Elliptische Kurven & Kryptologie Serie 12

Elliptische Kurven über Körpern der Ordnung 128 und 64 Abgabe: 26. Mai

Die folgenden Aufgaben können (und sollten) ohne Hilfe von `Maple` oder `Mathematica` gelöst werden.

Im Folgenden seien $r_7(x) = x^7 + x^5 + x^2 + x + 1$ und $r_6(x) = x^6 + x^5 + 1$ zwei Polynome aus $\mathbb{Z}_2[x]$. Beide Polynome sind irreduzibel über $\mathbb{F}_2$.

1. Sei $\mathbb{F}_{128} = \mathbb{Z}_2[x]/r_7(x)$.

(a) Berechne $\mathrm{tr}(1)$, $\mathrm{tr}(x)$, $\mathrm{tr}(x^4)$, und $\mathrm{tr}(x^3)$.

(b) Berechne $x^{12} \mod r_7$ und bestimme damit $\mathrm{tr}(x^5)$.

(c) Finde ein $\tilde{z}_0 \in \mathbb{Z}_2[x]$, so dass $\tilde{z}_0 \mod r_7$ in $\mathbb{F}_{128}$ eine Lösung ist der Gleichung $Z^2 + Z + (x + x^2) = 0$.

2. Sei wieder $\mathbb{F}_{128} = \mathbb{Z}_2[x]/r_7(x)$.

(a) Entscheide jeweils, ob ein $Y_0 \in \mathbb{F}_{128}$ existiert, so dass gilt:

- $(1, Y_0) \in C[0, x^2 + 1]$
- $(1, Y_0) \in C[x^5, x^2 + 1]$
- $(1, Y_0) \in C[x^4, x^2 + 1]$

(b) Finde irgend einen Punkt (X_1, Y_1) auf der Kurve $C[x^3 + x + 1, x^6 + x^2 + 1]$.

3. Sei $\mathbb{F}_{64} = \mathbb{Z}_2[x]/r_6(x)$.

(a) Berechne $\mathrm{tr}(1)$, $\mathrm{tr}(x)$, $\mathrm{tr}(x^4)$, und $\mathrm{tr}(x^3)$.

(b) Berechne $x^8 \mod r_6$ und bestimme damit $\mathrm{tr}(x^5)$.

(c) Finde ein $\tilde{z}_0 \in \mathbb{Z}_2[x]$, so dass $\tilde{z}_0 \mod r_6$ in $\mathbb{F}_{64}$ eine Lösung ist der Gleichung $Z^2 + Z + 1 = 0$.

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

- $Z^2 + Z = x^4 + 1$
- $Z^2 + Z = (x^5 + x^2 + 1)^2$

4. Sei wieder $\mathbb{F}_{64} = \mathbb{Z}_2[x]/r_6(x)$.

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: $x^3 \equiv x^8(x + 1) \mod r_6$.