PRO–SEMINAR ZUR ANALYSIS
29.05.2006
Zahlen von besonderem Interesse

Seit vielen Jahren hat man versucht geschickte Bildungsgesetze für Primzahlen anzugeben.

Bsp.: EULER zeigte, dass das Polynom $f(X) = X^2 - X + 41 \in Z[X]$ Primzahlen erzeugt für alle $n \in Z$ mit $-39 \leq n \leq 40$.

Frage: Gibt es also ein Polynom, das nur Primzahlen erzeugt oder alle Primzahlen erzeugt?

1) Satz: Sei $f(\mathrm{X}) \in Z[\mathrm{X}]$ nicht konstant.
Dann gibt es $a, b \in Z$ mit $a \neq 0$,
so dass $f(ak+b) \notin P$ für alle $k \in Z$.

Lemma: Für $0 \neq n \in Z$ und $d \in Z$ gilt:
a) Ist d ein Teiler von n, so gilt $1 \leq |d| \leq |n|$.
b) Ist d ein echter Teiler von n, so gilt $1 < |d| < |n|$.

Beweis Sei $f(X) = a_n X^n + ... + a_0$ mit $a_n \neq 0$, $n \geq 1, \deg(f) = n$
Dann nimmt f jeden Wert höchstens n-mal an.

Daher existiert ein $x_0 \in Z$ mit $y_0 = f(x_0) \notin \{0,1,-1\}$

$$
\begin{aligned}
f(x_0 + y_0 k) &= a_n (x_0 + y_0 k)^n + ... + a_1 (x_0 + y_0 k) + a_0 \\
&= a_n \cdot \sum_{k=0}^{n} \binom{n}{k} x_0^{n-k} y_0^k + ... + a_1 x_0 + a_1 y_0 k + a_0 \\
&= \underbrace{a_n x^n + ... + a_1 x}_{f(x_0)} \qquad + y_0 \cdot (...) \\
&= f(x_0) \qquad + y_0 \cdot g(k) \\
&= y_0 \qquad + y_0 \cdot g(k) \\
&= y_0 (1 + g(k))
\end{aligned}
$$

mit $g(X) = a_n \cdot y_0^{n-1} \cdot X^n + ... \in Z[X]$ und $\deg(g) = n$
Es ex. ein $m \in N$ mit $|g(k)| \geq 3 \quad \forall |k| \geq m$

Also ist y_0 echter Teiler von $f(x_0 + y_0 k) \quad \forall |k| \geq m$

$y_0 | y_0 (1 + g(k))$

Jochen Nehrings

Wähle dann $a = 2my_0$, $b = x_0 + my_0$ und es folgt

$$f(a \cdot l + b) = f(x_0 + y_0 \cdot \underbrace{(2 \cdot l + 1) \cdot m}_{\in N}) \quad \text{mit} \quad |(2 \cdot l + 1) \cdot m| \geq m$$

$$= y_0 + y_0 \cdot g((2 \cdot l + 1) \cdot m),$$

also $y_0 | f(a \cdot l + b)$ und daraus folgt $f(a \cdot l + b) \notin P$.

Ein andere Weise, Primzahlen zu konstruieren geht auf FERMAT zurück.

2) Lemma: Wenn $2^m + 1, m \in N$ eine Primzahl ist, dann ist m eine Potenz von 2, d.h. $m = 2^n, n \in N_0$.

Beweis: Sei $m = k \cdot l$, $k = 2^n$, $n \in N_0$, $l \in N$ ungerade und mit der geom. Summenformel gilt dann

$$\begin{aligned} 2^m + 1 &= 2^{k \cdot l} + 1 \\ &= 1 + (2^k)^l = 1 - (-2^k)^l \\ &= (1 - (-2^k)) \cdot \sum_{j=0}^{l-1} (-2^k)^j \\ &= (2^k + 1) \cdot \sum_{j=0}^{l-1} (-2^k)^j \end{aligned}$$

Daraus folgt $(2^k + 1) | (2^m + 1)$ und da $2^k + 1 > 1$, $2^m + 1 \in P$ gilt $2^k + 1 = 2^m + 1$ und man erhält $m = k = 2^n$ und $l = 1$.

3) Definition: Für $n \in N_0$ heißt $F_n := 2^{2^n} + 1$ die n-te FERMATsche Zahl. Ist F_n eine Primzahl, so spricht man von einer FERMATschen Primzahl.

Bsp.: $F_0 = 3 \quad F_1 = 5 \quad F_2 = 17 \quad F_3 = 257 \quad F_4 = 65537 \quad \in P$

Aber: $F_5 = 2^{32} + 1 \notin P$

Anwendung findet dies in der Algebra ...

4) Satz v Gauß: Das regelmäßige n-Eck ist genau dann mit Zirkel und Lineal konstruierbar, wenn n von der Form $n = 2^s \cdot t$ ist, wobei $s \in N_0$ und

$t = 1$

oder ein Produkt verschiedener FERMATscher Primzahlen ist.

Das größte bekannte derartige t ist damit
$t = F_0 \cdot F_1 \cdot F_2 \cdot F_3 \cdot F_4 = 2^{32} - 1$

Damit kommen wir zu einer anderen Bildung von Primzahlen.

5) Lemma: Seien $a, m \in N, m > 1$,
so dass $a^m - 1$ eine Primzahl ist.
Dann ist $a = 2$ und m eine Primzahl.

