4&=122^2,\\
17^7+76271^3&=21063928^2,\\
1414^3+2213459^2&=65^7,\\
9262^3+15312283^2&=113^7,\\
43^8+96222^3&=30042907^2,\\
33^8+1549034^2&=15613^3.
\end{aligned}$$

Diese Relationen tauchen im Artikel von Beukers (1988) auf. Es könnte einem auffallen, dass in jedem Fall einer der Exponenten gleich 2 ist. Muss dies immer so sein?

Der Satz (2.8) sagt nicht aus, wann die Gleichung nur triviale Lösungen besitzt. Diesbezüglich werde ich einen Satz zur Dichte angeben.

Sei $k\geq 1$ und S eine Menge von k-Tupeln natürlicher Zahlen. Für jedes $N\geq 1$ sei

$$S(N)=\{(a_1,\ldots,a_k)\in S\mid 1\leq a_1,\ldots,a_k\leq N\}.$$

Somit hat $S(N)$ höchstens N^k Elemente.

Die Zahl

$$\underline{\delta}(S)=\liminf\frac{\#S(N)}{N^k} \tag{9.13}$$

ist die *untere asymptotische Dichte* von S; die Zahl

$$\bar{\delta}(S)=\limsup\frac{\#S(N)}{N^k} \tag{9.14}$$

ist die *obere asymptotische Dichte* von S. Wenn die obere und die untere asymptotische Dichte gleich sind, werden sie einfach mit $\delta(S)$ bezeichnet und man nennt diese Zahl die *asymptotische Dichte* von S.

Sei $S = \{(l, m, n) \mid 2 \leq l, m, n$ und die Gleichung (9.12) hat nur triviale Lösungen$\}$. Zusammen mit POWELL habe ich 1985 bewiesen:

$$\underline{\delta}(S) = \liminf \frac{\#S(N)}{N^3} > 1 - \frac{8}{7} \times \frac{27}{26} \times \frac{1}{\zeta(3)} > 0$$

wobei $\zeta(3) = \sum_{n=1}^{\infty} \frac{1}{n^3}$ (Wert der Zetafunktion an der Stelle 3).

Dies ist natürlich ein schwaches Resultat, obwohl der Beweis im Wesentlichen den starken Satz von Faltings verwendet.

Im Jahr 1993 bewies ich weitere Sätze zur Dichte. Zur Klarheit werde ich speziell die Gleichung

$$X^l + Y^m = Z^n \tag{9.15}$$

mit l, m, $n \geq 2$ betrachten.

Für jedes $n \geq 2$ sei $D_n = \{(l, m) \mid$ Gleichung (9.15) hat nur triviale Lösungen$\}$. Dann (siehe Ribenboim (1993)):

2.9. (a) Die Menge $\{n \mid D_n \neq \varnothing\}$ hat Dichte 1.
(b) Die Menge $\{n \mid \delta(D_n) = 0\}$ hat Dichte 0.

In Worten: Für fast alle n gibt es eine $n$te Potenz, die gleich der Summe zweier Potenzen ist, und für fast alle n gibt es einen positiven Anteil von (l, m) derart, dass eine $l$te Potenz plus eine $m$te Potenz keine $n$te Potenz ist. Diese Aussagen zeigen, wie wenig bekannt ist.

Weitere Arbeiten mit der von WILES entwickelten Methode führten zu den folgenden Ergebnissen für sehr spezielle Gleichungen (RIBET 19?? und Darmon und Merel (1997)).

2.10. (a) Wenn $n \geq 3$, dann besitzt $X^n + Y^n = 2Z^n$ nur triviale Lösungen (in ganzen Zahlen mit Absolutwert von höchstens 1).
(b) Wenn n ungerade ist und $n \geq 3$, dann hat $X^n + Y^n = Z^2$ nur triviale Lösungen.
(c) Wenn $n \geq 3$, dann hat die Gleichung $X^n + Y^n = Z^3$ nur triviale Lösungen.

Die folgende Aussage wurden unter Verwendung des bedeutenden und heute berühmten Satzes von WILES bewiesen (1995, siehe auch Taylor (1995)):

Die Vermutung von Shimura und Taniyama ist für semi-stabile elliptische Kurven über $\mathbb{Q}$ richtig, d.h. jede solche Kurve ist eine modulare elliptische Kurve.

Die Suche nach einem Beweis der Vermutung von Shimura und Taniyama wurde fortgeführt und schließlich bewiesen Breuil, Conrad, Diamond und Taylor im Jahre 1999, dass jede über $\mathbb{Q}$ definierte elliptische Kurve (semi-stabil oder nicht) modular ist.

Der euklidische Fall

Wenn

$$\frac{1}{l}+\frac{1}{m}+\frac{1}{n}=1,$$

dann gibt es bis auf Permutation nur die folgenden Möglichkeiten:

$$(l,m,n)\in\{(2,3,6),(2,4,4),(3,3,3)\}.$$

In diesem Fall lässt sich die Gleichung (9.12) mit der Theorie der elliptischen Kurven behandeln, was an dieser Stelle aber nicht erfolgen wird.

Der spherische Fall

Wenn

$$\frac{1}{l}+\frac{1}{m}+\frac{1}{n}>1,$$

dann ist bis auf Permutation

$$(l,m,n)\in\{(2,2,n)\mid n\geq 2\}\cup\{(2,3,3),(2,3,4),(2,3,5)\}.$$

Im Jahr 1998 veröffentlichte Beukers einen Satz über Gleichung (9.12) im spherischen Fall. Zur Festlegung der Bezeichnungsweisen: die homogenen Polynome f, g, $h\in\mathbb{Z}[X,Y]$ liefern eine parametrische Familie von Lösungen von (9.12), wenn

$$Af^l+Bg^m=Ch^n.$$

Somit ist für alle Paare ganzer Zahlen (s,t),

$$Af(s,t)^l+Bg(s,t)^m=Ch(s,t)^n,$$

also sind $(f(s,t),g(s,t),h(s,t))$ Lösungen für alle s, t. Beukers bewies:

2.11. Die Menge der Lösungen von (9.12) besteht im spherischen Fall aus endlich vielen Familien parametrisierter Lösungen. Wenn die Gleichung eine nichttriviale Lösung besitzt, dann hat sie gleich unendlich viele Lösungen.

Das Resultat der pythagoreischen Gleichung war bereits beschrieben worden und ist seit langer Zeit bekannt.

ZAGIER bestimmte die Lösungen für die Gleichungen $X^3+Y^3 = Z^2$, $X^4 + Y^3 = Z^2$ und $X^4 + Y^2 = Z^3$, diese sind in BEUKERS' Artikel enthalten.

Die Gleichung $X^3 + Y^3 = Z^2$ besitzt die folgenden drei Familien parametrisierter Lösungen:

$$\begin{cases} x = s^4 + 6s^2t^2 - 3t^4, \\ y = -s^4 + 6s^2t^2 + 3t^4, \\ z = 6st(s^4 + 3t^4); \end{cases}$$

$$\begin{cases} x = (1/4)(s^4 + 6s^2t^2 - 3t^4), \\ y = (1/4)(-s^4 + 6s^2t^2 + 3t^4), \\ z = (3/4)st(s^4 + 3t^4); \end{cases}$$

$$\begin{cases} x = s^4 + 8st^3, \\ y = -4s^3t + 4t^4, \\ z = s^6 - 20s^3t^3 - 8t^6. \end{cases}$$

Die Gleichung $X^4 + Y^3 = Z^2$ besitzt die folgenden sechs Familien parametrisierter Lösungen:

$$\begin{cases} x = (s^2 - 3t^2)(s^4 + 18s^2t^2 + 9t^4), \\ y = -(s^4 + 2s^2t^2 + 9t^4)(s^4 - 30s^2t^2 + 9t^4), \\ z = 4st(s^2 + 3t^2)(s^4 - 6s^2t^2 + 81t^4)(3s^4 - 2s^2t^2 + 3t^4); \end{cases}$$

$$\begin{cases} x = 6st(s^4 + 12t^4), \\ y = s^8 - 168s^4t^4 + 144t^8, \\ z = (s^4 - 12t^4)(s^8 + 408s^4t^4 + 144t^8); \end{cases}$$

$$\begin{cases} x = 6st(3s^4 + 4t^4), \\ y = 9s^8 - 168s^4t^4 + 16t^8, \\ z = (3s^4 - 4t^4)(9s^8 + 408s^4t^4 + 16t^8); \end{cases}$$

$$\begin{cases} x = s^6 + 40s^3t^3 - 32t^6, \\ y = -8st(s^3 - 16t^3)(s^3 + 2t^3), \\ z = s^{12} - 176s^9t^3 - 5632s^3t^9 - 1024t^{12}; \end{cases}$$

$$\begin{cases} x = -5s^6 + 6s^5t + 15s^4t^2 - 60s^3t^3 + 45s^2t^4 - 18st^5 + 9t^6, \\ y = 6s^8 - 56ts^7 + 112t^2s^6 - 168t^3s^5 + 252t^4s^4 - 168t^5s^3 + 72t^7s - 18t^8, \\ z = -29s^{12} + 156ts^{11} - 726t^2s^{10} + 2420t^3s^9 - 4059t^4s^8 + 3960t^5s^7 \\ \quad -2772t^6s^6 + 2376t^7s^5 - 3267t^8s^4 + 3564t^9s^3 - 1782t^{10}s^2 \\ \quad +324t^{11}s + 27t^{12}; \end{cases}$$

$$\begin{cases} x = s^6 + 6s^5t - 15s^4t^2 + 20s^3t^3 + 15s^2t^4 + 30st^5 - 17t^6, \\ y = 2s^8 - 8ts^7 - 56t^3s^5 - 28t^4s^4 + 168t^5s^3 - 112t^6s^2 + 88t^7s + 42t^8, \\ z = -3s^{12} + 12ts^{11} - 66t^2s^{10} - 44t^3s^9 + 99t^4s^8 + 792t^5s^7 \\ \quad -924t^6s^6 + 2376t^7s^5 - 1485t^8s^4 - 1188t^9s^3 + 2046t^{10}s^2 - 156t^{11}s \\ \quad +397t^{12}; \end{cases}$$

Die Gleichung $X^4 + Y^2 = Z^3$ besitzt die folgenden vier Familien parametrisierter Lösungen:

$$\begin{cases} x = (s^2 + 3t^2)(s^4 - 18s^2t^2 + 9t^4), \\ y = 4st(s^2 - 3t^2)(s^4 + 6s^2t^2 + 81t^4)(3s^4 + 2s^2t^2 + 3t^4), \\ z = (s^4 - 2s^2t^2 + 9t^4)(s^4 + 30s^2t^2 + 9t^4); \end{cases}$$

$$\begin{cases} x = 6st(s^4 - 12t^4), \\ y = (s^4 + 12t^4)(s^8 - 408s^4t^4 + 144t^8), \\ z = s^8 + 168s^4t^4 + 144t^8; \end{cases}$$

$$\begin{cases} x = 6st(3s^4 - 4t^4), \\ y = (3s^4 + 4t^4)(9s^8 - 408s^4t^4 + 16t^8), \\ z = 9s^8 + 168s^4t^4 + 16t^8; \end{cases}$$

$$\begin{cases} x = (3/2)st(s^4 - 3t^4), \\ y = (1/8)(s^4 + 3t^4)(s^8 - 102s^4t^4 + 9t^8), \\ z = (1/4)(s^8 + 42s^4t^4 + 9t^8). \end{cases}$$

E Potenzen als Werte von Polynomen

Die Frage die nun behandelt wird, ist die folgende: Wie oft nimmt ein Polynom $f \in \mathbb{Z}[X]$ Werte an, die Potenzen sind? Die Frage ist natürlich nur dann sinnvoll, wenn f selbst keine Potenz eines anderen Polynoms ist.

Der folgende bedeutende und nützliche Satz wurde von Schinzel und Tijdeman im Jahr 1976 bewiesen und gilt für Polynome mit rationalen Koeffizienten:

2.12. Sei $f \in \mathbb{Q}[X]$ und angenommen, dass f mindestens drei einfache Nullstellen besitzt (bzw. zwei einfache Nullstellen). Dann gibt es eine effektiv berechenbare Konstante $C > 0$ (die von f abhängt) derart, dass wenn x, y, h ganze Zahlen mit $y \geq 2$, $h \geq 2$ (bzw. $h \geq 3$) sind und $f(x) = y^h$, dann $|x|$, y, $h \leq C$.

Also nimmt f nur endlich viele Potenzwerte an. Der Beweise dieses Ergebnisses erforderte die Theorie der Linearformen von Logarithmen wie von BAKER entwickelt.

3 Exponentielle Kongruenzen

A Die Wieferich-Kongruenz

Motiviert durch ein Kriterium für den ersten Fall von Fermats letztem Satz werde ich nun die folgende *Wieferich-Kongruenz* betrachten:

$$a^{p-1} \equiv 1 \pmod{p^2} \tag{9.16}$$

wobei p eine ungerade Primzahl ist und $2 \leq a$, $p \nmid a$.

Nach dem kleinen Satz von Fermat ist $q_p(a) = \frac{a^{p-1}-1}{p}$ eine ganze Zahl, die man den *Fermat-Quotienten von p zur Basis a* nennt. Somit gilt (9.16) genau dann, wenn

$$q_p(a) \equiv 0 \pmod{p}. \tag{9.17}$$

Der Fermat-Quotient erfüllt die folgende, erstmals von EISENSTEIN beobachtete Eigenschaft:

$$q_p(ab) \equiv q_p(a) + q_p(b) \pmod{p}. \tag{9.18}$$

Wie Berechnungen zeigen, ist $q_p(a) \equiv 0 \pmod{p}$ nur selten erfüllt. So gilt für $a = 2$ und $p < 2{,}5 \times 10^{15}$, dass wenn $q_p(2) \equiv 0 \pmod{p}$, dann $p = 1093$ oder 3511.

Ich werde allgemeiner auch die Kongruenzen

$$a^{p-1} \equiv 1 \pmod{p^k}, \tag{9.19}$$

betrachten, wobei $k \geq 1$, p eine ungerade Primzahl ist, $a \geq 2$ und $p \nmid a$.

Sei $l \geq 2$, l prim, $k \geq 1$ und sei

$$W_l^{(k)} = \{p \text{ prim und ungerade} \mid l^{p-1} \equiv 1 \pmod{p^k}\},$$
$$W_l^{(k)'} = \{p \text{ prim und ungerade} \mid l^{p-1} \not\equiv 1 \pmod{p^k}\}.$$

Somit ist $W_l^{(1)}$ die Menge aller Primzahlen $p \neq l$. Offensichtlich gilt

$$W_l^{(1)} \supseteq W_l^{(2)} \supseteq \cdots \supseteq W_l^{(k)} \supseteq \cdots .$$

Heuristisch gesehen ist $W_l^{(2)}$ eine unendliche Menge, während $W_l^{(k)}$ für alle $k \geq 3$ endlich ist. Dies kann man auf die folgende Weise einsehen: Wenn man nicht weiß, was $q_p(l)$-modulo p ist und voraussetzt, dass der Fermat-Quotient jeden Wert mit derselben Wahrscheinlichkeit annimmt, dann ergibt sich wenn x irgendeine positive reelle Zahl ist, dass

$$\#\{p \leq x \mid p \in W_l^{(2)}\} = \sum_{p \leq x} \frac{1}{p} = \log\log x + O(1);$$

somit sollte $W_l^{(2)}$ unendlich sein. Für $k \geq 3$,

$$\#\{p \leq x \mid p \in W_l^{(k)}\} = \sum_{p \leq x,\, p \nmid a} \frac{1}{p^{k-1}} < \zeta(k-1) < \infty.$$

Obwohl obige Argumente heuristisch akzeptabel sind, gibt es keine vollständige Begründung für sie. Für $k \geq 2$ ist nicht bekannt, ob $W_l^{(k)}$ oder $W_l^{(k)'}$ endlich oder unendlich sind.

Ich möchte das folgende interessante Ergebnis von Powell (1982) erwähnen:

3.1. Sei l irgendeine Primzahl. Dann ist die Menge

$$S = \bigcup_{k \text{ ungerade}} \left(W_l^{(k)} \setminus W_l^{(k+1)}\right)$$

unendlich.

Beweis. Die Primzahl q gehört genau dann zu S, wenn der q-adische Wert $v_q(l^{q-1} - 1)$ ungerade ist. Angenommen $\{q_1, \ldots, q_n\}$ (mit $n \geq 0$) sei die Menge aller ungeraden Primzahlen in S. Sei $s = 1$ wenn $n = 0$ oder $s = \prod_{i=1}^{n} (q_i - 1)^2$ für $n \geq 1$.

Da $q_i - 1$ Teiler von $4s$ ist, teilt q_i die Zahl $l^{4s} - 1$ (für jedes $i = 1, \ldots, n$). Es wird gezeigt werden, dass $l^{4s} + 1$ entweder ein Quadrat oder das Doppelte eines Quadrats ist.

Sei p irgendeine ungerade Primzahl, die $l^{4s} + 1$ teilt, also $p \mid l^{8s} - 1$ und $p \nmid l^{4s} - 1$. Demzufolge ist $p \neq q_i$ für jedes $i = 1, \ldots, n$. Sei r die Ordnung von l modulo p. Also $p - 1 = rk$ (woraus folgt, dass $p \nmid r$, $p \nmid k$), sowie $8s = rhp^f$ mit $f \geq 0$, $p \nmid h$. Da s ein Quadrat ist, muss f gerade sein.

Man beachte, dass

$$\begin{aligned} \frac{l^{p-1} - 1}{l^r - 1} &= l^{r(k-1)} + l^{r(k-2)} + \cdots + l^r + 1 \\ &\equiv k \pmod{p}, \end{aligned}$$

und in gleicher Weise

$$\frac{l^{rh} - 1}{l^r - 1} \equiv h \pmod{p}.$$

Also $v_p(l^{p-1} - 1) = v_p(l^r - 1) = v_p(l^{rh} - 1)$. Da $p \neq q_1, \ldots q_n$ gilt, ist $d = v_p(l^{p-1} - 1)$ gerade. Nun ist auch $v_p(l^{8s} - 1) = d + f$ gerade, wobei $8s = rhf$. Da p ein beliebiger Primteiler von $l^{4s} + 1$ ist folgt, dass $l^{4s} + 1 = c^2$ oder $2c^2$ (für ein $c \geq 1$). Aber wie wohlbekannt ist, hatte Fermat gezeigt, dass die Gleichungen $X^4 + Y^4 = Z^2$ oder $X^4 + Y^4 = 2Z^2$ nur triviale Lösungen (x, y, z) mit $|x|, |y|, |z| \leq 1$ besitzen. Dies ist ein Widerspruch, was beweist, dass die Menge S tatsächlich unendlich ist. □

Im Jahr 1985 zeigte Granville:

3.2. Sei $l \geq 2$ eine Primzahl. Wenn $W_l^{(3)}$ endlich ist, dann gibt es unendlich viele Primzahlen p derart, dass $p \equiv 1 \pmod 4$ und $l^{p-1} \not\equiv 1 \pmod{p^2}$. Insbesondere gilt, dass wenn $W_l^{(3)}$ endlich ist, dann ist $W_l^{(2)'}$ unendlich.

Aus Powells Resultat folgt, dass $W_l^{(2)'}$ unendlich ist; hier ist zudem sichergestellt, dass $W_l^{(2)'}$ unendlich viele Primzahlen $p \equiv 1 \pmod 4$ enthält.

Es ist auch interessant, einmal die folgende Frage zu betrachten. Gegeben sei eine ungerade Primzahl p. Bestimme die Anzahl der Elemente der Menge

$$B(p) = \{a \mid 2 \le a < p \text{ derart, dass } a^{p-1} \equiv 1 \pmod{p^2}\}$$

oder der Teilmenge

$$B'(p) = \{q \text{ prim} \mid 2 \le q < p, \text{ derart, dass } q^{p-1} \equiv 1 \pmod{p^2}\}.$$

Im Jahr 1966 zeigte KRUYSWIJK:

3.3. Es gibt eine Konstante $C > 0$ derart, dass für jedes p

$$\#B(p) < p^{\frac{1}{2} + \frac{C}{\log\log p}}.$$

Das Ergebnis für $B'(p)$ ist besser. GRANVILLE zeigte 1987:

3.4. Sei $u \ge 1$ eine ganze Zahl und p eine Primzahl derart, dass $p > u^{2u}$. Dann gilt

$$\#\{q \text{ prim} \mid 2 \le q < p^{\frac{1}{u}} \text{ und } q^{p-1} \equiv 1 \pmod{p^2}\} < up^{1/2u}.$$

Insbesondere ist für jede Primzahl p

$$\#\{q \text{ prime} \mid 2 \le q < p^{1/2} \text{ und } q^{p-1} \equiv 1 \pmod{p^2}\} < p^{1/2}.$$

B Primitive Primfaktoren

Den folgenden Satz bewies BANG im Jahr 1886 (für $a = 2$), die Erweiterung stammt von ZSIGMONDY aus dem Jahr 1892:

3.5. Sei $a \ge 2$. Für jedes $n \ge 2$ (mit den unten angegebenen Ausnahmen) gibt es eine Primzahl p, die ein primitiver Primfaktor von $a^n \mp 1$ ist, d.h. p teilt $a^n \mp 1$, aber p ist kein Teiler von $a^m \mp 1$ für alle $m < n$. Die einzigen Ausnahmen davon sind:

(i) $2^6 - 1$, $2^3 + 1$
(ii) $(2^k - 1)^2 - 1$

Ein detaillierter Beweis findet sich zum Beispiel in meinem Buch *Fermat's Last Theorem for Amateurs* (1999).

Sei $a^n \mp 1 = AB$ mit $\text{ggT}(A, B) = 1$ und es gelte $p \mid A$ genau dann, wenn p ein primitiver Primfaktor ist. Dann nennt man A den *primitiven Teil* von $a^n \mp 1$, ich werde die Bezeichnung $A = (a^n \mp 1)^*$ verwenden.

Obiger Satz lässt sich sowohl auf die Mersenne-Zahlen $M_q = 2^q - 1$ (q prim) als auch auf die Fermat-Zahlen $F_n = 2^{2^n} + 1$ anwenden. Es macht also Sinn, ihre primitiven Teile ${M_q}^*$ bzw. ${F_n}^*$ zu betrachten.

Für jedes prime $L \geq 2$ sei $\mathcal{N}_L = \{p \text{ prim} \mid \text{es gibt } c \geq 1,\ p \nmid c \text{ derart, dass } pc = a \pm b, \text{ wobei jeder Primfaktor von } ab \text{ höchstens gleich } L \text{ ist}\}$. Es ist nicht bekannt, ob die Mengen $\mathcal{N}_L$ endlich oder unendlich groß sind.

Um die Situation weiter zu analysieren, werde ich andere Primzahlmengen einführen. Für Primzahlen $k \geq 1$ und l sei

$$\mathcal{N}_l^{(k)} = \{p \text{ prim} \mid \text{es gibt } s \geq 1 \text{ derart, dass } p^k \text{ Teiler von } l^s + l \text{ ist, aber } p^{k+1} \text{ teilt nicht } l^s + l\}.$$

Zum Beispiel ist $\mathcal{N}_l^{(1)} \subseteq \mathcal{N}_L$ für $l \leq L$. Um also zu zeigen, dass $\mathcal{N}_L$ unendlich ist genügt es, eine Primzahl $l \leq L$ derart zu finden, dass $\mathcal{N}_l^{(1)}$ unendlich ist. Mit anderen Worten, betrachte die Folge ganzer Zahlen $\{l+1, l^2+1, l^3+1, \dots\}$. Nach (3.5) gibt es unendlich viele Primzahlen p, die irgendeine Zahl der Folge teilt, da (mit den einzigen Ausnahmen $l = 2$, $s = 3$) jede Zahl $l^s + 1$ einen primitiven Primfaktor besitzt. Gibt es noch unendlich viele solcher Primzahlen, die zu $\mathcal{N}_l^{(1)}$ gehören?

Dies wäre wahr, wenn es unendlich viele primitive Primfaktoren gäbe, deren Quadrate keine Faktoren sind. Eine schwierig zu entscheidende Frage, deren Antwort aber wiederum wichtige Konsequenzen nach sich ziehen würde.

Ein Ergebnis von Puccioni aus dem Jahre 1968 wurde wie folgt verbessert (siehe meinen eigenen Artikel (1998)):

3.6. Für jedes $k \geq 1$ und prime $l \geq 2$:

1. $\mathcal{N}_l^{(k)} \cap \mathcal{W}_l^{(k+1)} = \begin{cases} \varnothing & \text{wenn } l \not\equiv 1 \pmod{2^{k+1}}, \\ \{2\} & \text{wenn } l \equiv 1 \pmod{2^{k+1}}, \end{cases}$
2. $\mathcal{N}_l^{(k)} \cup \mathcal{W}_l^{(k+2)}$ ist eine unendliche Menge.

Beweis. (1) Es wird zunächst durch Induktion über k gezeigt, dass $\mathcal{N}_l^{(k)} \cap \mathcal{W}_l^{(k+1)} \subseteq \{2\}$.

Wenn $k = 1$ und p eine ungerade Primzahl mit der Eigenschaft ist, dass $p \in \mathcal{N}_l^{(1)} \cap \mathcal{W}_l^{(2)}$, dann $l^{p-1} \equiv 1 \pmod{p^2}$ und es gibt $s \geq 1$, $c \geq 1$ derart, dass $p \nmid c$, $l^s + 1 = pc$; da $l^p \equiv 1 \pmod{p^2}$, folgt $l^s \equiv l^{ps} = (pc-1)^p \equiv -1 \pmod{p^2}$, also $p^2 \mid l^s + 1$, was nicht sein kann.

Angenommen, die Aussage sei für $k \geq 1$ richtig. Man beachte zunächst, dass $\mathcal{N}_l^{(k)} \cap \mathcal{W}_l^{(k+2)} \subseteq \mathcal{N}_l^{(k)} \cap \mathcal{W}_l^{(k+1)} \subseteq \{2\}$. Es genügt zu zeigen, dass $(\mathcal{N}_l^{(k+1)} \setminus \mathcal{N}_l^{(k)}) \cap \mathcal{W}_l^{(k+1)} = \varnothing$. Sei p eine Primzahl dieser

Menge, also $l^{p-1} \equiv 1 \pmod{p^{k+2}}$ und es gibt $s \geq 1$, $c \geq 1$ derart, dass $p \nmid c$, $l^s + 1 = p^{k+1}c$; wegen $l^p \equiv l \pmod{p^{k+2}}$ ist $l^s \equiv l^{ps} \equiv (p^{k+1}c - 1)^p \pmod{p^k + 2}$. Wenn $p \neq 2$, dann $l^s \equiv -1 \pmod{p^{k+2}}$, was nicht sein kann. Wenn $p = 2$, dann $l^s \equiv 1 \pmod{2^{k+2}}$ und $2^{k+1}c \equiv l^s + 1 \equiv 2 \pmod{2^{k+2}}$, daher $k + 1 = 1$ und $k = 0$, was wiederum unmöglich ist.

Dies zeigt, dass $\mathcal{N}_l^{(k)} \cap \mathcal{W}_l^{(k+1)} \subseteq \{2\}$.

Schließlich, falls $2 \in \mathcal{N}_l^{(k)} \cap \mathcal{W}_l^{(k+1)}$, dann $l \equiv 1 \pmod{2^{k+1}}$.

Umgekehrt, wenn $l \equiv 1 \pmod{2^{k+1}}$, dann $2 \in \mathcal{W}_l^{(k+1)}$ und $l + 1 \equiv 2 \pmod{2^{k+1}}$, also $s \in \mathcal{N}_l^{(1)} \subseteq \mathcal{N}_l^{(k)}$.

(2) Bei diesem Beweis wird (2.12) verwendet werden. Für das Polynom $f(X) = 2X^{k+1} - 1$ sei C die entsprechende effektiv berechenbare Konstante.

Wenn man $\mathcal{N}_l^{(k)} \cup \mathcal{W}_l^{(k+2)}$ als endlich voraussetzt, sei m eine Primzahl derart, dass $m > C$ und $m > \max\{p \mid p \in \mathcal{N}_l^{(k)} \cup \mathcal{W}_l^{(k+2)}\}$. Sei $P = \prod_{l \neq q \leq m} q$ (wobei jeder Faktor q prim ist). Daher, $\varphi(P) = \prod_{l \neq q \leq m}(q-1)$ und so ist $\varphi(P)$ gerade und größer als C.

Es ist klar, dass $l^{\varphi(P)} \equiv 1 \pmod{P}$. Zudem ist $q > m$, falls $q \neq 2$ und q Teiler von $l^{\varphi(P)} + 1$ ist—ansonsten $l \neq q \leq m$, also wird P von q geteilt, damit $l^{\varphi(P)} - 1$ und $q = 2$.

Es ist wohlbekannt und einfach zu zeigen, dass wenn $n \geq 2$ und l prim ist, dann kann $l^h + 1$ keine Potenz sein. Ein Beweis findet sich in meinem Buch *Catalan's Conjecture* (1994) auf Seite 201.

Erster Fall. Es gibt eine Primzahl q derart, dass q^{k+2} Teiler von $l^{\varphi(P)} + 1$ ist. Wenn $q = 2$, so ist l ungerade und $l^{\varphi(P)} \equiv -1 \pmod{8}$. Aber $l^2 \equiv 1 \pmod{8}$ und $l^{\varphi(P)} \equiv 1 \pmod{8}$, was nicht sein kann.

Also $q \neq 2$, $q > m$, und damit $q \nmid \varphi(P)$.

Sei g die Ordnung von l modulo q, somit wird $q - 1$ von g geteilt. Aber $q \mid l^{2\varphi(P)} - 1$, also $g \mid 2\varphi(P)$ und damit $2\varphi(P) = gh$, wobei q kein Teiler von h ist.

Da $l^{gh} - 1 = (l^g - 1)(l^{g(h-1)} + l^{g(h-2)} + \cdots + l^g + 1)$ von q^{k+2} geteilt wird und $l^g \equiv 1 \pmod{q}$ folgt, dass der zweite Faktor oben kongruent zu $h \not\equiv 0 \pmod{q}$ ist. Daher ist q^{k+2} Teiler von $l^g - 1$. Also $l^{q-1} \equiv 1 \pmod{q^{k+2}}$, d.h. $q \in \mathcal{W}_l^{(k+2)}$ und somit $q < m$, was ein Widerspruch ist.

Zweiter Fall. Wenn $l^{\varphi(P)} + 1$ von q geteilt wird, dann ist q^{k+2} kein Teiler von $l^{\varphi(P)} + 1$.

Da $l^{\varphi(P)} + 1$ keine $(k+1)$te Potenz ist, gibt es eine Primzahl q derart, dass $q \mid l^{\varphi(P)} + 1$, aber $q^{k+1} \nmid l^{\varphi(P)} + 1$. Demzufolge, $q \in \mathcal{N}_l^{(k)}$

und $q \leq m$. Dies impliziert, dass $q = 2$, und so $l^{\varphi(P)}+1 = 2^e t^{k+1}$, wobei $1 \leq e \leq k$ und t ungerade ist. Aber l ist ungerade und $\varphi(P)$ gerade, also $l^{\varphi(P)} \equiv 1 \pmod 4$. Damit $e = 1$, d.h. $l^{\varphi(P)} + 1 = 2t^{k+1}$.

Daher sind die ganzen Zahlen t, $l \neq 0$, $\varphi(P) \geq 1$ Lösungen der Gleichung $2X^{k+1} - 1 = Y^Z$. Daraus folgt $\varphi(P) \leq C$, was Unsinn ist.

□

Insbesondere ist $\mathcal{N}_l^{(1)} \cup \mathcal{W}_l^{(3)}$ eine unendliche Menge. Es reicht zu zeigen, dass $\mathcal{W}_l^{(3)}$ eine endliche Menge ist (für irgendeine Primzahl l), um zu schließen, dass $\mathcal{N}_l^{(1)}$ unendlich ist. Zum Beispiel ist für $l = 2$ keine ganze Zahl in $\mathcal{W}_l^{(3)}$ bekannt.

4 Traummathematik

Eines Tages werden die Mathematiker schlauer werden und in der Lage sein, viele Aussagen zu beweisen, die man heute nur vermuten kann. Im Moment ist es nur möglich zu träumen. Aber solche Träume kann man organisieren.

A Die Aussagen

Um meine Ignoranz ohne jeglichen Zweifel zu offenbaren, lassen Sie mich Binomialzahlen, Mersenne-Zahlen, Fermat-Zahlen, quadratvolle Zahlen, quadratfreie Zahlen, Zahlen mit einem quadratischen Faktor, Primzahlen und Wieferich-Kongruenzen diskutieren. Ist das nicht genug?

Keiner weiß, ob die unten aufgelisteten Aussagen wahr oder falsch sind.

Bezeichnungen

$$\begin{aligned} P &= \text{prim} \\ C &= \text{zerlegbar} \\ SF &= \text{quadratfrei} \\ S &= \text{mit einem quadratischen Faktor (verschieden von 1)} \\ W &= \text{quadratvoll} \\ \neg W &= \text{nicht quadratvoll} \end{aligned}$$

Ein Stern markiert den primitiven Teil.

Sei $\alpha \in \{P, C, SF, S, W, \neg W\}$ und $\epsilon \in \{\text{endlich}, \infty\}$. Sei

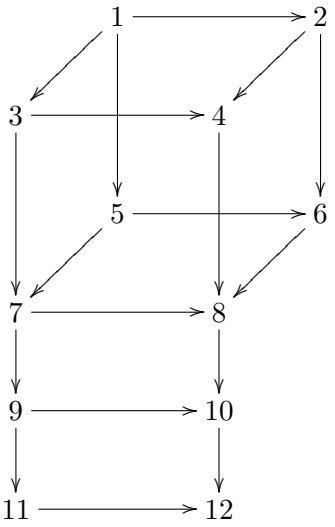
$$M_q = 2^q - 1 \text{ (für primes } q\text{): Mersenne-Zahl,}$$
$$F_n = 2^{2^n} + 1 \text{ (für } n \geq 0\text{): Fermat-Zahlen.}$$

B Aussagen

Ich werde als Erstes die Mersenne-Zahlen betrachten.

$$(M_{\alpha,\epsilon}) := \#\{q \mid M_q \text{ erfüllt } \alpha\} = \epsilon,$$
$$(M_{\alpha,\epsilon}{}^*) := \#\{q \mid M_q{}^* \text{ erfüllt } \alpha\} = \epsilon.$$

Es gibt zwischen den Aussagen viele offensichtliche Implikationen:



$$(1) = (M_{C,\,\text{endlich}}) \qquad (2) = (M_{P,\infty})$$
$$(3) = (M_{C,\,\text{endlich}}{}^*) \qquad (4) = (M_{P,\infty}{}^*)$$
$$(5) = (M_{S,\,\text{endlich}}) \qquad (6) = (M_{SF,\infty})$$
$$(7) = (M_{S,\,\text{endlich}}{}^*) \qquad (8) = (M_{SF,\infty}{}^*)$$
$$(9) = (M_{W,\,\text{endlich}}{}^*) \qquad (10) = (M_{\neg W,\infty}{}^*)$$
$$(11) = (M_{W,\,\text{endlich}}) \qquad (12) = (M_{\neg W,\infty})$$

Man könnte auch die Negationen dieser Aussagen betrachten, für diese gelten dann die umgekehrten Implikationen.

Man vermutet, dass $(M_{P,\infty})$ und $(M_{C,\infty})$ beide wahr sind. Es ist auch ein sehr tiefliegendes Problem zu entscheiden, ob (7), (9) oder sogar (11) wahr sind.

Ich werde nun zu den analogen Aussagen für Fermat-Zahlen kommen.

$$(F_{\alpha,\epsilon}) := \#\{n \mid F_n \text{ hat Eigenschaft } \alpha\} = \epsilon,$$
$$(F_{\alpha,\epsilon}{}^*) := \#\{n \mid F_n{}^* \text{ hat Eigenschaft } \alpha\} = \epsilon.$$

Dasselbe Diagramm offensichtlicher Implikationen gilt für die Fermat-Zahlen, man ersetze nur M durch F.

Es gibt keine Einigung darüber, ob $(F_{P,\infty})$ oder sogar $(F_{\neg W,\infty})$ wahr ist.

Die nächsten Aussagen betreffen Binomialzahlen $a^n \pm 1$ (wobei $a \geq 2$, $n \geq 1$).

Es ist einfach zu zeigen, dass wenn $a^n - 1$ eine Primzahl ist, so gilt $a = 2$ und n muss ebenfalls prim sein. Auch gilt für Primzahlen $a^n + 1$, dass $a = 2$ und n ist eine Zweierpotenz.

Betrachte die Aussagen

$$(B(a,\pm)_{\alpha,\epsilon}) := \#\{n \mid a^n \pm 1 \text{ hat Eigenschaft } \alpha\} = \epsilon,$$
$$(B(a,\pm)_{\alpha,\epsilon}{}^*) := \#\{n \mid (a^n \pm 1)^* \text{ hat Eigenschaft } \alpha\} = \epsilon.$$

Für $a = 2$, $(B(2,-)_{P,\epsilon}) = (M_{P,\epsilon})$ und $(B(2,-)_{C,\infty})$ ist wahr. Auch gilt $(B(2,+)_{P,\epsilon}) = (F_{P,\epsilon})$ und $(B(2,+)_{C,\infty})$ ist wahr. Dieselben offensichtlichen Implikationen des Diagramms (und der umgekehrten Implikationen) werden von den Eigenschaften der Folgen von Zahlen $a^n \pm 1$ erfüllt (bzw. ihren Negationen).

Ich stelle nun Aussagen zu Wieferich-Kongruenzen vor. Sei $a \geq 2$ und

$$(W(a)_\epsilon) := \#\{p \text{ prim} \mid a^{p-1} \equiv 1 \pmod{p^2}\} = \epsilon,$$
$$(\neg W(a)_\epsilon) := \#\{p \text{ prim} \mid a^{p-1} \not\equiv 1 \pmod{p^2}\} = \epsilon.$$

Offensichtlich gilt $(W(a)_{\text{endlich}}) \to (\neg W(a)_\infty)$ und $(\neg W(a)_{\text{endlich}}) \to (W(a)_\infty)$.

In Abschnitt 1 wies ich auf Erdös' Vermutung über quadratvolle Zahlen hin:

(E) Es gibt keine drei aufeinanderfolgenden quadratvollen Zahlen.

Im selben Gedankenzug betrachte man die Aussage

(E_{endlich}) Es gibt höchstens endlich viele n derart, dass $n-1$, n, $n+1$ quadratvoll sind.

Offensichtlich folgt (E_{endlich}) aus (E).

C Binomialzahlen und Wieferich-Kongruenzen

Ich beginne mit dem folgenden nützlichen Resultat, das Powell im Jahr 1977 als Problem formuliert hatte (Lösung von De Leon im Jahr 1978 veröffentlicht):

4.1. Sei p eine ungerade Primzahl und $a \geq 2$, $m \geq 1$. Wenn $a^m \equiv 1 \pmod{p}$ und $a^{m-1} \equiv 1 \pmod{p^2}$, dann $a^m \equiv 1 \pmod{p^2}$.

Beweis. Sei $h = \operatorname{ord}(a \mod p)$, also $h \mid m$, sagen wir $m = hk$. Auch $h \mid p-1$, also $p-1 = hl$. Schreibe $a^h = 1+cp$, dann $a^{p-1} = (1+cp)^l \equiv 1+lcp \pmod{p^2}$. Somit $p \mid lc$, also $p \mid c$ und daher $a^m = a^{hk} = (1+cp)^k \equiv 1 \pmod{p^2}$. □

Die folgenden Eigenschaften werden notwendig sein:

$$(\mathcal{P}B(a,-)_{\alpha,\epsilon}) := \#\{p \text{ prim} \mid a^p - 1 \text{ erfüllt Eigenschaft } \alpha\} = \epsilon,$$
$$(\mathcal{P}B(a,-)_{\alpha,\epsilon}{}^*) := \#\{p \text{ prim} \mid (a^p - 1)^* \text{ erfüllt Eigenschaft } \alpha\} = \epsilon.$$

4.2. Für jedes $a \geq 2$ gelten die folgenden Implikationen:

$$\begin{array}{ccccc}
(W(a)_{\text{endlich}}) & \longrightarrow & (\mathcal{P}B^*(a,-)_{SF,\infty}) & \longrightarrow & (B^*(a,-)_{SF,\infty}) \\
 & & \downarrow & & \downarrow \\
 & & (\mathcal{P}B^*(a,-)_{\neg W,\infty}) & \longrightarrow & (B^*(a,-)_{\neg W,\infty}) \longrightarrow (\neg W(a)_\infty) \\
 & & \downarrow & & \downarrow \\
 & & (\mathcal{P}B(a,-)_{\neg W,\infty}) & \longrightarrow & (B(a,-)_{\neg W,\infty})
\end{array}$$

Beweis. Bis auf zwei Implikationen sind alle trivial.

$(W(a)_{\text{endlich}}) \to (\mathcal{P}^*B(a,-)_{SF,\infty})$. Sei

$$\{p \text{ prim} \mid a^{p-1} \equiv 1 \pmod{p^2}\} = \{p_1, \ldots, p_m\}$$

und

$$h_0 = \max\{\operatorname{ord}(a \mod p_i) \mid i = 1, \ldots, m\},$$

und sei $p > h_0$. Sei $q = q(p)$ irgendein primitiver Primfaktor von $a^p - 1$, also $\operatorname{ord}(a \mod q) = p$. Insbesondere, falls $p \neq p'$, dann $q(p) \neq q(p')$.

