UNIVERSITÄT ULM
Institut für Zahlentheorie und Wahrscheinlichkeitstheorie

Übungen zur Angewandten Diskreten Mathematik

Prof. Dr. Helmut Maier, Hans- Peter Reck

Gesamtpunktzahl: 48 Punkte

Übungsblatt 5

Abgabe: Freitag, 17. Dezember 2010, vor den Übungen

1. Ein Element g einer Gruppe heißt selbstinvers, falls $g^{-1} = g$ ist. Zeige:
   (a) Ist in einer Gruppe jedes Element selbstinvers, so ist G abelsch.
   (b) Gibt es in einer Gruppe G außer dem neutralen Element noch weitere selbstinverse Elemente, so ist G entweder endlich oder nicht zyklisch. (7 Punkte)

2. Es sei G eine abelsche Gruppe. Zeige:
   (a) Sind $a, b \in G$ mit ord a und ord a teilerfremd, so gilt ord $(ab) =$ ord $a \cdot$ ord b.
   (b) Sei $m := \max_{a \in G} \operatorname{ord} a$, so gilt ord $a | m$ für alle $a \in G$. (7 Punkte)

3. Es sei
$$G = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix}, a, b, c, d \in \mathbb{Z},\ ad - bc = 1 \right\}.$$
   Zeige, daß G eine Gruppe bzgl. der Matrixmultiplikation bildet. (5 Punkte)

4. Zeige für $a, b \in \mathbb{N}$ und $p \in \mathbb{P}$:
$$a^p \equiv b^p \bmod p \Rightarrow a^p \equiv b^p \bmod p^2.$$
   (4 Punkte)

5. Es sei p eine Primzahl mit $p > 2$.
   (a) Zeige: $x^2 \equiv 1 \bmod p$ hat genau zwei Lösungen $\bmod p$.
   (b) Bestimme diese Lösungen.
   (c) Bestimme sämtliche Lösungen von $x^2 \equiv 1 \bmod 1001$.

   Hinweis:
   Es ist $1001 = 7 \cdot 11 \cdot 13$. (7 Punkte)

6. Entscheide für jeden der folgenden Moduln m, ob $r = 3$ eine Primitivwurzel mod m ist.

   (a) $m = 5$

   (b) $m = 7$

   (c) $m = 11$

   (d) $m = 13$

   (e) $m = 17$ (10 Punkte)

7. Der Ring $\mathbb{Z}[i]$ der Gaußschen Zahlen ist als $\mathbb{Z}[i] = \{a + b \cdot i |\ a, b \in \mathbb{Z}\}$ mit $i^2 = -1$ mit der üblichen Addition und Multiplikation komplexer Zahlen definiert.
   Für $\xi \in \mathbb{Z}[i]$ definiert man die Kongruenz $\bmod \xi$ durch

$$\alpha \equiv \beta \bmod \xi \Rightarrow \xi | (\beta - \alpha),$$

   d.h. es existiert ein η mit $\beta - \alpha = \eta \cdot \xi$. Die Äquivalenzklassen bzgl. $\bmod \xi$ heißen Restklassen $\bmod \xi$. Sie bilden den Ring $(\mathbb{Z}[i]/\xi\mathbb{Z}[i], +, \cdot)$.

   (a) Bestimme die Verknüpfungstafeln für Addition und Multiplikation für den Ring $(\mathbb{Z}[i]/\xi\mathbb{Z}[i], +, \cdot)$.

   (b) Für welche $\xi \in \{2, 3\}$ ist $(\mathbb{Z}[i]/\xi\mathbb{Z}[i], +, \cdot)$ ein Körper? (8 Punkte)