

Arithmétique

Dans ce chapitre, le terme « entier » désignera (sauf indication contraire) un entier relatif, c'est-à-dire un élément de \mathbb{Z} .

I Divisibilité

I.1 Diviseurs et multiples

I.1.a Définition

Définition. Soit $(a, b) \in \mathbb{Z}^2$. On dit que a divise b s'il existe $k \in \mathbb{Z}$ tel que $b = k \times a$. On dit alors que a est un diviseur de b et que b est un multiple de a .

Il faut bien sûr pouvoir adapter cette définition selon les cas. Par exemple, quand nous verrons le théorème de division euclidienne, nous nous demanderons si b divise a , donc s'il existe $k \in \mathbb{Z}$ tel que $a = k \times b$.

Notation :

- Si a divise b , on note $a \mid b$. Dans le cas contraire, on note $a \nmid b$.
- Si $a \in \mathbb{Z}$, l'ensemble des multiples de a est donc l'ensemble $\{a \times k \mid k \in \mathbb{Z}\}$, que l'on note $a\mathbb{Z}$. Par exemple, l'ensemble des multiples de 2, c'est-à-dire l'ensemble des nombres pairs, est $2\mathbb{Z} = \{\dots; -6; -4; -2; 0; 2; 4; 6; \dots\}$.

Exemples :

- Si $b \in \mathbb{Z}$, alors $b = b \times 1 = (-b) \times (-1)$. En d'autres termes, $\pm b$ et ± 1 divisent b .
- $-27 = (-9) \times 3$ donc $3 \mid -27$.
- Pour tout $k \in \mathbb{Z}$, $2 \times k$ est un nombre pair donc $2 \times k \neq -27 : 2 \nmid -27$.
- Pour tout $a \in \mathbb{Z}$, $0 = 0 \times a$ donc $a \mid 0$: tout entier divise 0.

Remarque : Cependant, pour tout $k \in \mathbb{Z}$, $0 \times k = 0$ donc le seul multiple de 0 est 0 lui-même, c'est-à-dire que $0\mathbb{Z} = \{0\}$. En d'autres termes, 0 ne divise que lui-même. Cela peut paraître surprenant de dire que 0 divise un nombre (lui-même, en l'occurrence), alors qu'on répète sans arrêt qu'il ne faut pas diviser par 0. Il faut bien comprendre qu'il y a une différence entre dire qu'un nombre en divise un autre, et diviser effectivement par ce nombre. Dire que 0 divise 0 ou que 0 ne divise pas 1 a du sens, mais écrire « $\frac{0}{0}$ » ou « $\frac{1}{0}$ » n'en a pas. Ainsi, la CNS de divisibilité ci-dessous (qui découle directement de la définition) n'a de sens que si a est non nul.

Remarque : Supposons que $a \mid b$. Dans le cas où a est non nul, l'entier k est égal à b/a et donc est unique. En particulier, si a et b sont de même signe, alors $k \in \mathbb{N}$. En d'autres termes, lorsque a est non nul et lorsque a et b sont de même signe, alors : $a \mid b \iff \exists k \in \mathbb{N}, b = k \times a$.

Proposition. Soit $(a, b) \in \mathbb{Z}^* \times \mathbb{Z}$. Alors : $a \mid b \iff \frac{b}{a} \in \mathbb{Z}$. De plus, dans le cas où a et b sont de même signe : $a \mid b \iff \frac{b}{a} \in \mathbb{N}$.



a est non nul !

DÉMONSTRATION. Découle de la définition.

Remarque : Encore une fois, cela n'a de sens que lorsque a est non nul. De toute façon, le cas $a = 0$ est marginal et sera très peu rencontré en pratique, mais le cas $b = 0$, lui, est assez fréquent donc il faut bien garder en tête que tout entier divise 0.

I.1.b Premières propriétés

Proposition. Soit $(a, b) \in \mathbb{Z} \times \mathbb{Z}^*$. Si $a \mid b$ alors $|a| \leq |b|$.

DÉMONSTRATION. Par hypothèse, il existe $k \in \mathbb{Z}$ tel que $b = k \times a$ donc $|b| = |k| \times |a|$. Or, $b \neq 0$ donc $k \neq 0$ donc $|k| \geq 1$. En multipliant cette inégalité par $|a| \geq 0$, il vient $|k| \times |a| = |b| \geq |a|$.

Remarque : En d'autres termes, si b est non nul, alors les diviseurs de b sont inférieurs ou égaux à b en valeur absolue. Par conséquent, **pour de petites valeurs de b** , si on cherche les diviseurs de b , il suffit de tester tous les entiers $a \in \llbracket -b; b \rrbracket$ (non nuls) et de regarder si le quotient b/a est un entier.

Exemple : Les diviseurs de 12 sont $\pm 1, \pm 2, \pm 3, \pm 4, \pm 6$ et ± 12 .

Remarque : Si $b \neq 0$ et si $a \mid b$, alors $a = \pm b$ ou $|a| \leq |b|/2$, c'est-à-dire qu'à part $\pm b$, les diviseurs de b sont inférieurs ou égaux à $|b|/2$ (en valeur absolue). En effet, il existe $k \in \mathbb{Z}^*$ (car $b \neq 0$) tel que $b = k \times a$ si bien que $a = b/k$. Si $k = \pm 1$ alors $a = \pm b$, sinon $|k| \geq 2$ ce qui donne le résultat voulu. Cela permet par exemple (cf. exercice 74 du chapitre 18) de montrer que si G est un groupe fini et si H est un sous-groupe strict de G , alors $\text{card}(H) \leq \text{card}(G)/2$.

Proposition. Soit $(a, b) \in \mathbb{Z}^2$ tel que $ab = 1$. Alors $a = b = 1$ ou $a = b = -1$.

DÉMONSTRATION. Tout d'abord, a et b sont non nuls et de même signe car $ab > 0$. De plus, $a \mid 1$ donc $|a| \leq |1| = 1$ et a est non nul donc $|a| = 1$. Par symétrie des rôles, $|b| = 1$. Ainsi, $a = \pm 1$ et $b = \pm 1$ et puisque a et b sont de même signe, on a le résultat.

Définition. Soit $(a, b) \in \mathbb{Z}^2$. On dit que a et b sont associés si $a \mid b$ et $b \mid a$.

Corollaire. Soit $(a, b) \in \mathbb{Z}^2$. Alors a et b sont associés si et seulement si $a = \pm b$.

DÉMONSTRATION. Supposons que $a \mid b$ et $b \mid a$.

Si $a = 0$ alors b est un multiple de 0 donc $b = 0$ si bien que $a = b$ donc, en particulier, $a = \pm b$. De même si $b = 0$.

Si a et b sont non nuls alors, d'après la proposition précédente, $|a| \leq |b|$ et $|b| \leq |a|$ donc $|a| = |b|$ si bien que $a = \pm b$.

La réciproque est immédiate.

Remarque : On peut se demander l'intérêt de définir la notion d'entiers associés puisqu'il s'agit simplement d'entiers ayant la même valeur absolue. C'est en fait un cas particulier d'une notion plus générale, la notion d'éléments associés dans ce qu'on appelle un anneau euclidien : deux éléments sont associés dans un anneau euclidien lorsque chacun des deux divise l'autre, et alors ces deux éléments sont égaux à un facteur inversible près, et c'est cohérent avec ce qu'on vient de voir puisque les inversibles de \mathbb{Z} sont exactement ± 1 . Nous verrons un autre exemple moins trivial dans le chapitre 19 et nous ferons peut-être le cas général en DM. Bref, on en reparle.

Proposition. Soit $(a, b) \in \mathbb{Z}^2$. Alors : $a \mid b \iff -a \mid b \iff a \mid -b$.

DÉMONSTRATION. Si a divise b alors il existe $k \in \mathbb{Z}$ tel que $b = ka$ donc $b = (-k) \times (-a)$. Or, $-k \in \mathbb{Z}$ donc $-a \mid b$. En appliquant ce résultat à $-a$ plutôt qu'à a , il en découle que si $-a$ divise b , alors $-(-a) = a$ divise b , d'où la réciproque. La deuxième équivalence est laissée en exo.



Ici, c'est b qui est non nul !



En particulier, il n'y a aucun diviseur de b compris strictement entre $b/2$ et b .



La réciproque est triviale.



Attention, si $a \mid b$ et $b \mid a$, on n'a pas forcément $a = b$. On ne peut conclure que $a = b$ que lorsque a et b sont de même signe.

Remarque : De cela on déduit que l'ensemble des diviseurs d'un entier b est toujours symétrique par rapport à 0, que b et $-b$ ont les mêmes diviseurs, et que a et $-a$ ont les mêmes multiples. Cela nous sera utile quand nous parlerons de PGCD et de PPCM dans les paragraphes I.3 et I.4.

Proposition. Soit $(a, b) \in \mathbb{Z}^2$ et soit $k \in \mathbb{Z}$. Si b est un multiple de a alors kb est un multiple de ka .

DÉMONSTRATION. Par hypothèse, il existe $p \in \mathbb{Z}$ tel que $b = pa$ donc $kb = p \times ka$.

Proposition. Soient $a \in \mathbb{Z}$, $n \geq 1$ et $b_1, \dots, b_n, \alpha_1, \dots, \alpha_n$ des entiers. Si $a \mid b_i$ pour tout $i \in \llbracket 1; n \rrbracket$, alors $a \mid \alpha_1 b_1 + \dots + \alpha_n b_n$.

DÉMONSTRATION. Pour tout $i \in \llbracket 1; n \rrbracket$, il existe k_i tel que $b_i = k_i \times a$. Dès lors,

$$\alpha_1 b_1 + \dots + \alpha_n b_n = \underbrace{(\alpha_1 k_1 + \dots + \alpha_n k_n)}_{\in \mathbb{Z}} \times a$$

ce qui permet de conclure. \square

En particulier, si a divise b et c alors a divise $b+c$ et $b-c$. De plus, si a divise b , alors a divise bc (même si a ne divise pas c).

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

DÉMONSTRATION.

\rightsquigarrow EXERCICE.

Proposition. Soit $(a, b, c, d) \in \mathbb{Z}^4$. Si $a \mid b$ et $c \mid d$ alors $a \times c \mid b \times d$.

DÉMONSTRATION. Il existe $(k_1, k_2) \in \mathbb{Z}^2$ tel que $b = k_1 \times a$ et $d = k_2 \times c$, si bien que $bd = (k_1 k_2) \times ac$. Or, $k_1 k_2 \in \mathbb{Z}$ ce qui permet de conclure.

Corollaire. Soit $(a, b) \in \mathbb{Z}^2$. Si $a \mid b$ alors, pour tout $n \in \mathbb{N}$, $a^n \mid b^n$.


DÉMONSTRATION. Par récurrence :


\rightsquigarrow EXERCICE.

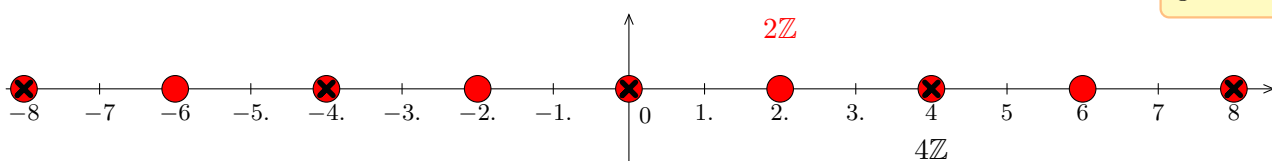
Proposition. Soit $(a, b) \in \mathbb{Z}^2$. Alors : $a \mid b \iff b\mathbb{Z} \subset a\mathbb{Z}$.

DÉMONSTRATION. Supposons que $a \mid b$. Il existe donc $k \in \mathbb{Z}$ tel que $b = ka$. Soit $n \in b\mathbb{Z}$. Il existe $p \in \mathbb{Z}$ tel que $n = pb$. Ainsi, $n = (pk) \times a$. Or, $pk \in \mathbb{Z}$ donc $n \in a\mathbb{Z}$, c'est-à-dire que $b\mathbb{Z} \subset a\mathbb{Z}$.

Réciproquement, supposons que $b\mathbb{Z} \subset a\mathbb{Z}$. En particulier, $b \in b\mathbb{Z}$ donc $b \in a\mathbb{Z}$, si bien qu'il existe $k \in \mathbb{Z}$ tel que $b = ka$, c'est-à-dire que a divise b .

Remarque :  Attention, on a d'un côté $a \mid b$, et de l'autre $b\mathbb{Z} \subset a\mathbb{Z}$. En d'autres termes, quand les entiers sont non nuls : si un entier divise un autre, alors il est **plus petit** en valeur absolue, et on a alors un ensemble de multiples **plus gros**. Par exemple, $2 \mid 4$ donc $4\mathbb{Z} \subset 2\mathbb{Z}$. Il faut bien avoir le dessin ci-dessous en tête.

 Attention, avoir $a \leq b$ ou $a \geq b$ ne suffit pas pour avoir $b\mathbb{Z} \subset a\mathbb{Z}$! Ce n'est pas une relation du type « plus grand ou plus petit » qu'il faut mais une relation de divisibilité. Par exemple, aucun des ensembles $3\mathbb{Z}$ et $4\mathbb{Z}$ n'est inclus dans l'autre. On donnera l'intersection de $a\mathbb{Z}$ et $b\mathbb{Z}$ dans le cas général dans le I.4.b.



Proposition. Soit $b \in \mathbb{Z}$ tel que $|b| \geq 2$ et soit $(n, m) \in \mathbb{N}^2$. Alors : $b^n \mid b^m \iff n \leq m$.

DÉMONSTRATION. Supposons que $n \leq m$. Alors $b^m = b^n \times b^{m-n}$ et $m-n \geq 0$ donc $b^{m-n} \in \mathbb{Z}$ si bien que $b^n \mid b^m$. Réciproquement, supposons que $n > m$. Puisque $|b| \geq 2$, alors $|b^n| > |b^m|$ et $b^m \neq 0$ donc b^n ne divise pas b^m .

I.2 Division euclidienne

Théorème (Théorème de la division euclidienne). Soit $(a, b) \in \mathbb{Z}^2$ avec $b \neq 0$. Il existe un unique couple $(q, r) \in \mathbb{Z}^2$ tel que $a = bq + r$ avec $0 \leq r < |b|$. L'entier q est appelé le quotient et r le reste de la division euclidienne de a par b .



b doit être non nul! On ne peut pas diviser par 0 dans le théorème de la division euclidienne.

Remarques :

- a est appelé le dividende, et b le diviseur (même si b ne divise pas a) de la division euclidienne de a par b .
- Attention, a, b et q peuvent être négatifs, mais r est forcément positif! Sinon, il n'y a plus l'unicité.
- On fera attention au fait que, dans l'énoncé, on effectue la division euclidienne de a par b et non pas la division euclidienne de b par a .
- On peut utiliser l'unicité de la façon suivante : quand on a une écriture du type $a = bq + r$ avec $0 \leq r < |b|$, alors c'est la bonne.
- Si b est positif, $q = \left\lfloor \frac{a}{b} \right\rfloor$. En effet, $0 \leq r < b$ donc $bq \leq a < b(q+1)$ donc $q \leq \frac{a}{b} < q+1$, ce qui permet de conclure.

Exemples :

- Si $a = -28$ et $b = 3$, alors $-28 = (-9) \times 3 - 1$ mais ce n'est pas l'écriture $a = bq + r$ puisque r est strictement négatif. L'écriture (unique) donnée par le théorème de division euclidienne est $-28 = (-10) \times 3 + 2$: le quotient q est égal à -10 et le reste est égal à 2 .
- C'est plus simple dans le cas où tout est positif : par exemple, $28 = 9 \times 3 + 1$, c'est-à-dire que si $a = 28$ et $b = 3$, alors $q = 9$ et $r = 1$. On remarquera que « si on change a en $-a$, on ne change pas q en $-q$ », c'est-à-dire que si $a = bq + r$ est la division euclidienne de a par b , la division euclidienne de $-a$ par b n'est pas forcément $-a = (-q) \times b - r$ car le reste doit être positif. Il est possible de trouver celle de $-a$ à partir de celle de a en séparant les cas selon la valeur de r (cf. exercice 8), mais plutôt que d'apprendre un résultat compliqué qu'on peut oublier facilement, il vaut mieux le refaire à la main quand on en a besoin.
- Dans le cas où a est « beaucoup plus grand que b », on peut effectuer la division euclidienne en plusieurs étapes, en retirant « un gros morceau » à chaque fois. Par exemple, si on veut effectuer la division euclidienne de 2023 par 12, on commence par retirer $100 \times 12 = 1200$ et il reste 823, puis on retire $50 \times 12 = 600$ et il reste 223, puis on retire $15 \times 12 = 180$ et il reste 43, et enfin on retire $3 \times 12 = 36$ et il reste 7, et on s'arrête car $0 \leq 7 < |12|$. Finalement,

$$\begin{aligned} 2023 &= (100 + 50 + 15 + 3) \times 12 + 7 \\ &= 168 \times 12 + 7 \end{aligned}$$

ce qu'on peut écrire sous la forme suivante, comme à l'école primaire :

$$\begin{array}{r|l} 2023 & 12 \\ - 1200 & 100 + 50 + 15 + 3 \\ \hline 823 & \\ - 600 & \\ \hline 223 & \\ - 180 & \\ \hline 43 & \\ - 36 & \\ \hline 7 & \end{array}$$



Si $b < 0$, un raisonnement analogue (exo) donne

$$q = - \left\lfloor \frac{-a}{b} \right\rfloor$$

qui n'est pas égal à $\left\lfloor \frac{a}{b} \right\rfloor$ en général.

En d'autres termes, on soustrait b autant de fois qu'il faut (quitte à faire des « paquets de b » pour aller plus vite et simplifier les calculs) et on s'arrête quand on arrive à un reste inférieur strict à b en valeur absolue. Morale de l'histoire : diviser, c'est soustraire.

- Bon, cela dépend quand même des signes de a et b . Par exemple, si $a > 0$ et $b < 0$, il faut plutôt *ajouter* b autant de fois qu'il le faut. Par exemple, si on veut effectuer la division euclidienne de 3000 par -13 , il faut faire $3000 + (-13) + (-13) + \dots$ autant de fois qu'il le faut pour avoir un reste inférieur ou égal à $|-13| = 13$. On peut encore une fois le faire « par paquets » :

$$\begin{array}{r|l} 3000 & -13 \\ - 2600 & -200 + -30 \\ \hline 400 & \\ - 390 & \\ \hline 10 & \end{array}$$

si bien que $3000 = (-230) \times (-13) + 10$.

DÉMONSTRATION. Montrons d'abord l'existence puis l'unicité (cf. chapitre 1).

Existence : Par récurrence sur $|a|$.

- Si $n \in \mathbb{N}$, notons H_n : « Pour tout a tel que $|a| \leq n$, il existe $(q, r) \in \mathbb{Z}^2$ tel que $a = bq + r$ avec $0 \leq r < |b|$ ».
- Tout d'abord, $0 = 0 \times b + 0$ donc, si on pose $q = 0$ et $r = 0$, on a bien $0 = q \times b + r$ avec $0 \leq r < |b|$ car $b \neq 0$. En d'autres termes, H_0 est vraie.
- Soit $n \in \mathbb{N}$. Supposons H_n vraie et montrons que H_{n+1} est vraie. Soit donc a tel que $|a| \leq n + 1$.
 - ★ Si $|a| \leq n$, alors il existe q et r qui conviennent par hypothèse de récurrence.
 - ★ Supposons que $a = n + 1$. Si $a < |b|$ alors $a = 0 \times b + a$ avec $0 \leq a < |b|$, si bien que les entiers $q = 0$ et $r = a$ conviennent. On suppose à présent que $a \geq |b| \geq \pm b$.

Supposons dans un premier temps que $b \geq 0$. Alors $a = (a - b) + b$, et puisque $a \geq b > 0$ (car b est non nul), alors $0 \leq a - b < a = n + 1$ donc $|a - b| \leq n$: par hypothèse de récurrence, il existe $(q, r) \in \mathbb{Z}^2$ tel que $a - b = q \times b + r$ avec $0 \leq r < |b|$. Par conséquent, $a = bq + r + b = (q + 1)b + r$ avec $0 \leq r < |b|$: $q + 1$ et r conviennent.

Si $b \leq 0$, alors on écrit $a = (a + b) - b$: $a \geq -b$ donc $a + b \geq 0$ et $b < 0$ (toujours car b est non nul) donc $0 \leq a + b < a = n + 1$. Par hypothèse de récurrence, il existe $(q, r) \in \mathbb{Z}^2$ tel que $a + b = bq + r$ avec $0 \leq r < |b|$ donc $a = (q - 1)b + r$, si bien que $q - 1$ et r conviennent.

- ★ Le cas $a = -(n + 1)$ est analogue et laissé en exo.

Finalement, H_{n+1} est vraie.

- D'après le principe de récurrence, H_n est vraie pour tout $n \in \mathbb{N}$. D'où l'existence.

Unicité : Soit $(q_1, q_2, r_1, r_2) \in \mathbb{Z}^4$ tel que $a = bq_1 + r_1$ et $a = bq_2 + r_2$, avec $0 \leq r_1, r_2 < |b|$. Dès lors, $b(q_1 - q_2) = r_2 - r_1$. Supposons que $q_1 \neq q_2$. Alors $r_1 \neq r_2$ car b est non nul. Sans perte de généralité, on suppose $r_1 > r_2 \geq 0$, si bien que $|r_2 - r_1| = r_1 - r_2 \leq r_1 < |b|$, ce qui est absurde car $|r_2 - r_1| = |b| \times |q_2 - q_1| \geq |b|$ car $q_1 \neq q_2$ et donc $|q_2 - q_1| \geq 1$. En conclusion, $q_1 = q_2$ donc $r_2 - r_1 = b(q_1 - q_2) = 0$ donc $r_1 = r_2$, d'où l'unicité.

La preuve n'est rien de plus que la méthode utilisée dans les exemples ci-dessus : on enlève ou on ajoute b selon qu'il est positif ou négatif, et ensuite on applique l'hypothèse de récurrence, c'est-à-dire qu'on recommence jusqu'à avoir un reste inférieur strictement à $|b|$.

Remarque : Soit $(a, b) \in \mathbb{Z} \times \mathbb{Z}^*$. Alors $b \mid a$ si et seulement si le reste dans la division euclidienne de a par b est nul. En effet, si $b \mid a$, alors il existe $k \in \mathbb{Z}$ tel que $a = kb = k \times b + 0$. Puisque $0 \leq 0 < |b|$, par unicité de l'écriture dans la division euclidienne, alors $r = 0$. Réciproquement, écrivons la division euclidienne de a par b : il existe $(q, r) \in \mathbb{Z}^2$ tel que $a = bq + r$ avec $0 \leq r < |b|$. Si $r = 0$, alors $a = bq$ donc b divise a .

Corollaire. Soit $n \in \mathbb{Z}$. Alors n est impair si et seulement s'il existe $k \in \mathbb{Z}$ tel que $n = 2k + 1$.

