WiSe'21/'22, hhu
K. Halupczok

Vorlesung Einführung in die Zahlentheorie

EZ6: Kongruenzrechnung

Stichworte: Kongruenz, modulo, Restklassen, inverse Restklasse, reduzierte Restklasse, Restklassensysteme, Lineare Kongruenz, Restklassenring, Chinesischer Restsatz, g-adische Darstellung / Ziffernsysteme, Teilbarkeitsregeln

---

6.1. Einleitung: Bei Division durch eine feste Zahl $m \in \mathbb{N}$ bilden die kleinsten nichtnegativen Reste eine m-periodische Folge. Zum Studium zahlentheoretischer Probleme ist die Reduzierung natürlicher Zahlen auf Reste häufig zielführend. Die Kongruenzenrechnung lässt sich als Rechnen in Restklassenringen algebraisch verstehen. Anwendungen sind der chinesische Restsatz und z.B. Teilbarkeitsregeln für natürliche Zahlen im Dezimalsystem.

6.2. Def. (Kongruenz modulo m): Für $m \in \mathbb{N}$ heißen $a, b \in \mathbb{Z}$ kongruent modulo m, wenn $m \mid (b-a)$, d.h. wenn $b = gm + a$ für ein $g \in \mathbb{Z}$ ist.

Kurz: $a \equiv b \ (m)$ oder $a \equiv b \bmod m$ "Kongruenz (mod m)"

Die nat. Zahl m heißt (der) Modul der Kongruenz. (Plural: die Moduln)

6.3. Folgerungen: Sein $a, b, c, a_1, a_2, b_1, b_2 \in \mathbb{Z}$, $k, m, m_1, \dots, m_k \in \mathbb{N}$, $f \in \mathbb{Z}[X]$. Dann:

(1) $a \equiv b \ (m) \iff a$ und b lassen bei Division durch m denselben kleinsten nichtnegativen Rest

(2) $a \equiv b \ (m) \wedge b \equiv c \ (m) \Rightarrow a \equiv c \ (m)$ [Kurz: $a \equiv b \equiv c \ (m) \Rightarrow a \equiv c \ (m)$]

(3) $a_1 \equiv b_1 \ (m) \wedge a_2 \equiv b_2 \ (m) \Rightarrow a_1 + a_2 \equiv b_1 + b_2 \ (m) \wedge a_1 a_2 \equiv b_1 b_2 \ (m)$

(4) $a \equiv b \ (m) \Rightarrow f(a) \equiv f(b) \ (m)$

(5) $ca \equiv cb \ (m) \Rightarrow a \equiv b \ \left(\frac{m}{(c,m)}\right)$, insb. gilt $a \equiv b \ (m)$, falls $(c, m) = 1$.

[Bem.: auch $c = 0$ ist ok]

(6) $a \equiv b \ (m_1), a \equiv b \ (m_2), \dots, a \equiv b \ (m_k) \Rightarrow a \equiv b \ ([m_1, \dots, m_k])$.

(7) $a \equiv b \ (m) \Rightarrow (a, m) = (b, m)$ (8) $a \equiv b \ (m) \wedge m' \mid m \Rightarrow a \equiv b \ (m')$.

Bew.: (1), (2), (3), (6), (8): klar laut Def. 6.2, (4) entsteht durch mehrfache Anwendung von (3),

zu (5): Haben $\frac{m}{(c,m)} \mid \frac{c}{(c,m)} \cdot (b-a)$. Wegen $\left(\frac{m}{(c,m)}, \frac{c}{(c,m)}\right) = 1$ und 1.16(2)(Gauß) gilt $\frac{m}{(c,m)} \mid (b-a)$.

zu (7): $a \equiv b \ (m) \Rightarrow \left(d \mid m \wedge d \mid a \iff d \mid m \wedge d \mid b\right)$. Jetzt 1.14(1). □

6.4. Bem.: • Prinzipiell ist auch $m=0$ möglich: $x \equiv y \bmod 0 \Rightarrow x=y$.
• $x \equiv y \bmod 1$ gilt für alle $x,y \in \mathbb{Z}$
• $x \equiv 0 \bmod m \iff m \mid x$
• Die Relation "$\equiv \bmod m$" ist für jedes $m \in \mathbb{N}$ offenbar eine Äquivalenzrelation auf $\mathbb{Z}$ [6.3.(2), refle.& symm. ✓] und zerlegt $\mathbb{Z}$ also in paarweise disjunkte Äquivalenzklassen.

6.5. Def.: Für alle $m \in \mathbb{N}$ heißen die Äquivalenzklassen von "$\equiv \bmod m$" auf $\mathbb{Z}$ die Restklassen modulo m. Kurz: Restklasse mod m.

6.6. Folgerungen: Sei $m \in \mathbb{N}$. Dann gilt:
(1) Die Restklassen mod m sind die Teilmengen $x+m\mathbb{Z} := \{x+ma;\ a \in \mathbb{Z}\}$ von $\mathbb{Z}$ mit $x \in \mathbb{Z}$. (Ist der Modul m klar, schreiben wir kurz $\underline{x} := x+m\mathbb{Z}$.)
(2) Für alle $x,y \in \mathbb{Z}$ gilt $x+m\mathbb{Z} = y+m\mathbb{Z} \iff x \equiv y\ (m)$.
(3) Die kleinsten nichtnegativen Reste mod m, d.h. $0,1,\dots,m-1$, repräsentieren alle Restklassen mod m, d.h. $0+m\mathbb{Z}, 1+m\mathbb{Z}, \dots, (m-1)+m\mathbb{Z}$ bzw. $\underline{0}, \underline{1}, \dots, \underline{m-1}$ sind genau alle (paarweise disjunkten) Restklassen mod m.

