ARITHMÉTIQUE DES ENTIERS RELATIFS

1 DIVISIBILITÉ ET DIVISION ENTIÈRES

1.1 RELATION DE DIVISIBILITÉ

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

Pour tout $a \in \mathbb{Z}$, l'ensemble des multiples de a n'est autre que l'ensemble $a\mathbb{Z} = \{ak \mid k \in \mathbb{Z}\}$. Quant à l'ensemble des diviseurs de a, il sera noté $\mathrm{div}(a)$ dans ce cours, mais il ne s'agit pas d'une notation universelle.

Deux remarques en passant : $\mathrm{div}(a) = \mathrm{div}(|a|)$ et pour $a \neq 0$: $\max \mathrm{div}(a) = |a|$.

Il est important de savoir lier les relations $\mid$ et $\leqslant$. Pour tous $a, b \in \mathbb{N}^*$ — ON EXCLUT 0, ATTENTION : $a \mid b \implies a \leqslant b.$

Exemple $\mathrm{div}(0) = \mathbb{Z}$, $\mathrm{div}(8) = \{\pm 1, \pm 2, \pm 4, \pm 8\}$ et $\mathrm{div}(12) = \{\pm 1, \pm 2, \pm 3, \pm 4, \pm 6, \pm 12\}$.

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

(i) **Relation d'ordre :** La relation de divisibilité $\mid$ est une relation d'ordre sur $\mathbb{N}$ MAIS elle est seulement réflexive et transitive sur $\mathbb{Z}$ car : $a \mid b$ et $b \mid a \iff |a| = |b| \iff a = b$ ou $a = -b$.

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

(iii) **Produit :** Si $a \mid b$ et $c \mid d$: $ac \mid bd$ et en particulier : $a^k \mid b^k$ pour tout $k \in \mathbb{N}$.

Que peut-on dire de a et b quand on sait qu'ils ont les mêmes diviseurs, i.e. que $\mathrm{div}(a) = \mathrm{div}(b)$? Le cas échéant : $a \mid b$ et $b \mid a$, donc $|a| = |b|$ d'après (i).

Démonstration

(i) Faisons l'hypothèse que $a \mid b$ et $b \mid a$. Ainsi $b = ak$ et $a = bl$ pour certains $k, l \in \mathbb{Z}$, donc $b = bkl$.

— Si $b = 0$: $a = bl = 0$ donc $|a| = |b|$.

— Si au contraire $b \neq 0$: $kl = 1$, donc soit $k = l = 1$, soit $k = l = -1$. Bref : $a = \pm b$, i.e. $|a| = |b|$.

(ii) Par hypothèse : $a = dk$ et $b = dl$ pour certains $k, l \in \mathbb{Z}$, donc : $au + bv = d(ku + vl)$ et $ku + vl \in \mathbb{Z}$ pour tous $u, v \in \mathbb{Z}$, et enfin $d \mid (au + bv)$.

(iii) Par hypothèse : $b = ak$ et $d = cl$ pour certains $k, l \in \mathbb{Z}$, donc : $bd = (ac)(kl)$ et $kl \in \mathbb{Z}$, donc $ac \mid bd$.

1.2 RELATION DE CONGRUENCE MODULO UN ENTIER

Définition **(Relation de congruence modulo un entier)** Soient $a, b, n \in \mathbb{Z}$. On dit que a *est congru à* b *modulo* n si $n \mid (b - a)$, i.e. s'il existe un entier $k \in \mathbb{Z}$ pour lequel $a = b + kn$. Cette relation se note : $a \equiv b\ [n]$.

Les relations de congruence généralisent la relation de divisibilité : $n \mid a \iff a \equiv 0\ [n].$

Fondamentale dans les deux sens, cette petite équivalence nous permettra de passer du vocabulaire de la divisibilité à celui des congruences et réciproquement.

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

(i) **Relation d'équivalence :** La relation $\equiv\ [n]$ est une relation d'équivalence sur $\mathbb{Z}$.

(ii) **Somme :** Si $a \equiv b\ [n]$ et $a' \equiv b'\ [n]$: $\quad a + a' \equiv b + b'\ [n]$.

(iii) **Produit :** Si $a \equiv b\ [n]$ et $a' \equiv b'\ [n]$: $\quad aa' \equiv bb'\ [n]$, et en particulier : $\quad a^k \equiv b^k\ [n]$ pour tout $k \in \mathbb{N}$.

(iv) **Multiplication/division par un entier non nul :** Si m est non nul : $\quad a \equiv b\ [n] \iff ma \equiv mb\ [mn]$.

Démonstration L'assertion (i) a été prouvée au chapitre « Relations binaires ».

(ii) Par hypothèse, n divise $b-a$ et $b'-a'$, donc aussi $(b+b')-(a+a')$ par somme, donc $a+a' \equiv b+b'\ [n]$.

(iii) Remarque : $\quad bb'-aa' = b(b'-a')+a'(b-a)$. Or par hypothèse, n divise $b-a$ et $b'-a'$, donc également $b(b'-a')+a'(b-a) = bb'-aa'$ par combinaison linéaire, donc $aa' \equiv bb'\ [n]$.

(iv) $\quad a \equiv b\ [n] \iff n \mid (b-a) \overset{m \neq 0}{\iff} mn \mid m(b-a) \iff ma \equiv mb\ [mn]$. ∎

Exemple $2^{345} + 5^{432}$ est divisible par 3.

Démonstration $2^{345} + 5^{432} \equiv (-1)^{345} + (-1)^{432} \equiv -1 + 1 \equiv 0\ [3]$.

Exemple Pour tout $n \in \mathbb{Z}$ impair : $\quad n^2 \equiv 1\ [8]$.

Démonstration Soit $n \in \mathbb{Z}$ impair, disons $n = 2k+1$ pour un certain $k \in \mathbb{Z}$.

Alors : $\quad n^2 = 4k^2 + 4k + 1 = 4k(k+1) + 1$. Or k ou $k+1$ est pair car ces deux entiers sont consécutifs, donc $k(k+1)$ est pair aussi : $\quad k(k+1) \equiv 0\ [2]$. A fortiori : $\quad 4k(k+1) \equiv 0\ [8]$, et enfin $n = 4k(k+1)+1 \equiv 1\ [8]$.

Un point de vue utile à présent sur les congruences. Pour un entier $n \in \mathbb{N}$ donné, raisonner modulo n^2+1 revient à considérer, en un sens, que « $n^2 = -1$ », MAIS pas vraiment en fait, seulement au sens d'une congruence : $\quad n^2 \equiv -1\ \left[n^2+1\right]$. Par exemple : $\quad n^4 - 3n^3 + 2n^2 + 1 \equiv \left(n^2\right)^2 - 3n \times n^2 + 2n^2 + 1 \equiv (-1)^2 - 3n \times (-1) + 2 \times (-1) + 1 \equiv 3n\ \left[n^2+1\right]$.

Si on raisonne maintenant modulo $n-2$, on peut considérer que « $n = 2$ » intuitivement, mais à proprement parler : $n \equiv 2\ [n-2]$. Dans ce cas, pour tout $k \in \mathbb{N}$: $\quad n^k \equiv 2^k\ [n-2]$, et si on additionne ces relations après les avoir multipliées par des entiers, on en tire que pour tout polynôme P à coefficients entiers : $\quad P(n) \equiv P(2)\ [n-2]$. En d'autres termes, si on considère que « $n = 2$ », alors il faut aussi considérer que « $P(n) = P(2)$ ».

1.3 Introduction aux nombres premiers

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

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

Il n'est pas inutile de connaître la liste des premiers nombres premiers : 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37… Nous étudierons plus loin un procédé mécanique — mais coûteux — pour les déterminer tous.

Le résultat suivant est un théorème d'EXISTENCE facile à démontrer. Nous aurons plus tard un théorème d'UNICITÉ, mais nettement plus difficile à obtenir.

Théorème **(Existence de la factorisation première)** Tout entier naturel non nul est un produit de nombres premiers.

Dans cet énoncé lapidaire, on considère 1 comme le produit de 0 nombre premier et tout nombre premier comme le produit d'1 nombre premier — soi-même.

Démonstration Par récurrence forte.

