# Arithmétique des entiers relatifs

## 1 Division dans $\mathbb{Z}$

### 1.1 Relation de divisibilité

**Définition (Divisibilité, diviseur, multiple)** Soient $a, b \in \mathbb{Z}$. On dit que $a$ *divise* $b$, ou que $a$ est un *diviseur de* $b$, ou que $b$ est *divisible par* $a$, ou que $b$ est un *multiple de* $a$, s'il existe $k \in \mathbb{Z}$ tel que $b = ak$. Cette relation se note $a|b$.

**Théorème (Propriétés de la relation de divisibilité)** Soient $a, b, c, d \in \mathbb{Z}$.

(i) La relation de divisibilité $|$ sur $\mathbb{Z}$ est réflexive et transitive. Elle n'est cependant pas antisymétrique puisque :

$$a|b \quad \text{et} \quad b|a \qquad \iff \qquad |a| = |b| \qquad \iff \qquad a = b \quad \text{ou} \quad a = -b.$$

En revanche, sa restriction à $\mathbb{N}$ l'est : c'est une relation d'ordre.

(ii) **Combinaisons linéaires :** Si $d|a$ et si $d|b$, alors $d|(au + bv)$ pour tous $u, v \in \mathbb{Z}$.

(iii) **Produit :** Si $a|b$ et si $c|d$, alors $ac|bd$. En particulier, si $a|b$, alors $a^k|b^k$ pour tout $k \in \mathbb{N}$.

(iv) **Multiplication/division par un entier :** Si $d \neq 0$ : $\quad a|b \iff ad|bd$.

**Démonstration**

(i) La réflexivité et la transitivité de $|$ ont été démontrées dans le chapitre sur les relations d'ordre. Contentons-nous de montrer l'équivalence relative au défaut d'antisymétrie de $|$. L'une des deux implications est triviale : si $|a| = |b|$, i.e. $a = b$ ou $a = -b$, il est clair que $a|b$ et que $b|a$.
Réciproquement, faisons l'hypothèse que $a|b$ et $b|a$. Alors il existe $k, l \in \mathbb{Z}$ tels que $b = ak$ et $a = bl$. Du coup $b = bkl$. Deux cas se présentent alors : si $b = 0$, alors $a = bl = 0$ et on a donc bien $|a| = |b|$ ; si au contraire $b \neq 0$, alors $kl = 1$ et donc, puisque $k$ et $l$ sont entiers, on a soit $k = l = 1$, soit $k = l = -1$, i.e. $a = b$ ou $a = -b$, i.e. $|a| = |b|$ comme voulu.

(ii) Faisons l'hypothèse que $d|a$ et $d|b$. Il existe donc $k, l \in \mathbb{Z}$ tels que $a = dk$ et $b = dl$. Alors $au + bv = d(ku + vl)$ avec $ku + vl \in \mathbb{Z}$ pour tous $u, v \in \mathbb{Z}$, et donc $d\big|(au + bv)$ comme annoncé.

(iv) Supposons $d \neq 0$. Si $a|b$, alors comme par ailleurs $d|d$, l'assertion (iii) affirme que $ad|bd$.
Réciproquement, supposons que $ad|bd$. Il existe alors $k \in \mathbb{Z}$ tel que $bd = kad$, et donc tel que $b = ak$. Ceci montre bien que $a|b$. ∎

### 1.2 Relation de congruence

**Définition (Congruence modulo un entier)** Soient $n \in \mathbb{N}$ et $a, b \in \mathbb{Z}$. On dit que $a$ *est congru à* $b$ *modulo* $n$ si $n\big|(b - a)$, i.e. s'il existe $k \in \mathbb{Z}$ tel que $b = a + kn$. Cette relation se note $a \equiv b \mod n$.

✌ ✌ ✌ **Explication** La relation de congruence est une généralisation de la relation de divisibilité. Il faut à tout prix avoir en tête le cas particulier suivant : $n|a \iff a \equiv 0 \mod n$.

**Théorème (Propriétés de la relation de congruence)** Soient $a, a', b, b' \in \mathbb{Z}$ et $m, n \in \mathbb{N}$.

(i) **Relation d'équivalence :** La relation $\cdot \equiv \cdot \mod n$ est réflexive, symétrique et transitive.

(ii) **Somme :** Si $a \equiv b \mod n$ et si $a' \equiv b' \mod n$, alors $a + a' \equiv b + b' \mod n$.

(iii) **Produit :** Si $a \equiv b \mod n$ et si $a' \equiv b' \mod n$, alors $aa' \equiv bb' \mod n$.
En particulier, si $a \equiv b \mod n$, alors $a^k \equiv b^k \mod n$ pour tout $k \in \mathbb{N}$.

(iv) **Multiplication/division par un entier :** Si $m \neq 0$ : $\quad a \equiv b \mod n \iff am \equiv bm \mod mn$.

**Démonstration**

(i) La réflexivité et la symétrie de $\cdot \equiv \cdot \mod n$ sont immédiates. Montrons seulement la transitivité. Trois entiers $a, b, c \in \mathbb{Z}$ étant donnés, faisons l'hypothèse que $a \equiv b \mod n$ et $b \equiv c \mod n$. Alors $n \big| (b-a)$ et $n \big| (c-b)$, donc par somme $n \Big| \big((c-b)+(b-a)\big)$, i.e. $n \big| (c-a)$, ou encore $a \equiv c \mod n$.

(ii) Si $a \equiv b \mod n$ et si $a' \equiv b' \mod n$, alors $n \big| (b-a)$ et $n \big| (b'-a')$, donc par somme $n \Big| \big((b-a)+(b'-a')\big)$, i.e. $n \Big| \big((b+b')-(a+a')\big)$, ou encore $a+a' \equiv b+b' \mod n$.

(iii) On remarque que $bb'-aa' = b(b'-a')+a'(b-a)$. Du coup, si $a \equiv b \mod n$ et si $a' \equiv b' \mod n$, alors $n \big| (b-a)$ et $n \big| (b'-a')$, et donc par combinaison linéaire $n \Big| \big(b(b'-a')+a'(b-a)\big)$, i.e. $n \big| (bb'-aa')$, ou encore $aa' \equiv bb' \mod n$.

