Mathematische Methoden in der Kommunikationstheorie

(Sommersemester 2018)

Dr. Tobias Moede
t.moede@tu-bs.de
Universitätsplatz 2, Raum 515
0531 391-7516

Alexander Cant, M.Sc.
a.cant@tu-bs.de
Universitätsplatz 2, Raum 515
0531 391-7516

Technische Universität Braunschweig

Übungsblatt 2

(Abgabe: 17.04.2018 in der VL)

Aufgabe 1. (Chinesischer Restsatz I)
Beweisen Sie den **chinesischen Restsatz**:
Seien $n_1, \ldots, n_k \in \mathbb{N}$ paarweise teilerfremd und $c_1, \ldots, c_k \in \mathbb{Z}$ vorgegeben. Dann existiert eine Zahl $x \in \mathbb{Z}$, welche die Kongruenzen

$$\begin{aligned} x &\equiv c_1 \mod n_1 \\ &\vdots \\ x &\equiv c_k \mod n_k \end{aligned}$$

erfüllt. Die Restklasse $x \bmod n_1 \cdots n_k$ ist eindeutig bestimmt.

Aufgabe 2. (Chinesischer Restsatz II)
Bestimmen Sie eine Lösung $x \in \mathbb{Z}$ für das folgende System von Kongruenzen.

$$\begin{aligned} x &\equiv 3 \mod 5 \\ x &\equiv 8 \mod 11 \\ x &\equiv 7 \mod 12 \end{aligned}$$

Aufgabe 3. (Eulersche φ-Funktion I)
Seien $m, n \in \mathbb{N}$ teilerfremd. Zeigen Sie, dass $\varphi(mn) = \varphi(m)\varphi(n)$ gilt.

Aufgabe 4. (Eulersche φ-Funktion II)
Bestimmen Sie $\varphi(537432)$ und $\varphi(928811)$.

Präsenzaufgabe 5. ($\varphi(n)$ und Faktorisierung von n)
Wenn Sie im RSA-Verfahren die Faktorisierung von n als $n = pq$ kennen, so können Sie leicht $\varphi(n) = (p-1)(q-1)$ berechnen. Zeigen Sie umgekehrt: Wenn Sie n und $\varphi(n)$ kennen, so können Sie daraus leicht p und q bestimmen (ohne vorher n zu faktorisieren).

Präsenzaufgabe 6. ($\varphi(n)$ und Teiler von n)
Zeigen Sie:

$$\sum_{d|n} \varphi(d) = n.$$