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

KATHRIN TOFALL

Aufgabe 7.1 (Symmetrischer EEA). (9 Punkte)

Ziel dieser Aufgabe ist es zu zeigen, was man gewinnt, wenn man bei der Division mit Rest auch negative Reste zulässt.

Seien a und b zwei ganze Zahlen. Man kann leicht zeigen, dass es immer zwei ganze Zahlen q und r gibt, so dass $a = qb + r$ und $-\frac{1}{2}|b| \leq r < \frac{1}{2}|b|$. Wir nennen dies *symmetrische Division mit Rest* und schreiben $q = a$ squo b. (*Idee:* Verwende normale Divison mit Rest und korrigiere das Ergebnis.)

(i) Berechne entsprechende q und r für $a = 100$ und $b = 53$. 1/2

Lösung. Es ist also eine Zerlegung $100 = q \cdot 53 + r$ gesucht mit $-26,5 \leq r < 26,5$. Normale Division mit Rest liefert dann:

$$100 = 1 \cdot 53 + 47.$$

47 ist offensichtlich zu groß. Aber es gilt: $47 = b - 6$. Das können wir jetzt einsetzen:

$$a = 1 \cdot b + b - 6 = 2 \cdot b - 6.$$

Damit ist $q = 2$ und $r = -6$. ◯

(ii) Berechne entsprechende q und r für $a = 807\,959$ und $b = 219\,215$. 1/2

Lösung. Hier suchen wir dann eine Zerlegung $807\,959 = q \cdot 219\,215 + r$ gesucht mit $-109\,607,5 \leq r < 109\,607,5$. Wenn wir normale Division mit Rest ausführen, erhalten wir:

$$a = 807\,959 = 3 \cdot 219\,215 + 150\,314 = 3 \cdot b + 150\,314.$$

Der Rest ist für symmetrische Division mit Rest deutlich zu groß. Wir können aber leicht ausrechnen, dass

$$150\,314 = 219\,215 - 68\,901 = b - 68\,901$$

gilt. Wenn wir das einsetzen, ergibt sich:

$$a = 3 \cdot b + b - 68\,901 = 4b - 68\,901.$$

Damit gilt $q = 4$ und $r = -68\,901$. ◯

Wir betrachten nun den Erweiterten Euklidischen Algorithmus mit symmetrischen Resten.

Algorithmus. Symmetrischer EEA.

Eingabe: $a, b \in \mathbb{Z}$.
Ausgabe: $\ell \in \mathbb{N}$, $r_i, s_i, t_i \in \mathbb{Z}$ für $0 \leq i \leq \ell + 1$, und $q_i \in \mathbb{Z}$ für $1 \leq i \leq \ell$, wie unten berechnet.

1. $r_0 \leftarrow a$, $\quad r_1 \leftarrow b$.
2. $s_0 \leftarrow 1$, $\quad t_0 \leftarrow 0$.
3. $s_1 \leftarrow 0$, $\quad t_1 \leftarrow 1$.
4. $i \leftarrow 1$.
5. While $r_i \neq 0$ do 6–10
6. $\quad q_i \leftarrow r_{i-1}$ squo r_i. // Hier symmetrische Division mit Rest.
7. $\quad r_{i+1} \leftarrow r_{i-1} - q_i r_i$.
8. $\quad s_{i+1} \leftarrow s_{i-1} - q_i s_i$.
9. $\quad t_{i+1} \leftarrow t_{i-1} - q_i t_i$.
10. $\quad i \leftarrow i + 1$.
11. $\ell \leftarrow i - 1$.
12. Return ℓ, r_i, s_i, t_i für $0 \leq i \leq \ell + 1$, und q_i für $1 \leq i \leq \ell$.

2 (iii) Benutze diesen Algorithmus, um einen ggT von $a = F_{10} = 55$ und $b = F_9 = 34$ zu berechnen.