Darüberhinaus folgt aus $p > h_0$, dass $q \neq p_1, \ldots, p_m$ und demnach $a^{q-1} \equiv 1 \pmod{q^2}$. Nach (4.1), $q^2 \nmid a^p - 1$. Dies zeigt, dass $(a^p - 1)^*$ quadratfrei ist.

$(B^*(a,-)_{\neg W,\infty}) \to (\neg W(a)_\infty)$. Sei n derart, dass $(a^n - 1)$ nicht quadratvoll ist, also gibt es eine Primzahl p_n derart, dass $p_n \mid (a^n - 1)^*$,

aber $p_n^2 \nmid (a^n-1)^*$. Demzufolge $p_n \mid a^n-1$, aber $p_n^2 \nmid a^n-1$. Nach (4.1), $p_n^2 \nmid (a^{p_n-1}-1)$. Man beachte, dass $n = \mathrm{ord}(a \mod p_n)$. Somit, wenn $n \neq m$, dann $p_n \neq p_m$. Dies zeigt $(\neg W(a)_\infty)$. □

Insbesondere folgt, wenn man $a = 2$ wählt, dass

$$(W(2)_{\text{endlich}}) \to ({M_{SF,\infty}}^*) \to ({M_{\neg W,\infty}}^*) \to (\neg W(2)_\infty).$$

Die folgende Implikation gilt für spezielle Werte von a:

4.3. Wenn a gerade ist und $\sqrt{a-1}$ quadratvoll, so $(B(a,-)_{W,\,\text{endlich}}) \to (B^*(a,-)_{\neg W,\infty})$.

Beweis. Wenn $(B^*(a,-)_{\neg W,\infty})$ unwahr ist, dann gibt es m_0 derart, dass für jedes $m > m_0$ und für jeden primitiven Primfaktor p_m von a^m-1 folgt, dass $p_m^2 \mid a^m-1$.

Wähle eine Primzahl $q > m_0$; wenn $s \geq 1$ und wenn l ein Primteiler von $a^{q^s}-1$ ist, dann gibt es h, $0 \leq h \leq s$ mit der Eigenschaft, dass l ein primitiver Primteiler von $a^{q^h}-1$ ist. Wenn $h = 0$, dann $l^2 \mid a-1$ nach Annahme. Wenn $h \geq 1$, dann folgt wieder $l^2 \mid a^{q^h}-1$, da $q > m_0$. Daher $l^2 \mid a^{q^s}-1$. Dies zeigt, dass $a^{q^s}-1$ im Widerspruch zur Annahme für jedes $s \geq 1$ eine quadratvolle Zahl ist. □

Ich notiere auch die folgende Implikation, die sich in Kürze als sehr nützlich erweisen wird:

4.4. $(B(a^2,-)_{W,\,\text{endlich}}) \to (\neg W(a)_\infty)$.

Beweis. Angenommen, dass $(\neg W(a)_\infty)$ nicht wahr ist. Dann gibt es p_0 derart, dass wenn p eine Primzahl ist mit $p > p_0$, dann gilt $a^{p-1} \equiv 1 \pmod{p^2}$. Sei $t = \prod_{p \leq p_0} p$, somit $\varphi(t) = \prod_{p \leq p_0}(p-1)$. Für jedes $h \geq 1$ sei $a_h = a^{ht\varphi(t)}$. Dann ist $a_h - 1$ eine quadratvolle Zahl, wie ich nun zeigen werde.

Man beachte, dass $2 \nmid a_h - 1$, somit ist a gerade. Wenn p eine Primzahl ist mit $2 < p \leq p_0$, dann ist $p(p-1)$ Teiler von $t\varphi(t)$; aus $a^{p-1} \equiv 1 \pmod{p}$ folgt, dass $a^{p(p-1)} \equiv 1 \pmod{p^2}$, daher $p^2 \mid a^{ht\varphi(t)} - 1 = a_h - 1$. Schließlich, wenn $p > p_0$ und $p \mid a_h - 1$, dann ist nach Annahme $a^{p-1} \equiv 1 \pmod{p^2}$; somit nach (4.1), $p^2 \mid a_h - 1$. Da h beliebig war, ist dies ein Widerspruch zur Annahme. □

Für das nächste Resultat werde ich die folgenden Notationen verwenden:

$$(QB(a,+)_{\alpha,\epsilon}) := \#\{2^n \mid a^{2^n}+1 \text{ erfüllt Eigenschaft } \alpha\} = \epsilon,$$
$$(QB^*(a,+)_{\alpha,\epsilon}) := \#\{2^n \mid (a^{2^n}+1)^* \text{ erfüllt Eigenschaft } \alpha\} = \epsilon.$$

Der nächste Satz ist das Analogon zu (4.2):

4.5. Für jedes $a \geq 2$ gelten die folgenden Implikationen:

$$\begin{array}{ccccc}
(W(a)_{\text{endlich}}) & \longrightarrow & (QB^*(a,+)_{SF,\infty}) & \longrightarrow & (B^*(a,+)_{SF,\infty}) \\
 & & \downarrow & & \downarrow \\
 & & (QB^*(a,+)_{\neg W,\infty}) & \longrightarrow & (B^*(a,+)_{\neg W,\infty}) \longrightarrow (\neg W(a)_\infty) \\
 & & \downarrow & & \downarrow \\
 & & (QB(a,+)_{\neg W,\infty}) & \longrightarrow & (B(a,+)_{\neg W,\infty})
\end{array}$$

Beweis. Nur zwei Implikationen erfordern einen Beweis.

$(W(a)_{\text{endlich}}) \to (QB^*(a,+)_{SF,\infty})$. Sei $\{p \mid a^{p-1} \equiv 1 \pmod{p^2}\} = \{p_1,\ldots,p_m\}$ und $h_0 = \max\{\text{ord}(a \mod p_i) \mid i = 1,\ldots,m\}$. Sei n derart, dass $2^n > h_0$ und sei q ein Primteiler von $(a^{2^n}+1)^*$. Also $q \mid a^{2^n}+1$, daher $q \mid a^{2^{n+1}}-1$ und $\text{ord}(a \mod q) = 2^{n+1} > h_0$; damit $q \neq p_i$ (für alle i) und demzufolge $a^{q-1} \not\equiv 1 \pmod{q^2}$. Da $2^{n+1} \mid q-1$ ist $a^{2^{n+1}} \not\equiv 1 \pmod{q^2}$ und wieder $a^{2^n} \not\equiv 1 \pmod{q^2}$, was zeigt, dass $(a^{2^n}+1)^*$ quadratfrei ist.

$(B^*(a,+)_{\neg W,\infty}) \to (\neg W(a)_\infty)$. Sei $n > 1$ derart, dass $(a^n+1)^*$ nicht quadratvoll ist, also gibt es eine Primzahl $p = p(a)$ mit der Eigenschaft, dass p Teiler von $(a^n+1)^*$ ist, aber $p^2 \nmid (a^n+1)^*$. Es folgt, dass $p \mid a^{2n}-1$, aber $p^2 \nmid a^n+1$ da $(a^n+1)^*$ und $\frac{a^n+1}{(a^n+1)^*}$ teilerfremd sind. Wenn $p^2 \mid a^{2n}-1$, dann $p \mid a^n-1$, also $p = 2$. Aber dies impliziert, dass a ungerade ist, somit $p \mid a+1$ und aufgrund der Annahme $n > 1$ würde folgen, dass p kein Teiler von $(a^n+1)^*$ wäre. Nach (4.1) wäre dann $a^{p-1} \not\equiv 1 \pmod{p^2}$.

Schließlich beachte man, dass $2n = \text{ord}(a \mod p_n)$, wenn also $n \neq n'$, dann $p_n \neq p_{n'}$. Daraus folgt, dass $(\neg W(a)_\infty)$ erfüllt ist. □

Wenn man $a = 2$ wählt, erhält man die Implikationen für Fermat-Zahlen:

$$(W(2)_{\text{endlich}}) \longrightarrow (F_{SF,\infty}{}^*) \longrightarrow (F^\alpha_{\neg W,\infty}) \longrightarrow (\neg W(2)).$$

Es gibt in dieser Richtung natürlich viele Aussagen, die der Leser als Übungsaufgabe beweisen könnte. Man betrachte beispielsweise die Folgenden, die auf Rotkiewicz (1965) und Warren und Bray (1967) zurückgehen:

1. Sei p eine Primzahl mit der Eigenschaft, dass p^2 eine Mersenne-Zahl teilt. Dann gilt $2^{p-1} \equiv 1 \pmod{p^2}$; umgekehrt, wenn p Teiler von M_q ist und $2^{p-1} \equiv 1 \pmod{p^2}$ gilt, dann teilt p^2 die Zahl M_q (diese Umkehrung ist nichts Anderes als (4.1)).
2. Die analoge Aussage gilt für Fermat-Zahlen.

D Erdös-Vermutung und Wieferich-Kongruenz

Ich beginne mit einer einfachen Darstellung der Verbindung zwischen der Wieferich-Kongruenz und der Vermutung von Erdös.

4.6. $(E_{\text{endlich}}) \to (B(a^2,-)_{W,\,\text{endlich}})$ (für jedes gerade a)

Beweis. Wenn a gerade und $a^{2k} - 1 = (a^k - 1)(a^k + 1)$ quadratvoll ist, dann folgt aus der Tatsache $\text{ggT}(a^k - 1, a^k + 1) = 1$, dass $a^k - 1$, a^k, $a^k + 1$ drei aufeinanderfolgende quadratvolle Zahlen sind. Somit folgt $(B(a^2,-)_{W,\,\text{endlich}})$ aus (E_{endlich}). □

Aus (4.4) und (4.6) folgt für alle geraden a, dass $(E_{\text{endlich}}) \to (\neg W(a)_\infty)$. Diese bemerkenswerte Implikation bewies Granville im Jahr 1986. Insbesondere gilt $(\neg W(2)_\infty)$. Hinsichtlich des Satzes von Wieferich folgt aus (E_{endlich}) der Satz von Adleman, Heath-Brown und Fouvry (der erste Fall von Fermats letztem Satz gilt für unendlich viele prime Exponenten), von dem bereits in (2.5) die Rede war. Ungeachtet der Tatsache, dass Wiles Fermats letzten Satz für alle Fälle bewies, ist obige Verbindung mit den quadratvollen Zahlen faszinierend.

E Der Traum im Traum

In Ihren Träumen haben Sie einen wunderbaren Traum und wünschten, er würde wahr. „Er“ buchstabiert man ABC und es ist die spannendste Vermutung, die man sich vorstellen (oder erträumen) kann. Dabei ist er so einfach zu erklären.

Mason (1983, 1984) bewies einen Satz über Polynome, der Masser im Jahr 1985 dazu inspirierte, eine Vermutung aufzustellen, die 1988

von OESTERLÉ folgendermaßen umformuliert wurde:

(ABC) Für jedes $\epsilon > 0$ gibt es $K(\epsilon) > 0$ derart, dass wenn A, B, C positive ganze Zahlen mit $\mathrm{ggT}(A, B, C) = 1$ und $A + B = C$ sind, dann gilt

$$C < K(\epsilon) R^{1+\epsilon} \tag{9.20}$$

wobei

$$R = \prod_{p|ABC} p.$$

In diesem Zusammenhang wird sich die folgende Terminologie als nützlich erweisen. Wenn $n \neq 0$, dann nennt man $r = \prod_{p|n,\, p \text{ prime}} p$ das *Radikal* von n. Somit ist R das Radikal von ABC. Innerhalb der Äußerung der Vermutung wird kein Versuch unternommen, irgendeine Andeutung einer effektiven unteren Schranke für $K(\epsilon)$ zu tätigen.

Was ist das Wesentliche an der Vermutung? Man nehme zum Beispiel $\epsilon = \frac{1}{2}$, $A = 2^m$ (m groß), $B = 3^n$ (n groß). Wenn (9.20) gilt, dann ist $C < K(\frac{1}{2}) 6^{3/2} \prod_{p|C} p^{3/2}$. Da C groß ist, muss C einen großen oder viele Primfaktoren besitzen. Auf jeden Fall bedeutet (ABC) eine tiefliegende Verbindung zwischen Addition und Multiplikation.

Eine Vermutung ist interessant, wenn sie für lange Zeit eine Vermutung bleibt und somit viele Versuche eines Beweises oder einer Widerlegung übersteht. Da $K(\epsilon)$ nicht explizit angegeben ist, fällt es schwer, einen Ansatz zum Widerlegen der (ABC)-Vermutung zu finden. Auf der anderen Seite impliziert die (ABC)-Vermutung viele weitere schwierige Vermutungen. Es ist also gleichermaßen wichtig wie schwer, (ABC) festzustellen.

Wie würde die Reaktion sein, wenn Sie als angesehener Mathematiker jemandem sagen, dass Sie (ABC) untersuchen? Vielleicht abfällig. Sagen Sie also stattdessen lieber, Sie studieren die (XYZ)-Vermutung. Das ist geheimnisvoller.

Spaß beiseite, ich werde nun angeben, was (ABC) zur Folge hat, wenn auch nicht alles. Hier eine eindrucksvolle Implikation (siehe Oesterlé (1988)).

4.7. (ABC) → Fermats letzter Satz ist für alle genügend großen Exponenten wahr.

Beweis. Angenommen, dass $n \geq 5$, a, b, c positive ganze Zahlen mit $\mathrm{ggT}(a, b, c) = 1$, $a < b < c$ und $a^n + b^n = c^n$ sind. Sei $\epsilon = \frac{1}{2}$ und $K = K(\frac{1}{2})$ wie bei der (ABC)-Vermutung.

Also,

$$c^n < K(abc)^{3/2} < Kc^{9/2},$$

und demzufolge $c^{n-\frac{9}{2}} < K$, damit ist n beschränkt, was Fermats letzten Satz für alle genügend großen Exponenten n beweist. □

Praktisch derselbe Beweis wurde von GRANVILLE im Jahr 1997 für die Gleichung

$$AX^n + BY^n = CZ^n \tag{9.21}$$

verwendet, wobei A, B, C teilerfremde ganze Zahlen ungleich Null sind.

4.8. (ABC) → Für alle genügend großen n besitzt die Gleichung (9.21) nur triviale Lösungen (x, y, z) mit $|x|, |y|, |z| \leq 1$.

In Abschnitt D hatte ich die Gleichung

$$AX^l + BY^m = CZ^n \tag{9.22}$$

betrachtet, wobei l, m, $n \geq 2$ und A, B, C teilerfremde ganze Zahlen verschieden von Null sind. Es wurde in (2.8) darauf hingewiesen, dass wenn $\frac{1}{l} + \frac{1}{m} + \frac{1}{n} < 1$, dann besitzt (9.22) nur endlich viele Lösungen (x, y, z) mit teilerfremden ganzen Zahlen x, y, z.

Ich habe (im Jahr 1999) gezeigt:

4.9. (ABC) → Es gibt nur endlich viele Tripel (l, m, n), die (9.22) erfüllen und für die Gleichung (9.21) eine nichttriviale Lösung (x, y, z) in teilerfremden ganzen Zahlen besitzt, d.h. $|x|$, $|y|$ oder $|z| > 1$.

Der Beweis von (4.9) erfordert die einfachere Implikation (4.10) weiter unten. Seien A, B, C teilerfremde ganze Zahlen verschieden von Null und sei U die Menge der 4-Tupel (l, m, x, y) derart, dass (1) $|x|, |y| > 1$, (2) $l, m \geq 2$, $\frac{1}{l} + \frac{1}{m} < 1$, und (3) $Ax^l + By^m = C$.

4.10. (ABC) → U ist eine endliche Menge.

Als Anwendung könnte man Differenzen von Potenzen betrachten ($A = 1$, $B = -1$). Dies beinhaltet Catalans Problem aufeinanderfolgender Potenzen (siehe Kapitel 7 dieses Buches). TIJDEMANs gefeierter Satz sagt aus, dass es eine effektiv berechenbare Schranke $C > 0$ mit der Eigenschaft gibt, dass wenn x, y, m, n ganze Zahlen mit $x, y \neq 0$, $m, n \geq 2$ sind und $x^m - y^n = 1$, dann sind $|x|, |y|, m, n < C$.

Sei $z_1 < z_2 < z_3 < \cdots$ die Folge aller ganzen Zahlen, die Potenzen mit beliebigem Exponenten (größer als 1) sind. Tijdemans Satz bedeutet, dass $\limsup(z_{i+1} - z_i) > 1$.

Landau vermutete, dass $\limsup(z_{i+1} - z_i) = \infty$. Dies wurde nie bewiesen. Jedoch:

4.11. (ABC) → Landaus Vermutung ist richtig.

Elkies bewies im Jahr 1991:

4.12. (ABC) → Faltings Satz (d.h., Mordells Vermutung ist wahr).

Der Beweis ist raffiniert.

Aus der Kombination der Resultate (4.7) und (4.10) lässt sich aus (ABC) folgern, dass es höchstens endlich viele 4-Tupel (x, y, z, n) mit $n \geq 3$, x, y, $z > 0$, $\mathrm{ggT}(x, y, z) = 1$ und $x^n + y^n = z^n$ gibt. Natürlich ist dabei keine Schranke explizit angegeben. Dies ist weniger, als die Aussage, dass (ABC) Wiles' Satz nach sich ziehen würde (d.h., dass Fermats letzter Satz wahr ist).

Das folgende Resultat wurde von Silverman im Jahr 1998 bewiesen; der einfachere Beweis an dieser Stelle wurde mir freundlicherweise von Ram Murty mitgeteilt.

4.13. (ABC) → $(\neg W(a)_\infty)$ für jedes $a \geq 2$.

Beweis. Für jedes $n \geq 1$ sei $a^n - 1 = u_n v_n$, wobei u_n quadratfrei ist und $\mathrm{ggT}(u_n, v_n) = 1$; also ist v_n quadratvoll. Man beachte, dass $\lim_{n\to\infty}(u_n v_n) = \infty$. Sei $U = \{p \text{ prim} \mid \text{es gibt } n \text{ derart, dass } p \mid u_n\}$. Da jedes u_n quadratfrei ist folgt, dass U genau dann endlich ist, wenn die Menge $\{u_n \mid n \geq 1\}$ beschränkt bleibt.

Für gegebenes $\epsilon = \frac{1}{2}$ sei $K = K(\frac{1}{2})$ wie in der (ABC)-Vermutung. Somit,

$$u_n v_n < a^n < K(a u_n v_n^{1/2})^{3/2},$$

da v_n quadratvoll ist. Also $v_n^{1/4} < K a^{3/2} u_n^{1/2}$. Wenn die Menge $\{u_n \mid n \geq 1\}$ beschränkt ist, dann gilt dies auch für $\{v_n \mid n \geq 1\}$, damit $\lim u_n v_n \to \infty$, ein Widerspruch.

Wenn $\{u_n \mid n \geq 1\}$ unbeschränkt ist, dann ist U unendlich. Wenn $p \in U$, dann $p^2 \nmid (a^n - 1)$, also nach (4.1), $a^{p-1} \not\equiv 1 \pmod{p^2}$, und somit ist $(\neg W(a)_\infty)$ wahr. □

Ich gebe nun eine weitere Implikation an. Mithilfe einer ähnlichen Argumentation lässt sich einfach zeigen, dass

4.14. (ABC) → Sei $a > b \geq 1$ mit $\mathrm{ggT}(a, b) = 1$. Dann ist die Menge $\{n \geq 1 \mid a^b \pm b^n \text{ ist quadratvoll}\}$ endlich.

Beweis. Für jedes n sei $a^n \pm b^n = u_n v_n$, wobei u_n quadratfrei, v_n quadratvoll und $\mathrm{ggT}(u_n, v_n) = 1$ ist. Sei $\epsilon = \frac{1}{2}$, $K = K(\frac{1}{2})$, also nach der (ABC)-Vermutung

$$u_n v_n < K(abu_n v_n^{1/2})^{3/2}.$$

Man beachte, dass $a^n \pm b^n$ genau dann quadratvoll ist, wenn $u_n = 1$. In diesem Fall gilt $v_n^{1/4} < K(ab)^{3/2}$. Damit ist v_n beschränkt und somit auch n. □

Als Spezialfall mit $a = 2$, $b = 1$ sei erwähnt

4.15. (ABC) $\rightarrow$ ($M_{W,\,\text{endlich}}$) und ($F_{W,\,\text{endlich}}$). In Worten: Es gibt nur endlich viele quadratvolle Mersenne- und Fermat-Zahlen.

Das Ergebnis (4.14) wurde von Ribenboim und Walsh (1999d) verallgemeinert. Sei $R > 0$ eine quadratfreie ganze Zahl, seien h, $k \geq 2$ und A, B, E ganze Zahlen verschieden von Null derart, dass $\mathrm{ggT}(A, ER) = \mathrm{ggT}(B, ER) = 1$. Betrachte für jedes $C \neq 0$ mit der Eigenschaft, dass das Radikal von C Teiler von R ist, die Gleichung

$$AX^h + BY^k = EC. \tag{9.23}$$

Sei $S_C = \{(x, y) \mid x \geq 1, y \geq 1, \mathrm{ggT}(x, y) = 1 \text{ und } Ax^h + By^k = EC\}$. Sei $S = \bigcup\{S_C \mid \text{Radikal von } C \text{ teilt } R\}$. Für jede ganze Zahl $n > 0$ bezeichne $w(n)$ den quadratvollen Teil von n. Also $n = w(n)n'$, wobei n' quadratfrei ist und $\mathrm{ggT}(w(n), n') = 1$. Mit obigen Notationen,

4.16. (ABC) $\rightarrow$ Für jedes $\epsilon > 0$ gibt es nur endlich viele $(x, y) \in S$ mit der Eigenschaft, dass $w(x) > x^\epsilon$ oder $w(y) > y^\epsilon$. Insbesondere gibt es nur endlich viele $(x, y) \in S$ derart, dass x oder y quadratvoll ist.

Es ist sinnvoll anzumerken, dass wenn $R = 1$ und $\max\{h, k\} \geq 3$, d.h. $\frac{1}{h} + \frac{1}{k} < 1$, dann folgt nach dem wohlbekannten Satz von Siegel, dass es nur endlich viele Paare (x, y) mit x, $y \geq 1$, $\mathrm{ggT}(x, y) = 1$ und der Eigenschaft gibt, dass $Ax^h + By^k = E$. Für $h = k = 2$ ist dies die Situation der Pellschen Gleichungen und wie allgemein bekannt ist, sind die Lösungen dieser Gleichungen Terme in bestimmten binären linear-rekurrenten Folgen.

Im selben Artikel wendeten Ribenboim und Walsh obiges Resultat an, um die quadratvollen Terme in binären linear-rekurrenten Folgen zu behandeln. Seien P, Q teilerfremde ganze Zahlen verschieden von

Null mit der Eigenschaft, dass $P > 0$, $D = P^2 - 4Q \neq 0$. Die folgenden zwei Lucas-Folgen gehören zu den Parametern (P, Q):

$$U_0 = 0, U_1 = 1, U_n = PU_{n-1} - QU_{n-2} \quad (\text{für } n \geq 2),$$

und

$$V_0 = 2, V_1 = P, V_n = PV_{n-1} - QV_{n-2} \quad (\text{für } n \geq 2).$$

Die additive Relation

$$V_n^2 - DU_n^2 = 4Q^n \tag{9.24}$$

gilt (für alle $n \geq 0$). Wenn $Q = \pm 1$ (zum Beispiel im Falle der Folgen der Fibonacci- und Lucas-Zahlen, die die Parameter $(1, -1)$ haben) erhält man:

$$V_n^2 - DU_n^2 = 4(-1)^n. \tag{9.25}$$

Das folgende Ergebnis ist bekannt (siehe Mollin (1996)):

4.17. (ABC) $\rightarrow$ Es gibt nur endlich viele quadratvolle Fibonacci- und Lucas-Zahlen.

Eine Erweiterung auf alle Lucas-Folgen mit Diskriminante $D > 0$ erfordert die Relation (9.24), die in (4.16) behandelt wird:

4.18. (ABC) $\rightarrow$ Wenn $D > 0$, dann sind die Mengen $\{n \geq 1 \mid w(U_n) > U_n^\epsilon\}$ und $\{n \geq 1 \mid w(V_n) \geq V_n^\epsilon\}$ für jedes $\epsilon > 0$ endlich. Insbesondere gibt es nur endlich viele $n \geq 1$ derart, dass U_n und V_n quadratvoll sind.

Im selben Artikel wurden weitere Typen binärer linear-rekurrenter Folgen behandelt, was zu ähnlichen Ergebnissen führte.

Eine Frage die behandelt wurde, betrifft die Differenzen zwischen Potenzen. Was aufeinanderfolgende Potenzen angeht, sei auf Kapitel 7 dieses Buches verwiesen. Mordell, Hall und viele andere untersuchten die Differenzen zwischen Quadraten und Kuben, d.h. die Gleichung

$$y^3 = x^2 + d$$

(wobei x, $y \geq 1$ und d eine nicht notwendigerweise positive ganze Zahl ist).

Hall vermutete:

(H) Für jedes $\epsilon > 0$ gibt es ein $K > 0$ (das von ϵ abhängt) mit der Eigenschaft, dass wenn $y^3 = x^2 + d$ mit x, $y \geq 1$, $d \neq 0$, dann $y < K|d|^{2+\epsilon}$.

Es macht Sinn, ähnliche Vermutungen $(H_{m,n})$ für jedes Paar (m, n) positiver ganzer Zahlen mit $\frac{1}{m} + \frac{1}{n} < 1$ aufzustellen:

$(H_{m,n})$ Für jedes $\epsilon > 0$ mit $0 < \epsilon < \frac{1}{6}$ gibt es ein $K > 0$ (das von ϵ, m, n abhängt) mit der Eigenschaft, dass wenn x, $y > 0$, $d \neq 0$ und $y^m = x^n + d$, dann $y < K|d|^{t+\epsilon}$, wobei $t = n/(mn - m - n)$.

In Ribenboim (1999a) ist gezeigt, dass

4.19. (ABC) $\rightarrow$ $(H_{m,n})$ hält für alle Paare (m, n) wie oben.

Die Vermutungen $(H_{m,n})$ ziehen interessante Konsequenzen nach sich, auf die im Artikel hingewiesen wird.

Es gibt auch starke Vermutungen über Primteiler von Polynomwerten und über quadratvolle Zahlen, die Werte von Polynomen sind.

Ich beginne mit einer Vermutung von Langevin (1993):

(L) Sei $f \in \mathbb{Z}[X]$ mit Grad $d \geq 2$ und nur einfachen Nullstellen. Für jedes $\epsilon > 0$ gibt es $K = K(f, \epsilon) > 0$ derart, dass wenn n genügend groß ist, dann $R(f(n)) > Kn^{d-1-\epsilon}$ (wobei $R(f(n))$ das Radikal von $f(n)$ ist).

Die Vermutung von Schinzel (1976) ist die folgende:

(ST) Sei $f \in \mathbb{Q}[X]$ mit mindestens drei einfachen Nullstellen. Dann $\#\{n \geq 1 \mid f(n) \text{ ist quadratvoll}\} < \infty$.

Diese Vermutung sollte man einmal mit dem Satz aus (2.12) vergleichen.

Es ist sehr einfach zu zeigen:

4.20. (ST) $\rightarrow$ (E_{endlich}).

Beweis. Sei $f(X) = X(X^2 - 1)$; also sind alle Nullstellen von f einfach. Wenn $n - 1$, n, $n + 1$ drei quadratvolle Zahlen sind, dann ist auch $f(n) = (n - 1)n(n + 1)$ quadratvoll. Da nach Annahme $\#\{n : |f(n)| \text{ ist quadratvoll}\} < \infty$, folgt (E_{endlich}). □

Walsh bewies im Jahr 1997 (erschienen 1999):

4.21. (L) $\rightarrow$ (ST).

Beweis. (1) Zunächst sei $f \in \mathbb{Z}[X]$ mit positivem Leitkoeffizient, $\deg(f) = d \geq 3$ und ausschließlich einfachen Nullstellen. Dann gibt es $C > 0$ derart, dass für alle genügend großen n die Ungleichung $|f(n)| < C|n|^d$ gilt.

Sei ϵ derart, dass $0 < \epsilon < \frac{1}{2}$ und sei $K > 0$ die Konstante aus Hypothese (L) mit der Eigenschaft, dass

$$R(f(n)) > K|n|^{d-1-\epsilon}$$

für alle genügend großen n.

Falls darüberhinaus $|f(n)|$ quadratvoll ist, so $R(f(n)) \leq |f(n)|^{1/2}$. Daher $C|n|^d > K^2|n|^{2(d-1-\epsilon)}$ und somit $C > K|n|^{d-2-2\epsilon}$. Aufgrund von $d - 2 - 2\epsilon > 0$ folgt, dass $|n|$ beschränkt bleibt, wenn $|f(n)|$ quadratvoll ist.

(2) Sei $f \in \mathbb{Z}[X]$ mit positivem Leitkoeffizient, $\deg(f) = d \geq 3$ und angenommen, dass f mindestens drei einfache Nullstellen besitzt. Das Polynom f lässt sich als Produkt von irreduziblen Polynomen schreiben, die nach dem Lemma von Gauß aus $\mathbb{Z}[X]$ gewählt werden können. Da f mindestens drei einfache Nullstellen hat, gibt es für die obige Zerlegung einen Ausdruck $f = gh$ mit g, $h \in \mathbb{Z}[X]$, $\deg(g) \geq 3$, wobei die Nullstellen von g die einfachen Nullstellen von f sind; darüberhinaus haben g und h positive Leitkoeffizienten und $\mathrm{ggT}(g, h) = 1$.

Demzufolge gibt es Polynome g_1, $h_1 \in \mathbb{Z}[X]$ derart, dass

$$g_1 g + h_1 h = 1.$$

Wenn $|n|$ genügend groß ist, dann sind $g(n)$, $g_1(n)$, $h(n)$, $h_1(n)$ verschieden von 0; da $g_1(n)g(n)+h_1(n)h(n) = 1$ folgt, dass $\mathrm{ggT}(g(n), h(n)) = 1$.

Da $|f(n)| = |g(n)||h(n)|$ quadratvoll ist, gilt dies auch für $|g(n)|$ und somit ist $|n|$ nach (1) beschränkt.

(3) Sei $f \in \mathbb{Q}[X]$ derart, dass es $a^2 \in \mathbb{Z}$ und $a^2 f \in \mathbb{Z}[X]$ gibt. Wenn f einen positiven Leitkoeffizienten hat und mindestens drei einfache Nullstellen besitzt, dann gilt dies auch für $a^2 f$. Nach (2) gibt es nur endlich viele $n \in \mathbb{Z}$ derart, dass $a^2 f(n)$ quadratvoll ist, *a fortiori* gilt dasselbe für f.

(4) Angenommen, dass der Leitkoeffizient a von f negativ ist. Wenn der Grad von f gerade ist, sei $f^-(X) = -f(X)$. Wenn d ungerade ist, sei $f^-(X) = f(-X)$. In beiden Fällen ist der Leitkoeffizient von f^- positiv. Nach (3) ist $\{n \in \mathbb{Z} : |f^-(n)| \text{ ist quadratvoll}\}$ endlich. Damit ist auch $\{n : |f(n)| \text{ ist quadratvoll}\}$ endlich. □

Langerin bewies (1993):

4.22. (ABC) → (L).

Aus obigen Resultaten lässt sich beispielsweise sagen, dass es nur endlich viele ganze Zahlen n derart gibt, dass $n^3 + n + 1$ quadratvoll ist.

Ich werde die Stärke der (ABC)-Vermutung anhand weiterer Beispiele aus meinem Artikel (1999) veranschaulichen. Das erste Ergebnis bezieht sich auf Differenzen zwischen kubikvollen Zahlen und quadratvollen Zahlen. Ich werde es der Einfachheit halber in einer speziellen Form darstellen.

Sei $R \geq 1$ eine quadratfreie ganze Zahl und sei V_R die Menge aller kubikvollen ganzen Zahlen k mit der Eigenschaft, dass es c, $1 \leq c < k$ mit $\mathrm{ggT}(k, c) = 1$ gibt, wobei das Radikal von c Teiler von R ist und gilt, dass $k + c$ oder $k - c$ quadratvoll ist. Dann,

4.23. (ABC) → Für jedes R wie oben ist die Menge V_R endlich.

Für den Fall $R = 1$ folgt insbesondere, dass es nur endlich viele kubikvolle Zahlen k derart gibt, dass $k+1$ oder $k-1$ quadratvoll sind. Wie in Abschnitt C angemerkt war, sind die einzig bekannten Beispiele $2^3 + 1 = 3^2$ und $23^3 + 1 = 2^3 \times 3^2 \times 13^2$.

Das nächste Resultat betrifft Tripel quadratvoller Zahlen, aus Gründen der Einfachheit werde ich einen Spezialfall angeben.

Sei $R \geq 1$ eine quadratfreie ganze Zahl, sei T_R die Menge aller Paare (k, c) derart, dass $1 \leq c < k$, $\mathrm{ggT}(k, c) = 1$, das Radikal von c teile R und $k-c$, k, $k+c$ seien quadratvolle Zahlen. Ich bewies (1999):

4.24. (ABC) → T_R ist für jede quadratfreie ganze Zahl $R \geq 1$ eine endliche Menge.

Insbesondere zeigt dies im Fall $R = 1$ erneut (ABC) → (E_{endlich}); siehe Granville (1990).

Es wurde nun in vielfältiger Weise dargestellt, wie interessant die (ABC)-Vermutung ist. Einen leicht zugänglichen Artikel über die Vermutung hat Nitaj (1996) verfasst.

Und falls es dazu kommen sollte, dass Sie wirklich antworten, die (ABC)- (und nicht die (XYZ)-) Vermutung zu untersuchen, wissen Sie nun, was sie erklären müssen.

Literaturverzeichnis

1857 A. Bunjakowski. Nouveaux théorèmes relatifs à la distributí on des nombres premiers et á la décomposition desl entiers en facteur. *Mém. Acad. Sci. St. Petersbourg*, 6:305–329.

1886 A. S. Bang. Taltheoretiske Untersogelser. *Tidskrift Math., Ser. 5*, 4:70–80 und 130–137.

1892 K. Zsigmondy. Zur Theorie der Potenzreste. *Monatsh. f. Math.*, 3:265–284.

1909 A. Wieferich. Zum letzten Fermatschen Theorem. *J. reine u. angew. Math.*, 136:293–302.

1935 P. Erdös und S. Szekeres. Uber die Anzahe der Abelsuhen Gruppen gegebner Ordnung und über ein verwandtes Zahlentheortisches. *Acta Sci. Math. Szeged*, 7:95–102.

1954 P. Bateman. Solution of problem 4459. *Amer. Math. Monthly*, 61:477–479.

1958 P. T. Bateman und E. Grosswald. On a theorem of Erdös and Szekeres. *Illinois J. Math.*, 2:88–98.

1958 A. Schinzel und W. Sierpiński. Sur certaines hypothèses concernant les nombres premiers. Remarques. *Acta Arith.*, 4:185–208 und 5:259 (1959).

1962 A. Makowski. Three consecutive integers cannot be powers. *Colloq. Math.*, 9:297.

1963 S. Hyyrö. On the Catalan problem (in Finnish). *Arkhimedes*, 1963, Nr. 1, 53–54. Siehe Math. Reviews, 28, 1964, #62.

1965 A. Rotkiewicz. Sur les nombres de Mersenne dépourvus de diviseurs carrés et sur les nombres naturels n tels que $n^2 \mid 2^n - 2$. *Matematicky Vesnik, Beograd, (2)*, 17:78–80.

1966 D. Kruyswijk. On the congruence $u^{p-1} \equiv 1 \pmod{p^2}$. *Math. Centrum Amsterdam*, 7 Seiten. In Dutch.

1966 L. J. Lander und T. R. Parkin. Counterexamples to Euler's conjecture on sums of like powers. *Bull. Amer. Math. Soc.*, 72:1079.

1967 L. J. Warren und H. Bray. On the square-freeness of Fermat and Mersenne numbers. *Pacific J. Math.*, 22:563–564.

1968 S. Puccioni. Un teorema per una resoluzione parziale del famoso teorema di Fermat. *Archimede*, 20:219–220.

1970 S. W. Golomb. Powerful numbers. *Amer. Math. Monthly*, 77: 848–852.

1972 E. Krätzel. Zahlen k-ter Art. *Amer. J. of Math.*, 94:309–328.

1975 P. Erdös. Problems, and results on consecutive integers. *Eureka*, 38:3–8.

1976 P. Erdös. Problems and results on consecutive integers. *Publ. Math. Debrecen*, 23:271–282.

1976 A. Schinzel und R. Tijdeman. On the equation $y^m = F(x)$. *Acta Arith.*, 31:199–204.

1976 D. T. Walker. Consecutive integer pairs of powerful numbers and related Diophantine equations. *Fibonacci Q.*, 11:111–116.

1977 B. Powell. Problem E2631 (prime satisfying Mirimanoff's condition). *Amer. Math. Monthly*, 84:57.

1978 B. H. Gross und D. E. Röhrlich. Some results on the Mordell-Weil groups of the Jacobian of the Fermat curve. *Invent. Math.*, 44:210–224.

1978 M. J. De Leon. Solution of problem E2631. *Amer. Math. Monthly*, 85:279–280.

1979 P. Ribenboim. *13 Lectures on Fermat's Last Theorem.* Springer-Verlag, New York. Zweite Ausgabe mit einem neuen Nachwort, 1995.

1981 R. W. K. Odoni. On a problem of Erdoös on sums of two squareful numbers. *Acta Arith.*, 39:145–162.

1981 W. A. Sentance. Occurrences of consecutive odd powerful numbers. *Amer. Math. Monthly*, 88:272–274.

1982 A. Ivić und P. Shiu. The distribution of powerful integers. *Illinois J. Math.*, 26:576–590.

1982 B. Powell. Problem E2948 ($p|x^{p-1} - y^{p-1}$, $2 \nmid pe$, p prime occurs frequently). *Amer. Math. Monthly*, 89:334.

1983 G. Faltings. Endlichkeitssätze für abelsche Varietäten über Zahlkörpern. *Invent. Math.*, 73:349–366.

1983 R. C. Mason. Equations over function fields. In *Number Theory Voondwijkerhout*, Lecture Notes in Mathematics, 1068, 149–157. Springer-Verlag.

1984 R. C. Mason. Diophantine equations over function fields. In *London Math. Soc. Lecture Notes 96*. Cambridge University Press, Cambridge.

1985 L. M. Adleman und D. R. Heath-Brown. The first case of Fermat's last theorem. *Invent. Math.*, 79:409–416.

1985 E. Fouvry. Théorème de Brun-Titchmarsh: applicatí ons au théorème de Fermat. *Invent. Math.*, 79:383–407.

1985 A. Granville. Refining the conditions on the Fermat quotient. *Math. Proc. Cambridge Phil. Soc.*, 98:5–8.

1985 A. Granville. The set of exponents for which Fermat's last theorem is true has density one. *C. R. Math. Rep. Acad. Sci. Canada*, 7:55–60.

1985 D. R. Heath-Brown. Fermat's last theorem is true for "almost all" exponents. *Bull. London Math. Soc.*, 17:15–16.

1985 D. W. Masser. Open problems. In *Proceedings Symposium Analytic Number Theory*, herausgegeben von W. W. L. Chen, London. Imperial College.

1985 A. Nitaj. On a conjecture of Erdös on 3-powerful numbers. *Bull. London Math. Soc.*, 27:317–318.

1985 B. Powell und P. Ribenboim. Note on a paper by M. Filaseta regarding Fermat's last theorem. *Ann. Univ. Turkuensis*, 187:3–22.

1986 A. Granville. Powerful numbers and Fermat's last theorem. *C. R. Math. Rep. Acad. Sci. Canada*, 8:215–218.

1986 R. A. Mollin und P. G. Walsh. A note on powerful numbers, quadratic fields and the Pellian. *C. R. Math. Rep. Acad. Sci. Canada*, 8:109–114.

1986 R. A. Mollin und P. G. Walsh. On powerful numbers. *Intern. J. Math. and Math. Sci.*, 9:801–806.

1986 C. Eynden Vanden. Differences between squares and powerful numbers. *Fibonacci Q.*, 24:347–348.

1987 A. Granville. *Diophantine Equations with Variable Exponents with Special Reference to Fermat's Last Theorem.* Dissertation, Queen's University.

1987 W. L. McDaniel. Representatations of every integer as the difference of nonsquare powerful numbers. *Port. Math.*, 44:69–75.

1987 R. A. Mollin. The power of powerful numbers. *Intern. J. Math. and Math. Sci.*, 10:125–130.

1988 F. Beukers. The Diophantine equation $AX^p + BY^q = CZ^r$. *Duke Math. J.*, 91:61–88.

1988 N. D. Elkies. On $A^4 + B^4 + C^4 = D^4$. *Math. of Comp.*, 51: 825–835.

1988 A. Granville und M. B. Monagan. The first case of Fermat's last theorem is true for all prime exponents up to 714,591,116,091,389. *Trans. Amer. Math. Soc.*, 306:329–359.

