2
Wie kann man Primzahlen erkennen?

In Artikel 329 der *Disquisitiones Arithmeticae* schreibt Gauß (1801):

> Dass die Aufgabe, die Primzahlen von den zusammengesetzten zu unterscheiden und letztere in ihre Primfactoren zu zerlegen, zu den wichtigsten und nützlichsten der gesamten Arithmetik gehört und die Bemühungen und den Scharfsinn sowohl der alten wie auch der neueren Geometer in Anspruch genommen hat, ist so bekannt, dass es überflüssig wäre, hierüber viele Worte zu verlieren. [...] Ausserdem aber dürfte es die Würde der Wissenschaft erheischen, alle Hülfsmittel zur Lösung jenes so eleganten und berühmten Problems fleissig zu vervollkommnen.

Die erste Feststellung im Zusammenhang mit den Fragen der Primalität und Faktorisierung von Zahlen ist klar: Für beide Probleme existiert ein Algorithmus. Damit ist ein Verfahren gemeint, das für beliebiges N in endlich vielen Schritten erkennen lässt, ob N eine Primzahl ist, oder im Falle der Zerlegbarkeit die Primfaktoren liefert. Für eine gegebene natürliche Zahl N muss man nur alle Zahlen $n = 2, 3, \ldots$ bis zu $[\sqrt{N}]$ (der größten ganzen Zahl, die $\sqrt{N}$ nicht überschreitet) der Reihe nach daraufhin prüfen, ob sie Teiler von N sind. Wenn dies für kein n der Fall ist, handelt es sich bei N um eine Primzahl. Falls jedoch etwa N_0 ein Teiler von N ist, schreibt man $N = N_0 N_1$, wobei $N_1 < N$,

P. Ribenboim, *Die Welt der Primzahlen*, 2. Aufl., Springer-Lehrbuch,
DOI 10.1007/978-3-642-18079-8_2, © Springer-Verlag Berlin Heidelberg 2011

und wiederholt den Vorgang für N_0 und N_1. Dies ergibt schließlich die vollständige Primfaktorenzerlegung von N.

Was ich gerade sagte, ist so offensichtlich, dass es fast schon belanglos erscheint. Es sollte allerdings nicht unerwähnt bleiben, dass es für große Zahlen N sehr lange dauern kann, bis dieser Algorithmus entschieden hat, ob N prim oder aber zerlegbar ist.

Diese Bemerkung berührt den wichtigsten praktischen Aspekt, nämlich ein effizientes Verfahren dafür zu finden – eines, das so wenig Rechenoperationen wie möglich erfordert und somit schneller und kostengünstiger durchzuführen ist.

Dieses Kapitel ist in mehrere Abschnitte unterteilt, in denen ich verschiedene Ansätze untersuchen und die dazu notwendigen theoretischen Grundlagen erläutern werde.

I Das Sieb des Eratosthenes

Wie bereits gesagt, kann man mit der Probedivision durch alle Zahlen n mit $n^2 \leq N$ feststellen, ob N eine Primzahl ist.

Da die Multiplikation eine einfachere Operation ist als die Division, hatte Eratosthenes im 3. Jahrhundert v. Chr. die Idee, die notwendigen Berechnungen mit Hilfe des seitdem bekannten Siebes zu organisieren. Es dient dazu, sämtliche Primzahlen sowie die Faktorisierungen der zerlegbaren Zahlen unterhalb einer gegebenen Grenze zu bestimmen. Dies wird nun anhand eines Beispiels (für $N = 101$) illustriert.

	2	3	~~4~~	5	~~6~~	7	~~8~~	~~9~~	~~10~~
11	~~12~~	13	~~14~~	~~15~~	~~16~~	17	~~18~~	19	~~20~~
~~21~~	~~22~~	23	~~24~~	~~25~~	~~26~~	~~27~~	~~28~~	29	~~30~~
31	~~32~~	~~33~~	~~34~~	~~35~~	~~36~~	37	~~38~~	~~39~~	~~40~~
41	~~42~~	43	~~44~~	~~45~~	~~46~~	47	~~48~~	~~49~~	~~50~~
~~51~~	~~52~~	53	~~54~~	~~55~~	~~56~~	~~57~~	~~58~~	59	~~60~~
61	~~62~~	~~63~~	~~64~~	~~65~~	~~66~~	67	~~68~~	~~69~~	~~70~~
71	~~72~~	73	~~74~~	~~75~~	~~76~~	~~77~~	~~78~~	79	~~80~~
~~81~~	~~82~~	83	~~84~~	~~85~~	~~86~~	~~87~~	~~88~~	89	~~90~~
~~91~~	~~92~~	~~93~~	~~94~~	~~95~~	~~96~~	97	~~98~~	~~99~~	~~100~~
101									

Man geht wie folgt vor: Schreibe alle Zahlen bis 101 auf; streiche alle Vielfachen der 2, die größer als 2 sind; in jedem weiteren Schritt streiche alle Vielfachen der kleinsten übrig gebliebenen Zahl p, die größer als p sind. Man ist fertig, wenn $p^2 > 101$ ist.

So werden alle Vielfachen von $2, 3, 5, 7 < \sqrt{101}$ ausgesiebt. Die Zahl 53 blieb übrig und ist deshalb prim. Die Primzahlen bis 101 sind also 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97, 101.

Dieses Verfahren bildet die Grundlage der Siebtheorie, die dazu entwickelt wurde, Abschätzungen für die Anzahl von Primzahlen zu gewinnen, die zusätzliche Bedingungen erfüllen.

II Einige grundlegende Sätze über Kongruenzen

In diesem Abschnitt beabsichtige ich, einige klassische Primzahltests und Faktorisierungsverfahren zu beschreiben. Diese stützen sich auf Sätze über Kongruenzen, vor allem auf den „kleinen Satz“ von Fermat, den alten Wilson'schen Satz sowie Eulers Verallgemeinerung des Satzes von Fermat. Ein Unterabschnitt wird den quadratischen Resten gewidmet sein. Dieses Thema ist von zentraler Bedeutung und steht auch im Zusammenhang mit Primzahltests, worauf ich bei passender Gelegenheit hinweisen werde.

A Der kleine Satz von Fermat und Primitivwurzeln modulo einer Primzahl

Kleiner Satz von Fermat. *Falls p eine Primzahl ist und a eine ganze Zahl, dann gilt $a^p \equiv a \pmod{p}$. Insbesondere gilt: Wenn p kein Teiler von a ist, dann ist $a^{p-1} \equiv 1 \pmod{p}$.*

Der erste Beweis des kleinen Satzes von Fermat wurde von Euler veröffentlicht.

Beweis. Die Aussage ist richtig für $a = 1$. Angenommen, sie gelte für ein a, dann ist durch Induktion $(a+1)^p \equiv a^p + 1 \equiv a + 1 \pmod{p}$. Somit ist der Satz für jede natürliche Zahl a bewiesen. □

Obiger Beweis benötigte allein die Tatsache, dass für eine Primzahl p und $1 \leq k \leq p-1$ der Binomialkoeffizient $\binom{p}{k}$ ein Vielfaches von p ist.

Man beachte diese unmittelbare Folgerung: Falls $p \nmid a$ und p^n die höchste Potenz von p ist, die $a^{p-1} - 1$ teilt, dann ist p^{n+e} die höchste

Potenz von p, die $a^{p^e(p-1)} - 1$ teilt (wobei $e \geq 1$); bei dieser Aussage muss n mindestens 2 betragen, falls $p = 2$ ist.

Aus dem Satz folgt, dass es für jede ganze Zahl a, die kein Vielfaches von p ist, einen kleinsten Exponenten $h \geq 1$ geben muss, so dass $a^h \equiv 1 \pmod{p}$. Darüber hinaus gilt $a^k \equiv 1 \pmod{p}$ genau dann, wenn h ein Teiler von k ist; insbesondere ist h Teiler von $p-1$. Diesen Exponenten h nennt man die *Ordnung von a modulo p*. Man beachte, dass $a \bmod p$, $a^2 \bmod p, \ldots, a^{h-1} \bmod p$, und $1 \bmod p$ alle verschieden sind.

Es ist nicht schwer zu zeigen, dass es für jede Primzahl p mindestens eine Zahl g gibt, die von p nicht geteilt wird und die modulo p genau die Ordnung $p-1$ hat. In diesem Fall sind die Mengen $\{g^0 \bmod p, g^1 \bmod p, \ldots, g^{p-2} \bmod p\}$ und $\{1 \bmod p, 2 \bmod p, \ldots, (p-1) \bmod p\}$ gleich.

Jede Zahl g, $1 \leq g \leq p-1$, für die $g \bmod p$ die Ordnung $p-1$ hat, nennt man *Primitivwurzel modulo p*. Ich erwähne hier den folgenden Satz:

Es sei p eine ungerade Primzahl, $k \geq 1$ und $S = \sum_{j=1}^{p-1} j^k$. Dann gilt

$$S \equiv \begin{cases} -1 \bmod p, & \text{falls } p-1 \mid k, \\ 0 \bmod p, & \text{falls } p-1 \nmid k. \end{cases}$$

Beweis. In der Tat gilt zunächst $j^k \equiv 1 \pmod{p}$ für $j = 1, 2, \ldots, p-1$, falls k von $p-1$ geteilt wird, so dass $S \equiv p-1 \equiv -1 \pmod{p}$. Falls $p-1$ kein Teiler von k ist, bezeichne g eine Primitivwurzel modulo p. Dann ist $g^k \not\equiv 1 \pmod{p}$. Da die Mengen von Restklassen $\{1 \bmod p, 2 \bmod p, \ldots, (p-1) \bmod p\}$ und $\{g \bmod p, 2g \bmod p, \ldots, (p-1)g \bmod p\}$ gleich sind, folgt

$$g^k S \equiv \sum_{j=1}^{p-1} (gj)^k \equiv \sum_{j=1}^{p-1} j^k \equiv S \pmod{p}.$$

Somit ergibt sich, dass $(g^k - 1)S \equiv 0 \pmod{p}$, und da p kein Teiler von $g^k - 1$ ist, muss $S \equiv 0 \pmod{p}$ gelten. □

Eine Primitivwurzel modulo p lässt sich mit Hilfe eines einfachen Verfahrens bestimmen, auf welches Gauß in den Artikeln 73, 74 der *Disquisitiones Arithmeticae* hinwies.

Man geht dazu wie folgt vor:

Schritt 1. Wähle eine beliebige Zahl a, $1 < a < p$, zum Beispiel $a = 2$, und schreibe jeweils die Reste von a, a^2, $a^3, \ldots$ modulo p auf.

Es sei t der kleinste Exponent, der $a^t \equiv 1 \pmod{p}$ erfüllt. Falls $t = p-1$, dann ist a eine Primitivwurzel modulo p. Ansonsten gehe zum nächsten Schritt.

Schritt 2. Wähle eine beliebige Zahl b, $1 < b < p$, so dass $b \not\equiv a^i \pmod{p}$ für $i = 1, \ldots, t$. Es sei nun u der kleinste Exponent, für den $b^u \equiv 1 \pmod{p}$ gilt. Es ist leicht einzusehen, dass u kein Faktor von t sein kann, sonst wäre $b^t \equiv 1 \pmod{p}$. Aber $1, a, a^2, \ldots, a^{t-1}$ sind t paarweise inkongruente Lösungen der Kongruenz $X^t \equiv 1 \pmod{p}$ und dies sind alle möglichen Lösungen, daher $b \equiv a^m \pmod{p}$ für irgendein m, $0 \leq m \leq t-1$, was der Annahme widerspräche. Falls $u = p-1$, dann ist b eine Primitivwurzel modulo p. Falls hingegen $u \neq p-1$, sei v das kleinste gemeinsame Vielfache von t und u; also $v = mn$, wobei m ein Teiler von t, n ein Teiler von u, und $\mathrm{ggT}(m, n) = 1$ ist. Es sei $a' \equiv a^{t/m} \pmod{p}$, $b' \equiv b^{u/n} \pmod{p}$, so dass $c = a'b'$ die Ordnung $mn = v$ modulo p hat. Falls also $v = p-1$, dann ist c eine Primitivwurzel modulo p. Andernfalls gehe zum nächsten Schritt, der ähnlich wie Schritt 2 verläuft.

Man beachte, dass $v > t$, so dass man in jedem Schritt entweder eine Primitivwurzel modulo p findet, oder aber eine Zahl mit einer größeren Ordnung modulo p konstruiert hat. Dieses Verfahren muss schließlich zum Ende kommen, und man erlangt eine Zahl mit Ordnung $p-1$ modulo p, also eine Primitivwurzel modulo p.

Gauß veranschaulichte das Verfahren anhand des Beispiels $p = 73$ und fand $g = 5$ als Primitivwurzel modulo 73.

Das obige Konstruktionsverfahren führt zwar immer zum Ziel, jedoch nicht notwendigerweise zur kleinsten Zahl g_p, $1 < g_p < p$, die eine Primitivwurzel modulo p darstellt.

Die Bestimmung von g_p erfordert die sukzessive Berechnung der Ordnungen der Zahlen $a = 2, 3, \ldots$ modulo p. Es kann nicht auf einheitliche Weise für alle Primzahlen p vorausgesagt werden, welche die kleinste Primitivwurzel modulo p ist. Jedoch wurden einige Resultate über die Größe von g_p erzielt. 1944 bewies Pillai, dass es unendlich viele prime p gibt, für die $g_p > C \log\log p$ ist (mit einer positiven Konstanten C). Insbesondere ist $\limsup_{p\to\infty} g_p = \infty$. Einige Jahre später gelang es Fridlender (1949) unter Verwendung eines tiefliegenden Satzes von Linnik über Primzahlen in arithmetischen Folgen (siehe Kapitel 4), und unabhängig von ihm Salié (1950), zu zeigen, dass $g_p > C \log p$ für eine Konstante C und unendlich viele Primzahlen p gilt. Andererseits

wächst g_p auch nicht allzu schnell, wie Burgess 1962 bewies:

$$g_p \leq Cp^{1/4+\varepsilon}$$

(für $\varepsilon > 0$, eine Konstante $C > 0$, und genügend großes p).

Grosswald gab im Jahre 1981 für Burgess' Ergebnis explizite Werte an: Falls $p > e^{e^{24}}$ dann gilt $g_p < p^{0,499}$.

Der Beweis eines schwächeren Resultats (mit 1/2 anstelle von 1/4), das Winogradoff zugeschrieben wird, findet sich in Landaus *Vorlesungen über Zahlentheorie*, Teil VII, Kapitel 14 (siehe die Literatur zu den Allgemeinen Grundlagen).

Der folgende Satz lässt sich einfach beweisen (als Problem von Powell 1983 gestellt, Lösung von Kearnes aus dem Jahre 1984):

Für jede positive ganze Zahl M existieren unendlich viele Primzahlen p derart, dass $M < g_p < p - M$.

Zur Illustration findet sich auf der folgenden Seite eine Tabelle mit der jeweils kleinsten Primitivwurzel modulo p für alle Primzahlen $p < 1000$.

Ein kurzer Blick auf die Tabelle legt sofort die Frage nahe, ob 2 eine Primitivwurzel für unendlich viele Primzahlen ist. Oder allgemeiner gefragt: Falls $a \neq \pm 1$ keine Quadratzahl ist, ist dann a eine Primitivwurzel modulo unendlich vieler Primzahlen? Auf dieses schwierige Problem werde ich in Kapitel 4 noch einmal zurückkommen.

B Der Satz von Wilson

Satz von Wilson. *Falls p eine Primzahl ist, so gilt*

$$(p-1)! \equiv -1 \pmod{p}.$$

Beweis. Folgt als Korollar aus Fermats kleinem Satz. Denn $1, 2, \ldots, p-1$ sind Wurzeln der Kongruenz $X^{p-1} - 1 \equiv 0 \pmod{p}$. Aber eine Kongruenz modulo p kann nicht mehr Wurzeln haben, als ihr Grad beträgt. Daher ist

$$X^{p-1} - 1 \equiv (X-1)(X-2)\cdots(X-(p-1)) \pmod{p}.$$

Wenn man die konstanten Terme beider Seiten vergleicht, erhält man $-1 \equiv (-1)^{p-1}(p-1)! = (p-1)! \pmod{p}$ (was auch für den Fall $p = 2$ zutrifft). □

Tabelle 1. Die kleinste Primitivwurzel modulo p

p	g_p	p	g_p	p	g_p	p	g_p	p	g_p	p	g_p
2	1	127	3	283	3	467	2	661	2	877	2
3	2	131	2	293	2	479	13	673	5	881	3
5	2	137	3	307	5	487	3	677	2	883	2
7	3	139	2	311	17	491	2	683	5	887	5
11	2	149	2	313	10	499	7	691	3	907	2
13	2	151	6	317	2	503	5	701	2	911	17
17	3	157	5	331	3	509	2	709	2	919	7
19	2	163	2	337	10	521	3	719	11	929	3
23	5	167	5	347	2	523	2	727	5	937	5
29	2	173	2	349	2	541	2	733	6	941	2
31	3	179	2	353	3	547	2	739	3	947	2
37	2	181	2	359	7	557	2	743	5	953	3
41	6	191	19	367	6	563	2	751	3	967	5
43	3	193	5	373	2	569	3	757	2	971	6
47	5	197	2	379	2	571	3	761	6	977	3
53	2	199	3	383	5	577	5	769	11	983	5
59	2	211	2	389	2	587	2	773	2	991	6
61	2	223	3	397	5	593	3	787	2	997	7
67	2	227	2	401	3	599	7	797	2		
71	7	229	6	409	21	601	7	809	3		
73	5	233	3	419	2	607	3	811	3		
79	3	239	7	421	2	613	2	821	3		
83	2	241	7	431	7	617	3	823	3		
89	3	251	6	433	5	619	2	827	2		
97	5	257	3	439	15	631	3	829	2		
101	2	263	5	443	2	641	3	839	11		
103	5	269	2	449	3	643	11	853	2		
107	2	271	6	457	13	647	5	857	3		
109	6	277	5	461	2	653	2	859	2		
113	3	281	3	463	3	659	2	863	5		

Der Satz von Wilson stellt zugleich eine Charakterisierung der Primzahlen dar. Wenn nämlich $N > 1$ eine zerlegbare natürliche Zahl ist, etwa $N = mn$ mit $1 < m, n < N - 1$, so ist m ein Teiler von N und $(N-1)!$, und damit $(N-1)! \not\equiv -1 \pmod{N}$.

Allerdings hat Wilsons Charakterisierung der Primzahlen keine praktische Bedeutung, wenn es darum geht, N auf Primalität hin zu testen. Denn es ist kein Algorithmus bekannt, der $N!$ schnell (z.B. in $\log N$ Schritten) berechnen könnte.

C Die Eigenschaften von Giuga und von Wolstenholme

Ich werde nun weitere Eigenschaften betrachten, die von Primzahlen erfüllt sind.

Die Eigenschaft von Giuga

Wie bereits erwähnt, erfüllt eine Primzahl p nach dem kleinen Satz von Fermat die Kongruenz

$$1^{p-1} + 2^{p-1} + \cdots + (p-1)^{p-1} \equiv -1 \pmod{p}.$$

Im Jahre 1950 fragte Giuga, ob auch die Umkehrung gilt: Falls $n > 1$ die Summe $1^{n-1} + 2^{n-1} + \cdots + (n-1)^{n-1} + 1$ teilt, ist n dann eine Primzahl?

Es ist leicht zu zeigen, dass n die Eigenschaft von Giuga genau dann erfüllt, wenn für jeden Primteiler p von n gilt, dass $p^2(p-1)$ Teiler von $n-p$ ist. Denn wenn man $n = pt$ setzt, entspricht Giugas Bedingung

$$A = 1 + \sum_{j=1}^{pt-1} j^{pt-1} \equiv 0 \pmod{p},$$

während die Forderung, dass $p^2(p-1)$ die Zahl $pt-p$ teilt, äquivalent zur Verknüpfung der Bedingungen $p \mid t-1$ und $p-1 \mid t-1$ ist. Aber $pt - 1 = (p-1)t + (t-1)$, und daher nach dem kleinem Satz von Fermat

$$A \equiv 1 + \sum_{j=1}^{pt-1} j^{t-1} \equiv 1 + tS \pmod{p},$$

wobei $S = \sum_{j=1}^{p-1} j^{t-1}$. Somit ist

$$A \equiv \begin{cases} 1-t \pmod{p}, & \text{falls} \quad p-1 \mid t-1 \\ 1 \pmod{p}, & \text{falls} \quad p-1 \nmid t-1. \end{cases}$$

Daher, wenn $A \equiv 0 \pmod{p}$, dann $p-1 \mid t-1$ und $p \mid t-1$. Umgekehrt implizieren letztere Bedingungen, dass $A \equiv 0 \pmod{p}$ und $p \nmid t$, also ist n quadratfrei und somit $A \equiv 0 \pmod{n}$. □

Es folgt sofort, dass $n \equiv p \equiv 1 \pmod{p-1}$, so dass mit $p \mid n$ auch $p-1 \mid n-1$ gilt. Eine zerlegbare Zahl mit dieser Eigenschaft nennt man eine *Carmichael-Zahl*.

In Abschnitt IX werde ich zeigen, dass diese Bedingung eine scharfe Einschränkung bedeutet. Jedenfalls weiß man heute, dass eine zerlegbare Zahl n, die Giugas Bedingung erfüllt (sofern es eine geben sollte), mindestens 13887 Stellen haben muss; siehe Bedocchi (1985) und Borwein, Borwein, Borwein & Girgensohn (1996).

Die Eigenschaft von Wolstenholme

Im Jahre 1862 bewies Wolstenholme den folgenden interessanten Satz: Falls $p \geq 5$ eine Primzahl ist, dann ist der Zähler von

$$1 + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{p-1}$$

durch p^2 teilbar und der Nenner von

$$1 + \frac{1}{2^2} + \frac{1}{3^2} + \cdots + \frac{1}{(p-1)^2}$$

ist ein Vielfaches von p.

Ein Beweis findet sich in Hardy & Wright (1938), siehe die Literatur zu den Allgemeinen Grundlagen. Von dieser Eigenschaft ausgehend lässt sich unschwer ableiten, dass für jede Primzahl $n \geq 5$ gilt:

$$\binom{2n-1}{n-1} \equiv 1 \pmod{n^3}.$$

Trifft auch die Umkehrung zu? Diese nach wie vor offene Frage wurde vor vielen Jahren von J.P. Jones gestellt. Eine Bejahung der Frage würde eine interessante und formal einfache Charakterisierung der Primzahlen liefern.

Das Problem führt auf natürliche Weise zu den folgenden Begriffen und Fragestellungen. Es sei $n \geq 5$ ungerade, und

$$A(n) = \binom{2n-1}{n-1}.$$

Für jedes $k \geq 1$ könnten wir nun die folgende Menge betrachten:

$$W_k = \{n \text{ ungerade}, n \geq 5 \mid A(n) \equiv 1 \pmod{n^k}\}.$$

Dann gilt $W_1 \supset W_2 \supset W_3 \supset W_4 \supset \ldots$. Nach dem Satz von Wolstenholme gehört jede Primzahl größer als 3 zu W_3. Die von Jones gestellte Frage besteht nun darin, ob W_3 genau die Menge der Primzahlen darstellt.

Eine Primzahl, die zu W_4 gehört, nennt man eine *Wolstenholme-Primzahl*. Es sind bisher nur zwei Wolstenholme-Primzahlen bekannt: 16843 wurde im Jahre 1964 von Selfridge und Pollack gefunden, die Zahl 2124679 wurde im Jahre 1993 von Crandall, Ernvall und Metsänkylä entdeckt. McIntosh zeigte 1995 durch Computerberechnungen, dass es keine weitere Wolstenholme-Primzahl $p < 5 \times 10^8$ gibt; diese Untersuchung wurde 2004 bis $p < 10^9$ ausgedehnt, siehe auch McIntosh & Roettger (2007).

Die Menge der zerlegbaren Zahlen aus W_2 enthält die Quadrate der Wolstenholme-Primzahlen. McIntosh vermutete sogar, dass beide Mengen übereinstimmen, und verifizierte dies bis 10^9: Das einzige zerlegbare $n \in W_2$ mit $n < 10^9$ ist $n = 283686649 = 16843^2$.

McIntosh vermutete zudem, dass es unendlich viele Wolstenholme-Primzahlen gibt und man geht heute davon aus, dass diese Vermutung richtig ist. Ein Beweis dafür dürfte aber sehr schwierig sein.

D Primzahlpotenzen als Teiler der Fakultät einer Zahl

Im Jahre 1808 bestimmte Legendre den genauen Exponenten der Potenz p^m einer Primzahl p, die eine Fakultät $a!$ teilt (derart, dass p^{m+1} kein Teiler mehr von $a!$ ist).

Es gibt einen sehr schönen Ausdruck von m in Form der p-adischen Entwicklung von a:

$$a = a_k p^k + a_{k-1} p^{k-1} + \cdots + a_1 p + a_0,$$

wobei $p^k \le a < p^{k+1}$ und $0 \le a_i \le p-1$ (für $i = 0, 1, \ldots, k$). Die Zahlen $a_0, a_1, \ldots, a_k$ sind die Ziffern von a zur Basis p.

Beispielsweise ist $328 = 2 \times 5^3 + 3 \times 5^2 + 3$, so dass 328 zur Basis 5 aus den Ziffern 2, 3, 0, 3 besteht. Unter Verwendung der obigen Bezeichnungsweise:

Satz von Legendre.

$$m = \sum_{i=1}^{\infty} \left[\frac{a}{p^i} \right] = \frac{a - (a_0 + a_1 + \cdots + a_k)}{p-1}\,.$$

Beweis. Nach Definition ist $a! = p^m b$, wobei $p \nmid b$. Es sei $a = q_1 p + r_1$ mit $0 \le q_1$, $0 \le r_1 < p$; also $q_1 = [a/p]$. Die Vielfachen von p kleiner als a sind $p, 2p, \ldots, q_1 p \le a$. Also $p^{q_1}(q_1!) = p^m b'$, wobei $p \nmid b'$. Daher

$q_1 + m_1 = m$, wobei p^{m_1} die maximale Potenz von p ist, die $q_1!$ teilt. Da nach Induktion $q_1 < a$, folgt

$$m_1 = \left[\frac{q_1}{p}\right] + \left[\frac{q_1}{p^2}\right] + \left[\frac{q_1}{p^3}\right] + \cdots .$$

Aber

$$\left[\frac{q_1}{p^i}\right] = \left[\frac{[a/p]}{p^i}\right] = \left[\frac{a}{p^{i+1}}\right],$$

wie man leicht überprüfen kann. Also

$$m = \left[\frac{a}{p}\right] + \left[\frac{a}{p^2}\right] + \left[\frac{a}{p^3}\right] + \cdots .$$

Nun leite ich den zweiten Ausdruck unter Verwendung der p-adischen Ziffern von $a = a_k p^k + \cdots + a_1 p + a_0$ her. Folglich,

$$\begin{aligned}
\left[\frac{a}{p}\right] &= a_k p^{k-1} + \cdots + a_1, \\
\left[\frac{a}{p^2}\right] &= a_k p^{k-2} + \cdots + a_2, \\
&\vdots \\
\left[\frac{a}{p^k}\right] &= a_k.
\end{aligned}$$

Also

$$\begin{aligned}
\sum_{i=0}^{\infty} \left[\frac{a}{p^i}\right] &= a_1 + a_2(p+1) + a_3(p^2+p+1) + \cdots \\
&\quad + a_k(p^{k-1} + p^{k-2} + \cdots + p + 1) \\
&= \frac{1}{p-1}\big\{a_1(p-1) + a_2(p^2-1) + \cdots + a_k(p^k-1)\big\} \\
&= \frac{1}{p-1}\big\{a - (a_0 + a_1 + \cdots + a_k)\big\}. \qquad \square
\end{aligned}$$

Kummer benutzte 1852 das Resultat von Legendre, um die maximale Potenz p^m von p zu bestimmen, die den Binomialkoeffizient

$$\binom{a+b}{a} = \frac{(a+b)!}{a!b!}$$

teilt, wobei $a \geq 1$, $b \geq 1$.

Es sei

$$a = a_0 + a_1 p + \cdots + a_t p^t,$$
$$b = b_0 + b_1 p + \cdots + b_t p^t,$$

wobei $0 \le a_i \le p-1$, $0 \le b_i \le p-1$, und entweder $a_t \neq 0$ oder $b_t \neq 0$. Es bezeichne $S_a = \sum_{i=0}^{t} a_i$, $S_b = \sum_{i=0}^{t} b_i$ die Summen der p-adischen Ziffern von a, b. Darüber hinaus sei c_i, $0 \le c_i \le p-1$, und $\varepsilon_i = 0$ oder 1 wie folgt definiert:

$$\begin{aligned} a_0 + b_0 &= \varepsilon_0 p + c_0, \\ \varepsilon_0 + a_1 + b_1 &= \varepsilon_1 p + c_1, \\ &\vdots \\ \varepsilon_{t-1} + a_t + b_t &= \varepsilon_t p + c_t. \end{aligned}$$

Sukzessive Multiplikation dieser Gleichungen mit $1, p, p^2, \ldots$ und Summation derselben liefert

$$\begin{aligned} &a + b + \varepsilon_0 p + \varepsilon_1 p^2 + \cdots + \varepsilon_{t-1} p^t \\ &\quad = \varepsilon_0 p + \varepsilon_1 p^2 + \cdots + \varepsilon_{t-1} p^t + \varepsilon_t p^{t+1} + c_0 + c_1 p + \cdots + c_t p^t. \end{aligned}$$

Also $a + b = c_0 + c_1 p + \cdots + c_t p^t + \varepsilon_t p^{t+1}$, was die Darstellung von $a+b$ zur Basis p ist. Analog erhält man durch Addition dieser Gleichungen:

$$S_a + S_b + (\varepsilon_0 + \varepsilon_1 + \cdots + \varepsilon_{t-1}) = (\varepsilon_0 + \varepsilon_1 + \cdots + \varepsilon_t)p + S_{a+b} - \varepsilon_t.$$

Unter Verwendung des Satzes von Legendre:

$$\begin{aligned} (p-1)m &= (a+b) - S_{a+b} - a + S_a - b + S_b \\ &= (p-1)(\varepsilon_0 + \varepsilon_1 + \cdots + \varepsilon_t). \end{aligned}$$

Daraus das folgende Ergebnis:

Satz von Kummer. *Der Exponent der maximalen Potenz von p, die $\binom{a+b}{a}$ teilt, ist gleich der Anzahl $\varepsilon_0 + \varepsilon_1 + \cdots + \varepsilon_t$ der Überträge, die bei der Addition von a und b zur Basis p entstehen.*

Dieser Satz wurde von Lucas 1878 erneut gefunden. Frasnay erweiterte dieses Resultat 1991, indem er ganze Zahlen durch p-adische Zahlen ersetzte.

Die Sätze von Legendre und Kummer kommen häufig zur Anwendung, sowohl in p-adischer Analysis, als auch beispielsweise in Kapitel 3, Abschnitt III.

E Der chinesische Restsatz

Obwohl unser vorrangiges Interesse hier bei den Primzahlen liegt, kommt man nicht umhin, sich auch mit gewöhnlichen ganzen Zahlen zu beschäftigen – was bei vielen Fragen aufgrund der eindeutigen Primfaktorenzerlegung ganzer Zahlen im Wesentlichen auf die simultane Betrachtung verschiedener Primzahlen hinausläuft.

Einer der Schlüssel zur Verknüpfung von Resultaten über ganze Zahlen n und ihrer Primfaktoren ist sehr alt. Tatsächlich wussten schon die Chinesen des Altertums davon und er wird daher als der chinesische Restsatz bezeichnet. Allerdings war er laut A. Zachariou (persönliche Mitteilung) bereits im antiken Griechenland bekannt. Da aber die Griechen so viele Theoreme entdeckten, werde ich in diesem Fall den traditionellen Namen beibehalten. Ich bin sicher, dass die meisten Leser den Satz bereits kennen:

Es seien $n_1, n_2, \ldots, n_k$ paarweise teilerfremde Zahlen größer als 1 *und $a_1, a_2, \ldots, a_k$ beliebige ganze Zahlen. Dann existiert eine Zahl a derart, dass*

$$\begin{cases} a \equiv a_1 & (\mathrm{mod}\ n_1) \\ a \equiv a_2 & (\mathrm{mod}\ n_2) \\ \quad \vdots & \\ a \equiv a_k & (\mathrm{mod}\ n_k). \end{cases}$$

Eine weitere Zahl a' erfüllt obige Kongruenzen nur genau dann, wenn $a \equiv a'$ (mod $n_1 n_2 \cdots n_k$). Es gibt also genau ein a mit $0 \leq a < n_1 n_2 \cdots n_k$.

Der Beweis ist sehr einfach, man kann ihn in vielen Büchern, aber auch in einem kurzen Artikel von Mozzochi (1967) nachlesen.

Der chinesische Restsatz hat viele Anwendungen. Es ist denkbar, dass eine dieser Anwendungen darin bestand, wie chinesische Generäle ihre Truppen zählten:

Aufstellung in Reihen zu 7!	(nicht 7 Fakultät, sondern ein GEBRÜLLTES militärisches Kommando.)
Aufstellung in Reihen zu 11!	
Aufstellung in Reihen zu 13!	
Aufstellung in Reihen zu 17!	

Durch Zählen der Reste der unvollständigen Reihen konnten die intelligenten Generäle nun die Anzahl ihrer Soldaten ermitteln.[1]

Hier ist eine weitere Anwendung des chinesischen Restsatzes: Es sei $n = p_1 p_2 \cdots p_k$ ein Produkt verschiedener Primzahlen und g_i eine Primitivwurzel modulo p_i (für jedes i). Falls nun g, mit $1 \le g \le n-1$ die Kongruenz $g \equiv g_i \pmod{p_i}$ für jedes $i = 1, 2, \ldots, k$ erfüllt, dann ist die Ordnung von g modulo p_i für jedes $i = 1, 2, \ldots, k$ gleich $p_i - 1$ und die Ordnung von g modulo n ist $\prod_{i=1}^{k}(p_i - 1)$.

F Die Eulersche φ-Funktion

Euler verallgemeinerte den kleinen Satz von Fermat, indem er eine Funktion einführte, die man *Eulersche φ-Funktion* nennt.

Für jedes $n \ge 1$ bezeichne $\varphi(n)$ die Anzahl der Zahlen a mit $1 \le a < n$ und $\mathrm{ggT}(a, n) = 1$. Für prime $n = p$ wird $\varphi(p) = p - 1$; zudem gilt

$$\varphi(p^k) = p^{k-1}(p-1) = p^k \left(1 - \frac{1}{p}\right).$$

Im Falle $m, n \ge 1$ und $\mathrm{ggT}(m, n) = 1$ erhält man darüber hinaus $\varphi(mn) = \varphi(m)\varphi(n)$, das heißt, φ ist eine multiplikative Funktion. Und so ergibt sich für eine beliebige ganze Zahl $n = \prod_p p^k$ (Produkt aller Primteiler p von n, $k \ge 1$), dass

$$\varphi(n) = \prod_p p^{k-1}(p-1) = n \prod_p \left(1 - \frac{1}{p}\right).$$

Eine weitere, einfache Eigenschaft ist: $n = \sum_{d|n} \varphi(d)$.

Euler bewies folgenden Satz:

Satz von Euler. *Wenn* $\mathrm{ggT}(a, n) = 1$*, dann gilt* $a^{\varphi(n)} \equiv 1 \pmod{n}$.

Beweis. Es sei $r = \varphi(n)$ und $b_1, \ldots, b_r$ paarweise modulo n inkongruente ganze Zahlen mit $\mathrm{ggT}(b_i, n) = 1$ für $i = 1, \ldots, r$.

Dann sind auch $ab_1, \ldots, ab_r$ paarweise modulo n inkongruent und es gilt $\mathrm{ggT}(ab_i, n) = 1$ für $i = 1, \ldots, r$. Somit sind die Mengen $\{b_1 \bmod n, \ldots, b_r \bmod n\}$ und $\{ab_1 \bmod n, \ldots, ab_r \bmod n\}$ gleich. Weiter

$$a^r \prod_{i=1}^{r} b_i \equiv \prod_{i=1}^{r} ab_i \equiv \prod_{i=1}^{r} b_i \pmod{n}.$$

[1] Unter uns gesagt, wurde das so wahrscheinlich nie praktiziert. Die Frage nach der Existenz intelligenter Generäle ist nach wie vor weit offen.

Somit ist

$$(a^r-1)\prod_{i=1}^{r} b_i \equiv 0 \pmod{n} \quad \text{und daher} \quad a^r \equiv 1 \pmod{n}. \qquad \square$$

Völlig analog zum kleinen Satz von Fermat folgt auch aus dem Satz von Euler, dass es einen kleinsten positiven Exponenten e mit $a^e \equiv 1 \pmod{n}$ gibt. Dieser wird *Ordnung von a modulo n* genannt. Wenn n eine Primzahl ist, fällt diese Definition mit der früheren zusammen. Man beachte auch, dass $a^m \equiv 1 \pmod{n}$ genau dann gilt, wenn m ein Vielfaches der Ordnung e von a mod n ist. Insbesondere ist e Teiler von $\varphi(n)$.

Wieder liegt es nahe, sich zu fragen, ob es für $n > 2$ immer eine zu n teilerfremde ganze Zahl a derart gibt, dass die Ordnung von a mod n gerade gleich $\varphi(n)$ ist. Man erinnere sich, dass solche Zahlen für prime $n = p$ existieren, dies sind die Primitivwurzeln modulo p. Für Potenzen $n = p^e$ ungerader Primzahlen gilt dies ebenso. Genauer sind folgende Aussagen gleichwertig:

(i) g ist eine Primitivwurzel modulo p und $g^{p-1} \not\equiv 1 \pmod{p^2}$;

(ii) g ist eine Primitivwurzel modulo p^2;

(iii) Für jedes $e \geq 2$ ist g eine Primitivwurzel modulo p^e.

Man beachte, dass 10 eine Primitivwurzel modulo 487 ist, aber $10^{486} \equiv 1 \pmod{487^2}$, so dass 10 keine Primitivwurzel modulo 487^2 sein kann. Die Zahl 487 ist für die Basis 10 das kleinste Beispiel mit dieser Eigenschaft. Ein weiteres Beispiel wäre 14 modulo 29.

Im Falle, dass n von $4p$ oder pq geteilt wird (wobei p, q verschiedene ungerade Primzahlen sind), gibt es jedoch keine zu n teilerfremde Zahl a mit einer Ordnung $\varphi(n)$. Tatsächlich kann man einfach zeigen, dass die Ordnung von a mod n höchstens gleich $\lambda(n)$ ist, wobei $\lambda(n)$ die folgende, von Carmichael 1912 definierte Funktion bezeichnet:

$$\lambda(1) = 1,\ \lambda(2) = 1,\ \lambda(4) = 2,\ \lambda(2^r) = 2^{r-2} \quad (\text{für } r \geq 3),$$

$$\lambda(p^r) = p^{r-1}(p-1) = \varphi(p^r) \quad \text{für prime } p > 2 \text{ und } r \geq 1,$$

$$\lambda\big(2^r p_1^{r_1} p_2^{r_2} \cdots p_s^{r_s}\big) = \mathrm{kgV}\big\{\lambda(2^r), \lambda(p_1^{r_1}), \ldots, \lambda(p_s^{r_s})\big\}$$

(mit kgV ist das kleinste gemeinsame Vielfache gemeint).

Man beachte, dass $\lambda(n)$ Teiler von $\varphi(n)$ ist, aber kleiner sein kann, und dass es eine ganze, zu n teilerfremde Zahl a gibt, die modulo n eine Ordnung $\lambda(n)$ hat.

Ich möchte diese Gelegenheit nutzen, um die Eulersche φ-Funktion genauer zu untersuchen. Zunächst werde ich mich dem Lehmer-Problem zuwenden, danach den Werten von φ, der Valenz, den nicht angenommenen Werten, der Durchschnittsfunktion usw.

Das Lehmer-Problem

Man erinnere sich, dass $\varphi(p)$ für prime p den Wert $p-1$ annimmt. Lehmer fragte im Jahre 1932, ob es eine zerlegbare Zahl n gibt, für die $\varphi(n)$ Teiler von $n-1$ ist. Sieben Jahrzehnte, nachdem Lehmer diese Frage aufwarf, scheint deren Beantwortung noch immer in weiter Ferne zu liegen. Die Verneinung würde eine weitere Charakterisierung der Primzahlen liefern.

Was kann überhaupt gesagt werden, solange das Problem noch ungelöst ist? Vielleicht nur, dass die Existenz zerlegbarer Zahlen n, für welche $\varphi(n)$ Teiler von $n-1$ ist, aus mancherlei Gründen höchst unwahrscheinlich ist:

(a) Eine solche Zahl müsste sehr groß sein (wenn es sie denn gibt);

(b) eine solche Zahl müsste viele Primfaktoren haben (wenn es sie denn gibt);

(c) die Anzahl derartiger zerlegbarer Zahlen, die kleiner als eine gegebene reelle Zahl x sind, ist durch eine sehr langsam wachsende Funktion von x beschränkt.

Lehmer zeigte 1932: Falls n zerlegbar und $\varphi(n)$ Teiler von $n-1$ ist, dann muss n ungerade und quadratfrei sein, und die Anzahl verschiedener Primfaktoren von n ist $\omega(n) \geq 7$. Eine spätere Arbeit von Schuh (1944) lieferte $\omega(n) \geq 11$ (obwohl sein Beweis fehlerhaft war). Lieuwens zeigte 1970: Wenn $3 \mid n$, dann ist $\omega(n) \geq 213$ und $n > 5{,}5 \times 10^{570}$; und falls $30 \nmid n$, dann ist $\omega(n) \geq 13$. Dabei wurde auch Schuhs Beweis berichtigt. Subbarao & Siva Rama Prasad (1985) verschärften die untere Grenze von Lieuwens für die Anzahl der Primfaktoren auf $\omega(n) \geq 1850$.

