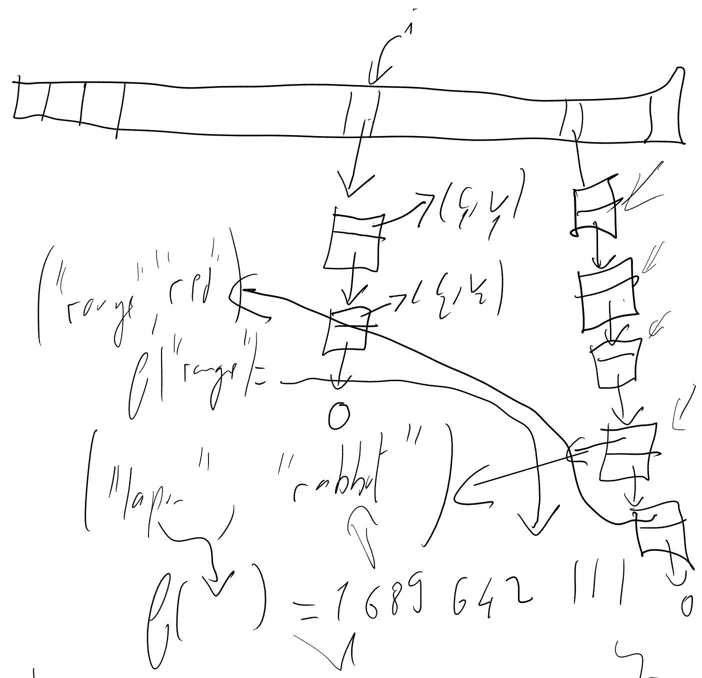
1

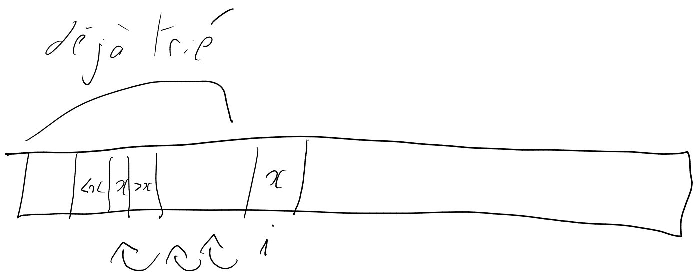
for l in data — $O(n)$

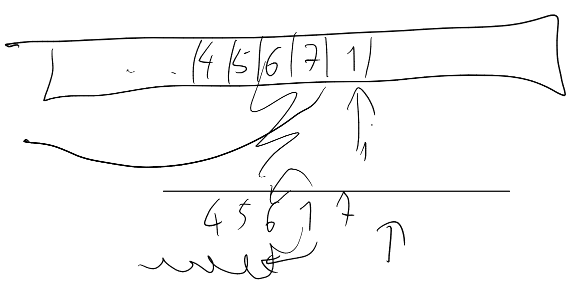
$h(l) = 1$

range − l ∈ tb ? — $O(1)$



+ * # ⊕





$$S = 1 + 2 + 3 + \dots + (n-1)$$

$$S = (n-1) + (n-2) + \dots + 1$$

$$2S = n + n + \dots + n$$

$$S = \frac{(n-1)n}{2}$$

$$1 + \dots + n = \frac{n(n+1)}{2}$$

$$T(n) = M \cdot \frac{(n-1)n}{2} = O(n^2).$$

$$\frac{2^n}{2^1} = \frac{\cancel{2} \times 2 \times \dots \times 2}{\cancel{2} \times 1}$$

$$= \underbrace{2 \times \dots \times 2}_{n-1}$$

$$= 2^{n-1}$$

$$O(2^{n-1}) + 2T(2^{n-1})$$

$$= n\,O(2^n) = O(n2^n)$$

$$T(2^n) = O(n2^n) \qquad n = \log_2(n)$$

$$T(n) = O(n \log(n))$$

2

~~7~~	~~8~~	10

~~6~~	11	13

$7 > 6$, $7 < 11$, $8 < 11$

6	7	8			

$O(n)$

⚠ corriger $O(n) \to O(2^n)$

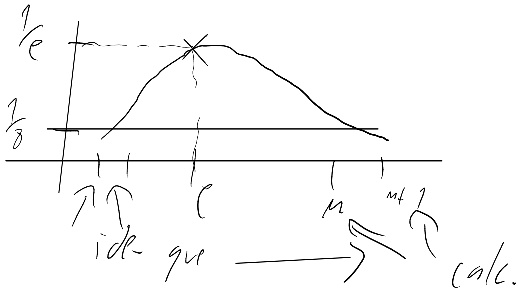
$8n^2$	i
$64 n \ln(n)$	f

$\frac{1}{8} < f(n)$

$8n^2 < 64 n \ln(n) \iff \frac{1}{8} < \frac{\ln(n)}{n}$

$f : x \mapsto \frac{\ln(x)}{x}$

$f'(x) = \frac{1}{x^2}\left(1 - \ln(x)\right) \leq 0 \; \forall x \geq e$

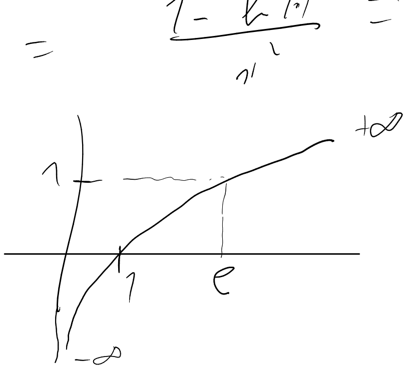


$f(e) = \frac{1}{e} \simeq \frac{1}{2,7}$

$$\left(\frac{\ln(x)}{x}\right)' = \frac{(\ln(x))' \times x - (\ln(x)) \times (x)'}{x^2}$$

