Arithmétique des entiers

1 Divisibilité et division euclidienne

1.1 Divisibilité

Définition **(Divisibilité, diviseur, multiple)** Soient $a, b \in \mathbb{Z}$. On dit que a *divise* b, ce qu'on note $a \mid b$, si $b = ak$ pour un certain $k \in \mathbb{Z}$. On dit aussi que a est un *diviseur de* b, que b est *divisible par* a ou que b est un *multiple de* a.

Pour tout $a \in \mathbb{Z}$, l'ensemble des multiples de a est 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 $a \neq 0$: $\max \mathrm{div}(a) = |a|$.

Les relations $\mid$ et $\leqslant$ ont des manières très différentes de structurer $\mathbb{Z}$, mais pour tous $a, b \in \mathbb{N}^*$: $a \mid b \implies a \leqslant b$.

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 $d \mid b$, alors $d \mid (au + bv)$ pour tous $u, v \in \mathbb{Z}$.

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

Si a et b ont les mêmes diviseurs, i.e. si $\mathrm{div}(a) = \mathrm{div}(b)$, alors $a \mid b$ et $b \mid a$, donc $|a| = |b|$ d'après (i).

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

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

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

Exemple Le produit de deux entiers consécutifs est pair. Plus généralement, pour tout $k \in \mathbb{N}$, le produit de k entiers consécutifs est divisible par $k!$.

Démonstration Soient $k \in \mathbb{N}$ et $n \in \mathbb{Z}$.

— Si $n \geqslant 1$, alors $n(n+1)\dots(n+k-1) = \dfrac{(n+k-1)!}{(n-1)!} = k! \times \binom{n+k-1}{k}$ et les coefficients binomiaux sont des entiers, donc $n(n+1)\dots(n+k-1)$ est divisible par $k!$.

— Si $n \in [\![-k+1, 0]\!]$, alors $n(n+1)\dots(n+k-1) = 0$ est divisible par $k!$.

— Si $n \leqslant -k$, alors $N = -n-k+1 \geqslant 1$, donc $n(n+1)\dots(n+k-1) = (-1)^k N(N+1)\dots(N+k-1)$ est divisible par $k!$ d'après le premier point.

1.2 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 ses seuls diviseurs sont ± 1 et $\pm p$. On dit que p est *composé* si p n'est ni égal à 1 ni premier.

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

La liste des nombres premiers commence ainsi : 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37…

L'existence de la factorisation première est facile à prouver. L'unicité est plus délicate et attendra la fin du chapitre.

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

On considère 1 comme le produit de 0 nombre premier et tout nombre premier est le produit d'un seul nombre premier.

Démonstration Par récurrence forte.

- **Initialisation :** 2 est premier, donc produit de nombres premiers !
- **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 $n = ab$ 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 (Infinitude de l'ensemble des nombres premiers) L'ensemble $\mathbb{P}$ des nombres premiers est infini.

Démonstration Par l'absurde, supposons $\mathbb{P}$ fini et notons $p_1, \dots, p_r$ ses éléments.

- **La preuve d'Euclide :** Supérieur à 2, l'entier $N = p_1 \dots p_r + 1$ possède un diviseur premier d'après le théorème précédent, disons 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.
- **La preuve whaou :** D'après le théorème précédent : $\mathbb{Z} \setminus \{-1, 1\} = p_1\mathbb{Z} \cup \dots \cup p_r\mathbb{Z}$. Pourtant, les ensembles $p_1\mathbb{Z}, \dots, p_r\mathbb{Z}$ sont $p_1 \dots p_r$-périodiques, donc leur réunion aussi, alors que $\mathbb{Z} \setminus \{-1, 1\}$ ne l'est pas — 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 $n \geqslant 2$ est composé et si nous notons p le plus petit de ses diviseurs premiers, alors $n = pk$ pour un certain $k \in \mathbb{N}^*$, mais tout diviseur premier de k est aussi supérieur à p, donc $n = pk \geqslant p^2$, i.e. $p \leqslant \sqrt{n}$. En résumé :

Tout entier COMPOSÉ n possède un diviseur premier inférieur à $\sqrt{n}$.

Tirons de cette observation la liste de tous les nombres premiers inférieurs à 100.

- L'entier 2 est premier, c'est notre point de départ. On efface tous ses multiples de la liste hormis lui-même, car ils sont composés.
- Le premier entier non effacé après 2 vaut 3. Il est forcément premier car s'il était composé, il aurait un diviseur premier strictement inférieur et on l'aurait déjà effacé. On efface alors tous les multiples de 3 hormis lui-même, car ils sont composés.
- Même chose avec 5, même chose avec 7. Le premier entier non effacé est 11, mais tout entier composé de $[\![2, 100]\!]$ possède un diviseur premier inférieur à $\sqrt{100} = 10$, donc les entiers composés de $[\![2, 100]\!]$ ont déjà tous été effacés. Les survivants sont exactement les nombres premiers inférieurs à 100.

	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

1.3 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 $r \in [\![0, b-1]\!]$. 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 : $q = \left\lfloor \frac{a}{b} \right\rfloor$.

Pour $b = 2$, le théorème montre que tout entier relatif est pair ou impair, mais jamais les deux.

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 ajoute b au lieu de le retrancher.

  L'ensemble $\mathscr{R} = (a+b\mathbb{Z}) \cap \mathbb{N}$ 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 $\mathscr{R}$, $a = bq + r$ 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 $r = \min \mathscr{R}$ — 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 $|q-q'| < 1$. Comme $q-q'$ est entier, il en découle 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 $q = \left\lfloor \frac{a}{b} \right\rfloor$. ∎

En résumé, DIVISER C'EST SOUSTRAIRE, mais pour diviser 1000 par 3, faut-il vraiment effectuer 333 soustractions ? Oui et non. Quand on pose la division de 347 par 5, on retranche dans un premier temps $6 \times 5 = 30$ de 34, du moins en apparence, car 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 effectué 69 soustractions, mais en deux fois seulement. Pour un ordinateur, un grand nombre de mini-soustractions n'est pas un problème. Pour nous autres cerveaux, c'en est un. Nous compensons en exploitant vite et bien les tables de multiplication. C'est grâce à elles que nous avons trouvé les chiffres 6 et 9 du quotient 69.

```
  3 4 7 | 5
- 3 0(0)| 6 9
    4 7
  - 4 5
      2
```

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

Démonstration Difficile de poser la division car 2^{65362} possède environ 20000 décimales, mais 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, on peut « raisonner modulo 3 dans l'exposant » car pour tous $q, r \in \mathbb{N}$: $2^{3q+r} \equiv 1^q \times 2^r \equiv 2^r\ [7]$. Ici, $65362 \equiv 1\ [3]$, donc $2^{65362} \equiv 2^1 \equiv 2\ [7]$.

