Stichworte: Kongruenz $a \equiv b \,(m)$

Zahlring $\mathbb{Z}_m := \mathbb{Z}/m\mathbb{Z} = \{x + m\mathbb{Z} : x \in \mathbb{Z}\} = \{0 + m\mathbb{Z}, 1 + m\mathbb{Z}, \dots, (m-1) + m\mathbb{Z}\}$

Einheiten: $\mathbb{Z}_m^* = \{x + m\mathbb{Z} : x \in \mathbb{Z},\ \text{ex. } y \in \mathbb{Z} : (x + m\mathbb{Z})(y + m\mathbb{Z}) = 1 + m\mathbb{Z}\}$

$= \{x + m\mathbb{Z} : x \in \mathbb{Z},\ ggT(x, m) = 1\} \rightsquigarrow \varphi(m) := \#\mathbb{Z}_m^*$

Ist m klar, schreibe $\underline{x}$ für $x + m\mathbb{Z}$

$\mathbb{Z}_m^*$ heißt auch multiplikative Gruppe von $\mathbb{Z}_m$

Invertieren von Elementen in $\mathbb{Z}_m^*$ geht mit euklidischem Algorithmus

CRS: $\mathbb{Z}_{mn} \overset{\text{Ring-iso}}{\cong} \mathbb{Z}_m \times \mathbb{Z}_n$, falls $ggT(m,n) = 1$, Version des CRS mit simultanen Kongruenzen

Rechenbeispiele zum Kongruenzenrechnen und für eine "modulare Brille"

1.1.2 Kongruenzenrechnen und die "modulare Brille"

Wir behandeln nun, wie man mit Teilmengen von $\mathbb{Z}$ und neuen Definitionen von "+" und "·" zu neuen algebraischen Strukturen (Gruppen, Ringe, Körper) kommt. Dazu ist das Kongruenzenrechnen modulo m wesentlich.

1.) **Def.:** Sei $m \in \mathbb{N}$. Dann heißen $a \in \mathbb{Z}$ und $b \in \mathbb{Z}$ kongruent modulo m, wenn $m \mid (b - a)$. Kurz: $a \equiv b \bmod m$ oder $a \equiv b \,(m)$.
Die Zahl m heißt Modul der Kongruenz.

2.) **Folgerungen:** (1) $a \equiv b \bmod m$ bedeutet, dass a und b bei Division durch m denselben kleinsten nichtnegativen [absolut kleinsten] Rest lassen.

(2) $a \equiv b \,(m)$ und $b \equiv c \,(m) \Rightarrow a \equiv c \,(m)$

(3) $a_1 \equiv b_1 \,(m)$ und $a_2 \equiv b_2 \,(m) \Rightarrow a_1 + a_2 \equiv b_1 + b_2 \,(m)$ und
$a_1 \cdot a_2 \equiv b_1 \cdot b_2 \,(m) \rightsquigarrow$ Kor.: $a_1^m \equiv b_1^m \,(m)$

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

(5) $a \equiv b \,(m_i)$ für $i = 1, \dots, k \Rightarrow a \equiv b \,(kgV(m_1, \dots, m_k))$

Dies zeigt, dass "$\equiv$" für festes m eine Äquivalenzrelation ist und $\mathbb{Z}$ in m paarweise disjunkte Äquivalenzklassen zerlegt.

3.) **Def.:** Die Äquivalenzklassen von $\equiv$ modulo m heißen Restklassen modulo m.
(auch: Kongruenzklassen modulo m).

4.) **Folgerungen:** Die Restklassen modulo m sind Teilmengen von $\mathbb{Z}$ der Gestalt $x + m\mathbb{Z} := \{x + ma;\ a \in \mathbb{Z}\}$.
Die Restklasse $x + m\mathbb{Z}$ heißt auch die Restklasse von x modulo m.
Davon gibt es m Stück; wird in jeder Restklasse ein Element x_i, $i = 1, \dots, m$, angewählt, können die m Restklassen mit $x_1 + m\mathbb{Z}, x_2 + m\mathbb{Z}, \dots, x_m + m\mathbb{Z}$ angegeben werden; die Menge $\{x_1, \dots, x_m\}$ heißt dann vollständiges Restsystem modulo m. Sind $y_1, \dots, y_m \in \mathbb{Z}$ so, dass $y_i \not\equiv y_j \bmod m$ für alle $i \neq j$, $1 \leq i, j \leq m$, gilt (d.h. sind die y_i paarweise inkongruent modulo m), dann ist $\{y_1, \dots, y_m\}$ ein vollständiges RS mod m.
Die Zahl x heißt Repräsentant der Restklasse $x + m\mathbb{Z}$, und $x + m\mathbb{Z} = z + m\mathbb{Z} \Leftrightarrow x \equiv z \bmod m$, weil in der Restklasse von x mod m genau alle zu x kongruenten Zahlen liegen laut Def.