$$= \frac{\frac{1}{x} \times x - \ln(x) \times 1}{x^2}$$

$$= \frac{1 - \ln(x)}{x^2} = f'(x)$$



$f'(x) \geq 0 \iff \frac{1 - \ln(x)}{x^2} \geq 0$

$\iff 1 - \ln(x) \geq 0$

$\iff 1 \geq \ln(x) \iff e \geq x$

$\ln(e)$

x	0		e	
$f'(x)$	‖	+	0	−
$f(x)$	‖	↗		↘

$$T(2^n) = O(1)$$

$$+ 2 \times T\left(\frac{2^n}{2}\right)$$

$$+ O(2^n)$$

$$= O(2^n) + 2 \times T(2^{n-1})$$

$$= O(2^n) + 2 \times \left(O(2^{n-1}) + 2T(2^{n-2}) \right)$$

$$= \dots = n\, O(2^n) + O(2^n)$$

$$= O(n 2^n)$$

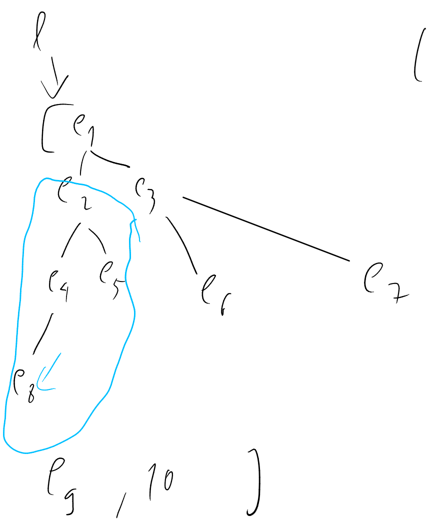
$$x = 2^n \iff n = \underbrace{\log_2(x)}_{\in \mathbb{N}}$$

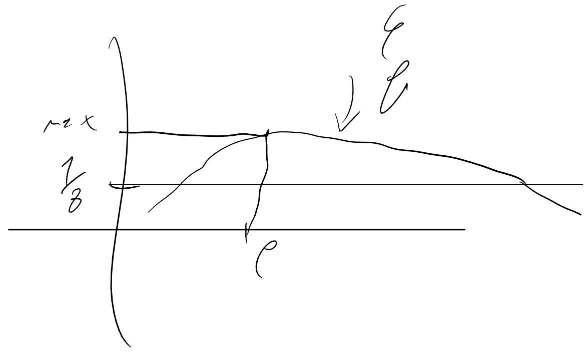
$$T(x) = T(2^n) = O(n 2^n)$$

$$= O(\log_2(x) \times x)$$

$$T(x) = O(x \log_2(x))$$

$$\left(l,\ \underset{8}{\underset{\parallel}{\text{taille}}},\ \underset{1}{\underset{\uparrow}{2}} \right)$$





