5

Welche besonderen Arten von Primzahlen wurden untersucht?

Wir waren bereits verschiedenen Arten besonderer Primzahlen begegnet. Zum Beispiel solchen, die Fermat- oder Mersenne-Zahlen sind (siehe Kapitel 2). Ich werde nun weitere Primzahl-Familien besprechen, darunter die regulären Primzahlen, Sophie-Germain-Primzahlen, Wieferich-Primzahlen, Wilson-Primzahlen, Repunit-Primzahlen sowie Primzahlen in linear rekurrenten Folgen zweiter Ordnung.

Reguläre Primzahlen, Sophie-Germain- und Wieferich-Primzahlen entstammen direkt aus Beweisversuchen von Fermats letztem Satz.

Der interessierte Leser möchte dazu vielleicht mein Buch *13 Lectures on Fermat's Last Theorem* konsultieren, in dem diese Angelegenheiten genauer besprochen werden. Insbesondere befindet sich darin ein umfassendes Literaturverzeichnis mit zahlreichen klassischen Arbeiten, die im vorliegenden Buch nicht aufgelistet sind.

I Reguläre Primzahlen

Reguläre Primzahlen traten erstmals in der Arbeit von Kummer in Verbindung mit Fermats letztem Satz in Erscheinung. In einem Brief an Liouville von 1847 erklärt Kummer, er habe Fermats letzten Satz für alle Primzahlen p bewiesen, die zwei Bedingungen genügen. Tatsächlich hatte er gezeigt, dass wenn p diese Bedingungen erfüllt, es keine ganzen Zahlen x, y, $z \neq 0$ mit $x^p + y^p = z^p$ gibt. Er bemerkte weiter, dass

P. Ribenboim, *Die Welt der Primzahlen*, 2. Aufl., Springer-Lehrbuch,
DOI 10.1007/978-3-642-18079-8_5, © Springer-Verlag Berlin Heidelberg 2011

„nur noch verbliebe zu untersuchen, ob dies gemeinsame Eigenschaften aller Primzahlen sind."

Um diese Eigenschaften beschreiben zu können, muss ich einige der von Kummer eingeführten Begriffe erläutern.

Es sei p eine ungerade Primzahl und

$$\zeta = \zeta_p = \cos\frac{2\pi}{p} + i\sin\frac{2\pi}{p}$$

eine primitive p-te Einheitswurzel. Man beachte, dass $\zeta^{p-1} + \zeta^{p-2} + \cdots + \zeta + 1 = 0$, da $X^p - 1 = (X-1)(X^{p-1} + X^{p-2} + \cdots + X + 1)$ und $\zeta^p = 1$, $\zeta \neq 1$. Folglich lässt sich ζ^{p-1} durch kleinere Potenzen von ζ ausdrücken. Es sei K die Menge aller Zahlen $a_0 + a_1\zeta + \cdots + a_{p-2}\zeta^{p-2}$ mit rationalen Zahlen $a_0, a_1, \ldots, a_{p-2}$ und A die kleinste Teilmenge von K, die aus denjenigen Zahlen besteht, für die $a_0, a_1, \ldots, a_{p-2}$ ganz sind. Dann ist K ein Körper, den man den p-ten Kreisteilungskörper (oder auch Körper der p-zyklotomischen Zahlen) nennt. A ist ein Ring, der Ganzheitsring der p-zyklotomischen (ganzen) Zahlen. Die Einheiten von A sind diejenigen Zahlen $\alpha \in A$, die die 1 teilen, das heißt, für die $\alpha\beta = 1$ für irgendein $\beta \in A$ erfüllt ist. Ein Element $\alpha \in A$ nennt man ein Primelement, wenn α sich nur dann in der Form $\alpha = \beta\gamma$ mit β, $\gamma \in A$ schreiben lässt, wenn β oder γ eine Einheit ist.

Ich werde die Arithmetik der p-zyklotomischen ganzen Zahlen als normal bezeichnen, wenn jede zyklotomische ganze Zahl ein bis auf Einheiten eindeutiges Produkt von Primelementen ist.

Kummer entdeckte bereits 1847, dass die Arithmetik der p-zyklotomischen Zahlen für $p \leq 19$ normal ist. Dies ist jedoch für $p = 23$ nicht der Fall.

Um einen Weg zu finden, mit nichteindeutigen Primfaktorzerlegungen umzugehen, führte Kummer ideale Zahlen ein. Später untersuchte Dedekind bestimmte Mengen zyklotomischer ganzer Zahlen, die er Ideale nannte. Ich werde von einer Definition des Begriffs Ideal absehen und sie als dem Leser bekannt voraussetzen. Dedekind-Ideale ermöglichten eine konkrete Beschreibung von Kummers idealen Zahlen. Es bietet sich daher an, Kummers Ergebnisse durch Dedekinds Ideale zu erklären. Ein Primideal P ist ein Ideal, das weder gleich 0 ist, noch mit dem Ring A übereinstimmt, und das nur dann ein Produkt $P = IJ$ zweier Ideale sein kann, wenn entweder I oder J gleich P ist. Kummer zeigte, dass für alle Primzahlen $p > 2$ jedes von 0 und A verschiedene Ideal des Ganzheitsrings der p-zyklotomischen Zahlen in eindeutiger Weise ein Produkt von Primidealen ist.

In diesem Zusammenhang erscheint es natürlich, zwei Ideale I und J ungleich dem Nullideal als äquivalent zu betrachten, wenn es zwei von 0 verschiedene zyklotomische ganze Zahlen $\alpha, \beta \in A$ mit der Eigenschaft gibt, dass $A\alpha.I = A\beta.J$. Die Menge der Äquivalenzklassen von Idealen bildet eine kommutative, reguläre Halbgruppe. Kummer zeigte, dass diese Menge endlich ist und damit eine Gruppe bildet, die man nun Idealklassengruppe nennt. Die Anzahl ihrer Elemente heißt Klassenzahl und wird mit $h = h(p)$ bezeichnet. Sie ist eine sehr wichtige arithmetische Invariante.

Die Begriffe gebrochener Ideale, Klassen von Idealen und der Endlichkeit der Anzahl der Klassen spielen eine zentrale Rolle in der Theorie algebraischer Zahlkörper. Außer den hier betrachteten Kreisteilungskörpern hatte ich bereits zuvor (Kapitel 3, Abschnitt III, B) den Fall der quadratischen Zahlkörper betrachtet.

Die Klassenzahl $h(p)$ ist genau dann gleich 1, wenn jedes Ideal von A ein Hauptideal ist, das heißt, wenn es die Form $A\alpha$ für ein $\alpha \in A$ hat. Somit gilt $h(p) = 1$ genau dann, wenn die Arithmetik der p-zyklotomischen ganzen Zahlen normal ist. Die Größe von $h(p)$ ist also ein Maß für die Abweichung von der normalen Arithmetik.

Es sei an dieser Stelle gesagt, dass Kummer eine sehr tiefschürfende Theorie entwickelt hat, dabei eine explizite Formel für $h(p)$ fand und in der Lage war, $h(p)$ für kleine p zu berechnen.

Eine der beiden Eigenschaften von p, die Kummer in Verbindung mit Fermats letztem Satz benötigte, war die folgende: p ist kein Teiler der Klassenzahl $h(p)$. Heute nennt man eine Primzahl mit dieser Eigenschaft eine *reguläre Primzahl*.

Die zweite Eigenschaft, die Kummer nannte, bezog sich auf Einheiten. Er zeigte später, dass diese von allen regulären Primzahlen erfüllt ist. Dies ist ein weiteres, schönes Resultat von Kummer, man nennt es heute Kummers Lemma.

In seinem Regularitätskriterium bewies Kummer, dass die Primzahl p genau dann regulär ist, wenn p die Zähler der Bernoulli-Zahlen B_2, B_4, $B_6, \ldots, B_{p-3}$ nicht teilt (die Bernoulli-Zahlen wurden in Kapitel 4, Abschnitt I, A definiert).

Kummer gelang es kurz darauf, alle irregulären Primzahlen unterhalb von 163 zu bestimmen, und zwar 37, 59, 67, 101, 103, 131, 149, 157. Er gab die Hoffnung nicht auf, dass unendlich viele reguläre Primzahlen existieren. Die Klärung dieser Frage stellt ein sehr schwieriges Problem dar, obwohl die Antwort positiv ausfallen sollte, worauf numerische Belege klar hindeuten.

Siegel bewies 1964 unter der Voraussetzung heuristischer Aussagen über die Reste von Bernoulli-Zahlen modulo Primzahlen, dass die Dichte regulärer Primzahlen unter allen Primzahlen $1/\sqrt{e} \cong 61\%$ beträgt.

Auf der anderen Seite war es ein wenig überraschend, als Jensen 1915 bewies, dass es unendlich viele irreguläre Primzahlen gibt. Der Beweis war eigentlich ziemlich einfach, er erforderte einige arithmetische Eigenschaften der Bernoulli-Zahlen.

Es sei $\pi_{\mathrm{reg}}(x)$ die Anzahl der regulären Primzahlen p mit $2 \le p \le x$ und

$$\pi_{\mathrm{ir}}(x) = \pi(x) - \pi_{\mathrm{reg}}(x).$$

Für jede irreguläre Primzahl p nennt man das Paar $(p, 2k)$ ein *irreguläres Paar*, wenn $2 \le 2k \le p-3$ und p den Zähler von B_{2k} teilt. Die Anzahl der irregulären Paare $(p, 2k)$ heißt *Irregularitätsindex* von p und wird mit $\mathrm{ii}(p)$ bezeichnet.

