10. Übungsblatt

Abgabe: Donnerstag, 20.12.2012

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

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

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

Aufgabe 2 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 3 Sei p eine Primzahl, $p \equiv 3 \bmod 4$. Sei a eine ganze Zahl, die ein Quadrat mod p ist. Zeigen Sie, dass $a^{(p+1)/4}$ eine Quadratwurzel von a mod p ist.

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 Aufgabe 3.

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