Arithmétique

Cornou Jean-Louis

23 juillet 2025

La notion de nombre est délicate à définir d'un point de vue mathématique. La construction axiomatique des ensembles $\mathbb{N}, \mathbb{Z}, \mathbb{Q}$ dépasse largement le programme. L'arithmétique est présentée de manière élémentaire et ne comporte rien de plus que le programme de maths expertes de Terminale. C'est toutefois l'occasion de retravailler (encore une fois) la théorie des ensembles.

1 Opérations dans $\mathbb{N}$ et $\mathbb{Z}$

L'addition et la multiplication dans $\mathbb{N}$ et $\mathbb{Z}$ vérifient les propriétés suivantes : soit $(a, b, c) \in \mathbb{Z}^3$. Alors

- $(a+b)+c = a+(b+c)$.
- $a+b = b+a$.
- $a+0 = a$.
- $a+(-a) = 0$.
- $(ab)c = a(bc)$.
- $ab = ba$.
- $a1 = a$.
- $a(b+c) = ab+ac$.

Définition 1 *Soit $(a, b) \in \mathbb{Z}^2$. On dit que $a \leq b$ lorsque $\exists n \in \mathbb{N}, a+n = b$.*

Ainsi définie, la relation d'ordre $\leq$ sur $\mathbb{Z}$ vérifie toutes les propriétés que vous connaissez sur $\mathbb{R}$. On rappelle la proprité du bon ordre de $\mathbb{N}$.

Propriété 1 (admis) *Soit* A *une partie non vide de $\mathbb{N}$. Alors* A *possède un minimum. Si* A *est de plus majorée,* A *possède un maximum.*

2 Relation de divisibilité

Définition 2 *Soit $(a, b) \in \mathbb{Z}^2$. On dit que a divise b lorsque :*

$$\exists n \in \mathbb{Z}, b = an$$

Lorsque c'est le cas, on le note $a \mid b$.

Propriété 2 *Soit $(a, b, c) \in \mathbb{Z}^3$. Si a divise b et b divise c, alors a divise c. On dit que la relation de divisibilité est transitive.*

Démonstration. D'après les hypothèses, on dispose de n, m dans $\mathbb{Z}$ tels que $b = an$ et $c = bm$. Donc $c = a(nm)$. Or $nm \in \mathbb{Z}$, donc a divise c.

Propriété 3 *Soit $(a, b) \in \mathbb{Z}^2$. On a l'équivalence*

$$(a \mid b) \wedge (b \mid a) \iff |a| = |b|$$

Dans ce cas, on dit que a et b sont associés.

Démonstration. Supposons que $a \mid b$ et $b \mid a$. On dispose de deux entiers relatifs m et n tels que $b = an$ et $a = bm$. Mais alors $b = bnm$. Si $b \neq 0$, alors $mn = 1$, donc $m = 1$ ou $m = -1$, donc $a = b$ ou $a = -b$. Si $b = 0$, alors $a = 0$ et la conclusion $|a| = |b|$ est encore valide.
Supposons que $|a| = |b|$. Alors $a = b$ ou $a = -b$. Dans le premier cas, l'entier naturel $n = 1$ vérifie $a = nb$ et $b = na$, donc a divise b et b divise a. Dans le deuxième cas, on utilise l'entier relatif -1, ce qui entraîne les mêmes relations de divisibilité.

Définition 3 *Soit $a \in \mathbb{Z}$. L'ensemble de ses diviseurs de a est l'ensemble*

$$\{b \in \mathbb{Z} | b \mid a\} = \{b \in \mathbb{Z} | \exists n \in \mathbb{Z}, a = bn\}$$

Notation
On note cet ensemble D_a ou $D(a)$. L'ensemble des diviseurs positifs de a, $D_a \cap \mathbb{N}$ est noté D_a^+ ou $D^+(a)$. Notation non standardisée.

Exemple 1 $D(4) = \{-4, -2, -1, 1, 2, 4\}$, $D^+(1) = \{1\}$, $D(0) = \mathbb{Z}$.

Propriété 4 *Soit $a \in \mathbb{Z}$, alors $D(a) = D(-a) = D(|a|)$.*

Démonstration. Soit $b \in D(a)$, alors il existe un entier relatif n tel que $a = bn$. Ainsi, $-a = b(-n)$ et $-n$ appartient à $\mathbb{Z}$. Ainsi b divise $-a$ et on a l'inclusion $D(a) \subset D(-a)$. Mais alors, $D(-a) \subset D(-(-a)) = D(a)$. Ainsi, $D(a) = D(-a)$. La seconde égalité s'en déduit par distinction de cas selon le signe de a.

☞ **Remarque**
On l'a compris, l'étude de la relation de divisibilité dans $\mathbb{Z}$ est indépendante du signe des entiers relatifs considérés.

Propriété 5 *Soit $a \in \mathbb{Z}^*$. Alors D_a est fini.*

Démonstration. Soit $a \in \mathbb{Z}^*$. Montrons que $D_a \subset [\![-|a|, |a|]\!]$. Soit $b \in D_a$. Alors il existe un entier relatif n tel que $a = bn$. Or a est non nul. Par conséquent, b et n sont non nuls. En particulier, $|n| \geq 1$. On en déduit que $|b| = |a|/|n| \leq |a|$, donc que $b \in [\![-|a|, |a|]\!]$. Ainsi, D_a est fini car inclus dans l'ensemble fini $[\![-|a|, |a|]\!]$ de cardinal $1 + 2|a|$.

⚠ **Attention**
L'implication $a|b \Rightarrow |a| \leq |b|$ est fausse dès que b est nul, puisque tout le monde divise 0.

Propriété 6 *Soit $(a, b) \in \mathbb{Z}^2$, $n \in \mathbb{Z}$. Alors $D(a) \cap D(b + na) = D(a) \cap D(b)$.*

Démonstration. Soit $d \in D(a) \cap D(b + na)$. Il existe deux entiers relatifs p et q tels que $a = dp$ et $b + na = dq$. On en déduit que $b = dq - na = dq - ndp = d(q - np)$. Or $q - np \in \mathbb{Z}$, donc d divise b. Ainsi, $d \in D(b)$ et on a prouvé l'inclusion $D(a) \cap D(b + na) \subset D(a) \cap D(b)$. Comme $-n$ appartient à $\mathbb{Z}$, ce qui précède appliqué à a , $b + na$ et $-n$ implique $D(a) \cap D(b + na - na) \subset D(a) \cap D(b + na)$, soit $D(a) \cap D(b) \subset D(a) \cap D(b + na)$.

