ELEMENTARE ZAHLENTHEORIE
10. ÜBUNGSBLATT

DR. BAPTISTE ROGNERUD

Aufgabe 1. [1+1+1+1 Punkte]

(a) Zeigen Sie, dass 3 eine Primitivwurzel modulo 101 ist.
(b) Zeigen Sie, dass $7 \times \mathrm{dlog}_3(2) \equiv 3 \pmod{100}$.
(c) Berechnen Sie $\mathrm{dlog}_3(17)$ mit Hilfe von (b).
(Hinweis: $17 \times 6 \equiv 1 \mod 101$).
(d) Lösen Sie die Gleichungen von $3^n \equiv 17 \pmod{101}$.

Aufgabe 2. [2+1 Punkte]

Bestimmen Sie mit Hilfe des erweiterten euklidischen Algorithmus jeweils den größten gemeinsamen Teiler $\mathsf{ggT}(f, g)$ und Polynome s und t, sodass $\mathsf{ggT}(f, g) = s \cdot f + t \cdot g$ gilt.

(a) $f = x^4 + 2x^3 + 4x^2 + 3x + 2 \in \mathbb{Q}[x]$ und $g = x^3 + x - 2 \in \mathbb{Q}[x]$,
(b) $f = x^4 + 2x^3 + 4x^2 + 3x + 2 \in \mathbb{F}_3[x]$ und $g = x^3 + x - 2 \in \mathbb{F}_3[x]$.

Aufgabe 3. [2+2 Punkte]

(a) Sei K ein Körper. Zeigen Sie, dass $K[x]$ ein Hauptidealring ist.
(b) Sei $n \in \mathbb{N}$. Zeigen Sie, dass $(x, 2) = \{x \cdot P(x) + 2 \cdot Q(x) \ ; \ P(x), Q(x) \in \mathbb{Z}[x]\}$ kein Hauptideal in $\mathbb{Z}[x]$ ist.

Aufgabe 4. [1+2+2 Punkte]

(a) Zeigen Sie, dass $f = x^3 + x^2 + 1$ und $g = x^3 + x + 1$ irreduzibel Polynome in $\mathbb{F}_2[x]$ sind.
(b) Sei $\mathbb{F}_8 := \mathbb{F}_2[x]/(f)$. Schreiben Sie die Multiplikationstafel für $\mathbb{F}_8$.
(c) Finden Sie einen expliziten Isomorphismus von $\mathbb{F}_2[x]/(f)$ nach $\mathbb{F}_2[x]/(g)$ von Körpern.
(Hinweis: Betrachten Sie $\phi : \mathbb{F}_2[x] \to \mathbb{F}_2[x]/(g)$ definiert durch $\phi(P(x)) = \overline{P(x+1)}$.)

Abgabe: Freitag, 22. Juni 2018, bis 10 Uhr in die Postfächer der Tutoren in V3-126.