Ungelöste Probleme der Zahlentheorie

Teil 2: Mersenne- und Fermatprimzahlen (A3 in [Guy])

Def. 1: Eine Mersenne-Primzahl ist eine Primzahl (q PZ: $n \mid q \Rightarrow n=1 \vee n=q$ $\Leftrightarrow q$ prim) der Form $M_p := 2^p - 1$.

Es gilt: 2^p-1 prim $\Rightarrow p$ prim, [Sonst $p = m \cdot n$, $m,n \geq 2$
$$\Rightarrow 2^{mn}-1 = (2^m)^n - 1 = \underbrace{(2^m-1)}_{\geq 2} \cdot \sum_{k=0}^{n-1} (2^m)^k \text{ nicht prim}]$$

aber nicht „$\Leftarrow$", wie $2^{11}-1 = 2047 = 23 \cdot 89$ zeigt.

Bsp.: $M_2 = 3$, $M_3 = 7$, $M_5 = 31$, $M_7 = 127$, $M_{13} = 8191, \ldots$

Die größten (numerisch) bekannten PZen sind Mersenne-PZen $\rightsquigarrow$ GIMPS:
Aktuell (seit 2009): die 47.te Mersenne-PZ $M_{42.643.801}$ (≈ 12.8 Mio Ziffern)

Sei $M(x) := \#\{p \leq x \mid 2^p - 1 \text{ prim}\}$.
Es wird vermutet, daß $M(x) \sim e^{\gamma} \cdot \frac{\log x}{\log 2}$ gilt. [Lenstra, Pomerance & Wagstaff]
(γ = Euler-Mascheroni-Konstante)

Satz (Lucas-Lehmer-Test):

Sei $(u_n)_{n \in \mathbb{N}}$ rekursiv def. durch $u_1 := 4$, $u_{n+1} := u_n^2 - 2$ für $n \geq 1$,

sei p prim, $p \geq 3$. Dann gilt: $M_p = 2^p - 1$ prim $\Leftrightarrow M_p \mid u_{p-2}$.

Bew. in §17, Forster, „Algor. ZT" Arbeiten mit $\xi := 2 + \sqrt{3} \in (\mathbb{Z}/M_n\mathbb{Z})[\sqrt{3}]$,

$\xi_k := \xi^{2^k}$ (alle ξ_k haben Norm 1). Dann verwende: M_n prim $\Leftrightarrow \xi_n = 1$ & $\xi_{n-1} \neq 1$. $\rightsquigarrow \square$

Um zusammengesetzte Mersenne-Pzen zu erkennen, bietet sich folgender Satz an:

Satz: $p \geq 3$ prim, $q \mid M_p = 2^p - 1 \Rightarrow q = 2kp + 1$ mit $k \in \mathbb{Z}$.

Bew.: 1. Bew. für Primteiler $q \mid M_p$:

$q \mid M_p \Rightarrow 2^p \equiv 1 \ (q) \Rightarrow 2 \bmod q$ hat in $\mathbb{F}_q^\times$ die Ordnung p,
also $p \mid \operatorname{ord}(\mathbb{F}_q^\times) = q-1$, d.h. $q - 1 = mp$, $m \in \mathbb{Z}$.
Da $q-1$ gerade, ist auch m gerade $\Rightarrow q = 1 + 2kp$. ✓

2. Für $q \mid M_p$, q nicht prim: $q = q_1 \cdots q_r$, $q_i \mid M_p$, die $q_i \equiv 1 \ (2p)$
$\Rightarrow q \equiv 1 \ (2p)$. □

Bsp.: M_p nicht prim für $p = 859423$ (Faktor 13750769 mit $k = 8$)

Zusammenhang mit perfekten Zahlen: n perfekt (auch: "vollkommen") $:\Leftrightarrow 2n = \sum_{d \mid n} d$.
Dann: M_p prim $\Rightarrow$ (Euklid) $2^{p-1}(2^p - 1)$ perfekt, und alle geraden perfekten Zahlen sind von dieser Form. (Euler)

Bsp.: $6 = 1+2+3$, $28 = 1+2+4+7+14, \ldots$

Ungelöst: ex. ungerade perfekte Zahlen?