5.) **Bsp.:** $\{0, 1, 2\}$ ist vollst. RS mod 3, und vollst. Restsysteme mod 8 sind etwa $\{1, \dots, 8\}$ und $\{3, 6, 9, 12, 15, 18, 21, 24\} = \{3 \cdot a;\ 1 \leq a \leq 8\}$ da $12 \equiv 4\ (8)$, $15 \equiv 7\ (8)$, $18 \equiv 2\ (8)$, $21 \equiv 5\ (8)$, $24 \equiv 0\ (8)$.
Die Menge $\{2a;\ 1 \leq a \leq 8\}$ ist kein vollst. RS mod 8. Die Reste $0, 1, 2, \dots, m-1$ könnte man auch als "Standardrepräsentanten" mod m bezeichnen, da $\{0, 1, 2, \dots, m-1\}$ immer vollst. RS mod m ist.

6.) **Folgerungen:** Ist $\{x_1, \dots, x_m\}$ ein vollst. RS mod m und $a \in \mathbb{Z}$, $c \in \mathbb{Z}$ mit $ggT(c, m) = 1$, so sind auch $\{x_1 + a, \dots, x_m + a\}$ und $\{x_1 \cdot c, \dots, x_m \cdot c\}$ vollst. RSe mod m (vgl. (4) aus Folgerung 2.)).

Das nützliche an den Restklassen modulo m ist, dass wir nun durch folgende naheliegende Definitionen von "+" und "·" mit ihnen neue algebraische Strukturen gewinnen können:

7) **Def.:** Ist der Modul $m \in \mathbb{N}$ klar, schreiben wir auch $\underline{x} := x + m\mathbb{Z}$ für die Restklasse von x mod m.

Wir definieren für $x, y \in \mathbb{Z}$ dann $\underline{x} + \underline{y} := \underline{x+y}$ und $\underline{x} \cdot \underline{y} := \underline{x \cdot y}$, d.h. $(x+m\mathbb{Z}) \dot{+} (y+m\mathbb{Z}) := (x \dot{+} y) + m\mathbb{Z}$. Dies erklärt "+", "·".

Weiter sei $\mathbb{Z}_m = \mathbb{Z}/m\mathbb{Z} = \mathbb{Z}/m := \{ x+m\mathbb{Z};\ x \in \mathbb{Z} \}$ die Menge der (m vielen) Restklassen modulo m.

8) **Folgerungen:**

Wir addieren/multiplizieren zwei Restklassen, indem wir Repräsentanten x, y auswählen und diese addieren/multiplizieren. Das ist nur sinnvoll, wenn bei unterschiedlicher Repräsentantenwahl dieselbe Restklasse als Ergebnis herauskommt, man sagt, die Def. von $\dot{+}$ bzw. $\cdot$ ist **wohldefiniert**, da repräsentantenunabh.

Dies ist klar: $\underline{x_1} = \underline{x_2}$ und $\underline{y_1} = \underline{y_2} \Rightarrow x_1 \equiv x_2\ (m)$ und $y_1 \equiv y_2\ (m)$

$\overset{\text{Folg. 2.1 (3)}}{\Rightarrow} x_1 \dot{+} y_1 \equiv x_2 \dot{+} y_2\ (m) \Rightarrow \underline{x_1 \dot{+} y_1} = \underline{x_2 \dot{+} y_2}$,

also erhalten wir so dieselbe Restklasse für $\underline{x_1} \dot{+} \underline{y_1}$ und $\underline{x_2} \dot{+} \underline{y_2}$, wenn $\underline{x_1} = \underline{x_2}$ und $\underline{y_1} = \underline{y_2}$.

