



9. Übungsblatt zur Vorlesung "Diskrete Strukturen für Informatiker"

Modulare Arithmetik

V. Die *Dezimaldarstellung* von $n \in \mathbb{N}$ ist das eindeutig bestimmte Tupel (n_0, n_1, \dots, n_k) , mit $0 \leq n_i \leq 9$ für alle i , sodass $n = \sum_{i=0}^k n_i 10^i$ und $n_k \neq 0$ gilt. Die *alternierende Quersumme* von n ist dann $\text{aq}(n) = \sum_{i=0}^k (-1)^i n_i$.

- (a) Bestimmen Sie $\text{aq}(924)$ und $\text{aq}(2143)$.
(b) Zeigen Sie, dass n genau dann durch elf teilbar ist, wenn $\text{aq}(n)$ durch elf teilbar ist.

Ü49. (a) Berechnen Sie für die folgenden Elemente $x \in \mathbb{Z}_n$ jeweils das multiplikative Inverse modulo n , falls es existiert.

- (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 Kongruenzen an.

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

Hinweis: Es gibt eine Regel zur Modulo-Rechnung, mit deren Hilfe die Kongruenz in (ii) geeignet umgeformt werden kann.

Ü50. Seien $a, b, n \in \mathbb{N}$. Um $a^b \pmod{n}$ zu berechnen, bietet sich der folgende *Square-and-Multiply-Algorithmus* an.

Zuerst berechnet man die *Binärdarstellung* von b , also das eindeutig bestimmte Tupel (b_0, b_1, \dots, b_k) mit $b_i \in \{0, 1\}$ für alle i , sodass $b = \sum_{i=0}^k b_i 2^i$ und $b_k = 1$ gilt. Anschließend initialisiert man $c_{k+1} = 1$ und führt für i von k bis 0 (absteigend) die Rekursion $c_i = c_{i+1}^2 a^{b_i} \pmod{n}$ aus. Der letzte berechnete Wert c_0 erfüllt dann $c_0 \equiv a^b \pmod{n}$.

(a) Berechnen Sie mit Hilfe dieses Algorithmus die folgenden Potenzen.

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

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

Ü51. Es sei $p \in \mathbb{N}$ eine Primzahl. Die *Logarithmentafel* zu $x \in \mathbb{Z}_p$ ist die Tabelle, die für $i \in \{1, 2, \dots, p-1\}$ in der i -ten Zeile die Werte i und $x^i \pmod{p}$ enthält. Die Zahl x ist *primitiv*, wenn $x^i \not\equiv 1 \pmod{p}$ für alle $i \in \{1, 2, \dots, p-2\}$ gilt.

- (a) Stellen Sie für 2, 3, und 6 die Logarithmentafeln in \mathbb{Z}_{11} auf, und schlussfolgern Sie, welche dieser Zahlen primitiv sind.
- (b) Berechnen Sie unter Ausnutzung der Ergebnisse aus (a) die folgenden Werte in \mathbb{Z}_{11} .

$$(i) \ 2^{35} - 2^{21}, \quad (ii) \ \frac{1}{6^5}, \quad (iii) \ \frac{3}{7}, \quad (iv) \ 17^{457}, \quad (v) \ 9^{-1}.$$

A52. **Hausaufgabe, bitte vor Beginn der 10. Übung (oder im Lernraum) unter Angabe von Name, Matrikelnummer, Übungsgruppe und Übungsleiter abgeben.**

Erzeugen Sie erneut mit Hilfe Ihrer Matrikelnummer die Zahlen x und y wie in Aufgabe A40.

- (a) Berechnen Sie jeweils das multiplikativ Inverse von x und y modulo 101, falls es existiert.
- (b) Berechnen Sie $x^y \pmod{\varphi(101)} \pmod{101}$ mittels Square-and-Multiply.

H53. Wir betrachten den Ring $(\mathbb{Z}_n, +, \cdot)$, wobei Addition und Multiplikation modulo n ausgeführt werden. Eine Zahl $x \in \mathbb{Z} \setminus \{0\}$ ist ein *Nullteiler*, wenn es $y \in \mathbb{Z}_n \setminus \{0\}$ gibt, sodass $x \cdot y \equiv 0 \pmod{n}$ gilt.

- (a) Bestimmen Sie alle Nullteiler und Einheiten in $(\mathbb{Z}_n, +, \cdot)$ für die folgenden Werte von n .

$$(i) \ n = 4, \quad (ii) \ n = 5, \quad (iii) \ n = 15, \quad (iv) \ n = 17.$$

- (b) Zeigen Sie, dass jedes von Null verschiedene Element in $(\mathbb{Z}_n, +, \cdot)$ entweder eine Einheit oder ein Nullteiler ist.
- (c) Zeigen Sie, dass es in $(\mathbb{Z}_n, +, \cdot)$ genau dann keine Nullteiler gibt, wenn $n = 1$ oder n eine Primzahl ist.

H54. (a) Berechnen Sie Lösungen der Kongruenz $225 + 7 \cdot 3^x \equiv 2992 \pmod{13}$.

- (b) Zeigen Sie, dass für alle $n \in \mathbb{N}$ die Zahl $\frac{1}{5}n^5 + \frac{1}{3}n^3 + \frac{7}{15}n$ eine natürliche Zahl ist.