Arithmétique dans $\mathbb{Z}$

Cornou Jean-Louis

31 janvier 2023

L'arithmétique est l'étude de la relation de divisibilité dans les anneaux commutatifs. Cette étude est triviale dans les corps puisque tout élément non nul divise tout autre élément dans une telle structure. Rappelons que $(\mathbb{Z}, +, \times)$ est un anneau et que $(\mathbb{Z}^*, \times)$ n'est pas un groupe (l'entier 2 n'a pas d'inverse dans $\mathbb{Z}^*$). Parmi tous les anneaux, l'anneau $\mathbb{Z}$ se distingue car sa structure multiplicative découle de sa structure additive. De plus, pour tout anneau A, il n'y a qu'un morphisme d'anneau de $\mathbb{Z}$ dans A (on dit que $\mathbb{Z}$ est un objet initial dans la catégorie des anneaux).
L'arithmétique dans $\mathbb{Z}$ peut être traitée de manière élémentaire. On lui privilégie une approche algébrique afin d'illustrer et de mettre en pratique les différentes notions sur les structures algébriques (groupes, anneaux, morphismes, etc).

1 L'anneau euclidien $\mathbb{Z}$.

1.1 Relation de divisibilité

Définition 1 *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 1 *La relation de divisbilité induit une relation d'ordre sur $\mathbb{N}$.*

Démonstration. — Réflexivité : Soit $a \in \mathbb{N}$. On pose alors $n = 1$. Cet entier relatif vérifie $a = na$, donc a divise a.

— Transitivité : Soit $(a, b, c) \in \mathbb{N}^3$ tel que a divise b et b divise c. Montrons que a divise c. D'après la définition de la divisibilité,

$$\exists (n, m) \in \mathbb{Z}^2, \quad b = na \quad \wedge \quad c = mb$$

Mais alors

$$c = mb = m(na) = (mn)a$$

puisque la mutliplicatiion dans $\mathbb{Z}$ est associative. De plus, $\mathbb{Z}$ est stable par multiplication, donc mn appartient à $\mathbb{Z}$. Cet entier relatif assure donc que a divise c.

— Antisymétrie : Soit $(a, b) \in \mathbb{N}^2$ tel que a divise b et b divise a. D'après la définition de la divisibilité,

$$\exists (n, m) \in \mathbb{Z}^2, \quad b = na \quad \wedge \quad a = mb$$

On en déduit que $b = na = nmb$, donc que $b(1 - nm) = 0$. On doit alors distinguer plusieurs cas :

— Premier cas : $b = 0$. Alors, l'égalité $a = mb$ entraîne $a = 0$. Ainsi, $b = a$.

— Deuxième cas : $b \neq 0$. Alors, ce qui précède assure que $nm = 1$. Or, les seuls couples d'entiers relatifs à vérifier cette relation sont les couples $(1, 1)$ et $(-1, -1)$. De plus, l'égalité $b = na$ assure que a est non nul et que n est strictement positif puisque a et b sont tous deux strictement positifs. Ainsi, on a $n = 1$, puis $b = a$.

⚠ **Attention**
La relation de divisibilité n'est pas une relation d'ordre sur $\mathbb{Z}$ car elle n'est pas antisymétrique.

Propriété 2 *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. Soit $(a,b) \in \mathbb{Z}^2$. Comme $\mathbb{Z}$ est stable par multiplication par -1, on a l'équivalence $a \mid b \iff |a| \mid |b|$. Ainsi,

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

Cependant, on sait que la relation de divisibilité est antisymétrique sur $\mathbb{N}$ et que $(|a|,|b|) \in \mathbb{N}^2$. Par conséquent,

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

Définition 2 *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 oiu $D(a)$. 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 3 *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. Plus généralement, l'étude de la divisibilité dans un anneau se fait à « inversible près ».

Propriété 4 *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 $1 + 2|a|$.

Définition 3 *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 5 *Soit $a \in \mathbb{Z}$. L'ensemble des multiples de a est l'ensemble $a\mathbb{Z}$. C'est un sous-groupe de $\mathbb{Z}$.*

Démonstration. Soit b un multiple de a, alors il existe un entier relatif n tel que $b = na$. Ainsi, b appartient à $a\mathbb{Z}$. Réciproquement, tout entier de la forme an avec n dans $\mathbb{Z}$ est un muliple de a. Montrons à présent que $a\mathbb{Z}$ est un sous-groupe de $\mathbb{Z}$. On peut effectuer les vérifications classiques des sous-groupes (non vide, stable par addition et opposé). Proposons une autre démonstration. On note

$$\varphi : \mathbb{Z} \to \mathbb{Z}, n \mapsto an$$

Montrons que l'application φ est un morphisme de groupes additifs. Soit $(n,m) \in \mathbb{Z}^2$, alors la distributivité de la multiplication sur l'addition dans l'anneau $\mathbb{Z}$ entraîne

$$\varphi(n+m) = a(n+m) = an + am = \varphi(n) + \varphi(m)$$

Ainsi, φ est un morphisme de groupes, donc son image est un sous-groupe de $\mathbb{Z}$. Or, celle-ci n'est autre que l'ensemble $a\mathbb{Z}$, ce qui conclut.

⚠ **Attention**
Si $a \notin \{-1,0,1\}$, l'ensemble $a\mathbb{Z}$ n'est pas un sous-anneau de $\mathbb{Z}$.

Propriété 6 *Soit $a \in \mathbb{Z}$. L'ensemble des générateurs de $a\mathbb{Z}$ est l'ensemble $\{a,-a\}$. En particulier, il possède un unique générateur positif.*

Démonstration. Soit $a \in \mathbb{Z}$. Soit b un générateur de $a\mathbb{Z}$. Comme l'entier relatif a appartient à $a\mathbb{Z}$, cela signifie qu'il existe un entier relatif n tel que $a = nb$, donc que b divise a. De plus, a engendre $a\mathbb{Z}$. Comme b appartient lui-même à $a\mathbb{Z}$, on en déduit comme précédemment que a divise b. D'après la propriété sur les éléments associés, on en déduit que $b = a$ ou $b = -a$. Réciproquement, a engendre clairement $a\mathbb{Z}$ et $-a$ engendre $a\mathbb{Z}$, puisque $\mathbb{Z}$ est stable par multiplication par -1.

Propriété 7 *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.

1.2 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 $n \in A$, alors $nb \leq a \leq \max(0,a)$. Or $b \geq 1$, on en déduit que $n \leq \max(0,a)$.

Ainsi, la partie de $\mathbb{Z}$, A 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 $(a,-b)$ pour l'existence.
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 8 *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 9 *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.

La conséquence la plus importante de la division euclidienne est l'ensemble des sous-groupes de $\mathbb{Z}$.