Rekord

Cohen und Hagis zeigten 1980: Falls n zerlegbar und $\varphi(n)$ Teiler von $n-1$ ist, dann muss $n > 10^{20}$ und $\omega(n) \geq 14$ sein. Wall (1980) bewies unter der Voraussetzung $\mathrm{ggT}(30, n) = 1$, dass $\omega(n) \geq 26$.

Das bislang beste Resultat für den ursprünglich von Lieuwens betrachteten Fall $3 \mid n$ wurde 1988 von Hagis geliefert, der eine computergestützte Beweistechnik verwendete. Er konnte nachweisen, dass jedes der fraglichen n den Beschränkungen $\omega(n) \geq 298848$ und $n > 10^{1937043}$ unterliegt.

Pomerance zeigte 1977, dass für jede hinreichend große positive reelle Zahl x die Anzahl $L(x)$ derjenigen zerlegbaren $n \leq x$, für die $\varphi(n)$ Teiler von $n-1$ ist, der folgenden Ungleichung genügt:

$$L(x) \leq x^{1/2}(\log x)^{3/4}.$$

Darüber hinaus gilt $n < k^{2^k}$, falls $\omega(n) = k$. Shan (1985) gelang es, obige Ungleichung zu verschärfen, indem er den Exponenten $3/4$ durch $1/2$ ersetzen konnte.

Von der Eulerschen φ-Funktion angenommene Werte

Es ist nicht schwer nachzuweisen, dass nicht jede gerade Zahl $m > 1$ von Eulers Funktion als Wert angenommen wird. Beispielsweise zeigte Schinzel im Jahre 1956, dass für jedes $k \geq 1$ die Zahl 2×7^k kein Wert der Eulerschen φ-Funktion ist.

Mendelsohn bewies 1976 die Existenz unendlich vieler Primzahlen p mit der Eigenschaft, dass $2^k p$ für kein $k \geq 1$ im Wertebereich von φ liegt. Hinsichtlich interessanter Werte, die von Eulers Funktion angenommen werden, stellte Erdös 1946 die folgende Aufgabe: Man zeige, dass es für jedes $k \geq 1$ ein n gibt, für das $\varphi(n) = k!$. Eine Lösung wurde von Lambek 1948 angegeben; das gleiche Ergebnis erzielte später Gupta (1950).

Die nächsten Resultate zeigen, wie sprunghaft sich die φ-Funktion verhält. So bewies Somayajulu im Jahre 1950, dass

$$\limsup_{n\to\infty} \frac{\varphi(n+1)}{\varphi(n)} = \infty \quad \text{und} \quad \liminf_{n\to\infty} \frac{\varphi(n+1)}{\varphi(n)} = 0.$$

Dieses Ergebnis wurde von Schinzel und Sierpiński verbessert, siehe Schinzel (1954): die Menge aller Zahlen $\varphi(n+1)/\varphi(n)$ liegt dicht in der Menge aller positiven reellen Zahlen.

Schinzel & Sierpiński (1954) und Schinzel (1954) bewiesen auch das Folgende:

Für jedes m, $k \geq 1$ existieren n, $h \geq 1$ derart, dass

$$\frac{\varphi(n+i)}{\varphi(n+i-1)} > m \quad \text{und} \quad \frac{\varphi(h+i-1)}{\varphi(h+i)} > m$$

für $i = 1, 2, \ldots, k$. Es gilt zudem, dass die Menge aller Zahlen $\varphi(n)/n$ im Intervall $(0, 1)$ dicht liegt.

Die Valenz der Eulerschen φ-Funktion

Ich werde nun die „Valenz“ der Eulerschen Funktion untersuchen, mit anderen Worten, wie oft ein Wert $\varphi(n)$ angenommen wird. Um die Ergebnisse systematisch erläutern zu können, ist es von Vorteil, eine spezielle Schreibweise einzuführen. Für $m \geq 1$ bezeichne

$$V_\varphi(m) = \#\{n \geq 1 \mid \varphi(n) = m\}.$$

Welche sind die möglichen Werte von $V_\varphi(m)$? Ich hatte bereits gesagt, dass es unendlich viele gerade Zahlen m gibt, für die $V_\varphi(m)$ den Wert 0 annimmt. Zudem gilt $\varphi(n) = m$ für $m = 2 \times 3^{6k+1}$ $(k \geq 1)$ genau dann, wenn $n = 3^{6k+2}$ oder $n = 2 \times 3^{6k+2}$. Somit gibt es unendlich viele ganze Zahlen m, für die $V_\varphi(m) = 2$.

Es ist nicht schwer zu zeigen, dass $V_\varphi(m) \neq \infty$ für alle $m \geq 1$.

Schinzel fand 1956 einen einfacheren Beweis des folgenden Satzes von Pillai (1929):

$$\sup\{V_\varphi(m)\} = \infty.$$

Mit anderen Worten, für jedes $k \geq 1$ gibt es eine Zahl m_k derart, dass mindestens k Zahlen n mit $\varphi(n) = m_k$ existieren.

Obiges Resultat ist schwächer als die alte Vermutung von Sierpiński: Für jede ganze Zahl $k \geq 2$ gibt es $m > 1$, so dass $k = V_\varphi(m)$. Mit sehr ausgeklügelten Methoden gelang es Ford erst vor relativ kurzer Zeit im Jahre 1999, diese Vermutung zu beweisen.

Die Vermutung von Carmichael

Die das Studium der Valenz von φ beherrschende Vermutung geht auf Carmichael (1922) zurück: V_φ nimmt niemals den Wert 1 an. Mit anderen Worten: Für jedes $n \geq 1$ gibt es ein $n' \geq 1$, $n' \neq n$ derart, dass $\varphi(n') = \varphi(n)$.

Diese Vermutung wurde von Klee untersucht, der 1947 nachwies, dass sie für jedes n mit $\varphi(n) < 10^{400}$ richtig ist. Masai & Valette (1982)

zeigten mit Hilfe von Klees Methode, dass man auch $\varphi(n) < 10^{10000}$ setzen kann. Im Jahre 1994 gelang es Schlafly & Wagon, die untere Grenze für Carmichaels Vermutung durch intensive Berechnungen – wiederum im Wesentlichen unter Verwendung von Klees Verfahren – erheblich zu erweitern: Falls $V_\varphi(n) = 1$, so muss $n > 10^{10^7}$ sein. Mit Hilfe viel leistungsfähigerer Methoden verbesserte Ford 1998 die untere Grenze weiter und erreichte $n > 10^{10^{10}}$.

Zuvor war bereits ein ebenfalls von Wagon verfasster Artikel über die Vermutung von Carmichael in der Zeitschrift *The Mathematical Intelligencer* (1986) erschienen. Numerische Belege weisen auf die Korrektheit der Vermutung hin. Allerdings zeigte Pomerance 1974: Angenommen m ist eine natürliche Zahl mit der Eigenschaft, dass wenn p eine Primzahl ist und $p - 1$ den Wert $\varphi(m)$ teilt, m von p^2 geteilt wird. Dann gilt $V_\varphi(\varphi(m)) = 1$. Natürlich wäre Carmichaels Vermutung falsch, wenn es ein derartiges m gäbe. Allerdings ist man weit davon entfernt, die Existenz einer solchen Zahl m nachzuweisen, und vielleicht wird dies auch nie gelingen.

Die wichtigste Arbeit der letzten Zeit bezüglich der Vermutung von Carmichael stammt von K. Ford (1998). Für jedes $x > 0$ sei $E(x) = \#\{n \mid 1 \leq n < x$, es gibt $k > 1$ mit $\varphi(k) = n\}$ und $E_1(x) = \#\{n \mid 1 \leq n < x$, es gibt ein eindeutiges k mit $\varphi(k) = n\}$. Carmichaels Vermutung bedeutet, dass $E_1(x) = 0$ für jedes $x > 0$. Ford bewies: Falls die Vermutung falsch ist, gibt es ein $C > 0$ derart, dass für jedes genügend große x gilt: $E(x) \leq C\,E_1(x)$. Es folgt, dass Carmichaels Vermutung äquivalent zur Aussage ist:

$$\liminf_{x\to\infty} \frac{E_1(x)}{E(x)} = 0.$$

Ford zeigte auch, dass $E_1(10^{10^{10}}) = 0$.

Schließlich – quasi als Gegenstück zur Vermutung von Carmichael – ist es nicht abwegig zu erwarten, dass jedes $s > 1$ von V_φ als Wert angenommen wird; dies wurde von Sierpiński vermutet. Tatsächlich werde ich in Kapitel 6, Abschnitt II darauf hinweisen, dass diese Aussage als Korollar aus einer höchst interessanten, unbewiesenen Hypothese folgt.

Wie steht es mit der Valenz der Valenz-Funktion V_φ? Ich hatte schon gesagt, dass es unendlich viele m gibt, die als Wert von φ nicht auftauchen, für die also $V_\varphi(m) = 0$. Also nimmt V_φ den Wert 0 unendlich oft an.

Dies wurde 1958 von Erdös verallgemeinert: Wenn $s \geq 1$ als Wert von V_φ angenommen wird, so geschieht dies sogar unendlich oft. (Man

versuche einmal, diese Aussage direkt durch Eulers φ-Funktion auszudrücken, um den Grund für meine zusätzliche Notation zu verstehen.)

Das Wachstum der Eulerschen φ-Funktion

Bis jetzt habe ich das Wachstum der Funktion φ noch nicht betrachtet. Da $\varphi(p) = p-1$ für alle primen p, ist $\limsup \varphi(n) = \infty$. Auf die gleiche Weise erhält man aus $\varphi(p) = p - 1$, dass $\limsup \varphi(n)/n = 1$.

Ich möchte das Vorstellen weiterer Resultate über das Wachstum von φ auf Kapitel 4 verschieben, denn sie erfordern Methoden, die erst dort diskutiert werden.

G Folgen von Binomialzahlen

Die vorangegangenen Betrachtungen bezogen sich auf Kongruenzen modulo einer gegebenen ganzen Zahl $n > 1$, wobei a eine beliebige zu n teilerfremde, natürliche Zahl war.

Es gibt eine weitere, sehr aufschlussreiche Anschauungsweise. Diesmal sei $a > 1$ gegeben und man betrachte die Folgen der Zahlen $a^n - 1$ und $a^n + 1$ (für $n \geq 1$). Allgemeiner könnte man, falls $a > b \geq 1$ mit $\mathrm{ggT}(a, b) = 1$, die Folgen $a^n - b^n$ $(n \geq 1)$ und $a^n + b^n$ $(n \geq 1)$ untersuchen.

Eine sich sofort aufdrängende Frage (mit einer sofortigen Antwort) ist die nach der Bestimmung sämtlicher Primzahlen p, für die es ein $n \geq 1$ derart gibt, dass p Teiler von $a^n - b^n$ ist. Dies sind Primzahlen p, die ab nicht teilen, denn a und b sind teilerfremd. Umgekehrt gilt: Falls $p \nmid ab$, $bb' \equiv 1 \pmod{p}$ und n ist die Ordnung von ab' mod p, dann teilt p die Differenz $a^n - b^n$.

Für die Binomialzahlen der Form $a^n + b^n$ wird es komplizierter. Falls $p \neq 2$ und es $n \geq 1$ derart gibt, dass p Teiler von $a^n + b^n$ ist, dann $p \nmid ab(a - b)$. Die Umkehrung ist falsch; beispielsweise ist 7 für kein $n \geq 1$ Teiler von $2^n + 1$.

Primitive Primfaktoren

Falls $n \geq 1$ die kleinste ganze Zahl mit der Eigenschaft ist, dass p die Binomialzahl $a^n - b^n$ (beziehungsweise $a^n + b^n$) teilt, dann heißt p *primitiver Primfaktor* der entsprechenden Folge von Binomialzahlen. In diesem Fall folgt aus dem kleinen Satz von Fermat, dass $p - 1$ von n geteilt wird, was Legendre auffiel.

Also taucht jedes prime $p \nmid ab$ als primitiver Faktor irgendeiner Binomialzahl $a^n - b^n$ auf. Gilt auch die Umkehrung, d.h. hat jede Binomialzahl einen primitiven Faktor?

Zsigmondy bewies im Jahre 1892 den folgenden, sehr interessanten Satz, der viele Anwendungen fand:

Es sei $a > b \geq 1$ und $\mathrm{ggT}(a, b) = 1$. Dann hat jede Zahl $a^n - b^n$ einen primitiven Primfaktor – mit den einzigen Ausnahmen $a - b = 1$, $n = 1$; $2^6 - 1 = 63$; und $a^2 - b^2$, wobei a, b ungerade sind und $a + b$ eine Zweierpotenz ist.

Analog gilt für $a > b \geq 1$, dass jede Zahl $a^n + b^n$ mit der einzigen Ausnahme $2^3 + 1 = 9$ einen primitiven Primfaktor besitzt.

Den Spezialfall $b = 1$ hatte Bang 1886 bewiesen. Im Laufe der Zeit wurde dieser Satz – auch Bangs Spezialfall genannt – von einer ganzen Reihe von Mathematikern teilweise unbewusst erneut bewiesen: Birkhoff & Vandiver (1904), Carmichael (1913), Kanold (1950), Artin (1955), Lüneburg (1981), und wahrscheinlich weiteren.

Der Beweis ist bestimmt nicht offensichtlich. Jedoch ist es sehr einfach, solche Folgen aufzuschreiben und das fortlaufende Auftreten neuer primitiver Primfaktoren zu beobachten.

Es ist interessant, den *primitiven Teil* t_n^* von $a^n - b^n$ zu betrachten, und zwar schreibe man $a^n - b^n = t_n^* t_n'$ mit $\mathrm{ggT}(t_n^*, t_n') = 1$, wobei eine Primzahl p genau dann Teiler von t_n^* ist, wenn es sich bei p um einen primitiven Faktor von $a^n - b^n$ handelt.

In numerischen Experimenten mit Folgen $a^n - b^n$ kann man beobachten, dass t_n^* abgesehen von ein paar anfänglichen Termen zerlegbar ist. Und tatsächlich bewies Schinzel 1962 den folgenden Satz:

Es sei $k(m)$ der quadratfreie Kern von m (das heißt, m geteilt durch seinen größten quadratischen Faktor) und

$$e = \begin{cases} 1, & \text{falls } \ k(ab) \equiv 1 \pmod 4, \\ 2, & \text{falls } \ k(ab) \equiv 2 \text{ oder } 3 \pmod 4. \end{cases}$$

Falls $n/ek(ab)$ ganzzahlig und ungerade und $n > 1$ ist, dann hat $a^n - b^n$ bis auf wenige Ausnahmen (von denen die größtmögliche $n = 20$ ist) mindestens zwei verschiedene primitive Primfaktoren. Für $n > 1$ und $b = 1$ sind diese Ausnahmen:

$$\begin{aligned} &\text{falls } \ a = 2: \quad n = 4, 12, 20; \\ &\text{falls } \ a = 3: \quad n = 6; \\ &\text{falls } \ a = 4: \quad n = 3. \end{aligned}$$

Es gibt also unendlich viele n, für die der primitive Teil von $a^n - b^n$ zerlegbar ist.

Schinzel zeigte auch: Wenn $ab = c^h$ mit $h \geq 3$, oder $h = 2$ und $k(c)$ ungerade, dann gibt es unendlich viele n derart, dass der primitive Teil von $a^n - b^n$ mindestens drei Primfaktoren besitzt.

Für die Binomialzahlen $a^n + b^n$ folgt die Zerlegbarkeit des primitiven Teils unmittelbar, sobald $n > 10$ und $n/ek(ab)$ ungerade ist. Man beachte nur, dass jeder primitive Primfaktor von $a^{2n} - b^{2n}$ auch ein primitiver Primfaktor von $a^n + b^n$ ist.

Hier einige Fragen, die sehr schwer zu beantworten sind:

Gibt es unendlich viele n derart, dass der primitive Teil von $a^n - b^n$ prim ist?

Gibt es unendlich viele n mit der Eigenschaft, dass der primitive Teil von $a^n - b^n$ quadratfrei ist?

Und wie verhält es sich mit den scheinbar einfacheren Fragen:

Gibt es unendlich viele n, für die der primitive Teil t_n^* von $a^n - b^n$ einen Primfaktor p derart hat, dass p^2 kein Teiler von $a^n - b^n$ ist?

Gibt es unendlich viele n mit der Eigenschaft, dass t_n^* einen quadratfreien Kern $k(t_n^*) \neq 1$ hat?

Diese Fragen sind für den Spezialfall $b = 1$ letztendlich in sehr überraschender Weise mit Fermats letztem Satz verbunden!

Der größte Primfaktor

Auch die Abschätzung der Größe des größten Primfaktors von $a^n - b^n$ (für $a > b \geq 1$ und $\mathrm{ggT}(a, b) = 1$) stellt sich als interessantes Problem heraus. Es bezeichne im Folgenden $P[m]$ den größten Primfaktor von $m \geq 1$.

Unter Verwendung des Satzes von Zsigmondy ist es nicht schwer zu zeigen, dass $P[a^n - b^n] \geq n + 1$, wenn $n > 2$.

Schinzel zeigte 1962, dass $P[a^n - b^n] \geq 2n+1$ in den folgenden Fällen gilt (mit $n > 2$): $4 \nmid n$, mit der Ausnahme von $a = 2$, $b = 1$, $n = 6$; $k(ab) \mid n$ oder $k(ab) = 2$, mit den Ausnahmen $a = 2$, $b = 1$, $n = 4, 6$, oder 12.

Erdös vermutete 1965, dass $\lim_{n\to\infty} P[2^n - 1]/n = \infty$. Trotz sehr interessanter Arbeiten dazu konnte diese Vermutung bis heute nicht abschließend geklärt werden. Allerdings gibt es sehr gute Teilergebnisse, von denen ich nun berichten werde.

Stewart zeigte 1975 unter Verwendung von Bakers Ungleichungen für Linearformen von Logarithmen das Folgende: Es sei $0 < r < 1/\log 2$ und S_r die Menge derjenigen ganzen Zahlen n, die höchstens

$r \log\log n$ verschiedene Primfaktoren haben (die Menge S_r hat Dichte 1). Dann gilt

$$\lim_{\substack{n\to\infty \\ n\in S_r}} \frac{P[a^n - b^n]}{n} = \infty.$$

Wie schnell wächst dieser Ausdruck? Diese Frage beantwortete Stewart im Jahre 1977 mit Hilfe schärferer Ungleichungen vom Bakerschen Typ:

$$\frac{P[a^n - b^n]}{n} > C\,\frac{(\log n)^\lambda}{\log\log\log n}\ ,$$

für eine geeignete Konstante $C > 0$ und $\lambda = 1 - r\log 2$, $n \in S_r$.

Stewart zeigte zudem, dass für jede hinreichend große Primzahl p $P[a^p - b^p]/p > C\log p$ mit $C > 0$. Der Spezialfall der Mersenneschen Zahlen $2^p - 1$ wurde 1976 von Erdös und Shorey behandelt.

Es gibt auch eine enge Beziehung zwischen den Zahlen $a^n - 1$, den Werten der Kreisteilungspolynome und Primzahlen in speziellen arithmetischen Folgen. Aber ich kann nicht alles auf einmal erklären – haben Sie ein wenig Geduld, bis ich dieses Thema erneut in Kapitel 4, Abschnitt IV aufgreifen werde.

H Quadratische Reste

In der von Fermat, Euler, Legendre und Gauß entwickelten Theorie quadratischer diophantischer Gleichungen ist es von enormer Wichtigkeit zu entscheiden, wann eine ganze Zahl a modulo einer Primzahl $p > 2$ ein Quadrat ist.

Falls $p > 2$ kein Teiler von a ist und falls es eine ganze Zahl b derart gibt, dass $a \equiv b^2 \pmod p$, dann nennt man a einen *quadratischen Rest modulo p*, andernfalls ist a ein *quadratischer Nichtrest modulo p*.

Legendre führte die folgende praktische Notation ein:

$$\left(\frac{a}{p}\right) = (a \mid p) = \begin{cases} +1 & a \text{ ist quadratischer Rest modulo } p, \\ -1 & \text{sonst.} \end{cases}$$

Es hat sich darüber hinaus als nützlich erwiesen, $(a \mid p) = 0$ zu setzen, falls p Teiler von a ist.

Ich werde nun die wichtigsten Eigenschaften des Legendre-Symbols angeben. Literaturhinweise gibt es reichlich – praktisch jedes Buch über elementare Zahlentheorie.

Falls $a \equiv a' \pmod p$, dann

$$\left(\frac{a}{p}\right) = \left(\frac{a'}{p}\right).$$

Für alle ganzen Zahlen a, a' gilt:

$$\left(\frac{aa'}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{a'}{p}\right).$$

Es reicht also für die Berechnung des Legendre-Symbols, $(q\,|\,p)$ zu bestimmen, wobei $q = -1$, 2 oder eine ungerade, von p verschiedene Primzahl ist.

Euler bewies die folgende Kongruenz:

$$\left(\frac{a}{p}\right) \equiv a^{(p-1)/2} \pmod{p}.$$

Insbesondere:

$$\left(\frac{-1}{p}\right) = \begin{cases} +1 & \text{wenn } p \equiv 1 \pmod 4, \\ -1 & \text{wenn } p \equiv -1 \pmod 4, \end{cases}$$

und

$$\left(\frac{2}{p}\right) = \begin{cases} +1 & \text{wenn } p \equiv \pm 1 \pmod 8, \\ -1 & \text{wenn } p \equiv \pm 3 \pmod 8. \end{cases}$$

Die Berechnung des Legendre-Symbols $(q\,|\,p)$ für beliebiges, ungerades $q \neq p$ kann man mit einem einfachen und schnellen Algorithmus durchführen, der nur ganzzahlige Divisionen mit Rest erfordert und auf dem Gauß'schen *Reziprozitätsgesetz* basiert:

$$\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right)(-1)^{\frac{p-1}{2}\times\frac{q-1}{2}}.$$

Das Legendre-Symbol stellte sich als so entscheidend heraus, dass es Jacobi zur folgenden Verallgemeinerung veranlasste, die man heute als Jacobi-Symbol bezeichnet. Wieder gibt es Literaturhinweise in Hülle und Fülle, zum Beispiel Grosswalds Buch (1966, zweite Auflage 1984), oder (warum nicht?) mein eigenes Buch (1972, erweiterte Auflage 2001). Es sei a eine ganze Zahl ungleich 0 und b eine ungerade Zahl mit $\mathrm{ggT}(a,b) = 1$. Das Jacobi-Symbol $(a\,|\,b)$ ist in folgender Weise als Erweiterung des Legendre-Symbols definiert. Es sei $b = \prod_{p|b} p^{e_p} > 0$ (mit $e_p \geq 1$). Dann sei

$$\left(\frac{a}{b}\right) = \prod_{p|b}\left(\frac{a}{p}\right)^{e_p},$$

$$\left(\frac{a}{-b}\right) = \begin{cases} \left(\dfrac{a}{b}\right), & \text{falls } a > 0, \\ -\left(\dfrac{a}{b}\right), & \text{falls } a < 0. \end{cases}$$

$(a \mid b)$ nimmt die Werte $+1$ oder -1 an. Man beachte, dass

$$\left(\frac{a}{1}\right) = \left(\frac{a}{-1}\right) = +1 \quad \text{wenn} \quad a > 0.$$

Hier ist eine Auflistung einiger Eigenschaften des Jacobi-Symbols (die in der Definition getroffenen Annahmen vorausgesetzt):

$$\left(\frac{aa'}{b}\right) = \left(\frac{a}{b}\right)\left(\frac{a'}{b}\right),$$
$$\left(\frac{a}{bb'}\right) = \left(\frac{a}{b}\right)\left(\frac{a}{b'}\right)$$
$$\left(\frac{-1}{b}\right) = (-1)^{(b-1)/2} = \begin{cases} +1 & \text{falls } b \equiv 1 \pmod 4, \\ -1 & \text{falls } b \equiv -1 \pmod 4, \end{cases}$$
$$\left(\frac{2}{b}\right) = (-1)^{(b^2-1)/8} = \begin{cases} +1 & \text{falls } b \equiv \pm 1 \pmod 8, \\ -1 & \text{falls } b \equiv \pm 3 \pmod 8. \end{cases}$$

Den Schlüssel zur Berechnung des Jacobi-Symbols stellt das Reziprozitätsgesetz dar, das leicht aus dem Gauß'schen Reziprozitätsgesetz für das Legendre-Symbol abzuleiten ist:

Für zwei teilerfremde, ungerade ganze Zahlen a, b gilt

$$\left(\frac{a}{b}\right) = \varepsilon\left(\frac{b}{a}\right)(-1)^{\frac{a-1}{2}\times\frac{b-1}{2}},$$

wobei

$$\varepsilon = \begin{cases} +1 & \text{falls } a > 0 \text{ oder } b > 0 \\ -1 & \text{falls } a < 0 \text{ und } b < 0. \end{cases}$$

Und schließlich, falls $b \geq 3$ und a ein Quadrat modulo b ist: $(a \mid b) = +1$.

III Klassische Primzahltests auf der Grundlage von Kongruenzen

Nach der Besprechung der Sätze von Fermat, Wilson, und Euler bin ich nun bereit. Für mich sind die klassischen, auf Kongruenzen basierenden Primzahltests diejenigen, die Lehmer angab. Sie erweitern oder verwenden frühere Tests von Lucas, Pocklington und Proth. Für klassische Tests, die auf rekurrenten Folgen beruhen, habe ich einen anderen Abschnitt reserviert.

Der Satz von Wilson, der ja eine Charakterisierung der Primzahlen darstellt, scheint zunächst als Primzahltest vielversprechend zu sein. Da die Berechnung der Fakultät jedoch viel zu aufwändig ist, scheidet er als praktischer Test aus.

Der kleine Satz von Fermat lautet für primes p und eine natürliche Zahl a, die kein Vielfaches von p ist, dass $a^{p-1} \equiv 1 \pmod{p}$ erfüllt ist. Allerdings möchte ich an dieser Stelle sofort anmerken, dass die Umkehrung dieses Satzes nicht gilt – es gibt zerlegbare Zahlen N und $a \geq 2$ mit $a^{N-1} \equiv 1 \pmod{N}$. Ich werde Abschnitt VIII dem Studium dieser für Primalitätsfragen außerordentlich wichtigen Zahlen widmen.

Dennoch entdeckte Lucas im Jahre 1876 eine richtige Umkehrung von Fermats kleinem Satz. Diese besagt:

Test 1. Es sei $N > 1$. Angenommen, es existiert eine ganze Zahl $a > 1$ mit den Eigenschaften

(i) $a^{N-1} \equiv 1 \pmod{N}$,

(ii) $a^m \not\equiv 1 \pmod{N}$ für $m = 1, 2, \ldots, N-2$.

Dann ist N prim.

Nachteil dieses zunächst perfekt aussehenden Tests: Er benötigt $N-2$ aufeinander folgende Multiplikationen mit a und das Finden der Reste modulo N – dies sind zu viele Operationen.

Beweis. Es reicht zu zeigen, dass jede Zahl m, $1 \leq m < N$, teilerfremd zu N ist, also $\varphi(N) = N-1$ gilt. Dazu wiederum genügt es nachzuweisen, dass es ein a mit $1 \leq a < N$ und $\mathrm{ggT}(a, N) = 1$ mit einer Ordnung von a mod N gleich $N-1$ gibt. Dies aber ist genau die Aussage der Annahme. □

Lucas gab 1891 den folgenden Test an:

Test 2. Es sei $N > 1$. Angenommen, es existiert eine ganze Zahl $a > 1$ mit den Eigenschaften

(i) $a^{N-1} \equiv 1 \pmod{N}$,

(ii) $a^m \not\equiv 1 \pmod{N}$ für jedes $m < N$, das Teiler von $N-1$ ist.

Dann ist N prim.

Nachteil dieses Tests: Er erfordert die Kenntnis aller Faktoren von $N-1$, so dass er nur für die Fälle einfach anwendbar ist, in denen $N-1$ leicht faktorisierbar ist, so wie bei $N = 2^n + 1$ oder $N = 3 \times 2^n + 1$.

Der Beweis von Test 2 ist natürlich der gleiche wie der von Test 1.

Im Jahre 1967 verbesserten Brillhart & Selfridge Lucas' Test und gestalteten ihn flexibler; siehe auch den 1975 erschienenen Artikel von Brillhart, Lehmer & Selfridge:

Test 3. Es sei $N > 1$. Angenommen, für jeden Primfaktor q von $N-1$ existiert eine ganze Zahl $a = a(q) > 1$ derart, dass

(i) $a^{N-1} \equiv 1 \pmod{N}$,

(ii) $a^{(N-1)/q} \not\equiv 1 \pmod{N}$.

Dann ist N prim.

Nachteil dieses Tests: Man benötigt wieder die gesamte Primfaktorenzerlegung von $N-1$, jedoch müssen diesmal weniger Kongruenzen erfüllt sein.

Wenn man aufmerksam liest, stellt man fest, dass es zur Verifikation von $a^{N-1} \equiv 1 \pmod{N}$ während der Rechnung notwendig ist, den Rest von a^n modulo N (für jedes $n \leq N-1$) zu bestimmen. Also hätte man ja eigentlich auch den ersten Lucas-Test verwenden können. Es gibt jedoch einen sehr schnellen Algorithmus zur Berechnung von a^n, also auch $a^n \bmod N$, ohne dabei sämtliche vorherigen Potenzen berücksichtigen zu müssen. Dieser funktioniert wie folgt:

Man schreibe den Exponenten n zur Basis 2:

$$n = n_0 2^k + n_1 2^{k-1} + \cdots + n_{k-1} 2 + n_k,$$

wobei jedes n_i gleich 0 oder 1 und $n_0 = 1$ ist.

Definiere nun die Zahlen $r_0, r_1, r_2, \ldots$ sukzessive wie folgt, wobei $r_0 = a$. Für $j \geq 0$:

$$r_{j+1} = \begin{cases} r_j^2 & \text{falls} \quad n_{j+1} = 0, \\ a r_j^2 & \text{falls} \quad n_{j+1} = 1. \end{cases}$$

Dann ist $a^n = r_k$.

So muss man höchstens $2k$ Operationen durchführen, jeweils entweder ein Quadrieren oder eine Multiplikation mit a. Falls es um die Berechnung von $a^n \bmod N$ geht, ist es sogar einfacher; in jedem Schritt muss man r_j durch den Rest modulo N ersetzen. Nun ist k gleich

$$\left[\frac{\log n}{\log 2}\right].$$

Und daher sind für $n = N - 1$ nur

$$2\left[\frac{\log N}{\log 2}\right]$$

Operationen notwendig, um $a^{N-1} \bmod N$ zu bestimmen. Insbesondere ist es unnötig, alle Potenzen $a^n \bmod N$ auszurechnen.

Man könnte diese Prozedur ja einmal zur Berechnung von $2^{1092} \bmod 1093^2$ heranziehen, das Ergebnis sollte $2^{1092} \equiv 1 \pmod{1093^2}$ sein, wenn man sich nicht verrechnet hat. Dies hat eigentlich gar nichts mit Primalität zu tun, wird allerdings viel später in Kapitel 5 eine Rolle spielen.

Ich möchte noch einmal zum Test von Brillhart und Selfridge zurückkehren und den Beweis angeben.

Beweis von Test 3. Es reicht zu zeigen, dass $\varphi(N) = N - 1$. Und da $\varphi(N) \leq N-1$ ist, genügt der Nachweis, dass $N-1$ die Zahl $\varphi(N)$ teilt. Falls dies nicht der Fall sein sollte, gibt es eine Primzahl q und $r \geq 1$ derart, dass q^r Teiler von $N - 1$ ist, jedoch ist $\varphi(N)$ kein Vielfaches von q^r. Es sei $a = a(q)$ und e die Ordnung von $a \bmod N$. Also ist e ein Teiler von $N - 1$, aber kein Teiler von $(N - 1)/q$, somit teilt q^r die Zahl e. Aus $a^{\varphi(N)} \equiv 1 \pmod{N}$ folgt, dass e Teiler von $\varphi(N)$ ist, so dass $q^r \mid \varphi(N)$, was einen Widerspruch darstellt und den Beweis abschließt. □

Im Abschnitt über Fermat-Zahlen werde ich Pepins Primzahltest für Fermat-Zahlen als Konsequenz von Test 3 entwickeln.

Um die Primzahltests effizienter zu gestalten, wäre es wünschenswert, wenn man auf die Bestimmung aller Primfaktoren von $N-1$ verzichten könnte. Es gibt Tests, die nur eine teilweise Faktorisierung von $N - 1$ erfordern. Das grundlegende Resultat wurde 1914 von Pocklington bewiesen und ist tatsächlich sehr einfach:

Es sei $N - 1 = q^n R$, wobei $n \geq 1$ und q eine Primzahl ist, die R nicht teilt. Angenommen, es gäbe eine ganze Zahl $a > 1$ mit den Eigenschaften:

(i) $a^{N-1} \equiv 1 \pmod{N}$,

(ii) $\mathrm{ggT}(a^{(N-1)/q} - 1, N) = 1$.

Dann hat jeder Primfaktor von N die Form $mq^n + 1$ mit $m \geq 1$.

Beweis. Es sei p ein Primfaktor von N und e die Ordnung von a mod p, so dass also e Teiler von $p-1$ ist. Nach Bedingung (ii) kann e den Quotienten $(N-1)/q$ nicht teilen, da p Teiler von N ist. Daher teilt q nicht $(N-1)/e$, also ist q^n Teiler von e und erst recht von $p-1$. □

Obige Aussage sieht weniger nach einem Primzahltest als nach einem Resultat über Faktoren aus. Wenn sich allerdings nachweisen lässt, dass jeder Primfaktor $p = mq^n + 1$ größer ist als $\sqrt{N}$, dann ist N eine Primzahl. Für relativ große q^n ist dieser Nachweis nicht zu zeitaufwändig.

Pocklington gab noch die folgende Verbesserung an:

Es sei $N-1 = FR$, wobei $\mathrm{ggT}(F,R) = 1$, und die Faktorisierung von F sei bekannt. Angenommen, für jeden Primfaktor q von F gibt es eine ganze Zahl $a = a(q) > 1$ derart, dass gilt:

(i) $a^{N-1} \equiv 1 \pmod{N}$,

(ii) $\mathrm{ggT}(a^{(N-1)/q} - 1, N) = 1$.

Dann hat jeder Primfaktor von N die Form $mF+1$, mit $m \geq 1$.

Dieselben Bemerkungen wie oben treffen auch hier zu. Falls also $F > \sqrt{N}$, dann ist N prim.

Dieses Resultat ist sehr nützlich, um die Primalität von Zahlen spezieller Form nachzuweisen. Das alte Kriterium von Proth (1878) lässt sich leicht ableiten:

Test 4. Es sei $N = 2^n h + 1$ mit ungeradem h und $2^n > h$. Angenommen, es existiert eine Zahl $a > 1$ derart, dass $a^{(N-1)/2} \equiv -1 \pmod{N}$. Dann ist N eine Primzahl.

Beweis. $N - 1 = 2^n h$, mit ungeradem h und $a^{N-1} \equiv 1 \pmod{N}$. Da N ungerade ist, folgt $\mathrm{ggT}(a^{(N-1)/2} - 1, N) = 1$. Nach obigem Resultat hat jeder Primfaktor p von N die Form $p = 2^n m + 1 > 2^n$. Aber $N = 2^n h + 1 < 2^{2n}$ und daher $\sqrt{N} < 2^n < p$, somit ist N prim. □

Im folgenden Test (unter Verwendung derselben Schreibweise) ist es notwendig vorauszusetzen, dass der nicht-faktorisierte Teil R von $N-1$ keinen Primfaktor kleiner als eine gegebene Grenze B hat. Genauer:

Test 5. Es sei $N - 1 = FR$, wobei $\mathrm{ggT}(F,R) = 1$, und die Faktorisierung von F sei bekannt. Darüber hinaus sei B derart, dass $FB > \sqrt{N}$ und R keinen Primfaktor kleiner als B hat.

Angenommen

(i) Für jeden Primfaktor q von F existiert ein Zahl $a = a(q) > 1$ mit $a^{N-1} \equiv 1 \pmod{N}$ und $\mathrm{ggT}(a^{(N-1)/q} - 1, N) = 1$.

(ii) Es gibt eine Zahl $b > 1$ derart, dass $b^{N-1} \equiv 1 \pmod{N}$ und $\mathrm{ggT}(b^F - 1, N) = 1$.

Dann ist N eine Primzahl.

Beweis. Es sei p ein Primfaktor von N und e die Ordnung von b modulo N, so dass e sowohl $p-1$ als auch $N-1 = FR$ teilt. Da e kein Teiler von F ist, folgt $\mathrm{ggT}(e, R) \neq 1$. Daher muss es eine Primzahl q mit $q \mid e$ und $q \mid R$ geben, somit gilt $q \mid p-1$. Allerdings teilt F nach obigem Test von Pocklington $p-1$ und da $\mathrm{ggT}(F, R) = 1$, muss qF Teiler von $p-1$ sein. Also $p - 1 \geq qF \geq BF > \sqrt{N}$. Dies impliziert, dass $p = N$, also ist N prim. □

Der Artikel von Brillhart, Lehmer & Selfridge (1975) enthält weitere Varianten dieser Tests, die sich bestens zum Nachweis der Primalität von Zahlen der Form $2^r + 1$, $2^{2r} \pm 2^r + 1$ und $2^{2r-1} \pm 2^r + 1$ eignen.

Ich habe nun schon genug gesagt, daher nur noch eine kurze Bemerkung: Obige Tests erfordern die Kenntnis von Primfaktoren von $N-1$. Später werden weitere Tests vorgestellt, die dann unter Verwendung linear rekurrenter Folgen die Kenntnis von Primfaktoren von $N+1$ voraussetzen.

IV Lucas-Folgen

Es seien P und Q zwei ganze Zahlen ungleich 0.

Man betrachte das Polynom $X^2 - PX + Q$ mit Diskriminante $D = P^2 - 4Q$ und den Wurzeln

$$\alpha = \frac{P + \sqrt{D}}{2}, \qquad \beta = \frac{P - \sqrt{D}}{2}.$$

Dann ist

$$\begin{cases} \alpha + \beta = P, \\ \alpha\beta = Q, \\ \alpha - \beta = \sqrt{D}. \end{cases}$$

Ich werde $D \neq 0$ annehmen. Man beachte, dass $D \equiv 0 \pmod 4$ oder $D \equiv 1 \pmod 4$. Definiere nun die Folgen von Zahlen

$$U_n(P,Q) = \frac{\alpha^n - \beta^n}{\alpha - \beta} \quad \text{und} \quad V_n(P,Q) = \alpha^n + \beta^n, \quad \text{für } n \geq 0.$$

Insbesondere gilt $U_0(P,Q) = 0$ und $U_1(P,Q) = 1$, während $V_0(P,Q) = 2$ und $V_1(P,Q) = P$.

Die Folgen

$$U(P,Q) = (U_n(P,Q))_{n\geq 0} \quad \text{und} \quad V(P,Q) = (V_n(P,Q))_{n\geq 0}$$

heißen *Lucas-Folgen zum Paar* (P,Q) *gehörend*. Spezialfälle wurden unter Anderem von Fibonacci, Fermat und Pell untersucht. Es waren bereits viele Einzelergebnisse über diese Folgen bekannt, bevor Lucas im Jahre 1878 in einem bahnbrechenden Artikel eine allgemeine Theorie dazu entwickelte; er erschien in Band I des *American Journal of Mathematics*. Die Arbeit ist ein umfangreicher und gehaltvoller Abriss, der Lucas-Folgen mit vielen interessanten Themenbereichen verknüpft, so zum Beispiel mit den trigonometrischen Funktionen, Kettenbrüchen, der Anzahl der Divisionen im Algorithmus zur Bestimmung des größten gemeinsamen Teilers und auch mit Primzahltests. Und genau aus diesem letzten Grund werde ich hier die Lucas-Folgen behandeln. Falls Sie die anderen Zusammenhänge neugierig gemacht haben, die ich erwähnte, dann sehen Sie im Literaturverzeichnis am Ende des Buches nach und/oder ziehen Sie den Artikel selbst zu Rate.

Ich sollte allerdings davor warnen, dass die verwendeten Methoden trotz der Tragweite des Artikels teilweise indirekt und mühsam sind. Vielleicht ist es daher ratsam, stattdessen die lange Abhandlung von Carmichael aus dem Jahre 1913 zu lesen, wo er Fehler korrigiert und Resultate verallgemeinert hat.

Wie man leicht nachrechnen kann, gilt zunächst für jedes $n \geq 2$,

$$\begin{cases} U_n(P,Q) = P\,U_{n-1}(P,Q) - Q\,U_{n-2}(P,Q), \\ V_n(P,Q) = P\,V_{n-1}(P,Q) - Q\,V_{n-2}(P,Q). \end{cases}$$

Insofern verdienen es diese Folgen, als *linear rekurrente Folgen der Ordnung* 2 bezeichnet zu werden (jeder Term hängt linear von den zwei vorherigen ab). Umgekehrt zeigte Binet im Jahre 1843 unter den Voraussetzungen P, Q wie oben, $D = P^2 - 4Q \neq 0$, $W_0 = 0$ (bzw. 2), $W_1 = 1$ (bzw. P) und $W_n = PW_{n-1} - QW_{n-2}$ für $n \geq 2$, dass

$$W_n = \frac{\alpha^n - \beta^n}{\alpha - \beta} \quad (\text{bzw. } W_n = \alpha^n + \beta^n) \quad \text{für } n \geq 0;$$

wobei α, β die Wurzeln des Polynoms $X^2 - PX + Q$ sind. Dies ist trivialerweise so, denn die Zahlenfolgen

$$(W_n)_{n\geq 0} \quad \text{und} \quad \left(\frac{\alpha^n - \beta^n}{\alpha - \beta}\right)_{n\geq 0} \quad (\text{bzw. } (\alpha^n + \beta^n)_{n\geq 0}),$$

haben die ersten beiden Terme gemeinsam und leiten sich aus derselben linear rekurrenten Definition zweiter Ordnung ab.

