Chapitre 12

Arithmétique des entiers

I Divisibilité dans $\mathbb{Z}$

1) Diviseurs et multiples

On note $a \nmid b$ lorsque a ne divise pas b.

Définition (diviseurs et multiples). *Soit $(a,b) \in \mathbb{Z}^2$. On dit que a divise b s'il existe $c \in \mathbb{Z}$ tel que $b = ac$. On note alors $a|b$. On dit aussi que a est un diviseur de b ou encore que b est un multiple de a.*

Exemples :

- $7|35$ *puisque* $35 = 7 \times 5$.
- *Pour tout* $c \in \mathbb{Z}$, $2c \neq 35$. *Ainsi* $2 \nmid 35$.
- *Lorsque* 2 *divise un entier, on dit que cet entier est pair. On dit qu'il est impair sinon.*

Remarques :

- Soit $(a,b) \in \mathbb{Z}^2$ avec a non nul. Si a divise b, alors il existe $c \in \mathbb{Z}$ tel que $b = ac$ et donc $c = \dfrac{b}{a}$ est uniquement déterminé. Réciproquement, si $\dfrac{b}{a}$ est un entier, alors $c = \dfrac{b}{a}$ vérifie $b = ac$ et donc a divise b. Retenons donc que, lorsque a est non nul,
$$a|b \quad \iff \quad \frac{b}{a} \in \mathbb{Z}.$$

Un diviseur d'un entier naturel a qui n'est pas a (ou $-a$) est appelé diviseur strict.

- Pour tout $a \in \mathbb{Z}$, $a = 1 \times a = (-1) \times (-a)$ donc $1|a$, $-1|a$, $a|a$ et $-a|a$.
- Pour tout $a \in \mathbb{Z}$, $0 = a \times 0$ donc $a|0$.
- Pour tout $c \in \mathbb{Z}$, $0 \times c = 0$ si bien que 0 est le seul diviseur de 0. Cela peut paraître provoquant de dire que 0 divise 0 puisque l'on répète sans cesse qu'on ne peut pas diviser par 0. Mais s'il est une chose de dire qu'un entier a divise un entier b, il en est une autre que de diviser ces deux nombres de façon effective (c'est-à-dire expliciter c tel que $b = ac$). Ici dire que 0 divise 0 a un sens (puisqu'il existe en effet c tel que $0 = 0 \times c$, par exemple $c = 1$ convient) tandis que $\dfrac{0}{0}$ n'a aucun sens (et plus généralement $\dfrac{b}{0}$ n'a de sens pour aucun entier b).

Dans ce cours, on notera $\mathrm{Div}(a)$ l'ensemble des diviseurs de a mais ce n'est pas une notation universelle et officielle.

- Pour tout $a \in \mathbb{Z}$, on note $a\mathbb{Z} = \{b \in \mathbb{Z} \,|\, \exists k \in \mathbb{Z}, \quad b = ak\}$ l'ensemble des multiples de a. Pour tout $b \in \mathbb{Z}$, on a donc
$$a|b \quad \iff \quad b \in a\mathbb{Z}.$$
Par exemple $0\mathbb{Z} = \{0\}$, $1\mathbb{Z} = \mathbb{Z}$, $2\mathbb{Z}$ *est l'ensemble des entiers pairs,* $3\mathbb{Z} = \{\ldots, -9; -6; -3; 3; 6; 9; \ldots\}$, *etc.*
- Si $(a,b) \in \mathbb{Z}^2$ sont tels que $ab = 1$, alors $a = b = 1$ ou $a = b = -1$. En effet on a alors $|a| \times |b| = 1$ donc $|a| \neq 0$ et $|b| \neq 0$ donc $|a| \leqslant |a| \times |b| = 1$ donc $a = 1$ ou $a = -1$ (et donc $b = 1$ ou $b = -1$ respectivement).

2) Premières propriétés des diviseurs

Toutes ces propositions sont donc encore équivalentes à $\pm|a|$ divise $\pm|b|$.

Proposition. *Soient $(a,b) \in \mathbb{Z}^2$. On a*

$$a|b \iff -a|b \iff a|-b \iff -a|-b.$$

Démonstration. Si $a|b$, alors il existe $c \in \mathbb{Z}$ tel que $b = ac$ donc $b = (-a)(-c)$, $-b = a(-c)$, $-b = (-a)c$ et donc $-a|b$, $a|-b$ et $-a|-b$. Les réciproques s'obtiennent de même. □

Et donc $\pm a$ divise $\pm|a|$.

Proposition. *Pour tout entier a, on a $a|a$, $a|-a$, $-a|a$ et $-a|-a$.*

Démonstration. Pour tout $a \in \mathbb{Z}$, $a = a \times 1$ donc $a|a$. Les autres découlent de la proposition précédente. □

Proposition. *Soit $(a,b) \in \mathbb{Z}^2$ avec b non nul. Si $a|b$, alors $|a| \leqslant |b|$.*

Démonstration.

□

Remarques :

- Il découle des deux dernières propositions que, pour tout $a \in \mathbb{Z}$, $|a|$ est le plus grand diviseur de a et aussi le plus petit multiple strictement positif de a.
- Si a est non nul, 1 est le plus petit diviseur positif de a.

Ainsi si on cherche tous les diviseurs de b, il suffit (mais cela est très fastidieux si b est grand) de tester tous les entiers naturels compris entre 2 et $|b|/2$. Ceux qui divisent b et leurs opposés, ainsi que ± 1 et $\pm b$ sont alors les diviseurs de b.

- Si b est non nul et si a est un diviseur de b qui n'est pas $-b$ ou b, alors il existe c tel que $b = ac$ et $|c| \geqslant 2$. Par conséquent $|a| \leqslant \dfrac{|b|}{2}$.
- On déduit des trois points précédents que les diviseurs positifs de $b \neq 0$ sont 1, $|b|$ et les autres appartiennent à $[\![2\,;\frac{|b|}{2}]\!]$.

Exemples : $\mathrm{Div}(12) = \{-12;-6;-3;-2;-1;1;2;3;6;12\}$, $\mathrm{Div}(11) = \{-11;-1;1;11\}$, $\mathrm{Div}(21) = \{-21;-7;-3;-1;1;3;7;21\}$, $\mathrm{Div}(1) = \{-1;1\}$, $\mathrm{Div}(0) = \mathbb{Z}$.

Proposition. *Soit $(a,b) \in \mathbb{Z}^2$. On a*

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

On dit que a et b sont des entiers associés.

Nous verrons des arithmétiques sur d'autres ensembles plus tard dans l'année où les diviseurs associés ne sont pas égaux ou opposés. Cela justifie l'intérêt de cette notion à ce stade.

Démonstration. Si $|a| = |b|$, alors on a déja vu que $a|b$ et $b|a$. Réciproquement, supposons que $a|b$ et $b|a$.

- Si $b = 0$, alors $a = 0$ et donc $|a| = |b|$.
- Supposons que $b \neq 0$. Comme $a|b$, on a $|a| \leqslant |b|$. Mais on a aussi $a \neq 0$ (puisque 0 ne divise b que lorsque $b = 0$) et, comme $b|a$, $|b| \leqslant |a|$. Ainsi $|a| = |b|$. □

On dira, dans le chapitre 16, que $|$ est une relation d'ordre partielle sur $\mathbb{N}$.

Proposition (transitivité). *Soit $(a,b,c) \in \mathbb{Z}^3$. Si $a|b$ et $b|c$, alors $a|c$.*

Démonstration. Supposons que $a|b$ et $b|c$. Il existe alors k et p des entiers tels que $b = ak$ et $c = bp$. On a donc $c = akp$ et, comme $kp \in \mathbb{Z}$, cela entraîne que $a|c$. □

En particulier, si $a \in \mathbb{Z}^*$ et $(b,c) \in \mathbb{Z}^2$ sont tels que $a|b$ et $a|c$ alors $a|b+c$ et même, pour tout $(u,v) \in \mathbb{Z}^2$, $a|bu+cv$.

Proposition (compatibilité avec les combinaisons linéaires). *Soit $n \in \mathbb{N}\backslash\{0;1\}$. Soient $a, b_1, \dots, b_n, k_1, \dots, k_n$ des entiers. Si, pour tout $i \in [\![1\,;n]\!]$, $a|b_i$, alors*

$$a|k_1a_1 + k_2a_2 + \cdots + k_na_n.$$

Démonstration. Supposons que, pour tout $i \in [\![1\,;n]\!]$, $a|b_i$. Pour tout $i \in [\![1\,;n]\!]$, il existe alors c_i tel que $b_i = ac_i$. On a donc

$$\sum_{k=1}^{n} k_ib_i = \sum_{k=1}^{n} k_iac_i = a \times \sum_{k=1}^{n} k_ic_i.$$

La somme à droite étant un entier, il s'ensuit que a divise $\sum_{k=1}^{n} k_ib_i$. □

Exemple : *Soit $n \in \mathbb{N}^*$. Si un entier a divise n et $n+1$, alors $a|(n+1)-n$ donc $a|1$ et donc $a = 1$ ou -1. Autrement dit, deux entiers consécutifs n'admettent que 1 et -1 pour diviseur commun.*

On dira dans le paragraphe II.2 que deux entiers consécutifs sont premiers entre eux

Proposition (compatibilité avec le produit). *Soient a, b, c et d des entiers. On a*

1. *Si $a|b$, alors $ac|bc$ et $a|bc$.*
2. *Si $a|b$ et $c|d$, alors $ac|bd$.*
3. *Si $a|b$ et $n \in \mathbb{N}^*$, alors $a^n|b^n$.*

Réciproquement, si $ac|bc$, alors $a|b$. Mais si $a|bc$, on ne peut pas conclure que $a|b$. Par exemple $10|8 \times 15$ mais $10 \nmid 8$ ni $10 \nmid 15$ (mais elle est vraie lorsque $a \wedge c = 1$, c'est le théorème de Gauss, cf. paragraphe II.2.b). La réciproque du point 2 est fausse (car $10 \times 12|8 \times 15$) et on verra que la réciproque du point 3 est vraie dans la paragraphe II.4.c.

Démonstration. Supposons que $a|b$. Il existe alors $k \in \mathbb{Z}$ tel que $b = ak$.

- On a donc $bc = akc = a(kc) = (ac)k$ et, comme $kc \in \mathbb{Z}$, $c \in \mathbb{Z}$, il vient que $ac|bc$ et $a|bc$.
- Si, de plus, $c|d$, alors il existe $\ell \in \mathbb{Z}$ tel que $d = c\ell$ et donc $bd = akc\ell = (ac)(k\ell)$. Comme $k\ell \in \mathbb{Z}$, on a bien $ac|bd$.
- Si $n \in \mathbb{N}^*$, $b^n = (ac)^n = a^nc^n$ et, comme $c^n \in \mathbb{Z}$, $a^n|b^n$. □

Exemple : *Puisque $2|8$ (car $8 = 2 \times 4$), $2^4|8^4$ c'est-à-dire $16|256$.*

Remarques :

- Si a et b sont deux entiers non nuls, alors :

  En effet

  .

- Si $a \in \mathbb{Z}^*$ et $(n,m) \in \mathbb{N}^2$, alors $a^n|a^m$ si et seulement si $n \leqslant m$. En effet si $n \leqslant m$, alors $m-n \in \mathbb{N}$ donc $a^{m-n} \in \mathbb{Z}$ et, comme $a^m = a^na^{m-n}$, on a bien $a^n|a^m$. Réciproquement, si $a^n|a^m$, alors $|a|^n = |a^n| \leqslant |a^m| = |a|^m$ et donc $n \leqslant m$.

Double erreur possible :
• penser que $a|b$ entraîne que $a\mathbb{Z} \subset b\mathbb{Z}$. C'est le contraire !
• penser que $a \leqslant b$ entraîne que $a\mathbb{Z} \subset b\mathbb{Z}$ ou même $b\mathbb{Z} \subset a\mathbb{Z}$. Par exemple aucun des ensembles $2\mathbb{Z}$ et $3\mathbb{Z}$ n'est inclus l'un dans l'autre. Attention avant d'utiliser les premières formules qui vous passent par la tête, il faut bien comprendre ce que tout cela signifie.

3) Le théorème de la division euclidienne

Théorème (division euclidienne). *Soit $(a,b) \in \mathbb{Z} \times \mathbb{Z}^*$. Il existe un unique couple $(q,r) \in \mathbb{Z}^2$ tel que $a = bq + r$ et $0 \leqslant r < |b|$. On dit que q est le quotient de la division euclidienne de a par b et r le reste.*

Exemple :

- *On a $49 = 11 \times 4 + 5$. Ainsi :*

- ⋆ *comme* $0 \leqslant 5 < 11$, *alors* 4 *et* 5 *sont respectivement le quotient et le reste de la division euclidienne de* 49 *par* 11.
- ⋆ *comme* $5 \geqslant 4$, 11 *et* 5 *ne sont pas respectivement le quotient et le reste de la division euclidienne de* 49 *par* 4. *Il faut encore retrancher* 4 *:* $49 = 12 \times 4 + 1$ *si bien que ce sont* 12 *et* 1 *qui sont respectivement le quotient et le reste de la division euclidienne de* 49 *par* 4.

- *On a* $-65 = (-9) \times 7 - 2$. *On pourrait penser que* -2 *est le reste de la division euclidienne de* -65 *par* -9 *mais, par définition/construction, il doit appartenir à* $[\![0\,;8]\!]$ *(puisque* $8 = |9| - 1$*). Il suffit de rajouter et enlever* 9 *:*

$$-65 = (-9) \times 7 - 9 + 9 - 2 = 8 \times (-9) + 7.$$

  Comme $0 \leqslant 7 < 9$, *il s'ensuit que* 8 *et* 7 *sont le quotient et le reste de la division euclidienne de* -65 *par* -9.
- *Reprenant le même exemple, on a aussi* $-65 = 9 \times (-8) + 7$ *donc* -8 *et* 7 *sont respectivement le quotient et le reste de la division euclidienne de* -65 *par* 9.
- *En exploitant de nouveau* $-65 = (-9) \times 7 - 2$, *on obtient*

$$65 = 9 \times 7 + 2 = (-9) \times (-7) + 2$$

  Comme $0 \leqslant 2 < 9$, *il vient que* 7 *et* 2 *sont respectivement le quotient et le reste de la division euclidienne de* 65 *par* 9 *quand* -7 *et* 2 *sont respectivement le quotient et le reste de la division euclidienne de* 65 *par* -9.

Remarques :

Le diviseur doit être non nul et le reste est forcément un entier naturel. En revanche a, b et q peuvent être négatifs.