Théorème 2 *Soit* G *une partie de* $\mathbb{Z}$*. On a l'équivalence :* G *est un sous-groupe de* $(\mathbb{Z}, +)$ *si et seulement s'il existe un entier relatif* n *tel que* $G = n\mathbb{Z}$ *si et seulement si il existe un unique entier naturel* n *tel que* $G = n\mathbb{Z}$*.*

Démonstration. On a déjà vu que tous les $n\mathbb{Z}$ sont des sous-groupes de $\mathbb{Z}$ et que leurs générateurs sont $\{n, -n\}$ donc qu'un seul d'entre eux est positif. Soit à présent G un sous-groupe de $\mathbb{Z}$. Si $G = \{0\}$, alors $n = 0$ convient. Supposons que $G \neq \{0\}$ et notons g un élément non nul de G. Comme G est un sous-groupe de $\mathbb{Z}$, il est stable par passage à l'opposé, donc $-g$ appartient également à G et c'est un élément non nul. Ainsi, $G\cap\mathbb{N}^*$ est une partie non vide de $\mathbb{N}^*$. Notons n son minimum et montrons que $G = n\mathbb{Z}$. Comme n appartient à G d'après sa définition, on en déduit par récurrence que $\forall k \in \mathbb{Z}, nk \in G$, donc que $n\mathbb{Z} \subset G$. Soit à présent a un élément de G. Effectuons alors la division euclidienne de a par n, ce qui est légitime puisque n est non nul par définition. On écrit donc

$$a = nq + r \quad \text{avec} \quad q \in \mathbb{Z}, \quad 0 \leq r < n-1$$

Mais alors, nq appartient à G car G est un groupe et n appartient à G. De plus, a appartient à G, donc $a - nq$ appartient à G, soit $r \in G$. Or r est strictement plus petit que n et positif, donc par minimalité de n, r est nul. Par conséquent, $a = nq$ donc $a \in n\mathbb{Z}$. On a ainsi montré par double inclusion que $G = n\mathbb{Z}$.

☞ **Remarque**
Une autre façon de formuler le résultat est de dire : tous les sous-groupes de $\mathbb{Z}$ *sont monogènes. On remarque qu'à part le sous-groupe nul, ils sont tous isomorphes à* $\mathbb{Z}$*. Ce fait sera remarquable pour traiter les sous-groupes de la forme* $a\mathbb{Z} + b\mathbb{Z}$ *et* $a\mathbb{Z}\cap b\mathbb{Z}$*.*

Propriété 10 *Soit* $(a, b) \in \mathbb{Z}^2$*, alors l'ensemble*

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

est un sous-groupe de $\mathbb{Z}$*. L'ensemble* $a\mathbb{Z}\cap b\mathbb{Z}$ *est également un sous-groupe de* $\mathbb{Z}$*.*

Démonstration. On note $f : \mathbb{Z}^2 \to \mathbb{Z}, (u, v) \mapsto au + bv$ et on montre que cette application est un morphisme de groupes. Rappelons que $\mathbb{Z}^2$ est muni de la structure de groupe produit. Soit $(u, v, u', v') \in \mathbb{Z}^4$. Alors d'après la distributivité et la commutativité de l'addition, on a

$$f((u, v) + (u', v')) = f((u + u', v + v')) = a(u + u') + b(v + v') = au + bv + au' + bv' = f((u, v)) + f((u', v'))$$

Par conséquent, f est un morphisme de groupes, et son image est nécessairement un sous-groupe de $\mathbb{Z}$. Or son image n'est rien d'autre que l'ensemble $a\mathbb{Z} + b\mathbb{Z}$.
Pour l'intersection, je vous renvoie à votre cours sur les structures algébriques.

2 Plus Grand Commun Diviseur, Plus Petit Commun Multiple

2.1 PGCD de deux entiers relatifs

Définition 4 *Soit* $(a,b) \in \mathbb{Z}^2$. *Si* $(a,b) = (0,0)$, *on convient que le plus grand diviseur commun de* a *et* b *est* 0. *Sinon, le maximum de* $D^+(a) \cap D^+(b)$ *est appelé plus grand (au sens de l'ordre habituel* $\leq$*) diviseur commmun de* a *et* b, *en abrégé pgcd de* a *et* b.

☞ **Remarque**
Cette définition est légitime pour deux raisons : cet ensemble est non vide puisque 1 *divise* a *et* b. *De plus, on a montré que pour tout entier* a *non nul,* D_a *est fini.*

Notation
La notation du programme est $a \wedge b$. *On rencontre aussi* $\gcd(a,b)$ *(greatest common divisor) ou pgcd*(a,b).

Exemple 3

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

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 $23987 \wedge 19196 = 1$.

Propriété 11 *Soit* $(a,b) \in \mathbb{Z}^2$. *On note* $d = a \wedge b$. *Alors*

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

Démonstration. Si $(a,b) = (0,0)$, il suffit de choisir $a' = 1$ et $b' = 1$. Supposons que a ou b est non nul. Alors, d appartient à $D^+(a) \cap D^+(b)$ puisque c'en est le maximum. En particulier d divise a et d divise b. Donc il existe $(a',b') \in \mathbb{Z}^2$ tel que $a = da'$ et $b = db'$. Notons alors $\delta = a' \wedge b'$ et montrons qu'il vaut 1. Par le même argument que précédemment, on peut écrire $a' = \delta a''$ et $b' = \delta b''$ avec $(a'',b'') \in \mathbb{Z}^2$. On en déduit par multiplication par d que $a = da' = d\delta a''$ et que $b = db' = b\delta b''$. Ainsi, $d\delta$ est un diviseur positif commun à a et b, donc plus petit que le maximum de $D^+(a) \cap d^+(b)$ à savoir d. On a par conséquent $d\delta \leq d$. Comme d est strictement positif, on en déduit que $\delta \leq 1$. Comme δ est également strictement positif, $\delta = 1$, ce qui conclut.

