16 Arithmétique des entiers

Dans ce chapitre, nous étudions les propriétés de $\mathbf{N}$ et de $\mathbf{Z}$, sans jamais nous préoccuper de l'existence d'ensembles plus grands (que ce soit $\mathbf{Q}$, $\mathbf{R}$ ou $\mathbf{C}$).
L'une des «faiblesses» de $\mathbf{Z}$ est l'absence d'une division toujours bien définie : dans $\mathbf{Q}, \mathbf{R}$ ou $\mathbf{C}$ tout nombre non nul divise n'importe quel nombre[1], ce qui n'est absolument pas vrai dans $\mathbf{Z}$.
Par exemple, on ne peut pas parler, en restant dans $\mathbf{Z}$ du quotient de 3 par 2.
Cette faiblesse fait toute la richesse[2] de $\mathbf{Z}$ car elle nous oblige à introduire les notions de diviseurs, multiples, nombres premiers, etc, que nous allons étudier dans ce chapitre.

[1] $a = b \times \frac{a}{b}$.

[2] Et la beauté !

16.1 Relation de divisibilité

16.1.1 Diviseurs, multiples

Définition 16.1 – Soient $(a, b) \in \mathbf{Z}^2$. On dit que a **divise** b et on note $a \mid b$ s'il existe $k \in \mathbf{Z}$ tel que $b = ak$.
On dit alors que a **est un diviseur de** b, et que b **est un multiple de** a.

Autrement dit
Les multiples de a sont les éléments de
$$a\mathbf{Z} = \{ak,\ k \in \mathbf{Z}\}.$$

Notons que -1 et 1 divisent tous les entiers, puisqu'on a toujours $a = 1 \times a = (-1) \times (-a)$.
En revanche, les seuls diviseurs de 1 ou de -1 sont ± 1.
Tous les entiers sont diviseurs de 0, puisque pour tout $k \in \mathbf{Z}$, $0 = 0 \times k$.
En revanche, 0 est le seul multiple de 0.

Proposition 16.2 : *Soit $n \in \mathbf{Z}$, non nul. Alors l'ensemble $\mathcal{D}(n) = \{a \in \mathbf{Z},\ a \text{ divise } n\}$ des diviseurs de n est un ensemble fini.*

Démonstration. Si $a \mid n$, alors il existe $k \in \mathbf{Z}$ tel que $n = ak$, et nécessairement, $k \neq 0$, donc $k \geqslant 1$.
Et donc $|a| \leqslant |n|$, de sorte que $a \in [\![-n, n]\!]$. Donc $\mathcal{D}(n) \subset [\![-n, n]\!]$, qui est un ensemble fini, donc $\mathcal{D}(n)$ est lui-même fini. □

Exemple 16.3

$\mathcal{D}(7) = \mathcal{D}(-7) = \{-7, -1, 1, 7\}$ et $\mathcal{D}(10) = \{-10, -5, -2, -1, 1, 2, 5, 10\}$.

Nous avons mentionné précédemment que la relation de divisibilité est une relation d'ordre sur $\mathbf{N}$, malheureusement cela n'est plus vrai sur $\mathbf{Z}$, car on perd l'antisymétrie.
Par exemple, on a $-2 \mid 2$, $2 \mid -2$, et pourtant $2 \neq -2$.
En revanche, la réflexivité et la transitivité restent vraies sur $\mathbf{Z}$, et on dispose du résultat suivant : si $a \mid b$ et $b \mid a$, alors $|a| = |b|$ (ou encore $a = \pm b$).

Proposition 16.4 : *Soient $a, b, n \in \mathbf{Z}$.*

1. *Si $n \mid a$ et $n \mid b$, alors $n \mid a + b$*
2. *Si $n \mid a$, alors pour tout $c \in \mathbf{Z}$, $n \mid ac$.*

Démonstration. 1. Si $n \mid a$, alors il existe $k \in \mathbf{Z}$ tel que $a = kn$ et de même, il existe $k' \in \mathbf{Z}$ tel que $b = k'n$.
Et donc $a + b = kn + k'n = (k + k')n$, donc $n \mid a + b$.
2. Si $a = kn$, alors $ac = n(kc)$, donc $k \mid ac$.

□

Corollaire 16.5 – *Si $n \mid a$ et $n \mid b$, alors pour tous $(u, v) \in \mathbf{Z}^2$, $n \mid au + bv$.*

16.1.2 Calcul modulaire

Rappelons que pour $n \in \mathbf{N}^*$, on dispose d'une relation d'équivalence sur $\mathbf{Z}$ qui est la relation de congruence modulo n :

$$a \equiv b \quad [n] \Leftrightarrow \exists k \in \mathbf{Z},\ a - b = kn \Leftrightarrow n \mid (a - b).$$

Notons qu'en particulier, n divise a si et seulement si $a \equiv 0 \quad [n]$.