Euler: N ungerade & perfekt $\Rightarrow N = p^\alpha m^2$, p prim, $p \equiv \alpha \equiv 1 \ (4)$
Touchard: " $\Rightarrow N = 12m + 1$ oder $N = 36m + 9$
Brent, Cohen & te Riele: " $\Rightarrow N \geq 10^{300}$
Heath-Brown (1994): " , k versch. Primfaktoren $\Rightarrow n < 4^{4^k}$
P.P. Nielsen (?) " $\Rightarrow n < 2^{4^k}$
integers-ejcnt.org/vol 3.html

Neue Mersenne-Vermutung (Bateman/Selfridge/Wagstaff):

Gelten zwei der folgenden Aussagen, so auch die dritte:

1.) $n = 2^k \pm 1$ oder $n = 4^k \pm 3$

2.) $2^n - 1$ ist eine Mersenne-Primzahl

3.) $\frac{2^n+1}{3}$ ist prim

Def. 2: Eine Fermat-Zahl ist eine Zahl $F_n = 2^{2^n} + 1$. (auch: [Guy], A3)

F_n prim für $0 \le n \le 4$, zus.gesetzt für $5 \le n \le 32$
und viele größere n.

Fermatsche PZen spielen bei der Konstruktion regelmäßiger n-Ecke eine prominente Rolle: Gauß hat gezeigt, daß das regelmäßige n-Eck genau dann m.Z.u.L. konstruierbar ist, wenn $n = 2^k p_1 \cdots p_l$ mit $k \ge 0$ und p.w.v. Fermat-PZen $p_1, \dots, p_l$.

m.Z.u.L. = "mit Zirkel und Lineal"

Vermutung (Hardy/Wright): es ex. nur endl. viele prime Fermat-Zahlen.

Unbekannt:

Sind $F_0, \dots, F_4$ die einzigen primen Fermatzahlen?

Gibt es ∞ viele zusammengesetzte Fermatzahlen?

Bem.: Eine Zahl der Form $2^n + 1$ ist höchstens dann prim, wenn n eine Zweierpotenz ist.
(für m ungerade ist $x^m + 1$ durch $x+1$ teilbar).

Ein Kriterium für prime Fermatzahlen lautet wie folgt:

Satz: 1) F_n ist für $n \geq 1$ genau dann prim, falls $3^{(F_n-1)/2} \equiv -1\ (F_n)$
(Pepin, 1877)

2) Jeder mögliche Primfaktor von F_n, $n \geq 5$, ist von der Gestalt $p = h \cdot 2^{n+2} + 1$ mit $h \in \mathbb{N}$. (von E. Lucas)

Bew.:

Zu 1): „$\Rightarrow$": Nach dem Satz von Euler [$p \geq 2$ prim, $a \in \mathbb{Z}$, $p \nmid a$ $\Rightarrow a^{(p-1)/2} \equiv \left(\frac{a}{p}\right)\ (p)$]

folgt: $3^{(F_n-1)/2} \equiv \left(\frac{3}{F_n}\right)\ (F_n)$.

Da $F_n \equiv 1\ (4)$, ist $\left(\frac{3}{F_n}\right) = \left(\frac{F_n}{3}\right)$ nach dem QRG,

nun ist $F_n \equiv (-1)^{2^n} + 1 \equiv 2\ (3)$, also

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

„$\Leftarrow$": Benutzen Satz ⊛: $N \geq 3$ ungerade, $N-1 = \prod_i^r p_i^{k_i}$ die PFZ von $N-1$.

Dann: N prim $\Leftrightarrow \exists a \in \mathbb{Z} : a^{N-1} \equiv 1\ (N)$, $\forall i = 1, \dots, r$: $a^{(N-1)/p_i} \not\equiv 1\ (N)$. (a ist dann Primitivw.)

[vgl. Forster, „Algorithm. ZT", Satz 11.5 & 10.3]

Zu 2): Ist $p \mid F_n$, so ist $2^{2^n} \equiv -1\ (p)$, also hat $2 \bmod p$ in $\mathbb{F}_p^*$ die Ordnung 2^{n+1}, also ist $2^{n+1} \mid p-1$. Insb. ist $p \equiv 1\ (8)$ und $\left(\frac{2}{p}\right) = 1$ (QRG), also ex. x mit $x^2 \equiv 2\ (p)$.

Dann hat $x \bmod p$ die Ordnung 2^{n+2} in $\mathbb{F}_p^*$, also $2^{n+2} \mid p-1$. □

Bsp.: F_{207} nicht prim, da durch $p = 3 \cdot 2^{209} + 1$ teilbar.

Bem.: Der größte Primteiler von F_n ist $\geq 2^{n+2}(4n+9)+1$.
[Grytczuk, Luca, Wojtowicz 2001]