Définition 4 *Soit $(a, b) \in \mathbb{Z}^2$. On dit que a est multiple de b lorsque $b \mid a$, autrement dit lorsqu'il existe un entier relatif n tel que $a = bn$. L'ensemble des multiples de a est l'ensemble $\{b \in \mathbb{Z} | a \mid b\}$.*

Propriété 7 *Soit $a \in \mathbb{Z}$. L'ensemble des multiples de a est l'ensemble $a\mathbb{Z}$. Il est stable par addition et opposé.*

Démonstration. Soit $(b_1, b_2) \in (a\mathbb{Z})^2$. On dispose de n_1, n_2 dans $\mathbb{Z}$ tels que $b_1 = n_1 a$ et $b_2 = n_2 a$. Mais alors $b_1 + b_2 = (n_1 + n_2)a$. Or $n_1 + n_2 \in \mathbb{Z}$, donc $b_1 + b_2 \in a\mathbb{Z}$. De plus $-b_1 = (-n_1)a$ et $-n_1 \in \mathbb{Z}$, donc $-b_1 \in a\mathbb{Z}$.

Propriété 8 *Soit $(a, b) \in \mathbb{Z}^2$. Alors a divise b si et seulement si $b\mathbb{Z} \subset a\mathbb{Z}$ si et seulement si b est multiple de a.*

Démonstration. Supposons que a divise b. Alors il existe un entier relatif n tel que $b = na$. Soit à présent q un élément de $b\mathbb{Z}$, montrons que q appartient à $a\mathbb{Z}$. Comme q appartient à $b\mathbb{Z}$, il existe un entier relatif m tel que $q = bm$. Mais alors, $q = (na)m = (nm)a$. Comme nm appartient à $\mathbb{Z}$, on en déduit que q appartient à $a\mathbb{Z}$. On a ainsi démontré l'inclusion $b\mathbb{Z} \subset a\mathbb{Z}$. Réciproquement, supposons que $b\mathbb{Z} \subset a\mathbb{Z}$ et montrons que a divise b. On remarque pour cela que b appartient à $b\mathbb{Z}$, donc que b appartient à $a\mathbb{Z}$. Alors, il existe un entier relatif n tel que $b = na$. Donc a divise b.

3 La division euclidienne

Théorème 1 (Division euclidienne) *Soit $(a,b) \in \mathbb{Z} \times \mathbb{Z}^*$. Alors*

$$\exists!(q,r) \in \mathbb{Z} \times [\![0, |b|-1]\!], \quad a = bq + r$$

L'entier q est appelé quotient de la division euclidienne de a par b, r est appelé son reste.

⚠ **Attention**
L'entier relatif b est supposé non nul.

Démonstration. Prouvons l'existence tout d'abord dans le cas où $b > 0$. Pour cela, on note $A = \{n \in \mathbb{Z} | nb \leq a\}$. Montrons que A est non vide majorée.

- Si $a \geq 0$, alors $0 \times b = 0 \leq a$, donc $0 \in A$ et A est non vide. Si $a < 0$, alors on multiplie l'inégalité $b \geq 1$ par a strictement négatif, donc $ab \leq a$. Donc $a \in A$ et A est non vide.
- Montrons que A est majoré par $\max(0,a)$. Soit $n \in A$. Si $n \geq 0$, comme $1 \leq b$, alors $n \leq nb \leq a \leq \max(0,a)$. Si $n \leq 0$, a fortiori, $n \leq \max(0,a)$.

Ainsi, la partie A de $\mathbb{Z}$ admet un maximum. Notons-le q et posons $r = a - bq$. Vérifions que le couple (q,r) convient. Il vérifie trivialement l'égalité et $(q,r) \in \mathbb{Z}^2$. Il reste à vérifier que $0 \leq r < b$. Comme q est le maximum de A, q appartient à A, donc $qb \leq a$ soit $0 \leq a - bq$, i.e $0 \leq r$. D'autre part, l'entier relatif $q+1$ n'appartient pas à A, donc $(q+1)b > a$, soit encore $b > a - bq$, i.e $b > r$.
Si l'entier relatif b est strictement négatif, on applique ce qui précède au couple $(a,-b)$. On dispose alors d'entiers relatifs (q',r') tels que $a = (-b)q' + r'$ et $0 \leq r' < -b - 1 = |b| - 1$. Le couple d'entiers relatifs $(-q',r')$ vérifie alors les critères attendus.
Prouvons à présent l'unicité d'un tel couple. Soit (q'',r'') un autre couple satisfaisant cette propriété. Alors $qb + r = q''b + r''$, donc $r - r'' = b(q - q'')$ est un multiple de b. Or on a les encadrements,

$$0 \leq r \leq |b| - 1, \quad -|b| + 1 \leq -r'' \leq 0, \quad \text{donc} \quad -|b| + 1 \leq r - r'' \leq |b| - 1$$

Or $b\mathbb{Z} \cap [\![-(|b|-1), |b|-1]\!] = \{0\}$, donc $r - r'' = 0$, soit $r = r''$. On en déduit que $qb = q''b$. Comme b est non nul, cela entraîne $q = q''$.

Propriété 9 *Soit $(a,b) \in \mathbb{Z} \times \mathbb{Z}^*$. Alors le quotient q et le reste r de la division euclidienne de a par b valent*

$$q = \frac{b}{|b|} \left\lfloor \frac{a}{|b|} \right\rfloor, \quad r = a - |b| \left\lfloor \frac{a}{|b|} \right\rfloor$$

Démonstration. Commençons par traiter le cas $b > 0$ et notons $x = \frac{a}{b}$. Alors les propriétés d'encadrement de la partie entière donnent

$$x - 1 < \lfloor x \rfloor \leq x$$

On en déduit après multiplication par l'entier strictement positif b que

$$a - b < b\lfloor x \rfloor \leq a$$

Ainsi, on a

$$0 \leq a - b\lfloor x \rfloor < b$$

Par conséquent, le couple $(\lfloor x \rfloor, a - b\lfloor x \rfloor)$ vérifie les conditions de la division euclidienne. D'après l'unicité du théorème précédent, on a alors $q = \lfloor x \rfloor$et $r = a - b\lfloor x \rfloor$. Cela correspond aux expressions indiquées dans le cas $b > 0$.
Dans le cas $b < 0$, on effectue la division euclidienne de a par $-b$. D'après ce qui précède, on a $a = (-b)q' + r'$ avec $q' = \lfloor a/(-b) \rfloor$ et $r' = a + bq'$. On vérifie que $0 \leq r' \leq |b| - 1$, alors on identifie $q = -\lfloor a/(-b) \rfloor$ et $r = a + bq'$, ce qui correspond aux expressions indiquées dans le cas $b < 0$.

