TECHNISCHE UNIVERSITÄT KAISERSLAUTERN

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

Mathematik für Informatiker: Algebraische Strukturen

Wintersemester 2016 - Übungsblatt 8

Abgabetermin: 6.1.2017, 8:15h

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 der Primfaktorzerlegungen von a und b.

(b) Zeigen Sie:

$$\mathrm{ggT}(a, b) \ni 1 \Leftrightarrow a \text{ und } b \text{ haben keinen gemeinsamen Primfaktor.}$$

Insbesondere beweist diese Aufgabe also Bemarkung 10.9.

Aufgabe 2. Bestimmen Sie alle Lösungen des Kongruenzgleichungssystems:

$$\begin{aligned} x &\equiv 5 \pmod 6 \\ x &\equiv -3 \pmod 7 \\ x &\equiv 2 \pmod{11} \end{aligned}$$

Hinweis: Legen Sie Ihren Lösungsweg dar. Lösungen und Zwischenergebnisse durch Ausprobieren werden nicht akzeptiert.

Aufgabe 3. Bob möchte Alice eine Zahl $N \in \mathbb{N}_{>0}$ mit $N < 3000$ mittels des RSA-Verfahrens verschlüsselt übermitteln. Alice wählt hierzu im Geheimen die beiden Primzahlen $p = 53$ und $q = 71$.

(a) Bestimmen Sie für Alice einen geeigneten geheimen Schlüssel sowie den zugehörigen öffentlichen Schlüssel.

(b) Alice veröffentlicht nun den öffentlichen Schlüssel. Dann verschlüsselt Bob die geheime Nachricht $N = 2017$ mithilfe dieses Schlüssels und sendet die verschlüsselte Nachricht an Alice. Wie berechnet Bob die verschlüsselte Nachricht? Welche Nachricht erhält Alice? Wie kann Alice diese entschlüsseln?

Aufgabe 4. (Präsenzaufgabe) 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 n 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 $1 < a, b \leq n - 1$.

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

(iii) Alice und Bob berechnen nun ihren gemeinsamen geheimen Schlüssel g^{ab}: Alice berechnet $(g^b)^a = g^{ab}$, Bob berechnet $(g^b)^a = g^{ba}$.

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?