

# EZT Cheatsheet

By Navid Roux from 2020-01-14 for EZT as taught in WS 20/21; licensed under [CC BY-SA 4.0](#).

1. Vor Abgabe der Klausur
2. Verschieden Kleines
3.  $\text{ggT}(a, b)$  und erw. Euklidischer Algorithmus
4.  $\text{kgV}(a, b)$
5. Lösungen von  $ax + by = c$  mit  $(x, y) \in \mathbb{Z}^2$
6. Inverse in  $\mathbb{Z}/m\mathbb{Z}$ 
  1. additiv
  2. multiplikativ
7. Bestimme Rest von  $a^b \div m$
8. Eulersche  $\varphi$ -Funktion, Satz von Euler und kleinem Fermat
9. Chinesischer Restsatz
10. Basissysteme
  1. Konvertierung Dezimalsystem  $\rightarrow$  b-System
  2. Schriftliches Addieren/Subtrahieren zur Basis b
11. Dezimalbruchentwicklung
  1. Konstruktion periodischer Zahlen
  2. Kettenbruchdarstellung rationaler Zahlen
12. Teilbarkeit
  1. Teilbarkeit bzgl. Zahl mit nur Primfaktoren  $\{2, 5\}$
  2. Quersummenregeln
  3. Teilbarkeit bzgl. 7 und 11

## Vor Abgabe der Klausur

- Sind überall Striche für Restklassen?
- Überall Proben berechnet? Auch bei CRT-Aufgabe?
- Überall Antwortsätze geschrieben?

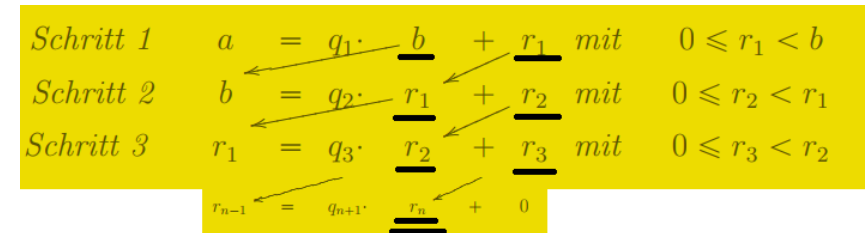
## Verschieden Kleines

- Über  $\mathbb{Z}$  gilt:  $(x \mid z) \wedge (y \mid z) \Rightarrow (ux + vy \mid z)$
- Teilbarkeit bzgl. 0:
  - $0 \mid 0, a \mid 0$
  - $0 \mid b \Rightarrow b = 0$  ("Null ist nur Teiler von Null")
- Umwandlung mod-Gleichung  $\leftrightarrow$  Teilbarkeitsgleichung:  $b \equiv c \pmod{a} \Leftrightarrow a \mid (b - c)$
- Alle ungeraden Quadratzahlen  $\equiv 1 \pmod{8}$ :  
 $q^2 = (2n + 1)^2 = 4n^2 + 4n + 1 = 4n(n + 1) + 1 \equiv 1$ , da  $8 \mid 4n(n + 1)$ , denn  $n(n + 1)$  enthält

Faktor 2.

- Für Ring  $R$  ist  $a \in R$  Nullteiler, wenn es  $b \in R$  gibt, sodass:  $a \neq 0 \wedge b \neq 0 \wedge ab = 0$ .  
(Diese Definition der Vorlesung sieht 0 nicht als Nullteiler entgegen weitläufiger Literatur.)
- $\mathbb{Z}/m\mathbb{Z}$  hat
  - invertierbare Elemente  $\{\bar{a} \mid a \in \{1, \dots, m-1\} \wedge \text{ggT}(a, m) = 1\}$
  - Nullteiler  $\{\bar{a} \mid a \in \{1, \dots, m-1\} \wedge \text{ggT}(a, m) \neq 1\}$

## $\text{ggT}(a, b)$ und erw. Euklidischer Algorithmus



Erweiterte Variante: durch Rückeinsetzen  $\text{ggT}(a, b) = r_n$  als Linearkombination von  $a$  und  $b$  ausdrücken.