Lösung.

i	r_i	q_i	s_i	t_i	Kommentar
0	55	–	1	0	
1	34	2	0	1	
2	−13	−3	1	−2	$55 = 2 \cdot 34 - 13$
3	−5	3	3	−5	$34 = -3 \cdot (-13) - 5$
4	2	−2	−8	13	$-13 = 3 \cdot (-5) + 2$
5	**−1**	−2	**−13**	**21**	$-5 = -2 \cdot 2 - 1$
6	0	–	−34	55	$2 = -2 \cdot (-1) + 0$

Damit ist der ggT $1 = |-1| = 13a - 21b$. ◯

2 (iv) Benutze diesen Algorithmus, um einen ggT von $a = 219\,215$ und $b = 807\,959$ zu berechnen.

Lösung.

i	r_i	q_i	s_i	t_i	Kommentar	
0	219 215	–	1	0		
1	807 959	0	0	1		
2	219 215	4	1	0	$219\,215$	$= 0 \cdot 807\,959 + 219\,215$
3	−68 901	−3	−4	1	$807\,959$	$= 4 \cdot 219\,215 - 68\,901$
4	12 512	−6	−11	3	$219\,215$	$= -3 \cdot (-68\,901) + 12\,512$
5	6 171	2	−70	19	$-68\,901$	$= -6 \cdot 12\,512 + 6\,171$
6	170	36	129	−35	$12\,512$	$= 2 \cdot 6\,171 + 170$
7	51	3	−4 714	1 279	$6\,171$	$= 36 \cdot 170 + 51$
8	**17**	3	**14 271**	**−3 872**	170	$= 3 \cdot 51 + 17$
9	0	–	−47 527	12 895	51	$= 3 \cdot 17 + 0$

Hier ist also der ggT $17 = 14\,271a - 3\,872b$. ◯

(v) Vergleiche die Anzahl der Schleifendurchläufe aus (iii) und (iv) mit dem normalen euklidischen Algorithmus. [Beide Angaben zum normalen EA sind bekannt!] 1

Lösung. Der EEA mit normaler Division mit Rest benötigt für die Zahlen aus (iii) 8 Schleifendurchläufe, da es sich um die Fibonacci-Zahlen F_{10} und F_9 handelt. Der EEA mit symmetrischer Division mit Rest braucht hier nur 5 Schleifendurchläufe. Für die beiden anderen Zahlen werden 10 und 8 Durchläufe gemacht. ◯

(vi) Zeige, dass ab $i = 1$ der Betrag jedes Restes r_{i+1} höchstens halb so groß ist wie der Betrag des vorangehenden Restes r_i. Genauer gesagt: $|r_{i+1}| \leq \frac{1}{2}|r_i|$, falls $1 \leq i \leq \ell$. 1

Lösung. Nach Voraussetzung gilt für den Quotienten $q \in \mathbb{Z}$ und den Rest $r \in \mathbb{Z}$ bei symmetrischer Division mit Rest von r_{i-1} durch r_i:

$$r_{i-1} = qr_i + r \text{ und } -\frac{1}{2}|r_i| \leq r < \frac{1}{2}|r_i|.$$

Wegen $q_i = r_{i-1}$ squo r_i folgt $q = q_i$ und dann ist

$$r_{i+1} = r_{i-1} - q_i r_i = r_{i-1} - qr_i = r.$$

Damit gilt $-\frac{1}{2}|r_i| \leq r_{i+1} < \frac{1}{2}|r_i|$, also $|r_{i+1}| \leq \frac{1}{2}|r_i|$. Die Bedingung „ab $i = 1$“ wird benötigt, weil vorher im Algorithmus noch keine Division mit Rest ausgeführt wird. ◯

(vii) Schließe, dass $|r_i| \leq \frac{1}{2^{i-1}}|b|$ für $1 \leq i \leq \ell + 1$ gilt. 1

Lösung. Diese Teilaufgabe wird natürlich mit Induktion gelöst. Wir wissen aus dem Algorithmus, dass $b = r_1$.

Induktionsanfang $i = 1$: Offensichtlich gilt $|r_1| = |b|$.

