Geheime Botschaften

Sommersemester 2017

Dr. T. Moede
t.moede@tu-bs.de
Universitätsplatz 2, Raum 426
0531 391-7527

Technische Universität Braunschweig

Übungsblatt 7

Wir wollen mit $\mathbb{Z}_p$ die Menge $\{0, \ldots, p-1\}$ bezeichnen. Außerdem sei $\mathbb{Z}_p^* = \mathbb{Z}_p \setminus \{0\}$.

Aufgabe 1. (Quadratische Reste modulo p)
Sei p eine ungerade Primzahl und betrachte auf $\mathbb{Z}_p^*$ die Multiplikation modulo p.

a) Berechnen Sie für $p \in \{3, 5, 7\}$ die Menge der **quadratischen Reste modulo p**, d.h. jeweils die Menge $R_p = \{x^2 \mid x \in \mathbb{Z}_p^*\}$.

b) Geben Sie eine Vermutung für die Anzahl der Elemente in der Menge R_p in Abhängigkeit von p. Begründen Sie Ihre Vermutung.

c) Berechnen Sie für $p \in \{3, 5, 7\}$ und $a \in \mathbb{Z}_p^*$ die Elemente

$$a^{|R_p|}.$$

d) Formulieren Sie eine Vermutung, wie Sie entscheiden können, ob eine Zahl modulo p betrachtet ein Quadrat ist. Um Ihre Vermutung zu beweisen, dürfen Sie eine Variante des **kleinen Satzes von Fermat** verwenden: Es gilt für alle $a \in \mathbb{Z}_p^*$:

$$a^{p-1} = 1.$$

Aufgabe 2. (Modulare Quadratwurzeln & Chinesischer Restsatz I)

a) Für Primzahlen p mit $p \equiv 3 \mod 4$ ist die Berechnung der modularen Quadratwurzeln einer Zahl $a \in R_p$ besonders einfach. Zeigen Sie, dass für solches p und a die modularen Quadratwurzeln gerade gegeben sind durch $\pm a^{\frac{p+1}{4}}$.

   (Für $p \equiv 1 \mod 4$ gibt es z.B. den **Shanks-Tonelli-Algorithmus**, den wir in der Vorlesung betrachten werden.)

b) Betrachten Sie die **simultanen Kongruenzen**

$$\begin{aligned} x &\equiv a_1 \mod m_1, \\ x &\equiv a_2 \mod m_2. \end{aligned}$$

   Zeigen Sie: Für $r, s \in \mathbb{Z}$ mit $rm_1 + sm_2 = 1$ ist

$$x = a_1 s m_2 + a_2 r m_1$$

   eine Lösung der simultanen Kongruenzen. Solche Zahlen r, s können Sie beispielsweise mit dem erweiterten euklidischen Algorithmus berechnen.

c) Berechnen Sie eine Lösung der simultanen Kongruenzen

$$\begin{aligned} x &\equiv 27 \mod 29, \\ x &\equiv 3 \mod 5. \end{aligned}$$