Exemple 4 *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* $x + y = 360$ *?*

Correction 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 12 *Soit* $(a,b) \in \mathbb{Z}^2$, $n \in \mathbb{Z}$. *Alors*

1. $a \wedge b = b \wedge a$.
2. $a \wedge b = |a| \wedge |b|$.
3. $D(a) \cap D(b+na) = D(a) \cap D(b)$ *et* $a \wedge (b+na) = a \wedge b$.
4. *Si* b *est non nul, on note* r *le reste de la division euclidienne de* a *par* b. *Alors* $a \wedge b = b \wedge r$. *En particulier, si* b *divise* a, $a \wedge b = |b|$

Démonstration.
1. Dans le cas $(a,b) = (0,0)$, c'est valide. Sinon, $D^+(a) \cap D^+(b) = D^+(b) \cap D^+(a)$, donc ces ensembles ont même maximum, soit $a \wedge b = b \wedge a$.h
2. Dans le cas $(a,b) = (0,0)$, c'est valide. Sinon, pour tout réel a, $D(a) = D(|a|)$, ainsi, $D^+(a) \cap D^+(b) = D^+(|a|) \cap D^+(|b|)$. Ces ensembles ont alors même maximum, donc $a \wedge b = |a| \wedge |b|$.
3. Si $(a,b) = (0,0)$, alors $a \wedge (b+na) = 0 \wedge 0 = 0 = a \wedge b$. Supposons à présent que a est non nul (sinon on utilise la symétrie précédemment démontrée). 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 $D(a) \cap D(b) \subset D(a) \cap D(b+na)$. Ainsi, on a l'égalité $D(a) \cap D(b+na) = D(a) \cap D(b)$. Ces ensembles ont alors même maximum, donc $a \wedge (b+na) = a \wedge b$.
4. 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, alors, $r = 0$ et $b \wedge 0 = \max(D^+(b) \cap \mathbb{Z}) = \max D^+(b) = |b|$.

✎ **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)
```

Propriété 13 *Soit* $(a,b) \in \mathbb{Z}^2$. *Alors* $D(a) \cap D(b) = D(a \wedge b)$.

Démonstration. Si $(a,b)=(0,0)$, $a\wedge b=0$, l'égalité $\mathbb{Z}\cap\mathbb{Z}=\mathbb{Z}$ est clairement vérifiée. Supposons que a ou b est non nul, alors $a\wedge b=\max(|a|,|b|)\wedge\min(|a|,|b|)$ et on peut appliquer l'algorithme d'Euclide qui s'arrête au rang $N+1$. On a pour tous entiers n, $D(a)\cap D(b)=D(r_n)\cap D(r_{n-1})=D(r_N)\cap D(0)=D(a\wedge b)\cap\mathbb{Z}=D(a\wedge b)$.

Propriété 14 *Soit $(a,b)\in\mathbb{Z}^2$ et $d=a\wedge b$.*

$$\forall\delta\in\mathbb{Z},\Big[(\delta\mid a)\bigwedge(\delta\mid b)\iff\delta\mid d\Big]$$

*Autrement dit, le pgcd de a et b est le plus grand, **au sens de la relation de divisibilité dans** $\mathbb{N}$, diviseur commun de a et b.*

Démonstration. L'équivalence indiquée n'est rien d'autre que l'égalité d'ensembles $D(a)\cap D(b)=D(d)$. Cette égalité vient juste d'être établie en propriété précédente.

☞ **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 $a\wedge b$.

Propriété 15 *Soit $(a,b)\in\mathbb{Z}^2$, $k\in\mathbb{Z}$. Alors*

1. $(ka)\wedge(kb)=|k|(a\wedge b)$.
2. $a\mid b\iff a\wedge b=a$.

Démonstration.
1. Si k est nul, l'égalité revient à écrire $0=0$ qui est bien vérifiée. Si k est non nul, k divise ka et kb, donc k divise leur pgcd : $ka\wedge kb$. On note alors c dans $\mathbb{Z}$ tel que $ka\wedge kb=kc$. Comme le pgcd est un diviseur commun, kc divise ka et kb (c'est leur pgcd). Comme k est non nul, c divise a et b, donc leur pgcd $a\wedge b$. On en déduit que $(ka)\wedge(kb)$ divise $k(a\wedge b)$. D'autre part, $a\wedge b$ divise a et b, donc $k(a\wedge b)$ divise ka et kb, donc divise leur pgcd $ka\wedge kb$. Ainsi, $ka\wedge kb$ et $k(a\wedge b)$ sont associés. Donc $(ka)\wedge(kb)=|k|(a\wedge b)$.
2. On a déjà vu que si a divise b, alors $a\wedge b=a$. Réciproquement, si $a\wedge b=a$, alors $D(a)\cap D(b)=D(a\wedge b)=D(a)$. Cela entraîne que $D(a)\subset D(b)$, donc que a divise b.

Propriété 16 (Caractérisation algébrique du pgcd) *Soit $(a,b)\in\mathbb{Z}^2$ et $d\in\mathbb{N}$. On a l'équivalence*

$$d=a\wedge b\iff a\mathbb{Z}+b\mathbb{Z}=d\mathbb{Z}$$

Démonstration. Dans le cas $(a,b)=(0,0)$ et $a\wedge b=0$, on retrouve bien entendu $\{0\}+\{0\}=\{0\}$. Supposons à présent que l'un des deux entiers relatifs a, b n'est pas nul. L'ensemble $a\mathbb{Z}+b\mathbb{Z}$ est un sous-groupe de $\mathbb{Z}$, donc il existe un unique entier naturel δ tel que $a\mathbb{Z}+b\mathbb{Z}=\delta\mathbb{Z}$. Montrons que $\delta=a\wedge b$ par double divisibilité. L'entier δ appartient à $\delta\mathbb{Z}$ donc à $a\mathbb{Z}+b\mathbb{Z}$. Ainsi, il existe des entiers relatifs n et m tels que $\delta=an+bm$. Mais alors, comme $a\wedge b$ est un maximum pour $\leq$ de $D^+(a)\cap D^+(b)$, il appartient à $D^+(a)\cap D^+(b)$, donc a divise $a\wedge b$ et b divise $a\wedge b$. Il existe des entiers relatifs p et q tels que $a=(a\wedge b)p$ et $b=(a\wedge b)q$. Il en résulte que

$$\delta=an+bm=(a\wedge b)(np+qm)$$

donc que $a\wedge b$ divise δ. Il existe donc un entier r tel que $\delta=r(a\wedge b)$. Comme δ et $a\wedge b$ sont tous deux strictement positifs, r est strictement positif. D'autre part, on a l'inclusion $a\mathbb{Z}\subset a\mathbb{Z}+b\mathbb{Z}=\delta\mathbb{Z}$, donc δ divise a. De même, $b\mathbb{Z}\subset a\mathbb{Z}+b\mathbb{Z}=\delta\mathbb{Z}$, donc δ divise b. Comme δ est positif, δ appartient à $D^+(a)\cap D^+(b)$, donc $\delta\leq a\wedge b$ d'après la définition du pgcd comme maximum. On a donc $r\leq 1$. Comme r n'est pas nul, on a $r=1$ et $\delta=a\wedge b$.
Le résultat s'ensuit par unicité des générateurs positifs d'un sous-groupe de $\mathbb{Z}$.

☞ **Remarque**
Une autre façon de formuler ce résultat est : le pgcd de a et b l'unique générateur positif du groupe $a\mathbb{Z}+b\mathbb{Z}$.

Théorème 3 (Relation de Bezout) *Soit $(a,b)\in\mathbb{Z}^2$. Alors*

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

Démonstration. D'après la caractérisation précédente, $a\wedge b$ appartient à $a\wedge b\mathbb{Z}$, donc à $a\mathbb{Z}+b\mathbb{Z}$. Ainsi, il existe des entiers relatifs u et v tels que $a\wedge b=au+bv$.

⚠ **Attention**
La réciproque est fausse dans le cas $d\neq 1$. En effet, l'ensemble $a\mathbb{Z}+b\mathbb{Z}$ est l'ensemble des multiples de $a\wedge b$, autrement dit, pour tout $(u,v)\in\mathbb{Z}^2$, $au+bv$ est multiple $a\wedge b$, mais on n'est pas assuré qu'il y a égalité.

Théorème 4 (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 caractérisation algébrique 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 $a\wedge b=1$.

✎ **Méthode (Algorithme d'Euclide étendu)**
La détermination d'un tel couple (u,v) a un intérêt pratique pour la résolution d'équation diophantiennes. L'algorithme d'Euclide étendu donne un méthode pour déterminer un tel couple. 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 $r_{n-1}=q_nr_n+r_{n+1}$. 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*

$$\forall n\in[\![1,N]\!],\quad u_{n+1}=u_{n-1}-q_nu_n,\quad v_{n+1}=v_{n-1}-q_nv_n$$

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

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

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 la 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.*

$$\begin{array}{lll} 258 & =145\times1 & +113\\ 145 & =113\times1 & +32\\ 113 & =32\times3 & +17\\ 32 & =17\times1 & +15\\ 17 & =15\times1 & +2\\ 15 & =2\times7 & +1\\ 2 & =1\times2 & +0 \end{array}$$

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

$$\begin{aligned} 1 &= 15-2\times7\\ &= 15-(17-15\times1)\times7\\ &= 8\times15-7\times17\\ &= 8\times(32-17)-7\times17\\ &= 8\times32-17\times15\\ &= 8\times32-(113-32\times3)\times15\\ &= 53\times32-113\times15\\ &= 53\times(145-113)-113\times15\\ &= 53\times145-113\times68\\ &= 53\times145-(258-145)\times68\\ &= 258\times(-68)+121\times145 \end{aligned}$$

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)
```

