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

11. Übungsblatt

Abgabe: Donnerstag, 21.1.2016

Aufgabe 1 Zeigen Sie, dass $h(x) = x^3 + ax + b$ genau dann mehrfache Nullstellen hat, wenn die Kurve $y^2 = h(x)$ singulär ist.

Aufgabe 2 Sei $E(\mathbb{F}_5) : y^2 = x^3 + 3$ eine elliptische Kurve.

(a) Zeigen Sie, dass $E(\mathbb{F}_5)$ supersingulär ist.

(b) Zeigen Sie, dass $P = (1, 2)$ in $E(\mathbb{F}_5)$ liegt und bestimmen Sie die Ordnung von P.

(c) Sei $Q = (2, -1)$. Bestimmen Sie das DL-Problem für P und Q.

Aufgabe 3 Gegeben sei die Edwardskurve Ed : $x^2 + y^2 = 1 + dx^2y^2$ über einem endlichen Körper K ungerader Charakteristik. Ferner sei d ein Nichtquadrat in K. Zeige:

(a) $(0, 1)$ ist das neutrale Element in $\mathrm{Ed}(K)$.

(b) Es gilt $-(x, y) = (-x, y)$ für alle $(x, y) \in \mathrm{Ed}(K)$.

(c) Teilt 4 die Zahl $|K| + 1$, dann enthält $\mathrm{Ed}(K)$ genau ein Element der Ordnung 2.

(d) $\mathrm{Ed}(K)$ enthält stets ein Element der Ordnung 4.

Aufgabe 4 Sei Ed : $x^2 + y^2 = 1 + 2x^2y^2$ eine Edwardskurve über $K = \mathbb{F}_5$.

(a) Bestimmen Sie die K-rationalen Punte auf $\mathrm{Ed}(K)$.

(b) Zeigen Sie, dass $\mathrm{Ed}(K)$ zyklisch ist.