DÉMONSTRATION. n est impair si et seulement s'il n'est pas pair si et seulement si $2 \nmid n$, si et seulement si le reste dans la division euclidienne de n par 2 n'est pas nul, si et seulement si son reste vaut 1 (car $0 \leq r < 2$).

Nous avons admis ce résultat dans le chapitre 0.

Remarque : Profitons-en pour donner pêle-mêle (sans démonstration) des résultats concernant les nombres pairs ou impairs, toutes plus intuitives les unes que les autres :

- Une somme de nombres pairs est un nombre pair.
- La somme de deux nombres impairs est un nombre pair.
- La somme d'un nombre pair et d'un nombre impair est un nombre impair.
- Le successeur d'un nombre pair est un nombre impair, et le successeur d'un nombre impair est un nombre pair.
- Pour tout $n \in \mathbb{Z}$, n et $n + 1$ sont de parités contraires.
- Le produit d'un entier (de parité quelconque) et d'un entier pair est un entier pair. En particulier, le produit de deux entiers consécutifs est un entier pair.
- Le produit de deux nombres impairs est un nombre impair.
- Un entier n est impair si et seulement s'il existe $k \in \mathbb{Z}$ tel que $n = 2k - 1$.
- Si $n \in \mathbb{N}$, alors n est impair si et seulement s'il existe $k \in \mathbb{N}$ tel que $n = 2k + 1$.
- etc.

Activité : écriture d'un entier en base b .

On rappelle que quand on écrit une égalité du type $N = 2023$, cela signifie :

$$N = 2 \times 10^3 + 0 \times 10^2 + 2 \times 10^1 + 3 \times 10^0$$

C'est tellement sous-entendu que c'est un automatisme, on fait ce calcul de tête, sans même y penser, mais c'est tout de même loin d'être évident (par exemple pour un enfant, un maya, un égyptien ou un mésopotamien...). On dit que 2023 est l'écriture de N en base 10. On cherche à généraliser cette notion.

3 est le chiffre des unités, 2 est le chiffre des dizaines, 0 celui des centaines et 2 celui des milliers.

Proposition/Définition. Soit b un entier supérieur ou égal à 2, et soit N un entier strictement positif. Alors il existe un unique $n \geq 1$ et des entiers a_0, \dots, a_{n-1} appartenant à $\llbracket 0; b-1 \rrbracket$ uniques tels que $a_{n-1} \neq 0$ et

$$N = a_{n-1} \times b^{n-1} + \dots + a_1 \times b + a_0 = \sum_{k=0}^{n-1} a_k b^k$$

On note alors $N = \overline{a_{n-1} \dots a_1 a_0}_b$, et on dit que cette écriture est l'écriture de N en base b .

DÉMONSTRATION. Par récurrence (forte) sur N .

- Si $N \geq 1$, notons H_N : « il existe un unique $n \geq 1$ et des entiers a_0, \dots, a_{n-1} appartenant à $\llbracket 0; b-1 \rrbracket$ uniques tels que $a_{n-1} \neq 0$ et $N = a_{n-1} \times b^{n-1} + \dots + a_1 \times b + a_0$. »

- Soit $N \in \llbracket 1; b-1 \rrbracket$. Alors $N = N \times b^0$, si bien que $n = 1$ et $a_0 = N \neq 0$ conviennent, d'où l'existence. Pour l'unicité, supposons qu'il existe m et des entiers $(\alpha_0, \dots, \alpha_{m-1})$ qui conviennent. Alors $N \geq \alpha_{m-1}b^{m-1} \geq b^{m-1}$ puisque $\alpha_{m-1} \geq 1$. Or, $N < b$ donc $m-1 = 0$ si bien que $m = 1 = n$ et $N = \alpha_0 = a_0$, d'où l'unicité. En d'autres termes, H_1, \dots, H_{b-1} sont vraies.

Précisons que n est le nombre de chiffres/termes.

- Soit $N \geq b-1$. Supposons H_1, \dots, H_N vraies et prouvons que H_{N+1} est vraie. Par conséquent, $N+1 \geq b$. Effectuons la division euclidienne de $N+1$ par b : il existe $(q, r) \in \mathbb{Z}^2$ unique tel que $N+1 = bq + r$ avec $0 \leq r < b$ (car b est positif) et donc $r \in \llbracket 0; b-1 \rrbracket$. Puisque $N+1 \geq b$, alors $q \geq 1$ et $q \leq N$ car $b \geq 2$. En particulier, H_q est vraie : par hypothèse de récurrence, il existe $m \geq 1$ et $(a_{m-1}, \dots, a_0) \in \llbracket 0; b-1 \rrbracket^m$ uniques tels que $q = a_{m-1} \times b^{m-1} + \dots + a_1b + a_0$, si bien que

$$N+1 = a_{m-1}b^m + \dots + a_1b^2 + a_0b + r$$

En d'autres termes, $n = m+1$ et (r, a_0, \dots, a_{m-1}) conviennent (a_{m-1} est bien non nul). De plus, cette écriture est unique : si $p \geq 1$ et $(\alpha_0, \dots, \alpha_{p-1})$ est une écriture qui convient, alors

$$\begin{aligned} N+1 &= \alpha_{p-1}b^{p-1} + \dots + \alpha_1b + \alpha_0 \\ &= b \times (\alpha_{p-1}b^{p-2} + \dots + \alpha_1) + \alpha_0 \end{aligned} \quad \square$$

Or, $0 \leq \alpha_0 < b$ donc, par unicité de la division euclidienne, $\alpha_0 = r$ et le terme entre parenthèse est égal à q . Or, l'écriture de q en base b est unique par hypothèse de récurrence, donc $p-1 = m = n-1$ donc $p = n$, et $\alpha_1 = a_0, \dots, \alpha_{p-1} = a_{m-1}$, c'est-à-dire qu'on a unicité : H_{N+1} est vraie, ce qui clôt la récurrence.

En pratique, comment fait-on ? Pour passer de la base 10 à la base b , un moyen simple consiste à effectuer la division euclidienne de N par b , puis à effectuer la division euclidienne de q par b etc. En d'autres termes, on effectue la division euclidienne des quotients successifs par b , et on s'arrête quand on a un quotient nul. Voyons avec un exemple.

Exemple : Écrivons 2023 en base 7. Tout d'abord, $2023 = 289 \times 7$. Ensuite, $289 = 41 \times 7 + 2$. Ensuite, $41 = 5 \times 7 + 6$, et enfin : $5 = 0 \times 7 + 5$. Il en découle :

$$\begin{aligned} 2023 &= 289 \times 7 + 0 \\ &= (41 \times 7 + 2) \times 7 + 0 \\ &= ((5 \times 7 + 6) \times 7 + 2) \times 7 + 0 \\ &= 5 \times 7^3 + 6 \times 7^2 + 2 \times 7 + 0 \times 7^0 \end{aligned}$$

c'est-à-dire que $2023 = \overline{5620}_7$.

Inversement, pour passer de la base b à la base 10, il suffit de calculer les puissances de b successives, de multiplier par les a_i correspondants et de sommer.

Exemple :

$$\begin{aligned} \overline{3345}_9 &= 3 \times 9^3 + 3 \times 9^2 + 4 \times 9^1 + 5 \times 9^0 \\ &= 2471 \end{aligned}$$

Remarques :

- Pour le deuxième exemple, il est possible de s'en tirer avec moins d'opérations, par exemple avec l'algorithme de Hörner, et on peut passer d'une base b_1 à une base b_2 sans passer par la base 10, par exemple lorsque b_1 et une puissance de b_2 , mais le but de ce paragraphe est d'appliquer le théorème de la division euclidienne et d'introduire l'écriture dans une base différente de la base 10, pas de donner un cours exhaustif ni les algorithmes les plus efficaces pour passer d'une base à une autre.

On effectue à chaque fois la division du **quotient** par b , c'est-à-dire par 7 ici. Ne pas confondre avec l'algorithme d'Euclide (cf. paragraphe I.3.b) où on effectue à chaque fois la division euclidienne du diviseur par le **reste**.

- Quand la base n'est pas précisée, sauf indication contraire, on travaille en base 10 (sans doute parce qu'on a 10 doigts).
- Les bases les plus utilisées à part la base 10 sont la base 2 (on dit qu'on écrit en binaire) et la base 16 (on dit qu'on travaille en hexadécimal). Pour la base 2, on travaille uniquement avec les chiffres 0 et 1 (voir ci-dessous), tandis qu'avec la base 16, on s'autorise les nombres 0 à 15, mais cela pose un problème, car il peut y avoir ambiguïté : quand on écrit $\overline{15}^{16}$, ce nombre est-il égal à $15 \times 16^0 = 15$, ou à $1 \times 16^1 + 5 \times 16^0 = 21$? Pour éviter cela, on introduit des symboles pour les nombres à deux chiffres. Plus précisément, pour représenter les nombres de 10 à 15, on utilise les lettres de A à F :

lettre	A	B	C	D	E	F
signification	10	11	12	13	14	15

Par conséquent, $\overline{15}^{16} = 1 \times 16^1 + 5 \times 16^0 = 21$ et $15 = \overline{F}^{16}$. De même que ci-dessus, $2023 = 126 \times 16 + 7$, $126 = 7 \times 16 + 14$ et $7 = 0 \times 16 + 7$, si bien que :

$$\begin{aligned}
 2023 &= 126 \times 16 + 7 \\
 &= (7 \times 16 + 14) \times 16 + 7 \\
 &= 7 \times 16^2 + 14 \times 16^1 + 7 \times 16^0
 \end{aligned}$$

c'est-à-dire que $2023 = \overline{7E7}^{16}$.

- Dans l'écriture $N = a_{n-1}b^{n-1} + \dots + a_0$ avec $a_{n-1} \neq 0$, on peut trouver n en remarquant que $b^{n-1} \leq N < b^n$. En effet, $N \geq a_{n-1}b^{n-1} \geq b^{n-1}$ car $a_{n-1} \geq 1$ et les autres termes sont positifs, et les a_k sont inférieurs à $b - 1$ si bien que

$$\begin{aligned}
 N &\leq (b-1) \times b^{n-1} + \dots + (b-1) \times b + (b-1) \\
 &\leq (b-1) \times \sum_{k=0}^{n-1} b^k \\
 &\leq (b-1) \times \frac{1-b^n}{1-b} \\
 &\leq b^n - 1
 \end{aligned}$$

Car $b \geq 2$ donc $b \neq 1$.

ce qui est le résultat voulu. En d'autres termes, la dernière puissance de b dans l'écriture de N en base b est la plus grande puissance de b inférieure ou égale à N . Ce sera particulièrement utile en binaire (voir ci-dessous). Cela permet aussi de montrer de façon analogue au chapitre 2 que n , le nombre de chiffres de N en base b , est égal à

$$\lfloor \log_b(N) \rfloor + 1 = \left\lfloor \frac{\ln(N)}{\ln(b)} \right\rfloor + 1$$

- On peut effectuer des additions et des multiplications de la même façon qu'à l'école primaire, sans oublier les retenues, ni qu'on n'a le droit d'utiliser que les nombres de 0 à $b - 1$. Donnons deux exemples en base 8 :

$$\begin{array}{r}
 \begin{array}{r}
 7 \ 1 \ 3 \ 5 \\
 + \ 3 \ 6 \ 0 \ 4 \\
 \hline
 1 \ 2 \ 7 \ 4 \ 1
 \end{array}
 \qquad
 \begin{array}{r}
 \begin{array}{r}
 3 \ 5 \\
 \times \quad 4 \ 6 \\
 \hline
 2 \ 5 \ 6 \\
 1 \ 6 \ 4 \ 0 \\
 \hline
 2 \ 1 \ 1 \ 6
 \end{array}
 \end{array}
 \end{array}$$

On travaille en fait modulo b : cf. partie III.

- Comme on l'a dit, la base la plus utilisée à part la base 10 est la base 2, c'est-à-dire en binaire. Il est très important d'être à l'aise avec le binaire, mais l'avantage est que la situation est très simple puisque les seuls chiffres sont 0 et 1. Il suffit de retenir les règles suivantes :

Idem, on travaille en fait modulo 2.

$$\star 0 + 0 = 0$$

$$\star 0 \times 0 = 0 \times 1 = 0$$

$$\star 0 + 1 = 1 + 0 = 1$$

$$\star 1 \times 1 = 1$$

$$\star 1 + 1 = 0 \text{ (avec une retenue)}$$

Donnons l'écriture binaire des entiers de 0 à 16 (à gauche, l'écriture décimale, à droite, l'écriture binaire) :

$$0 = 0$$

$$1 = 1$$

$$2 = 10$$

$$3 = 11$$

$$4 = 100$$

$$5 = 101$$

$$6 = 110$$

$$7 = 111$$

$$8 = 1000$$

$$9 = 1001$$

$$10 = 1010$$

$$11 = 1011$$

$$12 = 1100$$

$$13 = 1101$$

$$14 = 1110$$

$$15 = 1111$$

$$16 = 10000$$

• Donnons pêle-mêle des remarques concernant l'écriture en binaire :

- ★ Les nombres pairs (respectivement impairs) sont exactement ceux dont l'écriture binaire se termine par un 0 (respectivement par un 1).
- ★ Il y a 10 sortes de personnes : ceux qui savent compter en binaire et les autres.
- ★ Les nombres dont tous les coefficients valent 1 sont les nombres de la forme $2^n - 1$.
- ★ Les puissances de 2 ne contiennent qu'un 1, les autres coefficients sont nuls.
- ★ Quand on veut ajouter 1, on ajoute 1 sur le premier « 0 disponible », les 1 précédents sont « changés en 0 » (c'est-à-dire qu'on effectue une succession de retenues).
- ★ Puisque les a_i valent 0 ou 1, la proposition précédente devient (dans le cas $b = 2$) : tout entier N strictement positif s'écrit de façon unique comme une somme de puissances de 2 distinctes.
- ★ Si n est le nombre de chiffres (en binaire) de N , le fait que n vérifie $2^{n-1} \leq N < 2^n$ permet de donner l'écriture binaire d'un nombre N très rapidement : on prend la plus grande puissance de 2 inférieure ou égale à N , on la soustrait et on recommence. Par exemple, la plus grande puissance de 2 inférieure à 2023 est $1024 = 2^{10}$, et $2023 - 1024 = 999$. Ensuite, la plus grande puissance de 2 inférieure ou égale à 999 est $512 = 2^9$, et $999 - 512 = 487$. La plus grande puissance de 2 inférieure ou égale à 487 est $256 = 2^8$ et $487 - 256 = 231$. Ensuite, $231 - 128 = 103$ puis $103 - 64 = 39$, $39 - 32 = 7$, $7 - 4 = 3$ et $3 - 2 = 1$ si bien que :

$$\begin{aligned} 2023 &= 1024 + 512 + 256 + 128 + 64 + 32 + 4 + 2 + 1 \\ &= 2^{10} + 2^9 + 2^8 + 2^7 + 2^6 + 2^5 + 2^2 + 2^1 + 2^0 \\ &= \overline{11111100111}^2 \end{aligned}$$

Cette méthode marche aussi lorsque $b \neq 2$, mais comme les coefficients ne sont pas forcément égaux à 0 ou 1, il faut parfois soustraire plusieurs fois la même puissance et donc c'est sensiblement plus long.

Cette méthode n'est pas forcément plus rapide que la méthode générale vue plus haut, mais elle a l'avantage de ne nécessiter que des soustractions et pas de division.

I.3 PGCD

I.3.a PGCD de deux entiers naturels

Dans ce paragraphe et le suivant, on ne travaille qu'avec des entiers naturels : le mot « entier » désignera un entier naturel, et le mot « diviseur » un diviseur positif.

Définition. 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 de b . On le note $a \wedge b$.

Remarques :

- Quand on parle du plus grand diviseur commun, c'est pour l'ordre naturel \leq dans \mathbb{N} , c'est-à-dire que tout diviseur d commun de a et de b vérifie $d \leq a \wedge b$. En d'autres termes, $a \wedge b = \max\{d \in \mathbb{N} \mid d \text{ divise } a \text{ et } d \text{ divise } b\}$.
- Ce maximum est bien défini car a et b sont non tous nuls. Supposons (raisonnement analogue dans l'autre cas) que $b \neq 0$. Alors tout diviseur d de b vérifie $d \leq b$: en d'autres termes, l'ensemble $\{d \in \mathbb{N} \mid d \text{ divise } a \text{ et } d \text{ divise } b\}$ est majoré par b . Puisque cet ensemble est non vide (il contient 1), c'est une partie non vide majorée de \mathbb{N} donc admet un plus grand élément.
- Un moyen simple (mais nous en verrons d'autres) de montrer que $d = a \wedge b$ consiste à montrer que d divise a et b et que tout diviseur commun de a et b est inférieur ou égal à d .
- Puisque tout entier divise 0, l'ensemble des diviseurs communs à 0 et 0 est \mathbb{N} tout entier, qui n'admet pas de maximum, c'est pour cela qu'on suppose a et b non tous nuls : parler du PGCD de 0 et 0 n'a pas de sens (même si on dit parfois qu'il est nul, par convention).
- Les entiers a et b jouent le même rôle dans la définition donc $a \wedge b = b \wedge a$, c'est-à-dire que le PGCD est commutatif. Nous verrons dans le paragraphe I.5.a qu'il est aussi associatif.

On rappelle que si $d \mid b$ et si b est non nul, alors $|d| \leq |b|$ (cf. paragraphe I.1.b).

Exemple : Les diviseurs de 8 sont 1, 2, 4 et 8 et ceux de 12 sont 1, 2, 3, 4, 6 et 12, si bien que les diviseurs communs de 8 et 12 sont 1, 2 et 4. En conclusion, $8 \wedge 12 = 4$.

Encore une fois, dans ce paragraphe, on ne considère que des entiers naturels.

Proposition. Soit $b \in \mathbb{N}^*$. Alors $0 \wedge b = b$.

DÉMONSTRATION. Tout d'abord, b est un diviseur commun de 0 et b . De plus, b étant non nul, si $d \mid b$, alors $d \leq b$. En particulier, tous les diviseurs communs de 0 et b sont inférieurs ou égaux à b , d'où le résultat.

On se donne dans la suite de ce paragraphe et dans le suivant deux entiers naturels a et b **tous non nuls**, le cas où l'un des deux étant nul étant réglé.

Proposition. $a \wedge b \geq 1$.

DÉMONSTRATION. Découle de la remarque ci-dessus : $a \wedge b$ est le maximum de l'ensemble $\{d \in \mathbb{N} \mid d \text{ divise } a \text{ et } d \text{ divise } b\}$ et 1 appartient à cet ensemble, d'où le résultat.

Proposition. $a \wedge b \leq \min(a, b)$ avec égalité si et seulement si l'un des deux entiers divise l'autre. Plus précisément, $a \wedge b = a$ si et seulement si $a \mid b$, et $a \wedge b = b$ si et seulement si $b \mid a$.

DÉMONSTRATION. Les entiers a et b étant non nuls, tout entier d diviseur commun à a et b vérifie $d \leq a$ et $d \leq b$ donc $d \leq \min(a, b)$, et c'est en particulier vrai pour $a \wedge b$.

Si $a = a \wedge b$, alors $a \mid b$ car le PGCD de deux entiers divise ces entiers par définition. Réciproquement, supposons que $a \mid b$. Alors a est un diviseur commun de a et de b et on a déjà vu que tout diviseur commun de a et b est inférieur ou égal à a donc $a = a \wedge b$. Par symétrie des rôles on a l'autre équivalence.

I.3.b Algorithme d'Euclide

Lemme. Soient q et r respectivement le quotient et le reste de la division euclidienne de a par b . Alors $a \wedge b = b \wedge r$.

DÉMONSTRATION. Soit d un diviseur commun de a et de b . Alors $d \mid bq$ et puisque $r = a - bq$, alors $d \mid r$. Réciproquement, soit d un diviseur commun à b et r . Puisque $a = bq + r$, alors $d \mid a$. En conclusion, les couples (a, b) et (b, r) ont les mêmes diviseurs communs donc le même PGCD.

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

- 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 $i \geq 2$. 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 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, la suite des restes est strictement décroissante d'après le théorème de la division euclidienne, et une suite strictement décroissante d'entiers naturels finit par atteindre 0.

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

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

En d'autres termes :

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

Exemple : Donnons le PGCD de 2023 et 1789.

$$\begin{array}{r|l} 2023 & 1789 \quad 1789 \\ - 1789 & 1 \quad 1638 \\ \hline 234 & 151 \end{array} \quad \begin{array}{r|l} 234 & 234 \\ - 151 & 7 \quad 151 \\ \hline 83 & 83 \end{array} \quad \begin{array}{r|l} 151 & 151 \\ - 83 & 1 \quad 68 \\ \hline 68 & 68 \end{array} \quad \begin{array}{r|l} 83 & 83 \\ - 68 & 1 \quad 15 \\ \hline 15 & 15 \end{array} \quad \begin{array}{r|l} 68 & 68 \\ - 60 & 1 \quad 8 \\ \hline 8 & 8 \end{array} \quad \begin{array}{r|l} 15 & 15 \\ - 8 & 1 \quad 7 \\ \hline 7 & 7 \end{array} \quad \begin{array}{r|l} 8 & 8 \\ - 7 & 1 \quad 1 \\ \hline 1 & 1 \end{array} \quad \begin{array}{r|l} 7 & 7 \\ - 7 & 0 \end{array}$$

Finalement, $2023 \wedge 1789 = 1$.

Exemple : Donnons le PGCD de 525 et 385.

$$\begin{array}{r|l} 525 & 385 \\ - 385 & 1 \quad 140 \\ \hline 140 & 140 \end{array} \quad \begin{array}{r|l} 385 & 140 \\ - 280 & 2 \quad 105 \\ \hline 105 & 105 \end{array} \quad \begin{array}{r|l} 140 & 105 \\ - 105 & 1 \quad 35 \\ \hline 35 & 35 \end{array} \quad \begin{array}{r|l} 105 & 35 \\ - 105 & 0 \end{array}$$

si bien que $525 \wedge 385 = 35$.

Lemme. Soit $k \in \mathbb{N}^*$. Soient q et r respectivement le quotient et le reste de la division euclidienne de a par b . Alors le quotient et le reste de la division euclidienne de ka par kb sont, respectivement, q et kr .

DÉMONSTRATION. Par hypothèse, $a = bq + r$ avec $0 \leq r < b$ donc $ka = q \times bk + kr$. Or, $k \in \mathbb{N}^*$ donc $0 \leq kr < kb$, d'où le résultat par unicité de l'écriture de la division euclidienne.

Proposition. Soit $k \in \mathbb{N}^*$. Alors $(ka) \wedge (kb) = k \times (a \wedge b)$.

Pour être plus précis, on s'arrête en au plus b itérations. On peut en fait montrer (cf. exercice 16) que l'algorithme termine en au plus $5N$ étapes, où N est le nombre de chiffres en base 10 de b .

