Lemma: $p \in P, a \in \mathbb{Z}$

Aus $p \mid a^m - 1$ und $p^2 \mid a^{p-1} - 1$ folgt $p^2 \mid a^m - 1$

Bew. Aufgabe 42

F3 Sei p ein Primteiler einer Fermatschen Zahl F_n bzw. einer Mersenneschen Mg. Genau dann teilt auch p^2 in F_n bzw. M_q auf, wenn die Bedingung

(W) $$2^{p-1} \equiv 1 \bmod p^2$$

erfüllt ist.

Eine Primzahl p, die (W) erfüllt heißt eine Wieferich-Primzahl (Wieferich 1909 Promotion Münster).

Bisher sind nur die Wieferich-Primzahlen 1093 und 3511 bekannt; bis 10^{15} gibt es keine weiteren. Die Primzahlen $p = 1093$ und $p = 3511$ kommen aber wegen $1093 = 1 + 273 \cdot 2^2$ und $3511 = 1 + 1755 \cdot 2^1$ nicht als Primteiler einer Fermatzahl F_n in Frage. Und auch nicht als Primteiler einer Mersenne-zahl M_q, denn sonst wäre q - wegen $2^q \equiv 1 \bmod p$ - ein Primteiler von $p-1$, da wegen $1093 - 1 = 2^2 \cdot 3 \cdot 7 \cdot 13$ und $3511 - 1 = 2 \cdot 3^3 \cdot 5 \cdot 13$ eine der Primzahlen $q = 2, 3, 5, 7$ oder 13. Für alle diese q ist aber M_q prim (und verschieden von 1093 und 3511).

Beweis von F3: Im Fermatfall beachte

(1) $2^{2^{n+1}} - 1 = F_n (F_n - 2)$

Oder ist die Vor. $p | F_n$ gleichwertig mit

(2) $p | 2^{2^{n+1}} - 1$, $p \nmid 2^{2^n} - 1 = F_n - 2$

Dies wiederum ist äquivalent mit $\operatorname{ord}(2 \bmod p) = 2^{n+1}$; daher ist 2^{n+1} ein Teiler von $p-1$, und es folgt

(3) $2^{2^{n+1}} - 1 \mid 2^{p-1} - 1$

Gelte nun $p^2 | F_n$. Mit (1) und (3) folgt dann $p^2 | 2^{p-1} - 1$, d.h. es gilt (W). Im Mersennefall vereinfacht sich die Vor. $p | M_q$ einfach $\operatorname{ord}(2 \bmod p) = q$, also $q | p-1$ und damit

(3') $2^q - 1 \mid 2^{p-1} - 1$

Die Annahme $p^2 | M_q = 2^q - 1$ liefert ebenfalls (W). Sei nun umgekehrt (W) erfüllt, d.h. gelte $p^2 | 2^{p-1} - 1$. Dann liefert das Lemma, mit Blick auf (2) aber $p^2 | 2^{2^{n+1}} - 1$. Nach (1) ist daher p^2 ein Teiler von F_n, denn p geht nach (2) nicht in $2^{2^n} - 1 = F_n - 2$ auf. Im Mersennefall tritt an die Stelle von (2) einfach $p | 2^q - 1$. Das Lemma liefert dann sofort $p^2 | 2^q - 1 = M_q$. □

Bem. Die Fermatsche Vermutung besagt: Die Gleichung

(1) $$X^n + Y^n = Z^n$$

besitzt für $n \geq 3$ keine Lösung in natürlichen Zahlen, d.h. es gibt kein Tripel $(a,b,c) \in \mathbb{N}^3$ mit $a^n + b^n = c^n$.
Um dies für alle $n \geq 3$ zu etablieren, genügt es offenbar zu zeigen, daß (1) im Falle einer Primzahl $n = p \geq 3$ keine Lösung $(a,b,c) \in \mathbb{N}^3$ besitzt sowie im Falle $n = 4$. Den Fall $n=4$ konnte bereits Fermat erledigen (F3 auf S. 120).
Im Falle $n = p$ einer Primzahl ≥ 3 besagt der sogenannte erste Fall der Fermatschen Vermutung, daß die Gleichung (1) keine Lösung $(a,b,c) \in \mathbb{N}^3$ hat, bei der keine der Zahlen a,b,c durch p teilbar ist. Dies, so konnte Wieferich zeigen, ist unter der Voraussetzung, daß p die Bedingung

$$2^{p-1} \not\equiv 1 \bmod p^2$$

erfüllt.-
Es ist hier nicht der Platz, auf die Geschichte der Fermatschen Vermutung genauer einzugehen. Der Fall $n=3$ (der viel schwieriger als der Fall $n=4$ ist) wurde von Euler gelöst, der Fall $n=5$ von Dirichlet und Legendre. Ein systematisches Studium (seit ca 1840) ist besonders mit dem Namen E. Kummer verbunden, der tiefliegende und befriedigende Resultate erzielte, ohne doch die generelle Gültigkeit der Vermutung etablieren zu können. Das gelang erst am Ende des 20. Jahrhunderts, und zwar auf neuem, und frappierend indirektem Wege (A. Wiles 1995 und manche andere).

