§ 2. Kongruenzen

1. Def Sei $a, b, m \in \mathbb{Z}$. Wenn gilt

$m \mid (a-b)$, so schreiben wir

$a \equiv b \pmod{m}$ lies: "a kongruent b modulo m"

[oder kurz $a \equiv b \ (m)$]

Umformulierung: b entsteht aus a durch Addition oder Subtraktion eines Vielfachen von m.

Bsp
- $5 \equiv 7 \pmod{2}$
- $5 \not\equiv 7 \pmod{3}$
- $a \equiv 0 \pmod{2} \iff a$ gerade
- $a \equiv b \pmod{0} \iff a = b$

2. Rechenregeln für Kongruenzen. Sei $a, b, c, m \in \mathbb{Z}$

(i) $a \equiv 0 \pmod{m} \iff a \in m\mathbb{Z}$
$\iff m \mid a$

(ii) $a \equiv a \pmod{m}$ gilt immer

(iii) $a \equiv b \pmod{m} \iff b \equiv a \pmod{m}$

(iv) $a \equiv b \pmod{m}$ und $b \equiv c \pmod{m}$
$\implies a \equiv c \pmod{m}$

<u>Beweis</u> (i), (ii) klar.

(iii) $a \equiv b \pmod m \Leftrightarrow m \mid a-b \Leftrightarrow m \mid b-a$
$\Leftrightarrow b \equiv a \pmod m$

(iv) $a-b = s\cdot m$ und $b-c = t\cdot m \Rightarrow$
$a-c = (s\cdot m+b) + (t\cdot m - b) = (s+t)\cdot m$ $\square$

<u>Folgerung</u> Ist $m \in \mathbb{Z}$ fest gewählt, so ist Kongruenz modulo m eine <u>Äquivalenzrelation</u> auf $\mathbb{Z}$ (reflexiv, symmetrisch und transitiv).

<u>Zusammenhang zum Teilen mit Rest:</u> Sei $\boxed{m > 0}$

Seien $a, a' \in \mathbb{Z}$, teile durch m mit Rest,

$a = m\cdot s + r$ $\quad$ $a' = m\cdot s' + r'$
$0 \leq r < m$ $\quad$ $0 \leq r' < m$

Dann gilt: $a \equiv a' \mod m \Leftrightarrow r = r'$

3. <u>Satz</u> Sei $m \in \mathbb{Z}$. Dann ist Kongruenz modulo m verträglich mit Addition, Subtraktion und Multiplikation. Genauer:

Sind $a, a', b, b' \in \mathbb{Z}$ mit $a \equiv a' \pmod m$
$b \equiv b' \pmod m$

so gilt
$$a + b \equiv a' + b' \pmod m$$
$$a - b \equiv a' - b' \pmod m$$
$$a \cdot b \equiv a' \cdot b' \pmod m$$

<u>Beweis</u> Schritt $a' := a + s \cdot m$, $b' := b + t \cdot m$.

Es folgt
$$a' + b' = a + b + (s+t) \cdot m \quad (\checkmark)$$
$$a' - b' = a - b + (s-t) \cdot m \quad (\checkmark)$$
$$a' \cdot b' = ab + (b \cdot s + a \cdot t + st) m \quad (\checkmark) \qquad \square$$

<u>Vorsicht</u>. Das <u>Kürzen</u> ist bei Kongruenzen im Allgemeinen nicht erlaubt!

<u>Bsp</u> $2 \cdot 3 \equiv 0 \pmod 6$

aber $2 \not\equiv 0 \pmod 6$ und $3 \not\equiv 0 \pmod 6$.

4. <u>Anwendung: Teilbarkeitsregeln</u>

„Eine Zahl ist durch 3 (bzw 9) teilbar genau dann, wenn ihre Quersumme durch 3 (bzw 9) teilbar ist."

