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

Zahlentheorie

Arbeitsblatt 5

Übungsaufgaben

Aufgabe 5.1. Berechne die Restklasse von 2^{1563} modulo 23.

Aufgabe 5.2.*

Berechne 3^{1457} in $\mathbb{Z}/(13)$.

Aufgabe 5.3.*

Man berechne in $\mathbb{Z}/(80)$ die Elemente

(1) $3^{1234567}$,
(2) $2^{1234567}$,
(3) $5^{1234567}$.

Aufgabe 5.4. Beweise ausschließlich durch Anzahlbetrachtungen Lemma 5.9, dass also der kanonische Homomorphismus $(\mathbb{Z}/(p^r))^\times \to (\mathbb{Z}/(p))^\times$ surjektiv ist (p Primzahl).

Aufgabe 5.5. Bestimme die multiplikative Ordnung aller Einheiten im Restklassenkörper $\mathbb{Z}/(11)$.

Aufgabe 5.6. Bestimme sämtliche primitive Einheiten im Restklassenkörper $\mathbb{Z}/(23)$.

Aufgabe 5.7.*

Bestimme sämtliche primitive Einheiten im Restklassenkörper $\mathbb{Z}/(13)$.

Aufgabe 5.8. Sei p eine ungerade Primzahl und $\mathbb{Z}/(p)$ der zugehörige Restklassenkörper. Zeige, dass das Produkt von zwei primitiven Einheiten niemals primitiv ist.

Aufgabe 5.9.*

Bestimme in der Einheitengruppe $\mathbb{Z}/(17)^\times$ zu jeder möglichen Ordnung k ein Element $x \in \mathbb{Z}/(17)^\times$, das die Ordnung k besitzt. Man gebe auch eine Untergruppe

$$H \subseteq \mathbb{Z}/(17)^\times$$

an, die aus vier Elementen besteht.

Aufgabe 5.10.*

In dieser Aufgabe geht es um den Restklassenring $\mathbb{Z}/(360)$.

a) Schreibe $\mathbb{Z}/(360)$ als Produktring (im Sinne des chinesischen Restsatzes).

b) Wie viele Einheiten besitzt $\mathbb{Z}/(360)$?

c) Schreibe das Element 239 in komponentenweiser Darstellung. Begründe, warum es sich um eine Einheit handelt und finde das Inverse in komponentenweiser Darstellung.

d) Berechne die Ordnung von 239 in $\mathbb{Z}/(360)$.

Aufgabe 5.11. Zeige, dass die eulersche Funktion φ für natürliche Zahlen n, m die Eigenschaft

$$\varphi(\mathrm{ggT}(m,n)) \cdot \varphi(\mathrm{kgV}(m,n)) \;=\; \varphi(n) \cdot \varphi(m)$$

erfüllt.

Aufgabe 5.12. Finde primitive Einheiten in den Restklassenkörpern $\mathbb{Z}/(13)$, $\mathbb{Z}/(17)$ und $\mathbb{Z}/(19)$.

Aufgabe 5.13. Sei $n \in \mathbb{N}_+$. Zeige, dass die Gruppe der n-ten Einheitswurzeln in $\mathbb{C}$ und die Gruppe $\mathbb{Z}/(n)$ isomorph sind.

In den nächsten Aufgaben werden die folgenden Begriffe verwendet.

Ein Element a eines kommutativen Ringes R heißt *nilpotent*, wenn $a^n = 0$ ist für eine natürliche Zahl n.

Ein Element e eines kommutativen Ringes heißt *idempotent*, wenn $e^2 = e$ gilt.

Aufgabe 5.14. Bestimme die nilpotenten Elemente, die idempotenten Elemente und die Einheiten von $\mathbb{Z}/(60)$.

Aufgabe 5.15.*

a) Finde die Zahlen $z \in \{0, 1, \ldots, 9\}$ mit der Eigenschaft, dass die letzte Ziffer ihres Quadrates (in der Dezimaldarstellung) gleich z ist.

b) Finde die Zahlen $z \in \{0, 1, \ldots, 99\}$ mit der Eigenschaft, dass die beiden letzten Ziffern ihres Quadrates (in der Dezimaldarstellung) gleich z ist.