n tq $e(n) \geq \frac{7}{8}$

$[\![a ; b]\!]$

$\uparrow \quad \uparrow$

$? \quad ?$

$[\![1 ; 26]\!]$

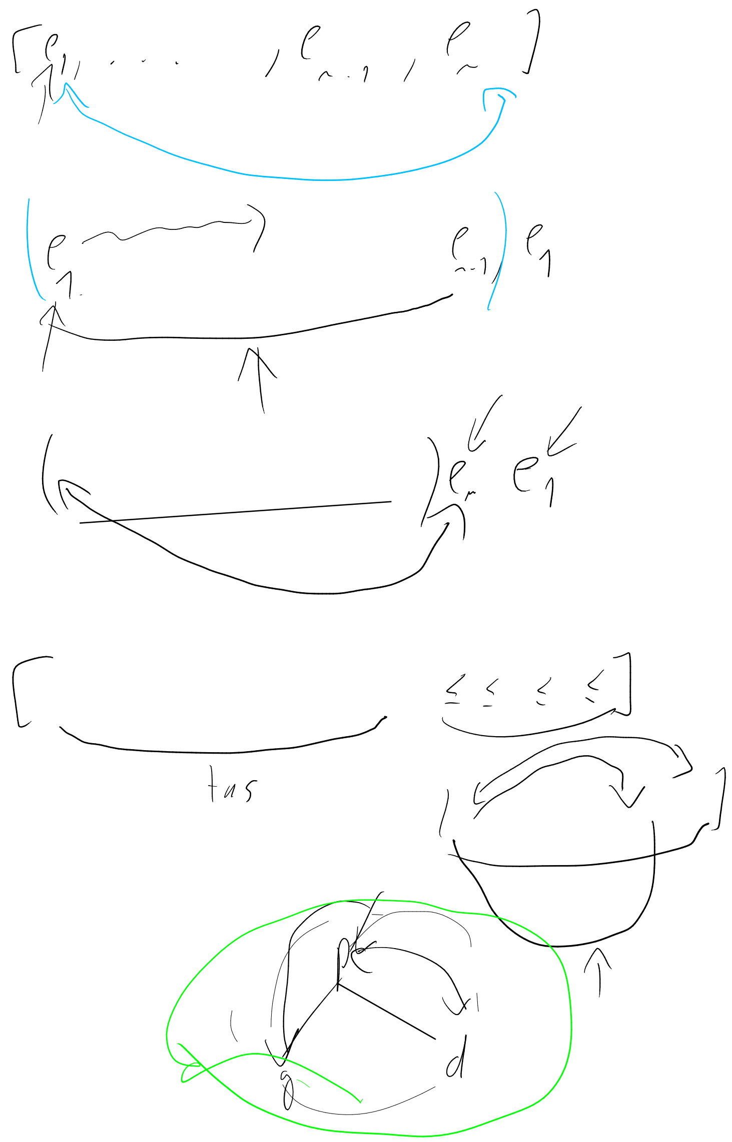
7	6	8	7	1	3

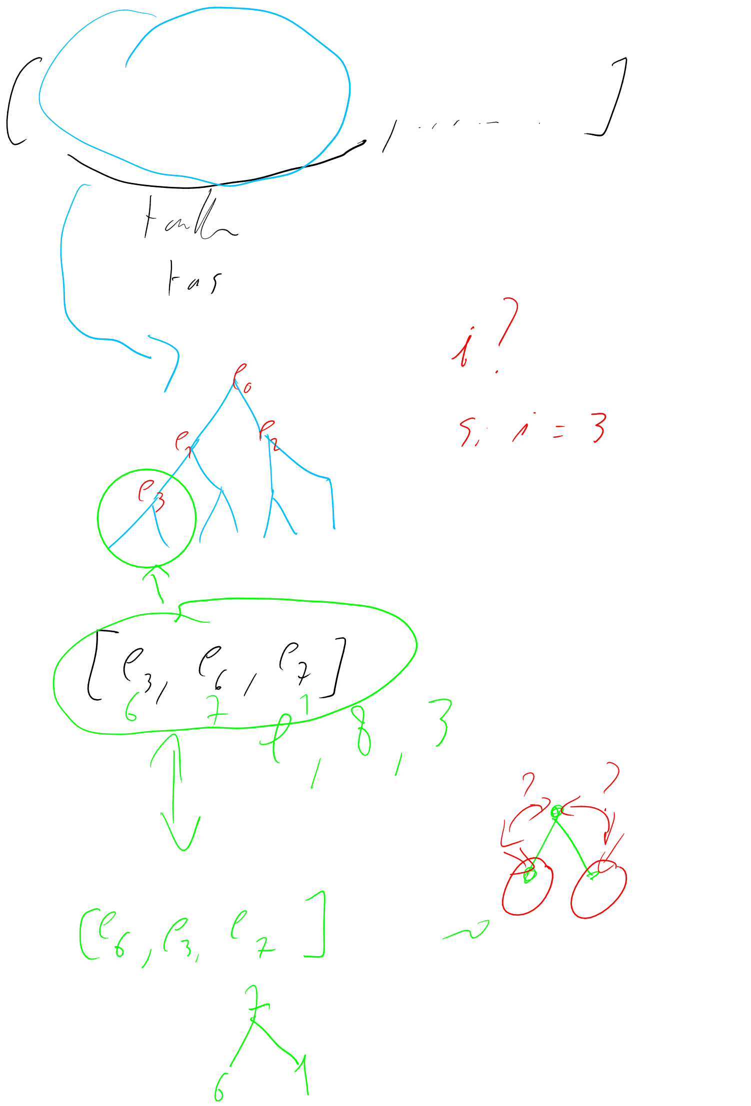
1 7 6 8 7 3

$$n + (n-1) + (n-2) + \dots + 1$$

$$= \frac{n(n+1)}{2} = O(n^2).$$

$$n^2 = n \times n = (n \ln(n)) \times \frac{n}{\ln(n)}$$





$O(\sqrt{n})$

$n \quad 2^n$

$T(n) = O(\sqrt{2^n}) = O((\sqrt{2})^n)$

5

("aa" * "bb") * "cc" = "aabb" * "cc" = "aabbcc"

"aa" * ("bb" * "cc") = "aa" * "bbcc"

= "aabbcc"

"aa"$^{-1}$? dans "aa" * x = ""

ds $(\mathbb{Z}, +)$, $3^{-1} = -3$ ⚠

$(G, \circ)$ $\quad M = \begin{pmatrix} a \\ b \end{pmatrix}$

$s_x \circ s_y (M) = s_x(s_y(M))$

$= s_x\left(\begin{pmatrix} -a \\ b \end{pmatrix}\right)$

$= \begin{pmatrix} -a \\ -b \end{pmatrix} = s_O(M)$

$\forall M \in P,\ s_x \circ s_y (M) = s_O(M)$

$$\boxed{s_x \circ s_y = s_O}$$

$s_x \circ s_y (M) = s_O(M)$

s_O

$\forall f, g, h \in G,\ (f \circ g) \circ h = f \circ (g \circ h)$

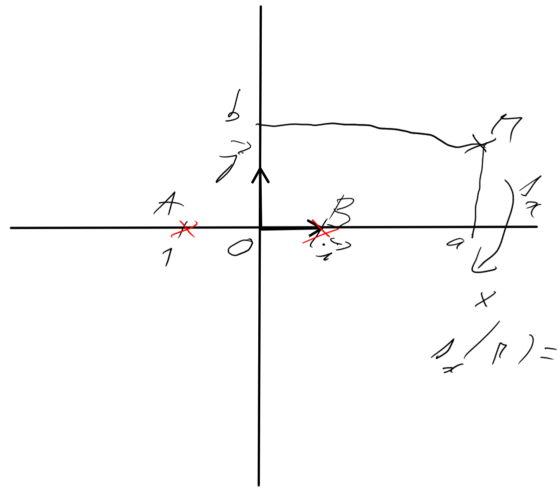
Soit $f, g, h \in G$.