Proposition 16.6 (Calculs en congruence) : *Soit $n \in \mathbf{N}^*$, et soient a, b, c, d des entiers.*

1. *Si $a \equiv b \quad [n]$ et $c \equiv d \quad [n]$, alors $a + c \equiv b + d \quad [n]$.*
2. *Si $a \equiv b \quad [n]$ et $c \equiv d \quad [n]$, alors $ac \equiv bd \quad [n]$.*
   En particulier, pour tout $k \in \mathbf{N}$, $a^k \equiv b^k \quad [n]$.
3. *Pour $m \in \mathbf{N}^*$, on a $a \equiv b \quad [n] \Leftrightarrow am \equiv bm \quad [mn]$.*

Démonstration. 1. Il existe $k_1, k_2 \in \mathbf{Z}$ tels que $a - b = nk_1$ et $c - d = nk_2$. Et donc en sommant ces relations, $(a + c) - (b + d) = n(k_1 + k_2)$ de sorte que $a + c \equiv b + d \quad [n]$.
2. Avec les mêmes notations :

$$ac = (b + nk_1)(d + nk_2) = bd + n(k_1 d + k_2 b + nk_1 k_2) \Leftrightarrow ac - bd = n\underbrace{(k_1 d + k_2 b + nk_1 k_2)}_{\in \mathbf{Z}}.$$

Donc $ac \equiv bd \pmod{n}$.
La relation sur les puissances en découle directement, par récurrence sur k.
3. On a

$$\begin{aligned} a \equiv b \quad [n] &\Leftrightarrow \exists k \in \mathbf{Z},\ a - b = kn \\ &\Leftrightarrow \exists k \in \mathbf{Z},\ m(a - b) = mnk \\ &\Leftrightarrow \exists k \in \mathbf{Z},\ am - bm = (mn)k \\ &\Leftrightarrow am \equiv bm \quad [mn]. \end{aligned}$$

□

⚠ La relation de congruence modulo α, avec $\alpha \in \mathbf{R} \setminus \mathbf{Z}$ (on pensera notamment à $\alpha = 2\pi$...)est encore compatible avec l'addition, mais pas avec la multiplication[3].

[3] Je vous laisse le soin de trouver ce qui ne va pas marcher dans la preuve ci-dessus...

Exemples 16.7

► $36^{2020} - 13^{2020}$ est divisible par 7. En effet, on a

$$36^{2020} - 13^{2020} \equiv 1^{2020} - (-1)^{2020} \equiv 1 - 1 \equiv 0 \quad [7].$$

► $117^{119} - 8$ est divisible par 17.
On a $117 = 7 \times 17 - 2 \equiv -2 \quad [17]$. Et donc $117^{119} \equiv (-2)^{119} \quad [17]$.
Or, par élévations au carré successives, on a

$$(-2)^2 \equiv 4 \quad [17],\ (-2)^4 \equiv 4^2 \equiv 16 \equiv -1 \quad [17],\ (-2)^8 \equiv (-1)^2 \equiv 1 \quad [17].$$

Mais $119 = 8 \times 14 + 7$ et donc $(-2)^{119} = (-2)^{8\times14+7} = \left((-2)^8\right)^{14}(-2)^7$, de sorte que

$$117^{119} \equiv (-2)^{119} \equiv \left((-2)^8\right)^{14}(-2)^7 \equiv 1 \times (-2)^7 \quad [117].$$

Et alors $(-2)^7 \equiv (-2)^4(-2)^2(-2) \equiv 4(-1)(-2) \equiv 8 \quad [17]$, d'où le résultat annoncé.

16.1.3 Division euclidienne

La division euclidienne dans $\mathbf{Z}$ n'est rien d'autre que la division telle que vous l'avez apprise à l'école primaire : on reste dans $\mathbf{Z}$, on ne fait pas apparaître un nombre à virgule, mais un quotient et un reste.
Par exemple, le quotient de la division de 131 par 7 vaut 18, et le reste vaut 5, ce qui signifie que $131 = 18 \times 7 + 5$.

Proposition 16.8 : *Soient $a \in \mathbf{Z}$ et soit $b \in \mathbf{N}^*$.*
Alors il existe un unique couple $(q, r) \in \mathbf{Z} \times \mathbf{N}$ tel que

$$a = bq + r \text{ et } 0 \leqslant r < b.$$

*L'écriture $a = bq + r$ est appelée **division euclidienne de a par b**, q est appelé quotient de la division euclidienne de a par b, et r est appelé le reste.*

Démonstration. Commençons par l'unicité, et supposons qu'on dispose de deux écritures $a = bq_1 + r_1 = bq_2 + r_2$, avec $0 \leqslant r_1 < b$ et $0 \leqslant r_2 < b$.
Alors $0 = a - a = bq_1 + r_1 - (bq_2 + r_2) = b(q_1 - q_2) + r_1 - r_2 \Leftrightarrow r_2 - r_1 = b(q_1 - q_2)$.
Donc b divise $r_2 - r_1$, alors que $-b < r_2 - r_1 < b$. Ceci n'est possible que si $r_2 - r_1 = 0 \Leftrightarrow r_1 = r_2$.
Et alors $bq_1 = bq_2 \Leftrightarrow q_1 = q_2$.