Nous dirons dans le paragraphe I.3.d qu'ils sont premiers entre eux. En fait, 1789 étant premier (cf. partie III), 1789 est premier avec tout nombre qui n'est pas un de ses multiples (et 2023 n'est pas l'un d'eux).

DÉMONSTRATION. Si l'on note (ρ_i) la suite des restes obtenus en appliquant l'algorithme d'Euclide à ka et kb , le lemme ci-dessus nous dit que, pour tout i , $\rho_i = k \times r_i$, où (r_i) est la suite obtenue en appliquant cet algorithme à a et b . En particulier, si r_n est le dernier reste non nul pour a et b , alors ρ_n est le dernier reste non nul pour ka et kb , et :

$$\begin{aligned}(ka) \wedge (kb) &= \rho_n \\ &= k \times r_n \\ &= k \times (a \wedge b)\end{aligned}\quad \square$$

I.3.c Extension aux entiers relatifs

Dans la suite, le mot « entier » désigne à nouveau un entier relatif, et le mot « diviseur » un diviseur quelconque (pas forcément positif).

Définition. 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 de b . On le note $a \wedge b$.

Remarques :

- Quand on parle du plus grand diviseur commun, c'est encore pour l'ordre naturel \leq dans \mathbb{Z} , c'est-à-dire que tout diviseur d commun de a et de b vérifie $d \leq a \wedge b$. En d'autres termes, $a \wedge b = \max\{d \in \mathbb{Z} \mid d \text{ divise } a \text{ et } d \text{ divise } b\}$.
- Ce maximum est encore bien défini car a et b sont non tous nuls. Supposons (raisonnement analogue dans l'autre cas) que $b \neq 0$. Alors tout diviseur d de b vérifie $|d| \leq |b|$ donc $d \leq |b|$ et on conclut que le maximum est bien défini comme précédemment.

Exemple : Les diviseurs de -8 sont $\pm 1, \pm 2, \pm 4$ et ± 8 et ceux de -12 sont $\pm 1, \pm 2, \pm 3, \pm 4, \pm 6$ et ± 12 , si bien que les diviseurs communs de -8 et -12 sont $\pm 1, \pm 2$ et ± 4 . En conclusion, $-8 \wedge -12 = 4$.

Proposition. Soient a et b deux entiers non tous nuls. Alors $a \wedge b = \pm a \wedge \pm b = |a| \wedge |b|$.

DÉMONSTRATION. Immédiat puisque a et $-a$ (et donc $|a|$) ont les mêmes diviseurs, ainsi que b et $-b$ (et donc $|b|$).

Remarque : Par conséquent, tous les résultats des deux paragraphes précédents sont encore valables : il suffit pour cela de remplacer a par $|a|$ et b par $|b|$, ce qui ne change pas le PGCD.

- $a \wedge b = b \wedge a$.
- Si $b \in \mathbb{Z}^*$, alors $0 \wedge b = |b|$.
- $a \wedge b \geq 1$. Ainsi, le PGCD de deux entiers est un entier supérieur ou égal à 1 (même si a et b sont négatifs!).
- Si a et b sont non nuls, alors $a \wedge b \leq \min(|a|, |b|)$ avec égalité si et seulement si l'un des deux divise l'autre. Plus précisément, $a \wedge b = |a|$ si et seulement si a divise b , et $a \wedge b = |b|$ si et seulement si b divise a .
- L'algorithme d'Euclide est encore valable pour des entiers relatifs. Cependant, en pratique, quand on cherchera le PGCD de deux entiers explicites, on s'arrangera pour l'appliquer à des entiers naturels. Par exemple, chercher le PGCD de -2023 et de 1789 revient à chercher le PGCD de 2023 et 1789 donc on appliquera l'algorithme d'Euclide à ces deux entiers.
- Si $k \in \mathbb{Z}^*$, alors $(ka) \wedge (kb) = |k| \times (a \wedge b)$.

En effet,

$$\begin{aligned}a \wedge b &= |a| \wedge |b| \\ &= |b| \wedge |a| \\ &= b \wedge a\end{aligned}$$

Les autres résultats sont laissés en exo.

Remarque : On sait également que l'ensemble des diviseurs d'un entier N est symétrique par rapport à 0. Par conséquent, quand on cherche les diviseurs d'un entier, on peut se contenter de donner les diviseurs positifs : les autres sont leurs opposés. De plus, le PGCD de deux entiers étant positifs, il est inutile de chercher les diviseurs négatifs car ils ne peuvent de toute façon pas être égaux au PGCD.

I.3.d Entiers premiers entre eux


Définition. Soient a et b deux entiers non tous nuls. On dit qu'ils sont premiers entre eux si $a \wedge b = 1$, c'est-à-dire si leur PGCD est égal à 1.

On dit aussi que a est premier avec b ou que a est premier à b (et idem pour b).

Remarque : En d'autres termes, deux entiers sont premiers entre eux lorsque leur unique diviseur positif commun vaut 1, ou lorsque leurs seuls diviseurs communs sont ± 1 . Par conséquent, un moyen simple (mais nous en verrons d'autres) de montrer que a et b sont premiers entre eux consiste à prendre un diviseur positif d de a et b et à montrer que $d = 1$, voir un exemple dans le paragraphe II.4.

Exemple : 2023 et 1789 sont premiers entre eux.

Remarques :

- Si $a \mid b$ et si $a \neq \pm 1$ alors a et b ne sont pas premiers entre eux car $|a|$ est un diviseur positif commun différent de 1.
- Cependant, la réciproque est fautive : dire que a et b ne sont pas premiers entre eux ne signifie pas que l'un des deux divise l'autre mais qu'ils ont un diviseur positif commun différent de 1. Par exemple, deux nombres pairs quelconques ne sont pas premiers entre eux car admettent 2 comme diviseur commun.
-  Deux nombres premiers entre eux ne sont pas forcément premiers (cf. partie II) : des nombres premiers entre eux ne sont pas des nombres premiers qui sont entre eux ! Par exemple, 9 et 10 ne sont pas premiers mais sont premiers entre eux. Plus généralement :

Par exemple, 16 et 20 ne sont pas premiers entre eux car admettent 2 comme diviseur commun. Plus précisément, $20 \wedge 16 = 4$.

Proposition. Deux entiers consécutifs sont premiers entre eux.

DÉMONSTRATION. Soit $n \in \mathbb{Z}$ et soit d un diviseur positif commun à n et $n + 1$, si bien que d divise $(n + 1) - n = 1$ donc $d = 1$.

Il est bien évident que la réciproque est fautive, mais ce cas particulier revient souvent.

Proposition. Si a et b sont premiers entre eux et si d est un diviseur de a , alors d et b sont premiers entre eux.

DÉMONSTRATION. Soit k un diviseur commun (positif) de d et b . Puisque d divise a , alors k divise a donc k est un diviseur commun de a et b donc $k \leq a \wedge b = 1$. Puisque k est positif, alors $k = 1$: 1 est le seul diviseur positif commun à b et d , d'où le résultat.

I.3.e Algorithme d'Euclide étendu et relation de Bézout

Algorithme d'Euclide étendu : Soient a et b tels que $0 < b \leq a$.

- 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 $i \geq 2$. 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.

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 l'algorithme d'Euclide ne considère que les restes tandis que l'algorithme d'Euclide étendu prend aussi en compte les quotients, et cela permet, non seulement d'obtenir $a \wedge b$, mais des entiers **relatifs** (même et surtout si a et b sont positifs) u et v tels que $au + bv = a \wedge b$.

En effet, par définition, pour tout i , $r_{i-1} = r_i \times q_{i+1} + r_{i+1}$ donc $r_{i+1} = r_{i-1} - r_i \times q_i$. Si on note encore r_n le dernier reste non nul (et donc le PGCD de a et b), cette égalité devient : $a \wedge b = r_{n-2} - r_{n-1} \times q_{n-1}$.

Or, on a également $r_{n-1} = r_{n-3} - r_{n-2}q_{n-2}$ si bien que

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

L'idée est de remplacer à chaque fois le dernier reste disponible (r_{n-2} puis r_{n-3} etc.) à l'aide de l'équation $r_{i+1} = r_{i-1} - r_i \times q_i$ 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 $b = q_1 r_0 + r_1$ si bien que $r_1 = b - q_1 r_0$ donc

$$\begin{aligned} a \wedge b &= c_0 r_0 + c_1 (b - q_1 r_0) \\ &= (c_0 - c_1 q_1) r_0 + c_1 b \end{aligned}$$

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

$$\begin{aligned} a \wedge b &= (c_0 - c_1 q_1) \times (a - bq_0) + c_1 b \\ &= (c_0 - c_1 q_1) \times a + (c_1 - q_0 c_0 + q_0 c_1 q_1) \times b \end{aligned}$$

Finalement, on a bien prouvé l'existence de u et v entiers relatifs tels que $au + bv = a \wedge b$.

Si $b = 0$ et $a > 0$, c'est toujours vrai car $a \wedge b = a$ et $a \times 1 + 0 \times b = a = a \wedge b$.

Si $0 \leq a \leq b$, il suffit d'appliquer l'algorithme d'Euclide étendu avec b à la place de a et a à la place de b .

Enfin, si a ou b est négatif, on applique ce qui précède avec $|a|$ et $|b|$: il existe c et d entiers relatifs tels que $c \times |a| + d \times |b| = |a| \wedge |b| = a \wedge b$. Si $a \leq 0 \leq b$ (raisonnement analogue dans les autres cas), cela donne : $(-c) \times a + d \times b = a \wedge b$. En conclusion, il existe toujours u et v tels que $au + bv = a \wedge b$.

Plus généralement, si M est un multiple de $d = a \wedge b$, il existe $k \in \mathbb{Z}$ tel que $M = kd$ si bien que $(ku) \times a + (kv) \times b = kd = M$. En d'autres termes, le résultat précédent est encore vrai si M est un multiple de $a \wedge b$.

Réciproquement, soit $(u, v) \in \mathbb{Z}^2$ et soit $c = au + bv$. Puisque $d = a \wedge b$ divise a et b alors d divise c . En d'autres termes, c est un multiple de $a \wedge b$. En particulier, si $c = 1$, alors $a \wedge b$ divise 1 donc $a \wedge b = 1$.

En conclusion, on a montré le théorème suivant :

Théorème (Théorème de Bézout). Soient a et b appartenant à \mathbb{Z} non tous nuls.

- Il existe $(u, v) \in \mathbb{Z}^2$ tel que $au + bv = a \wedge b$.
- Plus généralement, si $m \in \mathbb{Z}$, il existe $(u, v) \in \mathbb{Z}^2$ tel que $au + bv = m$ si et seulement si m est un multiple de $a \wedge b$.
- En particulier, a et b sont premiers entre eux si et seulement s'il existe $(u, v) \in \mathbb{Z}^2$ tel que $au + bv = 1$.

Une récurrence double immédiate (exo) permet en effet de prouver que, pour tout $k \in \llbracket 2; n \rrbracket$, il existe $(c_{n-k}, c_{n-k+1}) \in \mathbb{Z}^2$ tel que $a \wedge b = c_{n-k} r_{n-k} + c_{n-k+1} r_{n-k+1}$.

Ou, ce qui revient au même, si et seulement si m est divisible par $a \wedge b$. En termes ensemblistes :

$$a\mathbb{Z} + b\mathbb{Z} = (a \wedge b)\mathbb{Z}$$

C'est parfois comme cela qu'on définit le PGCD de a et b .

Remarque : Une égalité du type $au + bv = a \wedge b$ est appelée UNE relation de Bézout. En effet, il n'y a pas unicité des coefficients u et v . Par exemple, si $a = 2$ et $b = 5$, alors $3a - b = 1$ et $(-7)a + 5b = 1$. Il y a même une infinité de couples (u, v) qui conviennent (cf. paragraphe I.3.g).

En pratique : Lorsque a et b sont petits, on peut trouver un couple (u, v) qui convient de tête (voir l'exemple de 2 et 5 ci-dessus). Cependant, lorsque a et b sont grands, ce n'est plus possible. Heureusement, l'algorithme d'Euclide étendu nous permet d'obtenir un tel couple :

- On part de l'égalité $r_n = a \wedge b = r_{n-2} - r_{n-1} \times q_{n-1}$. En d'autres termes, on part de la division euclidienne dans laquelle le PGCD est le reste (l'avant-dernière) et on l'isole, c'est-à-dire qu'on l'exprime en fonction des autres éléments de la division euclidienne.
- À chaque étape, on remplace le plus petit des deux restes par les éléments de la division euclidienne dans lequel celui-ci apparaît.

Exemple : Trouver deux entiers u et v tels que $u \times 525 + v \times 385 = 35$.

$$\begin{aligned} 35 &= 140 - 105 \\ &= 140 - (385 - 2 \times 140) \\ &= 3 \times 140 - 385 \\ &= 3 \times (525 - 385) - 385 \\ &= 3 \times 525 - 4 \times 385 \end{aligned}$$

Exemple : Trouver deux entiers u et v tels que $u \times 2023 + v \times 1789 = 1$.

$$\begin{aligned} 1 &= 8 - 7 \\ &= 8 - (15 - 8) \\ &= 2 \times 8 - 15 \\ &= 2 \times (68 - 4 \times 15) - 15 \\ &= 2 \times 68 - 9 \times 15 \\ &= 2 \times 68 - 9 \times (83 - 68) \\ &= 11 \times 68 - 9 \times 83 \\ &= 11 \times (151 - 83) - 9 \times 83 \\ &= 11 \times 151 - 20 \times 83 \\ &= 11 \times 151 - 20 \times (234 - 151) \\ &= 31 \times 151 - 20 \times 234 \\ &= 31 \times (1789 - 7 \times 234) - 20 \times 234 \\ &= 31 \times 1789 - 237 \times 234 \\ &= 31 \times 1789 - 237(2023 - 1789) \\ &= 268 \times 1789 - 237 \times 2023 \end{aligned}$$

Ce théorème est très important. Il faut y penser (entre autres) à chaque fois qu'on parle d'entiers premiers entre eux. Il a de très nombreuses applications.

Proposition. Soit $(a, b, n) \in \mathbb{Z}^3$. Si a est premier avec n et si b est premier avec n , alors ab est premier avec n .

DÉMONSTRATION. D'après le théorème de Bézout, il existe $(u, v, x, y) \in \mathbb{Z}^4$ tel que $au + vn = 1$ et $bx + yn = 1$. Par produit : $ab \times ux + n \times (auy + vyn + vb x) = 1$ ce qui permet de conclure, toujours d'après le théorème de Bézout.

Proposition. Soient a et b deux entiers non tous nuls. Soit $k \in \mathbb{Z}$. Alors k divise a et b si et seulement si k divise $a \wedge b$.

Remarques :

Sans calculatrice, ce serait une perte de temps de vérifier ce calcul, mais il ne coûte pas cher de vérifier que les chiffres des unités (i.e. les congruences modulo 10, cf. paragraphe III) sont cohérents.

Nous donnerons une autre démonstration de ce résultat dans le paragraphe II.3.d.

- En d'autres termes, l'ensemble des diviseurs communs de a et b est l'ensemble des diviseurs de $a \wedge b$.
- Par conséquent, non seulement les diviseurs communs de a et b sont inférieurs au PGCD de a et b , mais en plus ils divisent le PGCD. Il en découle que le PGCD de a et b est aussi le plus grand diviseur de a et b au sens de la relation d'ordre divisibilité (c'est donc leur borne inférieure, cf. chapitre 16). Par exemple, il n'existe pas d'entiers a et b dont les diviseurs positifs communs soient 1, 2 et 3. Cependant, on a déjà vu que les diviseurs positifs communs de 8 et 12 sont 1, 2 et 4 : on voit bien que tous les diviseurs communs divisent le PGCD.

DÉMONSTRATION. Supposons que $k \mid a \wedge b$. Alors $k \mid a \wedge b$ et $a \wedge b$ divise a et b donc k divise a et b . Réciproquement, supposons que k divise a et b . D'après le théorème de Bézout, il existe $(u, v) \in \mathbb{Z}^2$ tel que $au + bv = a \wedge b$. Or, k divise a et b donc k divise $au + bv$, ce qui permet de conclure.

Proposition. Soient a et b des entiers non tous nuls. Soit $d = a \wedge b$. Alors $\frac{a}{d}$ et $\frac{b}{d}$ sont des entiers premiers entre eux.

DÉMONSTRATION. Tout d'abord, a/d et b/d sont des entiers car d divise a et b . De plus, d'après le théorème de Bézout, il existe $(u, v) \in \mathbb{Z}^2$ tel que $au + bv = d$ si bien que


$$u \times \left(\frac{a}{d}\right) + v \times \left(\frac{b}{d}\right) = 1 \quad \square$$

Toujours d'après le théorème de Bézout, cela signifie que a/d et b/d sont premiers entre eux.

I.3.f Théorème de Gauß et applications

Théorème (Théorème de Gauß). Soit $(a, b, c) \in \mathbb{Z}^3$. Si $a \wedge b = 1$ et si $a \mid bc$ alors $a \mid c$.

DÉMONSTRATION. a et b sont premiers entre eux donc, d'après le théorème de Bézout, il existe $(u, v) \in \mathbb{Z}^2$ tel que $au + bv = 1$ si bien que $cau + bcv = c$. Puisque a divise bc , alors il existe $k \in \mathbb{Z}$ tel que $bc = ak$ si bien que $cau + kav = c$ donc $a \times (cu + kv) = c$: a divise c .

Remarque :  C'est faux si a et b ne sont pas premiers entre eux ! Plus précisément, il est faux de dire : « si $a \mid bc$ alors a divise b ou c » ou « si $a \mid bc$ et si a ne divise pas b , alors a divise c ». Par exemple, 6 divise 4×3 mais ne divise ni 4 ni 3.

Corollaire. Soit $r \in \mathbb{Q}$. Il existe un unique couple $(a, b) \in \mathbb{Z} \times \mathbb{N}^*$ d'entiers premiers entre eux tel que $r = \frac{a}{b}$. Cette écriture est appelée écriture irréductible du rationnel q . De plus, si $r \neq 0$, alors toute écriture de r est de la forme $\frac{ac}{bc}$ avec $c \in \mathbb{Z}^*$.

DÉMONSTRATION. Par définition d'un rationnel, il existe $(a', b') \in \mathbb{Z} \times \mathbb{N}^*$ tel que $r = \frac{a'}{b'}$. Soit $d = a' \wedge b'$ et soient $a = \frac{a'}{d}$ et $b = \frac{b'}{d}$. Alors a et b sont des entiers premiers entre eux et

$$\begin{aligned} \frac{a}{b} &= \frac{a'd}{b'd} \\ &= r \end{aligned} \quad \square$$

D'où l'existence.

Quand on divise deux entiers par leur PGCD, ils n'ont plus de diviseur positif commun autre que 1 : on a « supprimé » les autres.

Ainsi, si r est un rationnel, on peut toujours écrire r sous la forme $\frac{a}{b}$ avec $a \in \mathbb{Z}$ et $b \in \mathbb{N}^*$ premiers entre eux, et cette écriture est unique. De plus, si $r \geq 0$, alors $a \in \mathbb{N}$. C'est en général avec le fait que a et b sont premiers entre eux qu'on obtient une absurdité dans les raisonnements d'irrationalité (voir par exemple le chapitre 0).

Si $\frac{p}{q}$ est une écriture qui convient, alors $\frac{a}{b} = \frac{p}{q}$ donc $aq = bp$. Il en découle que b divise aq . Or, $a \wedge b = 1$ donc, d'après le théorème de Gauß, b divise q . Par symétrie des rôles, q divise b c'est-à-dire que b et q sont associés et puisqu'ils sont positifs, $b = q$ donc $a = p$, d'où l'unicité.

Enfin, si $\frac{e}{f} = \frac{a}{b}$, alors $eb = af$ donc b divise af . Puisque $a \wedge b = 1$, d'après le théorème de Gauß, b divise f donc il existe $k_1 \in \mathbb{Z}^*$ tel que $f = bk_1$. De même, il existe $k_2 \in \mathbb{Z}^*$ tel que $e = ak_2$ si bien que $\frac{a}{b} = \frac{a}{b} \times \frac{k_1}{k_2}$ et puisque $a \neq 0$, $k_1 = k_2$ ce qui permet de conclure.

Activité : Soit $n \in \mathbb{N}$. Montrons que $\sqrt{n} \in \mathbb{N}$ ou $\sqrt{n} \in \mathbb{R} \setminus \mathbb{Q}$.


Supposons que $\sqrt{n} \in \mathbb{Q}$. Alors il existe $a \in \mathbb{N}$ (car \sqrt{n} est positif) et $b \in \mathbb{N}^*$ premiers entre eux tels que $\sqrt{n} = \frac{a}{b}$. Dès lors, $a^2 = nb^2 = nb \times b$. En particulier, $b \mid a^2 = a \times a$. Or, $a \wedge b = 1$ donc, d'après le théorème de Gauß, $b \mid a$ si bien que $a \wedge b = b$. Or, $a \wedge b = 1$ donc $b = 1$ si bien que $\sqrt{n} = a \in \mathbb{N}$.

Remarque : En d'autres termes, soit \sqrt{n} est un entier (si n est un carré parfait), soit \sqrt{n} est un irrationnel. On en déduit que $\sqrt{2}, \sqrt{3}, \sqrt{5}, \sqrt{6}, \sqrt{7}, \sqrt{8}, \sqrt{10}$ etc. sont irrationnels : toutes sont irrationnelles, sauf les racines des carrés parfaits ($\sqrt{4}, \sqrt{9}$ etc.) qui sont des entiers.

De façon tout à fait analogue : si $p \geq 2$, alors soit il existe $k \in \mathbb{N}$ tel que $n = k^p$ (et alors $\sqrt[p]{n} = n^{1/p} = k \in \mathbb{N}$) soit $\sqrt[p]{n} \notin \mathbb{Q}$. En d'autres termes : soit $\sqrt[p]{n}$ est un entier (lorsque n est une puissance p -ième), soit $\sqrt[p]{n}$ est un irrationnel. Par exemple, $\sqrt[3]{2} \notin \mathbb{Q}$.

Corollaire. Soient a et b deux entiers non tous nuls. Soit $n \in \mathbb{Z}$. Si a et b divisent n et si a et b sont premiers entre eux, alors ab divise n .

Exemple : Si n est divisible par 2 et par 3 alors n est divisible par 6 car 2 et 3 sont premiers entre eux.

Remarque :  C'est faux si a et b ne sont pas premiers entre eux ! Par exemple, 4 et 6 divisent 12 mais $4 \times 6 = 24$ ne divise pas 12.

DÉMONSTRATION. $b \mid n$ donc il existe $k_1 \in \mathbb{Z}$ tel que $n = bk_1$. Or, $a \mid n = bk_1$ et $a \wedge b = 1$ donc, d'après le théorème de Gauß, $a \mid k_1$: il existe $k_2 \in \mathbb{Z}$ tel que $k_1 = ak_2$ si bien que $n = abk_2$, ce qui est le résultat voulu.

