§4 Kongruenzen & der chinesische Lehrsatz

23.05.18

Kongruenzen beschreiben Teilbarkeitsrelationen. Solche Relationen tauchen auch im täglichen Leben auf. Die Stunden gibt man üblicherweise "modulo 12" an

Def. 4.1

Sei $m \in \mathbb{N}$ und seien $a, b \in \mathbb{Z}$.

Wir sagen, dass "a kongruent zu b modulo m" ist, falls $m \mid (b-a)$. Wir schreiben dafür $a \equiv b \bmod m$.

m nennt man den "Modul" der Kongruenz

Satz 4.2.

Kongruenz modulo m (mit $m \in \mathbb{N}$) definiert eine Äquivalenzrelation auf $\mathbb{Z}$.

Beweis:

Dies folgt aus den Eigenschaften der Teilbarkeit (vgl. 3.3)

Reflexivität: $a \equiv a \bmod m$, da $m \mid (a-a) = 0$

Symmetrie: Ist $a \equiv b \bmod m$, so gilt $m \mid (b-a)$

$\Rightarrow k \cdot m = b-a \Rightarrow -k \cdot m = a-b \Rightarrow m \mid (a-b)$

$\Rightarrow b \equiv a \bmod m$

Transitivität: Es gelte $a \equiv b \bmod m$ und $b \equiv c \bmod m$

Also $m \mid (b-a)$ und $m \mid (c-b) \Rightarrow m \mid \underbrace{(b-a)+(c-b)}_{(c-a)}$

$\Rightarrow a \equiv c \bmod m$ ▨

Nach dem obigen Satz können wir die ganzen Zahlen (für festes $m \in \mathbb{N}$) in sogenannte Kongruenzklassen einteilen.

Die Elemente in einer Kongruenzklasse sind alle ganzen Zahlen, die kongruent zu einer Zahl $a \in \mathbb{Z}$ modulo m sind.

Die Zahl a ist ein Repräsentant der Kongruenzklasse.

Wegen der Division mit Rest gibt es genau m verschiedene Kongruenzklassen.

Beispiel 4.3.

Sei $m = 2$

$a \equiv 0 \mod \frac{m}{2} \iff$ a ist gerade

$a \equiv 1 \mod 2 \iff$ a ist ungerade

Für die Klassen von [0] und [1] erhalten wir also:

$[0] = \{\dots, -4, -2, 0, 2, 4, \dots\}$

$[1] = \{\dots, -3, -1, 1, 3, \dots\}$

Def 4.4.

a) Die Menge aller Kongruenzklassen modulo m bezeichnen wir mit $\mathbb{Z}/m\mathbb{Z}$

b) Ein vollständiges Repräsentantensystem (modulo m) ist eine Menge ganzer Zahlen, s.d. jede Zahl in $\mathbb{Z}$ zu genau einer der Zahlen in dem vollst. Repräsentantensystem kongruent zu modulo m ist.

Jede ganze Zahl ist zu genau einer der $0, \dots, m-1$ kongruent modulo m.

$R = \{0, \dots, m-1\}$ ist ein vollst. Repräsentantensystem der Kongruenz modulo m.

Bemerkung 4.5.

Man überprüft leicht (vgl. Lemma 3.3), dass Kongruenz die folgenden Rechenregeln erfüllt.

Ist $a_1 \equiv b_1 \mod m$ & $a_2 \equiv b_2 \mod m$

$\Rightarrow$ 1) $a_1 \pm a_2 \equiv b_1 \pm b_2 \mod m$

$a_1 \cdot a_2 \equiv b_1 \cdot b_2 \mod m$

$\Rightarrow$ Auf $\mathbb{Z}/m\mathbb{Z}$ haben wir wohldefinierte repräsentantenweise definierte Verknüpfungen:

$$+ \; \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}, \; [a]+[b] := [a+b]$$

$$\cdot \; \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}, \; [a]\cdot[b] := [a\cdot b]$$

Man überprüft schnell (Übung!), dass $(\mathbb{Z}/m\mathbb{Z}, +, \cdot)$, die eines kommutativen Rings mit Einselement hat.