1.4 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, ce qu'on note $a \equiv b\ [n]$, si $a = b + kn$ pour un certain $k \in \mathbb{Z}$. Il est équivalent de dire que $n \mid (a-b)$.

L'équivalence suivante est fondamentale dans les deux sens : $n \mid a \iff a \equiv 0\ [n]$. Elle traduit les divisibilités en congruences et vice versa.

Le théorème de la division euclidienne par un entier $n \in \mathbb{N}^*$ peut être reformulé en termes de congruences :

$$\forall a \in \mathbb{Z}, \quad \exists!\, r \in [\![0, n-1]\!], \quad a \equiv r\ [n],$$

ce qui signifie que tout entier relatif a est congru modulo n à un unique entier r de $[\![0, n-1]\!]$. En d'autres termes, $[\![0, n-1]\!]$ est un ensemble de représentants des classes d'équivalence de $\equiv [n]$ et l'ensemble quotient $\mathbb{Z}/_{\equiv [n]} = \{n\mathbb{Z}, n\mathbb{Z}+1, \dots, n\mathbb{Z}+n-1\}$ est de cardinal n.

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 $a' \equiv b'\ [n]$, alors $a + a' \equiv b + b'\ [n]$.

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

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

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

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

(iii) Si n divise $a-b$ et $a'-b'$, alors n divise aussi $a(a'-b') + b'(a-b) = aa' - bb'$ par combinaison linéaire, donc $aa' \equiv bb'\ [n]$.

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

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 : $n^2 \equiv 1\ [8]$.

Démonstration $n = 2k+1$ pour un certain $k \in \mathbb{Z}$, donc $n^2 = 4k^2+4k+1 = 4k(k+1)+1$. Cela dit, k ou $k+1$ est pair car ces deux entiers sont consécutifs, donc leur produit est pair aussi : $k(k+1) \equiv 0\ [2]$. A fortiori $4k(k+1) \equiv 0\ [8]$, donc $n = 4k(k+1)+1 \equiv 1\ [8]$.

Intéressons-nous à présent aux premières *équations diophantiennes* 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 $x^3+7=y^4$ d'inconnue $(x,y) \in \mathbb{Z}^2$.

Pour étudier une équation diophantienne, on la réduit souvent modulo un entier n bien choisi. L'idée, c'est que toute solution qu'on peut trouver dans le vaste monde $\mathbb{Z}$ fournit une solution dans le petit « monde modulo n » — petit car fini de cardinal n. Par contraposition, si une équation n'a pas de solution modulo n, elle en a encore moins dans $\mathbb{Z}$.

Exemple L'équation $x^2-8y^2=3$ d'inconnue $(x,y) \in \mathbb{Z}^2$ n'a pas de solution.

Démonstration Modulo 2, l'équation s'écrit $x^2 \equiv 1\ [2]$ et tous les entiers x impairs en sont solutions — zut. Qu'à cela ne tienne, creusons plus profond. Raisonner plus profondément avec le nombre premier 2, c'est raisonner modulo $2^2=4$, voire modulo $2^3=8$, etc.

Modulo 4, l'équation s'écrit $x^2 \equiv -1\ [4]$, mais le tableau ci-contre montre qu'un carré n'est jamais congru à -1 modulo 4. L'équation étudiée n'a pas de solution dans $\mathbb{Z}^2$.

$x\ [4]$	$x^2\ [4]$
0	0
1	1
2	$4 \equiv 0$
$3 \equiv -1$	1

Exemple Soient $x,y,z \in \mathbb{Z}$ trois entiers pour lesquels $x^3+y^3=z^3$. L'un des entiers x, y ou z est alors divisible par 3. C'est tout ce que nous arriverons à savoir ici, mais c'est déjà ça.

Démonstration Supposons par l'absurde que ni x ni y ni z n'est divisible par 3.

- Modulo 3, x et y sont ainsi congrus chacun à ± 1 modulo 3 et leurs cubes aussi, donc x^3+y^3 est congru à $1+1=2$ ou $1-1=0$ ou $-1+1=0$ ou $-1-1=-2$, i.e. à ± 1 puisqu'on raisonne modulo 3. Le problème, c'est que z^3 aussi est congru à ± 1 modulo 3, donc pas de contradiction pour le moment…
- Qu'à cela ne tienne, creusons plus profond en raisonnant modulo 9. Comme x n'est pas divisible par 3, x est congru à 1, 2, 4, 5, 7 ou 8 modulo 9 et le tableau ci-contre montre que $x^3 \equiv \pm 1\ [9]$. De même, $y^3 \equiv \pm 1\ [9]$ et $z^3 \equiv \pm 1\ [9]$, mais cette fois, x^3+y^3 est congru à 2, 0 ou -2 modulo 9, donc $x^3+y^3 \not\equiv z^3\ [9]$ – 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

Et maintenant, un nouveau point de vue sur les congruences. Raisonner modulo 4, c'est considérer que « $4=0$ » en quelque sorte. Raisonner modulo $n-2$ revient de même à considérer que « $n=2$ », mais plus exactement, $n \equiv 2\ [n-2]$. Le cas échéant, $n^k \equiv 2^k\ [n-2]$ pour tout $k \in \mathbb{N}$, et si on additionne ces relations après les avoir multipliées par des entiers, on en tire que pour tout polynôme P à coefficients entiers : $P(n) \equiv P(2)\ [n-2]$. Par exemple : $n^4-n+3 \equiv 2^4-2+3 \equiv 17\ [n-2]$.

Même chose modulo n^2+1, on peut considérer que « $n^2=-1$ », mais à proprement parler, $n^2 \equiv -1\ \left[n^2+1\right]$. Le cas échéant : $n^3 \equiv -n\ \left[n^2+1\right]$ et $n^4 \equiv (-1)^2 \equiv 1\ \left[n^2+1\right]$, donc $n^4-5n^3+7n^2+1 \equiv 1+5n-7+1 \equiv 5n-5\ \left[n^2+1\right]$.