I.3.g Un cas simple d'équation diophantienne

Une équation diophantienne est une équation polynomiale à coefficients entiers dont les inconnues sont des entiers (ou parfois des rationnels). Nous avons par exemple déjà vu l'équation $x^2 - 2y^2 = 1$ dans l'exercice 13 du chapitre 1, et nous avons montré qu'elle admettait une infinité de couples (x, y) solutions. Citons aussi l'équation de Fermat $x^n + y^n - z^n = 0$ dont les solutions, pour $n \geq 3$, vérifient $xyz = 0$. On ne sait pas les résoudre en général, ni même déterminer si une équation diophantienne admet un nombre fini ou infini de solutions.

Nous allons nous intéresser dans ce paragraphe aux équations du type $ax + by = c$ d'inconnues x et y appartenant à \mathbb{Z} , où $(a, b, c) \in \mathbb{Z}^3$, avec a et b tous les deux non nuls, est fixé. On a vu par exemple que le couple $(3, -4)$ est solution de l'équation $525x + 385y = 35$ et que le couple $(268, -237)$ est solution de l'équation $1789x + 2023y = 1$.

On se donne dans tout le paragraphe $(a, b, c) \in \mathbb{Z}^3$ avec a et b non nuls et on cherche les solutions entières éventuelles de l'équation $ax + by = c$.

Tout d'abord, on se demande si l'équation $ax + by = c$ admet des solutions. Le résultat suivant découle immédiatement du théorème de Bézout :

Rappel (cf. chapitre 0) : pour montrer une assertion du type A ou B , il suffit de supposer A fausse et de prouver que B est vraie.

Nous donnons une autre démonstration dans l'exercice 29 du chapitre 12.

Si $a = 0$ ou $b = 0$, l'équation devient $ax = c$ ou $by = c$, et donner ses solutions éventuelles est trivial.

Proposition. L'équation $ax + by = c$ admet des solutions si et seulement si c est un multiple de $a \wedge b$.

On voit directement que l'équation $2x + 4y = 1$ n'admet aucune solution car le membre de gauche est forcément pair. Sans le résultat précédent, il est moins évident que l'équation $525x + 385y = 5$ n'admet aucune solution, ou que l'équation $525x + 385y = 35$ en admet, elle.

Commençons par le cas où a et b sont premiers entre eux et où $c = 1$, c'est-à-dire qu'on cherche les solutions de l'équation $ax + by = 1$. L'algorithme d'Euclide étendu fournit une solution particulière (u, v) . On peut obtenir toutes les solutions de l'équation à partir de cette solution particulière de la façon suivante : soit $(x, y) \in \mathbb{Z}^2$. Alors :

$$\begin{aligned}(x, y) \text{ est solution de l'équation} &\iff ax + by = 1 \\ &\iff ax + by = au + bv \\ &\iff a(x - u) = b(v - y)\end{aligned}$$

Si (x, y) est solution, alors a divise $b(v - y)$ et $a \wedge b = 1$ donc, d'après le théorème de Gauß, a divise $v - y$ donc il existe $k \in \mathbb{Z}$ tel que $ak = v - y$ i.e. $y = v - ak$. Or, $a(x - u) = b(v - y)$ donc $a(x - u) = bak$ et $a \neq 0$ donc $x - u = bk$ donc $x = u + bk$. Finalement, il existe $k \in \mathbb{Z}$ tel que $x = u + bk$ et $y = v - ak$. Réciproquement, tout couple de la forme $(u + bk, v - ak)$, pour $k \in \mathbb{Z}$, est solution de l'équation. En conclusion, l'ensemble des solutions est $S = \{(u + bk, v - ak) \mid k \in \mathbb{Z}\}$. En particulier, il y a une infinité de solutions.

On suppose encore que a et b sont premiers entre eux mais on ne suppose plus que $c = 1$. On trouve encore une solution particulière (u, v) à l'équation $ax + by = 1$, et donc le couple (cu, cv) est une solution particulière de l'équation $ax + by = c$. On montre de même que ci-dessus (à l'aide du théorème de Gauß, a et b étant premiers entre eux) que l'ensemble des solutions est $S = \{(cu + bk, cv - ak) \mid k \in \mathbb{Z}\}$.

On revient au cas général, c'est-à-dire qu'on ne suppose plus a et b premiers entre eux (mais on suppose tout de même que c est un multiple de $a \wedge b$). On se ramène au cas où a et b sont premiers entre eux en divisant l'équation par $a \wedge b$. Plus précisément, si $(x, y) \in \mathbb{Z}^2$, alors :

$$ax + by = c \iff \frac{a}{a \wedge b} \times x + \frac{b}{a \wedge b} \times y = \frac{c}{a \wedge b}$$

Par conséquent, ces deux équations ont les mêmes solutions, et puisque $\frac{a}{a \wedge b}$ et $\frac{b}{a \wedge b}$ sont premiers entre eux, la seconde équation se résout comme précédemment.

Méthode : Pour donner les solutions éventuelles de l'équation $ax + by = c$:

- On commence par calculer $a \wedge b$: s'il ne divise pas c , alors l'équation n'a pas de solution. On suppose dans la suite que $a \wedge b$ divise c .
- On divise l'équation par $a \wedge b$: on se ramène donc à une équation du type $a'x + b'y = c'$ avec a' et b' premiers entre eux.
- On donne une solution particulière (u, v) de l'équation $a'x + b'y = 1$ grâce à l'algorithme d'Euclide étendu utilisé à la première étape, et le couple $(c'u, c'v)$ est alors une solution particulière de l'équation $a'x + b'y = c'$.
- On exprime les solutions de l'équation en fonction de la solution particulière de la même façon que ci-dessus (le théorème de Gauß doit apparaître quelque-part).

Exemples : Cherchons si l'équation $45x + 75y = 20$ admet des solutions.

$$\begin{array}{r|l} 75 & 45 \\ - 45 & 1 \\ \hline 30 & \end{array}$$

$$\begin{array}{r|l} 45 & 30 \\ - 30 & 1 \\ \hline 15 & \end{array}$$

$$\begin{array}{r|l} 30 & 15 \\ - 30 & 2 \\ \hline 0 & \end{array}$$

Ou, ce qui revient au même, si c est divisible par $a \wedge b$.

On vérifie à la main que ce couple est solution en utilisant le fait que (u, v) est solution, ou il suffit de constater que ce couple vérifie l'égalité $a(x - u) = b(v - y)$.

En effet, si $au + bv = a \wedge b$, alors $a'u + b'v = 1$, où $a' = \frac{a}{a \wedge b}$ et $b' = \frac{b}{a \wedge b}$. En d'autres termes, quand on a une relation de Bézout pour a et b , elle reste valide (avec les mêmes coefficients) pour a' et b' .

Finalement, $45 \wedge 75 = 15$ et 15 ne divise pas 20 donc l'équation n'a pas de solution.

Réolvons à présent l'équation $45x + 75y = 150$. Soit $(x, y) \in \mathbb{Z}^2$. Alors : $45x + 75y = 150 \iff 3x + 5y = 10$. Or :

$$\begin{aligned} 15 &= 45 - 30 \\ &= 45 - (75 - 45) \\ &= 2 \times 45 - 75 \end{aligned}$$

et donc $2 \times 3 - 5 = 1$ si bien que $20 \times 3 - 5 \times 10 = 10$: $(20, -10)$ est solution de l'équation.

$$\begin{aligned} (x, y) \text{ est solution de l'équation} &\iff 3x + 5y = 10 \\ &\iff 3x + 5y = 3 \times 20 - 5 \times 10 \\ &\iff 3(x - 20) = -5(y + 10) \end{aligned}$$

Supposons que (x, y) soit solution. Alors 3 divise $-5(y + 10)$ et $3 \wedge -5 = 1$ donc, d'après le théorème de Gauß, 3 divise $y + 10$ donc il existe $k \in \mathbb{Z}$ tel que $y + 10 = 3k$ i.e. $y = 3k - 10$ et donc $3(x - 20) = -15k$ si bien que $x = -5k + 20$. Réciproquement, tout couple de la forme $(-5k + 20, 3k - 10)$ est bien solution donc l'ensemble des solutions est $S = \{(-5k + 20, 3k - 10) \mid k \in \mathbb{Z}\}$.

I.4 PPCM

I.4.a PPCM de deux entiers naturels

Dans ce paragraphe, on ne travaille qu'avec des entiers naturels : le mot « entier » désignera un entier naturel. De plus, les entiers seront tous supposés non nuls, mais nous le dirons explicitement à chaque fois.

Définition. Soient a et b deux entiers non nuls. On appelle PPCM (plus petit commun multiple) de a et b le... plus petit multiple commun strictement positif de a et de b . On le note $a \vee b$.

Remarques :

- Quand on parle du plus petit multiple commun, c'est pour l'ordre naturel \leq dans \mathbb{N} , c'est-à-dire que tout multiple m commun strictement positif de a et de b vérifie $a \vee b \leq m$. En d'autres termes, $a \vee b = \min\{m \in \mathbb{N}^* \mid a \text{ divise } m \text{ et } b \text{ divise } m\}$.
- Ce minimum est bien défini car ab est un multiple commun strictement positif (car a et b le sont) de a et de b : en d'autres termes, l'ensemble $\{m \in \mathbb{N}^* \mid a \text{ divise } m \text{ et } b \text{ divise } m\}$ est non vide : c'est une partie non vide de \mathbb{N} donc admet un plus petit élément.
- En particulier, un PPCM est un entier strictement positif par définition : en d'autres termes, $a \vee b \geq 1$. On verra ci-dessous qu'il y a égalité si et seulement si $a = b = 1$.
- Si m est un entier strictement positif, un moyen simple (mais nous en verrons d'autres) de montrer que $m = a \vee b$ consiste à montrer que m est divisible par a et b et que tout multiple commun de a et b est supérieur ou égal à m .
- Les entiers a et b jouent le même rôle dans la définition donc $a \vee b = b \vee a$.
- Puisque 0 est multiple de tout entier, il faut exiger d'un PPCM qu'il soit strictement positif car si on exige simplement qu'il soit positif, alors le PPCM de deux entiers serait toujours nul et cette notion n'aurait pas un grand intérêt...
- Nous supposons a et b tous non nuls (et non pas non tous nuls comme pour le PGCD) car le seul multiple de 0 est 0 lui-même : si a ou b est nul, alors 0 est leur seul multiple commun, et on ne peut pas définir leur PPCM comme leur plus petit multiple commun strictement positif. Tout dépend ensuite des conventions : on définit parfois le PPCM de deux entiers dont l'un est nul comme égal à 0.

- Lorsqu'on veut sommer deux fractions, le PPCM des deux dénominateurs est un dénominateur commun. Cependant, attention : même si les deux fractions sont sous forme irréductible, en les sommant, l'écriture obtenue n'est pas forcément l'écriture irréductible car, une fois les deux fractions mises au même dénominateur, il peut y avoir une simplification possible avec le numérateur.

Il faut y penser avant de calculer : même si les deux fractions sont sous forme irréductible, en les sommant, l'écriture obtenue n'est pas forcément l'écriture irréductible car, une fois les deux fractions mises au même dénominateur, il peut y avoir une simplification possible avec le numérateur.

Exemple : Les seuls multiples strictement positifs de 8 inférieurs ou égaux à 24 sont 8, 16 et 24 et ceux de 12 sont 12 et 24 : 24 est le seul multiple commun strictement positif de 8 et 12 inférieur ou égal à 24, c'est donc leur PPCM car leurs autres multiples communs sont forcément supérieurs strictement à 24. Finalement, $8 \vee 12 = 24$. Cela permet par exemple de calculer facilement la somme suivante :

$$\begin{aligned} \frac{3}{8} + \frac{1}{12} &= \frac{9}{24} + \frac{2}{24} \\ &= \frac{11}{24} \end{aligned}$$



On n'a pas forcément $a \vee b = a \times b$! Cela n'est le cas que lorsque a et b sont premiers entre eux, voir ci-dessous.

On se donne dans la suite de ce paragraphe deux entiers a et b strictement positifs.

Proposition. $a \vee b \geq \max(a, b)$ avec égalité si et seulement si l'un des deux entiers divise l'autre. Plus précisément, $a \vee b = b$ si et seulement si $a \mid b$, et $a \vee b = a$ si et seulement si $b \mid a$.

DÉMONSTRATION. Puisque $a \vee b$ est un multiple non nul de a , alors $|a| = a \leq |a \vee b| = a \vee b$. Par symétrie des rôles, $b \leq a \vee b$, d'où l'inégalité.

Si $a \mid b$ alors b est un multiple commun à a et b donc $b \geq a \vee b$ et puisque $b \leq a \vee b$, on a l'égalité.

Réciproquement, si $a \vee b = b$ alors b est un multiple de a donc $a \mid b$. Par symétrie des rôles on a l'autre équivalence.

La proposition suivante donne un lien entre PPCM et PGCD :

Théorème. $(a \wedge b) \times (a \vee b) = a \times b$, c'est-à-dire que le produit du PGCD et du PPCM donne le produit des deux entiers.

Remarque : En particulier : $a \vee b = ab \iff a \wedge b = 1$.

DÉMONSTRATION. Notons $d = a \wedge b$ et $m = a \vee b$. $a \mid m$ donc il existe $k_1 \in \mathbb{Z}$ tel que $k_1 a = m$ si bien que

$$k_1 \times \frac{a}{d} = \frac{m}{d}$$

Or, a/d est un entier : on en déduit que m/d est divisible par a/d . Par symétrie des rôles, m/d est divisible par b/d . Or, a/d et b/d sont premiers entre eux donc :

$$\frac{a}{d} \times \frac{b}{d} \mid \frac{m}{d}$$

si bien que ab/d divise m . En particulier, $ab/d \leq m$. Or :

$$\frac{ab}{d} = a \times \frac{b}{d} = \frac{a}{d} \times b$$

□

En particulier, ab/d est un multiple commun de a et b donc $m \leq ab/d$, d'où le résultat.

Remarque : On retrouve le fait que $8 \vee 12 = 24$ car $8 \times 12 = 96$ et $8 \wedge 12 = 4$. Nous verrons encore une autre façon de calculer le PPCM dans le paragraphe II.3.c.



En particulier, $a \vee b = 1$ si et seulement si $a = b = 1$ (mais cela arrive assez peu en pratique). En effet, si l'un des deux est strictement supérieur à 1, alors $a \vee b \geq \max(a, b) > 1$. La réciproque est immédiate : si $a = b = 1$ alors tout entier strictement positif est multiple commun de a et b donc $a \vee b = 1$.



De façon équivalente :

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



Tous les entiers de cette démonstration sont strictement positifs.

Proposition. Soit $k \in \mathbb{N}^*$. Alors $(ka) \vee (kb) = k \times (a \vee b)$.

DÉMONSTRATION. D'après ce qui précède,

$$(ka) \vee (kb) = \frac{ka \times kb}{(ka) \wedge (kb)}$$

Or, $ka \times kb = k^2 \times ab$ et $(ka) \wedge (kb) = k \times (a \wedge b)$ d'après le paragraphe I.3.b donc

$$\begin{aligned} (ka) \vee (kb) &= \frac{k^2 ab}{k \times (a \wedge b)} \\ &= k \times \frac{ab}{a \wedge b} \\ &= k \times (a \vee b) \end{aligned}$$

□

I.4.b Extension aux entiers relatifs

Dans la suite, le mot « entier » désigne à nouveau un entier relatif. La définition du PPCM reste la même pour deux entiers (relatifs) :

Définition. Soient a et b deux entiers non nuls. On appelle PPCM (plus petit commun multiple) de a et b le... plus petit multiple commun strictement positif de a et de b . On le note $a \vee b$.

Remarque : Ce minimum est encore bien défini car $|a| \times |b|$ est un multiple commun de a et de b . On conclut que le min est bien défini comme précédemment. En particulier, $a \vee b$ est, par définition, un entier supérieur ou égal à 1 donc un entier strictement positif, même si a ou b est strictement négatif.

Proposition. Soient a et b deux entiers non tous nuls. Alors $a \vee b = \pm a \vee \pm b = |a| \vee |b|$.

DÉMONSTRATION. Immédiat puisque a et $-a$ (et donc $|a|$) ont les mêmes multiples, ainsi que b et $-b$ (et donc $|b|$).

Remarque : Par conséquent, tous les résultats du paragraphe précédent sont encore valables : il suffit pour cela de remplacer a par $|a|$ et b par $|b|$, ce qui ne change pas le PPCM.

- $a \vee b = b \vee a$.
- $a \vee b \geq \max(|a|, |b|)$ avec égalité si et seulement si l'un des deux divise l'autre. Plus précisément...
- $(a \wedge b) \times (a \vee b) = |a| \times |b|$.
- Si $k \in \mathbb{Z}^*$, alors $(ka) \vee (kb) = |k| \times (a \vee b)$.

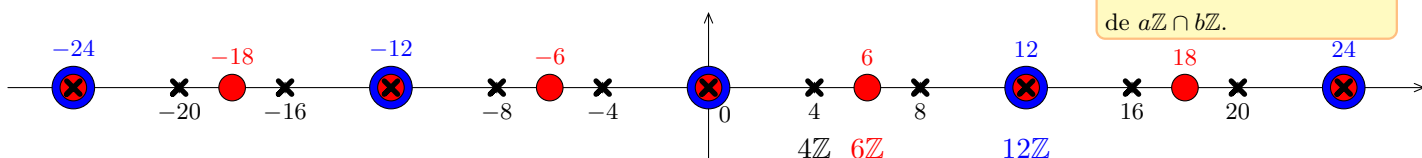
Proposition. Soit $m \in \mathbb{Z}$. Alors m est un multiple commun à a et b si et seulement si m est un multiple de $a \vee b$.

Remarques :

- En d'autres termes, l'ensemble des multiples communs de a et b est l'ensemble des multiples de $a \vee b$. En termes ensemblistes : $a\mathbb{Z} \cap b\mathbb{Z} = (a \vee b)\mathbb{Z}$. Cela se voit très bien sur le dessin ci-dessous : $4\mathbb{Z} \cap 6\mathbb{Z} = 12\mathbb{Z}$.

Si on ne sait plus s'il faut ou non une valeur absolue, il suffit de se demander le signe de la quantité qu'on manie, et qu'un PPCM ou un PGCD est positif.

On définit parfois le PPCM de cette manière, comme le plus petit élément strictement positif de $a\mathbb{Z} \cap b\mathbb{Z}$.



- Par conséquent, non seulement les multiples communs de a et b sont supérieurs au PPCM de a et b , mais en plus ils sont divisibles par le PPCM. Il en découle que le PPCM de a et b est aussi le plus petit diviseur de a et b au sens de la relation d'ordre divisibilité (c'est donc leur borne supérieure, cf. chapitre 16). Par exemple, il n'existe pas d'entiers a et b dont les multiples strictement positifs communs sont 8, 9, 10... Cependant, les multiples communs de 8 et 12 sont $\dots, -72, -48, -24, 0, 24, 48, 72 \dots$: on voit bien que le PPCM divise tous les multiples communs.

DÉMONSTRATION. Supposons que m soit un multiple commun à a et b . Effectuons la division euclidienne de m par $a \vee b$: il existe $(q, r) \in \mathbb{Z}^2$ tel que $m = q \times (a \vee b) + r$ avec $0 \leq r < a \vee b$. Les entiers m et $a \vee b$ sont divisibles par a et b donc $r = m - q \times (a \vee b)$ également. Si $r \neq 0$, alors r est un multiple strictement positif commun à a et b strictement inférieur à $a \vee b$ ce qui est absurde par définition du PPCM. Par conséquent, $r = 0$ donc $a \vee b$ divise m . La réciproque est immédiate.

Remarque : Nous reverrons cette méthode de démonstration dans le chapitre 18, quand nous montrerons que les sous-groupes de \mathbb{Z} sont les $n\mathbb{Z}$. Ce n'est pas étonnant : l'idée sous-jacente de la démonstration est les multiples communs à a et b forment un groupe. Ce genre de démonstration deviendra donc naturelle quand nous aurons les outils adéquats, i.e. dans le chapitre 18.

I.5 Extension à plus de deux entiers

Tous les résultats précédents peuvent aisément se généraliser à plus de deux entiers.

I.5.a PGCD

Définition. Soient $n \geq 2$ et $(a_1, \dots, a_n) \in \mathbb{Z}^n$ des entiers non tous nuls.

- On appelle PGCD de a_1, \dots, a_n le plus grand diviseur commun de a_1, \dots, a_n , et on le note $a_1 \wedge \dots \wedge a_n$.
- Si $a_1 \wedge \dots \wedge a_n = 1$, on dit que les a_i sont premiers entre eux **dans leur ensemble**.
- Si les a_i sont tous non nuls et si $a_i \wedge a_j = 1$ pour tous $i \neq j$, on dit que les a_i sont premiers entre eux **deux à deux**.

Remarques :

- On montre comme ci-dessus que ce PGCD est bien défini.
- En d'autres termes, des entiers sont premiers entre eux dans leur ensemble lorsqu'ils n'ont aucun diviseur commun positif autre que 1, et ils sont premiers entre eux deux à deux... quand ils sont premiers entre eux deux à deux. Par exemple, 15, 10 et 6 sont premiers entre eux dans leur ensemble mais ne sont pas premiers entre eux deux à deux. Plus fort : deux quelconques de ces entiers ne sont pas premiers entre eux car on a $15 \wedge 10 = 5$, $15 \wedge 6 = 3$ et $10 \wedge 6 = 2$.

Proposition. Soient a, b, c sont trois entiers non nuls. Alors :

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

On dit que le PGCD est associatif.

DÉMONSTRATION. Notons $d_1 = a \wedge (b \wedge c)$ et $d_2 = (a \wedge b) \wedge c$. d_1 divise a et $b \wedge c$ donc divise a , b et c donc $(a \wedge b)$ (un entier divise a et b si et seulement s'il divise leur PGCD) et c , si bien que d_1 est un diviseur commun à $a \wedge b$ et c donc $d_1 \leq d_2$. On montre l'autre inégalité de façon analogue. D'où la première égalité.

Notons $d_3 = a \wedge b \wedge c$. Nous avons déjà montré l'inégalité $d_1 \leq d_3$ car d_1 est un diviseur commun à a, b et c . Or, d_3 divise b et c donc d_3 divise $b \wedge c$, et d_3 divise a donc d_3 est un diviseur commun à a et $b \wedge c$ donc $d_3 \leq d_1$.

Remarque : On généralise aisément à un plus grand nombre d'entiers. Par conséquent, on peut calculer le PGCD d'un nombre quelconques d'entiers en calculant une succession de PGCD de deux entiers (s'il le faut, en appliquant plusieurs fois l'algorithme d'Euclide). Il est également inutile de s'embarrasser de parenthèses, mais on peut en mettre parfois pour bien se repérer dans les calculs.