1988 D. R. Heath-Brown. Ternary quadratic forms and sums of three square-full numbers. In *Sém. Th. Numbers Paris 1986–87*, herausgegeben von C. Goldstein. Birkhäuser, Boston.

1988 J. Oesterlé. Nouvelles approches du "théorème" de Fermat. Séminaire Bourbaki, 40ème anée, 1987/8, Nr. 694, *Astérisque*, 161–162, 165–186.

1988 P. Ribenboim. Remarks on exponential congruences and powerful numbers. *J. Nb. Th.*, 29:251–263.

1988 J. H. Silverman. Wieferich's criterion and the *abc*-conjecture. *J. Nb. Th.*, 30:226–237.

1990 A. Granville. Some conjectures related to Fermat's last theorem. In *Number Theory*, 177–192. W. de Gruyter, Berlin.

1990 K. A. Ribet. On modular representations of $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ arising from modular forms. *Invent. Math.*, 100(2):431–476.

1991 W. D. Elkies. *ABC* implies Mordell. *Internat. Math. Res. Notices (Duke Math. J.)*, 7:99–109.

1993 M. Langevin. Cas d'égalité pour le théorème de Mason et applications de la conjecture (*abc*). *C. R. Acad. Sci. Paris, Sér. I*, 317(5):441–444.

1993 P. Ribenboim. Density results on families of Diophantine equations with finitely many solutions. *L'Enseign. Math.*, 39:3–23.

1994 P. Ribenboim. *Catalan's Conjecture.* Academic Press, Boston.

1995 H. Darmon und A. Granville. On the equations $Z^m = F(x, y)$ and $A^p + By^q = CZ^r$. *Bull. London Math. Soc.*, 27:513–544.

1995 A. Granville. On the number of solutions of the generalized Fermat equation. *Can. Math. Soc. Conference Proc.*, 15:197–207.

1995 R. Taylor und A. Wiles. Ring theoretic properties of certain Hecke algebras. *Annals of Math. (2)*, 141:553–572.

1995 A. Wiles. Modular elliptic curves and Fermat's last theorem. *Annals of Math. (2)*, 141:443–551.

1996 R. A. Mollin. Masser's conjecture used to prove results about powerful numbers. *J. Math. Sci.*, 7:29–32.

1996 A. Nitaj. La conjecture *abc*. *L'Enseign. Math.*, 42:3–24.

1996 P. Ribenboim. *The New Book of Prime Number Records.* Springer-Verlag, New York.

1997 H. Darmon und L. Merel. Winding quotients and some variations of Fermat's last theorem. *J. reine u. angew. Math.*, 490: 81–100.

1997 K. A. Ribet. On the equation $a^p + 2^\alpha b^p + c^p = 0$. *Acta Arith.*, 79(1):7–16.

1999 P. G. Walsh. On the conjecture of Schinzel and Tijdeman. *Number Theory in Progress* (Tagungsband einer Konferenz zu Ehren des sechzigsten Geburtstags von A. Schinzel, Zakopane, Polen, 1997) Walter de Gruyter. 577–582.

1998 J. H. E. Cohn. A conjecture of Erdös on 3-powerful numbers. *Math. of Comp.*, 67:439–440.

1999 A. Kraus. On the equation $X^p + Y^q = Z^r$, a survey. *Hardy-Ramanujan J*, 3:315–333.

1999 P. Ribenboim. *ABC*-conjecture Vorabdruck.

1999 P. Ribenboim. *Fermat's Last Theorem for Amateurs.* Springer-Verlag, New York.

1999 P. Ribenboim. Hausaufgabe.

1999 P. Ribenboim und P. G. Walsh. The *ABC* conjecture and the powerful part of terms in binary recurring sequences. *J. Nb. Th.*, 74:134–147.

1999 C. Breuil, B. Conrad, F. Diamond und R. Taylor. On the modularity of elliptic curves over Q: Wild 3-adic exercises. *J. Am. Math. Soc.*, 14:843-939.

10

Was für eine Art Zahl ist $\sqrt{2}^{\sqrt{2}}$?[1]

1 Einführung

Ist $\sqrt{2}^{\sqrt{2}}$ eine rationale Zahl?

Eine Zahl ist genau dann rational, wenn ihre Dezimalbruchentwicklung endlich oder periodisch ist.

Da ein Taschen- (oder selbst ein Riesen-) Rechner nur mit endlich vielen Dezimalstellen umgehen kann, ist die Verwendung ungeeignet, um zu entscheiden, ob $\sqrt{2}^{\sqrt{2}}$ rational ist oder nicht.

Was für eine Art Zahl aber ist $\sqrt{2}^{\sqrt{2}}$, wie kann man dies feststellen?

2 Arten von Zahlen

Ich werde zunächst die verschiedenen Arten von Zahlen in Erinnerung rufen. Es gibt die ganzen Zahlen, die wie KRONECKER sagte, „Gott-gegeben“ sind und als Basis zum Aufbau der gesamten Mathematik dienen sollten.

Als Nächstes gibt es die rationalen Zahlen, die man aus den ganzen Zahlen durch Divisionen gewinnt.

PYTHAGORAS fiel auf, dass wenn die Seiten eines rechtwinkligen Dreiecks die Länge 1 haben, so ist die Hypotenuse der Länge $\sqrt{2}$ keine rationale Zahl: Denn wenn $\sqrt{2} = \frac{m}{n}$, dann $2 = \frac{m^2}{n^2}$, also $2n^2 = m^2$, d.h. die Potenz der 2 auf der linken Seite hat einen ungeraden Exponenten, auf der rechten Seite aber einen geraden, was der Eindeutigkeit der

[1] Ich bin P. BUNDSCHUH und M. WALDSCHMIDT für ihre Ratschläge bei der Vorbereitung dieses Textes dankbar.

Primfaktorenzerlegung widerspricht. Diese Entdeckung sorgte in der damaligen Zeit für große Verwirrung und erforderte eine wesentliche Änderung in der Vorstellung von Zahlen.

Allgemeiner gilt, dass wenn p eine Primzahl ist und $n \geq 2$, dann ist $\sqrt[n]{p}$ keine rationale Zahl.

Das Wurzelziehen kann also zu einer neuen Art von Zahlen führen. Dies kann man auch so ausdrücken, dass die Nullstellen der Gleichungen $X^n - a = 0$ $(a \geq 1)$ nicht unbedingt rationale Zahlen sind.

Ich werde allgemeiner die Lösungen von Polynomgleichungen mit rationalen Koeffizienten untersuchen.

Lösungen linearer Gleichungen sind wieder rationale Zahlen. Lösungen quadratischer Gleichungen kann man durch Quadratwurzeln ausdrücken. Cardano zeigte, dass Lösungen kubischer und biquadratischer Gleichungen sich auch durch Quadrat- und dritte Wurzeln ausdrücken lassen.

Diese Entdeckungen führten zur folgenden Frage:

Sind Lösungen jeder Polynomgleichung (mit rationalen Koeffizienten und beliebigem Grad) immer durch Wurzeln ausdrückbar?

Dieses Problem dominierte die Algebra von etwa 1750 bis 1830 und war Gegenstand wichtiger Arbeiten von Lagrange, Gauss, Abel, Ruffini und Galois. Dies wird in sachkundiger Weise in Nový̆s Buch beschrieben.

Bis zu dieser Stelle waren alle betrachteten Zahlen reelle Zahlen gewesen—Zahlen, die dem Maß einer Strecke entsprechen. Jede solche Zahl besitzt eine Dezimalbruchentwicklung, und wie wir oben gesagt hatten, sind die rationalen Zahlen solche, die eine endliche oder periodische Entwicklung haben. Reelle Zahlen die nicht rational sind, nennt man *irrationale Zahlen*.

Die Gleichung $X^2+1 = 0$ kann keine Nullstelle haben, die eine reelle Zahl ist, da die Summe zweier Quadrate reeller Zahlen ungleich Null positiv ist und so auch nicht gleich Null.

Daher war es notwendig, eine neue Art von Zahlen zu erfinden.

Die komplexen Zahlen wurden eingeführt um sicherzustellen, dass alle Polynomgleichungen mit rationalen Koeffizienten Lösungen besitzen.

Die komplexen Zahlen haben die Form $\alpha = a + bi$, wobei a, b reelle Zahlen sind und $i = \sqrt{-1}$ (also $i^2+1 = 0$). Die komplex Konjugierte von α ist $\bar{\alpha} = a - bi$, also sind α, $\bar{\alpha}$ Lösungen der quadratischen Gleichung $X^2 - 2aX + a^2 + b^2 = 0$, die reelle Koeffizienten besitzt.

D'Alembert und Gauss bewiesen den Fundamentalsatz der Algebra, der besagt, dass wenn $f(X) = 0$ irgendeine Polynomgleichung mit reellen Koeffizienten ist (oder sogar mit komplexen Koeffizienten), dann besitzt sie eine Nullstelle, die eine komplexe Zahl ist. Genauer gilt, dass wenn das Polynom den Grad $d \geq 1$ hat, dann besitzt die Gleichung d Nullstellen, die komplexe Zahlen sind (nicht notwendigerweise verschieden).

Der Übersicht halber hier noch einmal die üblichen Notationen:

$\mathbb{Z}$ = Menge aller ganzen Zahlen
$\mathbb{Q}$ = Menge aller rationalen Zahlen
$\mathbb{R}$ = Menge aller reellen Zahlen
$\mathbb{C}$ = Menge aller komplexen Zahlen

Die Mengen $\mathbb{Q}$, $\mathbb{R}$ und $\mathbb{C}$ sind Körper, was insbesondere heißt, dass sie bezüglich der Division abgeschlossen sind (d.h., lineare Gleichungen lösen), während der Fundamentalsatz der Algebra besagt, dass $\mathbb{C}$ bezüglich dem Lösen von Polynomgleichungen abgeschlossen ist. Daher nennt man $\mathbb{C}$ einen *algebraisch abgeschlossenen Körper*.

Die Betrachtung von Gleichungen mit Koeffizienten aus $\mathbb{Z}$ (oder aus $\mathbb{Q}$) führte zur Menge $\mathbb{Q}^{\text{alg}}$ aller komplexen Zahlen, die Nullstellen von Polynomgleichungen mit Koeffizienten aus $\mathbb{Q}$ sind. Die Menge $\mathbb{Q}^{\text{alg}}$ ist ein algebraisch abgeschlossener Körper und der kleinste, der $\mathbb{Q}$ umfasst.

Ein Element aus $\mathbb{Q}^{\text{alg}}$ nennt man *algebraische Zahl*. Darüberhinaus heißt jede algebraische Zahl, die eine Nullstelle eines normierten Polynoms mit Koeffizienten aus $\mathbb{Z}$ ist, eine *algebraische ganze Zahl*.

Wenn $\alpha \in \mathbb{Q}^{\text{alg}}$ eine Nullstelle eines Polynoms $f(X)$ vom Grad $d \geq 1$ mit Koeffizienten aus $\mathbb{Q}$ ist, aber von keinem mit kleinerem Grad, dann nennt man d den *Grad von* α. Das Polynom $f(X)$ nennt man *Minimalpolynom* von α und es ist über $\mathbb{Q}$ irreduzibel. Die Nullstellen jedes irreduziblen Polynoms vom Grad d sind algebraische Zahlen vom Grad d.

Damit ist α eine rationale Zahl genau dann, wenn es eine algebraische Zahl vom Grad 1 ist. Darüberhinaus gibt es für jedes $d \geq 1$ algebraische Zahlen und sogar algebraische ganze Zahlen α vom Grad d. Äquivalent ausgedrückt, für jedes $d \geq 1$ gibt es irreduzible normierte Polynome $f(X) \in Z[X]$ vom Grad d. Zum Beispiel ist $X^d - p$ irreduzibel, wenn p irgendeine Primzahl ist.

In diesem Zusammenhang sollte man beachten, dass wenn $f(X) \in \mathbb{Z}[X]$ und $f(X) = g(X)h(X)$ mit $g(X)$, $h(X) \in \mathbb{Q}[X]$, dann gibt es auch $g_1(X)$, $h_1(X) \in \mathbb{Z}[X]$ desselben Grades wie $g(X)$ bzw. $h(X)$ mit der Eigenschaft, dass $f(X) = g_1(X)h_1(X)$. Dieses Lemma geht auf

Gauss zurück. Damit ist $f(X) \in \mathbb{Z}[X]$ irreduzibel über $\mathbb{Q}$ genau dann, wenn es irreduzibel über $\mathbb{Z}$ ist.

Der Beweis der Irreduzibilität von $X^d - p$ ist im Wesentlichen derselbe wie der Beweis des allgemeineren Irreduzibilitätskriteriums von Eisenstein.

Wenn $f(X) = X^d + a_1 X^{d-1} + \cdots + a_{d-1}X + a_d \in \mathbb{Z}[X]$ und wenn es eine Primzahl p derart gibt, dass p jeden Koeffizienten a_i teilt, aber p^2 kein Teiler von a_d ist, dann ist $f(X)$ irreduzibel.

Jede komplexe Zahl, die keine algebraische Zahl ist, nennt man *transzendente Zahl*. Ausführlich: α ist eine transzendente Zahl, wenn es kein vom Nullpolynom verschiedenes Polynom $f(X)$ mit Koeffizienten aus $\mathbb{Q}$ gibt mit $f(\alpha) = 0$.

Allgemeiner nennt man die Zahlen $\alpha_1, \ldots, \alpha_n$ algebraisch unabhängig (über $\mathbb{Q}$), wenn es kein vom Nullpolynom verschiedenes Polynom $f(X_1, \ldots, X_n)$ mit Koeffizienten aus $\mathbb{Q}$ mit $f(\alpha_1, \ldots, \alpha_n) = 0$ gibt.

Ich fasse die obige Diskussion der verschiedenen Zahlen in Abbildung 10.1 zusammen.

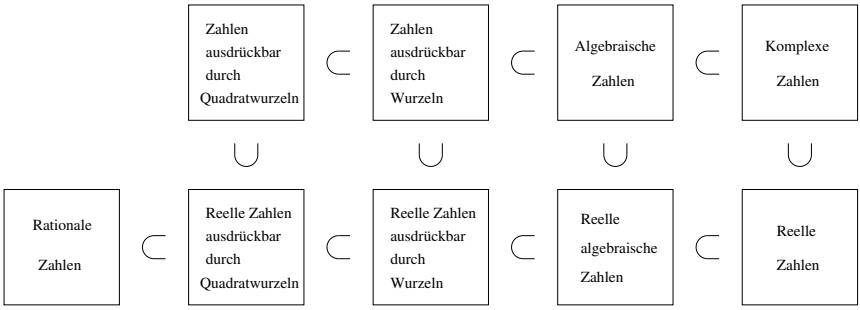


Abb. 10.1.

Dies ist der Moment, um einige bedeutende klassische Entdeckungen in Erinnerung zu rufen.

Eine reelle Zahl ist durch Quadratwurzeln genau dann ausdrückbar, wenn sie dem Maß eines Abschnitts entspricht, der mithilfe von Lineal und Zirkel konstruiert werden kann (beginnend mit einem Abschnitt der Länge 1). Gauss zeigte, dass die Seiten eines regulären Vielecks mit n Seiten genau dann mit Lineal und Zirkel konstruierbar sind (d.h., die Wurzeln von $X^n - 1 = 0$ sind durch Quadratwurzeln ausdrückbar), wenn n ein Produkt von Zweierpotenzen und verschiedenen primen Fermat-Zahlen ist:

$$p = F_m = 2^{2^m} + 1 \quad (\text{mit } m \geq 0).$$

Also $n = 3, 5, 17, 257, 65537, \ldots$ sowie deren Produkte mit Potenzen der 2.

Als Kuriosität sei erwähnt, dass RICHELOT im Jahr 1832 eine explizite Formel mit Quadratwurzeln für die Seiten des regulären Vielecks mit 257 Seiten angab—sie füllte 83 Seiten eines Artikels in Crelles Journal, Band 9, 1832.

ABEL, RUFFINI und GALOIS zeigten, dass es für $d \geq 5$ algebraische Zahlen vom Grad d gibt, die nicht durch Wurzeln ausdrückbar sind.

Genauer besagt GALOIS' Satz: Wenn $\alpha \in \mathbb{C}$ die Nullstelle eines irreduziblen Polynoms $f(X) \in \mathbb{Z}[X]$ ist, dann ist α genau dann durch Wurzeln ausdrückbar, wenn die Galois-Gruppe des Polynoms $f(X)$ (d.h. die Gruppe der Automorphismen des durch die Nullstellen von $f(X)$ generierten Körpers) auflösbar ist.

ABEL und RUFFINI fanden heraus, dass die symmetrische Gruppe sowie die alternierende Gruppe auf $d \geq 5$ Elementen nicht auflösbar sind. So ist zum Beispiel jede Nullstelle eines irreduziblen Polynoms vom Grad $d \geq 5$ mit symmetrischer oder alternierender Gruppe nicht durch Wurzeln ausdrückbar.

Übrigens zeigte VAN DER WAERDEN 1933, dass „fast alle“ irreduziblen Polynome eine Galois-Gruppe gleich der symmetrischen Gruppe haben. Wenn nämlich $f(X) \in \mathbb{Z}[X]$, so bezeichne $\sqcap f$ das Maximum der Absolutwerte der Koeffizienten. Für $d \geq 2$ sei für jedes $N \geq 1$

$$I_N = \{f(X) \in \mathbb{Z}[X] \mid \deg(f) = d, f(X) \text{ ist irreduzibel}, \sqcap f \leq N\},$$
$$S_N = \{f(X) \in I_N \mid \text{die Galois-Gruppe von } f(X) \text{ ist die symmetrische Gruppe auf } d \text{ Elementen}\}.$$

Dann gilt

$$\lim_{N\to\infty} \frac{\#(S_N)}{\#(I_N)} = 1.$$

Jede Menge die man in eine Eins-zu-Eins-Beziehung mit der Menge der natürlichen Zahlen setzen kann, nennt man *abzählbar*. So sind $\mathbb{Z}$ und $\mathbb{Q}$ abzählbar.

Da jedes Polynom nur endlich viele Nullstellen hat folgt, dass $\mathbb{Q}^{\text{alg}}$ auch abzählbar ist. Es ist ein berühmtes Resultat von CANTOR, dass $\mathbb{R}$ (und damit $\mathbb{C}$) überabzählbar ist.

Die Mengen der irrationalen und transzendenten Zahlen sind also überabzählbar.

3 Wie Zahlen gegeben sind

Die Methoden um zu entscheiden, ob eine gegebene Zahl transzendent ist beruhen darauf, „wie gut“ die Zahl durch rationale Zahlen oder algebraische Zahlen approximierbar ist. Dies wiederum wird anhand der Form ersichtlich, in der die Zahl gegeben ist. Es erscheint also sinnvoll, als vorbereitenden Schritt zu erläutern, wie Zahlen gebildet werden können.

Im Grunde gehen Zahlen durch „Prozeduren“ aus bekannten Zahlen hervor.

Rationale Zahlen zum Beispiel gewinnt man aus ganzen Zahlen durch Divisionen, algebraische Zahlen aus rationalen Zahlen durch Lösen von Polynomgleichungen.

Aber es gibt auch infinitistische Prozeduren wie die folgenden:

- Schreiben unendlicher Dezimalbrüche gemäß irgendeiner Regel oder auch „zufällig“
- Grenzwerte von Folgen
- Reihensummen
- Unendliche Produkte
- Werte bestimmter Integrale
- Kettenbrüche
- Werte von Funktionen an bestimmten Stellen
- Mathematische Konstanten
- usw....

Ich werde nun einige Beispiele behandeln.

Beispiele

(1) Die Funktion $x \mapsto \log x = \int_1^x \frac{dt}{t}$, definiert für $0 < x < \infty$, ist eins-eindeutig und bildet auf $\mathbb{R}$ ab. Die Zahl e ist die einzige reelle Zahl für die gilt $\log e = 1$.

Aber e wird auch gegeben durch

$$e = \lim_{n\to\infty} \left(1 + \frac{1}{n}\right)^n,$$

oder durch

$$e = \sum_{n=0}^{\infty} \frac{1}{n!}.$$

Darüberhinaus gab EULER eine einfache Kettenbruchentwicklung für e an:

$$e = [2, 1, 2, 1, 1, 4, 1, 1, 6, 1, 1, 8, 1, \dots]$$

d.h.

$$e = 2 + \cfrac{1}{1 + \cfrac{1}{2 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{4 + \cfrac{1}{1 + \cfrac{1}{1 + \frac{1}{6} + \cdots}}}}}}}$$

(Kettenbrüche werden in §5 behandelt.)

Allgemeiner zeigte EULER, dass wenn $a = 1, 2, 3, \dots$, dann

$$\frac{e^{2/\alpha} + 1}{e^{2/\alpha} - 1} = [a, 3a, 5a, 7a, \dots].$$

Insbesondere,

$$\frac{e^2 + 1}{e^2 - 1} = [1, 3, 5, 7, \dots] \quad \text{und} \quad \frac{e + 1}{e - 1} = [2, 6, 10, 14, \dots].$$

(2) Die Zahl π, definiert als das Verhältnis

$$\pi = \frac{\text{Länge eines Kreises}}{\text{Durchmesser eines Kreises}} \quad \text{(für jeden beliebigen Kreis)}$$

ist eine natürliche Konstante. Aber π ist auch auf mehrere andere Weisen gegeben.

GREGORYs Reihe:

$$\frac{\pi}{4} = 1 - \frac{1}{3} + \frac{1}{5} - \frac{1}{7} + \cdots.$$

VIÈTEs unendliches Produkt:

$$\pi = \frac{2}{\sqrt{\frac{1}{2}}\sqrt{\frac{1}{2} + \frac{1}{2}\sqrt{\frac{1}{2}}}\sqrt{\frac{1}{2} + \frac{1}{2}\sqrt{\frac{1}{2} + \frac{1}{2}\sqrt{\frac{1}{2}}}}\cdots}.$$

Wallis' unendliches Produkt (1685):

$$\frac{\pi}{2} = \prod_{n=1}^{\infty} \frac{2n}{2n-1} \times \frac{2n}{2n+1}.$$

Brounckers Kettenbruch (veröffentlicht von Wallis im Jahr 1655):

$$\frac{4}{\pi} = 1 + \cfrac{1^2}{2 + \cfrac{3^2}{2 + \cfrac{5^2}{2 + \cfrac{7^2}{2 + \cfrac{9^2}{2 + \cdots}}}}}$$

Dies ist kein einfacher Kettenbruch, d.h. die Zähler sind alle ungleich 1.

Unter Verwendung der Dezimalbruchentwicklung von π mit 35 Stellen berechnete Wallis 1685 die ersten 34 partiellen Quotienten der einfachen Kettenbruchentwicklung von π:

$$\pi = [3, 7, 15, 1, 292, 1, 1, 1, 2, 1, 3, 1, 14, 2, 1, 1, \\ 2, 2, 2, 2, 1, 84, 2, 1, 1, 15, 3, 13, 1, 4, 2, 6, 6, 1, \ldots].$$

Die ersten 26 partiellen Quotienten wurden erneut von Lambert im Jahr 1770 ermittelt.

Dieser einfache Kettenbruch für π weist auf keine regelmäßigen Muster hin. Bis heute hat niemand einen regulären einfachen Kettenbruch für irgendeine mit π nahe verwandte Zahl gefunden.

In einem Artikel von 1878 stellte Glaisher eine Sammlung von Reihen und unendlichen Produkten für π und Potenzen davon zusammen. Bei den Beweisen dazu handelt es sich um amüsante Übungsaufgaben. Und wer weiß, vielleicht sind die Formeln ja sogar auch nützlich. Es sei beispielhaft angeführt:

$$\frac{2\pi\sqrt{3}}{27} + \frac{1}{3} = \sum_{j=1}^{\infty} \frac{1}{\binom{2j}{j}},$$

$$\frac{\pi\sqrt{3}}{9} = \sum_{j=1}^{\infty} \frac{1}{j\binom{2j}{j}}.$$

Die Allgegenwärtigkeit von π ist in überzeugender Weise in Castellanos (1988) dargestellt.

(3) Die Zahl $\sqrt{2}^{\sqrt{2}}$ (mit der ich die Diskussion begonnen hatte) und allgemeiner, komplexe Zahlen $\alpha^\beta = e^{\beta \log \alpha}$ mit $\alpha, \beta \in \mathbb{C}$, $\alpha \neq 0$ sind Werte einer Exponentialfunktion. Die interessanteren Beispiele sind die, wo α, β algebraische Zahlen sind und β nicht rational ist. Ich werde auf diesen Punkt später zurückkommen.

(4) Die *Riemannsche Zetafunktion* ist für $s > 1$ definiert durch

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

Es ist interessant, die Werte von $\zeta(s)$ für $s = 2, 3, 4, \ldots$ zu betrachten.

Eulers berühmte Formel ergibt

$$\zeta(2k) = (-1)^{k-1} \frac{(2\pi)^{2k}}{2(2k)!} B_{2k}$$

wobei die Zahlen B_n $(n \geq 0)$ die Bernoulli-Zahlen sind, die durch die formale Potenzreihe

$$\frac{x}{e^x - 1} = \sum_{n=0}^{\infty} B_n \frac{x^n}{n!}$$

gegeben sind.

Somit $B_0 = 1$, $B_1 = -\frac{1}{2}$, $B_2 = \frac{1}{6}$, $B_4 = -\frac{1}{30}$, jedes B_n ist eine rationale Zahl und $B_{2n+1} = 0$ (für $n \geq 1$). So ist zum Beispiel $\zeta(2) = \frac{\pi^2}{6}$, $\zeta(4) = \frac{\pi^4}{90}$.

Es folgt, dass $\zeta(2k)/\pi^{2k}$ eine rationale Zahl ist (für $k \geq 1$).

Im Gegensatz dazu ist viel weniger über die Werte von $\zeta(2k+1)$ bekannt. Ramanujan gab ohne Beweis die unten folgende Formel an (siehe seine *Notizbücher, Band I*, Seite 259, Nummer 15 und Band II, Seite 177, Nummer 21, veröffentlicht im Jahr 1957).

Ramanujans Entdeckungen, wunderbare Formeln, die zumeist ohne Beweis blieben, haben die Mathematiker gequält. Die Arbeit von Ramanujan war Gegenstand maßgeblicher Bücher von Berndt. In diesen befinden sich Beweise und Einblicke in wahrscheinliche Methoden hinter den Beweisen sowie Einsichten über Ramanujans Denkweisen. Diesbezüglich sei auf die Bücher und Artikel von Berndt (1974, 1977, 1985, 1989), *Ramanujans Notizbücher*, Teil II, Seite 276 (1989) verwiesen, in denen auch die wesentlichen Referenzen enthalten sind.

Sei $\alpha, \beta > 0$, $\alpha\beta = \pi^2$, $k \neq 0$. Dann

$$\frac{1}{\alpha^k}\left\{\frac{1}{2}\zeta(2k+1) + \sum_{j=1}^{\infty}\frac{j^{-(2k+1)}}{e^{2\alpha j}-1}\right\} - \frac{(-1)^k}{\beta^k}\left\{\frac{1}{2}\zeta(2k+1) + \sum_{j=1}^{\infty}\frac{j^{-(2k+1)}}{e^{2\beta j}-1}\right\}$$
$$= 2^{2k}\sum_{j=0}^{k+1}(-1)^{j+1}\frac{B_{2j}}{(2j)!} \times \frac{B_{2k+2-2j}}{(2k+2-2j)!}\alpha^{k+1-j}\beta^j.$$

Wenn k gerade ist und $\alpha = \beta = \pi$, dann ist die linke Seite gleich 0, also beinhaltet diese Formel keine Werte der Riemannschen Zetafunktion.

Wenn k ungerade ist und $\alpha = \beta = \pi$, so

$$\zeta(2k+1) = (2\pi)^{2k}\pi\sum_{j=0}^{k+1}(-1)^{j+1}\frac{B_{2j}}{(2j)!} \times \frac{B_{2k+2-2j}}{(2k+2-2j)!} = 2\sum_{j=1}^{\infty}\frac{j^{-(2k+1)}}{e^{2\pi j}-1}$$

(die letzte Summation ist eigentlich eine zweifache unendliche Reihe mit Bernoulli-Zahlen).

Obiger Spezialfall wurde von Lerch im Jahr 1901 gezeigt.

Die allgemeine Ramanujan-Formel wurde zuerst von Malurkar (1925) bewiesen. Viele andere Mathematiker entdeckten diese Formeln erneut und/oder bewiesen sie, darunter Grosswald (1970, 1972) und Smart Katayama, Riesel, Rao, Zhang, Berndt und Sitaramachandara. Dies wird in den Büchern von Berndt sowie Smart und Katayama aus dem Jahr 1973 diskutiert.

Ein Spezialfall ist:

$$\zeta(3) = \frac{7\pi^3}{180} - \frac{1}{\pi}\sum_{j=1}^{\infty}\frac{1}{j^4} \times \frac{2\pi j}{e^{2\pi j}-1}.$$

Im Jahr 1954 bildete Margrethe Munthe Hjornaes die folgenden Reihenentwicklungen für $\zeta(2)$, $\zeta(3)$:

$$\zeta(2) = 3\sum_{j=1}^{\infty}\frac{1}{j^2\binom{2j}{j}},$$
$$\zeta(3) = \frac{5}{2}\sum_{j=1}^{\infty}\frac{(-1)^{j-1}}{j^3\binom{2j}{j}}.$$

Melzak gab (siehe Seite 85 vom Band I seines Buchs von 1973) die obige Formel für $\zeta(2)$ sowie die folgende für $\zeta(3)$ an, wobei er Teleskop-Streichungen verwendete:

$$\zeta(3) = \sum_{j=1}^{\infty} (-1)^{j+1} \frac{[(j-1)!]^2}{(3j-2)!} \left[\frac{1}{(2j-1)^2} + \frac{5}{12j(3j-1)} \right].$$

Die Reihe für $\zeta(2)$ war auch von COMTET (1974), Seite 89 angegeben worden.

Diese Formeln wurden erneut (und unabhängig) von APÉRY (1979) ermittelt. Er verwendete die Entwicklung von $\zeta(3)$ um zu beweisen, dass die Zahl irrational ist. Diese Entdeckung war eine große Sensation. In den Worten von VAN DER POORTEN (1978/9), „ein Beweis, den Euler verfehlte...". Man sollte es nicht versäumen, VAN DER POORTENS Artikel zu lesen, den er während seines Aufenthalts an der Queen's University verfasste. Eine andere Formel derselben Art ist:

$$\zeta(4) = \frac{\pi^4}{90} = \frac{36}{17} \sum_{j=1}^{\infty} \frac{1}{j^4 \binom{2j}{j}}.$$

(5) Die Zahl

$$\gamma = \lim_{n\to\infty} [(1 + \frac{1}{2} + \cdots + \frac{1}{n}) - \log n]$$

ist eine mathematische Konstante, die man *Mascheronis Konstante* oder *Eulers Konstante* nennt:

$$\gamma = 0{,}577215665\ldots$$

Es ist unbekannt, ob γ eine irrationale Zahl ist. HARDY sagte, er würde seinen Lehrstuhl in Cambridge aufgeben, wenn irgendjemand beweisen könnte, dass γ irrational ist—auch eine Weise um auszudrücken, dass dies ein sehr schwieriges Problem war (und dass er sich in Cambridge sicher im Sattel fühlte).

Es gibt viele Ausdrücke, die γ beinhalten und die sich durch die Gamma-Funktion ableiten lassen.

In einem Brief an GOLDBACH von 1779 definierte EULER die Gamma-Funktion $\Gamma(z)$ durch

$$\Gamma(z) = \frac{1}{z} \prod_{n=1}^{\infty} \left[\left(1 + \frac{1}{n}\right)^z \left(1 + \frac{z}{n}\right)^{-1} \right]$$

(gültig für jede komplexe Zahl z außer $0, -1, -2, \ldots$). Die Gamma-Funktion ist überall holomorph, außer an obigen Punkten, wo sie einfache Pole besitzt. EULER fand auch die folgende Integraldarstellung von $\Gamma(x)$:

$$\Gamma(x) = \int_0^\infty e^{-t} t^{x-1} dt,$$

dabei ist x reell und positiv. Eulers Konstante ist $\gamma = -\Gamma'(1)$.

Dirichlet gab im Jahr 1836 den folgenden Integralausdruck an:

$$\gamma = \int_0^\infty \left(\frac{-1}{1+t} - \frac{1}{e^t} \right) \frac{1}{t}\, dt.$$

Eulers Konstante ist auch mit der Riemannschen Zetafunktion verwandt:

$$\gamma = \lim_{s \to 1} \frac{\zeta(s) - 1}{s - 1}.$$

Mertens (1874) wiederum stellte eine Verbindung mit der Verteilung der Primzahlen her und zeigte, dass

$$\gamma = \lim_{x \to \infty} \left[\sum_{p \le x} \frac{1}{\log(1 - \frac{1}{p})} - \log \log x \right]$$

(wobei sich die obige Summe auf alle Primzahlen $p \le x$ bezieht). Dies lässt sich besser schreiben als

$$\frac{e^{-\gamma}}{\log x} \sim \prod_{p \le x} \left(1 - \frac{1}{p} \right) \quad \text{(asymptotisch mit } x \to \infty\text{)}.$$

Ein leicht verständlicher Beweis dieser Formel findet sich im Buch von Hardy und Wright (1938). Es lohnt sich vielleicht im Zusammenhang mit der Gamma-Funktion auch zu erwähnen, dass

$$\pi = \left[\Gamma\left(\frac{1}{2} \right) \right]^2,$$

was nichts Anderes als ein Spezialfall der von Euler entdeckten Funktionalgleichung ist:

$$\Gamma(x)\Gamma(1-x) = \frac{\pi}{\sin \pi x}.$$

(6) Glaisher wies auf einige Kuriositäten von Zahlen mit unterschiedlichen Darstellungen hin:

$$\sqrt{\frac{1{,}010001000001000000001\ldots}{1{,}2002000020000002\ldots}} = \frac{(1{,}01)(1{,}0001)(1{,}000001)\ldots}{(1{,}1)(1{,}001)(1{,}00001)\ldots},$$

$$\frac{1}{11} + \frac{1}{111} + \frac{1}{1111} + \frac{1}{11111} + \cdots$$
$$= \frac{1}{10} + \frac{1}{1100} + \frac{1}{110000} + \frac{1}{111000000} + \frac{1}{111000000000} + \cdots,$$

und

$$\log 2 = 1 - \frac{1}{2}\sum_{j=2}^{\infty} \frac{(-1)^{j-1}}{j} S_j$$

mit

$$S_j = \frac{1}{3^j} + \frac{1}{2}\left(\frac{1}{5^j} + \frac{1}{7^j}\right) + \frac{1}{4}\left(\frac{1}{9^j} + \frac{1}{11^j} + \frac{1}{13^j} + \frac{1}{15^j}\right) + \frac{1}{8}\left(\frac{1}{17^j} + \cdots + \frac{1}{31^j}\right) + \cdots .$$

(7) Im Jahr 1974 betrachtete SHANKS die zwei Zahlen

$$\alpha = \sqrt{5} + \sqrt{22 + 2\sqrt{5}}$$

$$\beta = \sqrt{11 + 2\sqrt{29}} + \sqrt{16 - 2\sqrt{29} + 2\sqrt{55 - 10\sqrt{29}}}.$$

Die Zahlen sind beide auf 25 Dezimalstellen gleich

$$7{,}38117594089565797098726 6.$$

aber sind sie identisch? Obwohl es unglaublich scheint, es gilt $\alpha = \beta$. Es ist nämlich $\alpha = \beta = 4x - 1$, wobei x die größte Nullstelle des Polynoms

$$f(X) = X^4 - X^3 - 3X^2 + X + 1$$

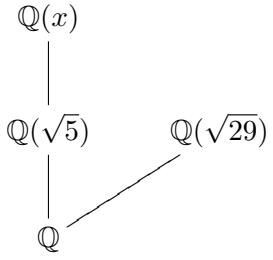
ist. SHANKS gab die folgende Erklärung an. Die Galois-Gruppe von $f(X)$ ist die oktische Symmetriegruppe des Quadrats, das von den zwei Elementen σ und τ mit den Relationen $\sigma^2 = 1$, $\tau^4 = 1$, $\sigma\tau\sigma = \tau^3$ generiert wird (hier bezeichnet 1 den Identitätsautomorphismus).

Die Resolvente von $f(X)$ ist das Polynom

$$g(X) = X^3 - 8X - 7 = (X + 1)(X^2 - X - 7).$$

Die Polynome $f(X)$, $g(X)$ haben dieselbe Diskriminante $5^2 \cdot 29$.

Der Körper $\mathbb{Q}(x)$ enthält $Q(\sqrt{5})$, jedoch nicht $Q(\sqrt{29})$.



Die Zahl x lässt sich durch jede Nullstelle z der Resolventen $g(X)$ ausdrücken. Wenn $z = -1$, dann $x = \frac{\alpha+1}{4}$. Wenn $z = \frac{1+\sqrt{29}}{2\sqrt{2}}$, dann $x = \frac{\beta+1}{4}$, also $\alpha = \beta$.

In einem Brief (auf den 23. August 1984 datiert) schlug AGOH eine einfachere Methode vor, um derartige Identitäten zu erhalten.

Es seien a, b ganze Zahlen mit $a \geq 0$, $b \geq 0$ und derart, dass $a^2 \geq 4b$. Seien $y = a - 2\sqrt{b} \geq 0$ und $k = 2ay - y^2$. Dann,

$$k = 2ay - y^2 = y(2a - y) = (a - 2\sqrt{b})(a + 2\sqrt{b}) = a^2 - 4b \geq 0.$$

Damit,

$$2a + 2\sqrt{k} = 2a - y + y + 2\sqrt{2ay - y^2} = (\sqrt{2a - y} + \sqrt{y})^2.$$

Dies ergibt

$$\sqrt{2a + 2\sqrt{k}} = \sqrt{2a - y} + \sqrt{y}$$

(das Minuszeichen kann man außer Acht lassen).

Daher,

$$\sqrt{k} + \sqrt{2a + 2\sqrt{k}} = \sqrt{2a - y} + \sqrt{k} + \sqrt{y} = \sqrt{2a - y} + \sqrt{k + y + 2\sqrt{ky}}.$$

Das Ergebnis folgt nun aus

$$\begin{aligned} ky &= (a^2 - 4b)a - 2(a^2 - 4b)\sqrt{b}\sqrt{a^2 - 4b} + \sqrt{2a + 2\sqrt{a^2 - 4b}} \\ &= \sqrt{a + 2\sqrt{b}} \\ &\qquad + \sqrt{a^2 - 4b + a - 2\sqrt{b} + 2\sqrt{(a^2 - 4b)a - 2(a^2 - 4b)\sqrt{b}}}. \end{aligned}$$

Wenn man zum Beispiel $a = 11$, $b = 29$ nimmt, erhält man Shanks' Identität.

Die Wahl von $a = 5$, $b = 3$ führt auf die gleiche Weise zu

$$\sqrt{13} + \sqrt{10 + 2\sqrt{13}} = \sqrt{5 + 2\sqrt{3}} + \sqrt{18 - 2\sqrt{3} + 2\sqrt{65 - 26\sqrt{3}}}.$$

Verschachtelte Wurzeln—die einen Alptraum für Setzer bedeuten—sind Gegenstand eines Artikels von LANDAU (1994).

4 Ein kurzer historischer Abriss

Eine vorzügliche Beschreibung der geschichtlichen Entwicklung der Theorie der transzendenten Zahlen findet sich in WALDSCHMIDTs Vorlesung am Séminaire d'Historie des Mathématiques in Paris von 1983.

Der folgende kurze Bericht gibt einen Teil des Inhalts dieser Vorlesung in einer etwas knapp gehaltenen Darstellung wieder.

Erste Phase Der Ursprung dieser Studien lässt sich bis zum Problem der „Quadratur des Kreises" zurückverfolgen. Also mit Zirkel und Lineal die Seite a eines Quadrates zu konstruieren, der dieselbe Fläche wie ein Kreis mit Radius 1 hat: $a^2 = \pi$, also $a = \sqrt{\pi}$.

Ein schöner und informativer Bericht zu diesem Problem und Eigenschaften von π findet sich in der der Zahl π gewidmeten Spezialausgabe der Zeitschrift „Petit Archimède" aus dem Jahr 1980.

Eine weitere Motivation war die Entdeckung von PYTHAGORAS, dass $\sqrt{2}$ keine rationale Zahl ist.

LEIBNIZ war anscheinend der erste Mathematiker, der den Begriff „transzendente Zahl" verwendete (1704).

Im Jahr 1737 bewies EULER mithilfe von Kettenbrüchen, dass e^2 und damit auch e irrational ist.

Wenn α, β zwei algebraische Zahlen ungleich Null und multiplikativ unabhängig sind (d.h., wenn aus $\alpha^r \beta^s = 1$ mit ganzen Zahlen r, s folgt $r = s = 0$), dann ist $\frac{\log \alpha}{\log \beta}$ sicher eine irrationale Zahl; im Jahr 1748 vermerkte EULER ohne Beweis, dass $\frac{\log \alpha}{\log \beta}$ eine transzendente Zahl darstellt. Dies wurde erneut, allerdings viel später von HILBERT untersucht.

Im Jahr 1755 vermutete EULER, dass π transzendent ist.