## $\text{kgV}(a, b)$

- manuell:

$$\begin{aligned} \text{kgV}(120, 315) &= 5 \cdot \text{kgV}(2 \cdot 12, 63) = 5 \cdot \text{kgV}(2 \cdot 3 \cdot 4, 3 \cdot 21) \\ &\quad \parallel \quad \parallel \\ &\quad 10 \cdot 12 \quad 5 \cdot 63 \\ &= 3 \cdot 5 \cdot \text{kgV}(2 \cdot 4, 3 \cdot 7) \\ &\quad \quad \quad \uparrow \quad \uparrow \\ &\quad \quad \quad \text{teilerfremd} \\ &= 3 \cdot 5 \cdot 2 \cdot 4 \cdot 3 \cdot 7 = 2^3 \cdot 3^2 \cdot 5 \cdot 7 = 2520 \end{aligned}$$

- geschickter: nutze  $\text{ggT}(a, b) \cdot \text{kgV}(a, b) = a \cdot b$
- für  $\text{ggT}(a, b) = 1 \Rightarrow \text{kgV}(a, b) = a \cdot b$

## Lösungen von $ax + by = c$ mit $(x, y) \in \mathbb{Z}^2$

**Problem:** gesucht ist Lösungsmenge von  $ax + by = c$  über  $\mathbb{Z}^2$  mit  $a, b, c \in \mathbb{Z}$  gegeben.

**Lösung:**

1. Berechne  $\text{ggT}(a, b)$  mit erw. Euklidischen Algorithmus
2. Falls *nicht*  $\text{ggT}(a, b) \mid c$ , dann unlösbar nach Satz 4.15. Terminiere.

**Satz 4.15:** Es gilt:

$$\text{im}(\underbrace{ax + by}_{\in \mathbb{Z}[x,y]}) = \text{ggT}(a, b)\mathbb{Z}$$

$$\text{im}(\underbrace{a_1x_1 + \dots + a_nx_n}_{\in \mathbb{Z}[x_1, \dots, x_n]}) = \text{ggT}(a_1, \dots, a_n)\mathbb{Z}$$

3. Berechne Bezout-Koeffizienten:  $\text{ggT}(a, b) = ax^* + by^*$

Falls  $\text{ggT}(a, b) \neq 1$ , dann betrachte restlichen Algorithmus über durch  $\text{ggT}(a, b)$  geteilte Gleichung (Lsg.menge bleibt gleich):

$$\underbrace{\frac{a}{\text{ggT}(a, b)}}_{\text{neues } a}x + \underbrace{\frac{b}{\text{ggT}(a, b)}}_{\text{neues } b}y = \frac{c}{\text{ggT}(a, b)}$$

Die Bezout-Koeffizienten für die "neuen  $a$ s und  $b$ s" sind *dieselben*, denn:

$$\frac{a}{\text{ggT}(a, b)}x^* + \frac{b}{\text{ggT}(a, b)}y^* = \frac{1}{\text{ggT}(a, b)}(ax^* + by^*) = 1.$$

Insgesamt nötig, da sonst Satz 4.18 in Schritt 5 nicht anwendbar.

4. Berechne **Partikularlösung**, angenommen  $ax^* + by^* = 1 = \text{ggT}(a, b)$

Sei  $\text{ggT}(a, b) \mid c$  via  $q$  (d.h.  $q \cdot \text{ggT}(a, b) = c$ ).

$$\Rightarrow a(qx^*) + b(qy^*) = q \cdot \text{ggT}(a, b) = c$$

$$\Rightarrow (x_0, y_0) := (qx^*, qy^*) \text{ Partikularlösung}$$

5. Berechne **alle Lösungen**:  $\mathcal{L} = \{(x_0 + t \cdot b, y_0 - t \cdot a) \mid t \in \mathbb{Z}\}$  (Satz 4.18)

Je nach Anwendungsaufgabe, stelle  $x_0 + t \cdot b \geq 0$  und  $y_0 - t \cdot a \geq 0$  auf; löse nach  $t$ , um alle (endlich) viele Lösungen zu erschließen.