Exemple : Vérifions que 15, 10 et 6 sont bien premiers entre eux dans leur ensemble :

$$\begin{aligned} 15 \wedge 10 \wedge 6 &= (15 \wedge 10) \wedge 6 \\ &= 5 \wedge 6 \\ &= 1 \end{aligned}$$

De même, calculons $d = 40 \wedge 60 \wedge 50 \wedge 100$.

$$\begin{aligned} d &= (40 \wedge 60) \wedge 50 \wedge 100 \\ &= (20 \wedge 50) \wedge 100 \\ &= 10 \wedge 100 \\ &= 10 \end{aligned}$$

Remarque : On a montré que $a \wedge b \wedge c$ divise $a \wedge b$. Là aussi, on généralise aisément à un plus grand nombre d'entiers (par exemple, $a \wedge b \wedge c \wedge d$ divise $a \wedge b \wedge c$ qui divise $a \wedge b$). En particulier :

Proposition. Soient a_1, \dots, a_n des entiers tous non nuls. Si les a_i sont premiers entre eux deux à deux, alors les a_i sont premiers entre eux dans leur ensemble.

DÉMONSTRATION. Pour tous $i \neq j$, $a_1 \wedge \dots \wedge a_n$ divise $a_i \wedge a_j = 1$ ce qui permet de conclure.

Remarque : En d'autres termes :

Premiers entre eux deux à deux \Rightarrow Premiers entre eux dans leur ensemble



Cependant, la réciproque est fausse ! Voir l'exemple de 10, 15 et 6 ci-dessus.

Tous les résultats précédents se généralisent au cas de n entiers par une récurrence immédiate et en utilisant l'associativité du PGCD. Plus précisément :

- On peut « supprimer » les entiers nuls sans changer le PGCD, c'est-à-dire que $a_1 \wedge \dots \wedge a_n$ est égal au PGCD des a_i non nuls.
- Le PGCD est encore commutatif.
- Si les a_i sont tous non nuls, $a_1 \wedge \dots \wedge a_n \leq \min(|a_1|, \dots, |a_n|)$ avec égalité si et seulement si un des a_i divise tous les autres.
- Le théorème de Bézout est encore vrai pour n entiers. De façon explicite :

Théorème (Théorème de Bézout). Soient $n \geq 1$ et a_1, \dots, a_n appartenant à \mathbb{Z} non tous nuls.

- Il existe $(u_1, \dots, u_n) \in \mathbb{Z}^n$ tel que $a_1 u_1 + \dots + a_n u_n = a_1 \wedge \dots \wedge a_n$.
- Plus généralement, si $m \in \mathbb{Z}$, il existe $(u_1, \dots, u_n) \in \mathbb{Z}^n$ tel que $a_1 u_1 + \dots + a_n u_n = m$ si et seulement si m est un multiple de $a_1 \wedge \dots \wedge a_n$.
- En particulier, a_1, \dots, a_n sont premiers entre eux **dans leur ensemble** si et seulement s'il existe $(u_1, \dots, u_n) \in \mathbb{Z}^n$ tel que $a_1 u_1 + \dots + a_n u_n = 1$.

On trouve des entiers u_1, \dots, u_n qui conviennent en appliquant plusieurs fois l'algorithme d'Euclide étendu. Par exemple, si on cherche u, v, w tels que $au + bv + cw = a \wedge b \wedge c$, on commence par trouver (grâce à l'algorithme d'Euclide étendu) x et y tels que

C'est-à-dire qu'être premiers entre eux deux à deux est plus fort qu'être premiers entre eux dans leur ensemble, ce qui est intuitif : premiers entre eux dans leur ensemble signifie que le seul diviseur positif commun à tous les a_i est 1, mais deux des a_i peuvent avoir d'autres diviseurs positifs, ce qui n'est pas possible lorsqu'ils sont premiers entre eux deux à deux.

En termes ensemblistes, si $d = (a_1 \wedge \dots \wedge a_n)$, alors :

$$a_1 \mathbb{Z} + \dots + a_n \mathbb{Z} = d\mathbb{Z}$$

En d'autres termes, on applique l'algorithme d'Euclide étendu à $a \wedge b$ et à c .

$$\begin{aligned}x \times (a \wedge b) + y \times c &= (a \wedge b) \wedge c \\ &= a \wedge b \wedge c\end{aligned}$$

et ensuite on trouve deux entiers z et t tels que $az + tb = a \wedge b$ si bien que

$$a \times (xz) + b \times (tx) + c \times y = a \wedge b \wedge c$$

On généralise aisément à un plus grand nombre d'entiers. Cela permet d'exhiber une solution particulière pour les équations diophantiennes du type


$$a_1x_1 + \dots + a_nx_n = m$$

où les a_i sont non nuls et où m est un multiple de $a_1 \wedge \dots \wedge a_n$.

Cependant, en pratique, on effectue rarement ce raisonnement pour plus de deux entiers car cela prend beaucoup de temps. Quand on a plus de deux entiers, on en général ce théorème simplement pour affirmer l'existence des entiers u_1, \dots, u_n , c'est-à-dire l'existence d'une relation de Bézout.

Continuons à donner les généralisations des résultats précédents :

- Si $k \in \mathbb{Z}^*$, alors $(ka_1) \wedge \dots \wedge (ka_n) = |k| \times (a_1 \wedge \dots \wedge a_n)$.
- Si a_1, \dots, a_n sont premiers avec un entier A , alors leur produit est premier avec A .
- Un entier divise $a_1 \wedge \dots \wedge a_n$ si et seulement s'il divise tous les a_i .
- Si $d = a_1 \wedge \dots \wedge a_n$, alors les entiers $a_1/d, \dots, a_n/d$ sont premiers entre eux **dans leur ensemble**.
- Si a_1, \dots, a_n sont premiers entre eux **deux à deux** et s'ils divisent un entier B , alors leur produit divise B .

Remarque :  Attention, le dernier résultat est faux si on suppose uniquement les entiers premiers entre eux dans leur ensemble. Par exemple, 10, 15 et 6 sont premiers entre eux dans leur ensemble et divisent 90 mais leur produit ne le divise pas. Cependant, dans l'avant-dernier, il est intuitif que les entiers sont premiers entre eux dans leur ensemble, puisqu'on divise par leur PGCD commun.

I.5.b PPCM (HP)

On définit de même le PPCM de n entiers non nuls. Il est aussi associatif ce qui permet de généraliser toutes les propriétés du paragraphe I.4 (par exemple, un entier est un multiple commun de tous les a_i si et seulement si c'est un multiple du PPCM) sauf une : l'égalité « $a \times b = (a \wedge b) \times (a \vee b)$ » ne se généralise pas à plus de 2 entiers. Par exemple, $6 \times 10 \times 15 \neq (6 \wedge 10 \wedge 15) \times (6 \vee 10 \vee 15)$!

II Nombres premiers

II.1 Définition, premiers exemples

Si $n \in \mathbb{Z}$, alors 1 et n divisent toujours n . Lorsque n est positif, lorsque ce sont ses seuls diviseurs positifs et lorsqu'ils sont distincts, on dit que n est premier. Plus précisément :

Définition. Soit $n \in \mathbb{N}^*$. On dit que n est premier lorsque n admet exactement deux diviseurs strictement positifs distincts : 1 et lui-même. Un nombre qui n'est pas premier est dit composé.

Remarque : Puisque les deux diviseurs positifs de n doivent être distincts, 1 n'est pas un nombre premier par définition.

Le thème de cette partie étant les nombres premiers qui sont des nombres strictement positifs, nous ne parlerons que de nombres strictement positifs. Par conséquent, les termes « entiers », « diviseurs » et « multiples » ne désigneront que des nombres strictement positifs.

Remarques :

- Par définition, un nombre est premier lorsque tous les entiers compris entre 2 et $n - 1$ ne divisent pas n . Un moyen simple (mais seulement efficace pour de petites valeurs de n) pour voir si un entier n est premier est de tester tous les entiers compris entre 2 et $n - 1$ et de voir si l'un d'eux divise n . Si aucun ne divise n , alors n est premier, et si l'un d'eux divise n , alors n n'est pas premier.
- En effet, par définition, un nombre n'est pas premier lorsqu'il admet un diviseur (positif) différent de 1 et de lui-même. Par exemple, 4 n'est pas premier car est divisible par 2 et 9 n'est pas premier car est divisible par 3.
- Plus généralement, si n n'est pas premier, alors il admet un diviseur strict a . Puisque $a \mid n$, n/a est un entier, qu'on note b . Puisque $a \neq 1$, $b \neq n$ et puisque $a \neq n$, $b \neq 1$. En conclusion, $n = ab$ avec a et b distincts de 1 et n , et la réciproque est immédiate, ce qui donne l'équivalence suivante, utile par exemple pour les raisonnements par l'absurde (cf. paragraphe II.4) :

Proposition. Soit $n \geq 1$. n n'est pas premier si et seulement s'il existe deux entiers a et b tels que $2 \leq a, b \leq n - 1$ et $n = a \times b$.

Exemples : Les nombres premiers inférieurs ou égaux à 30 sont 2, 3, 5, 7, 11, 13, 17, 19, 23 et 29. Les nombres 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30 sont pairs donc non premiers, $9 = 3 \times 3$, $15 = 3 \times 5$, $21 = 3 \times 7$, $25 = 5 \times 5$ et $27 = 3 \times 9$ ne sont pas premiers.

Remarque : Nous avons vu plus haut qu'un nombre n n'est pas premier si et seulement s'il existe a, b compris entre 2 et $n - 1$ tels que $n = ab$ (et cela peut s'avérer utile pour les raisonnements par l'absurde), mais on peut améliorer ce résultat.

Soit $n \geq 2$ qui n'est pas premier : il existe alors a et b compris entre 2 et $n - 1$ tels que $n = ab$. Supposons sans perte de généralité que $a \leq b$. Puisque b est un diviseur strict de n , alors $b \leq n/2$. En d'autres termes, n admet un diviseur inférieur ou égal à $n/2$ (et n'admet aucun diviseur compris strictement entre $n/2$ et n). Par conséquent, si on veut savoir si un entier est premier, inutile de s'intéresser à tous les entiers inférieurs ou égaux à $n - 1$ pour voir s'ils divisent n : il suffit de s'arrêter à $n/2$.

On peut même faire mieux ! Puisque $a \leq b$ alors $n = ab \geq a^2$ et donc $a \leq \sqrt{n}$. En d'autres termes, n admet un diviseur inférieur ou égal à \sqrt{n} . La réciproque étant immédiate par définition d'un nombre composé :

Proposition. Soit $n \geq 2$. Alors n est composé si et seulement s'il admet un diviseur $2 \leq d \leq \sqrt{n}$.

On en déduit un test de primalité un peu plus efficace que « regarder tous les entiers entre 2 et $n - 1$ » et même « regarder tous les entiers entre 2 et $n/2$ » : il suffit de regarder tous les entiers entre 2 et \sqrt{n} . On peut même se contenter d'examiner les nombres premiers car nous montrerons dans le paragraphe II.3 que n est composé si et seulement s'il admet un diviseur premier $2 \leq p \leq \sqrt{n}$: si aucun ne divise n , alors n est premier. Par exemple, $10 < \sqrt{113} < 11$ donc 113 est premier car il n'est divisible ni par 2, ni par 3, ni par 5, ni par 7 qui sont les seuls nombres premiers inférieurs à $\sqrt{113}$. Comme on peut le voir, ce test est assez efficace à la main jusqu'à 400 environ (car il suffit d'examiner les nombres premiers inférieurs ou égaux à 20), et avec une machine on peut aller plus loin (jusqu'à 10^6 par exemple), au-delà il faut des tests plus efficaces.

Donnons une méthode (peu efficace mais intéressante tout de même pour de petites valeurs, et aussi intéressante théoriquement et culturellement) pour donner tous les nombres premiers inférieurs ou égaux à un certain entier n .

Un diviseur strict de n est un diviseur de n distinct de 1 et de n . De même, un multiple strict de n est un multiple de n distinct de n ou, ce qui revient au même puisqu'on ne manipule que des entiers strictement positifs, un multiple de n strictement supérieur à n .

Et puisque d est entier, on peut même remplacer \sqrt{n} par $\lfloor \sqrt{n} \rfloor$.

Mais cela commence à être difficile : par exemple, il n'est pas immédiat de dire de tête si un nombre est divisible par 17 ou non.

Crible d'Eratosthène : Le crible d'Eratosthène est une méthode simple pour prouver qu'un nombre est premier ou pour donner tous les nombres premiers inférieurs à un certain entier n .

En faisant varier n , cela donne une méthode simple pour obtenir tous les nombres premiers, en théorie uniquement, car c'est beaucoup trop long pour de grandes valeurs de n .

- On écrit tous les entiers de 2 à n .
- On entoure 2 qui est premier.
- On barre tous les multiples de 2, sauf 2, car ils ne sont pas premiers (car divisibles par 2).
- On entoure 3 qui est premier.
- On barre tous les multiples de 3, sauf 3, qui ne sont pas encore barrés car ils ne sont pas premiers (car divisibles par 3).
- On réitère l'expérience : on entoure à chaque fois le premier nombre restant non barré qui est donc premier (il n'est divisible par aucun nombre strictement inférieur, sinon il serait barré) et on barre tous ses multiples stricts, qui ne sont donc pas premiers.
- On continue jusqu'à arriver à n . Les nombres entourés sont premiers, les nombres barrés ne le sont pas (on les a barrés car ce sont des multiples stricts d'un nombre donc ils admettent un diviseur strict).
- Il est même inutile d'aller jusqu'à n : d'après ce qui précède, on peut s'arrêter à \sqrt{n} (ou plutôt à sa partie entière), les nombres non barrés après cette valeur sont premiers (car, sinon, il admettraient un diviseur inférieur à \sqrt{n} et donc seraient barrés).

Ci-dessous, appliquons la méthode du crible d'Eratosthène pour donner les nombres premiers inférieurs à 100 :

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

Remarque : 2 est un nombre premier car ses seuls diviseurs sont 1 et 2. C'est le seul nombre premier pair car si n est un nombre pair différent de 2, il est divisible par 2 donc admet un diviseur qui n'est ni 1 ni lui-même donc n'est pas premier. En d'autres termes : les nombres premiers sont tous impairs à part 2. Évidemment, la réciproque est fausse car 9 est impair non premier. 2 est donc un nombre premier à part, et certaines propriétés sont vraies pour tous les nombres premiers sauf 2. Par conséquent, certains énoncés commencent par : « Soit p un nombre premier supérieur ou égal à 3 » ou, ce qui revient au même : « Soit p un nombre premier impair ».

Ce qui fait dire aux anglosaxons : « 2 is the oddest prime number ».

II.2 Infinitude de l'ensemble des nombres premiers

Lemme. Soit $n \geq 2$. Alors n admet un diviseur premier.

DÉMONSTRATION. Par récurrence (forte) sur n .

- Si $n \geq 2$, notons H_n : « n admet un diviseur premier ».
- H_2 est vraie car 2 admet un diviseur premier (2 lui-même).
- Soit $n \geq 2$. Supposons H_2, \dots, H_n vraies et montrons que H_{n+1} est vraie. Si $n+1$ est premier, alors il admet un diviseur premier (lui-même). Sinon, $n+1$ admet un diviseur strict a i.e. vérifiant $2 \leq a \leq n$. Par hypothèse de récurrence, H_a est vraie donc a admet un diviseur premier p . $p \mid a$ et $a \mid n+1$ donc $p \mid n+1$: $n+1$ admet un diviseur premier, H_{n+1} est vraie.

- D'après le principe de récurrence, H_n est vraie pour tout $n \geq 2$.

Remarque : Nous pouvons à présent prouver le résultat affirmé plus haut : si n est composé, alors n admet un diviseur d vérifiant $2 \leq d \leq \sqrt{n}$. D'après le lemme, d admet un diviseur premier p . $p \mid d$ donc $p \leq d$ si bien que $2 \leq p \leq \sqrt{n}$: n admet un diviseur premier inférieur à \sqrt{n} (et la réciproque est immédiate).

Notation : On note \mathbb{P} l'ensemble des nombres premiers.

Proposition. \mathbb{P} est infini.

DÉMONSTRATION. Supposons que \mathbb{P} soit fini et notons ses éléments p_1, \dots, p_n . Posons $N = p_1 \times \dots \times p_n + 1$. N admet un diviseur premier donc il existe i tel que p_i divise N . Or, p_i divise $p_1 \times \dots \times p_n$ donc p_i divise $N - p_1 \times \dots \times p_n = 1$, ce qui est absurde car $p_i \geq 2 > 1$.

Remarque : C'est une méthode que nous verrons souvent (par exemple dans l'exercice 74) : si on veut un nombre divisible par des entiers, on fait le produit de tous ces entiers. Ensuite, si on cherche un nombre que ces entiers ne divisent pas, il suffit d'ajouter un nombre qu'ils ne divisent pas (par exemple 1), et si on cherche plutôt un nombre qu'ils divisent, on ajoute un nombre qu'ils divisent. Pourquoi alors ne pas simplement donner le nombre que ces entiers divisent (ou ne divisent pas) ? Car on cherche en général un entier très grand (ou plus grand qu'un certain nombre donné). Donnons un exemple d'utilisation de cette méthode.

Exemple : Soit $n \geq 1$. Donnons n nombres consécutifs non premiers.

Cherchons le point de départ des ces n nombres consécutifs. Soit $N \in \mathbb{N}$. On se demande si on peut choisir N tel que $N + 1, N + 2, N + 3, \dots, N + n$ ne soient pas premiers.

Pour que $N + 2$ ne soit pas premier, il suffit que N soit divisible par 2 (car $N + 2$ est alors divisible par 2). De même, pour que $N + 3$ ne soit pas premier, il suffit que N soit divisible par 3, etc. On cherche donc un entier N divisible par $2, 3, \dots, n$: posons $N = 2 \times \dots \times n = n!$, qui est bien divisible par $2, 3, \dots, n$.

Aucun diviseur $n! + 1$ ne saute aux yeux. Cependant, $n! + 2$ n'est pas premier car est divisible par 2, $n! + 3$ n'est pas premier car est divisible par 3, et ainsi de suite jusque $n! + n$ qui n'est pas premier car est divisible par n . Cela donne $n - 1$ nombres consécutifs non premiers. On en demande n : il suffit de recommencer en partant de $(n + 1)!$. Plus précisément, $(n + 1)! + 2, \dots, (n + 1)! + (n + 1)$ sont n nombres consécutifs non premiers.

Remarques :

- On peut donc trouver des familles (finies) de nombres consécutifs non premiers arbitrairement longues, mais il faut aller loin pour les trouver. Le postulat de Bertrand (cf. DS n° 2 de l'an dernier) dit que, pour tout n , il existe un nombre premier p compris entre n et $2n$: il ne peut pas y avoir d'intervalles trop grands sans nombres premiers, à moins de manipuler des nombres énormes.
- Aucun diviseur de $n! + 1$ ne saute aux yeux mais cela ne veut pas forcément dire qu'il est premier. Par exemple, $4! + 1 = 25$ n'est pas premier. Cependant, son seul facteur premier est $5 > 4$. Plus généralement, pour tout $n \geq 2$, si p est un facteur premier de $n! + 1$ (un tel facteur premier existe forcément, voir ci-dessus), alors $p > n$: en effet, si $p \leq n$, alors p divise $n!$ donc p divise 1 ce qui est absurde. En particulier : pour tout $n \geq 2$, il existe p premier strictement supérieur à n . C'est une autre façon de démontrer qu'il existe une infinité de nombres premiers !
- Encore une autre façon (mais celle-ci est analogue à la première) de prouver que \mathbb{P} est infini consiste à raisonner par l'absurde, à écrire $\mathbb{P} = \{p_1; \dots; p_n\}$ avec $p_1 < \dots < p_n$ puis à montrer comme ci-dessus que $(p_n)! + 1$ n'admet pas de diviseur premier, ce qui est absurde.

C'est-à-dire qu'il existe une infinité de nombres premiers.

Rappelons que si $a \mid b$ et si $b \neq 0$ alors $|a| \leq |b|$.

Un nombre premier de la forme $n! + 1$ ou plus généralement de la forme $n! \pm 1$ est appelé un nombre premier factoriel : l'existence d'une infinité de nombres premiers factoriels est encore un problème ouvert. Par exemple, $5! + 1$ n'est pas premier, mais $11! + 1$ est premier. Cependant, même s'ils ne sont pas premiers, ces nombres sont utiles car leurs facteurs premiers sont « grands ».

II.3 Décomposition en produit de facteurs premiers

II.3.a Théorème fondamental

Lemme. Soit p un nombre premier.

1. Soit $n \geq 2$. Si $p \mid n$, alors $p \wedge n = p$, sinon $p \wedge n = 1$.
2. Soient $n \geq 1$ et (a_1, \dots, a_n) des entiers supérieurs ou égaux à 2. Si p divise le produit $a_1 \times \dots \times a_n$, alors p divise l'un des a_i .
3. Soit ρ un nombre premier, soit $\beta \geq 1$. Alors : $p \mid \rho^\beta \iff p = \rho$.

En particulier, $p \wedge n = 1$ si et seulement si p ne divise pas n .

DÉMONSTRATION. 1. Soit $d = p \wedge n$. Alors $d \mid p$. Or, les seuls diviseurs positifs de p sont 1 et p car p est premier. Par conséquent, $d = 1$ ou $d = p$. Si $p \mid n$ alors $d = p$ (cf. paragraphe I.3.a) et sinon $d \neq p$ donc $d = 1$.

2. Supposons que p ne divise aucun a_i . Alors p est premier avec tous les a_i d'après ce qui précède, donc avec leur produit, donc ne divise pas leur produit. D'où le résultat par contraposée.
3. Supposons que p divise ρ^β . D'après ce qui précède (avec a_1, \dots, a_β tous égaux à ρ), p divise ρ . Or, ρ est premier donc ses seuls diviseurs positifs sont 1 et ρ si bien que $p = \rho$. La réciproque est immédiate.

On pouvait aussi raisonner par récurrence et utiliser le théorème de Gauß : exo.

Théorème (Décomposition en produit de facteurs premiers). Soit $n \geq 2$. Il existe $r \geq 1$, p_1, \dots, p_r premiers distincts et $\alpha_1, \dots, \alpha_r$ supérieurs ou égaux à 1 tels que :

$$n = p_1^{\alpha_1} \times \dots \times p_r^{\alpha_r}$$

De plus, cette écriture est unique (à l'ordre près des termes).

Remarque : En d'autres termes, tout entier $n \geq 2$ s'écrit comme un produit de nombres premiers. Une telle écriture est appelée écriture ou décomposition de n en produit de facteurs premiers (et elle est donc unique, à l'ordre près des termes). On peut donc voir les nombres premiers comme « des briques » à l'aide desquelles on construit tous les entiers supérieurs ou égaux à 2. Dans le même genre, Paul Erdős disait qu'un « nombre premier est un nombre qui ne se casse pas en tombant par terre ».

DÉMONSTRATION. Existence : Par récurrence sur n .

