8. Übungsblatt zu Mathematik für Informatiker I, WS 2003/04

JOACHIM VON ZUR GATHEN, OLAF MÜLLER, MICHAEL NÜSKEN

Abgabe bis Freitag, 19. Dezember 2003, 11^{11}
in den jeweils richtigen grünen oder roten Kasten auf dem D1-Flur.

Aufgabe 8.1 (ISBN Ziffern). (1 Punkt)

Eine ISBN besteht aus 10 Ziffern $(z_1, z_2, z_3, \ldots, z_{10})$. Die letzte Ziffer, die sogenannte *Prüfziffer*, einer ISBN sorgt dafür, dass für jede ISBN $z_1 + 2z_2 + 3z_3 + 4z_4 + \cdots + 9z_9 + 10z_{10}$ durch 11 teilbar ist.

(i) Warum enden einige ISBN mit `X`?

(ii) Berechne die Prüfziffer für `1-239-09029-`□.

Aufgabe 8.2 (Geometrische Reihe). (2 Punkte)

Für jede natürliche Zahl n gilt

$$\sum_{0 \le k < n} q^k = 1 + q + q^2 + \cdots + q^{n-1} \quad \stackrel{!}{=} \quad \frac{1 - q^n}{1 - q} = \frac{q^n - 1}{q - 1}.$$

Aufgabe 8.3 (Modulare Inverse). (2 Punkte)

(i) Berechne $46199^{-1} \bmod 66013$.

(ii) Berechne $26/5 \bmod 828321$.

Aufgabe 8.4 (Eulersche φ-Funktion). (2 Punkte)

(i) Bestimme und zähle die invertierbaren Elemente von $\mathbb{Z}_3$, $\mathbb{Z}_5$ und $\mathbb{Z}_{15}$.

(ii) Bestimme und zähle die invertierbaren Elemente von $\mathbb{Z}_3$, $\mathbb{Z}_9$ und $\mathbb{Z}_{27}$.

Aufgabe 8.5 (Satz von Lagrange). (3 Punkte)

(i) Berechne $17^{10\,000}$ rem 101 (von Hand!).

(ii) Berechne $2^{10\,000}$ rem 15 (von Hand!).

(iii) Berechne $11^{10\,000}$ rem 81 (von Hand!).

Aufgabe 8.6 (Chinesischer Restsatz, Eindeutigkeit). (2 Punkte)

Seien p und q teilerfremd und c und c' Lösungen des Systems $x \equiv a \bmod p$, $x \equiv b \bmod q$. Zeige, dass

$$c \equiv c' \bmod pq$$

gilt.

Bemerkung: Zusammen mit dem in der Vorlesung Bewiesenen, sind die Lösungen von $x \equiv a \bmod p$, $x \equiv b \bmod q$ *genau* die Lösungen von $x \equiv c \bmod pq$, wenn nur c die Bedingungen $c \equiv a \bmod p$ und $c \equiv b \bmod q$ erfüllt.

Aufgabe 8.7 (Chinesischer Restsatz, Beispiel). (3 Punkte)

(i) Bestimme ein x mit $x \equiv 7 \bmod 37$ und $x \equiv 1 \bmod 51$.

(ii) Bestimme alle x mit $x \equiv 7 \bmod 373$ und $x \equiv 1 \bmod 513$.

(iii) Bestimme ein x mit $x \equiv 7 \bmod 373$, $x \equiv 1 \bmod 513$ und $x \equiv 3 \bmod 982$.

8. Übungsblatt zu Mathematik für Informatiker I, WS 2003/04, Mündlicher Teil

JOACHIM VON ZUR GATHEN, OLAF MÜLLER, MICHAEL NÜSKEN

Mündliche Aufgabe 8.8 (Modulare Inverse).

(i) Berechne $75496^{-1} \bmod 86881$.

(ii) Berechne $8/4399 \bmod 92375$.

Mündliche Aufgabe 8.9 (Eulersche φ-Funktion).

(i) Bestimme und zähle die invertierbaren Elemente von $\mathbb{Z}_3$, $\mathbb{Z}_7$ und $\mathbb{Z}_{21}$.

(ii) Bestimme und zähle die invertierbaren Elemente von $\mathbb{Z}_2$, $\mathbb{Z}_4$ und $\mathbb{Z}_8$.

Mündliche Aufgabe 8.10 (Satz von Lagrange).

(i) Berechne $17^{10\,000} \operatorname{rem} 997$ (von Hand!).

(ii) Berechne $11^{10\,000} \operatorname{rem} 256$ (von Hand!).

(iii) Berechne $2^{10\,000} \operatorname{rem} 21$ (von Hand!).

Mündliche Aufgabe 8.11 (Chinesischer Restsatz, Beispiel).

(i) Bestimme ein x mit $x \equiv 1 \bmod 7$ und $x \equiv 2 \bmod 11$.

(ii) Bestimme alle x mit $x \equiv 1 \bmod 3$ und $x \equiv 2 \bmod 5$.

(iii) Bestimme ein x mit $x \equiv 1 \bmod 3$, $x \equiv 2 \bmod 5$ und $x \equiv 3 \bmod 7$.