Damit kann $(\mathbb{Z}_m, +)$ oder $(\mathbb{Z}_m \setminus \{0\}, \cdot)$ auf alg. Strukturen hin untersucht werden. (Bem.: Schreiben ab jetzt die neuen, blau markierten $+, \cdot$ schwarz)

9) **Folgerung:** $(\mathbb{Z}_m, +)$ ist eine abelsche Gruppe mit neutr. El. $\underline{0} = 0 + m\mathbb{Z}$, denn Kommutativität und Assoziativität gelten wie in $\mathbb{Z}$, und $\underline{0} + \underline{x} = \underline{0+x} = \underline{x}$ gilt für alle $x \in \mathbb{Z}$, sowie $\underline{x} + \underline{-x} = \underline{x-x} = \underline{0}$, so dass $-\underline{x} = \underline{-x} = \underline{m-x}$ für alle $x \in \mathbb{Z}$ gilt. Ebenso gilt, dass $(\mathbb{Z}_m, +, \cdot)$ ein Kommutativer Ring mit $\underline{1}$ ist.

Das Beispiel $\underline{2} \cdot \underline{0} = \underline{0}$, $\underline{2} \cdot \underline{1} = \underline{2}$, $\underline{2} \cdot \underline{2} = \underline{0}$ modulo 4 zeigt, dass es Restklassen ohne Inversen bzgl. "·" (hier $\underline{2} \neq \underline{0}$) geben kann. Der Satz 10) gibt an, welche Restklassen invertierbar sind, d.h. im Ring $\mathbb{Z}_m$ eine Einheit sind:

10) **Satz:** Zu $\underline{x} \in \mathbb{Z}_m$ ex. genau dann ein multiplikatives Inverses, d.h. ein $\underline{y} \in \mathbb{Z}_m$ mit $\underline{x} \cdot \underline{y} = \underline{1} \Leftrightarrow x \cdot y \equiv 1\ (m)$, falls $\underline{ggT(x,m) = 1}$.

Wir schreiben dann $\underline{x}^{-1}$ oder $\underline{x}^*$ für $\underline{y}$, die Bezeichnungen $\frac{\hat{1}}{\underline{x}}$ oder $\frac{1}{\underline{x}}$ oder $1/\underline{x}$ sind didaktisch ungeschickt.

Bew.: „$\Rightarrow$": Sei $\underline{x} \in \mathbb{Z}_m$ mit $\underline{x}\cdot\underline{y} = \underline{1}$, d.h. $x \cdot y \equiv 1 \,(m)$, also ex. $k \in \mathbb{Z}$ mit $1 - xy = km \Rightarrow xy + km = 1$. Wäre $d = ggT(x,m) > 1$, folgt $d \mid xy + km = 1$ ↯.

„$\Leftarrow$": Sei $ggT(x,m) = 1$. Nach V2-Satz 20), dem Satz vom eukl. Algorithmus, ex. $y, k \in \mathbb{Z}$ mit $1 = yx + km$, also folgt $\underline{x}\cdot\underline{y} = \underline{1}$. □

Fazit: Mit dem euklidischen Algorithmus können wir also Inverse schnell explizit berechnen.

Bsp.: Gesucht: 7^{-1} mod 37, haben: $37 = 5\cdot 7 + 2$, $7 = 3\cdot 2 + 1$, $2 = 2\cdot 1 \rightsquigarrow$

q_a		1	5	3	2
c_a	0	1	5	16	37

$\rightsquigarrow +16 = 7^{-1}\,(37)$

11.) **Def.:** $\underline{x} = x + m\mathbb{Z}$ heißt prime oder reduzierte Restklasse mod m, falls $ggT(x,m) = 1$ gilt. Diese sind genau die Einheiten in $(\mathbb{Z}_m, +, \cdot)$, d.h. $\mathbb{Z}_m^* = \{\underline{x} \in \mathbb{Z}_m;\ ggT(x,m) = 1\}$.

Die Anzahl der Einheiten sei $\varphi(m) := \#\mathbb{Z}_m^* = \#\{a \in \mathbb{N};\ a \le m,\ ggT(a,m) = 1\}$, die so erklärte Fkt. $\varphi : \mathbb{N} \to \mathbb{N}$ heißt Eulersche φ-Funktion.

Jedes Repräsentantensystem $\{x_1, \dots, x_{\varphi(m)}\}$ von $\mathbb{Z}_m^*$ heißt reduziertes oder primes Restsystem modulo m.

12.) **Satz:** Es ist $\varphi(p^k) = p^k - p^{k-1}$ für alle p prim, alle $k \in \mathbb{N}$, und $\varphi(mn) = \varphi(m)\cdot\varphi(n)$ falls $ggT(m,n) = 1$ (d.h. φ ist „multiplikativ").