- Si $n \geq 2$, notons H_n : « n peut s'écrire comme un produit de facteurs premiers ».
- H_2 est vraie car 2 est premier.
- Soit $n \geq 2$. Supposons H_2, \dots, H_n vraies et prouvons que H_{n+1} est vraie. Si $n+1$ est premier, alors il s'écrit comme un produit (à un terme) de facteurs premiers. Si $n+1$ n'est pas premier, alors il existe a et b appartenant à $\llbracket 2; n \rrbracket$ tels que $n+1 = a \times b$. Par hypothèse de récurrence, H_a et H_b sont vraies donc a et b peuvent s'écrire comme un produit de facteurs premiers, et puisque $n+1 = a \times b$, $n+1$ également : H_{n+1} est vraie.
- D'après le principe de récurrence, H_n est vraie pour tout $n \geq 2$.

Nous avons déjà fait cette récurrence dans le chapitre 1.

Dès lors, tout entier n s'écrit comme un produit de nombres premiers, et en regroupant les nombres premiers égaux, on a bien l'existence d'une écriture comme celle de l'énoncé du théorème.

Unicité : Soit $q \geq 1$, (ρ_1, \dots, ρ_q) premiers distincts et $(\beta_1, \dots, \beta_q)$ supérieurs ou égaux à 1 tels que $n = p_1^{\alpha_1} \times \dots \times p_r^{\alpha_r} = \rho_1^{\beta_1} \times \dots \times \rho_q^{\beta_q}$.

Soit $i \in \llbracket 1; r \rrbracket$. Alors $p_i \mid n$ donc $p_i \mid \rho_1^{\beta_1} \times \dots \times \rho_q^{\beta_q}$. D'après le lemme, il existe $j \in \llbracket 1; q \rrbracket$ tel que $p_i \mid \rho_j^{\beta_j}$ et donc tel que $p_i = \rho_j$ (toujours d'après le lemme). En d'autres

termes, les nombres premiers p_1, \dots, p_r font partie des nombres premiers ρ_1, \dots, ρ_q donc, en particulier, $r \leq q$. Par symétrie des rôles, $q \leq r$ donc $q = r$. Dès lors, les ρ_j sont exactement les p_i donc, quitte à changer l'ordre des termes, on peut supposer que $p_1 = \rho_1, \dots, p_r = \rho_r$ (puisque $q = r$).

Supposons que $\alpha_1 \neq \beta_1$. Sans perte de généralité, supposons que $\alpha_1 > \beta_1$ et posons $m = n/p_1^{\beta_1}$. Dès lors :

$$m = p_1^{\alpha_1 - \beta_1} \times p_2^{\alpha_2} \dots \times p_r^{\alpha_r} = p_2^{\beta_2} \dots \times p_r^{\beta_r} \quad \square$$

Rappelons que $r = q$ et que $p_i = \rho_i$ pour tout i .

À l'aide de l'expression de gauche, puisque $\alpha_1 - \beta_1 > 0$, p_1 divise m donc divise l'expression de droite donc il existe $i \geq 2$ tel que p_1 divise $p_i^{\alpha_i}$ donc tel que $p_1 = p_i$ (toujours d'après le lemme), ce qui est absurde puisque les p_i sont distincts. En conclusion, $\alpha_1 = \beta_1$, et par symétrie des rôles, $\alpha_i = \beta_i$ pour tout i . D'où l'unicité.

Exemples : $60 = 2^2 \times 3 \times 5$, $1000 = 2^3 \times 5^3$, $2020 = 2^2 \times 5 \times 101$, $2021 = 23 \times 47$, $2022 = 2 \times 3 \times 337$, $2023 = 7 \times 17^2$.

Notation : Dans la suite, sauf indication contraire, quand nous écrirons « soit $p_1^{\alpha_1} \times \dots \times p_r^{\alpha_r}$ la décomposition de n en produit de facteurs premiers », ou « notons $n = p_1^{\alpha_1} \times \dots \times p_r^{\alpha_r}$ », cela signifiera que r est un entier supérieur ou égal à 1, que p_1, \dots, p_r sont des nombres premiers **distincts** et que les α_i sont aussi des entiers **supérieurs ou égaux à 1**. De plus, quand nous dirons qu'un nombre premier p apparaît dans cette décomposition, cela signifiera qu'un des p_i est égal à p .

Application : Redémontrons que $\sqrt{2}$ est irrationnel. Supposons que $\sqrt{2} \in \mathbb{Q}$ et écrivons $\sqrt{2}$ sous forme irréductible, c'est-à-dire qu'on écrit $\sqrt{2} = a/b$ avec $a, b \in \mathbb{N}^*$ (car $\sqrt{2} > 0$) premiers entre eux. Alors $a^2 = 2b^2$. Notons $a = p_1^{\alpha_1} \times \dots \times p_r^{\alpha_r}$. Alors $a^2 = p_1^{2\alpha_1} \times \dots \times p_r^{2\alpha_r}$. En d'autres termes, toutes les puissances de la décomposition de a^2 en produit de facteurs premiers sont paires, et c'est la même chose pour b^2 . C'est absurde car la puissance de 2 dans la décomposition de a^2 en facteurs premiers vaut 1+ la puissance de 2 dans celle de b^2 donc est impaire. En conclusion, $\sqrt{2}$ est irrationnel.

Éventuellement nulles si le nombre premier en question n'apparaît pas dans la décomposition.

II.3.b Une notation bien pratique

Définition. Soit $\alpha = (\alpha_p)_{p \in \mathbb{P}}$ une famille d'éléments de \mathbb{N} indexée par \mathbb{P} . On dit que α est une famille presque nulle si tous les α_p sont nuls sauf un nombre fini. On appelle alors support de α , noté $\text{supp}(\alpha)$, l'ensemble $\{p \mid \alpha_p \neq 0\}$, c'est-à-dire l'ensemble des indices p pour lesquels $\alpha_p \neq 0$.

Nous verrons les suites presque nulles dans le chapitre 19.

Définition. Soit $\alpha = (\alpha_p)_{p \in \mathbb{P}}$ une famille d'éléments de \mathbb{N} presque nulle indexée par \mathbb{P} . On pose :

$$\prod_{p \in \mathbb{P}} p^{\alpha_p} = \prod_{p \in \text{supp}(\alpha)} p^{\alpha_p}$$

Remarque : Cette définition est intuitive : on a envie de définir le produit des p^{α_p} , pour tout p premier. Le problème est que l'ensemble des nombres premiers est infini, et on ne sait définir un produit que pour un nombre fini de termes. Cependant, puisqu'il n'y a qu'un nombre fini de α_p non nul, on définit le produit pour tous les nombres premiers comme le produit pour tous les p du support, c'est-à-dire le produit sur tous les nombres p tels que $\alpha_p \neq 0$.

Cette définition est conforme à l'intuition : les autres nombres premiers p vérifie $\alpha_p = 0$ et donc $p^{\alpha_p} = 1$: ces termes ne changeront pas la valeur du produit et donc on ne les prend pas en compte pour la définition du produit. En d'autres termes : dans la définition du produit infini, on ne prend en compte que les termes (en nombre fini) qui apportent une vraie contribution, c'est-à-dire les termes différents de 1.

Si le support de α est vide, c'est-à-dire si tous les termes sont nuls, le produit est alors indexé par l'ensemble vide donc vaut 1 par convention, cf. chapitre 3.

Proposition. Soient $\alpha = (\alpha_p)_{p \in \mathbb{P}}$ et $\beta = (\beta_p)_{p \in \mathbb{P}}$ deux familles d'éléments de \mathbb{N} presque nulles indexées par \mathbb{P} . Alors $\alpha + \beta = (\alpha_p + \beta_p)_{p \in \mathbb{P}}$ est une famille presque nulle d'éléments de \mathbb{N} indexée par \mathbb{P} , et

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

En d'autres termes : on peut manipuler cette nouvelle notation comme un produit classique.

DÉMONSTRATION. Le fait que $\alpha + \beta$ est une famille d'éléments de \mathbb{N} est immédiat. Montrons qu'elle est presque nulle. Soit $p \in \mathbb{P}$. Puisque α_p et β_p sont positifs (ce sont des éléments de \mathbb{N}) : $\alpha_p + \beta_p \neq 0 \iff \alpha_p \neq 0$ ou $\beta_p \neq 0$. En d'autres termes : $\text{supp}(\alpha + \beta) = \text{supp}(\alpha) \cup \text{supp}(\beta)$. Or (cf. chapitre 17), l'union de deux ensembles finis est un ensemble fini donc $\text{supp}(\alpha + \beta)$ est fini : $\alpha + \beta$ est une famille presque nulle, et :

$$\begin{aligned} \prod_{p \in \mathbb{P}} p^{\alpha_p + \beta_p} &= \prod_{p \in \text{supp}(\alpha + \beta)} p^{\alpha_p + \beta_p} \\ &= \prod_{p \in \text{supp}(\alpha + \beta)} p^{\alpha_p} \times \prod_{p \in \text{supp}(\alpha + \beta)} p^{\beta_p} \end{aligned}$$

Or, $\text{supp}(\alpha) \subset \text{supp}(\alpha + \beta)$ si bien que :

$$\begin{aligned} \prod_{p \in \text{supp}(\alpha + \beta)} p^{\alpha_p} &= \prod_{p \in \text{supp}(\alpha)} p^{\alpha_p} \times \prod_{p \in \text{supp}(\alpha + \beta) \setminus \text{supp}(\alpha)} p^{\alpha_p} \\ &= \prod_{p \in \mathbb{P}} p^{\alpha_p} \times 1 \end{aligned}$$

Tous les termes du deuxième produit valent 1 car les puissances sont nulles, par définition du support. \square

En d'autres termes, $\prod_{p \in \text{supp}(\alpha + \beta)} p^{\alpha_p} = \prod_{p \in \mathbb{P}} p^{\alpha_p}$. Par symétrie des rôles, $\prod_{p \in \text{supp}(\alpha + \beta)} p^{\beta_p} = \prod_{p \in \mathbb{P}} p^{\beta_p}$, d'où le résultat.

II.3.c Valuation p -adique

La décomposition en produit de facteurs premiers permet de donner des CNS simples et faciles à visualiser pour qu'un entier en divise un autre, pour qu'un entier soit un carré, un cube etc. ou pour que deux entiers soient premiers entre eux.

Définition. Soit $n \geq 2$, soit p un nombre premier. On appelle valuation p -adique de n , notée $v_p(n)$, la puissance de p dans la décomposition en produit de facteurs premiers de n (avec la convention $v_p(n) = 0$ si p n'apparaît pas dans cette décomposition).

La valuation p -adique de n est bien définie par unicité de la décomposition.

Exemple : $v_2(60) = 2$, $v_3(60) = v_5(60) = 1$ et, si $p \neq 2, 3, 5$, alors $v_p(60) = 0$.

Remarque : Si p est premier et $k \in \mathbb{N}$, alors $v_p(p^k) = k$.

Remarque : Tout entier $n \geq 2$ s'écrit sous la forme suivante :

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

Ce produit est bien défini car la famille $(v_p(n))_{p \in \mathbb{P}}$ est une famille presque nulle d'éléments de \mathbb{N} : elle contient en effet un nombre fini de termes non nuls d'après le dernier théorème du paragraphe II.3.a. L'unicité dans ce théorème se reformule alors de la façon suivante :

Proposition (Unité de la décomposition en produit de facteurs premiers).

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

Remarque : L'écriture $n = \prod_{p \in \mathbb{P}} p^{v_p(n)}$ est tout à fait équivalente à l'écriture $n = p_1^{\alpha_1} \times \dots \times p_r^{\alpha_r}$ (elles sont d'ailleurs égales par définition de ce produit) et donc elle est aussi appelée la décomposition de n en produit de facteurs premiers. Cependant, attention : dans ce produit, toutes les puissances sont nulles, sauf un nombre fini, contrairement à la décomposition de n en produit de facteurs premiers vue dans le paragraphe II.3.a dans laquelle les puissances sont toutes non nulles (les autres nombres premiers n'apparaissant pas).

Nous allons voir que cette écriture est très pratique pour tout ce qui concerne les puissances, mais elle est parfois moins pratique que l'écriture $n = p_1^{\alpha_1} \times \dots \times p_r^{\alpha_r}$ car les facteurs premiers de n n'apparaissent pas de façon immédiate : ce sont ceux pour lesquels $v_p(n) \neq 0$. On manipulera tantôt une écriture, tantôt l'autre, selon les situations, chacune ayant ses avantages et ses inconvénients.

Proposition. Soient a et b supérieurs ou égaux à 2 et p premier. Alors $v_p(a \times b) = v_p(a) + v_p(b)$. En particulier, pour tout $k \in \mathbb{N}$, $v_p(a^k) = k \times v_p(a)$.

DÉMONSTRATION. Il suffit de voir que $ab = \prod_{p \in \mathbb{P}} p^{v_p(a) + v_p(b)}$ et on conclut par unicité de la décomposition en produit de facteurs premiers, comme dit ci-dessus. La deuxième partie en découle par récurrence immédiate.

Remarque : Il peut être fastidieux d'écrire plusieurs fois « la puissance de ... dans la décomposition de ... en facteurs premiers », surtout qu'on a maintenant un outil pour ça : la valuation p -adique ! Reprenons la démonstration de l'irrationalité ci-dessus avec la valuation 2-adique. $v_2(a^2) = 2v_2(a)$ donc est un nombre pair, mais :

$$\begin{aligned} v_2(a^2) &= v_2(2b^2) \\ &= v_2(2) + v_2(b^2) \\ &= v_2(2) + 2v_2(b) \\ &= 1 + 2v_2(b) \end{aligned}$$

On rappelle que $v_p(ab) = v_p(a) + v_p(b)$.

donc $v_2(a^2)$ est un nombre impair et on conclut de la même façon. C'est exactement la même démonstration, mais la valuation p -adique donne des calculs plus courts et permet une rédaction moins lourde. Elle est cependant moins intuitive et plus difficile à visualiser que « la puissance de ... dans la décomposition de ... en facteurs premiers ». À voir avec quelle notion on se sent le plus à l'aise !

Exemple : Montrons que $x = \sqrt[3]{\frac{4}{5}}$ est un irrationnel.

Supposons que $x \in \mathbb{Q}$: il existe a et b appartenant à \mathbb{N}^* premiers entre eux tels que $x = a/b$ si bien que $5a^3 = 4b^3$. Par conséquent,

$$\begin{aligned} v_2(5a^3) &= v_2(5) + 3v_2(a) \\ &= 3v_2(a) \end{aligned}$$

c'est-à-dire que $v_2(5a^3)$ (la puissance de 2 dans la décomposition de $5a^3$ en facteurs premiers) est divisible par 3, mais on a également

$$\begin{aligned} v_2(5a^3) &= v_2(4b^3) \\ &= v_2(4) + 3v_2(b) \\ &= 2 + 3v_2(b) \end{aligned}$$

et donc n'est pas divisible par 3 (car s'écrit sous la forme $3q + 2$ donc le reste dans la division euclidienne par 3 est 2), ce qui est absurde. On aurait pu aussi (exo) travailler avec la valuation 5-adique.

Remarquons que dans ces deux exemples, le fait que a et b soient premiers entre eux est inutile.

On le voit également en écrivant la décomposition de a en facteurs premiers, et en la mettant au cube : toutes les puissances sont divisibles par 3, et en multipliant par 5, cela ne change pas la puissance de 2.

Proposition. Soient a et b supérieurs ou égaux à 2. Alors $a \mid b$ si et seulement si, pour tout p premier, $v_p(a) \leq v_p(b)$.

Exemple : $17325 = 3^2 \times 5^2 \times 7 \times 11$ et $495 = 3^2 \times 5 \times 11$ donc $495 \mid 17325$.

DÉMONSTRATION. Supposons que $a \mid b$: si $a = b$ alors le résultat est immédiat. Sinon, il existe m supérieur ou égal à 2 tel que $b = am$. Soit $p \in \mathbb{P}$. Alors $v_p(b) = v_p(a) + v_p(m)$ et $v_p(m) \geq 0$ donc $v_p(b) \geq v_p(a)$.

Réciproquement, supposons que, pour tout $p \in \mathbb{P}$, $v_p(a) \leq v_p(b)$ et posons $m = \prod_{p \in \mathbb{P}} p^{v_p(b) - v_p(a)}$.

Alors $m \in \mathbb{N}^*$ et $b = am$, d'où l'équivalence.

Remarque : On sépare les cas $a = b$ et $a \neq b$ car, si $a = b$, alors $m = b/a = 1$ n'a pas de décomposition en produit de facteurs premiers, mais on pourrait lui en donner une en écrivant

$$1 = \prod_{p \in \mathbb{P}} p^0$$

et donc en posant $v_p(1) = 0$ pour tout p : le reste de la preuve serait alors le même.

Corollaire. Soient $n \geq 2$, $k \in \mathbb{N}$ et p un nombre premier. Alors : $p^k \mid n \iff k \leq v_p(n)$, c'est-à-dire que p^k divise n si et seulement si p apparaît dans la décomposition de n en produit de facteurs premiers avec une puissance supérieure ou égale à k . En particulier :

- $v_p(n) = \max\{k \mid p^k \text{ divise } n\}$.
- $p \mid n \iff v_p(n) \geq 1$.


Proposition. Soient a et b supérieurs ou égaux à 2. Alors :

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

DÉMONSTRATION. Notons $d = \prod_{p \in \mathbb{P}} p^{\min(v_p(a), v_p(b))}$. Pour tout $p \in \mathbb{P}$,

$$v_p(d) = \min(v_p(a), v_p(b)) \leq v_p(a) \quad \square$$

donc, d'après la proposition précédente, d divise a . Par symétrie des rôles, d divise b donc d est un diviseur commun à a et b . Si d' est un diviseur commun à a et b alors, pour tout $p \in \mathbb{P}$, $v_p(d') \leq v_p(a)$ et $v_p(d') \leq v_p(b)$ donc $v_p(d') \leq \min(v_p(a), v_p(b)) = v_p(d)$: on en déduit que d' divise d : d est un diviseur commun à a et b et est divisible par tous les diviseurs communs à a et b donc $d = a \wedge b$. L'autre égalité se démontre de façon analogue et est laissée en exo.

Remarque :  En d'autres termes, si $a = p_1^{\alpha_1} \times \dots \times p_r^{\alpha_r}$ et $b = p_1^{\beta_1} \times \dots \times p_q^{\beta_q}$:

- $a \wedge b$ est le produit des facteurs premiers apparaissant à la fois dans la décomposition de a et dans celle de b , mis à la puissance qui est **la plus petite des deux**.
- $a \vee b$ est le produit de tous les facteurs premiers apparaissant dans la décomposition de a ou dans celle de b , mis à la puissance qui est **la plus grande des deux**.

Exemple : $600 = 2^3 \times 3 \times 5^2$ et $740 = 2^2 \times 5 \times 37$ donc $600 \wedge 740 = 2^2 \times 5 = 20$ et $600 \vee 740 = 2^3 \times 3 \times 5^2 \times 37 = 22200$.

Remarque : Si $p \in \mathbb{P}$, alors $\min(v_p(a), v_p(b)) + \max(v_p(a), v_p(b)) = v_p(a) + v_p(b)$ (exo, distinguer les cas selon que $v_p(a) \leq v_p(b)$ ou le contraire). Par conséquent,

En d'autres termes, a divise p si et seulement si tous les facteurs premiers de la décomposition de a en facteurs premiers sont aussi des facteurs premiers de b , et apparaissent dans la décomposition de a avec une puissance plus petite.

En d'autres termes, un nombre premier divise un entier si et seulement s'il apparaît dans sa décomposition en produit de facteurs premiers.

$$(a \wedge b) \times (a \vee b) = \prod_{p \in \mathbb{P}} p^{v_p(a)+v_p(b)}$$

On retrouve bien le fait que $(a \wedge b) \times (a \vee b) = a \times b$, et on voit également que cela ne se généralise pas à plus de deux entiers, car $\min(v_p(a), v_p(b), v_p(c)) + \max(v_p(a), v_p(b), v_p(c)) \neq v_p(a) + v_p(b) + v_p(c)$ en général.

Corollaire. Soient a et b supérieurs ou égaux à 2. Alors a et b sont premiers entre eux si et seulement si leurs décomposition en facteurs premiers n'ont aucun terme commun, c'est-à-dire si a et b n'ont aucun facteur premier commun.

Exemple : $495 = 3^2 \times 5 \times 11$ et $364 = 2^2 \times 7 \times 13$ sont premiers entre eux.

II.3.d Applications

Proposition. Soient a et b supérieurs ou égaux à 2. Alors les facteurs premiers de ab sont exactement ceux de a et de b .

DÉMONSTRATION. Soit $p \in \mathbb{P}$.

$$\begin{aligned} p \text{ est un facteur premier de } ab &\iff v_p(ab) \geq 1 \\ &\iff v_p(a) + v_p(b) \geq 1 \\ &\iff v_p(a) \geq 1 \text{ ou } v_p(b) \geq 1 \end{aligned} \quad \square$$

Remarque : En particulier, il n'y a pas de « génération spontanée de nombres premiers ». En d'autres termes : si un nombre premier apparaît lorsqu'on fait un produit, lorsqu'on prend une puissance etc. c'est qu'il était déjà là au départ. Bien comprendre cette idée permet de deviner, de visualiser et de démontrer et facilement beaucoup de résultats (même si on peut les démontrer autrement, voir plus haut). Par exemple :

- si un nombre premier p divise un produit ab , alors il divise a ou b . En effet, si p divise ab , alors il apparaît dans la décomposition en produit de facteurs premiers de ab donc il apparaît dans celle de a ou celle de b , ce qui permet de conclure.
- Dans le même ordre d'idée, si p divise a^k , alors p divise a . En effet, notons $a = p_1^{\alpha_1} \times \dots \times p_r^{\alpha_r}$, si bien que $a^k = p_1^{k\alpha_1} \times \dots \times p_r^{k\alpha_r}$. Puisque p divise a^k , alors l'un des p_i est égal à p donc p divise a .
- Si a et b sont premiers avec n , alors ab est premier avec n . En effet, a et n n'ont aucun facteur premier commun donc il n'y a aucun facteur premier commun dans leurs décompositions en facteurs premiers, et c'est la même chose pour b et n , si bien qu'il n'y a toujours aucun facteur premier en commun dans les décompositions de ab et n , ce qui permet de conclure.

Donnons une autre application de ce principe, assez utile en pratique.

Proposition. Soient a et b supérieurs ou égaux à 2. Soient k_1 et k_2 supérieurs ou égaux à 1. Alors : $a \wedge b = 1 \iff a^{k_1} \wedge b^{k_2} = 1$.

DÉMONSTRATION. Les facteurs premiers de a^{k_1} sont exactement ceux de a , et ceux de b^{k_2} sont exactement ceux de b . Dès lors :

$$\begin{aligned} a \wedge b = 1 &\iff a \text{ et } b \text{ n'ont aucun facteur premier commun} \\ &\iff a^{k_1} \text{ et } b^{k_2} \text{ n'ont aucun facteur premier commun} \\ &\iff a^{k_1} \wedge b^{k_2} = 1 \end{aligned} \quad \square$$

En particulier, si $n \in \mathbb{N}^*$:

$$a \wedge b = 1 \iff a^n \wedge b^n = 1$$

Proposition. Soit $n = p_1^{\alpha_1} \times \dots \times p_r^{\alpha_r}$ un entier supérieur ou égal à 2. Alors les diviseurs positifs de n sont exactement les $p_1^{\beta_1} \times \dots \times p_r^{\beta_r}$ où, pour tout $i \in \llbracket 1; r \rrbracket$, on a $0 \leq \beta_i \leq \alpha_i$.