2.2 PPCM de deux entiers relatifs

Propriété 17 *Soit $(a,b) \in (\mathbb{Z}^*)^2$. Alors a et b possèdent un multiple commun strictement positif.*

Démonstration. On pose $m = |a| \times |b|$. Comme a et b sont non nuls, c'est un entier naturel non nul. De plus, c'est clairement un multiple de a et de b.

Définition 5 *Soit $(a,b) \in \mathbb{Z}^2$. Si a ou b est nul, on convient que le plus petit commun multiple de a et b vaut 0. Sinon, on appelle plus petit commun multiple de a et b, le minimum (pour l'ordre naturel $\leq$) de l'intersection de l'ensemble des multiples non nuls de a et des multiples non nuls de b. On l'appelle également ppcm de a et b.*

☞ **Remarque**
Cette définition est légitime puisqu'on a vu que cette partie de $\mathbb{N}^*$ est non vide, donc qu'elle admet un minimum.

Notation
Notation du programme $a \vee b$. On rencontre également $ppcm(a,b)$ ou $lcm(a,b)$ (least common multiple).

Propriété 18 *Soit $(a,b) \in \mathbb{Z}^2$ et $m \in \mathbb{N}$. Alors on a l'équivalence*

$$a\mathbb{Z} \cap b\mathbb{Z} = m\mathbb{Z} \iff m = a \vee b$$

Démonstration. Remarquons tout d'abord que $a\mathbb{Z} \cap b\mathbb{Z}$ est un sous-groupe de $\mathbb{Z}$. Par conséquent, il existe un unique entier naturel μ tel que $a\mathbb{Z} \cap b\mathbb{Z} = \mu\mathbb{Z}$. Montrons à présent que $\mu = a \vee b$. Si a ou b est nul, il est clair que $a\mathbb{Z} \cap b\mathbb{Z} = \{0\} = 0\mathbb{Z}$, ce qui est cohérent avec notre convention. Supposons que a et b sont tous deux non nuls. L'ensemble des multiples communs à a et b n'est autre que $a\mathbb{Z} \cap b\mathbb{Z}$, par conséquent l'ensemble des multiples strictement positifs de a et b est l'ensemble $\mathbb{N}^* \cap a\mathbb{Z} \cap b\mathbb{Z} = \mathbb{N}^* \cap \mu\mathbb{Z} = \mu\mathbb{N}^*$ puisque μ est strictement positif. Or le minimum de cet ensemble vaut μ, donc $a \vee b = \mu$. L'équivalence en découle via l'unicité du générateur positif des sous-groupes de $\mathbb{Z}$.

Propriété 19 *Soit $(a,b) \in \mathbb{Z}^2$, $m \in \mathbb{Z}$. On a l'équivalence*

$$\Big[(a \mid m) \bigwedge (b \mid m)\Big] \iff (a \vee b) \mid m$$

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

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 20 *Soit $(a,b,k) \in \mathbb{Z}^3$. Alors*

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

Démonstration. Écrivons rapidement $ka\mathbb{Z} \cap kb\mathbb{Z} = k(a\mathbb{Z} \cap b\mathbb{Z}) = |k|(a\mathbb{Z} \cap b\mathbb{Z})$. La démonstration nécessite en toute rigueur de traiter le cas $k = 0$ à part. D'après la caractérisation algébrique du ppcm, on en déduit que $[(ka) \vee (kb)]\mathbb{Z} = |k|((a \vee b)\mathbb{Z}) = |k|(a \vee b)\mathbb{Z}$. Par unicité des générateurs positifs des sous-groupes de $\mathbb{Z}$, on en déduit l'égalité $(ka) \vee (kb) = |k|(a \vee b)$.

2.3 PGCD, PPCM d'une famille finie d'entiers relatifs

Afin d'alléger le texte, on fixe n un entier naturel supérieur ou égal à 2, et $a = (a_1, \dots, a_n) \in \mathbb{Z}^n$ dans cette partie.

Définition 6 — *Si le n-uplet a est nul, on définit le pgcd de* $(a_1, \dots, a_n)$ *par* $\bigwedge_{i=1}^n a_i = a_1 \wedge \cdots \wedge a_n = 0$. *Sinon, on définit le pgcd de ce n-uplet comme le maximum des diviseurs communs à tous les* a_i, $i \in [\![1, n]\!]$, *i.e* $\max \bigcap_{1 \leq i \leq n} D^+(a_i)$.