Induktionsanfang $i = 2$: Es gilt

$$|r_2| \leq \frac{1}{2}|r_1| = \frac{1}{2^{2-1}}|b|.$$

Induktionsschritt $i \to i+1$: Wir schätzen r_{i+1} ab:

$$|r_{i+1}| \overset{\text{(vi)}}{\leq} \frac{1}{2}|r_i| \overset{\text{IV}}{\leq} \frac{1}{2} \cdot \frac{1}{2^{i-1}}|b| = \frac{1}{2^{(i+1)-1}}|b|.$$

○

1 (viii) Zeige, dass diese Variante des Euklidischen Algorithmus für $b \neq 0$ höchstens $\log_2 |b| + 1$ Schritte (also Durchläufe von Schritt 5–10 im Algorithmus) braucht.

Lösung. Zum Beweis dieser Aussage nehmen wir das Gegenteil an und führen die Annahme zum Widerspruch:

Annahme: $\ell > \log_2 |b| + 1$.

Dann wäre $\ell - 1 > \log_2 |b|$ und damit $2^{\ell-1} > |b|$. Wenn wir diese Gleichung jetzt durch $2^{\ell-1}$ teilen, erhalten wir:

$$1 > \frac{|b|}{2^{\ell-1}} \overset{(vii)}{\geq} |r_\ell|.$$

Also muß der Betrag von r_ℓ schon 0 sein. Das kann aber nicht sein, da nach Voraussetzung r_ℓ der letzte Rest ungleich 0 ist. Das ist ein Widerspruch, also ist unsere Annahme falsch. ○

Aufgabe 7.2 (Modulare Arithmetik). (6 Punkte)

1/3 (i) Löse $x \equiv 271\,828 + 314\,159 \bmod 125$ geschickt.

Lösung. Für die ersten drei Teilaufgaben führen wir zuerst zwei Divisionen mit Rest aus:

$$271\,828 = 2\,174 \cdot 125 + 78 \text{ und } 314\,159 = 2\,513 \cdot 125 + 34.$$

Jetzt kann man folgendes leicht berechnen:

$$271\,828 + 314\,159 \equiv 78 + 34 = 112 \bmod 125.$$

○

1/3 (ii) Löse $x \equiv 271\,828 - 314\,159 \bmod 125$ geschickt.

Lösung.

$$271\,828 - 314\,159 \equiv 78 - 34 = 44 \bmod 125.$$

○

(iii) Löse $x \equiv 271\,828 \cdot 314\,159 \bmod 125$ geschickt. 1/3

Lösung.

$$271\,828 \cdot 314\,159 \equiv 78 \cdot 34 = 312 + 2340 \equiv 62 + 2590 \equiv 62 + 90 = 152 \equiv 27 \bmod 125.$$

○

(iv) Löse $5(x + 27) \equiv 4x \bmod 31$. 1/2

Lösung. Die Gleichung kann in diese Form gebracht werden:

$$x + 135 \equiv 0 \bmod 31.$$

Dann $x \equiv -135 \equiv 20 \bmod 31$. ○

(v) Löse $5(x + 27) \equiv 25 \bmod 31$. 1/2

Lösung. Multiplizieren wir mit -6 (dh. wir kürzen eine 5), so erhalten wir

$$x + 27 \equiv 5 \bmod 31,$$

also ist $x \equiv -22 \equiv 9 \bmod 31$. ○

(vi) Löse $13(5 - x) \equiv 17x \bmod 31$. 1/2

Lösung. Dies Gleichung kann man erstmal so umformen:

$$-30x + 65 \equiv 0 \bmod 31.$$

Leicht ist zu sehen, dass $-30x \equiv x \bmod 31$ und $65 \equiv 3 \bmod 31$. Somit können wir unsere Gleichung schreiben als

$$x + 3 \equiv 0 \bmod 31,$$

und somit $x \equiv 28 \equiv -3 \bmod 31$. ○

(vii) Berechne $s, t \in \mathbb{Z}$ mit $1 = 5s + 17t$. 1/2

Lösung. Hier benutzen wir den EEA:

i	r_i	q_i	s_i	t_i	Kommentar
0	5	–	1	0	
1	17	0	0	1	
2	5	3	1	0	$5 = 0 \cdot 17 + 5$
3	2	2	-3	1	$17 = 3 \cdot 5 + 2$
4	**1**	2	**7**	**−2**	$5 = 2 \cdot 2 + 1$
5	0	–	-17	5	$2 = 2 \cdot 1 + 0$

Aus der Tabelle können wir dann sofort sehen:

$$1 = 7 \cdot 5 - 2 \cdot 17.$$

Also $s = 7$ und $t = -2$. ◯

1 (viii) Löse $5x \equiv 1 \bmod 17$.

