Universität Kassel
Fachbereich 10/16
Peter Dräxler

Wintersemester 2014/15
Blatt 10
14.01.2015

Übungen zur Vorlesung Diskrete Strukturen II

Aufgaben 1) und 2) sind relevant für den Scheinerwerb.

Aufgabe 1. Um sich mit dem RSA-Verfahren verschlüsselte Nachrichten schicken lassen zu können, hat Alice zwei ungerade Primzahlen $p \neq q$ gewählt und $n = pq$ berechnet. Des weiteren hat sie zwei Zahlen $e, d \in \{2, \cdots, \varphi(n) - 1\}$ mit $ed \equiv 1 \bmod \varphi(n)$ gewählt. Sie hat $n = 65$ und $e = 7$ öffentlich gemacht.

a) Die Nachricht $\overline{m} = \overline{2} \in \mathbf{Z}/65$ soll von Bob an Alice übermittelt werden. Was ist die Verschlüsselung von $\overline{m}$?

b) Der RSA-Modul $n = 65$ ist natürlich viel zu klein, um Sicherheit zu bieten. Faktorisieren Sie n und finden Sie den geheimen Entschlüsselungsexponenten d von Alice.

c) Was fällt Ihnen an d, e auf, das man in der Praxis tunlichst vermeiden sollte?

Aufgabe 2. Eine natürliche Zahl $n \geq 2$ heißt *Carmichael-Zahl*, wenn n keine Primzahl ist und $a^{n-1} \equiv 1 \bmod n$ für alle $a \in \{2, \cdots, n-1\}$ mit $\mathrm{ggT}(a, n) = 1$ gilt.

a) Sei $s \in \mathbf{N}$ mit $s > 1$, seien $p_1, \cdots, p_s$ verschiedene Primzahlen und sei $n = p_1 \cdots p_s$. Beweisen Sie: Wenn für alle $i \in \{1, \cdots, s\}$ die Zahl $n - 1$ durch $p_i - 1$ teilbar ist, dann ist n eine Carmichael-Zahl.

b) Entscheiden Sie mit Hilfe von a), ob 561, 1001 und 1105 Carmichael-Zahlen sind.

Aufgabe 3. Es sei $n \in \mathbf{N}$. Zeigen Sie: Ist $2^n + 1$ eine Primzahl, so gibt es $k \in \mathbf{N}_0$ mit $n = 2^k$.

Aufgabe 4. Seien $p \neq q$ ungerade Primzahlen, $n = pq$ und l das kleinste gemeinsame Vielfache von $p - 1$ und $q - 1$. Sei $e, d \in \{2, \cdots, n-1\}$ mit $ed \equiv 1 \bmod l$. Zeigen Sie: Es gilt $m^{ed} \equiv m \bmod n$ für alle $m \in \mathbf{Z}$.
Hinweis: Beweisen Sie zunächst, dass $m^{ed} \equiv m \bmod p$ und $m^{ed} \equiv m \bmod q$ für alle $m \in \mathbf{Z}$ gilt.
Bemerkung: Dies zeigt, daß man bei RSA konsequent $\varphi(n)$ durch l ersetzen darf.

Abgabe: Die Lösungen müssen am Mittwoch, 21.01.2015 spätestens bis 08:15 Uhr abgegeben werden.