

### Aufgabe 1

- (a) Sei  $n \in \mathbb{N}$ . Charakterisieren Sie die Einheiten im Ring  $\mathbb{Z}/n\mathbb{Z}$  auf zwei verschiedene Arten.
- (b) Bestimmen Sie das inverse Element zur Restklasse von 119 in der Einheitengruppe von  $\mathbb{Z}/384\mathbb{Z}$ .

### Lösung:

- (a) Die Einheiten in einem Ring sind die bezüglich der Multiplikation invertierbaren Elemente. Im Restklassenring  $\mathbb{Z}/n\mathbb{Z}$  gilt für die Einheitengruppe gerade

$$(\mathbb{Z}/n\mathbb{Z})^\times = \{a + n\mathbb{Z} \in \mathbb{Z}/n\mathbb{Z} \mid \text{ggT}(a, n) = 1\}.$$

- (b) Da 119 teilerfremd zu 384 ist, kann mithilfe des euklidischen Algorithmus die 1 als  $\mathbb{Z}$ -Linearkombination dargestellt werden.

$$384 = 3 \cdot 119 + 27$$

$$119 = 4 \cdot 27 + 11$$

$$27 = 2 \cdot 11 + 5$$

$$11 = 2 \cdot 5 + 1$$

Durch Zurückrechnen folgt  $1 = 71 \cdot 119 - 22 \cdot 384$ , und daher gilt  $71 \cdot 119 \equiv 1 \pmod{384}$ . Die Restklasse von 71 ist demnach das inverse Element zur Restklasse von 119.

## Aufgabe 2

- (a) Sei  $N \in \mathbb{N}$  kein Vielfaches von 7. Wieso gibt es eine Zahl  $d$ , die kongruent 1 modulo  $N$  und kongruent 2 modulo 7 ist?
- (b) Zeigen Sie, dass es unendlich viele Primzahlen gibt, die nicht kongruent  $\pm 1$  modulo 7 sind.

**Hinweis:** Den Primzahlsatz von Dirichlet dürfen Sie hier nicht verwenden.

### Lösung:

- (a) Da  $N$  und 7 teilerfremd sind, gilt nach dem chinesischen Restsatz  $\mathbb{Z}/N\mathbb{Z} \times \mathbb{Z}/7\mathbb{Z} \cong \mathbb{Z}/(N \cdot 7)\mathbb{Z}$ . Das Element  $(1+N\mathbb{Z}, 2+7\mathbb{Z})$  wird unter dem Isomorphismus aus der Vorlesung dann auf ein Element  $x + N \cdot 7\mathbb{Z}$  abgebildet, welches diese beiden Kongruenzen erfüllt.
- (b) Es seien  $p_1, \dots, p_k \in \mathbb{P}$  Primzahlen ungleich 7, die nicht kongruent  $\pm 1$  modulo 7 sind. Setze

$$N := \prod_{i=1}^k p_i.$$

Dann ist  $N$  kein Vielfaches von 7.

Nach dem a)-Teil gibt es ein  $x \in \mathbb{N}$ , das kongruent 1 modulo  $N$  und kongruent 2 modulo 7 ist. Da  $x \equiv 1 \pmod{N}$  ist, sind  $x$  und  $N$  teilerfremd.

Da  $x$  nicht kongruent  $\pm 1, 0$  modulo 7 ist, muss es mindestens einen Primteiler geben, der nicht kongruent  $\pm 1, 0$  modulo 7 ist.

Dieser ist wegen der Teilerfremdheit keine der vorgegebenen Primzahlen  $p_1, \dots, p_k$ , und folglich gibt es auch eine  $(k+1)$ te Primzahl ungleich 7, die modulo 7 nicht  $\pm 1$  ist.

