Def. 1: Sei $m \in \mathbb{N}$ fest. Für $x \in \mathbb{Z}$ sei $r_m(x)$ der Rest von x bei Division durch m.

$[q, r \in \mathbb{Z}]$ $$x = qm + r \qquad 0 \le r < m \qquad r = r_m(x) \text{ eindeutig}$$

$x \underset{m}{\sim} x'$ heiße: $r_m(x) = r_m(x')$ "Gleichheit bzgl. m"

Statt $x \underset{m}{\sim} x'$ schreibt man nach Gauß:

sehr glückliche Bez. [vgl. Kongruenz von Dreiecken]

$$x \equiv x' \bmod m$$

x kongruent x' mod m

$x' - x = (q'-q)m + (r'-r)$

F1: $x \equiv x' \bmod m \iff m \mid x' - x$

[für jedes $m \in \mathbb{Z}$ sinnvoll]

Bew. klar.

Def. 1': R komm. Ring, $m \in R$.

$x \equiv y \bmod m$ heiße: $m \mid x - y$

$x \equiv y \bmod 0 \implies x = y$

$x \equiv y \bmod 1$ gilt für alle $x, y \in R$

$x \equiv 0 \bmod m \iff m \mid x$

F2: (i) $x \equiv x \bmod m$, $x \equiv y \bmod m \Rightarrow y \equiv x \bmod m$,

$x \equiv y \bmod m$, $y \equiv z \bmod m \implies x \equiv z \bmod m$,

d.h. man hat Äquivalenzrelation in R (abhängig von m). Diese ist verträglich mit Addition u. Multiplikation:

(ii) $$\left.\begin{matrix} x \equiv x' \bmod m \\ y \equiv y' \bmod m \end{matrix}\right\} \implies \begin{matrix} x + y \equiv x' + y' \bmod m \\ xy \equiv x'y' \bmod m \end{matrix}$$

(iii) $x \equiv y \bmod m$, $m' \mid m \Rightarrow x \equiv y \bmod m'$

(iv) für $R = \mathbb{Z}$: $x \equiv y \bmod m_i,\ 1 \le i \le r \iff x \equiv y \bmod \overset{\text{kgV}}{[m_1, \dots, m_r]}$

Speziell: Sind $m_1, \dots, m_r$ paarweise teilerfremd, so

$$x \equiv y \bmod m_i,\ 1 \le i \le r \iff x \equiv y \bmod m_1 m_2 \cdots m_r$$

(v) $x \equiv y \bmod m \Rightarrow cx \equiv cy \bmod cm \Rightarrow cx \equiv cy \bmod m$

γ für Int.ring R: (vi)γ $x \equiv y \bmod m$ und $l \mid x$, $l \mid m$, $l \neq 0 \Rightarrow l \mid y$ und $\frac{x}{l} \equiv \frac{y}{l} \bmod \frac{m}{l}$

(vii) für $R = \mathbb{Z}$: Ist $(c, m) = d$ mit $d \neq 0$, so gilt:

$$ac \equiv bc \bmod m \Rightarrow a \equiv b \bmod \frac{m}{d} \quad (\Rightarrow a \equiv b \bmod m)$$

Speziell: Sind c, m teilerfremd, so

$$ac \equiv bc \bmod m \Rightarrow a \equiv b \bmod m$$

Bew. klar.

(vii): $m \mid ac - bc \Rightarrow m \mid c(a-b) \Rightarrow \frac{m}{d} \mid \frac{c}{d}(a-b)$

$$\xRightarrow{(\frac{m}{d}, \frac{c}{d}) = 1} \quad \frac{m}{d} \mid a - b$$

Def.2 Wegen (i): Ein $m \in R$ teilt R in disjunkte Mengen ein, die zugehörigen Äquivalenzklassen. Diese heißen die Restklassen mod(ulo) m.