☞ **Remarque**
On retiendra en pratique que pour tout b strictement positif, $q = \lfloor a/b \rfloor$ et $r = a - b\lfloor a/b \rfloor$. Autrement dit, bq est le plus grand multiple de b inférieur ou égal à a.

Exemple 2 *Division euclidienne de -31 par 7 :*

$$31 = 7 \times 4 + 3, \quad -31 = 7 \times (-5) + 4$$

Division euclidienne de 23 par -5 :

$$23 = 5 \times 4 + 3, \quad 23 = (-5) \times (-4) + 3$$

Division euclidienne de -41 par -11 :

$$41 = 11 \times 3 + 8, \quad -41 = (-11) \times 3 - 8, \quad -41 = (-11) \times 4 + 3$$

⚠ **Attention**
Toute écriture de la forme $a = bq + r$ ne garantit pas que q et r sont le quotient et le reste dans la division euclidienne de a par b. Il faut vérifier que q et r sont entiers puis que $0 \leq r \leq |b| - 1$.

Propriété 10 *Soit $(a, b) \in \mathbb{Z} \times \mathbb{Z}^*$. On a l'équivalence : b divise a si et seulement si le reste de la division euclidienne de a par b est nul.*

Démonstration. Supposons que b divise a. Il existe alors un entier relatif n tel que $a = bn$, soit $a = bn + 0$. Le couple $(n, 0)$ vérifie alors la division euclidienne de a par b, puisque $0 \leq 0 < |b|$. On en déduit par unicité que le reste de la division euclidienne de a par b vaut 0. Réciproquement, si ce reste est nul, alors le quotient q dans cette division euclidienne vérifie $a = bq + 0 = bq$. Comme q appartient à $\mathbb{Z}$, a divise b.

4 PGCD de deux entiers relatifs

Définition 5 *Soit $(a, b) \in \mathbb{Z}^2$. Si $(a, b) \neq (0, 0)$ alors $D(a) \cap D(b)$ est non vide fini et son maximum est appelé plus grand diviseur commun de a et b, noté $a \wedge b$. Si $(a, b) = (0, 0)$, on définit leur plus grand diviseur commun comme 0.*

Exemple 3 *Si $a = 0$ et $b \neq 0$, alors $D^+(a) = \mathbb{N}$, donc $D^+(a) \cap D^+(b) = D^+(b)$. Mais alors $\max(D^+(a) \cap D^+(b)) = \max(D^+(b)) = |b|$.*
Si $b \neq 0$ et a divise b, alors $D^+(a) \subset D^+(b)$ par transitivité de la relation de divisibilité, donc $D^+(a) \cap D^+(b) = D^+(a)$ dont le maximum vaut $|a|$. Dans ce cas, $a \wedge b = |a|$.
Si $(a, b) \neq 0$, alors $1 \in D^+(a) \cap D^+(b)$, donc $a \wedge b \geq 1 > 0$. Par contraposition, si $a \wedge b = 0$, alors $a = 0$ et $b = 0$.

Exemple 4

$$D^+(98) \cap D^+(28) = \{1, 2, 7, 14, 49, 98\} \cap \{1, 2, 4, 7, 14, 28\} = \{1, 2, 7, 14\}$$

On en déduit que $98 \wedge 28 = 14$. On remarque que $D^+(14) = \{1, 2, 7, 14\} = D^+(98) \cap D^+(28)$.

$$D^+(23987) \cap D^+(19196) = \{1, 17, 83, 289, 1411, 23987\} \cap \{1, 2, 4, 4799, 9598, 19196\} = \{1\}$$

On en déduit que $23987 \wedge 19196 = 1$.

Quelques propriétés opératoires sur le pgcd :

Propriété 11 *Soit $(a, b) \in \mathbb{Z}^2$, $n \in \mathbb{Z}$. Alors*

- *$a \wedge b = b \wedge a$.*
- *$a \wedge b = |a| \wedge |b|$.*
- *$a \wedge (b + na) = a \wedge b$.*
- *Si b est non nul, on note r le reste de la division euclidienne de a par b. Alors $a \wedge b = b \wedge r$.*
- *b divise a si et seulement si $a \wedge b = |b|$.*

Démonstration.
- $D^+(a) \cap D^+(b) = D^+(b) \cap D^+(a)$.
- $D^+(a) = D^+(|a|)$.
- D'après ce qui a été vu en 2e partie, $D(a) \cap D(b+na) = D(a) \cap D(b)$. Il reste seulement à traiter le cas $(a, b) = (0, 0)$ ou $(a, b + na) = (0, 0)$.
- Notons q le quotient de la division euclidienne de a par b, de sorte que $a = bq + r$. Alors, comme $q \in \mathbb{Z}$, d'après ce qui précède, $a \wedge b = b \wedge a = b \wedge (a - bq) = b \wedge r$.
- Si b divise a, $a\mathbb{Z} \subset b\mathbb{Z}$ et $a\mathbb{Z} + b\mathbb{Z} = b\mathbb{Z}$, donc $a \wedge b = |b|$. Réciproquement, si $a \wedge b = |b|$, $|b|$ est un diviseur de a, donc b divise a.

✎ **Méthode (L'algorithme d'Euclide)**
Soit $(a, b) \in (\mathbb{N}^*)^2$ et $d = a \wedge b$. On suppose pour simplifier que $a > b$. Si $a = b$, alors $a \wedge b = a$, si $a < b$, on les échange. On définit alors une suite d'entiers naturels $(r_n)_n$ via $r_0 = a$, $r_1 = b$, puis $r_2 = r_0 \% r_1$. Si $r_2 = 0$, on s'arrête et $d = r_1 = b$. Sinon, on pose $r_3 = r_1 \% r_2$. Soit $n \in \mathbb{N}^*$, supposons r_n et r_{n-1} construits. Si

$r_n = 0$, on s'arrête et $d = r_{n-1}$. Sinon, on pose $r_{n+1} = r_{n-1} \% r_n$. Cette définition est légitime puisque r_n est non nul.
Démontrons que la suite ainsi construite est strictement décroissante et qu'elle est finie. Soit n un entier naturel tel que r_n est construit. Si $r_n = 0$, la construction s'arrête. Sinon, $r_{n+1} < r_n$ d'après l'encadrement des restes dans la division euclidienne. Ainsi, la reste $(r_n)_n$ est bien à valeurs dans $\mathbb{N}$, strictement décroissante. Par conséquent, elle s'arrête. Notons N le rang auquel elle s'arrête, i.e l'unique entier non nul N tel que $r_{N+1} = 0$ et montrons que $r_N = d$. D'après la propriété sur les pgcd et la division euclidienne, pour tout entier $n \geq N-1$, $r_n \wedge r_{n-1} = r_{n-1} \wedge r_{n-2}$. On en déduit que

$$a \wedge b = r_0 \wedge r_1 = r_N \wedge r_{N+1} = r_N \wedge 0 = r_N.$$

Exemple 5 *Dans le cas $a = 258$ et $b = 145$, on a*

$$\begin{array}{lll} 258 & = 145 \times 1 & +113 \\ 145 & = 113 \times 1 & +32 \\ 113 & = 32 \times 3 & +17 \\ 32 & = 17 \times 1 & +15 \\ 17 & = 15 \times 1 & +2 \\ 15 & = 2 \times 7 & +1 \\ 2 & = 1 \times 2 & +0 \end{array}$$

Par conséquent, le dernier reste non nul vaut 1, donc $258 \wedge 145 = 1$.