Zur Bedeutung der Mersenneschen Primzahlen

Def. (z.B. Plato -429 bis -348): Eine natürliche Zahl n heißt **vollkommen**, wenn sie gleich der Summe ihrer nat. Teiler $d < n$ ist.

z.B. $6 = 1+2+3$

$n \in \mathbb{N}$ $\quad \sigma(n) := \sum_{d|n} d$ Summation über alle nat. Teiler von n.

n vollkommen $\iff \sigma(n) = 2n$

$\sigma(n) < 2n$: n defizient, z.B. $\sigma(15) = 1+3+5+15 = 24$

$\sigma(n) > 2n$: n abundant, z.B. $\sigma(12) = 1+2+3+4+6+12 = 28$

$\sigma(28) = 1+2+4+7+14+28 = 56$ 28 vollkommen (Mond! Umlauf in 28 Tagen)

(1) $\sigma(p^k) = 1+p+p^2+\dots+p^k = \frac{p^{k+1}-1}{p-1}$ $\quad (< 2p^k$, defizient,

(2) $(n_1, n_2) = 1 \implies \sigma(n_1 n_2) = \sigma(n_1)\sigma(n_2)$

$d_1 | n_1$, $d_2 | n_2 \implies d_1 d_2 | n_1 n_2$

$d | n_1 n_2 \implies d = d_1 d_2$ mit $d_i | n_i$

$(d_1, d_2) \leftrightarrow d_1 d_2$

$$\sum_{d | n_1 n_2} d = \sum_{d_1 | n_1,\, d_2 | n_2} d_1 d_2 = \sum_{d_1 | n_1} d_1 \cdot \sum_{d_2 | n_2} d_2$$

F6 (Euklid): Hat n die Gestalt

$$n = 2^{k-1}(2^k - 1)$$

und ist dabei $2^k - 1$ eine Primzahl, so ist n vollkommen.
($\Rightarrow k$ Primzahl)

Bew.: $\sigma(n) \overset{(2)}{=} \sigma(2^{k-1})\sigma(2^k-1) \overset{(1)}{=} (2^k-1)(1+(2^k-1)) = (2^k-1)2^k = 2n$

Also: Jede Zahl der Gestalt $2^{p-1}M_p$ mit M_p prim ist vollkommen.

$n = 2M_2$, $4M_3$, $16\overset{31}{M_5}$, $64\overset{127}{M_7}$ ...

6, 28, 496, 8128, ...

$n = 2^{11-1}M_{11} = 2^{10}\cdot\overset{23\cdot 89}{2047} = 2096128$ ist nicht vollkommen.

Dies folgt aus

F7 (Euler): Die geraden vollkommenen Zahlen n sind genau die Zahlen der Gestalt $n = 2^{p-1}M_p$ mit M_p prim.

Bew. Sei n vollkommen und gerade.

$n = 2^{k-1}a$ mit $k > 1$, a ungerade.

$\sigma(n) \overset{(2)}{=} \sigma(2^{k-1})\sigma(a) \overset{(1)}{=} (2^k-1)\sigma(a) \overset{\text{Vor.}}{=} 2n = 2^k a$, also

$$(2^k-1)\sigma(a) = 2^k a = (2^k-1)a + a, \Rightarrow$$

$$(*)\quad (2^k-1) \mid (\sigma(a) - a) = a,$$

$\Rightarrow \sigma(a) - a$ ist Teiler von a, $\quad 0 < \underbrace{\sigma(a)-a}_{\text{Summe der nat. Teiler} < a \text{ von } a} < a$ ($\neq 1$, $k \neq 2$)

$\Rightarrow \sigma(a) - a$ ist der einzige nat. Teiler $< a$ von a.

a ist Primzahl und $\sigma(a) - a = 1$

$\overset{(*)}{\Longrightarrow}$ $a = 2^k - 1$ Primzahl, $\Rightarrow$ Beh.

Problem (ungelöst): Gibt es ungerade vollkommene Zahlen?

üA: n ungerade mit höchstens 2 Primteilern $\Rightarrow \sigma(n) < 2n$
[n defizient]

Bem. Man weiß: n ungerade mit weniger als 8 Primteilern ist nicht vollkommen.

Jedes ungerade $n \leq 10^{200}$ nicht vollkommen (Hardy-Wright)

Bsp. $945 = 27 \cdot 5 \cdot 7$ $\quad \sigma(945) = \sigma(27)\sigma(5)\sigma(7) = \frac{3^4-1}{3-1} \cdot 6 \cdot 8 = 1920$.

also 945 abundant.

§8 Multiplikative zahlentheoretische Funktionen

Jede Funktion $f: \mathbb{N} \to \mathbb{C}$ heiße zahlenth. Fkt.
[manchmal auch Definitionsbereich $\mathbb{N}_0$ oder $\mathbb{Z}$ anstelle von $\mathbb{N}$]

Def. 1 f (nicht-null) heißt multiplikativ, wenn $f \neq 0$ und

$$f(n_1 n_2) = f(n_1) f(n_2), \text{ falls } (n_1, n_2) = 1$$

[$\Rightarrow f(1) = 1$, wegen $f \neq 0$]

Bsp'e: $\sigma(n) = \sum_{d \mid n} d$, $\varphi(n)$ Eulersche φ-Fkt.

$$\tau(n) = \sum_{d \mid n} 1 = \#\text{ der nat. Teiler } d \text{ von } n$$

Bem'n: 1) f multipl. $\iff f(n) = \prod_p f(p^{\nu_p(n)})$ für alle $n \in \mathbb{N}$

2) Eine multipl. Fkt. ist festgelegt durch ihre Werte auf den Primzahlpotenzen. Ordnet man umgekehrt jeder Primzahlpotenz > 1 eine Zahl $\neq 0$ zu, so existiert genau eine multiplikative Fkt mit den vorgegebenen Werten.

3) f, g multipl. $\Rightarrow fg$ multipl.

4) $f \neq 0$ heißt vollständig multiplikativ, wenn
$f(n_1 n_2) = f(n_1) f(n_2)$ für alle $n_1, n_2 \in \mathbb{N}$. Dann $f(p^k) = f(p)^k$.

Bsp'e: $i_\alpha(n) = n^\alpha$ ($\alpha \in \mathbb{C}$ bel.) $\quad i := i_1 \quad i(n) = n$

$i_0(n) = 1$