TECHNISCHE UNIVERSITÄT DRESDEN

Bereich Mathematik und Naturwissenschaften Fakultat Mathematik, Institut fur Algebra

Dr. E. Lehtonen, Dr. C. Zschalig

Algebra und Zahlentheorie für Lehramt (Modul ALGZTH), Sommersemester 2018

7. Übungsblatt für die Übungen vom 28.5.-1.6.2018

Anwendungen der Modulrechnung

Ein wesentliches Kriterium bei der Präsentation der folgenden Themen ist die Interaktion. Ziel ist es, die Probleme gemeinsam mit dem Auditorium zu erarbeiten und nicht frontal zu vermitteln. Setzen Sie dabei - falls die limitierte Zeit dazu ausreicht - Lerntechniken ein, die Sie im Studium kennengelernt haben. Die Vortragsdauer ist strikt auf 12 Minuten beschränkt.

T7.1 **Themenaufgabe: Das Square & Multiply-Verfahren**

Stellen Sie das Square & Multiply-Verfahren zur schnellen Berechnung hoher Potenzen (mod n) vor. Erklären Sie, wie das Verfahren durch die Sätze von Euler und Fermat beschleunigt werden kann. Nutzen Sie Beispiele zur Verdeutlichung.

T7.2 **Themenaufgabe: Diffie-Hellman-Schlüsselaustauch**

Erläutern Sie Nutzen und Wirkungsweise des o.g. Verfahrens. Rechnen Sie ein Beispiel mit kleinen Zahlen. Worauf beruht die Sicherheit dieses Kryptosystems?

Ü7.3 (a) Berechnen Sie zu den folgenden natürlichen Zahlen n den Wert $\varphi(n)$ der Eulerschen Funktion.

(i) $n = 30$, (ii) $n = 60$, (iii) $n = 100$, (iv) $n = 2520$.

(b) Beweisen Sie: Gilt $n = pq$ für zwei Primzahlen p und q, dann folgt $\varphi(n) = (p-1)(q-1)$. Wie können p und q aus n und $\varphi(n)$ berechnet werden?

(c) Zeigen Sie: Ist n eine ungerade Zahl, dann gilt $\varphi(n) = \varphi(2n)$.

(d) Berechnen Sie die folgenden Potenzen. Benutzen Sie den Satz von Euler, falls möglich:

(i) $19^{289} \pmod{21}$, (ii) $13^{54} \pmod{32}$, (iii) $7^{27} \pmod{36}$, (iv) $15^{13} \pmod{18}$.

Ü7.4 Alice und Ben benutzen das RSA-Verfahren zur verschlüsselten Nachrichtenübermittlung.

(a) Der öffentliche Schlüssel von Alice lautet $(e, n) = (19, 77)$. Verschlüsseln Sie den Klartext $m = 9$.

(b) Der öffentliche Schlüssel von Ben lautet $(e, n) = (53, 77)$. Wie lauten die Primfaktoren p und q und sein privater Schlüssel d?

(c) Carla möchte ebenfalls Nachrichten mit Alice und Ben austauschen und dafür den öffentlichen Schlüssel $(e, n) = (16, 77)$ bereitstellen. Zeigen Sie, dass Carla dann eine Verschlüsselungsfunktion verwenden würde, die nicht injektiv ist.

(d) Begründen Sie, warum die Verschlüsselungsfunktion $E : \mathbb{Z}_n \to \mathbb{Z}_n$ mit $E(m) = m^e$ injektiv sein sollte.

Ü7.5 Lösen Sie folgende Systeme von Kongruenzen:

(a)
$$\begin{aligned} x &\equiv 2 \pmod 3 \\ x &\equiv 3 \pmod 5 \\ x &\equiv 2 \pmod 7 \end{aligned}$$

(b)
$$\begin{aligned} x &\equiv 4 \pmod 5 \\ x &\equiv 6 \pmod 7 \\ x &\equiv 9 \pmod{11} \end{aligned}$$

Führen Sie jeweils die Probe durch!