Méthode récursive en Python :

```
def euclide(a,b) :
        r = a % b
        if r == 0 :
                return b
        else :
                return euclide(b,r)
```

Théorème 2 (Relation de Bezout) *Soit $(a,b) \in \mathbb{Z}^2$. Alors*

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

Une telle écriture s'appelle une relation de Bezout.

Démonstration. On propose une méthode algorithmique pour cela, l'algorithme d'Euclide étendu.
Si $a = 0$ ou $b = 0$, il suffit de prendre $u = \pm 1, v = 0$ ou $u = 0, v = \pm 1$. Quitte à changer le signe de a et b, puis à les échanger, on se place dans le cas $(a,b) \in (\mathbb{N}^*)^2$ et $a > b$. On note $r_0 = a$, $r_1 = b$ et on note à chaque étape, tant que le reste précédent est non nul, la division euclidienne $r_{n-1} = q_n r_n + r_{n+1}$. Notons N le rang d'arrêt qui satisfait $r_N = a \wedge b$ et $r_{N+1} = 0$. Nous allons construire une suite $(u_n, v_n)_n$ qui nous fournira un couple (u,v) adapté. On commence par poser $u_0 = 1$ et $v_0 = 0$, de sorte que $au_0 + bv_0 = r_0$. On pose également $u_1 = 0$ et $v_1 = 1$, ce qui vérifie $au_1 + bv_1 = r_1$. On construit alors par récurrence

$$\forall n \in [\![1, N]\!], \quad u_{n+1} = u_{n-1} - q_n u_n, \quad v_{n+1} = v_{n-1} - q_n v_n$$

Montrons alors par récurrence double que

$$\forall n \in [\![1, N]\!], \quad r_{n+1} = au_{n+1} + bv_{n+1}.$$

L'initialisation a bien été établie d'après les définitions de u_0, v_0, u_1, v_1. Soit $n \in [\![1, N-1]\!]$ tel que $r_{n+1} = au_{n+1} + bv_{n+1}$ et $r_n = au_n + bv_n$. Alors, d'après la définition de r_{n+2}, on a

$$r_{n+2} = r_n - q_n r_{n+1} = au_n + bv_n - q_n(au_{n+1} + bv_{n+1}) = a(u_n - q_n u_{n+1}) + b(v_n - q_n v_{n+1}) = au_{n+2} + bv_{n+2}$$

L'égalité est donc héréditaire et valable au rang N, ce qui entraîne

$$a \wedge b = r_N = au_N + bv_N$$

Le couple (u_N, v_N) satisfait donc une relation de Bezout.

Exemple 6 *Reprenons l'exemple $a = 258$ et $b = 145$, $a \wedge b = 1$ et les divsions euclidiennes que l'on a menées.*

$$\begin{array}{lll} 258 & = 145\times 1 & +113 \\ 145 & = 113\times 1 & +32 \\ 113 & = 32\times 3 & +17 \\ 32 & = 17\times 1 & +15 \\ 17 & = 15\times 1 & +2 \\ 15 & = 2\times 7 & +1 \\ 2 & = 1\times 2 & +0 \end{array}$$

On remonte les divisions euclidiennes de sorte à éliminier les quotients à chaque étape.

$$\begin{aligned} 1 &= 15-2\times 7 \\ &= 15-(17-15\times 1)\times 7 \\ &= 8\times 15-7\times 17 \\ &= 8\times(32-17)-7\times 17 \\ &= 8\times 32-17\times 15 \\ &= 8\times 32-(113-32\times 3)\times 15 \\ &= 53\times 32-113\times 15 \\ &= 53\times(145-113)-113\times 15 \\ &= 53\times 145-113\times 68 \\ &= 53\times 145-(258-145)\times 68 \\ &= 258\times(-68)+121\times 145 \end{aligned}$$

Ainsi, $u=-68$ et $v=121$ satisfont $1=au+bv$.

L'application aux résolutions d'équation diophantiennes se fera après avoir traité le lemme de Gauss.
Algorithme en Python de l'algorithme d'Euclide étendu

```
def bezout(a, b):
        s, t, u, v = 1, 0, 0, 1
        while b != 0:
                q = a // b
                a, s, t, b, u, v = b, u, v, a - q * b, s - q * u, t - q * v
        return (a, s, t) if a > 0 else (-a, -s, -t)
```

Théorème 3 *Soit $(a,b)\in\mathbb{Z}^2$. Alors $\mathrm{D}(a)\cap\mathrm{D}(b)=\mathrm{D}(a\wedge b)$. Autrement dit,*

$$\forall d\in\mathbb{Z},[(d\mid a)\ et\ (d\mid b)]\iff d\mid a\wedge b$$

Démonstration. — Soit $d\in\mathrm{D}(a)\cap\mathrm{D}(b)$. Alors on dispose d'entiers relatifs n et m tels que $a=dn$ et $b=dm$. D'après la relation de Bezout précédemment démontrée, on dispose d'entiers relatifs u,v tels que $a\wedge b=au+bv$, donc $a\wedge b=dnu+dmv=d(nu+mv)$. Comme $nu+mv\in\mathbb{Z}$, d divise $a\wedge b$, i.e $d\in\mathrm{D}(a\wedge b)$.

— Soit $d\in\mathrm{D}(a\wedge b)$. Comme $a\wedge b$ divise a, d divise a par transiviité. De même, $a\wedge b$ divise b, donc d divise b. Ainsi, $d\in\mathrm{D}(a)\cap\mathrm{D}(b)$.

Cette double inclusion prouve l'égalité.