Aufgabe 5.16. Es sei R ein kommutativer Ring und es seien $f, g \in R$ nilpotente Elemente. Zeige, dass dann die Summe $f + g$ ebenfalls nilpotent ist.

Aufgabe 5.17. Sei R ein kommutativer Ring und sei $f \in R$. Es sei f sowohl nilpotent als auch idempotent. Zeige, dass $f = 0$ ist.

Aufgabe 5.18. Es sei R ein kommutativer Ring und $f \in R$ ein nilpotentes Element. Zeige, dass $1 + f$ eine Einheit ist.

Aufgabe 5.19. Sei $\omega = \frac{-1+\sqrt{-3}}{2} = \frac{-1+\sqrt{3}i}{2}$. Betrachte die beiden Unterringe

$$R = \mathbb{Z}[\sqrt{-3}] \subset \mathbb{Z}[\omega] = S$$

der komplexen Zahlen (S ist also der Ring der Eisensteinzahlen). Finde ein Beispiel von zwei Elementen in R, die in R nicht assoziiert sind, wohl aber in S. Gebe daran anschließend ein Beispiel eines irreduziblen Elementes in R, dass nicht prim ist (in R). Ist es prim in S?

Aufgaben zum Abgeben

Aufgabe 5.20. (4 Punkte)

Sei p eine ungerade Primzahl. Beweise unter Verwendung des Satzes von Wilson, dass

$$1^2 \cdot 3^2 \cdot 5^2 \cdots (p-4)^2 \cdot (p-2)^2 = (-1)^{\frac{p+1}{2}} \mod p$$

gilt.

Aufgabe 5.21. (3 Punkte)

Beweise die *eulersche Formel* für die eulersche Funktion, das ist die Aussage, dass

$$\varphi(n) = n \cdot \prod_{p|n,\ p \text{ prim}} \left(1 - \frac{1}{p}\right)$$

gilt.

Aufgabe 5.22. (5 Punkte)

Bestimme die nilpotenten Elemente, die idempotenten Elemente und die Einheiten in $\mathbb{Z}/(72)$.

Aufgabe 5.23. (4 Punkte)

Zeige, dass für natürliche Zahlen k und n mit $k \mid n$ der kanonische Homomorphismus

$$(\mathbb{Z}/(n))^\times \longrightarrow (\mathbb{Z}/(k))^\times$$

surjektiv ist.

Aufgabe 5.24. (4 Punkte)

Sei n eine natürliche Zahl. Charakterisiere diejenigen Teiler k von n mit der Eigenschaft, dass für den kanonischen Ringhomomorphismus

$$\varphi\colon\ \mathbb{Z}/(n) \longrightarrow \mathbb{Z}/(k)$$

gilt, dass a in $\mathbb{Z}/(n)$ genau dann eine Einheit ist, wenn $\varphi(a)$ in $\mathbb{Z}/(k)$ eine Einheit ist.

Aufgabe 5.25. (4 Punkte)

Sei p eine fixierte Primzahl. Zu jeder ganzen Zahl $n \neq 0$ bezeichne $\nu_p(n)$ den Exponenten, mit dem die Primzahl p in der Primfaktorzerlegung von n vorkommt.

a) Zeige: die Abbildung $\nu_p : \mathbb{Z} \setminus \{0\} \to \mathbb{N}$ ist surjektiv.

b) Zeige: es gilt $\nu_p(nm) = \nu_p(n) + \nu_p(m)$.

c) Finde eine Fortsetzung $\nu_p : \mathbb{Q} \setminus \{0\} \to \mathbb{Z}$ der gegebenen Abbildung, die ein Gruppenhomomorphismus ist (wobei $\mathbb{Q}^\times = \mathbb{Q} \setminus \{0\}$ mit der Multiplikation und $\mathbb{Z}$ mit der Addition versehen ist).

d) Beschreibe den Kern des unter c) beschriebenen Gruppenhomomorphismus.