Für $s \ge 1$ sei $\pi_{\mathrm{ii}s}(x)$ die Anzahl der Primzahlen $p \le x$ mit $\mathrm{ii}(p) = s$.

Rekord

Die wichtigsten Berechnungen über reguläre Primzahlen stammen der Reihenfolge nach von Johnson (1975), Wagstaff (1978), Tanner & Wagstaff (1989), Buhler, Crandall & Sompolski (1992), Buhler, Crandall, Ernvall & Metsänkylä (1993) und Buhler, Crandall, Ernvall, Metsänkylä & Shokrollahi (2001). Alle irregulären Primzahlen bis $N = 12 \times 10^6$ wurden zusammen mit ihrem Irregularitätsindex bestimmt. Hier die Ergebnisse (die Primzahl 2 zählt man weder zu den regulären, noch zu den irregulären Primzahlen):

$$\begin{aligned}
\pi(N) &= 788060 \\
\pi_{\mathrm{reg}}(N) &= 477616 \\
\pi_{\mathrm{ir}}(N) &= 310443 \\
\pi_{\mathrm{ii}1}(N) &= 239483 && \text{(die Kleinste ist } 37) \\
\pi_{\mathrm{ii}2}(N) &= 59710 && \text{(die Kleinste ist } 157) \\
\pi_{\mathrm{ii}3}(N) &= 9824 && \text{(die Kleinste ist } 491) \\
\pi_{\mathrm{ii}4}(N) &= 1282 && \text{(die Kleinste ist } 12613) \\
\pi_{\mathrm{ii}5}(N) &= 127 && \text{(die Kleinste ist } 78233) \\
\pi_{\mathrm{ii}6}(N) &= 13 && \text{(die Kleinste ist } 527377) \\
\pi_{\mathrm{ii}7}(N) &= 4 && \text{(die Kleinste ist } 3238481) \\
\pi_{\mathrm{ii}s}(N) &= 0, \text{ für } s \ge 8.
\end{aligned}$$

Der gegenwärtige Stand des Wissens ist: Die größte bekannte reguläre Primzahl ist $p = 11999989$. Die längste bekannte Sequenz aufeinander folgender regulärer Primzahlen besteht aus 27 Primzahlen und beginnt mit 17881. Die längste bekannte Sequenz aufeinander folgender irregulärer Primzahlen besteht aus 14 Primzahlen und beginnt mit 670619.

Die einzigen „aufeinander folgenden" irregulären Paare $(p, 2k)$, $(p, 2k + 2)$ sind $p = 491$, $2k = 336$ bzw. $p = 587$, $2k = 90$. Es sind keine Drillinge $(p, 2k)$, $(p, 2k + 2)$, $(p, 2k + 4)$ irregulärer Paare bekannt.

Für alle Primzahlen $p \geq 11$ gilt, dass p genau dann eine Wolstenholme-Primzahl ist (siehe Kapitel 2, Abschnitt II, C), wenn p den Zähler der Bernoulli-Zahl B_{p-3} teilt, oder anders ausgedrückt, wenn $(p, p-3)$ ein irreguläres Paar ist.

Man vermutet, ohne es jedoch bisher beweisen zu können, dass es Primzahlen mit beliebig hohem Irregularitätsindex gibt.

Aus der Kombination des Satzes von Kummer, einem Kriterium von Vandiver sowie den oben erwähnten Berechnungen ergibt sich, dass Fermats letzter Satz für jeden primen Exponenten $p < 12 \times 10^6$ richtig ist.

Die Regularität einer Primzahl ist für viele Fragen der Zahlentheorie relevant, wobei seit dem Beweis der allgemeinen Gültigkeit des Fermatschen Satzes die Rolle der regulären Primzahlen in diesem Zusammenhang hauptsächlich von historischem Interesse ist. Die außergewöhnliche mathematische Leistung des kompletten Beweises war das Resultat der Verknüpfung von Arbeiten von G. Frey, K.A. Ribet, J.P. Serre, A. Wiles und R. Taylor.

II Sophie-Germain-Primzahlen

Ich war auf die Sophie-Germain-Primzahlen bereits in Kapitel 2 im Zusammenhang mit einem Kriterium von Euler über Teiler von Mersenne-Zahlen gestoßen.

Zur Erinnerung: p ist dann eine *Sophie-Germain-Primzahl*, wenn auch $2p + 1$ prim ist. Es war Sophie Germain, die solche Zahlen zuerst untersuchte und dabei diesen wunderbaren Satz bewies:

Wenn p eine Sophie-Germain-Primzahl ist, dann gibt es keine von 0 verschiedenen ganzen Zahlen x, y, z, die nicht von p geteilt werden und die $x^p + y^p = z^p$ erfüllen.

Mit anderen Worten, der „erste Fall von Fermats letztem Satz“ ist für Sophie Germains Primzahlen gültig. Eine detaillierte Diskussion findet sich in meinen Büchern (1979) oder (1999).

Man vermutet, dass es unendlich viele Sophie-Germain-Primzahlen gibt. Der Beweis dürfte jedoch den gleichen Schwierigkeitsgrad haben wie der Beweis der Existenz unendlich vieler Primzahlzwillinge.

Ich möchte nun etwas ausführlicher auf die Zusammenhänge zwischen dem ersten Fall von Fermats letztem Satz und Primzahlen wie denen von Sophie Germain eingehen.

Erweiterungen von Sophie Germains Satz stammen von Legendre, Dénes (1951) sowie aus jüngerer Zeit von Fee & Granville (1991).

Es folgen Abschätzungen für die Anzahl der Sophie-Germain-Primzahlen unterhalb einer Zahl $x \geq 1$. Allgemeiner sei a, $d \geq 1$ mit geradem ad und $\mathrm{ggT}(a, d) = 1$. Für jedes $x \geq 1$ sei

$$S_{d,a}(x) = \#\{p \text{ prim} \mid p \leq x, a + pd \text{ ist eine Primzahl}\}.$$

Wenn $a = 1$, $d = 2$, dann zählt $S_{2,1}(x)$ die Sophie-Germain-Primzahlen $p \leq x$.

Die gleichen Siebmethoden, die Brun zur Abschätzung der Anzahl $\pi_2(x)$ der Primzahlzwillinge kleiner als x verwendete, führen hier zu einer ähnlichen Schranke

$$S_{d,a}(x) < \frac{Cx}{(\log x)^2}\,.$$

Aus dem Primzahlsatz folgt

$$\lim_{x\to\infty} \frac{S_{d,a}(x)}{\pi(x)} = 0.$$

Es ist daher vernünftig zu sagen, dass die Menge der Primzahlen p, für die auch $a + pd$ prim ist, die Dichte 0 hat. Insbesondere hat die Menge der Sophie-Germain-Primzahlen und ebenso auch die Menge der Primzahlzwillinge die Dichte 0.

Powell fand 1980 einen Beweis für diese Tatsachen, ohne auf Siebmethoden zurückgreifen zu müssen.

Tabelle 20. Anzahl $S_{2,1}(x)$ von Sophie-Germain-Primzahlen bis x

x	$S_{2,1}(x)$
10^3	37
10^4	190
10^5	1 171
10^6	7 746
10^7	56 032
10^8	423 140
10^9	3 308 859
10^{10}	26 569 515
10^{11}	218 116 524

Die drei letzten Werte der Tabelle berechnete C.F. Kerchner 1999. Mittlerweile fand man sehr große Sophie-Germain-Primzahlen.

Rekorde

Tabelle 21. Die größten bekannten Sophie-Germain- Primzahlen

Sophie-Germain-Primzahl	Stellen	Entdecker	Jahr
$183027 \times 2^{265440} - 1$	79911	T. Wu und J. Penné	2010
$648621027630345 \times 2^{253824} - 1$	76424	Z. und A. Járai, G. Farkas, T. Csajbok und J. Kasza	2009
$620366307356565 \times 2^{253824} - 1$	76424	Z. und A. Járai, G. Farkas, T. Csajbok und J. Kasza	2009
$607095 \times 2^{176311} - 1$	53081	T. Wu und J. Penné	2009
$48047305725 \times 2^{172403} - 1$	51910	D. Underbakke und J. Penné	2007
$137211941292195 \times 2^{171960} - 1$	51780	Z. und A. Járai, G. Farkas, T. Csajbok und J. Kasza	2006
$33759183 \times 2^{123458} - 1$	37173	B. Tornberg, D. Underbakke, und J. Penné	2009
$7068555 \times 2^{121301} - 1$	36523	P. Minovic, D. Underbakke und J. Penné	2005
$2540041185 \times 2^{114729} - 1$	34547	D. Underbakke, G. Woltman und Y. Gallot	2003
$1124044292325 \times 2^{107999} - 1$	32523	D. Underbakke und J. Penné	2006

Das folgende Thema ist eng mit den Sophie-Germain-Primzahlen verbunden: Eine aufsteigende Folge von Primzahlen $q_1 < q_2 < \cdots < q_k$ heißt *Cunningham-Kette erster Art* (bzw. *zweiter Art*) *der Länge* k, wenn $q_{i+1} = 2q_i + 1$ (bzw. $q_{i+1} = 2q_i - 1$) für $i = 1, 2, \ldots, k-1$. Somit sind die ersten $k-1$ Zahlen einer Cunningham-Kette erster Art alles Sophie-Germain-Primzahlen.

Es ist nicht bekannt, ob es für jedes $k > 2$ eine Cunningham-Kette (unabhängig welcher Art) mit der Mindestlänge k gibt.

