ARITHMÉTIQUE

Dans ce chapitre les variables a, b, c, d, m, q et r représentent a priori des entiers relatifs.

L'anneau des entiers relatifs

Les propriétés de l'anneau des entiers

Anneau commutatif

• L'ensemble $\mathbb{Z} = \{0, \pm1, \pm2, \pm3, \pm4, \cdots\}$ des entiers relatifs est construit à partir de l'ensemble $\mathbb{N}$ des entiers naturels.
Tout entier naturel correspond à un entier relatif positif : $\mathbb{N} = \mathbb{Z}_+$.
L'addition $+$ et la multiplication $\times$ sur $\mathbb{Z}$ sont des lois de composition interne qui étendent de façon usuelle l'addition et la multiplication sur $\mathbb{N}$.

• L'ensemble $\mathbb{Z}$ des entiers relatifs est un anneau commutatif ; ceci signifie que pour les opérations $+$ et $\times$, tout triplet $(a, b, c) \in \mathbb{Z}^3$ vérifie ces propositions :

$+$ est une loi de composition interne : $a + b \in \mathbb{Z}$

Associativité	$(a + b) + c = a + (b + c)$
Élément neutre	$0 + a = a + 0 = a$
	L'élément neutre de $+$ est noté $0 \in \mathbb{Z}$
	et est appelé élément nul ou zéro.
Élément symétrique	$(-a) + a = a + (-a) = 0$
	Le symétrique de $a \in \mathbb{Z}$ est noté $-a$ et appelé opposé.
Commutativité	$a + b = b + a$

$\times$ est une loi de composition interne : $a \times b \in \mathbb{Z}$

Associativité	$(a \times b) \times c = a \times (b \times c)$
Distributivité	$(a + b) \times c = (a \times c) + (b \times c)$
	$a \times (b + c) = (a \times b) + (a \times c)$
Élément neutre	$1 \times a = a \times 1 = a$
	L'élément neutre de $\times$ est noté $1 \in \mathbb{Z}$,
	est appelé élément unité, et $1 \neq 0$.
Commutativité	$a \times b = b \times a$

• L'anneau $(\mathbb{Z}, +, \times)$ est dit commutatif car la multiplication $\times$ est commutative. La définition même des anneaux impose que l'addition soit commutative.

Anneau totalement ordonné

• L'anneau $(\mathbb{Z}, +, \times)$ est ordonnée pour la relation d'ordre total $\leq$, car tout triplet $(a, b, c) \in \mathbb{Z}^3$ vérifie ces propositions :

Réflexive	$a \leq a$
Anti-symétrique	$(a \leq b)$ ET $(b \leq a) \Longrightarrow a = b$
Transitive	$(a \leq b)$ ET $(b \leq c) \Longrightarrow a \leq c$
Ordre total	$(a \leq b)$ OU $(b \leq a)$
Compatibilité avec $+$	$a \leq b \Longrightarrow a + c \leq b + c$
Compatibilité avec $\times$	$(0 \leq a)$ ET $(0 \leq b) \Longrightarrow 0 \leq ab$

• L'anneau $\mathbb{Z}$ est discret, autrement dit :

$$\forall\, (a, b) \in \mathbb{Z} \quad a < b \Longrightarrow a + 1 \leq b$$

• La construction de $\mathbb{Z}$ à partir de $\mathbb{N}$ aboutit à ces propriétés sur $\mathbb{Z}$ à partir des propriétés équivalentes vérifiées par $\mathbb{N}$.

• Les règles des signes et les propriétés usuelles des inégalités se déduisent des propositions ci-dessous, par exemple :

$$a \leq b \Longleftrightarrow 0 \leq b - a \Longleftrightarrow -b \leq -a$$
$$(a \leq b) \text{ ET } (0 \leq c) \Longrightarrow ac \leq bc$$

• Les deux démonstrations reposent sur la compatibilité de la relation d'ordre $\leq$ avec l'addition et la multiplication ; la première opère par implications circulaires :

$$\begin{aligned} a \leq b &\Longrightarrow \quad 0 = a - a \qquad \leq b - a \\ &\Longrightarrow -b = 0 - b \qquad \leq (b-a) - b = -a \\ &\Longrightarrow \quad a = (a+b) - b \leq (a+b) - a = b \\ (a \leq b) \text{ ET } (0 \leq c) &\Longrightarrow (0 \leq b - a) \text{ ET } (0 \leq c) \\ &\Longrightarrow 0 \leq (b-a)c = bc - ac \\ &\Longrightarrow ac \leq bc \end{aligned}$$

• La valeur absolue $|\bullet|$ sur $\mathbb{Z}$ est définie ainsi :

$$|a| = \max(a, -a) = \begin{cases} a & \text{si } a \geq 0 \\ -a & \text{sinon} \end{cases}$$

La définition $|a| = \max(a, -a) \in \mathbb{Z}_+ = \mathbb{N}$ suppose que la relation d'ordre $\leq$ est totale pour permettre la comparaison de a et de $-a$.

• Les propriétés usuelles des valeurs absolues se déduisent des propriétés précédentes :

$$|ab| = |a|\,|b| \qquad |a+b| \leq |a| + |b|$$

• L'anneau commutatif $(\mathbb{Z}, +, \times)$ est dit intègre car il vérifie ces deux propositions équivalentes :

$$\Big(\forall\,(a,b) \in \mathbb{Z}^2 \quad a \times b = 0 \Longrightarrow (a = 0) \text{ OU } (b = 0)\Big)$$

$$\Longleftrightarrow \Big(\forall\,(a,b) \in \mathbb{Z}^2 \quad \forall\, c \in \mathbb{Z}^* \quad a \times c = b \times c \Longrightarrow a = b\Big)$$

Toute égalité d'entiers dans laquelle apparaît un même facteur c non nul est simplifiable, ou dit autrement, tout entier non nul est régulier pour la multiplication.

• La construction même de entiers naturels justifie que le produits de deux entiers naturels non nuls est non nul, la règle des signes étend cette propriété à $\mathbb{Z}$.

• Réciproquement tout $a \in \mathbb{Z}$ vérifie $a \times 0 = 0 \times a = 0$.
Cette propriété est commune à tous les anneaux.

Éléments inversibles

• Les seuls éléments inversibles de $\mathbb{Z}$ sont ± 1 :

$$\forall\,(u,v) \in \mathbb{Z} \quad uv = 1 \Longleftrightarrow (u = v = 1) \text{ OU } (u = v = -1)$$

$$\mathbb{U}(\mathbb{Z}) = \Big\{u \in \mathbb{Z} \;\Big/\; \exists\, v \in \mathbb{Z} \quad uv = vu = 1\Big\} = \{-1, 1\}$$

• Dans le cas où u et v sont positifs ; la contraposée de l'implication $v = 0 \Longrightarrow uv = 0$ justifie ces implications car $\mathbb{N}$ est discret :

$$\begin{aligned} uv = 1 &\Longrightarrow uv \neq 0 \\ &\Longrightarrow v \neq 0 \\ &\Longrightarrow v > 0 \\ &\Longrightarrow v \geq 1 \end{aligned}$$

Pour la même raison $u \geq 1$ car le produit $uv = vu$ est commutatif.
Ces produits justifient l'inégalité réciproque :

$$\begin{aligned} (0 \leq 1 \leq u) \text{ ET } (1 \leq v) &\Longrightarrow 1 \times u = u \leq u \times v = 1 \\ &\Longrightarrow u \leq 1 \end{aligned}$$

De même $v \leq 1$ par symétrie. En conclusion ces quatre inégalités démontrent $u = v = 1$ lorsque u et v sont positifs.
Dans le cas général où $(u, v) \in \mathbb{Z}^2$, les propriétés des valeurs absolues prouvent le résultat recherché :

$$\begin{aligned} uv = 1 &\Longrightarrow |uv| = |u|\,|v| = 1 \\ &\Longrightarrow |u| = |v| = 1 \\ &\Longrightarrow (u = \pm 1) \text{ ET } (v = \pm 1) \end{aligned}$$

Une dernière vérification de ces quatre possibilités démontre que seuls les deux cas $u = v = 1$ et $u = v = -1$ sont possibles.
Les égalités $1^2 = (-1)^2 = 1$ justifient l'inclusion $\{-1, 1\} \subset \mathbb{U}(\mathbb{Z})$.
Des deux propriétés montrent l'égalité $\mathbb{U}(\mathbb{Z}) = \{-1, 1\}$.

La division euclidienne

• Tout sous-ensemble E non vide et majoré de $\mathbb{Z}$ admet un plus grand élément noté $\max E$:

$$\max E \in E \qquad \forall\, x \in E \quad x \leq \max E$$

• Cette propriété est directement issue des trois propriétés caractéristiques de $\mathbb{N}$:

toute partie non vide majorée de $\mathbb{N}$ a un plus grand élément
ET toute partie non vide de $\mathbb{N}$ possède un plus petit élément
ET $\mathbb{N}$ n'a pas de plus grand élément

• Le quotient et le reste de la division de $a \in \mathbb{Z}$ par $b \in \mathbb{Z}^*$ est l'unique couple (q, r) défini ainsi :

$$\forall\, a \in \mathbb{Z} \quad \forall\, b \in \mathbb{Z}^* \quad \exists !\,(q,r) \in \mathbb{Z}^2 \quad a = bq + r \text{ ET } 0 \leq r < |b|$$

• Cette propriété suppose $b \neq 0$ et affirme l'existence et l'unicité du quotient et du reste de la division.
Le reste est par définition positif et strictement inférieur à $|b|$ pour

tenir compte du cas $b<0$.