Bew.: Unter den Zahlen $1, 2, \dots, p^k$ sind genau die Vielfachen von p zu p^k nicht teilerfremd, d.h. $p, 2p, \dots, p^{k-1}\cdot p$, was p^{k-1} viele Zahlen sind.

Den Bew. der Multiplikativität von φ verschieben wir auf später ($\rightsquigarrow$ 17.)). □

Ist $n = \prod_{p \mid n} p^{e(p)}$ die PFZ von n, folgt aus Satz 12.):

$$\varphi(n) = \prod_{p \mid n}\left(p^{e(p)} - p^{e(p)-1}\right) = \prod_{p \mid n} p^{e(p)}\cdot\left(1 - \frac{1}{p}\right) = n \cdot \prod_{p \mid n}\left(1 - \frac{1}{p}\right).$$

13.) **Folgerungen:** $(\mathbb{Z}_m^*, \cdot)$ ist eine Gruppe, die multiplikative Gruppe von $\mathbb{Z}_m$, und die Gruppe $(\mathbb{Z}_m, +)$ heißt additive Gruppe von $\mathbb{Z}_m$.

Im Fall wenn $\mathbb{Z}_m^* = \mathbb{Z}_m \setminus \{0\}$ ist, ist $(\mathbb{Z}_m, +, \cdot)$ ein Körper; dies ist genau dann richtig, wenn $m = p$ eine Primzahl ist, weil genau dann alle $1, 2, \dots, m-1$ zu m teilerfremd sind. Wir bezeichnen für p prim diesen Körper mit p Elementen mit $\mathbb{F}_p$ (weitere endliche Körper folgen noch).

Der Körper $\mathbb{F}_p$ hat die Eigenschaft, dass $p \cdot a := \overbrace{a+\ldots+a}^{p\text{-mal}} = 0$ in $\mathbb{F}_p$ für alle $a \in \mathbb{F}_p$ gilt. Wir sagen, er hat die Charakteristik p.

14.) **Def.:** Sei k ein Körper. Er hat die **Charakteristik** 0, falls für alle $m \in \mathbb{N}$ gilt: $m \cdot 1 := \underbrace{1+\ldots+1}_{m\text{-mal}} \neq 0$ (z.B. $\mathbb{Q}, \mathbb{R}, \mathbb{C}$).
Falls es ein $m \in \mathbb{N}$ mit $m \cdot 1 = 0$ gibt, so heißt das kleinste solche $m \in \mathbb{N}$ die **Charakteristik** von k, Kurz: $\mathrm{char}(k)$. Bsp.: $\mathrm{char}(\mathbb{Q}) = 0$, $\mathrm{char}(\mathbb{F}_p) = p$.
Bem.: Stets gilt: $\mathrm{char}(k) = 0$ oder $\mathrm{char}(k)$ eine PZ. [Sonst: $0 = (m \cdot n) \cdot 1 = m \cdot (n \cdot 1) = (m \cdot 1) \cdot (n \cdot 1)$ $\Rightarrow m \cdot 1 = 0 \vee n \cdot 1 = 0$, da $k^* = k \setminus \{0\}$ im Bzw. Minimalität von $m \cdot n$.]

Die Struktur der Zahlringe $(\mathbb{Z}_m, +, \cdot)$ versteht man besser, indem man sie auf "kleinere" Zahlringe zurückführt:

15.) **Chinesischer Restsatz** (Zahlring-Version):
Sei $m > 1$ eine natürliche Zahl und $m = m_1 \cdot m_2 \cdot \ldots \cdot m_r$ eine Zerlegung von m in paarweise teilerfremde Zahlen $m_i > 1$.
Dann ist die Abbildung $F: \mathbb{Z}/m\mathbb{Z} \to (\mathbb{Z}/m_1\mathbb{Z}) \times \ldots \times (\mathbb{Z}/m_r\mathbb{Z})$, $x + m\mathbb{Z} \mapsto (x + m_1\mathbb{Z}, \ldots, x + m_r\mathbb{Z})$ ein **Ringisomorphismus**, d.h. ein bijektiver Ringhomomorphismus.

