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

9. Übungsblatt

Abgabe: Donnerstag, 7.1.2016

Aufgabe 1 Sei K ein Körper der Charakteristik p, $p \neq 2, 3$. Sei

$$y^2 = x^3 + ax + b$$

die vereinfachte Weierstraß-Gleichung. Es ist

$$\Delta := -16(4a^3 + 27b^2)$$

die Diskriminate der Gleichung. Zeigen Sie, dass die ursprüngliche Gleichung F glatt ist genau dann, wenn $\Delta \neq 0$ gilt.

Aufgabe 2 Gegeben sei die elliptische Kurve $E: \ y^2 = x^3 - x + 1$.

(a) Berechnen Sie $|E(\mathbb{Z}_5)|$.

(b) Bestimmen Sie die Struktur der Gruppe $E(\mathbb{Z}_5)$.

Aufgabe 3 Sei $E \ : \ y^2 = x^3 + ax + b$ eine elliptische Kurve über dem Körper K. Wie viele Elemente der Ordnung 2 kann $E(K)$ höchstens besitzen?

Aufgabe 4 (a) Sei p eine Primzahl, $p \equiv 3 \bmod 4$ und sei E eine elliptische Kurve über $\mathbb{F}_p$. Finden Sie einen Polynomialzeit-Algorithmus, der für $x \in \mathbb{F}_p$ einen Punkt (x, y) auf E konstruiert, falls ein solcher Punkt existiert.
Hinweis: Verwenden Sie eine frühere Aufgabe zu diesem Thema.

(b) Verwenden Sie den Algorithmus, um einen Punkt $(2, y)$ auf E zu finden, wobei $p = 111119$ und $a = b = 1$ ist.