Soit $M \in P$

$[(f \circ g) \circ h](M) = (f \circ g)(h(M))$

$= f(g(h(M)))$

=



$s_x(M) = \begin{pmatrix} a \\ -b \end{pmatrix}$

$(f \circ g)(M) \stackrel{\text{def}}{=} f(g(M))$

$(f \circ (g \circ h))(M)$

$= f((g \circ h)(M))$

$= f(g(h(M)))$

∃ neutru ?

Fie $f \in G$ și $n \in D$

$(f \circ id)(n) = f(id(n))$

$= f(n)$

$f \circ id = f$

$(id \circ f)(n) = id(f(n))$

$= f(n)$

$id \circ f = f = f \circ id$

$id^{-1} = id$

$id \circ id = id$

$s_0^{-1} = s_0$

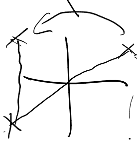
$s_0 \circ s_0 = id$

$s_x^{-1} = s_x$

$s_x \circ s_x = id = s_x \circ s_x$

Dc s_y alt s_y ... $\circ$.

și $s_y^{-1} = s_y$



! $f \circ id = f = id \circ f$

d

g:

$\circ$	id	s_x	s_y	s_0
id	id	s_x	s_y	s_0
s_x	s_x	id	s_0	s_y
s_y	s_y	s_0	id	s_x
s_0	s_0	s_y	s_x	id

$E = \{a, b, c, d\}$

$E \times E = \{(a,a), (a,b), \dots, (b,c), \dots\}$

$E \times E \setminus \{ \binom{x}{y} \in E \times E \mid x = y \}$

$s_x \circ s_0 \binom{a}{b} = s_x\left(s_0 \binom{a}{b}\right)$

$s_x \circ s_0 = (s_x \circ s_x) \circ s_y = id \circ s_y$

$= s_y$

$s_x s_y s_x =$

$j = e^{\frac{2i\pi}{3}}$

$A, B = \{-1; 1\}$

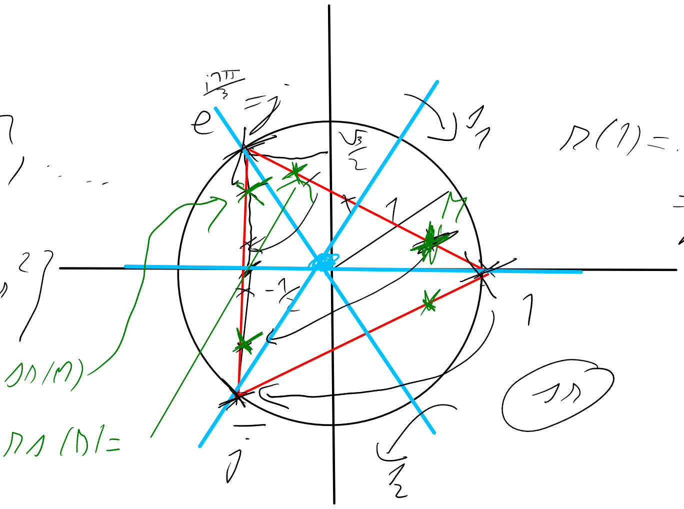
$D_3 = \{ id, \Delta_x, \Delta_1, \Delta_2, r, \dots$

$D_3 = \{ id, \Delta, r, r^2, \Delta r, \Delta r^2 \}$

$r = \mathrm{rot}_{O, \frac{2\pi}{3}}$

$r \circ r \circ r = id$

$r^3 = id$



$r(1) = e^{\frac{2i\pi}{3}} \cdot 1 = j$

$(-1)^2 = 1$

$1^2 = 1$

$z^3 = 1$

$z^n = 1$

$e^{\frac{2ik\pi}{n}}$, $k = 0, \dots, n-1$

$e^{\frac{2i \times 0 \times \pi}{3}} = 1$, $e^{\frac{2i\pi}{3}} = \cos\left(\frac{2\pi}{3}\right) + i \sin\left(\frac{2\pi}{3}\right)$

$e^{\frac{4i\pi}{3}} = \bar{j}$

$\left(e^{\frac{2ik\pi}{n}}\right)^n = e^{\frac{2ik\pi}{n} \times n} = e^{2ik\pi} = \dots$

$e^{i\alpha} = \cos(\alpha) + i \sin(\alpha)$

$n\mathbb{Z} = \{ \dots, -3n, -2n, -n, 0, n, 2n, 3n, \dots \}$

$7\mathbb{Z} = \{ 7 \times a, a \in \mathbb{Z} \}$

$= \{ \dots, -21, -14, -7, 0, 7, 14, 21, 28, \dots \}$

Mq $(n\mathbb{Z}, +)$ gp :

* Soit $a, b \in \mathbb{Z}$.

$na + nb \in n\mathbb{Z}$

$n(a+b) \in n\mathbb{Z}$

$+$ LCI sur $n\mathbb{Z}$.

