~~b~~ is a multiple of ~~B~~ a
a is a divisor of b
a divides b

18. 7. 2023

$a, m \in \mathbb{Z} \Rightarrow \exists\, b, q : a = mq + b$ $b < m$

$a \mid b \overset{\text{def}}{\Leftrightarrow} a \cdot q = b$ $\Longleftrightarrow$ $a \equiv b \mod m \Leftrightarrow m \mid a - b$

$m \cdot q = a - b$
$a = b + m \cdot q$
$b = a - m \cdot q$

$a \mid b \Rightarrow a \mid b \cdot c$
$a \mid b \Rightarrow ac \mid bc$

$\Longleftrightarrow$

$a \equiv b \mod m \Rightarrow$
$a \pm c \equiv b \pm c \mod m$
$a \cdot c \equiv b \cdot c \mod m$
$ac \equiv b \cdot c \mod m \cdot c$

Any module
$M = \{ n \cdot d \mid n \in \mathbb{Z} \}$

$\Downarrow$

Euclid $\leftarrow$ ~~smallest m~~ $\{ ax + by \mid x, y \in \mathbb{Z} \} = \{ n \cdot d \mid n \in \mathbb{Z} \}$

$\Downarrow$

extended Euclid $\leftarrow$ Bézout:
$ax + by = c$ solvable $\Leftrightarrow$
$(a, b) \mid c$

$a x = 1 \mod m \\ (a, m) = 1$ $\Big\}\; x = a^{-1}$ $\rightarrow$ $\mathbb{F}_p$ is a field

$ac \equiv bc \mod m \Rightarrow$
$a \equiv b \mod \frac{m}{(a, m)}$

$\Longleftrightarrow$

$\Downarrow$

Euler's lemma ①, ②
$\left.\begin{matrix}(a, b) = 1 \\ a \mid c, b \mid c\end{matrix}\right\} \Rightarrow ab \mid c$
$\left.\begin{matrix}(a, c) = 1 \\ c \mid a \cdot b\end{matrix}\right\} \Rightarrow c \mid b$

$\Longleftrightarrow$

① $a \cdot b \equiv 0 \mod m$
$(a, m) = 1 \Rightarrow$
$b \equiv 0 \mod m$

② $c \equiv 0 \mod a$
$c \equiv 0 \mod b$
$\Rightarrow c \equiv 0 \mod a \cdot b$

$\Downarrow$

$\Downarrow$

Unique decomposition of integers

Little Fermat, Euler's Theorem $aA = A$

$\mathbb{Z}/m \times \mathbb{Z}/\ldots$
$\mathbb{Z}/N \cong$

$x = a_1 \mod m_1$
$x \equiv \ldots \mod m_2$

Chinese Remainder

Chinese Remainder

$N = \prod m_i$

$x \equiv a_1 \mod m_1$

$x \equiv a_2 \mod m_2$

$\vdots$

$x \equiv a_k \mod m_k$

has a unique solution, iff

$(m_i, m_j) = 1 \quad (i \neq j)$

Proof:

(1) solution is unique:
(Euler 2)

$x - y \equiv 0 \mod m_1$

$x - y \equiv 0 \mod m_2$

$\Rightarrow x - y \equiv 0 \mod m_1 \cdot m_2$

(2) $(m_1, m_2) = 1$

$x \equiv a_1 \mod m_1$

$x \equiv a_2 \mod m_2$

$q_1 m_1 + q_2 m_2 = 1$ (Bezout ~~(Ext Euclid)~~)

$q_2 m_2 = 1 - q_1 m_1$

$a_{12} = a_1 q_2 m_2 + a_2 q_1 m_1$

$= \ldots =$

$= a_1 + (a_2 - a_1) \cdot q_1 \cdot m_1 \equiv a_1 \mod m_1$

or $\mathbb{Z}/_N \cong \mathbb{Z}/_{m_1} \times \cdots \times \mathbb{Z}/_{m_k}$