LAMBERT zeigte 1761, dass π irrational ist. Er bewies eigentlich sogar, dass wenn r eine rationale Zahl verschieden von Null ist, dann sind $\tan r$ und e^r irrational.

Als Nächstes zeigte LEGENDRE, dass π^2 irrational ist (1794) und FOURIER gab im Jahr 1815 einen einfachen Beweis für die Irrationalität von e an, wobei er die Reihenentwicklung von e verwendete (siehe STAINVILLE). Im Jahr 1840 erweiterte LIOUVILLE diese Methode um zu zeigen, dass e und e^2 irrational und nicht algebraisch vom Grad 2 sind.

Zweite Phase Diese Phase beinhaltet die ersten Arbeiten, die diophantische Approximation verwenden.

Im Jahr 1842 benutzte DIRICHLET das Schubfachprinzip, um zu Ergebnissen zur Approximation irrationaler Zahlen durch rationale Zahlen zu gelangen.

In seinen berühmten Artikeln von 1844 und 1851 konstruierte LIOUVILLE eine Klasse transzendenter Zahlen, die man heute Liouville-Zahlen nennt. Diese enthalten zum Beispiel die Zahlen

$$\sum_{n=0}^{\infty} \frac{k_n}{a^{n!}},$$

wobei $a_n \geq 2$, $0 \leq k_n \leq a-1$ für jedes $n \geq 0$ und $k_n \neq 0$ für unendlich viele Indizes n. Insbesondere ist

$$\sum_{n=0}^{\infty} \frac{1}{10^{n!}}$$

eine transzendente Zahl.

Diese Ergebnisse basieren auf Liouvilles Ungleichung zur Approximation algebraischer Zahlen durch rationale Zahlen.

In diese Phase gehören auch die mengentheoretischen Ergebnisse von CANTOR. Er zeigte 1874, dass $\mathbb{R}$ und $\mathbb{C}$ überabzählbare Mengen sind, während die Menge aller algebraischen Zahlen abzählbar ist. Somit ist die Menge aller transzendenten Zahlen nicht abzählbar.

Dritte Phase Die Methoden der diophantischen Approximation wurden verfeinert und erlaubten die Beweise wichtiger Resultate.

Im Jahr 1873 zeigte HERMITE, dass e transzendent ist. Dies war die erste Zahl (nicht-konstruiert), die als transzendent nachgewiesen wurde.

Im Jahr 1882 bewies LINDEMANN, dass π transzendent ist. Dies implizierte natürlich, dass sich π nicht durch Radikale ausdrücken lässt und daher π und $\sqrt{\pi}$ nicht mit Lineal und Zirkel konstruierbar sind. Das lange Zeit offene Problem der Quadratur des Kreises hatte damit eine negative Lösung gefunden.

In seinem Artikel gab LINDEMANN weitere Resultate ohne Beweis an. Diese wurden kurze Zeit später von HERMITE und WEIERSTRASS erbracht. Dies ist Lindemanns und Hermites Satz: *Wenn α eine von Null verschiedene algebraische Zahl ist, dann ist e^{α} transzendent.*

Eine äquivalente Aussage ist die folgende: *Wenn α eine algebraische Zahl ist, $\alpha \neq 0, 1$, dann ist* $\log \alpha$ *transzendent.*

Der verallgemeinerte Satz von Lindemann und Weierstrass besagt: *Wenn $\alpha_1, \ldots, \alpha_n$ linear unabhängige algebraische Zahlen über $\mathbb{Q}$ sind, dann sind $e^{\alpha_1}, \ldots, e^{\alpha_n}$ algebraisch unabhängig.*

Diese Sätze wurden von Lindemann lediglich vermerkt, aber nicht bewiesen. Er wandte sich stattdessen Fermats letztem Satz zu und veröffentlichte ein Buch mit einem allgemeineren Beweis des Satzes. Unglücklicherweise war sein Beweis falsch.

Im Jahr 1886 untersuchte Weierstrass die Frage, ob eine transzendente Funktion (wie die Exponential- oder trigonometrischen Funktionen) transzendente Werte an algebraischen Punkten annehmen (von einigen wenigen Ausnahmen abgesehen). Er zeigte, dass dies für spezielle Funktionen der Fall ist, aber für beliebige transzendente Funktionen nicht stimmt.

Vierte Phase Im Jahr 1900 fragte Hilbert in seinem siebten Problem, ob folgende Aussage wahr ist: wenn α eine algebraische Zahl ist $(\alpha \neq 0, 1)$ und β irrational und algebraisch, dann ist α^β transzendent.

Dies wurde von Hilbert als sehr schweres Problem angesehen. Er ging in einem Seminar in Göttingen um 1920 herum sogar so weit zu sagen, dass keiner der Anwesenden lang genug leben würde um zu erleben, dass diese Frage beantwortet würde.

Und doch gelang es 1934 Gel'fond und Schneider unabhängig voneinander und mit verschiedenen Methoden, Hilberts siebtes Problem im positiven Sinne zu lösen.

Insbesondere sind $e^\pi = (-1)^{-i}$ und die Zahl $\sqrt{2}^{\sqrt{2}}$ transzendente Zahlen.

Zur selben Zeit gab es wichtige Fortschritte in der Theorie der diophantischen Approximation durch Thue (1909), Siegel (1921) und Roth (1955) mit Anwendungen auf diophantische Gleichungen und transzendente Zahlen.

Erst vor relativ kurzer Zeit (beginnend im Jahr 1968) veröffentlichte Baker eine Reihe grundlegender Artikel über algebraische Unabhängigkeit von Logarithmen, die als Korollare die meisten der klassischen Resultate enthielten (siehe sein Buch, 1975).

Die Klassifikation transzendenter Zahlen war von Mahler im Jahr 1932 begonnen worden, ist aber noch bei Weitem nicht abgeschlossen.

Zur besseren Übersicht für den Leser fasse ich einige Resultate zu den oben erwähnten Zahlen zusammen.

Zahl	*Irrational*	*Transzendent*
e	Ja, Beweis von Euler (1737)	Ja, Beweis von Hermite (1873)
π	Ja, Beweis von Lambert (1761)	Ja, Beweis von Lindemann (1882)
γ	?	?
$\sqrt{2}^{\sqrt{2}}$	Ja	Ja, Spezialfall von Gel'fond und Schneiders Satz (1934)
$\zeta(3)$	Ja, Beweis von Apéry (1979)	?

Die Frage nach der Irrationalität von Eulers Konstante γ gibt große Rätsel auf. Und das, obwohl es viele klassische wie neue Formeln gibt, die γ enthalten. Ein weiteres Problem, das man nach Apérys Beweis der Irrationalität von $\zeta(3)$ untersuchte ist es festzustellen, ob $\zeta(n)$ für ungerade positive ganze Zahlen n irrational ist. Wenn $n = 2k$ gerade ist, so besagt die Formel von Euler

$$\zeta(2k) = (-1)^{k-1} \frac{(2\pi)^{2k}}{2(2k)!} B_{2K},$$

dass $\zeta(2k)$ transzendent ist, da π transzendent ist. Trotz vieler Versuche gelang es den Mathematikern nicht, die Methode Apérys geeignet anzupassen um zu beweisen, dass $\zeta(5)$ oder allgemeiner $\zeta(2k+1)$ für $k > 1$ irrational ist. Ein Durchbruch bezüglich der Irrationalität von $\zeta(2k+1)$ gelang Rivoal in seiner Dissertation (siehe seinen Artikel von 2001). Rivoal bewies nebst weiteren Resultaten, dass es für $k \geq 1$ in der Menge $\{1, \zeta(3), \zeta(5), \ldots, \zeta(2k+1)\}$ mindestens $\frac{1}{3}\log(2k+1)$ Zahlen geben muss, die linear unabhängig über $\mathbb{Q}$ sind. Aber der Satz gab keine Auskunft darüber, welche diese Zahlen sind. Weitere Arbeiten von Rivoal sowie Rivoal und Zudilin zeigten, dass mindestens eine der Zahlen $\zeta(5), \zeta(7), \zeta(9), \zeta(11)$ irrational ist.

5 Kettenbrüche

Kettenbrüche wurden erstmals von Bombelli im Jahr 1572 im Zusammenhang mit der näherungsweisen Berechnung der Quadratwurzeln von Nicht-Quadratzahlen eingeführt. Sie spielen eine fundamentale Rolle bei der Approximation von Zahlen durch rationale Zahlen und es

lohnt sich daher, die wichtigsten Definitionen und Eigenschaften zusammenzufassen. Sämtliche Beweise zu den Aussagen lassen sich in Büchern wie PERRON (1910, 1913), KHINTCHINE (1935), NIVEN (1957) und OLDS (1963) finden.

A Allgemeines

Sei α eine positive reelle Zahl. Ich werde nun die einfache Kettenbruchentwicklung von α definieren. Sei $a_0 \geq 0$ die eindeutig bestimmte ganze Zahl derart, dass $a_0 \leq \alpha < a_0 + 1$, d.h. $a_0 = [\alpha]$ ist der ganzzahlige Anteil von α. Wenn α keine ganze Zahl ist, so $0 < \alpha - a_0 < 1$. Sei $\alpha_1 = \frac{1}{\alpha - a_0}$. Dieser Prozess wird mit α_1 wiederholt und führt nach und nach zu Zahlen α_1, α_2, ... Der Abbruch erfolgt in einer endlichen Anzahl von Schritten genau dann, wenn α eine rationale Zahl ist. Die Notation $\alpha = [a_0, a_1, a_2, \dots]$ bedeutet, dass

$$\alpha = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cdots}}.$$

Dies ist die *einfache Kettenbruchentwicklung von* α. [Sie heißt „einfach“, da die „Zähler“ alle gleich 1 sind; Ich werde keine Kettenbrüche betrachten, die nicht einfach sind, außer einiger Beispiele in §3.]

Wenn $a_0 \geq 0$, $a_1, a_2, \dots$ positive ganze Zahlen sind, so sei umgekehrt $r_n = \frac{h_n}{k_n} = [a_0, a_1, \dots, a_n]$, wobei $1 \leq h_n, k_n$, $\mathrm{ggT}(h_n, k_n) = 1$. Dann

$$r_0 < r_2 < r_4 < \cdots \qquad \cdots < r_5 < r_3 < r_1,$$

und die folgenden Grenzwerte existieren und sind gleich irgendeiner irrationalen Zahl $\alpha = \lim r_{2n} = \lim r_{2n-1}$. Die einfache Kettenbruchentwicklung von α ist

$$\alpha = [a_0, a_1, a_2, \dots].$$

Die Konvergenten $r_n = \frac{h_n}{k_n}$ von α haben wichtige Eigenschaften einer guten Approximation von α. Genauer:

5.1. Für jedes $n \geq 1$: $|\alpha - \frac{h_n}{k_n}| < \frac{1}{k_n k_{n+1}} < \frac{1}{k_n^2}$.

5.2. Für jedes $n \geq 1$: $|\alpha k_n - h_n| < |\alpha k_{n-1} - h_{n-1}|$, damit

$$\left|\alpha - \frac{h_n}{k_n}\right| < \left|\alpha - \frac{h_{n-1}}{k_{n-1}}\right|.$$

5.3. Für jedes $n \geq 1$ ist die Konvergente $\frac{h_n}{k_n}$ die „beste Approximation“ mit Nenner höchstens gleich k_n, d.h. wenn $|b\alpha - a| < |k_n\alpha - h_n|$, dann $b > k_n$ und somit gilt, dass wenn $|\alpha - \frac{a}{b}| < |\alpha - \frac{h_n}{k_n}|$, dann $b > k_n$.

Umgekehrt:

5.4. Wenn $\frac{a}{b}$ eine bestmögliche Approximation von α ist, dann ist $\frac{a}{b}$ gleich einer Konvergenten $\frac{h_n}{k_n}$ mit $n \geq 0$.

B Periodische Kettenbrüche

Ein unendlicher einfacher Kettenbruch

$$\alpha = [a_0, a_1, a_2, \dots]$$

ist *periodisch*, wenn es $n_0 \geq 0$, $t > 0$ derart gibt, dass $a_{n+t} = a_n$ für jedes $n \geq n_0$. Wähle die kleinsten solchen t und n_0 und schreibe

$$\alpha = [a_0, \dots, a_{n_0-1}, \overline{a_{n_0}, a_{n_0+1}, \dots, a_{n_0+t-1}}].$$

$(a_0, \dots, a_{n_0-1})$ ist die *Vorperiode*, n_0 die Länge der Vorperiode, $(a_{n_0}, a_{n_0+1}, \dots, a_{n_0+t-1})$ die *Periode* und t die Länge der Periode. Wenn $n_0 = 0$, dann ist der Kettenbruch *rein periodisch*. Aufgrund der minimalen Wahl von n_0 ist $a_{n_0-1} \neq a_{n_0+t-1}$.

Ich werde nun die Kettenbruchentwicklung von reell quadratischen irrationalen Zahlen α untersuchen. Jede solche Zahl lässt sich in der Form $\alpha = \frac{p \pm \sqrt{D}}{q}$ schreiben, wobei p, $q \neq 0$, $D > 1$ ganze Zahlen sind und D kein Quadrat ist. Wegen $\frac{p-\sqrt{D}}{q} = \frac{-p+\sqrt{D}}{-q}$ kann immer angenommen werden, dass α sich in der Form $\frac{p+\sqrt{D}}{q}$ befindet.

Darüberhinaus gilt, dass wenn $\frac{D-p^2}{q}$ keine ganze Zahl ist, sagen wir $\frac{D-p^2}{q} = \frac{c}{d}$, so $\alpha = \frac{dp+\sqrt{Dd^2}}{dq}$, und nun ist $\frac{Dd^2-d^2p^2}{dq} = d\frac{D-p^2}{q} = c$ eine ganze Zahl.

Also kann man ohne Einschränkung der Allgemeinheit annehmen, dass $\alpha = \frac{p+\sqrt{D}}{q}$ und q Teiler von $D - p^2$ ist.

Euler bewies (1737):

5.5. Wenn α eine unendliche periodische einfache Kettenbruchentwicklung hat, dann ist α eine reell quadratische irrationale Zahl.

Das wichtigste Ergebnis über periodische Kettenbrüche ist die Umkehrung. Sie wurde von Lagrange im Jahr 1770 bewiesen:

5.6. Die Kettenbruchentwicklung einer jeden reell quadratischen irrationalen Zahl α ist periodisch.

Die goldene Zahl $\frac{\sqrt{5}+1}{2}$ und $\sqrt{2}$ haben beispielsweise die folgenden Kettenbruchentwicklungen:

$$\frac{\sqrt{5}+1}{2} = [1, 1, 1, \dots],$$
$$\sqrt{2} = [1, 2, 2, 2, \dots].$$

Es ist wichtig anzumerken, dass die einfachen Kettenbruchentwicklungen einer jeden reellen algebraischen Zahl mit Grad höher als zwei zufällige Quotienten zu haben scheinen, die nicht beschränkt bleiben. Eine umfassende numerische Berechnung und statistische Analyse befindet sich im Artikel von Brent, van der Poorten und te Riele (1996).

Das nächste Ergebnis betrifft rein periodische Kettenbrüche.

Die Konjugierte von $\alpha = \frac{p+\sqrt{D}}{q}$ wird mit $\alpha' = \frac{p-\sqrt{D}}{q} = \frac{-p+\sqrt{D}}{-q}$ bezeichnet.

5.7. Die einfache Kettenbruchentwicklung der reell quadratischen irrationalen Zahl α ist genau dann rein periodisch, wenn $1 < \alpha$ und $-1 < \alpha' < 0$. Darüberhinaus besteht die Vorperiode für $1 < \alpha$ und $\alpha' < -1$ aus nur einem Element.

Im Jahr 1828 bewies Galois:

5.8. Sei $\alpha = \frac{p+\sqrt{D}}{q}$ mit ganzen Zahlen p, $q \neq 0$, $D > 0$, D kein Quadrat, und q teile $D^2 - p$. Sei $\alpha' = \frac{-p+\sqrt{D}}{-q} = \frac{p-\sqrt{D}}{q}$ ihre Konjugierte. Wenn $\alpha = [\overline{a_0, a_1, \dots, a_{t-1}}]$, dann $\frac{1}{\alpha'} = [\overline{a_{t-1}, a_{t-2}, \dots, a_1, a_0}]$.

Im selben Jahr fand Legendre das folgende Resultat für die einfache Kettenbruchentwicklung von $\sqrt{D}$, wobei D eine nicht-quadratische positive ganze Zahl ist:

5.9. $\sqrt{D} = [a_0, \overline{a_1, a_2, \dots, a_2, a_1, 2a_0}]$, d.h. die Vorperiode hat die Länge 1, die Periode besteht aus dem symmetrischen Teil gefolgt vom Doppelten des Terms in der Vorperiode (man beachte, dass die Anzahl von Termen in der Periode gerade oder ungerade sein kann).

Das folgende Ergebnis ist interessant:

5.10. Wenn die Kettenbruchentwicklung von $\sqrt{D}$ eine Periode mit einer ungeraden Anzahl von Termen besitzt, dann ist D die Summe zweier Quadrate.

FERMAT betrachtete die Gleichung $X^2 - DY^2 = 1$ (wobei $D > 0$ eine quadratfreie ganze Zahl ist) und behauptete, dass sie unendlich viele Lösungen in natürlichen Zahlen besitzt. Dies wurde erstmalig von LAGRANGE im Jahr 1770 unter Verwendung der Theorie der Kettenbrüche bewiesen.

5.11. Sei $D > 0$ eine quadratfreie ganze Zahl. Seien $\frac{h_n}{k_n}$ die Konvergenten des Kettenbruchs von $\sqrt{D}$ und t die Länge der Periode.

(1) Die Lösungen von $X^2 - DY^2 = 1$ in natürlichen Zahlen sind $(1, 0)$ und (h_{nt-1}, k_{nt-1}) für gerades t und (h_{2nt-1}, k_{2nt-1}) für t ungerade, jeweils für alle $n \geq 1$. Damit besitzt die Gleichung unendlich viele Lösungen.

(2) Wenn t gerade ist, dann hat die Gleichung $X^2 - DY^2 = -1$ keine Lösung in natürlichen Zahlen, während im Falle eines ungeraden t die Paare (h_{nt-1}, k_{nt-1}) für alle ungeraden $n \geq 1$ Lösungen sind.

(3) Für alle $n \geq 1$: $h_{nt-1} + k_{nt-1}\sqrt{D} = (h_{t-1} + + k_{t-1}\sqrt{D})^n$.

C Einfache Kettenbrüche von π und e

Ich wende mich nun den Zahlen π und e zu.

Wie bereits in §3 bemerkt, ist die einfache Kettenbruchentwicklung von π

$$\pi = [3, 7, 15, 1, 292, 1, 1, 1, 2, 1, 3, 1, \dots].$$

Die Konvergenten sind

$$\frac{3}{1}, \frac{22}{7}, \frac{133}{106}, \frac{355}{113}, \frac{103993}{33102}, \frac{104348}{33215}, \frac{208341}{66317}, \frac{3123689}{99532}, \dots.$$

Nach **(5.3)** sind die Konvergenten die beste Approximation für π. Für einige Konvergenten ist die Approximation tatsächlich viel besser als erwartet. So ist

$$\left|\pi - \frac{22}{7}\right| \approx \frac{1}{10^3},$$

$$\left|\pi - \frac{333}{106}\right| \approx \frac{8}{10^5},$$

$$\left|\pi - \frac{355}{113}\right| \approx \frac{26}{10^8}.$$

Der Wert $\frac{22}{7}$ war bereits ARCHIMEDES bekannt, während ADRIANUS METIUS (1571–1635) die Werte $\frac{133}{106}$ und $\frac{355}{113}$ kannte. Bereits im Jahr 1685 hatte WALLIS die 34ste Konvergente berechnet. Es sei auch erwähnt, dass die Konvergenten

$$\frac{h_{12}}{k_{12}} = \frac{5419351}{1725033}, \qquad \frac{h_{27}}{k_{27}} = \frac{428224593349304}{136308121570117}$$

von R. ARIMA, dem Herrscher von Kurume in Japan aus dem Jahr 1769 stammen und diese eine Approximation für π mit einem Fehler von etwa 10^{-29} darstellen.

Wie bereits in §3 erwähnt, gab EULER einfache unendliche Kettenbrüche für

$$\frac{e^{2/a}+1}{e^{2/a}-1} \quad (\text{für } a \geq 1)$$

und auch für e an. Ich werde den schönen Beweis hier vorstellen.

5.12. Wenn $a \geq 1$ irgendeine ganze Zahl ist, dann

$$\frac{e^{2/a}+1}{e^{2/a}-1} = [a, 3a, 5a, 7a, \dots].$$

Insbesondere,

$$\frac{e^2+1}{e^2-1} = [1, 3, 5, 7, \dots],$$
$$\frac{e+1}{e-1} = [2, 6, 10, 14, \dots].$$

Beweis. Um die Entwicklung zu erhalten, betrachte ich für jedes $m \geq 0$ die Reihe

$$S_m = \sum_{i=0}^{\infty} \frac{2^m (m+i)!}{i!(2m+2i)!} \left(\frac{1}{a}\right)^{2i+m}.$$

Sie konvergiert, wie man im Vergleich mit der Reihe

$$\sum_{i=0}^{\infty} \frac{2^m}{i!} \left(\frac{1}{a}\right)^{2i+m} = \left(\frac{2}{a}\right)^m e^{1/a^2}$$

sehen kann.

Man beachte, dass

$$S_0 = \sum_{i=0}^{\infty} \frac{1}{(2i)!} \left(\frac{1}{a}\right)^{2i} = \frac{e^{1/a} + e^{-1/a}}{2},$$
$$S_1 = \sum_{i=0}^{\infty} \frac{1}{(2i+1)!} \left(\frac{1}{a}\right)^{2i+1} = \frac{e^{1/a} - e^{-1/a}}{2}.$$

Durch eine einfache Rechnung sieht man, dass

$$S_m - (2m+1)aS_{m+1} = S_{m+2}$$

für jedes $m \geq 0$ gilt.

Sei $R_m = \frac{S_m}{S_{m+1}}$, also

$$R_0 = \frac{e^{1/a} + e^{-1/a}}{e^{1/a} - e^{-1/a}} = \frac{e^{2/a} + 1}{e^{2/a} - 1}.$$

Auch ist $R_m = (2m+1)a + \frac{1}{R_{m+1}}$, daher insbesondere

$$R_0 = a + \frac{1}{R_1}, \quad R_1 = 3a + \frac{1}{R_2}, \quad R_2 = 5a + \frac{1}{R_3}, \quad \ldots.$$

Dies zeigt wie gefordert, dass

$$\frac{e^{2/a} + 1}{e^{2/a} - 1} = [a, 3a, 5a, 7a, \ldots].$$

□

Für irgendeine positive reelle Zahl α und positive ganze Zahlen a_0, a_2, … definiere $[\alpha] = \alpha$. Man erhält durch Induktion

$$[a_0, a_1, \ldots, a_n, \alpha] = [a_0, \ldots, a_{n-1}, a_n + \frac{1}{\alpha}].$$

Euler entdeckte zunächst bei Berechnungen die Kettenbruchentwicklung der Zahl e, er gab danach einen Beweis an; der einfache Beweis unten stammt von Hurwitz (1891b):

5.13. $e = [2, 1, 2, 1, 1, 4, 1, 1, 6, \ldots]$

Beweis. Aus $\frac{e+1}{e-1} = [2, 6, 10, 14, \dots]$ folgt, dass

$$\frac{2}{e-1} = \frac{e+1}{e-1} - 1 = [1, 6, 10, 14, \dots],$$

daher $\frac{e-1}{2} = [0, 1, 6, 10, 14, \dots]$. Man muss nun $2 \times [0, 1, 6, 10, 14, \dots]$ als Kettenbruch ausdrücken.

Wenn α irgendeine reelle Zahl ist, so $2\times[0, 2a+1, \alpha] = [0, a, 1, 1, \frac{\alpha-1}{2}]$.

Tatsächlich,

$$2 \times \frac{1}{(2a+1)+\frac{1}{\alpha}} = \frac{1}{a+(\frac{1}{2}+\frac{1}{2\alpha})} = \frac{1}{a+\frac{1}{\frac{2\alpha}{\alpha+1}}}$$
$$= \frac{1}{a+\frac{1}{1+\frac{\alpha-1}{\alpha+1}}} = \frac{1}{a+\frac{1}{1+\frac{1}{\frac{\alpha-1}{2}}}} = [0, a, 1, 1, \frac{\alpha-1}{2}].$$

Ich werde diese Formel wiederholt anwenden.

Sei $\alpha = [6, 10, 14, \dots]$, dann

$$2 \times [0, 1, \alpha] = [0, 0, 1, 1, \frac{\alpha-1}{2}] = [1, 1, \frac{\alpha-1}{2}].$$

Aber

$$\frac{\alpha-1}{2} = \frac{1}{2} \times [5, 10, 14, \dots] = \frac{1}{2} \times [0, 0, 5, 10, 14, \dots]$$
$$= [0, 2 \times [0, 5, 10, 14, \dots]].$$

Nun sei $\beta = [10, 14, 18, \dots]$ und berechne

$$2 \times [0, 5, \beta] = [0, 2, 1, 1, \frac{\beta-1}{2}].$$

Wieder,

$$\frac{\beta-1}{2} = \frac{1}{2}[9, 14, 18, \dots] = [0, 2 \times [0, 9, 14, 18, \dots]].$$

So hat man bereits $e = 1 + [1, 1, 0, 0, 2, 1, 1, \frac{\beta-1}{2}] = [2, 1, 2, 1, 1, \frac{\beta-1}{2}]$. Allgemeiner, wenn $\gamma = [4m+2, 4(m+1)+2, \dots]$, dann

$$2 \times [0, 4(m-1)+1, \gamma] = [1, 1, \frac{\gamma-1}{2}]$$

und durch Induktion,

$$e = [2, 1, 2, 1, 1, 4, 1, 1, \dots, 2m, 1, 1, \dots],$$

was den Beweis abschließt. □

Mit derselben Methode bewies HURWITZ auch, dass

$$e^2 = [7, 2, 1, 1, 3, 18, 5, 1, 1, 6, 30, 8, 1, 1, 9, 42, \dots],$$

und es lässt sich einfach erkennen, dass das Muster der Quotienten durch $a_{5(m-1)+1} = 3m - 1$, $a_{5(m-1)+2} = 1$, $a_{5(m-1)+3} = 1$, $a_{5(m-1)+4} = 3m$, $a_{5m} = 12m + 6$, für $m = 1, 2, 3, \dots$ gegeben ist.

Mithilfe einer selbsterklärenden Notation schreibe ich

$$e = [2, \overline{1, 2m, 1}]_{m>1} \quad \text{und} \quad e^2 = [7, \overline{3m - 1, 1, 1, 3m, 12m + 6}]_{m\geq 1}.$$

Aus **(5.7)** folgt sofort, dass e und e^2 keine Nullstellen quadratischer Gleichungen mit ganzzahligen Koeffizienten sind.

6 Approximation durch rationale Zahlen

Die Art einer irrationalen Zahl, ob sie algebraisch oder transzendent ist, hängt davon ab, wie gut sie sich durch rationale Zahlen approximieren lässt. Das Konzept der Approximation ist für das Studium der irrationalen Zahlen somit wesentlich.

Die Leitidee dieses Abschnitts geht auf LIOUVILLE und DIRICHLET zurück. Im Jahr 1909 untersuchte THUE im Rahmen des Studiums der Lösungen gewisser Typen diophantischer Gleichungen die Ordnung der Approximation reeller algebraischer Zahlen durch rationale Zahlen. Ich werde an späterer Stelle auf diese Verbindung zurückkommen.

A Die Ordnung der Approximation

Bei den folgenden Betrachtungen werden die rationalen Zahlen geschrieben als $\frac{a}{b}$, wobei $b \geq 1$ und $\mathrm{ggT}(a, b) = 1$.

Seien $\alpha \in \mathbb{R}$, $\nu \in \mathbb{R}$, $\nu \geq 1$. Die Zahl α nennt man *approximierbar durch rationale Zahlen bis zur Ordnung* $\nu \geq 1$, wenn es $C > 0$ gibt (abhängig von α, ν) und unendlich viele rationale Zahlen $\frac{a}{b}$ derart, dass

$$\left|\alpha - \frac{a}{b}\right| < \frac{C}{b^\nu}.$$

Offensichtlich gilt, dass wenn α durch rationale Zahlen bis zur Ordnung ν approximierbar ist und $\nu \geq \nu' \geq 1$, dann ist α auch bis ν' approximierbar.

Sei $\nu(\alpha) = \sup\{\nu \in \mathbb{R} \mid \alpha \text{ ist durch rationale Zahlen bis zur Ordnung } \nu \text{ approximierbar}\}$. Damit, $1 \leq \nu(\alpha) \leq \infty$.

Man leitet sofort ab:

6.1. Sei $\alpha \in \mathbb{R}$.

(1) Für jedes $\epsilon > 0$ gibt es eine ganze Zahl $b_0 \geq 1$ derart, dass wenn $\frac{a}{b}$ eine rationale Zahl mit Nenner $b \geq b_0$ ist, dann gilt $|\alpha - \frac{a}{b}| > \frac{1}{b^{\nu(\alpha)+\epsilon}}$.

(2) Für jedes $\epsilon > 0$ gibt es $C(\alpha, \epsilon) = C > 0$ derart, dass $0 < C < 1$ und $|\alpha - \frac{a}{b}| > \frac{C}{b^{\nu(\alpha)+\epsilon}}$, für alle $\frac{a}{b} \neq \alpha$.

Eine erste einfache Anmerkung ist die folgende:

6.2. Jede rationale Zahl ist durch rationale Zahlen bis zur Ordnung 1 approximierbar (unter Verwendung irgendeiner Konstante $C > 1$), aber nicht bis zu irgendeiner Ordnung $1 + \epsilon$ ($\epsilon > 0$); daher, $\nu(\alpha) = 1$ für jedes $\alpha \in \mathbb{Q}$.

Ich werde an späterer Stelle den Satz von Liouville über die Approximation irrationaler algebraischer Zahlen durch rationale Zahlen angeben (siehe **(6.9)**).

Das Schubfachprinzip beruht auf einer sehr einfachen Idee: Wenn es mehr Dinge in einen Schrank mit Schubfächern zu verteilen gibt als Schubfächer vorhanden sind, so muss man in mindestens einem Schubfach zwei Dinge unterbringen. Dirichlet wendete das Schubfachprinzip im Jahr 1842 an. Sein Ergebnis folgt genau genommen aus **(5.2)**:

6.3. Wenn α eine reelle irrationale Zahl ist, dann ist α bis zur Ordnung 2 durch rationale Zahlen approximierbar (unter Verwendung von $C = C(\alpha, 2) = 1$); genauer gibt es unendlich viele rationale Zahlen $\frac{a}{b}$ derart, dass $|\alpha - \frac{a}{b}| < \frac{1}{b^2}$.

Mit der hier verwendeten Bezeichnungsweise: Wenn $\alpha \in \mathbb{R} \setminus \mathbb{Q}$, dann $\nu(\alpha) \geq 2$.

Diesbezüglich bestimmte Hurwitz im Jahr 1891, dass $\frac{1}{\sqrt{5}}$ die beste Konstante in Dirichlets Satz ist. Ein einfacher Beweis findet sich im Buch von Niven von 1963.

6.4. (1) Für jede reelle irrationale Zahl α gibt es unendlich viele rationale Zahlen $\frac{a}{b}$ derart, dass

$$|\alpha - \frac{a}{b}| < \frac{1}{\sqrt{5}b^2}.$$

(2) Falls jedoch $0 < C < \frac{1}{\sqrt{5}}$ und $\alpha = \frac{1+\sqrt{5}}{2}$ (die goldene Zahl), dann gibt es nur endlich viele rationale Zahlen $\frac{a}{b}$, die $|\alpha - \frac{a}{b}| < \frac{C}{b^2}$ genügen.

B Die Markoff-Zahlen

Für jede irrationale Zahl α führte PERRON im Jahr 1921 eine Invariante $M(\alpha)$ ein. Ein damit nahe verwandtes Konzept hatte MARKOFF bereits 1879 untersucht.

Sei S_α die Menge aller positiven Zahlen λ mit der Eigenschaft, dass es unendlich viele rationale Zahlen $\frac{a}{b}$ gibt, die der Ungleichung $|\alpha - \frac{a}{b}| < \frac{1}{\lambda b^2}$ genügen.

Offensichtlich gilt für $\lambda \in S_\alpha$ und $0 < \lambda' < \lambda$, dass $\lambda' \in S_\alpha$.

Sei $M(\alpha) = \sup\{\lambda \mid \lambda \in S_\alpha\}$. Nach **(6.4)**, $\sqrt{5} \in S_\alpha$; somit $\sqrt{5} \leq M(\alpha)$ für jede irrationale Zahl α. Auch gilt für die goldene Zahl,

$$M\left(\frac{\sqrt{5}+1}{2}\right) = \sqrt{5}.$$

Das folgende Resultat ist leicht zu zeigen:

6.5. Sei $\alpha = [a_1, a_1, a_2, \dots]$. Dann gilt $M(\alpha) < \infty$ genau dann, wenn die Folge $(a_n)_{n\geq 0}$ beschränkt ist.

Obiges Resultat besagt, dass irrationale Zahlen, die Kettenbruchentwicklungen mit unbeschränkten Quotienten besitzen, beliebig nahe Approximierungen durch Konvergenten erlauben.

Ich werde mich nun für alle irrationalen Zahlen α den möglichen Werten von $M(\alpha)$ zuwenden.

Die reellen Zahlen α und α' heißen *äquivalent* ($\alpha \sim \alpha'$), wenn es ganze Zahlen a, b, c und d derart gibt, dass $ad - bc = \pm 1$ und $\alpha' = \frac{a\alpha+b}{c\alpha+d}$. Es folgt, dass $\alpha = \frac{-d\alpha'+b}{c\alpha'-a}$, so dass es sich tatsächlich um eine Äquivalenzrelation handelt. Darüberhinaus ist jede Äquivalenzklasse entweder endlich oder abzählbar unendlich.

HURWITZ gelangte im Jahr 1891 zu folgender Aussage:

6.6. Wenn $\alpha \sim \alpha'$, dann $M(\alpha) = M(\alpha')$.

Im Allgemeinen ist die Umkehrung von **(6.6)** nicht wahr. Für die goldene Zahl trifft sie allerdings zu:

6.7. Wenn α eine irrationale Zahl ist, die nicht äquivalent zur goldenen Zahl ist, dann ist $M(\alpha) \geq \sqrt{8}$.

Es gibt noch keine vollständige Beschreibung der Werte, die von $M(\alpha)$ angenommen werden. Die Untersuchung der Werte $M(\alpha) < 3$ hängt ab von Markoffs Gleichung

$$X^2 + Y^2 + Z^2 = 3XYZ.$$

Markoff wies 1879 die Existenz unendlich vieler natürlicher Zahlen x mit der Eigenschaft nach, dass es natürliche Zahlen y, z derart gibt, dass (x, y, z) eine Lösung der obigen Gleichung ist.

Diese Zahlen sind

$$x = 1, 2, 5, 13, 29, 34, 89, 169, 194, 233, 433, \ldots$$

(die *Markoff-Zahlen*).

Perron zeigte:

Die Werte $M(\alpha)$ kleiner als 3 sind genau die Zahlen $\frac{\sqrt{9x^2-4}}{x}$ für alle Markoff-Zahlen $x = 1, 2, 5, \ldots$. Es sind somit

$$\sqrt{5} < \sqrt{8} < \frac{\sqrt{221}}{5} < \frac{\sqrt{1521}}{13} < \frac{\sqrt{7569}}{29} < \cdots$$

und es ist

$$\lim_{x\to\infty} \frac{\sqrt{9x^2-4}}{x} = 3.$$

Darüberhinaus, $M(\alpha) = \frac{1}{x}\sqrt{9x^2-4}$ genau dann, wenn α äquivalent zu $\frac{1}{2x}(\sqrt{9x^2-4} + x + \frac{2y}{z})$ ist, wobei (x, y, z) eine Lösung von Markoffs Gleichung darstellt. Es folgt, dass wenn $M(\alpha) < 3$, dann gilt $\alpha \sim \alpha'$ genau dann, wenn $M(\alpha) = M(\alpha')$. Zudem ist $M(\alpha) \geq 3$, wenn α keine quadratisch irrationale Zahl ist.

Die Zahlen mit $M(\alpha) = 3$ sind diejenigen, die äquivalent zu

$$[2, 2, 1, 1, \ldots, 1, 2, 2, 1, 1, \ldots, 1, 2, 2, 1, 1, \ldots, 1, \ldots]$$

sind, mit Blöcken von m_1, m_2, m_3, ... Quotienten gleich 1, wobei $m_1 < m_2 < m_3 < \cdots$. Da diese Menge überabzählbar ist, gibt es überabzählbar viele paarweise nicht-äquivalente transzendente Zahlen α mit $M(\alpha) = 3$.

Das Studium der Werte $M(\alpha) > 3$ ist viel komplizierter. Zum Beispiel kann $M(\alpha)$ nicht im offenen Intervall zwischen $\sqrt{12}$ und $\sqrt{13}$ liegen, aber es gibt überabzählbar viele α derart, dass $M(\alpha) = \sqrt{12}$; andererseits gilt $M(\alpha) = \sqrt{13}$ genau dann, wenn $\alpha \sim \frac{3+\sqrt{13}}{2}$. Weiter kann

$M(\alpha)$ nicht im offenen Intervall zwischen $\sqrt{13}$ und $\frac{9\sqrt{13}+65}{22} = 3{,}6631\ldots$ sein; die Menge aller α mit $M(\alpha) = 3{,}6631\ldots$ ist überabzählbar.

Diese klassischen Resultate sind sehr gut im Buch von Koksma (1936) erklärt, der insbesondere auf die Arbeit von Shibata (1929) verweist.

In jüngerer Zeit (1982) untersuchte Zagier die Verteilung der Markoff-Zahlen. Sei $z > 0$ und $Z(z) = \{x \mid x \leq z,\ x \text{ ist eine Markoff-Zahl}\}$. Zagier bewies, dass $\#Z(z) = C \log^2 3x + O(\log x \log\log^2 x)$ mit $C = 0{,}1807\ldots$. Numerische Berechnungen weisen darauf hin, dass der Fehler sogar noch kleiner sein sollte.

C Maße für die Irrationalität

Sei α eine irrationale Zahl; die Zahl $\nu \geq 1$ ist ein *Maß für die Irrationalität* von α, wenn es für jedes $\epsilon > 0$ nur endlich viele rationale Zahlen $\frac{a}{b}$ derart gibt, dass $|\alpha - \frac{a}{b}| < \frac{1}{b^{\nu+\epsilon}}$.

Also ist $\nu(\alpha) \leq \nu$ für jedes Maß für die Irrationalität ν von α. Um $\nu(\alpha)$ zu bestimmen oder abzuschätzen versucht man, ein möglichst kleines Maß für die Irrationalität von α zu finden.

Manchmal kann es einfacher sein, Werte von ν zu bestimmen, die *keine* Ordnungen der Approximation für α sind anstatt solcher, die Ordnungen der Approximation sind.

Hier ein Kriterium um zu zeigen, dass eine Zahl ν ein Irrationalitätsmaß für α ist:

6.8. Sei α eine irrationale Zahl. Angenommen dass $\frac{p_n}{q_n}$ eine Folge rationaler Zahlen mit der Eigenschaft ist, dass für jedes $n \geq 1$, $q_{n+1} = q_n^{1+s_n}$ wobei $s_n > 0$ und $\lim_{n\to\infty} s_n = 0$. Wenn es λ, $0 < \lambda < 1$ und $C > 0$ derart gibt, dass $|\alpha - \frac{p_n}{q_n}| < \frac{C}{q_n^{1+\lambda}}$ für jedes $n \geq 1$ gilt, dann ist $\nu = 1 + \frac{1}{\lambda}$ ein Maß für die Irrationalität für α.

Der Beweis für dieses Kriterium ist einfach; siehe zum Beispiel Alladi (1979), der ein weiteres ähnliches Kriterium angibt.

Im nächsten Abschnitt werde ich Maße für die Irrationalität für einige spezielle Zahlen aufzeigen.

D Ordnung der Approximierung von irrationalen algebraischen Zahlen

Sei α eine algebraische Zahl vom Grad $d \geq 1$ und sei

$$f(X) = a_0X^d + a_1X^{d-1} + \cdots + a_d \in \mathbb{Z}[X]$$

das minimale Polynom von α über $\mathbb{Q}$, wobei $\mathrm{ggT}(a_0, a_1, \ldots, a_d) = 1$ und $a_0 \neq 0$.

Sei die *Höhe* von α definiert als $H(\alpha) = \max_{0\leq i\leq d}\{|a_i|\}$, also $H(\alpha) = \sqcap f$ wie in Kapitel 1.

Sei

$$C(\alpha) = \begin{cases} \frac{1}{d(d+1)H(\alpha)(|\alpha|+1)^{d-1}} & \text{wenn } \alpha \in \mathbb{R}, \\ \frac{|\gamma|}{2} & \text{wenn } \alpha = \beta + \gamma i \text{ mit } \beta, \gamma \in \mathbb{R}, \gamma \neq 0. \end{cases}$$

Liouville bewies im Jahr 1844:

6.9. Wenn α eine algebraische Zahl vom Grad $d \geq 1$ ist, dann ist $|\alpha - \frac{a}{b}| > \frac{C(\alpha)}{b^d}$ für jedes $\frac{a}{b} \in \mathbb{Q}$, $\frac{a}{b} \neq \alpha$.

