Universität Karlsruhe (TH)
Mathematisches Institut II
Prof. Dr. H.-W. Leopoldt

Karlsruhe, 3.5.1990

Elementare Zahlentheorie — Übungsblatt 2

Aufgabe 3 (7 Punkte)

Zeigen Sie:

(a) $M_n = 2^n - 1$ $(n \in \mathbb{N})$ ist nur dann Primzahl, wenn n Primzahl ist. M_n heißt *Mersennesche Primzahl.*

(b) $2^n + 1$ $(n \in \mathbb{N})$ ist nur dann Primzahl, wenn n eine Zweierpotenz $n = 2^k$ ist. Falls $F_k = 2^{2^k} + 1$ eine Primzahl ist, heißt es *Fermatsche Primzahl.* (Es ist nicht bekannt, ob es unendlich viele Fermatsche Primzahlen gibt.)

(c) Für $n \in \mathbb{N}$ gilt $\left(\prod_{\nu=1}^{n-1} F_\nu, F_n\right) = 1$. Zeigen Sie daraus, daß es unendlich viele Primzahlen gibt.

* (d) Wann kann $4^n + 2^n + 1$ eine Primzahl sein?

Aufgabe 4 (6 Punkte)

Man beweise die folgenden Aussagen bzw. weise mit einem Gegenbeispiel nach, daß sie falsch sind:
(Hierbei seien $a, b, c \in \mathbb{N}$, $p \in \mathbb{P}$.)

(a) $(a,b) = (a,c) \Rightarrow (a^2, b^2) = (a^2, c^2)$
(b) $(a,b) = (a,c) \Rightarrow (a,b) = (a,b,c)$
(c) $(a,b,c) = ((a,b),(a,c))$
(d) $(a,b) = 1 \Rightarrow (a^2, ab, b^2) = 1$
(e) $p \mid a \wedge p \mid (a^2 + b^2) \Rightarrow p \mid b$
(f) $p \mid a^7 \Rightarrow p \mid a$
(g) $a^3 \mid c^3 \Rightarrow a \mid c$
(h) $a^3 \mid c^2 \Rightarrow a \mid c$
(i) $a^2 \mid c^3 \Rightarrow a \mid c$
(j) $p \mid (a^2 + b^2) \wedge p \mid (b^2 + c^2) \Rightarrow p \mid (a^2 - c^2)$
(k) $p \mid (a^2 + b^2) \wedge p \mid (b^2 + c^2) \Rightarrow p \mid (a^2 + c^2)$
(l) $b \mid (a^2 + 1) \Rightarrow b \mid (a^4 + 1)$
(m) $b \mid (a^2 - 1) \Rightarrow b \mid (a^4 - 1)$

Aufgabe 5 (4 Punkte)

Sei p Primzahl. Zeigen Sie:

(a) Für $n \in \mathbb{N}_0$ ist die Vielfachheit von p in $n!$

$$\nu_p(n!) = \sum_{i=1}^{\infty} \left\lfloor \frac{n}{p^i} \right\rfloor$$

* (b) Für $m, n \in \mathbb{N}_0$ ist $\nu_p\left(\binom{m+n}{n}\right)$ gleich der Anzahl der Überträge, die beim Addieren von m und n im Ziffernsystem der Basis p auftreten.

Aufgabe 6 (5 Punkte)

Der euklidische Algorithmus liefert zu $a, b \in \mathbb{N}_0$ den ggT $g = (a, b)$. Folgende Variante liefert auch eine Darstellung $g = u \cdot a + v \cdot b$ mit $u, v \in \mathbb{Z}$, und zwar fast immer mit kleinstmöglichem $|u|$ und kleinstmöglichem $|v|$:

Seien $a, b \in \mathbb{N}_0$ gegeben.
Man betrachtet Tripel (x, y, z) mit $x \cdot a + y \cdot b = z$, $x \in \mathbb{Z}$, $y \in \mathbb{Z}$, $z \in \mathbb{N}_0$.
Man startet mit $(x_1, y_1, z_1) = (1, 0, a)$ und $(x_2, y_2, z_2) = (0, 1, b)$.
Für $n = 2, 3, \ldots$:
Falls $z_n > 0$, dividiere man z_{n-1} durch z_n mit Rest: $z_{n-1} = q \cdot z_n + z_{n+1}$ und setze $(x_{n+1}, y_{n+1}, z_{n+1}) := (x_{n-1}, y_{n-1}, z_{n-1}) - q \cdot (x_n, y_n, z_n)$.
Falls $z_n = 0$, breche man ab, setze $m := n$ und liefere $(x_{m-1}, y_{m-1}, z_{m-1})$ als Ergebnis.

$z_{m-1} = g$ ist aus der Vorlesung bekannt.

(a) Finden Sie u, v mit $u \cdot a + v \cdot b = (a, b)$, wobei $a = 279$, $b = 191$ bzw. $a = 123456$ und b Ihre Matrikelnummer sei.

(b) Zeigen Sie: Für das Ergebnis $(u, v, g) = (x_{m-1}, y_{m-1}, z_{m-1})$ gilt $g = (a, b) \geq 0$, $u \cdot a + v \cdot b = g$.
Falls $b = 0$: $m = 2$, $(u, v, g) = (1, 0, a)$.
Falls $b > 0$ und $b \mid a$: $m = 3$, $(u, v, g) = (0, 1, b)$.
Falls $b > 0$ und $b \nmid a$: $m > 3$, $g > 0$, $|u| \leq \frac{b}{2g}$, $|v| \leq \frac{a}{2g}$.
(Hinweise:
Untersuchen Sie die Vorzeichen von x_n und y_n.
Was passiert mit den Ausdrücken $x_n \cdot y_{n+1} - x_{n+1} \cdot y_n$, $x_n \cdot z_{n+1} - x_{n+1} \cdot z_n$, $y_n \cdot z_{n+1} - y_{n+1} \cdot z_n$ beim Schritt von $n-1$ auf n?
Setzen Sie dann $n = m - 1$ ein.)

* **Aufgabe 7** (6 Punkte)

Zeigen Sie: Für $n \in \mathbb{N}$ ist die Gleichung

$$\frac{4}{n} = \frac{1}{x} + \frac{1}{y}$$

genau dann in natürlichen Zahlen x, y lösbar, wenn n einen Primteiler hat, der nicht von der Form $p = 4k+1$ ist.

Abgabe: Bis spätestens Donnerstag, 10.5.1990, 15.30 Uhr in den Kasten bei Zi. 308 des Mathematikgebäudes oder in der Übung im Hörsaal Hauptbau.