§7 Fermatsche und Mersennesche Primzahlen

Kann man unendliche Serien von Primzahlen auf einfache Art angeben? Anscheinend nicht.

Versuch von **Fermat** (1607–1665):

$$2^{2^n} + 1$$

$n=0$	3
$n=1$	5
$n=2$	17
$n=3$	257

Bem. 2^k+1 prim $\Longrightarrow$ k Potenz von 2 (vgl. Aufg. 4)

Fermat vermutet (ja behauptet): Umkehrung gilt!

$F_n := 2^{2^n}+1$ *n-te Fermatsche Zahl*

(1) $F_0=3$, $F_1=5$, $F_2=17$, $F_3=257$, $F_4=65537$ sind prim.

*vgl. Algebra I, §11

***Satz** (Gauß 1777–1855): Ein regelmäßiges n-Eck ist mit Zirkel u. Lineal genau dann konstruierbar, wenn n von der Gestalt

$$n = 2^{\nu} p_1 p_2 \cdots p_r$$

mit paarw. versch. Fermatschen Primzahlen $p_1,\dots,p_r$ (und bel. $\nu \in \mathbb{N}_0$) ist. ($r=0$ zugelassen)

Also z.B. 17-Eck konstruierbar, das 7-Eck oder 9-Eck nicht.

Euler (1707–1783), vgl. Aufg. 27:

(2) $F_5 = 2^{2^5}+1 = 2^{32}+1$ ist <u>keine</u> Primzahl, sondern durch 641 teilbar. (1732)

(3) Für $n \geq 3$ hat jeder Primteiler von F_n die Gestalt

$$p = t2^{n+2}+1$$

Damit leicht zu sehen: $F_5 = 2^{32}+1 = 4.294.967.297$ ist Produkt der Primzahlen $641 = 5 \cdot 2^7+1$ und $6700417 = 52347 \cdot 2^7+1$. □

(4) Auch $F_6 = 2^{64}+1$ ist nicht prim, sondern teilbar durch $274177 = 1 + 1071 \cdot 2^8$. (Clausen 1855)

(5) F_n ist nicht prim für $5 \leq n \leq 32$

(6) Ob F_n für $n = 33, 34, 35$ prim ist oder nicht, ist unbekannt. Für $n = 36$ ist wieder bekannt, daß F_n nicht prim ist, ebenso für $n = 37, 38, 39$. Nächst offener Fall ist $n = 40$.

(7) Derzeit ist von 271 Fermatzahlen bekannt, daß sie nicht prim sind.*) Deren größte ist $F_{2747497}$; sie hat den Teiler $57 \cdot 2^{2747499}+1$. (Stand Mai 2013)

(8) Wie gesagt ist F_{20} nicht prim, aber es ist kein Primteiler von F_{20} bekannt; desgl. für F_{24}.

Offene (Unlösbare?) Probleme: 1) Gibt es unter den F_n nur endlich viele Primzahlen? Man kennt bisher nur die fünf in (1).

2) Sind unendlich viele F_n nicht prim?

3) Sind alle F_n quadratfrei? Oder wenigstens unendlich viele?

*) vor 10 Jahren waren es erst 217. Vor 40 Jahren war noch unsicher, je entscheiden zu können, ob F_{17} prim ist oder nicht.

F1: Es gilt $F_{n+1} - 2 = \prod_{k=0}^{n} F_k$

Insb. sind F_n, F_m für $m>n$ teilerfremd.

Bew. $F_{n+1} - 2 = 2^{2^{n+1}} - 1 = (2^{2^n}+1)(2^{2^n}-1) = F_n(F_n-2)$; nun Ind.

Für $m>n$ gilt $F_n \mid F_m - 2$. Ist daher $d \in \mathbb{N}$ Teiler von F_n und F_m, so $d \mid 2$ und d ungerade. Also $d=1$. $\square$

Für welche ungeraden n ist n-Teilung des Kreises (mit Zirkel u. Lineal) möglich?