- L'entier a est appelée le dividende et l'entier b le diviseur (même lorsque b ne divise pas a) de la division euclidienne par a.
- Lorsque a et b sont positifs, l'idée générale et que l'on retranche b un certain nombre de fois (q fois) à a suffisamment pour qu'il ne reste qu'un nombre strictement inférieur à b.
- Quelques cas particuliers simples :
  - ⋆ Si $a = b$, alors $a = b \times 1 + 0$, c'est-à-dire $(q, r) = (1, 0)$.
  - ⋆ Si $a = -b$, alors $a = b \times (-1) + 0$, c'est-à-dire $(q, r) = (-1, 0)$.
  - ⋆ Si $0 \leqslant a < |b|$, alors $a = b \times 0 + a$, c'est-à-dire $(q, r) = (0, a)$.
  - ⋆ Si b est positif alors

Dans le cas où $b \in \mathbb{N}^*$, une autre preuve classique (mais plus mystérieuse au premier abord) est la suivante : on introduit l'ensemble $E = (a + b\mathbb{Z}) \cap \mathbb{N}$. Il s'agit d'une partie non vide de $\mathbb{N}$ (puisqu'elle contient $a = a - b \times 0$ si $a \geqslant 0$ et $a - ba$ si $a < 0$) donc elle admet un plus petit élément r. Par définition de E, il existe $q \in \mathbb{Z}$ tel que $r = a + b(-q)$ et donc $a = bq + r$. On a forcément $r < b$ (car sinon $r \geqslant b$ donc $r - b = a - b(q+1) \in E$, ce qui contredit la minimalité de r puisque $0 \leqslant r - b < r$).

Démonstration. Commençons par montrer l'existence.

- On traite d'abord le cas où $a \geqslant 0$ et $b > 0$.

- Supposons que $b < 0$ et $a \geqslant 0$.

- Supposons que $a < 0$.

L'existence est donc prouvée dans tous les cas. Montrons l'unicité.

□

Dans le cas où le dividende est beaucoup plus gros que le diviseur, il est peu réaliste dans la pratique de retranche le diviseur un très grand nombre de fois à la main jusqu'à ce qu'on obtienne le reste. A la place, on retranche plusieurs fois des multiples du diviseur qui sont de plus en plus petit.

Exemple : *Si $a = 2024$ et $b = 13$, on commence par retirer 13×100 à 2024, ce qui donne 724. Puis, on retranche 13×50 à 724, ce qui donne 74. Ensuite, on retranche 13×5 à 74, ce qui donne 9. On a donc*

$$\begin{aligned} 2024 &= 13 \times 100 + 724 \\ &= 13 \times 100 + 13 \times 50 + 74 \\ &= 13 \times 100 + 13 \times 50 + 13 \times 5 + 9 \\ &= 13 \times 155 + 9. \end{aligned}$$

Morale de l'histoire : diviser, c'est soustraire !

On peut écrire cette succession de calculs sous la forme suivante, comme à l'école primaire :

$$\begin{array}{rr|l} & 2024 & 13 \\ - & 1300 & 155 \\ \hline & 724 & \\ - & 650 & \\ \hline & 74 & \\ - & 65 & \\ \hline & 9 & \end{array} \qquad \textit{ou encore} \qquad \begin{array}{rr|l} & 2024 & 13 \\ - & 13 & 155 \\ \hline & 72 & \\ - & 65 & \\ \hline & 74 & \\ - & 65 & \\ \hline & 9 & \end{array}$$

Le reste et le quotient de la division euclidienne de 2024 par 13 sont donc 155 et 9 respectivement.

On peut aussi poser la division euclidienne lorsque le dividende et le diviseur sont strictement négatif, ou seulement l'un des deux. Mais nous en avons moins l'habitude et on peut retrouver facilement le résultat à partir de la division euclidienne des valeurs absolues (cf. remarque dans la marge à gauche de la démonstration du théorème de la division euclidienne).

Exemple : *Si $a = -5107$ et $b = 29$, faisons plutôt la division euclidienne de 5107 par 29 :*

$$\begin{array}{rr|l} & 5107 & 29 \\ - & 2900 & 176 \\ \hline & 2207 & \\ - & 2030 & \\ \hline & 177 & \\ - & 174 & \\ \hline & 3 & \end{array}$$

On aurait pu la poser ainsi :

$$\begin{array}{rr|l} - & 5107 & 29 \\ + & 2900 & -177 \\ \hline - & 2207 & \\ + & 2030 & \\ \hline - & 177 & \\ + & 203 & \\ \hline & 26 & \end{array}$$

C'est-à-dire enlever $29 \times (-100)$ à -5107, ce qui donne -2207, puis enlever $29 \times (-70)$ à -2207, ce qui donne -177, puis enlever $29 \times (-7)$ à -177, ce qui donne 26.

Ainsi $5107 = 29 \times 176 + 3$ donc $-5107 = 29 \times (-176) - 3$. Il suffit d'ajouter/retirer 29 :

$$-5107 = 29 \times (-176) - 29 + 29 - 3 = 29 \times (-177) + 26.$$

Ainsi le quotient et le reste de la division euclidienne de -5107 par 29 sont -177 et 26 respectivement.

Au passage, on a aussi $5107 = (-29) \times (-176) + 3$ et $-5107 = (-29) \times 177 + 26$, les divisions euclidiennes de 5107 par -29 et de -5107 par -29.

Proposition. *Soit $(a, b) \in \mathbb{Z} \times \mathbb{Z}^*$. Alors $b|a$ si et seulement si le reste de la division euclidienne de a par b est nul.*

Démonstration. Notons q et r le quotient et le reste de la division euclidiennes de a par b. Si $r = 0$, alors $a = bq + r = bq$ donc $b|a$. Réciproquement, supposons que $b|a$ et notons $k = \dfrac{b}{a} \in \mathbb{Z}$. On a alors $a = bk + 0$ et, comme $0 \leqslant 0 < b$, par unicité du reste dans la division euclidienne de a par b, on a $r = 0$. □

Corollaire. *Un entier n est impair si et seulement si il existe $k \in \mathbb{Z}$ tel que $n = 2k + 1$.*

Ou encore si et seulement si il existe $k \in \mathbb{Z}$ tel que $n = 2k - 1$.

Démonstration. Un entier n est impair s'il n'est pas divisible par 2. La proposition suivante assure que c'est équivalent à dire que le reste r de la division euclidienne de n par 2 n'est pas nul. Mais puisque $0 \leqslant r < 2$, cela revient à dire que $r = 1$. □

Remarque : On en déduit de nombreuses propriétés (dont je vous laisse faire la preuve) classiques et intuitives sur la parité d'un entier :

- la somme de deux entiers est paire si et seulement si ils ont la même parité,
- le produit de deux entiers impairs est impair
- deux entiers successifs ont une parité contraire (et leur produit est donc pair),
- un entier et son carré ont la même parité,

Le fait que le produit de deux entiers dont l'un est pair est pair découle juste de la définition d'un entier pair (comme étant divisible par 2) et non de cette proposition.

Une application classique : l'écriture d'un entier dans une base donnée. Soient $b \geqslant 2$ et $n \in \mathbb{N}^*$.

- Notons q_0 et r_0 le quotient est le reste de la division euclidienne de n par b. On a alors $0 \leqslant r_0 \leqslant b - 1$ et $n = bq_0 + r_0$. Si $q_0 = 0$, on s'arrête là.
- Sinon notons q_1 et r_1 le quotient est le reste de la division euclidienne de q_0 par b. On a alors $0 \leqslant r_1 \leqslant b - 1$ et $q_0 = bq_1 + r_1$ donc $n = b^2q_1 + br_1 + r_0$. Si $q_1 = 0$, on s'arrête là.

- Sinon notons q_2 et r_2 le quotient est le reste de la division euclidienne de q_1 par b. On a alors $0 \leqslant r_2 \leqslant b-1$ et $q_1 = bq_2 + r_2$ donc $n = b^3q_2 + b^2r_2 + br_1 + r_0$. Si $q_2 = 0$, on s'arrête là.
- On continue ainsi jusqu'à ce qu'un quotient soit nul. Disons que cela arrive à l'issue de l'étape k : $q_{k-1} = 0$ et on a construit $(r_0, \dots, r_{k-1})$ tels que

$$n = b^{k-1}q_{k-2} + b^{k-2}r_{k-2} + \cdots + b^2r_2 + br_1 + r_0.$$

Comme $q_{k-2} = bq_{k-1} + r_{k-1} = r_{k-1}$, il vient que

$$n = b^{k-1}r_{k-1} + b^{k-2}r_{k-2} + \cdots + b^2r_2 + br_1 + r_0 = \sum_{i=0}^{k-1} r_i b^i.$$

et notons que $r_{k-1} = q_{k-2} \neq 0$ par définition de q_{k-1} comme étant le premier quotient nul. Cette écriture est unique (cf. exercice 11). On dit qu'il s'agit de l'écriture en base b de n et on la note $n = \overline{r_{k-1}r_{k-2}\dots r_2r_1r_0}^b$.

Par exemple, écrivons 466 *en base* 7*. On a*

Lorsque $b = 10$, on parle encore d'écriture décimale de n : k est le nombre de chiffres, r_0 est appelé chiffre des unité, r_1 chiffre des dizaines, r_2 chiffre des centaines, etc.

L'algorithme s'arrête puisque

$$q_0 > q_1 > q_2 > \dots \geqslant 0.$$

Il y a donc au plus n étapes puisque $n > q_0$.

On peut aussi montrer directement (par récurrence forte sur n) que, pour tout $n \in \mathbb{N}^*$, il existe un unique $k \in \mathbb{N}^*$ et un unique $(r_0, r_1, \dots, r_{k-1})$ dans $[\![0\,;b-1]\!]^k$ tels que $r_{k-1} \neq 0$ et

$$n = \sum_{i=0}^{k-1} r_i b^i.$$

II PGCD et PPCM

1) PGCD de deux entiers

a) PGCD de deux entiers naturels

Soient $a \in \mathbb{N}$ et $b \in \mathbb{N}^*$. Comme $b \neq 0$, tout diviseur d de b vérifie $d \leqslant b$ (cf. paragraphe précédent). Par conséquent l'ensemble $\{d \in \mathbb{N} \,|\, d \text{ divise } a \text{ et } d \text{ divise } b\}$ est majoré. Comme il est non vide (il contient 1), et qu'il s'agit d'une partie de $\mathbb{N}$, cet ensemble admet un plus grand élément : il existe donc un diviseur commun à a et b qui est le plus grand (pour l'ordre naturel $\leqslant$ dans $\mathbb{N}$) de tous leurs diviseurs communs. Le raisonnement est le même si $a \in \mathbb{N}^*$ et $b \in \mathbb{N}$. La définition suivante a donc un sens :

Définition (PGCD). *Soient a et b deux entiers naturels non tous nuls. On appelle PGCD (Plus Grand Commun Diviseur) de a et b, le plus grand diviseur commun de a et b. On le note $a \wedge b$. Autrement dit*

$$a \wedge b = \max\{d \in \mathbb{N} \,|\, d \text{ divise } a \text{ et } d \text{ divise } b\}.$$

Puisque tout entier divise 0, tout entier est un diviseur commun de 0 et 0. Il n'y a donc pas de plus grand diviseur commun de 0 et 0. Voilà pourquoi nous ne définissons pas $0 \wedge 0$.

Proposition. *Soient a et b deux entiers naturels non tous nuls. On a*

- $a \wedge b | a$ *et* $a \wedge b | b$.
- $a \wedge b = b \wedge a$,
- $a \wedge b \geqslant 1$.

Considérer les diviseurs positifs commun à a et b est donc suffisant puisque $a \wedge b \geqslant 1$.

Démonstration.

- Par définition le PGCD de a et b est un diviseur commun à a et b.
- Dans la définition de $a \wedge b$, a et b jouent le même rôle donc $a \wedge b = b \wedge a$.
- Puisque 1 est un diviseur commun de a et b, le plus grand d'entre eux est supérieur à 1. □

Nous allons voir des moyens beaucoup plus efficaces dans la suite.

Pour prouver que $d = a \wedge b$, il suffit donc de montrer que $d|a$, $d|b$ et que tout diviseur commun de a et b est inférieur à d. Typiquement, on fait la liste des diviseurs positifs communs à a et à b et c'est le plus grand.

Exemple : *Les diviseurs positifs de* 18 *sont* 1, 2, 3, 6, 9 *et* 18. *Les diviseurs positifs de* 12 *sont* 1, 2, 3, 4, 6 *et* 12. *Par conséquent les diviseurs positifs commun à* 18 *et* 12 *sont* 1, 2, 3 *et* 6 *si bien que* $18 \wedge 12 = 6$.

Proposition. *Si* $a \in \mathbb{N}^*$, $a \wedge 0 = a$.

Démonstration. Déjà a est un diviseur commun à 0 et a. Ensuite, si d est un diviseur de a, alors $d \leqslant a$ si bien que tout diviseur commun à 0 et à a est inférieur à a. Par conséquent $a \wedge 0 = a$. □

Par conséquent, si $a \in \mathbb{N}$, $a \wedge 1 = 1$.

Proposition. *Soient* $a \in \mathbb{N}^*$ *et* $b \in \mathbb{N}^*$. *On a* $a \wedge b \leqslant \max\{a; b\}$ *avec égalité si et seulement si* $a|b$ *ou* $b|a$. *Plus précisément,*

- $a \wedge b = a$ *si et seulement si* $a|b$,
- $a \wedge b = b$ *si et seulement si* $b|a$.

Démonstration. Notons $d = a \wedge b$. Puisque $d|a$, on a $d \leqslant a$. Puisque $d|b$, on a $d \leqslant b$. Ainsi $d \leqslant \max\{a; b\}$. Il y a égalité si et seulement si $d = a$ ou $d = b$.

- Si $a \wedge b = a$, alors $a|b$ (le PGCD de a et b divise b). Réciproquement, supposons que $a|b$. Alors a est un diviseur commun à a et à b. De plus, si d' est un diviseur de a et b, alors $d \leqslant a$ (tout diviseur de a est inférieur à a). Par conséquent $a \wedge b = a$.
- Même preuve en inversant les rôles de a et b. □

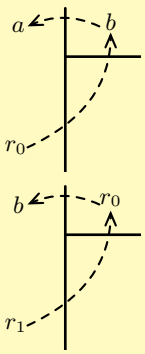
b) L'algorithme d'Euclide

L'algorithme d'Euclide repose sur la proposition suivante :

Proposition. *Soient* a *et* b *deux entiers naturels non nuls. Notons* r *le reste de la division euclidienne de* a *par* b. *Alors* $a \wedge b = b \wedge r$.

Démonstration.

□



Algorithme d'Euclide. Quitte à intervertir a et b, on peut supposer $a \geqslant b$.

- On note r_0 le reste de la division euclidienne de a par b.
- Si $r_0 = 0$, on s'arrête là. Sinon, on effectue la division euclidienne de b par r_0, et on appelle r_1 le reste.
- Si $r_1 = 0$, on s'arrête là. Sinon, on effectue la division euclidienne de r_0 par r_1, et on appelle r_2 le reste.
- Soit $i \geqslant 2$. Supposons $r_0, \ldots, r_i$ construits. Si $r_i = 0$, on s'arrête là, sinon on effectue la division euclidienne de r_{i-1} par r_i, et on note r_{i+1} le reste.
- On s'arrête dès qu'un reste est nul.

L'algorithme d'Euclide consiste en une succession de divisions euclidiennes, le diviseur prenant à chaque fois la place du dividende, et le reste celle du diviseur, et on s'arrête dès qu'un reste est nul.

Tout d'abord, l'algorithme termine. En effet, d'après le théorème de la division euclidienne, on a $b > r_0 > r_1 > r_2 > \ldots \geqslant 0$. Il y a donc au plus b restes possibles et donc l'algorithme s'arrête en au plus b étapes.