☞ **Remarque**

Il ne suffit pas à un entier δ de diviser a et b pour être le pgcd de a et b. Cela indique uniquement que δ divise $a\wedge b$. 3 divise 36 et 24, mais $36\wedge 24=12$. On a uniquement $3|12$.

Théorème 4 *Soit $(a,b)\in\mathbb{Z}^2$. Alors $a\mathbb{Z}+b\mathbb{Z}=(a\wedge b)\mathbb{Z}$.*

Démonstration. Soit $n\in a\mathbb{Z}+b\mathbb{Z}$. Il existe p,q dans $\mathbb{Z}$ tel que $n=ap+bq$. Or on dispose de s,t dans $\mathbb{Z}$ tels que $a=(a\wedge b)s$ et $b=(a\wedge b)t$. Donc $n=(a\wedge b)(ps+qt)$, i.e $n\in(a\wedge b)\mathbb{Z}$.
Soit $n\in(a\wedge b)\mathbb{Z}$. Il existe m dans $\mathbb{Z}$ tel que $n=(a\wedge b)m$. Or d'après Bezout, il existe u,v dans $\mathbb{Z}$ tels que $a\wedge b=au+bv$. Donc $n=a(um)+b(vm)\in a\mathbb{Z}+b\mathbb{Z}$.

Propriété 12 (Réduction) *Soit $(a,b)\in\mathbb{Z}^2$. On note $d=a\wedge b$ leur pgcd. Alors*

$$\exists(a',b')\in\mathbb{Z}^2,\quad a=da',\quad b=db',\quad a'\wedge b'=1$$

Démonstration. On traite à part le cas particulier $d = 0$, qui implique nécessairement $a = b = 0$, auquel cas on choisit $a' = b' = 1$. Supposons à présent d non nul, ce qui revient à dire qu'au moins un des deux entiers relatifs a et b est non nul. On a l'égalité $a = a \times 1 + b \times 0$, donc $a \in a\mathbb{Z} + b\mathbb{Z}$. D'après la propriété précédente du pgcd, $a \in d\mathbb{Z}$. On en déduit qu'il existe un entier relatif a' tel que $a = da'$ (autrement dit, d divise a). De même $b = a \times 0 + b \times 1$ amène à $b \in a\mathbb{Z} + b\mathbb{Z} = d\mathbb{Z}$, dont on déduit l'existence de $b' \in \mathbb{Z}$ tel que $b = db'$. Il reste à montrer que le pgcd de a' et b' vaut 1. On remarque alors que $d \in d\mathbb{Z} = a\mathbb{Z} + b\mathbb{Z}$, donc qu'on dispose d'entiers relatifs u, v tels que $d = au + bv = d(a'u + b'v)$. Comme d est non nul, on en déduit $a'u + b'v = 1$, mais alors $1 \in a'\mathbb{Z} + b'\mathbb{Z} = (a' \wedge b')\mathbb{Z}$ est un multiple de $a' \wedge b'$, donc $a' \wedge b' = 1$.

Exemple 7 *Dans le calcul précédent du pgcd de* 98 *et* 28*, on a* $98 = 14 \times 7$ *et* $28 = 14 \times 2$*. On vérifie bien que* $D^+(7) \cap D^+(2) = \{1, 7\} \cap \{1, 2\} = \{1\}$*, donc que* $7 \wedge 2 = 1$*.*

Exercice 1 *Quels sont les entiers naturels non nuls* x, y *tels que* $x \wedge y = 18$ *et* $x + y = 360$ *?*

Exercice 1 *Phase d'analyse : soit* $(x, y) \in (\mathbb{N}^*)^2$ *tel que* $x \wedge y = 18$ *et* $x + y = 360$*. Il existe alors* $(x', y') \in (\mathbb{N}^*)^2$ *tel que* $x = 18x'$*,* $y = 18y'$ *et* $x' \wedge y' = 1$*. La seconde égalité devient alors* $18(x' + y') = 360$*, soit encore* $x' + y' = 20$*. Alors* x' *et* y' *ont même parité puisque leur somme est paire. Comme* $x' \wedge y' = 1$*,* x' *et* y' *ne peuvent être pairs. Il reste à examiner toutes les autres possibilités. On établit alors le tableau*

x'	y'	$x' \wedge y'$
1	19	1
3	17	1
5	15	5
7	13	1
9	11	1

que l'on complète par symétrie. On constate qu'à part les couples $(5, 15)$ *et* $(15, 5)$*, tous les autres couples vérifient* $x' \wedge y' = 1$*.*
Phase de synthèse : On vérifie que les couples

$$(18, 342), (54, 306), (126, 234)\ (162, 198), (198, 162), (234, 126), (306, 54), (342, 18)$$

sont solutions, donc que ce sont les seules.

Propriété 13 (Homogénéité positive du pgcd) *Soit* $(a, b) \in \mathbb{Z}^2$*,* $k \in \mathbb{Z}$*. Alors*

$$(ka) \wedge (kb) = |k|(a \wedge b)$$

Démonstration. Laissée à titre d'exercice.

Théorème 5 (Théorème de Bezout) *Soit* $(a, b) \in \mathbb{Z}^2$*. Alors*

$$a \wedge b = 1 \iff \exists (u, v) \in \mathbb{Z}^2, 1 = au + bv$$

Dans ce cas, on dit que a et b sont ***premiers entre eux.***

Démonstration. Le sens direct a été prouvé dans le théorème précédent. Supposons à présent qu'il existe des entiers relatifs u, v tels que $au + bv = 1$. Alors d'après la définition du pgcd, 1 appartient à $a\mathbb{Z} + b\mathbb{Z} = (a \wedge b)\mathbb{Z}$. Donc $a \wedge b$ divise 1 et est positif, donc $a \wedge b = 1$.

5 PPCM de deux entiers relatifs

Définition 6 *Soit* $(a, b) \in (\mathbb{Z}\backslash\{0\})^2$*. Le minimum de* $a\mathbb{Z} \cap b\mathbb{Z} \cap \mathbb{N}^*$ *est appelé plus petit commun multiple de a et b, abrégé en ppcm de a et b, noté* $a \vee b$*. Dans le cas où* $a = 0$ *ou* $b = 0$*, on convient que* $a \vee b = 0$*.*

☞ **Remarque**
$a\mathbb{Z} \cap b\mathbb{Z} \cap \mathbb{N}^*$ *est bien non vide car il contient* $|ab|$ *puisque a et b sont tous deux non nuls dans le premier cas. Cela justifier l'existence du minimum de cet ensemble.*

Notation
On rencontre les notations $ppcm(a, b)$ *ou encore* $lcm(a, b)$*.*

Exemple 8 *$a \vee b \neq 0 \Rightarrow ab \neq 0$. Si $a = b$, alors $a \vee b = |a|$. Si a divise b, alors $b\mathbb{Z} \subset a\mathbb{Z}$, donc $a\mathbb{Z} \cap b\mathbb{Z} = b\mathbb{Z}$, puis $a \vee b = |b|$.*

Théorème 6 *Soit $(a, b) \in \mathbb{Z}^2$, alors $a\mathbb{Z} \cap b\mathbb{Z} = (a \vee b)\mathbb{Z}$*

Démonstration. Il s'agit de distinctions de signes et de transitivité de la relation de divisibilité.