Bisheriger Rekord (nach Satz 1):

$$n = 3 \cdot 5 \cdot 17 \cdot 257 \cdot \underbrace{65537}_{F_4} \overset{F1}{=} F_5 - 2 = 2^{32} - 1 = 4.294.967.295$$

Bem. Aus F1 folgt, daß es unendlich viele Primzahlen gibt: Jedes F_n hat einen Primteiler q_n. Nach F1 aber $q_n \neq q_m$ für $n \neq m$. Also $q_0, q_1, q_2, \dots$ unendlich viele Primzahlen

Für die n-te Primzahl p_n gilt $p_n \leq F_{n-2} = 2^{2^{n-2}} + 1$ (für $n \geq$
(sehr schlechte Abschätzung, aber nicht schlechter als die in §1 aus Bew. von Euklid: $p_n \leq 2^{2^{n-1}}$)

<u>F2 (Pepins Test):</u> Sei $n \geq 2$ und g sei eine ganze zu $F_n = 2^{2^n}+1$ teilerfremde Zahl mit $\left(\frac{g}{F_n}\right) = -1$. Dann sind äquivalent:
↑ Jacobisymbol

(i) F_n ist prim (ii) $g^{\frac{F_n-1}{2}} \equiv -1 \bmod F_n$

(iii) $\operatorname{ord}(g \bmod F_n) = F_n - 1 = 2^{2^n}$.

<u>Bew.</u> (i) $\Rightarrow$ (ii) klar nach Euler-Kriterium.

(ii) $\Rightarrow$ (iii): Aus (ii) folgt $g^{F_n-1} \equiv 1 \bmod F_n$, also ist $\operatorname{ord}(g \bmod F_n)$ ein Teiler von $F_n - 1 = 2^{2^n}$, und somit eine Potenz von 2. Nach (ii) ist aber $g^{2^{2^n-1}} \not\equiv 1 \bmod F_n$, also muß $\operatorname{ord}(g \bmod F_n) = 2^{2^n} = F_n - 1$ gelten.

(iii) $\Rightarrow$ (i): Aus (iii) folgt $F_n - 1 \mid \varphi(F_n)$, also insbesondere $\varphi(F_n) \geq F_n - 1$. Jede der Zahlen $1, 2, 3, \ldots, F_n-1$ muß also teilerfremd zu F_n sein. Also besitzt F_n keinen Primteiler $p < F_n$, d.h. F_n ist prim.

<u>Bem.</u> Den Test kann man z.B. mit $g = 3$, $g = 5$, $g = 10$ anwenden. Denn $F_n = 2^{2^n}+1 \equiv 2^{2\cdot 2^{n-1}} + 1 \equiv 1 + 1 \equiv 2 \bmod 3$ und $\left(\frac{3}{F_n}\right) = \left(\frac{F_n}{3}\right) = \left(\frac{2}{3}\right) = -1$.

$n \geq 2$ $F_n = 2^{4\cdot 2^{n-2}} + 1 \equiv 1 + 1 = 2 \bmod 5$, $\left(\frac{5}{F_n}\right) = \left(\frac{F_n}{5}\right) = \left(\frac{2}{5}\right) = -1$

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

Mersenne (1588–1648)

Minorit (Franziskaner) in Ordensklöstern, korrespondierte mit den Mathematikern seiner Zeit, z.B. Descartes u. Fermat.

Philosoph, Theologe, Musiktheoretiker

$$2^k - 1$$

Bem. $2^k - 1$ prim $\Rightarrow$ k prim (Aufgabe 1)

$$M_p := 2^p - 1 \quad , p \text{ Primzahl}$$

Mersenne untersucht M_p für $p \leq 257$

Leibniz denkt, alle M_p sind prim. Leibniz 1646–1716

(1) M_2 M_3 M_5 M_7 Mersennesche Primzahlen

3 7 31 127

(2) M_{11} keine Primzahl: $M_{11} = 2^{11} - 1 = 2047 = 23 \cdot 89$ (Fermat.

(3) M_{13}, M_{17}, M_{19} prim $M_{13} = 2^{13} - 1 = 8191$

(4) Für $23 \leq p \leq 100$ ist nur M_{31}, M_{61}, M_{89} prim

↑ 1886 entdeckt

M_{37} nicht prim (Fermat!)

(Euler glaubt, auch M_{41}, M_{47} sind prim]

(5) Mersenne hat 5 Fehler gemacht: die Primzahlen M_{61}, M_{89}, M_{107} 'vergessen'; M_{67}, M_{257} als prim behauptet.

(6) Für $100 \leq p \leq 257$ sind nur M_{107}, M_{127} prim

↑ entdeckt 1876 von Lucas

M_{127} bis 1951 größte bekannte Primzahl.