* $na + n \times 0 = na$

$\dots$

* $na + n \times (-a) = \dots$

ok.

$\times$ dist sur $+$

$na \times nb = nab \times n \in n\mathbb{Z}$.

$(A, *, \divideontimes)$

$U = \{ x \in A \mid (\exists y \in A \mid x \divideontimes y = y \divideontimes x = 1_A) \}$

Mq : $(U, \divideontimes)$ gp. $\longleftarrow$ Dc $1_A \in U$.

$\forall u \in U,\ 1_A \divideontimes u = u \divideontimes 1_A = u$

$1_A \divideontimes 1_A = 1_A$ Dc 1_A inv et $1_A^{-1} = 1_A$

$u \in U$ Dc : $\exists v \in A \mid u \divideontimes v = v \divideontimes u = 1_A$

$v \in U$

$\divideontimes$ assoc.

Mq : $(U, \divideontimes)$ gpe.

Soit $a, b, c \in U$ $(a, b, c \in A)$

$(a \divideontimes b) \divideontimes c = a \divideontimes (b \divideontimes c)$ car $\divideontimes$ assoc ds A.

Mq : $1_A \in U$

On cherche $x \in U$ tq $1_A \divideontimes x = x \divideontimes 1_A = x$

pour $x = 1_A$ c'est vrai.

$a \divideontimes 1_A = 1_A \divideontimes a = a$ 1_A neutre pr $(U, \divideontimes)$

$\underset{\in U \subset A}{a}$

Mq : $\exists d \in U$ tq $a \divideontimes d = d \divideontimes a = 1_A$.

$a \in U$ Dc : $\exists a^{-1} \in A$ tq $a \divideontimes a^{-1} = a^{-1} \divideontimes a = 1_A$

et $a^{-1} \in U$ car a est sym de a^{-1} / $\divideontimes$

$\bar{4} = \{4+7a, a \in \mathbb{Z}\}$ $\bar{a}$

$11 \in \bar{7}$ $\quad \overline{11} = \{11+7a, a \in \mathbb{Z}\}$

$\overline{11} = \bar{4}$ dans $\mathbb{Z}/7\mathbb{Z}$

$$\frac{\mathbb{Z}}{n\mathbb{Z}} = \underbrace{\{\underbrace{a+n\mathbb{Z}}_{\text{ss-e de } \mathbb{Z}}, a \in \mathbb{Z}\}}_{\text{ens de ss-ens de } \mathbb{Z}}$$

$11+7a = 4+7+7a$
$= 4+7(a+1)$
$\in 4+7\mathbb{Z}$

$a+n\mathbb{Z} = \{\dots, a-2n, a-n, a, a+n, a+2n, \dots\}$

$$\frac{\mathbb{Z}}{7\mathbb{Z}} = \{-3+7\mathbb{Z}, -2+7\mathbb{Z}, -1+7\mathbb{Z}, 0+7\mathbb{Z}, 1+7\mathbb{Z}, 2+7\mathbb{Z}, \dots, 5+7\mathbb{Z}, 6+7\mathbb{Z}, 7+7\mathbb{Z}, \dots\}$$

$= \bar{7}$

$(A, +, \times)$ $\quad I$

$a \times I = \{a \times i, i \in I\}$ ss-ens de A

$\frac{A}{I} = \{a \times I, a \in A\}$ ens de ss-ens de A.

$(\mathbb{Z}, +, \times)$ $\quad n\mathbb{Z} = \{-2n, -n, 0, n, 2n, \dots\}$

$a \in \mathbb{Z}$

$a+n\mathbb{Z} = \{a+nk, k \in \mathbb{Z}\}$ ss-ens de $\mathbb{Z}$

$$\frac{\mathbb{Z}}{n\mathbb{Z}} = \{\bar{0}, \bar{1}, \dots, \overline{n-1}\}.$$

$a+n\mathbb{Z} = a'+n\mathbb{Z}$

$b+n\mathbb{Z} = b'+n\mathbb{Z}$

$\implies$ $(a+b)+n\mathbb{Z} = (a'+b')+n\mathbb{Z}$

$a \times b + n\mathbb{Z} = a'b' + n\mathbb{Z}$

$\frac{\mathbb{Z}}{n\mathbb{Z}}$ $\quad \bar{a}+\bar{b} = \overline{a+b} \overset{?}{=} \overline{a'+b}$

$\bar{a} = \bar{a'}$

$\overline{17 \times 9} = \overline{7 \times 9}$

$\frac{\mathbb{Z}}{10\mathbb{Z}}$ $\quad \bar{7} = \overline{17}$

$\varphi_D : \frac{\mathbb{Z}}{10\mathbb{Z}} \to \frac{\mathbb{Z}}{10\mathbb{Z}}$

$\overline{x} \mapsto \overline{x-4}$

$\varphi_C : \frac{\mathbb{Z}}{10\mathbb{Z}} \to \frac{\mathbb{Z}}{10\mathbb{Z}}$

$\overline{x} \mapsto \overline{x+4}$

$\left(\mathfrak{Bij}\left(\frac{\mathbb{Z}}{10\mathbb{Z}}\right), \circ\right)$

$\varphi_C = \varphi_D^{-1}$

$(\mathbb{Z}, +)$

H s-grp de $(\mathbb{Z}, +)$

$\exists n \in \mathbb{N} \mid H = n\mathbb{Z}$

Mq:

$n := \min(H \cap \mathbb{N}^*)$

$n \in H$

Mq: $H = n\mathbb{Z}$

Mq: $n\mathbb{Z} \subset H$

Soit $a \in n\mathbb{Z}$.

