Reimund Albers, Arithmetik als Prozess, WiSe 05/06

Übung 5, Lösungsskizzen

1. a) $125 \cdot 37 = 4625$ (T H Z E) $\qquad (6-2)\cdot 26 + 4 + 5 - 2 = 104 + 7 = 111 = 3 \cdot 37$

$186 \cdot 37 = 6882 \qquad (8-8)\cdot 26 + 6 + 2 - 8 = 0 = 0 \cdot 37$

$52 \cdot 37 = 1924 \qquad (9-2)\cdot 26 + 1 + 4 - 2 = 185 = 5 \cdot 37$

$59 \cdot 37 = 2183 \qquad (1-8)\cdot 26 + 2 + 3 - 8 = -185 = -5 \cdot 37$

b) Vierstellige Zahl: $a = 1000a_3 + 100a_2 + 10a_1 + a_0$

durch 37 teilbar: $a \equiv 0 \mod 37$

Rechentrick: $(a_2 - a_1)\cdot 26 + a_3 + a_0 - a_1$

ordnen $= 26a_2 - 26a_1 + a_3 + a_0 - a_1$

$= a_3 + 26a_2 - 27a_1 + a_0$

Zu zeigen ist:

Wenn $1000a_3 + 100a_2 + 10a_1 + a_0 \equiv 0 \mod 37$

dann auch $a_3 + 26a_2 - 27a_1 + a_0 \equiv 0 \mod 37$

Das gilt, da $1000 \equiv 1 \mod 37$

$100 \equiv 26 \mod 37$

$10 \equiv -27 \mod 37$

und da in kongruenzen Zahlen durch kongruente Zahlen ersetzt werden können

c) →

2. a) $589656 \xrightarrow{QS} 39 \xrightarrow{QS} 12 \xrightarrow{QS} 3$

Rechner: $589656 = 65517 \cdot 9 + 3$ ✓

$12345 \xrightarrow{QS} 15 \xrightarrow{QS} 6$

Rechner: $12345 = 1371 \cdot 9 + 6$ ✓

b) $a = a_n \cdot 10^n + a_{n-1} \cdot 10^{n-1} + \cdots + a_2 \cdot 100 + a_1 \cdot 10 + a_0$

$b = a_n + a_{n-1} + \cdots + a_2 + a_1 + a_0$

Vorlesung: $a \equiv b \mod 9$

Ebenso erhält man eine zu b kongruente Zahl, wenn man für b die Quersumme bildet.

Also gilt für das fortgesetzte (iterierte) Bilden der Quersumme:

$a \equiv Q_1 \equiv Q_2 \equiv \dots \equiv Q_k \overset{\mod 9}{} \quad \text{mit } k \in \mathbb{N},\ 0 < Q_k \leq 9$

also letztlich (Transitivität der Kongruenz)

$a \equiv Q_k \mod 9 \iff a = k_a \cdot 9 + Q_k,\ k_a \in \mathbb{N}$

Q_k ist also der Rest beim Teilen durch 9 außer $Q_k = 9$, denn dann ist der Rest 0.

Nachtrag 1c)

Man ersetzt die Zehnerpotenzen durch kongruente, kleinere Zahlen und macht ggfs noch ein paar algebraische Umformungen.

z.B. $1000a_3 + 100a_2 + 10a_1 + a_0$ 4stellige Zahl, durch 13

$\equiv 12\cancel{11}a_3 - 4a_2 - 3a_1 + a_0 \mod 13$

$\equiv (a_3 - a_2) \cdot 4 + (a_3 - a_1) \cdot 3 + \cancel{5}a_3 + a_0 \mod 13$

Hausübungen

3.a) Für die Gewichte betrachtet man die Zehnerpotenzen mod 6

$10 \equiv \underline{\underline{4}} \mod 6 \quad | \quad 100 = 10 \cdot 10 \equiv 4 \cdot 4 = 16 \equiv \underline{\underline{4}} \mod 6$

$1000 = 10 \cdot 100 \equiv 4 \cdot 4 = 16 \equiv \underline{\underline{4}} \mod 6$

Die Gewichte sind ab der Zehnerziffer offensichtlich immer 4. $g_i = 4$ für $i = 1, 2, 3, 4, \dots$

Regel: Bilde ab der 2. Stelle die Quersumme, multipliziere diese mit 4 und addiere die Einerziffer. Ist das Ergebnis durch 6 teilbar, so auch die Ausgangszahl.

Beispiel: $\underbrace{15823}_{\text{QS } 19}4$ $\qquad 19 \cdot 4 + 4 = 80 = 6 \cdot 13 + 2$

Da die gewichtete QS kongruent zur Ausgangszahl ist, gilt $158234 \equiv 80 \mod 6$

$\equiv 2 \mod 6$

Probe mit dem Taschenrechner: $158234 = 6 \cdot 26372 + 2$

b. Formale Regel:

$$a = a_n \cdot 10^n + a_{n-1} \cdot 10^{n-1} + \cdots + a_2 \cdot 100 + a_1 \cdot 10 + a_0$$

$$b = a_n \cdot 2 + a_{n-1} \cdot 2 + \cdots + a_2 \cdot 2 + a_1 \cdot 2 + a_0$$

Für die gewichtete QS haben wir in a) ab der Zehnerstelle 4 genommen. Man könnte auch mit -2 rechnen, da $4 \equiv -2 \mod 6$ ist. Also:

$$b' = a_n \cdot (-2) + a_{n-1} \cdot (-2) + \cdots + a_2 \cdot (-2) + a_1 \cdot (-2) + a_0$$

Man sieht $b' = -b$

Also $a \equiv b' \mod 6$, da b' gewichtete QS zu a

Im Sonderfall $a \equiv b' \equiv 0 \mod 6$ gilt auch

$b' \equiv b \mod 6$

Ist b durch 6 teilbar (ohne Rest), so ist es auch a.

