

Diskrete Mathematik für Informatiker, WS13/14
Übungsblatt 8, Besprechung in den Übungen vom 6.–8. Jan.

Aufgabe 1. Berechnen Sie das multiplikative Inverse von 2, 3, 22 und 50 in $\mathbb{Z}_{101}$.

Aufgabe 2. Bei der Buchnummer 321910?737 ist die 7. Stelle leider unleserlich. Welche Ziffer fehlt, damit wir eine korrekte ISBN-10 erhalten? (Vergessen Sie nicht Ihre Begründung).

Aufgabe 3. Sei n eine natürliche Zahl. Finden Sie k mit $0 \leq k < n$, so daß

- (a) $k \equiv n + 1 \pmod{n}$
- (b) $k \equiv n^2 \pmod{n}$
- (c) $k \equiv 2n + 5 \pmod{n}$
- (d) $k \equiv 4n - 1 \pmod{n}$
- (e) $k \equiv n(n + 1) \pmod{n}$
- (f) $k \equiv (n - 1)^2 \pmod{n}$
- (g) $k \equiv (2n + 1)(n + 1) \pmod{n}$
- (h) $k \equiv (n - 1)^{10001} \pmod{n}$

Aufgabe 4. Die symmetrische Differenz zweier Mengen A, B ist definiert als

$$A \triangle B = (A \setminus B) \cup (B \setminus A) .$$

Zeigen Sie, daß für eine festgewählte Menge M die Menge aller Teilmengen von M zusammen mit der symmetrischen Differenz, also $(\mathcal{P}(M), \triangle)$ eine abelsche Gruppe ist. Sie können annehmen, daß $\triangle$ assoziativ ist.

Aufgabe 5. Dies hätte eine wunderbare Aufgabe zu einer Gruppe $(\{a, b, c, d, f, g\}, \circ)$ mit 6 Elementen sein sollen. Leider habe ich vergessen, wie genau die Gruppenverknüpfung aussieht. Wenn ich mich recht erinnere sollte die Gruppe abelsch sein. Ergänzen Sie den Rest der Verknüpfungstabelle.

$\circ$	a	b	c	d	f	g
a	f	c	g			
b		d				
c		a				
d						
f	d					
g					c	

Aufgabe 6. Beweisen Sie, daß wenn $(G, \circ)$ eine Gruppe ist, in der für jedes Element $x \in G$ gilt daß $x^2 = e$, dann ist $(G, \circ)$ eine kommutative Gruppe. Geben Sie in jedem Schritt an welches der Gruppenaxiome G1-G3 verwendet wird.

Tipp: Man beachte, daß für beliebige $x, y \in G$, auch gilt, daß $(x \circ y)^2 = e$, da $x \circ y$ ja auch wieder Element von G ist.

Aufgabe 7. (a) Was sind die Ordnungen der vier Elemente in $\mathbb{Z}_4$ und der vier Elemente von $\mathbb{Z}_5^*$?¹

(b) Geben Sie einen Isomorphismus zwischen $\mathbb{Z}_4$ und $\mathbb{Z}_5^*$ an (ohne Beweis).

(c) Zeigen Sie, daß $\mathbb{Z}_9$ und $\mathbb{Z}_3 \times \mathbb{Z}_3$ nicht isomorph sein können.

Hinweis: in $\mathbb{Z}_3 \times \mathbb{Z}_3$ hat jedes Element eine Ordnung kleiner gleich 3.

Zusatzaufgabe 8. Wie wir oben gesehen haben ist $(\mathcal{P}(M), \Delta)$ eine Gruppe. Zeigen Sie nun, daß wenn M endlich ist, diese Gruppe isomorph zu $(\mathbb{Z}_2)^{|M|}$ ist.

ENDE

¹Die Ordnung eines Elementes a war ja definiert als die kleinste natürliche Zahl m , so daß $a^m = e$. In dieser Definition ist mit a^m gemeint, daß das Element a m -mal mit sich selbst verknüpft wird. Im Falle von modulare Arithmetik mit Addition als Verknüpfung also m -mal mit sich selbst addiert wird, also mit m malgenommen und nicht hoch m genommen wird.