<u>Genauer</u>. Sei $n \in \mathbb{N}$ mit <u>Dezimaldarstellung</u>

$$n = \sum_{j=0}^{k} 10^j \cdot a_j \qquad 0 \le a_j < 9,$$

d.h. $a_0, \ldots, a_k$ sind die Ziffern in Dezimaldarstellung, zB
$$1044 = \underline{4} \cdot 10^0 + \underline{4} \cdot 10^1 + \underline{0} \cdot 10^2 + \underline{1} \cdot 10^3$$

Die Quersumme ist also $a_0 + a_1 + a_2 + \ldots + a_k$

Es gilt $10 \equiv 1 \pmod 3$ sowie $10 \equiv 1 \pmod 9$,

also für alle $j \geq 0$ $10^j \equiv 1 \pmod 3$

$10^j \equiv 1 \pmod 9$

Damit erhalten wir:

$$3 \mid n \Leftrightarrow n \equiv 0 \pmod 3 \Leftrightarrow \sum_{j=0}^{k} 10^j \cdot a_j \equiv 0 \pmod 3$$

$$\Leftrightarrow \sum_{j=0}^{k} a_j \equiv 0 \pmod 3 \Leftrightarrow 3 \mid \underbrace{a_0 + a_1 + \ldots + a_k}_{\text{Quersumme}}$$

Genauso $9 \mid n \Leftrightarrow \ldots \Leftrightarrow 9 \mid a_0 + a_1 + \ldots + a_k$

$\square$

Ganz ähnlich: n ist gerade $\Leftrightarrow a_0$ gerade

Denn n gerade $\Leftrightarrow 2 \mid n \Leftrightarrow n \equiv 0 \pmod 2$

$\Leftrightarrow a_0 + 10 \cdot a_1 + \ldots + 10^k \cdot a_k \equiv 0 \pmod 2$

$\Leftrightarrow a_0 \equiv 0 \pmod 2$

n ist durch 5 teilbar $\Leftrightarrow a_0$ ist durch 5 teilbar

$\square$

Teilbarkeit durch 11 Es gilt $10 \equiv -1 \pmod{11}$

damit $11 \mid n \Leftrightarrow n \equiv 0 \pmod{11} \Leftrightarrow$

$$\underbrace{a_0 - a_1 + a_2 - a_3 + a_4 \ldots}_{\text{"alternierende Quersumme"}} \equiv 0 \pmod{11}$$

Bsp 5731 ist durch 11 teilbar, denn

$1 - 3 + 7 - 5 = 0 \equiv 0 \pmod{11}$ $\square$

5. <u>Satz</u> Sei $a, b, c, m \in \mathbb{Z}$. Wenn gilt $ggT(c, m) = 1$ und wenn gilt $a \cdot c \equiv b \cdot c \pmod{m}$, so folgt $a \equiv b \pmod{m}$.

"Teilerfremde Faktoren darf man kürzen"!

<u>Beweis</u> Wenn $a \cdot c \equiv b \cdot c$, dann $m \mid (a-b) \cdot c$. Nach § 1.20 (erstes Lemma) folgt $m \mid a-b$, denn $ggT(m, c) = 1$. Also $a \equiv b \pmod{m}$ □

<u>Bsp</u>

$$4 \cdot x \equiv 1 \pmod{15}$$
$$\Leftrightarrow 4 \cdot x \equiv 16 \pmod{15}$$
$$\overset{(*)}{\Leftrightarrow} x \equiv 4 \pmod{15}$$

(*) weil $ggT(4, 15) = 1$ #

6. <u>Anwendung</u> Wir lösen damit die lineare Diophantische Gleichung $9 \cdot x + 16 \cdot y = 35$:

$$9 \cdot x + 16 \cdot y = 35 \Leftrightarrow 16 \cdot y \equiv 35 \pmod{9}$$
$$\Leftrightarrow 7 \cdot y \equiv 35 \pmod{9}$$
$$\overset{(*)}{\Leftrightarrow} y \equiv 5 \pmod{9}$$
$$\Leftrightarrow y = 5 + 9 \cdot t$$

(*) $ggT(9, 7) = 1$

Insgesamt $9\cdot x + 16(5+9\cdot t) = 35$

$$\Leftrightarrow 9\cdot x + 144\cdot t + 80 = 35$$

$$\Leftrightarrow 9x + 144\cdot t + 45 = 0 \quad |:9$$

$$\Leftrightarrow x + 16\cdot t + 5 = 0$$

$$\Leftrightarrow x = -(16\cdot t+5)$$

Lösungsmenge ist also $L = \{(-16\cdot t+5, 9\cdot t+5) \mid t \in \mathbb{Z}\}$

7. <u>Def</u> Sei $a, b, m \in \mathbb{Z}$. Eine Gleichung der Form

$$a\cdot x \equiv b \pmod m$$ heißt <u>lineare Kongruenz</u>,

gesucht sind Lösungen $x \in \mathbb{Z}$.