$\exists b \in \mathbb{Z} \mid a = nb$

Si $b > 0$: $a = \underbrace{(n + n + \dots + n)}_{b}$ $\in H$

Si $b < 0$: $a = (-n) + (-n) + \dots + (-n)$ $\in H$

Si $b = 0$; $a = 0 \in H$

$\boxed{n\mathbb{Z} \subset H}$

$A \subset B \overset{\text{déf}}{\iff} \forall a \in A, a \in B$

$A = B \iff (A \subset B \text{ et } B \subset A)$

$n\mathbb{Z} = \{\dots, -3n, -2n, -n, 0, n, 2n, \dots\}$,

$a = nx$

$\cap$

$n\mathbb{Z}$

Mq: $H \subset n\mathbb{Z}$

Soit $h \in H$.

$\exists (q, r) \in \mathbb{Z}^2$ tq:

$\begin{cases} h = q.n + r \\ 0 \leq r < n \end{cases}$

$n = h - \bar{9}m$ — $\in H$

$\in H$ $\quad$ $\in H$

$n \in H$

si $n \neq 0$, $n \in H \cap \mathbb{N}^*$

$n < m$

$m = \min(H \cap \mathbb{N}^*)$

impossible.

$n = 0$

$a\mathbb{Z} + b\mathbb{Z} = m\mathbb{Z}$

$m = au + bv.$

$n \in \mathbb{N}$

$n = a_n 10^n + a_{n-1} 10^{n-1} + \dots + a_2 10^2 + a_1 \times 10 + a_0$

$a_i \in \{0; 1, \dots, 9\}.$

$63\,742$

$= 6 \times 10^5 + 3 \times 10^4 + \dots + 2 \times 10^0$

$a_5 \quad a_0$

$a_5 + a_4 + \dots + a_0$

ds $\mathbb{Z}/9\mathbb{Z}$, $\bar{n} = \bar{0}$

Pg: $9 \mid n \iff 9 \mid \underbrace{\sum_{i=0}^{n} a_i}_{a_0 + a_1 + a_2 + \dots + a_n}$

$9 \mid n = \sum_{i=0}^{n} a_i 10^i \iff$ dans $\mathbb{Z}/9\mathbb{Z}$: $\overline{\sum_{i=0}^{n} a_i 10^i} = \bar{0}$

$\iff$ " " , $\sum_{i=0}^{n} \bar{a_i}\, \overline{10}^i = \bar{0}$ $\qquad 0 + 9 \times u$

$\iff$ " " , $\sum \bar{a_i} \times \cancel{\bar{1}} = \bar{0}$

$\iff 9 \mid \sum a_i$

$\overline{10} = \overline{1 \times 9 + 1}$

$= \bar{1}$

$\sum a_i n_i + \sum a_i n_i' = \sum a_i (n_i + n_i') \in \sum a_i \mathbb{Z}$

$\sum a_i \mathbb{Z}$ $+$ stable.

$\sum a_i n_i + 0 = \circlearrowleft_+ = \sum a_i n_i$

$+$ assoc.

$\sum a_i n_i + \underbrace{\left(-\sum a_i n_i\right)}_{? \in \sum a_i \mathbb{Z}?} = 0$ ok

$-\sum a_i n_i = \sum a_i (-n_i)$

$\in \sum a_i \mathbb{Z}$.

$\sum a_i \mathbb{Z}$ ss-gpe de $(\mathbb{Z}, +)$ donc: $\exists\, d \in \mathbb{N}$ tq $\boxed{\sum a_i \mathbb{Z} = d\mathbb{Z}}$

$a_{i_0} = a_1 \times 0 + a_2 \times 0 + \dots + a_{i_0-1} \times 0 + a_{i_0} \times 1 + a_{i_0+1} \times 0 + \dots \in \underbrace{\sum a_i \mathbb{Z}}_{d\mathbb{Z}}$

$a_{i_0} \in d\mathbb{Z}$

$\exists\, n \in \mathbb{Z} \mid a_{i_0} = dn$

$\forall i \in n, \; d \mid a_i$.

Soit $d' \in \bigcap_{i \in [\![1,n]\!]} \mathcal{D}(a_i)$

$\forall i, \; d' \mid a_i$

Donc: $\forall i \in [\![1,n]\!], \exists\, u_i \in \mathbb{Z} \mid a_i = d' \times u_i$

$d\mathbb{Z} = \sum_{i=1}^{n} a_i \mathbb{Z}$

$d\mathbb{Z} = \{\dots, -6d, -5d, \dots\}$

$d = d \times 1 \in d\mathbb{Z} = \sum_{i=1}^{n} a_i \mathbb{Z}$

$\frac{a}{b}$ $\quad bx ? = a$

$d \in \sum_{i=1}^{n} a_i \mathbb{Z}$

$\exists\, v_1, \dots, v_n \in \mathbb{Z} \mid d = \sum_{i=1}^{n} a_i v_i$

$d = \sum_{i=1}^{n} d' \times u_i \times v_i = d' \times \left(\sum_{i=1}^{n} u_i v_i\right)$

$d' \mid d$.