(iv) Enfin : $a \equiv b \mod n \iff n \big| (b-a) \overset{m \neq 0}{\iff} mn \big| m(b-a) \iff am \equiv bm \mod mn$. ■

## 1.3 Division euclidienne

**Théorème (Division euclidienne)** Soient $a \in \mathbb{Z}$ et $b \in \mathbb{N}^*$. Il existe un unique couple $(q, r) \in \mathbb{Z} \times \mathbb{N}$ tel que :

$$a = bq + r \qquad \text{et} \qquad 0 \leqslant r \leqslant b-1 \quad \text{(ce qu'on peut aussi écrire :} \quad 0 \leqslant r < b\text{)}.$$

Dans cet énoncé, $a$ est appelé le *dividende*, $b$ le *diviseur*, $q$ le *quotient* et $r$ le *reste*. On a : $q = \left\lfloor \frac{a}{b} \right\rfloor$ et $r \equiv a \mod b$.

✌ ✌ ✌ **Explication**

- Le théorème de la division euclidienne est un résultat d'**existence** et d'**unicité** : voilà l'essentiel.
- En termes de congruences, le théorème de la division euclidienne affirme simplement que tout entier relatif $a$ est congru modulo $b$ à un entier unique entier $r$ **compris entre** 0 **et** $b-1$. Par exemple, on peut ramener l'entier $a = 12839$ à l'un des entiers 0, 1, 2, 3 ou 4 modulo $b = 5$. Précisément : $\underbrace{12839}_{a} = \underbrace{5}_{b} \times \underbrace{2567}_{q} + \underbrace{4}_{r}$, et donc $12839 \equiv 4 \mod 5$.
- L'idée de la démonstration est fort simple. Si $a$ est positif, nous allons retrancher à $a$ l'entier $b$ une fois, deux fois, trois fois... jusqu'au moment où $a$ aura presque complètement fondu, c'est-à-dire jusqu'au moment où le résultat sera compris entre 0 et $b-1$. Si $a$ est négatif, l'idée est la même mais on ajoute $b$ au lieu de le retrancher. Le principe est donc simple mais un problème se pose tout de même : comment garantir avec rigueur que l'on finit bien par obtenir un entier compris entre 0 et $b-1$ ?

**Démonstration**

- **Existence du couple** $(q, r)$ **:** On démontre d'abord l'existence de $(q, r)$ dans le cas où $a \geqslant 0$. Introduisons pour cela l'ensemble $Q = \Big\{ k \in \mathbb{N} / \quad a - bk \geqslant 0 \Big\}$. Cet ensemble $Q$ est une partie non vide de $\mathbb{N}$ — non vide car elle contient 0. Mais par ailleurs $Q$ est majoré (par $a$). En effet, pour tout $k \in Q$, $a - bk \geqslant 0$ donc $k \leqslant bk \leqslant a$. L'ensemble $Q$ possède donc un plus grand élément $q$. Alors $a - bq \geqslant 0$. Mais comme $(q+1) \notin Q$, $a - b(q+1) < 0$. Ces deux inégalités s'écrivent aussi $0 \leqslant a - bq \leqslant b-1$.
  Posons donc $r = a - bq$. Alors tout va bien : nous l'avons trouvé, notre couple $(q, r)$.

  Etendons à présent le résultat au cas où $a < 0$. Or si $a < 0$, alors $-a \geqslant 0$ et on est ramené au cas précédent : il existe un couple $(q, r) \in \mathbb{Z} \times \mathbb{N}$ tel que $-a = bq + r$ et $0 \leqslant r \leqslant b-1$. Là encore, distinguons deux cas :

  1) Si $r = 0$, posons $q' = -q$ et $r' = 0$. Alors $a = -bq - r = bq' + r'$ et $0 \leqslant r' \leqslant b-1$.

  2) Si $r \geqslant 1$, posons $q' = -q-1$ et $r' = b - r$. Alors $a = -bq - r = bq' + r'$ et $0 \leqslant r' \leqslant b-1$. Et voilà !
- **Unicité du couple** $(q, r)$ **:** Donnons-nous deux couples $(q, r), (q', r') \in \mathbb{Z} \times \mathbb{N}$ tels que $a = bq + r = bq' + r'$, $0 \leqslant r \leqslant b-1$ et $0 \leqslant r' \leqslant b-1$. Alors $|r' - r| \leqslant b-1$, mais par ailleurs $b(q - q') = r' - r$.
  Supposons $q \neq q'$. Alors $|q - q'| \geqslant 1$, donc $b|q - q'| \geqslant b$. On a donc : $b \leqslant b|q - q'| = |r' - r| \leqslant b-1$, donc $b \leqslant b-1$. Contradiction. Donc $q = q'$. On en déduit aussitôt que $r = a - bq = a - bq' = r'$ comme voulu.
- Enfin, les conditions sur $q$ et $r$ peuvent se réécrire ainsi : $0 \leqslant a - bq < b$, puis : $\frac{a}{b} - 1 < q \leqslant \frac{a}{b}$. On retrouve ici la définition de $\left\lfloor \frac{a}{b} \right\rfloor$. ■

✎✎✎ **En pratique (Algorithme de la division euclidienne)** Comment calcule-t-on de fait le couple $(q,r)$ de la division euclidienne de $a$ par $b$ ? Comme on l'a vu, il convient pour cela, partant de $a$, de retrancher ou ajouter $b$ un certain nombre de fois. Cet algorithme simple à décrire est appelé l'*algorithme de la division euclidienne*.

Hélas, l'algorithme a beau être simple : sa mise en œuvre paraît bien pénible. Par exemple, pour diviser 1000 par 3, 333 soustractions sont nécessaires. Ne peut-on pas faire les choses plus simplement ? Oui et non. En réalité vous pratiquez sans le savoir la division euclidienne depuis le primaire comme une recette qu'on utilise sans réfléchir.

$$\begin{array}{rr|l} 3\ 4\ 7 & & 5 \\ -\ 3\ 0\ (0) & & 6\ 9 \\ \hline 4\ 7 & & \\ -\ 4\ 5 & & \\ \hline 2 & & \end{array}$$

Pour le comprendre, prenons l'exemple de la division posée ci-contre. On y divise 347 par 5. Dans un premier temps, en apparence, on retranche $6\times 5 = 30$ de 34 ; en fait, on retranche $60\times 5 = 300$ de 347, puisque le « 6 » apparaît comme chiffre des dizaines dans le quotient. Dans un second temps, on retranche $9\times 5 = 45$ de 47. Au total, on a retranché $(60+9)\times 5 = 69\times 5 = 345$ à 347 et le reste obtenu est 2.
Où donc est l'algorithme de la division euclidienne dans tout ça ? Avec cet algorithme, au lieu de retrancher en deux fois 345 de 347, on aurait retranché 5 une première fois, 5 une seconde fois, une troisième fois... jusqu'à ce que le reste soit strictement inférieur à 5. En tout, on aurait effectué 69 soustractions.