Bevor ich fortfahre, hier zunächst die wesentlichsten Spezialfälle, die schon vor der Entwicklung der allgemeinen Theorie behandelt worden waren.

Die den Werten $P = 1$, $Q = -1$, $U_0 = U_0(1,-1) = 0$ und $U_1 = U_1(1,-1) = 1$ zugehörige Folge wurde zuerst von Fibonacci betrachtet. Sie beginnt so:

$$0,\ 1,\ 1,\ 2,\ 3,\ 5,\ 8,\ 13,\ 21,\ 34,\ 55,\ 89,\ 144,\ 233,$$
$$377,\ 610,\ 987,\ 1597,\ 2584,\ 4181,\ 6765,\ \ldots$$

Diese Zahlen tauchten das erste Mal in einem Problem in Fibonaccis *Liber Abaci* auf, veröffentlicht im Jahre 1202. In diesem Buch wurden auch erstmalig arabische Zahlen in Europa vorgestellt. Das Problem, das sich heute in vielen Zahlentheoriebüchern wiederfindet, betrifft spezielle Vermehrungsmuster bei Kaninchen.

Ich muss ehrlich sagen, dass ich auf solcherlei Erklärungen keinen allzu großen Wert lege. Was Kaninchen anbelangt, ziehe ich einen guten Teller „lapin chasseur“[2] mit frischen Nudeln vor.

Die Begleitfolge der Fibonacci-Zahlen, immer noch aus $P = 1$, $Q = -1$ gebildet, ist die Folge der Lucas-Zahlen: $V_0 = V_0(1,-1) = 2$, $V_1 = V_1(1,-1) = 1$, und sie beginnt folgendermaßen:

$$2,\ 1,\ 3,\ 4,\ 7,\ 11,\ 18,\ 29,\ 47,\ 76,\ 123,\ 199,\ 322,$$
$$521,\ 843,\ 1364,\ 2207,\ 3571,\ 5778,\ 9349,\ 15127,\ \ldots$$

Wenn $P = 3$, $Q = 2$, dann erhält man die Folgen

$$U_n(3,2) = 2^n - 1 \quad \text{und} \quad V_n(3,2) = 2^n + 1, \quad \text{für } n \geq 0.$$

Diese Folgen bereiteten Fermat viele schlaflose Nächte (zu Details siehe Abschnitte VI und VII). Die zum Paar $P = 2$, $Q = -1$ assoziierten Folgen nennt man die Pell-Folgen; die ersten Folgenglieder sind:

$$U_n(2,-1): \quad 0,\ 1,\ 2,\ 5,\ 12,\ 29,\ 70,\ 169,\ 408,\ 985,$$
$$2378,\ 5741,\ 13860,\ \ldots$$
$$V_n(2,-1): \quad 2,\ 2,\ 6,\ 14,\ 34,\ 82,\ 198,\ 478,\ 1154,$$
$$2786,\ 6726,\ 16238,\ 39202,\ \ldots$$

[2] Kaninchen auf Jäger-Art

Lucas bemerkte eine große Ähnlichkeit zwischen den Folgen $U_n(P,Q)$ (bzw. $V_n(P,Q)$) und $(a^n-b^n)/(a-b)$ (bzw. a^n+b^n), wobei a, b gegeben sind, $a>b\geq 1$, $\mathrm{ggT}(a,b)=1$ und $n\geq 0$. Dies ist kein Wunder, denn die eine Folge ist ein Spezialfall der anderen. Man betrachte nur das Paar $(a+b,ab)$. Dann sind $D=(a-b)^2\neq 0$, $\alpha=a$, $\beta=b$ und

$$U_n(a+b,ab)=\frac{a^n-b^n}{a-b}\,,\quad V_n(a+b,ab)=a^n+b^n.$$

Es ist natürlich wünschenswert, die wichtigsten Ergebnisse zu den Zahlenfolgen $(a^n-b^n)/(a-b)$, a^n+b^n (was Teilbarkeit und Primalität angeht) auf die weitaus größere Klasse der Lucas-Folgen zu übertragen.

Ich werde daher die Verallgemeinerungen von Fermats kleinem Satz, dem Satz von Euler, usw., auf Lucas-Folgen vorstellen. Dies wird keine wesentlichen Schwierigkeiten bereiten, die Entwicklung erfordert allerdings eine erstaunliche Anzahl von Schritten, wenngleich auch sämtlich auf elementarem Niveau. Im Folgenden werde ich nach und nach die wichtigsten Fakten zusammenstellen, die zum Beweis der Hauptresultate notwendig sind. Wenn Sie möchten, können Sie die Details ja einmal ausarbeiten. Aber ich werde auch explizit den Beginn etlicher Lucas-Folgen angeben, so dass Sie vielleicht schon damit zufrieden sind, die Aussagen numerisch zu kontrollieren (siehe die Tabellen am Ende dieses Abschnitts).

Zunächst die algebraischen Fakten, danach die Teilbarkeitseigenschaften. Um die Formeln zu vereinfachen, werde ich nur $U_n=U_n(P,Q)$ und $V_n=V_n(P,Q)$ schreiben.

Es gelten die folgenden algebraischen Eigenschaften:

(IV.1) $U_n=PU_{n-1}-QU_{n-2}\ (n\geq 2),\quad U_0=0,\quad U_1=1,$
$V_n=PV_{n-1}-QV_{n-2}\ (n\geq 2),\quad V_0=2,\quad V_1=P.$

(IV.2) $U_{2n}=U_nV_n,$
$V_{2n}=V_n^2-2Q^n.$

(IV.3) $U_{m+n}=U_mV_n-Q^nU_{m-n},$
$V_{m+n}=V_mV_n-Q^nV_{m-n}\ (\text{für } m\geq n).$

(IV.4) $U_{m+n}=U_mU_{n+1}-QU_{m-1}U_n,$
$2V_{m+n}=V_mV_n+DU_mU_n.$

(IV.5) $DU_n=2V_{n+1}-PV_n,$
$V_n=2U_{n+1}-PU_n.$

(IV.6) $U_n^2=U_{n-1}U_{n+1}+Q^{n-1},$
$V_n^2=DU_n^2+4Q^n.$

(IV.7) $U_m V_n - U_n V_m = 2Q^n U_{m-n}$ (für $m \geq n$),
$U_m V_n + U_n V_m = 2U_{m+n}$.

(IV.8) $2^{n-1} U_n = \binom{n}{1} P^{n-1} + \binom{n}{3} P^{n-3} D + \binom{n}{5} P^{n-5} D^2 + \cdots,$
$2^{n-1} V_n = P^n + \binom{n}{2} P^{n-2} D + \binom{n}{4} P^{n-4} D^2 + \cdots.$

(IV.9) Wenn m ungerade ist und $k \geq 1$, dann

$$D^{(m-1)/2}\, U_k^m = U_{km} - \binom{m}{1} Q^k U_{k(m-2)} + \binom{m}{2} Q^{2k} U_{k(m-4)} - \cdots$$
$$\pm \binom{m}{(m-1)/2} Q^{\frac{m-1}{2}k}\, U_k,$$
$$V_k^m = V_{km} + \binom{m}{1} Q^k V_{k(m-2)} + \binom{m}{2} Q^{2k} V_{k(m-4)} + \cdots$$
$$+ \binom{m}{(m-1)/2} Q^{\frac{m-1}{2}k}\, V_k.$$

Wenn m gerade ist und $k \geq 1$, dann

$$D^{m/2} U_k^m = \Big[V_{km} - \binom{m}{1} Q^k V_{k(m-2)} + \binom{m}{2} Q^{2k} V_{k(m-4)} - \cdots$$
$$+ (-1)^{m/2} \binom{m}{m/2} Q^{(m/2)k} V_0 \Big] - (-1)^{m/2} \binom{m}{m/2} Q^{(m/2)\,k},$$
$$V_k^m = \Big[V_{km} + \tbinom{m}{1} Q^k V_{k(m-2)} + \tbinom{m}{2} Q^{2k} V_{k(m-4)} + \cdots$$
$$+ \binom{m}{m/2} Q^{(m/2)k} V_0 \Big] - \binom{m}{m/2} Q^{(m/2)k}.$$

(IV.10) $U_m = V_{m-1} + QV_{m-3} + Q^2 V_{m-5} + \cdots +$ (letzter Summand), wobei

$$\text{letzter Summand} = \begin{cases} Q^{(m-2)/2}\, P & \text{falls } m \text{ gerade,} \\ Q^{(m-1)/2} & \text{falls } m \text{ ungerade.} \end{cases}$$

$$P^m = V_m + \binom{m}{1} QV_{m-2} + \binom{m}{2} Q^2 V_{m-4} + \cdots + \text{(letzter Summand)},$$

wobei

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

Für die nächste Eigenschaft benötigt man zunächst die folgende Identität von Lagrange, die auf das Jahr 1741 zurückgeht:

$$\begin{aligned} X^n + Y^n = (X+Y)^n &- \frac{n}{1} XY(X+Y)^{n-2} \\ &+ \frac{n}{2}\binom{n-3}{1} X^2Y^2(X+Y)^{n-4} \\ &- \frac{n}{3}\binom{n-4}{2} X^3Y^3(X+Y)^{n-6} + \cdots \\ &+ (-1)^r \frac{n}{r}\binom{n-r-1}{r-1} X^rY^r(X+Y)^{n-2r} \pm \cdots, \end{aligned}$$

wobei die Summe bis $2r \le n$ läuft. Man beachte, dass alle Koeffizienten ganzzahlig sind.

(IV.11) Wenn $m \ge 1$ und q ungerade ist, dann

$$\begin{aligned} U_{mq} = D^{(q-1)/2} U_m^q &+ \frac{q}{1} Q^m D^{(q-3)/2} U_m^{q-2} \\ &+ \frac{q}{2}\binom{q-3}{1} Q^{2m} D^{(q-5)/2} U_m^{q-4} + \cdots \\ &+ \frac{q}{r}\binom{q-r-1}{r-1} Q^{mr} D^{(q-2r-1)/2} U_m^{q-2r} + \cdots \\ &+ \text{ letzter Summand,} \end{aligned}$$

mit dem letzten Summanden

$$\frac{q}{(q-1)/2}\binom{(q-1)/2}{(q-3)/2} Q^{\frac{q-1}{2}m}\, U_m = q\, Q^{\frac{q-1}{2}m}\, U_m.$$

Nun werde ich die Teilbarkeitseigenschaften vorstellen, und zwar in der Reihenfolge, in der man sie nach und nach beweisen kann.

(IV.12)
$$U_n \equiv V_{n-1} \pmod{Q},$$
$$V_n \equiv P^n \pmod{Q}.$$

Hinweis: Verwende (IV.10) oder Beweis durch Induktion.

(IV.13) Es sei p eine ungerade Primzahl. Dann ist

$$U_{kp} \equiv D^{\frac{p-1}{2}} U_k \pmod{p}$$

und für $e \geq 1$,

$$U_{p^e} \equiv D^{\frac{p-1}{2}e} \pmod{p}.$$

Insbesondere:

$$U_p \equiv \left(\frac{D}{p}\right) \pmod{p}.$$

Hinweis: Verwende (IV.9).

(IV.14) $$V_p \equiv P \pmod{p}.$$

Hinweis: Verwende (IV.10).

(IV.15) Wenn $n, k \geq 1$, dann ist U_n Teiler von U_{kn}.

Hinweis: Verwende (IV.3).

(IV.16) Wenn $n, k \geq 1$ mit ungeradem k, dann ist V_n Teiler von V_{kn}.

Hinweis: Verwende (IV.9).

Bezeichnung. Wenn es für $n \geq 2$ eine Zahl $r \geq 1$ derart gibt, dass n Teiler von U_r ist, dann bezeichne $\rho(n) = \rho(n, U)$ das kleinste solche r.

(IV.17) Angenommen, es existiert $\rho(n)$ mit $\mathrm{ggT}(n, 2Q) = 1$. Dann gilt $n \mid U_k$ genau dann, wenn $\rho(n) \mid k$.

Hinweis: Verwende (IV.15) und (IV.7).

Es wird sich zeigen, dass $\rho(n)$ für die meisten n mit $\mathrm{ggT}(n, 2Q) = 1$ existiert, jedoch nicht für alle.

(IV.18) Wenn Q und P gerade sind, dann sind U_n für $n \geq 2$ und V_n für $n \geq 1$ ebenfalls gerade.

Wenn Q gerade und P ungerade ist, dann sind U_n und V_n für $n \geq 1$ ungerade.

Wenn Q ungerade und P gerade ist, dann ist $U_n \equiv n \pmod{2}$ und V_n ungerade.

Wenn Q und P ungerade sind, dann sind U_n und V_n gerade, wenn n durch 3 teilbar ist, während sonst U_n und V_n ungerade sind.

Insbesondere ist V_n gerade, wenn U_n gerade ist.

Hinweis: Verwende (IV.12), (IV.5), (IV.2), (IV.6) und (IV.1).

Es folgt nun das erste Hauptresultat. Es ist ein Begleitergebnis von (IV.18) und verallgemeinert den kleinen Satz von Fermat:

(IV.19) Es sei p eine ungerade Primzahl.
Wenn $p \mid P$ und $p \mid Q$, dann $p \mid U_k$ für jedes $k > 1$.
Wenn $p \mid P$ und $p \nmid Q$, dann $p \mid U_k$ genau dann, wenn k gerade ist.
Wenn $p \nmid P$ und $p \mid Q$, dann $p \nmid U_k$ für jedes $k \geq 1$.
Wenn $p \nmid P$, $p \nmid Q$ und $p \mid D$, dann $p \mid U_k$ genau dann, wenn $p \mid k$.
Wenn $p \nmid PQD$, dann $p \mid U_{\psi(p)}$, wobei $\psi(p) = p - (D \mid p)$ und $(D \mid p)$ das Legendre-Symbol ist.

Beweis. Wenn $p \mid P$ und $p \mid Q$, dann folgt nach (IV.1) $p \mid U_k$ für jedes $k > 1$.

Wenn $p \mid P = U_2$, so folgt aus (IV.15), dass $p \mid U_{2k}$ für jedes $k \geq 1$. Da $p \nmid Q$ und $U_{2k+1} = PU_{2k} - QU_{2k-1}$, erhält man durch Induktion, dass $p \nmid U_{2k+1}$.

Wenn $p \nmid P$ und $p \mid Q$, so folgt wiederum durch Induktion und (IV.1), dass $p \nmid U_k$ für jedes $k \geq 1$.

Wenn $p \nmid PQ$ und $p \mid D$, dann ergibt (IV.8), dass $2^{p-1}U_p \equiv 0 \pmod{p}$, so dass $p \mid U_p$. Andererseits, falls $p \nmid n$, dann folgt mit (IV.8), dass $2^{n-1}U_n \equiv nP^{n-1} \not\equiv 0 \pmod{p}$ und daher $p \nmid U_n$.

Schließlich der interessanteste Fall: Angenommen, $p \nmid PQD$.

Wenn $(D \mid p) = -1$, erhält man mit (IV.8)

$$\begin{aligned} 2^p U_{p+1} &= \binom{p+1}{1} P^p + \binom{p+1}{3} P^{p-2} D + \cdots \\ &\quad + \binom{p+1}{p} P D^{(p-1)/2} \equiv P + P D^{(p-1)/2} \equiv 0 \pmod{p}, \end{aligned}$$

also $p \mid U_{p+1}$.

Falls $(D \mid p) = 1$, so existiert ein C mit $P^2 - 4Q = D \equiv C^2 \pmod{p}$; daher $P^2 \not\equiv C^2 \pmod{p}$ und $p \nmid C$. Nach (IV.8) sieht man unter Beachtung von

$$\binom{p-1}{1} \equiv -1 \pmod{p}, \quad \binom{p-1}{3} \equiv -1 \pmod{p}, \quad \ldots$$

dass

$$\begin{aligned}
2^{p-2}U_{p-1} &= \binom{p-1}{1}P^{p-2} + \binom{p-1}{3}P^{p-4}D \\
&\quad + \binom{p-1}{5}P^{p-6}D^2 + \cdots + \binom{p-1}{p-2}PD^{(p-3)/2} \\
&\equiv -[P^{p-2} + P^{p-4}D + P^{p-6}D^2 + \cdots + PD^{(p-3)/2}] \\
&\equiv -P\left(\frac{P^{p-1} - D^{(p-1)/2}}{P^2 - D}\right) \\
&\equiv -P\,\frac{P^{p-1} - C^{p-1}}{P^2 - C^2} \equiv 0 \pmod{p}.
\end{aligned}$$

Also $p \mid U_{p-1}$. □

Unter Verwendung der oben eingeführten Bezeichnung $\rho(p)$ lassen sich einige der Aussagen von (IV.19) wie folgt umformulieren:

Wenn p eine ungerade Primzahl ist und $p \nmid Q$, dann gilt:
Wenn $p \mid P$, dann $\rho(p) = 2$.
Wenn $p \nmid P$, $p \mid D$, dann $\rho(p) = p$.
Wenn $p \nmid PD$, dann ist $\rho(p)$ Teiler von $\psi(p)$.

Man schließe im letzten Fall nicht voreilig, dass $\rho(p) = \psi(p)$. Ich werde auf diesen Punkt noch zurückkommen, nachdem ich die wesentlichen Eigenschaften von Lucas-Folgen aufgelistet habe.

Die spezielle Lucas-Folge $U_n(a+1, a)$ hat die Diskriminante $D = (a-1)^2$; und wenn $p \nmid a(a^2-1)$, dann

$$\left(\frac{D}{p}\right) = 1 \qquad \text{und} \qquad p \mid U_{p-1} = \frac{a^{p-1} - 1}{a - 1},$$

also $p \mid a^{p-1} - 1$ (was trivial ist, wenn $p \mid a^2 - 1$) – und das ist Fermats kleiner Satz.

(IV.20) Es sei $e \geq 1$ und p^e die maximale Potenz von p, die U_m teilt. Wenn $p \nmid k$ und $f \geq 1$, dann ist p^{e+f} Teiler von U_{mkp^f}.

Darüber hinaus ist p^{e+f} die maximale Potenz von p, die U_{mkp^f} teilt, wenn $p \mid Q$ und $p^e \neq 2$, während $U_{mk}/2$ ungerade ist, wenn $p^e = 2$.

Hinweis: Verwende (IV.19), (IV.18), (IV.11) und (IV.6).

Nun zur Verallgemeinerung des Satzes von Euler:

Für Wurzeln α und β von $X^2 - PX + Q$ definiere das Symbol

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

und für $p \neq 2$:

$$\left(\frac{\alpha,\beta}{p}\right) = \left(\frac{D}{p}\right)$$

(also ist es 0, wenn $p \mid D$). Setze

$$\psi_{\alpha,\beta}(p) = p - \left(\frac{\alpha,\beta}{p}\right)$$

für jedes prime p, sowie

$$\psi_{\alpha,\beta}(p^e) = p^{e-1}\psi_{\alpha,\beta}(p) \quad \text{für } e \geq 1.$$

Für $n = \prod_{p|n} p^e$ sei die Carmichael-Funktion wie folgt definiert:

$$\lambda_{\alpha,\beta}(n) = \mathrm{kgV}\{\psi_{\alpha,\beta}(p^e)\}$$

(wobei kgV das kleinste gemeinsame Vielfache bezeichne). Definiere weiter die verallgemeinerte Euler-Funktion durch

$$\psi_{\alpha,\beta}(n) = \prod_{p|n} \psi_{\alpha,\beta}(p^e).$$

Also wird $\psi_{\alpha,\beta}(n)$ von $\lambda_{\alpha,\beta}(n)$ geteilt.

Es lässt sich leicht nachprüfen, dass $\psi_{a,1}(p) = p - 1 = \varphi(p)$ für jedes prime p gilt, das a nicht teilt; wenn also $\mathrm{ggT}(a,n) = 1$, dann $\psi_{a,1}(n) = \varphi(n)$ sowie $\lambda_{a,1}(n) = \lambda(n)$, wobei $\lambda(n)$ die ebenfalls von Carmichael definierte Funktion aus Abschnitt II ist.

Hier nun die Erweiterung des Satzes von Euler:

(IV.21) Wenn $\mathrm{ggT}(n,Q) = 1$, dann ist n Teiler von $U_{\lambda_{\alpha,\beta}(n)}$ und somit auch von $U_{\psi_{\alpha,\beta}(n)}$.

Hinweis: Verwende (IV.19) und (IV.20).

Man muss dazu sagen, dass die Teilbarkeitseigenschaften der Begleitfolge $(V_n)_{n\geq 1}$ nicht so einfach zu beschreiben sind. Man beachte zum Beispiel

(IV.22) Wenn $p \nmid 2QD$, dann $V_{p-(D|p)} \equiv 2Q^{\frac{1}{2}[1-(D|p)]} \pmod{p}$.

Hinweis: Verwende (IV.5), (IV.13), (IV.19) und (IV.14).

Dies kann nun dazu verwendet werden, um Aussagen über die Teilbarkeit von $U_{\psi(p)/2}$ und $V_{\psi(p)/2}$ herzuleiten.

(IV.23) Angenommen, $p \nmid 2QD$. Dann gilt

$$\begin{aligned} p \mid U_{\psi(p)/2} \quad &\text{genau dann, wenn} \quad \big(Q \mid p\big) = 1, \\ p \mid V_{\psi(p)/2} \quad &\text{genau dann, wenn} \quad \big(Q \mid p\big) = -1. \end{aligned}$$

Hinweis: Für die erste Behauptung, verwende (IV.2), (IV.6), (IV.22) und die Kongruenz $(Q \mid p) \equiv Q^{(p-1)/2} \pmod{p}$. Für die zweite Behauptung, verwende (IV.2), (IV.19), die erste Aussage, sowie (IV.6).

Für die nächsten Resultate setze ich $\mathrm{ggT}(P, Q) = 1$ voraus.

(IV.24) $\mathrm{ggT}(U_n, Q) = 1$ und $\mathrm{ggT}(V_n, Q) = 1$, für jedes $n \geq 1$.

Hinweis: Verwende (IV.12).

(IV.25) $\mathrm{ggT}(U_n, V_n) = 1$ oder 2.

Hinweis: Verwende (IV.16) und (IV.24).

(IV.26) Wenn $d = \mathrm{ggT}(m, n)$, dann $U_d = \mathrm{ggT}(U_m, U_n)$.

Hinweis: Verwende (IV.15), (IV.7), (IV.24), (IV.18) und (IV.6). Dieser Beweis ist nicht ganz so einfach und benötigt die Verwendung der Lucas-Folge $\big(U_n(V_d, Q^d)\big)_{n\geq 0}$.

(IV.27) Wenn $\mathrm{ggT}(m, n) = 1$, dann $\mathrm{ggT}(U_m, U_n) = 1$.

Kein Hinweis hierzu.

(IV.28) Wenn $d = \mathrm{ggT}(m, n)$ und m/d, n/d ungerade sind, dann $V_d = \mathrm{ggT}(V_m, V_n)$.

Hinweis: Verwende den gleichen Beweis wie für (IV.26).

Und hier ein Resultat ähnlich (IV.17), allerdings unter der Voraussetzung $\mathrm{ggT}(P, Q) = 1$:

(IV.29) Angenommen, $\rho(n)$ existiert. Dann gilt $n \mid U_k$ genau dann, wenn $\rho(n) \mid k$.

Hinweis: Verwende (IV.15), (IV.24) und (IV.3).

Ich unterbreche hier kurz, um einmal ausführlich aufzuschreiben, was im Falle der Fibonacci-Zahlen U_n sowie der Lucas-Zahlen V_n passiert; sei also nun $P = 1$, $Q = -1$, $D = 5$.

Eigenschaft (IV.18) wird zum *Gesetz des Erscheinens* von p. Und obwohl ich diese Zeilen am Halloween-Abend schreibe, würde es mir doch wehtun, es „Gesetz der Erscheinung“ zu nennen.[3]

Gesetz der Erscheinung (hoppla, des Erscheinens) von p:

$$\begin{aligned} p \mid U_{p-1} &\text{ wenn } (5 \mid p) = 1, \quad \text{das heißt, } p \equiv \pm 1 \pmod{10}, \\ p \mid U_{p+1} &\text{ wenn } (5 \mid p) = -1, \text{ das heißt, } p \equiv \pm 3 \pmod{10}. \end{aligned}$$

Eigenschaft (IV.19) ist das *Gesetz der Wiederholung*.

Für die Lucas-Zahlen gelten die folgenden Eigenschaften:

$$\begin{aligned} p \mid V_{p-1} - 2 &\text{ wenn } (5 \mid p) = 1, \quad \text{das heißt, } p \equiv \pm 1 \pmod{10}, \\ p \mid V_{p+1} + 2 &\text{ wenn } (5 \mid p) = -1, \text{ das heißt, } p \equiv \pm 3 \pmod{10}. \end{aligned}$$

Jarden zeigte 1958, dass im Falle der Fibonacci-Folge die Funktion

$$\frac{\psi(p)}{\rho(p)} = \frac{p - (5 \mid p)}{\rho(p)}$$

unbeschränkt ist (wenn die Primzahl p gegen Unendlich geht).

Dieses Resultat wurde von Kiss & Phong 1978 verallgemeinert: Es existiert $C > 0$ (das nur von P und Q abhängt), so dass $\psi(p)/\rho(p)$ unbeschränkt ist, jedoch gilt immer noch $\psi(p)/\rho(p) < C[p/(\log p)]$ (für p gegen Unendlich).

Ich werde nun das Verhalten der Lucas-Folgen modulo einer Primzahl p angeben.

Der Fall $p = 2$ verhält sich wie in (IV.18) beschrieben. Beispielsweise sind für ungerades P und Q die Folgen $(U_n \bmod 2)_{n\geq 0}$, $(V_n \bmod 2)_{n\geq 0}$ gleich

$$0,\ 1,\ 1,\ 0,\ 1,\ 1,\ 0,\ 1,\ 1,\ 0,\ \ldots .$$

Interessanter wird es, wenn p eine ungerade Primzahl ist.

(IV.30) Wenn $p \nmid 2QD$ und $(D \mid p) = 1$, dann

$$\begin{aligned} U_{n+p-1} &\equiv U_n \pmod{p}, \\ V_{n+p-1} &\equiv V_n \pmod{p}. \end{aligned}$$

[3] Anm. d. Übers.: Der Autor spielt im Original an dieser Stelle auf die direkte Übersetzung des französischen *loi d'apparition* ins Englische an, was zu „apparition law“ führt; dies bedeutet „Gesetz der (Geister-)Erscheinung“.

Die Folgen $(U_n \bmod p)_{n\geq 0}$, $(V_n \bmod p)_{n\geq 0}$ haben somit die Periodenlänge $p-1$.

Beweis. Nach (IV.4), $U_{n+p-1} = U_nU_p - QU_{n-1}U_{p-1}$; nach (IV.19) ist $\rho(p)$ Teiler von $p-(D \mid p) = p-1$; nach (IV.15) folgt $p \mid U_{p-1}$; was auch stimmt, wenn $p \mid P$, $p \nmid Q$, da $p-1$ dann gerade ist, und somit $p \mid U_{p-1}$ nach (IV.19). Mit (IV.13),

$$U_p \equiv (D \mid p) \equiv 1 \pmod p.$$

Also $U_{n+p-1} \equiv U_n \pmod p$.

Nun folgt aus (IV.5), $V_{n+p-1} = 2U_{n+p} - PU_n \equiv 2U_{n+1} - PU_n \equiv V_n \pmod p$. □

Das Begleitresultat sieht folgendermaßen aus:

(IV.31) Es sei $p \nmid 2QD$ und e die Ordnung von $Q \bmod p$. Wenn $(D \mid p) = -1$, dann

$$U_{n+e(p+1)} \equiv U_n \pmod p,$$
$$V_{n+e(p+1)} \equiv V_n \pmod p.$$

Somit haben die Folgen $(U_n \bmod p)_{n\geq 0}$, $(V_n \bmod p)_{n\geq 0}$ eine Periodenlänge von $e(p+1)$.

Beweis. Wenn $p \nmid P$, folgt aus (IV.19), (IV.15),

$$p \mid U_{p-(D\mid p)} = U_{p+1}$$

was auch stimmt, wenn $p \mid P$.

Nach (IV.22), $V_{p+1} \equiv 2Q \pmod p$. Ich werde nun durch Induktion über $r \geq 1$ zeigen, dass $V_{r(p+1)} \equiv 2Q^r \pmod p$.

Die Aussage ist richtig für $r \geq 1$. Dann folgt nach (IV.4)

$$2V_{(r+1)(p+1)} = V_{r(p+1)}V_{p+1} + DU_{r(p+1)}U_{p+1} \equiv 4Q^{r+1} \pmod p,$$

so dass $V_{(r+1)(p+1)} \equiv 2Q^{r+1} \pmod p$. Insbesondere $V_{e(p+1)} \equiv 2Q^e \equiv 2 \pmod p$. Nach (IV.7),

$$U_{n+e(p+1)}V_{e(p+1)} - U_{e(p+1)}V_{n+e(p+1)} = 2Q^{e(p+1)}\,U_n\,,$$

und somit $2U_{n+e(p+1)} \equiv 2U_n \pmod p$, womit die erste Kongruenz hergestellt ist.

Die zweite Kongruenz folgt aus (IV.5). □

Es ist sinnvoll, einige der vorangegangenen Ergebnisse einmal anhand der folgenden Mengen zusammenzufassen:

$$\mathcal{P}(U) = \{p \text{ prim} \mid \text{es gibt } n \text{ derart, dass } U_n \neq 0 \text{ und } p \mid U_n\},$$
$$\mathcal{P}(V) = \{p \text{ prim} \mid \text{es gibt } n \text{ derart, dass } V_n \neq 0 \text{ und } p \mid V_n\}.$$

Dies sind die Mengen der Primteiler der Folgen $U = (U_n)_{n\geq 1}$ bzw. $V = (V_n)_{n\geq 1}$.

Die Parameter (P, Q) seien zwei von 0 verschiedene, teilerfremde Zahlen, die Diskriminante ist $D = P^2 - 4Q \neq 0$.

Ein erster Fall ergibt sich, wenn es ein $n > 1$ gibt, für das $U_n = 0$, oder äquivalent, wenn $\alpha^n = \beta^n$, das heißt α/β ist eine Einheitswurzel. Wenn n der kleinste derartige Index ist, dann ist $U_r \neq 0$ für $r = 1, \ldots, n-1$ und $U_{nk+r} = \alpha^{nk} U_r$ (für jedes $k \geq 1$), so dass $\mathcal{P}(U)$ aus allen Primteilern von $U_2 \cdots U_{n-1}$ besteht. Analog setzt sich $\mathcal{P}(V)$ aus den Primzahlen zusammen, die $V_1 V_2 \cdots V_{n-1} V_n$ teilen.

Der interessantere Fall ist der, wenn α/β keine Einheitswurzel ist, also $U_n \neq 0$, $V_n \neq 0$ für jedes $n \geq 1$. Dann ist $\mathcal{P}(U) = \{p \text{ prim} \mid p \text{ teilt } Q \text{ nicht}\}$.

Dies folgt aus (IV.18) und (IV.19). Insbesondere ist $\mathcal{P}(U)$ für die Folge der Fibonacci-Zahlen gleich der Menge aller Primzahlen.

Für die begleitende Lucas-Folge $V = (V_n)_{n\geq 1}$ lässt sich keine ähnlich präzise Aussage treffen. Aus $U_{2n} = U_n V_n$ $(n \geq 1)$ folgt, dass $\mathcal{P}(V)$ eine Teilmenge von $\mathcal{P}(U)$ ist. Nach (IV.18) gilt $2 \in \mathcal{P}(V)$ genau dann, wenn Q ungerade ist. Es folgt zudem aus (IV.24) und (IV.6), dass wenn $p \neq 2$ und $p \mid DQ$, dann $p \notin \mathcal{P}(V)$, während wenn $p \nmid 2DQ$ und $(Q \mid p) = -1$, dann $p \in \mathcal{P}(V)$ [siehe (IV.23)]; andererseits ist $p \notin \mathcal{P}(V)$, wenn $p \nmid 2DQ$, $(Q \mid p) = 1$ und $(D \mid p) = -(-1 \mid p)$. Dies reicht ohne eine weitere Analyse nicht aus, um zu entscheiden, ob eine Primzahl p mit $p \nmid 2DQ$, $(Q \mid p) = 1$ und $(D \mid p) = (-1 \mid p)$ zu $\mathcal{P}(V)$ gehört oder nicht. Zumindest ist sicher, dass $\mathcal{P}(V)$ auch eine unendliche Menge ist.

Für die Folge der Lucas-Zahlen mit $P = 1$, $Q = -1$, $D = 5$, lassen sich die vorangegangenen Aussagen folgendermaßen angeben:

Wenn $p = 3, 7, 11, 19 \pmod{20}$, dann $p \in \mathcal{P}(V)$;

Wenn $p \equiv 13, 17 \pmod{20}$, dann $p \notin \mathcal{P}(V)$.

Für $p \equiv 1, 9 \pmod{20}$ kann man ohne eine sorgfältige Untersuchung, wie zum Beispiel der von Ward von 1961, zu keiner Entscheidung gelangen. Bereits im Jahre 1958 hatte Jarden die Existenz unendlich vieler Primzahlen p mit $p \equiv 1 \pmod{20}$ nachgewiesen, für die $p \notin \mathcal{P}(V)$ gilt. Andererseits zeigte er, dass in $\mathcal{P}(V)$ unendlich viele p mit $p \equiv 1 \pmod{40}$ enthalten sind.

An späterer Stelle (in Kapitel 5, Abschnitt VIII) werde ich auf die Mengen $\mathcal{P}(U)$, $\mathcal{P}(V)$ zurückkommen und der Frage nach ihrer Dichte innerhalb der Menge aller Primzahlen nachgehen.

In Analogie zum Satz von Bang und Zsigmondy betrachtete Carmichael auch die primitiven Primfaktoren der Lucas-Folgen mit Parametern (P, Q): p ist ein primitiver Primfaktor von U_k (bzw. V_k), wenn $p \mid U_k$ (bzw. $p \mid V_k$), aber p keine der vorangegangenen Zahlen in der betrachteten Folge teilt.

Der Beweis des Satzes von Zsigmondy ist nicht besonders einfach, und hier ist es noch etwas heikler.

Carmichael zeigte, dass U_n bei positiver Diskriminante für jedes $n \neq 1, 2, 6$ einen primitiven Primfaktor hat, außer wenn $n = 12$ und $P = \pm 1$, $Q = -1$.

Die Situation ist günstiger, wenn D ein Quadrat ist. Dann hat U_n für jedes n einen primitiven Primfaktor, außer wenn $n = 6$, $P = \pm 3$, $Q = 2$.

Ist Ihnen aufgefallen, dass diese zweite Aussage Zsigmondys Satz beinhaltet? Darüber hinaus ist der Ausnahmefall für $P = 1$ und $Q = -1$ genau die Fibonacci-Zahl $U_{12} = 144$.

Für die Begleitfolge V_n gilt, dass diese im Falle $D > 0$ für alle $n \neq 1, 3$ einen primitiven Primfaktor besitzt, außer wenn $n = 6$, $P = \pm 1$, $Q = -1$ (die Lucas-Zahl $V_6 = 18$). Falls D ein Quadrat ist, gibt es nur noch die einzige Ausnahme $n = 3$, $P = \pm 3$, $Q = 2$, was auch im Satz von Zsigmondy enthalten ist.

Für $D < 0$ gilt die obige Aussage jedoch nicht mehr. Wie schon Carmichael bemerkte, hat U_n mit $P = 1$, $Q = 2$ für $n = 1$, 2, 3, 5, 8, 12, 13, 18 keine primitiven Primfaktoren.

Schinzel zeigte 1962:

Es sei $(U_n)_{n \geq 0}$ die Lucas-Folge mit teilerfremden Parametern (P, Q) derart, dass die Diskriminante $D < 0$. Angenommen, dass α/β keine Einheitswurzel ist. Dann gibt es ein explizit berechenbares n_0 (in Abhängigkeit von P, Q), so dass U_n für $n > n_0$ einen primitiven Primfaktor hat.

Später bewies Schinzel im Jahre 1974 das gleiche Resultat mit absoluter Konstante n_0 – unabhängig von der Lucas-Folge. Dies war ein beachtliches Ergebnis.

Mit Hilfe der Methoden von Baker konnte Stewart 1977 zeigen, dass U_n einen primitiven Primfaktor besitzt, wenn $n > e^{452} 2^{67}$. Darüber hinaus bewies Stewart auch, dass es für gegebenes n ($n \neq 6$, $n > 4$)

nur endlich viele Lucas-Folgen gibt, die explizit bestimmbar sind (sagt Stewart, ohne es zu tun), so dass U_n keinen primitiven Primfaktor hat.

Es ist interessant, einmal den primitiven Teil U_n^* von U_n zu betrachten:

$$U_n = U_n^* U_n' \quad \text{mit} \quad \mathrm{ggT}(U_n^*, U_n') = 1$$

wobei p genau dann U_n^* teilt, wenn p primitiver Primfaktor von U_n ist.

Im Jahre 1963 gab Schinzel Bedingungen für die Existenz von zwei (oder geradem $e > 2$) verschiedenen primitiven Primfaktoren an. Es folgt, dass wenn $D > 0$ oder $D < 0$ und α/β keine Einheitswurzel ist, es unendlich viele n derart gibt, dass der primitive Teil U_n^* zerlegbar ist.

Kann man irgendeine Aussage darüber treffen, ob U_n^* quadratfrei ist? Dies ist eine sehr schwierige Frage. Man denke nur an den speziellen Fall, wenn $P = 3$, $Q = 2$, woraus sich die Folge $2^n - 1$ ergibt (siehe die Kommentare in Abschnitt II).

V Primzahltests auf der Grundlage von Lucas-Folgen

Was Lucas begann, setzte Lehmer fort, andere verfeinerten es. Die Primzahltests für eine Zahl N, die nun vorgestellt werden, erfordern die Kenntnis der Primfaktoren von $N + 1$. In diesem Sinne sind sie als eine Ergänzung zu den Tests aus Abschnitt III zu verstehen, in denen man Primfaktoren von $N - 1$ benötigte. Als Werkzeug werden die Lucas-Folgen dienen. Nach (IV.18) gilt: Wenn N eine ungerade Primzahl ist und $U = (U_n)_{n\geq 0}$ eine Lucas-Folge mit Diskriminante D, wobei $N \nmid DPQ$, dann wird $U_{N-(D|N)}$ von N geteilt. Wenn also das Jacobi-Symbol $(D \mid N) = -1$ ist, so teilt N die Zahl U_{N+1}.

Allerdings möchte ich (wie schon in Abschnitt III) sofort anmerken, dass die direkte Umkehrung nicht gilt. Denn es gibt zerlegbare Zahlen N und Lucas-Folgen $(U_n)_{n\geq 0}$ mit Diskriminante D, so dass N Teiler von $U_{N-(D|N)}$ ist. Solche Zahlen werden in Abschnitt X untersucht.