$d = d \times 1 \in d\mathbb{Z} = \sum a_i \mathbb{Z}$

$pgcd(a_1, \dots, a_n) \in \sum a_i \mathbb{Z}$

$\exists\, u_1, \dots, u_n \in \mathbb{Z} \mid pgcd(a_1 \dots) = \sum a_i u_i$

$A \subset B \overset{def}{\iff} (\forall a \in A,\ a \in B)$

$A = B \iff \begin{cases} A \subset B \\ B \subset A \end{cases}$

$(a, b) \in \mathbb{Z}^2 \mid |a| > |b|$

$D(x) = \{ u \in \mathbb{Z} \mid u \mid x \}$

$\begin{cases} a = q_0 b + r_0 \\ 0 \leq r_0 < b \end{cases}$

Pq: $D(a) \cap D(b) = D(b) \cap D(r_0)$

Pq: $D(a) \cap D(b) \subset D(b) \cap D(r_0)$

Soit $x \in D(a) \cap D(b)$ Donc $x \in D(a)$ et $x \in D(b)$ ok

$x \mid a$ et $x \mid b$

$(\exists u \in \mathbb{Z} \mid a = x \times u)$ et $(\exists v \in \mathbb{Z} \mid b = x \times v)$

$r_0 = a - q_0 b$

$r_0 = xu - q_0 xv$

$= x \cdot (u - q_0 v)$

$x \mid r_0$

$x \in D(b) \cap D(r_0)$

Cqfd: $D(a) \cap D(b) \subset D(b) \cap D(r_0)$

idée au moins: $D(b) \cap D(r_0) \subset D(a) \cap D(b)$

$D(a) \cap D(b) = D(b) \cap D(r_0)$

idée: $\dots\dots = D(r_n) \cap D(r_{n+1})$

$\uparrow$
$= 0$

$a = q_0 b + r_0 \quad , \quad 0 \leq r_0 < b$ $\qquad D(a) \cap D(b) = D(b) \cap D(r_0)$

Si $r_0 \neq 0$: $b = q_1 r_0 + r_1 \qquad 0 \leq r_1 < r_0$ $\qquad D(b) \cap D(r_0) = D(r_0) \cap D(r_1)$

Si $r_1 \neq 0$ $\quad r_0 = q_2 r_1 + r_2$ $\qquad D(r_0) \cap D(r_1) = D(r_1) \cap D(r_2)$

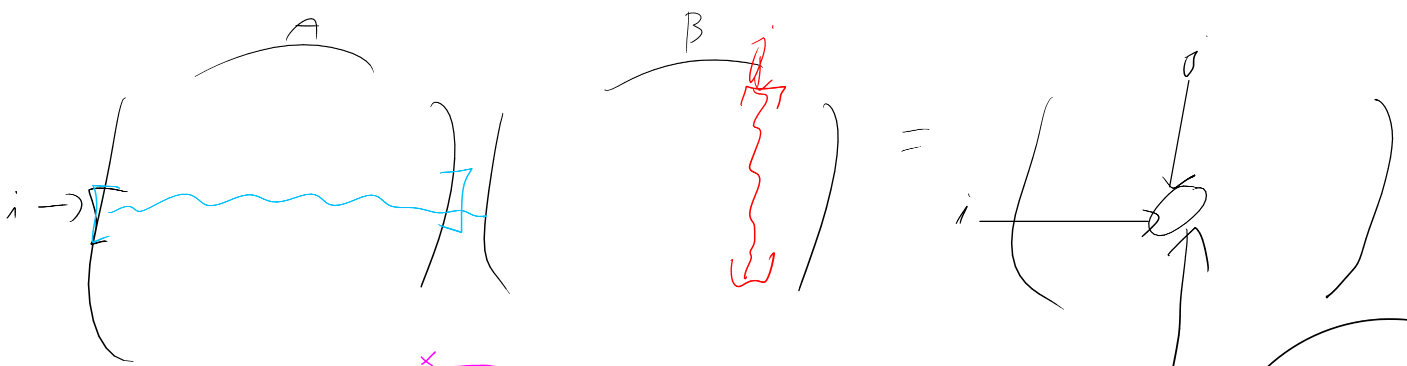
Si $r_{n+1} \neq 0$ $\quad r_n = q_{n+2} r_{n+1} + \underbrace{r_{n+2}}_{=0} \quad , \quad 0 \leq r_{n+2} < r_{n+1}$

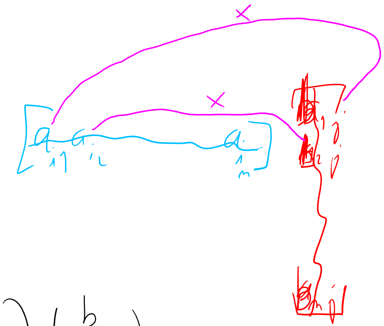
$D(a) \cap D(b) = D(b) \cap D(r_0) = D(r_0) \cap D(r_1) = \dots = D(r_{n+1}) \cap D(\underbrace{r_{n+2}}_{=0})$

