Bernhard Dietrich

[b|d] bernhard dietrich

Mathematik für Informatiker I
Übungsblatt 7
Matrikel-Nr.: 6256800 · Übungsgruppe 1

Aufgabe 7.1

(i) Es sei $a = qb + r$. Mit $-\frac{1}{2}|b| \le r < \frac{1}{2}|b|$ und $q, r \in \mathbb{Z}$ folgt für $a = 100$ und $b = 53$:

$100 = 2 \cdot 53 - 6$

(ii) Es sei $a = qb + r$. Mit $-\frac{1}{2}|b| \le r < \frac{1}{2}|b|$ und $q, r \in \mathbb{Z}$ folgt für $a = 807\ 959$ und $b = 219\ 215$:

$807\ 959 = 4 \cdot 219\ 215 - 68\ 901$

(iii) $ggT(55, 34)$

i	r_i	q_i	s_i	t_i
0	55		1	0
1	34	2	0	1
2	-13	-3	1	-2
3	-5	3	3	-5
4	2	-2	-8	13
5	-1	-2	-13	21
6	0		-34	55

$l = 6 - 1 = 5$

$ggT(55, 34) = -1$

(iv) $ggT(219\ 215, 807\ 959)$

i	r_i	q_i	s_i	t_i
0	219 215		1	0
1	807 959	0	0	1
2	219 215	4	1	0
3	-68 901	-3	-4	1
4	12 512	-6	-11	3
5	6171	2	-70	19
6	170	36	129	-35
7	51	3	-4714	1279
8	17	3	14271	-3872
9	0		-47527	12895

$l = 9 - 1 = 8$

$ggT(219\ 215, 807\ 959) = 17$

(v) Der EEA braucht für iii 8 und für iv 10 Schleifendurchläufe.
Der symmetrische EEA braucht dafür nur 5 bzw. 8 Schleifendurchläufe.
Der symmetrische EEA hat also – zumindest in diesen beiden Fällen – eine geringere und damit optimierte Laufzeit.

(vi) Zu zeigen: $|r_{i+1}| \le \frac{1}{2}|r_i|$, falls $1 \le i \le l$.

Gemäß Spezifikation des Algorithmus gilt:

$$-\frac{1}{2}|b| \le r < \frac{1}{2}|b|$$

Das r entspricht dem den Nachfolger des aktuellen Elements, also gilt

$$-\frac{1}{2}|b| \le r_{i+1} < \frac{1}{2}|b|$$

Da $r_1 = b$ und $r_0 = a$ (vgl. Algorithmus), folgt $r_i = b$ und $r_{i-1} = a$, so dass gilt:

$$-\frac{1}{2}|r_i| \le r_{i+1} < \frac{1}{2}|r_i|$$

Es folgt:

$$|r_{i+1}| < \frac{1}{2}|r_i| \le \left|-\frac{1}{2}r_i\right|$$

$$\Rightarrow |r_{i+1}| \le \left|\frac{1}{2}r_i\right|$$

(vii) Zu zeigen: $|r_i| \le \frac{1}{2^{i-1}}|b|$ für $1 \le i \le l+1$

I.A. Wir zeigen: Die Aussage gilt für ein beliebiges, festes i. Wir wählen $i = 1$

$r_1 \le \frac{1}{2^0}|b| \Leftrightarrow r_1 \le |b|$ (wahre Aussage, da $r_1 = |b|$ (vgl. Algorithmus)

I.S. Wir zeigen, gilt die Aussage für ein beliebiges, festes i, dann gilt sie auch für $i+1$

Zu zeigen: $|r_{i+1}| \le \frac{1}{2^i}|b|$

$$|r_{i+1}| \overset{\text{(vi)}}{\le} \left|\frac{1}{2}r_i\right| \overset{\text{I.V.}}{\le} \left|\frac{1}{2} \cdot \frac{1}{2^{i-1}}b\right| = \left|\frac{1}{2^i}b\right| \text{ für } 1 \le i \le l$$

Da i fest aber beliebig gewählt wurde, gilt die Behauptung auch für $i = l+1$, da

$$r_{l+1} = 0 \le \frac{1}{2^{l+1-1}}|b|$$

(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.
Der Symmetrische Erweiterte Euklidische Algorithmus beruht darauf, dass der Betrag des folgenden r_{i+1} maximal halb so groß ist, wie der Betrag des aktuellen r_i, so dass gilt

$|r_i| \le \frac{1}{2^{i-1}}|b|$ (für $1 \le i \le l+1$).