Rekord

Die längsten bekannten Cunningham-Ketten haben die Länge 17 und wurden von J. Wróblewski im Juni 2008 entdeckt. Diejenige der ersten Art beginnt mit der Primzahl 2759832934171386593519 und diejenige der zweiten Art beginnt mit der Primzahl 4024484478937992697914 1.

Frühere Rekorde hatten überdies die Eigenschaft, dass sie jeweils die kleinstmögliche Anfangsprimzahl aufwiesen. Sie stammten von P. Carmody und P. Jobling (erste Art, Länge 16, gefunden 2002) und von T. Forbes (zweite Art, ebenfalls Länge 16, gefunden 1997) sowie von G. Löh: Länge 12 für die erste Art, Länge 13 für die zweite Art, beide aus dem Jahre 1989.

III Wieferich-Primzahlen

Eine Primzahl p, die der Kongruenz

$$2^{p-1} \equiv 1 \pmod{p^2}$$

genügt, heißt *Wieferich-Primzahl*. Es war Wieferich, der 1909 den schwierigen Satz bewies:

Wenn der erste Fall von Fermats letztem Satz für den Exponenten p falsch ist, dann erfüllt p obige Kongruenz.

Im Gegensatz zur Kongruenz $2^{p-1} \equiv 1 \pmod{p}$, die von jeder ungeraden Primzahl erfüllt wird, gilt die Wieferich-Kongruenz nur sehr selten.

Vor dem Computerzeitalter entdeckten Meissner 1913 und Beeger 1922, dass die Primzahlen $p = 1093$ und $p = 3511$ Wieferichs Kongruenz genügen. Wenn Sie kein passiver Leser sind, haben Sie bereits in Kapitel 2, Abschnitt III berechnet, dass $2^{1092} \equiv 1 \pmod{1093^2}$. Genauso leicht lässt sich dies für 3511 nachweisen.

Rekord

Lehmer hat 1981 gezeigt, dass es mit Ausnahme von 1093 und 3511 keine Primzahlen $p < 6 \times 10^9$ gibt, die Wieferichs Kongruenz erfüllen. Seine Berechnungen wurden zunächst von Crandall, Dilcher & Pomerance (1997) bis 4×10^{12} erweitert, danach rechnete R. McIntosh bis 8×10^{12}, R. Brown bis $4{,}9 \times 10^{13}$ und J.K. Crump (mit Helfern) bis 2×10^{14}. Knauer & Richstein (2005) erreichten 2002 die Grenze von $1{,}25 \times 10^{15}$. Schließlich berichten Dorais und Klyve (2008) davon, diese Grenze auf $6{,}7 \times 10^{15}$ erhöht zu haben. Eine dritte Wieferich-Primzahl ist nicht aufgetaucht.

Zusammen mit früheren Resultaten aus Kapitel 2, Abschnitte III und IV, besagen diese Berechnungen, dass die einzig möglichen Faktoren p^2 (wobei p eine Primzahl kleiner als $6{,}7 \times 10^{15}$ ist) einer beliebigen Pseudoprimzahl Quadrate von $p = 1093$ oder $p = 3511$ sind. Dies wurde durch Berechnungen von Pinch (2000) bestätigt. Unterhalb der Grenze 10^{13} fand er 54 Pseudoprimzahlen mit einem mehrfach auftretenden Faktor.

Mirimanoff bewies 1910 den folgenden Satz, der dem von Wieferich ähnelt:

Wenn der erste Fall von Fermats letztem Satz für den Primzahlexponenten p falsch ist, dann gilt $3^{p-1} \equiv 1 \pmod{p^2}$.

Man kann verifizieren, dass 1093 und 3511 Mirimanoffs Kongruenz nicht erfüllen.

Diese beiden Resultate bildeten die Basis eines neuen Angriffspunktes für den ersten Fall von Fermats Satz. Dank der Arbeiten von Vandiver, Frobenius, Pollaczek, Morishima, Rosser und aus jüngerer Zeit Granville & Monagan (1988) sowie Suzuki (1994) war es möglich, den Gültigkeitsbereich des ersten Falls von Fermats letztem Satz erheblich zu erweitern. In diesem Zusammenhang war die Verknüpfung verschiedener Kriterien durch eine kombinatorische Methode von Gunderson von entscheidender Bedeutung. Dies ist in meinem bereits erwähnten Buch beschrieben, darin befinden sich auch Literaturangaben zu allen wesentlichen Artikeln.

Nachdem Fermats letzter Satz vollständig bewiesen ist, sind diese Entwicklungen nun Teil der Geschichte von Fermats Satz geworden. Obige Kongruenzen haben ihre Bedeutung in anderen Bereichen der Zahlentheorie jedoch behalten.

Allgemeiner könnte man für eine beliebige Basis $a \geq 2$ (wobei a prim oder zerlegbar sein kann) diejenigen Primzahlen p betrachten, die a nicht teilen und für die $a^{p-1} \equiv 1 \pmod{p^2}$ erfüllt ist. Tatsächlich fragte Abel erstmals 1828 nach solchen Beispielen. Jacobi gab daraufhin die folgenden Kongruenzen mit $p \leq 37$ an:

$$\begin{aligned} 3^{10} &\equiv 1 \pmod{11^2} \\ 9^{10} &\equiv 1 \pmod{11^2} \\ 14^{28} &\equiv 1 \pmod{29^2} \\ 18^{36} &\equiv 1 \pmod{37^2} \end{aligned}$$

Den Quotienten

$$q_p(a) = \frac{a^{p-1} - 1}{p}$$

nennt man *Fermat-Quotient von p zur Basis a*. Der Rest modulo p des Fermat-Quotienten verhält sich ähnlich wie ein Logarithmus (was bereits von Eisenstein 1850 bemerkt wurde): Wenn p kein Teiler von ab ist, dann gilt

$$q_p(ab) \equiv q_p(a) + q_p(b) \pmod{p}.$$

Außerdem folgt

$$q_p(p-1) \equiv 1 \pmod{p}, \qquad q_p(p+1) \equiv -1 \pmod{p}.$$

In meinem Artikel *1093* (1983) sind zahlreiche interessante Eigenschaften des Fermat-Quotienten enthalten. Als Beispiel sei die folgende Kongruenz von Eisenstein (1850) erwähnt:

$$q_p(2) \equiv \frac{1}{p}\left(1 - \frac{1}{2} + \frac{1}{3} - \frac{1}{4} + \cdots - \frac{1}{p-1}\right) \pmod{p}.$$

Die folgenden Probleme sind ungelöst:

(1) Existieren zu gegebenem $a \geq 2$ unendlich viele Primzahlen p derart, dass $a^{p-1} \equiv 1 \pmod{p^2}$?

(2) Existieren zu gegebenem $a \geq 2$ unendlich viele Primzahlen p derart, dass $a^{p-1} \not\equiv 1 \pmod{p^2}$?

Die Antwort auf (1) sollte positiv ausfallen, warum auch nicht? Meine Aussage ist jedoch nicht gerade fundiert, denn das Problem ist ohne Zweifel sehr schwierig.

Die nächste Frage bezieht sich auf eine feste Primzahl bei variabler Basis:

(3) Gibt es zu einer ungeraden Primzahl p eine oder mehrere Basen a mit $2 \le a < p$ derart, dass $a^{p-1} \equiv 1 \pmod{p^2}$?

Hierzu sind wenige Ergebnisse bekannt. Kruyswijk zeigte 1966, dass eine Konstante C existiert, so dass für jede ungerade Primzahl p gilt:

$$\#\{a \mid 2 \le a < p,\, a^{p-1} \equiv 1 \pmod{p^2}\} < p^{\frac{1}{2}+\frac{C}{\log\log p}}.$$

Es gibt also nicht besonders viele Basen, die für ein primes p geeignet sind.

Granville bewies 1987, dass

$$\#\{q \text{ prim} \mid 2 \le q < p,\, q^{p-1} \equiv 1 \pmod{p^2}\} < p^{1/2}$$

und allgemeiner, wenn $u \ge 1$ und p eine Primzahl mit $p \ge u^{2u}$ ist, dann ist

$$\#\{q \text{ prim} \mid 2 \le q \le u^{1/u},\, q^{p-1} \equiv 1 \pmod{p^2}\} \ge up^{u/2}.$$

Außerdem gilt

$$\#\{q \text{ prim} \mid 2 \le q < p,\, q^{p-1} \not\equiv 1 \pmod{p^2}\} \ge \pi(p) - p^{1/2}.$$

Rekord

Keller & Richstein ermittelten 2001, dass es für $p = 6692367337$ genau 16 Basen a mit $2 \le a < p$ gibt, für die $a^{p-1} \equiv 1 \pmod{p^2}$ erfüllt ist. Dies sind $a = 5^k$ für $k = 1, 2, \ldots, 14$ sowie $a = 4961139411$ und $a = 6462265338$. Für $p = 188748146801$ existiert die gleiche Anzahl Lösungen für $a < p$, in diesem Fall sind dies $a = 5^k$ für $k = 1, 2, \ldots, 16$.

Der frühere Rekord stammte von Ernvall & Metsänkylä (1997) mit $p = 1645333507$ und 14 Basen $a < p$. Man beachte, dass alle drei Werte von p der Kongruenz $5^{p-1} \equiv 1 \pmod{p^2}$ genügen, siehe auch die folgende Tabelle.