$a_{12} \equiv a_1 \mod m_1$

$a_{12} \equiv a_2 \mod m_2$

~~$a_{12} \equiv a$~~

$x \equiv a_{12} \mod m_1 \cdot m_2$

$x \equiv a_3 \mod m_3$

&

~~$a_1 =$~~

$x \equiv a_1 \mod m_1$

$x \equiv a_2 \mod m_2$

$x = a_1 \bmod m_1$

$x = a_2 \bmod m_2$

$(m_1, m_2) = 1$

$\Rightarrow \exists q_{1,2}\ q_1 m_1 + q_2 m_2 = 1$

$\Rightarrow a_1 q_1 m_1 + a_1 q_2 m_2 = a_1$

$\Rightarrow a_1 q_2 m_2 = a_1 (1 - q_1 m_1)$

compute q_1, q_2 by extended euclid, then

$a_{12} = x := a_1 q_2 m_2 + a_2 q_1 m_1 = F(a_1, a_2, m_1, m_2)$

$= a_1(1 - q_1 m_1) + a_2 q_1 m_1$

$= a_1 + (a_2 - a_1) q_1 m_1 \equiv a_1 \bmod m_1$

$3 \mid \cancel{x} \Rightarrow x = 3q_1$

$7 \mid x \Rightarrow x = 7q_2$

$\Rightarrow x = 21q_3$

$x \equiv a_{12} \bmod m_1$

$x \equiv a_{12} \bmod m_2$

$\cancel{x \equiv a_1}$

$x \equiv a_{12} \bmod m_1 \cdot m_2$

$x \equiv a_3 \bmod m_3$

$T(x \pm y)$ ≠

$\cancel{x+y=z}$

$\Rightarrow T(x+y) = T(x) + T(y)$

$x_i + y_i \equiv x + y \mod n_i$

$x_i = x \mod n_i$

$y_i = y_i \mod n_i$

$$\left.\begin{array}{l} x \equiv x_i \mod n_i \\ y \equiv y_i \mod n_i \end{array}\right\} \Rightarrow x \pm y \equiv x_i \pm y_i \mod n_i$$

$x \cdot y \equiv x_i \cdot y_i \mod n_i$

$T: \mathbb{Z}/N \to \mathbb{Z}/n_1 \times \dots \times \mathbb{Z}/n_k$

$x \mapsto (x_1 \dots x_k)$

$x \equiv x_i \mod n_i$

Chinese remainder computes T^{-1}

$x \cdot y \equiv 1 \mod N$

$x_i \cdot y_i \equiv 1 \mod n_i \Rightarrow x \cdot y \equiv 1 \mod N$

$\Rightarrow y = x^{-1}$

	3	5	3	5			
x	x_1	x_2	x_1^{-1}	x_2^{-1}	$x_1^{-1}\cdot x_2^{-1}$	$x_1\cdot x_2$	$\tau(x_1^{-1},x_2^{-1})$
0	0	0	–	–	–	0	–
1	1	1	1	1	1	1	1
2	2	2	2	3	6	4	8
3	0	3	–	2	–	0	–
4	1	4	1	4	4 ←	4	4
5	2	0	2	–	–	0	–
6	0	1	–	1	–	0	–
7	1	2	1	3	3	2	13
8	2	3	2	2	4 ←	6	2
9	0	4	–	4	–	0	–
10	1	0	1	–	–	0	–
11	2	1	2	1	2 ←	2	11
12	0	2	–	3	–	0	–
13	1	3	1	2	2 ←	3	7
14	2	4	2	4	8	8	14

1	
2	2
3	
4	4
6	
8	

1	1	1
2	8	2
4	4	3
7	13	4
8	2	5
11	11	6
13	7	7
14	14	8

$2x \equiv 1 \mod 15$ $\quad x = 8$

$4x = 1 \mod 15$ $\quad x = 4$

$7x \equiv 1 \mod 15$ $\quad x = 13$

$3x \equiv 1 \mod 15$ $\quad ↯$

$4 + 9 \to (1, 8)$

$\equiv (1, 3) \to 13$

$4 \cdot 9 = 36 \equiv 6 \mod 15$

$4 + 9 = 13 = 13 \mod 15$

$4 \to (1, 4)$

$9 \to (0, 4)$

$4 \cdot 9 \to (1 \cdot 0, 4 \cdot 4)$

$= (0, 16) \equiv (0, 1) \to 6$

$(x_1, x_2) \to x$

Euler ①

$$\left.\begin{array}{l}(a,c)=1\\ c\mid a,b\end{array}\right\}\Rightarrow c\mid b$$