• La preuve de l'existence de (q,r) et celle de l'unicité sont distinctes. La démonstration de l'existence commence par le cas $b>0$, le cas $b<0$ s'en déduit.
Supposons $b>0$, donc $b\geq 1$; le sous-ensemble E de $\mathbb{Z}$ est non vide et majoré par $|a|$:

$$E=\big\{p\in\mathbb{Z}\;\big/\;a-bp\geq 0\big\}\subset\mathbb{N}$$
$$a+|a|b=|a|(\pm 1+b)\geq 0\qquad -|a|\in E$$
$$p>|a|\Longrightarrow a-bp<a-|a|b=|a|(\pm 1-b)\leq 0$$
$$\Longrightarrow a-bp<0$$
$$\Longrightarrow p\notin E\qquad\qquad |a|\text{ majore }E$$

En conséquence E possède un plus grand élément noté $q=\max E$, et $q+1\notin E$ car $q+1>\max E$:

$$(a-bq\geq 0)\;\mathsf{ET}\;(a-(q+1)b)<0\Longleftrightarrow(a-bq\geq 0)\;\mathsf{ET}\;(a-bq<b)$$
$$\Longleftrightarrow 0\leq a-qb<b$$
$$r=a-bq\in[\![0,b-1]\!]$$

La division euclidienne de a par $b<0$ se déduit de la division euclidienne par $-b>0$:

$$a=(-b)q+r=b(-q)+r\qquad 0\leq r<|b|$$

Le reste est le même et le quotient l'opposé du quotient initial.
L'unicité du couple (q,r) provient de cet encadrement obtenu par différence :

$$a=bq+r=bq'+r'\Longrightarrow -|b|<b(q-q')=r-r'<|b|$$
$$\Longrightarrow 1-|b|\leq b(q-q')=r-r'\leq|b|-1$$
$$b(q-q')\in b\mathbb{Z}\cap[\![-|b|+1,|b|-1]\!]=\{0\}\qquad q=q'\qquad r=r'$$

• Le tableau ci-dessous énumère quelques exemples de divisions :

a	b	q	r	$a=$	$b\times q$	$+r$
101	5	20	1	$101=$	5×20	$+1$
101	-5	-20	1	$101=$	$-5\times(-20)$	$+1$
-101	5	-21	4	$-101=$	$5\times(-21)$	$+4$
-101	-5	21	4	$-101=$	-5×21	$+4$

Divisibilité

• Les conditions équivalentes suivantes définissent que « a divise b » :
$a\mid b\Longleftrightarrow b\in a\mathbb{Z}\Longleftrightarrow b$ est un multiple de a
$\Longleftrightarrow\exists\,k\in\mathbb{Z}\quad b=ka$
$\Longleftrightarrow$ le reste de la division de b par a est nul lorsque $a\neq 0$.

• Les diviseurs de 72 et de 64 sont les suivants :
$72:\pm1,\pm2,\pm3,\pm4,\pm6,\pm8,\pm9,\pm12,\pm18,\pm24,\pm36,\pm72$
$64:\pm1,\pm2,\pm4,\pm8,\pm16,\pm32,\pm64$

• L'arithmétique étudie les propriétés de divisibilité des entiers, pour cette raison les notations $a\mid b$ et $b=ka$ où $k\in\mathbb{Z}$ sont préférables à la notation fractionnaire b/a qui peut représenter un nombre rationnel non entier.

Formulaire de divisibilité

• Ce formulaire récapitule les principales propriétés de la divisibilité :

$1\mid a\quad a\mid 0\quad a\mid a\qquad a\mid b\Longleftrightarrow(-a)\mid b\Longleftrightarrow a\mid(-b)\Longleftrightarrow|a|\mid|b|$
$(a\mid b)\;\mathsf{ET}\;(b\mid c)\Longrightarrow a\mid c\qquad(a\mid b)\;\mathsf{ET}\;(a\mid c)\Longrightarrow a\mid(b\pm c)$
$(a\mid b)\;\mathsf{ET}\;(b\mid a)\Longrightarrow|a|=|b|\quad$ *i.e.* $a=\pm b\qquad a\mid 1\Longleftrightarrow|a|=1$
$(a\mid b)\;\mathsf{ET}\;(b\neq 0)\Longrightarrow|a|\leq|b|\qquad a\mid b\Longrightarrow a\mid bc$
$(c\neq 0)\;\mathsf{ET}\;(ac\mid bc)\Longrightarrow a\mid b\qquad a\mid b\Longrightarrow ac\mid bc$

• Ces appartenances à $a\mathbb{Z}$ des multiples justifie les premières propriétés :

$$a=1\times a\in 1\mathbb{Z}=\mathbb{Z}\quad\Longleftrightarrow 1\mid a$$
$$0=0\times a\in a\mathbb{Z}\quad\Longleftrightarrow a\mid 0$$
$$a=1\times a\in a\mathbb{Z}\quad\Longleftrightarrow a\mid a$$

Les égalités $b\mathbb{Z}=(-b)\mathbb{Z}=|b|\mathbb{Z}$ et la propriété $a\in(-b)\mathbb{Z}\Longleftrightarrow-a\in b\mathbb{Z}$ justifient ces équivalence :

$$a\mid b\Longleftrightarrow a\mid(-b)\Longleftrightarrow(-a)\mid b\Longleftrightarrow|a|\mid|b|$$

Si $b=ap\in a\mathbb{Z}$ est un multiple de a et $c=bq\in b\mathbb{Z}$ est un multiple de b alors $c=(ap)q=a(pq)\in a\mathbb{Z}$ est un multiple de a :

$$(a\mid b)\;\mathsf{ET}\;(b\mid c)\Longrightarrow a\mid c$$

La définition même de la divisibilité justifie l'existence de $p\in\mathbb{Z}$ et $q\in\mathbb{Z}$ vérifiant ces égalités :

$$a \mid b \qquad b = ap \in a\mathbb{Z} \qquad a \mid c \qquad c = aq \in a\mathbb{Z}$$
$$b \pm c = ap \pm aq = a(p \pm q) \in a\mathbb{Z} \qquad a \mid (b \pm c)$$
$$bc = a(pc) \in a\mathbb{Z} \qquad a \mid bc \qquad bc = (ac)p \in ac\mathbb{Z} \qquad ac \mid bc$$

Si $c \neq 0$ la réciproque repose sur $bc = acp \Longrightarrow b = ap$, donc $a \mid b$.
La démonstration de l'équivalence entre $(a \mid b)$ ET $(b \mid a)$ et $|a| = |b|$ se fait par deux implications.
L'hypothèse $|a| = |b|$ entraîne $a = \pm b$ donc a est un multiple de b et b un multiple de a, ainsi $a \mid b$ et $b \mid a$.
La démonstration réciproque distingue le cas $a = 0$ et $a \neq 0$.
Si $a = 0$ alors par hypothèse $0 \mid b$ et $b \in 0\mathbb{Z} = \{0\}$, donc $b = 0$ et $|a| = |b|$.
Supposons au contraire $a \neq 0$, les hypothèses $a \mid b$ et $b \mid a$ signifient que b est de la forme $b = pa$ et $a = qb$ où $(p, q) \in \mathbb{Z}^2$. Ainsi $a = qb = pqa$. L'hypothèse $a \neq 0$ entraîne $pq = 1$, donc $|p| = |q| = 1$ et $|a| = |b|$.
En particulier $a \mid 1$ entraîne $|a| = 1$ car $1 \mid a$ est vérifié pour tout $a \in \mathbb{Z}$.
Si $a \mid b$ et $b \neq 0$ alors $b = pa$ où $p \in \mathbb{Z}$ et $p \neq 0$, ainsi $|p| \geq 1$ et $|b| \geq |a|$.

• L'étude des restes de a et b par 7 justifient cette implication :
$$7 \mid (a^2 + b^2) \Longrightarrow (7 \mid a) \text{ ET } (7 \mid b)$$

• Les entiers a et b sont de la forme $7q+r$ et $7q'+r'$ où $(r, r') \in [\![0, 7]\!]^2$, l'expression a^2+b^2 est la suivante et elle est divisible par 7 en fonction de $r^2 + r'^2$:
$$\begin{aligned} a^2 + b^2 &= (7q + r)^2 + (7q' + r')^2 \\ &= 7(7q^2 + 2qr + 7q'^2 + 2q'r') + r^2 + r'^2 \\ 7 \mid (a^2 + b^2) &\Longleftrightarrow 7 \mid (r^2 + r'^2) \end{aligned}$$

Les 49 cas possibles sont donc les suivants ou l'abscisse correspond à r et l'ordonnée à r' :

	0	1	2	3	4	5	6
0	0	1	4	9	16	25	36
1	1	2	5	10	17	26	37
2	4	5	8	13	20	29	40
3	9	10	13	18	25	34	45
4	16	17	20	25	32	41	52
5	25	26	29	34	41	50	61
6	36	37	40	45	52	61	72

Le seul multiple de 7 de ce tableau est obtenu pour $r = r' = 0$:
$$\begin{aligned} 7 \mid (a^2 + b^2) &\Longleftrightarrow 7 \mid (r^2 + r'^2) \\ &\Longleftrightarrow r^2 + r'^2 = 0 \\ &\Longleftrightarrow (r = 0) \text{ ET } (r' = 0) \\ &\Longleftrightarrow (7 \mid a) \text{ ET } (7 \mid b) \end{aligned}$$

• Cette équivalence définit les congruences :
$$a \equiv b \quad [c] \Longleftrightarrow c \mid (b - a) \qquad \text{où } c \in \mathbb{N}^*$$
Ainsi les restes des divisions de a et de b par c sont les mêmes si et seulement si $a \equiv b \quad [c]$.