Conclusion : **DIVISER, C'EST SOUSTRAIRE** dans tous les cas. Simplement en primaire, *on suppose connues les tables de multiplication usuelles*. C'est grâce à elles que l'on trouve les chiffres « 6 » et « 9 » du quotient dans l'exemple précédent. Quiconque connaît ses tables de multiplication préférera utiliser la méthode des classes primaires. Pour un ordinateur en revanche, il est plus facile d'effectuer bêtement des soustractions que d'aller fouiller dans sa mémoire pour trouver des tables de multiplication.

**Exemple** Le reste de la division euclidienne de $2^{65362}$ par 7 est égal à 2.

**En effet** La démonstration de ce résultat est **TRÈS** longue si on applique l'algorithme précédent comme un rustre, car l'entier $2^{65362}$ possède près de 20000 décimales. Or on remarque que $2^3 \equiv 8 \equiv 1 \mod 7$. C'est l'idée-phare de cet exemple : dénicher la première puissance de 2 congrue à 1 modulo 7 — si elle existe.

On divise alors 65362 par 3 : $65362 = 3\times 21787 + 1$ et aussitôt $2^{65362} \equiv (2^3)^{21787}\times 2^1 \equiv 1^{21787}\times 2 \equiv 2 \mod 7$.

**Exemple** Soient $x,y,z\in\mathbb{Z}$ trois entiers solutions de l'*équation de Fermat* $x^3+y^3=z^3$. Alors l'un des entiers $x$, $y$ ou $z$ est divisible par 3.

**En effet** Raisonnons par l'absurde en supposant que ni $x$ ni $y$ ni $z$ n'est divisible par 3.

| $x \mod 9$ | $x^2 \mod 9$ | $x^3 \mod 9$ |
|---|---|---|
| 1 | 1 | 1 |
| 2 | 4 | $8\equiv -1$ |
| 4 | $16\equiv -2$ | $-8\equiv 1$ |
| $5\equiv -4$ | $16\equiv -2$ | $8\equiv -1$ |
| $7\equiv -2$ | 4 | $-8\equiv 1$ |
| $8\equiv -1$ | 1 | $-1$ |

Alors le reste de la division euclidienne de $x$ par 9 est l'un des entiers 1, 2, 4, 5, 7, 8 — on peut rejeter les cas 0, 3 et 6. Etudions un à un ces différents cas dans le tableau ci-contre. Il en ressort que $x^3 \equiv \pm 1 \mod 9$. On montrerait de même que $y^3 \equiv \pm 1 \mod 9$ et que $z^3 \equiv \pm 1 \mod 9$.

Or par hypothèse $x^3+y^3 \equiv z^3 \mod 9$. A gauche on a modulo 9 soit $1+1=2$, soit $1-1=0$, soit $-1+1=0$, soit $-1-1=-2$ ; à droite on a $\pm 1$. Impossible !

# 2 Diviseurs et multiples communs

**Définition (Diviseur commun, multiple commun)** Soient $a,b\in\mathbb{Z}$.

- On appelle *diviseur commun de $a$ et $b$* tout entier relatif qui est à la fois un diviseur de $a$ et un diviseur de $b$.
- On appelle *multiple commun de $a$ et $b$* tout entier relatif qui est à la fois un multiple de $a$ et un multiple de $b$.

## 2.1 PGCD

**Définition (PGCD)** Soient $a,b\in\mathbb{Z}$. On appelle *plus grand commun diviseur* (PGCD) *de $a$ et $b$* tout entier $d\in\mathbb{Z}$ tel que :

- $d$ est un diviseur commun de $a$ et $b$ : $d|a$ et $d|b$ ;
- $d$ est un multiple de tout diviseur commun de $a$ et $b$ : $\forall \delta\in\mathbb{Z},\quad \Big(\delta|a \text{ et } \delta|b\Big) \implies \delta|d$.

✌ ✌ ✌ **Explication** Dans le cas où $a$ et $b$ sont des entiers naturels, on demande ici deux choses à $d$ : 1) de minorer l'ensemble $\Big\{a,b\Big\}$ au sens de la relation d'ordre de divisibilité ; et 2) d'être plus grand pour cette relation que tout autre minorant de $\Big\{a,b\Big\}$. D'où l'idée que l'on définit bien là, au sens des relations d'ordre, le plus grand élément de l'ensemble des minorants de $\Big\{a,b\Big\}$, i.e. le *plus grand diviseur commun de $a$ et $b$*, ou encore la borne inférieure de l'ensemble $\Big\{a,b\Big\}$.

Un PGCD de deux entiers existe-t-il toujours ? Si oui, est-il unique ? Nous énonçons ci-après deux théorèmes essentiels. Tous deux seront prouvés simultanément au sein d'une preuve unique.

**Théorème (Existence et « unicité » du PGCD)** Soient $a,b\in\mathbb{Z}$. Il existe un et un seul PGCD **positif** de $a$ et $b$ ; ce PGCD est noté $\text{PGCD}(a,b)$ ou $a\wedge b$ et appelé **le** PGCD *de $a$ et $b$*. Le seul autre PGCD de $a$ et $b$ est alors $-\text{PGCD}(a,b)$.

✌ ✌ ✌ **Explication** On dira ainsi que $-3$ est **un** PGCD de 6 et 9, mais, au choix, que 3 est (**un** ou) **le** PGCD de 6 et 9.

**Théorème (Théorème de Bézout, première partie)** Soient $a,b\in\mathbb{Z}$.
Il existe des entiers $u,v\in\mathbb{Z}$ tels que $\text{PGCD}(a,b)=au+bv$. Un tel couple $(u,v)$ est appelé **un** *couple de coefficients de Bézout de $(a,b)$*.

✖ ✖ ✖ **Attention !** Les entiers $u$ et $v$ ne sont pas du tout uniques. Par exemple, $\text{PGCD}(4,6)=2$ et on a à la fois $\underbrace{4}_{a}\times\underbrace{(-1)}_{u}+\underbrace{6}_{b}\times\underbrace{1}_{v}=2$ et $\underbrace{4}_{a}\times\underbrace{2}_{u}+\underbrace{6}_{b}\times\underbrace{(-1)}_{v}=2$.

**Démonstration**

- Montrons d'abord que $a$ et $b$ possèdent au plus deux PGCD qui sont l'opposé l'un de l'autre. Soient $d$ et $d'$ deux PGCD de $a$ et $b$. Alors $d$ est un diviseur commun de $a$ et $b$, donc $d|d'$ puisque $d'$ est un PGCD de $a$ et $b$. De même $d'$ est un diviseur de $a$ et $b$, donc $d'|d$ puisque $d$ est un PGCD de $a$ et $b$. Comme voulu $|d|=|d'|$.