Notons r_n le dernier reste non nul (c'est-à-dire que $r_{n+1} = 0$). D'après la proposition précédente :

$$a \wedge b = b \wedge r_0 = r_0 \wedge r_1 = \cdots = r_{n-1} \wedge r_n = r_n \wedge r_{n+1} = r_n \wedge 0 = r_n.$$

On en déduit le théorème suivant :

Théorème. *$a \wedge b$ est le dernier reste non nul dans l'algorithme d'Euclide.*

Exemples :

- *Déterminons le PGCD de 2024 et 1683 avec l'algorithme d'Euclide :*

- *Déterminons le PGCD de 364 et 495 avec l'algorithme d'Euclide :*

- *Déterminons le PGCD de 2185 et 585 avec l'algorithme d'Euclide :*

$$\begin{array}{r|l} 2184 & 585 \\ \hline -\ 1755 & 3 \\ \hline 429 & \end{array} \quad \begin{array}{r|l} 585 & 429 \\ \hline -\ 429 & 1 \\ \hline 156 & \end{array} \quad \begin{array}{r|l} 429 & 156 \\ \hline -\ 312 & 2 \\ \hline 117 & \end{array} \quad \begin{array}{r|l} 156 & 117 \\ \hline -\ 117 & 1 \\ \hline 39 & \end{array} \quad \begin{array}{r|l} 117 & 39 \\ \hline -\ 117 & 3 \\ \hline 0 & \end{array}$$

Le dernier reste non nul est 39 si bien que $2184 \wedge 585 = 39$.

Remarque : Si deux entiers naturels non tous nuls sont implémentés en Python par les variables a et b, alors a//b et a%b renvoient respectivement le quotient et le reste de la division euclidienne de a par b. Ainsi la fonction en Python suivante prend en entrée deux entiers naturels non nuls et renvoie leur PGCD en utilisant l'algorithme d'Euclide :

```
def pgcd(a,b):
    while a%b!=0:
        a,b=b,a%b
    return b
```

c) Relations de Bezout

Pour faire simple, l'algorithme d'Euclide étendu est le même que l'algorithme d'Euclide classique (et donc il termine pour la même raison), mais il prend aussi en compte les quotients (pas seulement les restes).

Algorithme d'Euclide étendu. Soient a et b deux entiers naturels tels que $a \geqslant b$.

- On note q_0 et r_0 respectivement le quotient et le reste de la division euclidienne de a par b.
- Si $r_0 = 0$, on s'arrête là. Sinon, on effectue la division euclidienne de b par r_0, et on appelle q_1 le quotient et r_1 le reste.
- Si $r_1 = 0$, on s'arrête là. Sinon, on effectue la division euclidienne de r_0 par r_1, et on appelle q_2 le quotient et r_2 le reste.
- Soit $i \geqslant 2$. Supposons $r_0, \dots, r_i$ construits. Si $r_i = 0$, on s'arrête là, sinon on effectue la division euclidienne de r_{i-1} par r_i, et on note q_{i+1} le quotient et r_{i+1} le reste.
- On s'arrête encore dès qu'un reste est nul.

Cet algorithme étendu permet d'obtenir, non seulement $a \wedge b$, mais aussi des entiers **relatifs** (l'un des deux est forcément strictement négatif sinon $a \wedge b$ serait supérieur strictement à a ou à b) u et v tels que $au + bv = a \wedge b$.

Inutile de retenir les détails dans le cas général, il faut surtout savoir l'appliquer cette construction sur un exemple.

En effet, si r_n est le dernier reste non nul (et donc le PGCD de a et b) alors, pour tout $i \in [\![1\,;n-1]\!]$, $r_{i-1} = r_i \times q_{i+1} + r_{i+1}$ donc $r_{i+1} = r_{i-1} - r_i \times q_{i+1}$. Ainsi, pour tout $j \in [\![2\,;n]\!]$, $r_j = r_{j-2} - r_{j-1}q_j$.

En posant $r_{-1} = b$ et $r_{-2} = a$, une récurrence (que je vous laisse en exercice) permet de prouver que, pour tout $k \in [\![2\,;n+2]\!]$, il existe $(u_{n-k}, v_{n-k}) \in \mathbb{Z}^2$ tel que $a \wedge b = u_{n-k}r_{n-k} + v_{n-k}r_{n-k+1}$. Par ailleurs $u_{n-2} = 1$, $v_{n-2} = -q_n$ et, pour tout $k \in [\![2\,;n+2]\!]$, $u_{n-k+1} = v_{n-k}$ et $v_{n-k+1} = u_{n-k} - v_{n-k}q_{n-k+1}$.

On a $a \wedge b = r_n = r_{n-2} - r_{n-1} \times q_n$ et $r_{n-1} = r_{n-3} - r_{n-2}q_{n-1}$ si bien que

$$\begin{aligned} a \wedge b &= r_{n-2} - (r_{n-3} - r_{n-2}q_{n-1}) \times q_n \\ &= (1 + q_{n-1} \times q_n) \times r_{n-2} - q_n \times r_{n-3} \end{aligned}$$

L'idée est de remplacer à chaque fois le dernier reste disponible (r_{n-2} puis r_{n-3} etc.) à l'aide de des équations $r_j = r_{j-2} - r_{j-1}q_j$ et on s'arrête quand on ne peut plus aller plus loin, c'est-à-dire quand on a une équation du type $a \wedge b = c_0 \times r_0 + c_1 \times r_1$.

Il suffit ensuite de voir que $b = q_1r_0 + r_1$ si bien que $r_1 = b - q_1r_0$ donc

$$a \wedge b = c_0r_0 + c_1(b - q_1r_0) = (c_0 - c_1q_1)r_0 + c_1b$$

Enfin, $a = bq_0 + r_0$ donc $r_0 = a - bq_0$ si bien que

$$\begin{aligned} a \wedge b &= (c_0 - c_1q_1) \times (a - bq_0) + c_1b \\ &= (c_0 - c_1q_1) \times a + (c_1 - q_0c_0 + q_0c_1q_1) \times b \end{aligned}$$

Finalement, on a prouvé le théorème suivant :

Les coefficients u et v ne sont pas uniques. Par exemple $3 \wedge 5 = 1$ et

$$\begin{aligned} 3 \times (-3) + 5 \times 2 &= 1 \\ 3 \times 7 + 5 \times (-4) &= 1 \end{aligned}$$

On peut même montrer qu'il y en a une infinité. De plus la réciproque est fausse : par exemple

$$5 \times 1 + 3 \times (-1) = 2$$

alors que $5 \wedge 3 \neq 2$.

Théorème (Relations de Bézout – cas de deux entiers naturels). *Quels que soient les entiers naturels a et b non tous nuls, il existe $(u, v) \in \mathbb{Z}^2$ tel que $au + bv = a \wedge b$. Une telle relation est appelée une relation de Bezout de a et b.*

Exemples :

- *Reprenons l'exemple du paragraphe précédent avec le PGCD de 2024 et 1683, qui vaut 11. Pour cela nous avons réalisé des divisions euclidiennes successives. Les restes successifs, de l'avant dernier au premier, s'expriment alors ainsi : $11 = 319 - 22 \times 14$, $22 = 341 - 319$, $319 = 1683 - 341 \times 4$ et $341 = 2024 - 1683$. Par conséquent :*

- *Reprenons l'exemple du paragraphe précédent avec le PGCD de 364 et 495, qui vaut 1. Pour cela nous avons réalisé des divisions euclidiennes successives. Les restes successifs, de l'avant dernier au premier, s'expriment alors ainsi :* $1 = 15 - 14$, $14 = 29 - 15$, $15 = 102 - 29 \times 3$, $29 = 131 - 102$, $102 = 364 - 131 \times 2$, $131 = 495 - 364$. *Par conséquent :*

Proposition. *Soient a et b deux entiers naturels non nuls. Soit $m \in \mathbb{N}$. Il existe $(u, v) \in \mathbb{Z}^2$ tels que $au + bv = m$ si et seulement si $a \wedge b | m$.*

Démonstration. Si il existe $(u, v) \in \mathbb{Z}^2$ tels que $au+bv = m$ alors, puisque $a \wedge b$ divise a et b, il divise m. Réciproquement si $a \wedge b | m$ alors il existe $k \in \mathbb{N}$ tel que $k(a \wedge b) = m$. De plus il existe une relation de Bezout : $au' + bv' = a \wedge b$ avec $(u', v') \in \mathbb{N}^2$. En multipliant par k, on conclut en posant $u = ku'$ et $v = kv'$. □

Proposition. *Soient a et b deux entiers naturels non tous nuls. Soit $d \in \mathbb{N}^*$. On a*

$$d|a \quad \text{et} \quad d|b \qquad \Longleftrightarrow \qquad d|a \wedge b.$$

Démonstration. Si $d|a \wedge b$ alors, puisque $a \wedge b|a$ et $a \wedge b|b$, $d|a$ et $d[b$ (par transitivité). Réciproquement, supposons que $d|a$ et $d|b$. Le théorème précédent assure l'existence de u et v entiers tels que $au + bv = a \wedge b$ et donc $d|a \wedge b$. □

puisque d divise une combinaison linéaire entière de deux de ses multiples.

Remarque : Ainsi l'ensemble des diviseurs communs de a et b est l'ensemble des diviseurs de leur PGCD. Par conséquent, non seulement $a \wedge b$ est le plus grand des diviseurs de a et b au sens de l'ordre $\leqslant$ sur $\mathbb{N}$ mais c'est aussi le plus grand au sens de la relation d'ordre de divisibilité (cf. chapitre 16).

Proposition (factorisation dans un PGCD). *Soient a et b deux entiers naturels non tous nuls. Soit $k \in \mathbb{N}^*$. On a $(ka) \wedge (kb) = k \times (a \wedge b)$.*

Démonstration.

□

Exemple : *Puisque* $364 \wedge 495 = 1$*, on a*

$$1092 \wedge 1485 = (3 \times 364) \wedge (3 \times 495) = 3 \times (364 \wedge 495) = 3.$$

d) PGCD de deux entiers relatifs

Soit $a \in \mathbb{Z}$ et $b \in \mathbb{Z}^*$. Comme $b \neq 0$, tout diviseur d de b vérifie $|d| \leqslant |b|$ (cf. paragraphe précédent). Par conséquent l'ensemble $\{d \in \mathbb{Z} \,|\, d \text{ divise } a \text{ et } d \text{ divise } b\}$ est majoré. Comme il est non vide (il contient 1), et qu'il s'agit d'une partie de $\mathbb{Z}$, cet ensemble admet un plus grand élément : il existe donc un diviseur commun à a et b qui est le plus grand (pour l'ordre naturel $\leqslant$ dans $\mathbb{Z}$) de tous leurs diviseurs. Le raisonnement est le même si $a \in \mathbb{Z}^*$ et $b \in \mathbb{Z}$. La définition suivante a donc un sens :

Définition (PGCD). *Soient a et b deux entiers non tous nuls. On appelle PGCD (Plus Grand Commun Diviseur) de a et b, le plus grand diviseur commun de a et b. On le note $a \wedge b$. Autrement dit*

$$a \wedge b = \max\{d \in \mathbb{Z} \,|\, d \text{ divise } a \text{ et } d \text{ divise } b\}.$$

Exemple : *Les diviseurs de* -18 *sont* ± 1, ± 2, ± 3, ± 6, ± 9 *et* ± 18*. Les diviseurs de* -12 *sont* ± 1, ± 2, ± 3, ± 4, ± 6 *et* ± 12*. Par conséquent les diviseurs commun à* -18 *et* -12 *sont* ± 1, ± 2, ± 3 *et* ± 6 *si bien que* $(-18) \wedge (-12) = 6$.

Proposition. *Soient a et b des entiers non tous nuls. Alors*

$$a \wedge b = (-a) \wedge b = a \wedge (-b) = (-a) \wedge (-b) = |a| \wedge |b|.$$

Démonstration. Un entier et son opposé (et donc sa valeur absolue) ont les mêmes diviseurs. Par conséquent les couples (a, b), $(-a, b)$, $(a, -b)$, $(-a, -b)$ et $(|a|, |b|)$ ont les mêmes diviseurs communs et donc le même PGCD. □

On en déduit la proposition suivante qui reprend tous les résultats des derniers paragraphes et les étend dans le cas du PGCD de deux entiers relatifs non tous nuls :

Proposition. *Soient a et b deux entiers non tous nuls. On a :*

- $a \wedge b | a$ *et* $a \wedge b | b$,
- $a \wedge b = b \wedge a$,
- $a \wedge b \geqslant 1$,
- *Si* $a \neq 0$, $a \wedge 0 = |a|$.
- $a \wedge b \leqslant \max(|a|, |b|)$ *avec égalité si et seulement si* $a | b$ *ou* $b | a$*. Plus précisément* $a \wedge b = |a|$ *si et seulement si* $a | b$ *et* $a \wedge b = |b|$ *si et seulement si* $b | a$.
- *Si* $b \neq 0$ *et si* r *est le reste de la division euclidienne de* a *par* b*, alors* $a \wedge b = b \wedge r$.
- $a \wedge b$ *est le dernier reste non nul dans l'algorithme d'Euclide appliqué à* $|a|$ *et* $|b|$.
- *(relation de Bezout) Il existe* $(u, v) \in \mathbb{Z}^2$ *tel que* $au + bv = a \wedge b$.
- *Soit* $m \in \mathbb{Z}$*. Il existe* $(u, v) \in \mathbb{Z}^2$ *tel que* $au + bv = m$ *si et seulement si* $a \wedge b | m$*. Autrement dit* $a\mathbb{Z} + b\mathbb{Z} = (a \wedge b)\mathbb{Z}$.
- *(théorème de Bezout)* a *et* b *sont premiers entre eux si et seulement si il existe* $(u, v) \in \mathbb{Z}^2$ *tel que* $au + bv = 1$.
- *Soit* $d \in \mathbb{Z}^*$*. On a* $d | a$ *et* $d | b$ *si et seulement si* $d | a \wedge b$ *: tout diviseur commun à* a *et* b *divise leur PGCD.*
- *(factorisation) Si* $k \in \mathbb{Z}^*$, $(ka) \wedge (kb) = |k| \times (a \wedge b)$.

Dans la pratique, on applique la méthode vue dans le paragraphe précédent (avec l'algorithme d'Euclide étendu) pour déterminer u et v tels que

$$|a|u + |b|v = a \wedge b$$

puis on remplace u par $-u$ et/ou v par $-v$ pour obtenir $au + bv = a \wedge b$.

2) Entiers premiers entre eux

a) Définition et premières propriétés

Définition (entiers premiers entre eux). *Soient a et b deux entiers non tous nuls. On dit que a et b sont premiers entre eux si $a \wedge b = 1$.*

On dit aussi que a est premier avec b ou que b est premier avec a.

Remarque : Autrement dit, deux entiers sont premiers entre eux si leur seul diviseur positif commun est 1. Une façon de montrer que deux entiers a et b (non tous nuls) sont premiers entre eux est de se donner un diviseur positif d commun à a et b et de montrer que $d = 1$.

Exemples : *On a vu dans les paragraphes précédents que 3 et 5 sont premiers entre eux, que 364 et 495 sont premiers entre eux et que deux entiers consécutifs sont premiers entre eux.*

Rappel de la preuve : Si $n \in \mathbb{Z}$ et si d est un diviseur positif commun à n et $n+1$ avec $d|n+1-n$ donc $d = 1$.

