Primzahltests für Fermatzahlen

Olaf Michel

12.November 2002

1 Einleitung und Allgemeines über Fermatzahlen

Ich werde mich im folgenden mit Primzahltests für Fermatzahlen beschäftigen.

Definition 1 *Die Zahlen der Form*

$$F_n = 2^{2^n} + 1 \qquad\qquad ,n \in \mathbb{N}$$

heißen Fermatzahlen.

Benannt wurden sie nach *Pierre de Fermat*(1605-1665), der sie als Erster untersuchte. Durch Anregung von *F.M.Mersenne* beschäftigte er sich mit der Zahlentheorie und dann insbesondere mit Zahlen der Form $2^m \pm 1$. *Fermat* kannte zudem den Inhalt des folgenden Lemmas:

Lemma 1 $N = 2^m + 1$ *ist höchstens dann Primzahl, wenn* $m = 2^n$ *mit* $m, n \in \mathbb{N}$

*Beweis:*Wäre m keine Potenz von 2, so gäbe es $v, w \in \mathbb{N}$ mit v ungerade und $m = v \cdot w$.
Dann gilt:

$$2^m + 1 = 2^{vw} + 1 = (2^w + 1)(1 - 2^w + 2^{2w} - \ldots + 2^{(v-1)w})$$

Diese Zerlegung ist nicht trivial, da wegen $1 \leq w < m$, $1 < 2^w + 1 < 2^m + 1$ gilt.
Also ist $2^m + 1$ keine Primzahl. □

Im Jahre 1640 vermutete *Fermat*, daß es sich bei allen Fermatzahlen um Primzahlen handelt, was für $n \in \{0, 1, 2, 3, 4\}$ richtig ist:

$$\begin{aligned}
F_0 &= 2 + 1 = 3 \\
F_1 &= 2^2 + 1 = 5 \\
F_2 &= 2^4 + 1 = 17 \\
F_3 &= 2^8 + 1 = 257 \\
F_4 &= 2^{16} + 1 = 65537
\end{aligned}$$

Wie ich aber später zeigen werde, ist F_5 keine Primzahl. Bisher ist keine der anderen untersuchten Fermatzahlen eine Primzahl gewesen (siehe dazu auch Abschitt 3).
Im Folgenden noch eine Eigenschaft der Fermatzahlen:

Lemma 2 *Alle Fermatzahlen sind paarweise zueinander teilerfremd.*

Beweis: Dies zeige ich per Induktion.
Induktionsbehauptung:

$$\forall m \in \mathbb{N} : F_{m+1} - 2 = F_0 \cdot F_1 \cdot F_2 \cdot \ldots \cdot F_m$$

Induktionsanfang: Es gilt für $m = 0$:

$$F_{m+1} - 2 = F_1 - 2 = 5 - 2 = 3 = F_0$$

Induktionsschluß: Gelte die Induktionsbehauptung für $m-1$. Dann ist

$$\begin{aligned} F_0 \cdot F_1 \cdot F_2 \cdot \ldots \cdot F_{m-1} \cdot F_m &= (F_m - 2) \cdot F_m \\ &= (2^{2^m} + 1 - 2) \cdot (2^{2^m} + 1) = (2^{2^m} - 1) \cdot (2^{2^m} + 1) \\ &= (2^{2^m})^2 - 1 = 2^{2^{m+1}} + 1 - 2 \\ &= F_{m+1} - 2 \end{aligned}$$

Dann ist also, für $n < m$, $F_n | (F_m - 2)$.
Würde nun ein p mit $p|F_n$ und $p|(F_m)$ existieren, so würde auch $p|(F_m - 2)$ gelten. Damit auch $p|2$, und so $p = 2$. Da aber alle Fermatzahlen ungerade sind, ist dies ein Widerspruch. □

Bemerkung:
Aus diesem Lemma läßt sich auch auf die Existenz unendlich vieler Primzahlen schließen, da jede Fermat-Zahl Primfaktoren hat, die in den vorherigen Fermatzahlen noch nicht vorgekommen sind.

