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

# Zahlentheorie

## Arbeitsblatt 4

## Übungsaufgaben

Aufgabe 4.1. Bestimme alle Lösungen der linearen Kongruenz $12x = 3 \mod 21$.

Aufgabe 4.2. Bestimme alle Lösungen der linearen Kongruenz $13x = 11 \mod 141$.

Aufgabe 4.3. Berechne die Restklasse von $2^{1563}$ modulo 23.

Aufgabe 4.4.*

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

Aufgabe 4.5. Charakterisiere diejenigen positiven ungeraden Zahlen $n$ mit der Eigenschaft, dass bei dem in Aufgabe 1.26 beschriebenen Algorithmus genau zwei ungerade Zahlen auftreten (nämlich $n$ und 1, aber beliebig viele gerade Zahlen).

Aufgabe 4.6. Es sei $p$ eine Primzahl. Beweise durch Induktion den kleinen Fermat, also die Aussage, dass $a^p - a$ ein Vielfaches von $p$ für jede ganze Zahl $a$ ist.

Aufgabe 4.7. Bestimme den Rest von 27! modulo 31.

Aufgabe 4.8. 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 4.9.*

Es seien $a, b \geq 2$ und sei $n = ab$.

a) Zeige, dass die beiden Polynome $X^a - 1$ und $X^b - 1$ Teiler des Polynoms $X^n - 1$ sind.

b) Es sei $a \neq b$. Ist $(X^a - 1)(X^b - 1)$ stets ein Teiler von $X^n - 1$

c) Man gebe drei Primfaktoren von $2^{30} - 1$ an.

Aufgabe 4.10.*

a) Finde mit Hilfe des Euklidischen Algorithmus eine Darstellung der 1 für die beiden Zahlen 19 und 109.

b) Nach dem Chinesischen Restsatz haben wir die Isomorphie

$$\mathbb{Z}/(2071) \cong \mathbb{Z}/(19) \times \mathbb{Z}/(109).$$

Welche Restklasse modulo 2071 entspricht dem Restklassenpaar $(1, 0)$ und welche dem Paar $(0, 1)$?

c) Bestimme diejenige Restklasse modulo 2071, die modulo 19 den Rest 5 hat und die modulo 109 den Rest 10 hat.

Aufgabe 4.11.*

a) Bestimme für die Zahlen 3, 11 und 13 modulare Basislösungen, finde also die kleinsten positiven Zahlen, die in

$$\mathbb{Z}/(3) \times \mathbb{Z}/(11) \times \mathbb{Z}/(13)$$

die Restetupel $(1, 0, 0)$, $(0, 1, 0)$ und $(0, 0, 1)$ repräsentieren.

b) Finde mit den Basislösungen die kleinste positive Lösung $x$ der simultanen Kongruenzen

$$x = 2 \mod 3, \quad x = 5 \mod 11 \text{ und } x = 6 \mod 13\,.$$

Aufgabe 4.12.*

a) Bestimme für die Zahlen 2, 9 und 25 modulare Basislösungen, finde also die kleinsten positiven Zahlen, die in

$$\mathbb{Z}/(2) \times \mathbb{Z}/(9) \times \mathbb{Z}/(25)$$

die Restetupel $(1, 0, 0)$, $(0, 1, 0)$ und $(0, 0, 1)$ repräsentieren.

b) Finde mit den Basislösungen die kleinste positive Lösung $x$ der simultanen Kongruenzen

$$x = 0 \mod 2, \quad x = 3 \mod 9 \text{ und } x = 5 \mod 25\,.$$

Aufgabe 4.13. a) Bestimme für die Zahlen 4, 5 und 11 modulare Basislösungen, finde also die kleinsten positiven Zahlen, die in

$$\mathbb{Z}/(4) \times \mathbb{Z}/(5) \times \mathbb{Z}/(11)$$

die Restetupel $(1,0,0)$, $(0,1,0)$ und $(0,0,1)$ repräsentieren.

b) Finde mit den Basislösungen die kleinste positive Lösung $x$ der simultanen Kongruenzen

$$x = 3 \mod 4, \quad x = 2 \mod 5 \text{ und } x = 10 \mod 11\,.$$

Aufgabe 4.14.*

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

a) $3^{1234567}$,

b) $2^{1234567}$,

c) $5^{1234567}$.

Aufgabe 4.15. 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 4.16.*

Man gebe eine surjektive Abbildung

$$\varphi\colon\ \mathbb{Z} \longrightarrow \mathbb{Z}/(3)$$

an, die mit der Multiplikation verträglich (also ein Monoidhomomorphismus) ist, aber kein Ringhomomorphismus ist.

