Hochschule Bonn-Rhein-Sieg

Angewandte Kryptographie 2, SoSe 2024

Vorlesungsteil "Kryptographie mit elliptischen Kurven"
Guntram Wicke (guntram.wicke@lehrbeauftragte.h-brs.de)

2 Übungen zu Kapitel 2 ("Background on Elliptic Curves, Computation with Group Elements")

2.1 Punktaddition und Punktverdoppelung auf elliptischen Kurven über $GF(p)$

Gegeben sei die elliptische Kurve $E : y^2 = x^3 + 16x + 7$ über dem Grundkörper $GF(31)$.

1. Die folgenden Punkte (x, y) der affinen Ebene oder Punkte $(X : Y : Z)$ der projektiven Ebene sind gegeben. $A = (28, 26)$, $B = (28, 5)$, $C = (121, -5)$, $D = (0, 0)$, $E = (0 : 1 : 0)$, $F = (28 : 5 : 1)$, $G = (0, 10)$, $H = (56 : 52 : 2)$. Welche davon liegen auf der Kurve E und welche Punkte sind (bezogen auf den Grundkörper) kongruent zueinander und repräsentieren damit den gleichen Punkt auf E?

2. Die folgenden Punkte auf E sind in affinen Koordinaten gegeben: $P_0 = (0, 10)$, $P_1 = (2, 4)$ und $P_2 = (6, 3)$. Berechnen Sie $P_3 = P_1 + P_2$, dann $P_4 = P_1 - P_2$, sowie $P_5 = P_2 - P_1$ und $P_6 = P_1 + P_1$. Schließlich ist noch $P_7 = P_6 + P_0$ zu berechnen.

3. Berechnen sie die Summe Y aus den zwei Punkten $U = (6, 3)$ und $V = (22, 8)$, sowie die Summe Z aus den Punkten $W = (7, 11)$ und $X = (21, 26)$. Welches der Gruppenaxiome für Abelsche Gruppen wirkt hier offenbar?

4. Geben Sie, wenn möglich, eine Zerlegung für Y und für Z aus Aufgabe 3 in *drei* verschiedene affine Punkte der Kurve E an.

5. (*) Geben Sie die (formalen) partiellen Ableitungen $\frac{\partial f}{\partial x}$ und $\frac{\partial f}{\partial y}$ der Kurve $f(x, y) = y^2 - (x^3 + ax + b)$ an. Für nichtsinguläre Punkte $P = (x_1, y_1)$ der Kurve sind diese ungleich Null. Leiten Sie die Formel für den Anstieg s der Tangente für die Punktverdoppelung in affinen Koordinaten aus der Tangentengleichung $\frac{\partial f}{\partial x}(P)(x - x_1) + \frac{\partial f}{\partial y}(P)(y - y_1) = 0$ her.