2 Primzahltests für Fermatzahlen

Im folgenden stelle ich ein paar Möglichkeiten vor, Fermatzahlen auf Primzahleigenschaft zu testen.

Lemma 3 *Ist p Primzahl mit $p|F_n$, dann gilt:*

$$p \equiv 1 \bmod 2^{n+1}$$

Beweis: Ist p Primteiler von $F_n = 2^{2^n} + 1$, so gilt

$$2^{2^n} \equiv -1 \bmod p.$$

Damit ist $2^{2^{n+1}} \equiv 1 \bmod p$. Das heißt aber, daß die Ordnung von 2 mod p in der Gruppe $(\mathbb{Z}/p\mathbb{Z})^*$ ein Teiler von 2^{n+1} ist. Aus der ersten Formel folgt aber, daß sie 2^n nicht teilen kann, also ist sie 2^{n+1}. Da aber die Ordnung von $(\mathbb{Z}/p\mathbb{Z})^*$ gleich $p-1$ ist, gilt also $2^{n+1}|(p-1)$. Damit folgt die Behauptung. □

Bemerkung: 1877 bewies *Lucas*, daß für einen Primteiler p von F_n auch gilt, daß

$$p \equiv 1 \bmod 2^{n+2}$$

Beispiel: Mit diesem Satz läßt sich zeigen, daß $F_5 = 4294967297$ keine Primzahl ist. Ein eventueller Primteiler p von F_5 müßte die Kongruenz $p \equiv 1 \bmod 2^6$ erfüllen, wäre also unter den folgenen Zahlen zu finden:

$$65, 129, 193, 257, 321, 449, 513, 577, 641, \ldots$$

65, 129, 321 und 513 sind keine Primzahlen. $257 = F_3$ ist nach Lemma 2 teilerfremd zu F_5. $193 = 3 \cdot 2^6 + 1$ kann nach Satz 7 auch kein Primteiler von F_5 sein. Also teste ich die übriggebliebenen Zahlen, und es zeigt sich:

$$\begin{aligned} F_5 &\equiv 325 \bmod 449 \\ F_5 &\equiv 288 \bmod 577 \\ F_5 &\equiv 0 \bmod 641 \text{ (!)} \end{aligned}$$

Damit $641 | F_5$, also ist F_5 keine Primzahl.

Zur Vorbereitung auf den nächsten Test für Fermatzahlen zeige ich im folgenden einige Sätze, aber zuvor noch eine

Definition 2 *Für teilerfremde $a, p \in \mathbb{Z}$ mit p Primzahl ist*

$$\left(\frac{a}{p}\right) = \begin{cases} +1 & , \quad \text{falls } a \text{ quadratischer Rest mod } p \\ -1 & , \quad \text{falls } a \text{ kein quadratischer Rest mod } p \end{cases}$$

Dabei heißt $(\frac{a}{p})$ das Legendre-Symbol

Satz 1 *Seien $p \neq q$ ungerade Primzahlen. Dann gilt*
(a) Quadratisches Reziprozitätsgesetz:

$$\begin{aligned} \left(\frac{p}{q}\right) &= \left(\frac{q}{p}\right) \text{ falls } p \equiv 1 \bmod 4 \text{ oder } q \equiv 1 \bmod 4 \\ \left(\frac{p}{q}\right) &= -\left(\frac{q}{p}\right) \text{ falls } p \equiv q \equiv 3 \bmod 4 \end{aligned}$$