16.) **Chinesischer Restsatz** (Simultane Kongruenzen-Version):
Seien $m_1, \ldots, m_r > 1$ paarweise teilerfremde Zahlen, und seien $a_1, \ldots, a_r \in \mathbb{Z}$. Dann ist das simultane Kongruenzensystem
$x \equiv a_1 \bmod m_1$, $x \equiv a_2 \bmod m_2, \ldots, x \equiv a_r \bmod m_r$
in x lösbar, die Lösungen sind alle kongruent modulo $m_1 \cdots m_r$.
Bem.: Aus Version 15.) folgt Version 16.) wegen der Bijektivität von F, denn $(a_1 + m_1\mathbb{Z}, \ldots, a_r + m_r\mathbb{Z})$ hat dann genau ein Urbild $x + m\mathbb{Z}$.

17.) **Zusatz zum CRS** (= chinesischer Restsatz) in Variante 16.):
Genau alle $x \equiv x_0 \bmod m_1 \cdots m_r$ lösen das System, wobei $x_0 = a_1 M_1^* M_1 + \ldots + a_r M_r^* M_r$, $M_i := \frac{m_1 \cdots m_r}{m_i}$ $(i = 1, \ldots, r)$ und $M_i^* \in \mathbb{Z}$ ein multiplikatives Inverses von M_i mod m_i repräsentiert $(i = 1, \ldots, r)$, d.h. es gilt $M_i^* \cdot M_i \equiv 1 \bmod m_i$, wobei die M_i^* mit dem euklidischen Algorithmus (schnell) berechnet werden können.

18.) Ergänzt zum CRS in Variante 15.): Die Gruppe $\mathbb{Z}_m^*$ ist isom. zu $\mathbb{Z}_{m_1}^* \times \dots \times \mathbb{Z}_{m_r}^*$, beide Gruppen haben dann gleichviele Elemente, es folgt

$\varphi(m) = \varphi(m_1) \cdot \varphi(m_2) \cdots \varphi(m_r)$, speziell $r=2$: $\varphi(m_1 m_2) = \varphi(m_1)\varphi(m_2)$,

d.h. die Multiplikativität von φ ist ein Korollar des CRS.

Beweis des CRS: Wir beweisen Variante 16.), der von Variante 15.) ist im wesentlichen gleich.

Existenz der Lsg.: Ist $x \equiv x_0 \bmod m_1 \cdots m_r$ wie in 17.) angegeben so folgt für alle $1 \le i \le r$: $x \equiv x_0 = \underbrace{a_1 M_1^* M_1}_{\equiv 0 (m_i)} + \dots + \underbrace{a_i M_i^* M_i}_{\equiv a_i \cdot 1 \equiv a_i (m_i)} + \dots + \underbrace{a_r M_r^* M_r}_{\equiv 0 (m_i)} \equiv a_i (m_i)$ ✓

Eindeutigkeit der Lsg. mod $m_1 \cdots m_r$: Ist $y \in \mathbb{Z}$ weitere Lösung des Kongruenzensystems, so gilt $\forall j \neq i$: $y \equiv a_j (m_j)$, also $\underbrace{M_j^* \cdot M_j}_{\equiv 1 (m_j)} \cdot y \equiv a_j (m_j)$, und $M_i \cdot M_i^* \cdot a_i \equiv 0 (m_j)$, (↑ durch m_j teilbar)

und somit

$$y \equiv a_j (m_j) \equiv \sum_{j=1}^{r} M_j M_j^* a_j (m_j) \equiv x_0 (m_j) \text{ für alle } j = 1, \dots, r.$$ [→ $m_j \mid y - x_0$ gemeins. Vielf.]

Da die $m_1, \dots, m_r$ alle paarweise teilerfremd sind, folgt daraus $y \equiv x_0 (\underbrace{m_1 \cdots m_r}_{= \operatorname{kgV}(m_1, \dots, m_r)})$, vgl. Folg. 2.) Nr. (5). □

Bsp. zum CRS: Das System $x \equiv 2 (7)$, $x \equiv 3 (8)$ hat die Lösung $x \equiv 2 \cdot \underbrace{1}_{\text{Inv. von } 8 \bmod 7} \cdot 8 + 3 \cdot \underbrace{(-1)}_{\text{Inv. von } 7 \bmod 8} \cdot 7 = 16 - 21 = -5 \equiv 51 \bmod 56$.

Also: $\left\{ \begin{array}{l} x \equiv 2 (7) \\ \wedge\ x \equiv 3 (8) \end{array} \right\} \Leftrightarrow x \equiv 51 (56)$.

Bsp. dazu: Gegeben seien 2 Tüten mit gleichvielen Bonbons.