**Merke:** Eine lineare diophantische Gleichung hat entweder 0 oder unendlich viele Lösungen.

**Beispiele:**

- Finde alle Lösungen von  $6x + 4y = 14$ .

$$1. \text{ggT}(6, 4) = 2 = \underbrace{1}_{x^*} \cdot 6 + \underbrace{(-1)}_{y^*} \cdot 4$$

$$2. \text{ggT}(6, 4) = 2 \mid 14 \Rightarrow \text{lösbar.}$$

$$3. 6x + 4y = 14 \Leftrightarrow 3x + 2y = 7 \text{ und } \text{ggT}(3, 2) = \underbrace{1}_{x^*} \cdot 3 + \underbrace{(-1)}_{y^*} \cdot 2$$

$$4. \text{Partikularlösung } (x_0, y_0) = (7, -7)$$

5. Lösungsmenge

$$\mathcal{L} = \{(7 + 2 \cdot t, -7 - 3 \cdot t) \mid t \in \mathbb{Z}\} = \{\dots, (5, -4), \underline{(7, -7)}, (9, -10), (11, -13), \dots\}$$

- Werbegeschenkaufgabe von Skript S. 44: Wie viele nichtnegative Lösungspaare von  $19x + 13y = 1000$  gibt es? 4 mittels Algorithmus oben.

Wie viele gibt es für  $31x + 23y = 1000$ ? 13 Lösungspaare.

- Gleichung mit negativen Koeffizienten:  $-51x + 5y = 13$

$$1. \text{ggT}(-51, 5) = 1 (= \text{ggT}(51, 5))$$

$$\begin{aligned} -51 &= -11 \cdot 5 + 4 \\ 5 &= 1 \cdot 4 + 1 \\ 4 &= 4 \cdot 1 + 0 \end{aligned}$$

$$\Rightarrow 1 = (-1) \cdot (-51) + (-10) \cdot (5)$$

$$2. \text{ggT}(-51, 5) = 1 \mid 13 \Rightarrow \text{lösbar.}$$

3. -/-

$$4. \text{Partikularlösung } (x_0, y_0) = (-13, -130)$$

$$5. \text{Lösungsmenge } \mathcal{L} = \{(-13 + 5 \cdot t, -130 - (-51) \cdot t) \mid t \in \mathbb{Z}\}$$

## Inverse in $\mathbb{Z}/m\mathbb{Z}$

**additiv**

**Problem:** gesucht ist Inverses von  $\bar{a} \in \mathbb{Z}/m\mathbb{Z}$

**Lösung:**  $\overline{-a} = \overline{-a + m}$

**multiplikativ**

**Problem:** gesucht ist Inverses von  $\bar{a} \in \mathbb{Z}/m\mathbb{Z}$ ,  $0 \leq a < m$ !!!

**Lösung (wenn raten zu aufwendig):**

1. Wende erw. Euklidischen Algorithmus auf  $(m, a)$

- Inverses existiert gdw.  $\text{ggT}(a, m) = 1$ .
- Sei  $x^*$  der (ggf. negative!) Bezout-Koeffizient für  $a$ . Dann ist  $\bar{a}^{-1} = \overline{x^*}$ .

2. Normalisiere  $x^*$  auf kanonischen Repräsentanten in  $\{0, \dots, m-1\}$ .

(Alternative Sichtweise: löse  $ax + my = 1$ , nehme Partikularlösung  $x^*$  und normalisiere.

Denn i. Allg. ist  $x$  ein Inverses von  $a$  modulo  $m$  gdw.

$$ax \equiv 1 \pmod{m} \Leftrightarrow m \mid ax - 1 \Leftrightarrow \exists y. ax - my = 1 \Leftrightarrow \exists y. ax + my = 1.)$$

**Beispiele:**

$$\bullet \text{ In } \mathbb{Z}/13\mathbb{Z}: \bar{6}^{-1} = \overline{11}$$

$$\bullet \text{ In } \mathbb{Z}/89\mathbb{Z}: \overline{15}^{-1} = \bar{6}$$

## Bestimme Rest von $a^b \div m$

**Problem:** bestimme Rest von  $a^b \div m$  mit  $a, m$  teilerfremd

**Lösung:** Dekomponiere Exponent  $b = \varphi(m) \cdot c + d$  und wende Satz von Euler an:

$$\overline{a^b} = \overline{(a^{\varphi(m)})^c \cdot a^d} = \underbrace{\overline{(a^{\varphi(m)})^c}}_{=1 \text{ (Euler)}} \cdot \overline{a^d} = \overline{a^d}$$

(Rechnung in  $\mathbb{Z}/m\mathbb{Z}$ ; [Onlinetool hier](#))