$\cancel{ax+by=1}$

$\cancel{\Rightarrow c(ax+by)=cax+cby}$

$\cancel{=a(cx+cb}$

$ax+cy=1$

$bax+cby=c(\underbrace{\tfrac{ab}{c}}_{\in\mathbb{Z}}\cdot x+by)=b$

$\Rightarrow c\mid b$

$a\cdot b\equiv 0 \mod c$

$(a,c)=1$

Euler ②

$$\left.\begin{array}{l}(a,b)=1\\ a\mid c\\ b\mid c\end{array}\right\}\Rightarrow a\cdot b\mid c$$

$ax+by=1$

$\Rightarrow cax+cby=c$

$\Rightarrow ab(\underbrace{\tfrac{c}{b}}_{\in\mathbb{Z}}x+\underbrace{\tfrac{c}{a}}_{\in\mathbb{Z}}y)=c$

$\Rightarrow a\cdot b\mid c$

$\cancel{a\equiv 0 \mod c}$

$(a,b)=1$

$$\left.\begin{array}{l}c\equiv 0 \mod a\\ c\equiv 0 \mod b\end{array}\right\}\Rightarrow c\equiv 0 \mod ab$$

① Each module M of integers looks like

$M = \{ n \cdot d \mid n \in \mathbb{Z} \}$; d = smallest integer of M

② $M = \{ ax + by \mid x, y \in \mathbb{Z} \}$ $\Rightarrow$ $ax + by = c$ has an integer solution $\Leftrightarrow$ $(a,b) \mid c$

$= \{ n \cdot (a,b) \mid n \in \mathbb{Z} \}$

$=$ smallest module containing a and b

③ Euler's lemma

$c \mid a \cdot b \Rightarrow c \mid a$ or $c \mid b$

$\neg\, c \mid a$

$\Rightarrow ax + cy = 1$

$\Rightarrow b = b(ax + cy)$

$= abx + cby$

$= \left(\frac{ab}{c} x + by\right) \cdot c \Rightarrow c \mid b$

④ Congruences

$a \equiv 0 \mod m \Leftrightarrow m \mid a \Leftrightarrow a = x \cdot m$

$\left.\begin{array}{l} a \equiv b \mod m \\ c \equiv d \mod m \end{array}\right\} \Rightarrow \cancel{a \pm c \equiv b \pm d \mod m}$

$a \pm c \equiv b \pm d \mod m$

$ac \equiv bc \mod m \Rightarrow a \equiv b \mod \frac{m}{(c,m)}$

$\equiv b \mod m$ if $(c,m) = 1$

if $(c,m) = 1$, you can divide

$(a,m) = 1$: $a \equiv b \mod m$

$b = 0$ $\quad a \equiv 0 \mod m$

and : $a \cdot b \equiv 0 \mod p$

$\Rightarrow a \equiv 0$ or $b \equiv 0$

5 Fermat's little theorem

$$a^{p-1} \equiv 1 \mod p$$

$A = \{1, 2, \dots, p-1\}$ $\quad a \cdot A = \{a, 2a, \dots a \cdot (p-1)\}$

$A = a \cdot A$ because all elements of A are distinct :

$$\left(\begin{array}{l} a x_i \equiv a x_j \mod p \\ \Rightarrow \quad x_i = x_j \mod p \end{array} \right)$$

$$\Rightarrow \prod_{i=1}^{p-1} x_i = a \cdot \prod_{i=1}^{p-1} x_i \quad \Rightarrow \quad a^{p-1} \equiv 1 \mod p$$

Euler's theorem

$$a^{\varphi(m)} = 1 \mod m \qquad \text{if } (a, m) = 1$$

Proof as above with $A = \{x_1, x_2, \dots x_{\varphi(m)}\}$

a reduced residue system mod m

$(x_i, m) = 1 \quad (\text{all } i)$

$x_i \not\equiv x_j \mod m \quad (i \neq j)$

Every positive integer has a unique composition into prime factors

$$p_1^{\alpha_1} \mid \prod p_i^{\alpha_i} = p_1 \mid \prod q_j^{\beta_j} \Rightarrow p_1 = q_1, \alpha_1 = \beta_1 \quad p_i, q_j \text{ prime} \qquad p_1^{\alpha_1} \mid p_1^{\beta_1}$$

$$\Rightarrow p_i = q_i, \ \alpha_i = \beta_i$$

(a) $p_i = q_i$ (if correctly ordered)

because: $p_i \neq q_j$ (all j)

$$p \mid \prod q_j \Rightarrow p \mid q_{j_0} \text{ (at least one } q_{j_0}\text{)}$$

$$\Rightarrow p = q_{j_0}$$

(b) $p_1 \mid \prod q_j^{\beta_j} \Rightarrow p_1 = q_{j_0}$

$$\left.\begin{array}{l} a = n_a \cdot d \\ b = n_b \cdot d \end{array}\right\} \Rightarrow$$ ~~$d \in M$~~ any module containing a and b contains d

the smallest module as generated by the greatest c. d.