• La relation $\bullet \mid \bullet$ est une relation d'ordre partielle sur $\mathbb{N}$ car elle est réflexive, anti-symétrique et transitive :

Réflexive	$\forall a \in \mathbb{N}$	$a \mid a$
Anti-symétrique	$\forall (a, b) \in \mathbb{N}^2$	$(a \mid b)$ ET $(b \mid a) \Longrightarrow a = b \geq 0$
Transitive	$\forall (a, b, c) \in \mathbb{N}^3$	$(a \mid b)$ ET $(b \mid c) \Longrightarrow a \mid c$

La relation d'ordre $\bullet \mid \bullet$ est partielle et n'est pas totale car 6 et 10 par exemple ne peuvent pas être comparé : ni $6 \mid 10$ ni $10 \mid 6$.
L'entier 1 est le plus petit des entiers pour la relation de divisibilité car $1 \mid a$ pour tout $a \in \mathbb{N}$. L'entier 0 est le plus grand car $a \mid 0$ pour tout $a \in \mathbb{N}$.
L'anti-symétrie n'est pas vérifiée par la divisibilité sur $\mathbb{Z}$ pour une raison de signe :
$$(a \mid b) \text{ ET } (b \mid a) \Longleftrightarrow |a| = |b|$$

L'algorithme d'Euclide et ses conséquences

Lemme d'Euclide

• L'entier $d \in \mathbb{Z}$ est un diviseur commun à a et à b si et seulement si d est un diviseur commun à b et à $r = a - bq$:

$$a = bq + r \qquad r = a - bq \qquad (d \mid a) \text{ ET } \big(d \mid b\big) \Longleftrightarrow (d \mid b) \text{ ET } \big(d \mid r\big)$$

• Cette propriété est valable pour tous les entiers a, b et q, et s'applique le plus souvent lorsque q et r sont le quotient et le reste de la division euclidienne.

• Des sommes et les différences de multiples de d justifient l'équivalence :

$$\begin{aligned}
(d \mid a) \text{ ET } (d \mid b) &\Longrightarrow (d \mid a) \text{ ET } (d \mid b) \text{ ET } (d \mid bq) \\
&\Longrightarrow (d \mid (a - bq)) \text{ ET } (d \mid b) \\
&\Longrightarrow (d \mid r) \text{ ET } (d \mid b) \\
(d \mid b) \text{ ET } (d \mid r) &\Longrightarrow (d \mid b) \text{ ET } (d \mid bq) \text{ ET } (d \mid r) \\
&\Longrightarrow (d \mid b) \text{ ET } (d \mid (r + bq)) \\
&\Longrightarrow (d \mid b) \text{ ET } (d \mid a)
\end{aligned}$$

Algorithme d'Euclide

• *L'algorithme d'Euclide* appliqué à a et à b consiste à construire les suites $(a_k)_k$, $(b_k)_k$ et $(r_k)_k$ des restes successifs de divisions euclidiennes :

$a_0 = a \qquad b_0 = b$

pour tout $k \in \mathbb{N}$ tel que $b_k \neq 0$,

r_k est le reste de la division euclidienne de a_k par b_k

puis $a_{k+1} = b_k$ et $0_l e b_{k+1} = r_k < b_k$

$\text{pgcd}(a, b) = \big|a_p\big| \in \mathbb{N}$ lorsque $b_p = 0$.

Ces suites ne comportent qu'un nombre fini, noté p, de termes, car la famille d'entiers positifs $(b_k)_k$ est strictement décroissante à partir du rang 1 ; elle comporte au maximum $\big|b\big| + 1$ termes et le dernier terme $b_p = 0$ est nécessairement nul.

Le résultat de l'algorithme d'Euclide, noté $\text{pgcd}(a, b)$, est le dernier reste non nul : $\text{pgcd}(a, b) = \big|a_p\big| = \big|b_{p-1}\big| = r_{p-2} \geq 0$.

Dès que l'algorithme d'Euclide effectue au moins deux divisions, le résultat a_p est le reste de la division d'ordre $p-2$ et est donc positif.

La valeur absolue du résultat sert uniquement dans le cas où le premier ou le second reste est nul, par exemple si $b \mid a$ et $a < 0$.

• Si $b = 0$ alors $b_0 = 0$ et le résultat de l'algorithme d'Euclide est $\big|a_0\big| = \big|a\big|$.

En particulier l'algorithme a pour résultat $\text{pgcd}(0, 0) = 0$.

De même si $a = 0$ et $b \neq 0$ alors le reste $r_0 = 0$ est nul, et ainsi $a_1 = b$, $b_1 = 0$ et le résultat de l'algorithme d'Euclide est $b_1 = \big|a\big|$.

Plus grand commun diviseur

• Les diviseurs communs à 72 et 64 sont ± 1, ± 2, ± 4 et ± 8.

• Le résultat $\text{pgcd}(a, b)$ de l'algorithme d'Euclide est le plus grand diviseur commun à a et à b, d'où son nom :

$$\text{pgcd}(a, b) \mid a \qquad \text{pgcd}(a, b) \mid b$$

$\text{pgcd}(a, b) \in \mathbb{N}$ est un diviseur commun à a et à b.

$\text{pgcd}(a, b)$ est le plus grand diviseur de a et de b si $(a, b) \neq (0, 0)$.

• Le lemme d'Euclide sur la divisibilité prouve que $\text{pgcd}(a, b)$ divise tous les termes a_k et b_k, donc divise a et b ; plus précisément notons $d = \text{pgcd}(a, b) = \big|b_{p-1}\big|$, le lemme d'Euclide appliqué à chaque équation démontre $d \mid a$ et $d \mid b$:

$$\begin{array}{llll}
a_{p-1} = b_{p-1}\, q_{p-1} + r_{p-1} = b_{p-1}\, q_{p-1} & & & \text{car } r_{p-1} = 0 \\
\quad d \mid a_{p-1} & a_{p-1} = b_{p-2} & d \mid b_{p-1} & b_{p-1} = r_{p-2} \\
a_{p-2} = b_{p-2}\, q_{p-2} + r_{p-2} & & & \\
\quad d \mid a_{p-2} & a_{p-2} = b_{p-3} & d \mid b_{p-2} & b_{p-2} = r_{p-3} \\
\quad \cdots \quad \cdots & & & \\
a_1 = b_1\, q_1 + r_1 & & & \\
\quad d \mid a_1 & a_1 = b_0 & d \mid b_1 & b_1 = r_0 \\
a = a_0 = b_0\, q_0 + r_0 = bq_0 + r_0 & & & \\
\quad d \mid a_0 & a_0 = a & d \mid b_0 & b_0 = b
\end{array}$$

En conclusion $\text{pgcd}(a, b)$ divise a et b.

Réciproquement montrons que $\text{pgcd}(a, b)$ est le plus grand diviseur de a et de b dans le cas général où a et b ne sont pas simultanément nuls.

Si d est un diviseur commun à a et à b alors $d \mid a$ et $d \mid b$, puis $d \mid a_1$ et $d \mid b_1$ en appliquant le lemme d'Euclide à $a = q_0\, b + r_0$ où $a_1 = b_0 = b$ et $b_1 = r_0$.

Une construction par récurrence justifie ensuite $d \mid a_k$ et $d \mid b_k$ pour

des valeurs croissantes de l'indice k. En dernier lieu $d \mid a_p$, c'est-à-dire $d \mid \text{pgcd}(a,b)$.
Les entiers a et b ne sont pas simultanément nuls par hypothèse, donc la relation $d \mid \text{pgcd}(a,b)$ entraîne $d \leq \text{pgcd}(a,b)$.

- L'exemple suivant illustre l'algorithme d'Euclide :

$a=$	122	222	122	100	22	12	10
$b=$	222	122	100	22	12	10	2
$r=$	122	100	22	12	10	2	0
$q=$	0	1	1	4	1	1	5

$$\text{pgcd}(122,222) = 2$$

- Cette propriété fondamentale caractérise le pgcd :

$$(d \mid a) \;\mathsf{ET}\; (d \mid b) \iff d \mid \text{pgcd}(a,b)$$

- La démonstration précédente justifie le sens direct de cette équivalence.
La démonstration de l'implication réciproque provient de la transitivité de la divisibilité : $d \mid \text{pgcd}(a,b)$ et $\text{pgcd}(a,b) \mid a$ entraînent $d \mid a$, de même $d \mid b$.

- Le pgcd est commutatif et les calculs de pgcd privilégient les entiers positifs, ce qui explique la convention $\text{pgcd}(a,0) = |a|$.

$$\text{pgcd}(a,\pm 1) = 1 \qquad \text{pgcd}(a,a) = |a| = \text{pgcd}(a,0)$$
$$\text{pgcd}(a,b) = \text{pgcd}(b,a) = \text{pgcd}(-a,b) = \text{pgcd}(a,-b) = \text{pgcd}(|a|,|b|)$$

Ainsi $\text{pgcd}(0,0) = 0$ même si tout entier positif divise 0, dans ce seul cas particulier le nom pgcd semble trompeur.

