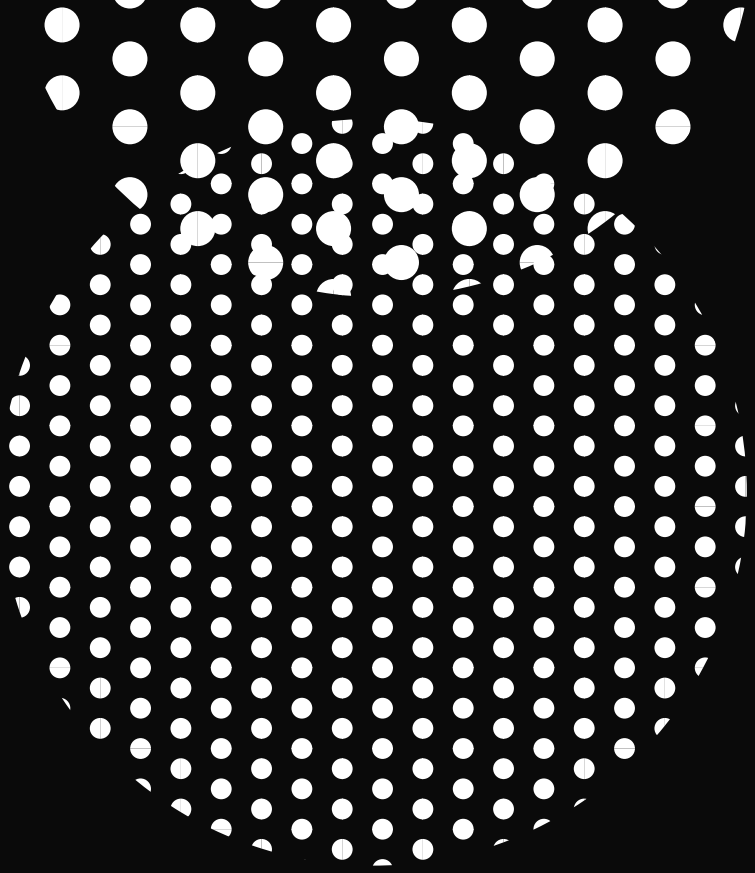

Déf: $a, b \in \mathbb{N}$ $a \geq 0,$ $b \geq 0$

$pgcd(0,0) := 0$

Si $(a,b) \neq (0,0)$ alors

$pgcd(a,b) := \max\{d \geq 1$ t.q $d | a$ et $d | b\}$

$a, b \in \mathbb{Z}$ $pgcd(a,b) := pgcd(|a|, |b|)$

Q: Déterminer ce pgcd?

OPS on peut supposer $1 \leq b \leq a$

Diviser $a = qb + r$ $0 \leq r \leq b-1$

Eurêka : $r \leq b-1$

Rediviser $b = ur + s$ avec $0 \leq s \leq r-1$

etc.

$r = vs + t$

Indicer:

$r_0 := a$ $r_1 := b$ $q_1 := q$ $r_2 := r$

$r_0 = q_1 r_1 + r_2$

$r_1 = q_2 r_2 + r_3$

$\ddots$

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

$\ddots$

$r_{l-2} = q_{l-1} r_{l-1} + r_l$

$r_{l-1} = q_l r_l + 0$

r_l ділить r_{l-1} без остачі

тоді $r_{l-2} = q_{l-1} r_{l-1} + r_l$

$= q_{l-1}(q_l \cdot r_l) + r_l = r_l(q_{l-1} \cdot q_l + 1)$

Оскільки якщо $d | a$ et $d | b$

тоді $a = qb + r$ $d | r$

тобто d ділить остачу

Таким чином, існує число, яке ділить a і b а значить і остачу r.

