TECHNISCHE UNIVERSITÄT KAISERSLAUTERN

Prof. Dr. Mathias Schulze
Dipl.-Math. Cornelia Rottner
Fachbereich Mathematik

Mathematik für Informatiker: Algebraische Strukturen

Sommersemester 2015 - Übungsblatt 8

Abgabetermin: 22.6.2015, 9:45h

Aufgabe 1. Seien $a, b \in \mathbb{Z} \setminus (\{0\} \cup \mathbb{Z}^*)$. Wir nennen eine Primzahl p Primfaktor von a falls a von p geteilt wird.

(a) Beschreiben Sie $\mathrm{ggT}(a, b)$ und $\mathrm{kgV}(a, b)$ mittels Primfaktorzerlegung.

(b) Zeigen Sie:

$$\mathrm{ggT}(a, b) \ni 1 \Leftrightarrow a \text{ und } b \text{ haben keine gemeinsamen Primfaktoren}$$

Aufgabe 2. (Diffie-Hellmann-Schlüsselaustausch) Alice und Bob möchten geheime Nachrichten austauschen. Da sie Angst haben, dass ihre Nachrichten mitgelesen werden, kreieren sie dazu einen geheimen Schlüssel. Dafür nutzen Sie eine öffentlich bekannte zyklische Gruppe G der Ordnung p und einen (ebenfalls öffentlich bekannten) Erzeuger g von G. Nun gehen sie folgendermaßen vor:

(i) Alice wählt (geheim) eine natürliche Zahl a und Bob wählt (geheim) eine natürliche Zahl b mit $1 \leq a, b \leq p - 1$.

(ii) Alice berechnet g^a und Bob berechnet g^b. Das Ergebnis schicken sie jeweils dem anderen.

(iii) Alice berechnet $(g^b)^a = g^{ab}$, Bob berechnet $(g^b)^a = g^{ba}$, diese Zahl $g^{ab} = g^{ba}$ ist nun ihr geheimer Schlüssel.

Sei $G = \mathbb{Z}/77\mathbb{Z}$ mit Erzeuger $g = \overline{23}$ die öffentlich bekannte zyklische Gruppe. Alice schickt Bob die Nachricht $\overline{75}$ und Bob schickt Alice die Nachricht $\overline{68}$. Wie lautet der gemeinsame Schlüssel von Alice und Bob?
Hinweis: Legen Sie Ihren Lösungsweg dar. Lösungen durch ausprobieren werden nicht akzeptiert.

Aufgabe 3. Seien $p, q \in \mathbb{Z}_{\geq 2}$ zwei verschiedene Primzahlen, $n := pq$ und $r = (p-1)(q-1)$. Weiterhin sei $c \in \mathbb{N}$ mit $c \equiv 1 \mod r$ und $m \in \mathbb{Z}$. Zeigen Sie:

(a) Es gilt $|\mathbb{Z}/p\mathbb{Z}^*| = p - 1$.

(b) Es gilt $|\mathbb{Z}/n\mathbb{Z}^*| = (p-1)(q-1)$.

(c) Es gilt $m^c \equiv m \mod n$.
Hinweis: Zeigen Sie zunächst $m^c \equiv m \mod p$ *und* $m^c \equiv m \mod q$.

Aufgabe 4. (RSA-Verfahren)
Wir nehmen an, dass Bob die Zahl $m \in \mathbb{N}_{>0}$ verschlüsselt an Alice verschicken will. Alice weiß, dass Bobs Nachricht kleiner als ein bestimmtes $N \in \mathbb{N}$ ist. Für den Nachrichtenaustausch kreiert Alice einen öffentlichen und einen geheimen Schlüssel (RSA-Schlüsselerzeugung):

(i) Alice wählt zwei verschiedene positive Primzahlen p, q (geheim), sodass $pq > N$. Sie berechnet $n = pq$ und $r = (p-1)(q-1)$.

Prof. Dr. Mathias Schulze
Dipl.-Math. Cornelia Rottner
Fachbereich Mathematik

(ii) Sie wählt ein $e \in \mathbb{N}$ mit $1 \in \mathrm{ggT}(e, r)$.

(iii) Mithilfe des euklidischen Algorithmus berechnet sie $0 < d < r$, sodass $\overline{d}$ das Inverse von $\overline{e}$ in $\mathbb{Z}/r\mathbb{Z}$ ist.

(iv) Alice veröffentlicht nun n und e und hält d geheim.

Nun kann Bob Alice seine Nachricht m verschlüsselt übermitteln (RSA-Nachrichtenaustausch): Bob berechnet $\overline{m}^e$ in $\mathbb{Z}/n\mathbb{Z}$ und schickt Alice das Ergebnis. Wie kann Alice das Ergebnis entschlüsseln?