- Pour l'existence du PGCD et le théorème de Bézout, commençons par le cas $a=b=0$. Il est clair dans ce cas que 0 est un diviseur commun de $a$ et $b$, nécessairement le plus grand puisque tout entier divise 0.

  Nous pouvons désormais supposer $a\neq 0$ ou $b\neq 0$. L'ensemble $(a\mathbb{Z}+b\mathbb{Z})\cap\mathbb{N}^*$ est alors une partie non vide de $\mathbb{N}$ — il contient $|a|$ ou $|b|$, l'un des deux étant non nul — donc possède un plus petit élément $d$ : $d$ est un entier naturel non nul et s'écrit $d=au+bv$ pour certains $u,v\in\mathbb{Z}$. Nous allons montrer que $d$ est un PGCD de $a$ et $b$. Cela montrera en même temps le théorème de Bézout puisque par définition $d=au+bv$ avec $u,v\in\mathbb{Z}$.

  1) Montrons que $d$ divise à la fois $a$ et $b$. Il suffit de le prouver pour $a$ par symétrie des rôles de $a$ et $b$. La division euclidienne de $a$ par $d$ s'écrit $a=dq+r$ où $q,r\in\mathbb{Z}$ et $0\leqslant r<d$. Alors $r\in(a\mathbb{Z}+b\mathbb{Z})\cap\mathbb{N}$ car $r=a-dq=a-(au+bv)q=a(1-uq)-bvq$. Or $r<d$ et $d$ est le plus petit élément de $(a\mathbb{Z}+b\mathbb{Z})\cap\mathbb{N}^*$ donc $r=0$. Bref, $a=dq$, i.e. $d$ divise $a$.

  2) Soit $\delta\in\mathbb{Z}$ divisant à la fois $a$ et $b$. Alors $\delta$ divise $d$ puisque $d=au+bv$. ■

La preuve précédente a ceci d'inconfortable qu'elle ne nous explique pas comment calculer le PGCD de deux entiers, ni comment calculer les deux entiers $u$ et $v$ du théorème de Bézout. Nous présentons ci-après deux algorithmes de calcul adaptés à ces questions : l'*algorithme d'Euclide* et l'*algorithme de Bézout*.

**Lemme (Idée fondamentale de l'algorithme d'Euclide)** Soient $a\in\mathbb{Z}$, $b\in\mathbb{N}^*$ et $r$ le reste de la division euclidienne de $a$ par $b$. Alors $\text{PGCD}(a,b)=\text{PGCD}(b,r)$.

**Démonstration** Notons $q$ l'unique entier pour lequel $a=bq+r$. Montrer que $\text{PGCD}(a,b)=\text{PGCD}(b,r)$ revient à montrer que ces deux entiers positifs ou nuls se divisent l'un l'autre.

- Pour commencer, $\text{PGCD}(a,b)$ divise $a$ et $b$, donc aussi $b$ et $r$ puisque $r=a-bq$. Par définition de $\text{PGCD}(b,r)$, on peut donc affirmer que $\text{PGCD}(a,b)$ divise $\text{PGCD}(b,r)$.
- De même, $\text{PGCD}(b,r)$ divise $b$ et $r$, donc aussi $a$ et $b$ puisque $a=bq+r$. Par définition de $\text{PGCD}(a,b)$, on peut donc affirmer que $\text{PGCD}(b,r)$ divise $\text{PGCD}(a,b)$. ■

✎✎✎ **En pratique (Algorithme d'Euclide)**

- Soient $a,b\in\mathbb{Z}$. L'*algorithme d'Euclide* va nous permettre de calculer rapidement le PGCD de $a$ et $b$. Tout d'abord, $\text{PGCD}(a,b)=|a|$ si $b=0$ et $\text{PGCD}(a,b)=|b|$ si $a=0$. Ensuite, $\text{PGCD}(a,b)=\text{PGCD}\Big(|a|,|b|\Big)$. Enfin, évidemment, $\text{PGCD}(a,b)=\text{PGCD}(b,a)$. Nous pouvons donc supposer que $0<b\leqslant a$. On définit alors les entiers naturels $r_0,r_1,r_2\ldots$ de la façon suivante :

  1) on commence par poser $r_0=a$ et $r_1=b$ ;

  2) ensuite, $k$ désignant un entier naturel, tant que $r_{k+1}\neq 0$, on note $r_{k+2}$ le reste de la division euclidienne de $r_k$ par $r_{k+1}$ — on a dans ce cas $r_{k+2}<r_{k+1}$.

  A l'issue de cette construction, on a les inégalités : $r_0\geqslant r_1>r_2>r_3>\ldots\geqslant 0$. Comme il n'existe qu'un nombre fini d'entiers naturels entre 0 et $r_0$, on obtient forcément $r_N=0$ pour un certain $N\in\mathbb{N}^*$. Alors $r_{N-1}$ est le **dernier reste non nul** de la suite $r_0,r_1,r_2\ldots$ et en vertu de l'idée fondamentale de l'algorithme d'Euclide :

$$\text{PGCD}(a,b)=\text{PGCD}(r_0,r_1)=\text{PGCD}(r_1,r_2)=\text{PGCD}(r_2,r_3)=\ldots=\text{PGCD}(r_{N-1},r_N)=\text{PGCD}(r_{N-1},0)=r_{N-1}.$$

  Bref, le PGCD de $a$ et $b$ est tout simplement le **dernier reste non nul** $r_{N-1}$ de la suite des restes successifs $r_0,r_1,r_2\ldots$

- Appliquons l'algorithme sur un exemple simple : $\text{PGCD}(1542,58)=2$. Il s'agit seulement d'effectuer quelques divisions euclidiennes : $\underline{1542}=26\times\underline{58}+\underline{34}$, $\underline{58}=1\times\underline{34}+\underline{24}$, $\underline{34}=1\times\underline{24}+\underline{10}$, $\underline{24}=2\times\underline{10}+\underline{4}$, $\underline{10}=2\times\underline{4}+\underline{2}$ et $\underline{4}=2\times\underline{2}+\underline{0}$. Le dernier reste non nul obtenu est 2.

