ELEMENTARE ZAHLENTHEORIE
10. Übungsblatt

Julia Sauter, Andrew Hubery

Aufgabe 1.

Seien $f = X^3 + 2X + 1$ und $g = X^3 + X^2 + 2$ in $\mathbb{F}_3[X]$. Finden Sie einen expliziten Isomorphismus $\phi\colon \mathbb{F}_3[X]/(f) \xrightarrow{\sim} \mathbb{F}_3[X]/(g)$.

(4 Punkte)

Aufgabe 2.

Seien $1 \leq m \leq k$ ganze Zahlen, p eine Primzahl, und $f \in \mathbb{Z}[X]$ ein Polynom.

(a) Zeigen Sie, dass für ganze Zahlen a, c gilt $f(c+ap^k) \equiv f(c)+f'(c)ap^k \pmod{p^{k+m}}$.

(b) Falls $f(c) \equiv 0 \pmod{p^k}$ schließen Sie daraus, dass $f(c + ap^k) \equiv 0 \pmod{p^{k+m}}$ genau dann, wenn $f'(c)a \equiv -(f(c)/p^k) \pmod{p^m}$.

(4 Punkte)

Aufgabe 3.

Sei $p \geq 5$ eine Primzahl.

(a) Zeigen Sie, dass $x^2 \equiv -1 \pmod{p}$ ein Lösung hat genau dann, wenn $p \equiv 1 \pmod{4}$.

Hinweis: Betrachten Sie eine Primitivwurzel modulo p.

(b) Zeigen Sie, dass $x^3 \equiv 1 \pmod{p}$ drei verschiedene Lösungen hat wenn $p \equiv 1 \pmod{3}$, und nur eine Lösung hat falls $p \equiv 2 \pmod{3}$.

Hinweis: Betrachten Sie eine Primitivwurzel modulo p.

(c) Benutzen Sie (b) um zu zeigen, dass $x^2 \equiv -3 \pmod{p}$ eine Lösung hat genau dann, wenn $p \equiv 1 \pmod{3}$.

Hinweis: Betrachten Sie die Faktorisierung $x^3 - 1 = (x - 1)(x^2 + x + 1)$ und die quadratische Ergänzung des zweiten Faktors.

(6 Punkte)

Aufgabe 4.

Sei $f = X^3 - 52X - 21 \in \mathbb{Z}[X]$.

Finden Sie alle Nullstellen von f modulo 5, 25, und 125.

Hinweis: Für 25 betrachten $a + 5k$ für eine Nullstelle a modulo 5.

(6 Punkte)

Abgabe: Montag 24. Juni, bis 12 Uhr in die Postfächer der Tutoren im V3–126