**Beispiel:** Rest von  $3^{387} \div 35$

3 und 35 sind teilerfremd,  $\varphi(35) = \varphi(5 \cdot 7) = \varphi(5) \cdot \varphi(7) = 4 \cdot 6 = 25$  und es gilt:

$$\overline{3^{387}} = \overline{(3^{24})^{16} \cdot 3^3} = \underbrace{\overline{(3^{24})^{16}}}_{=1} \cdot \overline{3^3} = \overline{27}$$

**Problem:** bestimme Rest von  $a^b \div m$  mit  $a, m$  nicht teilerfremd

**Lösung:**

1. Betrachte  $(\overline{a}, \overline{a^2}, \overline{a^3}, \dots, \overline{a^s} = \overline{a}, \dots) \subseteq \mathbb{Z}/m\mathbb{Z}$  und identifiziere Periodenlänge  $s$ .
2. Dekomponiere Exponent  $b = s \cdot c + d$  und vereinfache:

$$\overline{a^b} = \overline{(a^s)^c \cdot a^d} = \overline{a^s}^c \cdot \overline{a^d} = \overline{a^c} \cdot \overline{a^d} = \overline{a^{c+d}}$$

(Rechnung in  $\mathbb{Z}/m\mathbb{Z}$ )

**Beispiel:** Rest von  $2^{18} \div 10$

$$\overline{2^{18}} = \overline{(2^5)^3 \cdot 2^3} = \overline{2^5}^3 \cdot \overline{2^3} = \overline{2^3} \cdot \overline{2^3} = \overline{2^6} = \overline{64} = \overline{4}$$

da aus  $(\overline{2}, \overline{4}, \overline{8}, \overline{6}, \overline{2} = \overline{2^5}, \dots)$  Periodenlänge  $s = 5$  abgelesen werden kann.

# Eulersche $\varphi$ -Funktion, Satz von Euler und kleinem Fermat

**Satz (von Euler, 5.24):** Seien  $a, m$  teilerfremd, dann  $a^{\varphi(m)} \equiv 1 \pmod{m}$ .

*Beweis:*  $a, m$  teilerfremd  $\Rightarrow \overline{a} \in \mathbb{Z}_m^* \Rightarrow \overline{1} = \overline{a}^{\text{ord}(\mathbb{Z}_m^*)} = \overline{a}^{\varphi(m)}$ ; group element raised to group order always 1

**Korollar (vom kleinen Fermat, 5.26):** Für  $a \in \mathbb{N}, p$  prim gilt:  $a^p \equiv a \pmod{p}$

*Beweis:* Wenn  $p \mid a$ , trivial  $0 \equiv 0$ . Sonst  $\text{ggT}(a, p) = 1$  und  $a^p \equiv a^{p-1}a \equiv a$  nach Satz von Euler.

**Satz:** Es gilt

- für Primzahlen  $p, n \geq 1$

$$\varphi(p^n) = p^{n-1}(p-1)$$

- für  $\text{ggT}(a, b) = 1$

$$\varphi(a \cdot b) = \varphi(a) \cdot \varphi(b)$$

*Beweis erster Punkt:* Satz 5.28.

*Beweis zweiter Punkt (siehe auch hier):* Nach CRT haben wir  $\mathbb{Z}/(ab\mathbb{Z}) \cong \mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z}$  als Ringe. D.h. Anzahl invertierbarer Elemente von LHS ist dieselbe wie von RHS. Ein Element  $(x, y)$  von RHS ist invertierbar gdw.  $x$  in  $\mathbb{Z}/a\mathbb{Z}$  invertierbar und  $y$  in  $\mathbb{Z}/b\mathbb{Z}$  invertierbar ist. Es gibt also  $\varphi(a) \cdot \varphi(b)$  viele invertierbare Elemente der RHS.

# Chinesischer Restsatz

**Problem + Beispiel:** bestimme Lösungsmenge von Gleichungssystem mit Gleichungen der Form  $x \equiv a_i \pmod{m_i}$

- $x \equiv 3 \pmod{5}$
- $x \equiv 1 \pmod{7}$
- $x \equiv 2 \pmod{11}$

mit  $m_i$  paarweise teilerfremd.

