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), Wintersemester 2014/15

6. Übungsblatt für die Übungen vom 12.1.-23.1.2015

Rechnen mod n

Ü31. (a) Berechnen Sie mit „Square & Multiply“: $11^{53} \pmod 8$, $7^{199} \pmod{11}$, $37^{25} \pmod{19}$.

(b) Bestimmen Sie die letzten beiden Ziffern von 2^{333}.

(c) Bestimmen Sie alle ganzen Zahlen x, für die gilt $6^x \equiv 11 \pmod{13}$.

Ü32. Alice und Bob wollen mit dem Diffie-Hellman-Verfahren einen geheimen Schlüssel erzeugen. Dabei einigen sie sich auf den Modul 101.

(a) Alice schickt an Bob die Zahl 53 (mit $2^a \equiv 53 \pmod{101}$). Bob verwendet $b = 65$. Wie lautet der gemeinsame Schlüssel?

(b) Bei einem neuerlichen Schlüsselaustausch lauscht Eva den gemeinsamen Kommunikationskanal ab. Dabei erfährt sie $2^a = 96 \pmod{101}$ und $2^b = 66 \pmod{101}$. Wie lauten der geheime Schlüssel von Alice und der geheime Schlüssel von Bob?

Ü33. Eine natürliche Zahl n ist genau dann durch 3 teilbar, wenn ihre Quersumme (in Dezimaldarstellung) durch 3 teilbar ist. Beweisen Sie diese Aussage.

Finden Sie ähnliche Teilbarkeitsregeln für die Division durch 9 und durch 11.

Hinweis: Eine Zahl mit der Ziffernfolge $\ldots a_2a_1a_0$ kann als $\ldots + 10^2 \cdot a_2 + 10^1 \cdot a_1 + 10^0 \cdot a_0$ geschrieben werden. Betrachten Sie diese Darstellung modulo 3, 9 bzw. 11.

A34. **Hausaufgabe, bitte vor Beginn der nächsten Übung unter Angabe von Name, Matrikelnr. und Übungsgruppe abgeben.**

(a) Bestimmen Sie mit square & multiply $7^{50} \pmod{17}$

(b) Beweisen Sie, dass für beliebige $a, b \in \mathbb{Z}$ die Gleichung $(a+b)^3 = a^3 + b^3 \pmod 3$ gilt. Wenden Sie die Formel an, um $28^3 \pmod 3$ zu bestimmen.

H35. 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`.

H36. (a) Beweisen Sie: Eine (im gewöhnlichen Dezimalsystem) fünfstellige Zahl der Form *abcad* ist genau dann durch 7 teilbar, wenn $2c - b + d$ durch 7 teilbar ist.

(b) Wie lautet die Teilbarkeitsbedingung für beliebige fünfstellige Zahlen, also Dezimalzahlen der Form *uvwxy*?