$\left\{ \begin{array}{l} \text{Verteilen 1 Tüte Bonbons gleichmäßig an 7 Kinder} \rightsquigarrow 2 \text{ übrige Bonbons} \\ \& \quad " \quad " \quad " \quad " \quad " \quad 8 \quad " \quad \rightsquigarrow 3 \quad " \quad " \end{array} \right\}$

Dann waren 51, 107, ... viele Bonbons in jeder Tüte. Können es nicht mehr als 100 sein, waren es also 51 Stück, und man kann ausrechnen, wieviele Bonbons jedes Kind erhalten hat (7 bzw. 6).

Ein paar Beispiele zum Rechnen mit Kongruenzen bzw. Restklassen:

- **Bsp.:** $5x \equiv 4\ (12) \iff 5^{-1} \cdot 5x \equiv 4 \cdot 5^{-1}\ (12)$
  $\iff x \equiv 4 \cdot 5^{-1} \equiv 4 \cdot 5 = 20 \equiv 8\ (12)$

  [$5 \cdot 5 = 25 \equiv 1\ (12) \Rightarrow 5^{-1} \equiv 5\ (12)$]

Ebenso:
Rechnen mit Restklassen mod 12:

$$\underline{5} \cdot x = \underline{4} \quad | \cdot \underline{5}^{-1} \iff x = \underline{4} \cdot \underline{5}^{-1} = \underline{4} \cdot \underline{5} = \underline{20} = \underline{8}$$

- **Bsp.:** $8x^2 - 2x + 3 \equiv -1\ (7)$
  $\iff (x-1)^2 - 1 + 3 \equiv -1\ (7) \iff (x-1)^2 \equiv -3 \equiv 4\ (7)$.

sprechen auch von „quadratischen Resten"

Da nun wegen

z	0	± 1	± 2	± 3
z^2	0	1	4	2

Die Kongruenz $(x-1)^2 \equiv 4\ (7)$ hat die 2 Lösungen $x \equiv 3\ (7)$, $x \equiv -1\ (7)$.

Die Kongruenz $(x-1)^2 \equiv 5\ (7)$ hätte keine Lösung, da 5 kein Quadrat mod 5 ist.

- **Bsp.:** Die Kongruenz $(x-3) \cdot 4 \equiv 1\ (33)$ ist als Kongruenzensystem $(x-0) \cdot 1 \equiv 1\ (3) \wedge (x-3) \cdot 4 \equiv 1\ (11)$ schreibbar.
  Man kann beide Kongruenzen einzeln lösen, also
  1.) $x \equiv 1\ (3)$ sowie 2.) $(x-3) \equiv 4^{-1} \equiv 3\ (11) \iff x \equiv 6\ (11)$,
  und wieder mit dem CRS zusammensetzen mod 33:

$$x \equiv 1 \cdot \underbrace{2}_{\text{inv. von } 11 \bmod 3} \cdot 11 + 6 \cdot \underbrace{4}_{\text{inv. von } 3 \bmod 11} \cdot 3 = 22 + 6 \cdot 12 = 94 \equiv -5 \equiv 28\ (33).$$

- **Bsp.:** Bei manchen zahlentheoretischen Aufgaben wie z.B. die Frage, ob es ganzzahlige Lösungen zu bestimmten Gleichungen geben kann, ist die „modulare Brille" ein nützliches Hilfsmittel, hier ein Bsp., wo wir die modulare Brille mod 8 aufziehen, um mehr zu sehen:
  Betr. die Glg. $8x + 7 = u^2 + v^2 + w^2$ in $u, v, w, x \in \mathbb{N}_0$.
  Sie ist unlösbar: Denn mod 8 erhalten wir $7 \equiv u^2 + v^2 + w^2\ (8)$;

z	0	± 1	± 2	± 3	4
z^2	0	1	4	1	0

  alle quadratischen Reste mod 8 sind $0, 1, 4$,
  daher ist $v^2 + w^2 \equiv 0, 1, 4, 2, 5\ (8)$,
  also $u^2 + v^2 + w^2 \equiv 0, 1, 4, 2, 5,\ 1, 2, 5, 3, 6,\ 4, 5, 0, 6, 1\ (8)$,
  d.h. $u^2 + v^2 + w^2 \equiv 0, 1, 2, 3, 4, 5, 6\ (8)$, aber nie $\equiv 7\ (8)$.
  Es kann keine Lösungen mod 8 geben, also auch keine in $\mathbb{Z}$.