Wolfgang K. Seiler
Tel. 2515

A5, C201

31. März 2017

5. Übungsblatt Elliptische Kurven

Aufgabe 1: *(6 Punkte)*

E sei eine elliptische Kurve. Zeigen Sie:

a) Sind $P \neq Q$ zwei Wendepunkte von E, so liegt auf der Geraden durch P und Q noch ein dritter Wendepunkt.

b) Falls E neun Wendepunkte hat, gibt es zwölf Geraden, auf denen jeweils drei Wendepunkte liegen, und jeder Wendepunkt liegt auf vier dieser Geraden.

c) Im Reellen kann eine elliptische Kurve höchstens drei Wendepunkte haben.

Aufgabe 2: *(5 Punkte)*

Die elliptische Kurve E über dem Körper $\mathbb{F}_7$ sei gegeben durch die Gleichung

$$y^2 = x^3 + 2x + 3\,.$$

Bestimmen Sie die Ordnungen aller Punkte von E!

Aufgabe 3: *(5 Punkte)*

Die elliptische Kurve E über dem Körper $\mathbb{F}_{103}$ sei gegeben durch die Gleichung

$$y^2 = x^3 + 3x - 1\,,$$

und P sei der Punkt $(5, 6)$. Berechnen sie 20P nach dem Algorithmus von Montgomery!

Aufgabe 4: *(4 Punkte)*

Ein ElGamal-System benutzt die Paramater $p = 1009$ und $a = 2$.

a) Schicken Sie dem Teilnehmer mit dem öffentlichen Schlüssel 512 die Nachricht $m = 999$ verschlüsselt zu!

b) Bestimmen Sie den geheimen Schlüssel dieses Teilnehmers!