universität wien
Fakultät für Mathematik

Arman Sadeghi Rad
Matrikelnummer 12223560
Einführung in das mathematische Arbeiten
Wintersemester 2022/2023

Übungsblatt 6B

Aufgabe 1. (i) 601 ist eine Primzahl. Nach dem kleinen Satz von Fermat, $p = 601$ und wenn a und p teilerfremde Zahlen sind, $a^{p-1} \equiv 1 \mod p$. Dann gilt

$$27^{4800} \equiv \left(27^{600}\right)^8 \equiv 1^8 \equiv 1 \mod p.$$

(ii)

$$27^{300} \equiv 3^{900} \equiv 3^{600} \cdot 3^{300} \equiv 1 \cdot 3^{300} \mod p.$$

Aufgabe 2. (i) Sei G die Gruppe $\mathbb{Z}_4$

$$f_2(3 \cdot 3) = f_2(9) = 2 \cdot 3 \cdot 3 = 18 \equiv 2 \not\equiv 0 \equiv 36 = (2 \cdot 3) \cdot (2 \cdot 3) = f_2(3) \cdot f_2(3).$$

und f_a ist ein Homomorphismus, genau dann wenn $a^2 = a$. Sei a ein idempotentes Element, dann $f_a(xy) = axy = a^2xy = axay = f_a(x)f_a(y)$. Und wenn f_a ein Homomorphismus ist, dann $f_a(xy) = f_a(x)f_a(y)$ und $axy = axay = a^2axy$ und a ist ein idempotentes Element.

(ii) Die Abbildung ist nach Definition wohldefiniert. Und wenn $f_a(x) = f_a(y)$ dann $ax = ay$. Da G eine Gruppe ist, kann daraus gefolgert werden, dass $x = y$. Außerdem für jedes f_a existiert ein $a \in G$.

Aufgabe 3. (i) Erstens zeigen wir, dass die Abbildung surjektiv ist. Nehmen wir an, dass (a, b) ein beliebiges Element von $\mathbb{Z}_m \times \mathbb{Z}_n$ ist. Um das entsprechende Element von $\mathbb{Z}_{mn}$ zu finden, sollte man das System

$$\begin{aligned} x &\equiv a \mod m \\ x &\equiv b \mod n \end{aligned}$$

lösen. Da m und n teilerfremde Elemente sind, nach dem chinesischem Restsatz, gibt es eine Lösung dazu. Zunächst prüfen wir, ob die Abbildung wohldefiniert ist. Wenn $x = y$ dann $x \equiv y \mod m$ und $x \equiv y \mod n$. Daher $f(x) = f(y)$. Zum Schluss beweisen wir, dass die Abbildung injektiv ist. Wenn $(x_1, y_1) = (x_2, y_2)$, dann $x_1 \equiv x_2 \mod m$ und $x_1 \equiv x_2 \mod n$. Da $(m, n) = 1$, gilt $x_1 \equiv x_2 \mod mn$. Ähnlicherweise könnte man diese Aussage auch für y_1 und y_2 beweisen.

(ii)

$$(x_1, y_1) + (x_2, y_2) := (x_1 + x_2, y_1 + y_2), \quad (x_1, y_1) \cdot (x_2, y_2) := (x_1x_2, y_1y_2).$$

Aufgabe 4. (i)

$$0^2 \equiv 0, 1^2 \equiv 1, 2^2 \equiv 4, 3^2 \equiv 4, 4^2 \equiv 1 \mod 5.$$

$$0^2 \equiv 0, 1^2 \equiv 1, 2^2 \equiv 4, 3^2 \equiv 2, 4^2 \equiv 2, 5^2 \equiv 4, 6^2 \equiv 1 \mod 7$$

$a \in \{0, 1, 4\}$ für $n = 5$ und $a \in \{0, 1, 2, 4\}$ für $n = 7$.

(ii) Wenn die Kongruenz eine Lösung d hat, dann es gibt genau zwei Lösungen d und $-d$. Angenommen es gibt eine andere inkongruente Lösung wie k. Dann gilt

$$k^2 \equiv d^2 \equiv (k-d)(k+d) \mod p.$$

Da $k \neq d$ und $k \neq -d$, p ist die Produkt von zwei positiven Zahlen. es ist ein Widerspruch zu der Annahme, dass p eine Primzahl ist.

(iii)

x	x^2	x^2 mod 35
1	1	$\boxed{1}$
2	4	4
3	9	9
4	16	16
5	25	25
6	36	$\boxed{1}$
7	49	14
8	64	29
9	81	11
10	100	30
11	121	16
12	144	4
13	169	29
14	196	21
15	225	15
16	256	11
17	289	9
−17	289	9
−16	256	11
−15	225	15
−14	196	21
−13	169	29
−12	144	4
−11	121	16
−10	100	30
−9	81	11
−8	64	29
−7	49	14
−6	36	$\boxed{1}$
−5	25	25
−4	16	16
−3	9	9
−2	4	4
−1	1	$\boxed{1}$