- Les preuves reposent sur la définition même de plus grand diviseur commun.
En particulier les diviseurs communs à a et à b ne dépendent pas de l'ordre d'énumération de a et b et sont les mêmes que ceux de $\pm a$ et de $\pm b$.

- Ces propriétés sont une conséquence de la propriété fondamentale :

$$\text{pgcd}(ca,cb) = |c|\ \text{pgcd}(a,b) \qquad |a| = \text{pgcd}(a,b) \iff a \mid b$$

- La première égalité se ramène à $0 = 0$ si $c = 0$, la suite de la démonstration suppose $c \neq 0$. Justifier ces deux relations de divisibilité démontre l'égalité :

$$|c|\ \text{pgcd}(a,b) \mid \text{pgcd}(ca,cb) \qquad \text{pgcd}(ca,cb) \mid |c|\ \text{pgcd}(a,b)$$

Ces propositions démontrent la première relation :

$$d = \text{pgcd}(a,b) \qquad d \mid a \qquad cd \mid ca \qquad d \mid b \qquad cd \mid cb$$
$$cd \mid \text{pgcd}(ca,cb) \qquad |c|\, d = |c|\ \text{pgcd}(a,b) \mid \text{pgcd}(ca,cb)$$

La justification de la seconde exploite l'hypothèse $c \neq 0$ et note $k = \text{pgcd}(ca,cb)/c \in \mathbb{Z}$ car $c \mid ca$ et $c \mid cb$ donc $c \mid \text{pgcd}(ca,bc)$:

$$\text{pgcd}(ca,cb) = ck \mid ca \qquad k \mid a \qquad \text{pgcd}(ca,cb) = ck \mid cb \qquad k \mid b$$
$$k \mid \text{pgcd}(a,b) \qquad ck = \text{pgcd}(ca,cb) \mid |c|\ \text{pgcd}(a,b)$$

La preuve du sens direct de l'équivalence provient de $\text{pgcd}(a,b) \mid b$. Réciproquement l'hypothèse $a \mid b$ associée à $a \mid a$ justifie la divisibilité $a \mid \text{pgcd}(a,b)$; par ailleurs $\text{pgcd}(a,b) \mid a$; en conclusion $\text{pgcd}(a,b) = |a|$.

- Deux entiers a et b sont premiers entre eux lorsque $\text{pgcd}(a,b) = 1$.

- Le pgcd est associatif, d'où cette définition de $\text{pgcd}(a,b,c)$ et la propriété caractéristique qui en découle :

$$\text{pgcd}(a,b,c) = \text{pgcd}(a,\text{pgcd}(b,c)) = \text{pgcd}(\text{pgcd}(a,b),c)$$
$$d \mid \text{pgcd}(a,b,c) \iff d \mid a \;\mathsf{ET}\; d \mid b \;\mathsf{ET}\; d \mid c$$

- Ces équivalences reposent sur la propriété fondamentale des pgcd :

$$\begin{aligned} d \mid \text{pgcd}(a\,\text{pgcd}(b,c)) &\iff (d \mid a)\ \mathsf{ET}\ (d \mid \text{pgcd}(b,c)) \\ &\iff (d \mid a)\ \mathsf{ET}\ (d \mid b)\ \mathsf{ET}\ (d \mid c) \\ &\iff (d \mid \text{pgcd}\,a,b))\ \mathsf{ET}\ (d \mid c) \\ &\iff d \mid \text{pgcd}(\text{pgcd}(a,b),c)) \end{aligned}$$

Appliquer ces équivalences d'une part à $d = \text{pgcd}(a,\text{pgcd}(b,c))$ et d'autre part à $d' = \text{pgcd}(\text{pgcd}(a,b),c)$ justifient cette égalité par deux critères de divisibilité :

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

- Les propositions « les entiers (a,b,c) sont premiers entre eux deux à deux » et « les entiers (a,b,c) sont premiers entre eux dans leur ensemble » ne sont pas équivalentes :

$$\text{pgcd}(6,10,15) = \text{pgcd}(\text{pgcd}(6,10),15) = \text{pgcd}(2,15) = 1$$
$$\text{pgcd}(6,10) = 2 \qquad \text{pgcd}(10,15) = 5 \qquad \text{pgcd}(6,15) = 3$$

Aucun des entiers $(6,10,15)$ ne sont premiers entre eux deux à deux.
Les entiers $(6,10,15)$ sont premiers entre eux dans leur ensemble.

- Le pgcd vérifie $\text{pgcd}(a,b) = \text{pgcd}(b,r)$ lorsque r est le reste de la

division euclidienne de a par b.

• La première implication provient du lemme d'Euclide et de la propriété fondamentale du pgcd :

$$\begin{aligned}
&(\text{pgcd}(a,b) \mid a) \ \mathsf{ET}\ (\text{pgcd}(a,b) \mid b)\\
\Longrightarrow\ &(\text{pgcd}(a,b) \mid b) \ \mathsf{ET}\ (\text{pgcd}(a,b) \mid r)\\
\Longrightarrow\ &\text{pgcd}(a,b) \mid \text{pgcd}(b,r)\\
&(\text{pgcd}(b,r) \mid b) \ \mathsf{ET}\ (\text{pgcd}(b,r) \mid r)\\
\Longrightarrow\ &(\text{pgcd}(b,r) \mid a) \ \mathsf{ET}\ (\text{pgcd}(b,r) \mid b)\\
\Longrightarrow\ &\text{pgcd}(b,r) \mid \text{pgcd}(a,b)
\end{aligned}$$

La démonstration est similaire pour l'autre relation de divisibilité :

$$\begin{aligned}
&(\text{pgcd}(a,b) \mid \text{pgcd}(b,r)) \ \mathsf{ET}\ (\text{pgcd}(b,r) \mid \text{pgcd}(b,r))\\
\Longrightarrow\ &\text{pgcd}(a,b) = \text{pgcd}(b,r)
\end{aligned}$$

• Pour la relation d'ordre partiel $\bullet \mid \bullet$ sur $\mathbb{N}$, l'entier $\text{pgcd}(a,b)$ est plus grand que tous les diviseurs commun de a et b car $d \mid \text{pgcd}(a,b)$. En outre $\text{pgcd}(a,b)$ est un diviseur commun à a et à b. Ainsi $\text{pgcd}(a,b)$ est le plus grand des diviseurs de a et de b pour la relation d'ordre partiel $\bullet \mid \bullet$.

Théorèmes d'arithmétique

Théorème de Bezout et ses conséquences

Équation de Bezout

• L'algorithme d'Euclide construit une solution entière à l'équation $au+bv = \text{pgcd}(a,b)$ d'inconnues $(u,v)\in\mathbb{Z}^2$ par substitutions successives des restes des divisions euclidiennes à partir de la dernière :

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

• L'exemple ci-dessous illustre la résolution de $24u+17v=1$:

$$\begin{aligned}
24 &= 17\times 1+7 & \text{pgcd}(24,17) &= \text{pgcd}(17,7)\\
17 &= 7\times 2+3 & &= \text{pgcd}(7,3)\\
7 &= 3\times 2+1 & &= \text{pgcd}(3,1)\\
3 &= 1\times 3+0 & &= 1
\end{aligned}$$

$$\begin{aligned}
1 &= 7-\underline{3}\times 2 = 7-\underline{(17-2\times 7)}\times 2 = \underline{\underline{7}}\times 5-17\times 2\\
&= \underline{\underline{(24-17)}}\times 5-17\times 2 = 24\times 5-17\times 7 \qquad (u,v)=(5,-7)
\end{aligned}$$

• La méthode précédente de résolution de l'équation de Bezout est en fait générale et s'adapte à n'importe quel couple $(a,b)\in\mathbb{Z}^2$.

Théorème de Bezout

• Le *théorème de Bezout* énonce cette équivalence :

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

• Le sens direct est démontré par l'équation de Bezout.
Réciproquement s'il existe $(u,v)\in\mathbb{Z}^2$ vérifiant $au+bv=1$ alors ces règles de divisibilité justifient que $\text{pgcd}(a,b)=1$:

$$\left.\begin{array}{ll}\text{pgcd}(a,b)\mid a & \text{pgcd}(a,b)\mid au\\ \text{pgcd}(a,b)\mid b & \text{pgcd}(a,b)\mid bv\end{array}\right\} \Longrightarrow \text{pgcd}(a,b)\mid au+bv$$

$$\text{pgcd}(a,b)\mid 1 \qquad \text{pgcd}(a,b)=1$$

• Cette propriété est une conséquence du théorème de Bezout :

$$(\text{pgcd}(a,b)=1)\ \mathsf{ET}\ (\text{pgcd}(a,c)=1) \Longrightarrow \text{pgcd}(a,bc)=1$$

• Le produit des deux équations de Bezout associées à (a,b) et à (a,c) justifie $\text{pgcd}(a,bc)=1$ en appliquant l'équivalence énoncée par le théorème de Bezout :

$$\begin{aligned}
&(au+bv=1)\ \mathsf{ET}\ (au'+cv'=1)\\
\Longrightarrow\ &1=(au+bv)(au'+cv')=a^2uu'+abu'v+acuv'+bcvv'\\
\Longrightarrow\ &a(auu'+bu'v+cuv')+(bc)(vv')=1
\end{aligned}$$

• L'existence d'une solution à l'équation de Bezout pour (a,bc) prouve la réciproque du théorème précédent :

$$\begin{aligned}
\text{pgcd}(a,bc)=1 \Longrightarrow\ &1=au+(bc)v=au+b(cv)\\
\Longrightarrow\ &\text{pgcd}(a,b)=1
\end{aligned}$$

La symétrie de la formule justifie $\text{pgcd}(a,c)=1$.