Offensichtlich äquivalent dazu ist das Problem, alle $x \in \mathbb{Z}$ zu bestimmen, so dass

$$a\cdot x + y\cdot m = b$$ für ein $y \in \mathbb{Z}$ gilt.

Das ist eine lineare Diophantische Gleichung, also erhalten wir folgenden Satz.

<u>Satz</u> Sei $a, b, m \in \mathbb{Z}$ mit $m > 0$. Die lineare Kongruenz $a\cdot x \equiv b \pmod m$ ist genau dann lösbar, wenn gilt

$$ggT(a,m) \mid b.$$

<u>Beweis</u> Folgt mit der vorigen Umformulierung aus § 1.19. $\square$

8. Bem Falls gilt $d = ggT(a,m) \mid b$, so folgt aus § 1.20, wie die Lösungen aussieht:
Ist $x_0 \in \mathbb{Z}$ mit $a \cdot x_0 \equiv b \pmod m$, so ist jede weitere Lösung x der linearen Kongruenz
$a \cdot x \equiv b \pmod m$ von der Form

$x = x_0 + t \cdot m'$, wobei $d \cdot m' = m$
$t \in \mathbb{Z}$

Satz §2.5 lässt sich verbessern, das ist zum Rechnen hilfreich.

9. Satz Sei $a, b, c, m \in \mathbb{Z}$ mit $m > 0$, sei $d = ggT(c, m)$ und $d \cdot m' = m$. Dann sind äquivalent:

(i) $a \cdot c \equiv b \cdot c \pmod m$

(ii) $a \equiv b \pmod{m'}$

Bew: Angenommen, $m = m' \cdot d \mid c \cdot (a-b)$, etwa $k \cdot m = c (a-b)$. Schreibe $c = d \cdot c'$, so folgt

$m' \cdot \cancel{d} \cdot k = c' \cdot \cancel{d} \cdot (a-b)$ $\quad (d \neq 0 !)$

$\Rightarrow m' \cdot k = c'(a-b)$ $\quad (ggT(m', c') = 1)$

$\Rightarrow m' \mid a-b$ $\quad$ vgl. § 1.20

Angenommen, $m' \mid a-b$, etwa $m' \cdot l = a-b$

$\Rightarrow \underbrace{l \cdot c \cdot m'}_{= \underbrace{l \cdot d \cdot c' \cdot m'}_{= l \cdot m \cdot c'}} = c \cdot (a-b) \Rightarrow m \mid c \cdot (a-b)$

$\square$

Beispiel Lineare Kongruenz $6 \cdot x \equiv 15 \pmod{33}$

$$\Leftrightarrow \quad 2 \cdot x \equiv 5 \pmod{11} \qquad 33 = 11 \cdot \underline{3}$$

$$\Leftrightarrow \quad 2 \cdot x \equiv 16 \pmod{11} \qquad \mathrm{ggT}(33,3) = 3$$

$$\Leftrightarrow \quad x \equiv 8 \pmod{11}$$

$\uparrow$

$\mathrm{ggT}(2,11) = 1$

$$\Leftrightarrow \quad x \in L = \{ 11t + 8 \mid t \in \mathbb{Z} \}$$

10. **Ausblick** Für $a, m \in \mathbb{Z}$ definieren wir Kongruenzklassen modulo m

$$[a]_m = \{ a' \in \mathbb{Z} \mid a \equiv a' \bmod m \}.$$
$$= \{ a' \in \mathbb{Z} \mid \text{es gibt } t \in \mathbb{Z} \text{ mit } a' = mt + a \}$$
$$= \{ a + m \cdot t \mid t \in \mathbb{Z} \}$$

Es gilt $[a]_m = [b]_m \Leftrightarrow b \in [a]_m$
$\Leftrightarrow m \mid b - a$

Für $a, a', b, b' \in \mathbb{Z}$ mit $a \equiv a' \bmod m$
$b \equiv b' \bmod m$

Folgt mit §2.3, dass $[a \cdot b]_m = [a' \cdot b']_m$
$[a+b]_m = [a'+b']_m$

Wir können das zwei Verknüpfungen $+$ und $\cdot$ definieren durch

$$[a]_m + [b]_m = [a+b]_m$$

$$[a]_m \cdot [b]_m = [a \cdot b]_m$$

Das führt uns auf Gruppen und Ringe.