(b) Ergänzungssätze

$$\begin{aligned} \left(\frac{-1}{p}\right) &= (-1)^{(p-1)/2} = \begin{cases} +1 \text{ falls } p \equiv 1 \bmod 4 \\ -1 \text{ falls } p \equiv 3 \bmod 4 \end{cases} \\ \left(\frac{2}{p}\right) &= (-1)^{(p^2-1)/8} = \begin{cases} +1 \text{ falls } p \equiv \pm 1 \bmod 8 \\ -1 \text{ falls } p \equiv \pm 3 \bmod 8 \end{cases} \end{aligned}$$

Satz 2 ***(Satz von Euler)*** *Sei $p \neq 2$ eine Primzahl.*
Dann gilt für jede zu p teilerfremde Zahl $a \in \mathbb{Z}$:

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

*Beweis:*Sei g ein erzeugendes Element der zyklischen Gruppe $(\mathbb{Z}/p\mathbb{Z})^*$. Dann ist $(p-1)$ die Ordnung von g und

$$g^{p-1} \equiv 1 \bmod p.$$

Sei nun $a = g^{\alpha} \mod p$.
Ist a quadratischer Rest, dann ist α gerade, d.h. es gibt β mit $\alpha = 2\beta$, und es ist

$$a^{\frac{p-1}{2}} \equiv \left(g^{p-1}\right)^{\beta} \equiv 1 \mod p.$$

Ist a kein quadratischer Rest, dann ist α ungerade und es gibt β mit $\alpha = 2\beta + 1$ und es ist

$$a^{\frac{p-1}{2}} \equiv \left(g^{p-1}\right)^{\beta} \cdot g^{\frac{p-1}{2}} \equiv \mod p.$$

Nun ist $u = g^{\frac{p-1}{2}} \not\equiv 1$, aber $u^2 \equiv 1$. Da $(\mathbb{Z}/p\mathbb{Z})$ ein Körper ist, muss also $u \equiv -1$. □

Satz 3 *Sei $N - 1 = k \cdot q^n$ mit q prim, $n \geq 1$ und $q \not| k$. Außerdem existiere eine ganze Zahl $a > 1$ mit*
(i) $a^{(N-1)} \equiv 1 \mod N$
(ii) $ggT(a^{\frac{N-1}{q}} - 1, N) = 1$
Dann hat jeder Primteiler von N die Form $m \cdot q^n + 1$ mit $m \geq 1$.

Beweis: Sei p Primteiler von N und e die Ordnung von $a \mod p$.
Dann $e|(p-1)$ und $e|(N-1)$ nach (i).
Da $N - 1 = k \cdot q^n$, ist $e|k \cdot q^n$, aber nach (ii) gilt $e \not| k \cdot q^{n-1}$. Also $e|q^n$ und somit auch $q^n|(p-1)$. □

Der folgende Satz geht auf *F.Proth* zurück, der ihn 1878 formulierte.

Satz 4 *Sei $N = k \cdot 2^n + 1$ gegeben mit $0 < k < 2^n$ mit k ungerade. Dann gilt:*

$$N \text{ prim} \Leftrightarrow \exists a \in \mathbb{Z} : a^{\frac{N-1}{2}} \equiv -1 \mod N$$

Beweis: $\Rightarrow$: Wähle a mit $\left(\frac{a}{N}\right) = -1$. Dann gilt nach Satz 2 die Kongruenz.
$\Leftarrow$: Sei $a^{\frac{N-1}{2}} \equiv -1 \mod N$ mit $N - 1 = k \cdot 2^n$. Da k ungerade ist $ggT(2^n, k) = 1$. Außerdem sind $a^{\frac{N-1}{2}} - 1$ und N teilerfremd.
Denn wären $a^{\frac{N-1}{2}} - 1$ und N nicht teilerfremd, so gäbe es einen Primteiler p von N mit $p|a^{\frac{N-1}{2}} - 1$, und nach Vorraussetzung wäre auch $p|a^{\frac{N-1}{2}} + 1$. Damit $p|2$. Da aber N ungerade, ist dies ein Widerspruch.
Somit hat man $a^{N-1} \equiv 1 \mod N$ und $ggT(a^{\frac{N-1}{2}}, N) = 1$. Daraus folgt mit Satz 3, daß für jeden Primteiler p von N gilt, daß