6.7. Def./Satz: Sei $m \in \mathbb{N}$.
• Sei $\mathbb{Z}/m := \{x+m\mathbb{Z};\ x \in \mathbb{Z}\}$ die Menge der Restklassen mod m.
Sprich: "$\mathbb{Z}$ mod m", "$\mathbb{Z}$ modulo m"
• Durch $(x_1+m\mathbb{Z})+(x_2+m\mathbb{Z}) := (x_1+x_2)+m\mathbb{Z}$, Kurz: $\underline{x_1}+\underline{x_2} := \underline{x_1+x_2}$, wird auf $\mathbb{Z}/m$ eine Verknüpfung definiert, die $\mathbb{Z}/m$ zu einer (abelschen) Gruppe macht.
• Das neutrale Element ist die Nullrestklasse $0+m\mathbb{Z}$ bzw. $\underline{0}$.
• Für $m \in \mathbb{N}$ heißt $(\mathbb{Z}/m, +)$ mit "$+$" die additive Restklassengruppe mod m.

Bew.: • die Addition "$+$" auf $\mathbb{Z}/m$ ist unabhängig von den gewählten Repräsentanten der Restklasse, d.h. $+$ ist "wohldefiniert": Sind $x_1' \in x_1+m\mathbb{Z}$, $x_2' \in x_2+m\mathbb{Z}$, also $x_1' \equiv x_1\ (m)$, $x_2' \equiv x_2\ (m)$, dann folgt $x_1'+x_2' \equiv x_1+x_2\ (m)$ nach 6.3(3), also $(x_1'+m\mathbb{Z})+(x_2'+m\mathbb{Z}) = (x_1+x_2)+m\mathbb{Z}$.
• z.z. ist die Gruppeneigenschaft: • Assoziativität & Kommutativität gelten wie in $\mathbb{Z}$
• $0+m\mathbb{Z}$ ist neutrales El. zu $+$, da $\underline{0}+\underline{x} = \underline{0+x} = \underline{x}$,
und zu $x+m\mathbb{Z}$ ist $-x+m\mathbb{Z}$ das inverse Element, da $\underline{x}+\underline{-x} = \underline{x+(-x)} = \underline{0}$. □

6.8. **Bem.:** • Die Gruppe $(\mathbb{Z}/m, +)$ hat m Elemente, nämlich $\mathbb{Z}/m = \{\underline{0}, \underline{1}, \dots, \underline{m-1}\}$.
• $\mathbb{Z}/1 = \{\underline{0}\}$ hat 1 Element.

6.9. **Def.** Sei $m \in \mathbb{N}$.
$\{x_1, \dots, x_m\} \subseteq \mathbb{Z}$ heißt vollständiges Repräsentantensystem mod m,
wenn $x_j \not\equiv x_k \ (m)$ für alle $j, k \in \{1, \dots, m\}$, $j \neq k$, gilt. Kurz: vollst. RS mod m
bzw. wenn jede Restklasse mod m genau eines der x_j enthält.

6.10. **Bsp.:** • $\{1, \dots, m\}$, $\{0, \dots, m-1\}$, $\{-m, -(m-1), \dots, -1\}$ sind vollst. RSe mod m.
• Für $m = 10$ sind $\{0, \pm 1, \pm 2, \pm 3, \pm 4, 5\}$ oder $\{101, 102, \dots, 109, 120\}$
oder $\{0, 1, \dots, 9\}$ oder $\{2, 3, \dots, 10, 11\}$ vollst. RSe mod 10.
• Für $m = 7$ sind $\{0, 2, 4, 6, 8, 10, 12\}$ oder $\{0, \pm 1, \pm 2, \pm 3\}$ vollst. RSe mod 7.

6.11. **Satz (zu vollst. RSen):** Sei $m \in \mathbb{N}$ und $\{x_1, \dots, x_m\} \subseteq \mathbb{Z}$ ein vollst. RS mod m. Seien $a, b \in \mathbb{Z}$.
Dann: (1) $\{x_1 + a, \dots, x_m + a\}$ ist vollst. RS mod m.
(2) $\{x_1 b, x_2 b, \dots, x_m b\}$ ist vollst. RS mod m $\iff$ $(b, m) = 1$.

Bew.: (1): Sind x, y inkongruent mod m, so sind auch $x+a$ und $y+a$ inkongruent mod m.
(2): Dasselbe gilt nach 6.3(5) für xb, yb, falls $(b, m) = 1$ ist. (Das zeigt „$\Leftarrow$")
„$\Rightarrow$": Sei nun $d := (m, b) > 1$ vorausgesetzt. Dann ist $1 \leq \frac{m}{d} < m$ und $\frac{m}{d} \not\equiv 0 \ (m)$.
Gilt etwa $x_1 \equiv 0 \ (m)$, $x_2 \equiv \frac{m}{d} \ (m)$, dann folgt $x_1 b \equiv 0 \ (m)$
und $x_2 b \equiv \frac{m}{d} \cdot b = m \cdot \frac{b}{d} \equiv 0 \ (m)$, ($\frac{b}{d} \in \mathbb{Z}$),
d.h. dann ist $\{x_1 b, \dots, x_m b\}$ kein vollst. RS mod m. □

6.12. **Kor.:** $(\mathbb{Z}/m, +)$ ist zyklisch, d.h. es gibt ein erzeugendes El.,
das ist ein $\underline{a} \in \mathbb{Z}/m$ mit $\langle \underline{a} \rangle = \mathbb{Z}/m$,
wobei $\langle \underline{a} \rangle := \{k \cdot \underline{a} ; k \in \mathbb{N}\}$, wenn $k \cdot \underline{a} := \underline{a} + \dots + \underline{a} = a + \dots + a = \underline{ka}$
definiert wird.

