Fakultät für Mathematik
Universität Bielefeld
Joa Weber

WS 2010/11

Elementare Zahlentheorie

Übungsblatt 12

Abgabe: In den Übungsgruppen am 27.01. und 28.01.2011

Vermerken Sie bitte auf jeder Abgabe: **Name, Matrikelnummer, Übungsgruppe**
Präsenzübungsblätter können zur Lösung verwendet werden

Aufgabe 1. a) Bestimmen Sie die inversen Elemente zu $\bar{3}$ und zu $\bar{5}$ im Körper $\mathbb{Z}_{11}$. Wie viele Elemente besitzt die prime Restklassengruppe $\mathbb{Z}_{11}^*$? Wie viele Primitivwurzeln zu 11 gibt es?

b) Bestimmen Sie die prime Restklassengruppe $\mathbb{Z}_{10}^*$. Wie viele erzeugende Elemente besitzt $\mathbb{Z}_{10}^*$? Bestimmen Sie zu jedem Element von $\mathbb{Z}_{10}^*$ die Ordnung und das inverse Element. Bestimmen Sie den Exponenten von $\mathbb{Z}_{10}^*$.

c) Bestimmen Sie den Exponenten von $\mathbb{Z}_8^*$.

Aufgabe 2. Für zwei Gruppen G und H erhält man eine Gruppenstruktur auf dem kartesischen Produkt $G \times H := \{(g,h) \mid g \in G, h \in H\}$ durch die Vorschrift $(g,h) \cdot (g',h') := (gg', hh')$ für $g, g' \in G$ und $h, h' \in H$. Zeigen Sie: Sind G und H zyklische Gruppen der Ordnung m bzw. n, so ist die Gruppe $G \times H$ genau dann zyklisch, wenn m und n teilerfremd sind.

Aufgabe 3. Eine Abbildung $\Psi : G \to G'$ zwischen zwei Gruppen G, G' heißt **Gruppenhomomorphismus**, falls gilt

$$\Psi(ab) = \Psi(a)\Psi(b), \qquad \forall a, b \in G.$$

Für $m \in \mathbb{N}$ und $a \in \mathbb{Z}$ bezeichne ${}^m\overline{a}$ die Restklasse von a in $\mathbb{Z}_m$. Seien nun m, n teilerfremd. Beweisen Sie, daß durch

$$\Psi({}^{mn}\overline{a}) := ({}^m\overline{a}, {}^n\overline{a}), \qquad \forall a \in \mathbb{Z} \text{ teilerfremd zu } m \text{ und zu } n,$$

ein **bijektiver** (d.h. ein injektiver und surjektiver) Gruppenhomomorphismus von $\mathbb{Z}_{mn}^*$ nach $\mathbb{Z}_m^* \times \mathbb{Z}_n^*$ definiert wird.

Aufgabe 4. Sei $p \in \mathbb{P}$ mit $p \equiv 1(4)$ und sei w eine Primitivwurzel zu p. Zeigen Sie, daß dann auch $p - w$ eine Primitivwurzel zu p ist.