Prof. Dr. H. Brenner **Osnabrück SS 2025**

Zahlentheorie

Arbeitsblatt 6

Übungsaufgaben

Aufgabe 6.1. Man gebe für die Einheitengruppe $(\mathbb{Z}/(16))^\times$ explizit einen Isomorphismus zu einem Produkt von (additiven) zyklischen Gruppen an.

Aufgabe 6.2. Welche Ziffern treten im Dezimalsystem als Endziffern von Quadratzahlen auf?

Aufgabe 6.3. Bestimme sämtliche quadratische Reste modulo der Primzahlen < 20.

Aufgabe 6.4. Es sei p eine Primzahl mit $p = 1 \mod 4$. Zeige unter Verwendung des Satzes von Wilson, dass $\frac{p-1}{2}!$ eine Quadratwurzel von -1 ist.

Aufgabe 6.5. Finde Quadratwurzeln für 2 modulo p für alle Primzahlen p mit $p = \pm 1 \mod 8$ und $p \leq 32$.

Aufgabe 6.6. Es sei p eine ungerade Primzahl. Zeige, dass eine primitive Einheit von $\mathbb{Z}/(p)$ nie ein quadratischer Rest ist. Bestimme für die Primzahlen ≤ 20, ob darin jeder nichtquadratische Rest primitiv ist.

Aufgabe 6.7. Finde die kleinste Primzahl p derart, dass es in $\mathbb{Z}/(p)$ ein Element a gibt, das weder primitiv noch ein Quadrat noch gleich -1 ist.

Aufgabe 6.8.*

Wie viele Quadrate und wie viele primitive Elemente besitzt $\mathbb{Z}/(31)$? Wie viele Elemente besitzt $\mathbb{Z}/(31)$, die weder primitiv noch ein Quadrat sind? Es sei x ein primitives Element von $\mathbb{Z}/(31)$. Liste explizit alle Elemente x^i auf, die weder primitiv noch ein Quadrat sind.

Aufgabe 6.9. Bestimme die Quadrate in $\mathbb{Z}/(35)$.

Aufgabe 6.10.

(1) Finde die kleinste Zahl n mit der Eigenschaft, dass es eine Zahl $k < n$ gibt, die selbst kein Quadrat ist, aber ein Quadratrest modulo n.
(2) Finde die kleinste Primzahl p mit der Eigenschaft, dass es eine Zahl $k < p$ gibt, die selbst kein Quadrat ist, aber ein Quadratrest modulo p.
(3) Finde die größte Primzahl p mit der Eigenschaft, dass die einzigen Quadratreste modulo p die Quadratzahlen $k < p$ sind.
(4) Untersuche
$$n = 8, 16, 32$$
in Hinblick auf die Eigenschaft, ob es neben den Quadraten noch weitere Quadratreste modulo n gibt.
(5) Finde die größte (?) Zahl n mit der Eigenschaft, dass die einzigen Quadratreste modulo n die Quadratzahlen $k < n$ sind.

Aufgabe 6.11. Bestätige Satz 6.6 für $\mathbb{Z}/(25)$.

Aufgaben zum Abgeben

Aufgabe 6.12. (3 Punkte)

Es sei n eine natürliche Zahl derart, dass $(\mathbb{Z}/(n))^\times$ zyklisch ist. Zeige, dass die Anzahl der primitiven Elemente gleich $\varphi(\varphi(n))$ ist, wobei φ die Eulersche Funktion bezeichnet. Wie groß ist deren Anzahl, wenn $(\mathbb{Z}/(n))^\times$ nicht zyklisch ist?

Aufgabe 6.13. (3 Punkte)

Es sei p eine Primzahl und $e \in \mathbb{N}$. Zeige, dass das Potenzieren
$$(\mathbb{Z}/(p))^\times \longrightarrow (\mathbb{Z}/(p))^\times, \, x \longmapsto x^e,$$
genau dann eine Bijektion ist, wenn e und $p-1$ teilerfremd sind.

Aufgabe 6.14. (2 Punkte)

Bestätige Satz 6.6 für $\mathbb{Z}/(27)$.

Aufgabe 6.15. (3 Punkte)

Es sei p eine Primzahl und $\mathbb{F}_p = \mathbb{Z}/(p)$ der zugehörige Restklassenkörper. Konstruiere Ringe
$$\mathbb{F}_p[\mathrm{i}] = \mathbb{F}_p \oplus \mathbb{F}_p \mathrm{i} = \{a + b\mathrm{i} \mid a, b \in \mathbb{F}_p\}$$
in der gleichen Weise, wie man die komplexen Zahlen definiert. Charakterisiere, für welche p diese Konstruktion einen Körper liefert.

Abbildungsverzeichnis