DÉMONSTRATION. Soit $d \geq 1$. Alors : $d \mid n \iff \forall p \in \mathbb{P}, v_p(d) \leq v_p(n)$. Par conséquent, si d est de la forme ci-dessus, alors $d \mid n$. Réciproquement, supposons que d divise n . Si $v_p(n) = 0$, alors $v_p(d) = 0$: par contraposée, si $v_p(d) \geq 1$, alors $v_p(n) \geq v_p(d) \geq 1$. En d'autres termes, les facteurs premiers de d , i.e. vérifiant $v_p(d) \geq 1$, sont des facteurs premiers de n et ils ont une puissance inférieure ou égale à la puissance correspondante dans la décomposition de n , ce qui permet de conclure.

Exemple : Les diviseurs positifs de $700 = 2^2 \times 5^2 \times 7$ sont :

- $1 = 2^0 \times 5^0 \times 7^0$
- $2 = 2^1 \times 5^0 \times 7^0$
- $4 = 2^2 \times 5^0 \times 7^0$
- $5 = 2^0 \times 5^1 \times 7^0$
- $10 = 2^1 \times 5^1 \times 7^0$
- $20 = 2^2 \times 5^1 \times 7^0$
- $25 = 2^0 \times 5^2 \times 7^0$
- $50 = 2^1 \times 5^2 \times 7^0$
- $100 = 2^2 \times 5^2 \times 7^0$
- $7 = 2^0 \times 5^0 \times 7^1$
- $14 = 2^1 \times 5^0 \times 7^1$
- $28 = 2^2 \times 5^0 \times 7^1$
- $35 = 2^0 \times 5^1 \times 7^1$
- $70 = 2^1 \times 5^1 \times 7^1$
- $140 = 2^2 \times 5^1 \times 7^1$
- $175 = 2^0 \times 5^2 \times 7^1$
- $350 = 2^1 \times 5^2 \times 7^1$
- $700 = 2^2 \times 5^2 \times 7^1$

En particulier, 700 a 18 diviseurs (positifs). Plus généralement, si $n = p_1^{\alpha_1} \times \dots \times p_r^{\alpha_r}$, alors n admet $(\alpha_1 + 1) \times \dots \times (\alpha_r + 1)$ diviseurs : cf. chapitre 17.

Activité : Soit $n \geq 2$. Donner une CNS sur sa décomposition en facteurs premiers pour que n soit un carré parfait.

Si n est un carré parfait, il existe k supérieur ou égal à 2 tel que $n = k^2$. Notons $k = p_1^{\alpha_1} \times \dots \times p_r^{\alpha_r}$ donc $k^2 = p_1^{2\alpha_1} \times \dots \times p_r^{2\alpha_r}$ donc, par unicité de la décomposition en produit de facteurs premiers, c'est aussi la décomposition de n , c'est-à-dire que toutes les puissances de la décomposition de n en produit de facteurs premiers sont paires. La réciproque est immédiate : notons $n = p_1^{\beta_1} \times \dots \times p_r^{\beta_r}$, et on suppose que β_i est pair pour tout i alors, en posant

$$k = p_1^{\beta_1/2} \times \dots \times p_r^{\beta_r/2}$$

il vient : $n = k^2$, c'est-à-dire que n est un carré parfait. En conclusion : n est un carré parfait si et seulement si toutes les puissances apparaissant dans sa décomposition en produit de facteurs premiers sont paires. Par exemple, $4840000 = 2^6 \times 5^4 \times 11^2$ est un carré parfait mais $5000 = 2^3 \times 5^4$ n'en est pas un. On généralise aisément à une autre puissance : si $d \geq 3$, n est une puissance d -ième si et seulement si toutes les puissances apparaissant dans sa décomposition en facteurs premiers sont divisibles par d .

Remarque : On trouve parfois l'exercice suivant : « donner les entiers supérieurs ou égaux à 2 admettant un nombre impair de diviseurs positifs ». On a vu que si $n = p_1^{\alpha_1} \times \dots \times p_r^{\alpha_r}$, alors n admet $(\alpha_1 + 1) \times \dots \times (\alpha_r + 1)$ diviseurs. Ce nombre est impair si et seulement si tous les $\alpha_i + 1$ sont impairs, si et seulement si les α_i sont tous pairs, et on vient de voir que cela signifie que n est un carré parfait. En conclusion, les entiers admettant un nombre impair de diviseurs positifs sont exactement les carrés parfaits.

Par exemple, 16 admet 5 diviseurs mais 12 en admet 6.

II.3.e Formule de Legendre (HP mais très classique)

Théorème (Formule de Legendre). Soit $n \geq 2$ et soit p un nombre premier. Alors :

$$v_p(n!) = \sum_{k=1}^{+\infty} \left\lfloor \frac{n}{p^k} \right\rfloor$$

Remarque : On pourrait définir cette somme rigoureusement mais nous verrons les sommes infinies en détail au chapitre 25. Pour l'instant, on se contente de remarquer qu'il n'y a qu'un nombre fini de termes non nuls dans cette somme car, pour k assez grand, $p^k > n!$ (car $p^k \xrightarrow[k \rightarrow +\infty]{} +\infty$, cf. chapitre 12) donc $\lfloor n!/p^k \rfloor = 0$: cette somme est donc la somme de tous les termes non nuls.

DÉMONSTRATION. Puisque $n! = 1 \times 2 \times \cdots \times n$:

$$v_p(n!) = \sum_{i=1}^n v_p(i)$$

Écrivons ci-dessous cette inégalité dans le cas $n = 14$ et $p = 2$:

$$\begin{aligned} v_2(14!) = & v_p(1) + v_p(2) + v_p(3) + v_p(4) + v_p(5) + v_p(6) + v_p(7) + v_p(8) + v_p(9) \\ & + v_p(10) + v_p(11) + v_p(12) + v_p(13) + v_p(14) \end{aligned}$$

Ainsi, dans le cas $n = 14$, il y a sept entiers i pour lesquels $v_2(i) = 0$ (en noir), quatre entiers i pour lesquels $v_2(i) = 1$ (en bleu), deux entiers i pour lesquels $v_2(i) = 2$ (en rouge), un entier i pour lequel $v_2(i) = 3$ (en jaune) et aucun pour lequel $v_2(i) \geq 4$ si bien que $v_2(14!) = 0 \times 7 + 1 \times 4 + 2 \times 2 + 3 \times 1 = 11$.

Dans le cas général, l'idée est de regrouper les entiers i selon la valeur de $v_p(i)$, c'est-à-dire que

$$v_p(n!) = \sum_{k=0}^{+\infty} k \times \text{card}\{i \mid v_p(i) = k\}$$

Cela se voit bien avec un dessin : ci-dessous, on a mis en noir les nombres i pour lesquels $v_2(i) = 0$, en rouge les nombres i pour lesquels $v_2(i) = 1$, en bleu les nombres i tels que $v_2(i) = 2$, en vert les nombres i tels que $v_2(i) = 3$ etc.

Or, cette somme commence en fait en 1 puisque le terme sommé est nul pour $k = 0$, si bien que

$$v_p(n!) = \sum_{k=1}^{+\infty} k \times \text{card}\{i \mid v_p(i) = k\}$$

Si $q \geq 1$, le nombre d'entiers inférieurs ou égaux à n divisibles par q est $\lfloor n/q \rfloor$ (cf. chapitre 2). Par conséquent, il y a $\lfloor n/p \rfloor$ entiers inférieurs ou égaux à n divisibles par p , il y a $\lfloor n/p^2 \rfloor$ entiers divisibles par p^2 etc.

Seulement, un entier divisible par p^2 est divisible aussi divisible par p : il y a $\lfloor n/p \rfloor - \lfloor n/p^2 \rfloor$ entiers divisibles par p mais pas par p^2 , $\lfloor n/p^2 \rfloor - \lfloor n/p^3 \rfloor$ entiers divisibles par p^2 mais pas par p^3 etc. De façon générale, pour tout $k \geq 1$, il y a $\lfloor n/p^k \rfloor - \lfloor n/p^{k+1} \rfloor$ entiers i divisibles par k et non divisibles par $k+1$, c'est-à-dire tels que $v_p(i) = k$ car $v_p(i) = \max\{k \mid p^k \text{ divise } i\}$. Finalement :

$$\begin{aligned} v_p(n!) &= \sum_{k=1}^{+\infty} k \times \left(\left\lfloor \frac{n}{p^k} \right\rfloor - \left\lfloor \frac{n}{p^{k+1}} \right\rfloor \right) \\ &= \sum_{k=1}^{+\infty} k \left\lfloor \frac{n}{p^k} \right\rfloor - \sum_{k=1}^{+\infty} k \left\lfloor \frac{n}{p^{k+1}} \right\rfloor \\ &= \sum_{k=1}^{+\infty} k \left\lfloor \frac{n}{p^k} \right\rfloor - \sum_{k=2}^{+\infty} (k-1) \left\lfloor \frac{n}{p^k} \right\rfloor \\ &= \left\lfloor \frac{n}{p} \right\rfloor + \sum_{k=2}^{+\infty} (k - (k-1)) \left\lfloor \frac{n}{p^k} \right\rfloor \\ &= \left\lfloor \frac{n}{p} \right\rfloor + \sum_{k=2}^{+\infty} \left\lfloor \frac{n}{p^k} \right\rfloor \end{aligned}$$

Les sommes sont en fait finies donc on peut travailler sans se poser de questions.

□

ce qui permet de conclure.

Activité : Donnons le nombre de zéros à la fin de l'écriture décimale de $2023!$.

On demande en fait la puissance maximale de 10 qui divise $2023!$: en effet, un nombre se termine par trois zéros lorsqu'il est divisible par 1000 et pas par 10000, c'est-à-dire lorsqu'il est divisible par 10^3 et pas par 10^4 . Notons d cette puissance.

- Si on écrit la décomposition de n en produit de facteurs premiers, on obtient : $n! = 2^{v_2(n!)} \times 5^{v_5(n!)} \times K$ où K est premier avec 2 et avec 5 donc avec 10. On veut regrouper le 2 et le 5, et pour cela, il faut savoir quelle puissance est la plus petite.
- Montrons que $v_2(n!) \geq v_5(n!)$. Si $k \geq 1$, $n/2^k \geq n/5^k$ et la partie entière est une fonction croissante donc $\lfloor n/2^k \rfloor \geq \lfloor n/5^k \rfloor$ et, par somme, on a le résultat d'après la formule de Legendre.
- Il en découle que $n! = 10^{v_5(n!)} \times 2^{v_2(n!) - v_5(n!)} \times K$. Puisque 2 et K sont premiers avec 5, $2^{v_2(n!) - v_5(n!)} \times K$ est premier avec 5 donc n'est pas divisible par 10, et donc on a $d = v_5(n!)$.
- Finalement,

$$d = \sum_{k=1}^{+\infty} \left\lfloor \frac{2023}{5^k} \right\rfloor$$

Or, $\lfloor 2023/5 \rfloor = 404$, $\lfloor 2023/25 \rfloor = 80$, $\lfloor 2023/125 \rfloor = 16$, $\lfloor 2023/625 \rfloor = 3$ et, pour tout $k \geq 5$, $\lfloor 2023/5^k \rfloor = 0$ si bien que $d = 503$: $2023!$ se termine par 503 zéros.

II.4 Nombres de Fermat et de Mersenne (HP mais très classique)

On sait qu'il existe une infinité de nombres premiers. Un autre problème est de donner une infinité de nombres premiers **explicites**. Plusieurs familles de nombres ont été étudiées dans l'espoir qu'elles contiennent de nombreux nombres premiers (avec des fortunes diverses). Donnons deux des plus célèbres, qui sont de plus des classiques des concours.

Proposition. Soit $n \in \mathbb{N}$. Si $2^n + 1$ est premier, alors n est une puissance de 2.

DÉMONSTRATION. Supposons que n ne soit pas une puissance de 2. Alors il existe un nombre premier différent de 2 dans la décomposition de n en produit de facteurs premiers. En particulier, n est divisible par un nombre impair $m \geq 3$: il existe $k \in \mathbb{N}$ et $m \geq 3$ impair tel que $n = k \times m$. Par conséquent,

$$\begin{aligned} 2^n + 1 &= 2^{km} + 1 \\ &= (2^k)^m - (-1)^m \\ &= (2^k + 1) \times \sum_{i=0}^{m-1} 2^i (-1)^{m-1-i} \end{aligned}$$

On montre de même que si $(a, b) \in (\mathbb{N}^*)^2$, $n \geq 2$ et si $a^n + b^n$ est premier, alors n est une puissance de 2.

$(-1)^m = -1$ car m est impair.

Factorisation de $a^m - b^m$.

Par conséquent, $2^k + 1$ divise $2^n + 1$. Or, $2^k > 0$ donc $2^k + 1 > 1$. De plus, $m > 1$ donc $k < n$ si bien que $2^k + 1 < 2^n + 1$. Finalement, $2^n + 1$ n'est pas premier, d'où le résultat par contraposée. \square

Définition. Soit $n \in \mathbb{N}$. On appelle n -ième nombre de Fermat le nombre $F_n = 2^{2^n} + 1$.

Remarques :

- $F_0 = 3$, $F_1 = 5$, $F_2 = 17$, $F_3 = 257$ et $F_4 = 65537$, qui sont tous premiers.

- F_5 jusque F_{32} sont composés, et d'autres encore (par exemple F_{73}) mais on ne sait pas s'il existe d'autres nombres premiers parmi les F_n (Fermat conjecturait qu'ils étaient tous premiers mais Euler a montré que F_5 était composé, cf. exercice 42).

- Cependant, même si les nombres de Fermat ne sont pas tous premiers, ils sont tout de même premiers entre eux deux à deux. Soient $n \neq p$ deux entiers. Sans perte de généralité, on peut supposer $p < n$. Soit d un diviseur positif commun à F_n et F_p .

D'après l'exercice 22 du chapitre 3, $F_n = \prod_{k=0}^{n-1} F_k + 2$. Or, $n > p$ donc F_p est un terme

du produit ci-dessus, si bien que d divise ce produit, et comme d divise F_n , alors d divise 2, si bien que $d = 1$ ou $d = 2$. Or, les nombres de Fermat sont impairs donc ne sont pas divisibles par 2, si bien que $d = 1$.

- On en déduit une nouvelle preuve de l'infinitude de l'ensemble des nombres premiers : les nombres de Fermat étant premiers entre eux deux à deux, ils ont tous des facteurs premiers distincts, et comme il y a un nombre infini de nombres de Fermat, alors il y a un nombre infini de nombres premiers.

p est un entier quelconque, ce n'est pas forcément un nombre premier !

Proposition. Soit $n \in \mathbb{N}$. Si $2^n - 1$ est premier, alors n est premier.

DÉMONSTRATION. Si n n'est pas premier, alors il s'écrit sous la forme ab avec $2 \leq a, b \leq n - 1$. De même que ci-dessus,

$$\begin{aligned} 2^n - 1 &= 2^{ab} - 1 \\ &= (2^a)^b - 1^b \\ &= (2^a - 1) \times \sum_{i=0}^{b-1} 2^{ai} \end{aligned} \quad \square$$

Or, $a \geq 2$ donc $2^a - 1 \geq 3 > 1$ et $b \geq 2$ donc $\sum_{i=0}^{b-1} 2^{ai} \geq 1 + 2 > 1$ si bien que $2^a - 1 < 2^n - 1$, et on conclut comme précédemment que $2^n - 1$ n'est pas premier, d'où le résultat par contraposée.

Définition. Soit p un nombre premier. Le nombre de Mersenne d'indice p est $M_p = 2^p - 1$.

Remarque : Les premiers exemples sont $M_2 = 3$, $M_3 = 7$, $M_5 = 31$, $M_7 = 127$ qui sont premiers, et $M_{11} = 2047$ qui ne l'est pas. C'est parmi les nombres de Mersenne qu'on cherche et qu'on trouve les plus grands nombres premiers car on dispose pour ces nombres d'un test de primalité très efficace (test de Lucas-Lehmer). On connaît 48 nombres de Mersenne qui sont premiers (on ne sait pas s'il en existe une infinité). Le dernier trouvé (et qui est le plus grand nombre premier connu) possède plus de 28 millions de chiffres !

Remarque : Malheureusement, les seules méthodes (par exemple le crible d'Eratosthène) ou formules (cf. exercices 76 et 78 par exemple) permettant d'obtenir tous les nombres premiers sont inutilisables en pratique. On en est donc réduit à tester des nombres particuliers, en général des nombres de Mersenne, en espérant tomber sur un nombre premier.

III Congruence

III.1 Rappels (cf. chapitre 5)

Définition. Soient a , b et m des réels avec m non nul. On dit que a est congru à b modulo m si il existe $k \in \mathbb{Z}$ tel que $a = b + km$. On note alors $a \equiv b [m]$

Proposition. Soient a, b, c, d et m des réels, avec c et m non nul.

1. Si $a \equiv b[m]$ alors $b \equiv a[m]$ (symétrie).
2. Si $a \equiv b[m]$ et $b \equiv c[m]$ alors $a \equiv c[m]$ (transitivité).
3. $a \equiv b[m]$ si et seulement si $(a + c) \equiv (b + c)[m]$.
4. Si $a \equiv b[m]$ et $c \equiv d[m]$, alors $a + c \equiv b + d[m]$.

Proposition. Soient a, b, c et m des réels, avec c et m non nuls. Alors :

$$a \equiv b[m] \iff ac \equiv bc[mc].$$



Il ne faut pas oublier de multiplier par c dans la congruence !

III.2 Congruence et divisibilité

On se donne dans la suite de cette partie cinq entiers (relatifs) a, b, c, d, m et on suppose que m est non nul.

Proposition.

- $a \equiv b[m] \iff m \mid b - a$, c'est-à-dire si et seulement si a et b diffèrent d'un multiple de m . En particulier : $m \mid b \iff b \equiv 0[m]$.
- Soit d un diviseur de m . Si $a \equiv b[m]$ alors $a \equiv b[d]$.




Par exemple, si $a \equiv b[4]$, alors $a \equiv b[2]$.

DÉMONSTRATION. La première équivalence découle de la définition : $a \equiv b \iff \exists k \in \mathbb{Z}, b - a = km$. La seconde découle de la première en prenant $a = 0$. Enfin, si $a \equiv b[m]$, alors $m \mid b - a$ et $d \mid m$ donc $d \mid b - a$.

Exemple : Un nombre est pair si et seulement s'il est congru à 0 modulo 2. Un nombre est impair si et seulement s'il est congru à 1 modulo 2.

Remarque : Plus généralement, par transitivité, a est divisible par m si et seulement s'il est congru à un multiple de m modulo m . Par exemple, un nombre congru à 5 modulo 2 n'est pas divisible par 2, mais un nombre congru à 6 modulo 2 est divisible par 2.

Remarque :  Attention, si on arrive à une congruence non nulle, on ne peut pas conclure directement que m ne divise pas b car cette congruence peut être elle-même divisible par m . Par exemple, $100 \equiv 4[2]$ mais il serait faux d'en conclure que $100 \not\equiv 0[2]$ puisque $4 \not\equiv 0$ donc que 100 n'est pas divisible par 2. En effet, $4 \equiv 0[2]$ donc $100 \equiv 0[2]$. Pour pouvoir conclure comme cela, il faut que cette congruence soit « irréductible », il faut qu'elle soit la plus petite possible, c'est-à-dire :

Proposition.

- Soient q et r respectivement le quotient et le reste de la division euclidienne de a par m . Alors $a \equiv r[m]$.
- Réciproquement, supposons que $m > 0$ et soit $r \in \llbracket 0; m - 1 \rrbracket$. Si $a \equiv r[m]$ alors r est le reste de la division euclidienne de a par m . En particulier : $m \mid a \iff r = 0$.



On peut effectuer cette division car $m \neq 0$.

DÉMONSTRATION. Le premier point découle du fait que $a = qm + r$, le second de l'unicité de l'écriture de la division euclidienne et du fait que $m \mid a$ si et seulement si $r = 0$.



Par exemple, si $a \equiv 2[3]$ alors 3 ne divise pas a .

Remarque : Si $a \equiv b[m]$, a et b ne sont pas forcément égaux. Pour affirmer qu'ils sont égaux, ils ne doivent pas « être trop éloignés ». Plus précisément :

Proposition. Si $a \equiv b[m]$ et si $|b - a| < m$, alors $a = b$. En particulier, si a et b appartiennent à $\llbracket 0; m - 1 \rrbracket$ ou à $\llbracket 1; m \rrbracket$, alors $a = b$.



Si a et b appartiennent à $\llbracket 0; m \rrbracket$, on n'a pas forcément $a = b$! On peut avoir $a = 0$ et $b = m$.

DÉMONSTRATION. Il suffit de voir que $b - a$ est un multiple de m , et le seul multiple de m strictement inférieur à m en valeur absolue est 0.

Remarque : En particulier, si a et b sont distincts et appartiennent à $\llbracket 0; m - 1 \rrbracket$, alors $a \not\equiv b[m]$. Il découle des deux résultats précédents que tout entier a est congru à un et un seul élément de $\llbracket 0; m - 1 \rrbracket$ modulo m (cela peut être utile pour faire un raisonnement par disjonction de cas).

III.3 Résultats propres aux entiers

Le résultat suivant est propre aux entiers et est faux lorsqu'on travaille avec des réels quelconques (cf. chapitre 5) :

Proposition. Si $a \equiv b[m]$ et $c \equiv d[m]$ alors $ac \equiv bd[m]$. En particulier, pour tout $k \in \mathbb{N}$, $a^k \equiv b^k[m]$.



On généralise aisément à un produit de plus de deux termes. En particuliers, le produit modulo m est associatif, comme le produit « normal ».

DÉMONSTRATION. Il existe $(k_1, k_2) \in \mathbb{Z}^2$ tel que $a = b + k_1m$ et $c = d + k_2m$ donc $ac = bd + m \times (bk_2 + dk_1 + mk_1k_2)$. Or, $bk_2 + dk_1 + mk_1k_2 \in \mathbb{Z}$ (c'est là qu'on utilise le fait que tous les nombres sont des entiers) ce qui permet de conclure.

Exemple : Donner le reste de la division euclidienne de $a = 12 \times 21 \times 28 \times 18 \times 75 \times 23$ par 11.

Il suffit de prendre toutes les congruences modulo 11 :

$$\begin{aligned} a &\equiv 1 \times -1 \times 6 \times 7 \times -2 \times 1[11] \\ &\equiv -12[11] \\ &\equiv 10[11] \end{aligned}$$



On aurait aussi pu prendre les congruences modulo 11 les unes après les autres.

et donc le reste recherché vaut 10.