Proposition. *Soient a, b et d des entiers non nuls. Si $a \wedge b = 1$ et $d|a$, alors $d \wedge b = 1$.*

Démonstration. Supposons que $a \wedge b = 1$ et $d|a$. Donnons-nous un diviseur positif commun k à d et à b. On a alors $k|a$ par transitivité donc $k|a \wedge b$ et donc $k = 1$. Ainsi $d \wedge b = 1$. □

Proposition. *Soient a, b des entiers non tous nuls. Notons $d = a \wedge b$. On a $\frac{a}{d} \wedge \frac{b}{d} = 1$.*

Démonstration. Déjà $d|a$ et $d|b$ donc $\frac{a}{d}$ et $\frac{b}{d}$ sont des entiers. Ensuite, on a $d = a \wedge b = \left(d \times \frac{a}{d}\right) \wedge \left(d \times \frac{a}{d}\right) = d\left(\frac{b}{d} \wedge \frac{b}{d}\right)$. En divisant par $d \neq 0$, il vient que $\frac{a}{d} \wedge \frac{b}{d} = 1$. □

Exemples :

- *On a vu plus haut que 364 et 495 sont premiers entre eux et on a trouvé la relation de Bezout : $1 = 364u + 495v$ avec $u = 34$ et $v = -25$.*
- *On a $187 \times 7 - 218 \times 6 = 1$ donc 187 et 218 sont premiers entre eux.*

b) Théorème de Bezout, théorème de Gauss et conséquences

Théorème (de Bezout). *Deux entiers a et b non tous nuls sont premiers entre eux si et seulement si il existe $(u, v) \in \mathbb{Z}^2$ tel que $au + bv = 1$.*

Démonstration. Si $a \wedge b = 1$, alors on a vu dans le paragraphe précédent qu'il existe $(u, v) \in \mathbb{Z}^2$ tel que $au + bv = a \wedge b = 1$. Réciproquement, supposons qu'il existe $(u, v) \in \mathbb{Z}^2$ tel que $au + bv = 1$. Si d est un diviseur positif commun à a et à b, alors $d|au + bv = 1$ donc $d = 1$. Ainsi $a \wedge b = 1$. □

C'est faux en général si $a \wedge b \neq 1$. Par exemple, $6|4 \times 3$ mais ne divise ni 4 ni 3.

Théorème (de Gauss). *Soient a, c et c des entiers non nuls. Si $a \wedge b = 1$ et $a|bc$, alors $a|c$.*

Démonstration.

□

Exemple : *Si on sait que c est un réel tel que $4|3c$, comme $4 \wedge 3 = 1$, $4|c$.*

Théorème (produit d'entiers). *Soient a, b et c des entiers non nuls. On a :*

- *Si $a \wedge b = 1$ et $a \wedge c = 1$, alors $a \wedge (bc) = 1$.*
- *Si $a|c$, $b|c$ et $a \wedge b = 1$, alors $ab|c$.*

C'est faux en général si $a \wedge b \neq 1$. Par exemple, $6|12$ et $4|12$ mais $24 \nmid 12$.

Démonstration.

□

Exemples :

- *On a $4 \wedge 5 = 1$ et $6 \wedge 5 = 1$ donc $24 \wedge 5 = 1$.*
- *On a $5|700$, $7|700$ et $5 \wedge 7 = 1$ donc $35|700$.*

Théorème (Forme irréductible d'un rationnel). *Soit $r \in \mathbb{Q}$. Il existe un unique couple $(a, b) \in \mathbb{Z} \times \mathbb{N}^*$ tels que $a \wedge b = 1$ et $r = \frac{a}{b}$. Cette écriture est appelée forme irréductible du rationnel r. De plus, si $r \neq 0$, alors toute écriture de r est de la forme $\frac{ac}{bc}$ avec $c \in \mathbb{Z}^*$.*

Démonstration.

□

Plus précisément, la racine carrée d'un entier positif n est un entier si n est un carré parfait et est irrationnelle sinon.

Exemple : *Montrons que, pour tout $n \in \mathbb{N}$, $\sqrt{n} \in \mathbb{N}$ ou $\sqrt{n} \notin \mathbb{Q}$.*

c) Équations diophantiennes du type $au + bv = c$

On se donne a, b, c des entiers et on cherche tous les couples (u, v) d'entiers tels que $au + bv = c$. On procède ainsi :

- Déjà s'il existe une solution (u, v), alors $a \wedge b | c$ (puisque le PGCD divise a et b donc $au + bv$ donc c). Supposons que ce soit le cas. On note alors $a' = \dfrac{a}{a \wedge b}$, $b' = \dfrac{b}{a \wedge b}$ et $c' = \dfrac{c}{a \wedge b}$. Cela revient donc à chercher les couples (u, v) d'entiers tels que $a'u + b'v = c'$.
- Puisque $a' \wedge b' = 1$, le théorème de Bezout assure qu'il existe $(u_0, v_0) \in \mathbb{Z}^2$ tel que $a'u_0 + b'v_0 = 1$. On trouve un tel couple grâce à l'algorithme d'Euclide. On a alors $a'u_0c' + b'v_0c' = c'$.
- Si $(x, y) \in \mathbb{Z}^2$ est solution, alors

$$a'x + b'y = c = a'u_0c' + b'v_0c'$$

  donc $a'(x - u_0c') = b'(v_0c' - y)$ et donc $a' | v_0c' - y$. Comme $a' \wedge b' = 1$, le théorème de Gauss assure que $a' | v_0c' - y$: il existe $k \in \mathbb{Z}$ tel que $v_0c' - y = ka'$. On en déduit que $a'(x - u_0c') = b'ka'$ donc $x - u_0c' = kb'$. Finalement $(x, y) = (u_0c' + kb', v_0c' - ka')$.
- Réciproquement, si il existe $k \in \mathbb{Z}$ tel que $(x, y) = (u_0c' + kb', v_0c' - ka')$, alors

$$ax + by = au_0c' + kab' + bv_0c' - ka'b = c(a'u_0 + b'v_0) + k(ab' - a'b) = c \times 1 + k \times 0 = c,$$

  puisque $a'b = b'a$, $ac' = c'a$ et $bc' = c'b$.

De façon alternative, on peut chercher u_0 et v_0 entiers tels que

$$au_0 + bv_0 = a \wedge b,$$

puis on multiplie par c' :

$$au_0c' + bv_0c' = c.$$

On trouve alors que

$$a(x - u_0c') = b(v_0c' - y)$$

et on divise enfin par $a \wedge b$

Exemple : *Déterminons tous les couples (u, v) d'entiers tels que $429u + 63v = 6$.*

3) PPCM de deux entiers

On adopte la même démarche que pour le PGCD : d'abord on le définit pour deux entiers naturels puis on généralise aux entiers relatifs.

a) PPCM de deux entiers naturels

Soient $a \in \mathbb{N}^*$ et $b \in \mathbb{N}^*$. L'ensemble $\{m \in \mathbb{N}^* \,|\, a \text{ divise } m \text{ et } b \text{ divise } m\}$ est non vide (il contient $ab \in \mathbb{N}^*$) et il s'agit d'une partie de $\mathbb{N}$, cet ensemble admet un plus petit élément : il existe donc un multiple strictement positif commun à a et b qui est le plus petit (pour l'ordre naturel $\leqslant$ dans $\mathbb{N}$) de tous leurs multiples communs. La définition suivante a donc un sens :

Puisque 0 est un multiple commun de tout couple d'entiers naturels, il faut absolument exiger que le PPCM soit strictement positif sinon celui-ci serait nul et la notion n'aurait pas grand intérêt. Aussi, si a ou b est nul, alors 0 est leur multiple commun et le PPCM n'est donc pas défini.

Définition (PPCM). *Soient a et b deux entiers naturels non nuls. On appelle PPCM (Plus Petit Commun Multiple) de a et b, le plus petit multiple strictement positif commun à a et b. On le note $a \vee b$. Autrement dit*

$$a \vee b = \min \{m \in \mathbb{N}^* \,|\, a \text{ divise } m \text{ et } b \text{ divise } m\}.$$

Proposition. *Soient a et b deux entiers naturels non nuls. On a*

- $a | a \vee b$ *et* $b | a \vee b$.
- $a \vee b = b \vee a$,
- $1 \leqslant a \vee b \leqslant ab$.

Démonstration.

- Par définition le PPCM de a et b est un multiple commun à a et b.
- Dans la définition de $a \vee b$, a et b jouent le même rôle donc $a \vee b = b \vee a$.
- Un PPCM appartient à $\mathbb{N}^*$ donc est supérieur à 1 et inférieur à tout multiple commun de a et b. Or ab en est un. □

Mieux : si on connaît déjà un multiple commun m, il suffira de regarder les multiples de a et de b qui sont inférieurs à m.

Si on n'arrive pas à trouver un petit multiple commun, on cherche alors tous les multiples inférieurs ou égaux à $12 \times 28 = 216$. Mais c'est vite fastidieux : Les multiples de 12 inférieurs à 216 sont : 12, 24, 36, 48, 60, 72, 84, 96, 108, 120, 132, 144, 156, 168, 180, 192, 204, 216. Les multiples de 18 inférieurs à 216 sont : 18, 36, 54, 72, 90, 108, 126, 144, 162, 180, 198, 216.

Pour prouver que $d = a \vee b$, il suffit donc de montrer que $a|m$, $b|m$ et que tout multiple strictement positif commun à a et b est supérieur à m. Typiquement, on peut faire la liste des multiples strictement positifs communs à a et à b qui sont inférieurs à ab (puisque ab est un multiple strictement positif commun à a et b donc le plus petit lui est inférieur) et c'est le plus petit. Nous allons voir des moyens beaucoup plus efficaces dans la suite.

Exemple : *Cherchons $12 \vee 18$. Déjà remarquons que $18 \times 2 = 36 = 12 \times 3$ si bien que 36 est un multiple commun à 12 et 18 et donc $12 \vee 18 \leqslant 36$. Les multiples strictement positifs de 12 qui sont inférieurs à 36 sont 12, 24 et 36. Les multiples strictement positifs de 36 qui sont inférieurs à 18 sont 18 et 36. Ainsi $12 \vee 18 = 36$.*

Remarque : Un intérêt majeur de la notion de PPCM (on l'a vu) et lorsqu'on peut additionner deux fractions : on commencer par les mettre au même dénominateur et le choix optimal est donc que le dénominateur commun soit le PPCM des dénominateurs (et non pas le produit des dominateurs : ça marche mais complique tous les calculs puisque les nombres eu jeu sont alors rapidement très gros).

Exemple : *Par exemple, puisque $12 \vee 18 = 36$, on a*

$$\frac{7}{12} + \frac{5}{18} = \frac{3 \times 7}{36} + \frac{2 \times 5}{18} = \frac{31}{36}.$$

C'est bien mieux que de faire :

$$\frac{7}{12}+\frac{5}{18}=\frac{18\times 7}{216}+\frac{12\times 5}{216}=\frac{186}{216}=\frac{31}{36}.$$

Par conséquent, si $a\in\mathbb{N}^*$, $a\vee 1=a$.

Proposition. *Soient $a\in\mathbb{N}^*$ et $b\in\mathbb{N}^*$. On a $a\vee b\geqslant\max\{a;b\}$ avec égalité si et seulement si $a|b$ ou $b|a$. Plus précisément,*

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

Démonstration. Notons $m=a\vee b$. Puisque $a|m$, on a $a\leqslant m$. Puisque $b|m$, on a $b\leqslant m$. Ainsi $\max\{a;b\}\leqslant m$. Il y a égalité si et seulement si $m=a$ ou $m=b$.

- Si $a\vee b=a$, alors $b|a$ (le PPCM de a et b est un multiple de a). Réciproquement, supposons que $b|a$. Alors a est un multiple commun à a et à b. De plus, si m' désigne un multiple strictement positif de a et b, alors $m'\geqslant a$ (tout multiple de a est supérieur à a). Par conséquent $a\vee b=a$.
- Même preuve en inversant les rôles de a et b. □

Proposition. *Soient a et b deux entiers naturels non nuls. Soit $m\in\mathbb{N}^*$. On a*

$$a|m \quad \textit{et} \quad b|m \qquad\Longleftrightarrow\qquad a\vee b|m.$$

Démonstration.

□

Remarque : Ainsi l'ensemble des multiples communs à a et b est l'ensemble des multiples de leur PPCM. Par conséquent, non seulement $a\vee b$ est le plus petit des multiples de a et b au sens de l'ordre $\leqslant$ sur $\mathbb{N}^*$ mais c'est aussi le plus petit au sens de la relation d'ordre de divisibilité (cf. chapitre 16).

On sait rapidement trouver le PCDG de deux entiers naturels non nuls a et b grâce à l'algorithme d'Euclide. On obtient alors $a\vee b$ en utilisant

$$a\vee b=\frac{ab}{a\wedge b}.$$

Proposition (lien entre PPCM et PGCD). *Soient a et b deux entiers naturels non nuls. On a $(a\wedge b)(a\vee b)=ab$.*

Démonstration.

□

Exemple : *On retrouve le fait que* $12 \vee 18 = \dfrac{12 \times 18}{12 \wedge 18} = \dfrac{12 \times 18}{6} = 36$.

Corollaire. *Si a et b sont deux entiers naturels non nuls qui sont premiers entre eux, alors $a \vee b = ab$.*

Et la réciproque est vraie d'ailleurs (mais peu utile en pratique) : si $a \vee b = ab$, alors $a \wedge b = 1$.