- **Initialisation :** 1 n'est divisible par aucun nombre premier, c'est le produit de zéro d'entre eux.
- **Hérédité :** Soit $n \geqslant 2$. Faisons l'hypothèse que tout entier naturel non nul strictement inférieur à n est un produit de nombres premiers. Qu'en est-il de n ? Deux cas possibles — soit n est premier, soit n est composé. Si n est premier, c'est terminé, il est produit de nombres premiers. Et s'il est composé ? Il s'écrit dans ce cas : $\quad n = ab \quad$ où a et b sont deux diviseurs positifs de n strictement inférieurs à n. Par hypothèse de récurrence, a et b sont des produits de nombres premiers, donc n aussi par produit. ∎

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

Démonstration Raisonnons par l'absurde en supposant $\mathbb{P}$ fini et notons $p_1, \dots, p_r$ la liste complète des nombres premiers. Posons ensuite $N = p_1 \dots p_r + 1$. Cet entier N, au moins égal à 2, est un produit de nombres premiers d'après le théorème précédent, donc est divisible par p_k pour un certain $k \in [\![1, r]\!]$. En particulier, p_k divise $N - p_1 \dots p_r = 1$, donc $p_k = 1$ — contradiction.

Le *crible d'Ératosthène* permet une détermination simple de tous les nombres premiers inférieurs à un seuil donné et repose sur la remarque suivante. Si un entier $n \in \mathbb{N}^*$ est composé et si nous notons p le plus petit de ses diviseurs premiers : $n = pk$ pour un certain $k \in \mathbb{N}^*$, mais comme alors tout diviseur premier de k est supérieur ou égal à p, en particulier $k \geqslant p$, et donc : $n = pk \geqslant p^2$, i.e. $p \leqslant \sqrt{n}$. En résumé :

Tout entier COMPOSÉ $n \in \mathbb{N}^*$ possède un diviseur premier inférieur ou égal à $\sqrt{n}$.

Nous pouvons en déduire la liste de tous les nombres premiers inférieurs ou égaux à 100. On part d'une liste des entiers de 2 à 100, dont on va peu à peu rayer les entiers composés et dont ne resteront vierges à la fin que les nombres premiers.

- L'entier 2 est premier, c'est notre point de départ. On raye tous ses multiples hormis lui-même, car ceux-ci sont composés.
- Le premier entier non rayé est alors 3. Il est forcément premier car s'il était composé, il aurait un diviseur premier strictement inférieur — ici 2 — et on l'aurait déjà rayé. On raye tous les multiples de 3 hormis lui-même, car ceux-ci sont composés.
- Même chose avec 5, même chose avec 7. Le premier entier non rayé est alors 11. Or tout entier compris entre 2 et 100 possède un diviseur premier inférieur ou égal à $\sqrt{100} = 10$, donc en fait en rayant les entiers que nous avons rayés, nous avons rayés tous les entiers composés compris entre 2 et 100. Les entiers non rayés restants sont exactement tous les nombres premiers de la liste étudiée.

	2	**3**	4	**5**	6	**7**	8	9	10
11	12	**13**	14	15	16	**17**	18	**19**	20
21	22	**23**	24	25	26	27	28	**29**	30
31	32	33	34	35	36	**37**	38	39	40
41	42	**43**	44	45	46	**47**	48	49	50
51	52	**53**	54	55	56	57	58	**59**	60
61	62	63	64	65	66	**67**	68	69	70
71	72	**73**	74	75	76	77	78	**79**	80
81	82	**83**	84	85	86	87	88	**89**	90
91	92	93	94	95	96	**97**	98	99	100

1.4 Division euclidienne

Théorème (Théorème de la division euclidienne) Soient $a \in \mathbb{Z}$ et $b \in \mathbb{N}^*$. Il existe un et un seul couple $(q, r) \in \mathbb{Z} \times \mathbb{N}$ pour lequel : $a = bq + r$ et $0 \leqslant r \leqslant b - 1$ (ou encore : $0 \leqslant r < b$). On appelle a le *dividende* de la division euclidienne de a par b, b son *diviseur*, q son *quotient* et r son *reste*. Par ailleurs : $q = \left\lfloor \frac{a}{b} \right\rfloor$ et $r \equiv a\ [b]$.

Le théorème de la division euclidienne est un résultat d'EXISTENCE et d'UNICITÉ, voilà l'essentiel.

On peut le reformuler en termes de congruences : $\forall a \in \mathbb{Z},\ \exists!\, r \in [\![0, b-1]\!],\ a \equiv r\ [b]$, ce qui signifie que tout entier relatif a est congru modulo b à un unique entier r COMPRIS ENTRE 0 ET $b-1$. L'ensemble quotient de $\mathbb{Z}$ par la relation $\equiv\ [b]$ est donc l'ensemble $\left\{b\mathbb{Z}, b\mathbb{Z}+1, \dots, b\mathbb{Z}+b-1\right\}$ à b éléments noté généralement $\frac{\mathbb{Z}}{b\mathbb{Z}}$. Par exemple, on peut ramener $a = 433$ à l'un des entiers 0, 1, 2, 3 ou 4 modulo $b = 5$. Précisément : $\underbrace{433}_{a} = \underbrace{5}_{b} \times \underbrace{86}_{q} + \underbrace{3}_{r}$ donc $433 \equiv 3\ [5]$.

Démonstration

- **Existence :** L'idée de la preuve est simple. Si a est positif, on lui retranche b une fois, deux fois, trois fois… jusqu'à ce que a ait presque complètement fondu, c'est-à-dire jusqu'au moment où le résultat est compris entre 0 et $b-1$. Si a est négatif, on fait pareil mais en ajoutant b au lieu de le retrancher.

  L'ensemble $\mathscr{D} = (a + b\mathbb{Z}) \cap \mathbb{N}$ est une partie non vide de $\mathbb{N}$ car il contient $a = a - b \times 0$ si $a \geqslant 0$ et $a - ba$ si $a < 0$. Cet ensemble possède ainsi un plus petit élément r, et par définition de $\mathscr{D}$: $a = bq + r$ pour un certain $q \in \mathbb{Z}$. Se peut-il qu'on ait $r \geqslant b$? Si c'était le cas, $a - b(q+1) = r - b$ serait un élément de $\mathscr{D}$ strictement plus petit que $r = \min \mathscr{D}$ — impossible. Conclusion : $0 \leqslant r \leqslant b - 1$.
- **Unicité :** Soient (q, r) et (q', r') deux couples de division euclidienne de a par b. Aussitôt $|r' - r| < b$, mais par ailleurs : $b(q - q') = r' - r$, donc : $b \times |q - q'| < b$, donc $|q - q'| < 1$. Comme $q - q'$ est un entier, cela veut dire que $q = q'$, et en retour : $r = a - bq = a - bq' = r'$.
- Pour finir : $0 \leqslant r = a - bq < b$, donc : $\frac{a}{b} - 1 < q \leqslant \frac{a}{b}$, donc en effet $q = \left\lfloor \frac{a}{b} \right\rfloor$.

Ainsi, le couple (q,r) de la division euclidienne de a par b se calcule à partir de a par une série d'additions/soustractions, mais pour diviser 1000 par 3, sommes-nous vraiment obligés d'effectuer 333 soustractions ? Oui et non.

Tâchons de le comprendre sur la division de 347 par 5. Dans un premier temps, on retranche en apparence $6\times 5=30$ de 34, mais en réalité, c'est $60\times 5=300$ qu'on retranche de 347. Dans un second temps, on retranche $9\times 5=45$ de 47. Au total, on a donc effectué 69 soustractions mais en deux fois seulement — d'abord 60, puis 9. Le reste obtenu est 2. Conclusion :

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

DIVISER, C'EST SOUSTRAIRE.

Pour un ordinateur, un grand nombre de soustractions n'est pas un problème. Pour nous autres cerveaux c'en est un. Nous compensons en apprenant et en utilisant les tables de multiplication, car ça nous le faisons vite et bien. C'est grâce aux tables de multiplication que nous avons trouvé les chiffres « 6 » et « 9 » du quotient dans l'exemple précédent.

On s'intéresse dans l'exemple qui suit à la première *équation diophantienne* de ce chapitre. On appelle ainsi toute équation à inconnues entières construite à partir des seules opérations d'addition et de multiplication — par exemple, les équations $2x+3y=5$ ou $x^3+2=y^4$ d'inconnue $(x,y)\in\mathbb{Z}^2$.