**Lösung:** Es gibt eine Lösung  $x$  (eindeutig in  $\mathbb{Z}/m\mathbb{Z}$ , mit  $m := \prod m_i$ )

Konstruiere *eine* Lösung  $x := a_1q_1q'_1 + a_2q_2q'_2 + a_3q_3q'_3$  mit

- $q_1 := 7 \cdot 11 = 77$

In  $\mathbb{Z}/5\mathbb{Z}$ :  $\overline{q_1} = \overline{2}, \quad \overline{2}^{-1} = \overline{3} \Rightarrow$  wähle  $q'_1 := 3$ . (i. Allg. ist  $q'_1 \in 3 + 5\mathbb{Z}$  möglich)

- $q_2 := 5 \cdot 11 = 55$

In  $\mathbb{Z}/7\mathbb{Z}$ :  $\overline{q_2} = \overline{6}, \quad \overline{q_2}^{-1} = \overline{6} \Rightarrow$  wähle  $q'_2 := 6$

- $q_3 := 5 \cdot 7 = 35$

In  $\mathbb{Z}/11\mathbb{Z}$ :  $\overline{q_3} = \overline{2}, \quad \overline{q_3}^{-1} = \overline{6} \Rightarrow$  wähle  $q'_3 := 6$

$$\Rightarrow x = 3 \cdot 77 \cdot 3 + 1 \cdot 55 \cdot 6 + 2 \cdot 35 \cdot 6 = 1443$$

Mit  $m := m_1m_2m_3 = 385$  ist Lösungsmenge  $\mathcal{L} = x + m\mathbb{Z} = 1443 + 385\mathbb{Z} = 288 + 385\mathbb{Z}$ .

Hier ist  $x \% m = 1443 \% 385 = 288$  kanonischer Repräsentant.

**Beachte:** Bei Berechnung von  $x$  muss etwa 77 stehen, anderer Repräsentant bzgl.  $\mathbb{Z}/5\mathbb{Z}$  nicht möglich. Für  $q'_i$  ist jedoch beliebige Repräsentantenwahl in  $\mathbb{Z}/m_i\mathbb{Z}$  möglich.

Andere Formulierung:

**Satz (CRT, Formulierung aus Internet):** Wenn  $m_1, \dots, m_k$  paarweise teilerfremd, dann

$$\mathbb{Z}/m \cong \mathbb{Z}/m_1 \times \dots \times \mathbb{Z}/m_k$$

als Ringe.

Falls in Gleichungen Koeffizienten vor  $x$  auftauchen: wende erweiterten CRT an.

# Basissysteme

## Konvertierung Dezimalsystem $\rightarrow$ b-System

Immer durch  $b$  teilen, Reste sind  $b$ -Ziffern.

Gesucht: 8924 zur Basis 12

8924	=	743	·	12	+	8		^	least significant digit
743	=	61	·	12	+	11			
61	=	5	·	12	+	1			
5	=	0	·	12	+	5			
								----	
								^	
									terminiert bei 0
Ergebnis: 51B8 <sub>(12)</sub>									

**Nicht mit Euklidischem Algorithmus verwechseln!**

Probe mit TR! Auf Casio fx-991DE Plus: Mode -> Pfeil runter -> 3 (Base-N) -> 8924 eingeben -> Dec/Hex/Bin/Oct-Taste drücken

## Schriftliches Addieren/Subtrahieren zur Basis b

Beispiele:

- $455_6 + 1_6 = 500_6$
- $210_3 - 1_3 = 202_3$
- $2302_4 - 233_4 = 2003_4$  (tricky mit Borrow und Carry!)

$$\begin{array}{r} 2 \quad 3 \quad 0 \quad 2 \\ - \quad 2_1 \quad 3_1 \quad 3 \\ \hline 2 \quad 0 \quad 0 \quad 3 \end{array}$$

## Dezimalbruchentwicklung

**Problem:** bestimme Art der Dezimalbruchentwicklung (endlich, rein- oder gemischtperiodisch) eines gegebenen Bruches  $\frac{m}{n}$

**Lösung:**

1. Stelle sicher, dass Bruch vollständig gekürzt ist: bestimme  $\text{ggT}(m, n)$  und kürze damit.
2. Bestimme PFZ des Nenners.
3. Wende unten stehende Sätze an.