Wir kommen nun zur Multiplikation von Restklassen, und überlegen uns, wieweit sich die Definitionen bei „+" auf „·" übertragen lassen.

6.13. **Def:** Sei $m \in \mathbb{N}$.

- Durch $(x_1 + m\mathbb{Z}) \cdot (x_2 + m\mathbb{Z}) := (x_1 \cdot x_2) + m\mathbb{Z}$, Kurz: $\underline{x_1} \cdot \underline{x_2} := \underline{x_1 \cdot x_2}$, wird auf $\mathbb{Z}/m$ eine Verknüpfung definiert, die $\mathbb{Z}/m$ zu einer (abelschen) Halbgruppe macht. (Malpunkte können weggelassen werden, wenn keine Missverständnisse zu befürchten sind.)
- Das neutrale Element ist die Einsrestklasse $1 + m\mathbb{Z}$ bzw. $\underline{1}$.

Bew.: • die Multiplikation "$\cdot$" auf $\mathbb{Z}/m$ ist unabhängig von den gewählten Repräsentanten der Restklasse, d.h. $\cdot$ ist "wohldefiniert": Sind $x_1' \in x_1 + m\mathbb{Z}$, $x_2' \in x_2 + m\mathbb{Z}$, also $x_1' \equiv x_1 \ (m)$, $x_2' \equiv x_2 \ (m)$, dann folgt $x_1' \cdot x_2' \equiv x_1 \cdot x_2 \ (m)$ nach 6.3(3), also $(x_1' + m\mathbb{Z}) \cdot (x_2' + m\mathbb{Z}) = (x_1 \cdot x_2) + m\mathbb{Z}$.

• z.z. ist die Halbgruppeneigenschaft: • Assoziativität & Kommutativität gelten wie in $\mathbb{Z}$

• $1 + m\mathbb{Z}$ ist neutrales El. zu $\cdot$, da $\underline{1} \cdot \underline{x} = \underline{1 \cdot x} = \underline{x}$. □

6.14. **Bem.:** Für die Nullrestklasse $\underline{0} = 0 + m\mathbb{Z}$ kann niemals ein Inverses (bzgl. $\cdot$) gefunden werden. Aber auch nicht z.B. für $\underline{2} \neq \underline{0}$ in $\mathbb{Z}/10$, weil $\underline{2} \cdot \underline{5} = \underline{10} = \underline{0}$, und für ein Inverses $\underline{z}$ von $\underline{2}$ wäre dann $\underline{1} = \underline{2} \cdot \underline{z}$, also $\underline{5} = \underline{5} \cdot \underline{1} = \underline{5} \cdot \underline{2} \cdot \underline{z} = \underline{0} \cdot \underline{z} = \underline{0}$ ↯

Der folgende Satz gibt ein Kriterium, wann eine Restklasse mod m invertierbar ist:

6.15. **Satz (multiplikative Inverse):** Sei $m \in \mathbb{N}$, $a \in \mathbb{Z}$.

Zu $\underline{a} = a + m\mathbb{Z}$ ex. genau dann ein multiplikatives Inverses (d.h. ein $a^* \in \mathbb{Z}$ mit $(a + m\mathbb{Z}) \cdot (a^* + m\mathbb{Z}) = 1 + m\mathbb{Z}$ bzw. $\underline{a}\,\underline{a^*} = \underline{1}$), wenn $(a, m) = 1$ ist.

↓ Def. $\underline{a}^{-1} := \underline{a^*}$

Bew.: "$\Leftarrow$": Sei $(a, m) = 1$. Nach dem Satz von Bézout 3.2 ex. $a^* \in \mathbb{Z}$, $z \in \mathbb{Z}$: $a^* a + z m = 1$. Also ist $a a^* \equiv 1 \ (m)$ bzw. $\underline{a} \cdot \underline{a^*} = \underline{1}$.

"$\Rightarrow$": Gibt es ein a^* mit $\underline{a}\,\underline{a^*} = \underline{1}$, so gilt $a a^* \equiv 1 \ (m)$. Also ex. $g \in \mathbb{Z}$ mit $a a^* = 1 + g m$, und aus $(a, m) \mid a$, $(a, m) \mid m$ ergibt sich $(a, m) \mid a a^* - g m = 1$. Dies zeigt $(a, m) = 1$. □

6.16. **Wichtige Bem.:** Der Satz 6.15 zeigt, dass die Inverse a^* zu a als Bézout-Koeff. in der Darstellung $1 = (a, m) = a^* a + g m$ berechnet werden kann (mit Methoden aus EZ4).

6.17 **Def.:** Sei $m \in \mathbb{N}$.

(1) $a + m\mathbb{Z} = \underline{a} \in \mathbb{Z}/m$ heißt reduzierte Restklasse mod m, wenn $(a,m) = 1$ ist.
[Nach Folgerung 6.3(7) besteht die gesamte Restklasse aus zu m teilerfremden Zahlen, wenn dies für ein Element der Restklasse zutrifft.]

(2) Die Anzahl der reduzierten Restklassen mod m wird bezeichnet mit
$\varphi(m) := \#\{a \in \mathbb{N};\ 1 \le a \le m,\ (a,m) = 1\}$.
Die so erklärte Fkt. $\varphi: \mathbb{N} \to \mathbb{N}$, $m \mapsto \varphi(m)$, heißt Eulersche φ-Fkt. / Euler-Fkt. / φ-Fkt.

