ELEMENTARE ZAHLENTHEORIE
10. PRÄSENZBLATT

DR. BAPTISTE ROGNERUD

Aufgabe 1.

(a) Bestimmen Sie eine Primitivwurzel r modulo 19. Bestimmen Sie dann den zugehörigen diskreten Logarithmus:

$$\mathrm{dlog}_r\colon\ (\mathbb{Z}/19\mathbb{Z})^* \to \mathbb{Z}/18\mathbb{Z}$$

(b) Lösen Sie die Gleichungen von $n \in \mathbb{Z}$: $11^n \equiv 7 \pmod{19}$.

Aufgabe 2.

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) $f = x^3 + 2x^2 + 2x + 1$ und $g = x^3 + x^2 + x - 2 \in \mathbb{Q}[x]$,
(b) $f = x^3 + 2x^2 + 2x + 1$ und $g = x^3 + x^2 + x - 2 \in \mathbb{F}_3[x]$.

Aufgabe 3.

(a) Finden Sie alle irreduzible Polynome von Grad 2 in $\mathbb{F}_2[x]$ und in $\mathbb{F}_5[x]$.
(b) Zeigen Sie, dass $x^5 + x^4 + 1$ nicht irreduzibel in $\mathbb{F}_2[x]$ ist.
(c) Schreiben Sie die Multiplikationtaffel von $\mathbb{F}_4 := \mathbb{F}_2[x]/(x^2 + x + 1)$.

Aufgabe 4.

Sei p eine Primzahl. Zeigen Sie: $\mathbb{F}_{p^n}$ und $\mathbb{Z}/p^n\mathbb{Z}$ sind genau dann isomorph, wenn $n = 1$ gilt.