Also ist α nicht bis zu irgendeiner Ordnung $d + \epsilon$ ($\epsilon > 0$) durch rationale Zahlen approximierbar. Somit $\nu(\alpha) \leq d$.

Wir werden in §8 sehen, dass dieses Resultat durch Roth zur bestmöglichen Aussage verschärft wurde.

Beweis. Wenn $\alpha = \beta + \gamma i$ mit $\beta, \gamma \in \mathbb{R}$, $\gamma \neq 0$, dann

$$|\alpha - \frac{a}{b}| = |(\beta - \frac{a}{b}) + \gamma i| \geq |\gamma| > \frac{|\gamma|/2}{b^d}$$

für jedes $\frac{a}{b} \in \mathbb{Q}$.

Sei nun angenommen, dass α reell vom Grad $d \geq 1$ ist und ein minimales Polynom $f(X) = \sum_{i=0}^{d} a_i X^{d-i}$ hat.

Wenn $\frac{a}{b} \in \mathbb{Q}$ und $\frac{a}{b} \neq \alpha$, dann $f(\frac{a}{b}) \neq 0$ denn wenn $d \geq 2$, dann ist $f(X)$ irreduzibel und hat keine rationalen Nullstellen. Dann ist $b^d f(\frac{a}{b})$ eine ganze Zahl verschieden von 0 und somit $|b^d f(\frac{a}{b})| \geq 1$, also $|f(\frac{a}{b})| \geq \frac{a}{b^d}$.

Aus $f(\alpha) = 0$ folgt, dass

$$\frac{1}{b^d} \leq \left|f\left(\frac{a}{b}\right)\right| = |f\left(\frac{a}{b}\right) - f(\alpha)| = |\alpha - \frac{a}{b}||f'(\xi)|$$

für eine reelle Zahl ξ mit $|\xi - \alpha| < |\alpha - \frac{a}{b}|$.

Erster Fall: $|\alpha - \frac{a}{b}| \geq 1 \geq \frac{1}{b^d} > \frac{C(\alpha)}{b^d}$, da $C(\alpha) < 1$.

Zweiter Fall: $|\alpha - \frac{a}{b}| < 1$, also $|\xi - \alpha| < 1$ und $|\xi| < |\alpha| + 1$. Dann

$$\frac{1}{b^d} \leq |\alpha - \frac{a}{b}| \sum_{|\xi-\alpha|<1} |f'(\xi)|.$$

Aber $f'(\xi) = \sum_{i=0}^{d-1}(d-i)a_i\xi^{d-i-1}$, also

$$|f'(\xi)| \leq \sum_{i=0}^{d-1}(d-i)|a_i||\xi|^{d-i-1}.$$

Wenn $|\xi| \geq 1$, dann

$$\begin{aligned}|f'(\xi)| &\leq [\sum_{i=0}^{d-1}(d-i)]H(\alpha)|\xi|^{d-1} \\ &< \frac{d(d+1)}{2}H(\alpha)(|\alpha|+1)^{d-1} < \frac{1}{C(\alpha)}.\end{aligned}$$

Wenn $|\xi| < 1$, dann

$$\begin{aligned}|f'(\xi)| &\leq [\sum_{i=0}^{d-1}(d-i)]H(\alpha) \\ &= \frac{d(d+1)}{2}H(\alpha) = d(d+1)H(\alpha)(|\alpha|+1)^{d-1} = \frac{1}{C(\alpha)}.\end{aligned}$$

Daher $|\alpha - \frac{a}{b}| > \frac{C(\alpha)}{b^d}$, was den Beweis abschließt. □

Wie im historischen Überblick angemerkt ist, war Liouvilles Satz einer der Grundgedanken beim Aufbau der Theorie der Approximation durch rationale Zahlen. Und obwohl die Ungleichung die der Satz liefert eher etwas locker ist, kann man sie immer noch zum Beweis verschiedener Resultate über die Irrationalität spezieller Zahlen heranziehen. Dies wird im nächsten Abschnitt veranschaulicht.

7 Irrationalität spezieller Zahlen

In diesem Abschnitt werde ich beginnend mit der Zahl e die Irrationalität verschiedener interessanter Zahlen nachweisen.

7.1. e und e^2 sind irrationale Zahlen und darüberhinaus nicht algebraisch vom Grad 2. (Und tatsächlich sind diese Zahlen transzendent.)

Beweis. Wie in Abschnitt C gezeigt, gab Euler die folgenden Kettenbruchentwicklungen an:

$$\alpha = \frac{e+1}{e-1} = [2, 6, 10, 14, \dots],$$
$$\beta = \frac{e^2+1}{e^2-1} = [1, 3, 5, 7, \dots].$$

Es sind also α und β irrationale Zahlen, damit sind e und e^2 irrationale Zahlen und zudem nicht algebraisch vom Grad 2, was aus LAGRANGEs Satz **(5.7)** folgt. □

Ein anderer Beweis der Irrationalität von e, der unabhängig von der Kettenbruchentwicklung ist, stammt von FOURIER und erschien in STAINVILLEs Buch von 1815. Er basiert auf einem einfachen Kriterium:

7.2. Sei α eine reelle Zahl und $(f(n))_{n\geq 0}$ eine Folge positiver reeller Zahlen mit $\liminf_{n\to\infty} f(n) = 0$. Angenommen, es existiere n_0 mit der Eigenschaft, dass es für jedes $n \geq n_0$ ganze Zahlen a_n und b_n derart gibt, dass $0 < |b_n\alpha - a_n| \leq f(n)$. Dann ist α irrational.

Dies war FOURIERs Beweis:

Beweis. Es ist äquivalent zu zeigen, dass $\alpha = e-2 = \sum_{n=2}^{\infty} \frac{1}{n!}$ irrational ist. Für jedes $n \geq 2$ ist $n!\alpha = k_n + s_n$ mit $k_n = n!(\sum_{i=2}^{n} \frac{1}{i!})$ eine ganze Zahl und

$$\begin{aligned} 0 < s_n &= \frac{1}{n+1} + \frac{1}{(n+1)(n+2)} + \cdots \\ &< \frac{1}{(n+1)} + \frac{1}{(n+1)^2} + \frac{1}{(n+1)^3} + \cdots = \frac{1}{n}. \end{aligned}$$

Nach **(7.2)** ist α irrational. □

Das Kriterium **(7.2)** impliziert auch, dass für eine Folge von Primzahlen $p_1 < p_2 < p_3 < \cdots$ die Zahl

$$\alpha = \sum_{i=1}^{\infty} \frac{1}{p_1 p_2 \cdots p_i}$$

irrational ist.

Andere Irrationalitätskriterien kann man aus Verallgemeinerungen der Dezimaldarstellung positiver reeller Zahlen gewinnen. Es gibt einige erwähnenswerte Darstellungsweisen, die zum Beispiel in PERRONs Buch *Irrationalzahlen* erklärt sind.

Im Jahr 1869 bewies CANTOR:

7.3. Seien $a_1, a_1, a_3, \ldots \geq 2$ ganze Zahlen. Dann besitzt jede reelle Zahl α eine eindeutige Darstellung

$$\alpha = c_0 + \sum_{i=1}^{\infty} \frac{c_i}{a_1 a_2 \cdots a_i},$$

wobei jedes c_i eine ganze Zahl ist und für $i \geq 1$, $0 \leq c_i \leq a_i - 1$ und $c_i < a_i - 1$ für unendlich viele Indizes $i \geq 1$ gilt.

Umgekehrt ist jede Reihe der obigen Art konvergent. Wenn man $a_i = 10$ für jedes i wählt, erhält man die normale Dezimaldarstellung.

Dies ergibt das folgende Irrationalitätskriterium:

7.4. Wenn jedes prime p unendlich viele a_i teilt, dann ist α genau dann irrational, wenn $c_i \geq 1$ für unendlich viele Indizes i gilt.

Man beachte die folgenden Spezialfälle:

(a) Wenn jedes $a_i = i+1$ und jedes $c_i = 1$, dann ist $e = 2 + \sum_{n=2}^{\infty} \frac{1}{n!}$ irrational.

(b) Wenn F_1, F_2, …, F_i, … die Folge der Fibonacci-Zahlen ist, dann ist

$$\alpha = \sum_{i=1}^{\infty} \frac{1}{F_1 F_2 \cdots F_i} = 2 + \sum_{i=3}^{\infty} \frac{1}{F_3 \cdots F_i}$$

eine irrationale Zahl.

Im gleichen Sinne werde ich nun die Darstellungen von Sylvester, Lüroth und Engel beschreiben.

Im Jahr 1880 zeigte Sylvester:

7.5. Jede reelle Zahl α besitzt eine eindeutige Darstellung

$$\alpha = c + \sum_{i=1}^{\infty} \frac{1}{a_i}$$

wobei c eine ganze Zahl ist und a_1, a_2, a_3, … ≥ 2 ganze Zahlen mit der Eigenschaft sind, dass $a_{i+1} > (a_i - 1)a_i$.

Umgekehrt ist jede Reihe dieser Art konvergent und ihre Summe α ist irrational genau dann, wenn $a_{i+1} > (a_i - 1)a_i + 1$ für unendlich viele Indizes i gilt.

Zum Beispiel ist $\alpha = \sum_{i=0}^{\infty} \frac{1}{2^{2^i}}$ eine irrationale Zahl.

Im Jahr 1883 bewies Lüroth:

7.6. Jede reelle Zahl α hat eine eindeutige Darstellung

$$\alpha = c + \frac{1}{a_1} + \sum_{i=1}^{\infty} \frac{1}{(a_1-1)a_1(a_2-1)a_2\cdots(a_i-1)a_i} \times \frac{1}{a_{i+1}}$$

wobei c und a_1, a_2, a_3, $\ldots \geq 2$ ganze Zahlen sind.

Umgekehrt ist jede solche Reihe konvergent und ihre Summe α ist irrational genau dann, wenn die Folge a_1, a_2, a_3, $\ldots$ nicht periodisch ist.

Im Jahr 1913 gelangte Engel zu folgendem Ergebnis:

7.7. Jede reelle Zahl α besitzt eine eindeutige Darstellung

$$\alpha = c + \sum_{i=1}^{\infty} \frac{1}{a_1 a_2 \cdots a_i}$$

wobei c eine ganze Zahl und $2 \leq a_1 \leq a_2 \leq a_3 \leq \cdots$ eine Folge ganzer Zahlen ist.

Umgekehrt ist jede solche Folge konvergent und ihre Summe ist genau dann irrational, wenn $\lim_{i\to\infty} a_i = \infty$.

Ich weise auf die folgenden Spezialfälle hin:

(a) Wenn $p_1 < p_2 < p_3 < \cdots$ eine Folge von Primzahlen ist, dann ist $\alpha = \sum_{i=1}^{\infty} \frac{1}{p_1 p_2 \cdots p_i}$ eine irrationale Zahl (dieses Beispiel war bereits erwähnt worden)

(b) Sei E_2, E_4, E_6, $\ldots$ die Folge der Euler-Zahlen, auch als Sekantenkoeffizienten bezeichnet, da sie definiert sind durch

$$\sec x = 1 - \frac{E_2}{2!}x^2 + \frac{E_4}{4!}x^4 - \frac{E_6}{6!}x^6 + \cdots \qquad (\text{für } |x| < \tfrac{\pi}{2}).$$

Diese Zahlen sind ganze Zahlen, die der Rekurrenzrelation

$$E_{2n} + \binom{2n}{2n-2} E_{2n-2} + \binom{2n}{2n-4} E_{2n-4} + \cdots + \binom{2}{2} E_{2n} + 1 = 0$$

genügen. Darüberhinaus, $(-1)^n E_{2n} > 0$.

Damit folgt, dass

$$\alpha = \sum_{n=1}^{\infty} \frac{1}{|E_2 E_4 \cdots E_{2n}|}$$

eine irrationale Zahl ist.

Ich werde nun Beispiele anderer Zahlen betrachten, die als Reihensummen definiert sind.

Sei $(f(n))_{n\geq 0}$ eine streng monoton wachsende Folge positiver ganzer Zahlen, sei $d \geq 2$ eine ganze Zahl und

$$\alpha = \sum_{n=0}^{\infty} \frac{1}{d^{f(n)}}.$$

Ich untersuche nun, um was für eine Art Zahl es sich bei α handelt.

(1) Wenn $f(n) = n$, dann

$$\alpha = \sum_{n=0}^{\infty} \frac{1}{d^n} = 1 + \frac{1}{d} + \frac{1}{d^2} + \frac{1}{d^3} + \cdots = \frac{1}{1 - \frac{1}{d}} = \frac{d}{d-1},$$

also ist α rational.

(2) Sei $s \geq 2$ eine ganze Zahl und $f(n) = n^s$ (für $n \geq 0$).

Dann ist $\alpha = \sum_{n=0}^{\infty} \frac{1}{d^{n^s}}$ eine irrationale Zahl. Dies folgt aus **(7.7)**.

Nach **(6.3)** ist α damit durch rationale Zahlen mindestens bis zur Ordnung 2 approximierbar.

(3) Sei $s \geq 2$ eine ganze Zahl und $f(n) = s^n$ (für $n \geq 0$). Dann ist α bis zur Ordnung s durch rationale Zahlen approximierbar. Somit ist α irrational.

Man beachte, dass die Irrationalität von α aus **(7.7)** folgt.

(4) Sei $\limsup_{n\to\infty} \frac{f(n+1)}{f(n)} = \mu > 2$ und $\alpha = \sum_{n=0}^{\infty} \frac{1}{d^{f(n)}}$. Dann ist die Zahl α für jedes $0 < \epsilon < \mu - 2$ bis zur Ordnung $\mu - \epsilon$ durch rationale Zahlen approximierbar und somit ist α irrational. Man beachte, dass die Irrationalität von α wiederum aus **(7.7)** folgt.

Ich werde meine Aufmerksamkeit nun auf die Zahl π richten.

7.8. π^2 und somit auch π sind irrationale Zahlen.

Beweis. Der erste Beweis, dass π irrational ist, stammt von LAMBERT, wohingegen wie bereits im geschichtlichen Überblick erwähnt LEGENDRE die Irrationalität von π^2 bewies. Untenstehenden Beweis kann man in NIVENs Buch finden. Es handelt sich dabei um eine Modifikation seines eigenen Beweises, dass π irrational ist.

Ich benötige das folgende Lemma:

Lemma. *Sei $g \in \mathbb{Z}[X]$ und $h(X) = \frac{X^n g(X)}{n!}$, wobei $n \geq 1$. Dann ist $h^{(j)}(0) \in \mathbb{Z}$ für jedes $j \geq 0$.*

Beweis. In der Tat, sei $X^n g(X) = \sum_{j\geq 0} c_j X^j$, also $c_j = 0$ für $j < n$. Aus $h^{(j)}(0) = c_j \frac{j!}{n!}$ folgt, dass $h^{(j)}(0) \in \mathbb{Z}$ für jedes $j \geq 0$. □

Ich zeige nun, dass π^2 irrational ist.

Sei $h(X) = \frac{X^n(1-X)^n}{n!}$ (wobei n eine später zu wählende positive ganze Zahl ist); dann gilt für $0 < x < 1$, $0 < h(x) < \frac{1}{n!}$.

Unter Beachtung, dass $h^{(j)}(0)$ für $j \geq 0$ eine ganze Zahl ist folgt aus $h(1-X) = h(X)$, dass auch $h^{(j)}(1)$ für $j \geq 0$ ganz ist.

Für $\pi^2 = \frac{a}{b}$ mit teilerfremden ganzen Zahlen a, $b > 0$ sei

$$\begin{aligned} f(X) = b^n[\pi^{2n}h(X) - \pi^{2n-2}h^{(2)}(X) \\ +\pi^{2n-4}h^{(4)}(X) - \cdots + (-1)^n h^{(2n)}(X)], \end{aligned}$$

also sind $f(0)$, $f(1)$ ganz. Darüberhinaus,

$$\begin{aligned} \frac{d}{dx}[f'(x)\sin\pi x - \pi f(x)\cos\pi x] &= [f''(x) + \pi^2 f(x)]\sin\pi x \\ &= b^n\pi^{2n+2}h(x)\sin\pi x \\ &= \pi^2 a^n h(x)\sin\pi x, \end{aligned}$$

daher

$$\begin{aligned} \pi a^n \int_0^1 h(x)\sin\pi x\,dx &= \left[\frac{f'(x)\sin\pi x}{\pi} - f(x)\cos\pi x\right]_0^1 \\ &= f(1) + f(0) \in \mathbb{Z}. \end{aligned}$$

Also

$$0 < \pi a^n \int_0^1 h(x)\sin\pi x\,dx < \frac{\pi a^n}{n!} < 1$$

für genügend großes n. Dies ist ein Widerspruch. □

Dieselbe Methode verwendete Niven, um zu früheren Resultaten bezüglich der Werte der trigonometrischen und hyperbolischen Funktionen zu gelangen.

7.9. Wenn r eine rationale Zahl ungleich Null ist, dann ist $\cos r$ irrational.

Als Korollar ergibt sich, dass π irrational ist, da $\cos\pi = -1$ rational ist.

Es folgt aus $1 - 2\sin^2 r = \cos 2r$ und $\cos 2r = \frac{1-\tan^2 r}{1+\tan^2 r}$, dass wenn r rational ist mit $r \neq 0$, dann sind $\sin r$, $\tan r$ irrational, damit sind auch $\sec r$, $\csc r$ und $\cot r$ sämtlich irrational.

In gleicher Weise folgt für rationales r, dass $\arccos r$ (wenn $r \neq 1$) und $\arcsin r$ sowie $\arctan r$ (wenn $r \neq 0$) irrational sind.

7.10. Wenn r eine rationale Zahl ungleich Null ist, dann ist $\cosh r$ irrational.

Wegen $\cosh 2r = 2\sinh^2 r + 1 = \frac{1+\tanh^2 r}{1-\tanh^2 r}$, dann sind $\sinh r$ und $\tanh r$ irrational. Es folgt auch, dass die Werte der inversen hyperbolischen Funktionen an rationalen Stellen entweder gleich 0 oder irrational sind.

In dieser Weise gelangt man sofort zu einem neuen Beweis von Lambert's Resultat:

7.11. (1) Wenn r eine rationale Zahl verschieden von Null ist, dann ist e^r irrational.

(2) Wenn r eine positive rationale Zahl ist mit $r \neq 1$, dann ist $\log r$ irrational.

Beweis. (1) Wenn e^r rational ist, dann auch e^{-r}, damit auch $\cosh r = \frac{e^r+e^{-r}}{2}$ im Widerspruch zu **(7.10)**.

(2) Wenn $r \neq 1$ und $\log r$ rational ist, dann ist es ungleich Null und so wäre $r = e^{\log r}$ nach (1) irrational. □

Die folgende Bemerkung ist offensichtlich: Wenn r eine positive rationale Zahl ist und $a > 1$ ein ganze Zahl, dann ist $\log_a r = \frac{\log r}{\log a}$ genau dann irrational, wenn $r \neq a^s$ (mit rationalem s).

Somit ist zum Beispiel $\frac{\log 3}{\log 2}$ irrational. Dies gilt auch für $\log_{10} r$, sofern nicht $r^m = 10^n$ für irgendwelche ganzen Zahlen m und n gilt.

Andererseits ist es einfach zu zeigen:

7.12. Wenn r rational ist, dann sind die Werte der trigonometrischen Funktionen an $r\pi$ algebraische Zahlen.

Ich betrachte nun die Frage nach der Irrationalität der Werte $\zeta(k) = \sum_{j=1}^{\infty} \frac{1}{j^k}$ der Riemannschen Zetafunktion (für jede ganze Zahl $k \geq 2$).

Da $\zeta(2) = \frac{\pi^2}{6}$ und π^2 irrational ist, gilt dies auch für $\zeta(2)$. Eulers Formel für $\zeta(2k)$, die in §3 angegeben ist besagt, dass $\zeta(2k) = \pi^{2k} r_{2k}$, wobei r_{2k} eine rationale Zahl ist. Es wird in §3 gezeigt, dass π und

somit auch π^{2k} transzendent sind, daher ist $\zeta(2k)$ nicht nur irrational sondern auch transzendent.

Die Situation für $\zeta(2k+1)$ ist eine ganz andere. Es war für eine lange Zeit unbekannt, ob $\zeta(3)$ irrational ist. Dieses Problem wurde schließlich im positiven Sinne von APÉRY gelöst, wie bereits im geschichtlichen Überblick erwähnt. Seine raffinierte Methode war auch auf $\zeta(2)$ anwendbar.

7.13. $\zeta(2)$ und $\zeta(3)$ sind irrationale Zahlen.

Einen weiteren Beweis für die Irrationalität von $\zeta(2)$ und $\zeta(3)$ gab BEUKERS im Jahr 1979 an.

Weitere Zahlen, die man betrachtet hat, sind Summen von Reihen, deren Summanden Terme binärer rekurrenter Folgen sind. ANDRÉ-JEANNIN bewies im Jahr 1991:

7.14. Wenn $(F_n)_{n\geq 0}$ die Folge der Fibonacci-Zahlen bezeichnet, dann ist $\sum_{n=1}^{\infty} \frac{1}{F_n}$ eine irrationale Zahl.

Ein weiteres klassisches Resultat bezüglich der Fibonacci-Zahlen stammt von GOOD (1974) und HOGGATT (1976):

7.15. Die Summe

$$\sum_{n=0}^{\infty} \frac{1}{F_{2^n}} = \frac{7-\sqrt{5}}{2}$$

ist irrational.

Ein Korollar der Resultate von Becker und Töpfer (1994) ist zum Beispiel auf die Lucas-Zahlen $L_0 = 2$, $L_1 = 1$, $L_n = L_{n-1} + L_{n-2}$ (für $n \geq 2$ anwendbar).

7.16. Die Zahl

$$\sum_{n=0}^{\infty} \frac{1}{L_{2^n}}$$

ist irrational.

Das Folgende ist tatsächlich trivial. Sei $n \geq 3$. Die folgenden Aussagen sind äquivalent:

(1) Für jede rationale Zahl $x > 0$ ist die Zahl $(1 + x^n)^{1/n}$ irrational.

(2) Fermats letzter Satz ist für alle Exponenten n wahr.

Nun, jedermann weiß (sogar Laien!), dass WILES Fermats letzten Satz bewies. Daher gilt (1) für jedes $n \geq 3$. Aber angenommen, dass

jemand—sehr intelligentes—einen direkten Beweis von (1) mit Methoden diophantischer Approximation fände. Dies würde einen neuen Beweis von Fermats letztem Satz begründen. Ich habe hinsichtlich dieser Richtung keinerlei Einfälle.

Für viele Zahlen wurde das Maß ihrer Irrationalität abgeschätzt und in einigen Fällen explizit ausgerechnet.

So ist $\nu(e) = \nu(e^2) = 2$. Alladi zeigte im Jahr 1979, dass $\nu(e^r) = 2$ für jedes rationale r ungleich Null gilt.

Apéry führte 1979 Berechnungen durch, die die folgenden Schranken für das Maß der Irrationalität von $\zeta(2)$ und $\zeta(3)$ ergaben:

$$\nu(\zeta(2)) < 11{,}85,$$
$$\nu(\zeta(3)) < 13{,}42.$$

Es ist sehr wichtig, effektive untere Schranken für den Abstand zwischen einer gegebenen irrationalen Zahl und den rationalen Zahlen anzugeben. Einige Beispiele zur Veranschaulichung:

(a) Alladi (1979), als Verbesserung einer vorangegangenen Methode von Baker:

$$\left|\log 2 - \frac{a}{b}\right| > \frac{1}{10^{10} b^{5,8}}$$

für jede rationale Zahl $\frac{a}{b}$.

(b) Baker (1964b):

$$\left|\sqrt[3]{2} - \frac{a}{b}\right| > \frac{C}{b^{296}},$$

für jede rationale Zahl $\frac{a}{b}$, dabei ist C eine Konstante.

(c) Mahler (1953) bewies das bemerkenswerte Resultat

$$\left|\pi - \frac{a}{b}\right| > \frac{1}{b^{42}},$$

für jede rationale Zahl $\frac{a}{b}$, und

$$\left|\pi - \frac{a}{b}\right| > \frac{1}{b^{30}},$$

für jede rationale Zahl $\frac{a}{b}$ mit genügend großem Nenner. Mignotte (1974) zeigte, dass

$$\left|\pi - \frac{a}{b}\right| > \frac{1}{b^{20,6}}$$

für jede rationale Zahl $\frac{a}{b}$, und falls $b > q > 96$, dann

$$\left|\pi - \frac{a}{b}\right| > \frac{1}{b^{20}}.$$

Somit, $\nu(\pi) \leq 20$. Auch, $\nu(\pi^2) \leq 17{,}8$.

Dies bedeutet, dass $\nu = 30$ ein Maß für die Irrationalität von π ist. Mit dieser Frage beschäftigten sich viele Autoren und gelangten zu verbesserten Irrationalitätsmaßen für π. Ich notiere nur (ohne irgendeinen Hinweis auf die Methoden): MIGNOTTE, $\nu = 20$ (1974), darauf folgend die Arbeiten von G. V. CHUDNOVSKY und D. CHUDNOVSKY, F. BEUKERS, C. VIOLA, G. RHIN, R. DVORNICICH, E. A. BUKHADZE, und M. HATA, der im Jahr 1993 das beste Resultat erzielte:

$$\left|\pi - \frac{a}{b}\right| > \frac{1}{b^{8{,}0161}}$$

für alle genügend großen b.

Die Berechnungen waren langwierig und scharf; ihre Verifikation verlangt eine Zeit, die nur Spezialisten entbehren können.

8 Transzendente Zahlen

CANTOR bewies, dass die Menge $\mathbb{R}$ der reellen Zahlen überabzählbar ist. Dies war seinerzeit eine sehr bemerkenswerte Entdeckung. Einfacher ist es zu zeigen, dass die Menge aller algebraischen Zahlen abzählbar ist. Daher ist die Menge der transzendenten Zahlen ebenfalls überabzählbar, dabei ist es jedoch nicht so einfach, unendliche Familien transzendenter Zahlen zu erzeugen oder im Allgemeinen zu zeigen, dass Zahlen eines gewissen Typs transzendent sind.

Wieder wird es dabei wichtig sein zu untersuchen, wie gut die Zahl durch rationale Zahlen approximierbar ist.

A Liouville-Zahlen

LIOUVILLE untersuchte die folgenden Zahlen: $\alpha \in \mathbb{R} \setminus \mathbb{Q}$ nennt man eine *Liouville-Zahl*, wenn es für jede ganze Zahl $n \geq 2$ eine Zahl $\frac{a_n}{b_n} \in \mathbb{Q}$ mit $b_n \geq 2$ und der Eigenschaft gibt, dass $|\alpha - \frac{a_n}{b_n}| < \frac{1}{b_n^n}$.

8.1. Die reelle Zahl α ist eine Liouville-Zahl genau dann, wenn α bis auf jede beliebige Ordnung $\nu \geq 1$ durch rationale Zahlen approximierbar ist.

Insbesondere ist α transzendent (nach LIOUVILLEs Satz **(6.9)**). Damit ist α eine Liouville-Zahl genau dann, wenn $\nu(\alpha) = \infty$. Es bezeichne $\mathbb{L}$ die Menge aller Liouville-Zahlen.

Hier einige Beispiele von Liouville-Zahlen: Sei $d \geq 2$, $0 \leq k_n \leq d-1$ und $k_n \neq 0$ für unendlich viele Indizes n. Dann ist $\alpha = \sum_{n=0}^{\infty} \frac{k_n}{d^{n!}}$ eine Liouville-Zahl. Es genügt zu zeigen, dass α bis zu jeder Ordnung $n \geq 1$ durch rationale Zahlen approximierbar ist. Sei $n \geq 1$, $m \geq n$ und

$$b_m = d^{m!} a_m = \left(\sum_{i=0}^{m} \frac{k_i}{d^{i!}} d^{m!} \right).$$

Damit,

$$\begin{aligned} 0 < \alpha - \frac{a_m}{b_m} = \sum_{i=m+1}^{\infty} \frac{k_i}{d^{i!}} &\leq (d-1) \sum_{i=m+1}^{\infty} \frac{1}{d^{i!}} \\ &< \frac{d-1}{d^{(m+1)!} - 1} < \frac{1}{(d^{m!})^m} = \frac{1}{b_m^m} \leq \frac{1}{b_m^n}, \end{aligned}$$

da wenn $c = d^{m!}$, dann

$$\begin{aligned} \frac{1}{d^{(m+1)!}} + \frac{1}{d^{(m+2)!}} + \frac{1}{d^{(m+3)!}} + \cdots &< \frac{1}{c^{m+1}} + \frac{1}{c^{(m+1)^2}} + \frac{1}{c^{(m+1)^3}} + \cdots \\ &< \frac{1}{c^{m+1}} + \frac{1}{c^{2(m+1)}} + \frac{1}{c^{3(m+1)}} + \cdots \\ &= \frac{1}{c^{m+1}} \cdot \frac{1}{1 - \frac{1}{c^{m+1}}} \\ &= \frac{1}{c^{m+1} - 1} \\ &= \frac{1}{d^{(m+1)!} - 1}, \end{aligned}$$

und $d^{m!m+1} + 1 < d^{(m+1)!} + d^{m!m}$, also

$$\frac{d-1}{d^{(m+1)!} - 1} < \frac{1}{(d^{m!})^m}.$$

Da es unendlich viele n gibt mit $k_n \neq 0$, gibt es auch unendlich viele verschiedene rationale Zahlen $\frac{a_m}{b_m}$ die $0 < \alpha - \frac{a_m}{b_m} < \frac{1}{b_m^n}$ genügen; somit $\alpha \in \mathbb{L}$.

Insbesondere, $\sum_{n=0}^{\infty} \frac{1}{10^{n!}} \in \mathbb{L}$.

Dies waren die ersten bekannten Beispiele transzendenter Zahlen.

Liouville-Zahlen wurden von MAILLET untersucht (siehe sein Buch von 1906) und waren auch Gegenstand eines Kapitels in SCHNEIDERs Buch (1959).

Einige Eigenschaften:

8.2. Die Menge der Liouville-Zahlen ist überabzählbar.

8.3. Die Menge der Liouville-Zahlen liegt dicht in $\mathbb{R}$.

8.4. Die Menge der Liouville-Zahlen hat das Maß 0.

Damit sind „fast alle“ transzendenten Zahlen keine Liouville-Zahlen.

Da die Menge der Liouville-Zahlen überabzählbar ist, gibt es überabzählbar viele Liouville-Zahlen, die algebraisch unabhängig über $\mathbb{Q}$ sind.

PERRON (1932) und später SCHMIDT (1962) gaben die folgende abzählbare Menge algebraisch unabhängiger Liouville-Zahlen an:

8.5. Für jedes $i \geq 1$ sei $\alpha_i = \sum_{n=1}^{\infty} \frac{1}{2^{(in)!}}$. Dann sind $\alpha_1, \alpha_2, \alpha_3, \ldots$ algebraisch unabhängig über $\mathbb{Q}$ (d.h., für jedes $m \geq 1$ sind die Zahlen $\alpha_1, \alpha_2, \ldots, \alpha_m$ algebraisch unabhängig über $\mathbb{Q}$).

Es ist bekannt, dass e, π und $\log 2$ keine Liouville-Zahlen sind (siehe §7), allerdings ist unbekannt, ob es sich bei e^π um eine Liouville-Zahl handelt.

Obwohl es auf den ersten Blick paradox erscheinen mag (da die Menge der Liouville-Zahlen das Maß 0 hat) bewies ERDÖS im Jahr 1962, dass jede reelle Zahl ungleich Null die Summe und auch das Produkt zweier Liouville-Zahlen ist.

B Approximation durch rationale Zahlen: Schärfere Sätze

Der Satz von Liouville **(6.9)** über die Approximation von algebraischen Zahlen durch rationale Zahlen ergibt nur eine ungefähre Ordnung der Approximation die vom Grad der algebraischen Zahl abhängt; andererseits ist die Konstante in der Ungleichung explizit gegeben.

Die moderne Theorie der diophantischen Approximation wurde von THUE (1909) begründet, der einen neuen Zusammenhang zwischen den Lösungen bestimmter diophantischer Gleichungen und der Approximation algebraischer Zahlen durch rationale Zahlen fand.

Ich werde diese Ideen in kurzer Form beschreiben.

Sei $d \geq 3$ und $F(X,Y) = a_0X^d + a_1X^{d-1}Y + a_2X^{d-2}Y^2 + \cdots + a_{d-1}XY^{d-1} + a_dY^d$ ein homogenes Polynom vom Grad d mit ganzzahligen Koeffizienten mit $a_0 \neq 0$. Praktischerweise sei zudem angenommen, dass $f(X) = a_0X^d + a_1X^{d-1} + \cdots + a_d$ irreduzibel ist.

Betrachte für eine beliebige ganze Zahl a die Gleichung $F(X,Y) = a$. Die Absicht wird es sein zu zeigen, dass diese Gleichung nur endlich viele Lösungen in ganzen Zahlen besitzt.

Seien $\alpha_1, \ldots, \alpha_d \in \mathbb{C}$ die Lösungen von $f(X) = 0$. Da $f(X)$ irreduzibel ist folgt, dass $\alpha_1, \ldots, \alpha_d$ verschiedene algebraische Zahlen vom Grad d sind.

Wenn x und y ganze Zahlen mit der Eigenschaft $F(x,y) = a$ sind, dann $a_0 \prod_{k=1}^{d}(x - \alpha_k y) = a$.

Es gibt nun zwei Fälle. Wenn $a = 0$, dann gibt es j mit $1 \leq j \leq d$ derart, dass $x - \alpha_j y = 0$; aber $\alpha_j \notin \mathbb{Q}$, also $y = 0$ und notwendigerweise $x = 0$. Daher ist $(0,0)$ für $a = 0$ die einzige Lösung.

Andererseits, wenn $a \neq 0$, dann

$$\prod_{k=1}^{d}(x - \alpha_k y) = \frac{|a|}{|a_0|}.$$

Sei $C_1 = (\frac{|a|}{|a_0|})^{1/d}$, also gibt es einen Index und somit auch einen kleinsten Index j mit $|x - \alpha_j y| \leq C_1$.

Sei $C_2 = \min_{h \neq k} |\alpha_h - \alpha_k|$; also $C_2 > 0$. Man beachte, dass es für jede ganze Zahl y_0 höchstens d ganze Zahlen x derart gibt, dass (x, y_0) eine Lösung der Gleichung ist.

Um zu zeigen, dass $F(X,Y) = a$ nur endlich viele ganzzahlige Lösungen besitzt reicht es zu zeigen, dass die Menge $S = \{\text{Lösungen } (x,y) : |y| > \frac{2C_1}{C_2}\}$ endlich ist.

Wenn $(x,y) \in S$, dann gilt für jedes $k \neq j$ mit j wie oben,

$$\begin{aligned} 0 < \frac{C_2|y|}{2} < C_2|y| - C_1 &\leq |\alpha_k - \alpha_j| \cdot |y| - |x - \alpha_j y| \\ &\leq |(\alpha_k - \alpha_j)y - (x - \alpha_j y)| = |x - \alpha_k y|. \end{aligned}$$

Somit,

$$|x - \alpha_k y| = \frac{|a|}{|a_0| \prod_{k \neq j} |x - \alpha_k y|} < \frac{2^{d-1}|a|}{|a_0| C_2^{d-1} |y|^{d-1}} = \frac{C_3}{|y|^{d-1}}$$

wobei $C_3 = \frac{2^{d-1}|a|}{|a_0| C_2^{d-1}}$ (man beachte, dass C_3 wie auch C_1 und C_2 nur von der gegebenen Gleichung und nicht von der betrachteten Lösung (x,y)

abhängt). Setze $\operatorname{sgn}(y) = \frac{|y|}{y}$, dann

$$\alpha_j - \frac{x \operatorname{sgn}(y)}{|y|} = \left|\alpha_j - \frac{x}{y}\right| < \frac{C_3}{|y|^n}.$$

Für jedes $k = 1, \ldots, d$ sei

$$T_k = \left\{ \frac{m}{n} \in \mathbb{Q} \mid \operatorname{ggT}(m,n) = 1 \quad \text{und} \quad \left|\alpha_k - \frac{m}{n}\right| < \frac{C_3}{n^d} \right\}.$$

Wir haben gesehen, dass wenn $(x,y) \in S$, dann gehört die rationale Zahl $\frac{x \operatorname{sgn}(y)}{|y|}$ zu $\bigcup_{k=1}^{d} T_k$. Dies definiert eine Abbildung Φ von S in die vorstehende Menge. Darüberhinaus ist Φ eins-eindeutig. Tatsächlich gilt, dass wenn (x,y) und (x',y') in S liegen und $\frac{x \operatorname{sgn}(y)}{|y|} = \frac{x' \operatorname{sgn}(y')}{|y'|}$, dann $|y'| = r|y|$ und $x' \operatorname{sgn}(y') = rx \operatorname{sgn}(y)$ (für eine rationale Zahl r ungleich Null), somit $a = F(x',y') = \pm r^d F(x,y) = \pm r^d a$, woraus folgt, dass $r = \pm 1$, also $r = 1$.

Um also zu zeigen, dass S endlich ist genügt es zu zeigen, dass jede Menge $\Phi(S) \cap T_k$ endlich ist.

Sei $\frac{x \operatorname{sgn}(y)}{|y|} \in T_k$, wobei $(x,y) \in S$. Für $\alpha_k \notin \mathbb{R}$ sei $\alpha_k = \beta + i\gamma$ mit $\beta, \gamma \in \mathbb{R}$ und $\gamma \neq 0$. Dann

$$|\gamma| \leq \left|(\beta - \frac{x}{y}) + i\gamma\right| = \left|\alpha_k - \frac{x \operatorname{sgn}(y)}{|y|}\right| < \frac{C_3}{|y|^d},$$

somit

$$|y|^d < \frac{C_3}{|\gamma|}.$$

Also kann $|y|$ nur endlich viele Werte haben und nach einer früheren Bemerkung gilt dasselbe für x, also ist $\Phi(S) \cap T_k$ endlich.

Für $\alpha_k \in \mathbb{R}$ ist man geneigt zu untersuchen, ob die Menge T_k endlich ist.

Dies führte zur Verbindung zwischen der Approximation von algebraischen Zahlen durch rationale Zahlen und der Endlichkeit der Anzahl der Lösungen der oben betrachteten Gleichung. Für einen Überblick über einige grundlegende Methoden der Theorie von diophantischen Gleichungen, siehe Ribenboim (1986).

Schärfere und effektive Ungleichungen werden damit wichtige Hinweise auf die Anzahl und Größe der Lösungen liefern. Dieses Problem wurde daher von bedeutenden Mathematikern behandelt.

Liouvilles Satz wurde nacheinander von Thue (1909), Siegel (1921), Dyson (1947) und Schneider (1949) verbessert; schließlich bewies Roth im Jahr 1955 das bestmögliche Resultat:

8.6. Wenn α irgendeine algebraische Zahl ist, dann gibt es für jedes $\epsilon > 0$ ein $C = C(\alpha, \epsilon) > 0$ derart, dass für jede rationale Zahl $\frac{a}{b} \neq \alpha$ gilt $|\alpha - \frac{a}{b}| > \frac{C}{b^{2+\epsilon}}$.

Also ist α für kein $\epsilon > 0$ bis zur Ordnung $2 + \epsilon$ durch rationale Zahlen approximierbar. Somit $\nu(\alpha) \leq 2$. Daher $\nu(\alpha) = 2$, sofern $\alpha \notin \mathbb{Q}$ (was aus Dirichlets Satz folgt).

Ein Korollar ist das folgende Transzendenz-Kriterium:

8.7. Wenn α eine reelle Zahl ist, die durch rationale Zahlen bis zur Ordnung $\nu > 2$ approximierbar ist, dann ist α transzendent.

Wenn α einen Grad von mindestens 3 besitzt, dann ist die Zahl $C(\alpha, \epsilon)$ in **(8.6)** nicht effektiv berechenbar; obige Proposition sichert nur ihre Existenz.

Man betrachte die folgende Aussage, die schärfer ist als Roths Satz: Wenn α irgendeine algebraische Zahl ist, dann gibt es $C(\alpha) > 0$ derart, dass für jede rationale Zahl $\frac{a}{b} \neq \alpha$ gilt $|\alpha - \frac{a}{b}| > \frac{C(\alpha)}{b^2}$. Es lässt sich zeigen, dass obige Aussage äquivalent zu folgender Behauptung ist, die bislang unbewiesen ist:

Wenn α eine reelle algebraische Zahl ist und $\alpha = [a_0, a_1, a_2, \dots]$ ihre einfache Kettenbruchentwicklung, dann gibt es eine Zahl $M = M(\alpha) > 0$ mit $|a_0|, a_1, a_2, \cdots < M$.

Man glaubt jedoch allgemein, dass obige Aussage falsch ist. Es ist vielmehr im Gegenteil ziemlich gut möglich, dass für eine reelle algebraische Zahl α vom Grad $d \geq 3$ unter obiger Bezeichnungsweise folgt, dass $\sup\{a_i \mid i \geq 1\} = \infty$.