2 PGCD, PPCM

Définition-théorème **(PGCD, PPCM)** Soient $a_1,\dots,a_r \in \mathbb{Z}$.

- **PGCD :** On appelle *PGCD* (ou *plus grand commun diviseur*) *de* $a_1,\dots,a_r$ tout entier naturel d pour lequel :
$$\mathrm{div}(a_1) \cap \dots \cap \mathrm{div}(a_r) = \mathrm{div}(d)$$
S'il existe, un tel entier d est unique et noté $a_1 \wedge \dots \wedge a_r$.
- **PPCM :** On appelle *PPCM* (ou *plus petit commun multiple*) *de* $a_1,\dots,a_r$ tout entier naturel m pour lequel :
$$a_1\mathbb{Z} \cap \dots \cap a_r\mathbb{Z} = m\mathbb{Z}.$$
S'il existe, un tel entier m est unique et noté $a_1 \vee \dots \vee a_r$.

Attention, rien ne nous garantit pour le moment que $a_1,\dots,a_r$ possèdent un PGCD et un PPCM, mais nous verrons que c'est toujours le cas.

Démonstration Montrons l'unicité du PGCD. Pour tous PGCD d et d' de $a_1,\dots,a_r$: $\text{div}(d)=\text{div}(d')$, donc d et d' se divisent mutuellement, donc sont égaux puisqu'ils sont positifs. Même chose pour le PPCM. ∎

Exemple $12\wedge 18=6$ et $12\vee 18=36$.

Démonstration
$$\begin{aligned}\text{div}(12)\cap\text{div}(18)&=\{\pm1,\pm2,\pm3,\pm4,\pm6,\pm12\}\cap\{\pm1,\pm2,\pm3,\pm6,\pm9,\pm18\}\\&=\{\pm1,\pm2,\pm3,\pm6\}=\text{div}(6).\end{aligned}$$
Quant aux multiples communs de 12 et 18, ce 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.

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

Démonstration
$$\text{div}(a)\cap\text{div}(1)=\text{div}(a)\cap\{\pm1\}=\{\pm1\}=\text{div}(1)$$
et
$$\text{div}(a)\cap\text{div}(0)=\text{div}(a)\cap\mathbb{Z}=\text{div}(a)=\text{div}\big(|a|\big).$$

Dans $\mathbb{R}$, nous avons défini les notions de majorant, plus grand élément et borne supérieure d'une partie au sens de la relation d'ordre $\leqslant$. Les mêmes définitions auraient pu être énoncées dans le cas d'une relation d'ordre quelconque. En particulier, la relation de divisibilité $|$ a beau ne pas être une relation d'ordre sur $\mathbb{Z}$, c'en est au moins une sur $\mathbb{N}$. Pour cette raison, les lignes qui suivent ne portent que sur des entiers naturels et la relation d'ordre utilisée est la relation $|$ et non pas la relation $\leqslant$.

- Dire que a divise b, c'est dire que a est plus petit que b.
- Les diviseurs communs de $a_1,\dots,a_r$ sont exactement les minorants de $\{a_1,\dots,a_r\}$ et les multiples communs de $a_1,\dots,a_r$ sont exactement les majorants de $\{a_1,\dots,a_r\}$.
- L'ensemble $\text{div}^+(d)=\text{div}(d)\cap\mathbb{N}$ admet d pour plus grand élément. L'ensemble $m\mathbb{N}$ admet m pour plus petit élément.
- Dire que $\text{div}^+(a_1)\cap\ldots\cap\text{div}^+(a_r)=\text{div}^+(d)$, c'est dire que d est le plus grand minorant de $\{a_1,\dots,a_r\}$, i.e. sa borne inférieure. De même, dire que $a_1\mathbb{N}\cap\ldots\cap a_r\mathbb{N}=m\mathbb{N}$, c'est dire que m est le plus petit majorant de $\{a_1,\dots,a_r\}$, i.e. sa borne supérieure. Dans les acronymes « PGCD » et « PPCM », « plus grand » et « plus petit » sont à comprendre en priorité au sens de la divisibilité.

2.1 Existence et calcul du PGCD

L'existence du PGCD de deux entiers repose sur une idée simple que j'appelle personnellement l'*idée fondamentale de l'algorithme d'Euclide*. Soient $a,b,n\in\mathbb{Z}$. Sous l'hypothèse que $a\equiv b\ [n]$, montrons que $\text{div}(a)\cap\text{div}(n)=\text{div}(b)\cap\text{div}(n)$. Or puisque $b=a+kn$ 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.

En particulier, pour tous $a\in\mathbb{Z}$ et $b\in\mathbb{N}^*$: $\text{div}(a)\cap\text{div}(b)=\text{div}(b)\cap\text{div}(r)$ si on note r le reste de la division euclidienne de a par b.

Théorème (Existence du PGCD, cas de deux entiers) Deux entiers relatifs possèdent toujours un PGCD.

Plus précisément, pour tous $a,b\in\mathbb{Z}$:
$$a\wedge b=\begin{cases}\max\big(\text{div}(a)\cap\text{div}(b)\big) & \text{si } a\neq 0 \text{ ou } b\neq 0\\ 0 & \text{si } a=b=0.\end{cases}$$

C'était clair à l'avance, mais en passant, pour tous $a,b\in\mathbb{Z}$: $a\wedge b=|a|\wedge|b|$ et $a\wedge b=b\wedge a$.

Démonstration Soient $a,b\in\mathbb{Z}$. L'existence de $a\wedge b$ sera prouvée en deux temps, d'abord sous l'hypothèse que $0\leqslant b\leqslant a$, puis dans le cas général.

