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 3

(Abgabe: 24.04.2018 in der VL)

Aufgabe 1. (Modulare Inverse)
Berechnen Sie - falls existent - die folgenden modularen Inversen mit Hilfe des erweiterten Euklidischen Algorithmus.

a) Das Inverse von 7 in $\mathbb{Z}_{180}$.

b) Das Inverse von 63 in $\mathbb{Z}_{180}$.

Aufgabe 2. (RSA-Entschlüsselung)
Sie erhalten die verschlüsselte Nachricht $c = 67$. Es wurde das RSA-Verfahren mit dem öffentlichen Schlüssel $(e, n) = (7, 209)$ verwendet. Entschlüsseln Sie die Nachricht.

Aufgabe 3. (Fermat-Zahlen)
Für eine natürliche Zahl n ist die $\boldsymbol{n}$*-te Fermat-Zahl* definiert als

$$F_n = 2^{2^n} + 1.$$

Berechnen Sie zunächst die ersten sechs Fermat-Zahlen $F_0, \ldots, F_5$. Beweisen Sie dann die folgenden Aussagen:

a) Für alle $x, y \in \mathbb{Z}$ und $m \in \mathbb{N}$ gilt, dass $x - y$ die Zahl $x^m - y^m$ teilt.

b) Wenn für $k \in \mathbb{N}$ die Zahl $2^k + 1$ eine Primzahl ist, dann ist $k = 2^r$ für ein $r \in \mathbb{N}$.

c) Überlegen Sie sich Gründe, warum oft die Zahl F_4 als Exponent e im RSA-Verfahren gewählt wird.

*d) Beweisen oder widerlegen Sie, dass F_n für alle $n \geq 5$ zusammengesetzt, d.h. keine Primzahl, ist. Aktuell ist für 292 Fermat-Zahlen bekannt, dass es sich um zusammengesetzte Zahlen handelt. Komplett faktorisiert sind bisher nur $F_5, \ldots, F_{11}$.

Aufgabe 4. (RSA-Fixpunkte)

a) Sei $n = pq$ für zwei verschiedene, ungerade Primzahlen p und q. Weiter sei e invertierbar modulo $\varphi(n)$. Zeigen Sie, dass es in $\mathbb{Z}_n$ genau

$$(1 + ggT(e-1, p-1))(1 + ggT(e-1, q-1))$$

Fixpunkte des Potenzierens mit e, d.h. Elemente $m \in \mathbb{Z}_n$ mit

$$m^e \equiv m \bmod n$$

gibt.

Hinweis: Für eine Primzahl p hat die Gleichung $x^n = 1$ genau $ggT(n, p-1)$ Lösungen in $\mathbb{Z}_p$. Erinnern Sie sich außerdem an das „Zusammensetzen“ von Lösungen mit Hilfe des Chinesischen Restsatzes.

b) Überlegen Sie sich, dass jedes RSA-System mindestens 9 Fixpunkte besitzt.