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

Démonstration Supposons par l'absurde que ni x ni y ni z n'est divisible par 3. Le reste de la division euclidienne de x par 9 est alors l'un des entiers 1, 2, 4, 5, 7, 8 — on peut rejeter les cas 0, 3 et 6. Le tableau ci-contre montre que : $x^3\equiv\pm 1\ [9]$, et bien sûr de même : $y^3\equiv\pm 1\ [9]$ et $z^3\equiv\pm 1\ [9]$.

Or par hypothèse : $x^3+y^3\equiv z^3\ [9]$. À gauche, x^3+y^3 est congru modulo 9 à : $1+1=2$ ou $1-1=0$ ou $-1+1=0$ ou $-1-1=-2$, alors qu'à droite : $z^3\equiv\pm 1\ [9]$ — contradiction !

$x\ [9]$	$x^2\ [9]$	$x^3\ [9]$
1	1	1
2	4	$8\equiv -1$
4	$16\equiv -2$	$-8\equiv 1$
$5\equiv -4$	$16\equiv -2$	$8\equiv -1$
$7\equiv -2$	4	$-8\equiv 1$
$8\equiv -1$	1	-1

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

Démonstration La démonstration de ce résultat serait TRÈS longue si on appliquait l'algorithme précédent comme un rustre, car l'entier 2^{65362} possède près de 20000 décimales. Heureusement : $2^3\equiv 8\equiv 1\ [7]$. C'est l'idée-phare de cet exemple — dénicher, si elle existe, la première puissance de 2 congrue à 1 modulo 7. Une fois qu'on en a trouvé une, c'est facile, on peut « raisonner modulo 3 dans l'exposant » car pour tout $k,r\in\mathbb{N}$: $2^{3k+r}\equiv 1^k\times 2^r\equiv 2^r\ [7]$. En l'occurrence, ici : $65362\equiv 1\ [3]$, donc $2^{65362}\equiv 2^1\equiv 2\ [7]$.

2 PGCD, PPCM

Définition (Diviseur/multiple commun) Soient $a_1,\dots,a_r\in\mathbb{Z}$.

- **Diviseur commun :** On appelle *diviseur commun de* $a_1,\dots,a_r$ tout entier relatif qui divise à la fois $a_1,\dots,a_r$.
- **Multiple commun :** On appelle *multiple commun de* $a_1,\dots,a_r$ tout entier relatif divisible à la fois par $a_1,\dots,a_r$.

Exemple Les diviseurs communs de 12 et 18 sont ± 1, ± 2, ± 3 et ± 6 car :

$$\mathrm{div}(12)\cap\mathrm{div}(18)=\{\pm 1,\pm 2,\pm 3,\pm 4,\pm 6,\pm 12\}\cap\{\pm 1,\pm 2,\pm 3,\pm 6,\pm 9,\pm 18\}=\{\pm 1,\pm 2,\pm 3,\pm 6\}.$$

Les multiples communs de 12 et 18 sont tous les multiples de 36 : $12\mathbb{Z}\cap 18\mathbb{Z}=36\mathbb{Z}$, mais nous ne chercherons pas à le justifier pour le moment.

2.1 PGCD DE DEUX ENTIERS

Définition-théorème (PGCD de deux entiers) Soient $a,b\in\mathbb{Z}$ deux entiers dont l'un au moins est non nul. On appelle *plus grand commun diviseur* (ou *PGCD*) *de* a *et* b et on note $a\wedge b$ le plus grand élément au sens de la relation $\leqslant$ de l'ensemble des diviseurs communs de a et b. En résumé : $a\wedge b=\max\big(\mathrm{div}(a)\cap\mathrm{div}(b)\big)$.

On pose par ailleurs : $0\wedge 0=0$.

Démonstration Pour justifier l'existence de $a \wedge b$ dans le cas où a est non nul, remarquons simplement que l'ensemble des diviseurs communs de a et b contient 1 et est majoré par $|a|$. Cet ensemble est donc une partie non vide majorée de $\mathbb{Z}$, donc possède un plus grand élément. ■

Exemple $12 \wedge 18 = 6$ car d'après l'exemple précédent : $\operatorname{div}(12) \cap \operatorname{div}(18) = \{\pm 1, \pm 2, \pm 3, \pm 6\}$.

Exemple Pour tous $a, b \in \mathbb{Z}$: $a \wedge b = |a| \wedge |b|$, $a \wedge b = b \wedge a$, $a \wedge 1 = 1$ et $a \wedge 0 = |a|$.

Démonstration Pour $(a,b) \neq (0,0)$: $\operatorname{div}(a) \cap \operatorname{div}(b) = \operatorname{div}\big(|a|\big) \cap \operatorname{div}\big(|b|\big)$, $\operatorname{div}(a) \cap \operatorname{div}(b) = \operatorname{div}(b) \cap \operatorname{div}(a)$,
$\operatorname{div}(a) \cap \operatorname{div}(1) = \operatorname{div}(a) \cap \{\pm 1\} = \{\pm 1\}$ et $\operatorname{div}(a) \cap \operatorname{div}(0) = \operatorname{div}(a) \cap \mathbb{Z} = \operatorname{div}(a)$.

Théorème (Idée fondamentale de l'algorithme d'Euclide) Pour tous $a, b, n \in \mathbb{Z}$, si $a \equiv b\ [n]$: $a \wedge n = b \wedge n$.

En particulier, pour tous $a \in \mathbb{Z}$ et $b \in \mathbb{N}^*$, si on note r le reste de la division euclidienne de a par b : $a \wedge b = b \wedge r$, et la preuve ci-dessous montre en passant que : $\operatorname{div}(a) \cap \operatorname{div}(b) = \operatorname{div}(b) \cap \operatorname{div}(r)$.

Démonstration Supposons $a \equiv b\ [n]$, i.e. $b = a + kn$ pour un certain $k \in \mathbb{Z}$. Tout diviseur commun de a et n divise aussi $a + kn = b$ et n, et inversement, tout diviseur commun de b et n divise aussi $a = b - kn$ et n. Conclusion : $\operatorname{div}(a) \cap \operatorname{div}(n) = \operatorname{div}(b) \cap \operatorname{div}(n)$. Le résultat demandé est dès lors établi dans le cas où $n \neq 0$ car ces deux intersections ont le même maximum, et le résultat est une évidence pour $n = 0$. ■

Exemple Pout tout $n \in \mathbb{Z}$: $(3n+1) \wedge (2n+5) = \begin{cases} 13 & \text{si } n \equiv 4\ [13] \\ 1 & \text{sinon.} \end{cases}$

Démonstration
$$\begin{aligned} (3n+1) \wedge (2n+5) &= (n-4) \wedge (2n+5) && \text{car } 3n+1 \equiv n-4\ [2n+5] \\ &= (n-4) \wedge 13 && \text{car } n \equiv 4\ [n-4]. \end{aligned}$$

Théorème (Diviseurs communs et diviseurs du PGCD pour deux entiers) Soient $a, b \in \mathbb{Z}$. Les diviseurs communs de a et b sont exactement les diviseurs de $a \wedge b$: $\operatorname{div}(a) \cap \operatorname{div}(b) = \operatorname{div}(a \wedge b)$.

Démonstration Nous allons mettre en œuvre dans cette preuve un algorithme de calcul du PGCD qu'on appelle l'*algorithme d'Euclide*.

- **Algorithme d'Euclide :** Soient $a, b \in \mathbb{N}$ deux entiers pour lesquels $0 \leqslant b \leqslant a$. On définit une suite d'entiers naturels $r_0, r_1, r_2 \ldots$ de la manière suivante.
  - Au départ, on pose $r_0 = a$ et $r_1 = b$.
  - Ensuite, pour $k \in \mathbb{N}$, TANT QUE $r_{k+1} \neq 0$, on note r_{k+2} le reste de la division euclidienne de r_k par r_{k+1}, ce qui implique en particulier que $r_{k+2} < r_{k+1}$.

