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

Zahlentheorie

Arbeitsblatt 7

Übungsaufgaben

AUFGABE 7.1. Es sei n eine ungerade Zahl. Zeige, dass es in $\mathbb{Z}/(n)$ maximal $\frac{n+1}{2}$ Quadratreste gibt. Wie sieht dies bei n gerade aus?

AUFGABE 7.2.*

Betrachte die Quadratrestgruppe

$$\mathbb{Q}^\times/\mathbb{Q}^{\times 2}\,,$$

wobei $\mathbb{Q}^{\times 2}$ die Untergruppe der Quadrate bezeichne. Zeige, dass es zu jeder Restklasse $x \in \mathbb{Q}^\times/\mathbb{Q}^{\times 2}$ einen Repräsentanten aus $\mathbb{Z}$ gibt.

AUFGABE 7.3. Es sei K ein endlicher Körper mit $2 \neq 0$. Zeige, dass die Anzahl von K ungerade ist, und dass es in K genau $\frac{\#(K)+1}{2}$ Quadrate gibt.

AUFGABE 7.4.*

Berechne zu $p = 13$ und $k = 3$ die Vielfachen $ik \mod 13$ für $i = 1, \ldots, 6$ und repräsentiere sie durch Zahlen zwischen -6 und 6. Berechne damit die Vorzeichen $\epsilon_i = \epsilon_i(3)$ und bestätige das Gaußsche Vorzeichenlemma an diesem Beispiel.

AUFGABE 7.5. Berechne zu $p = 17$ und $k = 5$ die Vielfachen $ik \mod 17$ für $i = 1, \ldots, 8$ und repräsentiere sie durch Zahlen zwischen -8 und 8. Berechne damit die Vorzeichen $\epsilon_i = \epsilon_i(5)$ und bestätige das Gaußsche Vorzeichenlemma an diesem Beispiel.

AUFGABE 7.6. Wie viele Lösungen hat die Gleichung

$$x^5 = a$$

in $\mathbb{Z}/(19)$ für ein gegebenes $a \in \mathbb{Z}/(19)$?

Aufgabe 7.7. Beweise mit Hilfe des Gaußschen Vorzeichenlemmas eine Modulobedingung für die ungeraden Primzahlen p mit der Eigenschaft, dass 3 ein Quadrat modulo p ist.

Aufgabe 7.8. Charakterisiere, für welche Primzahlen p die Zahl -2 ein Quadratrest modulo p ist.

Aufgabe 7.9. Finde die Lösungen der Kongruenz

$$6x^2 + 4x + 1 = 0 \mod 35.$$

Aufgaben zum Abgeben

Aufgabe 7.10. (7 (1+1+1+4) Punkte)

Für einen Körper K bezeichnet $K^{\times 2} \subseteq K^\times$ die Untergruppe aller Quadrate. Bestimme für die folgenden Körper die Restklassengruppe

$$K^\times / K^{\times 2}.$$

(1) K ist ein endlicher Körper.
(2) $K = \mathbb{R}$.
(3) $K = \mathbb{C}$.
(4) $K = \mathbb{Q}$.

Die folgende Aufgabe verallgemeinert das Eulersche Kriterium für beliebige Potenzreste.

Aufgabe 7.11. (4 Punkte)

Es sei p eine Primzahl und sei e eine natürliche Zahl. Zeige, dass ein Element $k \in (\mathbb{Z}/(p))^\times$ genau dann eine e-te Wurzel besitzt, wenn $k^{\frac{p-1}{e}} = 1$ ist.

Aufgabe 7.12. (3 Punkte)

Berechne zu $p = 23$ und $k = 8$ die Vielfachen $ik \mod 23$ für $i = 1, \ldots, 11$ und repräsentiere sie durch Zahlen zwischen -11 und 11. Berechne damit die Vorzeichen $\epsilon_i = \epsilon_i(8)$ und bestätige das Gaußsche Vorzeichenlemma an diesem Beispiel.

Aufgabe 7.13. (3 Punkte)

Beweise mit Hilfe des Gaußschen Vorzeichenlemmas eine Modulobedingung für die ungeraden Primzahlen p mit der Eigenschaft, dass 5 ein Quadrat modulo p ist.

Aufgabe 7.14. (4 Punkte)

Finde die Lösungen der Kongruenz

$$5x^2 + 5x + 4 \;=\; 0 \mod 91.$$

Aufgabe 7.15. (4 Punkte)

Zeige, dass im Restklassenring $\mathbb{Z}/(n)$ die Äquivalenz gilt, dass zwei Elemente a, b genau dann assoziiert sind, wenn $(a) = (b)$ ist. Finde eine Charakterisierung für diese Äquivalenzrelation, die auf den Primfaktorzerlegungen von n, a und b aufbaut.

Die folgende Aufgabe setzt eine gewisse Routine im Umgang mit kommutativen Ringen voraus.

Aufgabe 7.16. (4 Punkte)

Man gebe ein Beispiel von zwei Elementen a und b eines kommutativen Ringes derart, dass $(a) = (b)$ ist, dass aber a und b nicht assoziiert sind.

Abbildungsverzeichnis