(1) $\boxed{\begin{array}{l}\text{Each module } M \text{ (of integers) looks like} \\ M = \{n \cdot d \mid n \in \mathbb{Z}\} \\ \text{with } d = \text{smallest integer in } M\end{array}}$

Because: Assume $x \in M$ with

$$n \cdot d < x < (n+1) \cdot d$$

$$\Rightarrow \quad 0 < y = x - n \cdot d < d$$

$$y \text{ integer}, \quad y < d \quad ↯$$

(2a) $\boxed{M = \{ax + by \mid x, y \in \mathbb{Z}\} = \{n \cdot d \mid n \in \mathbb{Z}\}}$ $d = (a,b)$

(2b) The equation

$$ax + by = c$$

has integer solutions ~~only~~ iff

$(a, b) \mid c$

$M = \{ax + by \mid x, y \in \mathbb{Z}\}$ is a module

$\Rightarrow \quad M = \{n \cdot d \mid n \in \mathbb{Z}\}, \; \cancel{A} \; d = (a, b)$

$\Rightarrow \quad c = d \cdot n \qquad d \mid c \qquad (a,b) \mid c$

$A \Rightarrow B$

M module $\Rightarrow$ ~~$M = \{n \cdot d \mid \ldots\}$~~

$\exists \, d \in M_+ :$

Proof:

$\cancel{\neg B} \Rightarrow$

$\forall x \in M_+ : d \leq x$

$\wedge \; M = \{n \cdot d \mid \ldots\}$

~~A~~ $A_1 \wedge A_2$

$\left. \begin{array}{l} M \text{ module } \wedge \\ d = \min \{x \in M \mid x > 0\} \end{array} \right\}$

$\Rightarrow \boxed{M = \{n \cdot d \mid \ldots\}} \; B$

$\neg B \Rightarrow \neg A = \neg A_1 \vee \neg A_2$

$A_1 \Rightarrow \neg A_2$

(4) If $c|(ab)$ and $(c,a)=1$ then $c|b$

$$\boxed{\left.\begin{array}{l} c\,|\,a\cdot b \\ (c,a)=1 \end{array}\right\} \Rightarrow c\,|\,b}$$

Euler's lemma

$$\boxed{\begin{array}{l} c|a\cdot b \quad \text{then} \\ c|a \ \text{or}\ c|b \end{array}}$$

$$\left.\begin{array}{l} ax+by=1 \\ (a,c)=1 \end{array}\right\} \Rightarrow b = b(ax+cy)$$

$$= abx + c\cdot by$$

$$= \Big(\underbrace{\frac{ab}{c}x + by}_{\text{integer}}\Big)\cdot c$$

$$\cancel{ax+by = n\cdot d}$$

$$\cancel{\Rightarrow d|}$$

$$\cancel{a = n_1\cdot d}$$

$$\cancel{b = n_2\cdot d}$$

5 Congruences

$$a \equiv 0 \mod m \iff m \mid a$$

$$\left.\begin{array}{l} a \equiv b \mod m \\ c \equiv d \mod m \end{array}\right\} \Rightarrow \begin{array}{l} a \pm c \equiv b \pm d \mod m \\ a \cdot c \equiv b \cdot d \mod m \end{array}$$

$$ac = bc \mod m \Rightarrow a \equiv b \mod \frac{m}{(c,m)}$$

$$a = b \mod m \quad \text{if } (c,m) = 1$$

$b = 0$!

