Wolfgang K. Seiler
Tel. 2515

B6, B4.18

28. April 2020

8. Übungsblatt Elliptische Kurven

Aufgabe 1: *(5 Punkte)*
Stellen Sie für die folgenden elliptischen Kurven aus $\mathbb{P}^2(\mathbb{F}_5)$ die Gruppentafeln auf und entscheiden Sie, welche der Gruppen zyklisch sind!

a) $Y^2Z = X^3 + XZ^2$

b) $Y^2Z = X^3 + 2XZ^2$

c) $Y^2Z = X^3 + 2XZ^2 + Z^3$

Aufgabe 2: *(4 Punkte)*
Die elliptische Kurve E über dem Körper $\mathbb{F}_7$ sei gegeben durch die Gleichung

$$Y^2 = X^3 + 2XZ^2 + 3Z^3 \,.$$

Bestimmen Sie die Ordnungen aller Punkte von E und identifizieren Sie E als abstrakte Gruppe!

Aufgabe 3: *(5 Punkte)*
Die elliptische Kurve E über dem Körper $\mathbb{F}_{103}$ sei gegeben durch die affine Gleichung

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

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

Aufgabe 4: *(6 Punkte)*

a) Die öffentlichen Parameter eines Kryptosystems nach Koyama, Maurer, Okamoto und Scott seien $N = 55$ und $e = 5$. Verschlüsseln Sie den Nachrichtenblock $(7, 13)$!

b) Finden Sie die Entschlüsselungsabbildung dazu, und entschlüsseln Sie den Chiffretext $(3, 7)$!