Übungen zur Vorlesung Kryptographie

Abt. Reine Mathematik SS 06 – Blatt 4

Abgabetermin: Fr., 02.06.2006 um 12:30 Uhr vor Beginn der Übung

---

1. Der Ursprung des Chinesischen Restsatzes:
   Im Handbuch der Arithmetik des Chinesen Sun-Tzun Suan-Ching, der vor ca. 2000 Jahren gelebt hat, steht folgende Aufgabe:

   > "Es soll eine Anzahl von Dingen gewählt werden. Zählt man sie zu je drei, dann bleiben zwei übrig. Zählt man sie zu je fünf, dann bleiben drei übrig. Zählt man sie zu je sieben, dann bleiben zwei übrig. Wie viele sind es?"

   Wir interessieren uns für die kleinste positive Lösung dieses Problems.

2. Löse die folgenden Systeme von Kongruenzen:

   (a)

   $$\begin{aligned} x &\equiv -1 \pmod 3 \\ x &\equiv -1 \pmod 4 \\ x &\equiv -1 \pmod 5 \\ x &\equiv -1 \pmod 6 \end{aligned}$$

   (b)

   $$\begin{aligned} x &\equiv 2 \pmod 3 \\ x &\equiv 1 \pmod 5 \\ x &\equiv 5 \pmod 2 \end{aligned}$$

3. Finde $x \in \mathbb{N}$ mit $17^x \equiv -2 \pmod{35}$.

4. Betrachte das Polynom $f(X) := X^2 + X + 1$ über $\mathbb{F}_2$. Sei $\alpha \in \mathbb{F}_4$ eine Nullstelle von f.

   (a) Zeige: $\alpha + 1$ ist ebenfalls Nullstelle von f.

   (b) Wir betrachten die Fibonacci-Folge $a_{n+2} := a_{n+1} + a_n$ mit $a_0 := a_1 := 1$, $a_i \in \mathbb{F}_2$. Finde $c_1, c_2 \in \mathbb{F}_4$ mit $a_i := c_1 \cdot \alpha^i + c_2 \cdot (\alpha + 1)^i$ für alle $i \in \mathbb{N}$.
   Löse die Aufgabe zunächst für $i = 0, 1$ und verifiziere das Ergebnis für $i = 2, 3, 4$