$a \equiv 0 \mod b$

because: $(d = (c,m))$

$$m \mid (a-b) \cdot c$$

$$\Rightarrow \left.\begin{array}{l} \frac{m}{d} \mid (a-b) \cdot \frac{c}{d} \\ \left(\frac{m}{d}, \frac{c}{d}\right) = 1 \end{array}\right\} \Rightarrow \frac{m}{d} \mid a-b$$

$$\Rightarrow a - b \equiv 0 \mod \frac{m}{d}$$

$a \cdot b = 0 \ \cancel{\equiv} \mod \cancel{b}\, m$

$\iff m \mid a \cdot b$

$\Rightarrow a = 0 \mod m$ or

$b = 0 \mod m$

⑥ Linear congruences

$ax \equiv b \mod m$

$\Leftrightarrow \cancel{(ax-b)/a}$

$\Leftrightarrow m \mid (ax-b)$

$\Leftrightarrow \cancel{(a/x - b)/a}$

$m \cdot y = ax - b$

$ax - m \cdot y = b$

solvable iff $\underbrace{(a,m)}_{=d} \mid b$

$\frac{a}{d} \cdot x \equiv \frac{b}{d} \mod \frac{m}{d}$

$ax \equiv b \mod m$

with $(a,m) = 1$

$\Rightarrow \mathbb{Z}_p$ is a field (unique inverse)

$(a,m) = 1$

$ax \equiv b \mod m$ has exactly one solution

because: let $x_i = 0, 1, \dots m-1$

$y \equiv ax \mod m$

$ax_i \equiv ax_j \mod m$

$\Rightarrow a(x_i - x_j) \equiv 0 \mod m$

$\Rightarrow m \mid a(x_i - x_j)$

$\cancel{a(x_i - x_j) = k \cdot m}$

$\Rightarrow m \mid x_i - x_j \quad , \quad x_i, x_j < m$

$\Rightarrow x_i = x_j$

$a \neq 0 \mod m$

$\Rightarrow x_i - x_j = 0 \mod m$

$\{ak \mid k = 0 .. m-1\} =$

$\{k \mid k = 0 - m-1\}$

Euclid's algorithm

$d = (a, b)$

$M = \{ n \cdot d \mid n \in \mathbb{Z} \}$ = smallest module containing a and b

$= \{ ax + by \mid x, y \in \mathbb{Z} \}$

$r_0 = a, \quad r_1 = b \in M$

$r_2 \equiv r_0 \mod r_1$

$\vdots$

$r_{n-1} \equiv r_{n-3} \mod r_{n-2}$

$0 = r_n \equiv r_{n-2} \mod r_{n-1}$

$r_i \in M \Rightarrow d \mid r_i \Rightarrow d \leq r_i$

$$\left.\begin{array}{l} r_{n-1} \mid r_{n-2} \\ \vdots \\ r_{n-1} \mid b \\ r_{n-1} \mid a \end{array}\right\} \Rightarrow d \leq r_{n-1}$$

$\Rightarrow d = r_{n-1}$

Extended Euclid

① $(a, m) = 1$ then:

$$ax + my = 1 \quad \text{is solvable}$$

$$\Leftrightarrow \quad ax \equiv 1 \bmod m \quad \text{is solvable}$$

② $\left.\begin{array}{l} a \cdot b \equiv 0 \bmod m \\ (a, m) = (b, m) = 1 \end{array}\right\} \Rightarrow$

$a \equiv 0 \bmod m$ or

$b \equiv 0 \bmod m$

$$r_n = a s_n + b t_n = 1$$

$$a \cdot s_n \equiv 1 \bmod b$$

$r_0 = a, \quad r_1 = b$

$s_0 = 1, \quad s_1 = 0$

$t_0 = 0, \quad t_1 = 1$

$r_{i+1} = r_{i-1} - q_i r_i$

$s_{i+1} = s_{i-1} - q_i s_i$

$t_{i+1} = t_{i-1} - q_i t_i$

$r_{n+1} = 0; \quad \boxed{d = r_n} = (a, b)$

$r_0 = a s_0 + b t_0$

$r_1 = a s_1 + b t_1$

$$\begin{aligned} r_{k+1} &= r_{k-1} - q_k r_k \\ &= (a \cdot s_{k-1} + b\, t_{k-1}) - q_k (a s_k + b\, t_k) \\ &= a\,(s_{k-1} - q_k s_k) + b\,(t_{k-1} + q_k t_k) \\ &= a \cdot s_{k+1} + b \cdot t_{k+1} \end{aligned}$$