Passons à l'existence, et notons $a + b\mathbf{Z} = \{a + bk,\ k \in \mathbf{Z}\}$ l'ensemble des entiers congrus à a modulo b.
Alors $(a + b\mathbf{Z}) \cap \mathbf{N}$ est non vide, car il contient $a = a + 0b$ si $a \geqslant 0$ et $a - ab$ si $a < 0$.
Comme toute partie non vide de $\mathbf{N}$, elle possède donc un plus petit élément, notons-le r.
Par définition, il existe donc $q_1 \in \mathbf{Z}$ tel que $a + bq_1 = r$.
On a alors $r < b$, car si on avait $r \geqslant b$, alors $r - b$ serait toujours un entier positif, et $r - b = a + b(q_1 - 1) \in a + b\mathbf{Z}$, contredisant la minimalité de r.
En posant $q = -q_1$, on a alors bien $a = bq + r$ et $0 \leqslant r < b$. □

Remarque
À ce stade, nous avons prouvé que la division euclidienne, **si elle existe**, est unique. Reste à prouver qu'elle existe !

Remarques.
- La méthode qu'on vous a expliquée au primaire[4] pour trouver q et r reste valable, et on ne peut pas faire beaucoup mieux !
- L'idée de base étant[5] globalement de partir de a et de retrancher b autant de fois que possible à a, en restant dans $\mathbf{N}$. Le nombre maximal de fois que l'on peut retrancher b à a est alors le quotient q.
- Il n'est pas très dur de constater que $q = \left\lfloor \frac{a}{n} \right\rfloor$ (et alors $r = a - bq$).
- Attention aux nombres négatifs ! Nous avons dit précédemment que $131 = 18\times7+5$. On n'en déduit pas que $-131 = -18 \times 7 - 5$ est la division euclidienne de -131 par 7, car -5 est négatif....
  La division cherchée est $-131 = -19 \times 7 + 2$.

[4] «Poser» la division.

[5] Au moins si a et b sont positifs.

Proposition 16.9 : *Soit $n \in \mathbf{N}^*$.*

1. *Soit $a \in \mathbf{Z}$ et soit $a = nq + r$ la division euclidienne de a par n, avec $0 \leqslant r < n$. Alors a est congru à r modulo n.*
2. *Soient $(a, b) \in \mathbf{Z}^2$. Alors a et b sont congrus modulo n si et seulement si ils ont le même reste dans la division euclidienne par n.*

Démonstration. 1. C'est immédiat en utilisant la compatibilité de la congruence avec l'addition et la multiplication : $a \equiv nq + r \equiv 0 + r \equiv r \quad [n]$.

2. Notons $a = nq_1 + r_1$ et $b = nq_2 + r_2$ les divisions respectives de a et b par n.
Supposons dans un premier temps a et b congrus modulo n : $a \equiv b \quad [n]$.
Et donc par le point 1), $r_1 \equiv r_2 \quad [n]$. Il existe donc $k \in \mathbf{Z}$ tel que $r_1 - r_2 = kn$.
Or, $-n < r_1 - r_2 < n$, de sorte que $k = 0$, et donc $r_1 - r_2 = 0 \Leftrightarrow r_1 = r_2$.

Inversement, si $r_1 = r_2$, alors $a \equiv r_1 \equiv r_2 \equiv b \quad [n]$.

□

Exemple 16.10

Déterminons le reste de la division euclidienne de 67^{2020} par 7.
Cela revient à trouver $r \in [\![0, 6]\!]$ tel que $67^{2020} \equiv r \pmod 7$.
Or, on a $67 = 63 + 4 \equiv 4 \pmod 7$.
Puis $4^2 \equiv 16 \equiv 2 \pmod 7$ et donc $4^3 \equiv 8 \equiv 1 \pmod 7$.
Par conséquent, pour tout $k \in \mathbf{N}$, $4^{3k} \equiv 1 \pmod 7$.
Il nous faut alors le reste de la division euclidienne par 3. Mais nous n'avons pas besoin de cette division euclidienne : 2019 est divisible[6] par 3, donc il existe $k \in \mathbf{N}$ tel que $2019 = 3k$ donc $2020 = 3k + 1$. Le reste cherché est 3.
On a donc $67^{2020} \equiv 4^{2020} \equiv 4^{3k} \times 4 \pmod 7 \equiv 4 \pmod 7$.
Et donc le reste de la division euclidienne de 67^{2020} par 7 vaut 4.

[6] Vois ci-dessous.

Profitons-en pour reprouver le critère usuel de divisibilité par 3 : un nombre est divisible par 3 si et seulement si la somme de ses chiffres (en base 10) est divisible par 3.

Soit donc $n = \sum_{k=0}^{p} a_k 10^k$ un entier.

Alors $10 \equiv 1 \pmod 3$ de sorte que pour tout k, $10^k \equiv 1^k \equiv 1 \pmod 3$.

Et donc $n \equiv \sum_{k=0}^{p} a_k 10^k \equiv \sum_{k=0}^{p} a_k \pmod 3$.

Par conséquent, $n \equiv 0 \pmod 3$ si et seulement si $\sum_{k=0}^{p} a_k \pmod 3$.

Corollaire 16.11 – *Soit $a \in \mathbf{Z}$ et soit $n \in \mathbf{N}^*$. Alors il y a équivalence entre :*

1. *a est divisible par n ;*
2. *le reste de la division euclidienne de a par n est nul.*
3. *$a \equiv 0 \quad [n]$;*

Unicité

Nous utilisons ici vraiment l'unicité de la division euclidienne, et pas seulement le fait qu'une telle écriture $a = qn + r$ existe, mais vraiment le fait qu'elle est unique :si on a une telle écriture sous les yeux, alors c'est nécessairement la division euclidienne.