### Aufgabe 3

Sei  $U$  die von  $\left\{\begin{pmatrix} 5 \\ 7 \\ 9 \end{pmatrix}, \begin{pmatrix} 8 \\ 3 \\ 6 \end{pmatrix}, \begin{pmatrix} 1 \\ 2 \\ 5 \end{pmatrix}\right\}$  erzeugte Untergruppe in  $\mathbb{Z}^3$ .

- Bestimmen Sie die Elementarteiler  $e_1, e_2, e_3$  von  $U$  in  $\mathbb{Z}^3$ .
- Bestimmen Sie eine Basis  $\{b_1, b_2, b_3\}$  von  $\mathbb{Z}^3$ , so dass  $\{e_1 b_1, e_2 b_2, e_3 b_3\}$  eine Basis von  $U$  ist.
- Welchen Index hat  $U$  in  $\mathbb{Z}^3$ ?

### Lösung:

Der Vektor  $c_1 := \begin{pmatrix} 1 \\ 2 \\ 5 \end{pmatrix}$  hat Inhalt 1 und ist daher ideal als erster Basisvektor geeignet.

Komplementär zu der von ihm aufgespannten Untergruppe von  $U$  ist die Gruppe aller Elemente, deren erste Komponente 0 ist ( $w = (1 \ 0 \ 0)^\top$  in der Vorlesung). Sie wird erzeugt von

$$\begin{pmatrix} 0 \\ 3 \\ 16 \end{pmatrix} \quad \text{und} \quad \begin{pmatrix} 0 \\ 13 \\ 34 \end{pmatrix}.$$

Beide Vektoren haben Inhalt 1, aber leichter zu rechnen ist es, wenn wir den zweiten abändern, indem wir 4 mal den ersten abziehen.

Das gibt  $c_2 := \begin{pmatrix} 0 \\ 1 \\ -30 \end{pmatrix}$  als zweiten Basisvektor.

Schließlich ist

$$c_3 := \begin{pmatrix} 0 \\ 3 \\ 16 \end{pmatrix} - 3c_2 = \begin{pmatrix} 0 \\ 0 \\ 106 \end{pmatrix}$$

ein dritter Basisvektor für  $U$ .

Die Vektoren

$$b_1 := c_1, \quad b_2 := c_2, \quad b_3 := \frac{1}{106}c_3$$

bilden offensichtlich eine Basis von  $\mathbb{Z}^3$ , und es folgt

$$e_1 = 1, \quad e_2 = 1, \quad e_3 = 106.$$

(NB: Man rechnet nach, dass die Determinante der Matrix, die aus den gegebenen Erzeugern von  $U$  besteht,  $-106$  ist. Sie ist das Produkt der Elementarteiler von  $U$ , und da diese sich in aufsteigender Reihenfolge teilen, 106 jedoch quadratfrei ist, müssen die ersten beiden Elementarteiler tatsächlich 1 sein, und der letzte daher 106.)

Die Vektoren

$$ab_3, \quad 0 \leq a \leq 105, \quad a \in \mathbb{Z},$$

bilden offensichtlich ein Repräsentantensystem von  $\mathbb{Z}^3/U$ , und der Index von  $U$  ist daher 106.

#### Aufgabe 4

Sei  $R = \mathbb{Z}[\sqrt{-10}]$  der Ganzheitsring in  $\mathbb{Q}(\sqrt{-10})$ .

- (a) In wieviel Primidealen in  $R$  liegen jeweils die Zahlen 3, 5, 7? Geben Sie jeweils eine  $\mathbb{Z}$ -Basis an.
- (b) Welches der Primideale aus a) ist ein Hauptideal? Bestimmen Sie ein primitives Element des Restklassenkörpers von  $R$  nach diesem Ideal.

#### Lösung:

- (a) Das Minimalpolynom von  $\omega_{-10} = \sqrt{-10}$  über  $\mathbb{Z}$  ist  $M := X^2 + 10$ .