Proposition (factorisation dans un PPCM). *Soient a et b deux entiers naturels non nuls. Soit $k \in \mathbb{N}^*$. On a $(ka) \vee (kb) = k \times (a \vee b)$.*

Démonstration. On a $(ka) \wedge (kb) = k(a \wedge b)$ donc

$$(ka) \vee (kb) = \frac{(ka)(kb)}{(ka) \wedge (kb)} = \frac{k^2 ab}{k(a \wedge b)} = k \times \frac{ab}{a \wedge b} = k(a \wedge b).$$

□

Exemple : *On a* $12 \vee 18 = (2 \times 6) \vee (3 \times 6) = 6(2 \vee 3)$ *et, comme* $2 \wedge 3 = 1$, $2 \vee 3 = 6$ *donc* $12 \vee 8 = 6 \times 6 = 36$.

b) PPCM de deux entiers relatifs

Soit $a \in \mathbb{Z}^*$ et $b \in \mathbb{Z}^*$. L'ensemble $\{m \in \mathbb{N}^* \,|\, a \text{ divise } m \text{ et } b \text{ divise } m\}$ est non vide (il contient $|ab| \in \mathbb{N}^*$) et il s'agit d'une partie de $\mathbb{N}$, cet ensemble admet un plus petit élément : il existe donc un multiple strictement positif commun à a et b qui est le plus petit (pour l'ordre naturel $\leqslant$ dans $\mathbb{N}$) de tous leurs multiples communs. La définition suivante a donc un sens :

Définition (PPCM). *Soient a et b deux entiers non nuls. On appelle PPCM (Plus Petit Commun Multiple) de a et b, le plus petit multiple strictement positif commun à a et b. On le note $a \vee b$. Autrement dit*

$$a \vee b = \min \{m \in \mathbb{N}^* \,|\, a \text{ divise } m \text{ et } b \text{ divise } m\}.$$

Proposition. *Soient a et b des entiers non tous nuls. Alors*

$$a \vee b = (-a) \vee b = a \vee (-b) = (-a) \vee (-b) = |a| \vee |b|.$$

Démonstration. Un entier et son opposé (et donc sa valeur absolue) ont les mêmes multiples. Par conséquent les couples (a, b), $(-a, b)$, $(a, -b)$, $(-a, -b)$ et $(|a|, |b|)$ ont les mêmes multiples communs et donc le même PPCM. □

On en déduit la proposition suivante qui reprend tous les résultats des derniers paragraphes et les étend dans le cas du PPCM de deux entiers relatifs non nuls :

Proposition. *Soient a et b deux entiers non nuls. On a :*

- $a | a \vee b$ *et* $b | a \vee b$,
- $a \vee b = b \vee a$,
- $1 \leqslant a \vee b \leqslant |ab|$,
- $a \vee b \geqslant \max(|a|, |b|)$ *avec égalité si et seulement si* $a | b$ *ou* $b | a$. *Plus précisément* $a \vee b = |a|$ *si et seulement si* $b | a$ *et* $a \vee b = |b|$ *si et seulement si* $a | b$.
- *Soit* $m \in \mathbb{Z}$. *On a* $a | m$ *et* $b | m$ *si et seulement si* $a \vee b | m$ *: tout multiple commun à a et b est un multiple de leur PPCM.*
- $(a \wedge b)(a \vee b) = |ab|$.
- *(factorisation) Si* $k \in \mathbb{Z}^*$, $(ka) \vee (kb) = |k| \times (a \vee b)$.

On a donc

$$a\mathbb{Z} \cap b\mathbb{Z} = (a \vee b)\mathbb{Z}.$$

On a vu plus haut que

$$\mathcal{D}(a) \cap \mathcal{D}(b) = \mathcal{D}(a \wedge b).$$

4) Extension à plus de deux entiers

Si on se donne un nombre fini d'entiers non tous nuls, l'ensemble de leurs diviseurs communs est une partie de $\mathbb{Z}$ qui est non vide (car contient 1) et majorée (par les valeurs absolues de chacun d'entre eux) donc il admet un plus grand élément (pour l'ordre naturel $\leqslant$ dans $\mathbb{Z}$).

Définition (PGCD). *Soient $n \in \mathbb{N}\backslash\{0;1\}$. Soient $a_1, \dots, a_n$ des entiers non tous nuls. On appelle PGCD de ces entiers leur plus grand diviseur commun. On le note $a_1 \wedge a_1 \wedge \cdots \wedge a_n$.*

Exemple : *$4 \wedge 6 \wedge 8 = 2$ puisque ± 1 et ± 2 sont les seuls diviseurs commun de 4, 6 et 8.*

Proposition (associativité du PGCD). *Soient a, b et c des entiers non nuls. On a*

$$a \wedge b \wedge c = (a \wedge b) \wedge c = a \wedge (b \wedge c).$$

Démonstration. Notons $d = a \wedge b \wedge c$, $k = (a \wedge b) \wedge c$. Puisque d est un diviseur commun à a, b et c, alors c'est un diviseur commun à a et b donc à $a \wedge b$. Il s'agit donc d'un diviseur commun à $a \wedge b$ et à c si bien que $d|k$ et donc $d \leqslant k$.
D'autre part k divise $a \wedge b$ et c donc divise a, b et c. C'est donc un diviseur commun à a, b et c donc $k \leqslant d$. On conclut que $d = k$.
Le fait que $a \wedge b \wedge c = a \wedge (b \wedge c)$ se démontre de façon analogue. □

A ce stade, on ne sait pas encore que $a \wedge b \wedge c$ est aussi le plus grand diviseur pour la relation de divisibilité mais seulement que $k \leqslant d$, ce qui suffit pour conclure.

Exemple :

- *On a $30 \wedge 18 \wedge 12 = 30 \wedge (18 \wedge 12) = 30 \wedge 6 = 6$ puisque $6|30$.*
- *On a $21 \wedge 14 \wedge 6 = (21 \wedge 14) \wedge 6 = 7 \wedge 6 = 1$. On peut aussi le calculer ainsi : $21 \wedge 14 \wedge 6 = 21 \wedge (14 \wedge 6) = 21 \wedge 2 = 1$.*

Remarque : Par récurrence immédiate, cela se généralise à un nombre quelconque d'entiers : on peut calculer leur PGCD en faisant les associations que l'on veut et dans l'ordre que l'on veut (par commutativité). Les parenthèses sont inutiles (mais peuvent être les bienvenues pour se repérer dans les associations d'entiers successives).

Définition. *Soient $a_1, \dots, a_n$ des entiers non nuls. On dit que $a_1, \dots, a_n$ sont :*

- *premiers entre eux dans leur ensemble si $a_1 \wedge \cdots \wedge a_n = 1$.*
- *premiers entre eux deux à deux, si pour tout $(i,j) \in [\![1\,;n]\!]^2$ tel que $i \neq j$, $a_i \wedge a_j = 1$.*

Exemple : *On a vu plus haut que 21, 14 et 6 sont premiers dans leur ensemble. En revanche $21 \wedge 14 = 7$, $21 \wedge 6 = 3$ et $14 \wedge 6 = 2$: il ne sont pas premiers deux à deux.*

Proposition. *Si des entiers non nuls sont premiers entre eux deux à deux, alors ils sont premiers entre eux dans leur ensemble.*

On voit même qu'il suffit que seulement deux entiers de la famille soient premiers entre eux pour qu'ils soient premiers entre eux dans leur ensemble.

Démonstration. Soient $a_1, \dots, a_n$ des entiers non nuls qui sont premiers entre eux deux à deux. Soit d un diviseur commun à $a_1, \dots, a_n$. En particulier, c'est un diviseur commun à a_1 et a_2 donc un diviseur de $a_1 \wedge a_2 = 1$. Ainsi $d = 1$. On en déduit qu'ils sont premiers dans leur ensemble. □

On démontre par récurrence simple (que je vous laisse rédiger), que la plupart des résultats vus dans les paragraphes précédents se généralisent à plusieurs entiers. Listons les plus importants :

Proposition. *Soit $n \in \mathbb{N}\backslash\{0;1\}$. Soient $a_1, \dots, a_n$ des entiers non nuls.*

- *(relation de Bezout) Il existe $(u_1, \dots, u_n) \in \mathbb{Z}^n$ tels que*
$$a_1u_1 + a_2u_2 + \cdots + a_nu_n = a_1 \wedge a_2 \wedge \cdots \wedge a_n.$$
- *Soit $m \in \mathbb{Z}$. Il existe $(u_1, \dots, u_n) \in \mathbb{Z}^n$ tels que $a_1u_1 + a_2u_2 + \cdots + a_nu_n = m$ si et seulement si $a_1 \wedge a_2 \wedge \cdots \wedge a_n | m$. Autrement dit*
$$a_1\mathbb{Z} + a_2\mathbb{Z} + \cdots + a_n\mathbb{Z} = (a_1 \wedge a_2 \wedge \cdots \wedge a_n)\mathbb{Z}.$$
- *(théorème de Bezout) $a_1, \dots, a_n$ sont premiers **dans leur ensemble** si et seulement si il existe $(u_1, \dots, u_n) \in \mathbb{Z}^n$ tels que $a_1u_1 + a_2u_2 + \cdots + a_nu_n = 1$.*
- *Soit $d \in \mathbb{Z}^*$. On a $d | a_1 \wedge a_2 \wedge \cdots \wedge a_n$ si et seulement si, pour tout $i \in [\![1\,;n]\!]$, $d | a_i$.*
- *(factorisation) Si $k \in \mathbb{Z}^*$, $(ka_1) \wedge (ka_2) \wedge \cdots \wedge (ka_n) = |k| \times (a_1 \wedge a_2 \wedge \cdots \wedge a_n)$.*
- *Si $d = a_1 \wedge a_2 \wedge \cdots \wedge a_n$, alors $\frac{a_1}{d}, \frac{a_2}{d}, \dots, \frac{a_n}{d}$ sont premiers entre eux **dans leur ensemble**.*
- *Si $c \in \mathbb{Z}^*$ est tel que, pour tout $i \in [\![1\,;n]\!]$, $a_i \wedge c = 1$, alors $(a_1a_2 \dots a_n) \wedge c = 1$.*
- *Si $c \in \mathbb{Z}^*$ est tel que, pour tout $i \in [\![1\,;n]\!]$, $a_i | c$, et si $a_1, \dots, a_n$ sont premiers entre eux **deux à deux**, alors $(a_1a_2 \dots a_n) | c$.*

⚠ C'est faux si les a_i sont seulement premiers entre eux dans leur ensemble. Par exemple $6|12$, $3|12$, $2|12$ mais $6 \times 3 \times 2 = 36 \nmid 12$ alors que 6, 3 et 2 sont premiers dans leur ensemble.

Remarque : Pour déterminer une relation de Bezout pour trois entiers a, b et c, on commencer par en chercher une pour $a \wedge b$ et pour c (par exemple à l'aide de l'algorithme d'Euclide étendu) : il existe $(u, v) \in \mathbb{Z}^2$ tel que
$$(a \wedge b)u + cv = (a \wedge b) \wedge c = a \wedge b \wedge c.$$
Puis on en cherche une pour $a \wedge b$ et c (grâce à l'algorithme d'Euclide étendu par exemple) : il existe $(x, y) \in \mathbb{Z}^2$ tel que $a \wedge b = ax + by$ si bien que
$$a(xu) + b(yu) + cv = (a \wedge b)u + cv = (a \wedge b) \wedge c.$$

📎 Et on peut généraliser de même la méthode de résolution des équations diophantiennes du type $au + bv = c$ à des équations du type $au + bv + cw = d$ (cf. exercices).

Proposition. *Soient a et b des entiers non nuls. Soient k et ℓ des entiers naturels non nuls. On a $a \wedge b = 1$ si et seulement si $a^k \wedge b^\ell = 1$.*

Démonstration.

- Supposons que $a^k \wedge b^\ell = 1$. Soit d un diviseur de $a \wedge b$. Alors d divise a et b sont d divise a^k et b^ℓ et donc $a^k \wedge b^\ell$. Ainsi $d = 1$. Par conséquent $a \wedge b = 1$.
- Supposons que $a \wedge b = 1$. En appliquant l'avant dernier point de la dernière proposition à $n = k$, $c = b$ et $(a_1, \dots, a_k) = (a, \dots, a)$, on obtient $a^k \wedge b = 1$. En appliquant de nouveau l'avant dernier point de la dernière proposition à $n = \ell$, $c = a^k$ et $(a_1, \dots, a_k) = (b, \dots, b)$, on obtient $a^k \wedge b^\ell = 1$. □

Corollaire. *Soient a et b des entiers non nuls. Soient $k \in \mathbb{N}^*$. On a $a^k \wedge b^k = (a \wedge b)^k$.*

Démonstration. Notons $d = a \wedge b$. On a $\frac{a}{d} \wedge \frac{b}{d} = 1$ donc $\frac{a^k}{d^k} \wedge \frac{b^k}{d^k} = 1$ d'après la proposition précédente. En multipliant par d^k et en utilisant la factorisation du PGCD, on conclut que $a^k \wedge b^k = d^k$. □

📎 Encore une fois, il existe puisque l'ensemble de leurs multiples strictement positifs commun est une partie non vide de $\mathbb{N}^*$ (elle contient le produit des valeurs absolues de ces entiers).

Remarque : On peut aussi (mais ⚠ ce n'est pas au programme) définir le PPCM de plusieurs entiers non nuls, comme étant le plus petit de leurs multiples strictement positifs. On peut montrer qu'il est associatif, qu'il est aussi le plus petit multiple pour la relation de divisibilité et que la propriété de factorisation est vraie.

⚠ En revanche la formule $(a \wedge b)(a \vee b) = |ab|$ ne se généralise pas à plus de deux entiers.

Par exemple : $(2 \wedge 4 \wedge 5) = (2 \wedge 4) \wedge 5 = 2 \wedge 5 = 1$ *et* $(2 \vee 4 \vee 5) = (2 \vee 4) \vee 5 = 4 \vee 5 = 20$.
Mais $1 \times 20 \neq 2 \times 4 \times 5$.

III Nombres premiers

1) Nombres premiers et nombres composés

Tout entier naturel n est divisible par 1 et par lui-même. Un nombre premier est donc un entier naturel qui admet exactement deux diviseurs distincts.

Définition. *Un entier naturel n est dit premier s'il est supérieur ou égal à 2 et s'il n'admet que 1 et n comme diviseurs positifs. Un nombre qui n'est pas premier est dit composé.*

⚠ Par définition, 1 n'est pas un nombre premier.

Exemple : *2 et 3 sont premiers mais 4 ne l'est pas puisque divisible par 2.*

D'ailleurs puisque $a \geqslant 2$, $b \geqslant 2$ et $ab = n$, on a forcément $a \leqslant \frac{n}{2}$ ou $b \leqslant \frac{n}{2}$.

Proposition. *Un entier $n \in \mathbb{N}\backslash\{0;1\}$ est composé si et seulement si il existe $(a,b) \in [\![2\,;n-1]\!]^2$ tel que $n = ab$.*

Démonstration. Soit $n \in \mathbb{N}\backslash\{0;1\}$. Si n est composé, alors il n'est pas premier donc il admet un diviseur positif a qui n'est ni 1, ni n. Autrement dit $a \in [\![2\,;n-1]\!]$. Il s'ensuit que $b = \dfrac{n}{a} \in [\![2\,;n-1]\!]$ et $n = ab$. Réciproquement, si il existe $(a,b) \in [\![2\,;n-1]\!]^2$ tel que $n = ab$, alors n est divisible par a qui n'est ni 1, ni n et donc est composé. □

Exemples :

Autrement dit 2 est l'unique nombre premier qui est pair.

- *Les dix premiers nombres premiers sont 2, 3, 5, 7, 11, 13, 17, 19, 23 et 29.*
- *A part 2, tous les nombres pairs sont composés.*
- $9 = 3 \times 3$, $15 = 3 \times 5$, $21 = 3 \times 7$, $25 = 5 \times 5$, $27 = 3 \times 9$ *sont composés.*

2) Premières propriétés

Et dans le cas contraire, on a $p|n$ donc $p \wedge n = p$.

Proposition. *Soient p est un nombre premier et n un entier naturel. On a $p \nmid n$ si et seulement si $p \wedge n = 1$.*

Démonstration. Supposons que $p \nmid n$. Soit d un diviseur positif commun à p et à n. Comme $p \wedge n | p$ et que p est premier, on a $p \wedge n = 1$ ou $p \wedge n = p$. Comme $p \wedge n | n$ et que $p \nmid n$, on a forcément $p \wedge n = 1$. Réciproquement, si $p|n$ alors $p \wedge n = p \neq 1$. □

Corollaire. *Deux nombres premiers distincts sont premiers entre eux.*

En particulier, si a et b sont deux entiers naturels non nuls tels que $p|ab$, alors $p|a$ ou $p|b$. C'est une conséquence directe du théorème de Gauss.