30. Jan. 1952: M_{521} ist prim! 2 Stunden später: M_{607} auch!

p Mersennesche Primzahl $\Rightarrow M_p$ prim ?

$M_3, M_7, \underset{\substack{\uparrow \\ \text{Euler}}}{M_{31}}, M_{127}$ prim, aber M_{8191} keine Primzahl

$8191 = M_{13}$

(7) Für $p \leq 12000$ sind unter den ca. 1250 vielen M_p genau 23 Primzahlen, M_{11213} die größte.

(8) Bislang sind 48 Mersennesche Primzahlen bekannt (Stand Oktober 2014); die größte ist

vgl. Aufgabe 1

$$M_{57885161}$$

Sie hat 17.425.170 Stellen.

in 2006: 100.000 \$ - Preis für die erste Primzahl mit mehr als 10 Millionen Stellen ausgezahlt ?

<u>F4</u> (<u>Euler 1707-1783</u>): Sei p eine Primzahl mit $p \equiv 3 \bmod 4$. Dann gilt:

$$2p+1 \text{ Primzahl} \Longleftrightarrow 2p+1 \text{ teilt } M_p$$

$2p+1 = 2^p - 1 \Rightarrow p = 3$

Ist also $2p+1$ eine Primzahl (mit p wie oben und $p \neq 3$), so ist M_p keine Primzahl.

<u>Bew.</u> Aufgabe 39.

<u>Bem.</u> Jeder Primteiler q von M_p, $p \geq 3$, hat die Gestalt
$$q = 2kp + 1$$

<u>Bew.</u> $q \mid 2^p - 1 \Rightarrow 2^p \equiv 1 \bmod q \Rightarrow p = \operatorname{ord}(2 \bmod q) \Rightarrow$
$p \mid q-1 \Rightarrow \underset{\text{ungerade}}{q} = 1 + ap \overset{\text{p ungerade}}{\Longrightarrow} a$ gerade, $\Rightarrow$ Beh.

<u>Anw. auf $p = 37$:</u> Potentielle Primteiler q von $M_{37} = 2^{37}-1$ haben Gestalt

$1 + 2pk$: ~~75~~, 149, 223, ...

$2^{37} \not\equiv 1$ mod 149, denn $2^{37\cdot 2} = 2^{\frac{149-1}{2}} \equiv \left(\frac{2}{149}\right) = -1$.

$2^{37} \equiv 1$ mod 223 mit leichter Rechnung:

$2^8 = 256 \equiv 33$ mod 223 $\qquad 2^{16} \equiv 1089 \equiv -26$

$2^{32} \equiv 676 \equiv 7 \quad , \quad 2^{37} \equiv 7 \cdot 2^5 = 7 \cdot 32 = 224 \equiv 1$ mod 223

Also $223 \mid M_{37}$ (Fermat!)

<u>F5 (Lucas-Test)</u>: Def'e Folge natürlicher Zahlen

$s_1, s_2, s_3, \ldots$ durch

$s_{n+1} = s_n^2 - 2 \quad , \quad s_1 = 4$ *)

⌜also 4, 14, 194, 37634, ... ⌟. Dann gilt

$$M_p \text{ prim} \iff s_{p-1} \equiv 0 \bmod M_p$$

<u>Bew.</u> später

<u>Bsp.</u> $M_7 = 2^7 - 1 = 127$

$$\overset{1}{4},\ \overset{2}{14},\ \underset{\overset{|||}{67}}{\overset{3}{194}},\ 67^2-2 = \underset{\overset{|||}{42}}{\overset{4}{4487}},\ 42^2-2 = \underset{\overset{|||}{111}}{\overset{5}{1762}},\ 111^2-2 = \underset{\overset{|||}{0}}{\overset{6}{12319}}$$

*) hat was mit Kettenbrüchen zu tun, und mit $\mathbb{Q}(\sqrt{3})$

Nachtrag (zu §7): Beweis des Lucas-Tests (§7, F5)

Def. $s_k = (\underbrace{2+\sqrt{3}}_{=a})^{2^{k-1}} + (\underbrace{2-\sqrt{3}}_{=b})^{2^{k-1}} = a^{2^{k-1}} + b^{2^{k-1}}$

$$\boxed{ab = 1}$$

$s_1 = a + b = 4$, $s_k^2 = (a^{2^{k-1}} + b^{2^{k-1}})^2 = a^{2^k} + 2 + b^{2^k} = s_{k+1} + 2$,

also

$\boxed{s_{k+1} = s_k^2 - 2}$, somit $(s_k)_k$ die im Kriterium von Lucas genannte Folge.

