TECHNISCHE UNIVERSITÄT BERLIN WS09/10
Fakultät II – Institut für Mathematik
Dozent: Tobias Finis
Assistent: Gerriet Möhlmann
www.math.tu-berlin.de/~kant/kryptows09

14. Übung Kryptographie

Die Punkte dieses Blattes sind Zusatzpunkte.

1. Aufgabe

Sei $p > 5$ eine Primzahl und E eine elliptische Kurve über $\mathbb{F}_p$ mit einem Punkt P der Ordnung p. Zeigt, dass für die Ordnung der Punktgruppe gilt

$$\#E(\mathbb{F}_p) = p.$$

(5 Punkte)

2. Aufgabe

Sei E eine elliptische Kurve über $\mathbb{F}_{41}$ gegeben durch $E : y^2 = x^3 + 2x + 1$. Dann sind $P = (0, 1)$ und $Q = (30, 40)$ zwei Punkte auf E. Bestimmt $m \in \mathbb{Z}$ mit $Q = [m]P$.

(5 Punkte)

3. Aufgabe

Sei $p > 3$ eine Primzahl und $E : y^2 = x^3 + ax + b$ eine elliptische Kurve über $\mathbb{F}_p$. Zeigt, dass die folgenden Gleichung gilt:

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

wobei die Summe über die Legendresymbole läuft. **(5 Punkte)**