Proposition (lemme d'Euclide). *Soit p un nombre premier. Soit $n \in \mathbb{N}^*$. Soient $a_1, \ldots, a_n$ des entiers naturels non nuls. On a $p|a_1 \ldots a_n$ si et seulement si il existe $i \in [\![1\,;n]\!]$ tel que $p|a_i$.*

Démonstration.

□

Théorème (existence de la décomposition en produit de facteurs premier). *Tout entier supérieur ou égal à 2 s'écrit comme le produit de nombres premiers.*

Il y a même unicité, cf. paragraphe II.4.a.

Ce théorème est équivalent au résultat montré dans le chapitre 2(pour illustrer le principe de récurrence forte) : tout entier supérieur ou égal à 2 admet un diviseur premier.

Démonstration. Pour tout $n \geqslant 2$, posons H_n : « n s'écrit comme le produit de nombres premiers ». Raisonnons par récurrence forte.

- Déjà 2 est premier donc H_2 est vraie.
- Soit $n \geqslant 2$. Supposons que H_k est vraie pour tout $k \in [\![2\,;n]\!]$.
  - ⋆ Si $n+1$ est premier, alors il s'écrit comme produit (à un terme) de nombres premiers.
  - ⋆ Supposons que $n+1$ n'est pas premier. Il est alors composé : il existe $(a,b) \in [\![2\,;n]\!]^2$ tel que $n+1=ab$. Comme H_a et H_b sont vraies par hypothèse de récurrence, a et b s'écrivent comme produit de facteurs premiers et donc $n+1=ab$ aussi.

  On en déduit que H_{n+1} est vraie.

Par récurrence forte, pour tout $n \geqslant 2$, H_n est vraie. □

3) A la recherche des nombres premiers

Proposition. *L'ensemble $\mathbb{P}$ des nombres premiers est infini.*

Démonstration.

□

Voyons des méthodes permettant de trouver des nombres premiers ou de vérifier qu'un entier naturel est premier ou non.

et même aucun entier compris entre 2 et $\lfloor n/2 \rfloor$.

- Une première méthode pour vérifier si un entier naturel n est premier est de vérifier qu'aucun entier compris entre 2 et $n/2$ de le divise (en les testant tous). En effet, si n est composé, on a vu qu'il s'écrit comme produit de deux entiers dont l'un est inférieur à $n/2$.

et même aucun entier compris entre 2 et $\lfloor \sqrt{n} \rfloor$. On peut même se contenter de ne tester que les nombres premiers inférieurs ou égaux à $\lfloor \sqrt{n} \rfloor$ (puisqu'un nombre composé est divisible par un nombre premier, par existence de la décomposition en produit de facteurs premiers).

- On peut même faire mieux en vérifiant qu'aucun entier compris entre 2 et $\sqrt{n}$ ne le divise (en les testant tous). En effet, si n est composé, il s'écrit comme produit de deux entiers a et b. En ayant supposé qu'aucun entier compris entre 2 et $\sqrt{n}$ ne divise n, on a $a > \sqrt{n}$ et $b > \sqrt{n}$ donc $n = ab > \sqrt{n}\sqrt{n} = n$, ce qui est absurde

  Par exemple 293 est premier puisque $\lfloor \sqrt{293} \rfloor = 17$ et que 2, 3, 5, 7, 11, 13 et 17 (et donc aucun réels de $[\![2\,;17]\!]$) ne divisent 293.

Mais, comme on l'a vu, s'arrêter à $\lfloor \sqrt{n} \rfloor$ suffit : tout nombre supérieur à $\sqrt{n}$ (et inférieur à n) est alors premier car sinon il admettrait un diviseur inférieur à $\sqrt{n}$ et serait barré.

- **Crible d'Eratosthène.** Il s'agit d'une méthode (mais peu efficace pour les grandes valeurs) pour donner tous les nombres premiers inférieurs ou égaux à un certain entier naturel n.
  - ⋆ On écrit tous les entiers de 2 à n.
  - ⋆ On entoure 2 qui est premier puis on barre tous les multiples de 2 sauf 2 (qui sont composés car divisibles par 2).
  - ⋆ On entoure 3 qui est premier puis on barre tous les multiples de 3 sauf 3 (qui sont composés car divisibles par 3).
  - ⋆ On continue : à chaque fois on entoure le premier nombre restant non barré (il est premier puisque divisible par aucun entier qui lui est strictement inférieur sinon il serait barré) et on barre tous ses multiples stricts.
  - ⋆ On s'arrête quand on arrête à n

  Voici le crible limité aux nombre 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~~

Mettre au point des tests de primalité est un enjeu important en mathématiques. Les méthodes ci-dessus fonctionnent mais ne sont pas très efficaces dans la pratique quand les valeurs deviennent grandes (rien que de tester si un nombre est divisible par 17 ou non n'est pas immédiat). Nous en verrons d'autres en exercices.

4) Décomposition en produit de facteurs premiers

a) Théorème de factorisation première

Lemme. *Soient p et q des nombres premiers. Soit $n \in \mathbb{N}^*$. On a $p|q^n$ si et seulement si $p = q$.*

Démonstration. Si $p = q$, alors il est immédiat que $p|q^n$. Réciproquement supposons que $p|q^n$. Alors, en appliquant le lemme d'Euclide (avec $a_1 = \cdots = a_n = q$), il vient que p divise q. Mais comme $p \neq 1$ et que q est premier, on obtient que $p = q$. □

0 et 1 n'admettent pas une telle décomposition.

Théorème (décomposition en produit de facteurs premiers). *Pour tout entier naturel n supérieur ou égal à 2, il existe $r \in \mathbb{N}^*$, $p_1, \dots, p_r$ des nombres premiers distincts et $\alpha_1, \dots, \alpha_r$ des entiers naturels non nuls tels que*

$$n = p_1^{\alpha_1} \times \cdots \times p_r^{\alpha_r} = \prod_{i=1}^{r} p_i^{\alpha_i}.$$

Cette écriture est unique à l'ordre près des termes et on l'appelle la décomposition de n en produit de facteurs premiers.

Elle est même unique tout court si on impose que l'on écrit les termes du plus petit nombre premier de la décomposition au plus grand.

Démonstration. Soit $n \geqslant 2$.

- **Existence.** On a montré dans le paragraphe III.2 que n s'écrit comme produit de nombres premiers. En regroupant les nombres premiers égaux dans la décomposition de n et en les écrivant avec une puissance, n s'écrit bien sous la forme $p_1^{\alpha_1} \times \cdots \times p_r^{\alpha_r}$.
- **Unicité.**

On peut donc voir les nombres premiers comme les briques élémentaires des entiers : à partir d'eux, on peut construire tous les entiers strictement supérieurs à 2 et ils ne peuvent pas être eux-mêmes décomposés en produit de deux termes non égaux à 1. Le mathématicien Paul Erdös disait qu'« un nombre premier est un nombre qui ne se casse pas en tombant par terre ».

□

Exemples :

- *Si p est un nombre premier, alors sa décomposition est simplement lui-même.*
- $120 = 2^3 \times 3 \times 5$, $2024 = 2^3 \times 11 \times 23$, $18375 = 3 \times 5^3 \times 7^2$.

b) Valuation p-adique

Définition. *Soient $n \in \mathbb{N}\backslash\{0;1\}$ et $p \in \mathbb{P}$. On appelle valuation p-adique de n, et on note $v_p(n)$, la puissance de p dans la décomposition de n en produit de facteurs premiers, avec la convention que $v_p(n) = 0$ lorsque $p \nmid n$. On pose $v_p(1) = 0$.*

Mais, comme on l'a vu, s'arrêter à $\lfloor\sqrt{n}\rfloor$ suffit : tout nombre supérieur à $\sqrt{n}$ (et inférieur à n) est alors premier car sinon il admettrait un diviseur inférieur à $\sqrt{n}$ et serait barré.

Exemples :

- $120 = 2^3 \times 3 \times 5$ *donc*
- $18375 = 3 \times 5^3 \times 7^2$ *donc*

Remarques :

- Si $p \in \mathbb{P}$ et $k \in \mathbb{N}$, $v_p(p^k) = k$.
- Si p et q sont des nombres premiers distincts, alors $v_p(q) = 0$.

Remarque : Une famille $(\alpha_p)_{p\in\mathbb{P}}$ d'éléments de $\mathbb{N}$ indexée par $\mathbb{P}$ est dite presque nulle lorsque tous ses termes sont nuls sauf un nombre fini d'entre eux. On pose

$$\prod_{p\in\mathbb{P}} p^{\alpha_p} = \prod_{\substack{p\in\mathbb{P}\\ \alpha_p\neq 0}} p^{\alpha_p}.$$

Cette définition est conforme à l'intuition puisque la suite $(p^{\alpha_p})_{p\in\mathbb{P}}$ ne contient qu'un nombre fini de termes différents de 1 (les termes valant 1 n'apportent aucune contribution au produit).

On vérifie aisément (je vous laisse le faire en exercice) que, si $(\alpha_p)_{p\in\mathbb{P}}$ désigne également une famille presque nulle d'éléments de $\mathbb{N}$ indexée par $\mathbb{P}$, alors

$$\prod_{p\in\mathbb{P}} p^{\alpha_p+\beta_p} = \prod_{p\in\mathbb{P}} p^{\alpha_p} \prod_{p\in\mathbb{P}} p^{\beta_p}.$$

Le théorème de décomposition en produit de facteurs premiers se réécrit ainsi :

Théorème (décomposition en produit de facteurs premiers). *Soit $n \in \mathbb{N}^*$. La famille $(v_p(n))_{p\in\mathbb{P}}$ est presque nulle et*

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

Si $(\alpha_p)_{p\in\mathbb{P}}$ est une famille presque nulle d'éléments de $\mathbb{N}$ indexée par $\mathbb{P}$ et si $n = \prod_{p\in\mathbb{P}} p^{\alpha_p}$ alors, pour tout $p \in \mathbb{P}$, $\alpha_p = v_p(n)$.

On a vu que 1 n'admettait pas de factorisation première. Cependant, avec cette écriture, on a

$$1 = \prod_{p\in\mathbb{P}} p^0 = \prod_{p\in\mathbb{P}} p^{v_p(1)},$$

puisqu'on a posé $v_p(1) = 0$ pour tout $p \in \mathbb{P}$.

Proposition. *Soient a et b deux entiers supérieurs ou égaux à 2. Pour tout $p \in \mathbb{P}$, $v_p(a \times b) = v_p(a) + v_p(b)$.*

Démonstration. On a

$$\prod_{p\in\mathbb{P}} p^{v_p(ab)} = ab = \prod_{p\in\mathbb{P}} p^{v_p(a)} \prod_{p\in\mathbb{P}} p^{v_p(b)} = \prod_{p\in\mathbb{P}} p^{v_p(a)+v_p(b)}.$$

Par unicité de la décomposition, on a donc $v_p(a \times b) = v_p(a) + v_p(b)$ pour tout $p \in \mathbb{P}$.□

Par récurrence immédiate, on obtient :

Proposition. *Soit $a \in \mathbb{N}^*$. Pour tous $k \in \mathbb{N}$ et $p \in \mathbb{P}$, $v_p(a^k) = k \times v_p(a)$.*

Exemple : $v_5(10000) = v_5(10^4) = 4 \times v_5(10) = 4$.

Il s'agit d'un critère de divisibilité puissant (cf. résultats ci-dessous et du paragraphe III.4.c pour plusieurs applications).

Proposition. *Soient a et b deux entiers naturels non nuls. On a $a|b$ si et seulement si, pour tout $p \in \mathbb{P}$, $v_p(a) \leqslant v_p(b)$.*

Démonstration.

- Supposons que $a|b$. Si $a = b$, alors le résultat est immédiat. Si $a \neq b$, alors il existe $c \geqslant 2$ tel que $b = ac$. Pour tout $p \in \mathbb{P}$, on a alors $v_p(b) = v_p(a) + v_p(c) \geqslant v_p(a)$.
- Supposons que pour tout $p \in \mathbb{P}$, $v_p(a) \leqslant v_p(b)$. Posons $c = \prod_{p\in\mathbb{P}} p^{v_p(b)-v_p(a)}$. On a alors $c \in \mathbb{N}^*$ et $b = ac$ si bien que $a|b$. □

Exemple : *On a* $18375 = 3 \times 5^3 \times 7^2$ *donc* $175 = 5^2 \times 7$ *divise* 18375.

En particulier $p|n$ si et seulement si $v_p(n) \geqslant 1$.

Corollaire. *Soient $n \in \mathbb{N}^*$ et $p \in \mathbb{P}$. On a $v_p(n) = \max\{k \in \mathbb{N} \mid p^k|n\}$. Autrement dit, pour tout $k \in \mathbb{N}$,*

$$p^k|n \iff k \leqslant v_p(n).$$

Proposition. *Soient a et b deux entiers naturels non nuls. On a*

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

Démonstration. Notons $d = \prod_{p\in\mathbb{P}} p^{\min(v_p(a),v_p(b))}$ et $m = \prod_{p\in\mathbb{P}} p^{\max(v_p(a),v_p(b))}$.

- Pour tout $p \in \mathbb{P}$, $v_p(d) = \min(v_p(a), v_p(b)) \leqslant v_p(a) \leqslant \max(v_p(a), v_p(b)) = v_p(m)$. Par conséquent $d|a$ et $a|m$. Par symétrie des rôles, $d|b$ et $b|m$. On en déduit que d est un diviseur commun à a et b et que m est un multiple commun à a et b.
- Soit d' un diviseur commun à a et b. Pour tout $p \in \mathbb{P}$, on a $v_p(d') \leqslant v_p(a)$ (puisque $d'|a$) et $v_p(d') \leqslant v_p(b)$ (puisque $d'|b$) donc $v_p(d') \leqslant \min(v_p(a), v_p(b)) = v_p(d)$. Par conséquent $d'|d$. On en déduit que d est divisible par tout diviseur commun à a et b si bien que donc $d = a \wedge b$.
- On montre de même que tout multiple commun à a et b est multiple de m si bien que $m = a \vee b$. □

Exemple : *On a* $1540 = 2^2 \times 5 \times 7 \times 11$ *et* $1176 = 2^3 \times 3 \times 7^2$ *donc* $1540 \wedge 1176 = 2^2 \times 7 = 28$ *et* $1540 \vee 1176 = 2^3 \times 3 \times 5 \times 7^2 \times 11 = 64680$.

c) Quelques applications

Proposition. *Deux entiers a et b supérieurs ou égaux à 2 sont premiers entre eux si et seulement si ils n'ont aucun terme en commun dans leur décomposition en produit de facteurs premiers.*

Démonstration. L'unité de la factorisation première et la proposition suivante entraînent que $a \wedge b = 1$ si et seulement si, pour tout $p \in \mathbb{P}$, $\min(v_p(a), v_p(b)) = 0$. Ceci est équivalent à dire que, pour tout $p \in \mathbb{P}$, $v_p(a) = 0$ ou $v_p(b) = 0$. Cela est encore équivalent au fait que tout nombre premier ne peut diviser a et b en même temps. □

Proposition. *Soient a et b deux entiers supérieurs ou égaux à 2. Les facteurs premiers de ab sont exactement les facteurs premiers de a et les facteurs premiers de b.*

Démonstration. Un nombre premier p est un facteur de ab si et seulement si $v_p(ab) \geqslant 1$ si et seulement si $v_p(a) + v_p(b) \geqslant 1$ si et seulement si $v_p(a) \geqslant 1$ ou $v_p(b) \geqslant 1$ si et seulement si p est un facteur premier de a ou de b. □

Ces derniers résultats permettent de redémontrer autrement (et même plus simplement) de nombreux résultats du cours vus précédemment : si a, b et c sont des entiers naturels non nuls,

- $\sqrt{a}$ est entier ou irrationnel.