✎✎✎ **En pratique (Algorithme de Bézout)** La méthode décrite ci-après, dite *algorithme de Bézout*, est à connaître impérativement. Nous la présenterons seulement sur un exemple : cherchons par exemple le PGCD de 525 et 3080 ainsi qu'une identité de Bézout associée. Tout commence avec les divisions euclidiennes successives de l'algorithme d'Euclide :

$$\overbrace{3080}^{r_0}=5\times\overbrace{525}^{r_1}+\overbrace{455}^{r_2},\qquad \overbrace{525}^{r_1}=1\times\overbrace{455}^{r_2}+\overbrace{70}^{r_3},\qquad \overbrace{455}^{r_2}=6\times\overbrace{70}^{r_3}+\overbrace{35}^{r_4},\qquad \overbrace{70}^{r_3}=2\times\overbrace{35}^{r_4}+\overbrace{0}^{r_5}.$$

Le dernier reste non nul est 35, c'est lui le PGCD de 525 et 3080. Partons alors de l'avant-dernière division écrite sous la forme $\overbrace{35}^{r_4}=\overbrace{455}^{r_2}-6\times\overbrace{70}^{r_3}$. Nous allons dans cette égalité éliminer progressivement $r_3$ puis $r_2$ et aurons ainsi exprimé $r_4=35$ en fonction de $r_0=3080$ et $r_1=525$.

$$\begin{aligned}\text{PGCD}(525,3080)&=\overbrace{35}^{r_4}=\overbrace{455}^{r_2}-6\times\overbrace{70}^{r_3}\\&=\overbrace{455}^{r_2}-6\times\big(\overbrace{525}^{r_1}-1\times\overbrace{455}^{r_2}\big)\qquad\text{(on élimine } r_3)\\&=-6\times\overbrace{525}^{r_1}+7\times\overbrace{455}^{r_2}\\&=-6\times\overbrace{525}^{r_1}+7\times\big(\overbrace{3080}^{r_0}-5\times\overbrace{525}^{r_1}\big)\qquad\text{(on élimine } r_2)\\&=7\times\overbrace{3080}^{r_0}-41\times\overbrace{525}^{r_1}.\qquad\text{La voilà, notre identité de Bézout.}\end{aligned}$$

**Théorème (Propriétés du PGCD)** Soient $a,b\in\mathbb{Z}$.

(i) Pour tout $k\in\mathbb{Z}$ : $\text{PGCD}(ak,bk)=|k|\,\text{PGCD}(a,b)$.

(ii) Pour tout diviseur commun $d\neq 0$ de $a$ et $b$ : $\text{PGCD}\left(\frac{a}{d},\frac{b}{d}\right)=\frac{\text{PGCD}(a,b)}{|d|}$.

**Démonstration**

(i) Soit $k\in\mathbb{Z}$. Nous pouvons supposer $k\neq 0$. Notons $\delta=\text{PGCD}(a,b)$ et $\Delta=\text{PGCD}(ak,bk)$.

- D'une part $\delta|a$ et $\delta|b$, donc $\delta k|ak$ et $\delta k|bk$, donc par définition de $\Delta$, $\delta k|\Delta$.
- D'autre part, $k|ak$ et $k|bk$, donc par définition de $\Delta$, $k|\Delta$, de sorte qu'il existe $n\in\mathbb{Z}$ tel que $\Delta=nk$. Ensuite $nk=\Delta|ak$ et $nk=\Delta|bk$, donc $n|a$ et $n|b$ car $k\neq 0$. Par définition de $\delta$, cela montre que $n|\delta$, puis que $\Delta=nk|\delta k$.

Nous obtenons ainsi la double divisibilité $\delta k|\Delta$ et $\Delta|\delta k$, et donc $|\delta k|=|\Delta|$, ou encore $\Delta=\delta|k|$.

(ii) Soit $d\neq 0$ un diviseur commun de $a$ et $b$. Notons $\alpha=\frac{a}{d}$ et $\beta=\frac{b}{d}$. Alors d'après (i) :

$$\text{PGCD}(a,b)=\text{PGCD}(\alpha d,\beta d)=|d|\,\text{PGCD}(\alpha,\beta)=|d|\,\text{PGCD}\left(\frac{a}{d},\frac{b}{d}\right),\qquad\text{d'où le résultat.}\qquad\blacksquare$$

## 2.2 Nombres premiers entre eux

**Définition (Nombres premiers entre eux)** Soient $a, b \in \mathbb{Z}$. On dit que $a$ et $b$ sont *premiers entre eux* si leurs seuls diviseurs communs sont 1 et $-1$, i.e. si leur PGCD est égal à 1.

**Exemple** 6 et 35 sont premiers entre eux car les diviseurs de 6 sont $\pm 1$, $\pm 2$, $\pm 3$ et $\pm 6$ et ceux de 35 sont $\pm 1$, $\pm 5$, $\pm 7$ et $\pm 35$.

✎ ✎ ✎ **En pratique**

- La remarque suivante est utile dans de très nombreux exercices. Soient $a, b \in \mathbb{Z}$ de PGCD $d$. Il existe $a', b' \in \mathbb{Z}$ tels que $a = da'$ et $b = db'$. Alors $\text{PGCD}(a', b') = \text{PGCD}\left(\frac{a}{d}, \frac{b}{d}\right) = \frac{\text{PGCD}(a,b)}{|d|} = 1$. Bref, $a'$ et $b'$ sont premiers entre eux.
- Pour montrer que deux entiers sont premiers entre eux, on peut **toujours** utiliser l'algorithme de Bézout. Nous verrons plus loin une autre technique à base de nombres premiers, parfois inutilisable mais souvent plus pratique.

**Théorème (Théorème de Bézout, deuxième partie)** Soient $a, b \in \mathbb{Z}$. Les assertions suivantes sont équivalentes :

(i) $a$ et $b$ sont premiers entre eux.

(ii) Il existe deux entiers $u, v \in \mathbb{Z}$ tels que $au + bv = 1$.

**Démonstration** L'implication (i) $\Longrightarrow$ (ii) résulte immédiatement du théorème de Bézout, première partie. Pour la réciproque (ii) $\Longrightarrow$ (i), supposons l'existence de deux entiers $u, v \in \mathbb{Z}$ tels que $au + bv = 1$ et fixons $d$ un diviseur commun de $a$ et $b$. Alors $d|(au + bv) = 1$, donc $d = \pm 1$. Comme voulu, $a$ et $b$ sont premiers entre eux. ■

**Théorème (Théorème de Gauss)** Soient $a, b, c \in \mathbb{Z}$. Si $a|bc$ et si $a$ et $b$ sont premiers entre eux, alors $a|c$.

**Démonstration** Faisons l'hypothèse que $a|bc$ et que $a$ et $b$ sont premiers entre eux. Alors $bc = ak$ pour un certain $k \in \mathbb{Z}$ et le théorème de Bézout affirme qu'il existe $u, v \in \mathbb{Z}$ tels que $au + bv = 1$. Multiplions cette identité par $c$ : $acu + bcv = c$, puis remplaçons $bc$ par $ak$ : $a(cu + kv) = c$. Il est bien clair que $a|c$ comme voulu. ■

**Corollaire (Divisibilité par un produit)** Soient $a, b, n \in \mathbb{Z}$. Si $a|n$, si $b|n$ et si $a$ et $b$ sont premiers entre eux, alors $ab|n$.