Ich betrachte nun einige Beispiele.

Beispiel 1. Es ist bisher nicht bekannt, ob $\alpha = \sum_{n=0}^{\infty} \frac{1}{d^{n^s}}$ eine transzendente Zahl ist (wobei $d \geq 2$, $s \geq 2$). Für $s = 2$ erfordert dies möglicherweise eine genauere Untersuchung der Theta-Funktionen.

Die Funktion $f(z) = \sum_{n=0}^{\infty} \frac{z^n}{2^{n(n-1)}}$ erfüllt die Funktionalgleichung $f(z) = 1 + zf(\frac{z}{4})$; dies wird benutzt, um zu zeigen, dass $f(\frac{1}{2}) = \sum_{n=0}^{\infty} \frac{1}{2^{n^2}}$ keine Liouville-Zahl ist. Allgemeiner zeigte BUNDSCHUH (1970): Wenn $d \geq 2$, dann ist $\sum_{n=0}^{\infty} \frac{1}{d^{n^2}}$ keine Liouville-Zahl.

Beispiel 2. Sei $s \geq 3$ eine ganze Zahl, $d \geq 2$, und $\alpha = \sum_{n=0}^{\infty} \frac{1}{d^{s^n}}$. Dann ist α transzendent.

Tatsächlich ist, wie in Abschnitt §7 gesehen, α bis zur Ordnung s durch rationale Zahlen approximierbar. Da $s > 2$ folgt nach **(8.7)**, dass α transzendent ist.

Allgemeiner:

Beispiel 3. Sei $(f(n))_{n\geq 1}$ eine Folge positiver ganzer Zahlen derart, dass $\lim_{n\to\infty} \frac{f(n+1)}{f(n)} = \mu > 2$. Dann ist für jede ganze Zahl $d \geq 2$ die Zahl $\alpha = \sum_{n=0}^{\infty} \frac{1}{d^{f(n)}}$ transzendent.

In der Tat ist α wie aus Abschnitt §7 hervorgeht, für $0 < \epsilon < \mu - 2$ durch rationale Zahlen bis zur Ordnung $\mu - \epsilon > 2$ approximierbar. Nach **(8.7)** ist α transzendent.

Das Folgende wurde zuerst von MAHLER (1929) bewiesen, man könnte auch eine Variante von Roths Satz als Beweis verwenden:

Beispiel 4. $\alpha = \sum_{n=0}^{\infty} \frac{1}{d^{2^n}}$ (mit $d \geq 2$) ist transzendent.

Allgemeiner:

Beispiel 5. Seien $r \in \mathbb{Q}$, $r \neq 0$, $C \geq 1$, $d \geq 2$, $s \geq 2$ ganze Zahlen. Für jedes n sei c_n eine ganze Zahl derart, dass $|c_n| \leq C^n$ und $c_n \neq 0$ für unendlich viele $n \geq 1$. Dann ist $\sum_{n=0}^{\infty} \frac{c_n r^n}{d^{s^n}}$ transzendent.

MAHLER erweiterte diese Konstruktion 1976. Sei f irgendeine Funktion, die auf den ganzen Zahlen definiert ist. Sei α diejenige Zahl zwischen 0 und 1, deren dezimale Darstellung wie folgt aussieht: $f(1)$ mal die Ziffer 1, gefolgt von $f(1)$ mal der Ziffer 2, ..., gefolgt von $f(1)$ mal der Ziffer 9, gefolgt von $f(2)$ mal der 2-ziffrigen Zahl 10, ..., gefolgt von $f(2)$ mal der 2-ziffrigen Zahl 99, gefolgt von $f(3)$ mal jede der Zahlen 100, 101, ..., 999 der Reihe nach, etc. Die resultierenden Zahlen α sind transzendente Zahlen, aber keine Liouville-Zahlen.

Für jedes $\mu > 2$ sei $\mathbb{R}_\mu = \{\alpha \in \mathbb{R} \mid \nu(\alpha) \geq \mu\}$. Somit ist jedes $\alpha \in \mathbb{R}_\mu$ transzendent. Darüberhinaus, $\mathbb{L} = \bigcap_{\mu>2} \mathbb{R}_\mu$.

Da $\mathbb{L}$ überabzählbar ist und dicht in $\mathbb{R}$ liegt, ist auch jedes $\mathbb{R}_\mu$ überabzählbar und ebenfalls dicht.

MAHLER (1937) gab eine Klasse transzendenter Zahlen an, die keine Liouville-Zahlen sind:

8.8. Sei $f(X) \in \mathbb{Z}[X]$ ein Polynom mit einem Grad von mindestens 1 mit der Eigenschaft, dass $f(k) \geq 1$ für jedes $k \geq 1$. Sei $a = 0{,}a_1a_2a_3a_4\ldots$ mit $a_k = f(k)$ (diese Bezeichnung wird anhand des folgenden Beispiels verständlich). Dann ist α transzendent, aber keine Liouville-Zahl.

Zum Beispiel ergibt $f(X) = X$: 0,12345678910111213... ist transzendent, aber keine Liouville-Zahl.

Im Jahr 1924 bewies KHINTCHINE einen allgemeinen Satz über Approximation durch rationale Zahlen (siehe auch sein Buch (1935)). Ein Spezialfall ist der folgende:

8.9. Für jedes $\mu > 2$ hat die Menge $\mathbb{R}_\mu$ das Maß 0.

Beispiel 6. (KNUTH (1964)) Sei $a \geq 2$ eine ganze Zahl und ξ_a die irrationale Zahl mit einfacher Kettenbruchentwicklung

$$\xi_a = [a^{F_0}, a^{F_1}, a^{F_2}, \dots]$$

wobei $(F_n)_{n\geq 0}$ die Folge der Fibonacci-Zahlen ist. Dann ist ξ_a bis zur Ordnung $\alpha+1$ durch rationale Zahlen approximierbar, wobei $\alpha = \frac{1+\sqrt{5}}{2}$ die goldene Zahl ist. Somit ist $\xi_a \in \mathbb{R}_{\alpha+1}$ und transzendent.

C Hermite, Lindemann und Weierstrass

Ich gebe nun die wichtigen klassischen Resultate von HERMITE und LINDEMANN an.

Im Jahr 1873 zeigte HERMITE

8.10. e ist eine transzendente Zahl.

Ein eher einfacher Beweis dieses Satzes, den HURWITZ 1893 fand, ist in NIVENs Buch angegeben.

Im Jahr 1882 bewies LINDEMANN die folgenden äquivalenten Aussagen (dies verbessert **(7.11)**):

8.11. (1) Wenn log irgendein Zweig des komplexen Logarithmus ist und r eine rationale Zahl mit $r \neq 0$, dann ist $\log r$ gleich 0 oder transzendent.

(2) Wenn α eine algebraische Zahl ist und $\alpha \neq 0$, dann ist e^α irrational.

Die Äquivalenz dieser Aussagen ist offensichtlich. Insbesondere zeigte LINDEMANN:

8.12. π ist transzendent.

Wenn π algebraisch wäre, so $i\pi \neq 0$, daher wäre $e^{i\pi} = -1$ irrational, ein Widerspruch.

Dieses wichtige Resultat bedeutete eine negative Lösung des Problems der Quadratur des Kreises.

Weitere Beweise dafür, dass e und π transzendent sind, finden sich zum Beispiel in POPKEN (1929A,B), VEBLEN (1904) und SCHENKMAN (1970).

HERMITE fand einen Beweis des folgenden Satzes, der **(8.11)** erweitert und von LINDEMANN angegeben worden war:

8.13. (1) Wenn log irgendein Zweig des komplexen Logarithmus ist und α eine algebraische Zahl ungleich Null, dann ist $\log \alpha$ entweder gleich 0 oder transzendent.

(2) Wenn α eine algebraische Zahl ist mit $\alpha \neq 0$, dann ist e^{α} transzendent.

Als Konsequenz ergeben sich die folgenden Resultate, die vorangegangene Aussagen verbessern:

8.14. Wenn α eine algebraische Zahl ist und $\alpha \neq 0$, dann sind $\cos \alpha$, $\sin \alpha$, $\tan \alpha$, $\cosh \alpha$, $\sinh \alpha$, $\tanh \alpha$ transzendente Zahlen.

WEIERSTRASS fand einen Beweis des folgenden von LINDEMANN angegebenen Satzes:

8.15. Wenn $\alpha_1, \ldots, \alpha_n$ verschiedene algebraische Zahlen sind, dann sind $e^{\alpha_1}, \ldots, e^{\alpha_n}$ über dem Körper der algebraischen Zahlen linear unabhängig.

Zum Beispiel erhält man durch die Wahl von $n = 2$, $\alpha_2 = 0$ den Satz von LINDEMANN und HERMITE.

Dieser Satz erlaubt die folgende äquivalente Formulierung, die ein Resultat zur algebraischen Unabhängigkeit darstellt.

8.16. Wenn $\alpha_1, \ldots, \alpha_n$ über $\mathbb{Q}$ linear unabhängige algebraische Zahlen sind, dann sind $e^{\alpha_1}, \ldots, e^{\alpha_n}$ algebraisch unabhängig über $\mathbb{Q}$.

Ein sehr nützliches Werkzeug im modernen Beweis der Sätze von LINDEMANN und WEIERSTRASS ist das folgende Ergebnis aus der Linearen Algebra, bekannt als Siegels Lemma.

Sei K ein Zahlkörper mit Grad $n = [K : \mathbb{Q}]$ und $\sigma_1, \ldots, \sigma_n$ die Isomorphismen von K in $\mathbb{C}$. Für jedes $\alpha \in K$ sei $\|\alpha\| = \max_{1<i<n}\{|\sigma_i(\alpha)|\}$.

Mit gegebener reeller Zahl $A > 0$, den ganzen Zahlen $d > 0$ und r mit $1 \le r < n$ sei $G_K(d, A, r)$ die Menge der Systeme linearer Gleichungen

$$\sum_{j=1}^{n} \alpha_{ij} X^j = 0 \quad (i = 1, \ldots, r)$$

mit den folgenden Eigenschaften:

(1) jedes $\alpha_{ij} \in K$;

(2) für jedes $i = 1, \ldots, r$ gibt es eine ganze Zahl d_i mit $0 < d_i \le d$ derart, dass $d_i \alpha_{ij}$ eine algebraische ganze Zahl ist (für jedes $j = 1, \ldots, n$);

(3) $\max_{i,j}\{\|\alpha_{ij}\|\} \le A$.

Siegels Lemma ist das folgende:

8.17. Seien K, d, A, r wie oben. Dann gibt es eine reelle Zahl $c_K > 0$ derart, dass jedes System linearer Gleichungen in der Menge $S_K(d, A, r)$ eine nichttriviale Lösung $(\zeta_1, \ldots, \zeta_n)$ besitzt, wobei jedes ζ_j eine algebraische ganze Zahl ist und

$$\max_{1 \le j \le n} \|\zeta_j\| \le c_K + c_K (c_K n d A)^{\frac{r}{n-r}}.$$

D Ein Resultat von Siegel über Exponenten

An das folgende interessante Resultat, ein Spezialfall eines Satzes von Siegel, wurde in einem Artikel von Halberstam erinnert. Es war im Putnam Wettbewerb von 1972 als Aufgabe gestellt worden und keiner der 2000 Kandidaten konnte diese lösen. Ich gebe den Beweis unten an, dieser folgt Halberstams Artikel.

8.18. Wenn α eine reelle positive Zahl ist und 2^α, 3^α, 5^α, …, p^α, … ganze Zahlen sind (für jedes prime p), dann ist α eine ganze Zahl.

Beweis. Aus der Voraussetzung folgt, dass n^α für jede ganze Zahl n ganz ist.

Angenommen α wäre keine ganze Zahl. Dann sei $k = [\alpha]$, also $0 \le k < \alpha < k + 1$. Die Beweismethode verwendet endliche Differenzen.

Für eine beliebig oftmalig differenzierbare Funktion $f(x)$ in der reellen Variablen x sei

$$\Delta f(x) = f(x + 1) - f(x).$$

Somit gibt es θ_1, $0 < \theta_1 < 1$ derart, dass

$$\Delta f(x) = f'(x + \theta_1).$$

(Man beachte, dass θ_1 von x abhängig ist.)

In gleicher Weise sei

$$\Delta^2 f(x) = \Delta(\Delta f(x)) = \Delta f(x+1) - \Delta f(x) = f(x+2) - 2f(x+1) + f(x).$$

Es gilt auch

$$\Delta^2 f(x) = f'(x + 1 + \theta_1) - f'(x + \theta_1) = f''(x + \theta_2),$$

wobei $0 < \theta_1 < \theta_2 < 2$ (θ_2 hängt von x, θ_1 ab).

Allgemein sei mit $r \geq 1$, $\Delta^r f(x) = \Delta(\Delta^{r-1} f(x))$, also

$$\Delta^r f(x) = \sum_{i=0}^{r} (-1)^{r-i} \binom{r}{i} f(x + i) = f^{(r)}(x + \theta_r),$$

mit $0 < \theta_r < r$.

Man nehme nun $f(x) = x^\alpha$, also

$$\Delta^r x^\alpha = \sum_{i=0}^{r} \binom{r}{i} (-1)^{r-i} (x + i)^\alpha,$$

somit ist $\Delta^r x^\alpha$ eine ganze Zahl für jede ganze Zahl $x > 0$. Aber es gilt auch

$$\Delta^r x^\alpha = \alpha(\alpha - 1) \cdots (\alpha - r + 1)(x + \theta)^{\alpha - r},$$

wobei $0 < \theta < r$. Wenn man $r = k + 1$, $x = n$ wählt und schreibt $(\Delta^r x^\alpha)(n) = \Delta^r n^\alpha$, so erhält man

$$\Delta^{k+1} n^\alpha = \alpha(\alpha - 1) \cdots (\alpha - k + 1)(\alpha - k)(n + \theta)^{\alpha - k - 1},$$

mit $0 < \theta < k + 1$. Daher,

$$0 < \Delta^{k+1} n^\alpha = \frac{\alpha(\alpha - 1) \cdots (\alpha - k)}{(n + \theta)^{k+1-\alpha}} < \frac{\alpha^{k+1}}{n^{k+1-\alpha}} < 1$$

sofern $n > \alpha^{\frac{k+1}{k+1-\alpha}}$. Dies ist ein Widerspruch, da $\Delta^{k+1} n^\alpha$ eine ganze Zahl ist. □

Siegel bewies eigentlich den folgenden Satz:

8.19. Wenn α eine reelle positive Zahl ist und wenn es drei verschiedene Primzahlen p_1, p_2, p_3 gibt mit der Eigenschaft, dass p_1^α, p_2^α, p_3^α algebraische Zahlen sind, dann ist $\alpha \in \mathbb{Q}$.

Oder äquivalent, wenn $\alpha > 0$ und wenn α nicht rational ist, dann gibt es höchstens zwei Primzahlen p_1, p_2 derart, dass p_1^α, p_2^α algebraische Zahlen sind.

E Hilberts siebtes Problem

Wie bereits im historischen Überblick erwähnt, wurde Hilberts siebtes Problem zur selben Zeit und unabhängig voneinander von Gel'fond und Schneider im Jahr 1934 gelöst.

Ich notiere zunächst die folgenden äquivalenten Formulierungen:

8.20. Die folgenden Aussagen sind äquivalent:

(1) Wenn α, β algebraische Zahlen sind mit $\alpha \neq 0$ sowie $\log \alpha \neq 0$, und wenn β irrational ist, dann ist $\alpha^\beta = \exp(\beta \log \alpha)$ transzendent.

(2) Wenn α, $\beta \in \mathbb{Q}^{\mathrm{alg}}$, α, $\beta \neq 0$ und wenn $\log \alpha$, $\log \beta$ linear unabhängig über $\mathbb{Q}$ sind, dann sind $\log \alpha$, $\log \beta$ linear unabhängig über $\mathbb{Q}^{\mathrm{alg}}$.

(3) Wenn β, $\lambda \in \mathbb{C}$, $\lambda \neq 0$, $\beta \notin \mathbb{Q}$, dann ist eine der Zahlen e^λ, β, $e^{\beta\lambda}$ transzendent.

Beweis. (1) $\Rightarrow$ (2) Sei α, $\beta \in \mathbb{Q}^{\mathrm{alg}}$ mit α, $\beta \neq 0, 1$ und angenommen, dass $\log \alpha$, $\log \beta$ linear unabhängig über $\mathbb{Q}$ sind. Wenn es γ, $\delta \in \mathbb{Q}^{\mathrm{alg}}$ gibt mit $\delta \neq 0$ (zum Beispiel) derart, dass $\gamma \log \alpha + \delta \log \beta = 0$, dann $\gamma \neq 0$ und $\frac{\log \alpha}{\log \beta} = -\frac{\gamma}{\delta} = \mu \in \mathbb{Q}^{\mathrm{alg}}$ mit $\mu \notin \mathbb{Q}$. Nach (1) ist α^μ transzendent. Allerdings ist $\alpha^\mu = e^{\mu \log \alpha} = e^{\log \beta} = \beta$, was ein Widerspruch ist.

(2) $\Rightarrow$ (3) Sei β, $\lambda \in \mathbb{C}$ mit $\lambda \neq 0$, $\beta \notin \mathbb{Q}$ und angenommen, dass e^λ, β, $e^{\beta\lambda}$ algebraische Zahlen sind. Man beachte, dass λ, $\beta\lambda$ linear unabhängig über $\mathbb{Q}$ sind. Nach (2) sind λ, $\beta\lambda$ auch linear unabhängig über $\mathbb{Q}^{\mathrm{alg}}$, daher ist $\beta = \frac{\beta\lambda}{\beta}$ transzendent, was ein Widerspruch ist.

(3) $\Rightarrow$ (1) Sei $\alpha \in \mathbb{Q}^{\mathrm{alg}}$ mit $\alpha \neq 0, 1$ und $\beta \in \mathbb{Q}^{\mathrm{alg}} \setminus \mathbb{Q}$. Sei $\lambda = \log \alpha \neq 0$. Da $\alpha = e^\lambda$ und β algebraische Zahlen sind, ist $e^{\beta\lambda} = e^{\beta \log \alpha} = \alpha^\beta$ nach (3) transzendent. □

Der Satz von GEL'FOND und SCHNEIDER ist der folgende:

8.21. Wenn $\alpha \in \mathbb{Q}^{\text{alg}}$, $\alpha \neq 0$, $\log \alpha \neq 0$ und wenn $\beta \in \mathbb{Q}^{\text{alg}} \setminus \mathbb{Q}$, dann ist α^β eine transzendente Zahl.

Mithilfe dieses Satzes kann man ableiten, dass $\sqrt{2}^{\sqrt{2}}$ eine transzendente Zahl ist und damit ist die Frage beantwortet, die dieses Kapitel motivierte. Aber man sieht auch, dass wenn a, b ganze Zahlen mit der Eigenschaft sind, dass $a^m \neq b^n$ (für alle ganzen Zahlen m, n ungleich Null), dann ist $\frac{\log a}{\log b}$ transzendent (dies war bereits von EULER vermutet worden).

In gleicher Weise,

8.22. e^π ist eine transzendente Zahl.

Beweis. Da i, $e^{i\pi} = -1$ algebraische Zahlen sind, folgt nach (3) oben, dass e^π transzendent ist. □

Bereits im Jahr 1932 hatten KOKSMA und POPKEN gezeigt, dass e^π transzendent ist. Die Methoden von GEL'FOND und von SCHNEIDER wurden auch für den Nachweis der Transzendenz anderer Zahlen eingesetzt.

F Die Arbeit von Baker

BAKER begann 1968 mit der Veröffentlichung einer Reihe entscheidender Artikel über effektive untere Schranken von Linearformen in Logarithmen. Ich werde mich an dieser Stelle damit begnügen, diejenigen seiner Resultate zu zitieren, die für die Theorie der transzendenten Zahlen am wichtigsten sind. BAKERs eigenes Buch (1975) sei für weitere Ergebnisse und Beweise wärmstens empfohlen.

8.23. Es seien $\alpha_1, \ldots, \alpha_n$ algebraische Zahlen verschieden von Null und $\log \alpha_1, \ldots, \log \alpha_n$ linear unabhängig über $\mathbb{Q}$. Dann sind $1, \log \alpha_1, \ldots, \log \alpha_n$ linear unabhängig über $\mathbb{Q}^{\text{alg}}$.

Dieses Resultat beinhaltet viele wichtige Korollare, die einfach abzuleiten sind.

8.24. Es seien $\alpha_1, \ldots, \alpha_n, \beta_1, \ldots, \beta_n$ algebraische Zahlen und $\alpha_1, \ldots, \alpha_n$ verschieden von Null. Dann ist $\theta = \sum_{i=1}^n \beta_i \log \alpha_i \neq 0$ transzendent.

Beweis. Wenn θ eine algebraische Zahl wäre, dann würde folgen, dass $(-\theta) \times 1 + \sum_{i=1}^{n} \beta_i \log \alpha_i = 0$, also wären $\log \alpha_1, \ldots, \log \alpha_n$ linear unabhängig über $\mathbb{Q}^{\text{alg}}$ und somit auch über $\mathbb{Q}$. Also gäbe es $r_1, \ldots, r_n \in \mathbb{Q}$, nicht alle gleich 0 derart, dass $\sum_{i=1}^{n} r_i \log \alpha_i = 0$. Beispielsweise sei $r_n \neq 0$; dann

$$\begin{aligned} 0 &= r_n(-\theta + \sum_{i=1}^{n} \beta_i \log \alpha_i) \\ &= r_n(-\theta) + (r_n\beta_1 - r_1\beta_n) \log \alpha_1 + (r_n\beta_2 - r_2\beta_n) \log \alpha_2 \\ &\quad + \cdots + (r_n\beta_{n-1} - r_{n-1}\beta_n) \log \alpha_{n-1}. \end{aligned}$$

Mit Induktion über n gelangt man dazu, dass $r_n\theta$ transzendent ist und somit konnte θ nicht algebraisch sein. □

8.25. Wenn $n \geq 0$ und $\alpha_1, \ldots, \alpha_n, \beta_1, \ldots, \beta_n$ algebraische Zahlen ungleich Null sind, dann ist $e^{\beta_0} \alpha_1^{\beta_1} \cdots \alpha_n^{\beta_n}$ transzendent.

Beweis. Wenn $\theta = e^{\beta_0} \alpha_1^{\beta_1} \cdots \alpha_n^{\beta_n}$ algebraisch ist, dann ist $\beta_1 \log \alpha_1 + \cdots + \beta_n \log \alpha_n - \log \theta = -\beta_0 \neq 0$ algebraisch, was dem vorangegangenen Satz widerspricht. □

Das folgende Lemma wird im nächsten Satz benötigt:

Lemma. *Es seien $\gamma_1, \ldots, \gamma_m$, $\delta_1, \ldots, \delta_m$ für $m \geq 1$ algebraische Zahlen, wobei jedes $\gamma_i \neq 0$, 1 sowie $\delta_1, \ldots, \delta_m$ linear unabhängig über $\mathbb{Q}$ sind. Dann ist $\sum_{i=1}^{m} \delta_i \log \gamma_i \neq 0$.*

Beweis. Für $m = 1$ ist die Aussage wahr. Durch Induktion über m: Falls $\sum_{i=1}^{m} \delta_i \log \gamma_i = 0$, dann sind $\log \gamma_1, \ldots, \log \gamma_m$ linear abhängig über $\mathbb{Q}^{\text{alg}}$ und somit sind sie nach **(8.22)** auch linear abhängig über $\mathbb{Q}$. Also gibt es $r_1, \ldots, r_m \in \mathbb{Q}$, nicht sämtlich gleich 0 derart, dass $\sum_{i=1}^{m} r_i \log \gamma_i = 0$. Zum Beispiel sei $r_m \neq 0$, damit

$$\sum_{i=1}^{m-1} r_m \delta_i \log \gamma_i = -r_m \delta_m \log \gamma_m = \delta_m (\sum_{i=1}^{m-1} r_i \log \gamma_i),$$

und so

$$\sum_{i=1}^{m-1} (r_m \delta_i - \delta_m r_i) \log \gamma_i = 0.$$

Aber $r_m\delta_1 - \delta_m r_1, \ldots, r_m\delta_{m-1} - \delta_m r_{m-1}$ sind linear unabhängig über $\mathbb{Q}$, wie man leicht sehen kann.

Nach Induktion ist dies ein Widerspruch. □

8.26. Es seien $\alpha_1, \ldots, \alpha_n$, $\beta_1, \ldots, \beta_n$ algebraische Zahlen, wobei jedes $\alpha_i \neq 0$, 1 sowie $1, \beta_1, \ldots, \beta_n$ linear unabhängig über $\mathbb{Q}$ sind. Dann ist $\alpha_1^{\beta_1} \cdots \alpha_n^{\beta_n}$ transzendent.

Beweis. Wenn $\theta = \alpha_1^{\beta_1} \cdots \alpha_n^{\beta_n}$ algebraisch ist, dann ist $\theta \neq 0$ sowie $\theta \neq 1$, sonst wäre $\sum_{i=1}^{n} \beta_i \log \alpha_i = 0$, was dem Lemma widerspricht. Also $\sum_{i=1}^{n} \beta_i \log \alpha_i - \log \theta = 0$.

Aber $1, \beta_1, \ldots, \beta_n$ sind linear unabhängig über $\mathbb{Q}$, ein Widerspruch zum Lemma. □

8.27. Wenn α irgendeine algebraische Zahl ungleich Null ist, dann ist $\pi + \log \alpha$ transzendent.

Beweis. Aus $e^{i\pi} = -1$ folgt, dass $\pi = -i \log(-1)$. Wenn $\pi + \log \alpha = \beta \in \mathbb{Q}^{\text{alg}}$, dann ist $-i \log(-1) + \log \alpha - \beta$. Also sind $\log(-1)$, $\log \alpha, 1$ linear abhängig über $\mathbb{Q}^{\text{alg}}$, damit sind nach **(8.22)** $\log(-1)$, $\log \alpha$ linear abhängig über $\mathbb{Q}$. Also gibt es ganze Zahlen m, n, nicht beide gleich Null, so dass $m \log(-1) + n \log \alpha = 0$. Wenn $n = 0$, dann $m \neq 0$ und so $\log(-1) = 0$, daher $\pi = 0$, ein Widerspruch. Also $n \neq 0$ und $(-1)^m \alpha^n = 1$ impliziert $\alpha^{2n} = 1$, daher $2n \log \alpha = 2ki\pi$ (für eine ganze Zahl k), somit $\beta = \pi + \pi ik$, also wäre π eine algebraische Zahl. Also ist $i\pi$ algebraisch und nach **(8.21)** folgte, dass $-1 = e^{i\pi}$ transzendent wäre, was nicht sein kann. □

Ich möchte anmerken, dass **(8.24)** den Satz von Lindemann und Hermite enthält, **(8.25)** enthält den Satz von Gel'fond und Schneider, während **(8.26)** als Spezialfall die Transzendenz von π beinhaltet. All dies zeigt die Stärke von Bakers Satz.

Eine weiterer wichtiger Punkt von Bakers Satz ist die *effektive* Bestimmung unterer Schranken für Linearformen in Logarithmen und deren Anwendung zur effektiven Bestimmung von Lösungen einer umfassenden Klasse diophantischer Gleichungen.

Bedauerlicherweise werde ich diese Verbindung hier nicht behandeln.

G Die Vermutung von Schanuel

Der Beweis, dass spezielle transzendente Zahlen algebraisch unabhängig über $\mathbb{Q}$ sind, ist selten eine einfache Aufgabe. Es ist also von Vorteil sich zu überlegen, was richtig sein *sollte*.

In seinem Buch von 1966 gab LANG eine interessante Vermutung von SCHANUEL an. Zunächst erinnere ich an einige Begriffe.

Sei L eine Körpererweiterung des Körpers K (ich werde meist mit dem Fall befasst sein, dass $K = \mathbb{Q}$ (oder $\mathbb{Q}^{\mathrm{alg}}$)).

Angenommen es existieren n Elemente $\alpha_1, \ldots, \alpha_n \in L$ mit den folgenden Eigenschaften:

(1) $\alpha_1, \ldots, \alpha_n$ sind algebraisch unabhängig über K; d.h. wenn $f \in K[X_1, \ldots, X_n]$ und $f(\alpha_1, \ldots, \alpha_n) = 0$, dann ist f das Nullpolynom;

(2) wenn $\beta \in L$, dann ist β algebraisch über dem von $\alpha_1, \ldots, \alpha_n$ erzeugten Körper $K(\alpha_1, \ldots, \alpha_n)$.

In diesem Fall ist $\{\alpha_1, \ldots, \alpha_n\}$ eine *Transzendenzbasis* von $L|K$. Man kann zeigen, dass jede andere Transzendenzbasis dieselbe Anzahl von n Elementen hat. Die Zahl n nennt man den *Transzendenzgrad* von $L|K$ und bezeichnet ihn mit $\mathrm{tr\,deg}(L|K)$.

Wenn $L = K(\alpha_1, \ldots, \alpha_n)$, dann $\mathrm{tr\,deg}(L|K) \leq n$ und es gibt eine Teilmenge von $\{\alpha_1, \ldots, \alpha_n\}$, die eine Transzendenzbasis von $L|K$ ist. Darüberhinaus ist die Menge $\{\alpha_1, \ldots, \alpha_n\}$ eine Transzendenzbasis, falls gilt $\mathrm{tr\,deg}(L|K) = n$.

Ich möchte auch erwähnen, dass

$$\mathrm{tr\,deg}(\mathbb{Q}(\alpha_1, \ldots, \alpha_n)|\mathbb{Q}) = \mathrm{tr\,deg}(\mathbb{Q}^{\mathrm{alg}}(\alpha_1, \ldots, \alpha_n)|\mathbb{Q}^{\mathrm{alg}})$$

(wobei $\alpha_1, \ldots, \alpha_n$ beliebige komplexen Zahlen sind).

Schanuels Vermutung ist die folgende:

Vermutung (S). *Wenn $\alpha_1, \ldots, \alpha_n \in \mathbb{C}$ linear unabhängig über $\mathbb{Q}$ sind, dann ist* $\mathrm{tr\,deg}(\mathbb{Q}(\alpha_1, \ldots, \alpha_n, e^{\alpha_1}, \ldots, e^{\alpha_n})|\mathbb{Q}) \geq n$.

Diese Vermutung ist zum Beispiel wahr, wenn $\alpha_1, \ldots, \alpha_n \in \mathbb{Q}^{\mathrm{alg}}$. Tatsächlich wird (S) unter dieser zusätzlichen Annahme zum Satz von LINDEMANN und WEIERSTRASS.

Es gibt viele interessante Vermutungen über transzendente Zahlen, die mehr oder weniger direkt aus der allumfassenden Vermutung von Schanuel folgen.

GEL'FOND schlug vor:

Vermutung (S_1). *Wenn $\alpha_1, \ldots, \alpha_n, \beta_1, \ldots, \beta_n \in \mathbb{Q}^{\mathrm{alg}}$, wobei jedes $\beta_i \neq 0$, und wenn sowohl $\alpha_1, \ldots, \alpha_n$ als auch $\log \beta_1, \ldots, \log \beta_n$ linear unabhängig über $\mathbb{Q}$ sind, dann sind $e^{\alpha_1}, \ldots, e^{\alpha_n}$, $\log \beta_1, \ldots, \log \beta_n$ algebraisch unabhängig über $\mathbb{Q}^{\mathrm{alg}}$.*

In der Tat folgt (S_1) aus (S), denn

$$\begin{aligned}&\text{tr deg}(\mathbb{Q}^{\text{alg}}(e^{\alpha_1},\dots,e^{\alpha_n},\log\beta_1,\dots,\log\beta_n)|\mathbb{Q}^{\text{alg}})\\&=\text{tr deg}(\mathbb{Q}^{\text{alg}}(\alpha_1,\dots,\alpha_n,e^{\alpha_1},\dots,e^{\alpha_n},\log\beta_1,\dots,\log\beta_n,\\&\qquad\qquad\beta_1,\dots,\beta_n)|\mathbb{Q}^{\text{alg}})\\&=2n,\end{aligned}$$

daher sind die Zahlen $e^{\alpha_1},\dots,e^{\alpha_n},\ \log\beta_1,\dots,\log\beta_n$ algebraisch unabhängig über $\mathbb{Q}^{\text{alg}}$.

Ein Spezialfall der Vermutung (S_1) ist der folgende:

Vermutung (S_2). *Wenn $\beta_1,\dots,\beta_n\in\mathbb{Q}^{\text{alg}}$, wobei jedes $\beta_i\neq 0$, und wenn $\log\beta_1,\dots,\log\beta_n$ linear unabhängig über $\mathbb{Q}$ sind, dann sind $\log\beta_1,\dots,\log\beta_n$ algebraisch unabhängig über $\mathbb{Q}^{\text{alg}}$.*

Ich erinnere daran, dass Baker Proposition **(8.21)** bewiesen hat, die allerdings schwächer ist als Vermutung (S_2).

Die folgende Vermutung ist ebenfalls eine Konsequenz aus (S):

Vermutung (S_3). *Wenn $\alpha,\beta_1,\dots,\beta_n\in\mathbb{Q}^{\text{alg}}$, $\alpha\neq 0,1$ und $1,\beta_1,\dots,\beta_n$ linear unabhängig über $\mathbb{Q}$ sind, dann sind $\log\alpha$, α^{β_1}, …, α^{β_n} algebraisch unabhängig über $\mathbb{Q}^{\text{alg}}$.*

Tatsächlich sind $\log\alpha,\beta_1\log\alpha,\dots,\beta_n\log\alpha$ linear unabhängig über $\mathbb{Q}$ und damit,

$$\text{tr deg}(\mathbb{Q}^{\text{alg}}(\log\alpha,\beta_1\log\alpha,\dots,\beta_n\log\alpha,\alpha,\alpha^{\beta_1},\dots,\alpha^{\beta_n})|\mathbb{Q}^{\text{alg}})\geq n+1.$$

Aus $\alpha,\beta_1,\dots,\beta_n\in\mathbb{Q}^{\text{alg}}$ folgt notwendigerweise, dass $\log\alpha,\alpha^{\beta_1},\dots,\alpha^{\beta_n}$ algebraisch unabhängig über $\mathbb{Q}$ sind.

Der Spezialfall von (S_3) für $n=1$ ist die Vermutung:

Vermutung (S_4). *Wenn $\alpha,\beta\in\mathbb{Q}^{\text{alg}}$, $\alpha\neq 0,1$, und $\beta\notin\mathbb{Q}$, dann sind $\log\alpha$, α^{β} algebraisch unabhängig über $\mathbb{Q}^{\text{alg}}$.*

Der folgende Spezialfall von (S_3) ist eine Vermutung von Gel'fond:

Vermutung (S_5). *Wenn $\alpha,\ \beta\in\mathbb{Q}^{\text{alg}}$ und wenn β den Grad $d\geq 2$ hat, dann gilt* $\text{tr deg}(\mathbb{Q}(\alpha^{\beta},\dots,\alpha^{\beta^{d-1}})|\mathbb{Q})=d-1$.

Es sind $1,\beta,\beta^2,\dots,\beta^{d-1}$ linear unabhängig über $\mathbb{Q}$; nach (S_3) sind $\log\alpha,\alpha^{\beta},\dots,\alpha^{\beta^{d-1}}$ algebraisch unabhängig über $\mathbb{Q}$, damit ist $\text{tr deg}(\mathbb{Q}(\alpha^{\beta},\dots,\alpha^{\beta^{d-1}})|\mathbb{Q})=d-1$.

Die folgende Vermutung, die auch aus (S) folgt, wurde in Spezialfällen von Lang und Ramachandra erwähnt:

Vermutung (S_6). *Wenn $\alpha_1, \ldots, \alpha_n$ linear unabhängig über $\mathbb{Q}$ sind und β transzendent ist, dann gilt*

$$\text{tr deg}(\mathbb{Q}(e^{\alpha_1}, \ldots, e^{\alpha_n}, e^{\alpha_1\beta}, \ldots, e^{\alpha_n\beta})|\mathbb{Q}) \geq n - 1.$$

Ich zeige, dass (S_6) aus (S) folgt: ordne die Zahlen $\alpha_1, \ldots, \alpha_n$ derart, dass $\{\alpha_1, \ldots, \alpha_n, \beta\alpha_1, \ldots, \beta\alpha_m\}$ mit $0 \leq m \leq n$ eine Basis des $\mathbb{Q}$-Vektorraumes ist, der durch $\{\alpha_1, \ldots, \alpha_n, \beta\alpha_1, \ldots, \beta\alpha_n\}$ erzeugt wird. Dann gilt $\text{tr deg}(\mathbb{Q}(\alpha_1, \ldots, \alpha_n, \beta)|\mathbb{Q}) \leq m + 1$. Da β transzendent ist, gibt es tatsächlich eine Transzendenzbasis von $\mathbb{Q}(\alpha_1, \ldots, \alpha_n, \beta)|\mathbb{Q}$, diese ist $\{\alpha_{i_1}, \ldots, \alpha_{i_s}, \beta\}$ (mit $1 \leq i_1 < i_2 < \cdots < i_s \leq n$); weiter sind $\alpha_1, \ldots, \alpha_n, \beta\alpha_{i_1}, \ldots, \beta\alpha_{i_s}$ linear unabhängig über $\mathbb{Q}$, also $s+n \leq m+n$ und daher $s \leq m$ wie gefordert.

Andererseits leitet sich aus (S) ab, dass

$$\text{tr deg}(\mathbb{Q}(\alpha_1, \ldots, \alpha_n, \beta\alpha_1, \ldots, \beta\alpha_m, e^{\alpha_1}, \ldots, e^{\alpha_n}, e^{\beta\alpha_1}, \ldots, e^{\beta\alpha_m})|\mathbb{Q}) \geq n + m,$$

damit auch

$$\text{tr deg}(\mathbb{Q}(\alpha_1, \ldots, \alpha_n, \beta\alpha_1, \ldots, \beta\alpha_n, e^{\alpha_1}, \ldots, e^{\alpha_n}, e^{\beta\alpha_1}, \ldots, e^{\beta\alpha_n})|\mathbb{Q}) \geq n + m.$$

Ein Vergleich mit dem Transzendenzgrad von $\mathbb{Q}(\alpha_1, \ldots, \alpha_n, \beta)|\mathbb{Q}$ ergibt, dass mindestens $n - 1$ der Zahlen e^{α_i}, $e^{\alpha_i\beta}$ $(i = 1, \ldots, n)$ algebraisch unabhängig sind.

Hier eine weitere interessante Konsequenz aus (S) (log bezeichnet den Hauptzweig des Logarithmus).

Vermutung (S_7). *Die Zahlen e, e^π, e^e, e^i, π, π^π, π^e, π^i, 2^π, 2^e, 2^i, $\log\pi$, $\log 2$, $\log 3$, $\log\log 2$, $(\log 2)^{\log 3}$, $2^{\sqrt{2}}$ sind algebraisch unabhängig über $\mathbb{Q}$ (und sind insbesondere transzendent).*

Beweis. Ich beginne mit der Bemerkung, dass $i\pi$, $\log 2$ linear unabhängig über $\mathbb{Q}$ sind. Nach (S) ist $\text{tr deg}(\mathbb{Q}(i\pi, \log 2, -1, 2|\mathbb{Q})) = 2$, also sind $i\pi$, $\log 2$ algebraisch unabhängig über $\mathbb{Q}$; dies gilt damit auch für π und $\log 2$. Daher sind 2, 3, π, $\log 2$ multiplikativ unabhängig: Wenn $2^a 3^b \pi^c (\log 2)^d = 1$ (mit a, b, c, $d \in \mathbb{Z}$), dann $a = b = c = d = 0$. Somit sind $\log\pi$, $\log 2$, $\log 3$, $\log\log 2$ linear unabhängig über $\mathbb{Q}$ und demzufolge auch $i\pi$, $\log\pi$, $\log 2$, $\log 3$, $\log\log 2$. Nach (S),

$$\text{tr deg}(\mathbb{Q}(i\pi, \log\pi, \log 2, \log 3, \log\log 2, -1, \pi, 2, 3, \log 2)|\mathbb{Q}) = 5,$$

daher sind $\pi, \log\pi, \log 2, \log 3, \log\log 2$ algebraisch unabhängig über $\mathbb{Q}$. Demnach sind $1,\ i\pi,\ \log\pi,\ \log 2,\ \log 3,\ \log\log 2$ linear unabhängig über $\mathbb{Q}$. Nach (S),

$$\operatorname{tr\,deg}(\mathbb{Q}(1, i\pi, \log\pi, \log 2, \log 3, \log\log 2, e, -1, \pi, 2, 3, \log 2)|\mathbb{Q}) = 6,$$

also sind $e,\ \pi,\ \log\pi,\ \log 2,\ \log 3,\ \log\log 2$ algebraisch unabhängig. Somit sind $1,\ i\pi,\ \pi,\ \log\pi,\ e,\ e\log\pi,\ \pi\log\pi,\ \log 2,\ \pi\log 2,\ e\log 2,\ i\log 2,\ i,\ i\log\pi,\ \log 3,\ \log\log 2,\ (\log 3)(\log\log 2),\ \sqrt{2}\log 2$ linear unabhängig über $\mathbb{Q}$. Nach (S),

$$\begin{aligned}\operatorname{tr\,deg}(\mathbb{Q}(&i\pi, \pi, \log\pi, e, e\log\pi, \pi\log\pi, \log 2, \pi\log 2, e\log 2, i\log 2,\\ &i, i\log\pi, \log 3, \log\log 2, (\log 3)(\log\log 2), \sqrt{2}\log 2, -1, e^\pi, \pi,\\ &e^e, \pi^e, \pi^\pi, 2, 2^\pi, 2^e, 2^i, e^i, \pi^i, 3, \log 2, (\log 2)^{\log 3}, 2^{\sqrt{2}})|\mathbb{Q}) = 17.\end{aligned}$$

Daher sind $\pi,\ \log\pi,\ e,\ \log 2,\ \log 3,\ \log\log 2,\ e^\pi,\ e^e,\ \pi^e,\ \pi^\pi,\ 2^\pi,\ 2^e,\ 2^i,\ e^i,\ \pi^i,\ (\log 2)^{\log 3},\ 2^{\sqrt{2}}$ algebraisch unabhängig über $\mathbb{Q}$. □

Lang untersuchte die folgende Vermutung. Sei K_1 der Körper aller Zahlen, die algebraisch über dem Körper $\mathbb{Q}^{\mathrm{alg}}(e^\alpha)$ sind. Sei K_2 der Körper aller Zahlen, die algebraisch über dem Körper $K_1(e^\alpha)_{\alpha\in K_1}$ sind. Definiere die Körper $K_3,\ K_4,\ \ldots$ in derselben Weise. Sei weiter $K = \bigcup_{n\geq 1} K_n$.

