Springer-Lehrbuch

Meine Zahlen, meine Freunde

Glanzlichter der Zahlentheorie

Bearbeitet von
Paulo Ribenboim, Jörg Richstein

1. Auflage 2009. Taschenbuch. x, 391 S. Paperback
ISBN 978 3 540 87955 8
Format (B x L): 15,5 x 23,5 cm
Gewicht: 608 g

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

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

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
   $n = 1, \quad m = 2, \quad P = \square,$ oder
   $n = 1, \quad m = 12, \quad P = 1,$ oder
   $n = 3, \quad m = 6, \quad P = 1,$ 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
   $n = 1, \quad m = 6, \quad P = 3,$ 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
   $n = 0, \quad m = 6, \quad P = 1,$ oder
   $n = 1, \quad m = 3, \quad P = 1,$ 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