Kryptographie *WS 2015/16*
Barbara Baumeister
Tutoren: Apolonia Gottwald, Soeren Senkovic

10. Übungsblatt

Abgabe: Donnerstag, 14.1.2016

Aufgabe 1 Sei P ein punkt der elliptischen Kurve $E(\mathbb{R}): \ y^2 = x^3 + ax + b$. Geben Sie eine geometrische Bedingung, die äquivalent ist zu der Eigenschaft, dass

(a) P die Ordnung 2;

(b) P die Ordnung 3;

(c) P die Ordnung 4 hat.

Aufgabe 2 Sei $E(\mathbb{R}) : y^2 = x^3 - 36x$. Dann sind $P = (-3, 9)$ und $Q = (-2, 8)$ Punkte in $E(\mathbb{R})$. Berechnen Sie $P + Q$ und $2P$.

Aufgabe 3 Ziel der Aufgabe ist es, den Beweis von Satz 5 weiter auszuführen. Sei $L = L(\alpha, \beta, \gamma) = \alpha X + \beta Y + \gamma Z = 0$ eine projektive Gerade mit $\alpha \neq 0$ und $\beta = 0$. Weiter sei $E = E(K)$ eine elliptische Kurve zu der homogenen Weierstraß-Gleichung $F(X, Y, Z)$. Zeigen Sie

(a) Bestimmen Sie die Elemente $(x_0 : y_0 : z_0)$ in L, indem Sie eine Fallunterscheidung $z_0 = 0$ und $z_0 \neq 0$ machen.

(b) $\mathcal{O} \in L \cap E$ und $m(\mathcal{O}, L, E) = 1$ (Hinweis: Betrachten Sie $\psi(t)$ für $P' = (-\gamma : 0 : 1)$).

(c) Sei $P = (x_0 : y_0 : z_0) \in L \cap E$, wobei $P \neq \mathcal{O}$. Bestimmen Sie $m(P, L, E)$ mit Hilfe von $P' = \mathcal{O}$.

(d) Folgern Sie $\sum_{P \in P^2(K)} m(P, L, E) \in \{0, 1, 3\}$ für diese projektive Gerade L.

Aufgabe 4 Gegeben sei das Alphabet $\mathcal{A} = \{A, \ldots, Z\}$ und die elliptische Kurve $E \ : \ y^2 = x^3 + 300x + 1011$. Es sollen Wörter der Länge 2 über $\mathcal{A}$ in Punkte der elliptischen Kurve "umgewandelt" werden, so dass mit einer Wahrscheinlichkeit von höchstens $1/1000$ zu k gegebenen Werten x_i kein Punkt auf der Kurve mit x-Koordinate gleich x_i existiert. Wählen Sie einen geeigneten Körper und wandeln Sie das Wort "Erle" in Punkte der Kurve um.