Es wird sich als nützlich herausstellen, für Zahlen $D > 1$ die folgendermaßen definierte Funktion ψ_D einzuführen:

Für $N = \prod_{i=1}^{s} p_i^{e_i}$, sei

$$\psi_D(N) = \frac{1}{2^{s-1}} \prod_{i=1}^{s} p_i^{e_i - 1} \left(p_i - \left(\frac{D}{p_i} \right) \right).$$

Tabelle 2. Fibonacci- und Lucas-Zahlen

$P = 1,\ Q = -1$

Fibonacci-Zahlen	Lucas-Zahlen
$U(0) = 0 \quad U(1) = 1$	$V(0) = 2 \quad V(1) = 1$
$U(2) = 1$	$V(2) = 3$
$U(3) = 2$	$V(3) = 4$
$U(4) = 3$	$V(4) = 7$
$U(5) = 5$	$V(5) = 11$
$U(6) = 8$	$V(6) = 18$
$U(7) = 13$	$V(7) = 29$
$U(8) = 21$	$V(8) = 47$
$U(9) = 34$	$V(9) = 76$
$U(10) = 55$	$V(10) = 123$
$U(11) = 89$	$V(11) = 199$
$U(12) = 144$	$V(12) = 322$
$U(13) = 233$	$V(13) = 521$
$U(14) = 377$	$V(14) = 843$
$U(15) = 610$	$V(15) = 1364$
$U(16) = 987$	$V(16) = 2207$
$U(17) = 1597$	$V(17) = 3571$
$U(18) = 2584$	$V(18) = 5778$
$U(19) = 4181$	$V(19) = 9349$
$U(20) = 6765$	$V(20) = 15127$
$U(21) = 10946$	$V(21) = 24476$
$U(22) = 17711$	$V(22) = 39603$
$U(23) = 28657$	$V(23) = 64079$
$U(24) = 46368$	$V(24) = 103682$
$U(25) = 75025$	$V(25) = 167761$
$U(26) = 121393$	$V(26) = 271443$
$U(27) = 196418$	$V(27) = 439204$
$U(28) = 317811$	$V(28) = 710647$
$U(29) = 514229$	$V(29) = 1149851$
$U(30) = 832040$	$V(30) = 1860498$
$U(31) = 1346269$	$V(31) = 3010349$
$U(32) = 2178309$	$V(32) = 4870847$
$U(33) = 3524578$	$V(33) = 7881196$
$U(34) = 5702887$	$V(34) = 12752043$
$U(35) = 9227465$	$V(35) = 20633239$
$U(36) = 14930352$	$V(36) = 33385282$
$U(37) = 24157817$	$V(37) = 54018521$
$U(38) = 39088169$	$V(38) = 87403803$
$U(39) = 63245986$	$V(39) = 141422324$
$U(40) = 102334155$	$V(40) = 228826127$

Tabelle 3. Zahlen $2^n - 1$ und $2^n + 1$

$P = 3,\ Q = 2$

Zahlen $2^n - 1$	Zahlen $2^n + 1$
$U(0) = 0 \quad U(1) = 1$	$V(0) = 2 \quad V(1) = 3$
$U(2) = 3$	$V(2) = 5$
$U(3) = 7$	$V(3) = 9$
$U(4) = 15$	$V(4) = 17$
$U(5) = 31$	$V(5) = 33$
$U(6) = 63$	$V(6) = 65$
$U(7) = 127$	$V(7) = 129$
$U(8) = 255$	$V(8) = 257$
$U(9) = 511$	$V(9) = 513$
$U(10) = 1023$	$V(10) = 1025$
$U(11) = 2047$	$V(11) = 2049$
$U(12) = 4095$	$V(12) = 4097$
$U(13) = 8191$	$V(13) = 8193$
$U(14) = 16383$	$V(14) = 16385$
$U(15) = 32767$	$V(15) = 32769$
$U(16) = 65535$	$V(16) = 65537$
$U(17) = 131071$	$V(17) = 131073$
$U(18) = 262143$	$V(18) = 262145$
$U(19) = 524287$	$V(19) = 524289$
$U(20) = 1048575$	$V(20) = 1048577$
$U(21) = 2097151$	$V(21) = 2097153$
$U(22) = 4194303$	$V(22) = 4194305$
$U(23) = 8388607$	$V(23) = 8388609$
$U(24) = 16777215$	$V(24) = 16777217$
$U(25) = 33554431$	$V(25) = 33554433$
$U(26) = 67108863$	$V(26) = 67108865$
$U(27) = 134217727$	$V(27) = 134217729$
$U(28) = 268435455$	$V(28) = 268435457$
$U(29) = 536870911$	$V(29) = 536870913$
$U(30) = 1073741823$	$V(30) = 1073741825$
$U(31) = 2147483647$	$V(31) = 2147483649$
$U(32) = 4294967295$	$V(32) = 4294967297$
$U(33) = 8589934591$	$V(33) = 8589934593$
$U(34) = 17179869183$	$V(34) = 17179869185$
$U(35) = 34359738367$	$V(35) = 34359738369$
$U(36) = 68719476735$	$V(36) = 68719476737$
$U(37) = 137438953471$	$V(37) = 137438953473$
$U(38) = 274877906943$	$V(38) = 274877906945$
$U(39) = 549755813887$	$V(39) = 549755813889$
$U(40) = 1099511627775$	$V(40) = 1099511627777$

Tabelle 4. Pell-Zahlen

$P = 2,\ Q = -1$

Pell-Zahlen	Begleitende Pell-Zahlen
$U(0) = 0 \quad U(1) = 1$	$V(0) = 2 \quad V(1) = 2$
$U(2) = 2$	$V(2) = 6$
$U(3) = 5$	$V(3) = 14$
$U(4) = 12$	$V(4) = 34$
$U(5) = 29$	$V(5) = 82$
$U(6) = 70$	$V(6) = 198$
$U(7) = 169$	$V(7) = 478$
$U(8) = 408$	$V(8) = 1154$
$U(9) = 985$	$V(9) = 2786$
$U(10) = 2378$	$V(10) = 6726$
$U(11) = 5741$	$V(11) = 16238$
$U(12) = 13860$	$V(12) = 39202$
$U(13) = 33461$	$V(13) = 94642$
$U(14) = 80782$	$V(14) = 228486$
$U(15) = 195025$	$V(15) = 551614$
$U(16) = 470832$	$V(16) = 1331714$
$U(17) = 1136689$	$V(17) = 3215042$
$U(18) = 2744210$	$V(18) = 7761798$
$U(19) = 6625109$	$V(19) = 18738638$
$U(20) = 15994428$	$V(20) = 45239074$
$U(21) = 38613965$	$V(21) = 109216786$
$U(22) = 93222358$	$V(22) = 263672646$
$U(23) = 225058681$	$V(23) = 636562078$
$U(24) = 543339720$	$V(24) = 1536796802$
$U(25) = 1311738121$	$V(25) = 3710155682$
$U(26) = 3166815962$	$V(26) = 8957108166$
$U(27) = 7645370045$	$V(27) = 21624372014$
$U(28) = 1845756052$	$V(28) = 52205852194$
$U(29) = 44560482149$	$V(29) = 126036076402$
$U(30) = 107578520350$	$V(30) = 304278004998$
$U(31) = 259717522849$	$V(31) = 734592086398$
$U(32) = 627013566048$	$V(32) = 1773462177794$
$U(33) = 1513744654945$	$V(33) = 4281516441986$
$U(34) = 3654502875938$	$V(34) = 10336495061766$
$U(35) = 8822750406821$	$V(35) = 24954506565518$
$U(36) = 21300003689580$	$V(36) = 60245508192802$
$U(37) = 51422757785981$	$V(37) = 145445522951122$
$U(38) = 124145519261542$	$V(38) = 351136554095046$
$U(39) = 299713796309065$	$V(39) = 847718631141214$
$U(40) = 723573111879672$	$V(40) = 2046573816377474$

Tabelle 5. Zahlen $U(4,3)$ und $V(4,3)$

$P = 4,\ Q = 3$

Zahlen	Begleitzahlen
$U(0) = 0 \quad U(1) = 1$	$V(0) = 2 \quad V(1) = 4$
$U(2) = 4$	$V(2) = 10$
$U(3) = 13$	$V(3) = 28$
$U(4) = 40$	$V(4) = 82$
$U(5) = 121$	$V(5) = 244$
$U(6) = 364$	$V(6) = 730$
$U(7) = 1093$	$V(7) = 2188$
$U(8) = 3280$	$V(8) = 6562$
$U(9) = 9841$	$V(9) = 19684$
$U(10) = 29524$	$V(10) = 59050$
$U(11) = 88573$	$V(11) = 177148$
$U(12) = 265720$	$V(12) = 531442$
$U(13) = 797161$	$V(13) = 1594324$
$U(14) = 2391484$	$V(14) = 4782970$
$U(15) = 7174453$	$V(15) = 14348908$
$U(16) = 21523360$	$V(16) = 43046722$
$U(17) = 64570081$	$V(17) = 129140164$
$U(18) = 193710244$	$V(18) = 387420490$
$U(19) = 581130733$	$V(19) = 1162261468$
$U(20) = 1743392200$	$V(20) = 3486784402$
$U(21) = 5230176601$	$V(21) = 10460353204$
$U(22) = 15690529804$	$V(22) = 31381059610$
$U(23) = 47071589413$	$V(23) = 94143178828$
$U(24) = 141214768240$	$V(24) = 282429536482$
$U(25) = 423644304721$	$V(25) = 847288609444$
$U(26) = 1270932914164$	$V(26) = 2541865828330$
$U(27) = 3812798742493$	$V(27) = 7625597484988$
$U(28) = 11438396227480$	$V(28) = 22876792454962$
$U(29) = 34315188682441$	$V(29) = 68630377364884$
$U(30) = 102945566047324$	$V(30) = 205891132094650$
$U(31) = 308836698141973$	$V(31) = 617673396283948$
$U(32) = 926510094425920$	$V(32) = 1853020188851842$
$U(33) = 2779530283277761$	$V(33) = 5559060566555524$
$U(34) = 8338590849833284$	$V(34) = 16677181699666570$
$U(35) = 25015772549499853$	$V(35) = 50031545098999708$
$U(36) = 75047317648499560$	$V(36) = 150094635296999122$
$U(37) = 225141952945498681$	$V(37) = 450283905890997364$
$U(38) = 675425858836496044$	$V(38) = 1350851717672992090$
$U(39) = 2026277576509488133$	$V(39) = 4052555153018976268$
$U(40) = 6078832729528464400$	$V(40) = 12157665459056928802$

Man beachte, dass wenn $(U_n)_{n\geq 0}$ eine Lucas-Folge mit Diskriminante D ist, und α, β die Wurzeln des zugehörigen Polynoms sind, die Funktion $\psi_{\alpha,\beta}$ aus Abschnitt IV in folgender Weise mit ψ_D verwandt ist:

$$\psi_{\alpha,\beta}(N) = 2^{s-1}\psi_D(N).$$

Da es notwendig sein wird, gleichzeitig verschiedene Lucas-Folgen mit derselben Diskriminante D zu betrachten, ist es vorteilhaft, ψ_D anstelle von $\psi_{\alpha,\beta}$ zu verwenden.

Beispielsweise haben $U(P,Q)$ und $U(P',Q')$ für $P' = P+2$, $Q' = P+Q+1$ dieselbe Diskriminante.

Ich werde mit einigen Vorbereitungen und einfachen Ergebnissen beginnen.

(V.1) Für ungerades N mit $\mathrm{ggT}(N,D) = 1$ gilt $\psi_D(N) = N-(D\,|\,N)$ genau dann, wenn N eine Primzahl ist.

Beweis. Falls N prim ist, folgt nach Definition $\psi_D(N) = N-(D\,|\,N)$. Falls $N = p^e$ mit primem p, $e\geq 2$, dann ist $\psi_D(N)$ ein Vielfaches von p, während dies für $N-(D\,|\,N)$ nicht gilt.

Falls $N = \prod_{i=1}^{s} p_i^{e_i}$ mit $s\geq 2$, dann ist

$$\begin{aligned}\psi_D(N) &\leq \frac{1}{2^{s-1}}\prod_{i=1}^{s} p_i^{e_i-1}(p_i+1) = 2N\prod_{i=1}^{s}\frac{1}{2}\left(1+\frac{1}{p_i}\right)\\ &\leq 2N\times\frac{2}{3}\times\frac{3}{5}\times\cdots\leq\frac{4N}{5} < N-1,\end{aligned}$$

da $N>5$. □

(V.2) Wenn N ungerade ist und $\mathrm{ggT}(N,D)=1$, wobei $N-(D\,|\,N)$ den Wert $\psi_D(N)$ teilt, dann ist N eine Primzahl.

Beweis. Angenommen, N sei zerlegbar. Es sei zunächst $N=p^e$ mit einer Primzahl p und $e\geq 2$; dann $\psi_D(N) = p^e - p^{e-1}(D\,|\,p)$. Daher,

$$p^e - p^{e-1} < p^e - 1 \leq N-(D\,|\,N) \leq \psi_D(N) = p^e - p^{e-1}(D\,|\,p),$$

also wird $(D\,|\,p) = -1$ und $N-(D\,|\,N) = p^e \pm 1$ teilt $\psi_D(N) = p^e + p^{e-1} = p^e + 1 + (p^{e-1}-1)$, was unmöglich ist.

Falls N mindestens zwei verschiedene Primfaktoren hat, so folgt aus dem Beweis von (V.1), dass $\psi_D(N) < N-1 \leq N-(D\,|\,N)$, was der Voraussetzung widerspricht. Also muss N eine Primzahl sein. □

(V.3) Wenn N ungerade und $U = U(P,Q)$ eine Lucas-Folge mit Diskriminante D ist, wobei $\mathrm{ggT}(N, QD) = 1$, dann gilt $N \mid U_{\psi_D(N)}$.

Beweis. Da $\mathrm{ggT}(N,Q) = 1$, folgt aus (IV.21), dass N den Wert $\lambda_{\alpha,\beta}(N)$ teilt, wobei α, β die Wurzeln von $X^2 - PX + Q$ sind. Wenn $N = \prod_{i=1}^{s} p_i^{e_i}$, dann gilt

$$\begin{aligned}\lambda_{\alpha,\beta}(N) &= \mathrm{kgV}\left\{p_i^{e_i-1}\left(p_i - \left(\frac{D}{p_i}\right)\right)\right\} \\ &= 2\mathrm{kgV}\left\{\frac{1}{2}\,p_i^{e_i-1}\left(p_i - \left(\frac{D}{p_i}\right)\right)\right\}\end{aligned}$$

und $\lambda_{\alpha,\beta}(N)$ teilt

$$2\prod_{i=1}^{s}\frac{1}{2}\,p_i^{e_i-1}\left(p_i - \left(\frac{D}{p_i}\right)\right) = \psi_D(N).$$

Nach (IV.15) ist N ein Teiler von $U_{\psi_D(N)}$. □

(V.4) Wenn N ungerade und $U = U(P,Q)$ eine Lucas-Folge mit Diskriminante D ist, wobei $(D \mid N) = -1$ und N die Zahl U_{N+1} teilt, dann gilt $\mathrm{ggT}(N, QD) = 1$.

Beweis. Da $(D \mid N) \neq 0$, folgt $\mathrm{ggT}(N,D) = 1$. Falls es eine Primzahl p derart gibt, dass $p \mid N$ und $p \mid Q$, dann $p \nmid P$, da $p \nmid D = P^2 - 4Q$. Nach (IV.18) $p \nmid U_n$ für jedes $n \geq 1$, was der Voraussetzung widerspricht. Daher $\mathrm{ggT}(N,Q) = 1$. □

Noch ein weiteres Resultat, das an späterer Stelle benötigt wird:

(V.5) Es sei N ungerade und q ein beliebiger Primfaktor von $N+1$. Angenommen, $U = U(P,Q)$ und $V = V(P,Q)$ sind die zu den Zahlen P, Q assoziierten Lucas-Folgen mit Diskriminante $D \neq 0$. Darüber hinaus sei $\mathrm{ggT}(P,Q) = 1$ oder $\mathrm{ggT}(N,Q) = 1$. Wenn N sowohl Teiler von $U_{(N+1)/q}$ als auch von $V_{(N+1)/2}$ ist, so teilt N auch $V_{(N+1)/2q}$.

Beweis.

$$\frac{N+1}{2} = \frac{N+1}{2q} + \frac{N+1}{q}u \quad \text{mit} \quad u = \frac{q-1}{2}\,.$$

Nach (IV.4):

$$2V_{(N+1)/2} = V_{(N+1)/2q}V_{[(N+1)/q]u} + DU_{(N+1)/2q}U_{[(N+1)/q]u}.$$

Nach (IV.15) ist N Teiler von $U_{[(N+1)/q]u}$, also teilt N auch das Produkt $V_{(N+1)/2q}V_{[(N+1)/q]u}$.

Falls $\mathrm{ggT}(P,Q)=1$, folgt mit (IV.21) $\mathrm{ggT}(U_{[(N+1)/q]u}, V_{[(N+1)/q]u}) = 1$ oder 2, daher $\mathrm{ggT}(N, V_{[(N+1)/q]u})=1$, also ist N Teiler von $V_{(N+1)/2q}$.

Falls $\mathrm{ggT}(N,Q)=1$ und falls es eine Primzahl p gibt, die N und $V_{[(N+1)/q]u}$ teilt, dann folgt mit (IV.6), dass p auch $4Q$ teilen muss und da p ungerade ist, müsste auch $p \mid Q$ gelten, Widerspruch. □

Bevor ich zu den Primzahltests komme, werde ich einige einfache hinreichende Bedingungen für die Zerlegbarkeit einer Zahl angeben:

Es sei $N>1$ ungerade. Angenommen, es gibt eine Lucas-Folge $(U_n)_{n\geq 0}$ mit Parametern (P,Q) und Diskriminante D derart, dass $\mathrm{ggT}(N,QD)=1$, $(Q\,|\,N)=1$ und $N \nmid U_{\frac{1}{2}[N-(D/N)]}$. Dann ist N zerlegbar.

Die analoge Aussage für die begleitende Lucas-Folge $(V_n)_{n\geq 0}$: Angenommen, eine solche existiere mit Parametern (P,Q) und Diskriminante D derart, dass $N \nmid QD$, $(Q\,|\,N)=-1$ und $N \nmid V_{\frac{1}{2}[N-(D/N)]}$. Dann ist N zerlegbar.

Beweis. Falls $N=p$ eine ungerade Primzahl wäre, die QD nicht teilt und wenn $(Q\,|\,p)=1$, dann folgte nach (IV.23) $p \mid U_{\psi(p)/2}$ bzw. im Falle $(Q\,|\,p)=-1$, $p \mid V_{\psi(p)/2}$. In beiden Fällen ergibt sich ein Widerspruch. □

Ich bin nun soweit, einige Tests vorzustellen; jeder nachfolgende wird besser sein als der vorangegangene.

Test 1. Es sei $N>1$ ungerade und $N+1=\prod_{i=1}^{s} q_i^{f_i}$. Angenommen, es existiert eine Zahl D mit $(D\,|\,N)=-1$ derart, dass es für jeden Primfaktor q_i von $N+1$ eine Lucas-Folge $(U_n^{(i)})_{n\geq 0}$ mit Diskriminante $D=P_i^2-4Q_i$ und $\mathrm{ggT}(P_i,Q_i)=1$ oder $\mathrm{ggT}(N,Q_i)=1$ gibt, wobei ferner $N \mid U_{N+1}^{(i)}$ und $N \nmid U_{(N+1)/q_i}^{(i)}$ gilt. Dann ist N eine Primzahl.

Nachteil dieses Tests: Er setzt die Kenntnis aller Primfaktoren von $N+1$ voraus und erfordert die Berechnung der $U_n^{(i)}$ für alle $n=1,2,\ldots,N+1$.

Beweis. Nach (V.3) und (V.4), $N \mid U_{\psi_D(N)}^{(i)}$ für jedes $i=1,\ldots,s$. Es sei $\rho^{(i)}(N)$ die kleinste Zahl r mit $N \mid U_r^{(i)}$. Nach (IV.29) oder (IV.22) und der Annahme folgt $\rho^{(i)}(N) \mid (N+1)$, $\rho^{(i)}(N) \nmid (N+1)/q_i$ sowie

$\rho^{(i)}(N) \mid \psi_D(N)$. Daher $q_i^{f_i} \mid \rho^{(i)}(N)$ für jedes $i = 1, \ldots, s$. Somit $(N+1) \mid \psi_D(N)$ und nach (V.2) ist N prim. □

Der folgende Test benötigt nur die halbe Anzahl an Rechenschritten:

Test 2. Es sei $N > 1$ ungerade und $N+1 = \prod_{i=1}^{s} q_i^{f_i}$. Angenommen, es gibt eine Zahl D mit $(D \,|\, N) = -1$ derart, dass es für jeden Primfaktor q_i von $N+1$ eine Lucas-Folge $(V_n^{(i)})_{n\geq 0}$ mit Diskriminante $D = P_i^2 - 4Q_i$ und $\mathrm{ggT}(P_i, Q_i) = 1$ oder $\mathrm{ggT}(N, Q_i) = 1$ gibt, wobei ferner $N \mid V^{(i)}_{(N+1)/2}$ und $N \nmid V^{(i)}_{(N+1)/2q_i}$ gilt. Dann ist N eine Primzahl.

Beweis. Nach (IV.2), $N \mid U^{(i)}_{N+1}$. Mit (V.5), $N \nmid U^{(i)}_{(N+1)/q_i}$. Die Primalität von N folgt nun aus Test 1. □

Die folgenden Tests erfordern nur eine partielle Faktorisierung von $N+1$.

Test 3. Es sei $N > 1$ ungerade und q ein Primfaktor von $N+1$ mit $2q > \sqrt{N}+1$. Angenommen, es existiert eine Lucas-Folge $(V_n)_{n\geq 0}$ mit Diskriminante $D = P^2 - 4Q$ und $\mathrm{ggT}(P, Q) = 1$ oder $\mathrm{ggT}(N, Q) = 1$, so dass $(D \,|\, N) = -1$ und $N \mid V_{(N+1)/2}$, $N \nmid V_{(N+1)/2q}$. Dann ist N eine Primzahl.

Nachteil dieses Tests: Er setzt die Kenntnis eines recht großen Primfaktors von $N+1$ voraus.

Beweis. Es sei $N = \prod_{i=1}^{s} p_i^{e_i}$. Nach (IV.2), $N \mid U_{N+1}$ und somit wegen (IV.29) oder (IV.22), $\rho(N) \mid (N+1)$. Nach (V.5), $N \nmid U_{(N+1)/q}$; daher $\rho(N) \nmid (N+1)/q$, also $q \mid \rho(N)$. Nach (V.4) und (V.3), $N \mid U_{\psi_D(N)}$, also ist $\rho(N)$ Teiler von $\psi_D(N)$, das wiederum $N \prod_{i=1}^{s}(p_i - (D \,|\, p_i))$ teilt.

Da $q \nmid N$ gibt es ein p_i derart, dass q Teiler von $p_i - (D \,|\, p_i)$ ist, damit $p_i \equiv (D \,|\, p_i) \pmod{2q}$. Und schließlich $p_i \geq 2q - 1 > \sqrt{N}$ und $1 \leq N/p_i < \sqrt{N} < 2q - 1$, und dies impliziert, dass $N/p_i = 1$, d.h. N ist prim. □

Der nächste Test stammt von Morrison aus dem Jahre 1975 und stellt ein Analogon zum Test von Pocklington aus Abschnitt III dar:

Test 4. Es sei $N > 1$ ungerade und $N+1 = FR$, wobei $\mathrm{ggT}(F, R) = 1$ und die Faktorisierung von F bekannt sei. Angenommen, es existiert

D mit $(D\,|\,N) = -1$ derart, dass es für jeden Primfaktor q_i von F eine Lucas-Folge $(U_n^{(i)})_{n\geq 0}$ mit Diskriminante $D = P_i^2 - 4Q_i$ gibt, wobei $\mathrm{ggT}(P_i, Q_i) = 1$ oder $\mathrm{ggT}(N, Q_i) = 1$ und ferner $N \mid U_{N+1}^{(i)}$ und $\mathrm{ggT}(U_{(N+1)/q_i}^{(i)}, N) = 1$ gilt. Dann erfüllt jeder Primfaktor p von N die Kongruenz $p \equiv (D\,|\,p) \pmod F$. Falls darüber hinaus $F > \sqrt{N} + 1$ gilt, dann ist N eine Primzahl.

Beweis. Nach Annahme, $\rho^{(i)}(N) \mid (N+1)$ und erst recht $\rho^{(i)}(p) \mid (N+1)$. Aber $p \nmid U_{(N+1)/q}^{(i)}$, also $\rho^{(i)}(p) \mid (N+1)/q_i$ nach (IV.29) oder (IV.22). Wenn $q_i^{f_i}$ die maximale Potenz von q_i ist, die F teilt, dann $q_i^{f_i} \mid \rho^{(i)}(p)$, also teilt $q_i^{f_i}$ nach (IV.18) $p - (D\,|\,p)$. Daraus folgt, dass F Teiler von $p - (D\,|\,p)$ ist.

Schließlich, wenn $F > \sqrt{N}+1$, dann $p+1 \geq p-(D\,|\,p) \geq F > \sqrt{N}+1$; somit $p > \sqrt{N}$. Dies aber bedeutet, dass N selbst eine Primzahl ist. □

Das nächste Ergebnis gibt genauere Auskunft über die möglichen Primfaktoren von N.

(V.6) Es sei N ungerade, $N + 1 = FR$, wobei $\mathrm{ggT}(F, R) = 1$ und die Faktorisierung von F bekannt sei. Angenommen, es existiert eine Lucas-Folge $(U_n)_{n\geq 0}$ mit Diskriminante $D = P^2 - 4Q$, wobei $\mathrm{ggT}(P, Q) = 1$ oder $\mathrm{ggT}(N, Q) = 1$ und $(D\,|\,N) = -1$, $N \mid U_{N+1}$ und $\mathrm{ggT}(U_F, N) = 1$. Falls p ein Primfaktor von N ist, dann gibt es einen Primfaktor q von R derart, dass $p \equiv (D\,|\,p) \pmod q$.

Beweis. $\rho(p) \mid (p - (D\,|\,p))$ nach (IV.18) und $\rho(p) \mid (N+1)$. Aber $p \nmid U_F$, also $\rho(p) \nmid F$. Daher $\mathrm{ggT}(\rho(p), R) \neq 1$, und es existiert ein primes q, so dass $q \mid R$ und $q \mid \rho(p)$; insbesondere, $p \equiv (D\,|\,p) \pmod q$. □

Dieses Ergebnis findet im folgenden Test eine Anwendung:

Test 5. Es sei $N > 1$ ungerade und $N+1 = FR$ mit $\mathrm{ggT}(F, R) = 1$. Die Faktorisierung von F sei bekannt, R habe keinen Primfaktor kleiner als B, wobei $BF > \sqrt{N}+1$. Angenommen, es existiert D mit $(D\,|\,N) = -1$ derart, dass die folgenden Bedingungen erfüllt sind:

(i) Für jeden Primfaktor q_i von F existiert eine Lucas-Folge $(U_n^{(i)})_{n\geq 0}$ mit Diskriminante $D = P_i^2 - 4Q_i$, wobei $\mathrm{ggT}(P_i, Q_i) = 1$ oder $\mathrm{ggT}(N, Q_i) = 1$ und $N \mid U_{N+1}^{(i)}$ sowie $\mathrm{ggT}(U_{(N+1)/q_i}^{(i)}, N) = 1$.

(ii) Es gibt eine Lucas-Folge $(U'_n)_{n\geq 0}$ mit Diskriminante $D = P'^2 - 4Q'$, wobei $\mathrm{ggT}(P', Q') = 1$ oder $\mathrm{ggT}(N, Q') = 1$ und $N \mid U'_{N+1}$ sowie $\mathrm{ggT}(U'_F, N) = 1$.

Dann ist N eine Primzahl.

Beweis. Es sei p ein Primfaktor von N. Es ist $p \equiv (D\,|\,p) \pmod F$ nach Test 4 und aufgrund von (V.6) gibt es einen Primfaktor q von R derart, dass $p \equiv (D\,|\,p) \pmod q$. Daher $p \equiv (D\,|\,p) \pmod{qF}$, und somit

$$p + 1 \geq p - (D\,|\,p) \geq qF \geq BF > \sqrt{N} + 1.$$

Daher ist $p > \sqrt{N}$ und N eine Primzahl. □

Dieser Test ist flexibler als die anderen, denn er benötigt nur eine teilweise Faktorisierung von $N + 1$ bis zu dem Punkt, an dem man sicher sein kann, dass der nicht faktorisierte Teil von $N + 1$ keine Faktoren kleiner als B hat.

Ich möchte nun kurz angeben, wie man Lucas-Folgenglieder mit großen Indizes schnell berechnen kann. Eine der Methoden ähnelt derjenigen aus Abschnitt III zur Berechnung von hohen Potenzen.

Schreibe $n = n_0 2^k + n_1 2^{k-1} + \cdots + n_k$, mit $n_i = 0$ oder 1 und $n_0 = 1$; also $k = [(\log n)/(\log 2)]$. Die Berechnung von U_n (oder V_n) erfordert nun die simultane Berechnung von U_m, V_m für verschiedene Werte m. Die folgenden Formeln werden benötigt:

$$\begin{cases} U_{2j} = U_j V_j, \\ V_{2j} = V_j^2 - 2Q^j, \end{cases} \qquad \text{[siehe Formeln (IV.2)]}$$

$$\begin{cases} 2U_{2j+1} = V_{2j} + PU_{2j}, \\ 2V_{2j+1} = PV_{2j} + DU_{2j}. \end{cases} \qquad \text{[siehe Formeln (IV.5)]}$$

Setze $s_0 = n_0 = 1$ und $s_{j+1} = 2s_j + n_{j+1}$. Dann ist $s_k = n$. Also reicht es, U_{s_j}, V_{s_j} für $j \leq k$ zu berechnen; man beachte, dass

$$U_{s_{j+1}} = U_{2s_j + n_{j+1}} = \begin{cases} U_{2s_j} & \text{oder} \\ U_{2s_j+1}, \end{cases}$$

$$V_{s_{j+1}} = V_{2s_j + n_{j+1}} = \begin{cases} V_{2s_j} & \text{oder} \\ V_{2s_j+1}. \end{cases}$$

Daher genügt es, $2k$ Zahlen U_i und $2k$ Zahlen V_i auszurechnen, das heißt, insgesamt nur $4k$ Zahlen.

Zur Berechnung von U_n modulo N muss man nur in jedem Schritt die Zahlen durch ihren kleinsten positiven Rest modulo N ersetzen.

Die zweite Methode ist ebenfalls sehr schnell. Für $j \geq 1$ ist

$$\begin{pmatrix} U_{j+1} & V_{j+1} \\ U_j & V_j \end{pmatrix} = \begin{pmatrix} P & -Q \\ 1 & 0 \end{pmatrix} \begin{pmatrix} U_j & V_j \\ U_{j-1} & V_{j-1} \end{pmatrix}.$$

Für

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

ist

$$\begin{pmatrix} U_n & V_n \\ U_{n-1} & V_{n-1} \end{pmatrix} = M^{n-1} \begin{pmatrix} U_1 & V_1 \\ 0 & 2 \end{pmatrix}.$$

Zur Bestimmung der Potenzen von M, beispielsweise M^m, schreibt man m in Binärdarstellung und verfährt wie bei der Berechnung der Potenzen einer Zahl.

Zur Berechnung von U_n modulo N muss man wiederum alle in obiger Rechnung auftretenden Zahlen durch ihren kleinsten positiven Rest modulo N ersetzen.

Am Ende dieses Abschnitts möchte ich noch darauf hinweisen, dass es viele weitere Primzahltests derselben Familie gibt, die sich besonders für Zahlen spezieller Form eignen und entweder auf Lucas- oder auf ähnlichen Folgen basieren.

Manchmal ist es nützlich, Tests, die Lucas-Folgen verwenden, mit solchen aus Abschnitt III zu kombinieren; siehe auch den Artikel von Brillhart, Lehmer & Selfridge (1975). Als Kommentar möchte ich (mit einem lachenden Auge) die folgende Faustregel hinzufügen: Je länger die Aussage der Test-Prozedur, desto schneller führt sie zu einer Entscheidung über die Primalität.

Die bisher vorgestellten Tests sind auf Zahlen der Form $2^n - 1$ anwendbar (siehe Abschnitt VII über Mersenne-Zahlen, in dem der Test explizit angegeben ist), sowie für Zahlen $k \times 2^n - 1$ geeignet (siehe beispielsweise den Artikel von Inkeri von 1960 oder Riesels Buch, 1985).

Im Jahre 1998 veröffentlichte H.C. Williams ein Buch, das sich dem historischen und mathematischen Studium der Arbeit von Lucas widmet. Seine sorgfältige und fundierte Ausarbeitung des Themas sei jedem ans Herz gelegt, der mehr lernen möchte, als ich hier in dieser kurzen Abhandlung vorstellen konnte.

VI Fermat-Zahlen

Für Zahlen einer speziellen Form gibt es geeignetere Methoden, um zu testen, ob es sich um Primzahlen handelt oder ob sie zerlegbar sind.

Die Zahlen der Form 2^m+1 wurden bereits vor langer Zeit betrachtet.

Falls 2^m+1 eine Primzahl ist, muss der Exponent m die Form $m=2^n$ haben, also handelt es sich um eine Fermat-Zahl $F_n=2^{2^n}+1$.

Die Fermat-Zahlen $F_0=3$, $F_1=5$, $F_2=17$, $F_3=257$, $F_4=65537$ sind Primzahlen. Fermat glaubte, dass alle Fermat-Zahlen prim sind und versuchte dies auch zu beweisen. Um die 10-ziffrige Zahl F_5 auf Primalität zu testen, benötigt man eine Tabelle aller Primzahlen unterhalb von 100 000 (die Fermat nicht zur Verfügung stand). Oder man leitet ein Kriterium ab, das hilft, einen Faktor einer Fermat-Zahl zu finden. Dies gelang Fermat nicht.

Euler zeigte, dass jeder Faktor von F_n (für $n\geq 2$) die Form $k\times 2^{n+2}+1$ haben muss, und fand auf diese Weise, dass 641 ein Teiler von F_5 ist:

$$F_5 = 641\times 6700417.$$

Beweis. Es genügt zu zeigen, dass jeder Primfaktor von F_n besagte Form hat. Aus $2^{2^n}\equiv -1 \pmod p$ folgt $2^{2^{n+1}}\equiv 1 \pmod p$, also ist 2^{n+1} die Ordnung von 2 modulo p. Nach dem kleinen Satz von Fermat wird $p-1$ von 2^{n+1} geteilt; insbesondere ist 8 ein Teiler von $p-1$. Daher ist das Legendre-Symbol $2^{(p-1)/2}\equiv (2\,|\,p)\equiv 1 \pmod p$, und so ist 2^{n+1} ein Teiler von $(p-1)/2$; dies zeigt, dass $p=k\times 2^{n+2}+1$. □

Da die Zahlen F_n mit wachsendem n sehr schnell größer werden, wird es zunehmend mühsam, ihre Primalität zu prüfen.

Unter Verwendung der von Lucas gefundenen Umkehrung des kleinen Satzes von Fermat gelang es Pepin im Jahre 1877, einen Primzahltest für Fermat-Zahlen anzugeben. Und zwar:

Pepins Test. Es sei $F_n=2^{2^n}+1$ (mit $n\geq 2$) und $k\geq 2$. Dann sind die folgenden Bedingungen äquivalent:

(i) F_n ist prim und $(k\,|\,F_n)=-1$.

(ii) $k^{(F_n-1)/2}\equiv -1 \pmod{F_n}$.

Beweis. Wenn man (i) voraussetzt, so ergibt sich aus Eulers Kriterium für das Legendre-Symbol

$$k^{(F_n-1)/2} \equiv \left(\frac{k}{F_n}\right) \equiv -1 \pmod{F_n}.$$

Falls umgekehrt (ii) als wahr angenommen wird, sei a, $1 \le a < F_n$ derart gewählt, dass $a \equiv k \pmod{F_n}$. Aus $a^{(F_n-1)/2} \equiv -1 \pmod{F_n}$ folgt $a^{F_n-1} \equiv 1 \pmod{F_n}$ und nach Test 3 aus Abschnitt III ist F_n prim. Daher

$$\left(\frac{k}{F_n}\right) \equiv k^{(F_n-1)/2} \equiv -1 \pmod{F_n}. \qquad \square$$

Mögliche Werte für k sind $k = 3$, 5, 10, da $F_n \equiv 2 \pmod 3$, $F_n \equiv 2 \pmod 5$, $F_n \equiv 1 \pmod 8$; somit nach Jacobis Reziprozitätsgesetz

$$\left(\frac{3}{F_n}\right) = \left(\frac{F_n}{3}\right) = \left(\frac{2}{3}\right) = -1,$$
$$\left(\frac{5}{F_n}\right) = \left(\frac{F_n}{5}\right) = \left(\frac{2}{5}\right) = -1,$$
$$\left(\frac{10}{F_n}\right) = \left(\frac{2}{F_n}\right)\left(\frac{5}{F_n}\right) = -1.$$

Dieser Test hat sich in der Praxis sehr bewährt. Allerdings erhält man bei zerlegbarem F_n keinen Faktor.

Lucas verwendete den Test zum Nachweis der Zerlegbarkeit von F_6. Im Alter von 82 Jahren zeigte Landry 1880, dass

$$F_6 = 274177 \times 67280421310721.$$

Landry erläuterte nie, auf welche Weise er F_6 faktorisiert hat. Williams rekonstruierte 1993 Landrys Methode aufgrund von Hinweisen, die er in Briefen und Arbeiten von Landry fand.

Das Beste an der Geschichte ist ihre plötzliche Wendung, die erst kürzlich bekannt wurde. In einer Biographie über Clausen, verfasst von Biermann im Jahre 1964, ist vermerkt, dass Clausen (der als kompetenter Rechner und wichtiger Astronom bekannt war) bereits am 1. Januar 1855 in einem Brief an Gauß die komplette Faktorisierung von F_6 angegeben hatte. In diesem Brief, der sich nach wie vor in der Bibliothek der Universität Göttingen befindet, vertritt Clausen darüber hinaus die Meinung, dass der größere der beiden Faktoren die

zur damaligen Zeit größte bekannte Primzahl war. Erstaunlicherweise ist diese Bemerkung in Biermanns Biographie lange Zeit unbemerkt geblieben.

Die Faktorisierung der als zerlegbar bekannten Fermat-Zahlen ist seit jeher Gegenstand intensiver Forschung gewesen.

Die folgende Tabelle zeigt den gegenwärtigen Stand der Dinge. Die Bezeichnung Pn bedeutet eine n-ziffrige Primzahl, während Cn für eine zerlegbare Zahl mit n Stellen steht.

Tabelle 6. Vollständig faktorisierte Fermat-Zahlen

$$F_5 = 641 \times 6700417$$
$$F_6 = 274177 \times 67280421310721$$
$$F_7 = 59649589127497217 \times 5704689200685129054721$$
$$F_8 = 1238926361552897 \times P62$$
$$F_9 = 2424833 \times 7455602825647884208337395736200454918783366342657 \times P99$$
$$F_{10} = 45592577 \times 6487031809 \times 4659775785220018543264560743076778192897 \times P252$$
$$F_{11} = 319489 \times 974849 \times 167988556341760475137 \times 35608419064458339205 13 \times P564$$

Bemerkungen.

F_5 : Euler (1732)

F_6 : Faktor 1 Clausen (unveröffentlicht, 1855), Landry und Le Lasseur (1880)

F_7 : Morrison und Brillhart (1970)

F_8 : Faktor 1 Brent und Pollard (1980)

F_9 : Faktor 1 Western (1903),
andere Faktoren A.K. Lenstra und Manasse (1990)

F_{10} : Faktor 1 Selfridge (1953), Faktor 2 Brillhart (1962),
andere Faktoren Brent (1995)

F_{11} : Faktoren 1 und 2 Cunningham (1899), andere Faktoren Brent (1988),
Primalität von Faktor 5 Morain (1988)

Es ist nicht ganz leicht, einerseits über die sich ständig ergebenden Resultate informiert zu sein und andererseits mit den neuesten Entwicklungen zur Faktorisierung solcher Zahlen vertraut zu bleiben. In diesem Zusammenhang sind die Artikel von Brent (1999) und von Brent, Crandall, Dilcher und van Halewyn (2000) sehr aufschlussreich. Ich möchte mich bei W. Keller dafür bedanken, mich auf dem Laufenden zu halten, was die Entwicklung bezüglich der Fermat-Zahlen angeht.

Die kleinsten Fermat-Zahlen mit unbekanntem Status sind F_{33}, F_{34}, F_{35}, F_{40}, F_{41}, F_{44}, ...

Tabelle 7. Unvollständig faktorisierte Fermat-Zahlen

$$
\begin{aligned}
F_{12} &= 114689 \times 26017793 \times \\
&\quad 63766529 \times 190274191361 \times 1256132134125569 \times \\
&\quad 5686306475353569551690334109408678048393607420608184 33 \times \\
&\quad C1133 \\
F_{13} &= 2710954639361 \times 2663848877152141313 \times \\
&\quad 3603109844542291969 \times 319546020820551643220672513 \times C2391 \\
F_{14} &= 1169280858730743698290359938345963713403867034233733 13 \times \\
&\quad C4880 \\
F_{15} &= 1214251009 \times 2327042503868417 \times \\
&\quad 1687688170295169723830241270169 61 \times C9808 \\
F_{16} &= 825753601 \times 188981757975021318420037633 \times C19694 \\
F_{17} &= 31065037602817 \times C39444 \\
F_{18} &= 13631489 \times 81274690703860512587777 \times C78884 \\
F_{19} &= 70525124609 \times 646730219521 \times \\
&\quad 37590055514133754286524446080499713 \times C157770 \\
F_{21} &= 4485296422913 \times C631294 \\
F_{22} &= 6465870599459185100905574868504577 \times C1262577 \\
F_{23} &= 167772161 \times C2525215
\end{aligned}
$$

Tabelle 8. Zerlegbare Fermat-Zahlen ohne bekannten Faktor

F_{20} :	Buell und Young (1987)
F_{24} :	Mayer, Papadopoulos und Crandall (1999)

Rekorde

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

B. Die größte bekannte zerlegbare Fermat-Zahl ist $F_{2478782}$ und besitzt den Faktor $3 \cdot 2^{2478785} + 1$. Dieser 746190-stellige Faktor wurde von J.B. Cosgrave und seiner Proth-Gallot-Gruppe am 10. Oktober 2003 gefunden. Wesentlich beteiligt an dieser Entdeckung waren Programme von P. Jobling, G. Woltman und Y. Gallot.

C. Bis Ende August 2010 waren 243 zerlegbare Fermat-Zahlen bekannt.

Einige offene Probleme:

(1) Gibt es unendlich viele Fermat-Zahlen, die Primzahlen sind?

Diese Frage gewann aufgrund eines berühmten Resultats von Gauß erheblich an Bedeutung (siehe *Disquisitiones Arithmeticae*, Artikel 365, 366 – die letzten im Buch, als krönender Abschluss für Vieles, was vorher entwickelt wurde). Er zeigte: Wenn das gleichseitige Polygon mit $n \geq 3$ Seiten mit Lineal und Zirkel konstruiert werden kann, dann ist $n = 2^k p_1 p_2 \cdots p_h$, wobei $k \geq 0$, $h \geq 0$ und $p_1, \ldots, p_h$ verschiedene ungerade Primzahlen sind, die sämtlich Fermat-Zahlen sein müssen.

Eisenstein stellte im Jahre 1844 die Aufgabe zu zeigen, dass es tatsächlich unendlich viele prime Fermat-Zahlen gibt. Ich sollte noch hinzufügen, dass bereits 1828 ein anonymer Autor behauptet hat, dass

$$2+1,\ 2^2+1,\ 2^{2^2}+1,\ 2^{2^{2^2}}+1,\ 2^{2^{2^{2^2}}}+1,\ \ldots$$

allesamt Primzahlen sind. Er ergänzte zudem, dass es sich dabei um alle primen Fermat-Zahlen handelt (abgesehen von $2^{2^3}+1$). Allerdings fand Selfridge 1953 einen Faktor von F_{16}, womit obige Vermutung widerlegt war.