Démonstration. 1) ⇒ 2) : si a est divisible par n, il existe $q \in \mathbf{Z}$ tel que $a = qn = qn + 0$. Par unicité de la division euclidienne, le quotient de la division euclidienne de a par n vaut q, et surtout le reste vaut 0.

2) ⇒ 3) Immédiat d'après le point 1) de la proposition précédente.

3) ⇒ 1) Si $a \equiv 0 \quad [n]$, alors il existe $k \in \mathbf{Z}$ tel que $a - 0 = kn \Leftrightarrow a = kn$, donc a est divisible par n. □

Corollaire 16.12 – *Il y a exactement n classes d'équivalence pour la congruence modulo n, qui sont $\overline{0}, \overline{1}, \ldots, \overline{n-1}$.*

Démonstration. Les restes possibles dans la division euclidienne par n sont $0, 1, 2, \dots, n-1$.
Et d'après le point 1) de la proposition 16.9, tout élément de $\mathbf{Z}$ est congru à l'un de ces nombres, donc dans l'une des classes d'équivalence $\overline{0}, \overline{1}, \dots, \overline{n-1}$.

Reste donc à voir que ces classes sont bien distinctes. Mais pour $r_1, r_2 \in [\![0, n-1]\!]$, on a $\overline{r_1} = \overline{r_2}$ si et seulement si $r_1 \equiv r_2 \pmod{n}$.
Soit encore si et seulement si il existe $r_1 - r_2$ est divisible par n.
Mais puisque $-(n-1) \leqslant r_1 - r_2 \leqslant n-1$, $r_1 - r_2$ n'est divisible par n que s'il vaut 0, c'est-à-dire si $r_1 = r_2$.
Donc par contraposée, si r_1, r_2 sont deux éléments distincts de $[\![0, n-1]\!]$, alors $\overline{r_1}$ et $\overline{r_2}$ sont distinctes[7]. □

[7] Et même disjointes, puisque deux classes d'équivalence qui ne sont pas égales n'ont aucun élément en commun.

16.1.4 Nombres premiers

Définition 16.13 – Un **nombre premier** est un entier positif qui possède exactement deux diviseurs positifs.
Un entier qui n'est pas premier est dit **composé**.

Notons qu'un nombre premier ne peut donc pas être nul[8], ne peut pas non plus être égal à 1 (qui ne possède que lui-même comme diviseur positif).
Et puisqu'un entier $n \geqslant 2$ est toujours divisible à la fois par 1 et par lui-même, les diviseurs positifs d'un nombre premier p sont nécessairement 1 et p.
On pourrait d'ailleurs donner comme définition d'un nombre premier : un nombre supérieur ou égal à 2 qui n'est divisible que par 1 et par lui-même.
Autrement dit, $p \geqslant 2$ est premier si et seulement si $\forall (a, b) \in \mathbf{N}^2,\ p = ab \Rightarrow (a = 1 \text{ ou } b = 1)$.

[8] Car 0 a une infinité de diviseurs.

Exemples 16.14

Les premiers nombres premiers sont $2, 3, 5, 7, 11, 13, 17$.
En revanche, $4 = 2 \times 2, 6 = 2 \times 3, 8 = 2 \times 4, 9 = 3 \times 3, 12 = 3 \times 4, 14 = 7 \times 2$ et $15 = 3 \times 5$ ne sont pas premiers.

Terminologie
Un nombre qui n'est pas premier est dit **composé**.

Notons que 2 est le seul nombre premier pair, puisqu'un nombre pair strictement supérieur à 2 possède 2 comme diviseur, et ne saurait donc être premier.
L'importance des nombres premiers réside dans le résultat suivant, que nous raffinerons très vite, et qui dit que les nombres premiers sont en quelque sorte les «briques» à partir desquelles on peut construire tous les entiers.

Proposition 16.15 : *Tout entier naturel non nul est produit de nombres premiers.*

Démonstration. Traitons tout de suite le cas peu intéressant de 1, qui est le produit de 0 nombres premiers.
Prouvons par récurrence forte sur $n \geqslant 2$ que n est produit de premiers.
L'initialisation est aisée : car 2 est premier et donc : $2 = 2$ (produit de 1 terme).
Supposons que tout entier de $[\![2, n]\!]$ soit produit de nombres premiers.
Soit $p_1 = \min(\mathcal{D}(n+1) \setminus \{1\})$ le plus petit diviseur de $n+1$ strictement supérieur à 1.
Notons qu'un tel diviseur existe puisque $\mathcal{D}(n+1) \setminus \{1\}$ n'est pas vide : il contient $n+1$.
Alors p_1 est premier. En effet, supposons par l'absurde que $p_1 = ab$, avec $a > 1$ et $b > 1$.
Alors $b \geqslant 2$ et donc $a = \dfrac{p_1}{b} < p_1$. Or, b étant un diviseur de p_1, c'est un diviseur de $n+1$, contredisant la minimalité de p_1.