Dies hat keine Nullstelle in  $\mathbb{F}_3$ , die doppelte Nullstelle 0 in  $\mathbb{F}_5$ , und zwei verschiedene Nullstellen in  $\mathbb{F}_7$ , nämlich  $\pm 2$ .

Entsprechend gibt es genau ein Primideal, das 3 enthält, es hat Index 9 und ist das Hauptideal  $3R$  mit der Basis  $\{3, 3\sqrt{-10}\}$ .

Es gibt genau ein Primideal, das 5 enthält, es hat Index 5 und als  $\mathbb{Z}$ -Basis zum Beispiel  $\{5, \sqrt{-10}\}$ .

Es gibt zwei Primideale, die 7 enthalten. Sie haben beide Index 7 in  $R$  und als  $\mathbb{Z}$ -Basis zum Beispiel  $\{7, \sqrt{-10} - 2\}$  bzw.  $\{7, \sqrt{-10} + 2\}$ .

- (b) Das Primideal  $3R$  ist ein Hauptideal, die drei anderen nicht, denn die Normen 5 bzw. 7 dieser Primideale sind keine Normen von Elementen aus  $R$ .

Denn: Die Norm von  $a + b\sqrt{-10}$  ist  $a^2 + 10b^2$ , und diese ist  $> 7$  für  $\mathbb{Z} \ni b \neq 0$  und weder 5 noch 7, wenn  $b = 0$ .

Also ist genau das Ideal  $3R$  ein Hauptideal, es hat als Restklassenkörper den Körper mit 9 Elementen. Ein primitives Element davon ist eine Einheit der Ordnung 8, also jedes Element, das keine Nullstelle von  $T^4 - 1$  ist. Da  $\pm 1$  und  $\pm\sqrt{-10}$  die 4 Nullstellen dieses Polynoms in  $R/3R$  repräsentieren, hat zum Beispiel die Restklasse von  $\sqrt{-10} + 1$  Ordnung 8 und ist damit ein primitives Element.

## Aufgabe 5

Zeigen Sie, dass

$$a = 3^6 + 3^5 + 3^4 + 3^3 + 3^2 + 3 + 1$$

höchstens zwei verschiedene Primteiler hat.

Ist  $a$  eine Primzahl?

### Lösung:

Es ist  $a = \frac{3^7-1}{3-1} = 1093 = \Phi_7(3)$ .

Weiter ist  $a = 700 + 350 + 42 + 1 \equiv 1 \pmod{7}$ .

Wenn  $p$  ein Primteiler von  $a$  ist, dann ist er also von 7 verschieden. In  $\mathbb{F}_p$  ist die Restklasse von 3 ein Element der Ordnung 7, und der Satz von Lagrange impliziert, dass  $p$  modulo 7 zu 1 kongruent ist.

Wenn  $p$  nicht größer als  $\sqrt{a}$  ist, dann ist

$$p < \sqrt{1093} < \sqrt{1600} = 40.$$

Es gibt genau eine Primzahl kleiner als 40, die bei Division durch 7 Rest 1 lässt, nämlich 29.

Da es auch höchstens einen Primteiler von  $a$  geben kann, der größer ist als  $\sqrt{a}$ , gibt es insgesamt höchstens 2 verschiedene Primteiler.

Modulo 29 ist

$$a \equiv 1 + 3 + 9 - 2 - 6 - 18 + 4 = -9,$$

also ist 29 kein Primteiler von  $a$ . Es gibt also keinen Primteiler von  $a$ , der kleiner als  $\sqrt{a}$  ist. Das zeigt, dass  $a$  tatsächlich prim ist.

