Elementare Zahlentheorie: Cheatsheet

Erstellt von Navid Roux am 2020-01-15 als Prüfungsvorbereitung für Vorlesung *Elementare Zahlentheorie* gehalten im Wintersemester 2020/21 von Christina Birkenhake an der FAU Erlangen-Nürnberg.

Vor Abgabe der Klausur

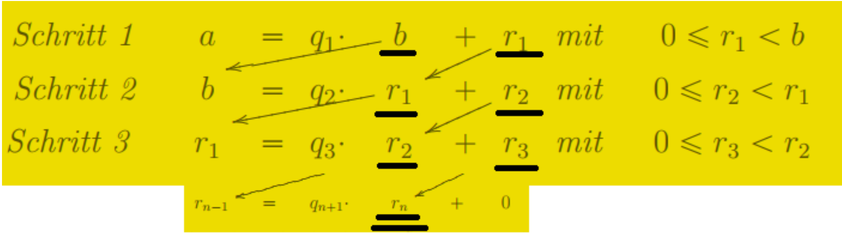
- Sind überall Striche für Restklassen?
- Überall Proben berechnet? Auch bei CRT-Aufgabe?
- Überall Antwortsätze geschrieben?

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 ↔ Teilbarkeitsgleichung: $b\equiv c \pmod a \Leftrightarrow a\mid(b-c)$
- Alle ungeraden Quadratzahlen $\equiv 1$ mod 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 $\{\overline{a}\mid a\in\{1,\dots,m-1\}\wedge\mathrm{ggT}(a,m)=1\}$
    - Nullteiler $\{\overline{a}\mid a\in\{1,\dots,m-1\}\wedge\mathrm{ggT}(a,m)\neq 1\}$

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



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

$\mathrm{kgV}(a,b)$

- manuell:

$$kgV(\underset{10\cdot 12}{\underset{\|}{120}},\underset{5\cdot 63}{\underset{\|}{315}}) = 5\cdot kgV(2\cdot 12, 63) = 5\cdot kgV(2\cdot 3\cdot 4, 3\cdot 21)$$
$$= 3\cdot 5\cdot kgV(\underbrace{2\cdot 4, 3\cdot 7}_{\text{teilerfremd}})$$
$$= 3\cdot 5\cdot 2\cdot 4\cdot 3\cdot 7 = 2^3\cdot 3^2\cdot 5\cdot 7 = 2520$$

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

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 $\mathrm{ggT}(a, b)$ mit erw. Euklidischen Algorithmus
> 2. Falls $\mathrm{ggT}(a, b) \nmid c$, dann unlösbar nach Satz 4.15. Terminiere.
>
>   > **Satz 4.15:** Es gilt:
>   >
>   > $$\mathrm{im}(\underbrace{ax + by}_{\in \mathbb{Z}[x,y]}) = \mathrm{ggT}(a, b)\mathbb{Z}$$
>
> $$\mathrm{im}(\underbrace{a_1x_1 + \ldots + a_nx_n}_{\in \mathbb{Z}[x_1,\ldots,x_n]}) = \mathrm{ggT}(a_1, \ldots, a_n)\mathbb{Z}$$
>
> 3. Berechne Bezout-Koeffizienten: $\mathrm{ggT}(a, b) = ax^* + by^*$
>
>   Falls $\mathrm{ggT}(a, b) \neq 1$, dann betrachte restlichen Algorithmus über durch $\mathrm{ggT}(a, b)$ geteilte Gleichung (Lsg.menge bleibt gleich):
>
> $$\underbrace{\frac{a}{\mathrm{ggT}(a, b)}}_{\text{neues } a} x + \underbrace{\frac{b}{\mathrm{ggT}(a, b)}}_{\text{neues } b} y = \frac{c}{\mathrm{ggT}(a, b)}$$
>
>   Die Bezout-Koeffzienten für die "neuen as und bs" sind *dieselben*, denn: $\frac{a}{\mathrm{ggT}(a,b)}x^* + \frac{b}{\mathrm{ggT}(a,b)}y^* = \frac{1}{\mathrm{ggT}(a,b)}(ax^* + by^*) = 1$.
>
>   Insgesamt nötig, da sonst Satz 4.18 in Schritt 5 nicht anwendbar.
>
> 4. Berechne **Partikularlösung**, angenommen $ax^* + by^* = 1 = \mathrm{ggT}(a, b)$
>
>   Sei $\mathrm{ggT}(a, b) \mid c$ via q (d.h. $q \cdot \mathrm{ggT}(a, b) = c$).
>
> $\Rightarrow a(qx^*) + b(qy^*) = q \cdot \mathrm{ggT}(a, b) = c$
> $\Rightarrow (x_0, y_0) := (qx^*, qy^*)$ 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 dipohantische Gleichung hat entweder 0 oder unendlich viele Lösungen.