Remarque : Par conséquent, lorsqu'on ne cherche que le reste, il peut être intéressant de prendre la congruence modulo m , mais cela n'est intéressant que lorsqu'on a écrit ce nombre sous la forme d'un produit de nombres plus petits dont les congruences sont faciles à calculer. Si on s'intéresse à un nombre a ne pouvant pas s'écrire sous cette forme (par exemple un nombre premier), il suffit de calculer la congruence d'un nombre « pas trop loin ». Par exemple, 2017 est premier mais $2016 = 32 \times 7 \times 9 \equiv -1 \times 7 \times -2 \equiv 3[11]$ donc $2017 \equiv 4[11]$ c'est-à-dire que le reste dans la division de 2017 par 11 vaut 4. Pour des entiers m dont les multiples sont simples à donner, on peut également repérer un multiple de m « proche » de a . Par exemple, 2016 est divisible par 4 (car vaut 4×504) et divisible par 3 (cf. paragraphe III.4) donc est divisible par 12 car $3 \wedge 4 = 1$ si bien que $2017 \equiv 1[12]$: le reste dans la division de 2017 par 12 vaut 1.

Donnons d'autres exemples de calculs de congruences.

Exemples :

- Montrons que $2^{2023} + 5^{2024}$ est divisible par 3.

Si on regarde la congruence modulo 3, il vient :

$$\begin{aligned} 2^{2023} + 5^{2024} &\equiv (-1)^{2023} + (-1)^{2024}[3] \\ &\equiv -1 + 1[3] \\ &\equiv 0[3] \end{aligned}$$

ce qui permet de conclure.

- Soit $n \in \mathbb{Z}$. Montrons que $n^2 \not\equiv 2[3]$.

Raisonnons par disjonction de cas :

- ★ Si $n \equiv 0[3]$ alors $n^2 \equiv 0[3]$.
- ★ Si $n \equiv 1[3]$ alors $n^2 \equiv 1[3]$.
- ★ Si $n \equiv 2[3]$ alors $n^2 \equiv 4[3]$ donc $n^2 \equiv 1[3]$.

- Soit $n \in \mathbb{Z}$ impair. Montrons que $n^2 \equiv 1[8]$.

On peut faire la même chose que ci-dessus i.e. faire une disjonction de cas selon la congruence modulo 8 mais on peut aller plus vite. Il existe $k \in \mathbb{N}$ tel que $n = 2k + 1$ si bien que $n^2 = 4k^2 + 4k + 1$ donc $n^2 = 4k(k + 1) + 1$. Or, $k(k + 1)$ est pair car est le produit de deux entiers consécutifs donc s'écrit sous la forme $2a$ si bien que $4k(k + 1) = 8a$ est divisible par 8, ce qui permet de conclure. Si n est pair, on a $n^2 \equiv 0[8]$ ou $n^2 \equiv 4[8]$ (exo).

Remarque : On voit avec les deux derniers exemples que l'équation diophantienne $x^2 = 2 + 3y$ n'a aucune solution (entière), tout comme l'équation $x^2 = k + 8y$ si $k = 2, 3, 5, 6$ ou 7. Un moyen simple (mais qui ne marche pas tout le temps sinon ce serait trop facile) de prouver qu'une équation diophantienne n'admet pas de solution est d'exhiber un entier n tel que l'équation n'a pas de solution modulo n . Nous verrons un autre exemple en TD.

Remarque : Encore une fois, quand on travaille avec des entiers, on peut multiplier dans une congruence **sans multiplier dans le crochet** ce qui fait qu'on peut travailler avec la congruence comme avec l'égalité, à une (grosse) exception près : la division ! On ne peut en général pas diviser dans une congruence, ce qui n'est pas très étonnant puis diviser par n revient à multiplier par $1/n$ qui n'est pas un entier.

Exemple : $4 \equiv 6[2]$ mais $2 \not\equiv 3[2]$. Pour pouvoir diviser dans une congruence, il faut une condition supplémentaire.



Encore une fois, ce n'est vrai que pour les entiers !

Proposition. Si $ac \equiv bc[m]$ et si $c \wedge m = 1$ alors $a \equiv b[m]$. En d'autres termes, on peut simplifier par les termes premiers avec m .

DÉMONSTRATION. $c \wedge m = 1$ donc, d'après le théorème de Bézout, il existe $(u, v) \in \mathbb{Z}^2$ tel que $cu + mv = 1$. En particulier, $cu \equiv 1[m]$. Dès lors, en multipliant la congruence $ac \equiv bc[m]$ par u , il vient : $cua \equiv cub[m]$ et puisque $cu \equiv 1[m]$, on a le résultat voulu.

Activité : Congruence d'une puissance. On cherche régulièrement la congruence d'une certaine puissance modulo m . La méthode est toujours la même, fondée sur le résultat suivant, appelé principe des tiroirs (cf. chapitre 17) : si on a un nombre fini de tiroirs et un nombre infini de paires de chaussettes, alors il existe au moins un tiroir qui contient au moins deux paires de chaussettes (et même une infinité).

Puisqu'il existe une infinité de puissances a^k (les chaussettes), pour $k \in \mathbb{N}$, et que pour tout k , il existe $r \in \llbracket 0 ; m - 1 \rrbracket$ tel que $a^k \equiv r[m]$, il n'y a qu'un nombre fini de congruences possibles (les tiroirs) donc existe $k_1 < k_2$ tel que $a^{k_1} \equiv a^{k_2}[m]$. Dès lors, $a^{k_1+1} \equiv a^{k_2+1}$ jusque

$$\begin{aligned} a^{k_2+(k_2-k_1)} &\equiv a^{k_2} \times a^{k_2-k_1}[m] \\ &\equiv a^{k_1} \times a^{k_2-k_1}[m] \\ &\equiv a^{k_2}[m] \\ &\equiv a^{k_1}[m] \end{aligned}$$

Plus généralement, si $n \geq k_1$, alors



Encore en d'autres termes, les entiers premiers avec m sont inversibles modulo m . Ce sont même les seuls, cf. exercice 2 du chapitre 16. De plus, comme on le voit dans la démonstration, on trouve un inverse explicite à l'aide d'une relation de Bézout.

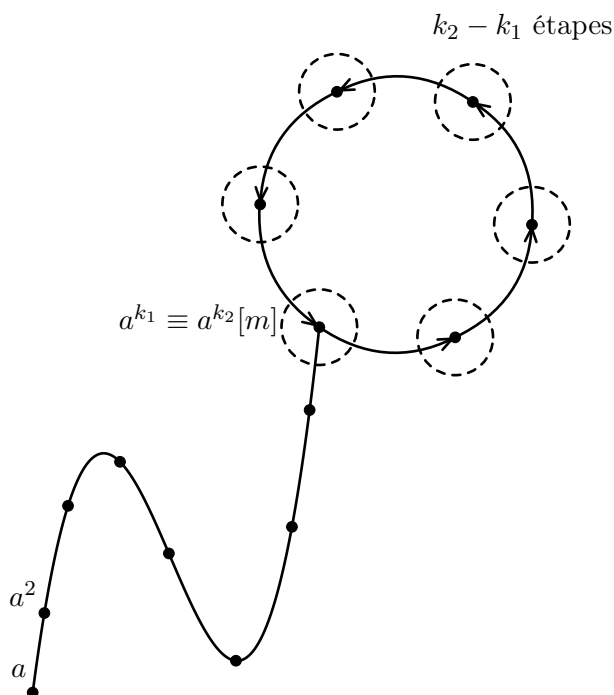


Attention, on ne peut pas simplifier par a^{k_1} et affirmer que $a^{k_2-k_1} \equiv 1[m]$: on ne peut simplifier que par les termes premiers avec m .

$$\begin{aligned}
a^{n+(k_2-k_1)} &\equiv a^{k_2} \times a^{n-k_1}[m] \\
&\equiv a^{k_1} \times a^{n-k_1}[m] \\
&\equiv a^n[m]
\end{aligned}$$

Possible car $n \geq k_1$.

c'est-à-dire que la suite $(a^n)_{n \in \mathbb{N}}$ est $(k_2 - k_1)$ -périodique (cf. chapitre 12) modulo m à partir du rang k_1 , ce qui est assez intuitif : $a^{k_2} \equiv a^{k_1}[m]$ donc on repart de a^{k_1} , et ce à chaque fois qu'on atteint a^{k_2} , c'est-à-dire qu'on effectue à chaque fois le même cycle de $k_2 - k_1$ étapes, comme sur le dessin ci-dessous :



Pour calculer a^n modulo m , il suffit alors de calculer n modulo $k_2 - k_1$. Il est inutile de retenir la démonstration générale, il suffit de savoir l'appliquer sur des exemples.

Exemple : Donner le chiffre des unités de $N = 7^{7^{7^7}}$ (c'est-à-dire le reste de la division euclidienne de N par 10, cf. paragraphe III.4).

D'après ce qui précède, il suffit de trouver deux entiers k_1 et k_2 tels que $7^{k_1} \equiv 7^{k_2}[10]$. On trouve successivement $7 \equiv 7[10]$, $7^2 \equiv -1 \equiv 9[10]$, $7^3 \equiv -7 \equiv 3[10]$, $7^4 \equiv 1[10]$ et $7^5 \equiv 7[10]$. Dès lors, $7^6 \equiv 9[10]$, $7^7 \equiv 3[10]$, $7^8 \equiv 1[10]$, $7^9 \equiv 7[10]$ etc. Par une récurrence immédiate, pour tout $k \in \mathbb{N}^*$:

$$7^{4k+1} \equiv 7[10], \quad 7^{4k+2} \equiv 9[10], \quad 7^{4k+3} \equiv 3[10] \quad \text{et} \quad 7^{4k} \equiv 1[10]$$

Ainsi, il suffit de connaître la congruence de $n = 7^{7^7}$ modulo 4, ce qu'on fait de la même manière : $7 \equiv 3[4]$, $7^2 \equiv 9 \equiv 1[4]$ et $7^3 \equiv 7 \equiv 3[4]$ puis $7^4 \equiv 1[4]$, $7^5 \equiv 3[4]$ etc. Par une récurrence immédiate, pour tout $k \in \mathbb{N}$, $7^{2k} \equiv 1[4]$ et $7^{2k+1} \equiv 3[4]$. Or, 7^{7^7} est impair donc $n \equiv 3[4]$ si bien que $N \equiv 3[10]$: le chiffre des unités de N est 3.

Exemple : Donner la congruence de 2^{65362} modulo 7.

$2 \equiv 2[7]$, $2^2 \equiv 4[7]$, $2^3 \equiv 1[7]$, $2^4 \equiv 2[7]$ si bien que $2^5 \equiv 4[7]$, $2^6 \equiv 1[7]$, $2^7 \equiv 2[7]$ etc. Par une récurrence immédiate, pour tout $k \in \mathbb{N}$,

$$2^{3k+1} \equiv 2[7], \quad 2^{3k+2} \equiv 4[7] \quad \text{et} \quad 2^{3k} \equiv 1[7]$$

Ainsi, il suffit de connaître la congruence de 65362 modulo 3 : d'après le paragraphe III.4, $65362 \equiv 1[3]$ si bien que $2^{65362} \equiv 2[7]$.

Dans le cas particulier où l'une des congruences vaut 1 (comme dans les deux exemples ci-contre), une récurrence est inutile : il suffit d'écrire, par exemple, que pour tout $k \in \mathbb{N}^*$,

$$\begin{aligned}
7^{4k+3} &= (7^4)^k \times 7^3 \\
&\equiv 1^k \times 3[10] \\
&\equiv 3[10]
\end{aligned}$$

Le problème est que ce n'est pas toujours possible (plus précisément lorsque a et m ne sont pas premiers entre eux, cf. exercice 39, par exemple si on demande la congruence de 2^n modulo 10, on ne tombera jamais sur 1).

III.4 Critères de divisibilité

Soit $N \geq 1$ qu'on écrit en base 10 sous la forme $N = \overline{a_{n-1} \dots a_1 a_0}^{10}$, c'est-à-dire que :

$$N = a_{n-1} \times 10^{n-1} + \dots + a_1 \times 10 + a_0 = \sum_{k=0}^{n-1} a_k 10^k$$

Le chiffre $a_0 \in \llbracket 0; 9 \rrbracket$ est alors le chiffre des unités de N , a_1 celui des dizaines etc. Les critères de divisibilité par 2, 5 ou 10 sont immédiats et connus depuis l'école primaire.

Proposition.

- N est divisible par 10 si et seulement si $a_0 = 0$.
- N est divisible par 5 si et seulement si $a_0 = 0$ ou $a_0 = 5$.
- N est divisible par 2 (i.e. N est pair) si et seulement si $a_0 = 0, 2, 4, 6$ ou 8 .

DÉMONSTRATION. Puisque $10 \equiv 0[5]$, $10^k \equiv 0[5]$ pour tout $k \geq 1$ donc $N \equiv a_0[5]$. Dès lors :

$$5 \mid N \iff N \equiv 0[5] \iff a_0 \equiv 0[5] \iff 5 \mid a_0 \quad \square$$

Or, les seuls chiffres de $\llbracket 0; 9 \rrbracket$ divisibles par 5 sont 0 et 5, d'où le résultat. De même pour les deux autres.

Pour la divisibilité par 4, le dernier chiffre ne suffit pas : il faut regarder les deux derniers chiffres.

Proposition. $N \equiv \overline{a_1 a_0}^{10}[4]$. En particulier, N est divisible par 4 si et seulement si $\overline{a_1 a_0}^{10}$, c'est-à-dire le nombre formé par les deux derniers chiffres de N , l'est.



Ne pas confondre $\overline{a_1 a_0}^{10}$ avec $a_1 \times a_0$!

DÉMONSTRATION. Il suffit de voir que $10^2 = 4 \times 25$ donc $10^k \equiv 0[4]$ dès que $k \geq 2$.

Exemple : 2022 n'est pas divisible par 4 car 22 ne l'est pas, mais 2024 l'est car 24 est divisible par 4.

Pour la divisibilité par 3 ou 9, commençons par un résultat préliminaire.

Proposition. N est congru à la somme de ses chiffres modulo 3 et modulo 9.

DÉMONSTRATION. Puisque $10 \equiv 1[3]$ alors, pour tout $k \in \mathbb{N}$ (même si $k = 0$), $10^k \equiv 1[3]$ si bien que :

$$\begin{aligned} N &\equiv \sum_{k=0}^{n-1} a_k 1^k [3] \\ &\equiv \sum_{k=0}^{n-1} a_k [3] \end{aligned} \quad \square$$

La preuve pour 9 est identique.

Remarque : Par transitivité de la congruence, on peut même répéter l'opération plusieurs fois i.e. calculer la somme des chiffres de la somme des chiffres de la somme des chiffres etc. sans changer la congruence modulo 3 ou 9.

Exemple : $65362 \equiv 22 \equiv 4 \equiv 1[3]$, comme affirmé ci-dessus.

Corollaire. N est divisible par 3 (respectivement par 9) si et seulement si la somme de ses chiffres est divisible par 3 (respectivement par 9).

Exemple : 2022 est divisible par 3.

Définition. On appelle somme alternée des chiffres de N la somme $\sum_{k=0}^{n-1} (-1)^k a_k$.

Remarque : En d'autres termes, le terme constant est compté positivement, le chiffre des dizaines négativement etc. : « en partant de la droite, on fait $+ - + - + - \dots$ ».

Exemple : La somme alternée des chiffres de 2023 vaut $3 - 2 + 0 - 2 = 0 - 1$.

Proposition. N est congru à la somme alternée de ses chiffres modulo 11.

DÉMONSTRATION. Analogie à ci-dessus puisque $10 \equiv -1[11]$.

Corollaire. N est divisible par 11 si et seulement si la somme alternée de ses chiffres est divisible par 11.

Exemple : 2023 n'est pas divisible par 11 mais 2024 l'est car la somme alternée de ses chiffres est nulle (donc divisible par 11) et 2090 l'est aussi car $0 - 9 + 0 - 2 = -11$ qui est divisible par 11.

III.5 Petit théorème de Fermat

Proposition. Soit p un nombre premier. Pour tout $k \in \llbracket 1; p-1 \rrbracket$, p divise $\binom{p}{k}$.

DÉMONSTRATION. Soit $k \in \llbracket 1; p-1 \rrbracket$. Puisque

$$\binom{p}{k} = \frac{p!}{k! \times (p-k)!}$$

alors $p! = k! \times (p-k)! \times \binom{p}{k}$. Puisque $k \in \llbracket 1; p-1 \rrbracket$, alors $k \leq p-1$ et $p-k \leq k-1$ si bien que $k!$ et $(p-k)!$ sont des produits de nombres strictement inférieurs à p donc premiers avec p donc sont eux-mêmes premiers avec p . Si $\binom{p}{k}$ n'est pas divisible par p , alors il est premier avec p donc $p!$ est un produit de trois nombres premiers avec p donc est premier avec p ce qui est absurde car $p \mid p!$.

Remarque : C'est faux si p n'est pas premier. Par exemple, 4 ne divise pas $\binom{4}{2} = 6$.

Corollaire. Soit $(a, b) \in \mathbb{Z}^2$ et soit p premier. Alors $(a+b)^p \equiv a^p + b^p[p]$.

Remarque : En d'autres termes, quand on travaille modulo p (avec p **premier**), alors on peut « oublier les identités remarquables ». Le rêve !

DÉMONSTRATION. Découle du binôme de Newton et de la proposition précédente puisque, pour tout $k \in \llbracket 1; k-1 \rrbracket$, $\binom{p}{k} \equiv 0[p]$.

Théorème (petit théorème de Fermat). Soit p premier et soit $a \in \mathbb{Z}$. Alors $a^p \equiv a[p]$. De plus, si a n'est pas divisible par p , alors $a^{p-1} \equiv 1[p]$.

Ce n'est pas le cas si $k = 0$ ou $k = p$ car alors le coefficient binomial vaut 1.

Rappelons que p est premier donc un entier est premier avec p si et seulement s'il n'est pas divisible par p .

On aurait aussi pu raisonner avec la valuation p -adique, ou le théorème de Gauß (exo).

DÉMONSTRATION. Montrons par récurrence (finie) que le résultat est vrai pour tout $a \in \llbracket 0; p-1 \rrbracket$.

- Si $a \in \llbracket 0; p-1 \rrbracket$, notons $H_a : \ll a^p \equiv a[p] \gg$.
- H_0 est trivialement vraie.
- Soit $a \in \llbracket 0; p-2 \rrbracket$. Supposons H_a vraie et prouvons que H_{a+1} est vraie. D'après le corollaire précédent, $(a+1)^p \equiv a^p + 1^p \equiv a^p + 1[p]$. Or, par hypothèse de récurrence, $a^p \equiv a[p]$ donc $(a+1)^p \equiv a + 1[p] : H_{a+1}$ est vraie.
- D'après le principe de récurrence, H_a est vraie pour tout $a \in \llbracket 0; p-1 \rrbracket$.

Soit $a \in \mathbb{Z}$. Notons r le reste de la division euclidienne de a par p . D'une part, $a \equiv r[p]$ donc $a^p \equiv r^p[p]$ et d'autre part, $r \in \llbracket 0; p-1 \rrbracket$ donc $r^p \equiv r[p]$ d'après ce qui précède. Finalement, $a^p \equiv r \equiv a[p]$.

Enfin, si p ne divise pas a alors a et p sont premiers entre eux donc on peut simplifier par a , ce qui donne le résultat voulu.

Activité : nombres de Carmichael (HP). L'inconvénient du (petit) théorème de Fermat est que la réciproque est fautive : si $a^p \equiv a[p]$ pour tout a , p n'est pas forcément un nombre premier.

Définition. Soit $n \geq 4$ un nombre composé. Si $a^n \equiv a[n]$ pour tout $a \in \mathbb{Z}$, on dit que n est un nombre de Carmichael.

Nous allons dans la suite examiner des propriétés des nombres de Carmichael (et aussi prouver que des nombres de Carmichael existent!).

- Montrons qu'un nombre de Carmichael est impair et sans facteur carré.

Soit $n \geq 4$ un nombre de Carmichael. Si n est pair alors $(-1)^n - (-1) = 2$ qui n'est pas divisible par n donc $(-1)^n \not\equiv -1[n]$, ce qui est absurde, donc n est impair. Si n admet un facteur carré, alors il existe $d \geq 2$ tel que d^2 divise n i.e. il existe k tel que $n = d^2 k$. Soit $a = dk$. Alors $a^n = d^n k^n = n \times d^{n-2} k^{n-1}$ si bien que $n \mid a^n$ et donc $a^n \equiv 0[n]$ mais n ne divise pas a donc $a \not\equiv 0[n]$ ce qui est absurde car n est un nombre de Carmichael.

- Soit $n \geq 4$ un nombre composé sans facteur carré. Montrer que si, pour tout p premier divisant n , $p-1$ divise $n-1$, alors n est un nombre de Carmichael.

Notons $n = p_1 \times \cdots \times p_r$ la décomposition en facteurs premiers de n . Par hypothèse, pour tout $i \in \llbracket 1; r \rrbracket$, il existe m_i tel que $n-1 = (p_i-1) \times m_i$. Soit $a \in \mathbb{Z}$ et soit $i \in \llbracket 1; r \rrbracket$.

- ★ Supposons que a soit premier avec p_i . D'après le théorème de Fermat, $a^{p_i-1} \equiv 1[p_i]$ donc

$$a^{n-1} = (a^{p_i-1})^{m_i} \equiv 1^{m_i} \equiv 1[p_i]$$

c'est-à-dire que p_i divise $a^{n-1} - 1$ donc p_i divise $a^n - a$.

- ★ Supposons que a ne soit pas premier avec p_i . Alors p_i divise a donc divise $a^n - a$.

Dans tous les cas, p_i divise $a^n - a$. Les p_i étant premiers distincts, ils sont premiers entre eux donc $n = p_1 \times \cdots \times p_r$ divise $a^n - a$ donc $a^n \equiv a[n] : n$ est un nombre de Carmichael.

- Montrer que 561 est un nombre de Carmichael.

$561 = 3 \times 11 \times 17$ et 560 est divisible par 2, 10 et 16 donc, d'après le critère précédent, 561 est un nombre de Carmichael.

Remarque : 561 est le plus petit nombre de Carmichael. On montre de même que $1105 = 5 \times 13 \times 17$ et $1729 = 7 \times 13 \times 19$ sont des nombres de Carmichael. On sait depuis peu (1994) qu'il y en a une infinité.

Les nombres de Carmichael sont donc les nombres qui font « mentir » la réciproque (fautive) du théorème de Fermat : ce sont les nombres qui, bien que composés, réussissent le test de primalité évident tiré du théorème de Fermat (et donc prouvent que ce « test » n'est en fait pas valable).

La réciproque est vraie : on peut le montrer à l'aide d'un résultat au programme de deuxième année appelé le lemme chinois. Cela permet par exemple de montrer qu'un nombre de Carmichael a au moins trois facteurs premiers distincts (exo).