**Sätze 7.1, 7.2 & 7.4, 7.6:** Ein Bruch  $\frac{m}{n}$  mit  $m < n$  und  $\text{ggT}(m, n) = 1$  ("vollständig gekürzt") hat

- *endliche* Dezimalentwicklung  $0.q_1 \dots q_s \Leftrightarrow n = 2^a \cdot 5^b$   
Entwicklung hat Stellen  $s := \max(a, b)$ .
- *reinperiodische* Dezimalentwicklung  $0.\overline{q_1 \dots q_s} \Leftrightarrow \text{ggT}(n, 10) = 1$   
Periodenlänge  $s := \min_{s \in \mathbb{N}} n \mid (10^s - 1)$
- *gemischtperiodische* Dezimalentwicklung  $0.p_1 \dots p_t \overline{q_1 \dots q_s} \Leftrightarrow n = n_1 \cdot n_2$  mit  $n_1, n_2 > 1$  und  $n_1 \mid 10^t$  ( $t$  minimal),  $\text{ggT}(n_2, 10) = 1$   
 $t$  Vorziffern; Periodenlänge  $s$  ist die von  $\frac{1}{n_2}$

**Beispiele:**

- $\frac{3}{125}$  hat endliche Dezimalbruchentwicklung:

$$\frac{3}{125} = \frac{3}{5^3} = \frac{3 \cdot 2^3}{5^3 \cdot 2^3} = \frac{24}{10^3} = 0.024$$

- $\frac{1}{15}$  hat gemischtperiodische Dezimalbruchentwicklung:

$$15 = 5 \cdot 3 =: n_1 \cdot n_2$$

$\Rightarrow t = 1$  Vorziffern und Periodenlänge  $1 = \min_{s \in \mathbb{N}} 3 \mid (10^s - 1)$ ; in der Tat  $15 = 0.0\overline{6}$ .

- $\frac{1}{28}$  hat gemischtperiodische Dezimalbruchentwicklung:

$$28 = 2^2 \cdot 7 =: n_1 \cdot n_2$$

$\Rightarrow t = 2$  Vorziffern und Periodenlänge  $6 = \min_{s \in \mathbb{N}} 7 \mid (10^s - 1)$ ; in der Tat  $28 = 0.03\overline{571428}$ .

## Konstruktion periodischer Zahlen

**Problem:** stelle  $0.\overline{0173}$  als Bruch dar

**Lösung:** Sei  $z = 173$  die Periode und  $s = 4$  die Periodenlänge  $s = 4$ . Suche also  $a, b$ , sodass

$$\begin{aligned} \frac{a}{b} \cdot 10^s &\stackrel{!}{=} z + \frac{a}{b} \\ \Leftrightarrow \frac{a}{b} &= \frac{z}{10^s - 1} = \frac{173}{9999} = 0.\overline{0173} \end{aligned}$$

## Kettenbruchdarstellung rationaler Zahlen

**Problem:** gesucht ist Kettenbruchdarstellung von  $\frac{a}{b}$

**Lösung (wenn  $a > b$ ):** wende Euklidischen Algorithmus an

(es ist egal, ob  $a, b$  teilerfremd oder nicht)

Beispiel:  $203/95$

$$\begin{array}{rcl} 203 & = & \overline{2} \cdot 95 + 13 \\ 95 & = & \overline{7} \cdot 13 + 4 \\ 13 & = & \overline{3} \cdot 4 + 1 \\ 4 & = & \overline{4} \cdot 1 + 0 \\ & & \text{-----} \end{array}$$

Darstellung:  $203/95 = [2; 7, 3, 4]$

$$\frac{203}{95} = 2 + \frac{13}{95} = 2 + \frac{1}{\frac{95}{13}} = 2 + \frac{1}{7 + \frac{4}{13}} = 2 + \frac{1}{7 + \frac{1}{\frac{13}{4}}} = 2 + \frac{1}{7 + \frac{1}{3 + \frac{1}{4}}}$$

Alternative Methode: manuell Kettenbrüche erzeugen, bis am Ende Bruch mit 1 im Zähler wie  $\frac{1}{4}$  (aka Stambruch).