  Pour montrer que $\sqrt{2}$ est irrationnel, on peur raisonner encore plus simplement : si il existe deux entiers naturels a et b non nuls tels que $\sqrt{2} = \frac{a}{b}$, alors $2b^2 = a^2$. Ainsi
  $$\begin{aligned} 2v_2(a) &= v_2(a^2) \\ &= v_2(2b^2) \\ &= v_2(2) + 2v_2(b) \\ &= 1 + 2v_2(b). \end{aligned}$$
  C'est absurde puisqu'un nombre ne peut être à la fois impair et pair.

- Si $d|a$ et $d|b$, alors $d|a \wedge b$.

  En effet, supposons que $d|a$ et $d|b$. Pour tout $p \in \mathbb{P}$, on a alors $v_p(d) \leqslant v_p(a)$ et $v_p(d) \leqslant v_p(b)$ donc
  $$v_p(d) \leqslant \min(v_p(a), v_p(b)) = v_p(a \wedge b).$$
  On en déduit que $d|a \wedge b$.

- Si $a \wedge b = 1$ et $a \wedge c = 1$, alors $a \wedge (bc) = 1$.

  En effet, si $a \wedge b = 1$ et $a \wedge c = 1$, alors a n'a pas de facteurs premiers en commun avec b, ni en commun avec c. Ainsi a n'a pas de facteurs premier en commun avec bc. Ainsi $a \wedge (bc) = 1$.

- Si $(k, \ell) \in (\mathbb{N}^*)^2$, alors on a $a \wedge b = 1$ si et seulement si $a^k \wedge b^\ell = 1$.

  En effet, si $(k, \ell) \in (\mathbb{N}^*)^2$, alors les facteurs premiers de a^k (respectivement b^ℓ sont exactement ceux de a (respectivement b). Par conséquent, $a \wedge b = 1$ si et seulement si a et b n'ont aucun facteur premier en commun si et seulement si a^k et b^ℓ n'ont aucun facteur premier en commun si et seulement si $a^k \wedge b^\ell = 1$.

- $(a \wedge b)(a \vee b) = ab$.

  En effet, pour tout $p \in \mathbb{P}$,
  $$\begin{aligned} v_p((a \wedge b)(a \vee b)) &= v_p(a \wedge b) + v_p(a \vee b) \\ &= \min(v_p(a), v_p(b)) + \max(v_p(a), v_p(b)) \\ &= v_p(a) + v_p(b) = v_p(ab) \end{aligned}$$

- (lemme d'Euclide) Si p est premier et $p|ab$, alors $p|a$ et $p|b$.

  En effet, supposons que p est premier et $p|ab$. On a donc

  $$1 = v_p(p) \leqslant v_p(ab) = v_p(a) + v_p(b)$$

  donc $v_p(a) \geqslant 1$ ou $v_p(b) \geqslant 1$ (une somme d'entiers naturels est non nulle si et seulement si l'un est non nul).

Et aussi de nombreux autres :

- Soit $n \geqslant 2$. Écrivons $n = p_1^{\alpha_1} \dots p_r^{\alpha_r}$ sa factorisation première. Soit $d \geqslant 2$ un diviseur de n. Pour tout $p \in \mathbb{P}$, on a alors $v_p(d) \leqslant v_p(n)$. Ainsi :
  - ⋆ pour tout $i \in [\![1\,;r]\!]$, $v_{p_i}(d) \leqslant v_{p_i}(n) = \alpha_i$.
  - ⋆ Si $p \in \mathbb{P}\backslash\{p_1, \dots, p_r\}$, $v_p(d) \leqslant v_p(n) = 0$ donc $v_p(d) = 0$.

  Par conséquent la factorisation première de d s'écrit sous la forme $d = p_1^{\beta_1} \dots p_r^{\beta_r}$ avec $\beta_i \leqslant \alpha_i$ pour tout $i \in [\![1\,;r]\!]$. Réciproquement il est immédiat que tout entier qui s'écrit sous cette forme divise n.

  Par exemple, $360 = 2^3 \times 3^2 \times 5$ *admet* $(3+1) \times (2+1) \times (1+1) = 24$ *diviseurs :*

  $1 = 2^0 \times 3^0 \times 5^0$, $6 = 2^1 \times 3^1 \times 5^0$, $36 = 2^2 \times 3^2 \times 5^0$,
  $5 = 2^0 \times 3^0 \times 5^1$, $30 = 2^1 \times 3^1 \times 5^1$, $180 = 2^2 \times 3^2 \times 5^1$,
  $3 = 2^0 \times 3^1 \times 5^0$, $18 = 2^1 \times 3^2 \times 5^0$, $8 = 2^3 \times 3^0 \times 5^0$,
  $15 = 2^0 \times 3^1 \times 5^1$, $90 = 2^1 \times 3^2 \times 5^1$, $40 = 2^3 \times 3^0 \times 5^1$,
  $9 = 2^0 \times 3^2 \times 5^0$, $4 = 2^2 \times 3^0 \times 5^0$, $24 = 2^3 \times 3^1 \times 5^0$,
  $45 = 2^0 \times 3^2 \times 5^1$, $20 = 2^2 \times 3^0 \times 5^1$, $120 = 2^3 \times 3^1 \times 5^1$,
  $2 = 2^1 \times 3^0 \times 5^0$, $12 = 2^2 \times 3^1 \times 5^0$, $72 = 2^3 \times 3^2 \times 5^0$,
  $10 = 2^1 \times 3^0 \times 5^1$, $60 = 2^2 \times 3^1 \times 5^1$, $360 = 2^3 \times 3^2 \times 5^1$.

En particulier, il y a exactement $\prod_{i=1}^{r}(\alpha_i + 1)$ diviseurs positifs de n d'après le principe multiplicatif (cf. chapitre 30).

- Soient a et b sont des entiers non nul Soit $k \in \mathbb{N}\backslash\{0;1\}$. Si $a^k|b^k|$, alors $a|b$.

La réciproque est vraie et on l'a montrée dans le paragraphe I.2.

- $\sqrt[3]{\frac{4}{5}} \in \mathbb{R}\backslash\mathbb{Q}$.

IV Congruences dans $\mathbb{Z}$

1) Rappels sur les congruences dans $\mathbb{R}$

On a vu dans le chapitre 5 la notion de congruence de réels :

Définition. *Soient $(a, b, m) \in \mathbb{R}^3$ avec $m \neq 0$. On dit que a est congru à b modulo m si il existe $k \in \mathbb{Z}$ tel que $a = b + km$. On note $a \equiv b\,[m]$.*

Proposition. *Soient $(a,b,c,d,m) \in \mathbb{R}^5$ tel que $m \neq 0$. On a :*

- ***Symétrie.*** *$a \equiv b\,[m]$ si et seulement si $b \equiv a\,[m]$.*
- ***Transitivité.*** *Si $a \equiv b\,[m]$ et $b \equiv c\,[m]$, alors $a \equiv b\,[m]$.*
- ***Somme dans une congruence.*** *$a \equiv b\,[m]$ si et seulement si $a + c \equiv b + c\,[m]$.*
- ***Somme de congruences.*** *Si $a \equiv b\,[m]$ et $c \equiv d\,[m]$, alors $a + c \equiv b + d\,[m]$.*
- ***Produit dans une congruence.*** *Si $a \equiv b\,[m]$, alors $ac \equiv bc\,[mc]$.*
- ***Division dans une congruence.*** *Si $c \neq 0$ et $a \equiv b\,[m]$, alors $\frac{a}{c} \equiv \frac{b}{c}\left[\frac{m}{c}\right]$.*

Ne pas oublier de multiplier par c dans la congruence.

Démonstration. Les propriétés de symétrie, de somme et de produit (et donc division) dans une congruences ont été montrés dans le chapitre 5. Les propriétés de transitivité et de somme de congruences sont laissées en exercice. □

2) Résultats propres aux entiers

Bien entendu la définition et les propriétés précédentes s'appliquent en se limitant à des entiers relatifs. Il y a alors de nombreuses autres propriétés :

Proposition (congruence et divisibilité). *Soit $(a,b,m) \in \mathbb{Z}^2$ avec $m \neq 0$.*

- *On a $a \equiv b\,[m]$ si et seulement si $m|b-a$.*
- *Si $m|b$, alors $b \equiv 0\,[m]$.*
- *Soit d un diviseur de m. Si $a \equiv b\,[m]$, alors $a \equiv b\,[d]$.*
- *Si $a \equiv b\,[m]$, alors $a \wedge m = b \wedge m$.*
- *Si r désigne le reste de la division euclidienne de a par m. Alors $a \equiv r\,[m]$.*
  On dit aussi que r est le reste de a modulo n.
- *Réciproquement, si $m > 0$, $r \in [\![0\,;m-1]\!]$ et $a \equiv r\,[m]$, alors r est le reste de la division euclidienne de a par m. En particulier $m|a$ si et seulement si $r = 0$.*

Ce quatrième point est l'idée fondamentale de l'algorithme d'Euclide

Si $a \equiv b\,[m]$ et que $b \neq 0$, on ne peut pas donc pas conclure que $m|b$. Plus généralement, on $m|a$ si et seulement si a est congru à un multiple de m modulo m.

Démonstration.

- On a $a \equiv b\,[m]$ si et seulement si il existe $k \in \mathbb{Z}$ tel que $a - b = km$ si et seulement si $m|a-b$.
- On applique le point précédent à $b = 0$.
- Si $a \equiv b\,[m]$, alors $m|a-b$. Comme $d|m$, il vient que $d|a-b$ et donc $a \equiv b\,[d]$.
- Supposons que $a \equiv b\,[m]$. Il existe alors $k \in \mathbb{Z}$ tel que $a = b + km$. Si d divise a et m, alors d divise b. Si d divise b et m, alors d divise a. Ainsi les couples (a,m) et (b,m) ont les mêmes diviseurs donc le même PGCD.
- On a $a = mq + r$ par définition. Comme $q \in \mathbb{Z}$, par définition, $a \equiv r\,[m]$.
- Supposons que $m > 0$, $r \in [\![0\,;m-1]\!]$ et $a \equiv r\,[m]$. Il existe $k \in \mathbb{Z}$ tel que $a - r = km$ donc $a = km + r$. Par unicité de la division euclidienne de a par m, r est bien le reste.

Proposition. *Soit $(a,b,m) \in \mathbb{Z}^2$ avec $m \neq 0$. Si $a \equiv b\,[m]$ et $|b-a| < m$, alors $a = b$.*

Si $m > 0$, alors $|b-a| < m$ lorsque, par exemple, a et b appartiennent à $[\![0\,;n-1]\!]$ tous les deux, ou encore à $[\![1\,;n]\!]$ tous les deux.

Démonstration. Supposons que $a \equiv b\,[m]$, $|b-a| < m$ et que $a \neq b$. On a alors $b - a \neq 0$ et $m|b-a$ donc $m \leqslant |b-a|$, ce qui est absurde. Ainsi $a = b$. □

Corollaire. *Soit $n \in \mathbb{N}^*$. Tout entier a est congru à un élément et un seul de $[\![0\,;m-1]\!]$ modulo m.*

En particulier deux entiers de $[\![0\,;m-1]\!]$ sont distincts ou non congrus modulo m.

Démonstration. L'élément recherché est le reste de la division euclidienne de a par m et il est bien unique. □

Proposition. *Soient $(a,b,c,d,m) \in \mathbb{Z}^5$ tel que $m \neq 0$. On a :*

- ***Produit dans une congruence d'entiers.*** *Si $a \equiv b\,[m]$, alors $ac \equiv bc\,[m]$.*
- ***Produit de congruences d'entiers.*** *Si $a \equiv b\,[m]$ et $c \equiv d\,[m]$, alors $ac \equiv bd\,[m]$.*
- ***Puissance dans une congruence d'entiers.*** *Si $a \equiv b\,[m]$ et si $k \in \mathbb{N}$, alors $a^k \equiv b^k\,[m]$.*

Contrairement au cas des réels, on n'est pas obligé de multiplier par c dans le crochet de la congruence. Attention, on perd alors la possibilité de rediviser par $c \neq 0$ (voir plus bas pour savoir comment diviser dans une congruence).

Démonstration.

- Supposons que $a \equiv b\,[m]$. Il existe alors $k \in \mathbb{Z}$ tel que $a = b + km$. On a alors $ac = bc + kmc = bc + (kc)m$. Comme $kc \in \mathbb{Z}$, on a bien $ac \equiv bc\,[m]$.
- Supposons que $a \equiv b\,[m]$ et $c \equiv d\,[m]$. Il existe alors k et ℓ des entiers tels que $a = b + km$ et $c = d + \ell m$. On a alors
$$ac = (b+km)(d+\ell m) = bd + (kd + b\ell + k\ell m)m$$
et, comme $kd + b\ell + k\ell m \in \mathbb{Z}$, on a bien $ac \equiv bd\,[m]$.
- S'obtient par récurrence sur k à l'aide du point précédent (je vous laisse la détailler en exercice). □

Exemples :

- *Cherchons le reste de la division euclidienne de 2024 par 13.*
- *Montrer que, $3|5^{2024} + 2^{2025}$.*
- *Justifier que l'équation $a^2 + 8b^5 = 3$, d'inconnues $(a,b) \in \mathbb{Z}^2$ n'admet pas de solutions.*
- *Montrons que, pour tout $n \in \mathbb{N}^*$ et $p \in \mathbb{P}$, alors $n^2 \equiv 1\,[p]$ si et seulement si $n \equiv 1\,[p]$ ou $n \equiv p-1\,[p]$.*

Le sens indirect est même vrai lorsque p n'est pas premier. Le sens direct est faux en général si p n'est pas premier. Par exemple $11^2 \equiv 1\,[15]$ (puisque $11^2 - 1 = 120 = 15 \times 8$) mais $11 \equiv 11\,[15]$.

C'est faux en général si c et m ne sont pas premiers entre eux. Par exemple $6 \equiv 4\,[2]$ mais $3 \not\equiv 2\,[2]$.

Proposition (division dans une congruence d'entiers). *Soit $(a,b,c,m) \in \mathbb{Z}^4$ avec $m \neq 0$ et $c \neq 0$. Si $ac \equiv bc\,[m]$ et si $c \wedge m = 1$, alors $a \equiv b\,[m]$.*

Démonstration. Supposons que $ac \equiv bc\,[m]$. On a alors $m|ac - bc$ c'est-à-dire $m|(a-b)c$. Comme $m \wedge c = 1$, le théorème de Gauss entraîne que $m|a-b$ et donc $a \equiv b\,[m]$. □

Exemple : *Si on sait que a est un entier tel que $2a \equiv 4\,[5]$ alors $a \equiv 2\,[5]$ puisque $2 \wedge 5 = 1$.*

3) Le petit théorème de Fermat

Commençons par deux lemmes :

C'est faux si $k = 0$ ou $k = n$ puisque le coefficient binomial vaut alors 1. C'est aussi faux en général si p n'est pas premier. Par exemple 4 ne divise pas $\binom{4}{2} = 6$.