- **Algorithme d'Euclide dans le cas où $0\leqslant b\leqslant a$:** On définit dans ce cas une famille 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 $r_{k+1}>0$, 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, $r_N = 0$ pour un certain $N \in \mathbb{N}^*$, autrement dit l'algorithme se termine. Or grâce à l'idée fondamentale de l'algorithme d'Euclide :

$$\begin{aligned}\operatorname{div}(a) \cap \operatorname{div}(b) &= \operatorname{div}(r_0) \cap \operatorname{div}(r_1) = \operatorname{div}(r_1) \cap \operatorname{div}(r_2) = \ldots = \operatorname{div}(r_{N-1}) \cap \operatorname{div}(r_N)\\ &= \operatorname{div}(r_{N-1}) \cap \operatorname{div}(0) = \operatorname{div}(r_{N-1}) \cap \mathbb{Z} = \operatorname{div}(r_{N-1}),\end{aligned}$$

donc a et b possèdent un PGCD, en l'occurrence r_{N-1}.

Pour finir, si $a = 0$, alors $a = b = 0$, donc $N = 1$, donc $a \wedge b = r_0 = 0$. Si au contraire $a > 0$, alors $r_{N-1} > 0$, donc $a \wedge b = r_{N-1} = \max \operatorname{div}(r_{N-1}) = \max\big(\operatorname{div}(a) \cap \operatorname{div}(b)\big)$.

- **Cas général :** On traite le cas général en se ramenant au cas précédent. On peut supposer a et b positifs car $\operatorname{div}(a) \cap \operatorname{div}(b) = \operatorname{div}\big(|a|\big) \cap \operatorname{div}\big(|b|\big)$, et supposer aussi $b \leqslant a$ car $\operatorname{div}(a) \cap \operatorname{div}(b) = \operatorname{div}(b) \cap \operatorname{div}(a)$. ∎

L'*algorithme d'Euclide* calcule rapidement le PGCD de deux entiers a et b pour lesquels $0 < b \leqslant a$. D'après ce qui précède :

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

Exemple $1542 \wedge 58 = 2$.

Démonstration On applique l'algorithme d'Euclide : $1542 = 26 \times 58 + 34$, $58 = 1 \times 34 + 24$, $34 = 1 \times 24 + 10$, $24 = 2 \times 10 + 4$, $10 = 2 \times 4 + 2$ et $4 = 2 \times 2 + 0$. Dernier reste non nul

L'idée fondamentale de l'algorithme d'Euclide gagne à être connue sous la forme suivante.

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

Démonstration On sait déjà que $\operatorname{div}(a) \cap \operatorname{div}(n) = \operatorname{div}(b) \cap \operatorname{div}(n)$, mais maintenant que les PGCD existent : $\operatorname{div}(a \wedge n) = \operatorname{div}(b \wedge n)$, puis $a \wedge n = b \wedge n$ par unicité. ∎

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 (Existence du PGCD, cas général) Toute collection finie d'entiers relatifs possède un PGCD.

Démonstration Par récurrence sur le nombre d'entiers.

- **Initialisation :** Deux entiers relatifs possèdent toujours un PGCD !
- **Hérédité :** Soit $r \geqslant 2$. On suppose que toute collection de r entiers relatifs possède un PGCD. Pour tous $a_1, \ldots, a_{r+1} \in \mathbb{Z}$: $\operatorname{div}(a_1) \cap \ldots \cap \operatorname{div}(a_{r+1}) = \big(\operatorname{div}(a_1) \cap \ldots \cap \operatorname{div}(a_r)\big) \cap \operatorname{div}(a_{r+1})$
$\overset{\text{HDR}}{=} \operatorname{div}(a_1 \wedge \ldots \wedge a_r) \cap \operatorname{div}(a_{r+1}) = \operatorname{div}\big((a_1 \wedge \ldots \wedge a_r) \wedge a_{r+1}\big)$,
donc $a_1, \ldots, a_{r+1}$ possèdent un PGCD. ∎

Le calcul du PGCD de plus de deux entiers se ramène toujours à de simples calculs de PGCD de deux entiers.

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

Théorème (Factorisation d'un PGCD) Pour tous $a_1, \ldots, a_r, k \in \mathbb{Z}$: $(ka_1) \wedge \ldots \wedge (ka_r) = |k|(a_1 \wedge \ldots \wedge a_r)$.

Démonstration Supposons $k \neq 0$ et contentons-nous du cas $r = 2$ pour simplifier. Il nous suffit de montrer que les entiers $(ka_1) \wedge (ka_2)$ et $k(a_1 \wedge a_2)$ se divisent mutuellement.

- Pour commencer, $k(a_1 \wedge a_2)$ divise ka_1 et ka_2, donc aussi $(ka_1) \wedge (ka_2)$ par définition du PGCD.
- Inversement, k divise ka_1 et ka_2, donc aussi $(ka_1) \wedge (ka_2)$ par définition du PGCD, donc $(ka_1) \wedge (ka_2) = |k| \times d$ pour un certain $d \in \mathbb{N}$. Dans ces conditions, $|k| \times d$ divise ka_1 et ka_2 avec $k \neq 0$, donc d divise a_1 et a_2, donc aussi $a_1 \wedge a_2$. En retour, $(ka_1) \wedge (ka_2) = |k| \times d$ divise $k(a_1 \wedge a_2)$. ∎

2.2 Relations de Bézout

Définition-théorème **(Relations de Bézout, cas de 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 $2=(-1)\times\underline{4}+1\times\underline{6}=2\times\underline{4}+(-1)\times\underline{6}$.

Démonstration On peut supposer sans perte de généralité que $0\leqslant b\leqslant a$ et s'intéresser de nouveau aux restes successifs $r_0,\dots,r_N$ de l'algorithme d'Euclide. Concrètement, $r_0=a$, $r_1=b$, $r_{N-1}=a\wedge b$ et $r_N=0$, et r_{k+2} est le reste de la division euclidienne de r_k par r_{k+1} pour tout $k\in[\![0,N-2]\!]$. Montrons par récurrence double que $r_k\in a\mathbb{Z}+b\mathbb{Z}$ pour tout $k\in[\![0,N]\!]$. Cela montrera en particulier comme voulu que $a\wedge b=r_{N-1}\in a\mathbb{Z}+b\mathbb{Z}$.

Observons en amont que toute combinaison linéaire à coefficients entiers d'éléments de $a\mathbb{Z}+b\mathbb{Z}$ est encore un élément de $a\mathbb{Z}+b\mathbb{Z}$. En d'autres termes, pour tous $x,y\in a\mathbb{Z}+b\mathbb{Z}$ et $m,n\in\mathbb{Z}$: $mx+ny\in a\mathbb{Z}+b\mathbb{Z}$ ★.