Il existe donc $k \in \mathbf{N}$ tel que $n+1 = p_1 k$. Puisque $p_1 > 1$, $k < n+1$ et donc $k \leqslant n$.
Par hypothèse de récurrence, il existe donc des nombres premiers $p_2, p_3, \dots, p_r$ tels que $k = p_2 p_3 \cdots p_r$.
Et donc $n+1 = p_1 p_2 \cdots p_r$ est produit de nombres premiers.
Par le principe de récurrence forte, tout entier supérieur ou égal à 2 est produit de nombres premiers. □

Rappel
Par **convention**, un produit de 0 termes vaut 1...

Théorème 16.16 : *Il existe une infinité de nombres premiers.*

Démonstration. Raisonnons par l'absurde et supposons qu'il existe un nombre fini N de nombres premiers, et notons $\{p_1, p_2, \dots, p_N\}$ l'ensemble de tous les nombres premiers.
Soit alors $n = \prod_{k=1}^{N} p_k + 1$. Alors n possède au moins un diviseur premier, donc il existe $i \in [\![1, N]\!]$ tel que $p_i \mid n$.
Mais p_i divise $\prod_{k=1}^{N} p_k$, et donc p_i divise $n - \prod_{k=1}^{N} p_k = 1$.
Par conséquent, $p_i = 1$, contredisant la primalité de p_i.
Nous tenons donc notre contradiction : c'est que notre hypothèse de départ est fausse, et donc il existe une infinité de nombres premiers. □

Pour déterminer les nombres premiers inférieurs à un entier n fixé, on utilise le crible d'Ératosthène vu en TP.

Mentionnons que le problème de déterminer si un grand nombre est premier est difficile, au sens où il nécessite beaucoup de calculs.
C'est plutôt une bonne nouvelle, puisque c'est sur ce principe que reposent la plupart des algorithmes cryptographiques utilisés aujourd'hui.

16.2 PLUS GRAND COMMUN DIVISEUR (PGCD), PLUS PETIT COMMUN MULTIPLE (PPCM)

16.2.1 PGCD de deux entiers

Définition 16.17 – Soient $(a, b) \in \mathbf{Z}^2$, $(a, b) \neq (0, 0)$ deux entiers non simultanément nuls[9]. Le **plus grand commun diviseur** (en abrégé PGCD) de a et b est $a \wedge b = \max(\mathcal{D}(a) \cap \mathcal{D}(b))$.
Par convention, on pose $0 \wedge 0 = 0$.

[9] Donc l'un des deux peut être nul, mais pas les deux.

Remarque
Comme son nom l'indique, c'est bien le plus grand (au sens de la relation d'ordre usuelle $\leqslant$) nombre qui divise à la fois a et b.

Remarques. ► Si $a \neq 0$, alors $\mathcal{D}(a)$ est majoré par $|a|$ et donc $\mathcal{D}(a) \cap \mathcal{D}(b)$ est majoré. Puisqu'il s'agit d'une partie non vide (elle contient 1) de $\mathbf{Z}$, elle admet bien un plus grand élément.
► Si $b = 0$, alors $\mathcal{D}(a) \cap \mathcal{D}(b) = \mathcal{D}(a)$ et donc $a \wedge 0 = |a|$.

Exemples 16.18

► $60 \wedge 18 = 6$ car $\mathcal{D}(60) \cap \mathcal{D}(18) = \{\pm 1, \pm 2, \pm 3, \pm 6\}$.
► Si $b \mid a$, alors $a \wedge b = |b|$.

Proposition 16.19 : *Soient $(a, b) \in \mathbf{Z}^2$, avec $(a, b) \neq (0, 0)$, et soit $d \in \mathbf{Z}$. S'il existe $(u, v) \in \mathbf{Z}^2$ tels que $au + bv = d$, alors $a \wedge b \mid d$.*

Démonstration. Le PGCD de a et b divise a et divise b, donc il divise $au + bv = d$. □

16.2.2 L'algorithme d'Euclide

Lemme 16.20. Soient $(a, b) \in \mathbf{Z}^2$. Alors, pour tout $k \in \mathbf{Z}$, $a \wedge b = (a + kb) \wedge b$.

Démonstration. Si $b = 0$, le résultat est trivial, on suppose donc $b \neq 0$.
Si un entier d divise à la fois a et b, alors il divise $a + kb$, et divise toujours b.
Inversement, si d divise à la fois $a + kb$ et b, alors il divise $a = (a + kb) - kb$ et b.
Nous venons donc de prouver que $\mathcal{D}(a) \cap \mathcal{D}(b) = \mathcal{D}(a + kb) \cap \mathcal{D}(b)$.
Et donc en passant au maximum $a \wedge b = (a + kb) \wedge b$. □

1	2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50
51	52	53	54	55	56	57	58	59	60
61	62	63	64	65	66	67	68	69	70
71	72	73	74	75	76	77	78	79	80
81	82	83	84	85	86	87	88	89	90
91	92	93	94	95	96	97	98	99	100

Le premier nombre premier est 2. On barre tous les multiples de 2, le premier nombre non barré, à savoir 3 est premier.

