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 2015/16

6. Übungsblatt für die Übung am 18.1.2016

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. (a) Besitzen die folgenden Elemente x ein Inverses in $\mathbb{Z}_n$? Berechnen Sie ggf. das Inverse $x^{-1} \pmod n$.

(i) $x=18, n=31$, (ii) $x=60, n=257$, (iii) $x=511, n=1001$, (iv) $x=512, n=1001$.

(b) Geben Sie die Lösungsmengen der folgenden Gleichungen an!

(i) $5x \equiv 1 \pmod 7$ (ii) $10x \equiv 9 \pmod{25}$ (iii) $32x \equiv 14 \pmod{82}$

Hinweis zu (iii): Es gibt eine Regel zur Modulo-Rechnung, mit deren Hilfe die Gleichung geeignet umgeformt werden kann!

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

(a) Bestimmen Sie mit square & multiply $7^{58} \pmod{19}$

(b) Bestimmen Sie alle Lösungen der Gleichung $143x \equiv 1001 \pmod{231}$.

H35. (a) Geben Sie alle zu 8 teilerfremden natürlichen Zahlen aus der Menge $\{0, \ldots, 7\}$ an. Wie viele Zahlen in $\mathbb{Z}_{80}$ sind zu 80 teilerfremd?

(b) Berechnen Sie - falls existent - mit dem erweiterten Euklidischen Algorithmus die multiplikativen Inversen zu $a = 33$, $b = 34$ und $c = 35$ in $\mathbb{Z}_{80}$.

(c) Berechnen Sie alle Lösungen der Gleichung $33x = 15$ in $\mathbb{Z}_{80}$.

(d) Gesucht ist jeweils die Anzahl der Lösungen der Gleichungen $11x = 5$ und $66x = 30$ in $\mathbb{Z}_{80}$.

H36. 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 $\ldots a_2 a_1 a_0$ 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.