Aber: Lässt b einen Rest ungleich 0, so ist das nicht unbedingt der Rest von a beim Teilen durch 6.

Beispiel: $a = 182 = 30 \cdot 6 + 2 \Rightarrow$ Rest 2 ← ungleich

$b = (1+8) \cdot 2 - 2 = 16 = 2 \cdot 6 + 4 \Rightarrow$ Rest 4

4. Zehnerpotenzen mod 7

$10 \equiv \underline{3} \mod 7 \parallel 100 = 10 \cdot 10 \equiv 3 \cdot 3 = 9 \equiv \underline{\underline{2}} \mod 7$

$1000 = 10 \cdot 100 \equiv 3 \cdot 2 = 6 \equiv \underline{-1} \mod 7$

$10.000 \equiv -3 \mod 7 \parallel 100.000 \equiv -2 \mod 7 \parallel 10^6 \equiv 1 \mod 7$

„Gewichte die Quersumme alternierend mit 1, 3, 2. Ist das Ergebnis durch 7 teilbar, so ist es auch die Ausgangszahl."

Beispiel 1: $5371 \cdot 7 = 37597$ (Gewichte: $-3\ -1\ 2\ 3\ 1$)

$-9 - 7 + 10 + 27 + 7 = 44 - 16 = 28 = 7 \cdot 4$

Rest 0

Beispiel 2: $68236 \cdot 7 + 5 = 477657$ (Gewichte: $-2\ -3\ -1\ 2\ 3\ 1$)

$-8 - 21 - 7 + 12 + 15 + 7 = 34 - 36 = -2$

Rest 5

Beispiel 3: 123123 (Gewichte: $-2\ -3\ -1\ 2\ 3\ 1$) gew. QS ist 0 $\Rightarrow$ durch 7 teilbar

$\Rightarrow$ Zahlen der Form abcabc sind durch 7 teilbar

5. A: Beweis über die Definition der Kongruenz

Voraus: $a \cdot b \equiv c \mod m \Leftrightarrow a \cdot b - c = k_1 m$, $k_1 \in \mathbb{Z}$

$b \equiv d \mod m \Leftrightarrow b - d = k_2 m$, $k_2 \in \mathbb{Z}$

$\Leftrightarrow d = b - k_2 m$

Behauptung: $a \cdot d \equiv c \mod m \Leftrightarrow ad - c = k_3 m$, $k_3 \in \mathbb{Z}$

Beweis:

$ad - c \overset{!}{=} a \cdot (b - k_2 m) - c$

$= ab - ak_2 m - c$ (ausklammultiplizieren)

$= \underbrace{ab - c} - ak_2 m$ (umordnen)

$= k_1 m - ak_2 m$ (Voraus. einsetzen)

$= m \underbrace{(k_1 - ak_2)}$ (ausklammern)

$= m \cdot k_3$ (umbenennen)

q.e.d.

B: Beweis durch Rechnen mit Kongruenzen

$b \equiv d \mod m$
$a \equiv a \mod m$ $\Big\} \cdot$

$ab \equiv ad \mod m$

$ab \equiv c \mod m$ (Voraus.)

$\Rightarrow ad \equiv c \mod m$

(Transitivität von $\equiv$)

6. Die Bedingung selbst fordert, dass man (A) und (B) umdrehen muss.
Auf der anderen Seite darf dann keine 5 stehen.
Äquivalent dazu ist die Kontraposition:
Wenn die Ziffer eine 5 ist, dann ist der Buchstabe nicht A und nicht B.
Man muss also (5) umdrehen und testen, ob dort weder A noch B steht.

7.a) Bildet man fortgesetzt Potenzen einer Zahl a modulo m, beobachtet man, dass die Folge periodisch wird.

Beisp. $10^0 = 1 \equiv 1 \bmod 7$ $\quad 10^1 = 10 \equiv 3 \bmod 7$

$10^2 = 100 \equiv 2 \bmod 7$ $\quad 10^3 \equiv \cancel{1}\,6 \bmod 7$

$10^4 \equiv 4 \bmod 7$ $\quad 10^5 \equiv 5 \bmod 7$

$10^6 \equiv 1 \bmod 7$

Für $a = 10$ und $m = 7$ (Aufg 4) ist $x = 0$ $y = 6$ eine gesuchte Lösung

oder $a = 10$, $m = 6$ (Aufg. 3)

$10^0 \equiv 1 \bmod 6$ $\quad 10^1 \equiv 4 \bmod 6$ $\quad 10^2 \equiv 4 \bmod 6$

also $x = 1$, $y = 1$

b) „Löst" man die Potenzen immer so auf, dass die kongruente Zahl b zwischen 0 (einschl.) und m (ausschl.) liegt, gilt

$a^0 = b_0 \bmod m$, $a^1 \equiv b_1 \bmod m$, ..., $a^k \equiv b_k \bmod m$

mit $b_k \in \{0, 1, 2, \ldots, m-1\}$ Das sind nur endlich viele Zahlen. Dann muss sich nach m Potenzen der Rest b_k mindestens einmal wiederholen.