Da $r_l \ge 1$ folgt:

$$1 \le |r_l| \le \frac{1}{2^{l-1}}|b|$$

$$\Leftrightarrow \quad 1 \le \frac{1}{2^{l-1}}|b|$$

$$\Leftrightarrow \quad 2^{l-1} \le |b|$$

$$\Leftrightarrow \quad l-1 \le \log_2|b|$$

$$\Leftrightarrow \quad l \le \log_2|b|+1$$

■

Aufgabe 7.2

(i) $x \equiv 271828 + 314159 \bmod 125$
$\equiv 78 + 34 \bmod 125$
$\equiv 112 \bmod 125$

(ii) $x \equiv 271828 - 314159 \bmod 125$
$\equiv 78 - 34 \bmod 125$
$\equiv 44 \bmod 125$

(iii) $x \equiv 271828 \cdot 314159 \bmod 125$
$\equiv 78 \cdot 34 \bmod 125$
$\equiv 2652 \bmod 125$
$\equiv 27 \bmod 125$

(iv) $5(x+27) \equiv 4x \bmod 31$
$\Leftrightarrow 5x + 135 \equiv 4x \bmod 31$
$\Leftrightarrow x \equiv -135 \bmod 31$
$\Leftrightarrow x \equiv 20 \bmod 31$

(v) $5(x+27) \equiv 25 \bmod 31$
$\Leftrightarrow x + 27 \equiv 5 \bmod 31$
$\Leftrightarrow x \equiv 9 \bmod 31$

(vi) $13(5-x) \equiv 17x \bmod 31$
$\Leftrightarrow 65 - 13x \equiv 17x \bmod 31$
$\Leftrightarrow 65 \equiv 30x \bmod 31$
$\Leftrightarrow 65 \equiv -x \bmod 31$
$\Leftrightarrow 28 \equiv x \bmod 31$

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

EEA für $a = 17$ und $b = 5$:

i	r_i	q_i	s_i	t_i
0	17	-	1	0
1	5	3	0	1
2	2	2	1	-3
3	1	2	-2	7
4	0	-	5	-17

Somit gibt es die Lösung $t = -2$ und $s = 7$, so dass folgt
$1 = 35 - 34 = 5 \cdot 7 + 17 \cdot (-2)$

(viii) $5x \equiv 1 \bmod 17$
$\Leftrightarrow 5x \equiv 35 \bmod 17$
$\Leftrightarrow x \equiv 7 \bmod 17$

(ix) Die Aussage $3x \equiv 0 \mod 15$ ist gleichbedeutend mit:
$15 \mid 3x$
Somit gilt: $x \in \{5 \cdot y, y \in \mathbb{Z}\}$

(x) Die Aussage $3x \equiv 2 \mod 1011$ ist gleichbedeutend mit:
$1011 \mid 3x - 2$
Da sich die Variable x nicht isolieren lässt, weil es kein Inverses zu 1011 gibt, gibt es keine Lösung.

Aufgabe 7.4

(i) Zu zeigen: Wenn die Quersumme einer Zahl x durch 9 teilbar ist, dann ist auch x durch 9 teilbar.

$$x = \sum_{0 \le j < k} x_j 10^j$$

$$9 \mid \sum_{0 \le j < k} x_j 10^j$$

$$\Leftrightarrow \quad \left(x_0 \cdot 10^0 + x_1 \cdot 10^1 + ... + x_{k-1} \cdot 10^{k-1}\right) \equiv 0 \mod 9$$

$$\Leftrightarrow \quad \left(x_0 \cdot 1^0 + x_1 \cdot 1^1 + ... + x_{k-1} \cdot 1^{k-1}\right) \equiv 0 \mod 9$$

$$\Leftrightarrow \quad \left(x_0 + x_1 + ... + x_{k-1}\right) \equiv 0 \mod 9$$

$$\Leftrightarrow \quad \sum_{0 \le j < k} x_j \equiv 0 \mod 9$$

$$\Leftrightarrow \quad 9 \mid \sum_{0 \le j < k} x_j$$

Somit ist eine Zahl x durch 9 teilbar, wenn ihre Quersumme durch 9 teilbar ist.

(ii) Leite eine Teilbarkeitsregel für 3 ab.
Da $9 \equiv 0 \mod 3$, gilt als Teilbarkeitsregel für 3:
Wenn die Quersumme einer Zahl durch 3 teilbar ist, ist auch die Zahl selbst durch 3 teilbar.

