Wolfgang K. Seiler
Tel. 2515

A5, C201

29. April 2017

6. Übungsblatt Elliptische Kurven

Aufgabe 1: *(4 Punkte)*

a) Zeigen Sie: Die Abbildung φ: $\begin{cases} \mathbb{F}_7 \to \mathbb{F}_7 \\ x \mapsto x^3 \end{cases}$ ist nicht bijektiv!

b) Bestimmen Sie alle Punkte der elliptischen Kurven mit den affinen Gleichungen $y^2 = x^3+3$ und $y^2 = x^3 + 4$ über $\mathbb{F}_7$!

c) Zu welchen abstrakten Gruppen sind die beiden Kurven isomorph?

Aufgabe 2: *(7 Punkte)*

a) Lösen Sie im Körper $\mathbb{F}_{17}$ die Gleichung $6x = 10$!

b) Berechnen Sie dort mit der *baby step – giant step* Methode eine Lösung der Gleichung $6^x = 10$!

Aufgabe 3: *(5 Punkte)*

A sei eine reelle 2×2-Matrix der Ordnung r, d.h. A^r ist die Einheitsmatrix und für jede natürliche Zahl $s < r$ ist $A^s \neq E$. Weiter sei G die Gruppe, die aus allen Potenzen von A besteht. Wie können Sie für große r das diskrete Logarithmenproblem in dieser Gruppe am einfachsten lösen?

Aufgabe 4: *(4 Punkte)*

Ein Spielzeug-RSA-Verfahren arbeitet mit den beiden Primzahlen $p = 223$ und $q = 229$.

a) Welches ist der kleinste öffentliche Exponent e, mit dem man hier arbeiten kann?

b) Bestimmen Sie dazu den geheimen Exponenten d!

c) Verschlüsseln Sie in diesem System die Nachricht 31415!