Elliptische Kurven und Kryptographie

Serie 11

Rechnen in Körpern der Ordnung 128 und 64 — Musterlösungen

---

33. Sei $r_7 = X^7 + X^5 + X^2 + X + 1$; dann ist $\mathbb{F}_{128} = \mathbb{F}_2[X]/\langle r_7 \rangle$ 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 $z^2 + z + X = 0$.

Lösung:

(a) $X^8 = X^7 X \equiv X^6 + X^3 + X^2 + X \pmod{r_7}$
$X^{10} = X^7 X^3 \equiv X^8 + X^5 + X^4 + X^3 \equiv X^6 + X^5 + X^4 + X^2 + X \pmod{r_7}$
$X^{12} = X^7 X^5 \equiv X^{10} + X^7 + X^6 + X^5 \equiv X^7 + X^4 + X^2 + X \equiv X^5 + X^4 + 1 \pmod{r_7}$

(b) Eine aufwendige Rechnung zeigt $\mathrm{tr}(X) = 0$. Daraus folgt $\mathrm{tr}(X^2) = \mathrm{tr}(X)^2 = 0$. Nun stellen wir fest, dass

$$\mathrm{tr}(X^5) = \mathrm{tr}(X^5)^2 = \mathrm{tr}(X^{10}) = \mathrm{tr}(X^6 + X^5 + X^4 + X^2 + X) = \mathrm{tr}(X^6) + \mathrm{tr}(X^5),$$

also muss $\mathrm{tr}(X^6) = 0$ sein. Daraus erhalten wir

$$0 = \mathrm{tr}(X^{12}) = \mathrm{tr}(X^5) + \mathrm{tr}(X^4) + \mathrm{tr}(1) = \mathrm{tr}(X^5) + 1$$

und somit $\mathrm{tr}(X^5) = 1$.

(c) Eine Lösung ist $\tau(X)$, also (mit etwas Rechenaufwand) $X^4 + X^3 + X^2$. Die zweite Lösung ist $X^4 + X^3 + X^2 + 1$.

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

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

i. $z^2 + z = X^4 + 1$

ii. $z^2 + z = (X^5 + X^2 + 1)^2$

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

i. $(X^4, y_0) \in C[0, X^3]$

ii. $(X^4, y_0) \in C[X^2 + X + 1, X^3]$

iii. $(X^4, y_0) \in C[X^5 + 1, X^3]$

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

Lösung:

(a) Mit viel Aufwand (oder mit sage) erhalten wir $\mathrm{tr}(X) = 1$ und $\mathrm{tr}(X^5) = 1$.

i. Es gilt $\mathrm{tr}(X^4) = \mathrm{tr}(X)^4 = 1$ und (da m gerade ist) $\mathrm{tr}(1) = 0$. Somit haben wir $\mathrm{tr}(X^4 + 1) = 0$ und die Gleichung ist nicht lösbar.

ii. Es gilt $\mathrm{tr}((X^5+X^2+1)^2) = \mathrm{tr}(X^5)^2+\mathrm{tr}(X)^4+\mathrm{tr}(1) = 0$, also ist die Gleichung lösbar.

(b) Wir dividieren jeweils die Kurvengleichung durch $x_0^2 = X^8$. Da durchgehend $a_6 = X^3 \equiv X^8(X + 1)$ gilt, erhalten wir $a_6/x_0^2 \equiv X + 1$. Schliesslich berechnen wir $\mathrm{tr}(x_0 + a_2 + a_6/x_0^2)$.

i. Ohne den Wert von $\mathrm{tr}(X)$ zu kennen, kann man sehen, dass $\mathrm{tr}(X^4 + X + 1) = \mathrm{tr}(X)^4 + \mathrm{tr}(X) + 1 = 0$. Es gibt also eine Lösung.

ii. Auch in $\mathrm{tr}(X^4 + X^2 + X + 1 + X + 1)$ löschen sich vor und nach Umformen schliesslich alle Terme aus. Auch hier existiert also ein y_0.

iii. Hier erhalten wir

$$\mathrm{tr}(X^4 + X^5 + 1 + X + 1) = \mathrm{tr}(X)^4 + \mathrm{tr}(X) + \mathrm{tr}(X^5) = \mathrm{tr}(X^5) = 1.$$