  À l'issue de cette construction : $r_0 \geqslant r_1 > r_2 > \ldots \geqslant 0$, et comme il n'existe qu'un nombre FINI d'entiers naturels entre 0 et r_0, on obtient forcément $r_N = 0$ pour un certain $N \in \mathbb{N}^*$ — l'algorithme se termine. Or, en vertu de l'idée fondamentale de l'algorithme d'Euclide :
  $$a \wedge b = r_0 \wedge r_1 = r_1 \wedge r_2 = \ldots = r_{N-1} \wedge r_N = r_{N-1} \wedge 0 = r_{N-1}$$
  et :
  $$\begin{aligned} \operatorname{div}(a) \cap \operatorname{div}(b) &= \operatorname{div}(r_0) \cap \operatorname{div}(r_1) = \operatorname{div}(r_1) \cap \operatorname{div}(r_2) = \ldots = \operatorname{div}(r_{N-1}) \cap \operatorname{div}(r_N) \\ &= \operatorname{div}(r_{N-1}) \cap \operatorname{div}(0) = \operatorname{div}(r_{N-1}) \cap \mathbb{Z} = \operatorname{div}(r_{N-1}) = \operatorname{div}(a \wedge b). \end{aligned}$$
- **Extension au cas général :** Dans le cas général de deux entiers a et b quelconques, on se ramène au cas où $0 \leqslant b \leqslant a$ de la manière suivante. On peut supposer a et b positifs car $a \wedge b = |a| \wedge |b|$, et on peut supposer $b \leqslant a$ car $a \wedge b = b \wedge a$. ■

L'*algorithme d'Euclide* est un algorithme de calcul effectif du PGCD de deux entiers relatifs. Dans le cas principal où $0 \leqslant b \leqslant a$, il a été montré en particulier que $a \wedge b = r_{N-1}$ où r_{N-1} est le dernier entier non nul de la liste $r_0, r_1, r_2 \ldots$

$a \wedge b$ est le DERNIER RESTE NON NUL de la suite des restes successifs $r_0, r_1, r_2 \ldots$

Exemple $1542 \wedge 58 = 2$.

Démonstration Il s'agit seulement d'effectuer quelques divisions euclidiennes : $\underline{1542} = 26 \times \underline{58} + \underline{34}$,
$\underline{58} = 1 \times \underline{34} + \underline{24}$, $\underline{34} = 1 \times \underline{24} + \underline{10}$, $\underline{24} = 2 \times \underline{10} + \underline{4}$, $\underline{10} = 2 \times \underline{4} + \underline{2}$ et $\underline{4} = 2 \times \underline{2} + \underline{0}$.

Théorème **(Relations de Bézout pour deux entiers)** Soient $a,b\in\mathbb{Z}$. Il existe des entiers $u,v\in\mathbb{Z}$ pour lesquels : $a\wedge b=au+bv$. Une telle relation est appelée UNE *relation de Bézout de a et b*.

Attention ! Les entiers u et v ne sont pas du tout uniques.

Par exemple : $4\wedge 6=2$, mais on a à la fois : $2=\underline{4}\times(-1)+\underline{6}\times 1$ et $2=\underline{4}\times 2+\underline{6}\times(-1)$.

Démonstration On peut supposer sans perte de généralité que $0\leqslant b\leqslant a$. Reprenons les restes successifs de l'algorithme d'Euclide en posant $r_0=a$ et $r_1=b$ et en notant pour tout $k\in\mathbb{N}$, tant que $r_{k+1}\neq 0$, r_{k+2} le reste de la division euclidienne de r_k par r_{k+1}. Le quotient de cette division euclidienne sera quant à lui noté q_{k+2} : $r_{k+2}=r_k-q_{k+2}r_{k+1}$. La suite ainsi construite est finie de rang final N pour lequel $r_N=0$.

On définit alors deux nouvelles suites $(u_k)_{0\leqslant k\leqslant N}$ et $(v_k)_{0\leqslant k\leqslant N}$ par : $(u_0,v_0)=(1,0)$, $(u_1,v_1)=(0,1)$ et pour tout $k\in[\![0,N-2]\!]$: $(u_{k+2},v_{k+2})=\big(u_k-q_{k+2}u_{k+1},v_k-q_{k+2}v_{k+1}\big)$. Montrons par récurrence double que pour tout $k\in[\![0,N]\!]$: $r_k=au_k+bv_k$.

Initialisation : $r_0=a=a\times 1+b\times 0=au_0+bv_0$ et $r_1=b=a\times 0+b\times 1=au_1+bv_1$.

Hérédité : Soit $k\in[\![0,N-2]\!]$. Si $r_k=au_k+bv_k$ et $r_{k+1}=au_{k+1}+bv_{k+1}$:

$$r_{k+2}=r_k-q_{k+2}r_{k+1}\overset{\text{HDR}}{=}\big(au_k+bv_k\big)-q_{k+2}\big(au_{k+1}+bv_{k+1}\big)=a\big(u_k-q_{k+2}u_{k+1}\big)+b\big(v_k-q_{k+2}v_{k+1}\big)=au_{k+2}+bv_{k+2}.$$

En particulier : $a\wedge b=r_{N-1}=au_{N-1}+bv_{N-1}$.

Le procédé de construction des entiers u et v de la démonstration qui précède s'appelle l'*algorithme d'Euclide étendu*. En résumé, alors que l'algorithme d'Euclide ne s'intéresse qu'aux restes des divisions euclidiennes successives effectuées, l'algorithme d'Euclide étendu va plus loin en tenant compte aussi des quotients successifs obtenus. Un tableau bien présenté peut faciliter les calculs, mais c'est sans obligation.

Quelle est finalement l'idée principale de l'algorithme ? Les entiers u_k et v_k sont construits de proche en proche avec un seul et unique souci — maintenir vraie l'égalité : $r_k=au_k+bv_k$. Ensuite, on passe de r_k et r_{k+1} à r_{k+2} grâce à la relation : $r_{k+2}=r_k-q_{k+2}r_{k+1}$ et le même calcul permet de passer de u_k et u_{k+1} à u_{k+2} (resp. v_k et v_{k+1} à v_{k+2}) : $u_{k+2}=u_k-q_{k+2}u_{k+1}$ (resp. $v_{k+2}=v_k-q_{k+2}v_{k+1}$).

Les colonnes « r_k » et « q_k » sont remplies selon les règles de division de l'algorithme d'Euclide simple.

k	q_k	$r_k=au_k+bv_k$	u_k	v_k
0		a	1	0
1		b	0	1
2	Quotient	Reste		
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$
$N-1$	q_{N-1}	$a\wedge b$	u	v

Les colonnes « u_k » et « v_k » de l'algorithme étendu sont remplies grâce aux relations : $u_{k+2}=u_k-q_{k+2}u_{k+1}$ et $v_{k+2}=v_k-q_{k+2}v_{k+1}$.

Le couple (u,v) cherché !

Et sur un exemple ? Voyons ce que cela donne sur les entiers 525 et 3080.

Le tableau ne contient que 5 lignes car $r_5=0$.

Relation de Bézout :

$$3080\wedge 525=35=7\times 3080-41\times 525.$$

k	r_k	q_k	u_k	v_k
0	3080		1	0
1	525		0	1
2	455	5	1	−5
3	70	1	−1	6
4	35	6	7	−41

Théorème **(Propriétés du PGCD de deux entiers)** Soient $a,b,c,k\in\mathbb{Z}$.

(i) **Associativité :** $(a\wedge b)\wedge c=a\wedge(b\wedge c)$.

(ii) **Factorisation par un diviseur commun :** $(ak)\wedge(bk)=|k|(a\wedge b)$.

Démonstration

(i) $\operatorname{div}\big((a\wedge b)\wedge c\big)=\operatorname{div}(a\wedge b)\cap\operatorname{div}(c)=\operatorname{div}(a)\cap\operatorname{div}(b)\cap\operatorname{div}(c)=\operatorname{div}(a)\cap\operatorname{div}(b\wedge c)=\operatorname{div}\big(a\wedge(b\wedge c)\big)$.