Satz 4.6 (Kürzungssatz)

Seien $a, b, c \in \mathbb{Z}$ und $m \in \mathbb{Z}$ mit $g := ggT(c, m)$

Gilt $a \cdot c \equiv b \cdot c \mod m$, so gilt auch, dass

$$a \equiv b \mod \frac{m}{g}$$

Beweis:

$a \cdot c \equiv b \cdot c \mod m \Rightarrow \exists x$ mit $x \cdot m = c \cdot (a-b)$

Also ist c ein Teiler von $x \cdot m$.

Mit $g = ggT(c, m)$ folgt $x \cdot \left(\frac{m}{g}\right) = \frac{c}{g}(a-b)$

Wegen Proposition 3.10 ist $ggT\left(\frac{m}{g}, \frac{c}{g}\right) = 1$.

$\Rightarrow \frac{m}{g}$ ist ein Teiler von $(a-b) \Rightarrow a \equiv b \mod \left(\frac{m}{g}\right)$

Korollar 4.7

Seien $a, b, c \in \mathbb{Z}$ und $m \in \mathbb{N}$ mit $ggT(c, m) = 1$

Gilt $a \cdot c \equiv b \cdot c \mod m$, so folgt $a \equiv b \mod m$.

Ähnlich zur linearen Algebra, in der man lineare Gleichungen löst, möchten wir die obigen Resultate nutzen, um lineare Kongruenzen der Form $a \cdot x \equiv b \mod m$ zu lösen.

Beispiel 4.8

(a) Betrachte $4 \cdot x \equiv 3 \mod 11$

Es ist $4 \cdot 3 = 12 \equiv 1 \mod 11$

Ergänzen der obigen Kongruenz (mit 3) liefert.

$12x \equiv 9 \mod 11$

$1 \cdot x \equiv 9 \mod 11$

$\Rightarrow$ die Kongruenz hat also modulo 11 eine eindeutige Lösung $x = [9]$ (alle x der Form $x = 9 + k \cdot 11$) lösen die Kongruenz.

(b) Betrachte $4 \cdot x \equiv 3 \mod 12$

Da keine Zahl $c \in \mathbb{Z}$ existiert mit $4 \cdot c \equiv 1 \mod 12$ klappt der Trick aus (a) nicht. Wegen $ggT(4, 3) = 1$ kann der Term 4 auch nicht gekürzt werden.

Tatsächlich hat die obige lineare Kongruenz keine Lösung.

Satz 4.9. (Lösen von linearen Kongruenzen)

Seien $a, b \in \mathbb{Z}$ und $m \in \mathbb{N}$. Sei ferner $g = ggT(a, m)$

(a) Gilt $g \nmid b$ so hat die Kongruenz $a \cdot x \equiv b \mod m$ keine Lösung

(b) Gilt $g \mid b$ so hat die Kongruenz $a \cdot x \equiv b \mod m$ genau g verschiedene Lösungen modulo m.

Beweis:

Wir zeigen zunächst, dass $a \cdot x \equiv b \bmod m$ lösbar ist, genau dann, wenn $g = ggT(a,m) \mid b$.

Nach dem erweiterten Euklidischen Algorithmus ex. $y, z \in \mathbb{Z}$ mit $g = y \cdot a + z \cdot m$. Gilt $g \mid b$, so ist $\frac{b}{g} \in \mathbb{Z}$

$\Rightarrow a \cdot \underbrace{y \cdot \frac{b}{g}}_{x} + m \cdot z \cdot \frac{b}{g} = \frac{b}{g} \cdot g = b$

$\Rightarrow x = y \cdot \frac{b}{g}$ löst die Kongruenz.

Umgekehrt: Ist x eine Lsg von $a \cdot x \equiv b \bmod m$, dann ex. $y \in \mathbb{Z}$ mit $\underbrace{a \cdot x - y \cdot m = b}$ $\Rightarrow g \mid b$

$g = ggT(a,m)$ teilt jede Darstellung dieser Form.