Propriété 14 *Soit $(a, b) \in \mathbb{Z}^2$, $m \in \mathbb{Z}$. On a l'équivalence*

$$[(a \mid m) \text{ et } (b \mid m)] \iff (a \vee b) \mid m$$

Autrement dit, le ppcm de a et b est le plus petit, au sens de la relation de divisibilité dans $\mathbb{N}$, multiple commun à a et b. On peut encore énoncer l'équivalence sous la forme : m est multiple commun de a et b si et seulement si il est multiple de $a \vee b$.

Démonstration. Cette équivalence n'est rien d'autre que l'égalité d'ensembles $a\mathbb{Z} \cap b\mathbb{Z} = (a \vee b)\mathbb{Z}$.

Propriété 15 *Soit $(a, b, n) \in \mathbb{Z}^3$.*

- *$a \vee b = b \vee a$.*
- *$a \vee b = |a| \vee |b|$.*
- *a divise b si et seulement si $a \vee b = |b|$.*

Démonstration. Laissée à titre d'exercice.

Propriété 16 (Homogénéité positive du ppcm) *Soit $(a, b, k) \in \mathbb{Z}^3$. Alors*

$$(ka) \vee (kb) = |k|(a \vee b)$$

Démonstration. Laissée à titre d'exercice

6 Entiers relatifs premiers entre eux

Définition 7 *Soit $(a, b) \in \mathbb{Z}^2$. On dit que a et b sont premiers entre eux lorsque $a \wedge b = 1$*

⚠ **Attention**
Ne pas confondre avec la notion d'entier premier tout court. Certains textes anglophones utilisent le mot « copremiers ».

On rappelle le résultat essentiel sur les entiers premiers : le théorème de Bezout.

Théorème 7 *Soit $(a, b) \in \mathbb{Z}^2$. a et b sont premiers entre eux si et seulement si*

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

Examinons à présent les conséquences de la relation de primalité entre deux entiers.

Propriété 17 (Lemme de Gauss) *Soit $(a, b, c) \in \mathbb{Z}^3$. On suppose que a divise bc et que a est premier avec b. Alors a divise c.*

Démonstration. Notons $n \in \mathbb{Z}$ tel que $na = bc$ et $(u, v) \in \mathbb{Z}^2$ tel que $au + bv = 1$. On déduit par la multiplication par c de la relation de Bezout que $auc + bvc = c$, donc $auc + vna = c$. On l'écrit sous la forme $a(uc + vn) = c$. L'entier relatif $k = uc + vn$ assure alors que a divise c.

Propriété 18 *Soit $(a, b) \in \mathbb{Z}^2$. Alors $(a \wedge b)(a \vee b) = |ab|$.*

☞ **Remarque**
Cette formule est parfois appelée formule des compléments.

Démonstration. Si a ou b est nul, on vérifie $0 = 0$. Sinon, on commence par traiter le cas où $a \wedge b = 1$. Soit alors x un multiple commun à a et b, on dispose d'entiers relatifs l et k tels que $x = al = bk$. Mais alors, a divise bk et est premier avec b. D'après le lemme de Gauss, a divise k, donc on dispose d'un entier relatif s tel que $k = as$. On en déduit que $x = bas$, donc que ba divise x. Par conséquent, tout multiple commun à a et b est divisible par ab. Comme ab est clairement un multiple commun à ab, on en déduit que $a \vee b = |ab|$.
Traitons à présent le cas général : Si $a \wedge b = d$ est non nul, on réduit la chose sous la forme $a = da'$, $b = db'$ et $a' \wedge b' = 1$. D'après ce qui précède, $a' \vee b' = |a'b'|$. Après multiplication par d^2, on obtient $dd(a' \vee b') = |ab|$. On utilise ensuite l'homogénéité du ppcm, ce qui donne $d[(da') \vee (db')] = (a \wedge b)(a \vee b) = |ab|$.

Exercice 2 *Déterminer tous les couples d'entiers relatifs (a, b) tels que $(a \wedge b)^2 = a \vee b$.*

Application 1 (Résolution d'équations diophantiennes) *Soit $(a, b, c) \in (\mathbb{Z}^*)^2 \times \mathbb{Z}$. On cherche à résoudre l'équation diophantienne $au + bv = c$ d'inconnues $(u, v) \in \mathbb{Z}^2$, i.e à déterminer l'ensemble*

$$\{(u, v) \in \mathbb{Z}^2 | au + bv = c\}$$

- *Si $a \wedge b$ ne divise pas c, alors cette ensemble est vide. Il n'y a pas de solutions à cette équation.*
- *Si $a \wedge b$ divise c, cet ensemble est non vide. On note (u_0, v_0) une solution particulière. L'ensemble des solutions est alors*
$$\{(\frac{b}{a \wedge b}k + u_0, -\frac{a}{a \wedge b}k + v_0) | k \in \mathbb{Z}\}$$

Démonstration. Notons $d = a \wedge b$. D'après la caractérisation algébrique du pgcd, $a\mathbb{Z} + b\mathbb{Z} = d\mathbb{Z}$. Par conséquent, si $c \notin d\mathbb{Z}$, i.e d ne divise pas c, $c \notin a\mathbb{Z} + b\mathbb{Z}$, donc cette équation diophantienne ne possède pas de solutions. Supposons à présent que d divise c, i.e $c \in d\mathbb{Z}$. On sait alors que cette équation possède des solutions via la relation de Bezout. On note a', b' des entiers relatifs tels que $a = da'$ et $b = db'$ et $a' \wedge b' = 1$. Soit $(u, v) \in \mathbb{Z}^2$, et notons (u_0, v_0) une solution particulière de cette équation, alors puisque d est non nul, on a les équivalences

$$au+bv = c \iff au+bv = au_0+bv_0 \iff a(u-u_0) = -b(v-v_0) \iff a'd(u-u_0) = -b'd(v-v_0) \iff a'(u-u_0) = -b'(v-v_0)$$

Soit (u, v) une solution, alors a' divise $b'(v - v_0)$. Comme $a' \wedge b' = 1$, le lemme de Gauss entraîne que a' divise $v - v_0$. On note alors k un entier $(v - v_0) = -ka'$. Cela entraîne $a'(u - u_0) = b'ka'$, donc $u - u_0 = b'k$. On a alors $(u, v) = (u_0 + b'k, v_0 - ka') = (u_0 + k\frac{b}{a \wedge b}, v_0 - k\frac{a}{a \wedge b})$.
Réciproquement, pour tout $k \in \mathbb{Z}$,

$$a(u_0 + k\frac{b}{a \wedge b}) + b(v_0 - k\frac{a}{a \wedge b}) = au_0 + bv_0 = c$$

Propriété 19 *Soit $r \in \mathbb{Q}$. Alors*

$$\exists!(p, q) \in \mathbb{Z} \times \mathbb{N}^*, p \wedge q = 1, r = \frac{p}{q}$$

Cette écriture s'appelle la forme irréductible du rationnel r.