(ii) Nous pouvons supposer $k \neq 0$. Pour commencer : $|k|(a \wedge b) \in \mathrm{div}(ak) \cap \mathrm{div}(bk) = \mathrm{div}\big((ak) \wedge (bk)\big)$, i.e. $|k|(a \wedge b)$ divise $(ak) \wedge (bk)$. Inversement : $|k| \in \mathrm{div}(ak) \cap \mathrm{div}(bk) = \mathrm{div}\big((ak) \wedge (bk)\big)$, donc : $(ak) \wedge (bk) = |k| \times d$ pour un certain $d \in \mathbb{N}$. Dans ces conditions, $|k| \times d$ divise ak et bk, or $k \neq 0$, donc : $d \in \mathrm{div}(a) \cap \mathrm{div}(b) = \mathrm{div}(a \wedge b)$. En d'autres termes, d divise $a \wedge b$, donc $(ak) \wedge (bk) = |k| \times d$ divise $|k|(a \wedge b)$. Comme voulu : $(ak) \wedge (bk) = |k|(a \wedge b)$. ∎

2.2 PGCD d'une famille finie d'entiers

Définition **(PGCD d'une famille finie d'entiers)** Soient $a_1, \dots, a_r \in \mathbb{Z}$ des entiers dont l'un au moins est non nul. On appelle *plus grand commun diviseur* (ou *PGCD*) *de* $a_1, \dots, a_r$ et on note $a_1 \wedge \dots \wedge a_r$ le plus grand élément au sens de la relation $\leqslant$ de l'ensemble des diviseurs communs de $a_1, \dots, a_r$. En résumé : $a_1 \wedge \dots \wedge a_r = \max\Big(\mathrm{div}(a_1) \cap \dots \cap \mathrm{div}(a_r)\Big)$.

On pose par ailleurs pour tout $r \geqslant 2$: $\overbrace{0 \wedge \dots \wedge 0}^{r \text{ fois}} = 0$.

Exemple $28 \wedge 42 \wedge 98 = 14$.

Démonstration Il n'est pas dur de vérifier que : $\mathrm{div}(28) \cap \mathrm{div}(42) \cap \mathrm{div}(98) = \big\{\pm 1, \pm 2, \pm 7, \pm 14\big\}$.

En prouvant l'associativité du PGCD de deux entiers, nous avons aussi montré sans le savoir que le calcul du PGCD d'une famille finie d'entiers peut être ramené à des calculs de PGCD de deux entiers. Par exemple :

$10 \wedge 12 \wedge 18 = 10 \wedge (12 \wedge 18) = 10 \wedge 6 = 2$, mais aussi, si on préfère : $10 \wedge 12 \wedge 18 = (10 \wedge 12) \wedge 18 = 2 \wedge 18 = 2$.

Nous admettrons la généralisation suivante de nos précédents résultats pour gagner du temps.

Théorème **(Reprise des résultats précédents dans le cas d'une famille finie d'entiers)** Soient $a_1, \dots, a_r \in \mathbb{Z}$.

- Les diviseurs communs de $a_1, \dots, a_r$ sont exactement les diviseurs de $a_1 \wedge \dots \wedge a_r$:
$$\mathrm{div}(a_1) \cap \dots \cap \mathrm{div}(a_r) = \mathrm{div}(a_1 \wedge \dots \wedge a_r).$$
- Pour tout $k \in \mathbb{Z}$: $(a_1 k) \wedge \dots \wedge (a_r k) = |k|(a_1 \wedge \dots \wedge a_r)$.
- Il existe des entiers $u_1, \dots, u_r \in \mathbb{Z}$ pour lesquels : $a_1 \wedge \dots \wedge a_r = a_1 u_1 + \dots + a_r u_r$. Une telle relation est appelée UNE *relation de Bézout de* $a_1, \dots, a_r$.

La remarque qui suit exploite dans le domaine de l'arithmétique le vocabulaire des relations d'ordre du chapitre « Relations binaires ». Comme on l'a vu, la relation de divisibilité est une relation d'ordre sur $\mathbb{N}$ MAIS PAS SUR $\mathbb{Z}$. Pour cette raison, nous ne parlerons dans les lignes qui suivent que d'entiers NATURELS. Le mot « diviseur » est à comprendre au sens restreint de « diviseur positif », mais nous omettrons la précision « positif » pour alléger.

- Dire que a DIVISE b, c'est dire que a est PLUS PETIT QUE b au sens de la divisibilité.
- Les DIVISEURS COMMUNS POSITIFS de a et b sont exactement les MINORANTS de $\{a, b\}$ au sens de la divisibilité. De même, les MULTIPLES COMMUNS POSITIFS de a et b sont exactement les MAJORANTS de $\{a, b\}$ au sens de la divisibilité.
- Nous avons défini le PGCD de a et b comme le plus grand élément de $\mathrm{div}(a) \cap \mathrm{div}(b)$ au sens de la relation $\leqslant$, mais nous avons vu ensuite que : $\mathrm{div}(a) \cap \mathrm{div}(b) = \mathrm{div}(a \wedge b)$ — or que signifie cette égalité ? Elle signifie que $a \wedge b$ est aussi le plus grand élément de $\mathrm{div}(a) \cap \mathrm{div}(b)$ au sens de la divisibilité. Conclusion : $a \wedge b$ est le plus grand minorant de $\{a, b\}$ au sens de la divisibilité, c'est-à-dire sa BORNE INFÉRIEURE.

2.3 Entiers premiers entre eux

Définition **(Entiers premiers entre eux, cas de deux entiers)** Soient $a, b \in \mathbb{Z}$. On dit que a et b sont *premiers entre eux* si leurs seuls diviseurs communs sont ± 1, i.e. si $a \wedge b = 1$.

Exemple 6 et 35 sont premiers entre eux car : $\mathrm{div}(6) = \{\pm 1, \pm 2, \pm 3, \pm 6\}$ et $\mathrm{div}(35) = \{\pm 1, \pm 5, \pm 7, \pm 35\}$. Autre manière de voir les choses, un simple calcul de PGCD par l'algorithme d'Euclide montre que $6 \wedge 35 = 1$.

Attention ! Ne confondez pas : $a \not| b$ et $a \wedge b = 1$. Par exemple : $4 \not| 2$ mais : $4 \wedge 2 = 2 \neq 1$.

Dire que $a \wedge b = 1$, c'est dire que a et b n'ont AUCUN diviseur commun hormis ± 1. La relation $a \not| b$ n'empêche pas quant à elle a et b de partager de nombreux diviseurs communs, elle empêche seulement a d'être intégralement « présent » dans b. Il se trouve tout de même que dans un cas particulier important, la confusion est permise car elle n'en est pas une :

Pour tout NOMBRE PREMIER p : $p \not| b \iff p \wedge b = 1$.

Sans transition. La remarque qui suit est utile dans de nombreux problèmes.

Pour tous $a, b \in \mathbb{Z}$ de PGCD d : $a = da'$ et $b = db'$ pour certains entiers $a', b' \in \mathbb{Z}$ PREMIERS ENTRE EUX.

Tout simplement, si $(a,b) \neq (0,0)$: $d = a \wedge b = (da') \wedge (db') = d\big(a' \wedge b'\big)$, donc $a' \wedge b' = 1$.

Exemple L'équation $x^2 = y^2 + (x \wedge y) + 2$ d'inconnue $(x,y) \in \mathbb{N}^2$ admet $(2,1)$ et $(2,0)$ pour seules solutions.

Démonstration

- **Analyse :** Soit $(x,y) \in \mathbb{N}^2$. On suppose que : $x^2 = y^2 + (x \wedge y) + 2$ et on pose $d = x \wedge y$. Clairement : $(x,y) \neq (0,0)$, donc d est non nul. En outre : $x = dx'$ et $y = dy'$ pour certains $x', y' \in \mathbb{N}$ premiers entre eux.

  L'équation devient $d^2x'^2 = d^2y'^2 + d + 2$, donc d divise 2, i.e. $d = 1$ ou $d = 2$.

  — **Cas où $d = 1$:** $(x'+y')(x'-y') = 3$, or 3 est premier et $x'-y' \leqslant x'+y'$, donc $x'+y' = 3$ et $x'-y' = 1$. Aussitôt $(x',y') = (2,1)$, et enfin $(x,y) = (2,1)$.

  — **Cas où $d = 2$:** $(x'+y')(x'-y') = 1$, donc $x'+y' = x'-y' = 1$, i.e. $(x',y') = (1,0)$, et enfin $(x,y) = (2,0)$.

- **Synthèse :** Les deux couples $(2,1)$ et $(2,0)$ conviennent en effet.

Définition **(Entiers premiers entre eux dans leur ensemble/deux à deux)** Soient $a_1, \dots, a_r \in \mathbb{Z}$.