(2) Gibt es unendlich viele zerlegbare Fermat-Zahlen?

Die Beantwortung der Fragen (1) und (2) scheint außerhalb der Reichweite heutiger Methoden zu liegen, was zudem zeigt, wie wenig man in diesem Zusammenhang weiß.

(3) Ist jede Fermat-Zahl quadratfrei (d.h., ohne quadratischen Faktor)?

Unter anderem vermuteten Lehmer und Schinzel, dass es unendlich viele quadratfreie Fermat-Zahlen gibt.

Es ist nicht schwer zu zeigen: Wenn p eine Primzahl ist und p^2 eine Fermat-Zahl teilt, dann gilt $2^{p-1} \equiv 1 \pmod{p^2}$ – dies wird im Detail in Kapitel 5, Abschnitt III bewiesen werden. Falls es unendlich viele Fermat-Zahlen mit einem quadratischen Faktor gibt, müssen auch unendlich viele Primzahlen p die Kongruenz erfüllen, da Fermat-Zahlen paarweise teilerfremd sind.

Obige Kongruenz wird in Kapitel 5 behandelt werden. An dieser Stelle sei gesagt, dass sie sehr selten erfüllt ist. Insbesondere ist unbekannt, ob sie unendlich oft gilt.

Sierpiński untersuchte 1958 Zahlen der Form $S_n = n^n + 1$ mit $n \geq 2$. Er bewies, dass es für primes S_n ein $m \geq 0$ mit der Eigenschaft $n = 2^{2^m}$ gibt, also dass S_n eine Fermat-Zahl ist:

$$S_n = F_{m+2^m}.$$

Daraus kann man ableiten, dass 5 und 257 die einzigen primen S_n mit weniger als 3×10^{20} Stellen sind: Tatsächlich ergeben sich für $m = 0, 1$ die Zahlen $F_1 = 5$, $F_3 = 257$; für $m = 2$, 3, 4 oder 5 sind dies F_6, F_{11}, F_{20} und F_{37}, die sämtlich zerlegbar sind. Für $m = 6$ erhält man F_{70}, deren Status unbekannt ist. Da $2^{10} > 10^3$, folgt

$$F_{70} > 2^{2^{70}} > 2^{10^{21}} = (2^{10})^{10^{20}} > 10^{3\times 10^{20}}.$$

Primzahlen der Form $n^n + 1$ sind sehr selten. Gibt es nur endlich viele solcher Primzahlen? Falls ja, dann gäbe es unendlich viele zerlegbare Fermat-Zahlen. Aber all dies ist pure Spekulation ohne jegliche Grundlage für eine plausible Vermutung.

Das im Jahre 2001 erschienene Buch der drei Autoren Křížek, Luca & Somer mit dem Titel *17 Lectures on Fermat's Last* (hoppla) *Numbers*, besteht aus 257 Seiten mit sehr interessanten Fakten über Fermat-Zahlen.

Wie viele Seiten wird das nächste Buch über Fermat-Zahlen wohl haben, wenn man den rasanten Fortschritt beim Studium dieser Zahlen bedenkt?

VII Mersenne-Zahlen

Falls eine Zahl der Form $2^m - 1$ prim ist, so muss dies schon für den Exponenten $m = q$ gelten. Darüber hinaus lässt sich leicht nachprüfen,

dass Primzahlpotenzen der Form $2^m - 1$ Primzahlen sein müssen und somit auch m eine Primzahl ist. [Wenn Sie dies nicht alleine können, sehen Sie im Artikel von Ligh & Neal (1974) nach.]

Zahlen $M_q = 2^q - 1$ (mit primem q) nennt man Mersenne-Zahlen. Man wurde durch das Studium der vollkommenen Zahlen auf sie aufmerksam (siehe den Anhang in diesem Abschnitt).

Bereits zu Zeiten Mersennes wusste man, dass einige Mersenne-Zahlen prim, andere zerlegbar sind. Beispielsweise sind $M_2 = 3$, $M_3 = 7$, $M_5 = 31$ und $M_7 = 127$ Primzahlen, hingegen ist $M_{11} = 23 \times 89$. Im Jahre 1640 erklärte Mersenne, dass M_q für $q = 13, 17, 19, 31, 67, 127$ und 257 prim sei, was für 67 und 257 nicht stimmt. Im Bereich kleiner als 257 übersah er zudem die Exponenten 61, 89, 107, die auch zu Mersenne-Primzahlen führen. Allerdings war seine Aussage recht beeindruckend, bedenkt man die Größe der betrachteten Zahlen.

Das Problem ist offensichtlich, die Primalität einer Mersenne-Zahl festzustellen oder gegebenenfalls ihre Faktoren zu bestimmen.

Ein klassisches Resultat über Faktoren von Mersenne-Zahlen wurde erstmals 1750 von Euler erwähnt und 1775 von Lagrange, später erneut von Lucas (1878) bewiesen:

Es sei q eine Primzahl mit $q \equiv 3 \pmod 4$. Dann teilt $2q+1$ die Zahl M_q genau dann, wenn $2q+1$ eine Primzahl ist. In diesem Fall ist M_q zerlegbar, falls $q > 3$.

Beweis. Es sei $n = 2q + 1$ ein Faktor von M_q. Da $2^2 \not\equiv 1 \pmod n$, $(-2n)^q \not\equiv 1 \pmod n$, $2^{2q} - 1 = (2^q + 1)M_q \equiv 0 \pmod n$, ist n nach Lucas' Test 3 (siehe Abschnitt III) prim.

Umgekehrt sei $p = 2q+1$ prim. Da $p \equiv 7 \pmod 8$, wird $(2 \mid p) = 1$, so dass es ein m gibt mit $2 \equiv m^2 \pmod p$. Es folgt, dass $2^q \equiv 2^{(p-1)/2} \equiv m^{p-1} \equiv 1 \pmod p$, also teilt p die Zahl M_q.

Wenn darüber hinaus $q > 3$, dann ist $M_q = 2^q - 1 > 2q + 1 = p$, also M_q zerlegbar. □

Daher hat M_q für $q = 11, 23, 83, 131, 179, 191, 239, 251$ die Faktoren 23, 47, 167, 263, 359, 383, 479, 503.

Um 1825 betrachtete Sophie Germain im Zusammenhang mit dem kleinen Satz von Fermat Primzahlen q, für die auch $2q + 1$ prim ist. Solche Primzahlen nennt man heute *Sophie-Germain-Primzahlen*, ich werde in Kapitel 5 auf sie zurückkommen.

Es ist sehr leicht, die Form der Faktoren der Mersenne-Zahlen zu bestimmen:

Teiler n von M_q $(q > 2)$ erfüllen $n \equiv \pm 1 \pmod 8$ und $n \equiv 1 \pmod q$.

Beweis. Es genügt zu zeigen, dass jeder Primfaktor p von M_q die angegebene Form hat.

Falls p die Zahl $M_q = 2^q - 1$ teilt, dann gilt $2^q \equiv 1 \pmod p$; also teilt q nach dem kleinen Satz von Fermat $p-1$, das heißt, $p - 1 = 2kq$ (da $p \neq 2$). Also

$$\left(\frac{2}{p}\right) \equiv 2^{(p-1)/2} \equiv 2^{qk} \equiv 1 \pmod p,$$

somit folgt $p \equiv \pm 1 \pmod 8$ nach der in Abschnitt II erwähnten Eigenschaft des Legendre-Symbols. □

Die Primzahlen M_{13} und M_{17} wurden von Cataldi durch Probedivision als solche nachgewiesen. Euler zeigte ebenfalls auf diese Weise, dass M_{31} prim ist, konnte sich aber aufgrund der oben erwähnten Form der Faktoren von Mersenne-Zahlen viele Berechnungen sparen. Siehe in diesem Zusammenhang auch Williams & Shallit (1994).

Die zur Zeit beste Methode zum Nachweis der Primalität oder der Zerlegbarkeit von M_q basiert auf der Berechnung einer rekursiven Folge, die auf Lucas (1878) und Lehmer (1930, 1935) zurückgeht; siehe auch Western (1932), Hardy & Wright (1938, S. 223) und Kaplansky (1945). Allerdings kann man mit dieser Methode keine Faktoren finden.

Für ungerades $n \geq 3$ ist $M_n = 2^n - 1 \equiv 7 \pmod{12}$. Darüber hinaus gilt für das Jacobi-Symbol im Falle $N \equiv 7 \pmod{12}$:

$$\left(\frac{3}{N}\right) = \left(\frac{N}{3}\right)(-1)^{(N-1)/2} = -1.$$

Primzahltest für Mersenne-Zahlen. Es sei $P = 2$, $Q = -2$. Betrachte die zugehörigen Lucas-Folgen $(U_m)_{m\geq 0}$, $(V_m)_{m\geq 0}$, mit Diskriminante $D = 12$. Dann ist $N = M_n > 3$ genau dann eine Primzahl, wenn N Teiler von $V_{(N+1)/2}$ ist.

Beweis. Es sei $N > 3$ prim. Nach (IV.2) ist

$$\begin{aligned} V_{(N+1)/2}^2 &= V_{N+1} + 2Q^{(N+1)/2} = V_{N+1} - 4(-2)^{(N-1)/2} \\ &\equiv V_{N+1} - 4\left(\frac{-2}{N}\right) \equiv V_{N+1} + 4 \pmod N, \end{aligned}$$

weil

$$\left(\frac{-2}{N}\right) = \left(\frac{-1}{N}\right)\left(\frac{2}{N}\right) = -1$$

wegen $N \equiv 3 \pmod 4$ und $N \equiv 7 \pmod 8$. Daher reicht es zu zeigen, dass $V_{N+1} \equiv -4 \pmod N$.

Nach (IV.4) ist $2V_{N+1} = V_N V_1 + DU_N U_1 = 2V_N + 12U_N$; also mit (IV.14) und (IV.13):

$$V_{N+1} = V_N + 6U_N \equiv 2 + 6(12 \,|\, N) \equiv 2 - 6 \equiv -4 \pmod N.$$

Nehme nun umgekehrt an, dass N Teiler von $V_{(N+1)/2}$ ist. Dann teilt N nach (IV.2) auch U_{N+1}. Es folgt nach (IV.6) $V^2_{(N+1)/2} - 12U^2_{(N+1)/2} = 4(-2)^{(N+1)/2}$; daher $\mathrm{ggT}(N, U_{(N+1)/2}) = 1$. Und wegen $\mathrm{ggT}(N, 2) = 1$ ist N nach Test 1 (Abschnitt V) eine Primzahl. □

Zur praktischen Berechnung ist es empfehlenswert, die Lucas-Folge $(V_m)_{m\geq 0}$ durch die rekursiv definierte Folge $(S_k)_{k\geq 0}$ zu ersetzen:

$$S_0 = 4, \qquad S_{k+1} = S_k^2 - 2.$$

Die ersten Folgenglieder sind 4, 14, 194, ... Der Test drückt sich nun so aus:

$M_n = 2^n - 1$ ist genau dann prim, wenn M_n Teiler von S_{n-2} ist.

Beweis. $S_0 = 4 = V_2/2$. Angenommen $S_{k-1} = V_{2^k}/2^{2^{k-1}}$, dann ist

$$S_k = S_{k-1}^2 - 2 = \frac{V_{2^k}^2}{2^{2^k}} - 2 = \frac{V_{2^{k+1}} + 2^{2^{k+1}}}{2^{2^k}} - 2 = \frac{V_{2^{k+1}}}{2^{2^k}}\,.$$

Aufgrund des Tests ist M_n genau dann eine Primzahl, wenn M_n Teiler von

$$V_{(M_n+1)/2} = V_{2^{n-1}} = 2^{2^{n-2}} S_{n-2}$$

ist, d.h. wenn $M_n \mid S_{n-2}$ gilt. □

Das Verfahren eignet sich durch seinen iterativen Charakter in der Praxis sehr gut. Sämtliche großen Mersenne-Primzahlen wurden auf diese Weise gefunden. Lucas selbst wies im Jahre 1876 die Primalität von M_{127} nach und zeigte, dass M_{67} zerlegbar ist. Kurze Zeit später fand Perwuschin, dass auch M_{61} prim ist. Schließlich gelang es Lehmer 1927 (veröffentlicht 1932) zu zeigen, dass M_{257} zerlegbar ist, und korrigierte damit Mersennes Aussage. Man beachte, dass es sich bei M_{127}

um eine 39-stellige Zahl handelt. Sie war die größte bekannte Primzahl vor dem Computerzeitalter.

Sämtliche Mersenne-Primzahlen mit $q \leq 127$ wurden vor dem Computerzeitalter entdeckt. A. Turing unternahm 1951 einen ersten Versuch, elektronische Computer bei der Suche nach Mersenne-Primzahlen einzusetzen, allerdings ohne Erfolg. Unterstützt von D.H. und E. Lehmer führte Robinson im Jahre 1952 den Lucas-Test auf einem SWAC-Computer (des National Bureau of Standards in Los Angeles) durch. Er entdeckte am 30. Januar 1952 die Mersenne-Primzahlen M_{521} und M_{607} – die erste derartige Entdeckung auf einem Computer. Noch im selben Jahr wurden die Primzahlen M_{1279}, M_{2203} und M_{2281} gefunden.

Der Lucas-Lehmer-Primzahltest für Mersenne-Zahlen M_q erfordert eine immense Rechenleistung, wenn q sehr groß ist. Um diese Aufgabe bewältigen zu können, muss man die Arbeit auf größere Teams aufteilen, die jeweils mit hochleistungsfähigen Computern ausgestattet sind. Darüber hinaus kommen sehr spezielle Programme zum Einsatz. Eine große Rolle spielt die Multiplikation mit schneller Fourier-Transformation, die 1971 von Schönhage & Strassen entwickelt wurde. Als maßgeblich haben sich die Programme von Crandall und Woltman herausgestellt.

G.F. Woltman hat ein weltumspannendes Projekt namens GIMPS („Great Internet Mersenne Prime Search“) organisiert, das einzig und allein der Entdeckung neuer Riesen-Mersenne-Primzahlen dient. Jeder, der möchte, kann mit seinem eigenen Computer daran teilnehmen. Man erhält die notwendige Software und ein Intervall primer Exponenten als sein Territorium für die Suche. Zur Zeit sind einige tausend Teilnehmer aktiv am GIMPS-Projekt beteiligt. Vor gar nicht allzu langer Zeit gaben Gold- und Diamantenschürfer ihre Familien und Freunde auf, nur um in irgendwelchen unwirtlichen Gegenden, Dschungeln mit Schlangen, krankheitsverseuchten Sümpfen oder hohen, schneebedeckten, felsigen Bergen irgendwann die kostbare Entdeckung zu machen, die sie reich machen sollte. Der moderne Mersenne-Primzahlen-Sucher erlebt ein ähnliches Abenteuer. Die Fundstellen sind unvorhersagbar, glücklich der, der SIE als Erster findet. Keine Reichtümer, aber Ruhm. Meine Metapher ist gar nicht so realitätsfremd. Man sehe sich dazu nur einmal Woltmans eigene Beschreibung zur Entdeckung der 38sten Mersenne-Primzahl (1999) an – der Kapitän der Mersenne-Forscher erzählt...

Tabelle 9. Mersenne-Primzahlen M_q

q	Jahr	Entdecker
2	–	–
3	–	–
5	–	–
7	–	–
13	1461	Unbekannt*
17	1588	P.A. Cataldi
19	1588	P.A. Cataldi
31	1750	L. Euler
61	1883	I.M. Perwuschin
89	1911	R.E. Powers
107	1913	E. Fauquembergue
127	1876	E. Lucas
521	1952	R.M. Robinson
607	1952	R.M. Robinson
1279	1952	R.M. Robinson
2203	1952	R.M. Robinson
2281	1952	R.M. Robinson
3217	1957	H. Riesel
4253	1961	A. Hurwitz
4423	1961	A. Hurwitz
9689	1963	D.B. Gillies
9941	1963	D.B. Gillies
11213	1963	D.B. Gillies
19937	1971	B. Tuckerman
21701	1978	L.C. Noll und L. Nickel
23209	1979	L.C. Noll
44497	1979	H. Nelson und D. Slowinski
86243	1982	D. Slowinski
110503	1988	W.N. Colquitt und L. Welsh, Jr.
132049	1983	D. Slowinski
216091	1985	D. Slowinski
756839	1992	D. Slowinski und P. Gage
859433	1993	D. Slowinski und P. Gage
1257787	1996	D. Slowinski und P. Gage

*Siehe Dicksons *History of the Theory of Numbers*, Bd. I, S. 6.

Tabelle 9 (Fortsetzung)

q	Jahr	Entdecker
1398269	1996	J. Armengaud, G.F. Woltman und GIMPS
2976221	1997	G. Spence, G.F. Woltman und GIMPS
3021377	1998	R. Clarkson, G.F. Woltman**
6972593	1999	N. Hajratwala, G.F. Woltman**
13466917	2001	M. Cameron, G.F. Woltman**
20996011	2003	M. Shafer, G.F. Woltman**
24036583	2004	J. Findley, G.F. Woltman**
25964951	2005	M. Nowak, G.F. Woltman**
30402457	2005	C. Cooper, S.R. Boone, G.F. Woltman**
32582657	2006	C. Cooper, S.R. Boone, G.F. Woltman**
37156667	2008	H.-M. Elvenich, G.F. Woltman**
42643801	2009	O.M. Strindmo, G.F. Woltman**
43112609	2008	E. Smith, G.F. Woltman**

**mit S. Kurowski und GIMPS

Rekord

Tabelle 9 zeigt alle 47 bisher gefundenen Mersenne-Primzahlen. Die größte bekannte Mersenne-Primzahl mit $q = 43112609$ hat 12978189 Ziffern. Ihre Entdeckung am 23. August 2008 wird Smith, Woltman, Kurowski u. a. zugeschrieben. Smith hatte als Systemverwalter des Mathematik-Departments der Universität von Los Angeles Monate zuvor die Bildschirmschoner durch das GIMPS-Programm ersetzt, und einer dieser Rechner bekam das glücksbringende Segment zu fassen.

Unter den drei bekannten Mersenne-Primzahlen, die mehr als zehn Millionen Stellen haben, war die größte als erste bekannt geworden. Deshalb bekamen deren Entdecker das von der *Electronic Frontier Foundation* ausgesetzte Preisgeld von 100 000 US-Dollar zugesprochen.

Man wird immer neue Begriffe erfinden müssen, denn bis dahin hatte man Primzahlen mit mindestens einer Million Stellen als *Megaprimzahlen* bezeichnet. Inzwischen kennt man 29 Megaprimzahlen; vergleiche auch Tabelle 24 in Kapitel 5, Abschnitt 6.

Nicht nur im bereits genannten Fall wurden die Mersenne-Primzahlen nicht nach ihrer wachsenden Größe entdeckt. Die Primzahl M_{110503} wurde erst lange nach der Entdeckung von M_{132049} und M_{216091} gefunden. Es kann also passieren, dass die nächste noch zu findende Mersenne-Primzahl einen Exponenten $q < 43112609$ hat, da zur Zeit

noch nicht alle M_q mit primem q unterhalb dieser Grenze auf Primalität hin untersucht worden sind. Bis Ende August 2010 wurden alle Exponenten bis $3{,}1 \times 10^7$ getestet und alle bis $2{,}1 \times 10^7$ ein weiteres Mal kontrolliert.

Die Suche nach Sophie Germain-Primzahlen q der Form $q = k \times 2^N - 1$ (so dass auch $2q + 1$ prim ist) führt, wie bereits erwähnt, zu zerlegbaren Mersenne-Zahlen M_q.

Rekord

Die größte bekannte zerlegbare Mersenne-Zahl M_q hat den Exponenten $q = 183027 \times 2^{265440} - 1$ und wurde im März 2010 von T. Wu und J. Penné gefunden. Die Primzahl q ist die größte bekannte Sophie-Germain-Primzahl (siehe Kapitel 5, Abschnitt II).

Das Buch von Riesel (1985) enthält eine Tabelle der vollständigen Faktorisierungen aller Zahlen $M_n = 2^n - 1$ mit ungeradem $n \leq 257$. Eine umfassendere Tabelle findet sich im Buch von Brillhart et al. (1983, 1988; siehe auch die dritte Auflage, 2002).

Wie schon bei den Fermat-Zahlen gibt es auch im Zusammenhang mit den Mersenne-Zahlen viele offene Probleme:

(1) Gibt es unendlich viele Mersenne-Primzahlen?

(2) Gibt es unendlich viele zerlegbare Mersenne-Zahlen?

Ich werde noch versuchen zu begründen, warum die Antwort in beiden Fällen „Ja“ sein sollte. Beispielsweise werde ich in Kapitel 6, Abschnitt I, nach (D5), darauf hinweisen, dass es in einigen Folgen, die der Folge der Mersenne-Zahlen ähneln, unendlich viele zerlegbare Zahlen gibt.

(3) Ist jede Mersenne-Zahl quadratfrei?

Rotkiewicz zeigte 1965, dass eine Primzahl p, deren Quadrat p^2 eine Mersenne-Zahl teilt, die Kongruenz $2^{p-1} \equiv 1 \pmod{p^2}$ erfüllt. Dies ist dieselbe Kongruenz, die bereits im Zusammenhang mit Fermat-Zahlen auftauchte, welche einen quadratischen Faktor enthalten.

Ich möchte an dieser Stelle noch zwei weitere Probleme erwähnen, die sich auf Mersenne-Zahlen beziehen. Eines davon ist gelöst, das andere noch offen.

Wenn M_q eine Mersenne-Primzahl ist, gilt dies dann auch für M_{M_q}?

Die Antwort ist negativ: M_{13} ist eine Primzahl, $M_{M_{13}} = 2^{8191} - 1$ jedoch zerlegbar, wie Wheeler nachwies, siehe Robinson (1954).

Man beachte, dass $M_{M_{13}}$ mehr als 2400 Stellen hat. Keller entdeckte 1976 den Primfaktor

$$p = 2 \times 20644229 \times M_{13} + 1 = 338193759479$$

der Mersenne-Zahl $M_{M_{13}}$ und gab damit zugleich einen einfachen Beweis für ihre Zerlegbarkeit an. Nur 13-maliges Quadrieren modulo p ist notwendig, um nachzuweisen, dass $2^{2^{13}} \equiv 2 \pmod{p}$. Dies wurde mir von Keller in einem Brief mitgeteilt.

Das zweite Problem stammt von Catalan aus dem Jahre 1876 und ist in Dicksons *History of the Theory Numbers*, Bd. I, S. 22 erwähnt: Man betrachte die Folge der Zahlen

$$\begin{aligned}
C_1 &= 2^2 - 1 = 3 = M_2\,,\\
C_2 &= 2^{C_1} - 1 = 7 = M_3\,,\\
C_3 &= 2^{C_2} - 1 = 127 = M_7\,,\\
C_4 &= 2^{C_3} - 1 = 2^{127} - 1 = M_{127}\,,\\
&\cdots\cdots\cdots\cdots\\
C_{n+1} &= 2^{C_n} - 1\\
&\cdots\cdots\cdots\cdots
\end{aligned}$$

Sind alle Zahlen C_n Primzahlen? Gibt es unendlich viele, die prim sind? Zur Zeit ist es noch unmöglich, C_5 zu testen. Diese Zahl hat mehr als 10^{37} Stellen!

Abschließend noch eine interessante Vermutung über die Mersenne-Primzahlen. Sie geht auf Bateman, Selfridge & Wagstaff (1989) zurück.

Vermutung. Es sei p eine ungerade natürliche Zahl (nicht notwendigerweise prim). Falls zwei der folgenden Bedingungen erfüllt sind, so ist auch die dritte erfüllt:

(a) p ist gleich $2^k \pm 1$ oder $4^k \pm 3$ (für ein $k \geq 1$).

(b) M_p ist prim.

(c) $(2^p + 1)/3$ ist prim.

R. Lifchitz hat gezeigt, dass die Vermutung für alle $p < 16777213$ richtig ist. In diesem Bereich sind $p = 3$, 5, 7, 13, 17, 19, 31, 61, 127 die einzigen Primzahlen, die allen drei Bedingungen genügen. Es ist denkbar, dass dies überhaupt die Einzigen mit dieser Eigenschaft sind.

Es sei noch angemerkt, dass die Primzahlen (bzw. Quasiprimzahlen) der Form $(2^p + 1)/3$ für alle $p < 720000$ bestimmt worden sind, wie mir von H. und R. Lifchitz mitgeteilt wurde. In denjenigen Fällen, in denen bereits zwei der obigen Bedingungen als nicht erfüllt erkannt sind, ist deren Kenntnis jedoch entbehrlich.

Nachtrag über vollkommene Zahlen

Ich werde nun vollkommene Zahlen behandeln und davon berichten, in welchem Zusammenhang sie mit den Mersenne-Zahlen stehen.

Eine natürliche Zahl $n > 1$ heißt *vollkommen*, wenn sie gleich der Summe ihrer Teiler d mit $d < n$ ist. Beispielsweise sind $n = 6$, 28, 496, 8128 die vollkommenen Zahlen kleiner als 10000.

Vollkommene Zahlen waren bereits in der Antike bekannt. Die erste vollkommene Zahl 6 wurde von den mystischen und religiösen Schreibern mit der Schöpfung in Zusammenhang gebracht; es dauerte 6 Tage, bis die Welt vollkommen war.

Euklid zeigte in seinen *Elementen*, Buch IX, Lehrsatz 36, dass wenn q und $M_q = 2^q - 1$ Primzahlen sind, die Zahl $N = 2^{q-1}(2^q - 1)$ vollkommen ist.

In einem posthum veröffentlichten Artikel bewies Euler die Umkehrung: Jede gerade vollkommene Zahl hat die von Euklid angegebene Form. Folglich ist die Kenntnis der geraden vollkommenen Zahlen gleichbedeutend mit der Kenntnis der Mersenne-Primzahlen.

Aber was ist mit ungeraden vollkommenen Zahlen? Existieren sie? Nicht eine Einzige wurde jemals gefunden! Diese Frage blieb trotz intensiver Bemühungen bis heute unbeantwortet.

Eine Kurzinformation über die Fortschritte hin zu einer Lösung des Problems kann man Guys Buch entnehmen (Neuauflage 2004, siehe Allgemeine Grundlagen). Neuere Ergebnisse sind zudem weiter unten erwähnt.

Es gibt eine ganze Heerschar von Methoden, mit Hilfe derer man versucht hat, das Problem anzugehen. Ich denke, es ist sinnvoll, einige davon zu beschreiben, um dem Leser ein Gefühl dafür zu geben, was möglich ist, wenn man sich scheinbar in einer Sackgasse befindet. Die Idee ist, die Existenz einer ungeraden vollkommenen Zahl N anzunehmen, um dann verschiedene Konsequenzen abzuleiten. Beispielsweise die Anzahl ihrer verschiedenen Primteiler $\omega(N)$ betreffend oder die Größe von N, die multiplikative und die additive Form von N usw. Ich möchte eine Übersicht über die Fortschritte bezüglich einiger Ansätze geben.

(a) Anzahl der verschiedenen Primfaktoren $\omega(N)$

Hagis (1980, angekündigt 1975) bewies, dass $\omega(N) \geq 8$. Das gleiche Resultat wurde von Chein (1979) in seiner Dissertation erzielt.

Im Jahre 1983 zeigten Hagis und unabhängig davon Kishore, dass wenn $3 \nmid N$, dann $\omega(N) \geq 11$.

Beide Resultate konnten von Nielsen (2007) verschärft werden. Für den Fall $3 \nmid N$ zeigte er $\omega(N) \geq 12$ und für den allgemeinen Fall $\omega(N) \geq 9$.

Ein weiteres Ergebnis in diesem Zusammenhang wurde von Dickson 1913 angegeben: Für jedes $k \geq 1$ gibt es höchstens endlich viele ungerade vollkommene Zahlen N derart, dass $\omega(N) = k$. Shapiro vereinfachte den Beweis im Jahre 1949.

Dicksons Satz wurde 1956 von Kanold auf Zahlen N verallgemeinert, die der Bedingung $\sigma(N)/N = \alpha$ genügen (α ist eine gegebene, rationale Zahl und $\sigma(N)$ bezeichnet die Summe aller Teiler von N). Im Beweis wurde die Tatsache verwendet, dass die Gleichung $aX^3 - bY^3 = c$ höchstens endlich viele Lösungen mit ganzzahligen x, y besitzt. Baker konnte unter Verwendung seiner berühmten Methode der Linearformen in Logarithmen eine effektive Abschätzung der Anzahl der Lösungen erreichen. Mit Hilfe dieser Abschätzung gelang es Pomerance 1977 (mit $\alpha = 2$) zu zeigen, dass für jedes $k \geq 1$ gilt: Wenn die Anzahl der verschiedenen Primfaktoren der ungeraden vollkommenen Zahl N gleich k ist, dann gilt

$$N < (4k)^{(4k)^{2^{k^2}}}.$$

Heath-Brown konnte die Aussage von Pomerance 1994 erheblich verschärfen: Falls die Anzahl der verschiedenen Primfaktoren der ungeraden vollkommenen Zahl N gleich k ist, dann gilt

$$N < 4^{4^k}.$$

Nach einer Verbesserung durch Cook im Jahre 1999 zeigte Nielsen 2003, dass auch

$$N < 2^{4^k}.$$

(b) Untere Schranke für N

Brent, Cohen & te Riele (1991) fanden heraus, dass eine ungerade vollkommene Zahl N größer als 10^{300} sein muss. Zuvor hatten Brent & Cohen 1989 gezeigt, dass $N > 10^{160}$. Hagis hatte 1973 bewiesen, dass $N > 10^{50}$.

Buxton & Elmore hatten 1976 behauptet, dass $N > 10^{200}$. Diese Aussage war jedoch nicht ausreichend begründet, so dass man dieses Ergebnis nicht akzeptieren sollte. Grytczuk & Wojtowicz veröffentlichten 1999 eine weitaus größere untere Schranke für N. Allerdings fand F. Saidak einen Fehler im Beweis, der von den Autoren im Jahre 2000 auch bestätigt wurde.

(c) Multiplikative Struktur von N

Das erste Ergebnis stammt von Euler: $N = p^e k^2$, wobei p eine Primzahl ist, die k nicht teilt und $p \equiv e \equiv 1 \pmod 4$.

Es gibt eine Vielzahl von Resultaten zur Zahl k. Beispielsweise zeigten Hagis & McDaniel 1972, dass k keine Kubikzahl sein kann.

(d) Größter Primfaktor von N

Im Jahre 2008 zeigten Goto & Ohno, dass N einen Primfaktor größer als 10^8 haben muss. Davor hatten Hagis & McDaniel (1972) bewiesen, dass der größte Primfaktor von N größer als 100110 sein muss. Diese Grenze wurde dann von Hagis & Cohen (1998) auf 10^6 und von Jenkins (2003) auf 10^7 erhöht.

Muskat ermittelte 1966, dass N einen Primzahlpotenzfaktor besitzen muss, der größer als 10^{12} ist.

(e) Andere Primfaktoren von N

Pomerance zeigte 1975, dass der zweitgrößte Primfaktor von N größer oder gleich 139 sein muss. Diese Grenze wurde von Hagis (1981) auf 10^3 und von Iannucci (1999) auf 10^4 erhöht. Im Jahre 2000 konnte Iannucci darüber hinaus nachweisen, dass der drittgrößte Primfaktor von N die Zahl 100 übertreffen muss.

Grün bewies 1952, dass der kleinste Primfaktor p_1 von N der Ungleichung $p_1 < \frac{2}{3}\omega(N) + 2$ genügen muss.

In seiner Dissertation zeigte Kishore (1977), dass der i-te Primfaktor von N (für $i = 2, 3, 4, 5, 6$) kleiner als $2^{2^{i-1}}(\omega(N) - i + 1)$ ist.

Perisastri bewies 1958, dass

$$\frac{1}{2} < \sum_{p|N} \frac{1}{p} < 2 \log \frac{\pi}{2}.$$

Dieses Resultat wurde von Suryanarayana (1963), Suryanarayana & Hagis (1970) und Cohen (1978) verschärft.

(f) Additive Struktur von N

Touchard bewies 1953, dass $N \equiv 1 \pmod{12}$ oder $N \equiv 9 \pmod{36}$. Später gab Satyanarayana (1959) einen einfacheren Beweis an.

(g) Ores Vermutung

Ore betrachtete 1948 das harmonische Mittel der Teiler von N (das ist der Kehrwert des arithmetischen Mittels der Kehrwerte der Teiler), genauer

$$H(N) = \frac{\tau(N)}{\sum\limits_{d|N}(1/d)} = \frac{N\tau(N)}{\sigma(N)},$$

wobei $\tau(N)$ die Anzahl der Teiler von N und $\sigma(N)$ die Summe aller Teiler von N bezeichnet.

Man nennt N eine *harmonische Zahl*, wenn $H(N)$ ganzzahlig ist. Aus Eulers Resultaten folgt, dass jede vollkommene Zahl eine harmonische Zahl ist. Ore vermutete, dass alle harmonischen Zahlen gerade sind. Wenn diese Vermutung wahr ist, dann folgt daraus, dass es keine ungerade vollkommene Zahl gibt.

Zur näheren Untersuchung seiner Vermutung bestimmte Ore 1954 alle harmonischen Zahlen $N < 10^4$. Die Liste der harmonischen Zahlen wurde später wie folgt erweitert: 1954 durch Garcia bis 10^7, 1997 durch Cohen bis 2×10^9 und 2003 durch Sorli bis 10^{12}. Im Jahre 2007 erstellten Goto & Okeya die Liste aller 937 harmonischen Zahlen unterhalb 10^{14}; sie sind alle gerade.

Im Jahre 2010 zeigten Cohen & Sorli, dass eine ungerade harmonische Zahl, falls es sie gibt, größer als 10^{24} sein muss.

Wie mir Pomerance freundlicherweise mitteilte, verifizierte er Ores Vermutung für $\omega(N) \leq 2$. Er zeigte, dass in diesem Fall aus der Ganzzahligkeit von $H(N)$ folgt, dass N eine gerade vollkommene Zahl ist.

Bei den folgenden Ergebnissen wird nicht zwischen geraden und ungeraden Zahlen unterschieden. Es geht um die Verteilung der vollkommenen Zahlen. Dazu wird für $x \geq 1$ eine Funktion $V(x)$ definiert, die die Anzahl der vollkommenen Zahlen kleiner oder gleich x zählt:

$$V(x) = \#\{N \text{ vollkommen} \mid N \leq x\}.$$

Der Grenzwert $\lim_{x\to\infty} V(x)/x$ stellt eine natürliche Dichte für die Menge der vollkommenen Zahlen dar. Kanold zeigte im Jahre 1954, dass $\lim_{x\to\infty} V(x)/x = 0$, d.h. $V(x)$ wächst langsamer gegen Unendlich als x.

Das folgende Resultat von Wirsing (1959) gibt genauere Auskunft über das Wachstum von $V(x)$: Es gibt x_0 und $C > 0$ derart, dass für $x \geq x_0$,

$$V(x) \leq e^{(C \log x)/(\log \log x)}.$$

Frühere Arbeiten stammen von Hornfeck (1955, 1956), Kanold (1957) und Hornfeck & Wirsing (1957), die herausgefunden hatten, dass es für jedes $\varepsilon > 0$ eine positive Konstante C derart gibt, dass $V(x) < Cx^{\varepsilon}$.

Sämtliche hier vorgestellten Aussagen über die Existenz ungerader vollkommener Zahlen waren das Ergebnis teilweise schwieriger und heikler Überlegungen. Trotzdem stellt sich das Problem nach wie vor wie eine uneinnehmbare Festung dar. Nach Allem, was bekannt ist, wäre es reines Glück, eine ungerade vollkommene Zahl zu finden. Andererseits ist bisher nichts bewiesen worden, das einen von der Nichtexistenz ungerader vollkommener Zahlen überzeugen könnte. Es sind neue Ideen gefragt.

Ich möchte diesen Überblick über vollkommene Zahlen mit den folgenden Resultaten von Sinha (1974) abschließen. Der elementar zu führende Beweis ist recht amüsant (man halte seinen Bleistift bereit!): 28 ist die einzige vollkommene Zahl der Form $a^n + b^n$ mit $n \geq 2$ und $\mathrm{ggT}(a, b) = 1$. Es ist auch die einzige gerade vollkommene Zahl der Form $a^n + 1$ mit $n \geq 2$. Und schließlich: Es existiert keine gerade vollkommene Zahl der Form

$$a^{n^{n^{\cdot^{\cdot^{\cdot^{n}}}}}} + 1$$

mit $n \geq 2$ und mindestens zwei Exponenten n.

Zurückblickend stellt man fest, dass vollkommene Zahlen dadurch definiert sind, dass man N mit der Summe der echten Teiler von N vergleicht. Wenn man nur fordert, dass N diese Summe teilt, landet man bei den *mehrfach vollkommenen Zahlen*. Zahlen N mit $2N < \sigma(N)$ heißen *abundant*, solche mit $2N > \sigma(N)$ *defizient*.

Es bezeichne $s(N) = \sigma(N) - N$ die Summe der echten Teiler von N. Da einige Zahlen abundant und andere defizient sind, liegt es nahe, den Prozess zur Erlangung von $s(N)$ durch Bildung dieser Folge zu iterieren: $s(N)$, $s^2(N)$, $s^3(N), \ldots$, wobei $s^k(N) = s\big(s^{k-1}(N)\big)$. Diese Vorgehensweise führt zu vielen faszinierenden Fragen, die im Buch von Guy beschrieben sind. Mangels Platz kann ich mich diesen Dingen hier nicht zuwenden.

VIII Pseudoprimzahlen

In diesem Abschnitt werde ich zerlegbare Zahlen betrachten, die Eigenschaften haben, von denen man annehmen würde, dass sie nur auf Primzahlen zuträfen.

A Pseudoprimzahlen zur Basis 2 (psp)

Ein Problem, das zumeist den Chinesen des Altertums zugeschrieben wird, ist die Frage, ob eine natürliche Zahl n eine Primzahl sein muss, wenn sie diese Kongruenz erfüllt:

$$2^n \equiv 2 \pmod{n}.$$

Um dieses Thema ranken sich Legenden und Spekulationen und man sollte sich vor voreiligen Schlüssen in Acht nehmen. Angesichts dessen, was man im alten China über Zahlen zu wissen schien, ist es schwer vorstellbar, dass eine solche Frage überhaupt formuliert werden konnte. Siu Man-Keung, ein Mathematiker aus Hong Kong, der sich für die Geschichte der Mathematik interessiert, schrieb mir Folgendes:

> Diese Sage geht auf einen Artikel von J.H. Jeans im *Messenger of Mathematics*, 27, 1897/8 zurück. Dieser schrieb dort, dass „ein Artikel, der unter denen des verstorbenen Sir Thomas Wade gefunden wurde und auf die Zeit von Konfuzius datiert ist“ den Satz enthielte, dass $2^n \equiv 2 \pmod{n}$ genau dann gilt, wenn n eine Primzahl ist. Allerdings weist J. Needham in einer Fußnote in seinem monumentalen Werk *Science and Civilisation in China*, Bd. 3, Kap. 19 (Mathematics) die Behauptung von Jeans zurück. Diese sei die Folge einer falschen Übersetzung einer Passage des berühmten Buches *The Nine Chapters of Mathematical Art*.

Der Fehler wurde von verschiedenen westlichen Gelehrten aufrechterhalten. In Dicksons *History of the Theory of Numbers*, Bd. I, S. 91 ist angegeben, dass Leibniz glaubte bewiesen zu haben, dass die oben erwähnte, sogenannte chinesische Kongruenz die Primalität von n impliziert. Die Geschichte wird beispielsweise auch in Honsbergers sehr nett geschriebenen Kapitel „An Old Chinese Theorem and Pierre de Fermat“ seines Buches *Mathematical Gems*, Bd. I, (1973) wiederholt.

Es gibt inzwischen eine besser fundierte Version der Abläufe. In einem Brief vom Februar 1992 schrieb Siu:

Ich sah gerade die in Chinesisch verfasste Doktorarbeit von Han Qi über die Mathematik der Qing-Zeit mit dem Titel *Transmission of Western Mathematics during the Kangxi Kingdom and its Influence Over Chinese Mathematics* (Peking, 1991). Der Autor weist auf neue Belege bezüglich des „alten chinesischen Satzes“ hin. Han zufolge geht dieser „Satz“ auf Li Shan-Lan (1811–1882) zurück, einen bekannten Mathematiker der Qing-Zeit (die Aussage ist daher nicht besonders alt). Li erwähnte sein Kriterium gegenüber Alexander Wylie, der sein Mitarbeiter bei der Übersetzung von westlichen Texten war. Wylie, der die Mathematik wahrscheinlich nicht verstand, präsentierte Li's Kriterium in einer Mitteilung „A Chinese theorem“ der Zeitschrift *Notes and Queries on China*, Hong Kong, 1869 (1873).

In den folgenden Monaten gaben mindestens vier Leser Kommentare über die Arbeit von Li ab; einer wies darauf hin, dass Li's Aussage falsch sei. Unter diesen Lesern war ein gewisser J. von Gumpach, ein Deutscher, der später Kollege von Li in Peking wurde. Offenbar informierte von Gumpach Li über seinen Fehler. Daraufhin strich Li in einer späteren Veröffentlichung über Zahlentheorie (1872) jeden Hinweis auf sein Kriterium. Allerdings veröffentlichte 1882 ein weiterer bekannter Mathematiker der Qing-Zeit namens Hua Heng-Fang eine Abhandlung über Zahlen, in der er Li's Kriterium anführt, als sei es korrekt. Dies könnte dabei helfen, zu verstehen, warum westliche Historiker chinesischer Mathematik dazu verleitet waren, das Kriterium als altes, chinesisches Theorem anzusehen. Han Qi hat angekündigt, dass er beabsichtigt, einen Artikel mit weiteren Details über dieses Thema zu veröffentlichen.

