Elliptische Kurven und Kryptographie

Serie 10

elliptische Kurven über endlichen Körpern — Musterlösungen

---

30. Sei $\mathbb{F} := \mathbb{Z}_{13}$ und sei $E = (C, \mathscr{O}, +)$ die elliptische Kurve über dem Körper $\mathbb{F}$ mit

$$C\colon y^2 = x^3 + x^2 + x\,.$$

Zeige: $E \cong \mathbb{Z}_2 \times \mathbb{Z}_8$.

Hinweis: Der Punkt $(2, 1)$ hat die Ordnung 8.

Beweis:

Die Kurve ist in WNF. Wir können also wie gewohnt den Punkt $(2, 1)$ verdoppeln und erhalten $(-1, 5)$. Eine weitere Verdopplung dieses Punkts liefert $(0, 0)$, von dem wir wissen, dass er Ordnung 2 hat. Somit besitzt der ursprüngliche Punkt $(2, 1)$ die Ordnung 8.

Als nächstes listen wir alle Punkte auf der Kurve auf. Dazu berechnen wir die möglichen Werte, welche die Terme y^2 und x^3+x^2+x annehmen können, und vergleichen. Wir erhalten die folgenden Punkte:

$$(0,0),\ (1,\pm 4),\ (2,\pm 1),\ (3,0),\ (5,\pm 5),\ (7,\pm 3),\ (8,\pm 5),\ (9,0),\ (12,\pm 5),\ \mathscr{O}\,,$$

wie gewünscht also 16. Da es mehrere Punkte der Ordnung 2 (alle mit x-Koordinate 0) und einen der Ordnung 8 gibt, muss die Gruppe isomorph zu $\mathbb{Z}_2 \times \mathbb{Z}_8$ sein.

31. Sei $C\colon y^2 + xy = x^3 + a_2x^2 + a_6$ eine cubische Kurve über einem Körper $\mathbb{F}_q$ der Charakteristik 2 und sei $(x_0, y_0) \in C$ mit $x_0 \neq 0$.

(a) Dividiere $y_0^2 + x_0y_0 + x_0^3 + a_2x_0^2 + a_6$ durch x_0^2, setze $x := x_0$ und $u_0 := \frac{y_0}{x_0}$, und schreibe die entsprechende quadratische Gleichung in u_0 auf.

(b) Zeige, dass nebst $u_0 := \frac{y_0}{x_0}$ auch $u_0 + 1$ eine Lösung dieser quadratischen Gleichung ist und finde so einen weiteren Punkt (x_0, y_1) auf C.

Lösung:

(a) Wir erhalten

$$u_0^2 + u_0 = x_0 + a_2 + \frac{a_6}{x_0^2}\,.$$

(b) Es gilt $(u_0+1)^2 + (u_0+1) = u_0^2 + 1 + u_0 + 1 = u_0^2 + u_0$. Setzen wir $u_1 := u_0 + 1$, so erhalten wir die zweite Lösung $y_1 = u_1\,x_0 = y_0 + x_0$.

32. Sei $\mathbb{F}_{64} = \mathbb{Z}_2[X]/(X^6 + X^5 + 1)$, sei

$$C\colon\, y^2 + xy = x^3 + a_2x^2 + a_6$$

eine cubische Kurve über $\mathbb{F}_{64}$, und sei $a_2 := (X^4 + X + 1)$.

(a) Bestimme a_6 so, dass der Punkt

$$\left(X^2 + 1,\; X^3 + X + 1\right)$$

auf C liegt.

(b) Bestimme einen weiteren Punkt (verschieden von $\mathscr{O}$) auf C.

Lösung:

(a) Setzen wir die Koordinaten ein, so vereinfacht sich die linke Seite der Kurvengleichung zu $X+1$ und die rechte zu $X^5+X^4+a_6$. Es muss also gelten, dass $a_6 = X^5+X^4+X+1$.

(b) Wir verwenden 31.(b) und erhalten den weiteren Punkt

$$\left(X^2 + 1,\; X^3 + X^2 + X\right).$$