p Primzahl, $p \geq 3$. $\qquad M_p = 2^p - 1$

Vor. $M_p \mid s_{p-1}$, d.h. $s_{p-1} \equiv 0 \bmod M_p$. $\quad$ ⌜z.z. M_p ist prim⌝

Sei q ein Primteiler von M_p. Dann $q > 3$ (denn die Primteiler von M_p haben Gestalt $2kp+1$).

$$\text{O.E. } \left(\frac{3}{q}\right) = -1$$

(Denn wäre $\left(\frac{3}{q}\right) = 1$ für alle Primteiler q von M_p, so $\left(\frac{3}{M_p}\right) = 1$, $\Rightarrow \left(\frac{M_p}{3}\right) = -1$, $\Rightarrow M_p \equiv 2 \bmod 3$, doch $2^p - 1 = 2 + 3k$ unmöglich.)

Wir haben

$$s_{p-1} \equiv 0 \bmod q, \text{ d.h. } a^{2^{p-2}} + b^{2^{p-2}} \equiv 0 \bmod q \quad {}^{*)}$$

Multipl. mit $a^{2^{p-2}}$ ergibt wegen $ab = 1$:

$$a^{2^{p-1}} \equiv -1 \bmod q, \text{ also } a^{2^p} \equiv 1 \bmod q, \text{ und es folgt}$$

$$\operatorname{ord}(a \bmod qR) = 2^p \quad (\text{da offenbar } a \not\equiv 1 \bmod q)$$

Andererseits ist

$a^{q+1} = a^q a = (2+\sqrt{3})^q a \equiv (2^q + (\sqrt{3})^q) a \equiv (2 + 3^{\frac{q-1}{2}} \sqrt{3}) a \equiv$

$(2 + \left(\frac{3}{q}\right)\sqrt{3}) a \equiv (2-\sqrt{3})(2+\sqrt{3}) \equiv 1 \bmod q$. Es folgt

$2^p \mid q+1$, $\Rightarrow 2^p \leq q+1$, $\Rightarrow 2^p - 1 \leq q$, $\Rightarrow M_p = q$ prim!

*) Wir rechnen im Ring $R = \mathbb{Z}[\sqrt{3}]$; dort sind a und b Einheiten.

Jetzt die Umkehrung:

<u>Vor.</u> $M_p = 2^p - 1$ sei prim. Setze $q = M_p$. Es gilt $\left(\frac{3}{q}\right) = -1$ (s.o.)

<u>z.z.</u> $q \mid S_{p-1}$, d.h. $S_{p-1} \equiv 0 \bmod q$

Wegen $S_p = S_{p-1}^2 - 2$, ist also $\boxed{S_p \equiv -2 \bmod q}$ zu zeigen.

$S_p = a^{2^{p-1}} + b^{2^{p-1}}$, also <u>z.z.</u> $a^{2^{p-1}} \equiv -1 \bmod q$ (denn wegen $ab = 1$ ist dann auch $b^{2^{p-1}} \equiv -1 \bmod q$).

<u>Bew. von $a^{2^{p-1}} \equiv -1 \bmod q$:</u>

Aus der Relation $(1+\sqrt{3})^2 = 2(2+\sqrt{3}) = 2a$ folgt

$$(1+\sqrt{3})^{2^p} = 2^{2^{p-1}} a^{2^{p-1}} .$$

Wegen $q = 2^p - 1$ ist

$$2^{2^{p-1}} = 2^{\frac{q+1}{2}} = 2\,2^{\frac{q-1}{2}} \equiv 2 \bmod q \quad \left(\text{denn } \left(\tfrac{2}{q}\right) = 1\right),$$

und wir erhalten

$$2a^{2^{p-1}} \equiv (1+\sqrt{3})^{2^p} = (1+\sqrt{3})^q (1+\sqrt{3}) \equiv (1^q + \sqrt{3}^q)(1+\sqrt{3})$$

$$\equiv \left(1 + 3^{\frac{q-1}{2}}\sqrt{3}\right)(1+\sqrt{3}) \equiv (1-\sqrt{3})(1+\sqrt{3}) = -2 \bmod q$$

Es folgt

$$a^{2^{p-1}} \equiv -1 \bmod q \qquad \square$$