Übungen zur Vorlesung Kryptographie

Abt. Reine Mathematik SS 06 – Blatt 7

Abgabetermin: Fr., 23.06.2006 um 12:30 Uhr vor Beginn der Übung

---

1. Wir wollen die Zahl $N := 5989$ mit dem quadratischen Sieb faktorisieren.
   (a) Wähle als Siebintervall $\{-5, \ldots, +5\}$ und finde eine passende (möglichst kleine) Faktorbasis, so dass sich N faktorisieren lässt.
   (b) Was passiert, wenn man das Siebintervall auf $\{-6, \ldots, +6\}$ ausdehnt?

2. Löse die folgenden quadratischen Gleichungen (von Hand):
   (a) $x^2 + 3x - 22 \equiv 0 \pmod{97}$
   (b) $x^2 + 6x + 7 \equiv 0 \pmod{23}$
   (c) $x^2 - 13x - 1 \equiv 0 \pmod{59}$

3. Implementiere den Algorithmus zum Wurzelziehen $\bmod p$ in MAPLE und löse die folgenden quadratischen Gleichungen:
   (a) $x^2 - 1207x + 665 \equiv 0 \pmod{3581}$
   (b) $x^2 + 1180x - 94 \equiv 0 \pmod{2833}$
   (c) $x^2 + 497x + 2431 \equiv 0 \pmod{5273}$
   (d) $x^2 - 3996x + 1475 \equiv 0 \pmod{9547}$