Initialisation : $r_0=a\times 1+b\times 0\in a\mathbb{Z}+b\mathbb{Z}$ et $r_1=a\times 0+b\times 1\in a\mathbb{Z}+b\mathbb{Z}$.

Hérédité : Soit $k\in[\![0,N-2]\!]$. Si $r_k\in a\mathbb{Z}+b\mathbb{Z}$ et $r_{k+1}\in a\mathbb{Z}+b\mathbb{Z}$, alors en notant q le quotient de la division euclidienne de r_k par r_{k+1}, le reste $r_{k+2}=r_k-qr_{k+1}$ appartient à $a\mathbb{Z}+b\mathbb{Z}$ d'après ★ et c'est tout. ■

Le procédé de construction des entiers u et v de cette démonstration s'appelle l'*algorithme d'Euclide étendu* et sa mise en œuvre concrète sera plus claire après un exemple. En résumé, alors que l'algorithme d'Euclide ne s'intéresse qu'aux restes des divisions euclidiennes successives, l'algorithme d'Euclide étendu va plus loin et tient compte aussi des quotients.

Exemple $3080\wedge 525=35=7\times 3080+(-41)\times 525$.

Démonstration On calcule d'abord les restes successifs associés aux entiers 3080 et 525 :

$$\underline{3080}=5\times\underline{525}+\underline{455},\qquad \underline{525}=1\times\underline{455}+\underline{70},\qquad \underline{455}=6\times\underline{70}+\underline{35},\qquad \underline{70}=2\times\underline{35}+\underline{0}.$$

Le dernier reste non nul vaut 35, c'est notre PGCD. Pour calculer un jeu de coefficients de Bézout associé, on remonte la chaîne des restes successifs en partant du PGCD 35 :

$$\begin{aligned}\underline{35}&=\underline{455}-6\times\underline{70} && \text{(On a éliminé } \underline{35}.\text{)}\\ &=\underline{455}-6\times\big(\underline{525}-1\times\underline{455}\big)=(-6)\times\underline{525}+7\times\underline{455} && \text{(On a éliminé } \underline{70}.\text{)}\\ &=(-6)\times\underline{525}+7\times\big(\underline{3080}-5\times\underline{525}\big)=7\times\underline{3080}+(-41)\times\underline{525}. && \text{(On a éliminé } \underline{455}.\text{)}\end{aligned}$$

Nous nous contenterons d'un exemple, mais le résultat qui précède reste vrai pour une collection quelconque d'entiers.

Définition-théorème **(Relations de Bézout, cas général)** Soient $a_1,\dots,a_r\in\mathbb{Z}$. Il existe des entiers $u_1,\dots,u_r\in\mathbb{Z}$ pour lesquels $a_1\wedge\dots\wedge a_r=a_1u_1+\dots+a_ru_r$. Une telle relation est appelée UNE *relation de Bézout de $a_1,\dots,a_r$*.

Exemple $10\wedge 15\wedge 24=1=(-5)\times 10+5\times 15+(-1)\times 24$.

Démonstration
$$\begin{cases}\text{Première relation de Bézout :} & 10\wedge 15=5=(-1)\times\underline{10}+1\times\underline{15}.\\ \text{Deuxième relation de Bézout :} & 5\wedge 24=1=5\times\underline{5}+(-1)\times\underline{24}.\end{cases}$$

On emboîte : $$\begin{aligned}10\wedge 15\wedge 24=5\wedge 24=5\times\underline{5}+(-1)\times\underline{24}&=5\times\big((-1)\times\underline{10}+1\times\underline{15}\big)+(-1)\times\underline{24}\\ &=(-5)\times\underline{10}+5\times\underline{15}+(-1)\times\underline{24}.\end{aligned}$$

2.3 Existence et calcul du PPCM

On rappelle que pour tous $a_1,\dots,a_r\in\mathbb{Z}$, le PPCM $a_1\vee\dots\vee a_r$ des entiers $a_1,\dots,a_r$ est positif et défini par la relation $a_1\mathbb{Z}\cap\dots\cap a_r\mathbb{Z}=(a_1\vee\dots\vee a_r)\mathbb{Z}$, du moins s'il existe.

Théorème **(PPCM, cas de deux entiers)** Deux entiers relatifs possèdent toujours un PPCM.

Plus précisément, pour tous $a,b\in\mathbb{Z}$: $(a\wedge b)(a\vee b)=|ab|$ et $a\vee b=\begin{cases}\min\big(a\mathbb{N}^*\cap b\mathbb{N}^*\big) & \text{si } a\neq 0 \text{ et } b\neq 0\\ 0 & \text{si } a=0 \text{ ou } b=0.\end{cases}$

Démonstration Si $a=0$ ou $b=0$, alors $a\mathbb{Z}\cap b\mathbb{Z}=\{0\}=0\mathbb{Z}$, donc $a\vee b=0$ et $(a\wedge b)(a\vee b)=|ab|$. Supposons désormais $a\neq 0$ et $b\neq 0$, de sorte que $a\wedge b\neq 0$. Pour tout $n\in\mathbb{Z}$:

$$n\in a\mathbb{Z}\cap b\mathbb{Z} \iff a\mid n \text{ et } b\mid n \iff ab\mid an \text{ et } ab\mid bn \iff ab\mid (an)\wedge(bn)$$
$$\iff ab\mid (a\wedge b)n \iff \frac{ab}{a\wedge b}\,\Big|\, n \iff n\in\frac{|ab|}{a\wedge b}\mathbb{Z},$$

donc $a\mathbb{Z}\cap b\mathbb{Z}=\dfrac{|ab|}{a\wedge b}\mathbb{Z}$, donc a et b possèdent un PPCM et en l'occurrence $a\vee b=\dfrac{|ab|}{a\wedge b}$.

Pour finir : $a\mathbb{N}^*\cap b\mathbb{N}^*=\dfrac{|ab|}{a\wedge b}\mathbb{N}^*$, donc $a\vee b=\min\big(a\mathbb{N}^*\cap b\mathbb{N}^*\big)$. ∎

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

Nous admettrons les résultats suivants pour ne pas perdre de temps.

Théorème **(Existence du PPCM, cas général)** Toute collection finie d'entiers relatifs possède un PPCM.