Bsp. $n \in \mathbb{N}$, n ungerade. $(n-1)! = 1 \cdot 2 \cdot 3 \cdot \ldots \cdot (n-2)(n-1) =$

$1(n-1) \cdot 2 \cdot (n-2) \ldots \frac{n-1}{2} \cdot (n - \frac{n-1}{2}) \equiv 1 \cdot (-1) \cdot 2(-2) \ldots \frac{n-1}{2}(-\frac{n-1}{2}) \bmod n$

also

F3: $n \in \mathbb{N}$, n ungerade. Dann

$$\boxed{(n-1)! \equiv 1^2 \cdot 2^2 \cdot \ldots \cdot \left(\frac{n-1}{2}\right)^2 \cdot (-1)^{\frac{n-1}{2}} \bmod n}$$

F4: $a, b, c \in \mathbb{Z}$, $d := (a,b)$. Die Gleichung

(1) $$aX + bY = c$$

ist genau dann lösbar (über $\mathbb{Z}$), wenn $d | c$. Sei $d \neq 0$.
Ist (x_0, y_0) eine Lösung von (1), so gehört zu jeder Lösung (x,y) von (1) genau ein $t \in \mathbb{Z}$ mit

(2) $$x = x_0 + t\frac{b}{d}, \quad y = y_0 - t\frac{a}{d}$$

Jedes (x,y) wie in (2) ist eine Lösung von (1).

Bew. 1) $ax + by = c \Rightarrow d | c$

2) $d = \tilde{x}a + \tilde{y}b$ Vor: $d | c \Rightarrow c = zd$. Es folgt

$$c = (z\tilde{x})a + (z\tilde{y})b$$

3) (x,y) Lsg. von (1) $\Leftrightarrow xa + yb = c$

$$\Leftrightarrow x\frac{a}{d} + y\frac{b}{d} = \frac{c}{d}.$$ Man hat $\left(\frac{a}{d}, \frac{b}{d}\right) = 1$

Jetzt vgl. Aufgabe 11.

F5: Die Kongruenz

(1) $$aX \equiv c \mod m$$

ist genau dann lösbar (alles über $\mathbb{Z}$), wenn

(2) $$(a,m) | c$$

Sei $d := (a,m) \neq 0$, und es gelte (2). Die Lösungsmenge von (1) ist dann eine Restklasse mod $\frac{m}{d}$. Die Kongruenz (1) besitzt genau $d = (a,m)$ viele Lösungen mod m. Insbesondere:

Ist $(a,m) = 1$, so ist (1) für jedes c lösbar und die Lsg'en sind modulo m eindeutig.

<u>Bew.</u> 1) (1) lösbar $\Leftrightarrow$ $\exists x \in \mathbb{Z}$ mit $ax \equiv c \bmod m$ $\Leftrightarrow$

$\exists x, y \in \mathbb{Z}$ mit $ax = c - ym$, d.h. (*) $ax + ym = c$ $\overset{F4}{\Longleftrightarrow}$ $(a,m) \mid c$, d.h. (2)

2) Sei x_0 Lsg. von (1). Wegen (*) sind (vgl. F4)

$$x = x_0 + t\frac{m}{d} \quad (t \in \mathbb{Z}) \text{ sämtliche Lsg'n von (1),}$$

also bilden diese eine Restklasse mod $\frac{m}{d}$. Setze $m' := \frac{m}{d}$.

Dann sind $x_0, x_0 + m', x_0 + 2m', \ldots, x_0 + (d-1)m'$

die <u>d verschiedenen Lsg'n</u> von (1) <u>mod m</u>. (Diese Sprechweise ist hoffentlich nicht verwirrend!)

<u>Def. 2'</u>: R komm. Ring, $m \in R$. Die Restklasse mod m, in der $a \in R$ liegt, hat die Gestalt

$$\{x \in R \mid x \equiv a \bmod m\} = a + mR = \{a + ym \mid y \in R\}$$

Die Menge aller Restklassen mod m bezeichnen wir mit

R/mR oder auch mit R/m

wichtigster Fall (für uns): $R = \mathbb{Z}$, in der Regel: <u>$m \in \mathbb{N}, m > 1$</u>

<u>Anderes (wichtiges) Beispiel:</u> $m \in \mathbb{N}, m > 1$

$R = \mathbb{Z}_{(m)} := \left\{ \frac{b}{a} \mid a, b \in \mathbb{Z}, (a,m) = 1 \right\}$ Teilring von $\mathbb{Q}$

$$\mathbb{Z} \subseteq \mathbb{Z}_{(m)} \subseteq \mathbb{Q}$$

Die Inklusionsabb. $\mathbb{Z} \to \mathbb{Z}_{(m)}$ vermittelt Homomorph.