Tabelle 22. Fermat-Quotienten, die durch p teilbar sind

Basis	Primzahlen p, die $a^{p-1} \equiv 1 \pmod{p^2}$ erfüllen
2	1093 3511
3	11 1006003
5	20771 40487 53471161 1645333507^{M} 6692367337^{K} 188748146801^{K}
7	5 491531
11	71
13	863 1747591
17	3 46021 48947 478225523351^{F}
19	3 7 13 43 137 63061489
23	13 2481757 13703077 15546404183^{R} 2549536629329^{F}
29	Keine
31	7 79 6451 2806861^{K}
37	3 77867 76407520781^{R}
41	29 1025273 138200401^{K}
43	5 103 13368932516573^{F}
47	Keine
53	3 47 59 97
59	2777 18088417183289^{F}
61	Keine
67	7 47 268573
71	3 47 331
73	3
79	7 263 3037 1012573^{K} 60312841^{K} 8206949094581^{F}
83	4871 13691 315746063^{C}
89	3 13
97	7 2914393^{K} 76704103313^{R}

Powell formulierte die Aussage, dass es unter der Voraussetzung $p \not\equiv 7 \pmod 8$ mindestens eine Primzahl $q < \sqrt{p}$ derart gibt, dass $q^{p-1} \not\equiv 1 \pmod{p^2}$ (1982 als Problem im *American Mathematical Monthly* gestellt, 1986 Veröffentlichung einer Lösung von Tzanakis).

Unter Verwendung stärkerer Methoden lässt sich zeigen, dass es für jede Primzahl $p \geq 11$ eine Primzahl q mit $2 \leq q < (\log p)^2$ derart gibt, dass $q^{p-1} \not\equiv 1 \pmod{p^2}$.

Angeregt durch die Berechnungen von Lehmer für den Fermat-Quotienten zur Basis 2 veröffentlichten Riesel (1964), Kloss (1965) und Brillhart, Tonascia & Weinberger (1971) Tabellen für Basen bis 100 und immer größere Exponentenbereiche.

Erweiterungen dieser Resultate stammen von Aaltonen & Inkeri (1991), Montgomery (1993), Keller & Richstein (2001, veröffentlicht 2005), sowie von R. Fischer (unveröffentlicht). Die aktuelle Tabelle umfasst alle Basen $a \leq 1000$ und folgende prime Exponenten:

$$\begin{aligned} p &< 2{,}1 \times 10^{13} \quad \text{für} \quad 3 \leq a \leq 61, \\ p &< 1{,}3 \times 10^{13} \quad \text{für} \quad 61 < a \leq 149, \\ p &< 4{,}1 \times 10^{12} \quad \text{für} \quad 149 < a \leq 1000. \end{aligned}$$

Für $a = 3, 5$ und 17 wurden von Mossinghoff (2009) sogar alle $p < 10^{14}$ untersucht.

Tabelle 22 beschränkt sich auf die primen Basen $a \leq 100$. Die Lösung, die mit einem C markiert ist, wurde von D. Clark gefunden, die mit einem M von P.L. Montgomery, solche mit einem K wurden von W. Keller und die mit einem R von J. Richstein entdeckt, während die mit einem F markierten von R. Fischer stammen.

IV Wilson-Primzahlen

Dieser Abschnitt ist sehr kurz – man weiß fast nichts.

Wilsons Satz besagt, dass die Kongruenz $(p-1)! \equiv -1 \pmod{p}$ für alle Primzahlen p erfüllt ist und daher der sogenannte *Wilson-Quotient*

$$W(p) = \frac{(p-1)! + 1}{p}$$

immer eine ganze Zahl darstellt.

Die Zahl p heißt eine *Wilson-Primzahl*, wenn $W(p) \equiv 0 \pmod{p}$ oder gleichbedeutend, wenn $(p-1)! \equiv -1 \pmod{p^2}$. Zum Beispiel sind $p = 5$, 13 Wilson-Primzahlen. Es ist unbekannt, ob es unendlich viele Wilson-Primzahlen gibt. Vandiver äußerte sich dazu folgendermaßen:

> Diese Frage scheint mir von solch besonderer Beschaffenheit zu sein, dass wenn ich irgendwann nach meinem Tod wiederauferstehen sollte und mir irgendein Mathematiker erzählte, dass sie endgültig gelöst ist, ich sofort wieder tot umfallen würde.

Rekord

Außer 5 und 13 ist nur eine weitere Wilson-Primzahl bekannt. Es ist 563, entdeckt von Goldberg im Jahre 1953 (eine der ersten erfolgreichen Suchen mit einem Computer).

Die Suche nach Wilson-Primzahlen wurde fortgesetzt durch E.H. Pearson, K.E. Kloss, W. Keller, H. Dubner sowie Gonter & Kundert (1988) bis 10^7. Im Jahre 1997 dehnten Crandall, Dilcher & Pomerance die Suche auf 5×10^8 aus. Ende Mai 2006 erreichten Carlisle, Crandall und Rodenkirch (persönliche Mitteilung) die Marke von 10^9.

Es wurde keine weitere Wilson-Primzahl gefunden.

V Repunit-Primzahlen

In der Vergangenheit entstand ein großes Interesse für Zahlen, deren Ziffern (zur Basis 10) sämtlich gleich 1 sind: 1, 11, 111, 1111, ... Man nennt solche Zahlen *Repunit-Zahlen*. Wann sind Repunit-Zahlen prim?

Für Zahlen der Form

$$111\ldots1 = \frac{10^n - 1}{9}\,,$$

deren n Ziffern alle gleich 1 sind, ist die Bezeichnung Rn gebräuchlich. Wenn Rn prim ist, dann muss dies schon für n gelten, denn wenn $a, b > 1$, dann gilt

$$\frac{10^{ab} - 1}{9} = \frac{10^{ab} - 1}{10^a - 1} \times \frac{10^a - 1}{9}$$

und beide Faktoren sind größer als 1.

Rekord

Lange Zeit waren die einzigen bekannten Repunit-Primzahlen $R2$, $R19$ und $R23$, nach Anbruch des Computerzeitalters kamen $R317$ (Williams 1978) und $R1031$ (Williams & Dubner 1986) hinzu.

Dubner hatte bis 1992 berechnet, dass die Repunit-Zahlen Rp für alle anderen Primzahlen $p < 20000$ zerlegbar sind. Diese Berechnungen wurden von J. Young, T. Granlund und H. Dubner bis $p < 60000$ erweitert. Im September 1999 (veröffentlicht 2002) entdeckte Dubner, dass $R49081$ eine Quasiprimzahl ist. Ein Jahr später (im Oktober 2000) fanden L. Baxter u. a., dass dies auch für $R86453$ gilt. Bis April 2007 hatte Dubner alle $p < 200000$ untersucht und dabei als nächsten Fall $R109297$ entdeckt. Unabhängig und fast gleichzeitig wurde diese Zahl auch von P. Bourdelais gefunden. Bald darauf zeigte M. Voznyy, dass $R270343$ ebenfalls eine Quasiprimzahl ist.

In der heutigen Zeit besteht praktisch keine Hoffnung, Zahlen dieser Größe als echte Primzahlen nachzuweisen. Im Rahmen eines von

Voznyy initiierten Gemeinschaftsprojekts wurden mittlerweile alle Rp mit $p < 1440000$ geprüft, ohne einen weiteren „Treffer“ zu erzielen.

Die vollständige Faktorisierung von Repunit-Zahlen Rp ist derzeit für alle $p \leq 271$ bekannt.

Offenes Problem: Gibt es unendlich viele Repunit-Primzahlen?

Mehr Informationen zu Repunit-Zahlen finden sich zum Beispiel im Buch von Yates (1982).

Man kann leicht einsehen, dass eine Repunit-Zahl (verschieden von 1) keine Quadratzahl sein kann. Kniffliger ist es zu zeigen, dass Repunit-Zahlen auch keine Kuben sein können (siehe Rotkiewicz, 1987). Auch eine fünfte Potenz ist ausgeschlossen (wie mir freundlicherweise R. Bond sowie K. Inkeri 1989 mitteilten). Es ist nicht bekannt, ob eine Repunit-Zahl für den Fall, dass k kein Vielfaches von 2, 3 oder 5 ist, eine k-te Potenz sein kann (siehe Obláth, 1956).

Williams & Seah betrachteten im Jahre 1979 auch Zahlen, die die Form $(a^n-1)/(a-1)$ haben, wobei $a \neq 2, 10$ (für $a = 2$ erhält man die Zahlen $2^n - 1$ und für $a = 10$ die Repunit-Zahlen). Diese Zahlen nennt man heute *verallgemeinerte Repunit-Zahlen* zur Basis a. Wie auch die „gewöhnlichen“ Repunit-Zahlen können auch sie höchstens dann prim sein, wenn dies schon für den Exponenten n gilt. Es ist im Allgemeinen sehr schwierig, die Primalität großer Zahlen dieses Typs nachzuweisen.

Tabelle 23. Primzahlen der Form $(a^n - 1)/(a - 1)$

a	n
3	3 7 13 71 103 541 1091 1367 1627 4177$^{\mathrm{DB}}$ 9011* 9551* 36913* [42700] 43063* 49681* 57917* 483611* 877843*
5	3 7 11 13 47 127 149 181 619 929 3407$^{\mathrm{W}}$ 10949* 13241* 13873* 16519* [31400] 201359* 396413*
6	2 3 7 29 71 127 271 509 1049 6389* 6883$^{\mathrm{S1}}$ 10613* 19889* [29800] 79987* 608099*
7	5 13 131 149 1699$^{\mathrm{DB}}$ 14221* [28200] 35201* 126037* 371669*
11	17 19 73 139 907 1907$^{\mathrm{S2}}$ 2029$^{\mathrm{S2}}$ 4801$^{\mathrm{B}}$ 5153* 10867* 20161* [24000] 293831*
12	2 3 5 19 97 109 317 353 701 9739* 14951* [26300] 37573* 46889*

In seinem 1993 veröffentlichten Artikel hatte Dubner die betrachteten Basen a bis mindestens $n \leq 10400$ abgedeckt. Seine viel umfangreichere Tabelle enthielt alle Basen $a \leq 99$. Die obige Tabelle wurde im Jahre 2002 durch A. Steward bis zu den Grenzen erweitert, die in eckige Klammern gesetzt sind. Später wurden die Berechnungen durch P. Bourdelais wieder aufgenommen.