Es bleibt die Anzahl der Lösungen zu bestimmen (im Fall $g \mid b$):

1) Ist $g = ggT(a,m) = 1 \Rightarrow \exists y, z \in \mathbb{Z}$ mit $1 = a \cdot y + m \cdot z$

$\Rightarrow a \cdot y \equiv 1 \bmod m$ (vgl. Bsp. 4.8 (a))

Ergänzen der Kongruenz $a \cdot x \equiv b \bmod m$ mit y liefert $x \equiv y \cdot b \bmod m$.

$\Rightarrow$ Die Kongruenz $a \cdot x \equiv b \bmod m$ hat eine eindeutige Lsg

2) Ist $g > 1$ so liefert Satz 4.6., dass man die Kongruenz $a \cdot x \equiv b \bmod m$ zu: $\frac{a}{g} \cdot x \equiv \frac{b}{g} \bmod \frac{m}{g}$ umstellen kann.

Dies hat man wegen $ggT\left(\frac{a}{g}, \frac{m}{g}\right) = 1$ (vgl. Prop. 3.10) mit (1) eine eindeutige Lösung modulo $\frac{m}{g}$.

Also hat $a \cdot x \equiv b \bmod m$ genau g verschiedene Lösungen modulo m.

Ist x_0 die eindeutige Lösung von $\frac{a}{g} \cdot x \equiv \frac{b}{g} \bmod \frac{m}{g}$

So sind die folgenden $x_0 + k \cdot \frac{m}{g}$ für $k = 0, \dots, g-1$ Lösungen von $a \cdot x \equiv b \bmod m$. ☐

Der vorherige Beweis liefert ein Verfahren zum Lösen von linearen Kongruenzen:

Betrachte $a \cdot x \equiv b \mod m$ mit $ggT(a,m) = g$

Eine Lösung $x \in \mathbb{Z}$ entspricht einer Lösung der Gleichung $a \cdot x - m \cdot y = b \quad (y \in \mathbb{Z})$

Mit dem erweiterten Eukl. Algorithmus berechnen wir $c, d \in \mathbb{Z}$ mit $a \cdot c - m \cdot d := g \equiv ggT(a,m)$

$x_0 := \frac{c \cdot b}{g}$ ist dann eine Lösung der Kongruenz.

Der obige Beweis zeigt, dass alle x der Form

$x = x_0 + k \cdot \frac{m}{g} \mod m \quad (k = 0, \dots, (g-1))$

Ein wenig allgemeiner erhalten wir den folgenden Satz:

Satz 4.10

Seien $a, b \in \mathbb{Z}$ und $g = ggT(a,b)$.

Die Gleichung $a \cdot x + b \cdot y = c$ mit $g \mid c$ hat unendlich viele Lösungen. Sind $x_0, y_0 \in \mathbb{Z}$ Lösungen, so ist auch $x = x_0 + \frac{b}{g} \cdot k$, $y = y_0 - \frac{b}{g} \cdot k$ (mit $k \in \mathbb{Z}$) eine Lösung ☰

Gleichungen der Form $a \cdot x + b \cdot y = c$ heißen lineare diophantische Gleichungen (Diophant i. gr. Math. ~250 n. Chr.)

Der indische Mathematiker Brahmagupta (7. Jht. n. Chr.) war der Erste, der lineare Diophantische Gleichungen vollständig gelöst hat.

Allgemeiner heißt eine Gleichung für die man ganzzahlige Lösungen sucht, eine Diophantische Gleichung.

Das Lösen von Diophantischen Gleichungen hat viele praktische Anwendungen wie das folgende Beispiel zeigt.

Beispiel 4.11 (Ein Briefmarkenproblem)

- Wir möchten 3,90 € an Briefmarken auf einen Brief kleben.
- Wir haben hierzu nur Briefmarken für 45 Cent & 55 Cent zur Verfügung.
- Können wir nur mit solchen Briefmarken 3,90 € bekommen?

Wir suchen also eine positive Lösung $(x, y > 0)$ der Gleichung

$x \cdot 55 + y \cdot 45 = 390$.