- **Dans leur ensemble :** On dit que $a_1, \dots, a_r$ sont *premiers entre eux dans leur ensemble* si leurs seuls diviseurs communs sont ± 1, i.e. si $a_1 \wedge \dots \wedge a_r = 1$.
- **Deux à deux :** On dit que $a_1, \dots, a_r$ sont *premiers entre eux deux à deux* si $a_i \wedge a_j = 1$ pour tous $i, j \in [\![1, r]\!]$ distincts.

Attention ! Premiers entre eux DEUX À DEUX $\implies$ Premiers entre eux DANS LEUR ENSEMBLE

mais LA RÉCIPROQUE EST FAUSSE ! Par exemple, 6, 10 et 15 sont premiers entre eux dans leur ensemble, mais pourtant : $6 \wedge 10 = 2 \neq 1$, $6 \wedge 15 = 3 \neq 1$ et $10 \wedge 15 = 5 \neq 1$.

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

(i) a et b sont premiers entre eux. (ii) Il existe deux entiers $u, v \in \mathbb{Z}$ pour lesquels $au + bv = 1$.

Démonstration L'implication (i) $\implies$ (ii) est une simple relation de Bézout — déjà prouvée. Pour la réciproque (ii) $\implies$ (i), supposons l'existence de deux entiers $u, v \in \mathbb{Z}$ pour lesquels $au + bv = 1$ et fixons d un diviseur commun positif de a et b. Alors d divise $au + bv = 1$, donc $d = 1$. Comme voulu : $a \wedge b = 1$.

Théorème **(Théorème de Gauss)** Soient $a, b, c \in \mathbb{Z}$. Si $a \mid bc$ avec $a \wedge b = 1$, alors $a \mid c$.

Démonstration Par hypothèse, $bc = ak$ pour un certain $k \in \mathbb{Z}$ et $au + bv = 1$ pour certains $u, v \in \mathbb{Z}$ — relation de Bézout. Multiplions par c : $acu + bcv = c$, puis remplaçons bc par ak : $a(cu + kv) = c$. Ainsi $a \mid c$.

Théorème **(Conséquences diverses du théorème de Gauss)** Soient $a, b, m, n, a_1, \dots, a_r \in \mathbb{Z}$.

(i) **Lemme d'Euclide :** Pour tout NOMBRE PREMIER p : $\quad p \mid ab \iff p \mid a$ ou $p \mid b$.

(ii) **Division dans une congruence :** Si $am \equiv bm\ [n]$ avec $m \wedge n = 1$, alors $a \equiv b\ [n]$.

(iii) **Produits d'entiers :**

— Si chacun des entiers $a_1, \dots, a_r$ est premier avec n, leur produit $a_1 \dots a_r$ l'est aussi.

— Si les entiers $a_1, \dots, a_r$ divisent n et sont premiers entre eux DEUX À DEUX, leur produit $a_1 \dots a_r$ divise n.

Attention !

(i) La primalité de p est indispensable au lemme d'Euclide. Par exemple : $\quad 4 \mid 2 \times 2 \quad$ mais : $\quad 4 \nmid 2$.

(ii) On ne peut pas toujours « simplifier par m » dans une congruence, encore faut-il que m et n n'aient rien de commun à part ± 1, i.e. que r et n soient premiers entre eux. Par exemple : $\quad 2 \times 3 \equiv 2 \times 0\ [6], \quad$ mais : $\quad 3 \not\equiv 0\ [6]$.

(iii) En général : $\quad a \mid n \quad \text{et} \quad b \mid n \quad \not\Longrightarrow \quad ab \mid n.$ Par exemple, 12 est divisible par 4 et 6, mais pas par 24.

Ensuite, il est impératif de supposer $a_1, \dots, a_r$ premiers entre eux DEUX À DEUX dans la deuxième partie de l'assertion (iii). Par exemple, pour : $\quad n = 30, \quad a_1 = 6, \quad a_2 = 10 \quad$ et $\quad a_3 = 15, \quad$ les entiers a_1, a_2 et a_3 divisent n mais sont seulement premiers entre eux DANS LEUR ENSEMBLE, et clairement leur produit $a_1 a_2 a_3 = 900$ ne divise pas n.

Démonstration

(i) Si p divise a ou b, p divise ab. Réciproquement, si p divise ab et si p ne divise pas a, alors p étant premier : $p \wedge a = 1, \quad$ donc d'après le théorème de Gauss : $\quad p \mid b$. Bref, si p divise ab : $\quad p \mid a \quad$ ou $\quad p \mid b$.

(ii) $\quad n \mid (a-b)m \quad$ et $\quad m \wedge n = 1, \quad$ donc d'après le théorème de Gauss : $\quad n \mid (b-a), \quad$ i.e. $a \equiv b\ [n]$.

(iii) Montrons le résultat dans le cas de deux entiers $a, b \in \mathbb{Z}$.

— Si $a \wedge n = b \wedge n = 1$: $\quad au + nv = bu' + nv' = 1 \quad$ pour certains $u, v, u', v' \in \mathbb{Z}$ d'après le théorème de Bézout, donc par produit : $\quad 1 = (au+nv)(bu'+nv') = (ab)(uu') + n\big(auv' + vbu' + nvv'\big), \quad$ donc de nouveau d'après le théorème de Bézout : $\quad (ab) \wedge n = 1$.

— Faisons l'hypothèse que : $\quad a \mid n, \quad b \mid n \quad$ et $\quad a \wedge b = 1$. Ainsi $n = ak$ pour un certain $k \in \mathbb{Z}$, donc b divise $n = ak$, or $a \wedge b = 1$, donc d'après le théorème de Gauss : $\quad b \mid k$. A fortiori, ab divise $ak = n$.

Théorème **(Forme irréductible d'un rationnel)** Tout rationnel peut être écrit d'une et une seule manière, appelée sa *forme irréductible*, sous la forme $\dfrac{p}{q}$ où $p \in \mathbb{Z}$ et $q \in \mathbb{N}^*$ avec p et q premiers entre eux.

En choisissant p dans $\mathbb{Z}$ et q dans $\mathbb{N}^*$, on impose que le signe de la fraction soit porté par son numérateur. Sans cela, il n'y aurait pas unicité de la forme irréductible.

Démonstration

- **Unicité :** Soient $(p,q), (p',q') \in \mathbb{Z} \times \mathbb{N}^*$. On suppose que $r = \dfrac{p}{q} = \dfrac{p'}{q'}$ avec $p \wedge q = 1$ et $p' \wedge q' = 1$. Comme $pq' = p'q$: $\quad q \mid pq'$. Or $p \wedge q = 1$, donc d'après le théorème de Gauss : $\quad q \mid q', \quad$ puis $q' \mid q$ par symétrie des rôles de q et q'. Conclusion : $\quad |q| = |q'|, \quad$ et comme q et q' sont positifs : $\quad q = q'$. Divisons enfin l'égalité $pq' = p'q$ par $q = q'$. Comme voulu : $\quad p = p'$.
- **Existence :** Par définition : $\quad r = \dfrac{a}{b} \quad$ pour certains $a, b \in \mathbb{Z}$ avec $b \neq 0$, et même $b > 0$ sans perte de généralité. En notant d le PGCD de a et b : $\quad a = dp \quad$ et $\quad b = dq \quad$ pour certains $p \in \mathbb{Z}$ et $q \in \mathbb{N}^*$ premiers entre eux, et donc $r = \dfrac{a}{b} = \dfrac{dp}{dq} = \dfrac{p}{q}$.

2.4 PPCM DE DEUX ENTIERS

Définition-théorème **(PPCM de deux entiers)** Soient $a, b \in \mathbb{Z}$ non nuls. On appelle *plus petit commun multiple* (ou *PPCM*) *de a et b* et on note $a \vee b$ le plus petit élément au sens de la relation $\leqslant$ de l'ensemble des multiples communs strictement positifs de a et b.

Pour tout $a \in \mathbb{Z}$, on pose par ailleurs : $\quad a \vee 0 = 0 \vee a = 0$.

Démonstration Pour justifier l'existence de $a \vee b$ dans le cas où a et b sont non nuls, remarquons simplement que l'ensemble des multiples communs strictement positifs de a et b contient le produit $|ab|$, donc est une partie non vide de $\mathbb{N}$, donc possède un plus petit élément.

Exemple Clairement, pour tous $a, b \in \mathbb{Z}$: $a \vee b = |a| \vee |b|$ et $a \vee b = b \vee a$.