$r_2 = r_0 - q_1 r_1$

$r_{i+1} = r_{i-1} - q_i r_i$

$s_0 = 1, \quad s_1 = 0$

$t_0 = 0, \quad t_1 = 1$

$r_0 = a$

$r_1 = b$

$r_{n+1} = 0$

$r_m = a \cdot s_m + b \cdot t_m$

$= r_0 s_m + r_1 \cdot t_m$

$r_0 = a \cdot s_0^{=1} + b \cdot t_0^{=0}$

$r_1 = a \cdot s_1^{=0} + b\, t_1^{=1}$

$r_{k-1} = a \cdot s_{k-1} + b \cdot t_{k-1}$

$r_k = a \cdot s_k + b \cdot t_k$

$r_{k+1} = r_{k-1} - q_k \cdot r_k$

$= a \cdot s_{k-1} + b \cdot t_{k-1}$

$- q_k (a\, s_k + b \cdot t_k)$

$= a \cdot (\underbrace{s_{k-1} - q_k \cdot s_k}_{= s_{k+1}}) + b(\underbrace{t_{k-1} - q_k \cdot t_k}_{= t_{k+1}})$

$= a \cdot$

For each module M :

$M = \{ n \cdot d \mid n \in \mathbb{Z} \}$

d = smallest integer of d

$0 < y = x - nd < (n+1) \cdot d - nd = d$

$d \in M$ smallest integer

$x \in M$ not ~~at~~ a multiple of d

$n \cdot d < x < (n+1) \cdot d$

$$\left.\begin{aligned} \Rightarrow \quad x - d - d \cdot \ldots - d &= x - n \cdot d \in M \\ &= y < d \\ 0 < x - nd = y &\in M \end{aligned}\right\} \lightning$$

Every integer module is generated by its smallest element

gcd : ~~...~~ what is the smallest model containing a and b ?

$d = gcd(a, b)$ $\qquad a > b$

$a = a_1 \cdot d \qquad a - q \cdot b = r \qquad r \in M$

$b = b_1 \cdot d \qquad a = b \cdot q + r \qquad 0 \leq r < b$

$r = 0 \Rightarrow a = b \cdot q ; \quad b = gcd(a, b)$

Module M :

if $x, y \in M$ then $x - y \in M$, $x + y \in M$

closed under (addition and) subtraction redundant

$0 \in M$ (always)

$y \in M \Rightarrow 0 - y = -y \in M$

$x, y \in M \Rightarrow x, -y \in M \Rightarrow x - (-y) = x + y \in M$

$\alpha \in M \Rightarrow n \cdot \alpha$ (all $n \in \mathbb{N}$)

all elements of M are multiples of an integer d,

the smallest positive integer of M

Ganzzahlige Division und Rest

(1) $a, b \in \mathbb{N} : \exists_1 m, r \in \mathbb{N}_0 :$

$a = m \cdot b + r \; , \quad r < b$ $\qquad a \equiv r \mod b$

Damit ist

$r = a - m \cdot b$

Beweis : $m := \max \{ k \in \mathbb{N}_0 \mid k \cdot b \leq a \} = \max \{ k \in \mathbb{N}_0 \mid k \leq \frac{a}{b} \}$

Die Menge $\{ .. \}$ ist beschränkt und nicht-leer,

hat also ein Maximum. ~~Angenommen~~ wäre

$r = a - m \cdot b \geq b,$

$\Rightarrow a \geq b(m+1)$ ↯

$2 \mid 10 \Rightarrow 2 \cdot 9 = 10$

② Dies funktioniert auch für $a, b \in \mathbb{Z}$, $b \neq 0$:

$$m = \max \{ k \in \mathbb{Z} \mid k \leq \tfrac{a}{b} \} = \begin{cases} \max \{ k \in \mathbb{Z} \mid k \cdot b \leq a \} & b > 0 \\ \max \{ k \in \mathbb{Z} \mid k \cdot b \geq a \} & b < 0 \end{cases}$$

$r = a - m \cdot b$.

Man definiert: $m = a // b$, $r = a \% b$.

