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

Zahlentheorie

Arbeitsblatt 6

Übungsaufgaben

Aufgabe 6.1. Bestimme alle primitiven Elemente von $\mathbb{Z}/(27)$.

Aufgabe 6.2.
(1) Finde ein primitives Element in $\mathbb{Z}/(3)$, in $\mathbb{Z}/(9)$ und in $\mathbb{Z}/(27)$.
(2) Finde eine ganze Zahl, die in $\mathbb{Z}/(3)$ primitiv ist, aber nicht in $\mathbb{Z}/(9)$.
(3) Zeige, dass jede ganze Zahl, die in $\mathbb{Z}/(9)$ primitiv ist, auch in $\mathbb{Z}/(27)$ primitiv ist.

Aufgabe 6.3. Man gebe für die Einheitengruppe $(\mathbb{Z}/(16))^\times$ explizit einen Isomorphismus zu einem Produkt von (additiven) zyklischen Gruppen an.

Aufgabe 6.4. Sei p eine Primzahl und $r \geq 2$. Beschreibe explizit die Elemente im Kern der Abbildung

$$(\mathbb{Z}/(p^r))^\times \longrightarrow (\mathbb{Z}/(p^{r-1}))^\times .$$

In der folgenden Aufgabe bezeichnet $\mathbb{F}_{121}$ den Körper mit 121 Elementen. Darüber hinaus muss muss man nichts über ihn wissen.

Aufgabe 6.5.*

Finde ein primitives Element in $\mathbb{Z}/(11)$ und in $\mathbb{Z}/(121)$. Man gebe ferner ein Element der Ordnung 10 und ein Element der Ordnung 11 in $\mathbb{Z}/(121)$ an. Gibt es Elemente der Ordnung 10 und der Ordnung 11 auch in $\mathbb{F}_{121}$?

Aufgabe 6.6. Bestimme sämtliche quadratische Reste modulo der Primzahlen < 20.

Aufgabe 6.7. 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 6.8. Bestimme die Zerlegung von $X^{p-1}-1$ in irreduzible Polynome im Polynomring $\mathbb{Z}/(p)[X]$. Beweise aus dieser Zerlegung den Satz von Wilson.

Aufgabe 6.9. Sei p eine ungerade Primzahl und $a \in \mathbb{Z}/(p)$ primitiv. Zeige, dass von den p Elementen aus $\mathbb{Z}/(p^2)$, die auf a abgebildet werden, genau $p-1$ Stück primitiv in $\mathbb{Z}/(p^2)$ sind. Finde für $p = 7$ und $a = 3$ dasjenige Element $b \in \mathbb{Z}/(49)$ mit $b = a \mod 7$, das nicht primitiv ist.

Aufgabe 6.10. Finde Quadratwurzeln für 2 modulo p für alle Primzahlen p mit $p = \pm 1 \mod 8$ und $p \leq 32$.

Aufgabe 6.11. Zeige, dass eine Restklassengruppe einer zyklischen Gruppe wieder zyklisch ist.

Aufgabe 6.12. Es sei

$$G = H_1 \times \cdots \times H_n$$

die Produktgruppe der endlichen Gruppen $H_1, \ldots, H_n$. Zeige die folgenden Aussagen.

(1)
$$\exp G = \operatorname{kgV}(\exp H_i, i = 1, \ldots, n).$$
(2) G ist genau dann zyklisch, wenn alle H_i zyklisch sind und wenn deren Ordnungen paarweise teilerfremd sind.

Aufgabe 6.13. Was besagt die Artinsche Vermutung über primitive Reste?

Aufgabe 6.14. Es seien R und $S_1, \ldots, S_n$ kommutative Ringe mit dem Produktring

$$S = S_1 \times \cdots \times S_n .$$

Zeige, dass ein Ringhomomorphismus

$$\varphi \colon R \longrightarrow S$$

dasselbe ist wie eine Familie von Ringhomomorphismen

$$\varphi_i \colon R \longrightarrow S_i$$

für $i = 1, \ldots, n$.

Aufgabe 6.15. Seien a, b und r positive natürliche Zahlen. Zeige, dass die Teilbarkeit $a^r | b^r$ die Teilbarkeit $a|b$ impliziert.

Aufgaben zum Abgeben

Aufgabe 6.16. (3 Punkte)

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 6.17. (7 (3+2+2) Punkte)

a) Sei K ein Körper. Zeige, dass die Einheitengruppe von K nicht zyklisch unendlich ist.

b) Sei R ein kommutativer Ring, dessen Charakteristik nicht zwei ist. Zeige, dass die Einheitengruppe von R nicht zyklisch unendlich ist.

c) Beschreibe einen kommutativen Ring, dessen Einheitengruppe zyklisch unendlich ist.

Aufgabe 6.18. (3 Punkte)

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 6.19. (3 Punkte)

Sei p eine Primzahl und $\mathbb{F}_p = \mathbb{Z}/(p)$ der zugehörige Restklassenkörper. Konstruiere Ringe

$$\mathbb{F}_p[i] = \mathbb{F}_p \oplus \mathbb{F}_p i = \{a + bi : a, b \in \mathbb{F}_p\}$$

in der gleichen Weise, wie man die komplexen Zahlen definiert. Charakterisiere, für welche p diese Konstruktion einen Körper liefert.

Aufgabe 6.20. (4 Punkte)

Seien a und b positive natürliche Zahlen. Seien $r_n \, , n \in \mathbb{N}$, und $s_n \, , n \in \mathbb{N}$, Folgen von positiven natürlichen Zahlen derart, dass die Teilbarkeitsbeziehung

$$a^{r_n} | b^{s_n}$$

für alle n gilt. Es sei vorausgesetzt, dass die Quotientenfolge r_n/s_n gegen 1 konvergiert. Zeige, dass a ein Teiler von b ist.