Mit einem Stern sind Quasiprimzahlen gekennzeichnet, deren Primalität noch nicht nachgewiesen werden konnte. Die Quasiprimzahlen, die jenseits der Grenzen von Steward gefunden wurden, sind folgenden Entdeckern zuzuordnen:

$a = 3$, $n = 43063$: R. Ballinger 2000,
$a = 3$, $n = 49681$ und 57917: H. Lifchitz 2003,
$a = 12$, $n = 37573$: H. Lifchitz 2007.

Alle übrigen wurden in den Jahren 2007 bis 2010 von Bourdelais entdeckt, der auch zeigte, dass bis zur höchsten der jeweils aufgelisteten Quasiprimzahlen keine weiteren existieren.

Diejenigen Einträge in der Liste, bei denen die verallgemeinerte Repunit-Zahl im strengen Sinne als prim nachgewiesen wurde, sind durch die Initialen der Beweisführer bezeichnet:

DB: H. Dubner und R.P. Brent 1996,
S1: A. Steward 2000,
B: D. Broadhurst 2001,
W: T. Wu 2005,
S2: A. Steward 2006.

VI Zahlen der Form $k \times b^n \pm 1$

Wie ich in Kapitel 2 erwähnte, haben die Teiler von Fermat-Zahlen die Form $k \times 2^n + 1$. Diese Eigenschaft brachte die Zahlen ins Rampenlicht, und so war es naheliegend, sie auf ihre Primalität hin zu untersuchen.

Außer den Mersenne-Zahlen (mit $k = 1$) wurden auch andere Zahlen der Form $k \times 2^n - 1$ auf Primalität getestet.

Aufgrund des Satzes von Dirichlet über Primzahlen in arithmetischen Folgen gibt es für jedes $n \geq 1$ unendlich viele Zahlen $k \geq 1$ und $k' \geq 1$ derart, dass $k \times 2^n + 1$ bzw. $k' \times 2^n - 1$ Primzahlen sind.

Eine sehr interessante Frage ergibt sich, wenn man den Faktor k fest wählt: Es sei $k \geq 1$ gegeben. Gibt es eine Zahl $n \geq 1$ derart, dass $k \times 2^n + 1$ (bzw. $k \times 2^n - 1$) prim ist? Diese Frage geht auf Bateman zurück, Erdös & Odlyzko (1979) fanden eine Antwort:

Für eine beliebige reelle Zahl $x \geq 1$ bezeichne $N(x)$ die Anzahl der ungeraden Zahlen k mit $1 \leq k \leq x$ derart, dass es ein $n \geq 1$ gibt, für das $k \times 2^n + 1$ (bzw. $k \times 2^n - 1$) eine Primzahl ist. Dann existiert ein effektiv berechenbares $C_1 > 0$, so dass $N(x) \geq C_1 x$ (für jedes $x \geq 1$). Die entwickelte Methode eignet sich auch zur Untersuchung anderer Folgen.

Obwohl es einen positiven Anteil von Zahlen $k \geq 1$ mit der Eigenschaft gibt, dass $k \times 2^n + 1$ (oder $k \times 2^n - 1$) für irgendein n Primzahl ist, fand Riesel 1956, dass für $k = 509203$ die Zahl $k \times 2^n - 1$ für alle $n \geq 1$ zerlegbar ist. Sein in Schwedisch verfasster Artikel war Sierpiński sicher nicht zugänglich, als er 1960 den folgenden interessanten Satz bewies:

Es gibt unendlich viele ungerade Zahlen k derart, dass $k \times 2^n + 1$ für jedes $n \geq 1$ zerlegbar ist.

Die Zahlen k mit obiger Eigenschaft nennt man *Sierpiński-Zahlen*. Es ist nur konsequent, die ungerade Zahl k eine *Riesel-Zahl* zu nennen, wenn $k \times 2^n - 1$ für jedes $n \geq 1$ zerlegbar ist.

Aus dem Satz von Dirichlet über Primzahlen in arithmetischen Folgen und Sierpińskis Resultat ergibt sich, dass es unendlich viele Sierpiński-Zahlen gibt, die prim sind. Auf die gleiche Weise kann man schließen, dass es unendlich viele Riesel-Zahlen gibt, die prim sind.

Rekord

Die kleinste bekannte Sierpiński-Zahl ist $k = 78557 = 17 \times 4621$ und wurde im Jahre 1963 von Selfridge entdeckt. Die kleinste bekannte prime Sierpiński-Zahl ist $k = 271129$. Die kleinste bekannte Riesel-Zahl ist die von Riesel selbst gefundene Primzahl $k = 509203$.

Über viele Jahre hinweg hat Keller große Anstrengungen unternommen, einem Beweis der Vermutung nahe zu kommen, dass keine kleinere Sierpiński-Zahl k existiert. Er zeigte (1991), dass $k \geq 4847$ und dass es nur 35 ungerade Zahlen k im Intervall $4847 \leq k < 78557$ gibt, die als mögliche Sierpiński-Zahlen in Frage kommen. Von diesen 35 Kandidaten wurden 14 von J. Young im Jahre 1997 ausgeschlossen.

Vier weitere der Liste konnten mit Hilfe von Gallots Testprogramm gestrichen werden: Zwei durch M. Thibeault (im Jahre 1999), eine durch L. Baxter und eine durch J. Szmidt, beide in 2001.

Ein groß angelegter Angriff auf die verbleibenden 17 Kandidaten wurde von L. Helm und D. Norris gestartet, die ein verteiltes Rechenprojekt organisierten, welches gegen Ende 2002 innerhalb weniger Wochen fünf Kandidaten zu Fall brachte. In der Zeit vom Dezember 2003 bis Oktober 2007 gelang es ihnen, noch weitere sechs der Vorfaktoren zu eliminieren. Demnach verbleiben jetzt nur noch die folgenden sechs Werte zur weiteren Untersuchung:

$$k = 10223,\ 21181,\ 22699,\ 24737,\ 55459,\ 67607.$$

Neuerdings hat man sich auch der Frage zugewandt, ob sich die Vermutung, dass $k = 271129$ tatsächlich die kleinste prime Sierpiński-Zahl sei, auf rechnerischem Wege bestätigen lässt. Außer den obigen Kandidaten $k = 10223,\ 22699,\ 67607$ wären dazu nur noch $k = 79309,\ 79817,\ 152267,\ 156511,\ 168451,\ 222113,\ 225931,\ 237019$ auszuschließen.

In Bezug auf mögliche Riesel-Zahlen k mit $k < 509203$ zeigte Keller, dass $k \geq 659$. Auch für dieses Problem hat sich ein koordiniertes Rechenprojekt etabliert, welches unter der Leitung von L. Stephens dafür sorgte, dass derzeit noch 64 Werte zu untersuchen sind. Die ersten dieser Werte lauten

$$k = 2293,\ 9221,\ 23669,\ 31859,\ 38473,\ 40597,\ 46663,\ 65531,\ \ldots\ .$$

Die umfangreichen Berechnungen, die eigentlich dazu dienten, diverse Kandidaten zu eliminieren, führten zugleich zur Entdeckung sehr großer Primzahlen. So wurden $k = 19249,\ 27653,\ 28433,\ 33661,\ 90527$ und $k = 258317$ als Sierpiński-Zahlen ausgeschlossen, indem Primzahlen entdeckt wurden, die in Tabelle 24 sechs Positionen einnehmen, darunter die obersten fünf.

Die größte Primzahl, die im Zusammenhang mit dem Riesel-Problem gefunden wurde, ist die 1086531-stellige Zahl $485767 \times 2^{3609357} - 1$. Im Rahmen des betreffenden Rechenvorhabens war C. Cardall ihr glücklicher Entdecker, der sie im Juni 2008 fand. Es ist übrigens sichergestellt (was für die Eliminierung nicht erforderlich ist), dass $485767 \times 2^n - 1$ für alle $n < 3609357$ zerlegbar ist.

Rekorde

Die größte bekannte Primzahl der Form $k \times 2^n + 1$ ist $19249 \times 2^{13018586} + 1$ (3918990 Stellen), gefunden im Mai 2007. Sie ist zugleich die größte, die nicht vom Mersenne-Typ ist, siehe die nachfolgende Tabelle. Die größte bekannte Primzahl der Form $k \times 2^n - 1$ ist $3 \times 2^{6090515} - 1$

(1833429 Stellen). Sie wurde im April 2010 im Rahmen eines Projekts namens PrimeGrid von D. Mumper, G. Reynolds und J. Penné entdeckt.

PrimeGrid beherbergt seit 2006 diverse Primzahlprojekte, die bei der systematischen Suche nach Rekordprimzahlen bereits große Erfolge verzeichnen konnten, von denen an verschiedenen Stellen dieses Buches zu berichten ist. Das Gesamtprojekt steht unter der Federführung von R. Slatkevičius und J. Blazek.