$$p \equiv 1 \mod 2^n.$$

Also $2^n|(p-1) \Rightarrow p > 2^n \Rightarrow p^2 > 2^{2n}$. Weiterhin ist $2^n > k \Rightarrow 2^{2n} \geq (k+1) \cdot 2^n$. So ist

$$p^2 > 2^{2n} \geq (k+1) \cdot 2^n > N$$

für alle Primteiler p von N, insbesondere für den kleinsten Primteiler, also ist N Primzahl. □

Der folgende Satz ist die Basis für einen Primtest für Fermatzahlen. Er geht auf *Pepin* aus dem Jahr 1877 zurück.

Satz 5 *Für $n \geq 2$ gilt:*

$$F_n \text{ prim} \Leftrightarrow 5^{\frac{F_n - 1}{2}} \equiv -1 \mod F_n$$

Bemerkung: Diese Fassung ist die von *Pepin* 1877 bewiesene. Die Äquivalenz ist auch mit den Basen 3 und 10 richtig, wobei 3 die heute gebräuchliche Aussage liefert.

Beweis:$\Leftarrow$: Mit dem Satz von *Proth* (Satz 4) ist diese Richtung klar.
$\Rightarrow$: Sei F_n prim. Dann gilt nach dem Satz von Euler (Satz 2):

$$5^{\frac{F_n-1}{2}} \equiv \left(\frac{5}{F_n}\right) \mod F_n.$$

Da $F_n \equiv 1 \mod 4$, ist nach Satz 1 a) :

$$\left(\frac{5}{F_n}\right) = \left(\frac{F_n}{5}\right)$$

Nun gilt

$$F_n = 2^{2^n} + 1 \equiv (2^4)^{2^{n-2}} + 1 \equiv 2 \mod 5$$

und nach Satz 1 b): $(\frac{F_n}{5}) = (\frac{2}{5}) = -1$. Damit also:

$$5^{\frac{F_n-1}{2}} \equiv \left(\frac{5}{F_n}\right) \mod F_n \equiv \left(\frac{F_n}{5}\right) \mod F_n \equiv \left(\frac{2}{5}\right) \mod F_n \equiv -1 \mod F_n$$

□

Damit ergibt sich ein Primtest für Fermatzahlen:
Für eine Fermatzahl F_n läßt sich für $5^{2^{n+1}}$ der Repräsentant R_n der Kongruenz modulo F_n in den Zahlen $\{0, 1, 2, \ldots, F_n - 1\}$ bestimmen. Wenn nun $R_n = F_n - 1$ ist, ist F_n prim, anderenfalls zusammengesetzt.
Da $\frac{F_n-1}{2} = 2^{2^n-1}$ ist, läßt sich $5^{\frac{F_n-1}{2}}$ durch $(2^n - 1)$maliges Quadrieren berechnen.

Beispiel:
Hier zeige ich nun, daß $F_3 = 257$ eine Primzahl ist. Dafür muss ich die 5 also $(2^3 - 1) = 7$mal quadrieren.

$$\begin{aligned}
&5 \mod 257\\
&5^2 \mod 257 \equiv 25 \mod 257\\
&25^2 \mod 257 \equiv 625 \mod 257 \equiv 111 \mod 257\\
&111^2 \mod 257 \equiv 12321 \mod 257 \equiv 242 \mod 257\\
&242^2 \mod 257 \equiv 58564 \mod 257 \equiv 225 \mod 257\\
&225^2 \mod 257 \equiv 50625 \mod 257 \equiv 253 \mod 257\\
&253^2 \mod 257 \equiv 64003 \mod 257 \equiv 16 \mod 257\\
&16^2 \mod 257 \equiv 256 \mod 257
\end{aligned}$$

Also gilt $5^{\frac{F_3-1}{2}} \equiv -1 \mod 257$.