(3) Die Menge der $\varphi(m)$ reduzierten Restklassen mod m ist
$(\mathbb{Z}/m)^* := \{\underline{a} \in \mathbb{Z}/m;\ (a,m) = 1\}$.
Die (nach Satz 6.15) abelsche Gruppe $((\mathbb{Z}/m)^*, \cdot)$ heißt multiplikative Restklassengruppe mod m.

(4) Jedes Vertretersystem $\{x_1, \dots, x_{\varphi(m)}\} \subseteq \mathbb{Z}$ der $\varphi(m)$ vielen reduzierten Restklassen modulo $m \in \mathbb{N}$ heißt reduziertes Restklassensystem mod m.
Kurz: red. RS mod m

6.18 **Bem.:** Eine reduzierte Restklasse wird auch als prime Restklasse bezeichnet, ein reduziertes Restklassensystem auch als primes Restklassensystem.
Dabei besagt "prim" hier nicht, dass die x_i Primzahlen sein sollen!

6.19 **Folgerung:** Sei $m \in \mathbb{N}$. Ist $\{x_1, \dots, x_{\varphi(m)}\} \subseteq \mathbb{Z}$ ein red. RS mod m und $a \in \mathbb{Z}$ mit $(a,m) = 1$, so ist auch $\{ax_1, ax_2, \dots, ax_{\varphi(m)}\}$ eines.

Bew.: analog wie für 6.11(2). □

Bem.: Für $m > 1$ sind die $m \in \mathbb{P}$ offenbar die einzigen Moduln, zu denen alle $\underline{a} = a + m\mathbb{Z}$ mit $\underline{a} \neq 0$ ein multiplikatives Inverses besitzen,
d.h. $(\mathbb{Z}/p, +, \cdot)$ mit $\underline{0}, \underline{1}$ als neutr. El. von $+, \cdot$ ist für $p \in \mathbb{P}$ ein Körper (genannt $\mathbb{F}_p$), und für kein anderes $m > 1$ hat $\mathbb{Z}/m$ diese Eigenschaften.
In Algebra wird gezeigt, dass es exakt zu den Primpotenzen $\{p^k;\ p \in \mathbb{P}, k \in \mathbb{N}\}$ einen Körper $\mathbb{F}_{p^k}$ mit $\#\mathbb{F}_{p^k} = p^k$ gibt (bis auf Isomorphie), und sonst gibt es keine weiteren endlichen Körper mehr! (vgl. Vorl. "Algebra", Satz 21.5)

6.20 **Def.**: Wir nennen $(\mathbb{Z}/m, +, \cdot)$ den **Restklassenring mod m**.

Bem.: • Die invertierbaren Elemente (auch Einheiten genannt) sind die reduzierten Restklassen und bilden $(\mathbb{Z}/m)^*$. Genau für $m=p$ prim ist $(\mathbb{Z}/m)^* = (\mathbb{Z}/m) \setminus \{\bar{0}\}$, d.h. genau für $m=p$ prim ist $(\mathbb{Z}/m, +, \cdot)$ ein Körper (nämlich $\mathbb{F}_p$).

• Kongruenzrechnung mod m kann genausogut als Rechnen mit den Elementen des Restklassenrings mod m verstanden werden.

Eine wichtige Anwendung der Kongruenzrechnung ist der Chinesische Restsatz, mit dem verschiedene Kongruenten zu einer einzigen zusammengefasst werden können (oder eine mit zusammengesetztem Modul in mehrere Kongruenzen aufgeteilt).

6.21. **Satz (Chinesischer Restsatz, Kurz: CRS):**
Seien $m_1, \dots, m_k \in \mathbb{N}$ paarweise teilerfremd, d.h. $\forall i \neq j : (m_i, m_j) = 1$.
Sei $m := m_1 \cdots m_k$. Dann gibt es zu jedem k-Tupel $(x_1, \dots, x_k) \in \mathbb{Z}^k$ genau ein x_0 modulo m, so dass für alle $x \in \mathbb{Z}$ gilt:

"simultane Kongruenzen"
$$\left.\begin{array}{l} x \equiv x_1 \ (m_1) \\ \wedge\ x \equiv x_2 \ (m_2) \\ \quad\vdots \\ \wedge\ x \equiv x_k \ (m_k) \end{array}\right\} \iff x \equiv x_0 \ (m).$$

6.22. **Bem.:** • Andere Formulierungen der Beh.: $\bigcap_{j=1}^{k} (x_j + m_j\mathbb{Z}) = x_0 + m\mathbb{Z}$. oder:
Es gibt einen (Ring-) Isomorphismus $\mathbb{Z}/m_1 \times \dots \times \mathbb{Z}/m_k \xrightarrow{\cong} \mathbb{Z}/m$
$(x_1, \dots, x_k) \longmapsto x_0$,
d.h. die Beziehung zwischen den Tupeln $(x_1, \dots, x_k)$ und Lösungen x_0 ist eineindeutig:
- Zu x_0 ex. ein Tupel $(x_1, \dots, x_k)$ mit $x_j \equiv x_0 \ (m_j)$ für alle $j \leq k$, d.h. die genannte Abb. ist surjektiv.
- Lösungen x_0 und x_0' zu Tupeln $(x_1, \dots, x_k)$ und $(x_1', \dots, x_k')$ sind mod m genau dann verschieden, wenn sich die Tupel in mind. einer Komponente mod m_j unterscheiden, d.h. die Abb. ist injektiv.