$= D(r_{n+1}) \cap \mathbb{Z}$

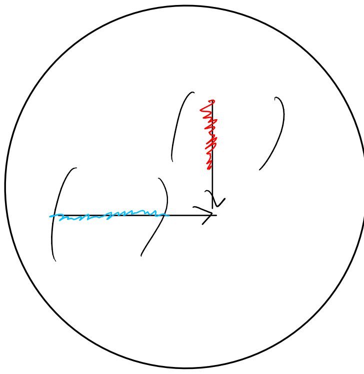
$D(a) \cap D(b) = D(r_{n+1})$

$AB = C$





$$= \sum_{k=1}^{m} a_{ik} b_{kj}$$



$$\begin{pmatrix} a_n \\ b \end{pmatrix} = \begin{pmatrix} ? \end{pmatrix} \begin{pmatrix} b \\ n_0 \end{pmatrix}$$

$$C_{ij} = \sum_{k=1}^{m} a_{ik} b_{kj}$$

$$? \begin{pmatrix} q_0 & 1 \\ \cancel{0} & \cancel{1} \end{pmatrix} \begin{pmatrix} b \\ n_0 \end{pmatrix} = \begin{pmatrix} \\ 0 \times b + 1 \times n_0 \end{pmatrix} = \begin{pmatrix} \\ n_0 \end{pmatrix}$$

$$\begin{pmatrix} q_0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} b \\ n_0 \end{pmatrix} = \begin{pmatrix} q_0 b + n_0 \\ b \end{pmatrix}$$

$\exists n_1, \ldots, n_n \in \mathbb{Z} \mid \text{pgcd}(a_1, \ldots, a_n) = \sum_{i=1} n_i a_i$

Si $\text{pgcd}(a,b) = 1$ alors $\exists u, v \in \mathbb{Z} \mid 1 = au + bv$.

$\text{pgcd}(a,b) = 1 \Rightarrow \exists (u,v) \in \mathbb{Z}^2 \mid au + bv = 1$

Rq: $\exists (u,v) \in \mathbb{Z}^2 \mid au + bv = 1 \Rightarrow \text{pgcd}(a,b) = 1$

Supposons $\exists (u,v) \in \mathbb{Z}^2 \mid au + bv = 1$

Mq: $\text{pgcd}(a,b) = 1$

Soit $d \in \mathcal{D}(a) \cap \mathcal{D}(b)$.

$24, 52$

$52 = 2 \times 24 + 4$

$24 = 6 \times 4 + 0$

$4 = 1 \times 52 + (-2) \times 24$

$4 = (-2) \times 24 + 1 \times 52$

$52 = 2 \times 25 + 2$

$52 - 2 \times 25 = 2$

$52 = 2 \times 25 + 2$

$25 = 12 \times 2 + 1$

$2 = 2 \times 1 + 0$

$a = 52,\ b = 25,\ q_0 = 2,\ r_0 = 2$

$q_1 = 12,\ r_1 = 1$

$\text{pgcd} = 25 - 12 \times 2$

$= 25 - 12 \times (52 - 2 \times 25)$

$= 1 \times 25 + \underline{(-12) \times 52} + 24 \times 25$

$= \underbrace{(-12)}_{u} \times 52 + \underbrace{25}_{v} \times 25$

$r_1 = 25 - 12 \times 2$

$= \dots$

$(\mathbb{Z}/n\mathbb{Z}, +, \times)$

$\bar{0}, \bar{1}, \dots, \overline{n-1}$

$= n\mathbb{Z}, 1 + n\mathbb{Z}, \dots, (n-1) + n\mathbb{Z}$

$g \in U(\mathbb{Z}/n\mathbb{Z})$

$\underbrace{\{\dots, g^{-2}, g^{-1}, \bar{1}, g, g^2, \dots\}}$

$\exists k \in \mathbb{N} \mid g^k = 1$

$g^k = g^\ell$

$g^{k-\ell} = 1$

Si H sous-groupe de G, $\# G < \infty$ Alors $|H| \mid |G|$

$k \in U(\mathbb{Z}/n\mathbb{Z}) \iff \text{PGCD}(k, n) = 1$

$\phi(n) = \text{card}\{k \in [\![1, n]\!] \mid \text{PGCD}(k, n) = 1\} = |U(\mathbb{Z}/n\mathbb{Z})|$

$\bar{a} \in U\left(\frac{\mathbb{Z}}{n\mathbb{Z}}\right) \iff \exists\, k \in \mathbb{Z}$ tq $\bar{a}\,\bar{k} = \bar{1}$

?

soit $k \in \mathbb{Z}$ tq $\longrightarrow$ $a \times k \equiv 1 \quad [n]$

$\iff n \mid (ak - 1)$

$\iff \exists\, v \in \mathbb{Z}$ tq $ak - 1 = nv$

$\iff \exists\, v \in \mathbb{Z}$ tq $k \times a + (-v)n = 1$

$p \in \mathcal{P}$

$\underbrace{1, 2, 3, \dots, p-2, p-1, p}$

$1, \dots, p-1, \cancel{p}, p+1, \dots, p^2-1, \cancel{p^2}$

$\dots$

$$\begin{cases} \phi(p) = p-1 \\ \phi(p^\alpha) = p^\alpha - p^{\alpha-1} \end{cases}$$

Si $\operatorname{PGCD}(a, n) = 1$ alors $a^{\phi(n)} \equiv 1 \quad [n]$.

Si $\operatorname{PGCD}(p, q) = 1$ alors $\phi(p \times q) = \phi(p) \times \phi(q)$

$e \in U\left(\frac{\mathbb{Z}}{\phi(n)\mathbb{Z}}\right) \iff \operatorname{PGCD}(e, \phi(n)) = 1$