Vermutung (S_8). $\pi \notin K$.

Lang skizzierte, wie ein Beweis dieser Vermutung sich als Konsequenz von (S) ergeben kann.

Es gab die klassischen Resultate algebraischer Unabhängigkeit von Hermite, Weierstrass und die späteren Ergebnisse von Baker, die allesamt die Exponential- und Logarithmusfunktionen beinhalten. Lange Zeit wünschte man sich, ein Ergebnis zu algebraischer Unabhängigkeit mit der Gamma-Funktion $\Gamma(x)$ zu finden.

Ein Meisterstück tiefschürfender Erforschung algebraischer Unabhängigkeit gelang Nesterenko 1997 mit untenstehendem Resultat (siehe auch Gramain (1998)):

8.28. Die Zahlen $\pi,\ e^\pi,\ \Gamma(\frac{1}{4})$ sind algebraisch unabhängig über $\mathbb{Q}$.

Dieser Satz wurde von Experten des Gebiets wie auch von Mathematikern mit breiterer Ausrichtung gleichermaßen bejubelt. In anderen Mathematikerkreisen—und darunter sogar guten—wunderte man sich,

warum Zeit und Energie Fragen von praktischer Belanglosigkeit wie dieser geopfert werden sollten. Oder auch Zahlen wie $\sqrt{2}^{\sqrt{2}}$ ....

Mathematik hat den einzigartigen Charakter, eine wissenschaftliche Disziplin zu sein, die viele Anwendungen in allen möglichen Arten anderer Wissenschaften sowie im praktischen Leben findet. Aber Mathematik ist auch eine Kunst, wobei die Schönheit in den Symmetrien, Mustern und tief verwundenen Beziehungen liegt, die den Betrachter verzaubern. Entdeckungen die die Erfindung neuer Methoden sowie großen Scharfsinn erfordern, müssen in der Tat bejubelt werden—zumindest von einem gewissen Standpunkt aus betrachtet. Werden diese Entdeckungen eines Tages irgendeine praktische Verwendung haben? Ist dies eine berechtigte Frage? Tatsächlich gibt es unzählige Beispiele von Theorien, bei denen man jahrhundertelang annahm, sie seien überflüssige Spekulation. Wie beim Studium der Primzahlen, die heute die Hauptstütze kritischer Anwendungen im Nachrichtenwesen sind. Es ist die innewohnende Qualität eines neuen Resultats, das ihm Bedeutung verleiht.

H Transzendenzmaß und die Klassifikation von Mahler

Um komplexe Zahlen zu klassifizieren, betrachtete Mahler die Werte von Polynomausdrücken und maß, wie nahe sie bei Null liegen können.

Seien $n \geq 1$, $H \geq 1$ ganze Zahlen, $\mathbb{Z}_{n,H}[X]$ die Menge aller Polynome $f(X) \in \mathbb{Z}[X]$ mit einem Grad von höchstens n und einem maximalen Koeffizienten von höchstens H; d.h., $f(X) = \sum_{i=0}^{n} a_i X^i$ mit $a_i \in \mathbb{Z}$ und $\max\{|a_i|\} \leq H$. Die Menge $\mathbb{Z}_{n,H}[X]$ ist offensichtlich endlich.

Für $\alpha \in \mathbb{C}$ sei

$$w_{n,H}(\alpha) = \min\{|f(\alpha)| : f \in \mathbb{Z}_{n,H}[X] \text{ und } f(\alpha) \neq 0\}.$$

Wenn man $f(X) = 1$ nimmt, so erhält man $0 < w_{n,H}(\alpha) \leq 1$. Auch gilt für $n \leq n'$, $H \leq H'$, dass $w_{n,H}(\alpha) \geq w_{n',H'}(\alpha)$.

Sei $w_n(\alpha) = \limsup_{H\to\infty} \frac{-\log w_{n,H}(\alpha)}{\log H}$ für alle $n \geq 1$, und sei $w(\alpha) = \limsup_{n\to\infty} \frac{w_n(\alpha)}{n}$.

Daher $0 \leq w_n(\alpha) \leq \infty$ und $w_n(\alpha) \leq w_{n+1}(\alpha)$ für $n \geq 1$. Somit $0 \leq w(\alpha) \leq \infty$.

Sei $\mu(\alpha) = \inf\{n \mid w_n(\alpha) = \infty\}$, also $1 \leq \mu(\alpha) \leq \infty$, und wenn $\mu(\alpha) < \infty$, dann $w(\alpha) = \infty$.

Dies führt zu folgender Unterteilung der komplexen Zahlen in vier disjunkte Klassen wie von Mahler (1930, 1932b) vorgeschlagen:

(1) α ist eine *A-Zahl*, wenn $w(\alpha) = 0$, $\mu(\alpha) = \infty$;
(2) α ist eine *S-Zahl*, wenn $0 < w(\alpha) < \infty$, $\mu(\alpha) = \infty$;
(3) α ist eine *T-Zahl*, wenn $w(\alpha) = \infty$, $\mu(\alpha) = \infty$;
(4) α ist eine *U-Zahl*, wenn $w(\alpha) = \infty$, $\mu(\alpha) < \infty$.
Mahler bewies:

8.29. α ist eine A-Zahl genau dann, wenn es eine algebraische Zahl ist.

Darüberhinaus:

8.30. Wenn α, β Zahlen verschiedener Klassen sind, dann sind α, β algebraisch unabhängig.

Die S-Zahlen kann man anhand ihres Typs klassifizieren, den ich nun definieren werde. Aus $w(\alpha) < \infty$ ergibt sich, dass die Folge $\frac{w_n(\alpha)}{n}$ nach oben beschränkt ist, also gibt es $t > 0$ derart, dass

$$\limsup_{H\to\infty} \frac{-\log w_{n,H}(\alpha)}{\log H} = w_n(\alpha) < tn$$

für jedes $n \geq 1$. Demzufolge gibt es für jedes $\epsilon > 0$ ein $H_0 \geq 1$ (abhängig von n, t, ϵ) mit der Eigenschaft, dass $\frac{-\log w_{n,H}(\alpha)}{\log H} < n(t+\epsilon)$ für alle $H > H_0$. Daher $w_{n,H}(\alpha) > H^{-n(t+\epsilon)}$ für $H > H_0$. Wähle $c_n = \min_{1\leq H\leq H_0}\{1, \frac{1}{2} w_{n,H}(\alpha) H^{n(t+\epsilon)}\}$, dann $w_{n+1}(\alpha) > \frac{c_n}{H^{n(t+\epsilon)}}$ für alle $H \geq 1$. Somit gibt es $\theta > 0$ derart, dass es für jedes $n \geq 1$ ein $c_n > 0$ gibt, das $w_{n,H}(\alpha) > \frac{c_n}{H^{n-\theta}}$ für alle $H \geq 1$ erfüllt.

Der *Typ* α ist definiert als das Infimum aller θ mit der obigen Eigenschaft. Man kann zeigen, dass $\theta(\alpha) = \sup_{n\geq 1}\{\frac{w_n(\alpha)}{n}\}$.

Ich untersuche nun die Mächtigkeit und das Maß der Mengen von S-Zahlen, T-Zahlen und U-Zahlen.

Im Jahr 1932 zeigte Mahler, dass die Mengen reeller bzw. komplexer S-Zahlen das Maß 1 (im Sinne eines linearen bzw. Lebesgue-Maßes). Die folgende genauere Aussage vermutete Mahler im selben Artikel.

Unter Verwendung einer Klassifikation, die Koksma in Analogie zu Mahlers Klassifikation angab, bewies Sprindžuk im Jahr 1965 Mahlers Vermutung:

8.31. (1) Alle reellen Zahlen (mit Ausnahme einer Teilmenge mit Maß 0 in $\mathbb{R}$) sind S-Zahlen vom Typ 1.

(2) Alle komplexen Zahlen (mit Ausnahme einer Teilmenge mit Maß 0 in $\mathbb{C}$) sind S-Zahlen vom Typ $\frac{1}{2}$.

Die Menge der S-Zahlen ist also überabzählbar.

Allerdings ist es im Allgemeinen nicht einfach, Beispiele von S-Zahlen anzugeben und *a fortiori* ihren Typ zu berechnen.

Mahler zeigte, dass $\alpha = 0{,}123456789101112\ldots$ (bereits in Abschnitt B, Beispiel 5 betrachtet) eine S-Zahl ist.

Viele Jahre wusste man nicht, ob die Menge der T-Zahlen leer ist oder nicht. Schmidt zeigte 1968 (ohne ein Beispiel explizit vorzulegen), dass die Menge der T-Zahlen nicht leer ist. Einen einfacheren Beweis gab er 1969 an.

Was die U-Zahlen angeht, so folgt aus einer einfachen Charakterisierung sofort:

8.32. Jede Liouville-Zahl ist eine U-Zahl.

Darüberhinaus zeigte LeVeque (1953):

8.33. Für jede ganze Zahl $\mu \geq 1$ gibt es eine U-Zahl α mit $\mu(\alpha) = \mu$.

Es folgt, dass die Menge der U-Zahlen überabzählbar ist, obwohl sie das Maß Null hat (nach **(8.30)**).

In den Jahren 1971 und 1972 veränderte Mahler seine Klassifikation transzendenter Zahlen; verschiedene daraus resultierende Probleme löste Durand im Jahr 1974.

Ich führe nun das Konzept des Transzendenzmaßes einer transzendenten Zahl ein.

Die Funktion $T(n, H)$ (mit reellen, positiven Werten), definiert für ganze Zahlen $n \geq 1$, $H \geq 1$, ist ein *Transzendenzmaß* für die transzendente Zahl α, wenn $|f(\alpha)| \geq T(n, H)$ für jede $f \in \mathbb{Z}_{n,H}[X]$ gilt.

Das beste Transzendenzmaß ist natürlich $w_{n,H}(\alpha)$ wie oben von Mahler definiert. Allerdings ist es normalerweise sehr schwer zu berechnen.

Ich erwähne nun einige Resultate über Transzendenzmaße für Zahlen wie e, π, $\log r$ (r rational, $r \neq 1$, $r > 0$).

Borel (1899) und Popken (1929a) gaben Transzendenzmaße für e an.

Insbesondere folgte aus Popkens Resultat, dass e keine Liouville-Zahl ist. Man sollte anmerken, dass man dies auch aus der Kettenbruchentwicklung von e ableiten kann, was impliziert, dass

$$\left|e - \frac{a}{b}\right| \geq \frac{\log\log(4b)}{18\log(4b)b^2}$$

für alle rationalen Zahlen $\frac{a}{b}$, $b > 0$ gilt (siehe auch Bundschuh (1971)).

Mahler bewies im Jahr 1932:

8.34. Für jedes $n \geq 1$ gibt es $H_0(n) \geq 1$ derart, dass wenn $H > H_0(n)$, dann

$$|f(e)| > \frac{1}{H^{n+Cn^2\frac{\log(n+1)}{\log\log H}}}$$

für jedes $f(X) \in \mathbb{Z}_{n,H}[X]$, wobei $C > 0$ eine Konstante unabhängig von n und H ist.

Es folgt, dass

8.35. e ist eine S-Zahl vom Typ $\theta(e) = 1$; daher ist e keine Liouville-Zahl.

Als Nächstes zeigte Mahler (1932):

8.36. Sei $\alpha = \pi$ oder $\alpha = \log r$, wobei r eine positive rationale Zahl ist mit $r \neq 1$. Dann gilt für jedes $n \geq 1$ und $H \geq 1$, dass $|f(\alpha)| > \frac{C(n)}{H^{s^n}}$ für jedes $f(X) \in \mathbb{Z}_{n,H}[X]$, wobei $C(n) > 0$ und $s > 0$ eine von n und H unabhängige Konstante ist.

Es folgt, dass

8.37. π und $\log r$ (r rational, $r > 0$, $r \neq 1$) sind keine U-Zahlen, demzufolge sind sie auch keine Liouville-Zahlen.

Für weitere Informationen über Transzendenzmaße sei der Leser auf den Artikel von Waldschmidt (1978) verwiesen.

9 Schlussbemerkungen

Es ist besser, diese Übersicht an dieser Stelle abzubrechen, damit es für den Leser nicht zu ermüdend wird (jedoch niemals für mich). Abgesehen von der Tatsache, dass viele Punkte, die in diesem Überblick angesprochen wurden nicht mehr als angesprochen wurden, gibt es viele Aspekte, die vollkommen ausgelassen wurden: metrische Probleme bezüglich der Kettenbrüche, normale Zahlen, Gleichverteilung modulo 1, Fragen der Irrationalität und Transzendenz von Werten ganzer Funktionen, gewisser meromorpher Funktionen oder von Funktionen, die Lösungen bestimmter Typen von Differentialgleichungen sind. Auch habe ich keine Fragen über simultane Approximation erwähnt, auch habe ich nicht ....

Glücklicherweise gibt es viele Bücher und Übersichtsartikel über die verschiedenen Aspekte der Theorie (einige dieser sind bereits zitiert worden): Maillet (1906) (das erste Buch, das den transzendenten Zahlen gewidmet war), Minkowski (1907), Perron (1910, 1913), Khintchine (1935), Koksma (1936), Siegel (1949), Gel'fond (1952), Niven (1956), Cassels (1957), Schneider (1957), Mahler (1961, 1976a), Niven (1963), Lang (1966), Lipman (1966), Fel'dman (1967), Ramachandra (1969), Schmidt (1972), Waldschmidt (1974, 1979), Baker (1975), und Mignotte (1976).

Ich hoffe, dass der Leser diesem Überblick einiges Vergnügen abgewinnen konnte und der Wunsch nach weiteren Untersuchungen zu den Zahlen geweckt worden ist.

Literaturverzeichnis

1572 R. Bombelli. *L'Algebra, Parte Maggiore dell'Aritimetica Divisa in Tre Libri.* Bologna. Nachdruck von Feltrinelli, Milano, 1966.

1655 J. Wallis. *Arithmetica Infinitorum.* Nachdruck in *Opera Mathematica*, Vol. I, Oxford, 1695.

1685 J. Wallis. *Tractatus de Algebra.* Nachdruck in *Opera Mathematica*, Vol. II, Oxford, 1695.

1737 L. Euler. De fractionibus continuis dissertation. *Comm. Acad. Sci. Petr.*, 9:98–137. Nachdruck in *Opera Omnia*, Ser. I, Vol. 14, *Commentationes Analyticae*, 187–215. B. G. Teubner, Leipzig, 1924.

1748 L. Euler. *Introductio in Analysin Infinitorum,* Vol. I, Chapter VI, §105. Lausanne. Nachdruck in *Opera Omnia*, Ser. I, Vol. 8, 108–109. B. G. Teubner, Leipzig, 1922.

1755 L. Euler. De relatione inter ternas pluresve quantitates instituenda. *Opuscula Analytica*, 2:91–101. Nachdruck in *Opera Omnia*, Ser. I, Vol. 4, *Commentationes Arithmeticae*, 136–146. B. G. Teubner, Leipzig, 1941.

1761 J. H. Lambert. Mémoire sur quelques propriétés remarquables des quantités transcendantes circulaires et logarithmiques. *Mém. Acad. Sci. Berlin*, 17:265–322.

1769 J. L. Lagrange. Solution d'un probléme d'arithmétique. *Miscellanea Taurinensia, 1769–79*, 4. Nachdruck in *Oeuvres*, Vol. I, 671–731. Gauthier-Villars, Paris, 1867.

1769 J. L. Lagrange. Sur la solution des problèmes indéterminés du second degré. *Mém. Acad. Royale Sci. Belles-Lettres de Berlin*,

23. Nachdruck in *Oeuvres*, Vol. II, 377–535. Gauthier-Villars, Paris, 1868.

1770 J. L. Lagrange. Additions au mémoire sur la résolution des équations numériques. *Mém. Acad. Royale Sci. Belles-Lettres de Berlin*, 24. Nachdruck in *Oeuvres*, Vol. II, 581–652. Gauthier-Villars, Paris, 1868.

1770 J. H. Lambert. *Vorläufige Kenntnisse für die, so die Quadratur und Rectification des Circuls suchen.* Berlin. Beitrage zum Gebrauche der Mathematik und deren Anwendung (2. Teil), 144–169, Berlin, 1770.

1779 L. Euler. De formatione fractionum continuarum. *Acta. Acad. Sci. Imper. Petropolitane, I (1779)*, 9:3–29. Nachdruck in *Opera Omnia*, Vol. XV, 314–337. B. G. Teubner, Leipzig, 1927.

1794 A. M. Legendre. *Éléments de Géométrie* (12^e édition), Note IV, 286–296. Firmin Didot, Paris. 1823 (12^e édition), 1794 (1^e édition).

1801 C. F. Gauss. *Disquisitiones Arithmeticae.* G. Fleischer, Leipzig.

1808 A. M. Legendre. *Essai sur la Théorie des Nombres (Seconde Édition).* Courcier, Paris.

1815 M. J. De Stainville. *Mélanges d'Analyse Algébrique et de Géométrie.* Courcier, Paris.

1829 E. Galois. Démonstration d'un théorème sur les fractions continues périodiques. *Ann. Math. Pures et Appl., de M. Gergonne*, 19: 294–301. Nachdruck in *Écrits et Mémoires Mathématiques*, (par R. Bourgne et J. P. Azra), 365–377. Gauthier-Villars, Paris, 1962.

1832 F. Richelot. De resolutione algebraica aequationes $X^{257} = 1$, sive de divisione circuli per bisectionem anguli septies repetitam in partes 257 inter se aequalis commentatio coronata. *J. reine u. angew. Math.*, 9:1–26, 146–161, 209–230, 337–358.

1836 G. L. Dirichlet. Sur les intégrales eulériennes. *J. reine u. angew. Math.*, 15:258–263. Nachdruck in *Werke*, Vol. I, 273–282. G. Reimer, Berlin, 1889.

1840 J. Liouville. Additif à la note sur l'irrationalité du nombre e. *J. Math. Pures et Appl.*, 5(1):193.

1840 J. Liouville. Sur l'irrationalité du nombre e. *J. Math. Pures et Appl.*, 5(1):192.

1842 G. L. Dirichlet. Verallgemeinerung eines Satzes aus der Lehre von den Kettenbrüchen nebst einigen Anwendungen auf die Theorie der Zahlen. *Sitzungsber. Preuss. Akad. d. Wiss.,* Berlin, 93–95.

Nachdruck in *Werke*, Vol. I, 633–638. G. Reimer, Berlin, 1889. Nachdruck von Chelsea Publ. Co., New York, 1969.

1844 J. Liouville. Nouvelle démonstration d'un théorème sur les irrationalles algébriques, inséré dans le compte rendu de la dernière séance. *C. R. Acad. Sci. Paris*, 18:910–911.

1844 J. Liouville. Sur des classes très étendues de quantités dont la valeur n'est ni algébrique, ni même réductible à des irrationnelles algébriques. *C. R. Acad. Sci. Paris*, 18:883–885.

1851 J. Liouville. Sur des classes très étendues de quantités dont la valeur n'est ni algébrique, ni même réductible à des irrationnelles algébriques. *J. Math. Pures et Appl.*, 16(1):133–142.

1869 G. Cantor. Über die einfachen Zahlensysteme. *Zeitsch. f. Math. u. Physik*, 14:121–128. Nachdruck in *Gesammelte Abhandlungen*, 35–42. Springer-Verlag, Berlin, 1932.

1873 C. Hermite. Sur la fonction exponentielle. *C. R. Acad. Sci. Paris*, 77:18–24, 74–79, 226–233, 285–293. Nachdruck in *Oeuvres*, Vol. III, 150–181. Gauthier-Villars, Paris, 1912.

1874 G. Cantor. Über eine Eigenschaft der Inbegriffes aller reellen algebraischen Zahlen. *J. reine u. angew. Math.*, 77:258–262. Nachdruck in *Gesammelte Abhandlungen*, 115–118. Springer-Verlag, Berlin, 1932.

1874 F. Mertens. Ein Beitrag zur analytischen Zahlentheorie Über die Verteilung der Primzahlen. *J. reine u. angew. Math.*, 78:46–63.

1874 T. Muir. *The expression of a quadratic surd as a continued fraction.* Glasgow.

1876 J. W. L. Glaisher. Three theorems in arithmetics. *Messenger of Math.*, 5:21–22.

1878 G. Cantor. Ein Beitrag zur Mannigfaltigkeitslehre. *J. reine u. angew. Math.*, 84:242–258. Nachdruck in *Gesammelte Abhandlungen*, 119–133. Springer-Verlag, Berlin, 1932.

1878 J. W. L. Glaisher. Series and products for π and powers of π. *Messenger of Math.*, 7:75–80.

1879 A. Markoff. Sur les formes quadratiques binaires indéfinies. *Math. Annalen*, 15:381–409.

1880 J. J. Sylvester. On a point in the theory of vulgar fractions. *Amer. J. of Math.*, 3:332–335. Nachdruck in *Mathematical Papers*, Vol. III, 440–445. University Press, Cambridge, 1909.

1882 F. Lindemann. Sur le rapport de la circonférence au diamètre, et sur les logarithmes népériens des nombres commensurables ou des irrationnelles algébriques. *C. R. Acad. Sci. Paris*, 95:72–74.

1882 F. Lindemann. Über die Ludolph'sche Zahl. *Sitzungsber. Preuß. Akad. Wiss. zu Berlin*, 679–682.

1882 F. Lindemann. Über die Zahl π. *Math. Annalen*, 20:213–225.

1883 J. Lüroth. Über die eindeutige Entwicklung von Zahlen in eine unendliche Reihe. *Math. Annalen*, 21:411–423.

1884 L. Kronecker. Näherungsweise ganzzahlige Auflösung linearer Gleichungen. *Sitzungsber. Preuß. Akad. d. Wiss. zu Berlin*, 1179–1193 und 1271–1299. Nachdruck in *Werke*, Vol. III, 47–110. B. G. Teubner, Leipzig, 1930.

1885 K. Weierstrass. Zu Lindemann's Abhandlung "Über die Ludolph'sche Zahl". *Sitzungsber. Preuß. Akad. Wiss. zu Berlin*, 1067–1085. Nachdruck in *Mathematische Werke*, Vol. 11, 341–362. Mayer & Müller, Berlin, 1895.

1891 A. Hurwitz. Über die angenäherte Darstellung der Irrationalzahlen durch rationale Brüche. *Math. Annalen*, 39:279–284. Nachdruck in *Mathematische Werke*, Vol. II, 122–128. Birkhäuser, Basel, 1963.

1891 A. Hurwitz. Über die Kettenbruch-Entwicklung der Zahl e. *Schriften phys. ökon. Gesellschaft zu Königsberg*, 32 Jahrg.:59–62. Nachdruck in *Mathematische Werke*, Vol. II, 129–133. Birkhäuser, Basel, 1933.

1893 A. Hurwitz. Beweis der Transzendenz der Zahl e. *Math. Annalen*, 43:220–222. Nachdruck in *Mathematische Werke*, Vol. II, 134–135. Birkhäuser, Basel, 1933.

1899 E. Borel. Sue la nature arithme'tique du nombre e. *C. R. Acad. Sci. Paris*, 128:596–599.

1899 E. Landau. Sur la série des inverses des nombres de Fibonacci. *Bull. Soc. Math. France*, 27:298–300.

1900 D. Hilbert. Mathematische Probleme. Göttinger Nachrichten, 253–297 sowie *Archiv d. Math. u. Physik, Ser. 3*, 1, 1901, 44–63 und 213–237.

1901 M. Lerch. Sur la fonction $\zeta(s)$ pour valeurs impaires de l'argument. *Jornal Ciencias Mat. e Astron.*, 14:65–69. Published by F. Gomes Teixeira, Coimbra.

1904 O. Veblen. The transcendence of π and e. *Amer. Math. Monthly*, 11:219–223.

1906 E. Maillet. *Introduction à la Théorie des Nombres Transcendants et des Propriétés Arithmétiques des Fonctions.* Gauthier-Villars, Paris.

1907 H. Minkowski. *Diophantische Approximationen.* B. G. Teubner, Leipzig.

1909 A. Thue. Über Annäherungswerte algebraische Zahlen. *J. reine u. angew. Math.*, 135:284–305. Nachdruck in *Selected Mathematical Papers*, 232–253. Universitetsforlaget, Oslo, 1982.

1910 O. Perron. *Irrationalzahlen.* W. de Gruyter, Berlin. Nachdruck von Chelsea Publ. Co., New York, 1951.

1910 W. Sierpiński. Sur la valeur asymptotique d'une certaine somme. *Bull. Intern. Acad. Sci. Cracovie*, 9–11. Nachdruck in *Oeuvres Choisies*, Vol. I, 158–160. Warszawa, 1974.

1912 A. Thue. Über eine Eigenschaft, die keine transcendente Grössen haben kann. *Kristiania Vidensk. Selskab Skr., I, Mat. Nat. Kl.*, Nr. 20. Nachdruck in *Selected Mathematical Papers*, 479–492. Universiteteforlaget, Oslo, 1982.

1913 F. Engel. *Verhandl. d. 52. Versammlung deutsche Philologen u. Schulmänner*, 190–191. Marburg.

1913 O. Perron. *Die Lehne von den Kettenbrüche.* B. G. Teubnen, Leipzig. Nachdruck von Chelsea Publ. Co., New York, 1950.

1914 S. Kakeya. On the partial sums of an infinite series. *Science Reports Tôhoku Imp. Univ.*, 3(1):159–163.

1919 F. Hausdorff. Dimension und äußeres Maß. *Math. Annalen*, 79:157–179.

1921 O. Perron. Über die Approximation irrationaler Zahlen durch rationale, I, II. *Sitzungsber. Heidelberg Akad. d. Wiss.,* Abh. 4, 17 Seiten und Abh. 8, 12 Seiten.

1921 C. L. Siegel. Über den Thueschen Satz. *Norske Vidensk. Selskab Skrifter, Kristiania, Ser. 1.,* Nr. 16, 12 Seiten. Nachdruck in *Gesammelte Abhandlungen*, Vol. I, 103–112. Springer-Verlag, Berlin, 1966.

1924 A. J. Khintchine. Einige Sätze über Kettenbrüche mit Anwendungen auf die Theorie der Diophantióchen Approximationen. *Math. Annalen*, 92:115–125.

1924 G. Pólya und G. Szegö. *Aufgaben und Lehrsätze der Analysis, I.* Springer-Verlag, Berlin.

1925 S. L. Malurkar. On the application of Herr Mellin's integrals to some series. *J. Indian Math. Soc.*, 16:130–138.

1929 K. Mahler. Arithmetische Eigenshaften def Lösungen einer klasse von Funktionalgleichungen. *Math. Annalen*, 101:342–366.

1929 J. Popken. Zur Transzendenz von e. *Math. Z.*, 29:525–541.

1929 J. Popken. Zur Transzendenz von π. *Math. Z.*, 29:542–548.

1929 K. Shibata. On the order of approximation of irrational numbers by rational numbers. *Tôhoku Math. J*, 30:22–50.

1930 K. Mahler. Über Beziehungen zwischen der Zahl e und den Liouvilleschen Zahlen. *Math. Z.*, 31:729–732.

1932 J. F. Koksma und J. Popken. Zur transzendenz von e^{π}. *J. reine u. angew. Math.*, 168:211–230.

1932 K. Mahler. Über das Mass der Menge aller S-Zahlen. *Math. Annalen*, 106:131–139.

1932 K. Mahler. Zur Approximation der Exponentialfunktion und des Logarithmus, I, II. *J. reine u. angew. Math.*, 166:118–136 und 137–150.

1932 O. Perron. Über mehrfach transzendente Erweiterungen des natürlichen Rationalitäts bereiches. *Sitzungsber. Bayer Akad. Wiss., H2*, 79–86.

1933 B. L. van der Waerden. Die Seltenheit der Gleichungen mit Affekt. *Math. Annalen*, 109:13–16.

1934 A. O. Gel'fond. Sur le septième problème de Hilbert. *Dokl. Akad. Nauk SSSR*, 2:1–6.

1934 A. O. Gel'fond. Sur le septième problème de Hilbert. *Izv. Akad. Nauk SSSR*, 7:623–630.

1934 T. Schneider. Tranzendenzuntersuchungen periodischer Funktionen. *J. reine u. angew. Math.*, 172:65–74.

1935 A. J. Khintchine. *Continued Fractions.* Moskau. Übersetzung der 3. Ausgabe durch P. Wynn, Noordhoff, Gröningen, 1963.

1936 J. F. Koksma. *Diophantische Approximationen.* Springer-Verlag, Berlin. Nachdruck von Chelsea Publ. Co., New York, 1953.

1937 K. Mahler. Eigenshaften eines Klasse von Dezimalbrüchen. *Nederl. Akad. Wetensch., Proc. Ser. A*, 40:421–428.

1938 G. H. Hardy und E. M. Wright. *An Introduction to the Theory of Numbers.* Clarendon Press, Oxford, 5. Ausgabe (1979).

1939 J. F. Koksma. Über die Mahlersche Klasseneinteilung der transzendente Zahlen und die Approximation komplexer Zahlen durch algebraischen Zahlen. *Monatshefte Math. Phys.*, 48:176–189.

1943 F. J. Dyson. On the order of magnitude of the partial quotients of a continued fraction. *J. London Math. Soc.*, 18:40–43.

1947 F. J. Dyson. The approximation of algebraic numbers by rationals. *Acta Arith.*, 79:225–240.

1949 T. Schneider. Über eine Dysonsche Verschärfung des Siegel-Thuesche Satzes. *Arch. Math.*, 1:288–295.

1949 C. L. Siegel. *Transcendental Numbers.* Annals of Math. Studies, 16, Princeton, N.J.

1952 A. O. Gel'fond. *Transcendental and Algebraic Numbers* (in Russian). G.I.T.T.L., Moskau. Englische Übersetzung bei Dover, New York, 1960.

1953 W. J. LeVeque. Note on S-numbers. *Proc. Amer. Math. Soc.*, 4:189–190.

1953 W. J. LeVeque. On Mahler's U-numbers. *J. London Math. Soc.*, 28:220–229.

1953 K. Mahler. On the approximation of π. *Indag. Math.*, 15: 30–42.

1954 M. M. Hjortnaes. Overføng av rekken $\sum_{k=1}^{\infty} \frac{1}{k^3}$ til et bestemt integral. In *Proc. 12th Congr. Scand. Math., Lund, 1953.* Lund Univ.

1955 K. F. Roth. Rational approximations to algebraic numbers. *Mathematika*, 2:1–20. Corrigendum, p. 168.

1956 I. Niven. *Irrational Numbers.* Math. Assoc. of America, Washington.

1957 J. W. S. Cassels. *An Introduction to Diophantine Approximation.* Cambridge Univ. Press, Cambridge.

1957 S. Ramanujan. *Notebooks of Srinivasan Ramanujan (2 volumes).* Tata Institute of Fund. Res., Bombay.

1957 T. Schneider. *Einführung in die Transzendenten Zahlen.* Springer-Verlag, Berlin.

1959 G. H. Hardy und E. M. Wright. *The Theory of Numbers, 4th ed.* Clarendon Press, Oxford.

1961 K. Mahler. *Lectures on Diophantine Approximations.* Notre Dame Univ., South Bend, IN.

1962 P. Erdös. Representation of real numbers as sums and products of Liouville numbers. *Michigan Math. J.*, 9:59–60.

1962 W. M. Schmidt. Simultaneous approximation and algebraic independence of numbers. *Bull. Amer. Math. Soc.*, 68:475–478.

1963 I. Niven. *Diophantine Approximations.* Wiley-Interscience, New York.

1963 C. D. Olds. *Continued Fractions.* Math. Assoc. of America, Washington.

1964 A. Baker. Approximations to the logarithms of certain rational numbers. *Acta Arith.*, 10:315–323.

1964 A. Baker. Rational approximations to $\sqrt[3]{2}$ and other algebraic numbers. *Quart. J. Math. Oxford*, 15:375–383.

1964 D. Knuth. Transcendental numbers based on the Fibonacci sequence. *Fibonacci Q.*, 2:43–44.

1965 V. G. Sprindžuk. A proof of Mahler's conjecture on the measure of the set of S-numbers. *Izv. Akad. Nauk SSSR, Ser. Mat.*, 29:379–436. Übersetzung ins Englische in *Amer. Math. Soc. Transl. (2)*, 51, 1960, 215–272.

1966 S. Lang. *Introduction to Transcendental Numbers.* Addison-Wesley, Reading, MA.

1966 J. N. Lipman. *Transcendental Numbers.* Queen's Papers in Pure and Applied Mathematics, Nr. 7. Queen's University, Kingston, Ont., 1966.

1967 N. I. Fel'dman und A. B. Shidlovskii. The development and present state of the theory of transcendental numbers. *Russian Math. Surveys*, 22:1–79. Übersetzung aus Uspehi Mat. Nauk SSSR, 22:3–81.

1968 W. M. Schmidt. T-numbers do exist. In *Symp. Math., IV, 1st. Naz. di Alta Mat., Roma*, 3–26. Academic Press, London, 1970.

1969 K. Ramachandra. *Lectures in Transcendental Numbers.* Ramanujan Institute, Madras.

1970 P. Bundschuh. Ein Satz über ganze Funktionen und Irrationalitätsaussagen. *Invent. Math.*, 9:175–184.

1970 E. Grosswald. Die Werte der Riemannschen Zetafunktion an ungeraden Argumentstellen. *Nachr. der Akad. Wiss. Göttingen*, 9–13.

1970 E. Schenkman. The independence of some exponential values. *Amer. Math. Monthly*, 81:46–49.

1971 J. L. Brown. On generalized bases for real numbers. *Fibonacci Q.*, 9:477–496.

1971 P. Bundschuh. Irrationalitätsmasse für e^a, $a \neq 0$, rational oder Liouville Zahl. *Math. Annalen*, 192:229–242.

1971 L. Carlitz. Reduction formulas for Fibonacci summations. *Fibonacci Q.*, 9:449–466 und 510.

1971 S. Lang. Transcendental numbers and diophantine approximation. *Bull. Amer. Math. Soc.*, 77:635–677.

1971 K. Mahler. On the order function of a transcendental number. *Acta Arith.*, 18:63–76.

1971 W. M. Schmidt. Mahler's T-numbers. *Proc. Sympos. Pure Math., Vol. XX*, 275–286.

1972 E. Grosswald. Comments on some formulae of Ramanujan. *Acta Arith.*, 21:25–34.

1972 W. M. Schmidt. *Approximation to Algebraic Numbers.* Enseign. Math., Monograph #19, Génève.

1973 K. Katayama. On Ramanujan's formula for values of Riemann zeta function at positive odd integers. *Acta Arith.*, 22:149–155.

1973 K. Mahler. The classification of transcendental numbers. In *Analytic Number Theory (Proc. Sympos. Pure Math., Vol. XXIV, St. Louis Univ., St. Louis, MO, 1972)*, 175–179. Amer. Math. Soc., Providence, R.I.

1973 Z. A. Melzak. *Companion to Concrete Mathematics, 2 volumes.* John Wiley & Sons, New York. 1973, 1976.

1973 M. Mignotte. Construction de nombres transcendants, grâce aux théorèmes de Liouville, Thue, Siegel et Roth. In *Sém. Waldschmidt*, chapter 3. Orsay.

1973 L. Nový. *Origins of Modern Algebra.* P. Noordhoff, Leyden.

1973 J. R. Smart. On the values of the Epstein zeta function. *Glasgow Math. J.*, 14:1–12.

1973 M. Waldschmidt. La conjecture de Schanuel. In *Sém. Waldschmidt*, Orsay.

1974 B. C. Berndt. Ramanujan's formula for $\zeta(2n+1)$. In *Professor Srinivasan Ramanujan Commemoration Volume*, 2–9. Jupiter Press, Madras.

1974 L. Comtet. *Advanced Combinatorial Analysis.* D. Reidel, Dordrecht.

1974 A. Durand. Quatre problèmes de Mahler sur la fonction ordre d'un nombre transcendant. *Bull. Soc. Math. France*, 102:365–377.

1974 I. J. Good. A reciprocal series of Fibonacci numbers. *Fibonacci Q.*, 12:346.

1974 H. Halberstam. Transcendental numbers. *Math. Gaz.*, 58: 276–284.

1974 M. Mignotte. Approximations rationnelles de π et de quelques autres nombres. *Bull. Soc. Math. France*, 37:121–132.

1974 D. Shanks. Incredible identities. *Fibonacci Q.*, 12:271 und 280.
1974 M. Waldschmidt. *Nombres Transcendants.* Lecture Notes in Mathematics #402. Springer-Verlag, Berlin.
1975 A. Baker. *Transcendental Number Theory.* Cambridge Univ. Press, London.
1976 V. E. Hoggatt und M. Bicknell. A reciprocal series of Fibonacci numbers with subscripts $2^n k$. *Fibonacci Q.*, 14:453–455.
1976 K. Mahler. *Lectures on Transcendental Numbers.* Lecture Notes in Mathematics #546. Springer-Verlag, New York.
1976 Kurt Mahler. On a class of transcendental decimal fractions. *Comm. Pure Appl. Math.*, 29:717–725.
1976 M. Mignotte. *Approximation des Nombres Algébriques.* Publ. Math. Orsay, no. 77–74, Orsay, France.
1977 B. C. Berndt. Modular transformations and generalizations of some formulae of Ramanujan. *Rocky Mt. J. Math.*, 7:147–189.
1978 A. J. van der Poorten. Some wonderful formulae... footnotes to Apéry's proof of the irrationality of $\zeta(3)$. *Sém. Delange-Pisot-Poitou*, 20^e année(29):7 Seiten.
1978 M. Waldschmidt. Transcendence measures for exponentials and logarithms. *J. Austral. Math. Soc. Ser. A*, 25(4):445–465.
1979 K. Alladi. Legendre polynomials and irrational numbers. Matscience report no. 100, Inst. Math. Sciences, Madras. 83 Seiten.
1979 R. Apéry. Irrationalité de $\zeta(2)$ et $\zeta(3)$. *Astérisque*, 61:11–13. Société Math. France.
1979 F. Beukers. A note on the irrationality of $\zeta(2)$ and $\zeta(3)$. *Bull. London Math. Soc.*, 11:268–272.
1979 M. Waldschmidt. *Transcendence Methods.* Queen's Papers in Pure and Applied Mathematics, Nr. 52. Queen's University, Kingston, Ont.
1979 A. J. van der Poorten. A proof that Euler missed... Apéry's proof of the irrationality of $\zeta(3)$. *Math. Intelligencer*, 1:193–203.
1980 _____. *Numéro Spécial* π. Supplément au "Petit Archimède".
1981 H. Cohen. Généralisation d'une construction de R. Apéry. *Bull. Soc. Math. France*, 109:269–281.
1982 D. Zagier. On the number of Markoff numbers below a given bound. *Math. of Comp.*, 39:709–723.
1983 M. Waldschmidt. Les débuts de la théorie des nombres transcendants. *Cahiers Sém. Histoire Math.*, 4:93–115.

1984 F. Gramain. Les nombres transcendants. *Pour la Science*, 80: 70–79.

1985 B. C. Berndt. *Ramanujan's Notebooks, Part I.* Springer-Verlag, NY.

1986 P. Ribenboim. Some fundamental methods in the theory of Diophantine equations. In *Aspects of mathematics and its applications*, 635–663. North-Holland, Amsterdam.

1988 D. Castellanos. The ubiquity of π. *Math. Mag.*, 61:67–98, 148–163.

1989 B. C. Berndt. *Ramanujan's Notebooks, Part II.* Springer-Verlag, New York.

1989 D. V. Chudnovsky und G. V. Chudnovsky. Transcendental methods and theta-functions. In *Theta functions—Bowdoin 1987, Part 2 (Brunswick, ME, 1987)*, 167–232. Amer. Math. Soc., Providence, RI.