• Les puissances d'entiers premiers entre eux sont aussi premiers entre eux :

$$\text{pgcd}(a,b)=1 \Longrightarrow \text{pgcd}(a^m,b^n)=1 \quad \text{pour tout couple } (m,n)\in\mathbb{N}^2$$

• Une étape intermédiaire de la démonstration justifie par récurrence $\text{pgcd}(a,b^n)=1$ à partir de la propriété précédente :

$$\left.\begin{array}{r}\gcd(a,b)=1\\ \gcd(a,b)=1\end{array}\right\}\Longrightarrow \gcd(a,b^2)=1$$

$$\left.\begin{array}{r}\gcd(a,b)=1\\ \gcd(a,b^2)=1\end{array}\right\}\Longrightarrow \gcd(a,b^3)=1$$

$$\begin{array}{rr}\cdots & \cdots\end{array}$$

$$\left.\begin{array}{r}\gcd(a,b)=1\\ \gcd(a,b^n)=1\end{array}\right\}\Longrightarrow \gcd(a,b^{n+1})=1$$

Le résultat final consiste à appliquer de nouveau le résultat précédent à b à la place de a, a^n à la place de b, m à la place de n :

$$\gcd(a,b^n)=1\Longrightarrow \gcd(a^m,b^n)=1$$

Théorème de Gauss et ses conséquences

• Le *Théorème de Gauss* énonce cette implication :

$$(\gcd(a,b)=1)\ \mathsf{ET}\ (a\mid bc)\Longrightarrow a\mid c$$

• La démonstration découle du produit par c de l'équation de Bezout associée à (a,b) de solution $(u,v)\in\mathbb{Z}^2$, en notant $k=bc/a\in\mathbb{Z}$:

$$\begin{aligned}au+bv=1&\Longrightarrow acu+bcv=c\\&\Longrightarrow acu+akv=a(cu+kv)=c\\&\Longrightarrow a\mid c\end{aligned}$$

• Cette proposition est une conséquence du théorème de Gauss :

$$(\gcd(a,b)=1)\ \mathsf{ET}\ (a\mid c)\ \mathsf{ET}\ (b\mid c)\Longrightarrow ab\mid c$$

• La démonstration consiste à appliquer le théorème de Gauss au quotient entier $k=c/a\in\mathbb{Z}$:

$$\begin{aligned}(\gcd(a,b)=1)\ \mathsf{ET}\ (b\mid c)\ \mathsf{ET}\ (c=ka)&\Longrightarrow b\mid k\\&\Longrightarrow ab\mid ak\\&\Longrightarrow ab\mid c\end{aligned}$$

Ensemble des solutions de l'équation de Bezout

Dans cette partie le couple $(a,b)\in\mathbb{N}^2$ vérifie $\gcd(a,b)=1$, $a\geq 2$ et $b\geq 2$, et l'équation de Bezout $\mathcal{B}$ d'inconnues $(u,v)\in\mathbb{Z}^2$ est définie par $au+bv=1$.

• Les familles (a_k), (b_k), (q_k), (r_k), (u_k) et (v_k) sont définies ainsi :

$a_0=a$ $\quad b_0=b$ $\quad u_0=0$ $\quad v_0=1$ $\quad u_1=1$ $\quad v_1=-q_0$

Pour tout $k\in\mathbb{N}$ tel que $b_k\neq 0$, q_k et r_k sont respectivement le quotient et le reste de la division euclidienne de a_k par b_k, $a_{k+1}=b_k$ et $b_{k+1}=r_k$:

$$u_{k+1}=u_{k-1}-q_k\,u_k\qquad v_{k+1}=v_{k-1}-q_k\,v_k\qquad \text{pour } k\geq 1$$

Les familles (a_k) et (b_k) sont construites à partir de l'algorithme d'Euclide, ces familles sont finies et le dernier terme est noté $b_p=0$.

• Tout $k\in[\![0,p]\!]$ vérifie l'égalité suivante, et en particulie ces suites construisent un couple solution à l'équation de Bezout :

$$r_k=au_{k+1}+bv_{k+1}\qquad \gcd(a,b)=r_{p-2}=u_{p-1}a+v_{p-1}b$$

• Une démonstration par récurrence justifie cette dernière égalité. Cette égalité est vérifiée pour $k=0$ et $k=1$:

$au_1+bv_1=a-q_0\,b=r_0$ $\quad u_2=-q_1$ $\quad v_2=1+q_0\,q_1$

$au_2+bv_2=-q_1\,a+(1+q_0\,q_1)b=b-q_1(a-q_0b)=a_1-q_1\,r_1=r_2.$

Les deux premiers termes sont bien vérifiés, cette démonstration par récurrence suppose l'égalité vérifiée aux rangs k et $k+1$ et la démontre au rang $k+2$:

$$\begin{aligned}au_{k+1}+bv_{k+1}&=r_k\\au_{k+2}+bv_{k+2}&=r_{k+1}\\au_{k+3}+bv_{k+3}&=a(u_{k+1}-q_{k+2}\,u_{k+2}+b(v_{k+1}-q_{k+2}\,q_{k+2}v_{k+2})\\&=au_{k+1}+bv_{k+1}-q_{k+2}(au_{k+2}+bv_{k+2})\\&=r_k-q_{k+2}\,r_{k+1}=a_{k+2}-q_{k+2}\,b_{k+2}=r_{k+2}\end{aligned}$$

• L'ensemble $\mathcal{S}$ des couples (u,v) solutions de l'équation de Bezout $au+bv=1$ où $\gcd(a,b)=1$ est construit à partir d'une solution particulière $(u',v')\in\mathbb{Z}^2$:

$$\mathcal{S}=\left\{(u'+kb,v'-ka)\ /\ k\in\mathbb{Z}\right\}$$

• Une simple vérification justifie une inclusion :

$$a(u'+kb)+b(v'-ka)=au'+bv'+ab(k-k)=1+0=1$$

$$\left\{(u'+kb,v'-ka)\ /\ k\in\mathbb{Z}\right\}\subset\mathcal{S}$$

Réciproquement soit $(u,v)\in\mathcal{S}$ la différence des deux équations abou-

tit au théorème de Gauss :

$$au+bv=1 \qquad au'+bv'=1$$
$$a(u'-u)+b(v'-v)=0 \qquad a(u'-u)=b(v-v')\in b\mathbb{Z}$$
$$(b \mid a(u'-u)) \;\mathsf{ET}\; (\mathrm{pgcd}(a,b)=1) \Longrightarrow b \mid (u'-u)$$

Notons $k=(u'-u)/b\in\mathbb{Z}$, ainsi $u=u'+kb$, substituer u dans l'équation initiale démontre $v=v'-kb$:

$$bv=1-au=(au'+bv')-a(u'+kb)=bv'-kab=b(v'-ka)$$
$$v=v'-ka$$

Cette égalité termine la preuve de l'inclusion vérifiée par $\mathcal{S}$.

Une solution particulière

• Lorsque a et b sont des entiers premiers entre eux supérieurs à 2, il existe une unique solution $(\widetilde{u},\widetilde{v})$ vérifiant en plus ces inégalités :

$$\forall\,(a,b)\in\mathbb{N}^{*2} \quad \exists!\,(\widetilde{u},\widetilde{v})\in[\![1,b-1]\!]\times[\![1,a-1]\!] \quad a\widetilde{u}-b\widetilde{v}=1$$

• L'algorithme d'Euclide construit une solution à l'équation de Bezout, la propriété précédente énumère toutes les solutions. Notons (u,v) est une solution quelconque de l'équation de Bezout, et q et r le quotient et le reste de la division de u par b. Ainsi $0\leq r<b$, et vérifions que $(\widetilde{u},\widetilde{v})=(u-qb,-v-qa)$ vérifie toutes les propriétés recherchées.
Le couple $(\widetilde{u},\widetilde{v})$ est bien solution de l'équation $a\widetilde{u}-b\widetilde{v}=1$, et $0\leq\widetilde{u}<b$.
Par ailleurs $\widetilde{u}=0$ est impossible car $b\widetilde{v}\neq 1$ du fait que $b>2$, ainsi $\widetilde{u}\neq 0$ et $1\leq\widetilde{u}\leq b-1$.
Il reste à vérifier que $1\leq\widetilde{v}<a$ à partir de l'égalité $b\widetilde{v}=1+a\widetilde{u}$.

$$\begin{aligned}0\leq\widetilde{u}\leq b-1 &\Longrightarrow 1\leq b\widetilde{v}=1+a\widetilde{u}\leq 1+(b-1)a\\ &\Longrightarrow 1\leq b\widetilde{v}\leq ba-a+1<ba\\ &\Longrightarrow 0<b\widetilde{v}<ba\\ &\Longrightarrow 0<\widetilde{v}<a\\ &\Longrightarrow 1\leq\widetilde{v}\leq a-1\end{aligned}$$

Cette méthode à partir d'une division euclidienne construit bien un couple-solution $(\widetilde{u},\widetilde{v})$.
La preuve de l'unicité se fait par différence de équations associées à deux couples-solutions ; le théorème de Gauss et un encadrement terminent la démonstration :

$$a\widetilde{u}-b\widetilde{v}=1 \qquad a\widehat{u}-b\widehat{v}=1$$
$$a(\widetilde{u}-\widehat{u})-b(\widetilde{v}-\widehat{v})=0 \qquad a(\widetilde{u}-\widehat{u})=b(\widetilde{v}-\widehat{v})$$
$$(\mathrm{pgcd}(a,b)=1)\;\mathsf{ET}\;(b \mid a(\widetilde{u}-\widehat{u}))\Longrightarrow b \mid (\widetilde{u}-\widehat{u})$$
$$1\leq\widetilde{u}\leq b-1 \quad 1\leq\widehat{u}\leq b-1 \qquad -b<2-b\leq\widetilde{u}-\widehat{u}\leq b-2<b$$
$$(\widetilde{u}-\widehat{u}\in b\mathbb{Z})\;\mathsf{ET}\;(-b<\widetilde{u}-\widehat{u}<b)\Longrightarrow\widetilde{u}-\widehat{u}=0$$

En conclusion $\widetilde{u}=\widehat{u}$, puis $a(\widetilde{v}-\widehat{v})=0$ et $\widetilde{v}=\widehat{v}$.