Beachte: Man kann immer mit -1 durchmultiplizieren; wegen:

$$\max \{ k \in \mathbb{Z} \mid k \leq \tfrac{a}{b} \} = \max \{ k \in \mathbb{Z} \mid k \leq \tfrac{-a}{-b} \}$$

Beispiel:

$10 // 7 = 1$ $\qquad$ $10 \% 7 = 3$

$-10 // 7 = -2$ $\qquad$ $-10 \% 7 = 4$

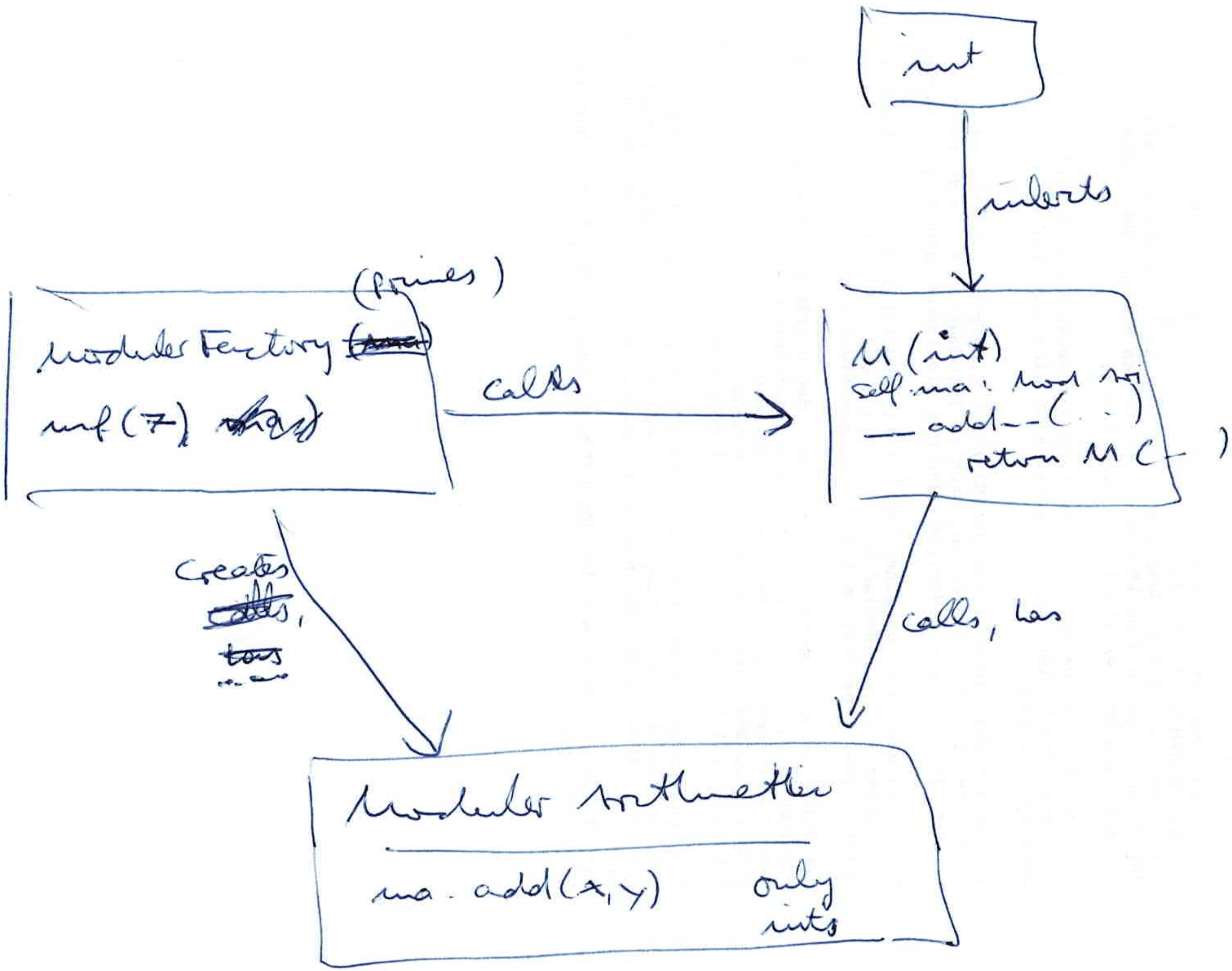
$10 // -7 = -2$ $\qquad$ $10 \% -7 = -4$

$-10 // -7 = 1$ $\qquad$ $-10 \% -7 = -3$

Der Rest hat das Vorzeichen des Nenners b, denn:

$b > 0$: $m \cdot b \leq a \Rightarrow r = a - m \cdot b \geq 0$

$b < 0$: $m \cdot b \geq a \Rightarrow r = a - m \cdot b \leq 0$


int
inherits
ModularFactory
(primes)
mf(7)
calls
M(int)
__add__(...)
return M(...)
creates
calls, has
Modular Arithmetic
ma.add(x,y)
only ints