**Technische Universität Clausthal**
**Institut für Mathematik**
**Prof. Dr. L. G. Lucht**

**WS 1999/2000**
**06.12.1999**
**7. Übungsblatt**

# Elementare Zahlentheorie

Diese Aufgaben werden in der Übungsstunde vom 15.12.1999 besprochen;
Abgabe schriftlicher Lösungen (Aufgaben 1 bis 4) bitte am Montag, 13.12.1999, vor der Vorlesung.

1. Zeigen Sie, daß sich keine Zahl der Form $4^m\,(8k+7)$ mit $m, k \in \mathbb{N}_0$ als Summe von drei Quadratzahlen darstellen läßt.

2. Es sei $p$ eine ungerade Primzahl. Zeigen Sie $\displaystyle\sum_{n=1}^{p-2} \Big(\frac{n(n+1)}{p}\Big) = -1\,.$

   Hinweis: $n(n+1) = n^2\,(1+n^{-1})\,.$

3. Es seien $a, b, \alpha, \beta, d \in \mathbb{R}$ und $d > 0$. Zeigen Sie durch Rechnung im Komplexen

$$(a^2 + d\,b^2)(\alpha^2 + d\,\beta^2) = (a\alpha \pm d\,b\beta)^2 + d\,(a\beta \mp b\alpha)^2.$$

4. Zeigen Sie, daß jede Primzahl $p \equiv 1 \bmod 6$ eine Darstellung $p = x^2 + 3\,y^2$ mit $x, y \in \mathbb{Z}$ besitzt und daß keine andere Primzahl $p \neq 3$ diese Eigenschaft aufweist.

5. Arbeiten Sie den Beweis des folgenden Satzes so durch, daß Sie ihn vortragen können. Zur Erinnerung: Eine zusammengesetzte Zahl $n \in \mathbb{N}$ heißt Carmichael-Zahl, wenn $x^n \equiv x \bmod n$ für alle $x \in \mathbb{N}$ mit $\mathrm{ggT}\,(n, x) = 1$ gilt.

   **Satz.**

   (a) Jede Carmichael-Zahl ist ungerade.

   (b) Keine Carmichael-Zahl ist durch eine Quadratzahl $> 1$ teilbar.

   (c) Ist $n$ Carmichael-Zahl, so gilt $(p-1) \mid (n-1)$ für jeden Primteiler $p$ von $n\,.$

   (d) Jede Carmichael-Zahl besitzt mindestens drei Primfaktoren.

   (e) Genau dann ist $n$ Carmichael-Zahl, wenn $n = p_1 \cdots p_r$ mit $r \geq 3$ verschiedenen ungeraden Primzahlen $p_\varrho$ gilt, die $(p_\varrho - 1) \mid (n-1)$ erfüllen.

*Beweis des Satzes.*

(a) Angenommen, es ist $n = 2m$ mit ganzem $m \in \mathbb{N}$ eine Carmichael-Zahl. Dann gilt für jedes $x \in \mathbb{Z}$ mit $\operatorname{ggT}(x, n) = 1$ stets $x^{2m} - x \equiv 0 \bmod n$, speziell für $x = -1$ also $2 \equiv 0 \bmod n$ und damit $n = 2$ entgegen der Definition (als Carmichael-Zahl ist $n$ nicht prim).

(b) Vorbemerkung: Wir verwenden (ohne Beweis) die Existenz von Primitivwurzeln modulo ungerader Primzahlpotenzen $p^k$ (Aufgabe 5 (b) von Übungsblatt 6 behandelte nur den Fall $k = 1$).

Angenommen, es ist $n$ nicht quadratfrei. Dann existieren $p \in \mathbb{P}$ mit $n = p^k m$, $k \geq 2$, $p \nmid m$, und nach der Vorbemerkung eine Primitivwurzel $g \bmod p^k$. Nach dem Chinesischen Restsatz ist das lineare Kongruenzsystem

$$\begin{aligned} a &\equiv g \bmod p^k \\ a &\equiv 1 \bmod m \end{aligned}$$

(wegen $p \nmid m$) lösbar mit einer eindeutigen Lösung $a \bmod p^k m = n$. Es ist $a$ zu $n$ teilerfremd: Wir nehmen die Existenz einer Primzahl $q$ mit $q \mid a$ und $q \mid p^k m$ an. Wäre $q = p$, so würde $p$ die Primitivwurzel $g \bmod p^k$ teilen, was unmöglich ist. Also gilt $q \mid m$ (und $q \mid a$) im Widerspruch zu $a \equiv 1 \bmod m$. Aus $\operatorname{ggT}(a, n) = 1$ folgt $a^{n-1} \equiv 1 \bmod n$ (da $n$ Carmichael-Zahl ist). Hieraus folgt wegen $a^{n-1} \equiv g^{n-1} \bmod p^k$

$$g^{n-1} \equiv 1 \bmod p^k.$$

Nun hat aber $g$ die Ordnung $\varphi(p^k) = p^{k-1}(p-1)$, und daher gilt

$$(*) \qquad p^{k-1}(p-1) \mid n-1.$$

Aus $k \geq 2$ folgt $p \mid n-1$ im Widerspruch zu $p \mid n$. Also ist $n$ quadratfrei.

(c) Es sei $p$ ein Primteiler von $n$. Nach (a) können wir $n = pm$ mit $p \nmid m$ annehmen. Aus der Teilerbeziehung $(*)$ mit $k = 1$ kommt $p - 1 \mid n - 1$.

(d) Wir nehmen an, die Carmichael-Zahl $n = pq$ sei aus den Primzahlen $p, q$ zusammengesetzt. Nach (c) gilt $p - 1 \mid pq - 1$, und aus $pq - 1 = (p-1)q + q - 1$ folgt $p - 1 \mid q - 1$. Analog sieht man $q - 1 \mid p - 1$. Dann ist aber $p = q$ im Widerspruch zu (b).

(e) Zu zeigen ist nur noch, daß $n \mid \left(x^n - x\right)$ für alle $x \in \mathbb{Z}$ mit $\operatorname{ggT}(x, n) = 1$ gilt, wenn $n$ aus wenigstens drei verschiedenen ungeraden Primzahlen $p$ mit $(p-1) \mid (n-1)$ zusammengesetzt ist. In der Tat ist für jeden Primteiler $p$ von $n$ mit $\lambda := \frac{n-1}{p-1} \in \mathbb{N}$ wegen der kleinen Fermatschen Satzes die Kongruenz

$$x^n = x^{n-1}\, x = \left(x^{p-1}\right)^{\lambda} x \equiv x \bmod p$$

oder gleichwertig $p \mid \left(x^n - x\right)$ für alle $x \in \mathbb{Z}$ erfüllt, woraus $n \mid \left(x^n - x\right)$ für (sogar) alle $x \in \mathbb{Z}$ kommt. Folglich ist $n$ Carmichael-Zahl.

□