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

(i) **Multiples communs et multiples du PPCM :** Les multiples communs de a et b sont exactement les multiples de $a \vee b$: $a\mathbb{Z} \cap b\mathbb{Z} = (a \vee b)\mathbb{Z}$.

(ii) **Lien avec le PGCD :** $(a \wedge b)(a \vee b) = |ab|$.

(iii) **Factorisation par un diviseur commun :** $(ak) \vee (bk) = |k|(a \vee b)$.

Démonstration Nous pouvons supposer $a > 0$ ou $b > 0$ sans perte de généralité. En particulier : $a \wedge b \neq 0$, et nous pouvons nous donner deux entiers $a', b' \in \mathbb{N}$ premiers entre eux pour lesquels : $a = (a \wedge b)a'$ et $b = (a \wedge b)b'$. Aussitôt : $\dfrac{ab}{a \wedge b} = ba' = ab'$. Nous montrerons simultanément les assertions (i) et (ii).

- Pour commencer, $a \vee b$ est un multiple de a et b, donc tout multiple de $a \vee b$ est a fortiori lui aussi un multiple de a et b. En résumé : $(a \vee b)\mathbb{Z} \subset a\mathbb{Z} \cap b\mathbb{Z}$.
- Pour l'autre inclusion, soit $m \in a\mathbb{Z} \cap b\mathbb{Z}$. Par définition : $m = au = bv$ pour certains $u, v \in \mathbb{Z}$, donc $ua' = vb'$ après division par $a \wedge b \neq 0$. En particulier $a' \mid vb'$, mais par ailleurs $a' \wedge b' = 1$, donc $a' \mid v$ d'après le théorème de Gauss, donc $v = a'k$ pour un certain $k \in \mathbb{Z}$.

  Conclusion : $m = bv = ba'k = k \times \dfrac{ab}{a \wedge b}$, donc $m \in \left(\dfrac{ab}{a \wedge b}\right)\mathbb{Z}$. En résumé : $a\mathbb{Z} \cap b\mathbb{Z} \subset \left(\dfrac{ab}{a \wedge b}\right)\mathbb{Z}$.
- Ainsi, $\dfrac{ab}{a \wedge b}$ divise tout multiple commun strictement positif de a et b, donc minore l'ensemble des multiples communs strictement positifs de a et b au sens de la relation $\leqslant$. L'entier $\dfrac{ab}{a \wedge b}$ étant lui-même un tel multiple : $a \vee b = \dfrac{ab}{a \wedge b}$ par définition de $a \vee b$, ce qui achève aussi de prouver (i).

Exemple Les multiples communs de 12 et 18 sont tous les multiples de 36 car : $12 \vee 18 = \dfrac{12 \times 18}{12 \wedge 18} = \dfrac{12 \times 18}{6} = 36$.

De même que nous avons pu interpréter le PGCD comme une borne inférieure au sens de la divisibilité sur $\mathbb{N}$, nous pouvons dire à présent que pour tous $a, b \in \mathbb{N}$, le PPCM de a et b n'est autre que le plus petit majorant de l'ensemble $\{a, b\}$ au sens de la divisibilité, i.e. sa **borne supérieure**.

3 Nombres premiers

3.1 Valuations p-adiques et factorisation première

Définition-théorème (Valuation p-adique) Soient $p \in \mathbb{P}$ et $n \in \mathbb{Z} \setminus \{0\}$. L'ensemble $\{k \in \mathbb{N} \mid p^k \mid n\}$ possède un plus grand élément, appelé la *valuation p-adique de n* et noté $v_p(n)$.

Clairement : $v_p(n) = v_p(|n|)$.

Démonstration Tout d'abord : $p^0 \mid n$. Ensuite, pour tout $k \in \mathbb{N}$ pour lequel p^k divise n : $k \leqslant p^k \leqslant |n|$. Conclusion : $\{k \in \mathbb{N} \mid p^k \mid n\}$ est une partie non vide majorée de $\mathbb{N}$, donc possède un plus grand élément.

Exemple $v_2(60) = 2$, $v_3(60) = 1$, $v_5(60) = 1$ et pour tout $p \in \mathbb{P} \setminus \{2, 3, 5\}$: $v_p(60) = 0$.

Théorème (Additivité des valuations p-adiques) Pour tous $p \in \mathbb{P}$ et $a, b \in \mathbb{Z} \setminus \{0\}$: $v_p(ab) = v_p(a) + v_p(b)$.

Démonstration Par définition des valuations p-adiques : $a = p^{v_p(a)}a'$ et $b = p^{v_p(b)}b'$ pour certains $a', b' \in \mathbb{Z}\setminus\{0\}$ NON divisibles par p. En d'autres termes, p étant premier : $p \wedge a' = p \wedge b' = 1$, donc $p \wedge (a'b') = 1$, donc toujours parce que p est premier : $p \nmid a'b'$. L'égalité $ab = p^{v_p(a)+v_p(b)}a'b'$ montre ainsi que $v_p(ab) = v_p(a) + v_p(b)$.

Exemple Pour tous $p, q \in \mathbb{P}$ et $k \in \mathbb{N}$: $v_p\big(q^k\big) = kv_p(q) = \begin{cases} k & \text{si } q = p \\ 0 & \text{sinon.} \end{cases}$

Nous avons montré en début de chapitre l'EXISTENCE de la décomposition de tout entier naturel non nul en produit de nombres premiers, nous pouvons enfin en prouver l'UNICITÉ — à l'ordre près des facteurs.

Théorème (Factorisation première) Pour tout $n \in \mathbb{N}^*$, il existe une et une seule famille *presque nulle* $\big(v_p(n)\big)_{p\in\mathbb{P}}$ d'entiers naturels — i.e. dont tous les éléments sont nuls sauf un nombre fini d'entre eux — telle que :
$$n = \prod_{p\in\mathbb{P}} p^{v_p(n)}.$$
Cette décomposition est appelée la *factorisation première de n*.

Dans la preuve qui suit, c'est le théorème de Gauss qui nous fournit l'unicité de la factorisation première via l'additivité des valuations p-adiques. Alors que l'existence était facile à prouver, l'unicité requiert au contraire une certaine artillerie.

Démonstration Pour l'unicité, soient $n \in \mathbb{N}^*$ et $(\alpha_p)_{p\in\mathbb{P}}$ une famille presque nulle d'entiers naturels pour laquelle $n = \prod_{q\in\mathbb{P}} q^{\alpha_q}$. Pour tout $p \in \mathbb{P}$: $v_p(n) = v_p\left(\prod_{q\in\mathbb{P}} q^{\alpha_q}\right) = \sum_{q\in\mathbb{P}} v_p\big(q^{\alpha_q}\big) = \alpha_p$ par additivité des valuations p-adiques, donc la famille $(\alpha_p)_{p\in\mathbb{P}}$ est nécessairement la famille $\big(v_p(n)\big)_{p\in\mathbb{P}}$ — unicité.

Théorème (Divisibilité, PGCD, PPCM et valuations p-adiques) Soient $a, b \in \mathbb{Z}\setminus\{0\}$.

(i) a divise b si et seulement si pour tout $p \in \mathbb{P}$: $v_p(a) \leqslant v_p(b)$.

(ii) $a \wedge b = \prod_{p\in\mathbb{P}} p^{\min\{v_p(a),v_p(b)\}}$ et $a \vee b = \prod_{p\in\mathbb{P}} p^{\max\{v_p(a),v_p(b)\}}$.

Vous utilisez la formule (ii) sur le PPCM depuis fort longtemps quand vous réduisez une somme de fractions d'entiers au même dénominateur. Quel est le plus petit dénominateur commun de $\frac{13}{12} + \frac{7}{30}$? Ce n'est pas 12×30 mais $12\vee30$. Et comme $12 = 2^2\times3$ et $30 = 2\times3\times5$: $12\vee30 = 2^2\times3\times5 = 60$. Bref : $\frac{13}{12} + \frac{7}{30} = \frac{5\times13+2\times7}{60} = \frac{79}{60}$.

Démonstration

(i) Si $a \mid b$: $b = ak$ pour un certain $k \in \mathbb{Z}\setminus\{0\}$, donc : $v_p(b) = v_p(a) + v_p(k) \geqslant v_p(a)$ pour tout $p \in \mathbb{P}$. Inversement, si $v_p(a) \leqslant v_p(b)$ pour tout $p \in \mathbb{P}$, $p^{v_p(a)}$ divise $p^{v_p(b)}$, donc $\prod_{p\in\mathbb{P}} p^{v_p(a)} = a$ divise $\prod_{p\in\mathbb{P}} p^{v_p(b)} = b$.