Während die neun größten derzeit bekannten Primzahlen Mersenne-Zahlen sind, zeigt Tabelle 24 die zehn größten bekannten Primzahlen, die keine Mersenne-Zahlen sind. Auf sieben dieser Zahlen wurde bereits gesondert hingewiesen. Den beiden Primzahlen der Form $n \times 2^n + 1$ werden wir bald noch einmal begegnen.

Rekorde

Tabelle 24. Die größten bekannten Nicht-Mersenne-Primzahlen

Primzahl	Stellen	Entdecker	Jahr
$19249 \times 2^{13018586} + 1$	3918990	K. Agafonov, G. Woltman, L. Helm, D. Norris u. a.	2007
$27653 \times 2^{9167433} + 1$	2759677	D. Gordon, G. Woltman, L. Helm, D. Norris u. a.	2005
$90527 \times 2^{9162167} + 1$	2758093	P. Salah, G. Reynolds, J. Penné und PrimeGrid	2010
$28433 \times 2^{7830457} + 1$	2357207	N.N., G. Woltman, L. Helm, D. Norris u. a.	2004
$33661 \times 2^{7031232} + 1$	2116617	S. Sunde, G. Woltman, L. Helm, D. Norris u. a.	2007
$6679881 \times 2^{6679881} + 1$	2010852	N.N., G. Reynolds, J. Penné und PrimeGrid	2009
$6328548 \times 2^{6328548} + 1$	1905090	D.R. Gesker, G. Reynolds, J. Penné und PrimeGrid	2009
$3 \times 2^{6090515} - 1$	1833429	D. Mumper, G. Reynolds, J. Penné und PrimeGrid	2010
$258317 \times 2^{5450519} + 1$	1640776	S. Gilvey, G. Reynolds, J. Penné und PrimeGrid	2008
$3 \times 2^{5082306} + 1$	1529928	A. Brady, G. Reynolds, J. Penné und PrimeGrid	2009

Verallgemeinerte Fermat-Zahlen

Es handelt sich um Primzahlen der Form $b^{2^m} + 1$. Dies ist ein Spezialfall von $k \times b^n + 1$ mit $k = 1$, $n = 2^m$ und geradem b. Zahlen $b^{2^m} + 1$ mit $b \geq 2$ und $m \geq 1$ heißen *verallgemeinerte Fermat-Zahlen*. Es war Dubner, der 1985 erstmals größere Primzahlen dieser Gestalt (auch kurz *verallgemeinerte Fermat-Primzahlen* genannt) ermittelte. Die größte darunter war die Zahl $150^{2^{11}} + 1$ mit 4457 Stellen.

Etwa 1998 bemerkte Y. Gallot, dass verallgemeinerte Fermat-Zahlen mit einer vergleichbaren Geschwindigkeit getestet werden können wie Mersenne-Zahlen der gleichen Größe. Dass dies in der Praxis funktioniert, zeigte er durch die Entwicklung eines Computerprogramms, das er nach und nach weiter optimierte. Tatsächlich ist der Test deutlich schneller als für Zahlen der Formen $k \times 2^n \pm 1$ mit $k > 1$. Die verwendete Arithmetik benutzt die Methode der diskreten gewichteten Transformation (Discrete Weighted Transform, abgekürzt DWT) von Crandall & Fagin (1994), die auch beim Nachweis der 13 größten bekannten Mersenne-Primzahlen zum Einsatz kam (Projekt GIMPS).

Historisch gesehen war die größte bekannte Primzahl fast immer eine Mersenne-Primzahl. Mit einer Ausnahme im August 1989, als die Primzahl $391581 \times 2^{216193} - 1$, entdeckt von den sechs ergebenen Numerologen J. Brown, L.C. Noll, B. Parady, G. Smith, J. Smith und S. Zarantonello, die Mersenne-Primzahl M_{216091} entthront hatte. Armer Mersenne, der sich eine Zeit lang vor lauter Sorgen und Trauer im Grabe herumdrehen musste, bis ihn schließlich der Erfolg seiner Mersenne-Primzahlen wieder in Frieden ruhen ließ. Aber wie lange wird dieser Frieden andauern?

Wie Dubner & Gallot (2002) in ihrem Artikel erläutern, gibt es erwartungsgemäß sehr viel mehr verallgemeinerte Fermat-Primzahlen vergleichbarer Größenordnung, und daher könnte nach ihren Aussagen eine gut organisierte Suche die Rangordnung unter den größten bekannten Primzahlen schon bald verändern. Etwa 40 Primzahlen der genannten Form mit mehr als 400000 Stellen konnten bereits bestimmt werden, darunter auch eine Megaprimzahl. Der erwartete Durchbruch lässt allerdings noch auf sich warten.

Weitere interessante Rekorde, die sich auf Zahlen der Form $k \times b^n + 1$ mit $b > 2$ beziehen, sind die folgenden:

Rekorde

A. Die 1150678-stellige verallgemeinerte Fermat-Zahl $24518^{2^{18}} + 1$ ist die größte bekannte Primzahl der Form $N^2 + 1$. Sie wurde im März 2008 von S. Scott, D. Underbakke und Y. Gallot entdeckt. Man erinnere sich, dass bis heute nicht bekannt ist, ob es unendlich viele Primzahlen dieser Form gibt.

B. Die größten bekannten Primzahlen der Formen $k \times b^n \pm 1$ mit $k > 1$ und ungeradem $b > 2$ sind $2 \times 3^{1175232} + 1$ (560729 Stellen), im Februar 2010 von D. Broadhurst, P. Jobling und J. Fougeron entdeckt, und $563528 \times 13^{563528} - 1$ (627745 Stellen), im Dezember 2009 von L. Vogel, G. Reynolds, M. Rodenkirch, J. Fougeron und PrimeGrid entdeckt.

Cullen-Zahlen

Zahlen der Form $Cn = n \times 2^n + 1$ sind unter der Bezeichnung *Cullen-Zahlen* bekannt. Robinson zeigte 1958, dass $C141$ eine Primzahl ist und wies die Zerlegbarkeit aller Cn mit $1 < n \leq 1000$ nach. Gut 25 Jahre lang war dies die einzige bekannte Cullen-Primzahl, außer natürlich $C1 = 3$.

Keller bestimmte 1987 (veröffentlicht 1995) alle Cullen-Primzahlen Cn mit $n \leq 30000$. Diese Berechnungen wurden von J. Young (1997) bis $n \leq 100000$ ausgedehnt. Danach konnten dank Y. Gallots Programm weitere drei Primzahlen gefunden werden. Wie man heute weiß, war damit die Liste bis $n \leq 1000000$ komplett. Jenseits dieser Grenze fanden zunächst M. Rodenkirch und J. Penné im August 2005 eine weitere Cullen-Primzahl mit $n = 1354828$. Seitdem wurden im Rahmen des PrimeGrid-Projekts alle Exponenten $n \leq 7870000$ untersucht und dabei zwei Cullen-Megaprimzahlen entdeckt. Die größte wurde im August 2009 von einem japanischen Teilnehmer gefunden, dessen Identität nicht ermittelt werden konnte. Die bekannten Cullen-Primzahlen finden sich in Tabelle 25.

In seinem Buch (1976) weist Hooley darauf hin, dass fast alle Cullen-Zahlen Cn zerlegbar sind. Genauer gilt

$$\lim_{x \to \infty} \frac{C\pi(x)}{x} = 0,$$

wobei $C\pi(x)$ die Anzahl der Cullen-Zahlen $Cn \leq x$ bezeichnet, die prim sind. Bislang ist jedoch unbekannt, ob es unendlich viele Cullen-Primzahlen Cn gibt.

Tabelle 25. Cullen-Primzahlen Cn

n	Entdecker	Jahr
6679881	N.N. u. a. und PrimeGrid	2009
6328548	D.R. Gesker u. a. und PrimeGrid	2009
1354828	M. Rodenkirch und J. Penné	2005
481899	M. Morii und Y. Gallot	1998
361275	D. Smith und Y. Gallot	1998
262419	D. Smith und Y. Gallot	1998
90825	J. Young	1997
59656	J. Young	1997
32469	M. Morii	1997
32292	M. Morii	1997
18496	W. Keller	1984
6611	W. Keller	1984
5795	W. Keller	1984
4713	W. Keller	1984
141	R.M. Robinson	1958
1	–	–

Die Zahlen $Wn = n \times 2^n - 1$ nennt man *Woodall-Zahlen* oder auch Cullen-Zahlen der zweiten Art.

Im Bereich $n \leq 20000$ ist Wn genau dann prim, wenn $n = 2$, 3, 6, 30, 75, 81 (Riesel, 1969), 115, 123, 249, 362, 384, 462, 512, 751, 822, 5312, 7755, 9531, 12379, 15822 und 18885 (Keller, 1987). Die Berechnungen wurden von J. Young bis $n \leq 100000$ fortgesetzt. Mit Hilfe von Y. Gallots Programm wurden weitere drei Primzahlen entdeckt, mit denen die Liste hier ebenfalls bis $n \leq 1000000$ vollständig ist. Wiederum fanden M. Rodenkirch und J. Penné (Juli 2005) eine Primzahl jenseits dieser Grenze, diesmal mit $n = 1195203$.

Im Rahmen des PrimeGrid-Projekts wurden seitem alle $n \leq 8090000$ untersucht – mit dem in Tabelle 26 gezeigten Erfolg. In der Tabelle sind nur die bekannten Woodall-Primzahlen mit $n > 20000$ aufgelistet.

Im Übrigen haben W. Keller & W. Niebuhr (1995) die vollständigen Faktorisierungen der Zahlen Cn und Wn für alle $n \leq 300$ bestimmt. Diese Berechnungen hat P. Leyland bis November 1998 auf alle $n \leq 400$ und bis August 2000 auf alle $n \leq 450$ ausgedehnt. Unter Mitwirkung verschiedener Helfer wurden die Faktortabellen inzwischen bis $n \leq 650$ komplettiert (August 2009).

