Punkte auf elliptischen Kurven

Reinhold Hübl

Wir betrachten einen endlichen Körper $\mathbb{F}_q$ der Charakteristik > 3 und eine elliptische Kurve $\overline{E}$ über $\mathbb{F}_q$ gegeben durch die Gleichung

$$y^2 = x^3 + ax + b \tag{1}$$

mit $a, b \in \mathbb{F}_q$, wobei $4 \cdot a^3 + 27 \cdot b^2 \neq 0$. Ferner seine zwei Punkte $P = (x_1, y_1)$ und $Q = (x_2, y_2)$ auf $\overline{E}$ gegeben (die nicht der unendlich ferne Punkte sind), wobei $x_1 \neq x_2$.

Satz 0.1. *Die Gerade L durch P und Q schneidet die Kurve $\overline{E}$ noch in (genau) einem weiteren Punkt $R = (x_3, y_3)$. Setzen wir*

$$s = \frac{y_2 - y_1}{x_2 - x_1}$$

so gilt für die Koordinaten von R:

$$\begin{aligned} x_3 &= s^2 - x_1 - x_2 \\ y_3 &= s \cdot (x_3 - x_1) + y_1 \end{aligned}$$

Beweis: Der Wert s beschreibt die Steigung der Gerade L durch P und Q. Die Gleichung dieser Geraden ist gegeben durch

$$y = s \cdot (x - y_1) + y_1 = s \cdot x + y_1 - s \cdot x_1$$

Setzen wir $m = y_1 - s \cdot x_1$, so können wir die Geradengleichung schreiben als

$$y = s \cdot x + m$$

Die Koordinaten eines Punktes auf L und $\overline{E}$ müssen daher die folgenden Gleichungen erfüllen

$$\begin{aligned} y &= s \cdot x + m \\ y^2 &= x^3 + a \cdot x + b \end{aligned}$$

Setzen wir die erste Gleichung in die zweite ein, so erhalten wir

$$(s \cdot x + m)^2 = x^2 + a \cdot x + b$$

also, nach ausmultiplizieren,

$$0 = x^3 - s^2 \cdot x^2 + (a - 2m) \cdot x + b - m^2 \tag{2}$$

Schreibe

$$g(x) = x^3 - s^2 \cdot x^2 + (a - 2m) \cdot x + b - m^2 \tag{3}$$

Da P und Q auf L und $\overline{E}$ liegen, erfüllen x_1 und x_2 die Gleichung (2), d.h. x_1 und x_2 sind Nullstellen von $g(x)$. Das bedeutet wiederum, dass das Polynom $g(x)$ ohne Rest durch $(x - x_1)$ und $(x - x_2)$ teilbar ist,

$$g(x) \div ((x - x_1) \cdot (x - x_2)) = l(x) \quad \text{Rest } 0$$

Da $g(x)$ den Grad 3 hat, muss $l(x)$ notwendig den Grad 1 haben, $l(x) = u \cdot x + v$. Da

$$l(x) \cdot (x - x_1) \cdot (x - x_2) = g(x)$$

muss notwendig gelten

$$u \cdot x \cdot x \cdot x = x^3$$

(Vergleich der Terme gleichen Grades), und deshalb muss $u = 1$ sein, also

$$l(x) = x + v$$

damit ist $x_3 = -v$ eine weitere Lösung von Gleichung (2), also die x–Komponente eines dritten Punktes R auf L und $\overline{E}$. Aus

$$g(x) \div ((x - x_1) \cdot (x - x_2)) = (x - x_3)$$

folgt nun

$$g(x) = (x - x_1) \cdot (x - x_2) \cdot (x - x_3)$$

Multiplizieren wir das aus, so erhalten wir

$$g(x) = x^3 - (x_1 + x_2 + x_3) \cdot x^2 + (x_1x_2 + x_1x_3 + x_2x_3) \cdot x - x_1x_2x_3 \tag{4}$$

Vergleichen wir nun die beiden Darstellungen (3) und (4), so folgt durch Koeffizientenvergleich

$$s^2 = x_1 + x_2 + x_3$$

also

$$x_3 = s^2 - x_1 - x_2$$

Da der Punkt R auch noch auf der Gerade L liegt, ist seine y–Komponente gegeben durch

$$y_3 = s \cdot (x_3 - x_1) + y_1 = s \cdot x_3 + m$$