Théorème **(Factorisation d'un PPCM)** Pour tous $a_1,\dots,a_r,k\in\mathbb{Z}$: $(ka_1)\vee\dots(ka_r)=|k|(a_1\vee\dots\vee a_r)$.

3 Unicité de la factorisation première

Théorème **(Deux propriétés des nombres premiers)** Soient p un NOMBRE PREMIER, $a,b\in\mathbb{Z}$ et $n\in\mathbb{N}$.

(i) **Être ou ne pas être divisible par un nombre premier :** $p\not\mid a \iff a\wedge p=1$.

(ii) **Lemme d'Euclide :** $p\mid ab \iff p\mid a$ ou $p\mid b$. En particulier : $p\mid a^n \iff p\mid a$.

✖ **Attention !** La primalité de p est indispensable. Par exemple, pour l'assertion (i), $6\not\mid 10$ mais $6\wedge 10=2$. Et pour le lemme d'Euclide, $4\mid 2^2$ mais $4\not\mid 2$.

Démonstration

(i) Comme p est premier, ses diviseurs sont ±1 et $\pm p$, donc $a\wedge p$ vaut 1 ou p, en l'occurrence p si a est divisible par p et 1 sinon.

(ii) Si p divise a ou b, alors p divise ab. Réciproquement, faisons l'hypothèse que p divise ab mais pas a. Ainsi, $a\wedge p=1$ d'après (i), donc $au+pv=1$ pour certains $u,v\in\mathbb{Z}$. En retour, $b=abu+pbv$ est divisible par p car ab l'est. ∎

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

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

Démonstration Tout d'abord $p^0\mid n$. Ensuite, pour tout $k\in\mathbb{N}$ pour lequel p^k divise n : $k\leqslant p^k\leqslant|n|$. Ainsi, $\big\{k\in\mathbb{N}\mid p^k\mid n\big\}$ 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. Ainsi, la contraposée du lemme d'Euclide affirme que $a'b'$ n'est pas divisible par p. L'égalité $ab=p^{v_p(a)+v_p(b)}a'b'$ montre donc comme voulu que $v_p(ab)=v_p(a)+v_p(b)$. ∎

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

Et voilà, nous sommes enfin en mesure de prouver l'unicité de la factorisation première — à l'ordre près. Alors que l'existence était facile à obtenir, l'unicité requiert une certaine artillerie. Elle repose sur l'additivité des valuations p-adiques, qui découle du lemme d'Euclide, qui découle de l'existence des relations de Bézout.

Théorème **(Factorisation première)** Pour tout $n\in\mathbb{N}^*$, il existe une et une seule famille *presque nulle* $\left(v_p(n)\right)_{p\in\mathbb{P}}$ d'entiers naturels — i.e. dont tous les éléments sont nuls sauf un nombre fini d'entre eux — pour laquelle :

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

Cette décomposition est appelée la *factorisation première de n*.

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 $p\in\mathbb{P}$: $\quad v_p(n)=v_p\left(\prod_{q\in\mathbb{P}}q^{\alpha_q}\right)=\sum_{q\in\mathbb{P}}v_p\left(q^{\alpha_q}\right)=\alpha_p$ par additivité des valuations p-adiques, donc la famille $(\alpha_p)_{p\in\mathbb{P}}$ est nécessairement la famille $\left(v_p(n)\right)_{p\in\mathbb{P}}$ — 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 $v_p(a)\leqslant v_p(b)$ pour tout $p\in\mathbb{P}$.

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

La réduction d'une somme de rationnels au même dénominateur exploite l'expression (ii) du PPCM. Le plus petit dénominateur commun de $\frac{13}{12}+\frac{7}{30}$ vaut $12\vee 30=2^2.3\vee 2.3.5=2^2.3.5=60$. Bref : $\quad\frac{5}{12}+\frac{7}{30}=\frac{25+14}{60}=\frac{39}{60}=\frac{13}{20}$.

Démonstration

(i) Si $a\mid b$, alors $b=ak$ 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 a et b. Montrer que $d=a\wedge b$ revient donc à montrer que $\frac{a}{d}\wedge\frac{b}{d}=1$. Raisonnons pour cela par l'absurde en supposant $\frac{a}{d}\wedge\frac{b}{d}\neq 1$. L'entier $\frac{a}{d}\wedge\frac{b}{d}$ possède alors un diviseur premier q, donc $v_q(a)=v_q(d)+v_q\left(\frac{a}{d}\right)\geqslant v_q(d)+1$ et de même $v_q(b)\geqslant v_q(d)+1$. En retour : $\quad\min\{v_q(a),v_q(b)\}\geqslant v_q(d)+1=\min\{v_q(a),v_q(b)\}+1\quad$ — contradiction.

Pour le PPCM : $\quad x+y=\min\{x,y\}+\max\{x,y\}\quad$ 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 $600\wedge 740=2^3.3.5^2\wedge 2^2.5.37=2^2.5=20$.

Exemple Pour tout $n\in\mathbb{N}^*$, l'entier n possède exactement $\prod_{p\in\mathbb{P}}\left(v_p(n)+1\right)$ diviseurs positifs.

Démonstration D'après l'assertion (i) du théorème précédent, les diviseurs positifs de n sont exactement les entiers $\prod_{p\in\mathbb{P}}p^{\alpha_p}$ où $\alpha_p\in[\![0,v_p(n)]\!]$ pour tout $p\in\mathbb{P}$, et il y en a autant que de familles $(\alpha_p)_{p\in\mathbb{P}}$, à savoir $\prod_{p\in\mathbb{P}}\left|[\![0,v_p(n)]\!]\right|=\prod_{p\in\mathbb{P}}\left(v_p(n)+1\right)$. Vous noterez bien que ce produit est fini en dépit des apparences.

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 $v_3\left(3a^5\right)=v_3\left(4b^5\right)$, ce qui s'écrit aussi $5v_3(a)+1=5v_3(b)$, puis $1\equiv 0\ [5]$ après réduction modulo 5 — contradiction !

4 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 $a \wedge b = 1$. Il est équivalent de dire que a et b n'ont aucun diviseur premier commun.