— *Si l'un des* a_i *est nul, on définit le ppcm de ce n-uplet par* $\bigvee_{i=1}^n a_i = 0$. *Sinon, on définit le ppcm de ce n-uplet comme le minimum des multiples strictement positifs communs à tous les* a_i, $i \in [\![1, n]\!]$, *i.e* $\min \bigcap_{1 \leq i \leq n} |a_i|\mathbb{N}^*$, *noté* $\bigvee_{i=1}^n a_i$.

Propriété 21 (Associativité) *On suppose dans cette propriété que* $n \geq 3$.

$$\bigwedge_{i=1}^n a_i = (a_1 \wedge a_2) \wedge \bigwedge_{i=3}^n a_i$$

$$\bigvee_{i=1}^n a_i = (a_1 \vee a_2) \vee \bigvee_{i=3}^n a_i$$

Démonstration. Il suffit de constater, modulo les cas particuliers, que l'intersection d'ensembles est associative, et que $\max(\max I, \max J) = \max(I \cap J)$ pour toutes parties finies I et J. De même, $\min(\min(I), \min(J)) = \min(I \cap J)$ pour toutes parties finies I et J.

Propriété 22 (Commutativité) *Soit* σ *une permutation de* $[\![1, n]\!]$. *Alors*

$$\bigwedge_{i=1}^n a_i = \bigwedge_{i=1}^n a_{\sigma(i)}$$

$$\bigvee_{i=1}^n a_i = \bigvee_{i=1}^n a_{\sigma(i)}$$

Démonstration. De même que précédemment, il suffit de remarquer que l'intersection d'ensembles est commutative.

Propriété 23

$$\sum_{i=1}^n (a_i\mathbb{Z}) = \left(\bigwedge_{i=1}^n a_i\right)\mathbb{Z}$$

$$\bigcap_{i=1}^n (a_i\mathbb{Z}) = \left(\bigvee_{i=1}^n a_i\right)\mathbb{Z}$$

Démonstration. On le prouve par récurrence sur l'entier n. Le cas $n = 2$ a été prouvé dans les sections précédentes. Soit n un entier naturel tel que cette propriété est vraie. Alors

$$\sum_{i=1}^{n+1} (a_i\mathbb{Z}) = \sum_{i=1}^{n} (a_i\mathbb{Z}) + a_{n+1}\mathbb{Z} = \left(\bigwedge_{i=1}^n a_i\right)\mathbb{Z} + a_{n+1}\mathbb{Z} = \left(\left(\bigwedge_{i=1}^n a_i\right) \wedge a_{n+1}\right)\mathbb{Z} = \left(\bigwedge_{i=1}^{n+1} a_i\right)\mathbb{Z}$$

$$\bigcap_{i=1}^{n+1} (a_i\mathbb{Z}) = \bigcap_{i=1}^{n} (a_i\mathbb{Z}) \cap a_{n+1}\mathbb{Z} = \left(\bigvee_{i=1}^n a_i\right)\mathbb{Z} \cap a_{n+1}\mathbb{Z} = \left(\left(\bigvee_{i=1}^n a_i\right) \vee a_{n+1}\right)\mathbb{Z} = \left(\bigvee_{i=1}^{n+1} a_i\right)\mathbb{Z}$$

Ceci assure l'hérédité et la validité pour tout entier n.

Théorème 5 (Relation de Bezout)

$$\exists (u_1, \dots, u_n) \in \mathbb{Z}^n, \quad \bigwedge_{i=1}^n a_i = \sum_{i=1}^n a_i u_i$$

Démonstration. Il suffit de constater que $\bigwedge_{i=1}^n a_i \in \left(\bigwedge_{i=1}^n a_i\right)\mathbb{Z}$.

☞ **Remarque**
De même que précédemment, il ne suffit pas de disposer d'une relation $\sum_{i=1}^n a_i u_i = d$ pour conclure que d est le pgcd de ce n-uplet. Il s'agit uniquement d'un multiple de ce pgcd.

Propriété 24 (Homogénéité positive) *Soit $k \in \mathbb{Z}$. Alors*

$$\bigwedge_{i=1}^n (ka_i) = |k|\left(\bigwedge_{i=1}^n a_i\right)$$

$$\bigvee_{i=1}^n (ka_i) = |k|\left(\bigvee_{i=1}^n a_i\right)$$

Démonstration. Il suffit de passer par les sous-groupes de $\mathbb{Z}$.

$$\sum_{i=1}^n (ka_i\mathbb{Z}) = |k|\left(\sum_{i=1}^n a_i\mathbb{Z}\right) = |k|\left(\bigwedge_{i=1}^n a_i\right)\mathbb{Z}$$

$$\bigcap_{i=1}^n (ka_i\mathbb{Z}) = |k|\bigcap_{i=1}^n (a_i\mathbb{Z}) = |k|\left(\bigvee_{i=1}^n a_i\right)\mathbb{Z}$$

Application 1 (Réduction au même dénominateur) *Soit $n \in \mathbb{N}^*$, $(r_1,\dots,r_n) \in \mathbb{Q}^n$. On note $(p_1,\dots,p_n) \in \mathbb{Z}^n$, $(q_1,\dots,q_n) \in \mathbb{N}^*$ tels que $\forall i \in [\![1,n]\!], r_i = p_i/q_i$. On note $m = \bigvee_{i=1}^n q_i$ le ppcm des dénominateurs, alors $m\sum_{i=1}^n r_i$ appartient à $\mathbb{Z}$.*

Démonstration. Comme m est un multiple commun à tous les $(q_i)_{1\leq i\leq n}$, on a $\forall i \in [\![1,n]\!], \exists m_i \in \mathbb{Z}, m = m_i q_i$. Mais alors,

$$m\sum_{i=1}^n r_i = \sum_{i=1}^n \frac{m_i q_i p_i}{q_i} = \sum_{i=1}^n m_i p_i \in \mathbb{Z}$$

☞ **Remarque**
On aurait pu choisir le produit des $(q_i)_i$ pour réduire au même dénominateur, mais cela amène parfois des coefficients gigantesques.

Exercice 2 *Sans calculatrice, démontrer que*

$$\forall t \in \mathbb{R}, t^2 \leq \frac{36}{5} \Rightarrow \frac{t^4}{120} \leq \frac{t^4}{72} - \frac{t^6}{1296}$$

Correction 2 *L'inégalité souhaitée est vérifiée pour $t = 0$. Pour t non nul, elle est équivalente à $\frac{1}{120} \leq \frac{1}{72} - \frac{t^2}{1296}$, soit encore $t^2 \leq \frac{1296}{72} - \frac{1296}{120}$. On réduit alors la fraction $\frac{1}{72} - \frac{1}{120}$ au même dénominateur, et non n'allons pas calculer le produit 72×120. On a $72 = 24\times3$ et $120 = 24\times5$, donc $72\wedge120 = 24$ et $72\vee120 = 24\times15 = 360$. Ainsi,*

$$\frac{1296}{72} - \frac{1296}{120} = \frac{1296}{360}(5-3) = 2\frac{36^2}{36\times10} = \frac{36}{5}$$

3 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.

