Geheime Botschaften

Sommersemester 2017

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

Technische Universität Braunschweig

Übungsblatt 8

Aufgabe 1. (Euklidischer Algorithmus I)
Seien $a, b, q \in \mathbb{Z}$ und sei $a = qb + r$ mit $0 < r < |b|$. Zeigen Sie, dass dann

$$ggT(a, b) = ggT(b, r)$$

gilt.

Aufgabe 2. (Modulare Quadratwurzeln & Chinesischer Restsatz II)

- Sei $n = pq$ für zwei verschiedene, ungerade Primzahlen p und q. Überlegen Sie sich, wie Sie aus den Quadratwurzeln modulo p bzw. q die Quadratwurzeln modulo n konstruieren können. Verwenden Sie hierzu den **Chinesischen Restsatz** für jeweils zwei simultane Kongruenzen.

  Zur Erinnerung:

  Für die **simultanen Kongruenzen**

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

  und $r, s \in \mathbb{Z}$ mit $rm_1 + sm_2 = 1$ ist

  $$x = a_1 sm_2 + a_2 rm_1$$

  eine Lösung.

- Berechnen Sie mit diesem Ansatz die Quadratwurzeln von 16 modulo $21 = 3 \cdot 7$.

Aufgabe 3. (Modulare Quadratwurzeln & Primfaktorzerlegung)

Wieder sei $n = pq$ für ungerade Primzahlen $p \neq q$. Zeigen Sie: Die Berechnung der Quadratwurzeln modulo n ist äquivalent zur Berechnung der Primfaktorzerlegung von n, d.h. überlegen Sie sich:

- Wenn Sie die Primfaktorzerlegung von n kennen, dann können Sie die Quadratwurzeln modulo n effizient bestimmen.
- Wenn Sie die Quadratwurzeln modulo n kennen, dann können Sie die Primfaktoren von n effizient bestimmen.

(Gehen Sie davon aus, dass der euklidische Algorithmus und der Shanks-Tonelli-Algorithmus effizient sind.)