Situation fondamentale : Quand on factorise a et b par leur PGCD : $a = (a \wedge b)a'$ et $b = (a \wedge b)b'$, les entiers a' et b' sont premiers entre eux — à condition de choisir $a' = 1$ si $a = 0$ et $b' = 1$ si $b = 0$.

Factoriser a et b par $a \wedge b$, c'est leur arracher à chacun ce qu'ils ont de commun au sens de la divisibilité. Pas étonnant que a' et b' n'aient plus rien en commun après coup, i.e. qu'ils soient premiers entre eux ! De façon plus technique, si $(a, b) \neq (0, 0)$, alors en posant $d = a \wedge b \neq 0$: $d = a \wedge b = (da') \wedge (db') = d(a' \wedge b')$, donc $a' \wedge b' = 1$.

Exemple 6 et 35 sont premiers entre eux car $6 \wedge 35 = 2.3 \wedge 5.7 = 1$. Sans factorisation première, un simple calcul de PGCD par l'algorithme d'Euclide montre que $6 \wedge 35 = 1$.

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

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 $d \neq 0$. 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 $(x', y') = (2, 1)$, donc $(x, y) = (2, 1)$.

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

- **Synthèse :** Les couples $(2, 1)$ et $(2, 0)$ sont bel et bien solutions de l'équation étudiée.

Lançons-nous à présent dans une petite réflexion pratique sur la notion d'entier. La plupart du temps, quand on trouve l'arithmétique difficile, c'est d'abord parce qu'on se représente mal les entiers. Moralement, tout entier $p_1^{\alpha_1} \dots p_r^{\alpha_r}$ gagne à être vu comme une sorte d'urne contenant α_1 boules de numéro p_1, α_2 boules de numéro p_2, etc. Cette vision des choses rapproche les entiers naturels non nuls des ensembles, mais dans un ensemble, chaque élément n'est présent qu'une fois alors qu'une urne peut contenir plusieurs boules de même numéro. L'entier $40 = 2^3 \times 5$ est l'urne contenant 3 boules de numéro 2 et 1 boule de numéro 5. L'entier 1 est simplement l'urne vide.

- Multiplier deux entiers revient à les concaténer en tant qu'urnes, i.e. à en superposer les contenus. Les exposants d'un même nombre premier sont additionnés. Par exemple, $12 \times 20 = 2^2.3 \times 2^2.5 = 2^4.3.5 = 240$.
- Se demander si a divise b revient à se demander si on trouve a dans b intégralement ou non. Par exemple, $20 = 2^2.5$ divise $120 = 2^3.3.5$ car les exposants de nombres premiers sont tous plus grands dans 120 que dans 20.
- Calculer $a \wedge b$ revient à chercher le contenu commun des urnes a et b. Ainsi, $36 \wedge 90 = 2^2.3^2 \wedge 2.3^2.5 = 2.3^2 = 18$.
- La confusion la plus courante en arithmétique est celle des propositions « a ne divise pas b » et « a et b sont premiers entre eux ». Nous avons vu que pour tout p PREMIER : $p \nmid a \iff a \wedge p = 1$, mais cette équivalence est fausse en général. Simplement, quand p est premier, l'urne p ne contient qu'une boule, donc c'est tout ou rien — soit a contient p intégralement, soit a et p n'ont rien de commun.

  En toute généralité, dire que a ne divise pas b, c'est juste dire que b ne contient pas l'intégralité de a, ce qui n'empêche pas a et b d'avoir beaucoup de diviseurs communs. Dire que $a \wedge b = 1$, c'est dire beaucoup plus, c'est affirmer que a et b n'ont rien de commun si ce n'est ± 1. Bref :

  $$a \nmid b \quad \not\Longrightarrow \quad a \wedge b = 1$$

  Par exemple, $4 \nmid 2$ mais $4 \wedge 2 = 2 \neq 1$, et $6 \nmid 15$ mais $6 \wedge 15 = 3 \neq 1$. En passant, la proposition $a \wedge b = 1$ donne des rôles symétriques à a et b alors que les propositions $a \nmid b$ et $b \nmid a$ n'ont pas du tout la même signification.

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 $\Longrightarrow$ Premiers entre eux DANS LEUR ENSEMBLE

… mais la réciproque est fausse ! Par exemple, 6, 10 et 15 sont premiers entre eux dans leur ensemble, i.e. n'ont rien de commun à trois, mais cela ne les empêche pas d'avoir un contenu commun deux par deux : $6 \wedge 10 = 2$, $6 \wedge 15 = 3$ et $10 \wedge 15 = 5$.

Théorème (Théorèmes de Bézout et Gauss) Soient $a, b, c \in \mathbb{Z}$.

(i) **Théorème de Bézout :** $a \wedge b = 1 \iff \exists u, v \in \mathbb{Z},\ au + bv = 1$.

(ii) **Théorème de Gauss :** Si $a \mid bc$ avec $a \wedge b = 1$, alors $a \mid c$.

D'après le théorème de Gauss, si a est dans bc mais n'a rien de commun avec b, alors a est dans c. Assez logique !

Démonstration

(i) Pour l'implication directe, nous avons déjà montré en toute généralité que $a \wedge b = au + bv$ pour certains $u, v \in \mathbb{Z}$. Réciproquement, faisons l'hypothèse que $au + bv = 1$ pour certains $u, v \in \mathbb{Z}$. Pour tout diviseur commun d et a et b, d divise $au + bv = 1$, donc $d = \pm 1$, donc $a \wedge b = 1$.

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

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

(ii–i) Si chacun des entiers $a_1, \dots, a_r$ est premier avec n, leur produit $a_1 \dots a_r$ l'est aussi.

(ii–ii) 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) On ne peut pas toujours simplifier par m dans une congruence $ma \equiv mb\ [n]$. Par exemple, $2 \times 3 \equiv 2 \times 0\ [6]$ mais $3 \not\equiv 0\ [6]$.

(ii–ii) En général : $a \mid n$ et $b \mid n \not\Longrightarrow ab \mid n$. Par exemple, $4 \mid 12$ et $6 \mid 12$ mais $24 \nmid 12$.

En tant qu'urne, n peut être assez grand pour contenir a et b mais pas assez pour contenir ab car $a \wedge b$ est compté deux fois dans ab, une fois dans a et une fois dans b. D'où l'importance de supposer a et b premiers entre eux.

