Kryptographie *WS 2012/13*
Barbara Baumeister

12. Übungsblatt

Abgabe: Donnerstag, 17.1.2013

Aufgabe 1 Sei $E : y^2 = x^3 + ax + b$ eine elliptische Kurve über $\mathbb{F}_p$, wobei $p > 2$ eine Primzahl ist. Zeigen Sie, dass gilt

$$|E(\mathbb{F}_p)| = p + 1 + \sum_{x \in \mathbb{F}_p} \left(\frac{x^3 + ax + b}{p} \right).$$

Aufgabe 2

(a) Zeigen Sie, dass alle elliptische Kurven der Form $E : y^2 = x^3 + ax + b$ sowohl über $\mathbb{F}_2$ als auch über $\mathbb{F}_3$ supersingulär sind.

(b) Finden Sie eine elliptische Kurve, die supersingulär über $\mathbb{F}_5$ ist.

Aufgabe 3 Sei $Y^2 + a_1XY + a_3Y = X^3 + a_2X^2 + a_4X + a_6$ eine Weierstraß-Kurve über dem Körper K, wobei char $K = 2$ ist. Zeigen Sie:

(a) Falls $a_1 \neq 0$, dann könnnen wir durch einen Variablenwechsel zu einer Gleichung übergehen, in der $a_1 = 1$ und $a_3 = 0$ gilt.

(b) Falls $a_1 = a_3 = 0$, dann ist die Kurve singulär.

(c) Falls $a_1 \neq 0$ (und $a_3 = 0$), dann können wir ausserdem durch Variablenwechsel $a_4 = 0$ erreichen.

(d) Falls $a_3 \neq 0$ (und $a_1 = 0$), dann können wir durch Variablenwechsel $a_2 = 0$ erreichen.

Aufgabe 4 Sei $Y^2 + a_1XY + a_3Y = X^3 + a_2X^2 + a_4X + a_6$ eine Weierstrass-Kurve über dem Körper $K = \mathbb{F}_2$. Bestimmen Sie welche der reduzierten Kurven, die Sie in Aufgabe 3 erhalten haben, über $\mathbb{F}_2$ supersingulär sind.