Démonstration. Soit $(p', q') \in \mathbb{Z} \times \mathbb{Z}^*$ tel que $r = p'/q'$. Alors, en notant $d = p' \wedge q'$, $\exists (p, q) \in \mathbb{Z} \times \mathbb{Z}^*, p' = dp, q' = dq, p \wedge q = 1$. Notons que d est non nul, puisque q' est non nul, on a alors $r = (dp)/(dq) = p/q = (-p)/(-q)$. Alors q ou $-q$ appartient à $\mathbb{N}^*$, ce qui garantit l'existence d'un tel couple. Soit p'', q'' un couple vérifiant toutes ces propriétés. Alors $p''q = pq''$, donc q divise pq''. Or q est premier avec p, donc d'après le lemme de Gauss, q divise q''. De manière symétrique, on obtient que q'' divise q, donc que q et q'' sont associés. Comme ils sont tous deux strictement positifs, ils sont égaux. Par conséquent, $p = p''$ et l'unicité est prouvée.

Propriété 20 *Soit $(a, b, n) \in \mathbb{Z}^3$. On suppose que $a \wedge b = 1$, a divise n et b divise n. Alors ab divise n.*

Démonstration. Notons a', b' des entiers relatifs tels que $n = aa' = bb'$. Alors b divise aa'. Comme b est premier avec a, le lemme de Gauss entraîne que b divise a'. On note alors a'' un entier relatif tel que $a' = a''b$. Cela entraîne $n = aba''$, donc ab divise n.

Propriété 21 *Soit $(a, b, n) \in \mathbb{Z}^2$. On suppose que $a \wedge n = 1$ et $b \wedge n = 1$. Alors $(ab) \wedge n = 1$.*

Démonstration. On note u, v, u', v' des entiers relatifs tels que $au + nv = 1$ et $bu' + nv' = 1$. Alors

$$(au)(bu') = (1 - nv)(1 - nv') = 1 - n(v + v' - nvv')$$

Par conséquent, on dispose de la relation de Bezout, $(ab)uu' + n(v + v' - nvv') = 1$. D'après le théorème de Bezout, cela suffit à établir que ab est premier avec n.

7 Entiers premiers et factorisations

Définition 8 *Soit $p \in \mathbb{Z}$. On dit que p est premier lorsque $|\mathrm{D}^+(p)| = 2$.*

Exemple 9 *1 n'est pas premier, la liste des premiers entiers premiers positifs est*

$$2,3,5,7,11,13,17,19,23,29,31,37,41,43,47,53,59,61,67,71,73,79,83,89,97,101,103,107,109,113,$$

$$127,131,137,139,149,151,157,163,167,173,179,181,191,193,197,199,211,223,227,229,233,239,\ldots$$

L'un des grands défis de l'arithmétique est de comprendre la répartition de ces nombres.

☞ **Remarque**
Les entiers premiers sont également dit irréductibles pour la relation de divisibilité. On ne peut pas les factoriser en produit non trivial (i.e autre que $1 \times p$).

Propriété 22 *Soit $n \in \mathbb{Z}\backslash\{-1,0,1\}$. Alors, $\min(\mathrm{D}^+(n)\backslash\{1\})$ est premier. En particulier, n admet un diviseur premier.*

Démonstration. On note $A = \mathrm{D}^+(n)\backslash\{1\}$. C'est une partie non vide de $\mathbb{N}^*$ puisqu'elle contient n car $|n| > 1$. Par conséquent, elle admet un minimum, que l'on note p. Montrons que p est alors un entier premier. Pour cela, on considère d un diviseur positif de p. Comme p divise n, par transitivité, d divise n. Si d est différent de 1, on en déduit que d appartient à A. Mais alors par minimalité de p, $p \leq d$. D'autre part, comme d divise p, on a également $d \leq p$. Ainis, $d = p$. En conclusion, $\mathrm{D}^+(p) = \{1,p\}$ et p est premier.

Notation
L'ensemble des entiers premiers positifs est noté classiquement $\mathcal{P}$.

Théorème 8 (Euclide) *L'ensemble $\mathcal{P}$ est infini.*

Démonstration. Procédons par l'absurde et supposons que $\mathcal{P}$ est fini. On introduit alors l'entier $q = 1 + \prod_{p\in\mathcal{P}} p$. Or, d'après la propriété précédente, q admet un diviseur premier positif p et celui apparaît alors dans le produit $\prod_{p'\in\mathcal{P}} p'$. Ainsi, p divise q et p divise $q-1$. Par conséquent, p divise $q-(q-1) = 1$. Comme p est positif, $p = 1$, ce qui absurde puisque 1 n'est pas premier. Ainsi, l'ensemble $\mathcal{P}$ est infini.

Propriété 23 *Soit $n \in \mathbb{Z}\backslash\{-1,0,1\}$. Alors n est premier si et seulement si*

$$\forall k \in [\![1,|n|-1]\!], \quad k \wedge n = 1$$

Démonstration. Supposons n premier. On a $1 \wedge n = 1$. Soit $k \in [\![2,|n|-1]\!]$. Alors k est distinct de 1 et de $|n|$, donc $k \notin \mathrm{D}^+(n)$ et par transitivité, aucun diviseur positif de 1 différent de k ne divise n. Par conséquent, $\mathrm{D}^+(k) \cap \mathrm{D}^+(n) = \{1\}$, d'où $k \wedge n = 1$. Réciproquement, si n est premier avec tous les entiers dans $[\![1,|n|-1]\!]$, alors

$$\mathrm{D}^+(n)\backslash\{|n|\} = \bigcup_{k=1}^{n-1} \mathrm{D}^+(n) \cap \{k\} \subset \bigcup_{k=1}^{n-1} \mathrm{D}^+(n) \cap \mathrm{D}^+(k) = \bigcup_{k=1}^{n-1} \{1\} = \{1\}$$

Ainsi, $\mathrm{D}^+(n) = \{1,n\})$ et n est premier.