## Aufgabe 6

Sei  $p \equiv 1 \pmod{6}$  eine Primzahl. Zeigen Sie:

- (a) Es existiert ein  $u \in \mathbb{Z}$  mit  $u^2 \equiv -3 \pmod{p}$ .  
(b) Sei  $v \equiv u^{-1} \pmod{p}$  und  $\Gamma$  das von  $\begin{pmatrix} 1 \\ v \end{pmatrix}, \begin{pmatrix} 0 \\ p \end{pmatrix}$  aufgespannte Gitter. Dann existiert ein  $\begin{pmatrix} 0 \\ p \end{pmatrix} \neq \begin{pmatrix} x \\ y \end{pmatrix} \in \Gamma$  mit  $0 < x^2 + 3y^2 < 3p$ .

**Hinweis:** Das Volumen der Ellipse  $\{ \begin{pmatrix} x \\ y \end{pmatrix} \in \mathbb{R}^2 \mid ax^2 + by^2 \leq r^2 \}$  ist  $\pi \cdot \frac{r^2}{\sqrt{a \cdot b}}$ .

- (c) Für den Gitterpunkt aus b) gilt  $x^2 + 3y^2 = p$ .

## Lösung:

- (a) Wir benutzen das Legendre-Symbol. Es gilt aufgrund des quadratischen Reziprozitätsgesetzes und seiner Ergänzungen

$$\left(\frac{-3}{p}\right) = \left(\frac{-1}{p}\right) \cdot \left(\frac{3}{p}\right) = (-1)^{\frac{p-1}{2}} \cdot (-1)^{\frac{p-1}{2} \cdot \frac{3-1}{2}} \left(\frac{p}{3}\right) = ((-1)^{\frac{p-1}{2}})^2 \cdot 1 = 1.$$

Dabei ist natürlich  $\left(\frac{p}{3}\right) = \left(\frac{1}{3}\right) = 1$  aufgrund der Kongruenzbedingung an  $p$ .

Damit gibt es tatsächlich ein  $u$ , sodass  $u^2 + 3$  durch  $p$  teilbar ist.

- (b) Das Kovolumen des Gitters ist gleich der Determinante der Matrix  $\begin{pmatrix} 1 & 0 \\ v & p \end{pmatrix}$ , also  $p$ .

Es sei

$$K = \left\{ \begin{pmatrix} x \\ y \end{pmatrix} \mid x^2 + 3y^2 \leq 3p - \varepsilon \right\}$$

für ein sehr kleines, positives  $\varepsilon$ .

$K$  ist zentralsymmetrisch, konvex und hat nach der geschenkten Volumenformel den Flächeninhalt

$$\frac{\pi(3p - \varepsilon)}{\sqrt{3}} = p \cdot \pi\sqrt{3} - \frac{\varepsilon\pi}{\sqrt{3}} > 4p$$

für hinreichend kleines  $\varepsilon$ . (NB:  $\pi \cdot \sqrt{3} > 3, 1 \cdot 1, 7 = 5, 27$ .)

Es folgt die Behauptung mit dem Minkowskischen Gitterpunktsatz.

- (c) Für den Gitterpunkt  $\begin{pmatrix} x \\ y \end{pmatrix} \in \Gamma \subseteq \mathbb{Z}^2$  aus Teil b) ist  $0 < x^2 + 3y^2 < 3p$ , und aufgrund der Konstruktion von  $\Gamma$  gibt es  $z \in \mathbb{Z}$  mit

$$\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} x \\ xv + pz \end{pmatrix}.$$

Daher ist

$$x^2 + 3y^2 = x^2 + 3(xv + zp)^2 = (1 + 3v^2)x^2 + 3(2xvz + z^2p) \cdot p.$$

Nach Konstruktion von  $v$  ist auch der erste Summand durch  $p$  teilbar, und damit die Zahl  $x^2 + 3y^2$ . Da sie kleiner ist als  $3p$  ist sie  $p$  oder  $2p$ . Wäre sie aber  $2p$ , so folgte wegen  $p \equiv 1 \pmod{3}$  dass 2 in  $\mathbb{F}_3$  ein Quadrat ist – das ist nicht der Fall!

Also bleibt nur die Möglichkeit  $x^2 + 3y^2 = p$ .