Übungen zur Vorlesung Kryptographie

Abt. Reine Mathematik SS 06 – Blatt 10

Abgabetermin: Fr., 14.07.2006 um 12:30 Uhr vor Beginn der Übung

---

1. (a) Schreibe eine Funktion in Maple, die zwei Punkte auf einer elliptischen Kurve über $\mathbb{C}$ addiert.

   (b) Wiederhole (a) für eine elliptische Kurve über einem endlichen Körper $\mathbb{F}_p$, p eine Primzahl.

   Man beschränke sich der Einfachheit halber auf elliptische Kurven der Form $y^2 = x^3 + ax + b$, $a, b \in \mathbb{C}$ bzw. $a, b \in \mathbb{F}_p$.

2. (a) Betrachte die elliptische Kurve $y^2 = x^3 - 43x + 166$ über $\mathbb{C}$ und den Punkt $P = (3, 8)$. Finde die Ordnung von P.

   (b) Betrachte die elliptische Kurve $y^2 = x^3+22x+472$ über $\mathbb{F}_p$ mit $p := 1234567891$. Berechne alle y, so dass der Punkt $P_y = (1, y)$ auf der Kurve liegt. Berechne jeweils $10000 \cdot P_y$.

3. Betrachte die elliptische Kurve $y^2 = x^3 + x + 1$ über $\mathbb{F}_7$. Gib alle Punkte an und konstruiere die Verknüpfungstafel der Gruppenoperation.

4. Sei $i^2 = -1$, $R = \mathbb{Z}[i] = \{a + ib : a, b \in \mathbb{Z}\}$. Wir wählen folgendes Vertretersystem aller Primelemente von R:

   - $1 + i$
   - p Primzahl mit $p \equiv 3 \pmod 4$
   - $s = a + ib$, $t = a - ib$ mit $a \geqslant b > 0$, wobei $p = a^2 + b^2 = st \equiv 1 \pmod 4$ eine Primzahl ist

   Bestimme die eindeutige Primfaktorzerlegung der folgenden Elemente von R.

   (a) $4 + 5i$

   (b) $13 + 11i$

   (c) $41 + 169i$