Ich möchte bei dieser Gelegenheit Siu Man-Keung für seine wohlbegründeten und interessanten Informationen danken.

Über die Arbeiten von Li Shan-Lan kann man sich in der englischen Übersetzung (1987) des Buchs von Li Yan & Du Shiran informieren.

Nach diesen historischen Anmerkungen möchte ich nun zum Problem der Kongruenz $2^n \equiv 2 \pmod{n}$ zurückkehren, die man vielleicht passenderweise oder eher scherzhaft die „pseudo-chinesische Kongruenz über Pseudoprimzahlen“ nennen könnte.

Das erste Gegenbeispiel wurde 1819 angegeben, viel früher als die Ereignisse in China stattfanden. Sarrus zeigte $2^{341} \equiv 2 \pmod{341}$,

jedoch ist $341 = 11 \times 31$ zerlegbar. Insbesondere ist die direkte Umkehrung von Fermats kleinem Satz falsch.

Weitere zerlegbare Zahlen mit dieser Eigenschaft sind beispielsweise 561, 645, 1105, 1387, 1729, 1905.

Eine zerlegbare Zahl, die der Kongruenz $2^{n-1} \equiv 1 \pmod{n}$ genügt, heißt *Pseudoprimzahl* oder auch eine *Poulet-Zahl*. Poulet untersuchte solche Zahlen und berechnete schon 1926 eine Tabelle aller Pseudoprimzahlen bis 5×10^7, die er 1938 bis 10^8 erweitert hatte; siehe die Referenzen in Kapitel 4.

Jede Pseudoprimzahl n ist ungerade und erfüllt ebenso die Kongruenz $2^n \equiv 2 \pmod{n}$; umgekehrt ist jede ungerade zerlegbare Zahl, die dieser Kongruenz genügt, eine Pseudoprimzahl.

Natürlich gilt obige Kongruenz für jede ungerade Primzahl, also muss n im Falle $2^{n-1} \not\equiv 1 \pmod{n}$ zerlegbar sein. Dies ist ein sinnvoller erster Schritt beim Test auf Primalität.

Um mehr über Primzahlen zu erfahren, liegt es nahe, diejenigen Zahlen n zu untersuchen, die $2^{n-1} \equiv 1 \pmod{n}$ erfüllen.

Angenommen, ich wollte ein Kapitel über Pseudoprimzahlen für das *Guinness Buch der Rekorde* schreiben. Wie würde ich dieses aufbauen?

Die nahe liegenden Fragen würden dieselben sein wie bei den Primzahlen. Zum Beispiel: Wie viele Pseudoprimzahlen gibt es? Wie kann man erkennen, ob eine Zahl pseudoprim ist? Gibt es Methoden, um Pseudoprimzahlen zu erzeugen? Wie sind sie verteilt?

Wie sich nicht ganz überraschenderweise herausstellt, gibt es unendlich viele Pseudoprimzahlen, und es gibt viele Methoden, unendliche Folgen pseudoprimer Zahlen zu erzeugen.

Der einfachste Beweis stammt von Malo aus dem Jahre 1903. Er zeigte, dass wenn n pseudoprim ist, dies auch für die Zahl $n' = 2^n - 1$ zutrifft. In der Tat ist n' offensichtlich zerlegbar, denn wenn $n = ab$ mit $1 < a, b < n$, dann ist

$$2^n - 1 = (2^a - 1)\big(2^{a(b-1)} + 2^{a(b-2)} + \cdots + 2^a + 1\big).$$

Darüber hinaus ist n Teiler von $2^{n-1}-1$, daher teilt n die Zahl $2^n - 2 = n' - 1$; also ist $n' = 2^n - 1$ Teiler von $2^{n'-1} - 1$.

Unter Verwendung der Fermat-Zahlen gab Cipolla 1904 einen weiteren Beweis an:

Es seien $m > n > \cdots > s > 1$ ganze Zahlen und N das Produkt der Fermat-Zahlen $N = F_m F_n \cdots F_s$. Dann ist N genau dann pseudoprim, wenn $2^s > m$. Tatsächlich ist 2^{m+1} die Ordnung von 2 modulo N, und dies ist gleich dem kleinsten gemeinsamen Vielfachen der Ordnungen

2^{m+1}, $2^{n+1}, \ldots, 2^{s+1}$ von 2 modulo jedem Faktor F_m, $F_n, \ldots, F_s$ von N. Daher gilt $2^{N-1} \equiv 1 \pmod{N}$ genau dann, wenn $N-1$ durch 2^{m+1} teilbar ist. Aber $N - 1 = F_m F_n \cdots F_s - 1 = 2^{2^s} Q$ mit ungeradem Q. Somit ist $2^s > m$ die erforderliche Bedingung. □

Wie bereits in Kapitel 1 angedeutet, sind die Fermat-Zahlen paarweise teilerfremd, so dass obige Methode zu paarweise teilerfremden Pseudoprimzahlen führt. Man kann auch Pseudoprimzahlen mit einer beliebigen Anzahl von Primfaktoren erzeugen.

Cipolla gab noch ein anderes Verfahren an, das weiter unten beschrieben wird.

Lehmer fand 1936 eine sehr einfache Methode, um unendlich viele Pseudoprimzahlen zu generieren, die jeweils das Produkt zweier Primzahlen p und q sind. Und zwar sei $k \geq 5$ eine beliebige ungerade Zahl, p ein primitiver Primfaktor von $2^k - 1$ und q ein primitiver Primfaktor von $2^k + 1$. Dann ist pq eine Pseudoprimzahl. Das heißt, für jedes $m \geq 1$ gibt es mindestens m pseudoprime $n = pq$ derart, dass

$$n \leq \left(2^{2m+3} - 1\right)\left(\frac{2^{2m+3}+1}{3}\right) = \frac{4^{2m+3}-1}{3}.$$

Es gibt auch gerade zerlegbare Zahlen, die die Kongruenz $2^n \equiv 2 \pmod{n}$ erfüllen. Man könnte sie *gerade Pseudoprimzahlen* nennen. Die Kleinste ist $m = 2 \times 73 \times 1103 = 161038$, sie wurde im Jahre 1950 von Lehmer entdeckt. Beeger zeigte 1951, dass es unendlich viele gerade Pseudoprimzahlen gibt, wobei jede mindestens zwei ungerade Primfaktoren besitzen muss.

Wie „weit entfernt“ sind Pseudoprimzahlen davon, prim zu sein? Das Resultat von Cipolla besagt, dass es Pseudoprimzahlen mit beliebig vielen Primfaktoren gibt. Dies ist nicht etwa die Ausnahme. Erdös bewies 1949, dass es für jedes $k \geq 2$ unendlich viele Pseudoprimzahlen gibt, die das Produkt von genau k verschiedenen Primfaktoren sind.

Lehmer gab 1936 Kriterien dafür an, wann ein Produkt von zwei bzw. drei verschiedenen Primzahlen pseudoprim ist: $p_1 p_2$ ist pseudoprim genau dann, wenn die Ordnung von 2 modulo p_2 Teiler von $p_1 - 1$ und die Ordnung von 2 modulo p_1 Teiler von $p_2 - 1$ ist. Für Pseudoprimzahlen $p_1 p_2 p_3$ gilt: Das kleinste gemeinsame Vielfache von $\mathrm{ord}(2 \bmod p_1)$ und $\mathrm{ord}(2 \bmod p_2)$ teilt $p_3(p_1 + p_2 - 1) - 1$.

Hier eine offene Frage: Gibt es unendlich viele ganze Zahlen $n > 1$ derart, dass $2^{n-1} \equiv 1 \pmod{n^2}$? Diese Frage ist jeweils äquivalent zu den folgenden Problemen (siehe Rotkiewicz, 1965):

Gibt es unendlich viele Pseudoprimzahlen, die Quadrate sind?

Gibt es unendlich viele Primzahlen p mit $2^{p-1} \equiv 1 \pmod{p^2}$?

Diese Kongruenz tauchte bereits im Zusammenhang mit quadratischen Faktoren von Fermat- und Mersenne-Zahlen auf. Im Abschnitt III von Kapitel 5 komme ich nochmal auf solche Primzahlen p zurück.

Andererseits muss eine Pseudoprimzahl nicht quadratfrei sein. Die kleinsten solcher Beispiele sind $1\,194\,649 = 1093^2$, $12\,327\,121 = 3511^2$, $3\,914\,864\,773 = 29 \times 113 \times 1093^2$.

B Pseudoprimzahlen zur Basis a (psp(a))

Es ist sinnvoll, die Kongruenz $a^{n-1} \equiv 1 \pmod{n}$ auch für $a > 2$ zu betrachten. Für eine Primzahl n und $1 < a < n$ ist diese Kongruenz notwendigerweise erfüllt. Das heißt, wenn beispielsweise $2^{n-1} \equiv 1 \pmod{n}$, aber $3^{n-1} \not\equiv 1 \pmod{n}$, dann ist n keine Primzahl.

Dies führt zur allgemeineren Untersuchung von *Pseudoprimzahlen zur Basis a* (oder *a-Pseudoprimzahlen*), also zerlegbaren Zahlen $n > a$, die $a^{n-1} \equiv 1 \pmod{n}$ genügen.

Cipolla zeigte 1904 auch, wie man a-Pseudoprimzahlen gewinnt. Es sei $a \geq 2$ und p eine beliebige ungerade Primzahl, die $a(a^2 - 1)$ nicht teilt. Sei

$$n_1 = \frac{a^p - 1}{a - 1}, \quad n_2 = \frac{a^p + 1}{a + 1}, \quad n = n_1 n_2;$$

dann sind n_1 und n_2 ungerade und n zerlegbar. Mit $n_1 \equiv 1 \pmod{2p}$ und $n_2 \equiv 1 \pmod{2p}$ gilt auch $n \equiv 1 \pmod{2p}$. Aus $a^{2p} \equiv 1 \pmod{n}$ folgt schließlich $a^{n-1} \equiv 1 \pmod{n}$, also ist n eine a-Pseudoprimzahl.

Aufgrund der Tatsache, dass es unendlich viele Primzahlen gibt, existieren auch unendlich viele a-Pseudoprimzahlen (auch für $a > 2$).

In der Literatur sind noch weitere Methoden zu finden, mit denen man wachsende Folgen von a-Pseudoprimzahlen schnell erzeugen kann.

Beispielsweise ging Crocker 1962 wie folgt vor: Es sei a gerade, habe aber nicht die Form 2^{2^r} mit $r \geq 0$. Dann ist für jedes $n \geq 1$ die Zahl $a^{a^n} + 1$ eine a-Pseudoprimzahl.

Steuerwald bildete im Jahre 1948 eine unendliche Folge a-pseudoprimer Zahlen auf diese Weise: Es sei n eine zu $a - 1$ teilerfremde a-Pseudoprimzahl. Beispielsweise setze man $a = q + 1$ für eine Primzahl q. Es sei weiter p eine Primzahl mit $p > a^2 - 1$; setze analog zur

Konstruktion von Cipolla,

$$n_1 = \frac{a^p - 1}{a - 1} \equiv a^{p-1} + a^{p-2} + \cdots + a + 1 \equiv p \pmod{q},$$
$$n_2 = \frac{a^p + 1}{a + 1} \equiv a^{p-1} - a^{p-2} + \cdots + a^2 - a + 1 \equiv 1 \pmod{q},$$

so dass $n = n_1 n_2 \equiv p \pmod{q}$. Sei nun $f(n) = (a^n - 1)/(a - 1) > n$. Dann ist auch $f(n)$ eine a-Pseudoprimzahl. Denn zunächst ist

$$f(n) = \frac{a^{n_1 n_2} - 1}{a^{n_2} - 1} \times \frac{a^{n_2} - 1}{a - 1}$$

zerlegbar. Und da n und $a - 1$ teilerfremd sind und $a^{n-1} \equiv 1 \pmod{n}$ gilt, ist $(a^n - a)/(a - 1) = f(n) - 1$ ein Vielfaches von n. Daher ist $f(n)$ Teiler von $a^n - 1$, das wiederum $a^{f(n)-1} - 1$ teilt, und somit ist $f(n)$ eine a-Pseudoprimzahl. Unter Beachtung der Tatsache, dass $f(n)$ und $a - 1$ teilerfremd sind, kann man diesen Prozess iterieren:

$$f(n) = \frac{\big[(a-1)+1\big]^n - 1}{a - 1} = (a-1)^{n-1} + \binom{n}{1}(a-1)^{n-2} + \cdots + \binom{n}{n-2}(a-1) + n \equiv n \pmod{a-1},$$

also ist $f(n)$ eine zu $a - 1$ teilerfremde a-Pseudoprimzahl.

Dieser Prozess führt zu einer unendlichen Folge von a-Pseudoprimzahlen

$$n < f(n) < f(f(n)) < f(f(f(n))) < \cdots,$$

die wie n, a^n, a^{a^n} $a^{a^{a^n}}, \ldots$ wächst. Die oben erwähnte Methode von Lehmer auf Binome $a^k - 1$ und $a^k + 1$ angewandt, erzeugt a-Pseudoprimzahlen, die aus zwei verschiedenen Primfaktoren bestehen.

Aufgrund dieser Überlegungen ist es zwecklos, die größte a-Pseudoprimzahl entdecken zu wollen.

Schinzel zeigte 1958, dass es für jedes $a \geq 2$ unendlich viele Pseudoprimzahlen zur Basis a gibt, die das Produkt von zwei verschiedenen Primzahlen sind.

In seiner Dissertation von 1971 erweiterte Lieuwens sowohl dieses Resultat von Schinzel, als auch das von Erdös über Pseudoprimzahlen zur Basis 2: Für jedes $k \geq 2$ und $a > 1$ gibt es unendlich viele Pseudoprimzahlen zur Basis a, die das Produkt von genau k verschiedenen Primzahlen sind.

Rotkiewicz zeigte 1972, dass wenn $p \geq 2$ eine Primzahl ist, die $a \geq 2$ nicht teilt, es unendlich viele Pseudoprimzahlen zur Basis a gibt, die

Vielfache von p sind. Der Spezialfall $p = 2$ geht auf das Jahr 1959 und ebenfalls Rotkiewicz zurück.

Es kann vorkommen, dass eine Zahl zu mehreren verschiedenen Basen pseudoprim ist, so wie 561 zu den Basen 2, 5 und 7. Baillie & Wagstaff sowie Monier bewiesen 1980 unabhängig voneinander den folgenden Satz: Es sei n zerlegbar und $B_{\mathrm{psp}}(n)$ die Anzahl der Basen a mit $1 < a < n$ und $\mathrm{ggT}(a, n) = 1$, für die n eine a-Pseudoprimzahl ist. Dann gilt

$$B_{\mathrm{psp}}(n) = \left\{ \prod_{p|n} \mathrm{ggT}(n-1, p-1) \right\} - 1.$$

Es folgt, dass eine zerlegbare ungerade Zahl n, die keine Kubikzahl ist, zu mindestens zwei Basen a mit $1 < a \leq n-1$ pseudoprim ist.

In Abschnitt IX wird gezeigt, dass es zerlegbare Zahlen n gibt, die zu allen Basen a mit $1 < a < n$ und $\mathrm{ggT}(a, n) = 1$ Pseudoprimzahlen sind.

Es folgt eine Tabelle aus dem Artikel von Pomerance, Selfridge & Wagstaff (1980), die die kleinsten Pseudoprimzahlen zu verschiedenen bzw. simultanen Basen angibt.

Tabelle 10. Kleinste Pseudoprimzahlen zu verschiedenen Basen

Basen	Kleinste psp
2	$341 = 11 \times 31$
3	$91 = 7 \times 13$
5	$217 = 7 \times 31$
7	$25 = 5 \times 5$
2, 3	$1105 = 5 \times 13 \times 17$
2, 5	$561 = 3 \times 11 \times 17$
2, 7	$561 = 3 \times 11 \times 17$
3, 5	$1541 = 23 \times 67$
3, 7	$703 = 19 \times 37$
5, 7	$561 = 3 \times 11 \times 17$
2, 3, 5	$1729 = 7 \times 13 \times 19$
2, 3, 7	$1105 = 5 \times 13 \times 17$
2, 5, 7	$561 = 3 \times 11 \times 17$
3, 5, 7	$29341 = 13 \times 37 \times 61$
2, 3, 5, 7	$29341 = 13 \times 37 \times 61$

Wie ich gesagt habe, ist n zerlegbar, wenn es ein a derart gibt, dass $1 < a < n$ und $a^{n-1} \not\equiv 1 \pmod{n}$, die Umkehrung gilt jedoch nicht. Damit steht eine praktische Methode zum Nachweis der Zerlegbarkeit vieler Zahlen zur Verfügung. Es gibt weitere, ähnliche Kongruenzeigenschaften, um festzustellen, dass bestimmte Zahlen zerlegbar sind.

Ich werde einige dieser Eigenschaften beschreiben, um zu weiteren Ergebnissen im Zusammenhang mit Primzahltests zu gelangen. Ohne es explizit zu sagen, habe ich diese in den Abschnitten III und V bereits behandelt. Zunächst wird es um Eigenschaften der Kongruenz $a^m \equiv 1 \pmod{n}$ gehen, die zu Euler-a-Pseudoprimzahlen und starken a-Pseudoprimzahlen führen. In einem weiteren Abschnitt werde ich die Lucas-Pseudoprimzahlen betrachten. Diese beziehen sich auf Kongruenzeigenschaften, die von Termen der Lucas-Folgen erfüllt sind.

C Euler-Pseudoprimzahlen zur Basis a (epsp(a))

Gemäß Eulers Kongruenz für das Legendre-Symbol gilt

$$\left(\frac{a}{p}\right) \equiv a^{(p-1)/2} \pmod{p},$$

wenn $a \geq 2$ und p eine Primzahl ist, die a nicht teilt. Dies führt zum Begriff der *Euler-Pseudoprimzahl zur Basis* a (epsp(a)), vorgeschlagen von Shanks im Jahre 1962. epsp(a) sind ungerade zerlegbare Zahlen n derart, dass $\mathrm{ggT}(a, n) = 1$ und das Jacobi-Symbol die Kongruenz

$$\left(\frac{a}{n}\right) \equiv a^{(n-1)/2} \pmod{n}$$

erfüllt. Offensichtlich ist jede epsp(a) auch a-pseudoprim.

Es gibt viele naheliegende Fragen im Zusammenhang mit epsp(a), die ich nun aufzählen möchte:

(e1) Gibt es für jedes a unendlich viele epsp(a)?

(e2) Gibt es für jedes a eine epsp(a) mit einer beliebig großen Anzahl verschiedener Primfaktoren?

(e3) Gibt es für jedes $k \geq 2$ und jede Basis a unendlich viele epsp(a), die ein Produkt von genau k verschiedenen Primfaktoren sind?

(e4) Kann eine ungerade zerlegbare Zahl n eine epsp(a) für jedes mögliche a mit $1 < a < n$ und $\mathrm{ggT}(a, n) = 1$ sein?

(e5) Für wie viele Basen a mit $1 < a < n$ und $\mathrm{ggT}(a, n) = 1$ kann die Zahl n eine epsp(a) sein?

Kiss, Phong & Lieuwens zeigten 1986, dass es zu gegebenen $a \geq 2$, $k \geq 2$ und $d \geq 2$ unendlich viele epsp(a) gibt, die ein Produkt von k verschiedenen Primzahlen und kongruent zu 1 modulo d sind.

Diese klare Antwort auf (e3) beantwortet zugleich (e2) und (e1).

Lehmer zeigte 1976, dass eine ungerade zerlegbare Zahl n nicht für alle a mit $1 < a < n$ und $\mathrm{ggT}(a, n) = 1$ eine epsp(a) sein kann, was Frage (e4) negativ beantwortet.

Es gilt sogar mehr, wie von Solovay & Strassen 1977 gezeigt wurde: Eine zerlegbare Zahl n kann zu höchstens $\frac{1}{2}\varphi(n)$ Basen a mit $1 < a < n$ und $\mathrm{ggT}(a, n) = 1$ eine Euler-Pseudoprimzahl sein, was Frage (e5) beantwortet. Der Beweis folgt unmittelbar, wenn man beachtet, dass die Restklassen a mod n, für die $(a \,|\, n) \equiv a^{(n-1)/2} \pmod{n}$ gilt, eine Untergruppe von $\left(\mathbb{Z}/n\right)^{\times}$ bilden (Gruppe der invertierbaren Restklassen modulo n), diese ist nach Lehmer eine echte Untergruppe und hat daher nach dem guten alten Satz von Lagrange höchstens $\frac{1}{2}\varphi(n)$ Elemente.

Es sei n eine ungerade zerlegbare Zahl und es bezeichne $B_{\mathrm{epsp}}(n)$ die Anzahl der Basen a mit $1 < a < n$ und $\mathrm{ggT}(a, n) = 1$, so dass n eine epsp(a) ist. Monier zeigte 1980, dass

$$B_{\mathrm{epsp}}(n) = \delta(n) \prod_{p|n} \mathrm{ggT}\left(\frac{n-1}{2}, p-1\right) - 1.$$

Dabei ist

$$\delta(n) = \begin{cases} 2 & \text{falls } v_2(n) - 1 = \min\limits_{p|n}\{v_2(p-1)\}, \\ \frac{1}{2} & \text{falls es einen Primteiler } p \text{ von } n \text{ derart gibt, dass} \\ & v_p(n) \text{ ungerade ist und } v_2(p-1) < v_2(n-1) \text{ gilt}, \\ 1 & \text{sonst}, \end{cases}$$

und für jede Zahl m und primes p bezeichnet $v_p(m)$ den Exponenten von p in der Primfaktorenzerlegung von m, das heißt, den p-adischen Wert von m.

D Starke Pseudoprimzahlen zur Basis a (spsp(a))

Eine verwandte Eigenschaft ist die Folgende: Es sei n eine ungerade zerlegbare Zahl, $n - 1 = 2^s d$ mit ungeradem d und $s \geq 1$, sowie a dergestalt, dass $1 < a < n$ und $\mathrm{ggT}(a, n) = 1$.

Dann heißt n *starke Pseudoprimzahl zur Basis* a (spsp(a)), wenn gilt $a^d \equiv 1 \pmod{n}$ oder $a^{2^r d} \equiv -1 \pmod{n}$ für ein r, $0 \leq r < s$.

Primzahlen n erfüllen diese Bedingung für alle a mit $1 < a < n$ und $\mathrm{ggT}(a, n) = 1$.

Selfridge zeigte (siehe den Beweis in Williams' Artikel, 1978), dass jede spsp(a) auch eine epsp(a) ist. Es gibt partielle Umkehrungen.

Nach Malm (1977): Eine epsp(a) n, die $n \equiv 3 \pmod{4}$ erfüllt, ist auch eine spsp(a).

Nach Pomerance, Selfridge & Wagstaff (1980): Eine ungerade epsp(a) n mit $(a \mid n) = -1$ ist zugleich eine spsp(a). Insbesondere ist eine epsp(2) n eine spsp(2), wenn $n \equiv 5 \pmod{8}$ gilt.

Hinsichtlich der starken Pseudoprimzahlen könnte man sich Fragen (s1)–(s5) stellen, analog derer zu den Euler-Pseudoprimzahlen aus Abschnitt VIII, C.

Pomerance, Selfridge & Wagstaff bewiesen 1980, dass es für jede Basis $a > 1$ unendlich viele spsp(a) gibt, was zugleich (s1) und (e1) positiv beantwortet. Ich werde darauf bei der Untersuchung der Verteilung der Pseudoprimzahlen (Kapitel 4, Abschnitt VI) noch genauer eingehen.

Zur Basis 2 kann man unendlich viele spsp(2) explizit angeben: Wenn n eine psp(2) ist, dann ist $2^n - 1$ eine spsp(2). Da es unendlich viele psp(2) gibt, erhält man damit unendlich viele spsp(2), unter denen sich sämtliche zerlegbaren Mersenne-Zahlen befinden. Man kann sich auch leicht überlegen, dass jede zerlegbare Fermat-Zahl eine spsp(2) ist.

Auch (s2) und (e2) lassen sich auf ähnliche Weise bejahend beantworten, denn es gibt Pseudoprimzahlen mit beliebig vielen verschiedenen Primfaktoren; man beachte dazu nur, dass wenn $p_1, p_2, \ldots, p_k$ die Pseudoprimzahl n teilen, $2^{p_i} - 1$ $(i = 1, \ldots, k)$ Teiler der spsp(2) $2^n - 1$ sind.

Aufgrund von Lehmers negativer Antwort auf (e4) und des Resultats von Selfridge ist (s4) offensichtlich auch zu verneinen. Wie später im Zusammenhang mit dem Monte-Carlo-Primzahltest offensichtlich wird, ist der folgende Satz von Rabin überaus wichtig. Er stellt ein Analogon zu Solovay & Strassens Ergebnis für Euler-Pseudoprimzahlen dar und ist nicht ganz einfach zu beweisen:

Falls $n > 4$ zerlegbar ist, dann gibt es mindestens $3(n-1)/4$ Zahlen a, $1 < a < n$, für die n keine spsp(a) ist. Anders ausgedrückt ist die Anzahl der Basen a mit $1 < a < n$ und $\mathrm{ggT}(a, n) = 1$, für die eine

zerlegbare Zahl eine spsp(a) sein kann, höchstens gleich $(n-1)/4$. Dies beantwortet Frage (s5).

Monier (1980) ermittelte auch eine Formel für die Anzahl $B_{\mathrm{spsp}}(n)$ der Basen a mit $1 < a < n$ und $\mathrm{ggT}(a,n) = 1$, für die die ungerade zerlegbare Zahl n eine spsp(a) ist. Nämlich:

$$B_{\mathrm{spsp}}(n) = \left(1 + \frac{2^{\omega(n)\nu(n)} - 1}{2^{\omega(n)} - 1}\right)\left(\prod_{p|n} \mathrm{ggT}(n^*, p^*)\right) - 1,$$

wobei

$$\begin{aligned}
\omega(n) &= \text{ Anzahl der verschiedenen Primfaktoren von } n,\\
\nu(n) &= \min_{p|n} \big\{v_2(p-1)\big\},\\
v_p(m) &= \text{ Exponent von } p \text{ in der Primfaktorenzerlegung von } m\\
&\quad\ \text{(eine beliebige natürliche Zahl)},\\
m^* &= \text{ größter ungerader Teiler von } m-1.
\end{aligned}$$

Nur um den Rekord nicht unerwähnt zu lassen: Die kleinste spsp(2) ist $2047 = 23 \times 89$. Es ist nicht nur interessant, sondern auch nützlich, die kleinste Zahl zu kennen, die gleichzeitig zu mehreren Basen eine starke Pseudoprimzahl ist, denn dieses Wissen kann einen strikten Primzahltest ermöglichen.

Für gegebenes $k \geq 1$ bezeichne t_k die kleinste Zahl, die gleichzeitig zu den Basen $p_1 = 2$, $p_2 = 3$, …, p_k stark pseudoprim ist. Dann liefern die Berechnungen von Pomerance, Selfridge & Wagstaff (1980), erweitert von Jaeschke (1993), die folgenden Werte:

$$\begin{aligned}
t_2 &= 1\,373\,653 = 829 \times 1657,\\
t_3 &= 25\,326\,001 = 2251 \times 11251,\\
t_4 &= 3\,215\,031\,751 = 151 \times 751 \times 28351,\\
t_5 &= 2\,152\,302\,898\,747 = 6763 \times 10627 \times 29947,\\
t_6 &= 3\,474\,749\,660\,383 = 1303 \times 16927 \times 157543,\\
t_7 &= t_8 = 341\,550\,071\,728\,321 = 10670053 \times 32010157.
\end{aligned}$$

Darüber hinaus gab Jaeschke obere Schranken für t_9, t_{10} und t_{11} an, die von Zhang (2001) und von Zhang & Tang (2003) wie folgt verbessert wurden:

$$t_9 \leq t_{10} \leq t_{11} \leq 3\,825\,123\,056\,546\,413\,051 = 149491 \times 747451 \times 34233211.$$

Die letzteren Autoren sprechen zudem die begründete Vermutung aus, dass in allen drei Fällen die Gleichheit gilt.

Jaeschkes Arbeit zeigte auch, dass es nur 101 Zahlen unterhalb von 10^{12} gibt, die gleichzeitig zu den Basen 2, 3 und 5 stark pseudoprim sind. Die vollständige Liste ist recht groß, daher sei hier nur der Teil angegeben, der von den drei Rittern der Numerologie veröffentlicht wurde. Dieser beschränkt sich auf Zahlen kleiner als 25×10^9.

Tabelle 11.

Zahlen kleiner als 25×10^9, die spsp zu den Basen 2, 3, 5 sind

	psp zur Basis			
Zahl	7	11	13	Faktorisierung
25 326 001	–	–	–	2251×11251
161 304 001	–	spsp	–	7333×21997
960 946 321	–	–	–	11717×82013
1 157 839 381	–	–	–	24061×48121
3 215 031 751	spsp	psp	psp	$151 \times 751 \times 28351$
3 697 278 427	–	–	–	30403×121609
5 764 643 587	–	–	spsp	37963×151849
6 770 862 367	–	–	–	41143×164569
14 386 156 093	psp	psp	psp	$397 \times 4357 \times 8317$
15 579 919 981	psp	spsp	–	88261×176521
18 459 366 157	–	–	–	67933×271729
19 887 974 881	psp	–	–	81421×244261
21 276 028 621	–	psp	psp	103141×206281

Dieser Tabelle füge ich die Liste der nicht quadratfreien Pseudoprimzahlen bis 25×10^9 sowie deren Faktorisierung hinzu:

$$\begin{aligned} 1\,194\,649 &= 1093^2, \\ 12\,327\,121 &= 3511^2, \\ 3\,914\,864\,773 &= 29 \times 113 \times 1093^2, \\ 5\,654\,273\,717 &= 1093^2 \times 4733, \\ 6\,523\,978\,189 &= 43 \times 127 \times 1093^2, \\ 22\,178\,658\,685 &= 5 \times 47 \times 79 \times 1093^2. \end{aligned}$$

Mit Ausnahme der letzten beiden sind alle Zahlen der Liste starke Pseudoprimzahlen.

Man beachte, dass die einzigen Primfaktoren, die im Quadrat vorkommen, 1093 und 3511 sind. Das Auftreten dieser Zahlen wird in Kapitel 5, Abschnitt III erklärt werden.

IX Carmichael-Zahlen

In einem kurzen Artikel, der weitgehend unbeachtet blieb, betrachtete Korselt 1899 eine eher seltene Art von Zahlen; unabhängig wurden diese von Carmichael 1912 eingeführt, der ihre Eigenschaften als Erster studierte. Seit Bekanntwerden seines Artikels werden diese Zahlen *Carmichael-Zahlen* genannt. Nach Definition sind dies zerlegbare Zahlen n mit der Eigenschaft, dass $a^{n-1} \equiv 1 \pmod{n}$ für jede Zahl a mit $1 < a < n$ und $\mathrm{ggT}(a, n) = 1$ erfüllt ist. Die kleinste Carmichael-Zahl ist $561 = 3 \times 11 \times 17$.

Ich werde nun eine Charakterisierung der Carmichael-Zahlen angeben. Man erinnere sich, dass ich in Abschnitt II die Carmichael-Funktion $\lambda(n)$ eingeführt habe, die das Maximum der Ordnungen von $a \bmod n$ für $1 \leq a < n$ und $\mathrm{ggT}(a, n) = 1$ angibt; insbesondere ist $\lambda(n)$ Teiler von $\varphi(n)$.

Carmichael zeigte, dass n genau dann eine Carmichael-Zahl ist, wenn n zerlegbar und $\lambda(n)$ Teiler von $n - 1$ ist (was der Aussage entspricht, dass wenn p ein beliebiger Primteiler von n ist, dann $p - 1$ auch $n - 1$ teilt).

Es folgt, dass jede Carmichael-Zahl ungerade und das Produkt von mindestens drei verschiedenen Primzahlen ist.

Genauer: Wenn $n = p_1 p_2 \cdots p_r$ (Produkt verschiedener Primzahlen), dann ist n genau dann eine Carmichael-Zahl, wenn $p_i - 1$ Teiler von $(n/p_i) - 1$ ist (für alle $i = 1, 2, \ldots, r$). Daher gilt $a^n \equiv a \pmod{n}$ für jede Carmichael-Zahl n und jedes $a \geq 1$.

Schinzel bemerkte 1959, dass für jedes $a \geq 2$ die kleinste pseudoprime Zahl m_a zur Basis a notwendigerweise $m_a \leq 561$ erfüllt. Ferner gibt es ein a, so dass $m_a = 561$. Ausführlich ausgedrückt seien p_i $(i = 1, \ldots, s)$ die Primzahlen $2 < p_i < 561$; für jedes p_i sei e_i der Exponent, für den $p_i^{e_i} < 561 < p_i^{e_i+1}$ gilt. Sei g_i eine Primitivwurzel modulo $p_i^{e_i}$, und nach dem chinesischen Restsatz sei a diejenige Zahl, für die $a \equiv 3 \pmod{4}$ und $a \equiv g_i \pmod{p_i^{e_i}}$ für $i = 1, \ldots, s$. Dann gilt $m_a = 561$.

Carmichael und Lehmer bestimmten die kleinsten Carmichael-Zahlen:

$561 = 3 \times 11 \times 17$	$15841 = 7 \times 31 \times 73$	$101101 = 7 \times 11 \times 13 \times 101$
$1105 = 5 \times 13 \times 17$	$29341 = 13 \times 37 \times 61$	$115921 = 13 \times 37 \times 241$
$1729 = 7 \times 13 \times 19$	$41041 = 7 \times 11 \times 13 \times 41$	$126217 = 7 \times 13 \times 19 \times 73$
$2465 = 5 \times 17 \times 29$	$46657 = 13 \times 37 \times 97$	$162401 = 17 \times 41 \times 233$
$2821 = 7 \times 13 \times 31$	$52633 = 7 \times 73 \times 103$	$172081 = 7 \times 13 \times 31 \times 61$
$6601 = 7 \times 23 \times 41$	$62745 = 3 \times 5 \times 47 \times 89$	$188461 = 7 \times 13 \times 19 \times 109$
$8911 = 7 \times 19 \times 67$	$63973 = 7 \times 13 \times 19 \times 37$	$252601 = 41 \times 61 \times 101$
$10585 = 5 \times 29 \times 73$	$75361 = 11 \times 13 \times 17 \times 31$	

Ich werde nun die folgenden, natürlich nahe miteinander verwandten Fragen betrachten:

(1) Gibt es unendlich viele Carmichael-Zahlen?

(2) Gibt es für gegebenes $k \geq 3$ unendlich viele Carmichael-Zahlen mit genau k Primfaktoren?

Das erste Problem wurde 1992 in einem brillanten Artikel von Alford, Granville & Pomerance mit einer positiven Antwort gelöst; der Artikel erschien 1994, siehe auch den Übersichtsartikel von Pomerance (1993).

Man glaubt, dass auch die zweite Frage zu bejahen ist, dies muss allerdings noch bewiesen werden. Es ist beispielsweise noch nicht einmal bekannt, ob es unendlich viele Carmichael-Zahlen gibt, die Produkte von genau drei Primfaktoren sind. In diesem Zusammenhang gibt es ein Ergebnis von Duparc (1952) (siehe auch Beeger, 1950):

Für jedes $r \geq 3$ gibt es nur endlich viele Carmichael-Zahlen mit r Primfaktoren, von denen $r - 2$ vorgegeben sind. Auf diese Fragen werde ich noch einmal in Kapitel 4 zurückkommen.

Chernick gab 1939 die folgende Methode an, um Carmichael-Zahlen zu erzeugen. Es sei $m \geq 1$ und

$$M_3(m) = (6m + 1)(12m + 1)(18m + 1).$$

Falls m die Eigenschaft hat, dass alle drei Faktoren Primzahlen sind, dann ist $M_3(m)$ eine Carmichael-Zahl. Dies ergibt zwar Carmichael-Zahlen mit drei Primfaktoren, allerdings weiß man natürlich nicht, ob es unendlich viele Zahlen m mit der geforderten Eigenschaft gibt.

In der gleichen Weise sei für $k \geq 4$ und $m \geq 1$

$$M_k(m) = (6m + 1)(12m + 1) \prod_{i=1}^{k-2} (9 \times 2^i m + 1).$$

Falls m die Eigenschaft hat, dass alle k Faktoren prim sind und außerdem m von 2^{k-4} geteilt wird, dann ist $M_k(m)$ eine Carmichael-Zahl mit k Primfaktoren.

Diese Methode und Varianten davon wurden dazu verwendet, große Carmichael-Zahlen sowie Carmichael-Zahlen mit großen Primfaktoren zu erzeugen.

Es seien erwähnt: Wagstaff 1980 (321 Stellen), Atkin 1980 (370 Stellen), Woods & Huenemann 1982 (432 Stellen), Dubner 1985 (1057 Stellen) und Dubner 1989 (3710 Stellen).

Alle diese Beispiele bestehen nur aus wenigen Primfaktoren. Yorinaga (1978) fand Carmichael-Zahlen mit bis zu 15 Primfaktoren.

Die Suche nach großen Carmichael-Zahlen mit vielen Primfaktoren ging weiter. Löh & Niebuhr konstruierten 1994 (veröffentlicht 1996) eine Carmichael-Zahl mit 16142049 Stellen und 1101518 Primfaktoren.

Rekord

Die größte bekannte Carmichael-Zahl wurde 1998 von W.R. Alford und J. Grantham entdeckt; sie hat 20163700 Stellen und 1371497 Primfaktoren. Diese Zahl hat außerdem die folgende Eigenschaft: Für jedes k mit $62 \leq k \leq 1371435$ wird sie von einer Carmichael-Zahl mit genau k Primfaktoren geteilt.

Dieser unveröffentlichte Rekord wurde mir freundlicherweise von den Autoren mitgeteilt.

Durch ein tieferes Verständnis dieser Art von Berechnungen gelang es Alford, Granville & Pomerance (1994), die alte Vermutung über die Existenz unendlich vieler Carmichael-Zahlen zu bestätigen.

Was die Berechnung von Carmichael-Zahlen betrifft, so erstellte Pinch 2007 eine vollständige Liste dieser Zahlen bis 10^{21}. Ich werde die Ergebnisse seiner Berechnungen in Kapitel 4, Abschnitt VI, B besprechen.

Die Verteilung von Carmichael-Zahlen wird in Kapitel 4, Abschnitt VIII untersucht.

Anhang zu Knödel-Zahlen

Für jedes $k \geq 1$ bezeichne C_k die Menge aller zerlegbaren Zahlen $n > k$ derart, dass für $1 < a < n$ und $\mathrm{ggT}(a, n) = 1$ die Kongruenz $a^{n-k} \equiv 1 \pmod{n}$ erfüllt ist.

Folglich ist C_1 die Menge der Carmichael-Zahlen. Knödel untersuchte 1953 die Mengen C_k für $k \geq 2$. Schon vor dem Beweis der Existenz unendlich vieler Carmichael-Zahlen zeigte Mąkowski im Jahre 1962:

Für jedes $k \geq 2$ ist C_k eine unendliche Menge.

Beweis. Für jedes a mit $1 < a < k$ und $\mathrm{ggT}(a,k) = 1$ sei r_a die Ordnung von a modulo k. Sei $r = \prod r_a$ (Produkt über alle wie oben definierten a). Also gilt $a^r \equiv 1 \pmod{k}$.

Es gibt unendlich viele Primzahlen p mit der Eigenschaft, dass $p \equiv 1 \pmod{r}$; in Kapitel 4, Abschnitt IV befindet sich ein Beweis dieses sehr nützlichen Satzes. Für jedes solche $p > k$ setze man $p - 1 = hr$ und $n = kp$. Dann gilt $n \in C_k$.

Denn sei $1 \leq a < n$ und $\mathrm{ggT}(a,n) = 1$, also $\mathrm{ggT}(a,k) = 1$, und daher

$$\begin{aligned} a^{n-k} &= a^{k(p-1)} = a^{khr} \equiv 1 \pmod{k}, \\ a^{n-k} &= a^{k(p-1)} \equiv 1 \pmod{p}. \end{aligned}$$

Wegen $p \nmid k$ gilt $a^{n-k} \equiv 1 \pmod{n}$, und somit liegt $n = kp$ in C_k. □

Aus obigem Beweis folgt für $k = 2$, dass $2p \in C_2$ für jede Primzahl $p > 2$. Falls $k = 3$, dann $3p \in C_3$ für jedes prime $p > 3$; letztere Aussage wurde von Morrow 1951 bewiesen.

X Lucas-Pseudoprimzahlen

In Hinblick auf die Analogie zwischen Folgen von Binomen $a^n - 1$ ($n \geq 1$) und Lucas-Folgen ist es nicht überraschend, dass es für Pseudoprimzahlen ein Pendant gibt, das mit Lucas-Folgen in Zusammenhang steht. Für jeden Parameter $a \geq 2$ gab es die a-Pseudoprimzahlen sowie ihre Kollegen, die Euler- und starken Pseudoprimzahlen zur Basis a.

In diesem Abschnitt werden allen Paaren (P,Q) von ganzen Zahlen ungleich Null die korrespondierenden Lucas-, Euler-Lucas- und starken Lucas-Pseudoprimzahlen zugeordnet. Ihre Verwendung wird derjenigen der Pseudoprimzahlen entsprechen.

Es seien P und Q ganze Zahlen ungleich Null, $D = P^2 - 4Q$, und seien $(U_n)_{n\geq 0}$ und $(V_n)_{n\geq 0}$ die zugehörigen Lucas-Folgen.

Man rufe sich nochmals die folgenden Aussagen (aus Abschnitt IV) über eine ungerade Primzahl n in Erinnerung:

(X.1) Wenn $\mathrm{ggT}(n, D) = 1$, dann $U_{n-(D\,|\,n)} \equiv 0 \pmod{n}$.

(X.2) $U_n \equiv (D\,|\,n) \pmod{n}$.