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

Théorème 6 *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 25 (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 $n \in Z$ 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 26 *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, il s'écrit sous la forme $x = al = bk$ avec l et k des entiers relatifs. Mais alors, a divise bk et est premier avec b. D'après le lemme de Gauss, a divise k, donc k s'écrit sous la forme $k = as$ avec s un entier relatif. 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 $d[(da') \vee (db')] = (a \wedge b)(a \vee b) = |ab|$.

Application 2 (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 $c \notin dZ$, 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 27 *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 28 *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 29 *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.

Définition 8 *Soit $n \in \mathbb{N}$, $n \geq 2$ et $(a_1, \ldots, a_n) \in \mathbb{Z}^n$.*

- *On dit que les $(a_i)_{1 \leq i \leq n}$ sont premiers dans leur ensemble lorsque $\bigwedge_{i=1}^{n} a_i = 1$.*
- *On dit que les $(a_i)_{1 \leq i \leq n}$ sont premiers entre eux deux à deux lorsque $\forall (i,j) \in [\![1,n]\!], i \neq j, a_i \wedge a_j = 1$.*

Propriété 30 *Soit $n \in \mathbb{N}$, $n \geq 2$, et $(a_1, \ldots, a_n) \in \mathbb{Z}^n$. On suppose que les $(a_i)_{1 \leq i \leq n}$ sont premiers entre eux deux à deux, alors ils sont premiers dans leur ensemble.*

Démonstration. D'après la propriété d'associativité du pgcd, on a

$$\bigwedge_{i=1}^{n} a_i = (a_1 \wedge a_2) \wedge \bigwedge_{i=3}^{n} a_i = 1 \wedge \bigwedge_{i=3}^{n} a_i = 1$$

Les $(a_i)_{1 \leq i \leq n}$ sont donc premiers dans leur ensemble.

⚠ **Attention**
La réciproque est FAUSSE ! $6 \wedge 10 \wedge 15 = 2 \wedge 15 = 1$, donc $6, 10, 15$ sont premiers dans leur ensemble. Toutefois, $6 \wedge 10 = 2$, $6 \wedge 15 = 3$ et $10 \wedge 15 = 5$.

☞ **Remarque**
On remarquera qu'il suffit que deux d'entre eux soient premiers entre eux pour les $(a_i)_{1 \leq i \leq n}$ soient premiers dans leur ensemble.

4 L'anneau factoriel $\mathbb{Z}$.

Définition 9 *Soit $p \in \mathbb{Z}$. On dit que p est premier lorsque $|D^+(p)| = 2$.*

Exemple 7 *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 31 *Soit $n \in \mathbb{Z}\backslash\{-1, 0, 1\}$. Alors, $\min(D^+(n)\backslash\{1\})$ est premier. En particulier, n admet un diviseur premier.*

Démonstration. On note $A = D^+(n)\backslash\{1\}$. 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, $D^+(p) = \{1, p\}$ et p est premier.

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

Théorème 7 (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 32 *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 $k \notin D^+(n)$ et par transitivité, aucun diviseur positif de 1 différent de k ne divise n. Par conséquent, $D^+(k) \cap D^+(n) = \{1\}$, d'où $k \wedge n = 1$. Réciproquement, si n est premier avec tous les entiers dans $[\![1, |n| - 1]\!]$, alors

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

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

Propriété 33 (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. Comme p divise $|ab|$, il est plus petit que $|a|$ ou que $|b|$. Supposons un instant que p ne divise pas a, alors p est premier avec a puisque p est premier. D'après le lemme de Gauss, p divise b.

Propriété 34 *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 $p \leq \sqrt{n}$.

Théorème 8 (Théorème fondamental de l'arithmétique) *« Tout entier naturel supérieur ou égal à 2 peut s'écrire comme un produit de nombres premiers ». Soit $n \in \mathbb{Z}\backslash\{-1,0,1\}$, alors*

$$\exists u \in \{-1,1\}, r \in \mathbb{N}^*, (p_1,\dots,p_r) \in \mathcal{P}^r, \forall i \neq j, p_i \neq p_j, (\alpha_1,\dots,\alpha_r) \in (\mathbb{N}^*)^r, \quad n = u\prod_{i=1}^{r} p_i^{\alpha_i}$$

Cette écriture est unique à l'ordre près des facteurs, i.e si

$$u\prod_{i=1}^{r} p_i^{\alpha_i} = u'\prod_{i=1}^{r'} q_i^{\beta_i},$$

alors, $u = u'$, $r = r'$, il existe une permutation σ de $[\![1,r]\!]$ telle que $\forall i \in [\![1,r]\!], p_i = q_{\sigma(i)}, \alpha_i = \beta_{\sigma(i)}$.

☞ **Remarque**
On dit que l'anneau $\mathbb{Z}$ est factoriel.

Démonstration. Ce théorème se prouve classiquement par récurrence forte. Attelons-nous à l'existence pour $n \geq 2$. Si $n = 2$, les entiers $u = 1, r = 1, p_1 = 2$ et α_2 conviennent. Soit à présent n un entier naturel tel que l'existence de la décomposition soit acquise pour tout entier naturel k inférieur ou égal à n. Montrons que l'entier $n+1$ peut se décomper d'une telle façon. Si $n+1$ est premier, on choisit alors $u = 1, r = 1, p_1 = n+1, \alpha_1 = 1$. Si $n+1$ n'est pas premier, alors on sait qu'il possède un diviseur positif premier p qui lui est strictementi inférieur, on écrit alors $n+1 = pk$ avec $k < n+1$. L'hypothèse de récurrence appliquée à k fournit alors une décomposition adéquate de k. En la multipliant par l'entier premier p, on obtient une décomposition adaptée de $n+1$ et la récurrence forte s'achève. Pour $n \leq -2$, il suffit d'appliquer ce qui précède à $-n$.
Démontrons l'unicité à l'ordre près par récurrence forte. Pour simplifier les choses, nous ordonnons les facteurs premiers. Pour tout entier $n \geq 2$, on note $\mathcal{H}_n$ le prédicat

$$\forall (r,s) \in (\mathbb{N}^*)^2, (p_1,\dots,p_r) \in \mathcal{P}^r, p_1 \leq \dots \leq p_r, (q_1,\dots,q_s) \in \mathcal{P}^s, q_1 \leq \dots \leq q_s, n = \prod_{i=1}^{r} p_i = \prod_{j=1}^{s} q_j \Rightarrow r = s \wedge (\forall i \in [\![1,r]\!], p_i = q_i)$$

