TECHNISCHE UNIVERSITÄT DRESDEN

Fakultät Mathematik und Naturwissenschaften, Fachrichtung Mathematik, Institut für Algebra

Prof. Ulrike Baumann, Henri Mühle Wintersemester 2017/18

6. Übungsblatt zur Vorlesung "Algebra für Informationssystemtechniker"

Teilbarkeit, Diskrete Logarithmen

Ü31. Eine natürliche Zahl ist genau dann durch drei teilbar, wenn ihre Quersumme durch drei teilbar ist. Beweisen Sie diese Aussage.

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

Hinweis: Eine Zahl mit Ziffernfolge $\ldots a_2a_1a_0$ kann als $\ldots + 10^2 \cdot a_2 + 10^1 \cdot a_1 + 10^0 a_0$ dargestellt werden.

Ü32. (a) Berechnen Sie mit "Square & Multiply" die folgenden Ausdrücke:

$$\text{(i) } 11^{53} \pmod 8, \quad \text{(ii) } 7^{199} \pmod{11}, \quad \text{(iii) } 37^{25} \pmod{19}.$$

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

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

Ü33. Zwei Personen wollen mit dem Diffie-Hellman-Verfahren einen geheimen Schlüssel erzeugen. Dabei einigen sie sich auf den Modul 101 und die Basis 2.

(a) Person A schickt an Person B die Zahl 53 (es gilt also $2^a \equiv 53 \pmod{101}$). Person B verwendet $b = 65$. Wie lautet der gemeinsame Schlüssel?

(b) Bei einem erneuten Schlüsselaustausch wird der gemeinsame Kommunikationskanal belauscht. Dabei werden $2^a \equiv 96 \pmod{101}$ und $2^b \equiv 66 \pmod{101}$ abgehört. Wie lauten der geheime Schlüssel von Person A und der geheime Schlüssel von Person B?

A34. **Hausaufgabe, bitte vor Beginn der 7. Übung unter Angabe von Name, Matrikelnummer und Seminargruppe abgeben.**
Erzeugen Sie erneut mit Hilfe Ihrer Matrikelnummer die Zahlen x und y aus Aufgabe A28.

(a) Berechnen Sie die Werte $\varphi(x)$ und $\varphi(y)$ der Eulerschen φ-Funktion von x und y.

(b) Berechnen Sie den Ausdruck $x^y \pmod{101}$ mit "Square & Multiply". Vereinfachen Sie dazu den Ausdruck zunächst mit Hilfe der bekannten Homomorphieregeln und des Satzes von Euler-Fermat.

H35. Von der Zahl 14803 ist bekannt, dass sie das Produkt von genau zwei Primzahlen ist, und dass $\varphi(14803) = 14560$ gilt. Wie können Sie mit diesen Informationen die Primfaktoren von 14803 bestimmen?

H36. (a) Zeigen Sie, dass eine (im gewöhnlichen Dezimalsystem) fünfstellige Zahl der Form *abcad* genau dann durch sieben teilbar ist, wenn $2c - b + d$ durch sieben teilbar ist.

(b) Wie lautet die Bedingung an die Teilbarkeit durch sieben für beliebige fünfstellige Zahlen, also Dezimalzahlen der Form *uvwxy*?