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

WS 1999/2000
29.11.1999
6. Übungsblatt

Elementare Zahlentheorie

Diese Aufgaben werden in der Übungsstunde vom 08.12.1999 besprochen;
Abgabe schriftlicher Lösungen bitte am Montag, 06.12.1999, vor der Vorlesung.

1. Untersuchen Sie, ob die folgenden Kongruenzen lösbar sind:

   (a) $x^2 \equiv 82 \bmod 229$,

   (b) $x^2 \equiv 238 \bmod 263$,

   (c) $2x^2 + 93x - 83 \equiv 0 \bmod q$, wobei $q := 29^2 \cdot 37$.

2. Zeigen Sie, daß die Gleichung $(*)\ x^2 + 3xy - 2y^2 = 122$ keine Lösungen $x, y \in \mathbb{Z}$ besitzt.

   Anleitung: Zeigen Sie zunächst, daß aus der Lösbarkeit von $(*)$ die Lösbarkeit der Kongruenz $z^2 \equiv 488 \bmod 17$ folgt.

3. Ermitteln Sie alle Primteiler der Folge $(n^2 - 28)$.

Es sei $1 \neq q \in \mathbb{N}$. Gibt es in der primen Restklassengruppe $G(q)$ ein Element a der Ordnung $\varphi(q)$, so ist $G(q)$ zyklisch und a heißt eine Primitivwurzel $\bmod q$. Die beiden folgenden Aufgaben haben die Existenz von Primitivwurzeln $\bmod p$ für Primzahlen p zum Ziel.

4. Es sei p eine Primzahl und $a \in G(p)$ ein Element der Ordnung h. Zeigen Sie:

   (a) Alle Lösungen der Kongruenz $x^h \equiv 1 \bmod p$ sind gegeben durch die Restklassen a^k mit $k = 0, 1, \ldots, h-1$.

   (b) Alle Elemente von $G(p)$ der Ordnung h sind durch a^k mit $k \in \{0, \ldots, h-1\}$, $\mathrm{ggT}\,(h, k) = 1$, gegeben.

5. Es sei p eine Primzahl. Zu jedem Teiler $h \in \mathbb{N}$ von $p - 1$ bezeichne $\psi(h)$ die Anzahl der Elemente von $G(p)$ der Ordnung h.

   (a) Zeigen Sie $\displaystyle\sum_{h|p-1} \psi(h) = \sum_{h|p-1} \varphi(h)$.

   (b) Folgern Sie, daß $G(p)$ zyklisch ist.