(ii) Pour le PGCD, posons $d = \prod_{p\in\mathbb{P}} p^{\min\{v_p(a),v_p(b)\}}$. D'après (i), d divise à la fois a et b. Pour montrer que $d = a \wedge b$, nous allons prouver que $\frac{a}{d} \wedge \frac{b}{d} = 1$.

Soit $p \in \mathbb{P}$. Si $v_p(a) \leqslant v_p(b)$: $v_p(d) = v_p(a)$, donc $v_p\left(\frac{a}{d}\right) = v_p(a) - v_p(d) = 0$, donc p ne divise pas $\frac{a}{d}$. Si au contraire $v_p(a) > v_p(b)$, p ne divise pas $\frac{b}{d}$. Dans les deux cas, p ne divise pas à la fois $\frac{a}{d}$ et $\frac{b}{d}$. En résumé, $\frac{a}{d}$ et $\frac{b}{d}$ n'ont aucun diviseur commun premier, donc sont premiers entre eux.

Pour le PPCM : $x + y = \min\{x, y\} + \max\{x, y\}$ pour tous $x, y \in \mathbb{R}$, donc :
$$a \vee b = \frac{ab}{a\wedge b} = \prod_{p\in\mathbb{P}} p^{v_p(a)+v_p(b)-\min\{v_p(a),v_p(b)\}} = \prod_{p\in\mathbb{P}} p^{\max\{v_p(a),v_p(b)\}}.$$

Exemple $600 \wedge 740 = 20 = 2^2\times5$ car : $600 = 2^3\times3\times5^2$ et $740 = 2^2\times5\times37$.

Exemple Soient $a \in \mathbb{Z}$, $n \in \mathbb{N}^*$ et $p \in \mathbb{P}$. Alors p divise a si et seulement si p divise a^n.

Démonstration Si p divise a, p divise a^n. Les valuations p-adiques se révèlent utiles pour la réciproque :
$$p \text{ divise } a^n \iff v_p\big(a^n\big) \geqslant 1 \iff nv_p(a) \geqslant 1 \iff v_p(a) \geqslant \frac{1}{n} \overset{\frac{1}{n}>0}{\underset{v_p(a)\in\mathbb{N}}{\iff}} v_p(a) \geqslant 1 \iff p \text{ divise } a.$$

Exemple $\sqrt[5]{\frac{4}{3}}$ est irrationnel.

Démonstration Par l'absurde, supposons $\sqrt[5]{\frac{4}{3}}$ rationnel, disons $\sqrt[5]{\frac{4}{3}} = \frac{a}{b}$ pour certains $a, b \in \mathbb{N}^*$. Aussitôt $3a^5 = 4b^5$, donc en particulier : $v_3\big(3a^5\big) = v_3\big(4b^5\big)$, ce qui s'écrit aussi : $5v_3(a)+1 = 5v_3(b)$, et modulo 5 : $1 \equiv 0\,[5]$ — contradiction !

3.2 Petit théorème de Fermat

Théorème (Petit théorème de Fermat) Pour tous $p \in \mathbb{P}$ et $a \in \mathbb{Z}$: $a^p \equiv a\,[p]$,
et si $p \wedge a = 1$, i.e. si $p \nmid a$: $a^{p-1} \equiv 1\,[p]$.

Démonstration

- Pour tout $k \in [\![1, p-1]\!]$: $k\binom{p}{k} = p\binom{p-1}{k-1}$, donc p divise $k\binom{p}{k}$. Or p est premier et $k \in [\![1, p-1]\!]$, donc p est premier avec k, donc divise $\binom{p}{k}$ d'après le théorème de Gauss, i.e. : $\binom{p}{k} \equiv 0\,[p]$ ★.
- Montrons à présent par récurrence que pour tout $a \in [\![0, p-1]\!]$: $a^p \equiv a\,[p]$ — comme on raisonne modulo p, ce sera alors vrai aussi pour tout $a \in \mathbb{Z}$. **Initialisation :** $0^p = 0 \equiv 0\,[p]$.
  Hérédité : Soit $a \in [\![0, p-2]\!]$. Si $a^p \equiv a\,[p]$: $(a+1)^p = \sum_{k=0}^{p}\binom{p}{k}a^k \overset{\star}{\equiv} \underbrace{a^p}_{k=p} + \underbrace{1}_{k=0} \overset{\text{HDR}}{\equiv} a+1\,[p]$.
- Enfin, si a n'est pas divisible par p : $p \wedge a = 1$ car p est premier. Or p divise $a^p - a = a\big(a^{p-1}-1\big)$, donc d'après le théorème de Gauss, p divise $a^{p-1}-1$, i.e. $a^{p-1} \equiv 1\,[p]$. ∎

Exemple Pour tout $n \in \mathbb{Z}$, tout diviseur premier impair de n^2+1 est congru à 1 modulo 4.

Démonstration Soient $n \in \mathbb{Z}$ et $p \in \mathbb{P} \setminus \{2\}$. On suppose que p divise n^2+1. Aussitôt : $n^2 \equiv -1\,[p]$ et n n'est pas divisible par p. En outre, p étant impair, $\frac{p-1}{2}$ est un entier, donc d'après le petit théorème de Fermat : $1 \equiv n^{p-1} \equiv \big(n^2\big)^{\frac{p-1}{2}} \equiv (-1)^{\frac{p-1}{2}}\,[p]$. Or $(-1)^{\frac{p-1}{2}} \in \{\pm 1\}$ et $p \geqslant 3$, donc cette congruence est en fait une égalité, autrement dit : $(-1)^{\frac{p-1}{2}} = 1$. Comme voulu, $\frac{p-1}{2}$ est pair, i.e. $p \equiv 1\,[4]$.

Exemple Il existe une infinité de nombres premiers congrus à 1 modulo 4.

Plus généralement, le TRÈS DIFFICILE *théorème de la progression arithmétique* de Dirichlet, démontré vers 1840, affirme que pour tous $a, b \in \mathbb{N}^*$ premiers entre eux, il existe une infinité de nombres premiers congrus à a modulo b.

Démonstration Supposons par l'absurde qu'il n'existe qu'un nombre fini de nombres premiers congrus à 1 modulo 4, notons $p_1, \dots, p_r$ leur liste complète et posons $N = (2p_1 \dots p_r)^2 + 1$. Supérieur ou égal à 2 et impair, N possède un diviseur premier p impair, et comme $p_1, \dots, p_r$ ne divisent pas N, p n'est aucun d'entre eux. Pourtant, d'après l'exemple précédent, p est lui-même congru à 1 modulo 4 — contradiction.

Exemple L'équation $y^2 = x^3 - 3$ d'inconnue $(x, y) \in \mathbb{Z}^2$ n'a pas de solution.

Démonstration Supposons par l'absurde qu'elle en possède une (x, y). Si x est pair : $y^2 = x^3 - 3 \equiv -3 \equiv 5\,[8]$, or il n'est pas dur de vérifier que a^2 est congru à 0, 1 ou 4 modulo 8 pour tout $a \in \mathbb{Z}$. Conclusion : x est impair. A fortiori, y est pair, disons $y = 2y'$ pour un certain $y' \in \mathbb{Z}$.

Remarquons alors que : $(x+1)\big(x^2-x+1\big) = x^3+1 = y^2+4 = 4\big(y'^2+1\big)$ ★. Or $x^2-x+1 = x(x-1)+1$ est impair, et de plus positif car $x^2-x+1 = \left(x-\frac{1}{2}\right)^2 + \frac{3}{4}$. Tout diviseur premier éventuel de x^2-x+1 se trouve ainsi être impair, donc divise y'^2+1 d'après ★, donc est congru à 1 modulo 4 d'après un exemple précédent. En retour, x^2-x+1 étant un produit de puissances de ces nombres premiers : $x^2-x+1 \equiv 1\,[4]$, donc $x(x-1)$ est divisible par 4. Comme x est impair, il en découle que $x \equiv 1\,[4]$, donc enfin que : $(x+1)\big(x^2-x+1\big) \equiv 2\,[4]$, ce qui contredit la relation ★.