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

KATHRIN TOFALL

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`? 1/2

Lösung. $\mathbb{Z}_{11}$ hat 11 Elemente, davon sind aber nur die ersten 10 im Dezimalsystem einstellig darstellbar. Deshalb ersetzt das `X` die 10 aus $\mathbb{Z}_{11}$. Schließlich könnte $z_1 + 2z_2 + 3z_3 + 4z_4 + \cdots + 9z_9$ gleich 10 modulo 11 sein und dann ist die Prüfziffer 10. (Beachte, dass $10 \equiv -1 \bmod 11$.) Z.B. `0-553-28942-X`. ◯

(ii) Berechne die Prüfziffer für `1-239-09029-`□. 1/2

Lösung. Berechnen wir zunächst $z_1 + 2z_2 + 3z_3 + 4z_4 + \cdots + 9z_9 \bmod 11$:

$$1 + 2 \cdot 2 + 3 \cdot 3 + 4 \cdot 9 + 5 \cdot 0 + 6 \cdot 9 + 7 \cdot 0 + 8 \cdot 2 + 9 \cdot 9 \equiv 3 \bmod 11.$$

Die nächste Ziffer der Zahl wird danach subtrahiert, da $10 \equiv -1 \bmod 11$, und sollte also eine 3 sein: `1-239-09029-3`. ◯

Aufgabe 8.2 (Geometrische Reihe). (2 Punkte)

Für jede natürliche Zahl n gilt

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

Lösung. Diese Aufgabe wird natürlich mit Induktion gelöst:

Induktionsanfang $n = 0$:

$$\sum_{0 \le k < 0} q^k = 0 = \frac{1 - 1}{1 - q} = \frac{1 - q^0}{1 - q}.$$

Induktionsschritt $n \to n+1$:

$$\begin{aligned}
\sum_{0 \le k < n+1} q^k &= \sum_{0 \le k < n} q^k + q^n \\
&\overset{\text{IV}}{=} \frac{1-q^n}{1-q} + q^n \\
&= \frac{1-q^n}{1-q} + \frac{(1-q)\cdot q^n}{1-q} \\
&= \frac{1-q^n+q^n-q^{n+1}}{1-q} \\
&= \frac{1-q^{n+1}}{1-q}.
\end{aligned}$$

○

Aufgabe 8.3 (Modulare Inverse). (2 Punkte)

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

Lösung. Wir berechnen das Inverse mit dem EEA:

i	r_i	q_i	s_i	t_i	Kommentar	
0	66 013	–	1	0		
1	46 199	1	0	1		
2	19 814	2	1	−1	66 013	$= 1 \cdot 46\,199 + 19\,814$
3	6 571	3	−2	3	46 199	$= 2 \cdot 19\,814 + 6\,571$
4	101	65	7	−10	19 814	$= 3 \cdot 6\,571 + 101$
5	6	16	−457	653	6 571	$= 65 \cdot 101 + 6$
6	5	1	7 319	−10 458	101	$= 16 \cdot 6 + 5$
7	**1**	5	**−7 776**	**11 111**	6	$= 1 \cdot 5 + 1$
8	0	–	46 199	−66 013	5	$= 5 \cdot 1 + 0$

Wir können also ablesen: $1 = 11111 \cdot 46199 - 7776 \cdot 66013$. Diese Gleichung modulo 66013 betrachtet, ergibt:

$$46199 \cdot 11111 \equiv 1 \bmod 66013.$$

Damit ist $46199^{-1} \equiv 11111 \bmod 66013$. ○

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

Lösung. Hier brauchen wir das Inverse von 5 modulo 828321. Wir berechnen wieder mit dem EEA:

i	r_i	q_i	s_i	t_i	Kommentar	
0	828 321	–	1	0		
1	5	165 664	0	1		
2	**1**	5	**1**	**−165 664**	828 321	$= 165\,664 \cdot 5 + 1$
3	0	–	−5	828 321	5	$= 5 \cdot 1 + 0$