Тобто ділить b і r а значить і остачу $b : q$ і т.д. ділення. Так повторюємо поки остача не $= 0$

Остання остача, яка була $\neq 0$ і є pgcd

Aff°: $r_\ell = 0$ à partir d'un certain rang

pv: $0 \leq \dots < r_3 < r_2 < r_1$ □

Thm: Le dernier reste $r_\ell \neq 0$
non nul dans l'algo de div euclidienne itérée

$$r_\ell = pgcd(a,b)$$

pv: Abréger $d := pgcd(a,b)$
donc $d \mid a$ et $d \mid b$ (le plus g d)
i.e $d \mid r_0$ et $d \mid r_1$
mais $r_2 = r_0 - q_1 r_1$ aussi un multiple de d
càd $d \mid r_2$
puis $d \mid r_1$ et $d \mid r_2$ avec $r_3 = r_1 - q_2 r_2$
donne $d \mid r_3$

Fin: $d \mid r_{\ell-2}$ et $d \mid r_{\ell-1}$ $\Rightarrow d \mid r_\ell$ **Rappel:** $c \mid d \Rightarrow c \leq d$
$d = pgcd(a,b) \leq r_\ell$

Ensuite: dernière égalité dit $r_\ell \mid r_{\ell-1}$ penultième
$r_{\ell-2} = q_{\ell-1} r_{\ell-1} + r_\ell$ ← multiple de r_ℓ
↳ donc $r_{\ell-2}$ multiple de r_ℓ i.e $r_\ell \mid r_{\ell-2}$

Rec: $\forall 0 \leq i \leq \ell$ $r_\ell \mid r_i$. En particulier $r_\ell \mid r_0$ et $r_\ell \mid r_1$
Fin: $r_\ell \mid a$ et $r_\ell \mid b$ Mais le pgcd est le plus grand diviseur commun
Donc $r_\ell \leq pgcd(a,b)$

CCL: $r_\ell = pgcd(a,b)$

Q: Calculer r_ℓ ? Magie ! r_ℓ = combi-linéaire de a et de b

$r_0 := a \quad r_1 := b \qquad r_{i+1} = r_{i-1} - q_i r_i \quad (1 \le i \le \ell - 1)$

Introduire deux suites auxiliaires :

$u_0 := 1 \quad u_1 := 0 \qquad u_{i+1} := u_{i-1} - q_i u_i \qquad (1 \le i \le \ell - 1)$

$v_0 := 0 \quad v_1 := 1 \qquad v_{i+1} := v_{i-1} - q_i v_i$

Lm: $\forall\, 0 \le i \le \ell$ le reste $r_i = u_i a + v_i b$ pour $i = \ell$: $r_\ell = u_\ell a + v_\ell b$

pv: Pour $i = 0$ a-t-on ? $r_0 \overset{?}{=} u_0 a + v_0 b$ ($r_0 = a$, $u_0 = 1$, $v_0 = 0$)

Pour $i = 1$ a-t-on ? $r_1 \overset{?}{=} u_1 a + v_1 b$ ($r_1 = b$, $u_1 = 0$, $v_1 = 1$)

Hyp-réc: $u_{i-1} a + v_{i-1} b = r_{i-1}$

$u_i a + v_i b = r_i \quad \overset{?}{\Rightarrow} \quad u_{i+1} a + v_{i+1} b \overset{?}{=} r_{i+1}$ (RPL, RPL)

c.à.d

pour un certain $1 \le i \le \ell - 1$

$(u_{i-1} - q_i u_i) a + (v_{i-1} - q_i v_i) b \overset{?}{=} r_{i-1} - q_i r_i$

réorganiser

$\underbrace{u_{i-1} a + v_{i-1} b}_{\text{Hyp-réc 1}} + q_i \underbrace{(u_i a - v_i b)}_{\text{HYP-RÉC}} \overset{?}{=} r_{i-1} - q_i r_i$

$= r_{i-1} \qquad = r_i$

Thm: $\text{pgcd}(a,b) = u_\ell a + v_\ell b = r_\ell$ — pgcd = Combi-lin (a,b)