Tabelle 26. Die größten bekannten Woodall-Primzahlen Wn

n	Entdecker	Jahr
3752948	M.J. Thompson u. a. und PrimeGrid	2007
2367906	S. Kohlman u. a. und PrimeGrid	2007
2013992	L.M. Andersen u. a. PrimeGrid	2007
1467763	W. Siemelink u. a. PrimeGrid	2007
1268979	W. Siemelink u. a. PrimeGrid	2007
1195203	M. Rodenkirch und J. Penné	2005
667071	M. Toplic und Y. Gallot	2000
151023	K. O'Hare und Y. Gallot	1998
143018	R. Ballinger und Y. Gallot	1998
98726	J. Young	1997
23005	J. Young	1997
22971	J. Young	1997

Cullen-Zahlen (beider Arten) lassen sich in der Form $n \times b^n + 1$ und $n \times b^n - 1$ mit $b > 2$ verallgemeinern. *Verallgemeinerte Cullen-Zahlen* $n \times b^n + 1$ wurden von Dubner in 1989 eingeführt. Er untersuchte das mögliche Auftreten von Primzahlen dieser Form und bemerkte dabei, dass es für prime Basen $b > 3$ kaum Primzahlen gibt. Tatsächlich fand er für $b = 13, 17, 19, 23, 29, 31, 41, 47, 53, 71, 73$ keine einzige Primzahl. Es erschien jedoch unwahrscheinlich, dass man für auch nur eine dieser Basen die Nichtexistenz von Primzahlen beweisen könnte.

Durch intensive Berechnungen konnte später gezeigt werden, dass der erste Exponent n, für den eine Primzahl auftaucht, recht groß sein kann. Mit Hilfe von Gallots Programm, das auch Zahlen dieser Form handhaben kann, wurden „kleinste" Primzahlen für $b = 19, 23$ (Keller 1998) und für $b = 17, 71$ (Löh 2000) gefunden. Zuletzt entdeckte Löh (April 2002) für $b = 31$ die Primzahl $82960 \times 31^{82960} + 1$ mit 123729 Stellen. Trotz weiterer Bemühungen sind die verbleibenden Fälle $b = 13, 29, 41, 47, 53, 73$ bislang ungeklärt geblieben.

VII Primzahlen und linear rekurrente Folgen zweiter Ordnung

In diesem Abschnitt werde ich Folgen $T = (T_n)_{n\geq 0}$ betrachten, die durch lineare rekurrente Folgen zweiter Ordnung definiert sind.

Allgemeine lineare rekurrente Folgen zweiter Ordnung

Es seien P, Q zwei von Null verschiedene ganze Zahlen derart gegeben, dass $D = P^2 - 4Q \neq 0$. Diese Zahlen P, Q sind die Parameter der Folge T, die nun definiert werden soll. Seien T_0, T_1 ganze Zahlen (von 0 verschieden) und für jedes $n \geq 2$ sei

$$T_n = PT_{n-1} - QT_{n-2}.$$

Das charakteristische Polynom der Folge T ist $X^2 - PX + Q$; seine Wurzeln sind

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

Somit ist $\alpha + \beta = P$, $\alpha\beta = Q$, $\alpha - \beta = \sqrt{D}$.

Die Folgen $(U_n)_{n\geq 0}$, $(V_n)_{n\geq 0}$ mit Parametern (P, Q) und $U_0 = 0$, $U_1 = 1$ (bzw. $V_0 = 2$, $V_1 = P$) sind exakt die Lucas-Folgen, die bereits in Kapitel 2, Abschnitt IV untersucht worden sind.

Es sei $\gamma = T_1 - T_0\beta$, $\delta = T_1 - T_0\alpha$. Dann lässt sich leicht zeigen, dass

$$T_n = \frac{\gamma\alpha^n - \delta\beta^n}{\alpha - \beta} = T_1\frac{\alpha^n - \beta^n}{\alpha - \beta} - QT_0\frac{\alpha^{n-1} - \beta^{n-1}}{\alpha - \beta}$$

für jedes $n \geq 0$ gilt.

Wenn $U = (U_n)_{n\geq 0}$ die Lucas-Folge mit den gleichen Parametern ist, dann ist $T_n = T_1U_n - QT_0U_{n-1}$ (für $n \geq 2$).

Man kann auch die Begleitfolge $W = (W_n)_{n\geq 0}$ definieren. Sei

$$W_0 = 2T_1 - PT_0, \qquad W_1 = T_1P - 2QT_0$$

und

$$W_n = PW_{n-1} - QW_{n-2}, \quad \text{für } n \geq 2.$$

Wieder gilt $W_n = \gamma\alpha^n + \delta\beta^n = T_1V_n - QT_0V_{n-1}$, wobei $V = (V_n)_{n\geq 0}$ die begleitende Lucas-Folge mit Parametern (P, Q) ist.

Ich könnte nun genau wie bei den Lucas-Folgen aus Kapitel 2, Abschnitt IV algebraische Zusammenhänge und Teilbarkeitseigenschaften dieser Folgen herleiten. Meine Absicht ist jedoch, nur solche Eigenschaften zu untersuchen, die mit Primzahlen zu tun haben.

Die Primteiler einer Folge T

Man betrachte die Menge

$$\mathcal{P}(T) = \{p \text{ prim} \mid \text{es gibt } n \text{ derart, dass } T_n \neq 0 \text{ und } p \mid T_n\}.$$

Die Folge T heißt *entartet*, wenn $\alpha/\beta = \eta$ eine Einheitswurzel ist. Dann ist auch $\beta/\alpha = \eta^{-1}$ eine Einheitswurzel; daher $|\eta + \eta^{-1}| \leq 2$. Aber

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

so dass für entartetes T gilt: $P^2 - 2Q = 0, \pm Q, \pm 2Q$.

Es ist nicht schwer zu zeigen, dass die Menge $\mathcal{P}(T)$ für entartetes T endlich ist.

Ward zeigte 1954, dass auch die Umkehrung richtig ist:

Für eine nicht-entartete Folge T ist $\mathcal{P}(T)$ unendlich.

Ein natürliches Problem stellt sich in der Frage, ob $\mathcal{P}(T)$ notwendigerweise eine positive Dichte hat (in der Menge aller Primzahlen), und falls möglich, sie auszurechnen.

Pionierarbeit leistete Hasse (1966), der die Menge der Primzahlen p untersuchen wollte, für die die Ordnung von 2 modulo p gerade ist. Das bedeutet, dass es ein $n \geq 1$ derart gibt, dass p Teiler von $2^{2n} - 1$ ist, aber p die Zahl $2^m - 1$ für alle $1 \leq m < 2n$ nicht teilt. Somit $2^n \equiv -1 \pmod{p}$, also ist p Teiler von $2^n + 1$ und umgekehrt.

Die Folge $H = (H_n)_{n\geq 0}$ mit $H_n = 2^n + 1$ ist die begleitende Lucas-Folge mit Parametern $P = 3$, $Q = 2$. Sei

$$\pi_H(x) = \#\{p \in \mathcal{P}(H) \mid p \leq x\}, \quad \text{für jedes } x \geq 1.$$

Hasse zeigte, dass

$$\lim_{x\to\infty} \frac{\pi_H(x)}{\pi(x)} = \frac{17}{24}.$$

Die Zahl 17/24 stellt die Dichte der Primzahlen p dar, die die Folge H teilen, das heißt, für die es ein n derart gibt, dass $p \mid H_n$.

Lagarias überarbeitete 1985 Hasses Methode und zeigte unter Anderem, dass für die Folge $V = (V_n)_{n\geq 0}$ der Lucas-Zahlen die Menge $\mathcal{P}(V)$ die Dichte 2/3 hat.

Die vorherrschende Vermutung ist, dass die Menge $\mathcal{P}(T)$ für jede nicht-entartete Folge T eine positive Dichte hat.

Primzahlen in Folgen T

Ich wende mich nun einem weiteren sehr interessanten und schwierigen Problem zu.

Es sei $T = (T_n)_{n\geq 0}$ eine linear rekurrente Folge zweiter Ordnung, zum Beispiel die Folge der Fibonacci-Zahlen oder der Lucas-Zahlen. Diese Folgen enthalten Primzahlen, aber es ist unbekannt, ob es unendlich viele sind, und der Nachweis wäre sicher sehr schwierig.

Aus den Formeln (IV.15) und (IV.16) des Kapitels 2, Abschnitt IV folgt:

Wenn U_m prim ist, dann ist $m = 4$ oder m ist eine Primzahl.

Wenn V_m prim ist, dann ist m eine Zweierpotenz oder m ist eine Primzahl.

Natürlich muss die jeweilige Umkehrung nicht wahr sein.

Man hat sehr viel Rechenzeit in die Suche nach Fibonacci- und Lucas-Primzahlen sowie in deren Faktorisierung investiert (siehe Kapitel 2, Abschnitt XI, D). Da die Zahlen dieser Folgen schnell anwachsen, ist man beim Test auf Primalität und bei der Faktorisierung mit schwierigen Problemen konfrontiert.

Von den veröffentlichten Arbeiten möchte ich Jardens Buch von 1958 in seiner dritten Auflage erwähnen, überarbeitet und erweitert von Brillhart (1973). Außerdem die Artikel von Brillhart, Montgomery & Silverman (1988) und von Dubner & Keller (1999). Der gegenwärtige Wissensstand ist wie folgt.