• Die algebraische Formulierung hat als Konsequenz, dass sich algebraische Eigenschaften der Elemente wie "ist Einheit / Quadrat / ..." von einem Ring auf den anderen übertragen lassen. So ist z.B. $(\mathbb{Z}/m_1)^* \times \dots \times (\mathbb{Z}/m_k)^* \cong (\mathbb{Z}/m)^*$ ein Kor. des CRS.
(In Algebra wird die allgemeine Ringversion gezeigt, vgl. Satz A12.4/A12.5 der Vorlesung "Algebra".)

• Die Bedingung der paarweisen Teilerfremdheit ist notwendig. Andernfalls gibt es entweder keine oder mehr als eine Lösung mod m. Kann man als (Ü) untersuchen.

6.23. **Bem.:** Die Namensgebung geht zurück auf chinesische Quellen um 1200. Das Prinzip des Satzes tritt unabhängig davon in zahlreichen früheren Schriften auf.

6.24. Vorbem. zum Beweis des CRS: Der in Algebra geführte ringtheoretische Beweis (Algebra A12.4) führt nicht unmittelbar zu einer expliziten Lösungsangabe. Der folgende Beweis liefert darüberhinaus Lösungsformeln zur konkreten Berechnung der Lösung x_0.
(Umgekehrt aus x_0 die x_j zu bestimmen, ist trivial: $x_j \equiv x_0 \ (m_j)$ für $1 \le j \le k$.)

6.25. Beweis (des CRS):

Angabe eines x_0: Seien $x_1, \dots, x_k \in \mathbb{Z}$ gegeben.

Für $m := m_1 \cdots m_k$ setze $M_1 := \frac{m}{m_1}, \dots, M_k := \frac{m}{m_k}$.

Dann bewirkt die Vor., dass $(M_j, m_j) = 1$ für alle $j \le k$ gilt.

Die Restklasse M_j ist also mod m_j invertierbar, d.h.

ex. M_j^* mit $M_j M_j^* \equiv 1 \ (m_j)$. (Bestimmbar mit Bézout-Lemma)

Setze: $x_0 := M_1 M_1^* x_1 + \dots + M_k M_k^* x_k$.

Beh.: 1.) x_0 mod m erfüllt die simultanen Kongruenzen, und 2) jede Lsg. davon ist $\equiv x_0 \ (m)$.

1.): Sei $x \equiv x_0 \ (m)$. Nun teilt m_j den Modul m als auch alle M_ℓ mit $\ell \neq j$.

Es folgt $x \equiv \sum_{\ell=1}^{k} M_\ell M_\ell^* x_\ell \ (m_j) \equiv M_j M_j^* x_j + 0 \equiv 1 \cdot x_j = x_j \ (m_j)$.

2.): Sei y Lösung der simultanen Kongruenzen, d.h. $y \equiv x_j \ (m_j)$ für alle $j \le k$.

Für alle $j \le k$ und alle $\ell \le k$ mit $\ell \neq j$ gilt $M_j M_j^* x_j \equiv x_j \ (m_j)$,

und $M_\ell M_\ell^* x_\ell \equiv 0 \ (m_j)$.

Damit folgt $y \equiv x_j \equiv \sum_{\ell=1}^{k} M_\ell M_\ell^* x_\ell = x_0 \ (m_j)$ für alle $j \le k$.

Wegen 6.3. folgt $y \equiv x_0 \ ([m_1, \dots, m_k])$,

und mit der paarweisen Teilerfremdheit folgt $[m_1, \dots, m_k] = m_1 \cdots m_k = m$,

vgl. Bem. 1.21, und somit ist $y \equiv x_0 \ (m)$. □

6.26. Bsp.: Das simultane Kongruenzensystem $\left\{ \begin{array}{l} x \equiv 1 \ (3) \\ x \equiv 2 \ (4) \\ x \equiv 3 \ (5) \end{array} \right\}$ hat die Lösung $x \equiv 58 \equiv -2 \ (60)$.

Dies ist sofort überprüfbar: $-2 \equiv 1 \ (3)$ ✓, $-2 \equiv 2 \ (4)$ ✓, $-2 \equiv 3 \ (5)$ ✓.

Die Lösung findet man mit der Formel im CRS: $m = 3 \cdot 4 \cdot 5$, $M_1 = 4 \cdot 5$, $M_2 = 3 \cdot 5$, $M_3 = 3 \cdot 4$.

Dann ist $M_1^* = 2$, da $2 \cdot M_1 = 2 \cdot (4 \cdot 5) \equiv 2 \cdot 2 \equiv 1 \ (3)$,

$M_2^* = -1$, da $(-1) \cdot M_2 = (-1) \cdot (3 \cdot 5) \equiv (-1) \cdot (-1) \equiv 1 \ (4)$,

$M_3^* = -2$, da $(-2) \cdot M_3 = (-2) \cdot (3 \cdot 4) \equiv (-2) \cdot 2 \equiv 1 \ (5)$.

} die M_j^* sind hier durch Probieren gefunden worden

Also ist $x_0 = 1 \cdot 2 \cdot (4 \cdot 5) + 2 \cdot (-1) \cdot (3 \cdot 5) + 3 \cdot (-2) \cdot (3 \cdot 4) = 40 - 30 - 24 \cdot 3 = 10 - 72 = -62 \equiv -2 \ (60)$.