✖ ✖ ✖ **Attention !** Il est impératif de supposer ici $a$ et $b$ premiers entre eux. Par exemple, pour $a = b = n = 2$, $a$ et $b$ divisent $n$ mais $ab$ ne divise pas $n$.

**Démonstration** Comme $a|n$, il existe $k \in \mathbb{Z}$ tel que $n = ak$. Mais $b|n$ donc $b|ak$. Or $a$ et $b$ sont premiers entre eux. Le théorème de Gauss a donc pour conséquence que $b|k$. Finalement $ab|ak = n$ comme voulu. ■

**Corollaire (Forme irréductible d'un nombre rationnel)** Soit $r \in \mathbb{Q}$. Il existe un unique couple $(p, q) \in \mathbb{Z} \times \mathbb{N}^*$ tel que $r = \frac{p}{q}$ et tel que $p$ et $q$ soient premiers entre eux. Cette écriture $r = \frac{p}{q}$ est appelée la *forme irréductible de* $r$.

🐰 🐰 🐰 **Explication** Une fraction d'entiers est irréductible quand plus aucune simplification n'est possible entre le numérateur et le dénominateur, sauf par $\pm 1$.

**Démonstration**

- Commençons par l'unicité du couple $(p, q)$. Soient donc $(p, q), (p', q') \in \mathbb{Z} \times \mathbb{N}^*$. On suppose que $r = \frac{p}{q} = \frac{p'}{q'}$ et que $p$ et $q$ d'une part, $p'$ et $q'$ d'autre part sont premiers entre eux.
  On a donc $pq' = p'q$. En particulier $q|pq'$. Or $p$ et $q$ sont premiers entre eux, donc d'après le théorème de Gauss, $q|q'$. Par symétrie, $q'|q$, et donc $|q| = |q'|$. Mais $q$ et $q'$ sont positifs ou nuls, donc $q = q'$. Comme par ailleurs $q$ et $q'$ sont non nuls, on peut diviser l'égalité $pq' = p'q$ par $q = q'$ et du coup $p = p'$ comme voulu.
- Et l'existence à présent ? Ce qu'on sait par définition de $r$, c'est qu'il existe deux entiers $a$ et $b$, $b \neq 0$, tels que $r = \frac{a}{b}$. On peut toujours supposer que $b$ est positif. Notant $d$ le PGCD de $a$ et $b$, nous pouvons alors écrire $a = dp$ et $b = dq$ pour deux entiers $p \in \mathbb{Z}$ et $q \in \mathbb{N}^*$. Tout va bien : nous savons que $p$ et $q$ sont premiers entre eux, et d'autre part $r = \frac{a}{b} = \frac{dp}{dq} = \frac{p}{q}$. ■

## 2.3 PPCM

**Définition (PPCM)** Soient $a, b \in \mathbb{Z}$. On appelle *plus petit commun multiple* (PPCM) *de $a$ et $b$* tout entier $m \in \mathbb{Z}$ tel que :

- $m$ est un multiple commun de $a$ et $b$ : $a|m$ et $b|m$ ;
- $m$ est un diviseur de tout multiple commun de $a$ et $b$ : $\forall \mu \in \mathbb{Z}, \quad \Big(a|\mu \text{ et } b|\mu\Big) \implies m|\mu$.

✌ ✌ ✌ **Explication** Dans le cas où $a$ et $b$ sont des entiers naturels, on demande ici deux choses à $m$ : 1) de majorer l'ensemble $\Big\{a, b\Big\}$ au sens de la relation d'ordre de divisibilité ; et 2) d'être plus petit pour cette relation que tout autre majorant de $\Big\{a, b\Big\}$. D'où l'idée que l'on définit bien là, au sens des relations d'ordre, le plus petit élément de l'ensemble des majorants de $\Big\{a, b\Big\}$, i.e. le *plus petit multiple commun de $a$ et $b$*, ou encore la borne supérieure de l'ensemble $\Big\{a, b\Big\}$.

Un PPCM de deux entiers existe-t-il toujours ? Si oui, est-il unique ? Le théorème suivant répond à ces questions.

**Théorème (Existence et « unicité » du PPCM)** Soient $a, b \in \mathbb{Z}$. Il existe un et un seul PPCM **positif** de $a$ et $b$. Ce PPCM est noté $\text{PPCM}(a, b)$ ou $a \vee b$ et appelé **le** PPCM *de $a$ et $b$*. Le seul autre PPCM de $a$ et $b$ est alors $-\text{PPCM}(a, b)$.

On a l'égalité : $$|ab| = \text{PGCD}(a, b)\ \text{PPCM}(a, b).$$

✌ ✌ ✌ **Explication** On dira ainsi que $-18$ est **un** PPCM de 6 et 9, mais, au choix, que 18 est (**un** ou) **le** PPCM de 6 et 9.

**Démonstration**

- L'« unicité » du PPCM se démontre comme dans le cas des PGCD.
- Si $a$ ou $b$ est nul, comme 0 est le seul multiple de 0, $a$ et $b$ possèdent un PPCM unique, à savoir 0.
- Supposons désormais que $a \neq 0$ et que $b \neq 0$ et posons $d = \text{PGCD}(a, b) \neq 0$. Nous allons montrer que $\dfrac{ab}{d}$ est un PPCM de $a$ et $b$. Cela prouvera d'un coup d'un seul l'existence d'un PPCM de $a$ et $b$ et la formule $|ab| = \text{PGCD}(a, b)\ \text{PPCM}(a, b)$.

  D'abord, $a = da'$ et $b = db'$ pour certains $a', b' \in \mathbb{Z}$ premiers entre eux. Ensuite $\dfrac{ab}{d} = ba' = ab'$.

  1) Montrons que $\dfrac{ab}{d}$ est un multiple commun de $a$ et $b$. Facile : $a\Big|ab' = \dfrac{ab}{d}$ et $b\Big|ba' = \dfrac{ab}{d}$.

