11. Übungsblatt

MATHEMATIK FÜR INFORMATIKER I (WS 2000/01)

Abgabe: Montag, 22.1.2001 bis **13.00 Uhr !!!**

Internet–Adresse der Vorlesung:
http://math–www.uni–paderborn.de/~chris/index9.html

39. Aufgabe: a) Es sei $n \in \mathbb{N}$ eine natürliche Zahl, die weder von 2 noch von 3 geteilt wird. Zeige, daß sich n in der Form $n = 6k + 1$ oder $n = 6k - 1$ mit einem geeigneten $k \in \mathbb{N}$ darstellen läßt (Hinweis: Überlege dir, daß bei Division von n durch 6 die Reste 0,2,3 und 4 nicht auftreten können).

b) Beweise: Ist $p \geq 5$ eine Primzahl, so gilt $p \equiv \pm 1 \pmod 6$.

c) Finde eine Zahl $k \in \mathbb{N}$, für die die Zahlen $6k - 1$ und $6k + 1$ beide keine Primzahlen sind. (4)

40. Aufgabe: Mit dem folgenden Verfahren von Fermat wird ein Teiler einer ungeraden natürlichen Zahl n bestimmt:

1. Setze $x := \lfloor \sqrt{n} \rfloor$
2. Teste, ob $x^2 - n$ eine Quadratzahl ist
3. Wenn ja, brich das Verfahren ab. $x - \sqrt{x^2 - n}$ und $x + \sqrt{x^2 - n}$ sind dann zwei zueinander komplementäre Teiler von n
4. Wenn nein, erhöhe x um 1 und gehe mit 2. weiter

a) Begründe, daß in 3. wirklich Teiler von n gefunden werden.

b) Zeige, daß das Verfahren spätestens bei $x = \frac{n+1}{2}$ abbricht. (Warum ist $\frac{n+1}{2} \in \mathbb{N}$?)

c) Was bedeutet es für n, wenn das Verfahren erst bei $x = \frac{n+1}{2}$ abbricht?

d) Berechne einen Teiler von $n := 96133$ mit dem Verfahren von Fermat. (5)

41. Aufgabe: Sei p eine Primzahl. Beweise, daß p ein Teiler der Binomialkoeffizienten $\binom{p}{1}, \binom{p}{2}, \ldots, \binom{p}{p-1}$ ist, d.h. $p \left| \binom{p}{k} \right.$ für alle $k = 1, 2, \ldots, p-1$. (3)

42. Aufgabe: Die natürliche Zahl n besitze die Darstellung $n = (a_r a_{r-1} \ldots a_1 a_0)_7$ $(a_k \in \{0, 1, \ldots, 6\}\ \forall k)$ bzgl. der Basiszahl 7, und es bezeichne $Q_7(n) := \sum_{k=0}^{r} a_k$ die Quersumme und $Q_7^{alt}(n) := \sum_{k=0}^{r} (-1)^k a_k$ die alternierende Quersumme von n .

a) Beweise: $Q_7(n) \equiv n \pmod 3$, $Q_7^{alt}(n) \equiv n \pmod 4$.

b) Leite aus a) her: $3 \mid n \iff 3 \mid Q_7(n)$, $4 \mid n \iff 4 \mid Q_7^{alt}(n)$. (4)