Ex: $\text{pgcd}(126, 35) = ?$ 7

$126 = 3 \cdot 35 + 21$

$35 = 1 \cdot 21 + 14$

$21 = 1 \cdot 14 + \boxed{7}$

$14 = 2 \cdot 7 + 0$

Lire

TOUJOURS SE VÉRIFIER

Vérif: $252 - 245 = 7$

Sens d'écriture

$2 \cdot 126 - 7 \cdot 35 = -1 \cdot 35 + 2 \cdot (126 - 3 \cdot 35) =$

$-1 \cdot 35 + 2 \cdot 21 = 21 - 1 \cdot (35 - 1 \cdot 21) =$

RPL

$21 - 1 \cdot 14 = \boxed{7}$

RPL

Q2: Trouver u et v

$\boxed{7} = 126 \cdot u + 35 \cdot v$

Déf: a et b sont premiers entre eux si $1 = \text{pgcd}(a, b)$

On note aussi $\text{pgcd}(a, b) = a \wedge b$ donc $a \wedge b = 1$

Thm *7 : [de Bézout] Pour $a,b \in \mathbb{Z}$ avec $(a,b) \neq (0,0)$,
il existe $u,v \in \mathbb{Z}$ t.q $\text{pgcd}(a,b) = ua+vb = 1$
DÉJÀ VU

On a :

(i) $a \wedge b = 1$

⇕ OK

(ii) $\exists u,v \in \mathbb{Z}$ avec $ua + vb = 1$

pv : Suffit (i) ⇔ (ii) Hyp : $\exists u\, ua + \exists v\, vb = 1$

Noter $d := \text{pgcd}(a,b)$ But $d \overset{?}{=} 1$

Or $d \mid a$ et $d \mid b$

$\overset{\text{vu}}{\Rightarrow} d \mid (ua + vb)$ $\forall u \in \mathbb{Z}$ $\forall v \in \mathbb{Z}$

$\Rightarrow d \mid 1$

$\Rightarrow d = 1$ □

Thm de Gauss : Soient $a,b \in \mathbb{Z}$ avec $a \wedge b = 1$
Alors, $\forall c \in \mathbb{Z}$ (si a et b sont premiers et $a \mid bc$ donc $a \mid c$ et pas $a \mid b$)
si $a \mid bc \Rightarrow a \mid c$
(étranger ; donc a se trouve dans)

Ex : $3 \mid 2n \Rightarrow 3 \mid n$
$3 \mid 6 \Rightarrow 3 \mid 3$

pv : Hyp : $a \wedge b = 1$ Thm Bézout : $\exists u,v$ $(ua + bv = 1)\ c$
$uac + vbc = c$

Observer que $a \mid ac$ trivialement
$a \mid bc$ par hyp
$\overset{\text{vu}}{\Rightarrow} a \mid (uac + vbc) \Leftrightarrow a \mid c$ □

Prop : pgcd $a \wedge c \overset{1}{=} 1$ aussi
$b \wedge c \overset{2}{=} 1$ $\Rightarrow$ $ab \wedge c = 1$

pv : Soient $a,b \in \mathbb{Z}$ tq $a \wedge b = 1$. Soit $c \in \mathbb{Z}$
On suppose que $a \mid bc$
D'après le thm de Bézout $\exists u,v \in \mathbb{Z}$ tq $ua + vb = 1$ [on multiplie par c]
$\Leftrightarrow uac + vbc = c$
$a \mid uac$ trivialement et $a \mid vbc$ car $a \mid bc$ par hyp.
donc $a \mid (uac + vbc)$ donc $a \mid c$ □

pv: Bézout

$\exists u, v \quad 1 = ua + vc$ multiplier

$\exists r, s \quad 1 = rb + sc$

$1 \cdot 1 = (ua + vc)(rb + sc)$

$1 = urab + (aus + vbn + vcs)c$

Relation de Bézout entre ab et c

donc $ab \wedge c = 1$ □

Prop: Si $a \wedge b = 1$ alors $(a|c$ et $b|c) \Rightarrow ab|c$

pv: $au = c$ (RPL) mais b divise c (Hyp)

càd $b | au$

mais $b \wedge a = 1$ Thm gauss force $b|u$

càd $bv = u$

$ab\,v = c$ ceci dit que $ab|c$ □

Prp générale:

Soient $a_1, a_2, \ldots, a_n$ avec

$1 = pgcd(a_{i_1}, a_{i_2}) \quad \forall 1 \le i_1 \ne i_2 \le 2$

Alors

$(a_1|c$ et $a_2|c \Rightarrow a_1 \cdot a_2|c)$ □

Obs*: $a, b \in \mathbb{N} \quad 1 \le a, b$

$d := pgcd(a, b)$ $d|a$ et $d|b$ max

$\exists a' \in \mathbb{N} \quad \exists b' \in \mathbb{N}$ avec $a = da' \quad b = db'$

Bezout: $d = ua + vb \quad (\exists u, v \in \mathbb{Z})$

$d = uda' + vdb'$

$\Rightarrow 1 = ua' + vb' \Rightarrow$ Bézout $a' \wedge b' = 1$

Si on divise n'importe quels nombres $\in \mathbb{N}$ par leur pgcd on obtient les nombres premiers entre eux.

Prop: Pour $a, b \geq 1$ $(\in \mathbb{N})$

$a = a' \,\text{pgcd}(a,b)$

$b = b' \,\text{pgcd}(a,b)$

avec $a' \wedge b' = 1$

Déf: Pour $a, b \in \mathbb{N}$ $\text{ppcm}(0,0) = 0$. Pour $(a,b) \neq (0,0)$

$$\text{ppcm}(a,b) := \min\{ n \in \mathbb{N}^* : a \mid n \text{ et } b \mid n \}$$

НСК двох чисел ≤ їхньому добутку

Obs: $a\,b \rightsquigarrow a \mid ab$ et $b \mid ab$ **Déf:** $\text{ppcm}(a,0) = a$

donc $\text{ppcm}(a,b) \leq ab$

Mieux: $a = da'$ $b = db'$ regarder $da'b'$ **Obs:** $a \mid \underbrace{da'}_{a}b'$ et $b \mid d\underbrace{a'b'}$ (avec $d\,b' = b$)

Thm: Pour $a \geq 1$, $b \geq 1$ avec $d := \text{pgcd}(a,b)$, avec $a = da'$, $b = db'$,

On a

$$m := \text{ppcm}(a,b) = da'b'$$

$ab = d\,d\,a'b'$

$= \text{pgcd} \cdot \text{ppcm}$

pv: Comme $a \mid m$, $\exists\, k \geq 1$ avec $m = ak = da'k$

Mais $b \mid m$ càd $b \mid da'k$

càd $db' \mid da'k$

càd $b' \mid a'k$

Or $b' \wedge a' = 1$ Gauss $b' \mid k$

Donc $k = b'k'$

Donc $m = da'k$

$= da'b'k'$

$\geq da'b'$

le nombre qui est divisible à la fois par a et par b est de la forme

$d\,a'\,b'\,k'$

d : pgcd ; a' : $\frac{a}{\text{pgcd}}$; b' : $\frac{b}{\text{pgcd}}$; k' : un nombre quelconque

→ ce nombre est le plus petit quand $k' = 1$, donc

$\text{ppcm} = da'b'$

Bilan: On a mq tout m mult de a et de b

est de la forme $da'b' \cdot$ qqchose k'

CCL: Le plus petit possible, c'est avec $k' = 1$

On a bien $\text{ppcm}(a,b) = da'b'$ □

Les nombres premiers

$\mathcal{P} = \{2, 3, 5, 7, 11, 13, 17 \dots\}$ $1 \notin \mathcal{P}$

Déf: $p \in \mathbb{N}_{\geq 2}$ est premier si $d \mid p \Rightarrow (d = 1$ ou $d = p)$