(*) $\mathbb{Z}/m\mathbb{Z} \longrightarrow \mathbb{Z}_{(m)}/m\mathbb{Z}_{(m)}$

vgl. S.60 <u>Beh.</u> (*) ist bijektiv, also <u>Isomorphismus</u> von Ringen.

Bew. 1) $x, y \in \mathbb{Z}$. $\quad x \equiv y \bmod m$ in $\mathbb{Z} \Rightarrow x \equiv y \bmod m$ in $\mathbb{Z}_{(m)}$

$x \equiv y \bmod m$ in $\mathbb{Z}_{(m)} \Rightarrow x - y = \frac{b}{a} m$ mit $(a,m) = 1 \Rightarrow$

$$a(x-y) = bm,\ (a,m) = 1 \Rightarrow m \mid x - y$$

$$\Rightarrow x \equiv y \bmod m \text{ in } \mathbb{Z}.$$

Also (*) wohldefiniert und injektiv.

2) $\frac{b}{a} \in \mathbb{Z}_{(m)}$ gegeben, $(a,m) = 1$.

z.z. $\exists x \in \mathbb{Z}$ mit $x \equiv \frac{b}{a} \bmod m$ (in $\mathbb{Z}_{(m)}$).

Wegen $(a,m) = 1$ ex. nach F5 ein $x \in \mathbb{Z}$ mit

$$ax \equiv b \bmod m \quad (\text{in } \mathbb{Z})$$

$$\Rightarrow \quad \frac{1}{a} ax \equiv \frac{1}{a} b \bmod \frac{1}{a} m \quad \text{in } \mathbb{Z}_{(m)}, \quad \text{d.h.}$$

$$x \equiv \frac{b}{a} \bmod \underset{\underset{R}{\Uparrow}}{\frac{1}{a}} m \quad \overset{\text{trivial}}{\Longrightarrow} \quad x \equiv \frac{b}{a} \bmod m$$

Bem. Sei $(a,m) = 1$. Wohlverstanden, darf man also sagen: Die Kongruenz

$$aX \equiv c \bmod m$$

besitzt die Lösung $\frac{c}{a} \bmod m$. Es gibt dann ein $x \in \mathbb{Z}$ mit $x \equiv \frac{c}{a} \bmod m$ (und für diesen ist $ax \equiv c \bmod m$)

Bsp. Die Kongruenz $7X \equiv 1 \bmod 123$ ist „eindeutig" lösbar.

$7x \equiv 1 \bmod 123 \Rightarrow x \equiv \frac{1}{7} = \frac{4}{28} \equiv \frac{-119}{28} = -\frac{17}{4} \equiv -\frac{140}{4} \equiv -35 \bmod 123$

Das funktioniert nicht immer so gut, aber allgemein kann man Folgendes sagen:

[S.47] **Bem.** Zur Lösung der Kongruenz

(1) $\qquad aX \equiv 1 \bmod m \quad$ mit $(a,m) = 1$ und $a \in \mathbb{N}$.

Betrachte $\alpha = \frac{m}{a} \in \mathbb{Q}$. Kettenbruchentw. durchführen.

Diese ende mit $\frac{m}{a} = \frac{c_n}{d_n}$. Dann gilt (vgl. §2, Bsp. nach Satz 2)

$$(-1)^n c_{n-1} a - (-1)^n d_{n-1} m = 1$$

$$\Rightarrow \qquad a(-1)^n c_{n-1} \equiv 1 \bmod m . \qquad \text{Somit}$$

<u>$x = (-1)^n c_{n-1}$ ist Lösung von (1).</u>

Beispiel: (1) $\;4x \equiv 1 \bmod 123$

q			30	1	3
c	0	1	30	$\boxed{31}$	123
d	1	0	1	1	4

$123 : 4 = 30$
$\underline{120}$
$4 : 3 = 1$
$\underline{3}$
$3 : 1 = 3$

$\boxed{n=2}$

gestrichene untere Zeile und letzte Spalte braucht man eigentlich nicht, aber gut zur Kontrolle.

also $x = 31$ ist eine Lösung der Kongruenz (1)

$\{x \in \mathbb{Z} \mid x \equiv 31 \bmod 123\}$ ist die Menge <u>aller</u> Lösungen von (1) in $\mathbb{Z}$.

Man sagt auch, "$x \equiv 31 \bmod 123$ ist <u>die</u> Lsg. von (1)".