(X.3) $V_n \equiv P \pmod{n}$.

(X.4) Wenn $\mathrm{ggT}(n, D) = 1$, dann $V_{n-(D\,|\,n)} \equiv 2Q^{(1-(D|n))/2} \pmod{n}$.

Eine ungerade, zerlegbare Zahl n, die Kongruenz (X.1) erfüllt, heißt *Lucas-Pseudoprimzahl* (mit Parametern (P, Q)), abgekürzt $\mathrm{lpsp}(P, Q)$.

Eine solche Definition ist legitim, aber existieren solche Zahlen überhaupt? Und falls ja, lohnt es sich, sie zu studieren?

A Fibonacci-Pseudoprimzahlen

Zunächst einmal ist es interessant, den Spezialfall der Fibonacci-Zahlen zu betrachten, wenn $P = 1$, $Q = -1$ und $D = 5$. In dieser Situation ist es eher angebracht, die $\mathrm{lpsp}(1, -1)$ *Fibonacci-Pseudoprimzahlen* zu nennen.

Die kleinsten Fibonacci-Pseudoprimzahlen sind $323 = 17 \times 19$ und $377 = 13 \times 29$; tatsächlich gilt $(5\,|\,323) = (5\,|\,377) = -1$, und man kann ausrechnen, dass $U_{324} \equiv 0 \pmod{323}$ und $U_{378} \equiv 0 \pmod{377}$.

E. Lehmer zeigte 1964, dass es unendlich viele Fibonacci-Pseudoprimzahlen gibt. Genauer, falls p eine beliebige Primzahl größer als 5 ist, dann ist U_{2p} eine Fibonacci-Pseudoprimzahl.

Eigenschaft (X.2) wurde 1970 von Parberry und später von Yorinaga (1976) untersucht.

Unter anderem zeigte Parberry: Wenn $\mathrm{ggT}(h, 30) = 1$ und wenn h die Bedingung (X.2) erfüllt, dann ist sie auch für $k = U_h$ erfüllt; darüber hinaus ist $\mathrm{ggT}(k, 30) = 1$ und wenn h zerlegbar ist, gilt dies offenbar auch für U_h. Dies zeigt, dass die Existenz nur einer einzigen zerlegbaren Fibonacci-Zahl U_n mit $U_n \equiv (5\,|\,n) \pmod{n}$ gleich die Existenz unendlich vieler solcher Zahlen zur Folge hat. Wie ich (in Kürze) erläutern werde, gibt es solche Fibonacci-Zahlen tatsächlich.

Eigentlich folgt dies auch aus einem anderen Resultat von Parberry: Wenn p prim ist und $p \equiv 1$ oder $4 \pmod{15}$ gilt, dann ist $n = U_{2p}$ ungerade und zerlegbar und erfüllt sowohl Bedingung (X.1) als auch (X.2). Insbesondere gibt es unendlich viele Fibonacci-Pseudoprimzahlen, die auch (X.2) erfüllen. (Hierbei verwende ich die in Kapitel 4, Abschnitt IV beschriebene Tatsache, dass es unendlich viele Primzahlen p derart gibt, dass $p \equiv 1 \pmod{15}$, bzw. $p \equiv 4 \pmod{15}$.)

Falls $p \not\equiv 1$ oder 4 (mod 15), dann ist (X.2) nicht erfüllt, was aus verschiedenen, in Abschnitt IV angegebenen Teilbarkeitseigenschaften und Kongruenzen folgt.

Yorinaga betrachtete den primitiven Teil der Fibonacci-Zahl U_n. Falls Sie sich erinnern, hatte ich in Abschnitt IV darauf hingewiesen, dass jede Fibonacci-Zahl U_n (mit $n \neq 1, 2, 6, 12$) einen primitiven Primfaktor p besitzt; dies sind diejenigen Primzahlen, die U_n, aber für keinen nichttrivialen Teiler d von n die Zahl U_d teilen. Daher $U_n = U_n^* \times U_n'$, wobei $\mathrm{ggT}(U_n^*, U_n') = 1$ und p Teiler von U_n^* genau dann ist, wenn p ein primitiver Primfaktor von U_n ist.

Yorinaga zeigte: Wenn m Teiler von U_n^* (mit $n > 5$) ist, dann gilt $U_m \equiv (5 \,|\, m) \pmod{m}$.

Gemäß dem in Abschnitt IV besprochenen Resultat von Schinzel (1963) gibt es unendlich viele ganze Zahlen n derart, dass U_n^* keine Primzahl ist. Daher hat das Ergebnis von Yorinaga zur Folge, dass es unendlich viele ungerade zerlegbare Zahlen n gibt, die der Kongruenz (X.2) genügen.

Yorinaga veröffentlichte eine Tabelle aller 109 zerlegbaren Zahlen n bis 707000, die $U_n \equiv (5 \,|\, n) \pmod{n}$ erfüllen. Unter diesen befinden sich einige Fibonacci-Pseudoprimzahlen, wie etwa $n = 4181 = 37 \times 113$, $n = 5777 = 53 \times 109$ und viele mehr. Vier der Zahlen aus der Tabelle sind zur Basis 2 pseudoprim:

$$\begin{aligned} 219781 &= 271 \times 811, \\ 252601 &= 41 \times 61 \times 101, \\ 399001 &= 31 \times 61 \times 211, \\ 512461 &= 31 \times 61 \times 271. \end{aligned}$$

Ein weiteres Resultat von Parberry, das später von Baillie & Wagstaff verallgemeinert wurde, ist das Folgende:

Falls n eine ungerade zerlegbare Zahl ist, die nicht durch 5 teilbar ist, aber den Kongruenzen (X.1) und (X.2) genügt, dann gilt

$$\begin{cases} U_{(n-(5|n))/2} \equiv 0 \pmod{n} & \text{falls} \quad n \equiv 1 \pmod 4, \\ V_{(n-(5|n))/2} \equiv 0 \pmod{n} & \text{falls} \quad n \equiv 3 \pmod 4. \end{cases}$$

Insbesondere existieren unendlich viele ungerade zerlegbare Zahlen n, welche die Kongruenz $U_{(n-(5\,|\,n))/2} \equiv 0 \pmod{n}$ erfüllen, denn es gibt unendlich viele zerlegbare Zahlen n mit $n \equiv 1 \pmod 4$.

Auch die zerlegbaren Zahlen n mit $V_n \equiv 1 \pmod{n}$ (wobei $(V_k)_{k\geq 0}$ die Folge der Lucas-Zahlen ist) wurden untersucht. Sie wurden *Lucas-*

Pseudoprimzahlen genannt, doch hier wird dieser Bezeichnung eine andere Bedeutung gegeben.

Singmaster fand 1983 die folgenden 25 zerlegbaren Zahlen $n < 10^5$ mit obiger Eigenschaft:

$$705,\ 2465,\ 2737,\ 3745,\ 4181,\ 5777,\ 6721,$$
$$10877,\ 13201,\ 15251,\ 24465,\ 29281,\ 34561,$$
$$35785,\ 51841,\ 54705,\ 64079,\ 64681,\ 67861,$$
$$68251,\ 75077,\ 80189,\ 90061,\ 96049,\ 97921.$$

B Lucas-Pseudoprimzahlen (lpsp(P,Q))

Ich werde nun lpsp(P,Q) behandeln, die zu beliebigen Paaren (P,Q) gehören. Um der Analogie zu den Pseudoprimzahlen zur Basis a Ausdruck zu verleihen, sollte die Diskussion denselben Weg gehen. Allerdings wird sich zeigen, dass über die nun betrachteten Zahlen viel weniger bekannt ist. Beispielsweise ist für gegebenes P und Q kein Algorithmus zur Generierung unendlich vieler lpsp(P,Q) bekannt, abgesehen von den im Zusammenhang mit den Fibonacci-Pseudoprimzahlen erwähnten Ergebnissen.

Allerdings legt Lieuwens in seiner Dissertation 1971 dar, dass es für jedes $k \geq 2$ und gegebenen Parametern (P,Q) unendlich viele Lucas-Pseudoprimzahlen gibt, die das Produkt von genau k verschiedenen Primzahlen sind.

Es ist für eine ungerade Zahl n durchaus normal, eine Lucas-Pseudoprimzahl zu vielen verschiedenen Parameterkombinationen zu sein. Es sei $D \equiv 0$ oder $1 \pmod 4$ und $B_{\mathrm{lpsp}}(n,D)$ bezeichne die Anzahl der Zahlen P, $1 \leq P \leq n$, so dass es ein Q mit $P^2 - 4Q \equiv D \pmod n$ gibt und n eine lpsp(P,Q) ist. Baillie & Wagstaff zeigten 1980, dass

$$B_{\mathrm{lpsp}}(n,D) = \prod_{p|n} \left\{ \mathrm{ggT}\left(n - \left(\frac{D}{n}\right),\ p - \left(\frac{D}{p}\right)\right) - 1 \right\}.$$

Insbesondere gibt es für ungerades, zerlegbares n ein D und dementsprechend mindestens drei Paare (P,Q) mit $P^2 - 4Q = D$ und verschiedenen Werten von P modulo n derart, dass n eine lpsp(P,Q) ist.

Eine weitere Frage stellt sich wie folgt: Falls n ungerade ist, für wie viele verschiedene D modulo n gibt es (P,Q) mit $P^2 - 4Q \equiv D \pmod n$, $P \not\equiv 0 \pmod n$ derart, dass n eine lpsp(P,Q) ist? Baillie & Wagstaff behandelten diesen Punkt auch für den Fall $n = p_1 p_2$, wobei p_1, p_2 verschiedene Primzahlen sind.

C Euler-Lucas-Pseudoprimzahlen (elpsp(P,Q)) und starke Lucas-Pseudoprimzahlen (slpsp(P,Q))

Es seien P, Q gegeben, $D = P^2 - 4Q$ wie zuvor und n eine ungerade Primzahl. In Abschnitt V wurde gezeigt, dass mit $\mathrm{ggT}(n, QD) = 1$ gilt:

$$\text{(el)} \quad \begin{cases} U_{(n-(D\mid n))/2} \equiv 0 \pmod{n}, & \text{falls } (Q \mid n) = 1, \\ V_{(n-(D\mid n))/2} \equiv D \pmod{n}, & \text{falls } (Q \mid n) = -1. \end{cases}$$

Dies führt zur folgenden Definition. Eine ungerade zerlegbare Zahl n mit $\mathrm{ggT}(n, QD) = 1$, die die obige Bedingung erfüllt, heißt *Euler–Lucas-Primzahl* mit Parametern (P, Q), abgekürzt elpsp(P, Q).

Es sei n eine ungerade zerlegbare Zahl mit $\mathrm{ggT}(n, D) = 1$ und $n - (D \mid n) = 2^s d$, d ungerade, $s \geq 0$. Falls

$$\text{(sl)} \quad \begin{cases} U_d \equiv 0 \pmod{n}, & \text{oder} \\ V_{2^r d} \equiv 0 \pmod{n} & \text{für ein } r,\ 0 \leq r < s \end{cases}$$

gilt, dann heißt n eine *starke Lucas-Pseudoprimzahl* mit Parametern (P, Q), kurz slpsp(P, Q). In diesem Fall gilt $\mathrm{ggT}(n, Q) = 1$ notwendigerweise.

Eine ungerade Primzahl n mit $\mathrm{ggT}(n, QD) = 1$ erfüllt die Kongruenzen (el) und (sl). Offensichtlich ist eine elpsp(P, Q) mit $\mathrm{ggT}(n, Q) = 1$ auch eine lpsp(P, Q).

In welchem Zusammenhang stehen elpsp(P, Q) und slpsp(P, Q)? Genau wie im Falle der Euler- und starken Pseudoprimzahlen zur Basis a zeigten Baillie & Wagstaff, dass eine slpsp(P, Q) – analog zum Resultat von Selfridge – auch eine elpsp(P, Q) ist.

Umgekehrt gilt: Ist n eine elpsp(P, Q), die zusätzlich $(Q \mid n) = -1$ oder $n - (D \mid n) \equiv 2 \pmod 4$ erfüllt, dann ist n auch eine slpsp(P, Q); dies ist das Gegenstück zu Malms Ergebnis.

Eine Zahl n, die sowohl lpsp(P, Q), als auch elpsp(P, Q) ist, und für die darüber hinaus $\mathrm{ggT}(n, Q) = 1$ und $U_n \equiv (D \mid n) \pmod n$ gilt, ist auch eine slpsp(P, Q). Der Spezialfall für Fibonacci-Zahlen war, wie bereits angedeutet, von Parberry bewiesen worden.

Ich hatte schon an früherer Stelle ein Resultat von Lehmer erwähnt, das besagte, dass eine ungerade Zahl für keine Basis a eine epsp(a) sein kann. Hier das analoge Resultat von Williams (1977): Gegeben sei $D \equiv 0$ oder $1 \pmod 4$. Für eine ungerade, zerlegbare Zahl n mit $\mathrm{ggT}(n, D) = 1$ existieren P, Q ungleich Null mit $P^2 - 4Q = D$, $\mathrm{ggT}(P, Q) = 1$, $\mathrm{ggT}(n, Q) = 1$ derart, dass n keine elpsp(P, Q) ist.

Wie bereits erwähnt, hatte Parberry für die Fibonacci-Folge gezeigt, dass es unendlich viele elpsp$(1,-1)$ gibt (unter der hier verwendeten Terminologie).

Dieses Resultat wurde von Kiss, Phong & Lieuwens (1986) verbessert: Gegeben sei (P,Q) derart, dass die Folge $(U_n)_{n\geq 0}$ nicht entartet ist (das heißt, $U_n \neq 0$ für jedes $n \geq 0$). Dann gibt es für jedes $k \geq 2$ unendlich viele elpsp(P,Q), die das Produkt von genau k verschiedenen Primzahlen sind. Ferner kann man diese Primfaktoren, falls $D = P^2 - 4Q > 0$ gilt, für $d \geq 2$ so wählen, dass sie die Form $dm+1$ $(m \geq 1)$ haben.

Was die Fibonacci-Zahlen betrifft, betrachte ich nun die Kongruenzen (X.2) sowie (X.3) und (X.4). Man kann zeigen, dass wenn $\mathrm{ggT}(n, 2PQD) = 1$ und wenn n zwei der Kongruenzen (X.1) bis (X.4) erfüllt, auch die anderen beiden gelten.

Kiss, Phong & Lieuwens erweiterten 1986 ein Resultat von Rotkiewicz (1973) und bewiesen: Gegeben seien $P, Q = \pm 1$ (mit $(P,Q) \neq (1,1)$) sowie $k \geq 2$, $d \geq 2$. Dann existieren unendlich viele Zahlen n, die Euler-Pseudoprimzahlen zur Basis 2 sind und die Kongruenzen (X.1) bis (X.4) erfüllen; ferner ist jede solche Zahl n das Produkt von genau k verschiedenen Primzahlen, die alle die Form $dm+1$ (mit $m \geq 1$) haben.

D Carmichael-Lucas-Zahlen

Wenn man denselben Gedankengang vollzieht, der von den Pseudoprimzahlen zu den Carmichael-Zahlen geführt hat, stößt man auf natürliche Weise auf die folgenden Zahlen:

Gegeben sei $D \equiv 0$ oder $1 \pmod 4$. Dann heißt die Zahl n eine *Carmichael-Lucas-Zahl* (zugehörig zu D), wenn $\mathrm{ggT}(n,D) = 1$ und für alle teilerfremden Zahlen P, Q ungleich Null mit $P^2 - 4Q = D$ und $\mathrm{ggT}(n,Q) = 1$ gilt, dass n eine lpsp(P,Q) ist.

Existieren solche Zahlen? Dies ist nicht von vornherein klar. Natürlich ist n eine Carmichael-Zahl, wenn n eine zu $D = 1$ zugehörige Carmichael-Lucas-Zahl ist.

Williams, der als Erster Carmichael-Lucas-Zahlen untersuchte, zeigte 1977:

Wenn n eine zu D zugehörige Carmichael-Lucas-Zahl ist, dann ist n das Produkt von $k \geq 2$ verschiedenen Primzahlen p_i, wobei $p_i - (D \mid p_i)$ Teiler von $n - (D \mid n)$ ist.

Man beachte, dass $323 = 17 \times 19$ eine Carmichael-Lucas-Zahl ist (mit $D = 5$); aber es kann sich nicht um eine Carmichael-Zahl handeln, denn das Produkt besteht nur aus zwei verschiedenen Primzahlen.

Unter Verwendung einer geeignet modifizierten Variante von Chernicks Verfahren ist es möglich, viele Carmichael-Lucas-Zahlen zu generieren. Zum Beispiel ist $1649339 = 67 \times 103 \times 239$ eine solche Zahl (mit $D = 8$).

XI Primzahltests und Faktorisierung

Der letzte Abschnitt ist einem Thema von brennendem Interesse gewidmet, das in Anbetracht unmittelbarer Anwendungen Gegenstand intensiver Forschung ist und spannende Ideen hervorbrachte.

Unmittelbare, direkte Anwendungen der Zahlentheorie! Wer hätte selbst vor etwa 50 Jahren davon geträumt? Von Neumann ja, ich nicht, viele Leute nicht. Arme Zahlentheorie, die Königin tritt ab (oder steigt auf?), um zum Objekt einer Begierde zu werden, die nicht durch Ehrfurcht, sondern durch Notwendigkeit inspiriert ist.

In den letzten Jahren gab es rasche Fortschritte auf dem Gebiet der Primzahltests und der Faktorisierung. Immer häufiger kamen tiefliegende Resultate der Zahlentheorie zum Einsatz. Brillante Köpfe ersannten intelligente Prozeduren, nicht weniger brillante Techniker erfanden Tricks und Optimierungen, um die Methoden in vernünftiger Zeit ausführen zu können. Auf diese Weise entstand ein völlig neuer Zweig der Zahlentheorie.

In den vorangegangenen Abschnitten dieses Kapitels habe ich versucht, die Grundlagen für eine übersichtliche Darstellung der wichtigsten Verfahrensweisen bei Primzahltests zu schaffen. Allerdings war dieser Versuch eigentlich zum Scheitern verurteilt. In Wirklichkeit benötigt man für die neuesten Entwicklungen Ergebnisse beispielsweise zur Theorie der Jacobi-Summen, algebraischen Zahlentheorie, elliptischen Kurven, abelschen Varietäten usw. Dies geht weit über das hinaus, was ich hier behandeln wollte. Es ist vernünftiger, diejenigen, die sich besonders für das Problem interessieren, auf ergänzende Literatur zu verweisen. Glücklicherweise gibt es inzwischen viele exzellente Übersichtsartikel und Bücher, die ich an gegebener Stelle empfehlen werde.

Ungeachtet der soeben erwähnten Unzulänglichkeiten halte ich einen – wenn auch nicht lückenlosen – Überblick über die Problemstellung

immer noch für sinnvoll. Nach dieser Entschuldigung möchte ich nun mit der unvollständigen Bearbeitung fortfahren.

Zunächst zu den Kosten: Wie teuer ist es, den Zauber zu enthüllen? Danach werde ich umfangreichere Primzahltests behandeln und auf einige beachtenswerte Faktorisierungen der letzten Zeit hinweisen, um schließlich eine kurze Beschreibung von Anwendungen in der Kryptografie mit öffentlichem Schlüssel zu geben.

Es würde mich freuen, wenn die folgende Darstellung die Leser durstig machte. Durstig danach, mehr über das zu erfahren, was hier zu lesen war. Zu diesem Zwecke möchte ich die Bücher von Williams (1998) und von Crandall & Pomerance (2001, 2. Auflage 2005) empfehlen.

A Aufwand für einen Primzahltest

Der Aufwand, einen Algorithmus auf eine Zahl N anzuwenden, ist proportional zur benötigten Zeit und hängt daher von der Maschine, vom Programm und der Größe der Zahl ab.

Die Anzahl der Operationen sollte in einer angemessenen Weise gezählt werden, denn eine Addition oder Multiplikation von sehr großen Zahlen ist aufwändiger, als wenn kleine Zahlen verknüpft werden.

So läuft die Analyse darauf hinaus, dass der Aufwand proportional zur Anzahl der auf Ziffern angewandten Operationen ist. Solche unteilbaren Operationen nennt man Bitoperationen. Daher wird zur Berechnung des Aufwandes nicht die Zahl N, sondern die Anzahl ihrer Ziffern zu einer beliebigen Basis verwendet. Diese ist proportional zu $\log N$.

Ein Algorithmus läuft in *polynomialer Zeit*, wenn es ein Polynom $f(X)$ derart gibt, dass für jedes N die Zeit zur Abarbeitung des Algorithmus für N durch $f(\log N)$ beschränkt ist. Ein nicht-polynomialer Algorithmus heißt *exponentiell*, wenn seine Laufzeit für jede Eingabe N durch den Wert $f(N)$ des Polynoms $f(X)$ beschränkt ist (exponentiell, da $N = e^{\log N}$). Ein Algorithmus kann im Allgemeinen nur dann als praktisch durchführbar bezeichnet werden, wenn er eine polynomiale Laufzeit hat.

In der Komplexitätstheorie beschäftigt man sich speziell mit der Bestimmung von Schranken für die Laufzeit von Algorithmen. Derartige Bestimmungen sind im Grunde eine komplizierte Art der Buchführung, die eine sorgfältige Analyse der verwendeten Methoden erfordert.

Durch die Entdeckung schlauer Tricks können komplexe Algorithmen manchmal durch einfachere ersetzt werden, die vielleicht nur eine polynomiale Laufzeit benötigen.

Man kann sagen, dass das Hauptproblem im Zusammenhang mit Primzahltests (und mit vielen anderen Fragestellungen) das folgende ist:

Existiert ein Algorithmus, der in polynomialer Zeit läuft?

Erst vor kurzer Zeit gelang es, diese Frage mit „Ja“ zu beantworten. Dies werde ich schon bald an passender Stelle besprechen.

Zunächst aber möchte ich andere Primzahltests behandeln, die zwar keine polynomiale Laufzeit haben, aber trotzdem sehr praktisch sind.

Die vorangegangenen Überlegungen sollten keineswegs mit dem Folgenden verwechselt werden.

Wenn man von einer Zahl N weiß, dass sie zerlegbar ist, genügt eine einzige Operation, um dies zu beweisen. Denn es reicht, zwei Zahlen a und b zu finden, so dass $N = ab$ gilt, d.h. die Anzahl der Bitoperationen ist höchstens $(\log N)^2$. Lenstra drückte es einmal so aus: Es ist unerheblich, ob man a und b nach der Konsultation eines Hellsehers fand oder nach drei Jahren sonntäglicher Rechenarbeit, wie sie Cole für die Faktorisierung der Mersenne-Zahl M_{67} benötigte:

$$2^{67} - 1 = 193707721 \times 761838257287.$$

Wie viele Bitoperationen sind aber notwendig, um den Beweis der Primalität einer als Primzahl bekannten Zahl p zu führen? Diese Frage ist nicht so leicht zu beantworten. Pratt zeigte 1975, dass $C(\log p)^4$ Bitoperationen genügen (dabei ist C eine positive Konstante).

Pomerance brachte 1987 den Satz von Hasse-Weil über die Anzahl der Punkte auf elliptischen Kurven modulo einer ganzen Zahl n zur Anwendung. Es gelang ihm zu zeigen, dass wenn p als prim bekannt ist, der Beweis dieser Tatsache höchstens $C \log p$ Multiplikationen modulo p erfordert. Dieses Ergebnis war besser als alle vorangegangenen Zertifizierungsbeweise.

B Weitere Primzahltests

Ich möchte mich nun ein weiteres Mal mit den Primzahltests befassen. Es gibt viele Arten von Tests, die man je nach Standpunkt folgendermaßen klassifizieren kann:

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

oder

$$\left\{\begin{array}{l}\text{Strikte Tests}\\ \text{Tests, die auf Vermutungen basieren}\end{array}\right.$$

oder

$$\left\{\begin{array}{l}\text{Deterministische Tests}\\ \text{Probabilistische oder Monte-Carlo-Tests.}\end{array}\right.$$

Im Folgenden werde ich Tests jeder dieser Klassen begegnen.

Wenn hinreichend viele Primfaktoren von $N-1$ oder $N+1$ bekannt sind, laufen die Tests aus den Abschnitten III und V in polynomialer Zeit mit der Ziffernzahl der Eingabegröße. Dies sind *spezielle* Primzahltests. Jeder von ihnen ist sehr effizient, vorausgesetzt, die Eingabe hat die jeweils passende Form.

Im Gegensatz dazu sind *universelle* Primzahltest nicht darauf zugeschnitten, irgendeine Art von Zahlen effizienter zu behandeln als andere, sondern sind auf alle Zahlen gleichermaßen anwendbar.

Primzahltests sollten sich auf Sätze aus der Zahlentheorie gründen. Aber es gibt Fälle, in denen keine ausreichenden Hilfsmittel zur Verfügung stehen, ohne auf unbewiesene Annahmen wie etwa einer Form der Riemannschen Vermutung zurückzugreifen.

Viele der Tests sind deterministisch und die Schritte sind von Beginn an fest vorgeschrieben. In anderen Tests gibt es Stellen, an denen man zufällige Entscheidungen trifft.

Wenn man eine Zahl N einem Primzahltest unterwirft, ist es erwünscht, eine der folgenden beiden Antworten als Ausgabe zu erhalten: „N ist eine Primzahl“ oder „N ist zerlegbar“. Jedoch gibt es Tests, die etwas ausgeben wie „N ist zerlegbar“ oder „N hat eine Eigenschaft, die auch Primzahlen haben“. Aufgrund der Tatsache, dass diesen Tests eine Wahrscheinlichkeit beigemessen wird, nennt man sie auch probabilistische oder Monte-Carlo-Tests.

Falls sich herausgestellt hat, dass eine Zahl N mit hoher Wahrscheinlichkeit eine Primzahl ist, soll sie als *Quasiprimzahl* [4] bezeichnet werden. Natürlich sollte man nicht vergessen, dass eine Zahl $N > 1$ entweder prim oder zerlegbar ist. Die Bezeichnung „Quasiprimzahl“ spiegelt eine momentane Wissenslücke über den eigentlichen Status von N wider.

Sobald eine Zahl getestet ist und nach zumeist umfangreichen Berechnungen (die allen möglichen menschlichen und maschinellen Fehlern ausgesetzt sind) als Primzahl deklariert wird, ist es von äußerster

[4] Engl. *probable prime*

Wichtigkeit, das Resultat zu überprüfen. Eine zweite oder dritte Wiederholung des Tests, vorzugsweise mit einem anderen Programm und auf anderen Maschinen durchgeführt, gibt bei gleichem Ergebnis zwar eine gewisse Sicherheit, stellt aber keinen Beweis dafür dar, dass das Ergebnis richtig war.

Es wäre daher erstrebenswert, für eine als Primzahl festgestellte Zahl eine Art Zertifikat der Primalität zu erlangen, das dann als Beweis dienen könnte.

Ich möchte nun einige wenige – sehr wenige – Testmethoden besprechen.

Probedivision

Für Zahlen N, die keine spezielle Form haben, liegt es zunächst nahe, durch die – wenn auch sehr naive – Probedivision aller Primzahlen $p \leq \sqrt{N}$ auf Primalität zu testen. In Kapitel 4 wird man sehen, dass die Anzahl der Primzahlen kleiner als $\sqrt{N}$ für eine große Zahl N etwa gleich $2\sqrt{N}/\log N$ ist (diese Aussage wird später sehr viel weiter präzisiert). Die Anzahl der Operationen ist also höchstens $C\sqrt{N}/\log N$ (dabei ist $C > 0$ eine Konstante), was bedeutet, dass diese Prozedur nicht in polynomialer Zeit läuft.

Millers Test

Miller stellte 1976 einen Primzahltest vor, der auf einer verallgemeinerten Form der Riemannschen Vermutung beruht. Ich werde die genaue Bedeutung dieser Hypothese hier nicht erläutern, aber in Kapitel 4 auf die klassische Riemannsche Vermutung eingehen.

Millers Test beinhaltet jene Kongruenzen, die in der Definition der starken Pseudoprimzahlen verwendet wurden. Zur bequemen Formulierung dient die von Rabin eingeführte Terminologie.

Es sei N eine ganze Zahl, $N - 1 = 2^s d$ mit $s \geq 0$ und ungeradem d. Sei $1 < a < N$ mit $\mathrm{ggT}(a, N) = 1$. Dann heißt a ein *Beleg* für N, wenn $a^d \not\equiv 1 \pmod{N}$ und $a^{2^r d} \not\equiv -1 \pmod{N}$ für jedes r, $0 \leq r < s$.

Falls N einen Beleg hat, ist es zerlegbar. Falls N zerlegbar und die Zahl a mit $1 < a < N$ und $\mathrm{ggT}(a, N) = 1$ kein Beleg ist, dann ist N eine $\mathrm{spsp}(a)$. Umgekehrt ist a kein Beleg für N, wenn N ungerade und eine $\mathrm{spsp}(a)$ ist.

In dieser Terminologie reicht es für den Nachweis der Primalität von N zu zeigen, dass keine Zahl a, $1 < a < N$, $\mathrm{ggT}(a, N) = 1$ ein Beleg ist. Da N als sehr groß angenommen wird, ist diese Aufgabe überwältigend! Es wäre wunderbar, wenn man die Sache mit nur wenigen kleinen Zahlen a erledigen könnte, indem man zeigt, dass diese

sämtlich keine Belege für N sind. An dieser Stelle kommt die verallgemeinerte Riemannsche Vermutung ins Spiel. Mit ihrer Hilfe wurde gezeigt:

Millers Test. *Es sei N eine ungerade Zahl. Falls es eine Zahl a mit $\mathrm{ggT}(a, N) = 1$ und $1 < a < 2(\log N)^2$ gibt, die ein Beleg für N ist, dann ist N zerlegbar. Andernfalls ist N eine Primzahl.*

Man sollte hinzufügen, dass aufgrund der Berechnungen, die in Abschnitt VIII vorgestellt wurden, die Zahl 3 215 031 751 die einzige zerlegbare Zahl ist, die bis 25×10^9 gleichzeitig zu den Basen 2, 3, 5, 7 stark pseudoprim ist. Wenn also $N < 25 \times 10^9$ nicht diese Zahl ist und 2, 3, 5, 7 keine Belege sind, dann ist N eine Primzahl. Wie von Jaeschke (1993) gezeigt, gilt dies sogar für $N < 118\,670\,087\,467$.

Dieser Test könnte einfach auf einem Taschenrechner implementiert werden.

Die Anzahl der Bitoperationen, die notwendig sind, um den Nachweis für einen Beleg für N zu erbringen, ist höchstens $C(\log N)^5$ (mit einer positiven Konstante C). Dementsprechend läuft dieser Test in polynomialer Zeit, wenn man die verallgemeinerte Riemannsche Vermutung als bewiesen voraussetzt.

Lenstra veröffentlichte 1979 eine kompaktere Version von Millers Test, die er später noch einmal in seinem Artikel von 1982 bespricht. Siehe auch den guten Übersichtsartikel von Wagon (1986).

Der APR-Test

Der von Adleman, Pomerance & Rumely (1983) erdachte Test (normalerweise als der APR-Test bezeichnet) bedeutete einen Durchbruch. Und zwar:

(i) Es ist ein deterministischer, universeller Primzahltest, also auf beliebige natürliche Zahlen N anwendbar, ohne die Kenntnis von Faktoren von $N - 1$ oder $N + 1$ vorauszusetzen.

(ii) Die Laufzeit $t(N)$ ist fast polynomial; genauer, es gibt explizit berechenbare Konstanten $0 < C' < C$ derart, dass

$$(\log N)^{C' \log\log\log N} \le t(N) \le (\log N)^{C \log\log\log N}.$$

(iii) Der Test stützt sich nicht auf unbewiesene Vermutungen, und zum allerersten Mal auf diesem Gebiet musste man tiefliegende

> Ergebnisse der Theorie der algebraischen Zahlen heranziehen. Der Test beinhaltet Berechnungen mit Einheitswurzeln und dem verallgemeinerten Reziprozitätsgesetz für Potenzreste. (Ist Ihnen aufgefallen, dass ich diese Begriffe nicht besprochen habe? Es geht weit über das hinaus, was ich hier behandeln wollte.)

Bis zum Jahre 2002 hatte der APR-Test die beste Laufzeit unter allen deterministischen, universellen Primzahltests.

Kurz nach seiner Veröffentlichung verbesserten Cohen & Lenstra (1984) den APR-Test unter Verwendung von Jacobi-Summen im Beweis (anstelle des Reziprozitätsgesetzes) und ließen ihn für praktische Anwendungen programmieren. Es war der erste Test, der routinemäßig Zahlen bis zu 200 Dezimalstellen in etwa zehn Minuten handhaben konnte. Für Zahlen bis zu 100 Stellen wurden etwa 45 Sekunden benötigt.

Cohen & Lenstra, Br. (Bruder, nicht Junior) testeten 1987 eine 247-stellige Zahl (einen Primfaktor von $2^{892}+1$) in etwa 15 Minuten.

Lenstra stellte den APR-Test im Séminaire Bourbaki, Exposé 576 (1981) vor. Darüber hinaus wurde er in Artikeln von Lenstra (1982) und Nicolas (1984) sowie in dem wichtigen Buch von Cohen (1993) besprochen.

Tests mit elliptischen Kurven

Im Jahre 1986 stellte Atkin seinen eigenen neuen Primzahltest vor, in dem erstmalig elliptische Kurven über endlichen Körpern verwendet wurden. Der Test läuft in zufallsbedingter polynomialer Zeit und stützt sich nicht auf unbewiesene Vermutungen. Falls das Programm die Meldung „prim“ ausgibt, liefert es zudem eine Liste von Zahlen, mit deren Hilfe man das Ergebnis leicht nachvollziehen kann, ohne die gesamte Berechnung erneut durchführen zu müssen. Eine solche Liste von Zwischenresultaten nennt man ein *Zertifikat* für die Primzahl.

Atkin & Morain (1993) veröffentlichten einen umfangreichen Artikel über ihr Verfahren, das mit dem Kürzel ECPP („elliptic curve primality proving“) bezeichnet wird. Darin werden die verschiedenen Aspekte des Verfahrens detailliert beschrieben. Der Algorithmus ist von Morain weiter verfeinert worden. Ihm gelang es auch, die Primalität verschiedener interessanter Zahlen mit mehr als 1000 Dezimalstellen zu beweisen und die zugehörigen Zertifikate zu erstellen.

Aufgrund der Komplexität des ECPP-Algorithmus werde ich hier gar nicht erst den Versuch unternehmen, dessen grundlegende Schritte zu erläutern.

Derzeit sind verschiedene, höchst effiziente Implementierungen des Tests im Gebrauch. Man sollte unterscheiden zwischen Versionen, die auf einem einzelnen Arbeitsplatzrechner (mit einem Prozessor) ablaufen, und solchen, die ein verteiltes Rechnen auf mehreren vernetzten PCs erlauben. Der aktuelle Rekord wurde naturgemäß mit der letzteren Variante erzielt.

Rekord

Die größte durch einen universellen (nicht auf Vermutungen beruhenden und auf beliebige Zahlen anwendbaren) Primzahltest nachgewiesene Primzahl ist die 20562-stellige Zahl

$$((((((2521008887^3+80)^3+12)^3+450)^3+894)^3+3636)^3+70756)^3+97220.$$

Hierbei handelt es sich um die elfte Mills-Primzahl (vgl. Kapitel 3, Abschnitt II). Der Nachweis wurde von F. Morain geführt und im Juni 2006 zum Abschluss gebracht. Das verwendete Programm war in Zusammenarbeit mit J. Franke, T. Kleinjung und T. Wirth von der Universität Bonn entwickelt worden. Die akkumulierte Gesamtrechenzeit betrug 2219 Tage der Leistung eines der schnellsten verfügbaren PCs. Die Bestätigung des Ergebnisses mit Hilfe des erzeugten Zertifikats benötigt etwa 10 Tage.

Um den rasanten Fortschritt in der Leistungsfähigkeit des ECPP-Verfahrens zu dokumentieren, ist es sinnvoll, nur solche Tests miteinander zu vergleichen, die mit der Einprozessor-Version durchgeführt wurden. In dieser Kategorie ist $2^{38090}+47269$ mit 11467 Stellen die Rekordzahl. Der Nachweis der Primalität wurde im Mai 2010 von N. Luhn abgeschlossen, der das Programm von M. Martin verwendete, mit dessen Hilfe auch die meisten der vorausgegangenen Rekorde aufgestellt wurden. Das zugehörige Zertifikat ist eine Textdatei mit 13 000 000 Schriftzeichen (überschlagen Sie doch einmal, wie viele Bücher, die langweiliger sind als dieses, benötigt würden, um eine solche Anzahl von Zeichen aufzunehmen).

Einen vorherigen Rekord hatte Luhn im Juli 2009 mit der 8949-stelligen Primzahl $2^{29727}+20273$ aufgestellt. Nur drei Wochen zuvor gab A. Steward den Primbeweis für eine 8125-stellige Zahl bekannt, dem größten Primteiler von $3429^{3774}+1$.

Hier nun die früheren Rekorde:

Primzahl	Stellen	Datum
$E_{2762}/(101 \times 137 \times 193)$	7760	Juli 2004
$(32 \times 10^{6959} - 23)/9$	6959	Juli 2003
$16282536 \ldots 36478311$	5878	Februar 2003
$10^{5019} + (3^2 \times 7^5 \times 11^{11})$	5020	September 2001
$10^{3999} + 4771$	4000	Mai 2001
$(348^{1223} - 1)/347$	3106	Januar 2001
$(30^{1789} - 1)/29$	2642	Oktober 2000
$(2^{7331} - 1)/458072843161$	2196	Oktober 1997

Einige dieser Primzahlen verdienen es, besonders hervorgehoben zu werden. Die früheste unter ihnen ist der zweite und größte Faktor der Mersenne-Zahl

$$M_{7331} = 458072843161 \times P2196.$$

Der Beweis der Primalität wurde von E. Mayer mit einem ECPP-Programm von F. Morain erbracht.

Die 5878-stellige Primzahl, deren Dezimaldarstellung nur angedeutet wurde, ist deshalb beachtenswert, weil sie der Schlusspunkt einer Reihe von 233821 aufeinander folgenden zerlegbaren Zahlen ist. Diese Primzahllücke wurde von J.L. Gómez Pardo ausfindig gemacht, der auch das Zertifikat erstellte.

In dem Ausdruck $E_{2762}/(101 \times 137 \times 193)$ für die 7760-stellige Primzahl bedeutet E_n die n-te Euler-Zahl, so dass die Primzahl *E-irregulär* ist (siehe mein Buch *13 Lectures on Fermat's Last Theorem*, S. 203). Der Nachweis der Primalität wurde von M. Oakes erbracht, während die Zahl selber unabhängig auch von D. Broadhurst bestimmt wurde.

Eine bewährte Methode, um ein Gefühl dafür zu bekommen, wie gut universelle Primzahltests funktionieren, besteht darin, sie auf Zufallszahlen anzuwenden, genauer auf solche Zahlen, deren Ziffern dadurch erzeugt werden, dass man ein Rad mit zehn möglichen Positionen wiederholt dreht. Einige in der Natur vorkommende Zahlen wie die allgegenwärtige Konstante π scheinen die Eigenschaft zu haben, dass die Ziffern ihrer Dezimaldarstellung zufällig verteilt sind.

Tatsächlich berechneten Y. Kanada und seine Mitarbeiter im September 1999 mehr als 206 Milliarden Dezimalstellen von π. Eine statistische Analyse zeigte, dass jede Ziffernfolge ebenso häufig auftritt, wie man es bei einer zufallsbedingten Erzeugung erwarten würde. Insbesondere untersuchten Caldwell & Dubner (1998) das Auftreten von

Primzahlen, die sich aus aufeinander folgenden Ziffern innerhalb der Dezimalbruchentwicklung von π zusammensetzen, wobei sie eine bemerkenswerte Übereinstimmung feststellten.

Im Dezember 2002 gab Kanada die Berechnung von 1,2411 Billionen Stellen von π bekannt; Einzelheiten finden sich bei Bailey (2003). Dies erinnert an eine Geschichte, die nicht in Vergessenheit geraten sollte. Ludolph van Ceulen wurde dafür berühmt, dass er 35 Stellen von π korrekt berechnet hatte (posthum im Jahre 1615 veröffentlicht). Diese Ziffern sind auf seinem Grabstein eingraviert. Ich wünsche Kanada ein langes Leben – sein Grabstein wird Probleme bereiten.

Monte-Carlo-Methoden

Zu Beginn des letzten Jahrhunderts lockte das Casino in Monte Carlo spielsüchtige Aristokraten und Abenteurer an. Tragik und Reichtum wurden vom Glücksrad bestimmt.

Mit besonderem Vergnügen habe ich den Roman von Luigi Pirandello gelesen, in dem davon berichtet wird, wie sich das Leben des Mattia Pascal änderte, als ihm das Glück sowohl in Monte Carlo als auch in seinem sizilianischen Heimatdorf zuteil wurde. Aber Monte Carlo meint es nicht immer so gut. Meistens ist ein hoher Preis zu zahlen, in Form des totalen Ruins, bis hin zum Selbstmord!

Ich hoffe aufrichtig, dass niemand, der das Spiel der Monte-Carlo-Primalität beginnt und dem ein Monte-Carlo-Test misslingt, dadurch in den Selbstmord getrieben wird.

Ich möchte an dieser Stelle drei Monte-Carlo-Tests erwähnen, nämlich die von Baillie & Wagstaff (1980), von Solovay & Strassen (1977) und von Rabin (1976, 1980). In jedem dieser Tests wird eine Anzahl von Belegen a verwendet, in Verbindung mit Kongruenzen, die denen ähnlich sind, welche für psp(a)-, epsp(a)-, spsp(a)-Zahlen gelten.