Die Fibonacci-Zahl U_n ist prim für

$$\begin{aligned} n = {} & 3, 4, 5, 7, 11, 13, 17, 23, 29, 43, 47, 83, 131, 137, 359, 431, 433, \\ & 449, 509, 569, 571, 2971^{\mathrm{W}}, 4723^{\mathrm{WM}}, 5387^{\mathrm{WM}}, 9311^{\mathrm{DK}}, 9677^{\mathrm{deW}}, \\ & 14431^{\mathrm{BdeW}}, 25561^{\mathrm{BdeW}}, 30757^{\mathrm{BdeW}}, 35999^{\mathrm{BdeW}}, 37511^{\mathrm{BdeW}}, \\ & 50833^{\mathrm{BdeW}}, 81839^{\mathrm{BdeW}}, \end{aligned}$$

und wurde bislang nur als quasiprim erkannt für

$$\begin{aligned} n = {} & 104911, 130021, 148091, 201107, 397379, 433781, 590041, \\ & 593689, 604711, 931517, 1049897, 1285607, 1636007, 1803059, \\ & 1968721. \end{aligned}$$

Die letzte dieser Zahlen, $U_{1968721}$, hat 411439 Dezimalstellen. Die Quasiprimzahl U_{104911} wurde von B. de Water entdeckt, U_{130021} von

D. Fox, U_{148091} von T.D. Noe, und alle weiteren von H. Lifchitz. Die Liste ist bis $n = 2253000$ vollständig.

Die an einigen Zahlen angebrachten Buchstaben bedeuten, dass die Primalität der betreffenden Fibonacci-Zahl nachgewiesen wurde von

W: H.C. Williams,
WM: H.C. Williams und F. Morain,
DK: H. Dubner und W. Keller,
deW: B. de Water,
BdeW: D. Broadhurst und B. de Water.

Der Primalitätsbeweis für die 17103-stellige Zahl U_{81839} stellt eine bemerkenswerte Leistung dar.

Des Weiteren ist bekannt, dass die Lucas-Zahl V_n prim ist für

$$n = 2, 4, 5, 7, 8, 11, 13, 16, 17, 19, 31, 37, 41, 47, 53, 61, 71, 79, 113, 313, 353, 503^{\mathrm{W}}, 613^{\mathrm{W}}, 617^{\mathrm{W}}, 863^{\mathrm{W}}, 1097^{\mathrm{DK}}, 1361^{\mathrm{DK}}, 4787^{\mathrm{DK}}, 4793^{\mathrm{DK}}, 5851^{\mathrm{DK}}, 7741^{\mathrm{DK}}, 8467^{\mathrm{deW}}, 10691^{\mathrm{DK}}, 12251^{\mathrm{BdeW}}, 13963^{\mathrm{Oak}}, 14449^{\mathrm{DK}}, 19469^{\mathrm{BdeW}}, 35449^{\mathrm{deW}}, 36779^{\mathrm{deW}}, 44507^{\mathrm{BdeW}}, 51169^{\mathrm{BdeW}}, 56003^{\mathrm{BI}},$$

und bislang nur als quasiprim erkannt wurde für

$$n = 81671, 89849, 94823, 140057, 148091, 159521, 183089, 193201, 202667, 344293, 387433, 443609, 532277, 574219, 616787, 631181, 637751, 651821, 692147, 901657, 1051849.$$

Die Quasiprimzahlen V_{81671} und V_{89849} sind Dubner zu verdanken, V_{140057} und V_{148091} wurden von de Water entdeckt, und alle übrigen von H. oder R. Lifchitz (Henri und Renaud, Vater und Sohn). Diese Liste ist bis $n = 1200000$ komplett.

Für die Primbeweise gelten die gleichen Bezeichnungen wie oben, mit den zusätzlichen Abkürzungen

Oak: M. Oakes,
BI: D. Broadhurst und S.A. Irvine.

Wenn Sie sich die obigen Listen noch einmal anschauen, werden Sie feststellen, dass für die Primzahlen $n = 5$, 7, 11, 13, 17, 47 sowohl U_n als auch V_n prim sind. Dies passiert dann zunächst nicht wieder, bis man auf $n = 148091$ stößt, wo überraschenderweise U_n und V_n beide quasiprim sind. Wenn (oder falls) gezeigt werden sollte, dass diese

Zahlen tatsächlich Primzahlen sind, dann könnte man den Eindruck gewinnen, dass es womöglich unendlich viele prime n gibt, für die U_n und V_n beide Primzahlen sind. Diese Nuss wird wohl schwer zu knacken sein. Lassen Sie sich nicht den Schlaf rauben, Nüsse sind schwer verdaulich.

Folgen T mit ausschließlich zerlegbaren Zahlen

Man sollte beachten, dass eine Folge T, die weder eine Lucas-Folge noch eine begleitende Lucas-Folge ist, durchaus keine Primzahl enthalten kann. Graham entdeckte 1964 ein Beispiel mit $P = 1$, $Q = -1$; allerdings erwies sich die Berechnung von T_0 und T_1 als fehlerhaft. Im Jahre 1990 gab Knuth die richtigen Werte an,

$$T_0 = 331635635998274737472200656430763,$$
$$T_1 = 151002891108840197118959030549878 5,$$

sowie ein weiteres Beispiel mit kleineren Werten von T_0 und T_1:

$$T_0 = 62638280004239857,$$
$$T_1 = 49463435743205655.$$

Ebenfalls mit $P = 1$, $Q = -1$ fand Vsemirnov im Jahre 2004 ein Beispiel mit den bisher kleinsten Anfangswerten

$$T_0 = 106276436867,$$
$$T_1 = 35256392432.$$

Es sei nun $P = 3$, $Q = 2$. Die Lucas-Folge und die begleitende Lucas-Folge mit diesen Parametern sind U, V mit $U_n = 2^n - 1$, $V_n = 2^n + 1$, und diese Folgen enthalten Primzahlen. Mit $T_0 = k+1$, $T_1 = 2k+1$ und den Parametern $P = 3$, $Q = 2$ erhält man die Folge mit $T_n = k \times 2^n + 1$. Für $T'_0 = k - 1$, $T'_1 = 2k - 1$ ergibt sich $T'_n = k \times 2^n - 1$.

Diese Folgen wurden im vorigen Abschnitt behandelt, wo gesagt wurde, dass es unendlich viele ungerade Zahlen k gibt (die Sierpiński-Zahlen), für die jedes T_n zerlegbar ist; analog gibt es unendlich viele Zahlen k (die Riesel-Zahlen), für die T'_n zerlegbar ist.

Im Jahre 2002 beschrieb Izotov unendlich viele Paare teilerfremder Parameter (P, Q) und für jedes dieser Paare unendlich viele Paare von Anfangswerten derart, dass die entsprechende Folge nur aus zerlegbaren Zahlen besteht.

Die NSW-Zahlen

NSW bedeutet nicht Nord-Süd-West oder New South Wales, sondern steht für Newman, Shanks & Williams (1980), und ich hatte die Ehre, deren Artikel bereits einsehen zu dürfen, als er noch nicht zur Veröffentlichung freigegeben war. Dies war kurz nach dem Besuch von Dan Shanks an der Queen's University, der aus mehr als einem Grund denkwürdig ist.

Die NSW-Zahlen, wie sie in dem Artikel vorgestellt werden, sind für ungerade Indizes definiert: $S_1 = 1$, $S_3 = 7$, $S_5 = 41$, $S_7 = 239$, $S_9 = 1393$, ... Diese Zahlen treten im Zusammenhang mit der Frage nach der Existenz einfacher endlicher Gruppen mit quadratischer Ordnung auf.

Die Zahlen $W_n = S_{2n+1}$, $n \geq 0$ sind die Werte der linear rekurrenten Folge zweiter Ordnung mit Parametern $P = 6$, $Q = 1$ und Anfangswerten $W_0 = 1$, $W_1 = 7$. Für jedes $n \geq 2$ gilt also

$$W_n = \frac{(1+\sqrt{2})^{2n+1} + (1-\sqrt{2})^{2n+1}}{2}.$$

Es ist unbekannt, ob es unendliche viele prime NSW-Zahlen gibt. Auf der anderen Seite bewiesen Sellers & Williams (2002), dass die Folge $(W_n)_{n\geq 0}$ (und viele andere, ähnliche Folgen) unendlich viele zerlegbare Zahlen enthält.

In der ursprünglichen Schreibweise gilt, dass wenn S_{2n+1} eine Primzahl ist, dies auch für $2n+1$ der Fall sein muss. Die folgenden Werte von $p < 2000$ führen zu primen NSW-Zahlen S_p:

$$p = 3, 5, 7, 19, 29, 47, 59, 163, 257, 421, 937, 947, 1493, 1901.$$

F. Morain hat 1989 gezeigt, dass die letzten zwei Werte tatsächlich Primzahlen ergeben. Im Jahre 1999 ermittelte H. Dubner, dass S_p im Intervall $2000 < p < 80000$ genau dann quasiprim ist, wenn

$$p = 6689, 8087, 9679, 28953, 79043.$$

Im selben Jahr gelang Dubner und Keller der Nachweis der Primalität von S_{6689}. Die Primalität von S_{8087} und S_{9679} wurde 2001 von D. Broadhurst nachgewiesen, was im Falle von S_{8087} äusserst schwierig war.

In den Jahren 2006 und 2007 bestimmte E.W. Weisstein die nächsten Quasiprimzahlen S_p mit

$$p = 129127, 145969, 165799, 168677, 170413, 172243.$$