Damit gilt $5^{-1} \equiv -165664 \equiv 662657 \bmod 828321$. Die Lösung der Aufgabe ist dann:

$$26 \cdot (-165664) = -4307264 \equiv 662662 \bmod 828321. \qquad \bigcirc$$

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

(i) Bestimme und zähle die invertierbaren Elemente von $\mathbb{Z}_3$, $\mathbb{Z}_5$ und $\mathbb{Z}_{15}$. 1

Lösung.
- $\mathbb{Z}_3^\times = \{1, 2\}$, $\varphi(3) = \#\mathbb{Z}_3^\times = 2$.
- $\mathbb{Z}_5^\times = \{1, 2, 3, 4\}$, $\varphi(5) = \#\mathbb{Z}_5^\times = 4$.
- $\mathbb{Z}_{15}^\times = \{1, 2, 4, 7, 8, 11, 13, 14\}$, $\varphi(15) = \#\mathbb{Z}_{15}^\times = 8$. $\bigcirc$

(ii) Bestimme und zähle die invertierbaren Elemente von $\mathbb{Z}_3$, $\mathbb{Z}_9$ und $\mathbb{Z}_{27}$. 1

Lösung.
- $\mathbb{Z}_3^\times = \{1, 2\}$, $\varphi(3) = \#\mathbb{Z}_3^\times = 2$.
- $\mathbb{Z}_9^\times = \{1, 2, 4, 5, 7, 8\}$, $\varphi(9) = \#\mathbb{Z}_9^\times = 6 = 3^{2-1} \cdot (3-1)$.
- $\mathbb{Z}_{27}^\times = \{1, 2, 4, 5, 7, 8, 10, 11, 13, 14, 16, 17, 19, 20, 22, 23, 25, 26\}$, $\varphi(27) = \#\mathbb{Z}_{27}^\times = 18 = 3^{3-1} \cdot (3-1)$. $\bigcirc$

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

(i) Berechne $17^{10\,000}$ rem 101 (von Hand!). 1

Lösung. 101 ist prim, also $\mathbb{Z}_{101}^\times = 100$. Also wissen wir für alle $x \in \mathbb{Z}$: Wenn $101 \nmid x$, dann gilt $x^{100} \equiv 1 \bmod 101$. Damit können wir jetzt leicht die gestellte Aufgabe lösen:

$$17^{10000} = \left(17^{100}\right)^{100} \equiv 1^{100} = 1 \bmod 101. \qquad \bigcirc$$

(ii) Berechne $2^{10\,000}$ rem 15 (von Hand!). 1

Lösung. Die Gruppengröße $\#\mathbb{Z}_{15}^\times = \varphi(15) = 8$ war in Aufgabe 8.4(i) zu berechnen. Wir wissen also: $2^8 \equiv 1 \bmod 15$. Damit jetzt

$$2^{10000} = \left(2^8\right)^{1250} \equiv 1^{1250} = 1 \bmod 15. \qquad \bigcirc$$

(iii) Berechne $11^{10\,000}$ rem 81 (von Hand!). 1

Lösung. Wir können $\varphi(81) = \mathbb{Z}_{81}^{\times}$ wie folgt bestimmen:

$$\varphi(81) = \varphi(3^4) = 3^3 \cdot (3-1) = 27 \cdot 2 = 54.$$

Also wissen wir: $11^{54} \equiv 1 \bmod 81$. Division mit Rest des Exponenten 10000 durch die Gruppengröße 54 ergibt

$$10000 = 185 \cdot 54 + 10.$$

Damit erhalten wir dann:

$$\begin{aligned} 11^{10000} &= 11^{185 \cdot 54 + 10} \\ &= \left(11^{54}\right)^{185} \cdot 11^{10} \\ &\equiv 1^{185} \cdot 11^{10} \\ &= 11^{10} \bmod 81. \end{aligned}$$

Also müssen wir nur noch $11^{10} \bmod 81$ ausrechnen:

$$\begin{aligned} 11^2 &= 121 \equiv 40 \bmod 81, \\ 11^4 &\equiv (40)^2 = 1600 \equiv -20 \bmod 81, \\ 11^8 &\equiv (-20)^2 = 400 \equiv -5 \bmod 81. \end{aligned}$$

Jetzt können wir leicht sehen:

$$11^{10} = 11^{2+8} = 11^2 \cdot 11^8 \equiv 40 \cdot (-5) = -200 \equiv 43 \bmod 81. \qquad \bigcirc$$

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.