  2) Montrons que $\dfrac{ab}{d}$ est un diviseur de tout multiple commun de $a$ et $b$. Soit $m$ un multiple commun de $a$ et $b$. Alors $m = au = bv$ pour certains $u, v \in \mathbb{Z}$, donc $ua' = vb'$ après division par $d$, donc $a'|vb'$. Or $a'$ et $b'$ sont premiers entre eux, donc en vertu du théorème de Gauss, $a'|v$. Bref, $v = a'k$ pour un certain $k \in \mathbb{Z}$. Concluons : $m = bv = ba'k = k\ \dfrac{ab}{d}$, donc en effet $\dfrac{ab}{d}\Big|m$. ■

✎ ✎ ✎ **En pratique** La formule « $|ab| = \text{PGCD}(a, b)\text{PPCM}(a, b)$ » permet de calculer un PPCM à partir d'un PGCD, d'après l'algorithme d'Euclide. Partant de $a$ et $b$, on détermine $\text{PGCD}(a, b)$ à l'aide de l'algorithme d'Euclide et on en déduit $\text{PPCM}(a, b)$.

**Exemple** Nous avons déjà montré que $\text{PGCD}(1542, 58) = 2$. Du coup $\text{PPCM}(1542, 58) = \dfrac{1542 \times 58}{2} = 44718$.

Pour la démonstration du théorème suivant, vous vous inspirerez de la démonstration donnée dans le cas analogue des PGCD.

**Théorème (Propriétés du PPCM)** Soient $a, b \in \mathbb{Z}$.

(i) Pour tout $k \in \mathbb{Z}$ : $\text{PPCM}(ak, bk) = |k|\text{PPCM}(a, b)$.

(ii) Pour tout diviseur commun $d \neq 0$ de $a$ et $b$ : $\text{PPCM}\left(\dfrac{a}{d}, \dfrac{b}{d}\right) = \dfrac{\text{PPCM}(a, b)}{|d|}$.

# 3 Nombres premiers

**Définition (Nombre premier, nombre composé)** Soit $p \in \mathbb{N}$. On dit que $p$ est *premier* si $p \neq 1$ et si les seuls diviseurs positifs de $p$ sont 1 et $p$. On dit que $p$ est *composé* si $p \neq 1$ et si $p$ n'est pas premier.

L'ensemble des nombres premiers est parfois noté $\mathbb{P}$.

**Exemple** Il n'est pas inutile de connaître la liste des premiers nombres premiers : 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37...

**Lemme** Soient $r \in \mathbb{N}^*$, $p_1, p_2, \dots, p_r$ des nombres premiers distincts et $\alpha_1, \alpha_2, \dots, \alpha_r$ des entiers naturels non nuls. Alors tout diviseur premier de $p_1^{\alpha_1} p_2^{\alpha_2} \dots p_r^{\alpha_r}$ est l'un des $p_i$, $i \in [\![1, r]\!]$.

**Démonstration** Notons $\mathcal{D}$ l'ensemble des entiers de la forme $p_1^{\alpha_1} p_2^{\alpha_2} \dots p_r^{\alpha_r}$ — comme dans le lemme — dont au moins un diviseur premier n'est pas l'un des $p_i$, $i \in [\![1, r]\!]$. Nous voulons montrer que $\mathcal{D}$ est vide.
Raisonnons par l'absurde en supposant $\mathcal{D}$ non vide. Alors $\mathcal{D}$ est une partie non vide de $\mathbb{N}$ et possède donc un plus petit élément $p_1^{\alpha_1} p_2^{\alpha_2} \dots p_r^{\alpha_r}$ dont un certain diviseur premier $p$ n'est aucun des $p_i$, $i \in [\![1, r]\!]$.
Par hypothèse $p | p_1(p_1^{\alpha_1 - 1} p_2^{\alpha_2} \dots p_r^{\alpha_r})$, et par ailleurs $p$ et $p_1$, en tant que nombres premiers distincts, sont premiers entre eux, donc d'après le théorème de Gauss, $p | p_1^{\alpha_1 - 1} p_2^{\alpha_2} \dots p_r^{\alpha_r}$. Or $p_1^{\alpha_1 - 1} p_2^{\alpha_2} \dots p_r^{\alpha_r}$ n'est pas un élément de $\mathcal{D}$ car $p_1^{\alpha_1} p_2^{\alpha_2} \dots p_r^{\alpha_r}$ en est par définition le plus petit. Par conséquent, puisque $p | p_1^{\alpha_1 - 1} p_2^{\alpha_2} \dots p_r^{\alpha_r}$, $p$ est l'un des $p_i$, $i \in [\![1, r]\!]$, ce qui est contradictoire et nous permet d'affirmer que $\mathcal{D} = \varnothing$. ■

Le théorème suivant est parfois appelé le *théorème fondamental de l'arithmétique*.

**Théorème (Existence et unicité de la décomposition en produit de facteurs premiers)**

• Pour tout $n \geqslant 2$, il existe un unique entier $r \in \mathbb{N}^*$, une unique famille $(p_1, p_2, \dots, p_r)$ de nombres premiers rangés dans l'ordre $p_1 < p_2 < \dots < p_r$ et une unique famille $(\alpha_1, \alpha_2, \dots, \alpha_r)$ d'entiers naturels non nuls tels que :

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

Les entiers $p_1, p_2, \dots, p_r$ sont tous les nombres premiers qui divisent $n$. Pour tout $i \in [\![1, r]\!]$, $p_i^{\alpha_i}$ est la plus grande puissance de $p_i$ qui divise $n$ et $\alpha_i$ est appelé l'*ordre de multiplicité de $p_i$ dans $n$*.

Par convention, on considère que l'entier 1 possède lui aussi une et une seule décomposition de ce genre, avec $r = 0$ — bref, 1 est le « produit de zéro nombre premier ».

• Ce résultat gagne parfois à être énoncé sous la forme suivante : pour tout $n \in \mathbb{N}^*$, il existe une unique famille $(\nu_p)_{p \in \mathbb{P}}$ d'entiers naturels *presque tous nuls*, i.e. dont tous les éléments sont nuls sauf un nombre fini d'entre eux, telle que :

$$n = \prod_{p \in \mathbb{P}} p^{\nu_p}.$$

✌ ✌ ✌ **Explication** Dans la deuxième formulation du théorème, le produit $\prod_{p \in \mathbb{P}} p^{\nu_p}$ est **fini**. Rien à voir avec un produit infini puisque la famille $(\nu_p)_{p \in \mathbb{P}}$ est « presque nulle ».

**Démonstration** Le programme stipule que vous n'êtes pas obligés de savoir refaire cette démonstration. Je vous conseille néanmoins de la travailler.

• **Existence :** Par récurrence sur $n$.

1) **Initialisation :** 1 n'est divisible par aucun nombre premier, c'est le produit de zéro d'entre eux.

