# ELEMENTARE ZAHLENTHEORIE
# 11. ÜBUNGSBLATT

DR. BAPTISTE ROGNERUD

**Aufgabe 1.** [1+3 Punkte]

(a) Zeigen Sie, dass $f = x^2 + 1$ ein irreduzibel Polynom in $\mathbb{F}_3[x]$ ist.
(b) Sei $\mathbb{F}_9 := \mathbb{F}_3[x]/(f)$. Finden Sie ein $\rho \in \mathbb{F}_9$ mit $<\rho> = \mathbb{F}_9^\times$.

**Aufgabe 2.** [3 Punkte]

Sei $f = x^2 + x + 34 \in \mathbb{Z}[x]$. Lösen Sie die Gleichung

$$f \equiv 0 \pmod{3^k} \text{ für } k \in \mathbb{N}_{>0}.$$

**Aufgabe 3.** [2+2 Punkte] Seien $f \in \mathbb{Z}[x]$ und $a, c \in \mathbb{Z}$. Sei $p$ eine Primzahl.

(a) Sei $k \in \mathbb{N}_{>0}$. Zeigen Sie, dass

$$f(c + ap^k) \equiv f(c) + f'(c)ap^k \pmod{p^{k+l}}$$

für $1 \leqslant l \leqslant k$.

(b) Sei $c \in \mathbb{Z}$ mit $f(c) \equiv 0 \pmod{p^k}$ für ein $k \in \mathbb{N}_{>0}$. Sei $1 \leqslant l \leqslant k$. Zeigen Sie, dass

$$f(c + ap^k) \equiv 0 \pmod{p^{k+l}} \text{ genau dann wenn } f'(c)a \equiv -\frac{f(c)}{p^k} \pmod{p^l}$$

gilt.

**Aufgabe 4.** [3+2 Punkte] Sei $f = x^3 + x^2 + 20x + 3 \in \mathbb{Z}[x]$.

(a) Lösen Sie die Gleichung $f(x) \equiv 0 \pmod{5^k}$ für $k = 1, 2$ und $3$.
(b) Zeigen Sie: Das Polynom $f$ besitzt $11$ Nullstellen modulo $5^k$ für $k \geqslant 3$.
(Hinweis: Aufgabe 3.)

Abgabe: Freitag, 29. Juni 2018, bis 10 Uhr in die Postfächer der Tutoren in V3-126.