Plus petit commun multiple

• Les multiples de 6 et de 8 sont les suivants :

$$6:0,\pm6,\pm12,\pm18,\pm24,\pm30,\pm36,\pm42,\pm48,\pm54,\cdots$$
$$8:0,\pm8,\pm16,\pm24,\pm32,\pm40,\pm48,\pm56,\cdots$$

Ainsi 0, ±24, ±48 sont des multiples communs à 6 et à 8.

• Le plus petit commun multiple strictement positif de a et b lorsque $ab\neq 0$ est défini ainsi :

$$\mathrm{ppcm}(a,b)=\min\left\{m\in\mathbb{N}^* \;\middle/\; a \mid m \;\mathsf{ET}\; b \mid m\right\}\in\mathbb{N}^*$$
$$\mathrm{ppcm}(a,0)=\mathrm{ppcm}(0,a)=\mathrm{ppcm}(0,0)=0 \qquad \text{par convention}$$

• Le sous-ensemble précédent de $\mathbb{N}$ est non vide car il contient $|ab|$, il possède donc un plus petit élément et le ppcm est donc bien défini comme étant le plus petit élément d'un sous-ensemble non vide de $\mathbb{N}$.

• Le ppcm est commutatif et ses premières propriétés sont les suivantes :

$$\mathrm{ppcm}(a,\pm1)=\mathrm{ppcm}(a,a)=|a| \qquad a \mid \mathrm{ppcm}(a,b) \quad b \mid \mathrm{ppcm}(a,b)$$
$$\mathrm{ppcm}(a,b)=\mathrm{ppcm}(b,a)=\mathrm{ppcm}(\pm a,\pm b)=\mathrm{ppcm}(|a|,|b|)$$

• Les preuves reposent sur la définition même de plus petit multiple strictement positif commun.
En particulier les multiples communs à a et à b sont les mêmes que ceux de $\pm a$ et de $\pm b$.

• Cette équivalence fondamentale caractérise le ppcm :

$$(a \mid m)\;\mathsf{ET}\;(b \mid m)\Longleftrightarrow \mathrm{ppcm}(a,b) \mid m$$

• La propriété est vérifiée si $a=0$ ou $b=0$, les deux propositions sont vraies si $m=0$ et fausses sinon.
La suite de la démonstration suppose $a\neq 0$ et $b\neq 0$.
La démonstration du sens direct de l'implication suppose $a \mid m$ et

$b \mid m$ et prouve $\text{ppcm}(a,b) \mid m$. Notons q et r le quotient et le reste de la division euclidienne de m par $\text{ppcm}(a,b)$:

$m = q\ \text{ppcm}(a,b) + r \qquad r = m - q\ \text{ppcm}(a,b) \in [\![0, \text{ppcm}(a,b) - 1]\!]$

Ainsi $a \mid m$ et $a \mid \text{ppcm}(a,b)$, donc $a \mid r$, et pour une raison symétrique $b \mid r$, donc r est un multiple commun à a et à b et par ailleurs ce reste vérifie $0 \leq r < \text{ppcm}(a,b)$.

L'hypothèse $r \neq 0$ aboutit à une contradiction car r est d'une part un multiple commun à a et à b qui vérifie donc $r \geq \text{ppcm}(a,b)$ par définition du ppcm, et d'autre part $r < \text{ppcm}(a,b)$ comme tout reste de division euclidienne. En conclusion $r \neq 0$ est impossible, donc $r = 0$, et $\text{ppcm}(a,b) \mid m$.

La preuve de la réciproque associe l'hypothèse $\text{ppcm}(a,b) \mid m$ à la propriété $a \mid \text{ppcm}(a,b)$ et justifie par transitivité $a \mid m$; la raison pour laquelle $b \mid m$ est similaire.

• Ces deux propriétés sont des conséquences directes de la précédente :

$$\text{ppcm}(ca, cb) = |c|\ \text{ppcm}(a,b) \qquad a \mid b \iff \text{ppcm}(a,b) = |b|$$

• La méthode de démonstration est comparable à celle des propriétés analogues sur les pgcd.

La première égalité est vérifiée si $c = 0$. La suite de la démonstration suppose $c \neq 0$, et k est un entier :

$$\left.\begin{array}{ll} a \mid \text{ppcm}(a,b) & ca \mid c\ \text{ppcm}(a,b) \\ b \mid \text{ppcm}(a,b) & cb \mid c\ \text{ppcm}(a,b) \end{array}\right\} \qquad \text{ppcm}(ca,cb) \mid c\ \text{ppcm}(a,b)$$

$$c \mid ca \qquad ca \mid \text{ppcm}(ac,bc) \qquad c \mid \text{ppcm}(ac,bc)$$

$$\text{il existe } k \in \mathbb{Z} \text{ tel que } \text{ppcm}(ac,bc) = kc$$

$$\left.\begin{array}{ll} ca \mid ck & a \mid k \\ cb \mid ck & b \mid k \end{array}\right\} \qquad \text{ppcm}(a,b) \mid k \qquad c\ \text{ppcm}(a,b) \mid ck$$

$$c\ \text{ppcm}(a,b) \mid \text{ppcm}(ca,cb)$$

Ces deux dernières relations de divisibilité justifient l'égalité recherchée $|c|\ \text{ppcm}(a,b) = \text{ppcm}(ca,cb)$.

Par construction $a \mid \text{ppcm}(a,b)$, donc $\text{ppcm}(a,b) = |b|$ entraîne $a \mid b$.

Pour démontrer l'implication réciproque supposons $a \mid b$. Dans tous les cas $b \mid b$ et $a \mid b$ par hypothèse, ainsi $\text{ppcm}(a,b) \mid b$ par la propriété fondamentale.

Réciproquement $b \mid \text{ppcm}(a,b)$, ainsi $|b| = \text{ppcm}(a,b)$.

• Le pgcd et le ppcm sont reliés par cette égalité :

$$\text{pgcd}(a,b)\ \text{ppcm}(a,b) = |ab|$$

• La démonstration s'effectue en deux étapes ; dans le premier cas si $\text{pgcd}(a,b) = 1$, alors une conséquence du théorème de Gauss prouve $\text{ppcm}(a,b) = |ab|$:

$$\left.\begin{array}{ll} & \text{pgcd}(a,b) = 1 \\ \mathsf{ET} & a \mid \text{ppcm}(a,b) \\ \mathsf{ET} & b \mid \text{ppcm}(a,b) \end{array}\right\} \Longrightarrow ab \mid \text{ppcm}(a,b)$$

Réciproquement $a \mid ab$ et $b \mid ab$ donc $\text{ppcm}(a,b) \mid ab$; ces deux relations de divisibilité prouvent $\text{ppcm}(a,b) = |ab|$.

La démonstration dans le cas général applique cette propriété à $a' = a/d$ et $b' = b/d$ où $d = \text{pgcd}(a,b)$; avec ces notations a' et b' sont premiers entre eux :

$$\begin{aligned} \text{pgcd}(a,b) &= \text{pgcd}(da', db') = d\ \text{pgcd}(a',b') = d \\ \text{pgcd}(a',b') &= 1 \\ \text{ppcm}(a,b) &= \text{ppcm}(da', db') = d\ \text{ppcm}(a',b') = da'b' \\ \text{ppcm}(a',b') &= a'b' \\ \text{pgcd}(a,b)\ \text{ppcm}(a,b) &= d(da'b') = (da')(db') = ab \end{aligned}$$

• Un pgcd est nul si et seulement si ses deux arguments sont nuls, alors que le ppcm est nul dès que l'un des deux arguments est nul. Ces équivalences décrivent différentes façon de présenter ces conditions :

$$\begin{aligned} \text{pgcd}(a,b) = 0 &\iff (a = 0)\ \mathsf{ET}\ (b = 0) \iff (a,b) = (0,0) \\ &\iff |a| + |b| > 0 \\ \text{pgcd}(a,b) \neq 0 &\iff (a \neq 0)\ \mathsf{OU}\ (b \neq 0) \iff (a,b) \neq (0,0) \\ &\iff |a| + |b| > 0 \\ \text{ppcm}(a,b) = 0 &\iff (a = 0)\ \mathsf{OU}\ (b = 0) \iff ab = 0 \\ \text{ppcm}(a,b) \neq 0 &\iff (a \neq 0)\ \mathsf{ET}\ (b \neq 0) \iff (a,b) \in \mathbb{R}^{*2} \\ &\iff ab \neq 0 \iff |ab| > 0 \end{aligned}$$