2) **Hérédité :** Soit $n \geqslant 2$. Faisons l'hypothèse que tout entier supérieur ou égal à 2 mais strictement inférieur à $n$ peut est un produit de nombres premiers. Qu'en est-il de $n$ ? Deux cas possibles : soit $n$ est premier, soit $n$ est composé. Si $n$ est premier, c'est terminé, il est produit de nombres premiers. Supposons-le donc composé. Il s'écrit donc $n = ab$ où $a$ et $b$ sont deux diviseurs positifs de $n$ autres que 1 et $n$. Notre hypothèse de récurrence indique alors que $a$ et $b$ sont des produits de nombres premiers. A fortiori c'est aussi le cas de $n$ par produit.

- **Unicité :** Egalement par récurrence sur $n$.

  1) **Initialisation :** 1 n'est divisible par aucun nombre premier, donc sa décomposition en produit de (zéro) nombres premiers est unique !

  2) **Hérédité :** Soit $n \geqslant 2$. Faisons l'hypothèse que tout entier supérieur ou égal à 2 mais strictement inférieur à $n$ se décompose d'une unique façon en un produit de nombres premiers. Qu'en est-il de $n$ ? Soient $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_r^{\alpha_r} = q_1^{\beta_1} q_2^{\beta_2} \dots q_s^{\beta_s}$ deux décompositions de $n$ en nombres premiers — notations évidentes. Alors d'après le lemme établi juste avant, $q_1 = p_i$ pour un certain $i \in [\![1, r]\!]$ et $p_1 = q_j$ pour un certain $j \in [\![1, s]\!]$. Du coup $p_1 = q_j \geqslant q_1 = p_i \geqslant p_1$, et donc $p_1 = q_1$.
  Dans ces conditions, $\dfrac{n}{p_1} = p_1^{\alpha_1 - 1} p_2^{\alpha_2} \dots p_r^{\alpha_r} = q_1^{\beta_1 - 1} q_2^{\beta_2} \dots q_s^{\beta_s}$. Or $\dfrac{n}{p_1}$ possède une unique décomposition en produit de nombres premiers par hypothèse de récurrence. On en déduit que $r = s$ et que $p_i = q_i$ et $\alpha_i = \beta_i$ pour tout $i \in [\![1, r]\!]$. Ainsi nos deux décompositions sont égales, c'est l'unicité cherchée. ■

**Théorème (Infinité de l'ensemble des nombres premiers)** L'ensemble $\mathbb{P}$ des nombres premiers est infini.

**Démonstration** Raisonnons par l'absurde en supposant $\mathbb{P}$ fini. Notons dans ce cas $p_1, p_2, \dots, p_r$ la liste **complète** des nombres premiers et posons $N = p_1 p_2 \dots p_r + 1$. Alors $N \in \mathbb{N}$, $N \geqslant 2$, et donc $N$ peut être décomposé en produit de facteurs premiers en vertu du théorème fondamental de l'arithmétique. Soit $p_k$ un tel diviseur premier de $N$, où $k \in [\![1, r]\!]$. Alors $N \equiv 0 \mod p_k$. Or par définition de $N$, $N \equiv 1 \mod p_k$, donc finalement $1 \equiv 0 \mod p_k$ — contradiction. ■

**Théorème (PGCD, PPCM et nombres premiers)** Soient $a, b \in \mathbb{N}^*$. Nous savons qu'il existe deux familles uniques $(\nu_p)_{p\in\mathbb{P}}$ et $(\mu_p)_{p\in\mathbb{P}}$ telles que $a = \prod_{p\in\mathbb{P}} p^{\mu_p}$ et $b = \prod_{p\in\mathbb{P}} p^{\nu_p}$.
Alors : $\quad \mathrm{PGCD}(a,b) = \prod_{p\in\mathbb{P}} p^{\min(\mu_p,\nu_p)} \quad$ et $\quad \mathrm{PPCM}(a,b) = \prod_{p\in\mathbb{P}} p^{\max(\mu_p,\nu_p)}$.

✎ ✎ ✎ **En pratique** Quand on connaît la décomposition en facteurs premiers de $a$ et $b$, on peut donc déterminer $\mathrm{PGCD}(a,b)$ et $\mathrm{PPCM}(a,b)$ sans utiliser l'algorithme de Bézout. La limite de cette méthode, c'est qu'il peut être **très long** de déterminer la décomposition d'un entier en produit de nombres premiers. Pour les grands nombres, l'algorithme de Bézout est nettement plus utilisable.

**Démonstration** Contentons-nous de traiter le cas des PGCD. Posons $d = \prod_{p\in\mathbb{P}} p^{\min(\mu_p,\nu_p)}$.

On a : $\quad \mathrm{PGCD}(a,b) = \mathrm{PGCD}\left(d \times \dfrac{a}{d}, d \times \dfrac{b}{d}\right) = |d|\ \mathrm{PGCD}\left(\dfrac{a}{d}, \dfrac{b}{d}\right) = \prod_{p\in\mathbb{P}} p^{\min(\mu_p,\nu_p)} \times \mathrm{PGCD}\left(\dfrac{a}{d}, \dfrac{b}{d}\right)$.

Il ne nous reste plus qu'à montrer que $\mathrm{PGCD}\left(\dfrac{a}{d}, \dfrac{b}{d}\right) = 1$, i.e. que $\dfrac{a}{d}$ et $\dfrac{b}{d}$ sont premiers entre eux.

Soit $\delta$ un diviseur commun positif de $\dfrac{a}{d}$ et $\dfrac{b}{d}$. Nous devons montrer que $\delta = 1$. Raisonnons par l'absurde et supposons $\delta \neq 1$. Nous pouvons alors nous donner un diviseur premier $q$ de $\delta$.
Dans ces conditions, puisque $q | \delta$ et $\delta \Big| \dfrac{a}{d} = \prod_{p\in\mathbb{P}} p^{\mu_p - \min(\mu_p,\nu_p)}$, alors $q$ est au moins à la puissance 1 dans ce produit, i.e. $\mu_q - \min(\mu_q, \nu_q) \geqslant 1$. On montre de la même façon que $\nu_q - \min(\mu_q, \nu_q) \geqslant 1$. On a donc $\mu_q \geqslant \min(\mu_q, \nu_q) + 1$ et $\nu_q \geqslant \min(\mu_q, \nu_q) + 1$, donc $\min(\mu_q, \nu_q) \geqslant \min(\mu_q, \nu_q) + 1$ — contradiction.
Conclusion : $\quad \delta = 1$. Les entiers $\dfrac{a}{d}$ et $\dfrac{b}{d}$ sont ainsi bien premiers entre eux, ce qui achève cette preuve. ■

**Exemple** Le PGCD de 600 et 740 est $20 = 2^2 \times 5$ car $600 = 2^3 \times 3 \times 5^2$ et $740 = 2^2 \times 5 \times 37$.