1991 R. André-Jeannin. A note on the irrationality of certain Lucas infinite series. *Fibonacci Q.*, 29:132–136.

1991 K. Nishioka. *Mahler Functions and Transcendence (Springer Lect. Notes in Math. #1631).* Springer-Verlag, Berlin.

1993 D. V. Chudnovsky und G. V. Chudnovsky. Hypergeometric and modular function identities, and new rational approximations to and continued fraction expansions of classical constants and functions. *Contemp. Math.*, 143:117–162.

1993 M. Hata. Rational approximations to π and some other numbers. *Acta Arith.*, 63:335–349.

1994 P. G. Becker und T. Töpfer. Irrationality results for reciprocal sums of certain Lucas numbers. *Arch. Math. (Basel)*, 62: 300–305.

1994 S. Landau. How to tangle with a nested radical. *Math. Intelligencer*, 16(2):49–55.

1996 R. P. Brent, A. J. van der Poorten und H. J. J. te Riele. A comparative study of algorithms for computing continued fractions of algebraic numbers. In *Algorithmic Number Theory (Talence, 1996)*, Lecture Notes in Computer Science #1122, 35–47. Springer-Verlag, Berlin.

1997 Y. V. Nesterenko. On the measure of algebraic independence of values of Ramanujan functions (in Russian). *Tr. Mat. Inst. Steklova*, 218:299–334.

1998 F. Gramain. Quelques résultats d'indépendance algébrique. In *Proceedings of the International Congress of Mathematicians, Vol. II (Berlin, 1998)*, 173–182.

2001 K. Ball und T. Rivoal. Irrationalité d'une infinité de valeurs de la fonction zêta aux entiers impairs. *Invent. Math.*, 146(1):193–207.

2001 W. Zudilin. One of the numbers zeta(5), zeta(7), zeta(9), zeta(11) is irrational. *Russian Math. Surveys*, 56(4), 774–776;

11

Galimatias Arithmeticae[1]

Im *Oxford English Dictionary* findet sich, dass *galimatias* soviel wie „confused language“ oder „meaningless talk“ heißt, was übersetzt etwa „Geschwafel“ oder „Gewäsch“ bedeutet. Und genau das ist es, was man in diesem Kapitel erwarten muss. Als Zeichen der Bewunderung von Gauss wage ich es, das Wort *Arithmeticae* an meine Überschrift anzufügen. Dies sollte keineswegs als Beleidigung des Prinzen aufgefasst werden, der im Alter von 24 Jahren das unvergängliche Meisterwerk *Disquisitiones Arithmeticae* veröffentlichte.

Da ich mich zur Ruhe setze (oder vom Ruhestand betroffen bin), ist es an der Zeit, einen Blick zurück auf die Ereignisse meiner Karriere zu werfen. Anders als die meisten anderen Leute möchte ich gerne über mathematische Eigenschaften oder Probleme einiger Zahlen sprechen, die mit Höhepunkten meines Lebens verknüpft sind. Die verblüffendste Verbindung werde ich mir dabei für den Schluss aufheben.

Ich werde mit der hoffnungsvollen Zahl 11 beginnen und mit der ominösen Zahl 65 schließen.

11

- Im Alter von 11 Jahren lernte ich es, x zur Darstellung einer unbekannten Größe zu verwenden, um Probleme wie diese zu lösen: „Drei Brüder, die jeweils im Abstand von zwei Jahren geboren wurden, haben als Summe ihrer Alter die Zahl 33. Wie alt sind die Brüder?“

[1] Dieses Kapitel ist eine veränderte Version eines Vortrags an der Universität München, der im November 1994 im Rahmen eines Festkolloquiums zu Ehren von Professor Sibylla Priess-Crampe gehalten wurde.

Ich verstand die Mächtigkeit dieser Methode sofort und entschied mich für Zahlen zu interessieren, sogar noch als mein Alter das doppelte der Summe des Alters der drei Brüder übertraf.

Aber es gibt viele bessere Gründe, warum 11 interessant ist.

- 11 ist die kleinste prime Repunit-Zahl. Eine Zahl mit n Ziffern sämtlich gleich 1 nennt man eine *Repunit-Zahl*, bezeichnet mit R_n. So ist $11 = R_2$. Die folgenden Repunit-Zahlen sind als Primzahlen bekannt: R_n mit $n = 2$, 19, 23, 317 und 1031. Es ist nicht bekannt, ob es unendlich viele prime Repunit-Zahlen gibt.
- Wenn $n > 11$, dann gibt es eine Primzahl $p > 11$ mit der Eigenschaft, dass

$$p \text{ teilt } n(n+1)(n+2)(n+3).$$

  Eine Kuriosität? Nicht ganz. Ein guter Satz (von MAHLER) besagt, dass wenn $f(x)$ ein Polynom mit ganzzahligen Koeffizienten vom Grad zwei oder mehr ist (für zwei ist dies PÓLYAs Satz), und wenn H eine endliche Menge von Primzahlen ist (so wie $\{2, 3, 5, 7, 11\}$), dann gibt es n_0 derart, dass wenn alle Primfaktoren von $f(n)$ in H liegen, dann gilt $n \leq n_0$.

  Man kann dies auch anders ausdrücken: $\lim_{n\to\infty} P[f(n)] = \infty$, wobei $P[f(n)]$ den größten Primfaktor von $f(n)$ bezeichnet. Mithilfe der Theorie von BAKER über Linearformen in Logarithmen gab COATES eine effektive Schranke für n_0 an. Für das bestimmte Polynom $f(x) = x(x+1)(x+2)(x+3)$ ist der Beweis elementar.
- 11 ist die größte positive ganze Zahl d, die quadratfrei ist und die Eigenschaft hat, dass $\mathbb{Q}(\sqrt{-d})$ einen euklidischen Ring von ganzen Zahlen besitzt. Die anderen solchen Körper sind diejenigen mit $d =$ 1, 2, 3 und 7. D.h. dass wenn α, $\beta \in \mathbb{Z}[\sqrt{-d}]$, dann gibt es γ, $\delta \in \mathbb{Z}[\sqrt{-d}]$ derart, dass $\alpha = \beta\gamma + \delta$ wobei $\delta = 0$ oder $N(\delta) < N(\beta)$. (Hierbei ist für $\alpha = a + b\sqrt{-d}$, $N(\alpha) = a^2 + db^2$. Die Situation ist genau wie bei der euklidischen Division im Ring $\mathbb{Z}$ der gewöhnlichen ganzen Zahlen.)
- Es ist unbekannt, ob es einen Quader mit ganzzahligen Seitenlängen a, b und c sowie sämtlich ganzzahliger Diagonalen gibt. Mit anderen Worten ist unbekannt, ob das folgende System eine Lösung in ganzen Zahlen ungleich Null besitzt:

$$\begin{cases} a^2 + b^2 = d^2 \\ b^2 + c^2 = e^2 \\ c^2 + a^2 = f^2 \\ a^2 + b^2 + c^2 = g^2 \end{cases}$$

Falls es solche ganzen Zahlen gibt, so teilt 11 das Produkt *abc*.

- 11 ist die kleinste ganze Zahl, die keine *numerus idoneus* ist.
  Sie wissen nicht, was eine *numerus idoneus* ist? Ich musste es auch erst bis 65 schaffen, bis ich verstand, was dieses Alter mit *idoneus*-Zahlen zu tun hat. Seien Sie also geduldig.
- Nach der Theorie der Supersymmetrie hat die Welt 11 Dimensionen: 3 für die Raumposition, 1 für die Zeit sowie 7 für die verschiedenen möglichen Superstrings und ihre unterschiedlichen Schwingungszustände, um das Verhalten der subatomaren Teilchen zu erklären.
  Ist dies ein Witz oder eine neue Theorie, um die Welt zu erklären?
- Bei den Mersenne-Zahlen handelt es sich um die ganzen Zahlen $M_q = 2^q - 1$, wobei q eine Primzahl ist. Eine große Sache: manche sind prim, manche zerlegbar. Eine sogar noch größere Sache: Wieviele von jeder Art sind es? Ein totales Rätsel!
  $M_{11} = 2^{11} - 1 = 2047 = 23 \cdot 28$. Es ist die kleinste zerlegbare Mersenne-Zahl. Die größte bekannte zerlegbare Mersenne-Zahl ist M_q mit $q = 137211941292195 \times 2^{171960} - 1$.

19

- 19 war immer eine meiner Lieblingszahlen gewesen. In diesem Alter gewann Napoleon Schlachten—was wir vergessen sollten. Im selben Alter entdeckte Gauss das quadratische Reziprozitätsgesetz— was man nicht mehr vergessen kann, wenn man es einmal kennengelernt hat.
- Zunächst eine Kuriosität bezüglich der Zahl 19. Es ist die größte Zahl n derart, dass

$$n! - (n-1)! + (n-2)! - \cdots \pm 1!$$

  eine Primzahl ist. Die anderen ganzen Zahlen n mit dieser Eigenschaft sind

$$n = 3, 4, 5, 6, 7, 8, 9, 10 \text{ und } 15.$$

- Sowohl die Repunit-Zahl R_{19} als auch die Mersenne-Zahl M_{19} sind Primzahlen.
- Seien $U_0 = 0$, $U_1 = 1$ und $U_n = U_{n-1} + U_{n-2}$ für $n \geq 2$; dies sind die Fibonacci-Zahlen. Wenn U_n prim ist, so muss auch n prim sein, aber nicht umgekehrt. 19 ist der kleinste prime Index eines Gegenbeispiels: $U_{19} = 4181 = 37 \cdot 113$.

- Die Zahlkörper $\mathbb{Q}(\sqrt{-19})$, $\mathbb{Q}(\sqrt{19})$ haben die Klassenzahl 1. (Die Klassenzahl ist eine natürliche Zahl, die man einem jeden Zahlkörper zuordnet. Sie ist 1 für den Körper der rationalen Zahlen; sie ist auch 1 für den Körper der Gaußschen Zahlen sowie für jeden Körper, dessen arithmetische Eigenschaften denen der rationalen Zahlen ähnlich sind. Je größer die Klassenzahl eines Zahlkörpers ist, desto mehr werden seine arithmetischen Eigenschaften von denen der rationalen Zahlen „abweichen“. Mehr über diese Konzepte findet sich in Ribenboim (2000).) Der Ring der ganzen Zahlen von $\mathbb{Q}(\sqrt{19})$ ist euklidisch, während der Ring der ganzen Zahlen von $\mathbb{Q}(\sqrt{-19})$ nicht euklidisch ist.
- Sei $n > 2$, $n \not\equiv 2 \pmod 4$, und $\zeta_n = e^{2\pi i/n}$ bezeichne eine primitive $n$te Einheitswurzel. 19 ist die größte Primzahl p derart, dass $\mathbb{Q}(\zeta_p)$ die Klassenzahl 1 besitzt. Dies war im Zusammenhang mit Kummers Forschung zu Fermats letztem Satz von Bedeutung.
  Masley und Montgomery bestimmten im Jahr 1976 alle ganzen Zahlen n, $n \not\equiv 2 \pmod 4$ mit der Eigenschaft, dass $\mathbb{Q}(\zeta_n)$ die Klassenzahl 1 hat. Dies sind:

$$n = 1, 3, 4, 5, 7, 8, 9, 11, 12, 13, 15, 16, 17, 19, 20, 21, 24, 25,$$
$$27, 28, 32, 33, 35, 36, 40, 44, 45, 48, 60 \text{ und } 84.$$

- Balasubramanian, Dress und Deshouillers zeigten im Jahr 1986, dass jede natürliche Zahl die Summe von höchstens 19 Viererpotenzen ist. Davenport hatte 1939 gezeigt, dass jede genügend große natürliche Zahl Summe von höchstens 16 Viererpotenzen ist. Dies war die vollständige Lösung der zwei Formen von Warings Problem für Viererpotenzen.

29

- Primzahlzwillinge so wie 29 und 31 unterscheiden sich vom Alter von Zwillingen—ihre Differenz ist 2. Warum? Es gibt viele Zwillinge und viele Primzahlzwillinge, aber in beiden Fällen weiß man nicht, ob es unendlich viele sind ....
  Euler zeigte, dass

$$\sum_{p \text{ prim}} \frac{1}{p} = \infty.$$

Im Gegensatz dazu bewies Brun, dass

$$\sum_{p,\, p+2 \text{ prim}} \frac{1}{p} < \infty$$

Bruns Ergebnis besagt, dass es entweder nur endlich viele Primzahlzwillinge gibt, oder aber, dass ihre Größe im Falle unendlich vieler rapide abnehmen muss, damit obige Summe beschränkt bleibt. All dies wird in meinem Buch über Primzahlen Ribenboim (2006) ausführlich besprochen.

- Eine Kuriosität, die Euler beobachtete: Falls 29 die Summe $a^4 + b^4 + c^4$ teilt, so teilt 29 auch $\mathrm{ggT}(a, b, c)$.
- Es sei p eine Primzahl. Die *Primfakultät* von p ist

$$p\sharp = \prod_{q \le p,\, q\ \{\text{prim}\}} q;$$

$29 = 5\sharp - 1$. Die Ausdrücke $p\sharp + 1$ und $p\sharp - 1$ wurden im Zusammenhang mit Varianten von Euklids Beweis der Unendlichkeit der Primzahlen untersucht. Folgende Primzahlen p sind die einzigen unterhalb von 120000 mit der Eigenschaft, dass $p\sharp - 1$ prim ist:

$$p = 3,\ 5,\ 11,\ 13,\ 41,\ 89,\ 317,\ 991,\ 1873,\ 2053,\ 2371,\ 4093,\ 4297,\ 4583,\ 6569,\ 13033,\ 15877.$$

Für diese und ähnliche Folgen, siehe Ribenboim (2006).

- $2 \cdot 29^2 - 1 = \square$ (ein Quadrat), genauso $2 \cdot 1^2 - 1 = \square$, $2 \cdot 5^2 - 1 = \square$. Tatsächlich gibt es unendlich viele natürliche Zahlen x derart, dass $2x^2 - 1 = \square$. Sämtliche Paare (t, x) natürlicher Zahlen mit der Eigenschaft, dass $t^2 - 2x^2 = -1$ findet man auf folgende Weise. Aus $(t+\sqrt{2}x)(t-\sqrt{2}x) = -1$ folgt, dass $t+\sqrt{2}x$ eine Wurzel des Körpers $\mathbb{Q}(\sqrt{2})$ ist. Die Fundamentaleinheit ist $1 + \sqrt{2}$ und hat die Norm $(1 + \sqrt{2})(1 - \sqrt{2}) = -1$, also $t + \sqrt{2}x = (1 + \sqrt{2})^n$ mit ungeradem n. Somit ist

$$\begin{aligned}(1 + \sqrt{2})^2 &= 3 + 2\sqrt{2},\\ (1 + \sqrt{2})^3 &= 7 + 5\sqrt{2},\\ (1 + \sqrt{2})^5 &= 41 + 29\sqrt{2}.\end{aligned}$$

Die nächste Lösung gewinnt man aus

$$(1 + \sqrt{2})^7 = 239 + 169\sqrt{2},$$

nämlich $2 \cdot 169^2 - 1 = 239^2$.

- Der Ring der ganzen Zahlen von $\mathbb{Q}(\sqrt{29})$ ist euklidisch. Es gibt 16 reelle quadratische Zahlkörper $\mathbb{Q}(\sqrt{d})$ mit einem euklidischen Ring ganzer Zahlen, dies sind

$$d = 2,\ 3,\ 5,\ 6,\ 7,\ 11,\ 13,\ 17,\ 19,\ 21,\ 29,\ 33,\ 37,\ 41,\ 57,\ 73.$$

- $2X^2 + 29$ ist ein *optimales primzahlerzeugendes Polynom*. Derartige Polynome wurden erstmals von Euler untersucht—es sind Polynome $f \in \mathbb{Z}[X]$, die soviele initiale Primzahlwerte wie nur möglich annehmen. Genauer sei $f \in \mathbb{Z}[X]$ mit positivem Leitkoeffizient und $f(0) = q$ prim. Es gibt ein kleinstes $r > 0$ derart, dass $f(r) > q$ und $q \mid f(r)$. Das Polynom ist *optimal primzahlerzeugend*, wenn $f(k)$ für $k = 0, 1, \ldots, r-1$ prim ist.
  Euler beobachtete, dass $X^2 + X + 41$ optimal primzahlerzeugend ist, da es für alle $k = 0, 1, \ldots, 39$ prime Werte annimmt, während $40^2 + 40 + 41 = 41^2$.
  Im Jahr 1912 zeigte Rabinowitsch, dass das Polynom $f(X) = X^2 + X + q$ (mit q prim) optimal primzahlerzeugend genau dann ist, wenn der Körper $\mathbb{Q}(\sqrt{1-4q})$ die Klassenzahl 1 besitzt.
  Heegner, Stark und Baker bestimmten alle imaginär-quadratischen Zahlkörper $\mathbb{Q}(\sqrt{d})$ (mit $d < 0$ und d quadratfrei) mit Klassenzahl 1:

$$d = -1,\ -2,\ -5,\ -7,\ -11,\ -19,\ -43,\ -67,\ -163.$$

  Diese gehören zu den einzigen optimal primzahlerzeugenden Polynomen der Form $X^2 + X + q$, nämlich zu $q = 2,\ 3,\ 5,\ 11,\ 17,\ 41$. $X^2 + X + 41$ ist das Rekord-primzahlerzeugende Polynom der Form $X^2 + X + q$.
  Frobenius (1912) und Hendy (1974) untersuchten optimal primzahlerzeugende Polynome in Verbindung mit imaginär-quadratischen Zahlkörpern mit Klassenzahl 2. Es gibt drei Typen derartiger Körper:
  (i) $\mathbb{Q}(\sqrt{-2p})$, wobei p eine ungerade Primzahl ist;
  (ii) $\mathbb{Q}(\sqrt{-p})$, wobei p eine Primzahl ist und $p \equiv 1 \pmod 4$;
  (iii) $\mathbb{Q}(\sqrt{-pq})$, wobei p, q ungerade Primzahlen sind mit $p < q$ und $pq \equiv 3 \pmod 4$.

  Für obige Typen von Körpern gelten die folgenden Sätze:
  (i) $\mathbb{Q}(\sqrt{-2p})$ hat Klassenzahl 2 genau dann, wenn $2X^2 + p$ für $k = 0, 1, \ldots, p-1$ Primzahlwerte annimmt.

(ii) $\mathbb{Q}(\sqrt{-p})$ hat Klassenzahl 2 genau dann, wenn $2X^2 + 2X + \frac{p+1}{2}$ für $k = 0, 1, \ldots, \frac{p-3}{2}$ Primzahlwerte annimmt.

(iii) $\mathbb{Q}(\sqrt{-pq})$ hat Klassenzahl 2 genau dann, wenn $pX^2 + pX + \frac{p+q}{4}$ für $k = 0, 1, \ldots, \frac{p+q}{4} - 2$ Primzahlwerte annimmt.

Stark und Baker bestimmten die imaginär-quadratischen Zahlkörper $\mathbb{Q}(\sqrt{d})$ (mit $d < 0$ und d quadratfrei) mit Klassenzahl 2. Entsprechend ihrer Typen sind dies:

(i) $d = -6, -10, -22, -58$.

(ii) $d = -5, -13, -37$.

(iii) $d = -15, -35, -51, -91, -115, -123, -187, -235, -267, -403, -427$.

Mit diesen Werten von d erhält man optimal primzahlerzeugende Polynome.

Insbesondere ist $2X^2 + 29$ ein optimal primzahlerzeugendes Polynom mit Primzahlwerten für $k = 0, 1, \ldots, 28$; es gehört zum Körper $\mathbb{Q}(\sqrt{-58})$, der die Klassenzahl 2 hat.

- 29 ist die Anzahl verschiedener Topologien auf einer Menge mit 3 Elementen. Es bezeichne τ_n die Anzahl der Topologien auf einer Menge mit n Elementen; also $\tau_1 = 1$ und $\tau_2 = 2$. Man kennt die Werte von τ_n für $n \leq 9$ (Radoux (1975)).

Sich den Dreißigern nähernd, dem Alter der Zuversicht, lächelte einen das Leben an. 29 war das erste Primzahlzwillingsalter, das ich erreichte, nachdem ich von Beruf Mathematiker geworden war. Also wähle ich die Zahl

30

- In diesem Alter war ich in Bahia Blanca, Argentinien, und arbeitete an einem Buch, das so glaube ich das am weitesten südlich veröffentlichte mathematische Buch ist (dies stimmt zumindest für Bücher über geordnete Gruppen—und meins ist darunter sicher nicht das nördlichste seiner Art).
- Es gibt nur ein einfaches pythagoreisches Dreieck, dessen Fläche gleich seinem Umfang ist, nämlich $(5, 12, 13)$ mit Umfang 30.
- 30 ist die größte ganze Zahl d mit der Eigenschaft, dass a prim ist, wenn $1 < a < d$ und $\mathrm{ggT}(a, d) = 1$. Andere Zahlen mit dieser Eigenschaft sind: 3, 4, 6, 8, 12, 18 und 24. Dies war zunächst von Schatunowsky im Jahr 1893 und unabhängig von Wolfskehl 1901

bewiesen worden. (WOLFSKEHL ist ein reicher Mathematiker gewesen, der 100.000 Goldmark für denjenigen ausgeschrieben hatte, der den ersten Beweis von Fermats letztem Satz in einem angesehenen mathematischen Journal veröffentlichen würde.)
Dieses Resultat besitzt die folgende Interpretation. Gegeben seien $d > 1$ und a, $1 \leq a < d$, $\mathrm{ggT}(a, d) = 1$. Nach Dirichlets Satz gibt es unendlich viele Primzahlen der Form $a + kd$ $(k \geq 0)$. Sei $p(a, d)$ die kleinste derartige Primzahl und

$$p(d) = \max\{p(a, d) \mid 1 \leq a < d, \mathrm{ggT}(a, d) = 1\}.$$

Wenn $d > 30$, dann $p(d) > d + 1$. Insbesondere,

$$\liminf \frac{p(d)}{d+1} > 1.$$

POMERANCE bewies:

$$\liminf \frac{p(d)}{\varphi(d) \log d} \geq e^{\gamma}$$

wobei $\varphi(d)$ der Wert von EULERs φ-Funktion für d ist und γ die Euler-Mascheroni-Konstante bezeichnet.
Andererseits bewies LINNIK, dass $p(d) \leq d^L$, wobei L eine Konstante ist und d genügend groß sei. HEATH-BROWN zeigte, dass $L \leq 5{,}5$.

32

- 32 ist die kleinste ganze Zahl n derart, dass die Anzahl γ_n von Gruppen der Ordnung n (bis auf Isomorphie) größer ist als n: $\gamma_{32} = 51$.
  Ich kann die Zahl 32 nicht ausstehen. Bei 32 Grad Fahrenheit wird Wasser zu Eis und es fängt an zu schneien. Lassen Sie uns das Thema wechseln!

Ältere Leute erinnern sich am Besten an die Ereignisse ihrer Jugend oder aber an das, was sich erst kürzlich ereignete. Ich habe nichts von dem vergessen, das ich nicht vergessen wollte, also könnte ich Ihnen alles über die Jahre 33, 34, ... erzählen. Aber ich möchte mich lieber auf die 60er konzentrieren.

60

- 60 war die Basis des Zahlsystems der Sumerer (ca. 3500 v.Chr.). Wir verwenden das Sexagesimal-System heute immer noch in der Astronomie und bei der Unterteilung der Stunde.
- 60 ist eine *stark zerlegbare Zahl*. Derartige Zahlen wurden von Ramanujan (1915) eingeführt und untersucht: Die natürliche Zahl n ist *stark zerlegbar*, wenn $d(n) > d(m)$ für jedes m, $1 \le m < n$, wobei $d(n) =$ Anzahl der Teiler von n. So ist $d(60) = d(2^2 \cdot 3 \cdot 5) = 3 \cdot 2 \cdot 2 = 12$. Die kleinsten stark zerlegbaren Zahlen sind

$$2, 4, 6, 12, 24, 32, 48, 60, 120, 180, 240, 360, 720, 840, \ldots.$$

- 60 ist eine *einheitlich perfekte Zahl*, was ich nun definiere. Eine Zahl d ist ein *einheitlicher Teiler* von n, wenn $d \mid n$ und $\mathrm{ggT}(d, n/d) = 1$; n ist *einheitlich perfekt*, wenn

$$n = \sum \{d \mid 1 \le d < n,\ d \text{ einheitlicher Teiler von } n\}.$$

  Einheitliche Teiler von 60 sind 1, 3, 4, 5, 12, 15, 20 und ihre Summe ist in der Tat 60.
  Vermutung: Es gibt nur endlich viele einheitlich perfekte Zahlen.
  Die einzigen bekannten einheitlich perfekten Zahlen sind

$$6, 60, 90, 87360 \quad \text{und} \quad 2^{18} \cdot 3 \cdot 7 \cdot 11 \cdot 13 \cdot 19 \cdot 37 \cdot 79 \cdot 109 \cdot 157 \cdot 313.$$

- 60 ist die Anzahl von Geraden, die Schnittlinien der Paare von Ebenen der Flächen eines Dodekaeders sind.
- 60 ist die Ordnung der Gruppe von Isometrien des Ikosaeders. Dies ist die alternierende Gruppe von 5 Zeichen. Es ist die nicht-abelsche einfache Gruppe mit kleinster Ordnung. Die einfachen Gruppen wurden klassifiziert—was ein großer Erfolg ist! Es gibt 18 unendliche Familien:
  - zyklische Gruppen mit Primzahlordnung;
  - alternierende Gruppen A_n mit $n \ge 5$;
  - sechs Familien in Verbindung mit den klassischen Gruppen;
  - zehn Familien in Verbindung zu Lie-Algebren (entdeckt von Dickson, Chevalley, Suzuki, Ree und Steinberg.

  Es gibt zudem 26 „sporadische“ Gruppen, die nicht zu obigen Familien gehören. Die sporadische Gruppe mit der größten Ordnung ist Fischers Monster, die

$$2^{46} \cdot 3^{20} \cdot 5^9 \cdot 7^6 \cdot 11^2 \cdot 13^3 \cdot 17 \cdot 19 \cdot 23 \cdot 29 \cdot 31 \cdot 41 \cdot 47 \cdot 59 \cdot 71 \ge 8 \cdot 10^{53}$$

  Elemente besitzt.

61

- Eine Kuriosität: Sei $k \geq 0$ und seien $a_1, \ldots, a_k$, x, y Ziffern. Wenn die Zahl (in Dezimalschreibweise)

$$a_1 a_2 \ldots a_k xyxyxyxyxy$$

ein Quadrat ist, dann $xy = 21, 61$ oder 84. Beispiele:

$$1739288516161616161 = 1318820881^2;$$
$$258932382121212121 = 508853989^2.$$

- Die Mersenne-Zahl $M_{61} = 2^{61} - 1$ ist eine Primzahl. Es sind heute nur 46 Mersenne-Primzahlen $M_p = 2^p - 1$ bekannt, nämlich die mit

$p = 2, 3, 5, 7, 13, 17, 19, 31, 61, 89, 107, 127, 521, 607, 1279, 2203, 2281,$
$3217, 4253, 4423, 9689, 9941, 11213, 19937, 21701, 23209, 44497,$
$86243, 110503, 132049, 216091, 756839, 859433, 1257787, 1398269,$
$2976221, 3021227, 6972593, 13466917, 20996011, 24036583,$
$25964951, 30402457, 32582657, 37156667$ und 43112609.

$2^{43112609} - 1$ ist auch die größte heute bekannte Primzahl.

62

Diese Zahl ist bemerkenswert, da sie so uninteressant ist. Tatsächlich sei angenommen, dass es eine Zahl gäbe, die aus welchem Grund auch immer uninteressant ist. Damit gibt es eine kleinste uninteressante Zahl und diese wäre interessant, da es sich um die kleinste uninteressante Zahl handelt.

Aber dies ist nur ein weiteres Beispiel für Russells Paradoxon ....

63

- Diese Zahl taucht im Zusammenhang mit *Kaprekars Algorithmus* für Zahlen mit zwei Ziffern auf. Dieser Algorithmus für Zahlen mit k Ziffern funktioniert wie folgt: Gegeben seien k Ziffern $a_1 \ldots a_k$, nicht alle identisch, mit $a_1 \geq a_2 \geq \cdots \geq a_k \geq 0$. Betrachte zwei Zahlen, die aus diesen Ziffern gebildet sind: $a_1 a_2 \ldots a_k$ und $a_k a_{k-1} \ldots a_1$.

Berechne ihre Differenz und wiederhole den Prozess mit den so gewonnenen k Ziffern.
Kaprekars Algorithmus für 2, 3, 4 und 5 Ziffern führt zu den folgenden Fixpunkten bzw. Zyklen.

2 Ziffern $\rightarrow$ Zyklus 63 - 27 - 45 - 09 - 81
3 Ziffern $\rightarrow$ 495
4 Ziffern $\rightarrow$ 6174
5 Ziffern $\rightarrow$ einer der 3 Zyklen: 99954 - 95553
98532 - 97443 - 96642 - 97731
98622 - 97533 - 96543 - 97641

Beispiel: $\{3, 5\}$: $53-35 = 18$, $81-18 = 63$, $63-36 = 27$, $72-27 = 45$, $54 - 45 = 09$, $90 - 09 = 81$.

- 63 ist die einzige Zahl der Form $2^n - 1$ mit $n > 1$, die keinen *primitiven Primfaktor* besitzt. Erklärung: Betrachte für $1 \leq b < a$ mit $\mathrm{ggT}(a, b) = 1$ die Folge von Binomen $a^n - b^n$ für $n \geq 1$. Die Primzahl p ist ein *primitiver Primfaktor* von $a^n - b^n$, wenn $p \mid a^n - b^n$, aber $p \nmid a^m - b^m$ für $1 \leq m < n$.
ZSIGMONDY bewies unter obigen Voraussetzungen, dass jedes Binom $a^n - b^n$ einen primitiven Primfaktor besitzt, ausgenommen die folgenen Fälle:
(i) $n = 1$, $a - b = 1$;
(ii) $n = 2$, a und b ungerade und $(a + b)$ eine Zweierpotenz;
(iii) $n = 6$, $a = 2$, $b = 1$.
Dieser Satz besitzt viele Anwendungen beim Studium von exponentiellen diophantischen Gleichungen; siehe Ribenboim (1994). Für $a = 2$ und $b = 1$ sieht die Folge so aus:

$$1, 3, 7, 15 = 3 \cdot 5, 31, 63 = 3^2 \cdot 7, 127, 257, 511, 1023 = 3 \cdot 11 \cdot 31, \ldots$$

64

64 ist fast 65, eine Zahl die ich zu erreichen gehasst habe, die aber trotzdem viele interessante Eigenschaften besitzt.

65

- 65 ist die kleinste Zahl, die sich auf zwei verschiedene Weisen als Summe von zwei Quadraten natürlicher Zahlen darstellen lässt (bis auf Reihenfolge der Summanden):

$$65 = 8^2 + 1^2 = 7^2 + 4^2.$$

Man erinnere sich an Fermats Ergebnis: n ist Summe von zwei Quadraten genau dann, wenn für jedes prime $p \equiv 3 \pmod 4$ der Wert $v_p(n)$ gerade ist. (Dabei bezeichnet $v_p(n)$ den p-adischen Wert von n, d.h. $p^{v_p(n)} \mid n$ aber $p^{v_p(n)+1}$ teilt n nicht.) Es folgt eine Formel für die Zahl

$$r(n) = \#\{(a,b) \mid 0 \le b \le a \text{ und } n = a^2 + b^2\}.$$

Für jedes $d \ge 1$, sei

$$\chi(d) = \begin{cases} (-1)^{\frac{d-1}{2}} & \text{für } d \text{ ungerade,} \\ 0 & \text{für } d \text{ gerade.} \end{cases}$$

Sei $R(n) = \sum_{d|n} \chi(d)$. Dann

$$r(n) = \begin{cases} \frac{R(n)}{2} & \text{für } R(n) \text{ gerade,} \\ \frac{1+R(n)}{2} & \text{für } R(n) \text{ ungerade.} \end{cases}$$

Beispiel: $65 = 5 \cdot 13$ hat die Teiler 1, 5, 13, 65 und $R(65) = \sum_{d|65} \chi(d) = 4$, also $r(65) = 2$.

- 65 ist die kleinste Hypotenuse, die zwei pythagoreische Dreiecke gemeinsam haben. Dies folgt aus der Parametrisierung der Seiten pythagoreischer Dreiecke: Wenn $0 < x$, y, z mit y gerade und $x^2 + y^2 = z^2$, dann gibt es a und b, $1 \le b < a$ derart, dass

$$x = a^2 - b^2; \quad y = 2ab; \quad z = a^2 + b^2.$$

Darüberhinaus ist das Dreieck primitiv (d.h. $\mathrm{ggT}(x,y,z) = 1$) genau dann, wenn $\mathrm{ggT}(a,b) = 1$. Aus $65 = 8^2 + 1^2 = 7^2 + 4^2$ erhält man die pythagoreischen Dreiecke $(63, 16, 65)$ und $(33, 56, 65)$.

- Eine Kuriosität: 65 ist die einzige Zahl mit 2 Ziffern d, e, $0 \le e < d \le 9$ und der Eigenschaft, dass $(de)^2 - (ed)^2 = \square$, also ein Quadrat ist. Tatsächlich ist $65^2 - 56^2 = 33^2$ und die Eindeutigkeit folgt aus der oben angegebenen Parametrisierung.
- 65 ist auch eine bemerkenswerte Zahl der *zweiten Art,* d.h. sie zählt die Anzahl bemerkenswerter Zahlen, die eine bestimmte Eigenschaft besitzen. In diesem Fall ist 65 vielleicht die Anzahl von Eulers *numeri idonei.* Ich sage „vielleicht“, weil es sich immer noch um ein offenes Problem handelt und es anstelle von 65 eventuell auch 66 solcher Zahlen gibt.

Numeri idonei

Was sind diese *numeri idonei* von Euler? Auch als *geeignete Zahlen* bezeichnet, wurden sie von Euler in geeigneter Weise verwendet, um Primzahlen zu erzeugen.

Ich werde nun erklären, was *numeri idonei* sind. Sei $n \geq 1$. Wenn q eine ungerade Primzahl ist und es ganze Zahlen x, $y \geq 0$ derart gibt, dass $q = x^2 + ny^2$, dann:

(i) $\mathrm{ggT}(x, ny) = 1$;
(ii) wenn $q = x_1^2 + ny_1^2$ mit ganzen Zahlen x_1, $y_1 \geq 0$, dann $x = x_1$ und $y = y_1$.

Wir könnten die folgende Frage stellen. *Angenommen, dass q eine ungerade ganze Zahl ist und dass $q = x^2 + ny^2$ mit ganzen Zahlen x, $y \geq 0$ derart, dass die Bedingungen (i) und (ii) oben erfüllt sind. Ist q dann eine Primzahl?*

Die Antwort hängt von n ab. Wenn $n = 1$, dann ist die Antwort „ja“, wie Fermat wusste. Für $n = 11$ ist die Antwort „nein“: $15 = 2^2 + 11 \cdot 1^2$ und Bedingungen (i) und (ii) sind erfüllt, aber 15 ist zerlegbar. Euler nannte n eine *numerus idoneus*, falls die Antwort auf obige Frage „ja“ ist.

Euler gab ein Kriterium an, mithilfe dessen man in endlich vielen Schritten verifizieren kann, ob eine gegebene Zahl geeignet ist, aber sein Beweis war fehlerhaft. Später fand Grube im Jahr 1874 das folgende Kriterium, wobei er in seinem Beweis Ergebnisse von Gauss verwendete, die ich gleich angeben werde. Demnach ist n genau dann eine geeignete Zahl, wenn für jedes $x \geq 0$ mit $q = n + x^2 \leq \frac{4n}{3}$ gilt, dass wenn $q = rs$ und $2x \leq r \leq s$, dann $r = s$ oder $r = 2x$.

Beispielsweise ist 60 eine geeignete Zahl, denn

$$\begin{aligned} 60 + 1^2 &= 61\,(\star), \\ 60 + 2^2 &= 64 = 4 \cdot 16 = 8 \cdot 8, \\ 60 + 3^2 &= 69\,(\star), \\ 60 + 4^2 &= 76\,(\star) \end{aligned}$$

und die Zahlen, die mit einem $(\star)$ markiert sind, besitzen keine Faktorisierung der angegebenen Form.

Euler zeigte beispielsweise, dass 1848 eine geeignete Zahl ist und dass es sich bei

$$q = 18518809 = 197^2 + 1848 \cdot 100^2$$

um eine Primzahl handelt. Zu EULERs Zeiten war dies ein besondere Leistung.

GAUSS verstand geeignete Zahlen im Sinne seiner Theorie der binären quadratischen Formen. Die Zahl n ist genau dann geeignet, wenn jedes Geschlecht der Form $x^2 + ny^2$ nur eine Klasse besitzt.

Hier eine Auflistung der 65 geeigneten Zahlen, die EULER fand:

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.

Gibt es weitere geeignete Zahlen? CHOWLA zeigte, dass es höchstens endlich viele geeignete Zahlen gibt; später führte eine feinere Analyse (zum Beispiel von BRIGGS, GROSSWALD und WEINBERGER) zum Ergebnis, dass es höchstens 66 geeignete Zahlen geben kann.

Das Problem ist schwierig. Der Ausschluss einer weiteren *numerus idoneus* ist von derselben Art wie der Ausschluss eines hypothetischen zehnten imaginär-quadratischen Zahlkörpers (von HEEGNER, STARK und BAKER), wie ich bereits erwähnt hatte.

Eine außergewöhnliche Verbindung

Falls Ihre Neugier bis jetzt noch nicht nachgelassen hat: Im Jahr 1989 traf ich in Athen aus Anlass meiner „Griechischen Vorlesungen über Fermats letzten Satz“ auf eine außergewöhnliche Verbindung von Zahlen. Etwas, das einem nur einmal im Leben widerfährt und sich nie wiederholt....

In diesem Jahr war das Alter meiner Frau und von mir 59 und 61—Primzahlzwillinge (wobei wir keine Zwillinge sind); im selben Jahr waren wir 37 Jahre verheiratet—die kleinste irreguläre Primzahl. Falls Sie noch interessiert sind: KUMMER hatte bewiesen, dass Fermats letzter Satz für alle ungeraden Primzahlexponenten p, die reguläre Primzahlen sind, wahr ist. Dies sind diejenigen Primzahlen p, die die Klassenzahl des von der $p$ten Einheitswurzel erzeugten Kreisteilungskörpers nicht teilen. KUMMER entdeckte auch, dass 37 die kleinste irreguläre Primzahl ist. Schade, dass 1989 (das Jahr meiner Athen-Vorlesung) keine Primzahl ist.

Nun sind Sie herausgefordert, das nächste Auftreten von Zahlen wie 37, 59, 61 zu finden, das Ganze aber in einem Primzahljahr.

Bemerkungen. Dieses Kapitel über bemerkenswerte Zahlen wäre nicht möglich gewesen ohne das originäre Buch von F. Le Lionnais, *Les Nombres Remarquables*, erschienen 1983 bei Hermann in Paris.

François Le Lionnais war kein professioneller Mathematiker, sondern eher ein Wissenschaftsautor, und als solcher sehr gut informiert. Sein Buch *Les Grands Courants de la Pensée Mathématique* fesselt den Leser auch heute noch. Kurz nach dem Krieg sammelte er in seinem Buch die Ideen verschiedener junger Mathematiker—zu jener Zeit noch wenig bekannt—die bald zum Gipfel aufsteigen würden. Eine englische Übersetzung und das Original sind in guten Bibliotheken vorhanden. Ich bin im Besitz eines signierten Exemplars des Buchs über bemerkenswerte Zahlen, worin Le Lionnais sich bei mir dafür bedankt, ihn auf die Zahl 1093 aufmerksam gemacht zu haben. Sie können über diese Zahl im Kapitel 8 dieses Buches nachlesen.

Ein weiteres Buch derselben Art, das mir sehr half ist: D. Wells, *The Penguin Dictionary of Curious und Interesting Numbers*, Penguin, London, UK, 1986.

Für Ergebnisse zu algebraischen ganzen Zahlen ist nichts leichter für mich, als auf mein eigenes Buch Ribenboim (2000) zu verweisen, das im Springer-Verlag erschien. Für *numeri idonei*, siehe Frei (1984). Bezüglich primitiver Faktoren von Binomen, siehe Ribenboim (1994). Über Primzahlen, Fibonacci-Zahlen und ähnliche Themen, siehe Ribenboim (2006). Weitere Hinweise finden sich in Guy (2004).

Es versteht sich von selbst, dass die folgende Literaturliste unvollständig ist.

Literaturverzeichnis

1984 G. Frei. Les nombres convenables de Leonhard Euler. In *Number theory (Besançon), 1983–1984*, Exp. Nr. 1, 58. Univ. Franche-Comté, Besançon.

1994 P. Ribenboim. *Catalan's Conjecture.* Academic Press, Boston.

1996 P. Ribenboim. *The New Book of Prime Number Records.* Springer-Verlag, New York.

2000 P. Ribenboim. *The Classical Theory of Algebraic Numbers.* Springer-Verlag, New York.

2004 R. K. Guy. *Unsolved Problems in Number Theory.* Springer-Verlag, Berlin, 3. Ausgabe.

2006 P. Ribenboim. *Die Welt der Primzahlen.* Springer-Verlag, Heidelberg.

Namensverzeichnis

Sachverzeichnis