Als letzte Anwendung der Kongruenzenrechnung behandeln wir verschiedene Teilbarkeitsregeln im Dezimalsystem.
Zunächst der Satz, dass zu jeder Basis $g>1$ die g-adische Darstellung natürlicher Zahlen eindeutig bestimmt ist:

6.27. **Satz (Ziffernsysteme):** Sei $g\in\mathbb{N}$, $g>1$. Dann ex. zu jedem $n\in\mathbb{N}$ eindeutig ein $m\in\mathbb{N}_0$ ($m+1$ = Stellenzahl) und für alle $0\le j\le m$ je ein $a_j\in\mathbb{N}_0$ mit $a_j\le g-1$ (Ziffern), so dass $a_m\neq 0$ und $n=\sum_{j=0}^{m} a_j g^j$ ist.
Dabei ist die endliche Ziffernfolge $a_m, a_{m-1},\dots,a_1,a_0$ (auch) eindeutig bestimmt.

Bew.: Ex.: Zu jedem $n\in\mathbb{N}$ ex. genau ein m mit $g^m\le n<g^{m+1}$, nämlich $m:=\left\lfloor \frac{\log n}{\log g}\right\rfloor$.
Mit diesem gilt die Ex., wie durch Induktion nach m gezeigt wird:
$m=0$: Hier ist nichts zu zeigen: da ist $n<g$, also tut's $a_0:=n$.
$m\to m+1$: Sei $g^{m+1}\le n<g^{m+2}$, setze $n':=n-\left\lfloor\frac{n}{g^{m+1}}\right\rfloor\cdot g^{m+1}$.
Aufgrund der Def. der Gaußklammer ist $0\le n'<g^{m+1}$,
d.h. auf n' ist die Ind.vor. anwendbar.
Wegen $1\le\frac{n}{g^{m+1}}<g$ ist $1\le\left\lfloor\frac{n}{g^{m+1}}\right\rfloor<g$,
d.h. $\left\lfloor\frac{n}{g^{m+1}}\right\rfloor$ ist als Ziffer $a_{m+1}\neq 0$ verwendbar.
Eind.: Seien $k=\sum_{j=0}^{m} a_j g^j$ und $k=\sum_{j=0}^{r} b_j g^j$ zwei verschiedene Darstellungen eines $k\in\mathbb{N}$.
Ist $m<r$, so seien $a_{m+1}:=0,\dots,a_r:=0$.
Sei $\ell:=\max\{j\le\max\{m,r\};\ a_j\neq b_j\}$ die größte Stelle, an der sich die Darstellungen unterscheiden. Dann folgt $(b_\ell-a_\ell)g^\ell=\sum_{j=0}^{\ell-1}(a_\ell-b_j)g^j$.
Im Fall $\ell=0$ ist dies ein $\lightning$. [l.S. $\neq 0$, r.S. $=0$]
Für $\ell\ge 1$ ist $|(b_\ell-a_\ell)\cdot g^\ell|\ge g^\ell$, Wohingegen ist andererseits
$\left|\sum_{j=0}^{\ell-1}(a_j-b_j)g^j\right|\le(g-1)\sum_{j=0}^{\ell-1}g^j=(g-1)\cdot\frac{g^\ell-1}{g-1}<g^\ell$, $\lightning$. □

Wir führen eine Kurznotation für die Dezimaldarstellung ein:

6.28. **Notation:** $[a_m a_{m-1}\dots a_2 a_1 a_0]:=\sum_{i=0}^{m} a_i 10^i$ für $a_i\in\{0,1,\dots,9\}$ (Ziffern), $0\le i\le m$.

6.29. **Def.:** Für $n \in \mathbb{N}$ sei $[a_m \dots a_1 a_0]$ die Dezimalentwicklung von n,
$s_m := \sum_{i=0}^{m} a_i$ heißt die Quersumme,
und $t_m := \sum_{i=0}^{m} (-1)^i a_i$ heißt die alternierende Quersumme.

Wir formulieren zunächst einige klassische, wohl bekannte Teilbarkeitsregeln für nat. Zahlen, die im Dezimalsystem dargestellt sind. Mit ihnen kann die Teilbarkeit durch bestimmte kleine Primzahlen an der Ziffernderstellung abgelesen/leicht überprüft werden.

6.30. (a) $10 \mid n \Leftrightarrow n \equiv 0 \,(10) \Leftrightarrow a_0 = 0$, da $n = \sum_{i=0}^{m} a_i 10^i \equiv a_0 \,(10)$.
($10^i \equiv 0$ für $i \geq 1$)
Die Endziffer a_0 gibt den Rest von n mod 10 an.

(b) $2 \mid n \Leftrightarrow n \equiv 0 \,(2) \Leftrightarrow a_0 \equiv 0 \,(2)$, da $n \equiv a_0 \,(10)$ [also auch $n \equiv a_0 \,(2)$].
Gerade Zahlen haben eine gerade Endziffer: $a_0 \in \{0, 2, 4, 6, 8\}$.

(c) $5 \mid n \Leftrightarrow n \equiv 0 \,(5) \Leftrightarrow a_0 \equiv 0 \,(5)$, da $n \equiv a_0 \,(10)$ [also auch $n \equiv a_0 \,(5)$].
Durch 5 teilbare Zahlen haben die Endziffer 0 oder 5: $a_0 \in \{0, 5\}$

(a') $100 \mid n \Leftrightarrow n \equiv 0 \,(100) \Leftrightarrow [a_1 a_0] = 0$, da $n = \sum_{i=0}^{m} a_i 10^i \equiv [a_1 a_0] \,(100)$.
($10^i \equiv 0$ für $i \geq 2$)
Die Endziffern $[a_1 a_0]$ geben den Rest von n mod 100 an.

(d) $25 \mid n \Leftrightarrow n \equiv 0 \,(5^2) \Leftrightarrow [a_1 a_0] \equiv 0 \,(5^2)$, da $n \equiv [a_1 a_0] \,(100)$ [also auch $n \equiv [a_1 a_0] \,(5^2)$].
Durch 25 teilbare Zahlen haben die Endziffern $[a_1 a_0] \in \{00, 25, 50, 75\}$.

