Elliptische Kurven und Kryptographie

Serie 11

Rechnen in Körpern der Ordnung 128 und 64 — Besprechung am 12. Dezember

---

33. Sei $r_7 = X^7 + X^5 + X^2 + X + 1$; dann ist $\mathbb{F}_{128} = \mathbb{Z}_2[X]/r_7$ ein Körper der Ordnung 128.

(a) Berechne $X^8, X^{10}, X^{12} \pmod{r_7}$.

(b) Berechne $\mathrm{tr}(X)$, $\mathrm{tr}(X^2)$, $\mathrm{tr}(X^5)$.

(c) Finde in $\mathbb{F}_{128}$ eine Lösung der Gleichung $z^2 + z + X = 0$.

34. Sei $r_6 = X^6 + X^5 + 1$; dann ist $\mathbb{F}_{64} = \mathbb{Z}_2[X]/r_6$ ein Körper der Ordnung 64.

(a) Bestimme welche der folgenden Gleichungen in $\mathbb{F}_{64}$ lösbar sind:

- $z^2 + z = X^4 + 1$
- $z^2 + z = (X^5 + X^2 + 1)^2$

(b) Entscheide jeweils, ob ein $y_0 \in \mathbb{F}_{64}$ existiert, so dass gilt:

- $(X^4, y_0) \in C[0, X^3]$
- $(X^4, y_0) \in C[X^2 + X + 1, X^3]$
- $(X^4, y_0) \in C[X^5 + 1, X^3]$

Hinweis: $X^3 \equiv X^8(X + 1) \pmod{r_6}$.