• Le ppcm est associatif, d'où cette définition de $\text{ppcm}(a,b,c)$ et la propriété fondamentale qui s'en déduit :

$$\text{ppcm}(a,b,c) = \text{ppcm}(a, \text{ppcm}(b,c)) = \text{ppcm}(\text{ppcm}(a,b), c)$$

$$(a \mid m)\ \mathsf{ET}\ (b \mid m)\ \mathsf{ET}\ (c_m idm) \iff \text{ppcm}(a,b,c) \mid m$$

• Ces équivalences reposent sur la propriété fondamentale des ppcm :

$$\begin{aligned} d \mid \text{pgcd}(a\,\text{pgcd}(b,c)) &\iff (a \mid m)\ \mathsf{ET}\ (\text{ppcm}(b,c) \mid m) \\ &\iff (a \mid m)\ \mathsf{ET}\ (b \mid m)\ \mathsf{ET}\ (c \mid m) \\ &\iff (\text{ppcm}(a,b) \mid m)\ \mathsf{ET}\ (c \mid m) \\ &\iff \text{ppcm}(\text{ppcm}(a,b),c) \mid m) \end{aligned}$$

La méthode est la même que pour le pgcd, elle consiste à appliquer ces équivalences d'une part à $m = \text{ppcm}(a, \text{ppcm}(b,c))$ et d'autre part à $m' = \text{ppcm}(\text{ppcm}(a,b),c)$ pour justifier cette égalité par deux critères de divisibilité :

$$\begin{gathered} \text{ppcm}(a, \text{ppcm}(b,c)) \mid \text{ppcm}(\text{ppcm}(a,b),c) \\ \text{ppcm}(\text{ppcm}(a,b),c) \mid \text{ppcm}(a, \text{ppcm}(b,c)) \\ \text{ppcm}(a, \text{ppcm}(b,c)) = \text{ppcm}(\text{ppcm}(a,b),c) \end{gathered}$$

- Le pgcd et le ppcm vérifient ces égalités :

$$\text{pgcd}(a, a+b) = \text{pgcd}(a,b) \qquad \text{pgcd}(a+b, \text{ppcm}(a,b)) = \text{pgcd}(a,b)$$

- Ces divisibilités démontrent la première égalité :

$$\begin{gathered} \text{pgcd}(a,b) \mid a \qquad \text{pgcd}(a,b) \mid b \qquad \text{pgcd}(a,b) \mid (a+b) \\ \text{pgcd}(a,b) \mid \text{pgcd}(a, a+b) \\ \text{pgcd}(a, a+b) \mid a \qquad \text{pgcd}(a, a+b) \mid a+b \\ \text{pgcd}(a, a+b) \mid (a+b-a) \qquad \text{pgcd}(a, a+b) \mid \text{pgcd}(a,b) \end{gathered}$$

La preuve de la seconde égalité commence par traiter le cas particulier $\text{pgcd}(a,b) = 1$, donc $\text{ppcm}(a,b) = ab$. Cette relations de divisibilité fait intervenir la précédente sur a, b et $a+b$ et une conséquence du théorème de Bezout.

$$\left.\begin{gathered} \text{pgcd}(a+b, a) = 1 \\ \text{pgcd}(a+b, b) = 1 \\ \text{pgcd}(a,b) = 1 \end{gathered}\right\} \qquad \text{pgcd}(a+b, ab) = 1$$

Le cas général découle de ce cas particulier, en notant $d = \text{pgcd}(a,b)$, $a = da'$ et $b = db'$:

$$\begin{gathered} \text{pgcd}(a,b) = \text{pgcd}(da, db) = d\ \text{pgcd}(a', b') = d \\ \text{pgcd}(a', b') = 1 \qquad \text{ppcm}(a', b') = a'b' \\ \text{ppcm}(a,b) = \text{ppcm}(da', db') = d\ \text{ppcm}(a', b') = da'b' \\ \begin{aligned} \text{pgcd}(a+b, \text{ppcm}(a,b)) &= \text{pgcd}(da' + db', da'b') \\ &= d\ \text{pgcd}(a'+b', a'b') = 1 \end{aligned} \end{gathered}$$

Les nombres premiers

- Un entier positif p est un nombre premier si et seulement s'il possède exactement deux diviseurs strictement positifs : 1 et lui-même.

$$d \mid p \Longrightarrow (|d| = 1)\ \mathsf{OU}\ (|d| = p)$$

- L'entier 1 n'est pas premier ; il possède un unique diviseur positif.
- Cette condition caractérise les entiers $a \in \mathbb{N}^*$ non premiers :

$$\exists\,(u,v) \in \mathbb{N}^2 \quad (1 < u < a)\ \mathsf{ET}\ (1 < v < a)\ \mathsf{ET}\ (uv = a)$$

Tout entier est premier ou est un produit de deux entiers autres que 1.

- Tout entier $a \geq 2$ a au moins un diviseur premier.
- La démonstration s'effectue par récurrence. L'entier 2 est un nombre premier, et est divisible par 2.

Supposons que tous les entiers inférieurs ou égaux à a vérifient cette propriété. Deux cas sont possibles pour $a+1$: soit $a+1$ est premier et est divisible par lui-même, soit $a+1$ est de la forme $a+1 = uv$ où $1 < u \leq a$ et $1 < v \leq a$. Dans ce second cas l'hypothèse de récurrence appliquée à u justifie que u possède un diviseur premier p, et donc p divise $a+1 = uv$.

En conclusion, tout entier $a \geq 2$ a au moins un diviseur premier.

- L'ensemble $\mathcal{P} \subset \mathbb{N}$ des nombres premiers est infini et n'est pas majoré :

$$\mathcal{P} = \{2, 3, 5, 7, 11, 13, \cdots\}$$

- Tout sous-ensemble E de $\mathbb{N}$ est majoré si et seulement si l'ensemble E est fini. « Ne pas être majoré » et « être infini » sont donc deux caractéristiques équivalentes de l'ensemble des nombres premiers.

Une démonstration par l'absurde suppose que l'ensemble $\mathcal{P}$ de tous les nombres premiers est fini ; dans ce cas $n = 1 + \prod_{p \in \mathcal{P}} p$ possède un facteur premier q. Ce facteur premier q n'est pas dans $\mathcal{P}$ puisque par construction n est de la forme $n = 1 + qk$ et le reste de la division de n par $q \geq 2$ est 1 ; ainsi il existe un facteur premier $q \notin \mathcal{P}$, d'où la contradiction.

- Les propriétés élémentaires d'un nombre premier p sont les suivantes :

$$\text{pgcd}(a,p)=\begin{cases} p & \text{si } p\mid a\\ 1 & \text{sinon}\end{cases}$$

$$p\mid ab\Longrightarrow (p\mid a)\ \mathsf{OU}\ (p\mid b)\qquad p\mid a^n\Longrightarrow p\mid a\quad \text{lorsque } n\in\mathbb{N}^*$$

• Le $\text{pgcd}(a,p)$ est un diviseur positif de p. Deux valeurs sont donc possibles $\text{pgcd}(a,p)=p$ ou $\text{pgcd}(a,p)=1$. La condition $p\mid p$ permet justifie donc ces équivalences :

$$p\mid a\Longleftrightarrow \text{pgcd}(a,p)=p$$
$$p\not\mid a\Longleftrightarrow \text{pgcd}(a,p)\neq p\Longleftrightarrow \text{pgcd}(a,p)=1$$

Deux cas sont possibles $\text{pgcd}(a,p)=p$ ou $\text{pgcd}(a,p)=1$; dans le premier cas $\text{pgcd}(a,p)=p$ et $p\mid a$, et dans le second le théorème de Gauss affirme que $p\mid b$.
La dernière démonstration repose sur la contraposée de cette implication :

$$\begin{aligned}\text{pgcd}(u,a)=1&\Longrightarrow \text{pgcd}(u,a^n)=1\\ p\mid a^n&\Longrightarrow \text{pgcd}(p,a^n)\neq 1\\ &\Longrightarrow \text{pgcd}(p,a)\neq 1\\ &\Longrightarrow \text{pgcd}(p,a)=p\\ &\Longrightarrow p\mid a\end{aligned}$$

Petit théorème de Fermat

• Le nombre premier p divise le coefficient du binôme $\binom{p}{k}$ si $1\leq k<p$.

• La condition $1_l ek<p$ évite $k\in p\mathbb{Z}$ et donc $\text{pgcd}(k,p)=1$:

$$\binom{p}{k}=\frac{p!}{k!\,(p-k)!}=\frac{p}{k}\,\frac{(p-1)!}{(k-1)!\,(p-k)!}\in\mathbb{N}$$
$$k\binom{p}{k}=p\,\frac{(p-1)!}{(k-1)!\,(p-k)!}=p\binom{p-1}{k-1}\in p\mathbb{N}$$
$$\left(p\mid k\binom{p}{k}\right)\ \mathsf{ET}\ (\text{pgcd}(p,k)=1)\Longrightarrow p\mid\binom{p}{k}$$

Cette proposition n'est pas valable si p n'est pas un nombre premier, par exemple $\binom{4}{2}=6$ et 4 ne divise pas 6.