(e) $4 \mid n \Leftrightarrow n \equiv 0 \,(4) \Leftrightarrow [a_1 a_0] \equiv 0 \,(4)$, da $n \equiv [a_1 a_0] \,(100)$ [also auch $n \equiv [a_1 a_0] \,(4)$].
$4 \mid [ab] \Leftrightarrow 4 \mid 2a + b$ → Durch 4 teilbare Zahlen haben zwei Endziffern, die eine durch 4 teilbare Zahl ergeben.
$10 \equiv 2 \,(4)$

(a'') $1000 \mid n \Leftrightarrow n \equiv 0 \,(1000) \Leftrightarrow [a_2 a_1 a_0] = 0$, da $n = \sum_{i=0}^{m} a_i 10^i \equiv [a_2 a_1 a_0] \,(1000)$.
($10^i \equiv 0$ für $i \geq 3$)
Die Endziffern $[a_2 a_1 a_0]$ geben den Rest von n mod 1000 an.

(f) $125 \mid n \Leftrightarrow n \equiv 0 \,(5^3) \Leftrightarrow [a_2 a_1 a_0] \equiv 0 \,(5^3)$, da $n \equiv [a_2 a_1 a_0] \,(1000)$ [also auch $n \equiv [a_2 a_1 a_0] \,(5^3)$].
Durch 125 teilbare Zahlen haben die Endziffern $[a_2 a_1 a_0] \in \{000, 125, 250, 375, 500, \dots\}$

(g) $8 \mid n \Leftrightarrow n \equiv 0 \,(8) \Leftrightarrow [a_2 a_1 a_0] \equiv 0 \,(2^3)$, da $n \equiv [a_2 a_1 a_0] \,(1000)$ [also auch $n \equiv [a_2 a_1 a_0] \,(2^3)$].
↳ Durch 8 teilbare Zahlen haben drei Endziffern, die eine durch 8 teilbare Zahl ergeben.
$8 \mid [abc] \Leftrightarrow 8 \mid 4a + 2b + c$
$100 \equiv 4 \,(8)$

(h) $9 \mid n \Leftrightarrow n \equiv 0 \,(9) \Leftrightarrow s_m \equiv 0 \,(9)$, da $n = \sum a_i 10^i \equiv \sum a_i = s_m \,(9)$.
($10^i \equiv 1 \,(9)$)
Der Rest von n mod 9 ist der Rest von s_n mod 9.

(i) $3 \mid n \Leftrightarrow n \equiv 0 \,(3) \Leftrightarrow s_m \equiv 0 \,(3)$, da $n \equiv s_n \,(9)$ [also auch $n \equiv s_m \,(3)$].
Der Rest von n mod 3 ist der Rest von s_n mod 3.

(j) $11 \mid n \Leftrightarrow n \equiv 0 \,(11) \Leftrightarrow t_n \equiv 0 \,(11)$, da $n = \sum a_i \underbrace{10^i}_{\equiv -1 \,(11)} \equiv \sum a_i (-1)^i = t_n \,(11)$.
Der Rest von n mod 11 ist der Rest von t_n mod 11.

6.31. **Beispiele** zu den bisherigen (klassischen) Teilbarkeitsregeln (a)–(j):
- $3 \mid 9\,112.139.752$, da $3 \mid 9+1+2+\ldots+7+5+2 = 39$, da $3 \mid 3+9 = 12$,
- $206.240 \equiv 5\,(9)$, da $2+6+2+4 = 14 \equiv 5\,(9)$, } da $3 \mid 1+2 = 3$ ✓
  also: $206.240 \equiv 2\,(3)$.
- $8 \mid 718.976$, da $8 \mid 976$, da $976 = 9 \cdot \underbrace{10^2}_{\equiv 4\,(8)} + 7 \cdot \underbrace{10}_{\equiv 2\,(8)} + 6 \equiv 9 \cdot 4 + 7 \cdot 2 + 6 = 56$
  $\equiv 5 \cdot 2 + 6 = 16 \equiv 0\,(8)$
- $11 \mid 360.318.299$, da $11 \mid 3-6-3+1-8+2-9+9 = -11$ ✓
- $261.390 \equiv -3\,(11)$, da $0-9+3-1+6-2 = -3$ (v.z. beachten: nicht $-0+9-\ldots$)

6.32. (k) **Die 1001-Regel** ($1001 = 7 \cdot 11 \cdot 13$): (vgl. "1001 Nacht")
Sei $v_n = [a_2 a_1 a_0] - [a_5 a_4 a_3] + [a_8 a_7 a_6] - \ldots = \sum_{i=0}^{\lfloor \frac{m}{3} \rfloor} [a_{3i+2}\, a_{3i+1}\, a_{3i}] (-1)^i$
(ev. Leitziffern "0" ergänzen).
Dann: $10^3 \equiv -1 \,(1001)$, also ist $n = \sum_{i=0}^{\lfloor m/3 \rfloor} [a_{3i+2}\, a_{3i+1}\, a_{3i}] \cdot \underbrace{10^{3i}}_{\equiv (-1)^i \,(1001)} \equiv v_n \,(1001)$.
Somit: $k \mid 1001 \rightsquigarrow (k \mid n \Leftrightarrow k \mid v_n)$
→ ergibt Teilbarkeitsregel für 7, 11, 13: (11 wegen (j) nicht so interessant)
Ob n durch 7 teilbar ist, teste iterativ: $7 \mid n$, wenn $7 \mid v_n$, wenn $7 \mid v_{v_n}$ ...