Lösung. Diese Aufgabe ist jetzt keine Schwierigkeit mehr mit der Vorarbeit aus (vii):

$$5s + 17t \equiv 5s \bmod 17.$$

Also gilt $x = -10$, bzw. $x = 7$. ◯

1 (ix) Finde alle Lösungen von $3x \equiv 0 \bmod 15$.

Lösung. Genau alle durch 5 teilbaren x sind in der Lösungsmenge dieser Gleichung,

$$x \in \{y \cdot 5 \mid y \in \mathbb{Z}\}.$$

◯

1 (x) Finde alle Lösungen von $3x \equiv 2 \bmod 1011$.

Lösung. Diese Gleichung hat keine Lösung, weil jede Linearkombination von 3 und 1011 durch 3 teilbar ist. Die Lösungsmenge ist also leer. ◯

Aufgabe 7.3 (Modular Potenzieren). (0 Punkte)

Achtung: Diese Aufgabe wird nicht korrigiert.

1 (i) Berechne 3^{16} rem 17 (von Hand!).

Lösung.

$$\begin{aligned} 3^2 &\equiv -8 \bmod 17 \\ 3^4 &\equiv (-8)^2 = 64 \equiv -4 \bmod 17 \\ 3^8 &\equiv (-4)^2 = 16 \equiv -1 \bmod 17 \\ 3^{16} &\equiv (-1)^2 \equiv 1 \bmod 17. \end{aligned}$$

◯

(ii) Berechne $3^{10\,000}$ rem 85 (von Hand!). 1

Lösung. Die Zahl 85 ist das Produkt von 5 und 17 und modulo 17 war 3^{16} besonders einfach. Wir betrachten also mal $3^{16} \bmod 85$:

$$\begin{aligned} 3^2 &= 9 \bmod 85 \\ 3^4 &= 9^2 = 81 \equiv -4 \bmod 85 \\ 3^8 &= (-4)^2 = 16 \bmod 85 \\ 3^{16} &\equiv (16)^2 = 256 \equiv 1 \bmod 85. \end{aligned}$$

Mit diesem Wissen läßt sich jetzt die ursprüngliche Aufgabe leicht lösen:

$$3^{10\,000} = \left(3^{16}\right)^{625} \equiv 1^{625} = 1 \bmod 85.$$

(Man sieht leicht, dass $16 = 2^4$ ein Teiler von $10000 = 10^4$ ist.) ◯

Aufgabe 7.4 (Teilbarkeitsregeln). (5 Punkte)

Du kennst bestimmt einige Teilbarkeitsregeln. Zum Beispiel ist eine Zahl durch 2 teilbar, wenn ihre Dezimaldarstellung auf 2, 4, 6, 8 oder 0 endet. Und eine Zahl ist durch 3 teilbar genau dann, wenn auch ihre Quersumme durch 3 teilbar ist. Woher kommen diese Regeln? Wir wollen einige interessante anschauen, die in Deiner Sammlung vielleicht noch fehlen:

(i) Beweise die Teilbarkeitsregel für 9: 1

Satz. *Wenn die Quersumme einer Zahl x durch 9 teilbar ist, dann ist auch x durch 9 teilbar.*

Tipp: Betrachte $x = \sum_{0 \le j < k} x_j 10^j$ modulo 9.

Lösung. Eine ganze Zahl x läßt sich darstellen als $x = \sum_{0 \le j < k} x_j 10^j$. Außerdem können wir leicht sehen, daß gilt:

$$10 \equiv 1 \bmod 9.$$

Wenn wir jetzt unsere Darstellung von x modulo 9 betrachten, fällt folgendes auf:

$$x = \sum_{0 \le j < k} x_j 10^j \equiv \sum_{0 \le j < k} x_j 1^j \bmod 9.$$

Wir erhalten also sogar viel mehr:

Lemma. *Die Zahl x ist modulo 9 kongruent zu ihrer Quersumme.* □

Wenn jetzt die Quersumme $y = \sum_{0 \le j < k} x_j$ von $x \in \mathbb{Z}$ durch 9 teilbar — also gleich $0 \bmod 9$ — ist, dann offensichtlich auch x selbst.