Beispiele:

- Finde alle Lösungen von $6x + 4y = 14$.
  1. $\mathrm{ggT}(6, 4) = 2 = \underbrace{1}_{x^*} \cdot 6 + \underbrace{(-1)}_{y^*} \cdot 4$
  2. $\mathrm{ggT}(6, 4) = 2 \mid 14 \Rightarrow$ lösbar.
  3. $6x + 4y = 14 \Leftrightarrow 3x + 2y = 7$ und $\mathrm{ggT}(3, 2) = \overbrace{1}^{x^*} \cdot 3 + \overbrace{(-1)}^{y^*} \cdot 2$
  4. Partikularlösung $(x_0, y_0) = (7, -7)$
  5. Lösungsmenge
     $\mathcal{L} = \{(7 + 2 \cdot t, -7 - 3 \cdot t) \mid t \in \mathbb{Z}\} = \{\ldots, (5, -4), \underline{(7, -7)}, (9, -10), (11, -13), \ldots\}$
- 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. $\mathrm{ggT}(-51, 5) = 1\ (= \mathrm{ggT}(51, 5))$

     ```
     -51 = -11 · 5 + 4
       5 =   1 · 4 + 1
       4 =   4 · 1 + 0

     ⇒ 1 = (-1)·(-51) + (-10)·(5)
     ```

  2. $\mathrm{ggT}(-51, 5) = 1 \mid 13 \Rightarrow$ lösbar.
  3. -/-
  4. Partikularlösung $(x_0, y_0) = (-13, -130)$
  5. 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 $\overline{a} \in \mathbb{Z}/m\mathbb{Z}$

> **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. $\mathrm{ggT}(a, m) = 1$.
>   - Sei x^* der (ggf. negative!) Bezout-Koeffizient für a. Dann ist $\overline{a}^{-1} = \overline{x^*}$.
> 2. Normalisiere x^* auf kanonischen Repräsentanten in $\{0, \ldots, m - 1\}$.
>
> (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:

- In $\mathbb{Z}/13\mathbb{Z}$: $\overline{6}^{-1} = \overline{11}$
- In $\mathbb{Z}/89\mathbb{Z}$: $\overline{15}^{-1} = \overline{6}$

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

> (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:

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

> **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 identifziere 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 φ-Funktion, Satz von Euler und kleinem Fermat

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

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

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

Beweis: Wenn $p \mid a$, trivial $0 \equiv 0$. Sonst $\mathrm{ggT}(a, p) = 1$ 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 $\mathrm{ggT}(a, b) = 1$
>
> $$\varphi(a \cdot b) = \varphi(a) \cdot \varphi(b)$$

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 $\mathbb{Z}/bZ$ 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 $x \equiv a_i$ (mod m_i)
>
> - $x \equiv 3$ (mod 5)
> - $x \equiv 1$ (mod 7)
> - $x \equiv 2$ (mod 11)
>
> **mit m_i paarweise teilerfremd**.

> **Lösung:** Es gibt eine Lösung x (eindeutig in $\mathbb{Z}/m\mathbb{Z}$, mit $m := \Pi m_i$)
>
> Konstruiere *eine* Lösung $x := a_1 q_1 q_1' + a_2 q_2 q_2' + a_3 q_3 q_3'$ mit
>
> - $q_1 := 7 \cdot 11 = 77$
>
>   In $\mathbb{Z}/5\mathbb{Z}$: $\bar{q_1} = \bar{2}, \quad \bar{2}^{-1} = \bar{3} \Rightarrow$ wähle $q_1' := 3$. (i. Allg. ist $q_1' \in 3 + 5\mathbb{Z}$ möglich)
> - $q_2 = 5 \cdot 11 = 55$
>
>   In $\mathbb{Z}/7\mathbb{Z}$: $\bar{q_2} = 6, \quad \bar{q_2}^{-1} = \bar{6} \Rightarrow$ wähle $q_2' := 6$
> - $q_3 = 5 \cdot 7 = 35$
>
>   In $\mathbb{Z}/11\mathbb{Z}$: $\bar{q_3} = 2, \quad \bar{q_3}^{-1} = \bar{6} \Rightarrow$ wähle $q_3' := 6$
>
> $\Rightarrow x = 3 \cdot 77 \cdot 3 + 1 \cdot 55 \cdot 6 + 2 \cdot 35 \cdot 6 = 1443$
>
> Mit $m := m_1 m_2 m_3 = 385$ 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' is jedoch beliebige Repräsentenwahl 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 $\to$ 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₍₁₂₎
```

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!)

```
  2  3  0  2
-    2₁ 3₁ 3
------------
  2  0  0  3
```

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 $\mathrm{ggT}(m, n)$ 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 $\mathrm{ggT}(m, n) = 1$ ("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 $0.\overline{q_1 \dots q_s} \Leftrightarrow \mathrm{ggT}(n, 10) = 1$
>
>   Periodenlänge $s := \min_{s \in \mathbb{N}} n \mid (10^s - 1)$
> - *gemischtperiodische* Dezimalentwicklung $0.p_1 \dots p_t \overline{q_1 \dots q_s} \quad \Leftrightarrow \quad n = n_1 \cdot n_2$ mit $n_1, n_2 > 1$ und $n_1 \mid 10^t$ (t minimal), $\mathrm{ggT}(n_2, 10) = 1$
>
> 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
>
> $$\frac{a}{b} \cdot 10^s \overset{!}{=} z + \frac{a}{b}$$
>
> $$\Leftrightarrow \quad \frac{a}{b} = \frac{z}{10^s - 1} = \frac{173}{9999} = 0.\overline{0173}$$

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
>
>              ___
> 203 = | 2 | · 95 + 13
>  95 = | 7 | · 13 +  4
>  13 = | 3 | ·  4 +  1
>   4 = | 4 | ·  1 +  0
>       -----
>
> 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 $a < b$):** bereche Darstellung für $\frac{b}{a}$ und prepende 0
>
> ```
> Beispiel: 95/203
>
> wie oben: 203 /  95 = [2; 7, 3, 4]
> daher:     95 / 203 = [0; 2, 7, 3, 4]
> ```

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: $z_n \dots z_0 = \sum_{i=0}^{n} z_i 10^i \equiv \sum_{i=0}^{s-1} z_i 10^i = z_{s-1} \dots z_0$ (mod t).

Beispiele:

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

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

- 8, 125, 200, ... Teiler von 1000 ⇒ 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 $t \mid 999$*):*

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

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.