Kryptographie - Algebraischer Hintergrund
Prof . Dr. F.-O. Schreyer
Übungsblatt 3: Elliptische Kurven und Faktorisierung

Abgabetermin 21.5.2002
Voraussetzungen: Vorlesungskapitel Faktorisierung, Elliptische Kurven.

1. Für q eine Primzahl. Schreiben Sie eine Maple-Prozedur, die die Punke einer elliptischen Kurve
$$E_{a,b}(\mathbb{F}_q) = \left\{(x,y) \in \mathbb{F}_q^2 \mid y^2 = x^3 + ax + b\right\} \cup \{O\}$$
$a, b \in \mathbb{F}_q$ bestimmt.

2. Für q eine Primzahl. Schreiben Sie eine Maple-Prozedur, die die Anzahl $|E_{a,b}(\mathbb{F}_q)|$ der Punke der elliptischen Kurve $E_{a,b}(\mathbb{F}_q)$ bestimmt (Vergessen Sie den Punkt im Unendlichen nicht).

3. Bestimmen Sie für alle Primzahlen $5 \leq p \leq 29$ die Anzahl der Punkte von $E(\mathbb{F}_p)$: $y^2 = x^3 + 1$. Wann ist $|E(\mathbb{F}_p)| = p + 1$?

4. Für q eine Primzahl. Schreiben Sie eine Maple-Prozedur, die $|E_{a,b}(\mathbb{F}_q)|$ für alle $a, b \in \mathbb{F}_q$ bestimmt und damit den Satz von Hasse verifiziert.

5. Schreiben Sie eine Maple-Prozedur, die $P + Q$ für zwei Punkte P und Q auf einer elliptischen Kurve $E_{a,b}(\mathbb{F}_q)$ berechnet. Vergessen Sie den Fall $P = Q$ und den Punkt O im Unendlichen nicht.

6. Sei $t \in \mathbb{N}$ und $P \in E_{a,b}(\mathbb{F}_q)$. Schreiben Sie ein Maple-Skript, das $t \cdot P$ berechnet.

7. Schreiben Sie ein Maple-Skript, das die elliptische-Kurven-Faktorisierung wie in der Vorlesung beschrieben durchführt.

8. Versuchen Sie die Zahlen aus dem Übungsblatt 2 mit Ihrem Skript zur elliptischen-Kurven-Faktorisierung zu faktorisieren.

Abgabe der Aufgaben bitte als Maple-file per email an boehm@math.uni-sb.de.