A7.6 **Hausaufgabe, Abgabe (mit Name und Matrikelnr.) bis 1.6.2018, 12:00 Uhr**

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

(i) Codieren Sie die Buchstaben $A_1, \ldots, A_n$ Ihres Nachnamens durch $m_1, \ldots, m_n \in \mathbb{Z}_{33}$ durch die Zuordnung $\mathrm{A} \to 2, \mathrm{B} \to 3, \ldots, \mathrm{Z} \to 27, \ddot{\mathrm{A}} \to 28, \ddot{\mathrm{O}} \to 29, \ddot{\mathrm{U}} \to 30, \mathrm{ß} \to 31$.

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

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

(b) Schreiben Sie Ihre Matrikelnummer auf. Die (von links gelesen) 5. Ziffer sei die Zahl a, die 6. Ziffer b und die 7. Ziffer c.

Bestimmen Sie die Lösungen des Kongruenzensystems

$$\begin{aligned} x &\equiv a \pmod 5 \\ x &\equiv b \pmod 6 \\ x &\equiv c \pmod 7 \end{aligned}$$

Die folgenden Selbststudiumsaufgaben dienen der Festigung und Vertiefung des Stoffes in der Nachbereitung der Lehrveranstaltung.

H7.7 Es war einmal eine Bande von 17 Piraten, die stahl einen Sack mit Goldstücken. Als sie ihre Beute in gleiche Teile teilen wollten, blieben 3 Goldstücke übrig. Beim Streit darüber, wer ein Goldstück mehr verdient habe, wurde ein Pirat erschlagen. Wieder wurde gleichmäßig verteilt, doch nun blieben dabei 10 Goldstücke übrig. Erneut kam es zu Streit und wieder verlor ein Seeräuber sein Leben. Da aber ließ sich endlich die Beute gleichmäßig verteilen. Wie viele Goldstücke waren mindestens im Sack?

H7.8 Wir betrachten das aus nur 6 Buchstaben bestehende Alphabet $\mathcal{A} = \{A, B, E, G, L, R\}$. Diesen Buchstaben werden in gleicher Reihenfolge die Zahlen $0, 1, \ldots, 5$ zugeordnet. Weiterhin seien f, g Abbildungen auf der Menge $\{0, 1, \ldots, 5\}$, die so definiert sind:

$$f(n) := (4n + 1) \mod 6 \qquad g(n) := (5n + 3) \mod 6.$$

(a) Verschlüsseln Sie das Wort G A B E L einmal mit der Funktion f und einmal mit g.

(b) Das Wort G R A B E L G ist das Ergebnis der Verschlüsselung mit g. Wie lautet das unverschlüsselte Wort? Kann das Originalwort auch angegeben werden, wenn die Verschlüsselung mit f erfolgt ist?

Hinweis: Solche Verschlüsselungen sind nach heutigen Maßstäben nicht sicher, wurden aber früher tatsächlich genutzt, siehe z.B. `http://de.wikipedia.org/wiki/Caesar-Verschlüsselung`.

H7.9 (a) Finden Sie alle natürlichen Zahlen $n \in \mathbb{N}$, für die gilt:

(i) $\varphi(n) = 2$, (ii) $\varphi(n) = 3$, (iii) $\varphi(n) = 4$, (iv) $\varphi(n) = 6$.

(b)* Für fast alle natürlichen Zahlen $n > 1$ gilt $\varphi(n) \geq \sqrt{n}$. Beweisen Sie diese Aussage und finden Sie die beiden Ausnahmen.

Hinweis: Betrachten Sie die Aussage zunächst für quadratfreie Zahlen, d.h. für solche Zahlen $n \in \mathbb{N}$, die nicht durch ein Quadrat $m^2 \in \mathbb{N} \setminus \{1\}$ teilbar sind.