Aufgabe 4.17.*

Es sei $n$ eine positive natürliche Zahl mit der Faktorzerlegung

$$n = 2^r \cdot 5^s \cdot d,$$

wobei $d$ zu $n$ teilerfremd sei ($r, s = 0$ und $d = 1$ sind erlaubt). Zeige, dass die Periodenlänge der Dezimalentwicklung von $\frac{1}{n}$ gleich der multiplikativen Ordnung von 10 in $\mathbb{Z}/(d)$ ist.

Aufgabe 4.18. Es sei $R$ ein kommutativer Ring, der einen Körper der positiven Charakteristik $p > 0$ enthalte (dabei ist $p$ eine Primzahl). Zeige, dass die Abbildung

$$R \longrightarrow R,\ f \longmapsto f^p,$$

ein Ringhomomorphismus ist, den man den *Frobeniushomomorphismus* nennt.

Tipp: Benutze Aufgabe 3.22.

Aufgabe 4.19.*

Es sei $p$ eine Primzahl und sei $f(x)$ ein Polynom mit Koeffizienten in $\mathbb{Z}/(p)$ vom Grad $d \geq p$. Zeige, dass es ein Polynom $g(x)$ mit einem Grad $< p$ derart gibt, dass für alle Elemente $a \in \mathbb{Z}/(p)$ die Gleichheit

$$f(a) = g(a)$$

gilt.

Aufgabe 4.20. Zeige, dass eine Untergruppe einer zyklischen Gruppe wieder zyklisch ist.

Aufgabe 4.21. Zeige, dass eine Restklassengruppe einer zyklischen Gruppe wieder zyklisch ist.

Aufgabe 4.22. 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)
$$\exp G = \mathrm{kgV}(\exp H_i, i = 1, \ldots, n).$$

(2) $G$ ist genau dann zyklisch, wenn alle $H_i$ zyklisch sind und wenn deren Ordnungen paarweise teilerfremd sind.

Aufgabe 4.23. Es seien $n_1, \ldots, n_k$ positive natürliche Zahlen und es sei

$$G = \mathbb{Z}/(n_1) \times \mathbb{Z}/(n_2) \times \cdots \times \mathbb{Z}/(n_k)$$

die Produktgruppe. Bestimme den Exponenten von $G$.

Aufgabe 4.24.*

Wir betrachten die endliche Permutationsgruppe $S_n$ zu einer Menge mit $n$ Elementen.

a) Zeige, dass es in $S_n$ Elemente der Ordnung $n$ gibt.

b) Man gebe ein Beispiel für eine Permutationsgruppe $S_n$ und einem Element darin, dessen Ordnung größer als $n$ ist.

Aufgabe 4.25.*

Zeige, dass es in der Restklassengruppe $\mathbb{Q}/\mathbb{Z}$ zu jedem $n \in \mathbb{N}_+$ Elemente gibt, deren Ordnung gleich $n$ ist.

Aufgabe 4.26. Für eine Gruppe $G$ bezeichne $T(G)$ die Menge aller Elemente mit endlicher Ordnung in $G$. Zeige folgende Aussagen.

(1) Ist $G$ abelsch, so ist $T(G)$ eine Untergruppe von $G$.
(2) Ist $T(G)$ eine Untergruppe, so ist $T(G)$ ein Normalteiler in $G$.
(3) Es gibt eine Gruppe $G$, für die $T(G)$ keine Untergruppe von $G$ ist.

## Aufgaben zum Abgeben

Aufgabe 4.27. (3 Punkte)

Formuliere und beweise (bekannte) Teilbarkeitskriterien für Zahlen im Dezimalsystem für die Teiler $k = 2, 3, 5, 9, 11$.

Aufgabe 4.28. (4 Punkte)

Es 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 4.29. (3 Punkte)

Es sei $f(x) = x^7 + 2x^3 + 3x + 4 \in (\mathbb{Z}/(5))[x]$. Finde ein Polynom $g(x) \in (\mathbb{Z}/(5))[x]$ vom Grad $< 5$, das für alle Elemente aus $\mathbb{Z}/(5)$ mit $f(x)$ übereinstimmt.

AUFGABE 4.30. (3 Punkte)

a) Bestimme für die Zahlen 2, 3 und 7 modulare Basislösungen, finde also die kleinsten positiven Zahlen, die in

$$\mathbb{Z}/(2) \times \mathbb{Z}/(3) \times \mathbb{Z}/(7)$$

die Restetupel $(1, 0, 0)$, $(0, 1, 0)$ und $(0, 0, 1)$ repräsentieren.

b) Finde mit den Basislösungen die kleinste positive Lösung $x$ der simultanen Kongruenzen

$$x = 1 \mod 2, \quad x = 2 \mod 3 \text{ und } x = 2 \mod 7\,.$$

# Abbildungsverzeichnis