1	2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50
51	52	53	54	55	56	57	58	59	60
61	62	63	64	65	66	67	68	69	70
71	72	73	74	75	76	77	78	79	80
81	82	83	84	85	86	87	88	89	90
91	92	93	94	95	96	97	98	99	100

On barre à présent les multiples de 3 qui n'ont pas été barrés précédemment. Le premier nombre non encore barré, ici 5, est premier.

1	2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50
51	52	53	54	55	56	57	58	59	60
61	62	63	64	65	66	67	68	69	70
71	72	73	74	75	76	77	78	79	80
81	82	83	84	85	86	87	88	89	90
91	92	93	94	95	96	97	98	99	100

On barre à présent les multiples de 5. Le premier nombre non encore barré, ici 7, est premier.

1	2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50
51	52	53	54	55	56	57	58	59	60
61	62	63	64	65	66	67	68	69	70
71	72	73	74	75	76	77	78	79	80
81	82	83	84	85	86	87	88	89	90
91	92	93	94	95	96	97	98	99	100

On barre les multiples de 7. On a traité le cas de tous les premiers jusqu'à $10 = \sqrt{100}$. Tous les nombres encore non barrés sont premiers.

FIGURE 16.1 – Le crible d'Ératosthène pour déterminer les premiers inférieurs à 100.

Corollaire 16.21 – *Soient $a \in \mathbf{Z}$, $b \in \mathbf{N}^*$, et soit $a = bq + r$ la division euclidienne de a par b. Alors $a \wedge b = r \wedge b$.*

Démonstration. Il s'agit juste de remarque que $r = a - bq$. □

Les résultats qui précèdent nous permettent de mettre en œuvre un algorithme simple, appelé **algorithme d'Euclide** pour le calcul du PGCD de deux entiers, qui ne nécessite pas de déterminer tous les multiples de ces deux entiers.
Soient donc a et b deux entiers naturels[10] non nuls.
Notons r_1 le reste de la division euclidienne de a par b. On a donc $0 \leqslant r_1 < b$.
Par le corollaire 16.21, $a \wedge b = r_1 \wedge b$.
Notons alors r_2 le reste de la division euclidienne de b par r_1. On a alors $0 \leqslant r_2 < r_1$.
De proche en proche, on définit alors r_{k+1} comme étant le reste de la division euclidienne de r_{k-1} par r_k. Ceci n'est possible que tant que $r_k \neq 0$.
On obtient alors une suite strictement décroissante (car $r_{k+1} < r_k$) d'éléments de $[\![0, b-1]\!]$.
Cette suite est donc nécessairement finie[11], puisque $[\![0, b-1]\!]$ est fini.

[10] Changer le signe de a et/ou de b ne change pas le PGCD.

[11] Et même de cardinal au plus b.

Autrement dit, il existe un rang n tel que $r_n = 0$.
Et alors, par applications successive du corollaire 16.21,

$$a \wedge b = b \wedge r_1 = r_1 \wedge r_2 = \cdots = r_{n-1} \wedge r_n = r_{n-1} \wedge 0 = r_{n-1}.$$

Ainsi, dans le procédé décrit ci-dessus, $a \wedge b$ est le dernier reste **non nul.**

Exemple 16.22

Calculons $1540 \wedge 882$. On a $1540 = 882 + 658$.
Puis $882 = 658 + 224$, $658 = 2 \times 224 + 210$, $224 = 210 + 14$, $210 = 15 \times 14 + 0$.
Et donc $1540 \wedge 882 = 14$.

En Python, l'algorithme d'Euclide s'écrit de la manière suivante :

```
1 def pgcd(a,b) :
2         while a%b  != 0 :
3                 a,b = b,a%b
4         return b
```

Proposition 16.23 : *Soit $(a,b) \in \mathbf{Z}^2$, $(a,b) \neq (0,0)$. Alors un entier d divise à la fois a et b si et seulement si il divise leur PGCD.*
Autrement dit, $\mathcal{D}(a) \cap \mathcal{D}(b) = \mathcal{D}(a \wedge b)$.

Démonstration. Une fois de plus, nous ne traitons que le cas de a et b positifs, puisque les signes n'ont ici aucune importance.
En reprenant les notations de l'algorithme d'Euclide, on a[12]

$$\mathcal{D}(a) \cap \mathcal{D}(b) = \mathcal{D}(r_1) \cap \mathcal{D}(b) = \cdots = \mathcal{D}(r_{n-1}) \cap \mathcal{D}(r_n) = \mathcal{D}(r_{n-1}) \cap \mathbf{Z} = \mathcal{D}(r_{n-1}) = \mathcal{D}(a \wedge b).$$

□

[12] Cf la preuve 16.20.

Remarque. Le PGCD $a \wedge b$ avait été défini comme étant le plus grand (au sens de la relation d'ordre) élément de $\mathcal{D}(a) \cap \mathcal{D}(b)$.
Ce que prouve la proposition qui précède, c'est que c'est également le plus grand élément, au sens de la relation d'ordre liée à la divisibilité[13] de $\mathcal{D}(a) \cap \mathcal{D}(b) \cap \mathbf{N}$. En effet, tout diviseur commun à a et à b est un diviseur de $a \wedge b$, donc plus petit que $a \wedge b$ pour la relation $|$.
On peut également noter que $a \wedge b = \inf\{a,b\}$, la borne inférieure étant entendu au sens de la relation de divisibilité : c'est le plus grand (au sens de la divisibilité) minorant de $\{a,b\}$ (donc diviseur de a et de b).