Plus généralement, il est impératif que $a_1, \dots, a_r$ soient premiers entre eux DEUX À DEUX dans (ii–ii). Par exemple, les entiers $6 = 2.3$, $10 = 2.5$ et $15 = 3.5$ sont premiers entre eux dans leur ensemble et divisent $30 = 2.3.5$, mais 30 n'est pas divisible par leur produit $2^2.3^3.5^2 = 900$.

Démonstration Nous nous contenterons du cas de deux entiers a et b pour l'assertion (ii).

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

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

(ii–ii) Supposons n divisible par a et b avec $a \wedge b = 1$. Ainsi, $n = ak$ pour un certain $k \in \mathbb{Z}$, donc b divise $n = ak$ avec $a \wedge b = 1$, donc $b \mid k$ d'après le théorème de Gauss. A fortiori, ab divise $ak = n$.

Le résultat qui suit n'est pas officiellement au programme, mais il intervient naturellement dans la résolution d'un certain nombre d'équations diophantiennes.

Théorème (Une recette pour casser les puissances) Soient $a, b \in \mathbb{Z}$ et $k \geqslant 2$.

(i) **Avec des entiers positifs :** Si ab est une puissance $k^{\text{ème}}$ d'entier avec $a \wedge b = 1$ et a et b positifs, alors a et b sont chacun une puissance $k^{\text{èmes}}$ d'entier.

(ii) **Avec des entiers quelconques :** Dans le cas général, la parité de k complique un peu la conclusion :

— si k est impair, a et b sont chacun une puissance $k^{\text{èmes}}$ d'entier,

— si k est pair, a et b sont soit chacun une puissance $k^{\text{èmes}}$ d'entier, soit chacun l'opposé d'une telle puissance.

Démonstration

(i) Pour commencer, si $a=0$, alors $b=0\wedge b=a\wedge b=1$, donc $0=0^k$ et $1=1^k$ sont des puissances $k^{\text{èmes}}$ d'entier. Même chose si $b=0$. Supposons désormais a et b non nuls. Par hypothèse, $ab=c^k$ pour un certain $c\in\mathbb{N}^*$.

Fixons $p\in\mathbb{P}$. Alors d'une part : $\min\{v_p(a),v_p(b)\}=v_p(a\wedge b)=v_p(1)=0$, donc $v_p(a)=0$ ou $v_p(b)=0$, mais d'autre part : $v_p(a)+v_p(b)=v_p(ab)=v_p(c^k)=kv_p(c)$. Ainsi, si $v_p(a)=0$, alors $v_p(b)=v_p(a)+v_p(b)=kv_p(c)$, et si $v_p(b)=0$, alors $v_p(a)=v_p(a)+v_p(b)=kv_p(c)$. Dans les deux cas, les deux valuations $v_p(a)$ et $v_p(b)$ sont divisibles par k car l'une est nulle et l'autre vaut $kv_p(c)$.

Conclusion : $A=\prod_{p\in\mathbb{P}}p^{\frac{v_p(a)}{k}}$ et $B=\prod_{p\in\mathbb{P}}p^{\frac{v_p(b)}{k}}$ sont des entiers, donc $a=A^k$ et $b=B^k$ sont des puissances $k^{\text{èmes}}$ d'entiers.

(ii) Par hypothèse, $ab=c^k$ pour un certain $k\in\mathbb{Z}$, donc $|ab|=|c|^k$, donc $|a|$ et $|b|$ sont chacun une puissance $k^{\text{ème}}$ d'entier d'après (i). A fortiori, a et b sont soit chacun une puissance $k^{\text{èmes}}$ d'entier, soit chacun l'opposé d'une puissance $k^{\text{èmes}}$ d'entier. Cela dit, si k est impair, ces deux cas n'en font qu'un car $(-1)^k=1$.

Exemple L'équation $y^3=x^2+x$ d'inconnue $(x,y)\in\mathbb{Z}$ possède deux solutions, à savoir $(0,0)$ et $(-1,0)$.

Démonstration Soit $(x,y)\in\mathbb{Z}^2$. On suppose que $y^3=x^2+x$. Ainsi, $x(x+1)$ est un cube parfait avec $x\wedge(x+1)=1$, donc d'après le théorème précédent, sachant que l'exposant 3 est impair, x et $x+1$ sont eux-mêmes des cubes parfaits, disons $x=a^3$ et $x+1=b^3$ pour certains $a,b\in\mathbb{Z}$. En particulier, $a^3<b^3$ donc $a<b$. L'égalité $(b-a)\left(a^2+ab+b^2\right)=b^3-a^3=1$ montre en retour que $b-a=a^2+ab+b^2=1$, puis que $a^2+a(a+1)+(a+1)^2=1$. Après simplification, $a(a+1)=0$ donc $a\in\{0,-1\}$, donc $x=a^3\in\{0,-1\}$, puis $(x,y)\in\{(0,0),(-1,0)\}$. Réciproquement, les couples $(0,0)$ et $(-1,0)$ sont solutions de l'équation étudiée.

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

En choisissant p dans $\mathbb{Z}$ et q dans $\mathbb{N}^*$, on impose que le signe soit porté par le numérateur. Sans cela, pas d'unicité !

Démonstration

- **Unicité :** Soient $(p,q),(p',q')\in\mathbb{Z}\times\mathbb{N}^*$. On suppose que $r=\frac{p}{q}=\frac{p'}{q'}$ avec $p\wedge q=1$ et $p'\wedge q'=1$. Aussitôt $pq'=p'q$, donc $q\mid pq'$. Cela dit $p\wedge q=1$, donc $q\mid q'$ d'après le théorème de Gauss, puis $q'\mid q$ par symétrie des rôles de q et q'. En d'autres termes, $|q|=|q'|$ avec q et q' positifs donc $q=q'$, et enfin $p=p'$.
- **Existence :** Par définition, $r=\frac{a}{b}$ pour certains $a,b\in\mathbb{Z}$ avec $b\neq0$, et même $b>0$ sans perte de généralité. En notant d le PGCD de a et b, $a=dp$ et $b=dq$ pour certains $p\in\mathbb{Z}$ et $q\in\mathbb{N}^*$ premiers entre eux, donc $r=\frac{a}{b}=\frac{dp}{dq}=\frac{p}{q}$.