# ELEMENTARE ZAHLENTHEORIE
# 9. Übungsblatt

Julia Sauter, Andrew Hubery

## Aufgabe 1.

Sei $n \geq 3$. Wir haben in Übungsblatt 8 Aufgabe 3 gesehen, dass 3 die Ordnung $2^{n-2}$ modulo $2^n$ hat. Nun wollen wir zeigen, dass

$$f\colon (\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2^{n-2}\mathbb{Z}) \xrightarrow{\sim} (\mathbb{Z}/2^n\mathbb{Z})^\times, \quad (a,b) \mapsto (-1)^a 3^b \pmod{2^n},$$

ein Isomorphismus ist.

(a) Zeigen Sie, dass $-1$ nicht in die Untergruppe $\langle 3\rangle \subseteq (\mathbb{Z}/2^n\mathbb{Z})^\times$ liegt. Hinweis: betrachten Sie zuerst $n = 3$.

(b) Zeigen Sie, dass die obengegebene Abbildung $f$ ein injektiver Gruppenhomomorphismus ist.

(c) Schließen Sie daraus, dass $f$ ein Isomorphismus ist.

*(1+2+1 Punkte)*

## Aufgabe 2.

(a) Zeigen Sie, dass 3 eine Primitivwurzel modulo 101 ist.

Hinweis: Wie in Übungsblatt 7, Aufgabe 1 hat 3 die Ordnung 100 genau dann, wenn $3^{100/p} \not\equiv 1 \pmod{101}$ für alle Primteiler $p \mid 100$.

(b) Kontrollieren Sie, dass $7 \times \mathrm{dlog}_3(2) \equiv 3 \pmod{100}$.

(c) Finden Sie die Inverse von $19 \pmod{101}$. Benutzen Sie ihre Antwort, um $\mathrm{dlog}_3(19) \pmod{100}$ zu berechnen.

*(2+2+2 Punkte)*

## Aufgabe 3.

(a) Sei $f = x^4 + 2x^3 + 4x^2 + 3x + 2$ und $g = x^3 + x - 2$ in $\mathbb{Q}[x]$. Bestimmen Sie mit Hilfe des euklidischen Algorithmus den (normierten) größten gemeinsamen Teiler $\mathrm{ggT}(f,g)$ und Polynome $s, t$ mit $sf + tg = \mathrm{ggT}(f,g)$.

(b) Faktorisieren Sie die folgenden Polynome als Produkte $uf_1 \cdots f_r$ mit $u$ eine Einheit und $f_i$ normierte irreducible Polynome.

(i) $2x^3 + x^2 + 2$ in $\mathbb{F}_3[x]$.

(ii) $3x^3 - x^2 - 2x + 2$ in $\mathbb{F}_5[x]$.

(iii) $x^5 + x^2 + x + 1$ in $\mathbb{F}_2[x]$.

*(2+3 Punkte)*

---

Abgabe: Montag 17. Juni, bis 12 Uhr in die Postfächer der Tutoren im V3–126

## Aufgabe 4.

(a) Sei $k$ ein Körper und $f \in k[x]$ von Grad 3. Zeigen Sie, dass $f$ irreduzibel ist genau dann, wenn $f(a) \neq 0$ für alle $a \in k$ (also wenn $f$ keine Nullstellen in $k$ hat).

(b) Finden Sie alle irreduzible Polynome in $\mathbb{F}_2[x]$ von Grad höchstens 4.

Hinweis: Schreiben Sie alle Polynome aus und verwenden Sie ein Analogon des Siebs von Erastothenes.

(c) Wählen Sie ein irreducibles Polynom $f \in \mathbb{F}_2[x]$ von Grad 3 aus. Schreiben Sie alle Potenzen $\bar{x}^r$ von $\bar{x} \in \mathbb{F}_8 = \mathbb{F}_2[x]/(f)$ bezüglich der $\mathbb{F}_2$-Basis $1, \bar{x}, \bar{x}^2$.

*(1+2+2 Punkte)*