• Tout nombre premier p vérifie la proposition suivante :

$$\forall\, n\in\mathbb{N}\quad p\mid n^p-n$$

• La démonstration s'effectue par récurrence. La proposition est valable pour $n=0$ et $n=1$ car $p\mid 0$.
Supposons la proposition vérifiée à l'ordre n et montrons la à l'ordre $n+1$ par la formule du binôme :

$$\begin{aligned}(n+1)^p-(n+1)&=\sum_{k=0}^{p}\binom{p}{k}n^k-n-1\\ &=1+\sum_{k=1}^{p-1}\binom{p}{k}n^k+n^p-n-1\\ &=\sum_{k=1}^{p-1}\binom{p}{k}n^k+(n^p-n)\in p\mathbb{Z}\end{aligned}$$

Le terme n^p-n et tous ces coefficients du binôme sont des multiples de p. En conclusion $p\mid n^p-n$ pour tout entier n.

• Si l'entier p est premier et $\text{pgcd}(n,p)=1$ alors $p\mid n^{p-1}-1$.

• La propriété précédente et le théorème de Gauss aboutissent à ce résultat :

$$(p\mid n(n^{p-1}-1))\ \mathsf{ET}\ (\text{pgcd}(p,n)=1)\Longrightarrow p\mid(n^{p-1}-1)$$

Factorisation des entiers

• Tout nombre entier $a\in\mathbb{N}^*$ possède une factorisation unique, à l'ordre près des facteurs, sous la forme de produits de puissances de nombres premiers différents deux à deux :

$a=p_1^{e_1}\,p_2^{e_2}\cdots p_s^{e_s}$ où $p_1<p_2<\cdots<p_s$ sont s nombres premiers et $(e_k)_{k=1}^{s}$ sont s entiers strictements positifs

• Une récurrence distinguant si a est premier ou non prouve l'existence de cette factorisation.
Les factorisations de $2=2^1$, $3=3^1$ et $4=2^2$ existent bien ; la factorisation de 1 est constituée d'une produit vide de nombres premiers de valeur l'élément unité 1.
Supposons que cette factorisation existe jusqu'à l'ordre $a\geq 1$. Deux cas sont possibles $a+1$ est un nombre premier ou $a+1$ n'est pas premier et se factorise sous la forme $a+1=uv$ où $1<u\leq a$ et $1<v\leq a$.
Dans le premier cas la factorisation $(a+1)^1$ de la forme recherchée.
Dans l'autre cas le produit des factorisations de u et de v est bien un

produit de nombres premiers, qu'il suffit de réordonner en ordre croissant en regroupant les facteurs premiers identiques $p^e \times p^f = p^{e+f}$.
Prouvons l'unicité de la factorisation à partir de ces notations :

$$a = p_1^{e_1}\, p_2^{e_2} \cdots p_s^{e_s} = q_1^{f_1}\, q_2^{f_2} \cdots q_t^{f_t}$$

Si un nombre premier q est différent de tous les p_k intervenant dans la factorisation de a, alors $\text{pgcd}(q, p_k) = 1$, et la conséquence du théorème de Bezout prouve par produit $\text{pgcd}(q, a) = 1$, donc q ne divise pas a.
La contraposée de cette implication justifie que q_k est l'un des nombres premiers p_k car q_k divise a, ainsi la famille $(q_k)_{k=1}^t$ est incluse dans la famille $(p_k)_{k=1}^s$.
Par symétrie des rôles des nombres premiers p_k et q_k, les entiers p_k appartiennent donc à la famille $(q_k)_{k=1}^t$, et les deux familles de facteurs premiers sont égales.
La factorisation de a est donc de la forme suivante et il reste à montrer l'égalité des exposants $e_k = f_k$. Quitte à échanger les deux factorisations supposons $e_1 \leq f_1$:

$$a = p_1^{e_1}\, p_2^{e_2} \cdots p_s^{e_s} = p_1^{f_1}\, p_2^{f_2} \cdots p_s^{f_s}$$
$$a' = a/p_1^{e_1} = p_2^{e_2} \cdots p_s^{e_s} = p_1^{f_1-e_1}\, p_2^{f_2} \cdots p_s^{f_s}$$

Les facteurs premiers des deux décompositions de a' sont les mêmes. Par construction le nombre premier p_1 n'intervient pas dans la première décomposition de a' et son exposant dans le second est $f_1 - e_1 \geq 0$.
Le début de cette démonstration a justifié que ces deux décompositions ont les mêmes facteurs premiers, donc p_1 n'intervient pas dans la deuxième décomposition de a', $f_1 - e_1 = 0$ et $f_1 = e_1$.
Cette méthode est valable pour tous les facteurs premiers p_k. Les exposants $e_k = f_k$ sont donc tous égaux, et la factorisation de a est unique.

• Si les familles des facteurs premiers de a et de b sont disjointes alors a et b sont premiers entre eux :

$$a = p_1^{e_1}\, p_2^{e_2} \cdots p_s^{e_s} \qquad b = q_1^{f_1}\, q_2^{f_2} \cdots q_t^{e_t} \qquad \text{pgcd}(a, b) = 1$$
$$\left\{p_k \;\middle/\; 1 \leq k \leq s\right\} \cap \left\{q_k \;\middle/\; 1 \leq k \leq t\right\} = \emptyset$$

• Les facteurs premiers de a et de b sont distincts ; la conséquence du théorème de Bezout rappelée en premier justifie ces pgcd par

produits et puissances :

$$\begin{aligned}(\text{pgcd}(u, w) = 1)\ \mathsf{ET}\ (\text{pgcd}(v, w) = 1) &\Longrightarrow \text{pgcd}(uv, w) = 1\\ \text{pgcd}(p_i, q_j) = 1 &\Longrightarrow \text{pgcd}(p_i, q_j^{f_j}) = 1\\ &\Longrightarrow \text{pgcd}(p_i, b) = 1\\ &\Longrightarrow \text{pgcd}(p_i^{e_i}, b) = 1\\ &\Longrightarrow \text{pgcd}(a, b) = 1\end{aligned}$$

• Les factorisations de $\text{pgcd}(a, b)$ et de $\text{ppcm}(a, b)$ sont les suivantes lorsque les factorisations de a et de b comportent les mêmes nombres premiers, avec des exposants e_k ou f_k éventuellements nuls :

$$a = p_1^{e_1}\, p_2^{e_2} \cdots p_s^{e_s} = \prod_{k=1}^{s} p_k^{e_k}$$
$$b = p_1^{f_1}\, p_2^{f_2} \cdots p_s^{f_s} = \prod_{k=1}^{s} p_k^{f_k}$$
$$\text{pgcd}(a, b) = p_1^{\min(e_1,f_1)}\, p_2^{\min(e_2,f_2)} \cdots p_s^{\min(e_s,f_s)} = \prod_{k=1}^{s} p_k^{\min(e_k,f_k)}$$
$$\text{ppcm}(a, b) = p_1^{\max(e_1,f_1)}\, p_2^{\max(e_2,f_2)} \cdots p_s^{\max(e_s,f_s)} = \prod_{k=1}^{s} p_k^{\max(e_k,f_k)}$$

où $p_1 < p_2 < \cdots < p_s$ sont s nombres premiers
et $(e_k)_{k=1}^s$ et $(f_k)_{k=1}^s$ sont des entiers positifs ou nuls

• La démonstration dans le cas général se déduit de la propriété préliminaire appliquée à $a' = a/d$ et $b' = b/d$:

$$d = p_1^{\min(e_1,f_1)}\, p_2^{\min(e_2,f_2)} \cdots p_s^{\min(e_s,f_s)}$$
$$a' = a/d = p_1^{e_1-\min(e_1,f_1)}\, p_2^{e_2-\min(e_2,f_2)} \cdots p_s^{e_s-\min(e_s,f_s)} \in \mathbb{N}^*$$
$$b' = b/d = p_1^{f_1-\min(e_1,f_1)}\, p_2^{f_2-\min(e_2,f_2)} \cdots p_s^{f_s-\min(e_s,f_s)} \in \mathbb{N}^*$$

Les familles des facteurs premiers de a' et de b' sont disjointes car l'un au moins des deux exposants positifs $e_k - \min(e_k, f_k) \in \mathbb{N}$ ou $f_k - \min(e_k, f_k) \in \mathbb{N}$ est nul. La propriété précédente s'applique à a' et à b', et ainsi :

$$\begin{aligned}\text{pgcd}(a', b') &= 1\\ \text{pgcd}(a, b) &= \text{pgcd}(da', db') = d\ \text{pgcd}(a', b') = d\\ &= p_1^{\min(e_1,f_1)}\, p_2^{\min(e_2,f_2)} \cdots p_s^{\min(e_s,f_s)}\end{aligned}$$

Ces égalités permettent d'aboutir à $\text{ppcm}(a,b)$; la première est aussi bien valable si $e_k \leq f_k$ que si $e_k \geq f_k$:

$$\begin{aligned} e_k + f_k &= \min(e_k, f_k) + \max(e_k, f_k) \\ ab &= \text{pgcd}(a,b)\ \text{ppcm}(a,b) \\ \text{ppcm}(a,b) &= ab/\ \text{pgcd}(a,b) \\ &= p_1^{e_1+f_1-\min(e_1,f_1)}\, p_2^{e_2+f_2-\min(e_2,f_2)} \cdots p_s^{e_s+f_s-\min(e_s,f_s)} \\ &= p_1^{\max(e_1,f_1)}\, p_2^{\max(e_2,f_2)} \cdots p_s^{\max(e_s,f_s)} \end{aligned}$$

• Cette méthode est efficace lorque la factorisation en produits de facteurs premiers de a et de b est connue.
Si cette factorisation n'est pas connue l'algorithme d'Euclide de divisions successives demande moins de calculs que de rechercher tous les facteurs premiers de a et b.