$6 \notin \mathcal{P}$ $2 \mid 6$ $3 \mid 6$

Prop: $p \neq p' \in \mathcal{P}$ premiers $\Rightarrow p \wedge p' = 1$

Pv: $d := pgcd(p, p')$ $d \mid p$ et $d \mid p'$. Mais p et p' sont premiers $(d = 1$ ou $d = p)$ et $(d = 1$ ou $d = p')$
$\overset{p \neq p'}{\Rightarrow} d = 1 = pgcd(p, p')$

Prop: Soit $p \in \mathcal{P}$ alors $\forall a \in \mathbb{Z}$:
(i) $p \wedge a = 1$

(ii) $p \nmid a$ ne divise pas

Pv: $\Downarrow$ Hyp $p \wedge a = 1$ si (ii) fausse i.e si $p \mid a$ par l'absurde
$\Leftrightarrow a = p \cdot k$
$\Leftrightarrow p \mid p \cdot k$
donc $p \mid p$ et $p \mid pk = a$
donc $pgcd(p, a) \geq p$

on aurait $pgcd(p, a) = p \geq 2$

contredisant $pgcd(p, a) = 1$

$\Uparrow$ Hyp: $p \nmid a$ Noter: $d := pgcd(p, a)$
But $d = 1$

pv de MERKER

$d \mid p \overset{\text{def}}{\Rightarrow} (d = 1$ ou $d = p)$

contrad

IMPOSSIBLE car sinon $d = p \mid a$

Donc $d = 1$ □

Le mien:

Supposons que $d \geq 2$
Or p est un nbre 1^{er}
donc si $d \mid p \Rightarrow (d = 1$ ou $d = p)$
Alors une seul possibilité c'est $d = p$. Or $d := pgcd(p, a)$
alors $d \mid a \Rightarrow p \mid d$ "p" contrad

Donc $d = 1$ □

Thm: [d'Euclide] Soit $p \in \mathcal{P}$ nombre premier.
Alors : $\forall a, b \in \mathbb{Z}$
$p \mid ab \Rightarrow (p \mid a \text{ ou } p \mid b)$

De plus, si a et b sont aussi premiers, alors $(p = a \text{ ou } p = b)$.

Pv: Hyp $p \mid ab$. Si $p \mid a$ rien à faire.
Donc OPS $p \nmid a$.

Prp donne $p \wedge a = 1$

Donc $(p \mid ab$ et $p \wedge a = 1) \overset{\text{gauss}}{\Longrightarrow} p \mid b$ le 2ème cas ! □

REC FACILE
Prp: Soit $p \in \mathcal{P}$ Alors $\forall a, b, c, \dots, l \in \mathbb{Z}$

$p \mid abc \dots l \Rightarrow (p \mid a \text{ ou } p \mid b \text{ ou } p \mid c \text{ ou } \dots \text{ ou } p \mid l)$

De plus $a, b, c, \dots, l \in \mathcal{P}$ alors $(p = a \text{ ou } p = b \text{ ou } \dots \text{ ou } p = l)$ □

Thm: Tout nombre $n \geq 2$ entier se décompose comme produit de nombres premiers.

$n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_r^{\alpha_r}$

avec

$2 \leq p_1 < p_2 < p_3 \dots < p_r$

avec $\alpha_1 \geq 1, \alpha_2 \geq 1, \dots, \alpha_r \geq 1$

Ex: $888 = 2^3 \cdot 3 \cdot 37$
$1235 = 5 \cdot 13 \cdot 19$

Thm 2: Cette décomposition est unique : $n := p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \dots \cdot p_r^{\alpha_r}$ deux déc de ce type

$= q_1^{\beta_1} \cdot q_2^{\beta_2} \cdot \dots \cdot q_s^{\beta_s}$

$\Rightarrow r = s$ et $p_1 \; p_2 \; \dots \; p_3$ et $\alpha_1 \; \alpha_2 \; \alpha_3$
$\| \; \| \; \| \qquad \| \; \| \; \|$
$q_1 \; q_2 \; q_3 \qquad \beta_1 \; \beta_2 \; \beta_3$