Um weitere Zahlen, die Teiler von F_n seien könnten , gibt es einige Aussagen über Eigenschaften von Primteiler von Fermatzahlen (ohne Beweis):

Satz 6 *Für Primzahlen $N = k \cdot 2^m + 1$ gilt:*

$$N | F_n \Leftrightarrow \exists x \in \mathbb{Z} : x^k \equiv 2 \mod N$$

Satz 7 *Eine Primzahl $N = 3 \cdot 2^m + 1$ mit m gerade, kann nicht Faktor einer Fermat-Zahl F_n sein.*

Satz 8 *Eine Fermat-Zahl F_n kann keine Primzahlpotenz sein.*

Satz 9 *Sei p ein Primteiler einer Fermat-Zahl F_n.*
p^2 ist Teiler von F_n genau dann, wenn p der sogenannten Wieferich-Kongruenz $2^{p-1} \equiv 1 \mod p^2$ genügt.

Bemerkung: Bisher sind noch keine Fermatzahlen bekannt, welche die Wieferich-Kongruenz erfüllen[1].

Als Abschluß nenne ich noch einen weiteren Test für Fermatzahlen, der auf *Lucas* zurückgeht, auch ohne Beweis.

Satz 10 *Sei $S_1 = 6$ und $S_{i+1} = S_i^2 - 2$.*
Dann gilt:
(i) F_n ist Primzahl, wenn $F_n | S_k$ für ein k mit $2^{n-1} \leq k \leq 2^n - 1$.
(ii) Wenn $F_n \not| S_k$ für alle $k \leq 2^n - 1$, so ist F_n zusammengesetzt.
(iii) Teilt F_n ein S_k mit $k < 2^{n-1}$, so hat jeder Primteiler von F_n die Form $2^{k+1}q+1$

3 Aktueller Stand der Fermatzahlen

Hier ein kleiner Überblick über den Stand der Forschung bezüglich den Fermatzahlen:

Eigenschaft	Nummer n der Fermat-Zahl F_n
prim	0,1,2,3,4
zusammengesetzt mit exakt 2 Faktoren	5,6,7,8
zusammengesetzt mit exakt 3 Faktoren	9
zusammengesetzt mit exakt 4 Faktoren	10
zusammengesetzt mit exakt 5 Faktoren	11
zusammengesetzt mit 5 bekannten Faktoren	12
zusammengesetzt mit 4 bekannten Faktoren	13
zusammengesetzt mit 3 bekannten Faktoren	15,25
zusammengesetzt mit 2 bekannten Faktoren	16, 18, 19, 27, 30, 36, 38, 52, 77, 147, 150, 284, 416
zusammengesetzt mit 1 bekanntem Faktor	17, 21, 23, 26, 28, 29, 31, 32, 37, 39, 42, 43 und 167 weitere Zahlen zwischen 43 und 382447
zusammengesetzt, aber ohne bekannten Faktor	14,20, 22, 24

Insgesamt sind 207 zusammengesetzte Fermatzahlen bekannt.

1. Bisher sind überhaupt nur zwei Zahlen bekannt, welche die Wieferich-Kongruenz erfüllen, nämlich 1093 und 3511. Die Suche nach weiteren Wieferich-Primzahlen war bisher erfolglos, wobei bisher alle Primzahlen kleiner als $4 \cdot 10^{12}$ untersucht wurden.

4 Quellen

- H.C.Williams and J.O.Shallit, Factoring Integers Before Computers, Proceedings of Symposia in Applied Mathematics, Vol. 48, pp. 498-501, 1994
- Ivka Curic, Zur Faktorisierung von Fermatzahlen, Diplomarbeit Bremen, 1998
- http://www.prothsearch.net/fermat.html , Stand: 15. Oktober 2002