**Lösung (wenn  $a < b$ ):** berechne Darstellung für  $\frac{b}{a}$  und prepende 0

Beispiel:  $95/203$

$$\begin{aligned} \text{wie oben: } 203 / 95 &= [2; 7, 3, 4] \\ \text{daher: } 95 / 203 &= [0; 2, 7, 3, 4] \end{aligned}$$

## Teilbarkeit

Teilbarkeit bzgl. Zahl mit nur Primfaktoren  $\{2, 5\}$

**Satz (Endstellenregeln; Generalisierung der Sätze 8.1, 8.3):** Sei  $t \mid 10^s$ , dann gilt

$$z_n \dots z_0 \equiv z_{s-1} \dots z_0 \pmod{t}$$

*Beweis:*  $z_n \dots z_0 = \sum_{i=0}^n z_i 10^i \equiv \sum_{i=0}^{s-1} z_i 10^i = z_{s-1} \dots z_0 \pmod{t}$ .

**Beispiele:**

- 2, 5, 10 Teiler von 10  $\Rightarrow$  Teilbarkeit auf letzte Stelle reduzierbar
- 4, 25, 50, 100 Teiler von 100  $\Rightarrow$  Teilbarkeit auf letzte zwei Stellen reduzierbar

$$4 \mid 87954236 \Leftrightarrow 4 \mid 36 \Leftrightarrow \text{wahr}$$

- 8, 125, 200, ... Teiler von 1000  $\Rightarrow$  Teilbarkeit auf letzte drei Stellen reduzierbar

## Quersummenregeln

**Satz (Quersummenregeln; Sätze 8.4, 8.5, und Paragraph danach im Skript):**

Für  $t \mid 9$ :

$$z_n \dots z_0 \equiv z_n + \dots + z_0 \pmod{t}$$

Für  $t \mid 99$ :

$$z_n \dots z_0 \equiv z_n z_{n-1} + \dots + z_1 z_0 \pmod{t}$$

Für  $t \mid 999$ :

$$z_n \dots z_0 \equiv z_n z_{n-1} z_{n-2} + \dots + z_2 z_1 z_0 \pmod{t}$$

Das sind Quersummen 1-, 2-, 3- und i. Allg.  $s$ -ter Ordnung. (Um Notation für die Gruppierungen oben zu sparen, setzen wir oBdA.  $s \mid (n+1)$  voraus, ansonsten linkspadde mit Nullen.)

**Beispiele:**

- $11 \mid 21748 \Leftrightarrow 11 \mid (01 + 17 + 48) \Leftrightarrow 11 \mid 66 \Leftrightarrow \text{wahr}$
- $111 \mid 21748 \Leftrightarrow 111 \mid (021 + 748) = 769 \Leftrightarrow \text{falsch}$

*Beweis:* (für  $t \mid 999$ ):

$$\begin{aligned} z_n \dots z_0 &= \sum_{i=0}^n z_i 10^i = (z_n \cdot 10^2 + z_{n-1} 10^1 + z_{n-2}) \cdot 10^{(3 \cdot k)} \\ &\quad + \dots \\ &\quad + (z_5 \cdot 10^2 + z_4 \cdot 10^1 + z_3) \cdot 10^{(3 \cdot 1)} \\ &\quad + (z_2 \cdot 10^2 + z_1 10^1 + z_0) \cdot 10^{(3 \cdot 0)} \\ &\equiv z_n z_{n-1} z_{n-2} + \dots + z_5 z_4 z_3 + z_2 z_1 z_0 \end{aligned}$$

**Satz (Alternierende Quersummenregel, Sätze 8.6, 8.7 + eigene Generalisierung):**

Für  $t \mid 11 = 10^1 + 1$ :

$$z_n \dots z_0 \equiv \dots - z_3 + z_2 - z_1 + z_0 \pmod{t}$$

Für  $t \mid 101 = 10^2 + 1$ :

$$z_n \dots z_0 \equiv \dots + z_5 z_4 - z_3 z_2 + z_1 z_0 \pmod{t}$$

Allgemein für  $t \mid (10^s + 1)$ :

$z_n \dots z_0 \equiv \text{alt. Quersumme } s\text{-ter Ordnung} \pmod{t}$

**Beispiele:**

- $11 \mid 6391 \Leftrightarrow 11 \mid (-6 + 3 - 9 + 1) = -11 \Leftrightarrow \text{wahr}$
- $101 \mid 691244 \Leftrightarrow 101 \mid (69 - 12 + 44) = 101 \Leftrightarrow \text{wahr}$
- $7 \mid 1001$ , daher:  $7 \mid z \Leftrightarrow 7 \mid \text{alt. Quersumme 3-ter Ordnung}$

## Teilbarkeit bzgl. 7 und 11

Siehe Skript S. 106ff.