Initialisation : pour $n = 2$, il est clair que cette décomposition est unique, $r = s = 1$ et $p_1 = q_1 = 2$. Soit $n \geq 2$ tel que $\forall k \leq n$, l'assertion $\mathcal{H}_k$ est vraie et montrons que $\mathcal{H}_{k+1}$ est vérifiée. Soit

$$n+1 = p_1 \dots p_r = q_1 \dots q_s$$

deux décompositions en facteurs premiers ordonnés de $n+1$. On considère alors les facteurs p_1 et q_1. Quitte à échanger les décompositions, on peut supposer que $p_1 \leq q_1$. Comme p_1 divise n, il divise le produit $q_1 \dots q_s$. Comme p_1 est premier, d'après le lemme d'Euclide, il existe un entier j dans $[\![1,s]\!]$ tel que p_1 divise q_j. Mais alors, comme q_j est premier, $p_1 = q_j$. D'après l'ordre croissant des $(q_j)_j$, on a alors $p_1 \leq q_1 \leq q_j = p_1$. On en déduit par double inégalité que $p_1 = q_1$. On a alors l'égalité d'entiers

$$k = \frac{n+1}{p_1} = p_2 \dots p_r = q_2 \dots q_r$$

Si $n+1$ est premier, il est égal à $p_1 = q_1$ et la décomposition est unique. Sinon, l'entier k appartient à $[\![2,n]\!]$ et l'hypothèse de récurrence $\mathcal{H}_k$ assure alors que $r-1 = s-1$ et $\forall j \in [\![2,r]\!], p_i = q_i$. En conclusion, $r = s$ et $\forall j \in [\![1,r]\!], p_j = q_j$. L'unicité est donc héréditaire et valide pour tout entier naturel $n \geq 2$ par récurrence. Si n est négatif, on applique ce qui précède à $-n$.

Afin de rendre cette écriture plus pratique à manipuler, on introduit la notion de valuation p-adique.

Définition 10 *Soit $p \in \mathcal{P}$ et $n \in \mathbb{Z}^*$. Si $|n| \geq 2$, on appelle valuation p-adique de n l'exposant de p dans la décomposition de n en facteurs premiers. Si l'entier p n'apparaît pas dans cette décomposition, on a $v_p(n) = 0$. Si $|n| = 1$, on convient que $v_p(\pm 1) = 0$.*

☞ **Remarque**
Cette définition est légitime d'après l'existence et l'unicité d'une telle décomposition. On convient parfois que $v_p(0) = +\infty$.

Propriété 35 *Soit $n \in \mathbb{N}^*$. Alors*

$$n = \prod_{p \in \mathcal{P}} p^{v_p(n)}$$

Démonstration. Si $n = 1$, alors pour tout entier premier p, $p^0 = 1$ et le produit vaut 1, ce qui est cohérent. Si $n \geq 2$, il s'agit essentiellement d'un jeu d'écriture. Le produit apparaissant à droite est fini, puisque la décomposition en produit de facteurs premiers ne comporte qu'un nombre fini de facteurs premiers. Si un facteur premier p n'apparaît pas dans la décomposition de n, $v_p(n) = 0$, donc $p^{v_p(n)} = p^0 = 1$, ce qui ne modifie pas le produit restant.

Propriété 36 *Soit $p \in \mathcal{P}$ et $n \in \mathbb{Z}^*$. Alors*

$$v_p(n) = \max\{k \in \mathbb{N} | p^k \mid n\}$$

Démonstration. D'après la décomposition de n en facteur premiers, $p^{v_p(n)}$ est un facteur de n, donc divise n. Si $p^{v_p(n)+1}$ divise n, ceci contredit l'unicité de cette décomposition. Donc $v_p(n) = \max\{k \in \mathbb{N} | p^k \mid n\}$.

Application 3 (Calculs de pgcd et de ppcm) *Soit $(a, b) \in (\mathbb{Z}^*)^2$ et $p \in \mathcal{P}$. Alors*

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

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

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

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 $D(a) \cap D(b)$ 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,

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

Définition 11 *Soit $n \in \mathbb{N}^*$, on note $\varphi(n)$ le cardinal de l'ensemble $\Delta_n = \{k \in [\![1, n]\!] | k \wedge n = 1\}$. L'application φ ainsi construite s'appelle l'indicatrice d'Euler.*

Exemple 8 $\varphi(1) = 1, \varphi(2) = 1, \varphi(3) = 2, \varphi(4) = 2, \varphi(12) = 4$.

Propriété 37 *Soit $p \in \mathcal{P}$, $k \in \mathbb{N}^*$, alors $\varphi(p^k) = (p-1)p^{k-1}$.*

Démonstration. Commençons par le cas $k = 1$, alors $A_p = [\![1, p-1]\!]$, donc $\varphi(p) = (p-1)$. Dans le cas général, soit $d \in [\![1, p^k]\!]$ tel que $d \wedge p^k = 1$. Alors d et p n'ont aucun facteur commun dans leur décomposition. En particulier, d n'est pas multiple de p. Réciproquement, si d n'est pas multiple de p et inférieur à p^k, il ne contient pas de facteur p dans sa décomposition en facteurs premiers, il est donc premier à p. Ainsi

$$A_{p^k} = [\![1, p^k]\!] \backslash p\mathbb{Z} = [\![1, p^k]\!] \backslash \{pm | m \in [\![1, p^{k-1}]\!]\}$$

On en déduit que $|A_{p^k}| = p^k - p^{k-1} = (p-1)p^{k-1}$.

Exemple 9 $\varphi(49) = 7 \times 6 = 42, \varphi(64) = 2^{6-1}(2-1) = 2^5 = 32$.

5 Congruences, arithmétique modulaire

On fixe n un entier naturel dans tout ce qui suit.

Définition 12 *Soit $(a,b) \in \mathbb{Z}^2$. On dit que a est congru à b modulo n lorsqu'il existe un entier relatif k tel que $a = b + kn$. On le note $a \equiv b[n]$.*

Propriété 38 *La relation de congruence modulo n est une relation d'équivalence.*

Démonstration. Soit $a \in \mathbb{Z}$, l'entier relatif $k = 0$ assure que $a = a + 0 \times 0$, donc que $a \equiv a[n]$. La relation est ainsi réflexive. Soit $(a,b) \in \mathbb{Z}^2$ tel que $a \equiv b[n]$. Soit alors $k \in \mathbb{Z}$ tel que $a = b + kn$, on en déduit que $b = a + (-k)n$. Comme $-k$ est un entier relatif, on en déduit que $b \equiv a[n]$, donc $b \equiv a[n]$. Ainsi, la relation est symétrique. Enfin, soit $(a,b,c) \in \mathbb{Z}^3$ tel que $a \equiv b[n]$ et $b \equiv c[n]$. On note alors k et k' des entiers relatifs tels que $a = b + kn$ et $b = c + k'n$. Cela entraîne $a = c + k'n + kn = c + (k + k')n$. Comme $k + k'$ est un entier relatif, $a \equiv c[n]$ et la relation est transitive.