Propriété 24 *Soit p,q deux entiers premiers distincts. Alors $p \wedge q = 1$.*

Démonstration. On applique ce qui précède en ordonnant p et q. Plus simplement, on peut écrire directement, $\mathrm{D}^+(p) \cap \mathrm{D}^+(q) = \{1,p\} \cap \{1,q\} = \{1\}$.

Propriété 25 (Lemme d'Euclide) *Soit $(a,b) \in \mathbb{Z}^2$ et p un entier premier. On suppose que p divise ab, alors p divise a ou p divise b.*

Démonstration. Supposons un instant que p ne divise pas a. Comme p est premier, les seuls diviseurs positifs de p sont 1 et p, donc le seul diviseur positif commun à p et a est 1. D'après le lemme de Gauss, p divise b.

Propriété 26 *Soit n un entier naturel supérieur ou égal à 2. Si n n'est pas premier, alors il admet un diviseur premier p tel que $p \leq \sqrt{n}$.*

Démonstration. On sait que n possède un diviseur premier positif. Notons p le minimum de ces diviseurs premiers positifs de n, ce qui permet d'écrire $n = pk$ avec k dans $\mathbb{Z}$. Comme n n'est pas premier p est différent de n, donc k est différent de 1. De plus, 1 n'est pas premier, donc k est différent de n. Comme p est le plus petit diviseur positif de n non égal à 1 et que k est un diviseur positif de n non égal à 1, $p \leq k$. Après multiplication par l'entier positif p, on en déduit $p^2 \leq kp = n$. Par croissance de la racine carrée, on en déduit $p \leq \sqrt{n}$.

Avant d'attaquer le théorème fondamental de l'arithmétique, on introduit quelques outils pour aider la formalisation :

Définition 9 *Soit $(\alpha_i)_{i\in \mathrm{I}}$ une famille d'entiers naturels indexées par un ensemble d'indices* I. *On dit que cette famille à support fini (ou presque nulle) lorsqu'il existe un ensemble fini* $\mathrm{K} \subset \mathrm{I}$ *tel que* $\forall i \in \mathrm{I}\backslash\mathrm{K}, \alpha_i = 0$. *Autrement dit, tous ses éléments sont nuls sauf un nombre fini d'entre eux.*

Notation
L'ensemble des familles d'entiers naturels indexées par I *à support fini est noté* $\mathbb{N}^{(\mathrm{I})}$ *(à différencier de* $\mathbb{N}^{\mathrm{I}}$*).*

Théorème 9 (Théorème fondamental de l'arithmétique) *Soit $n \in \mathbb{Z}^*$. Il existe un unique signe u dans $\{-1, 1\}$ et une unique famille d'entiers naturels indexée par $\mathcal{P}$ à support fini $(\alpha_p)_{p\in\mathcal{P}}$ telle que $n = u\prod_{p\in\mathcal{P}} p^{\alpha_p}$. On peut écrire de manière équivalente*

$$\exists!(u, (\alpha_p)_{p\in\mathcal{P}}) \in \{-1, 1\} \times \mathbb{N}^{(\mathcal{P})}, n = u\prod_{p\in\mathcal{P}} p^{\alpha_p}$$

☞ **Remarque**
On dit que l'anneau $\mathbb{Z}$ est factoriel. Notez que le produit $\prod_{p\in\mathcal{P}} p^{\alpha_p}$ est bien défini car la famille des exposants est à support fini, donc seul un nombre fini de termes de ce produit diffère de 1.

Démonstration. La preuve est hors-programme.

Définition 10 *Soit $n \in \mathbb{Z}^*$ et $p \in \mathcal{P}$. L'unique exposant α_p de p dans la décomposition de n en produit de facteurs premiers est appelé valuation p-adique de n (ou p-valuation de n), désormais noté $\nu_p(n)$.*

Corollaire
Soit $(a, b) \in \mathbb{Z}^2\backslash\{(0, 0)\}$. On a l'équivalence

$$a \mid b \iff \left(\forall p \in \mathcal{P}, \nu_p(a) \leq \nu_p(b)\right)$$

Application 2 (Calculs de pgcd et de ppcm) *Soit $(a, b) \in (\mathbb{Z}^*)^2$ et $p \in \mathcal{P}$. Alors*

$$\nu_p(ab) = \nu_p(a) + \nu_p(b)$$

$$\nu_p(a \wedge b) = \min(\nu_p(a), \nu_p(b))$$

$$\nu_p(a \vee b) = \max(\nu_p(a), \nu_p(b)$$

Démonstration.
— On écrit le produit des décompositions de a et b via

$$ab = u\prod_{p\in\mathcal{P}} p^{v_p(a)}u'\prod_{p\in\mathcal{P}} p^{v_p(b)} = uu'\prod_{p\in\mathcal{P}} p^{v_p(a)+v_p(b)}$$

Or $ab = u''\prod_{p\in\mathcal{P}} p^{v_p(ab)}$. L'unicité de la décomposition en facteurs premiers permet donc d'identifier

$$v_p(ab) = v_p(a) + v_p(b)$$

— Si p ne divise pas a,ou b, alors il n'appartient pas à $\mathrm{D}(a) \cap \mathrm{D}(b)$ donc il ne divise pas $a \wedge b$. Ainsi, $v_p(a \wedge b) = 0$ et $v_p(a) = 0$ ou $v_p(b) = 0$, de sorte que $\min(v_p(a), v_p(b)) = 0$ et l'égalité est vérifiée. Si p divise à la fois a et b, alors $p^{\min(v_p(a),v_p(b))}$ divise à la fois a et b, donc divise $a \wedge b$. De plus, $p^{\min(v_p(a),v_p(b))+1}$ ne divise pas l'un des deux entiers a et b, d'après la propriété précédente. Ce n'est donc pas un diviseur commun à $a \wedge b$. Ainsi, $v_p(a \wedge b) = \min(v_p(a), v_p(b))$.

— On remarque que $\min(v_p(a), v_p(b)) + \max(v_p(a), v_p(b)) = v_p(a) + v_p(b)$. Mais alors, comme $(a \wedge b)(a \vee b) = |ab|$, on a d'après les deux égalités précédentes,

$$v_p(a \vee b) = v_p(a) + v_p(b) - \min(v_p(a), v_p(b)) = \max(v_p(a), v_p(b))$$