6.33. **Bsp.:**
- $7 \mid 3.952.269.524$, da $7 \mid -003+952-269+524 = 1204$,
  da $7 \mid -1+204 = 203 = 7 \cdot 29$ (oder s. (e)).
- $13 \mid 69.137.081$, da $13 \mid 69 - 137 + 81 = 13$

6.34. **Bem.:** Durch iteriertes Anwenden nur noch Teilbarkeitstests mod 7, 13 mit 3-stelligen Zahlen nötig ~ in (l), (m)

6.35. (l) $n = [a\ b\ c] = \underbrace{100a}_{\equiv 2\,(7)} + \underbrace{10b}_{\equiv 3\,(7)} + c \rightsquigarrow 7 \mid n \Leftrightarrow n \equiv 0\,(7) \Leftrightarrow 2a + 3b + c \equiv 0\,(7)$
Bsp.: $7 \mid 203$, da $7 \mid 2 \cdot 2 + 3 \cdot 0 + 3 = 7$ ✓

(m) $n = [a\ b\ c] = \underbrace{100a}_{\equiv -4\,(13)} + \underbrace{10b}_{\equiv -3\,(13)} + c \rightsquigarrow 13 \mid n \Leftrightarrow n \equiv 0\,(13) \Leftrightarrow 4a + 3b - c \equiv 0\,(13)$
Bsp.: $13 \mid 624$, da $13 \mid 4 \cdot 6 + 3 \cdot 2 - 4 = 26$,
und $13 \mid 26$, da $13 \mid 4 \cdot 0 + 3 \cdot 2 - 6 = 0$

(6) **17-Regel**: Wegen $10^8+1 = 17 \cdot 5\,882\,353$ kann wie bei der 1001-Regel analog eine (10^8+1)-Regel formuliert werden mit einer alternierenden Blocksumme mit Ziffernblöcken der Länge 8 $\rightsquigarrow$ es reicht, Zahlen $< 10^8$ mit 8 Stellen auf Teilbarkeit mod 17 zu testen. Wegen $17 \mid 102$ kann dafür eine einfache Regel aufgestellt werden: $n = [a_7 a_6 a_5 a_4 a_3 a_2 a_1 a_0] = \sum_{i=0}^{3} [a_{2i+1} a_{2i}] \cdot \underbrace{10^{2i}}_{\equiv (-2)^i \,(17)}$

$\equiv [a_1 a_0] - 2\cdot[a_3 a_2] + 4\cdot[a_5 a_4] - 8\cdot[a_7 a_6]$ (17)

(mit $17 \mid 1003$ und 3er-Blöcken wird es komplizierter).

6.36 **Bsp.**: $17 \mid 90.807.421$, da $21 - 2\cdot 74 + 4\cdot 80 - 8\cdot 90 = -527$ und $17 \mid 527$, da $27 - 2\cdot 5 = 17$ ✓. Man muss die Vielfachen < 102 von 17 kennen: 17, 34, 51, 68, 85 (oder $10 \equiv -7\,(17)$ verwenden: $51 \equiv 5\cdot(-7)+1 = -34 \ldots$)

(Bem.: $\mathrm{ord}(10) = 18 \mod 19$)

6.37 (p) **19-Regel**: Wegen $19 \mid 10^9+1$ reicht es, 9-stellige Zahlen zu betrachten.

1. Idee: Verwende $100 \equiv 5\,(19)$, also:

$[a_8\, a_7 \ldots a_1 a_0] \equiv \sum [a_{2i+1} a_{2i}] \cdot 5^i \equiv [a_1 a_0] + 5[a_3 a_2] + 6\cdot[a_5 a_4] + 11\cdot[a_7 a_6] - 2\cdot a_8\,(19)$

Bsp.: $19 \mid 640\,337.582$, da $82 + 5\cdot 75 + 6\cdot 33 + 11\cdot 40 - 2\cdot 6 = 1083 \equiv 0\,(19)$, da $83 + 5\cdot 10 = 133 \equiv 0\,(19)$, da $33 + 5\cdot 1 = 38 \equiv 0\,(19)$, da $3\cdot(-9) + 8 = -19 \equiv 0\,(19)$.

2. Idee: Verwende $20 \equiv 1\,(19)$, also:

$n \equiv \sum_{i=0}^{m} a_i 10^i \cdot 20^{m-i} = \left(\sum_{i=0}^{m} a_i 2^{m-i}\right) 10^m$ (19), d.h. $19 \mid n \Leftrightarrow 19 \mid \sum_{i=0}^{m} a_i 2^{m-i}$

$\rightsquigarrow$ Regel: $19 \mid [a_8\, a_7 \ldots a_1 a_0] \Leftrightarrow 19 \mid a_8 + 2a_7 + 4a_6 + 8a_5 + 16a_4 + 32a_3 + 64a_2 + 128a_1 + 256a_0 \Leftrightarrow 19 \mid a_8 + 2a_7 + 4a_6 + 8a_5 - 3a_4 - 6a_3 + 7a_2 - 5a_1 + 9a_0$

(anderes Bsp.: $1\cdot 1 + 2\cdot 3 + 4\cdot 3 = 19 \Rightarrow 19 \mid 133$)

im Bsp.: $6 + 2\cdot 4 + 4\cdot 0 + 8\cdot 3 - 3\cdot 3 - 6\cdot 7 + 7\cdot 5 - 5\cdot 8 + 9\cdot 2 = 0 \equiv 0\,(19)$ ✓

Viel Spaß beim Auffinden/Erfinden von neuen Teilbarkeitsregeln!

z.B.: [$1000 \equiv 1\,(37) \rightsquigarrow$ 1000-Regel für 37... ☺]