[13] Qui n'est une relation d'ordre uniquement sur $\mathbf{N}$.

Proposition 16.24 : *Soient $a,b \in \mathbf{Z}$, avec $(a,b) \neq (0,0)$ et soit $d \in \mathbf{N}$.*

$$\text{Alors } d = a \wedge b \text{ si et seulement si } \begin{cases} d \mid a \\ d \mid b \\ \forall n \in \mathbf{Z},\ (n \mid a \text{ et } n \mid b) \Rightarrow n \mid d \end{cases}$$

Démonstration. Le sens direct découle de la proposition précédente.
Inversement, supposons que $d \in \mathbf{N}$ soit un diviseur commun de a et b tel que

$$\forall n \in \mathbf{Z},\ (n \mid a \text{ et } n \mid b) \Rightarrow n \mid d.$$

Alors $d \mid (a \wedge b)$ et en prenant $n = a \wedge b$, qui divise a et b, on a donc $a \wedge b \mid d$.
Donc $d = a \wedge b$. □

Proposition 16.25 : *Soient $(a,b,c,k) \in \mathbf{Z}$.*

1. $(a \wedge b) \wedge c = a \wedge (b \wedge c)$
2. $\forall k \in \mathbf{Z},\ (ak) \wedge (bk) = |k|(a \wedge b)$.

Démonstration. 1. Il s'agit de noter que

$$(\mathscr{D}(a)\cap\mathscr{D}(b))\cap\mathscr{D}(c)=\mathscr{D}(a)\cap\mathscr{D}(b)\cap\mathscr{D}(c)=\mathscr{D}(a)\cap(\mathscr{D}(b)\cap\mathscr{D}(c)).$$

2. Puisque $a\wedge b$ divise à la fois a et b, $|k|(a\wedge b)$ divise à la fois ak et bk.
Inversement, $|k|$ divise ak et bk, donc divise leur PGCD : il existe $d\in\mathbf{N}$ tel que $|k|d=(ak)\wedge(bk)$.
Donc $|k|d$ divise ak, et donc d divise a. De même, d divise b. Donc d divise $a\wedge b$.
Et après multiplication par $|k|$, $|k|d=(ak)\wedge(bk)$ divise $)|k|(a\wedge b)$.
On en déduit[14] que $(ak)\wedge(bk)=|k|(a\wedge b)$.

□

[14] C'est l'antisymétrie de la relation de divisibilité sur $\mathbf{N}$

16.2.3 Théorème de Bézout

Théorème 16.26 (Identité de Bézout, ou petit théorème de Bézout) : *Soient $(a,b)\in\mathbf{Z}^2$. Alors il existe $(u,v)\in\mathbf{Z}^2$ tels que $a\wedge b=au+bv$.*

Démonstration. Encore une fois, prouvons le résultat pour $b\geqslant 1$.
Plus précisément, nous allons prouver par récurrence forte sur $b\in\mathbf{N}^*$ la propriété $\mathscr{P}(b)$: «pour tout $a\in\mathbf{Z}$, $\exists(u,v)\in\mathbf{Z}^2$, $a\wedge b=au+bv$».
Initialisation : si $b=1$, alors pour tout $a\in\mathbf{Z}$, $a\wedge b=1=0\times a+1\times 1$.
Hérédité : supposons la propriété vraie jusqu'au rang $b-1$.
Soit $a\in\mathbf{Z}$, et soit $a=bq+r$ la division euclidienne de a par b.
Si $r=0$, alors $b\mid a$, et donc $a\wedge b=b=a\times 0+b\times 1$.
Si $r\neq 0$, alors $a\wedge b=b\wedge r$, et $1\leqslant r<b$.
Donc par hypothèse de récurrence, il existe $(u_1,v_1)\in\mathbf{Z}^2$ tels que $b\wedge r=bu_1+rv_1$.
Et donc $a\wedge b=b\wedge r=bu_1+(a-bq)v_1=av_1+b(u_1-qv_1)$.
Donc $\mathscr{P}(b)$ est vraie, et par le principe de récurrence, elle est vraie pour tout $b\geqslant 1$. □

⚠ L'identité de Bézout nous donne une implication, et pas une équivalence. Si un entier d vérifie $d=au+bv$, alors d n'est pas nécessairement le PGCD de a et de b, mais en revanche est un multiple de celui-ci.
Par exemple, $4\wedge 6=2$, et $8=14\times 4-6\times 8$.

⚠ Il n'y a pas unicité du couple (u,v) tel que $au+bv=a\wedge b$.
Par exemple, $18\wedge 30=6=(-3)\times 18+2\times 30=2\times 18+(-1)\times 30$.
Plus généralement, si $d=a\wedge b$ et si $au+bv=d$ est une relation de Bézout, alors pour tout $k\in\mathbf{Z}$, $a\left(u+k\dfrac{b}{d}\right)+b\left(v-k\dfrac{a}{d}\right)=d$ est une autre relation de Bézout.

Terminologie
Une telle relation est appelée relation de Bézout.