In wenigen Worten sei der Test von Rabin vorgestellt, der dem von Miller sehr ähnlich ist. Auf derselben Idee von Solovay & Strassen basierend, schlug Rabin folgenden Test vor:

Schritt 1. Wähle zufällig $k > 1$ kleine Zahlen a mit $1 < a < N$ und $\mathrm{ggT}(a, N) = 1$.

Schritt 2. Prüfe nacheinander für jede gewählte Basis a, ob N die Bedingung in der Definition der starken Pseudoprimzahl zur Basis a erfüllt. Schreibe $N - 1 = 2^s d$ mit ungeradem d und $s \geq 0$. Dann ist entweder $a^d \equiv 1 \pmod{N}$ oder $a^{2^r d} \equiv -1 \pmod{N}$ für ein r mit $0 \leq r < s$.

Wenn ein a gefunden wird, das die obige Bedingung nicht erfüllt, erkläre N als zerlegbar. Im gegenteiligen Fall beträgt die Wahrscheinlichkeit, dass eine für prim erklärte Zahl N tatsächlich eine Primzahl ist, mindestens $1 - 1/4^k$. Also geschieht für $k = 30$ der Wahrscheinlichkeit nach höchstens in einem von 10^{18} Tests eine Fehlentscheidung.

Vielleicht möchten Sie ja Primzahlen für kryptographische Zwecke verkaufen (seien Sie geduldig, ich werde bald zu dieser Anwendung von Primalität und Faktorisierung kommen). Ja, ich meine wirklich „verkaufen“. Und Sie möchten ja sicher sein, oder zumindest mit einer vernachlässigbaren Fehlerquote davon überzeugt sein, dass Sie tatsächlich Primzahlen verkaufen, so dass Sie werben könnten: „Garantierte Zufriedenheit oder Geld zurück.“

Auf der Grundlage von Rabins Test können Sie ein solides Unternehmen aufbauen und das Produkt guten Gewissens verkaufen.

Der AKS-Test

Im August 2002 veröffentlichten Agrawal, Kayal & Saxena auf ihrer Webseite einen Artikel (2004 im Druck erschienen), der einen universellen, deterministischen und nicht auf unbewiesenen Vermutungen basierenden Algorithmus enthält, der zudem in polynomialer Zeit abläuft. Dies bedeutet die Lösung des in diesem Abschnitt weiter oben erwähnten alten Problems.

Die theoretische Grundlage dieses Tests ist ein Satz, der bis auf eine Stelle nur Aussagen beinhaltet, die sich auf einfache Polynome mit ganzzahligen Koeffizienten modulo N und ein Binom beziehen. Der entscheidende, derzeit noch benötigte Schritt ist ein tiefliegender Satz von Fouvry (1985) aus der Siebtheorie. Ich möchte den Satz hier angeben (jedoch nicht in seiner stärkeren, ursprünglichen Form):

Es sei $\theta = 0,6687\ldots > 2/3$. *Für jedes* $x > 2$ *gibt es eine Primzahl* p *derart, dass* $x^\theta < p < x$, *sowie ein nicht durch* 3 *teilbares* k, *für welches* $2kp + 1 \leq x$ *und* $2kp + 1$ *prim ist.*

Es besteht die begründete Hoffnung, dass der Test in einer Weise modifiziert werden kann, dass er nicht mehr von einem so tiefschürfenden Resultat wie dem von Fouvry abhängig ist.

Was die Laufzeit betrifft (unter Verwendung der schnellen Multiplikation), so wurde sie zunächst im Wesentlichen mit $(\log N)^{12}$ abgeschätzt und dann auf $(\log N)^{7,5}$ verbessert. Eine nähere Untersuchung der Laufzeit findet sich in dem Manuskript von Morain (2002).

Indem ich von meinen eigenen Regeln abweiche, welche die Genauigkeit der in diesem Buch gemachten Aussagen gewährleisten, möchte ich

eine Arbeit der bedeutenden Autoren H.W. Lenstra, Jr. und C. Pomerance erwähnen, die sich noch in der Entwicklung befindet. In dem Manuskript *Primality testing with Gaussian periods* werden Verfeinerungen des AKS-Verfahrens dargestellt, die eine Reduzierung der Ausführungszeit auf $(\log N)^6$ ermöglichen.

Ich habe Agrawal darum gebeten, eine kurze Beschreibung des AKS-Algorithmus zur Verfügung zu stellen, die ich hier wiedergeben möchte. Ich bin ihm dankbar für seine Mitwirkung.

Die zentrale Idee in diesem neuen Primzahltest ist die folgende Charakterisierung der Primzahlen:

N ist genau dann prim, wenn $(1-X)^N \equiv 1 - X^N \pmod{N}$.

Die einfachste Weise, diese Identität effizient zu prüfen, besteht darin, ein zufälliges Polynom $Q(X)$ niedrigen Grades zu wählen und die Prüfung modulo $Q(X)$ vorzunehmen. Mit einer hohen Wahrscheinlichkeit wird das Ergebnis korrekt sein. Dies liefert einen sehr einfachen Algorithmus, der zufallsbedingt in polynomialer Zeit abläuft.

Um zu einem deterministischen Algorithmus zu gelangen, kann man nun zeigen, dass dann, wenn die Identität falsch ist, die Überprüfung modulo nur „weniger“ Polynome niedrigen Grades fehlschlägt. Und eine der einfachsten Mengen solcher Polynome ist $Q(X) = X^r - 1$ für niedrige Grade r.

Im Folgenden bezeichne $P_1(X) \equiv P_2(X) \pmod{X^r - 1, n}$ die Identität der Reste von $P_1(X)$ und $P_2(X)$ nach Division durch $X^r - 1$ und nach Division der Koeffizienten durch n. Dann ist die folgende schwächere Version der obigen Aussage bewiesen:

$N = p^k$ (wobei p eine Primzahl ist) genau dann, wenn $(a-X)^N \equiv a - X^N \pmod{X^r - 1, p}$ *für einige „wenige“ Werte von a und r.*

Tatsächlich kann man für r einen festen Wert wählen. Die Charakterisierung ergibt sofort einen deterministischen und effizienten Primzahltest, da die Identität modulo N (aber natürlich nicht modulo p) verifiziert werden kann, und für den Fall, dass N eine nichttriviale Potenz von p ist, das Standardverfahren zur Anwendung kommt.

Die eine Richtung der Äquivalenz ist einfach zu zeigen. Um die andere Richtung zu beweisen, macht man von den folgenden Aussagen Gebrauch:

(i) Falls $(a-X)^N \equiv a - X^N \pmod{X^r - 1, p}$ für mehrere Werte von a gilt, dann ist die folgende Eigenschaft für jedes Polynom der multiplikativen Gruppe, die durch die entsprechenden linearen

Polynome $(X - a)$ erzeugt wird, erfüllt:

$$g(X)^N \equiv g(X^N) \pmod{X^r - 1, p}.$$

Vorausgesetzt, dass die Ordnung von p modulo r groß ist, erhält man exponentiell viele Polynome $g(X)$, welche der Identität genügen. Dies ist durch vorhandene Resultate der Siebtheorie sichergestellt.

(ii) Falls, wie oben, $g(X)^N \equiv g(X^N) \pmod{X^r - 1, p}$, sowie (trivialerweise) $g(X)^p \equiv g(X^p) \pmod{X^r - 1, p}$, dann gilt für jedes $s = n^i p^j$:

$$g(X)^s \equiv g(X^s) \pmod{X^r - 1, p}.$$

(iii) Da die Potenzen von X modulo $X^r - 1$ reduziert werden, gibt es s und t, $s \neq t$ derart, dass

$$g(X)^s \equiv g(X^t) \pmod{X^r - 1, p}.$$

Dies ist nicht möglich, wenn sowohl s als auch t kleiner als die Größe der Gruppe in (i) ist, aber dies ist, wie oben bemerkt, durch bekannte Ergebnisse aus der Siebtheorie gesichert.

C Titanische und sonderbare Primzahlen

In einem Artikel von 1983/84 prägte Yates den Begriff der „titanischen Primzahl“, womit jede Primzahl mit mindestens 1000 Dezimalstellen gemeint ist. In dem Artikel mit dem zweideutigen Titel *Sinkers of the Titanics* (1984/85) stellte Yates eine Liste der größten bekannten titanischen Primzahlen zusammen. Am 1. Januar 1985 waren ihm 581 titanische Primzahlen bekannt, von denen 170 mehr als 2000 Stellen hatten. Diese sind im Artikel aufgelistet.

Im September 1988 umfasste die von Yates geführte Liste bereits 876 titanische Primzahlen. Die *Sechs von Amdahl* (J. Brown, L.C. Noll, B. Parady, G. Smith, J. Smith & S. Zarantonello) gaben Anfang 1990 die Entdeckung von 550 neuen titanischen Primzahlen bekannt.

Es ist nicht überraschend, dass diese Primzahlen eine besondere Form haben: einige sind Mersenne-Primzahlen, andere von der Form $k \times 2^n \pm 1$ oder $k \times b^n + 1$ $(b > 2)$. Der Grund ist einfach der, dass es für Zahlen dieser Formen viel effizientere Primzahltests gibt.

Im Jahre 1992 bezeichnete Yates alle Primzahlen mit mehr als 10000 Stellen als *gigantisch*. Für Primzahlen mit 1 000 000 oder mehr Stellen

verwenden wir den Begriff *Megaprimzahlen*. Wie schon erwähnt sind die größten Mersenne-Primzahlen Megaprimzahlen, von denen drei sogar mehr als 10 Millionen Stellen haben. Nach dem Tode von Yates übernahm C. Caldwell die Buchführung über die titanischen Primzahlen, die gigantischen Primzahlen und andere Schmuckstücke. Aber er ist auch Autor und Verwalter einer sehr informativen und stets aktuellen Website über „Primzahlangelegenheiten“. Ich habe vom Besuch dieser Website profitiert – sie ist nicht minder interessant als der Zoo von San Diego.

Der stürmische Fortschritt beim Testen von Primzahlen führte zu einer fast täglichen Erweiterung dieser Listen. Im August 2010 hatten die 5000 größten bekannten Primzahlen (nur diese sind in Caldwells Liste aufgeführt) jeweils mehr als 160000 Stellen. Es wäre ein sinnloses Unterfangen, alle diese Zahlen angeben zu wollen. Da es inzwischen mehr titanische, gigantische und Megaprimzahlen gibt als dieses Buch Zeilen hat, habe ich kein schlechtes Gewissen bei dieser Unterlassung. Allerdings wäre es unverzeihlich, Ihnen die folgenden Kuriositäten vorzuenthalten.

Eine *palindromische* Zahl (zur Basis 10) ist eine Zahl $N = a_1a_2\ldots a_{n-1}a_n$ mit Dezimalziffern a_i $(0 \le a_i \le 9)$, für die gilt $a_1 = a_n$, $a_2 = a_{n-1}, \ldots$. Aufgrund des Überlebens eines alten Mystizismus, der oft mit Zahlen verbunden war (vollkommenen Zahlen, befreundeten Zahlen, abundanten Zahlen, usw.), beherrschen die palindromischen Zahlen noch immer die Aufmerksamkeit der Numerologen.

Bereits 1984 fand H. Dubner zahlreiche titanische Primzahlen, die palindromisch sind, darunter die Zahl $10^{2976} + 3 \times 10^{1488} + 1$, die sich in der Liste von Yates findet. Seitdem entdeckte Dubner immer größere palindromische Primzahlen. Bis auf gelegentliche Unterbrechungen konnte er seinen Titel als Rekordhalter bis heute bewahren.

Rekord

Die größte bekannte palindromische Primzahl ist

$$10^{190004} + 214757412 \times 10^{94998} + 1.$$

Sie hat 190005 Dezimalstellen und wurde von Dubner im Mai 2010 entdeckt.

Ein anderer Rekord, den Dubner innehat, beruht auf einem Gedanken, den er 1994 erstmals publiziert hat. Es handelt sich um eine Zahl,

die man eine dreifach palindromische Primzahl nennen könnte:

$$10^{98689} - 429151924 \times 10^{49340} - 1.$$

Die Primzahl hat 98689 Ziffern und wurde in Zusammenarbeit mit J.K. Andersen gefunden. Die Stellenanzahl ist selber eine Primzahl mit 5 Stellen – wiederum eine palindromische Primzahl!

Man könnte nun das folgende, vielleicht etwas albern erscheinende Problem betrachten: Für gegebenes $k \geq 4$ bestimme man eine Zahlenfolge $N_1, N_2, \ldots, N_k$, wobei jedes N_i eine palindromische Primzahl und N_{i+1} die Anzahl der Stellen von N_i ist (für $i = 1, \ldots, k-1$).

Für die Beschreibung der nachfolgenden Perlen ist diese Bezeichnungsweise nützlich: $(d)_n$ bedeutet, dass n Ziffern d aufeinander folgen.

Rekorde

A. Die größte bekannte Primzahl, deren Ziffern sämtlich Primzahlen sind (2, 3, 5, 7), ist die 82000-stellige Zahl

$$(10^{40950}+1) \times (10^{20055}+1) \times (10^{10374}+1) \times \\ (10^{4955}+1) \times (10^{2507}+1) \times (10^{1261}+1) \times M + 1,$$

wobei M die Zahl $(3)_{940}22222222777753223(2)_{940}$, ist, deren Ziffern ebenfalls nur Primzahlen sind.

Die bemerkenswerte Konstruktion der Rekordzahl und der Primalitätsbeweis stammen von D. Broadhurst, der in seiner Bekanntgabe vom Oktober 2003 die Mitwirkung von P. Carmody, G. Childers und anderen würdigt.

B. Die größte bekannte Primzahl, deren Dezimaldarstellung sich lediglich aus den Ziffern 0 oder 1 zusammensetzt, ist die 78943-stellige palindromische Zahl

$$10^{78942} + 10111100100111101 \times 10^{39463} + 1,$$

die 2004 von R. Chaglassian und P. Carmody gefunden wurde.

C. Die größten bekannten Primzahlen, deren Dezimaldarstellung bis auf eine Ziffer d am Anfang nur noch aus n Ziffern 9 besteht (wobei d natürlich nicht durch 3 teilbar ist), sind:

d	n	Jahr
1	55347	2002
2	119292	2006
4	85142	2005
5	34936	2001
7	74318	2004
8	107663	2004

Die größte unter diesen Primzahlen, mit $d = 2$, wurde von D. Heuer entdeckt, und die mit $d = 8$ von J. Sun. Alle übrigen wurden von E.J. Sorensen ermittelt.

D. Die größte bekannte Primzahl, die aus lauter ungeraden Ziffern besteht, ist die oben angeführte Zahl $7(9)_{74318}$, die man auch als $8 \times 10^{74318} - 1$ schreiben kann.

E. Die derzeit bekannte Primzahl mit den meisten Ziffern gleich 0 ist die Primzahl $207777 \times 10^{207777} + 1$, die im Februar 2010 von G. Löh und Y. Gallot entdeckt wurde.

F. Die exotischste unter den sonderbaren Primzahlen ist

$$(1)_{2000}(2)_{2000}(3)_{2000}(4)_{2000}(5)_{2000}(6)_{2000}(7)_{2000}(8)_{2000}(9)_{2000}(0)_{20902}1.$$

Diese Primzahl hat 38903 Stellen und wurde 2006 gefunden. Sie ersetzt eine frühere von 2002, die nach dem gleichen Muster konstruiert war, aber „nur“ 15646 Stellen hatte. Der Entdecker ist in beiden Fällen – wer wohl: H. Dubner.

G. Und schließlich (aber gewiss auch endgültig): Die kleinste Primzahl mit 1000 Stellen ist $10^{999} + 7$. Ihre Primalität wurde 1998 von P. Mihăilescu verifiziert.

D Faktorisierung

Große Zahlen in ihre Faktoren zu zerlegen stellt eine schwierige Aufgabe dar: Es gibt keinen Algorithmus, der in polynomialer Zeit abläuft. Aufgrund der sattsam bekannten Anwendung in der Kryptographie mit öffentlichem Schlüssel hat die Faktorisierung auch große praktische Bedeutung erlangt.

Ungeachtet dessen werde ich die Methoden zur Faktorisierung hier nicht besprechen – dies würde mich erneut zu weit vom eigentlichen Thema der Primzahlrekorde abbringen. Das Beste, was ich an dieser

Stelle tun kann, ist einige Bücher und Forschungsartikel zu erwähnen, die einem Ariadnefaden gleich durch das Labyrinth führen können. Dies sind empfehlenswerte Bücher, in chronologischer Reihenfolge:

Der Band von Brillhart, Lehmer, Selfridge, Tuckerman & Wagstaff (1983) enthält Tabellen der bekannten Faktoren von $b^n \pm 1$ ($b = 2$, 3, 5, 6, 7, 10, 11, 12) für verschiedene Bereiche von n. Beispielsweise erstreckt sich die Tabelle der Faktoren von 2^n-1 und 2^n+1 auf alle $n < 1200$; für größere Basen b ist der Bereich kleiner. Die zweite Auflage von 1988 enthält 2045 neue Faktorisierungen und spiegelt die bedeutsamen Fortschritte wider, die in diesen wenigen Jahren erzielt wurden, sowohl hinsichtlich der Methoden als auch der Technologie. Die dritte Auflage des Buches (2002) umfasst weitere 2332 neue Faktorisierungen.

Diese Gemeinschaftsarbeit, die auch als das „Cunningham-Projekt“ bekannt ist, war ursprünglich als Erweiterung der Tabellen von Cunningham & Woodall von 1925 gedacht. Die Aktivitäten in dieser Richtung werden wahrscheinlich unvermindert weitergehen. Nur der Himmel ist die Grenze!

Das Buch von Riesel (1985) behandelt die Faktorisierung (und Primalität) in aller Ausführlichkeit. Es enthält zudem Tabellen mit Faktoren von Fermat-Zahlen, Mersenne-Zahlen, Zahlen der Formen 2^n+1, 10^n+1, Repunit-Zahlen $(10^n-1)/9$ und vielen mehr. Das Buch bietet eine gute Grundlage zum Studium der Techniken zur Faktorisierung; sie sind in einer schlüssigen und vereinheitlichten Form beschrieben. Aufgrund seines wohlverdienten Erfolges ist 1994 eine zweite Auflage dieses Buches erschienen, die auch eine Beschreibung der Faktorisierungsmethode mit elliptischen Kurven enthält.

Bressoud veröffentlichte 1989 ein einführendes Lehrbuch über Faktorisierung und Primzahltests, das nicht nur die wesentlichen Hintergründe behandelt, sondern auch die Methoden des quadratischen Siebs und der elliptischen Kurven.

Die Verwendung der elliptischen Kurven in der Faktorisierung kann man aus erster Hand dem Artikel von Lenstra (1987) entnehmen. Darüber hinaus ist die Arbeit der Brüder Lenstra von 1990 über Faktorisierungsverfahren von grundlegender Bedeutung. Besonders erfolgreich wurden Verfahren eingesetzt, die auf Siebtechniken beruhen. Hervorheben möchte ich das quadratische Sieb (QS) von Pomerance und das Zahlkörpersieb (NFS), das auf J.M. Pollard zurückgeht. Für eine Beschreibung dieser Verfahren empfehle ich den Artikel von Pomerance (1996). An den Verfeinerungen des Zahlkörpersiebs und deren Implementationen, insbesondere dem speziellen Zahlkörpersieb (SNFS) und

dem allgemeinen Zahlkörpersieb (GNFS), haben unter vielen anderen die Brüder Lenstra, Manasse & Pollard (1993) mitgewirkt.

Die hier erwähnten Verfahren stellen einen beträchtlichen Fortschritt dar gegenüber dem, was in den Übersichtsartikeln von Guy (1975), Williams (1984), Dixon (1984) und dem Vorlesungsskript eines kleinen Kurses von Pomerance (1984) beschrieben ist. Zu ihrer Zeit waren diese Artikel richtungweisend und wurden viel gelesen. Sie enthalten auch umfangreiche Literaturverzeichnisse.

Zur Illustration und zur Freude der Liebhaber großer Zahlen werde ich nun die Primfaktorzerlegung einiger Mersenne-, Fermat- und anderer Zahlen explizit angeben. Die älteren Erwähnungen stammen aus Dicksons *History of the Theory of Numbers*, Bd. I, S. 22, 29, 377 und von Archibald (1935):

$$M_{59} = 2^{59} - 1 = 179951 \times 3203431780337,$$

durch Landry 1869;

$$M_{67} = 2^{67} - 1 = 193707721 \times 761838257287,$$

durch Cole 1903, bereits erwähnt;

$$M_{73} = 2^{73} - 1 = 439 \times 2298041 \times 9361973132609,$$

der Faktor 439 von Euler, die anderen von Poulet 1923;

$$\begin{aligned} F_6 = 2^{2^6} + 1 &= (1071 \times 2^8 + 1) \times (262814145745 \times 2^8 + 1) \\ &= 274177 \times 67280421310721, \end{aligned}$$

durch Clausen 1856.

Obige Faktorisierungen wurden vor dem Aufkommen von Computern erzielt!

Folgende Faktorisierungen stammen aus jüngerer Zeit:

$$\begin{aligned} M_{113} = 2^{113} - 1 = 3391 &\times 23279 \times 65993 \times 1868569 \\ &\times 1066818132868207, \end{aligned}$$

der kleinste Faktor von Reuschle 1856, die übrigen Faktoren von Lehmer 1947;

$$\begin{aligned} M_{193} = 2^{193} - 1 = 13821503 &\times 61654402332483406165 59 \\ &\times 14732265321145317331353282383, \end{aligned}$$

durch Naur (1983) und unabhängig davon durch Pomerance & Wagstaff (1983). Die nächste Faktorisierung steht in historischem Zusammenhang mit Mersenne selbst (siehe Abschnitt VII):

$$M_{257} = 2^{257} - 1 = 535006138814359 \\ \times 1155685395246619182673033 \\ \times 374550598501810936581776630096313181393,$$

durch Penk, der 1979 den ersten Faktor, und Baillie, der 1980 die beiden letzten Faktoren fand. Man beachte, dass Lehmer bereits 1927 die Zerlegbarkeit von M_{257} nachgewiesen hatte, ohne jedoch einen Faktor bestimmen zu können.

Zu den Fermat-Zahlen:

$$F_7 = 2^{2^7} + 1 = 59649589127497217 \times 5704689200685129054721,$$

durch Morrison & Brillhart 1970 (veröffentlicht 1971);

$$F_8 = 2^{2^8} + 1 = 1238926361552897 \\ \times 93461639715357977769163558199606896584051237541638188580280321,$$

durch Brent & Pollard 1980 (veröffentlicht 1981).

Die Fermat-Zahl F_{11} wurde 1988 vollständig faktorisiert. Zwei kleinere Primfaktoren waren schon länger bekannt; zwei weitere wurden von Brent gefunden (mit der Methode der elliptischen Kurven). Er wies darauf hin, dass der 564-stellige Restfaktor wahrscheinlich prim sei. Dass dies tatsächlich der Fall ist, wurde von F. Morain gezeigt.

Die Zahl F_9 wurde 1990 von A.K. Lenstra und M.S. Manasse faktorisiert. Sie konnte dem Zahlkörpersieb nicht standhalten. Die zuletzt vollständig faktorisierte Fermat-Zahl ist F_{10}, deren Primfaktorzerlegung 1995 von Brent abgeschlossen wurde.

All dies und vieles mehr wurde bereits in den Abschnitten erwähnt, die sich mit den Fermat- und Mersenne-Zahlen befassen.

In einem Artikel von 1988, der Dov Jarden gewidmet ist, gaben Brillhart, Montgomery & Silverman alle damals bekannten Faktoren der Fibonacci-Zahlen U_n (für ungerades $n \leq 999$) und der Lucas-Zahlen V_n (für $n \leq 500$) an. Die Faktorisierungen waren für $n \leq 387$ bzw. $n \leq 397$ vollständig. Im April 2003 berichtete Montgomery, dass die Faktorisierungen von U_n und V_n für alle $n \leq 1000$ abgeschlossen sind. Dies bedeutet eine erhebliche Erweiterung der Arbeiten vieler anderer Numerologen, unter ihnen Jarden selbst (siehe die dritte Auflage seines ursprünglich 1958 veröffentlichten Buches).

Hier noch einige erwähnenswerte Faktorisierungen, die zum Zeitpunkt ihrer Entdeckung jeweils einen großen Fortschritt darstellten:

$$\begin{aligned}\frac{10^{103}+1}{11} &= 1237 \times 44092859 \times 102860539 \times 984385009\\ &\quad \times 612053256358933 \times 182725114866521155647161\\ &\quad \times 14718654539938553026608876141375219 79,\end{aligned}$$

durch Atkin und Rickert 1984 vollendet.

A.K. Lenstra und M.S. Manasse waren „erfreut, die erste Faktorisierung einer 100-stelligen Zahl unter Verwendung eines universellen Faktorisierungsalgorithmus' bekannt zu geben" (12. Oktober 1988); ein solcher Algorithmus faktorisiert eine Zahl N in deterministischer Weise, allein abhängig von der Größe von N, und nicht von irgendeiner besonderen Gestalt der Faktoren. Selbst im ungünstigsten Fall weicht die Laufzeit kaum von der durchschnittlichen Laufzeit ab.

Die glückliche Zahl war

$$\begin{aligned}\frac{11^{104}+1}{11^8+1} &= 867592223134283908122180770958507080489 77\\ &\quad \times 10848810485363747061296139984297294840983461152579057721675 3.\end{aligned}$$

Das spezielle Zahlkörpersieb SNFS (Special Number Field Sieve) wurde verwendet, um die 138-stellige Zahl $2^{457}+1$ vollständig zu faktorisieren. Sie ist gleich $3 \times P49 \times P89$, wobei Pn eine Primzahl mit n Stellen bezeichnet. Dies war einer der großen Erfolge des SNFS-Verfahrens, erzielt von A.K. Lenstra und M.S. Manasse im November 1989. Zeitungen berichteten von dieser Meisterleistung, teilweise sogar auf der Titelseite!

Im Jahre 1992 zerlegten A.K. Lenstra und D. Bernstein die 158-stellige Mersenne-Zahl M_{523} in zwei Primfaktoren mit 69 bzw. 90 Stellen, indem sie das SNFS-Verfahren auf zwei massiv-parallelen Supercomputern laufen ließen.

Eine weitere herausragende Faktorisierung wurde im April 1999 von einer Gruppe bekannt gegeben, die sich selbst *The Cabal*[5] nennt. Wiederum mit Hilfe des SNFS-Verfahrens zerlegte sie die Repunit-Zahl $(10^{211}-1)/9$ in ein Produkt $P93 \times P118$ und stellte damit einen vorläufigen Rekord für den größten gefundenen vorletzten Primfaktor einer Zahl auf. Dies war die gemeinsame Leistung von S. Cavallar,

[5] *Die Clique*

B. Dodson, A.K. Lenstra, P. Leyland, W. Lioen, P. Montgomery, H. te Riele und P. Zimmermann.

Hier sei angemerkt, dass das Adjektiv „speziell“ darauf verweist, dass das SNFS-Verfahren bei einer speziellen Form der zu zerlegenden Zahl besonders wirksam ist. Über die Gestalt der Faktoren wird allerdings nichts vorausgesetzt. Zu dieser Kategorie gehören alle Zahlen aus dem Cunningham-Projekt, dem auch die obigen Beispiele entnommen sind. Ein wirklich universelles Verfahren, wie oben definiert, ist demgegenüber das allgemeine Zahlkörpersieb GNFS (General Number Field Sieve).

Rekord

Die größte bisher mit dem SNFS-Verfahren zerlegte Zahl ist die 307-stellige Zahl $(2^{1039}-1)/5080711$, die in ein Produkt $P80 \times P227$ zerlegt wurde. Der Rekord wurde von K. Aoki, J. Franke, T. Kleinjung, A.K. Lenstra und D.A. Osvik aufgestellt und im Mai 2007 bekannt gegeben.

Der vorherige Rekord vom Januar 2006 bleibt dennoch bemerkenswert wegen der Rekordgröße des kleineren Faktors. Er betraf die 274-stellige Zahl $(6^{353}-1)/5$, die in ein Produkt $P120 \times P155$ zerfiel. Diese Faktorisierung wurde von den japanischen Forschern K. Aoki, Y. Kida, T. Shimoyama und H. Ueda erzielt.

Die größte bislang mit dem GNFS-Verfahren zerlegte Zahl stammt aus einem früheren RSA-Wettbewerb (siehe den nächsten Unterabschnitt), sie hat 232 Dezimalstellen und zerfällt in zwei gleich lange Primfaktoren. Diese schwierige und bedeutsame Faktorisierung wurde im Dezember 2009 von T. Kleinjung, K. Aoki, J. Franke, A.K. Lenstra, E. Thomé und anderen bewerkstelligt.

Im folgenden Unterabschnitt werde ich die Kryptographie mit öffentlichem Schlüssel behandeln. Dabei werden Zahlen verwendet, die extrem schwer zu faktorisieren sein sollten.

Um zu einem tieferen Verständnis von Primalität und Faktorisierung zu gelangen, möchte ich dem Leser das neuere Buch von Crandall & Pomerance (2001, Neuauflage 2005) ans Herz legen. Es beschreibt die wichtigsten Methoden und Beweise und stammt von zwei renommierten Experten des Fachs.

Jeder, der sich für Primzahltests, Faktorisierung oder ähnliche Berechnungen mit sehr großen Zahlen interessiert, benötigte in der Vergangenheit den Zugriff auf zentrale Hochleistungsrechner der jeweils neuesten Generation. Mittlerweile verfügt man über derart leistungs-

fähige Arbeitsplatzrechner und PCs sowie über die Möglichkeit, diese zu vernetzen, dass man mit frei zugänglichen Spezialprogrammen auch in der Behaglichkeit des eigenen Heims nennenswerte Ergebnisse erzielen kann. Wenn es draussen schneit – wie es in Kanada häufig der Fall ist – dann kann man einfach seine Primzahl testen und sich dabei die Füße wärmen.

E Kryptographie mit öffentlichem Schlüssel

Die ausufernde Präsenz der Kommunikationsmedien und das Erfordernis, Nachrichten aller Art zu versenden – etwa Banküberweisungen, Liebesbriefe, Anweisungen zum Kauf von Wertpapieren, geheime diplomatische Nachrichten, wie zum Beispiel Berichte über Spionagetätigkeit – hat den Wunsch nach einer sicheren Methode der Verschlüsselung zunehmend verstärkt. In der Vergangenheit wurden die Codes von den Kommunikationspartnern geheim gehalten, es war jedoch oft möglich, mit Hilfe abgefangener Nachrichten die Codierung zu knacken. In einfacheren Fällen reichte es aus, die Häufigkeit der gesendeten Zeichen zu untersuchen, was in Kriegszeiten verheerende Folgen haben konnte.

Mit Einzug der Verschlüsselungssysteme mit öffentlichem Schlüssel erlebte die Kryptographie einen entscheidenden Fortschritt. Die wesentlichen Merkmale des Verfahrens sind seine Einfachheit, die Verwendung eines öffentlichen Schlüssels und die extreme Schwierigkeit, diesen zu durchbrechen. Die Grundidee stammt von Diffie & Hellman aus dem Jahre 1976, und eine erste praktische Implementierung wurde von Rivest, Shamir & Adleman im Jahre 1978 vorgeschlagen. Das resultierende Verschlüsselungsverfahren wurde nach seinen Erfindern RSA-Verfahren genannt. Ich möchte es nun beschreiben.

Jedem Buchstaben oder sonstigem Schriftzeichen, einschließlich des Leerzeichens, wird eine dreistellige Zahl zugeordnet. Im *American Standard Code for Information Interchange* (ASCII) sieht diese Zuordnung wie folgt aus:

—	A	B	C	D	E	F	G	H
032	065	066	067	068	069	070	071	072
I	J	K	L	M	N	O	P	Q
073	074	075	076	077	078	079	080	081
R	S	T	U	V	W	X	Y	Z
082	083	084	085	086	087	088	089	090

Jeder Buchstabe und jedes Zeichen einer Nachricht wird durch ihren Zahlenwert ersetzt, wobei sich durch Aufreihung eine Zahl M ergibt, die nun die Nachricht darstellt.

Jeder Benutzer A des Systems gibt in einem öffentlich einsehbaren Verzeichnis seinen Schlüssel bekannt, der aus einem Paar (n_A, s_A) positiver ganzer Zahlen besteht. Die erste Zahl $n_A = p_A q_A$ ist das Produkt von zwei großen, geheim gehaltenen Primzahlen. Außerdem wird s_A so gewählt, dass es zu $p_A - 1$ und $q_A - 1$ teilerfremd ist.

Um einem anderen Benutzer B eine Nachricht M zu übermitteln, wird M von A verschlüsselt – in einer Weise, die davon abhängt, wer die Nachricht empfangen soll. Nach Erhalt der verschlüsselten Nachricht von A entschlüsselt B diese mit Hilfe seines eigenen, geheimen Schlüssels.

Im Einzelnen sieht das folgendermaßen aus. Im Falle $M \geq n_B$ genügt es, M in kleinere Blöcke aufzuteilen. Deshalb kann angenommen werden, dass $M < n_B$ ist. Falls $\mathrm{ggT}(M, n_B) \neq 1$, wird ein zusätzlicher, redundanter Buchstabe angefügt, so dass $\mathrm{ggT}(M, n_B) = 1$ erfüllt ist.

A sendet B die verschlüsselte Nachricht $E_B(M) = M'$, $1 \leq M' < n_B$, wobei M' der Rest von M^{s_B} modulo n_B ist: $M' \equiv M^{s_B} \pmod{n_B}$.

Um nun M' zu entschlüsseln, berechnet der Benutzer B den Wert t_B, $1 \leq t_B < (p_B - 1)(q_B - 1) = \varphi(n_B)$, so dass $t_B s_B \equiv 1 \pmod{\varphi(n_B)}$. Dies muss nur ein einziges Mal geschehen. Dann ist

$$D_B(M') = M'^{t_B} \equiv M^{s_B t_B} \equiv M \pmod{n_B},$$

also kann B nun die Nachricht M lesen. Wie einfach!

In Wahrheit sind die Dinge, wie so oft, etwas komplizierter. Die technischen Einzelheiten werden in einschlägigen Fachbüchern und in zahlreichen Artikeln behandelt. Ich möchte hier eine vereinfachte Sichtweise einnehmen, die durch folgendes Beispiel illustriert wird. Die Nachricht soll in Gruppen von je zwei Buchstaben codiert werden, was in der Praxis so nicht geschieht.

Nehmen Sie nun ihren kleinen Taschenrechner zur Hand. Unten befindet sich eine codierte Nachricht, die eine bestimmte Person an jemanden schickt, dessen öffentlicher Schlüssel sich aus dem Paar (n, s) zusammensetzt, wobei $n = 156287$, $s = 181$:

151474036925076974117964029299026654036925101743109701
095179152070068045055176008329001574149966031533117864
154599013907031533013986012353068045133750126510137349
117864113338128986117864110052047607001574010738003772

096642117864070838109145011098117864028600117864056547
11786408356704127110914505600 6

Sie kennen die geheimen Primfaktoren von n nicht. Können Sie die Nachricht entschlüsseln? Der Text findet sich irgendwo in diesem Buch.

Ich sollte nun auch noch etwas darüber sagen, wie das Kryptosystem zu knacken ist. Dazu ist es notwendig, für jeden Benutzer A den Wert $\varphi(n_A)$ zu ermitteln. Dies ist gleichbedeutend damit, die Faktorisierung von n_A zu kennen. Denn man erhält $\varphi(n_A) = (p_A - 1)(q_A - 1)$, sobald p_A, q_A bekannt sind. Umgekehrt, setzt man $p = p_A$, $q = q_A$, $n = n_A$, dann ist $\varphi(n) = (p-1)(q-1) = n+1-(p+q)$, $(p+q)^2 - 4n = (p-q)^2$ (falls $p > q$), daher

$$\begin{aligned} p + q &= n + 1 - \varphi(n), \\ p - q &= \sqrt{[n + 1 - \varphi(n)]^2 - 4n}, \end{aligned}$$

womit p und q durch n und $\varphi(n)$ ausgedrückt sind.

Über das RSA-Kryptosystem wäre noch viel mehr zu sagen:

(a) Wie kann man „signierte“ Nachrichten versenden, so dass der Empfänger den Absender fehlerfrei identifizieren kann?

(b) Wie sind die Primfaktoren der Zahlen n_A des Schlüssels vernünftig zu wählen, damit das System mit den heute verfügbaren Mitteln nicht zu unterlaufen ist?

Wenn jemand etwas liest, was ich mit der Hand geschrieben habe, wird kein Zweifel aufkommen: Niemand hat eine so hässliche Handschrift wie ich! Es ist jedoch etwas anderes, wenn man eine elektronische Nachricht erhält. Selbst wenn sie verschlüsselt ist, könnte der geheime Code ja gefälscht sein. Es gibt ein Verfahren, das ich beschreiben werde, mit dem man „signierte“ Nachrichten versenden kann, die sich nicht vortäuschen lassen.

Das Verfahren ist einfach und pfiffig.

A möchte an B eine Nachricht senden, welche die Signatur von A enthalten soll.

Fall 1: $n_A < n_B$. A teilt seine Ausgangsnachricht in Blöcke $M < n_A$ auf, die er einzeln versenden muss. Hierfür benutzt A seinen eigenen Schlüssel wie bereits beschrieben: t_A erfüllt $1 \leq t_A < \varphi(n_A)$ und $t_A s_A \equiv 1 \pmod{n_A}$; $D_A(M)$ ist der Rest von M^{t_A} modulo n_A.

A sendet nun die Nachricht $D_A(M)$ unter Verwendung des öffentlichen Schlüssels von B. Der Empfänger B erhält $L = E_B((D_A(M)) \equiv$

$M^{t_A s_B} \pmod{n_B}$. Die Nachricht L wird durch B entschlüsselt, wobei sich $D_B(L) = L^{t_B} \equiv M^{t_A s_B t_B} \equiv M^{t_A} \pmod{n_B}$ ergibt. Mit Hilfe des öffentlichen Schlüssels von A kann B schließlich die Nachricht $E_A(M^{t_A}) \equiv M^{s_A t_A} \equiv M \pmod{n_A}$ lesen.

Fall 2: $n_B \leq n_A$. A zerlegt seine Nachricht in Blöcke $M < n_B$. Es wird ganz ähnlich verfahren: Man erhält $L = E_A((D_B(M)) \equiv M^{t_A s_B} \pmod{n_B}$ und anschließend $E_A((D_B(L)) \equiv M^{s_A t_B (t_A s_B)} \equiv M \pmod{n_B}$.

Die Verwendung von E_A bei diesem Vorgang garantiert dem Empfänger B, dass die Nachricht von A verschlüsselt wurde.

Hinsichtlich (b) ist es zur Sicherung der Nachricht am Wichtigsten, dass der öffentliche Schlüssel nicht faktorisiert werden kann. Eine gute Voraussetzung dafür ist es, dass die beiden Faktoren gleich lang sind. Wie viele Stellen sollte der Schlüssel also haben, um eine mögliche Faktorisierung zeitlich unerschwinglich zu machen?

Um diesen Gesichtspunkt zu prüfen, wurden den Mathematikern verschiedene Schlüssel vorgelegt, die als Herausforderung zur Faktorisierung gedacht waren. Unter diesen befand sich die folgende 232-stellige Zahl, deren Bezeichnung RSA-768 auf ihre Länge in Bits verweist:

RSA-768 =
12301866845301177551304949583849627207728535695953
34792197322452151726400507263657518745202199786469
38995647494277406384592519255732630345373154826850
79170261221429134616704292143116022212404792747377
94080665351419597459856902143413

Diese Zahl war als möglicher Schlüssel für das Rivest-Shamir-Adleman-Verfahren sorgfältig generiert worden. Die Aufgabe wurde von einem internationalen Wissenschaftlerteam gelöst, dem es im Dezember 2009 gelang, diese beiden 116-stelligen Primfaktoren zu enthüllen:

33478071698956898786044169848212690817704794983713
76856891243138898288379387800228761471165253174308
7737814467999489,

36746043666799590428244633799627952632279158164343
08764267603228381573966651127923337341714339681027
0092798736308917

Das verwendete Verfahren war das allgemeine Zahlkörpersieb GNFS (vergleiche den Rekord im vorigen Unterabschnitt), wobei die Software großenteils an der Universität Bonn entwickelt wurde. Die benötigte Rechenzeit, die im Laufe von 20 Monaten auf viele Hundert PCs verteilt wurde, entspricht der Leistung eines 2,2-GHz-Prozessors von etwa 1500 Jahren.

Angesichts dieses Aufwandes und der tiefgründigen Sachkenntnis der Forscher, ohne die das Verfahren nicht praktikabel ist, muss man im Grunde nicht befürchten, dass ein Schlüssel von 1024 Bits Länge, wie er derzeit zum Einsatz kommt, eine reale Gefahr darstellt. Dennoch schätzen die Wissenschaftler, dass diese Schlüssellänge im kommenden Jahrzehnt geknackt werden kann, und empfehlen, in spätestens drei bis vier Jahren keine 1024-Bit-Schlüssel mehr zu verwenden.

Bezüglich all dieser Fragen kann man die Originalarbeiten von Rivest, Shamir & Adleman (1978) und von Rivest (1978) zu Rate ziehen. Es gibt natürlich auch viele Übersichtsartikel und Bücher zum Thema. Siehe den Artikel von Couvreur & Quisquater (1982) sowie – die anderen Autoren schöner Übersichtsartikel mögen mir verzeihen – die Bücher von Riesel (1985), Koblitz (1987), Bressoud (1989), Coutinho (1999) und Wagstaff (2003). Oder vielleicht auch das Vorlesungsskript von Lemos (1989), das in Portugiesisch geschrieben ist – es ist, als würde man die Kryptographie in einer verschlüsselten Sprache studieren. Der Strand von Copacabana wäre ein schöner Ort dafür.