Lösung. Nach Voraussetzung gilt

$$c \equiv a \equiv c' \bmod p \text{ und } c \equiv b \equiv c' \bmod q,$$

d.h.

$$p \mid (c - c') \text{ und } q \mid (c - c').$$

Wegen der Eindeutigkeit der Primfaktorzerlegung folgt dann:

$$pq \mid (c - c'),$$

also $c \equiv c' \bmod pq$. $\bigcirc$

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

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

Lösung. Um das gesuchte x zu bestimmen, benutzen wir den EEA. Bei Eingabe von $a = 51$ und $b = 37$ liefert er $s = 8$ und $t = -11$. Außerdem ist der ggT 1, was für die Anwendung des Chinesischen Restsatzes Voraussetzung ist. Wir wissen dann also:

$$\begin{aligned} 1 &= 8 \cdot 51 - 11 \cdot 37 \\ &= \underbrace{408}_{=:u} + \underbrace{(-407)}_{=:v} \end{aligned}$$

Betrachten wir nochmal u und v modulo unserer beiden Primzahlen:

$$\begin{aligned} 408 &\equiv 1 \bmod 37, & -407 &\equiv 0 \bmod 37, \\ 408 &\equiv 0 \bmod 51, & -407 &\equiv 1 \bmod 51. \end{aligned}$$

Um ein gesuchtes x zu erhalten, multiplizieren wir jetzt einfach 408 mit 7 und -407 mit 1. Wir kriegen dann:

$$7 \cdot 408 - 1 \cdot 407 = 2449 \equiv 562 \bmod (51 \cdot 37).$$

Nach den vorherigen Überlegungen gilt dann $2449 \equiv 562 \equiv 7 \bmod 37$ und $2449 \equiv 562 \equiv 1 \bmod 51$. ◯

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

Lösung. Der EEA liefert bei Eingabe $a = 513$ und $b = 373$ den ggT 1, $s = 8$ und $t = -11$. Dann:

$$\begin{aligned} 1 &= 8 \cdot 513 - 11 \cdot 373 \\ &= \underbrace{4104}_{=:u} + \underbrace{(-4103)}_{=:v} \end{aligned}$$

Für das x berechnen wir hier einfach:

$$x = 7 \cdot u + 1 \cdot v = 24625 \equiv 24625 \bmod (\underbrace{513 \cdot 373}_{=191349}).$$

Es gilt dann $24625 \equiv 7 \bmod 373$ und $24625 \equiv 1 \bmod 513$. Es sind alle x Lösungen, die die Gleichung $x \equiv 24625 \bmod 191349$ erfüllen. ◯

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

Lösung. Für die Lösung dieser Aufgabe benutzen wir das Ergebnis der vorhergehenden. Wir wissen ja schon, dass eine Lösung x für die ersten beiden Gleichungen genau folgende Gleichung erfüllen muss:

$$x \equiv 24625 \bmod 191349.$$

Wir wenden also den EEA auf $a = 191349$ und $b = 982$ an. Wir erhalten wieder ggT 1 und außerdem $s = 195$ und $t = -37997$.

$$\begin{aligned} 1 &= 195 \cdot 191349 - 37997 \cdot 982 \\ &= \underbrace{37313055}_{=:u} + \underbrace{(-37313054)}_{=:v} \end{aligned}$$

Ein gesuchtes x ist dann:

$$x = u \cdot 3 + v \cdot 24625 = -918722015585 \equiv 132055435 \bmod (982 \cdot 191349).$$

Es gilt dann

$$-918722015585 \equiv 132055435 \equiv 24625 \bmod 191349,$$

also $-918722015585 \equiv 132055435 \equiv 7 \bmod 373$ und $-918722015585 \equiv 132055435 \equiv 1 \bmod 513$, und ferner

$$-918722015585 \equiv 132055435 \equiv 3 \bmod 982.$$ ◯