Lemme. *Soit p un nombre premier. Pour tout $k \in [\![1\,;p-1]\!]$, p divise $\binom{p}{k}$.*

Démonstration.

□

Les identités remarquables (et plus généralement la formule du binôme de Newton) sont donc très simplifiées modulo p premier.

Lemme. *Soient a et b des entiers. Pour tout p premier, on a $(a+b)^p \equiv a^p + b^p\,[p]$.*

Démonstration.

□

Théorème (petit théorème de Fermat). *Soit p un nombre premier et soit a un entier. On a alors $a^p \equiv a\,[p]$. De plus, si $p \nmid a$, alors $a^{p-1} \equiv 1\,[p]$.*

Plan de la preuve : on montre que c'est vrai pour $a \in [\![0\,;p-1]\!]$ puis pour $a \in \mathbb{Z}$ en prenant le reste de la division euclidienne par p.

Démonstration.

- **Étape 1.**

- **Étape 2.**

- **Étape 3.**

□

Exemples :

- *Montrons que* $5^{12} \equiv 1\,[91]$.

- *Montrons que, pour tout* $n \in \mathbb{N}$, $n^5 - n$ *est divisible par* 30.

4) Quelques applications classiques

a) Critères de divisibilité

La plupart sont même connus des élèves dès l'école primaire...

Les résultats de ce paragraphe ne sont pas explicitement au programme mais sont très classiques et utiles en pratique.

k est le nombre de chiffres, a_0 est appelé chiffre des unité, a_1 chiffre des dizaines, a_2 chiffre des centaines, etc.

Soit $n \in \mathbb{N}^*$. On a vu dans le paragraphe I.3 que n peut s'écrire de façon unique sous la forme

$$n = \sum_{i=0}^{k-1} a_i 10^i.$$

Il s'agit de l'écriture décimale de 10, son écriture avec laquelle nous sommes habitués depuis longtemps. On peut la note $\overline{a_{k-1}a_{k-2}\dots a_1a_0}^{10}$.

Proposition (critères de divisibilité par 2, 5 ou 10).

- n *est divisible par* 2 *si et seulement si* $a_0 \in \{0;2;4;6;8\}$.
- n *est divisible par* 5 *si et seulement si* $a_0 \in \{0;5\}$.
- n *est divisible par* 10 *si et seulement si* $a_0 = 0$.

Démonstration.
- Puisque $10^i \equiv 0\,[2]$ pour tout $i \in \mathbb{N}^*$, on a $n \equiv a_0\,[2]$ et donc n est divisible par 2 si et seulement si a_0 est un entier naturel de $[\![0\,;9]\!]$ divisible par 2. C'est le cas si et seulement si $a_0 \in \{0;2;4;6;8\}$.
- Puisque $10^i \equiv 0\,[5]$ pour tout $i \in \mathbb{N}^*$, on a $n \equiv a_0\,[5]$ et donc n est divisible par 5 si et seulement si a_0 est un entier naturel de $[\![0\,;9]\!]$ divisible par 5. C'est le cas si et seulement si $a_0 \in \{0;5\}$.
- Puisque $10^i \equiv 0\,[10]$ pour tout $i \in \mathbb{N}^*$, on a $n \equiv a_0\,[10]$ et donc n est divisible par 10 si et seulement si a_0 est un entier naturel de $[\![0\,;9]\!]$ divisible par 10. C'est le cas si et seulement si $a_0 = 10$. □

Proposition (congruences modulo 3, 4, 9 ou 11).
- *n est congru à la somme de ses chiffres modulo 3.*
- *n est congru au nombre formé par ses deux derniers chiffres (c'est-à-dire $n \equiv \overline{a_1a_0}^{10}$) modulo 4.*
- *n est congru à la somme de ses chiffres modulo 9.*
- *n est congru à $\sum_{i=0}^{k-1}(-1)^i a_i$ modulo 11.*

Cette somme est appelée somme alternée de ses chiffres.

Démonstration.
- On a $10 \equiv 1\,[3]$ donc, pour tout $i \in \mathbb{N}^*$, $10^i \equiv 1\,[3]$. Ainsi
$$n = \sum_{i=0}^{k-1} a_i 10^i \equiv \sum_{i=0}^{k-1} a_i\,[3]\,.$$

Dans le même genre (mais c'est moins usuel), puisque $8|1000$, n est congru à $\overline{a_2a_1a_0}^{10}$ modulo 8. Ainsi n est divisible par 8 si et seulement si $\overline{a_2a_1a_0}^{10}$ l'est. Pour vérifier cela, on montre que l'on est divisible par 2, puis par 2 puis par 2 (ou pas), ce qui est assez facile pour un nombre à trois chiffres).

- On a $4|100$ donc $10^i \equiv 0\,[4]$ pour tout $i \geqslant 2$. Il s'ensuit que
$$n = \sum_{i=0}^{k-1} a_i 10^i \equiv \sum_{i=0}^{1} a_i 10^i + 0\,[4]$$
donc $n \equiv a_0 + 10a_1\,[4]$. On conclut en remarquant que $a_0 + 10a_1$ est le nombre formé par les deux derniers chiffres de n.
- On a $10 \equiv 1\,[9]$ donc, pour tout $i \in \mathbb{N}^*$, $10^i \equiv 1\,[9]$. Ainsi
$$n = \sum_{i=0}^{k-1} a_i 10^i \equiv \sum_{i=0}^{k-1} a_i\,[9]\,.$$
- On a $10 \equiv -1\,[11]$ donc, pour tout $i \in \mathbb{N}^*$, $10^i \equiv (-1)^i\,[11]$. Ainsi
$$n = \sum_{i=0}^{k-1} a_i 10^i \equiv \sum_{i=0}^{k-1} a_i(-1)^i\,[11]\,.$$
□

Exemples : *Notons $N = 2380579963$.*
- $N \equiv 63\,[4]$ *donc* $N \equiv 3\,[4]$.
- $N \equiv 2+3+8+0+5+7+9+9+6+3\,[11]$ *c'est-à-dire* $N \equiv 52\,[9]$. *Mais* $52 \equiv 5+2\,[9]$ *donc* $N \equiv 7\,[9]$.
- $N \equiv 2-3+8-0+5-7+9-9+6-3\,[11]$ *c'est-à-dire* $N \equiv 8\,[11]$.

On en déduit les critères suivants :

Proposition (critère de divisibilité modulo 3, 4, 9 ou 11).

- *n est divisible par 3 si et seulement si la somme de ses chiffres est divisible par 3.*
- *n est divisible par 4 si et seulement si le nombre formé par ses deux derniers chiffres est divisible par 4.*
- *n est divisible par 9 si et seulement si la somme de ses chiffres est divisible par 9.*
- *n est divisible par 11 si et seulement si la somme alternée de ses chiffres est divisible par 11.*

Rappelons que, si a et b sont des entiers naturels non nuls premiers entre eux, alors $ab|n$ si et seulement si $a|n$ et $b|n$. Ainsi, en particulier :
• n est divisible par $6 = 2\times3$ si et seulement si n est pair et la somme de ses chiffres est divisible par 3.
• n est divisible par $12 = 4 \times 3$ si et seulement si la somme de ses chiffres est divisible par 3 et le nombre formé par ses deux derniers chiffres par 4.

Exemples :

- 267 *est divisible par* 3 *puisque* $2+6+7=15$ *l'est.*
- 17432 *est divisible par* 4 *puisque* 32 *l'est.*
- 245001 *n'est pas divisible par* 9 *puisque* $2+4+5+0+1=12$ *ne l'est pas*
- 2519 *est divisible par* 11 *puisque* $2-5+1-9=-11$ *l'est.*

Remarque : Il existe des critères de divisibilité par 7, 13, etc. (cf. wikipedia par exemple) mais c'est moins connu et moins aisé à mettre en œuvre.

b) Congruence d'une puissance

Soient $a \in \mathbb{N}^*$, $n \in \mathbb{N}^*$ et $m \in \mathbb{N}^*$. On cherche le reste de la division euclidienne de a^n par m, c'est-à-dire $b \in [\![0\,;m-1]\!]$ tel que $a^n \equiv b\,[m]$.

La méthode est toujours la même :

- On commence par calculer le reste modulo n de a, puis a^2, puis a^3 jusqu'à ce que le reste d'une certaine puissance soit le même que celui d'une puissance antérieure. Plus précisément, on cherche k et ℓ des entiers tels que $1 \leqslant k < \ell$ et $a^\ell \equiv a^k\,[m]$.
- Pour tout $n \geqslant k$, on a alors

$$\begin{aligned} a^{n+(\ell-k)} &\equiv a^\ell \times a^{n-k}\,[m] \\ &\equiv a^k \times a^{n-k}\,[m] \\ &\equiv a^n\,[m]\,. \end{aligned}$$

  Ainsi, la suite $(a^n)_{p\geqslant k}$ est $(\ell-k)$-périodique (cf. chapitre 14) modulo m.
- Pour calculer a^n modulo m, il suffit alors de trouver le reste de n modulo $\ell-k$.

Il est toujours possible de trouver k et ℓ. C'est une application du principe des tiroirs : si on a un nombre fini N de tiroirs et un nombre supérieur strictement à N (voire une infinité) de paires de chaussettes, alors il existe au moins un tiroir qui contient au moins deux paires de chaussettes. Ici il existe une infinité de puissances a^k (les chaussettes) pour $k \in \mathbb{N}$ et un nombre fini de congruences (les tiroirs) modulo m qui appartiennent à $[\![0\,;m-1]\!]$.

Exemples :

- *Montrons que* $7|4^{1789}+6$.

- *Déterminons le chiffre des unités de* $N = 7^{7^{7^7}}$.

Cela découle d'un récurrence immédiate ou en remarquant que

$$4^{3k} \equiv (4^3)^k \equiv 1\,[7]\,,$$
$$4^{3k+1} \equiv 4(4^3)^k \equiv 4\,[7]\,,$$
$$4^{3k+2} \equiv 7^2(4^3)^k \equiv 2\,[7]\,.$$

Cela découle d'un récurrence immédiate ou en remarquant que

$$7^{4k+1} \equiv 7(7^4)^k \equiv 7\,[10]\,,$$
$$7^{4k+2} \equiv 7^2(7^4)^k \equiv 9\,[10]\,,$$
$$7^{4k+3} \equiv 7^3(7^4)^k \equiv 3\,[10]\,,$$
$$7^{4k} \equiv (7^4)^k \equiv 1\,[10]\,.$$

c) Utilisation des inverses modulo n

Cette notion sera revue et étendue en deuxième année.

Définition. *Soient $n \in \mathbb{N}^*$ et $a \in \mathbb{Z}$. On dit que a admet un inverse modulo n si il existe $b \in \mathbb{Z}$ tel que $ab \equiv 1\,[n]$. On dit alors que b est **un** inverse de a modulo n.*

Remarques :

- Par symétrie des rôles, si b est un inverse de a modulo m, alors a est un inverse de b modulo m.
- Bien sûr 0 n'admet pas d'inverse modulo m puisque $0b \equiv 0\,[m]$ pour tout $b \in \mathbb{Z}$.
- Un entier peut ne pas admettre d'inverse modulo m.

  Par exemple, pour tout $b \in \mathbb{Z}$, $2b$ est congru à 0 ou à 2 modulo 4 donc 2 n'admet pas d'inverse modulo 4.
- On parle bien d'**un** inverse modulo n et non de l'inverse. En effet il en existe une infinité : si b est un inverse de a modulo n, alors $ab \equiv 1\,[m]$ donc, pour tout $k \in \mathbb{Z}$, $b + km$ est un inverse de a modulo m puisque $a(b + km) = ab + kam \equiv 1 + 0\,[m]$.
- Si on connaît un inverse modulo b de a, le reste r de la division euclidienne de b par m est encore un inverse de a modulo m. En effet $r \equiv b\,[m]$ donc $ar \equiv ab\,[m]$ donc $ar \equiv 1\,[m]$.

Il est souvent plus simple de remplacer a par son reste r_a modulo m pour déterminer une relation de Bezout : comme

$$r_a \wedge m = a \wedge m = 1,$$

il existe $\ell \in \mathbb{Z}$ tel que $r_a u + mv = 1$ si bien que $r_a u \equiv 1\,[m]$ et donc $au \equiv 1\,[m]$.

- Méthode pour trouver un inverse modulo m : Supposons que a admette un inverse b modulo n. Il existe alors $k \in \mathbb{Z}$ tel que $ab = 1 + kn$ donc $ab - kn = 1$ et donc le théorème de Bezout entraîne que $a \wedge n = 1$. Réciproquement, supposons que $a \wedge n = 1$. Le théorème de Bezout entraîne qu'il existe $(u, v) \in \mathbb{Z}^2$ tel que $au + nv = 1$. Ainsi $au \equiv 1\,[n]$ et donc u est un inverse de a modulo n.

  Par exemple, cherchons un inverse de 7 modulo 11.

Au passage, on a montré :

Proposition. *Soit $n \in \mathbb{N}^*$. Un entier a admet un inverse modulo n si et seulement si $a \wedge n = 1$.*

Corollaire. *Si p est premier, alors tout entier non multiple de p admet un inverse modulo p.*

Remarques :

- Si a admet un inverse modulo n, alors il est unique modulo m. En effet, s'il admet b et c pour inverse alors $ab \equiv ac\,[n]$. On peut diviser par a puisque $a \wedge n = 1$ (c'est la condition d'existence d'un inverse) et on obtient $b \equiv c\,[n]$. Lorsque l'on connait un inverse, on prend souvent le reste modulo n qui est alors le plus petit inverse de a qui est strictement positif.
- Soit $c \in \mathbb{Z}$. L'existence d'un inverse modulo n permet de résoudre des équations du type $ax = c\,[n]$, d'inconnue $x \in \mathbb{Z}$, lorsque $a \wedge n = 1$. En effet :
  - ⋆ Comme $a \wedge n = 1$, il admet un inverse b modulo n. On a alors $bax \equiv bc\,[n]$ et donc $x \equiv bc\,[n]$.
  - ⋆ Réciproquement, si $x \equiv bc\,[n]$, alors $ax \equiv abc\,[n]$ et donc $ax \equiv c\,[n]$.

En fait il s'agit du même problème que la résolution d'équation diophantiennes simples du paragraphe II.2.c puisque $ax \equiv c\,[n]$ si et seulement si il existe $k \in \mathbb{Z}$ tel que $ax + nk = c$. A ceci près que l'on ne demande pas de trouver k mais seulement x.

Exemples :

- *On cherche à résoudre* $7x \equiv 6\,[11]$ *d'inconnue* $x \in \mathbb{Z}$.
- *On cherche à résoudre* $6x \equiv 4\,[9]$ *d'inconnue* $x \in \mathbb{Z}$.
- *On cherche à résoudre* $8x \equiv 6\,[30]$ *d'inconnue* $x \in \mathbb{Z}$.