☞ **Remarque**
Si $n = 0$, cette relation n'est rien d'autre que la relation d'égalité et l'ensemble quotient vaut $\mathbb{Z}$. Si $n = 1$, tout entier est congru à tout entier modulo 1, et l'ensemble quotient ne contient qu'un élément. En pratique, seuls les cas $n \geq 2$ nous intéressent.

Propriété 39 *Soit $(a,b) \in \mathbb{Z}^2$. Alors a divise b si et seulement si $b \equiv 0[a]$.*

Démonstration. Laissée à titre d'exercice.

Propriété 40 *La relation de congruence modulo n est compatible avec l'addition et la multiplication. Soit $(a,b,a',b') \in \mathbb{Z}^4$. On suppose que $a \equiv b[n]$ et $a' \equiv b'[n]$. Alors*

$$a + a' \equiv b + b'[n] \quad et \quad aa' \equiv bb'[n]$$

Démonstration. On note k, k' des entiers relatifs tels que $a = b + kn$ et $a' = b' + k'n$. Alors $a + a' = b + b' + n(k + k')$. Comme $k + k' \in \mathbb{Z}$, on a la relation $a + a' \equiv b + b'[n]$. En outre, $aa' = (b + kn)(b' + k'n) = bb' + n(kb' + k'b + nkk')$. On remarque alors que $k'b + kb' + nkk'$ est un entier relatif. Ainsi, $aa' \equiv bb'[n]$.

Propriété 41 *On suppose que n est non nul ici. Soit $(a,b) \in \mathbb{Z}^2$. Alors a est congru à b modulo n si et seulement si a et b ont même reste dans leur division euclidienne par n.*

Démonstration. Notons $a = q_a n + r_a$ et $b = q_b n + r_b$ les divisions euclidiennes respectives de a et b par n. Si a est congru à b modulo n, on note k un entier relatif tel que $a = b + kn$. Ces égalités entraînent alors $(q_a - q_b - k)n = r_b - r_a$ avec $-n + 1 < r_b - r_a < n$. Par conséquent, $r_b - r_a = 0$ puisque 0 est le seul multiple de n dans $[\![-n + 1, n - 1]\!]$. Réciproquement si $r_a = r_b$, alors $a = b + (q_a - q_b)n$ et $q_- q_b \in \mathbb{Z}$, donc $a \equiv b[n]$.

Définition 13 *Soit $a \in \mathbb{Z}$. On dit que a est inversible modulo n lorsqu'il existe un entier relatif b tel que $ab \equiv 1[n]$. Dans ce cas, on dit que b est un inverse de a modulo n.*

Propriété 42 *Soit $a \in \mathbb{Z}$. Alors a est inversible modulo n si et seulement si a est premier avec n.*

Démonstration. Supposons a inversible modulo n. D'après la définition, il existe un entier relatif b tel que $ab \equiv 1[n]$. On dispose alors d'un entier relatif k tel que $ab = 1 + kn$, mais alors dispose d'une relation de Bezout $ab + (-k)n = 1$ entre a et n, donc $a \wedge n = 1$. Réciproquement, si a est premier avec n, on dispose d'une relation de Bezout, $au + nv = 1$ avec $(u,v) \in \mathbb{Z}^2$. Mais alors $au \equiv 1[n]$ puisque v appartient à $\mathbb{Z}$. Ainsi, a est inversible modulo n et u en est un inverse modulo n.

✎ **Méthode**
Comment rechercher un inverse modulo n ? En examinant la preuve ci-dessous, on comprend que c'est la détermination d'une relation de Bezout qui fera tout fonctionner. On détermine via l'algorithme d'Euclide étendu un couple (u,v) d'entiers relatifs tel que $au + nv = 1$. Cela suffit à affirmer que u est un inverse modulo n de a.

Application 4 (Résolution de congruences) *Soit $(a,b) \in \mathbb{Z}^* \times \mathbb{Z}$. On cherche à déterminer l'ensemble des entiers relatifs x tels que $ax \equiv b[n]$. On envisage différents cas*

- *Les entiers a et n sont premiers entre eux. Alors, en notant u un inverse de a modulo n, l'ensemble des solutions vaut $\{bu + kn | k \in \mathbb{Z}\}$.*

— *Les entiers a et n ne sont pas premiers entre eux. On note alors $d = a \wedge n$. L'ensemble des solutions est non vide si et seulement si d divise b. Dans ce cas, si l'on note u un inverse de a/d modulo n/d auquel cet ensemble vaut $\{u\frac{b}{d} + k\frac{n}{d} | k \in \mathbb{Z}\}$.*

Théorème 9 (Petit théorème de Fermat) *Soit $a \in \mathbb{Z}$ et $p \in \mathcal{P}$. On suppose que $a \wedge p = 1$. Alors*

$$a^{p-1} \equiv 1[p]$$

Plus généralement,

$$\forall a \in \mathbb{Z}, a^p \equiv a[p]$$

Démonstration. L'application $g : [\![1, p-1]\!] \to [\![1, p-1]\!], j \mapsto aj \mod p$ (comprendre le reste de aj dans la divsion euclidienne par p) est bien définie et bijective. En effet, p est premier avec a donc, pour tout j dans $[\![1, p-1]\!]$, le reste de aj modulo p est non nul. De plus, si aj et ai ont même reste, comme a est inversible modulo p, $i = j$. On en déduit par commutativité du produit que

$$\prod_{j=1}^{p-1} (aj) \equiv \prod_{j=1}^{p-1} j[p]$$

soit encore

$$a^{p-1}(p-1)! \equiv (p-1)![p]$$

Toutefois, $(p-1)!$ est premier avec p, donc inversible modulo p, on en déduit après multiplication par un inverse modulo p de $(p-1)!$ que $a^{p-1} \equiv 1[p]$. Dans le cas plus général, si $a \wedge p \neq 1$, alors p divise a, donc p divise a^p. On a de manière cohérente $a^p \equiv 0 \equiv a[p]$.

⚠ **Attention**
La réciproque est fausse. L'entier $q = 561$ n'est pas premier (il vaut $3 \times 11 \times 17$). Pourtant pour tout entier a, q divise $a^q - a$.

Exercice 3
1. *Montrer que pour tout p dans $\mathcal{P}$, tout n dans $[\![1, p-1]\!]$, p divise $\binom{p}{n}$ via le lemme de Gauss.*
2. *En déduire, à l'aide du binôme, le petit théorème de Fermat par récurrence sur a.*