TECHNISCHE UNIVERSITÄT DRESDEN

Fakultät Mathematik und Naturwissenschaften Fachrichtung Mathematik, Institut für Algebra

Prof. U. Baumann, Dr. C. Zschalig

Algebra für Informationssystemtechniker (Modul ET - 01 04 04), Sommersemester 2015

8. Übungsblatt für die Übung am 14.4.2015

Restklassenringe, RSA

Ü43. In dieser Aufgabe betrachten wir den Restklassenring $\underline{\mathbb{Z}_6}$. Stellen Sie die Operationstafeln für die Addition und für die Multiplikation auf. Welche Elemente besitzen ein Inverses bezüglich der Multiplikation?
Geben Sie analog die Operationstafeln für Addition und Multiplikation im Restklassenring $\underline{\mathbb{Z}_7}$ an.

+	0	1	2	3	4	5
0						
1						
2						
3						
4						
5						

Hinweis: In eine Operationstafel einer Menge M mit Operation $\circ$ werden alle möglichen Summen bzw. Produkte der Elemente aus M eingetragen. Rechts ein Beispiel der Operationstafel für $\mathbb{Z}_6$ mit der Addition (mod 6).

Ü44. Zum Verschlüsseln eines Textes verwenden wir das RSA-Verfahren. Wir codieren die Buchstaben $\mathrm{A}, \mathrm{B}, \ldots, \mathrm{Z}$ durch die Zahlen $0, 1, \ldots, 25$.

(a) Verschlüsseln Sie den Klartext `GEHEIM` mit dem öffentlichen Schlüssel

(i) $(n, e) = (33, 3)$, (ii) $(n, e) = (15, 5)$

(b) Zeigen Sie, dass $e = \frac{1}{2}\varphi(n) + 1$ eine schlechte Wahl für den öffentlichen Schlüssel ist, da dann jeder Buchstabe auf sich selbst abgebildet wird.

Ü45. Alice hat Ben eine RSA-verschlüsselte Nachricht geschickt. Eva hat die Nachricht `QUTCIM` mitgehört (die Buchstaben sind wie in Ü44 durch Zahlen codiert). Außerdem kennt sie den öffentlichen Schlüssel $(21, 5)$ von Ben. Wie kann Eva die Nachricht entschlüsseln? Wie lautet die gesendete Nachricht?

A46. **Hausaufgabe, bitte vor Beginn der nächsten Übung unter Angabe von Name, Matrikelnr. und Übungsgruppe abgeben.**

(a) Verschlüsseln Sie Ihren Nachnamen mit dem RSA-Verfahren mit dem öffentlichen Schlüssel $(n, e) = (33, 13)$. Führen Sie dazu folgende Schritte aus:

(i) Codieren Sie die Buchstaben $A_1, \ldots, A_n$ Ihres Nachnamens durch Zahlen $m_1, \ldots, m_n$ ($A \to 2, B \to 3, \ldots, Z \to 27, \ddot{A} \to 28, \ddot{O} \to 29, \ddot{U} \to 30, ß \to 31$).

(ii) Bestimmen Sie zu jedem Klartextbuchstaben m_i den Schlüsseltextbuchstaben c_i. *Bewertet wird die sorgfältige Formulierung des Lösungsweges, nicht nur das Ergebnis.*

(b) Bestimmen Sie den privaten Schlüssel d mit Hilfe des erweiterten Euklidischen Algorithmus und entschlüsseln Sie den entstandenen Schlüsseltext.

H47. Von der Zahl 14803 ist bekannt, dass sie Produkt von genau zwei Primzahlen ist und dass $\varphi(14803) = 14560$ gilt. Wie können mit diesen Informationen die Primfaktoren von 14803 bestimmt werden?

H48. Es sei $n \in \mathbb{N}$ und $\underline{\mathbb{Z}_n}$ der Restklassenring bezüglich n.

(a) Für welche n ist jedes Element $a \in \mathbb{Z}_n \setminus \{0\}$ eine Einheit?

(b) Beweisen oder widerlegen Sie: Das Produkt von zwei Einheiten ist wieder eine Einheit.

(c) Beweisen oder widerlegen Sie: Die Summe von zwei Einheiten ist wieder eine Einheit.

(d) Beweisen oder widerlegen Sie: Ist a eine Einheit, dann ist auch $n - a$ eine Einheit.