Prof. Dr. H. Brenner **Osnabrück WS 2016/2017**

Zahlentheorie

Arbeitsblatt 7

Übungsaufgaben

AUFGABE 7.1. 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 7.2. 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 7.3.*

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?

Sei x ein primitives Element von $\mathbb{Z}/(31)$. Liste explizit alle Elemente x^i auf, die weder primitiv noch ein Quadrat sind.

AUFGABE 7.4. Welche Ziffern treten im Dezimalsystem als Endziffern von Quadratzahlen auf?

AUFGABE 7.5. Bestimme die Quadrate in $\mathbb{Z}/(35)$.

AUFGABE 7.6.

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

AUFGABE 7.8. 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 7.9. 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 7.10. 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 7.11. 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 7.12. Wie viele Lösungen hat die Gleichung

$$x^5 = a$$

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

AUFGABE 7.13. Charakterisiere diejenigen positiven ungeraden Zahlen n mit der Eigenschaft, dass bei dem in Aufgabe 1.25 beschriebenen Algorithmus genau zwei ungerade Zahlen auftreten (nämlich n und 1).

Die Begriffe teilen, irreduzibel und prim machen in jedem Monoid Sinn (nicht nur im multiplikativen Monoid eines Ringes). In den folgenden Aufgaben werden Teilbarkeitseigenschaften in einigen kommutativen Monoiden besprochen.

Aufgabe 7.14. Betrachte die natürlichen Zahlen $\mathbb{N}$ als kommutatives Monoid mit der Addition und neutralem Element 0. Bestimme die irreduziblen Elemente und die Primelemente von diesem Monoid. Gilt die eindeutige Primfaktorzerlegung?

Aufgabe 7.15. Betrachte die Menge M derjenigen positiven Zahlen, die modulo 4 den Rest 1 haben. Zeige, dass M mit der Multiplikation ein kommutatives Monoid ist. Bestimme die irreduziblen Elemente und die Primelemente von M. Zeige, dass in M jedes Element Produkt von irreduziblen Elementen ist, aber keine eindeutige Primfaktorzerlegung in M gilt.

Aufgaben zum Abgeben

Die folgende Aufgabe verallgemeinert das Eulersche Kriterium für beliebige Potenzreste.

Aufgabe 7.16. (4 Punkte)

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 7.17. (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 7.18. (4 Punkte)

Finde die Lösungen der Kongruenz

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

Aufgabe 7.19. (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 7.20. (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.

Aufgabe 7.21. (3 Punkte)

Betrachte die Menge G der positiven geraden Zahlen zusammen mit 1. Zeige, dass G ein kommutatives Monoid ist. Bestimme die irreduziblen Elemente und die Primelemente von G. Zeige, dass in G jedes Element Produkt von irreduziblen Elementen ist, aber keine eindeutige Primfaktorzerlegung in G gilt.