(iii) Zu zeigen. Wenn die alternierende Quersumme einer Zahl x durch 11 teilbar ist, dann ist auch x durch 11 teilbar.

$$x = \sum_{0 \le j < k} x_j 10^j$$

$$11 \mid \sum_{0 \le j < k} x_j 10^j$$

$$\Leftrightarrow \quad \left(x_0 \cdot 10^0 + x_1 \cdot 10^1 + x_2 \cdot 10^2 + ... + x_{k-1} \cdot 10^{k-1}\right) \equiv 0 \mod 11$$

$$\Leftrightarrow \quad \left(x_0 \cdot 1 + x_1 \cdot (-1) + x_2 \cdot 1 + ... + x_{k-1} \cdot (\pm 1)^{k-1}\right) \equiv 0 \mod 11$$

$$\Leftrightarrow \quad \left(x_0 - x_1 + x_2 - ... \pm x_{k-1}\right) \equiv 0 \mod 11$$

$$\Leftrightarrow \quad \sum_{0 \le j < k} (-1)^j x_j \equiv 0 \mod 11$$

$$\Leftrightarrow \quad 11 \mid \sum_{0 \le j < k} (-1)^j x_j$$

Somit muss die alternierende Quersumme einer Zahl durch 11 teilbar sein, damit diese die Zahl selbst durch 11 teilbar ist.

(iv) Zu zeigen: Wenn 1001 die Summe $\sum_{0\le j<k} (-1)^{\left\lfloor \frac{x_j}{3} \right\rfloor} \cdot 10^{x_j \bmod 3}$ einer Zahl x teilt, dann ist auch x durch 1001 teilbar.

$$x = \sum_{0\le j<k} x_j 10^j$$

$$1001 \mid \sum_{0\le j<k} x_j 10^j$$

$$\sum_{0\le j<k} x_j 10^j \equiv 0 \bmod 1001$$

$$\Leftrightarrow \quad x_0 \cdot 10^0 + x_1 \cdot 10^1 + x_2 \cdot 10^2 + x_3 \cdot 10^3 + x_4 \cdot 10^4 + x_5 \cdot 10^5 + x_6 \cdot 10^6 + \ldots + x_{k-1} \cdot 10^{k-1} \equiv 0 \bmod 1001$$

$$\Leftrightarrow \quad x_0 \cdot 1 + x_1 \cdot 10 + x_2 \cdot 100 + x_3 \cdot (-1) + x_4 \cdot (-10) + x_5 \cdot (-100) + x_6 \cdot 1 + \ldots + x_{k-1} \cdot (\pm 100) \equiv 0 \bmod 1001$$

$$\Leftrightarrow \quad x_0 \cdot 1 + x_1 \cdot 10 + x_2 \cdot 100 - x_3 - 10 \cdot x_4 - 100 \cdot x_5 + x_6 + \ldots \pm 100 \cdot x_{k-1} \equiv 0 \bmod 1001$$

$$\Leftrightarrow \quad \sum_{0\le j<k} (-1)^{\left\lfloor \frac{x_j}{3} \right\rfloor} \cdot 10^{x_j \bmod 3} \equiv 0 \bmod 1001$$

$$\Leftrightarrow \quad 1001 \mid \sum_{0\le j<k} (-1)^{\left\lfloor \frac{x_j}{3} \right\rfloor} \cdot 10^{x_j \bmod 3}$$

Somit muss die die Summe $\sum_{0\le j<k} (-1)^{\left\lfloor \frac{x_j}{3} \right\rfloor} \cdot 10^{x_j \bmod 3}$ einer Zahl x durch 1001 teilbar sein, damit die Zahl selbst auch durch 1001 teilbar ist.

(v) Leite eine Teilbarkeitsregel für 7 und 13 ab.
Da $7 \mid 1001$ und $13 \mid 1001$, gilt für 7 und 13 ebenfalls:
Wenn 7 bzw. 13 die Summe $\sum_{0\le j<k} (-1)^{\left\lfloor \frac{x_j}{3} \right\rfloor} \cdot 10^{x_j \bmod 3}$ einer Zahl x teilt, dann ist auch x durch 7 bzw. 13 teilbar.

Aufgabe 7.5

Zu zeigen: Sei $n \mid m$. Gilt $a \equiv b \bmod m$, dann gilt auch $a \equiv b \bmod n$ mit $n \mid m$.

$$a \equiv b \bmod m$$

$$\Leftrightarrow \quad m \mid a - b$$

Da $n \mid m$, folgt:

$$n \mid m \mid a - b$$

$$\Rightarrow \quad n \mid a - b$$

$$\Leftrightarrow \quad a \equiv b \bmod n$$

■