Beweis Es gilt $1^m - 1 = 0 \quad \notin P$
Also muss gelten: $a > 1$.

mit der geom. Summenformel (wie im 2. Beweis) folgt

$$a^m - 1 = (a-1) \cdot \sum_{j=0}^{m-1} a^j$$

$$\Rightarrow \qquad a - 1 \,|\, a^m - 1$$

Da $0 < a - 1 < a^m - 1$ und $(a^m - 1) \in P$,
kann nur $1 \,|\, a^m - 1$
Daraus folgt $a - 1 = 1$ äquivalent zu $a = 2$.

Angenommen $m \notin P$,
daraus folgt $m = r \cdot s$ mit $1 < r, s < m$ und es gilt

$$a^m - 1 = (a^r)^s - 1 = (a^r - 1) \cdot \sum_{j=0}^{s-1} (a^r)^j$$

Daraus würde folgen, dass $(a^r - 1) \,|\, (a^m - 1)$.
da aber $a^r - 1 > 1$ mit $a = 2$, $r > 1$,
ist das ein Wiederspruch zur Voraussetzung $(a^m - 1) \in P$

Damit kann $a^r - 1$ nicht $a^m - 1$ teilen und es muss $m \in P$ gelten.

6) Definition: Die Zahlen $M_q = 2^q - 1, q \in P$ heißen MERSENNEsche Zahlen
bzw. MERSENNEsche Primzahlen, falls sie zu P gehören.

Bsp.: $M_2 = 3 \quad M_3 = 7 \quad M_5 = 31 \quad M_7 = 127 \quad \in P$
Aber: $M_{11} = 2^{11} - 1 = 2047 = 23 \cdot 89 \quad \notin P$

Der Primzahl-Weltrekord wird regelmäßig mit MERSENNEschen Primzahlen aufgestellt.
Seit Dezember 2005 ist die größte Primzahl $M_{30.402.457} = 2^{30.402.457} - 1$ mit 9.152.052 Stellen.

www.mersenne.org

Jochen Nehrings

Nun zu einer anderen Charakterisierung von Zahlen.

7) Definition: Man nennt $n \in N$

vollkommen , wenn $\sigma(n) = 2n$,

bzw. *defizient* , wenn $\sigma(n) < 2n$,

bzw. *abundant* , wenn $\sigma(n) > 2n$.

Mit $\sigma(n) := \sum_{d \in N, d|n} d$ (Teilersumme von n)

Bsp.: 6 ist vollkommen, denn $\sigma(6) = 1+2+3+6 = 12 = 2 \cdot 6$.

12 ist abundant, denn $\sigma(12) = 1+2+3+4+6+12 = 28 > 2 \cdot 12 = 24$.

Jede Primzahl ist defizient, da $\sigma(p) = 1 + p < 2p$ für $p \in P$.

Man kann gerade vollkommene Zahlen beschreiben.

8) Satz: Für eine gerade natürliche Zahl n sind äquivalent:

(i) n ist *vollkommen*

(ii) $n = 2^{q-1} \cdot M_q$, mit einer MERSENNEschen Primzahl M_q.

Beweis

(ii) $\longrightarrow$ (i) Für $n = 2^{q-1} \cdot M_q$ mit $M_q = 2^q - 1 \in P$, MERSENNEschen Primzahl

gilt mit der Identität von $\sigma(n) = \prod_{\substack{p \in P \\ p|n}} \frac{p^{\upsilon_p(n)+1} - 1}{p-1}$

$$
\begin{aligned}
\sigma(n) &= \frac{2^{(q-1)+1} - 1}{2-1} \cdot (M_q + 1) \\
&= \frac{2^q - 1}{1} \cdot (2^q - 1 + 1) \\
&= (2^q - 1) \cdot 2^q \\
&= 2 \cdot 2^{q-1} \cdot (2^q - 1) \\
&= 2 \cdot n
\end{aligned}
$$

Daraus folgt, dass n vollkommen ist.

(i) $\longrightarrow$ (ii) Sei n vollkommen , $n = 2^{q-1} \cdot m$, $q \geq 2$, $m \in N$ ungerade und mit der Identität bzw. der Definition von $\sigma(n)$ gilt:

$$
\begin{aligned}
\sigma(n) = 2 \cdot n &= 2 \cdot 2^{q-1} \cdot m = 2^q \cdot m \\
&= \sigma(2^{q-1}) \cdot \sigma(m) \\
&= (2^q - 1) \cdot \sigma(m)
\end{aligned}
$$

Damit folgt

$$\sigma(m) = \frac{2^q}{2^q - 1} \cdot m = m + k \quad \text{mit } 0 < k = \frac{m}{2^q - 1} < m$$

Wegen $\sigma(m) \in N$, folgt $k \in N$ und damit $m \geq 3$.

Also gilt $m = k \cdot (2^q - 1)$,
daraus folgt $k \mid m$, d.h. k ist positiver Teiler von m.

Da $\sigma(m) = m + k$, sind k und m die einzigen Teiler von m.
Das bedeutet $k = 1$.
Dann gilt $m = k \cdot (2^q - 1)$ bzw. $m = 2^q - 1 = M_q$
Somit muss m Mersenne'sche Primzahl sein .

Mit Hilfe dieses Satzes erhält man die vollkommenen Zahlen

$$2^1 M_2 = 6 \quad 2^2 M_3 = 28 \quad 2^4 M_5 = 496 \quad 2^6 M_7 = 8128$$

Offene Probleme:

a) Gibt es Fermatsche Primzahlen $F_n, n > 5$?
b) Gibt es unendlich viele MERSENNEsche Primzahlen?
c) Gibt es ungerade, vollkommene Zahlen?

Jochen Nehrings