Bei sehr großen Zahlen betrachtet man gegebenenfalls die Quersumme der Quersumme usw. ◯

1 (ii) Leite eine Teilbarkeitsregel für 3 ab.

Lösung. Da 3 ein Teiler von 9 ist, folgt diese Regel sofort aus dem vorhergehenden Lemma. Alternativ kann man wegen $10 \equiv 1 \bmod 3$ auch den letzten Beweis wiederholen. ◯

1 (iii) Finde und zeige eine Teilbarkeitsregel für 11.

Lösung. Auch $10 \equiv -1 \bmod 11$ ist ein schönes Ergebnis, mit dem man hier weiterarbeiten kann:

$$\begin{aligned} x &= \sum_{0 \le j < k} x_j 10^j \\ &\equiv \sum_{0 \le j < k} x_j (-1)^j \\ &= x_0 - x_1 + x_2 - x_3 \ldots \\ &= \sum_{0 \le j < \frac{k}{2}-1} x_{2j} - \sum_{0 \le j < \frac{k}{2}-1} x_{2j+1} \bmod 11. \end{aligned}$$

Man bildet eine sogenannte „Wechselsumme“, also die Quersumme der geraden Stellen von x minus der Quersumme der ungeraden Stellen von x. Wenn jetzt diese Wechselsumme durch 11 teilbar ist, dann auch x selbst. ◯

1 (iv) Finde und zeige eine Teilbarkeitsregel für $1\,001$.

Lösung. Diese Teilbarkeitsregel ist ähnlich zu der „11er“-Regel. Es gilt nämlich:

$$1000 \equiv -1 \bmod 1001.$$

Jetzt wird die betrachtete Zahl x in 3er-Blöcke zerteilt, also:

$$x = (x_{k-1}x_{k-2}x_{k-3}|\dots|x_2x_1x_0)\,.$$

(Wenn die Zahl nicht lang genug ist, kann man mit Nullen auffüllen…)
Eine zu den ersten Aufgabenteilen analoge Darstellung für x wäre dann:

$$x = \sum_{0\le j<\frac{k}{3}-1} (x_{3j+2}\,x_{3j+1}\,x_{3j})\,1000^j.$$

Modulo 1001 betrachtet, bedeutet das:

$$x \equiv \sum_{0\le j<\frac{k}{3}-1} (x_{3j+2}\,x_{3j+1}\,x_{3j})\,(-1)^j = x_2\,x_1\,x_0 - x_5\,x_4\,x_3 + x_8\,x_7\,x_6 \dots\,.$$

Es wird also wieder eine Art Wechselsumme gebildet und wir erhalten auch, dass x und diese Wechselsumme modulo 1001 übereinstimmen. ◯

(v) Leite eine Teilbarkeitsregel für 7 und 13 ab. [*Tipp*: $1\,001 = 7 \cdot 11 \cdot 13$.] 1

Lösung. 7 und 13 sind Teiler von 1001, also gilt auch für diese Zahlen:

$$\begin{aligned} 1000 &\equiv -1 \bmod 7 \text{ und} \\ 1000 &\equiv -1 \bmod 13. \end{aligned}$$

Also kann die gleiche Teilbarkeitsregel verwendet werden. ◯

Aufgabe 7.5 (Von großen zu kleinen Moduln). (1 Punkt)

Zeige: Sei n ein Teiler von m. Sind zwei Zahlen a, b modulo m kongruent, $a \equiv b \bmod m$, dann sind sie auch modulo des Teilers n kongruent, $a \equiv b \bmod n$.

Lösung. $a \equiv b \bmod m$ heißt nichts anderes als $m \mid (a-b)$. Wegen $n \mid m$ folgt sofort $n \mid (a-b)$, also $a \equiv b \bmod n$. ◯