La preuve du théorème nous permet en fait de donner un algorithme pour trouver u et v, il suffit de modifier légèrement l'algorithme d'Euclide.
En effet, si $a=bq+r$, alors la connaissance d'une relation de Bézout pour le couple (b,r) nous donne une relation de Bézout pour le couple (a,b).
Plus précisément, si $b\wedge r=bu+rv$, alors

$$a\wedge b=b\wedge r=bu+rv=bu+(a-bq)v=av+b(u-qv).$$

Notons, $r_1,r_2,\dots,r_n$ (resp. $q_1,\dots,q_n$) les restes (resp. les quotients) successifs obtenus dans l'algorithme d'Euclide, où $a=q_1b+r_1$, et où $r_n=a\wedge b$.
Alors $a\wedge b=r_n=r_{n-2}-r_{n-1}q_{n-1}$: on a une relation de Bézout pour le couple (r_{n-2},r_{n-1}), relation que l'on notera $\mathscr{R}_{n-1}$.
Or, $r_{n-3}=r_{n-2}q_{n-1}+r_{n-1}\Leftrightarrow r_{n-1}=r_{n-3}-r_{n-2}q_{n-1}$.
En remplaçant alors r_{n-1} par $r_{n-3}-r_{n-2}q_{n-1}$ dans la relation $\mathscr{R}_{n-1}$, on obtient une relation de Bézout pour le couple (r_{n-3},r_{n-2}), relation que l'on notera $\mathscr{R}_{n-2}$.
De proche en proche, on finit donc par arriver à une relation de Bézout $(\mathscr{R}_1)$ pour le couple (b,r_1). Et puisque $r_1=a-bq_1$, on arrive alors à une relation de Bézout pour le couple (a,b).
Ce procédé est appelé algorithme d'Euclide étendu.

Autrement dit
On suppose que r_n est le dernier reste non nul lors de notre succession de divisions euclidiennes.

Exemple 16.27

Nous avons déjà calculé $1540 \wedge 882 = 14$.
Et en reprenant le détail des divisions euclidiennes effectuées, on a

$$\begin{aligned} 1540 = 882 + 658 &\Leftrightarrow 658 = 1540 - 882 \\ 882 = 658 + 224 &\Leftrightarrow 224 = 882 - 658 \\ 658 = 2 \times 224 + 210 &\Leftrightarrow 210 = 658 - 2 \times 224 \\ 224 = 210 + 14 &\Leftrightarrow 14 = 224 - 210. \end{aligned}$$

Donc il vient

$$\begin{aligned} 14 &= 224 - 210 \\ &= 224 - (658 - 2 \times 224) = -658 + 3 \times 224 \\ &= -658 + 3 \times (882 - 658) = 3 \times 882 - 4 \times 658 \\ &= 3 \times 882 - 4(1540 - 882) = 7 \times 882 - 4 \times 1540. \end{aligned}$$

16.2.4 Entiers premiers entre eux

Définition 16.28 – Soient $(a, b) \in \mathbf{Z}^2 \setminus \{(0,0)\}$. On dit que a et b sont **premiers entre eux** si $a \wedge b = 1$.
Autrement dit si et seulement si les seuls entiers divisant à la fois a et b sont ± 1.

Exemples 16.29

- 2 et 5 sont premiers entre eux.
- Plus généralement, deux nombres premiers distincts sont toujours premiers entre eux.

Théorème 16.30 (De Bézout) : *Deux entiers a et b sont premiers entre eux si et seulement si il existe $(u, v) \in \mathbf{Z}^2$ tel que $au + bv = 1$.*

Démonstration. Le sens $\Rightarrow$ a déjà été vu, puisque $a \wedge b = 1$.
Pour la réciproque, rappelons nous que si $n \in \mathbf{Z}$ est un diviseur à la fois de a et de b, alors c'est un diviseur de $au + bv$.
Et donc si il existe u et v tels que $au + bv = 1$, alors $a \wedge b$, qui divise à la fois a et b, divise 1, et donc vaut ± 1.
Étant positif, il vaut 1 et on a donc $a \wedge b = 1$. □

⚠ Si $au + bv = d$ n'est pas égal à 1, on peut toujours uniquement affirmer que $a \wedge b \mid d$, mais pas qu'il est égal à d.
Par exemple, $28 = 882 \times 2 - 1540 \times 8$, mais le PGCD de 882 et 1540 ne vaut pas 28, il divise seulement 28.

Proposition 16.31 : *Soient a, b, c trois entiers non nuls. Alors a est premier avec bc si et seulement si a est premier avec b et premier avec c.*

Démonstration. $\Rightarrow$ Si $a \wedge bc = 1$, soit alors d un diviseur commun à a et b.
Alors d divise à la fois a et bc, et donc divise 1. Donc $a \wedge b = 1$.
Et sur le même principe, $a \wedge c = 1$.

$\Leftarrow$ Inversement, supposons que $a \wedge b = a \wedge c = 1$.
Alors par le théorème de Bézout[15], il existe deux couples d'entiers (u_1, v_1) et (u_2, v_2) tels

[15] En fait, ici on n'utilise que le sens «identité de Bézout».

que $1 = au_1 + bv_1$ et $1 = au_2 + cv_2$.
Alors, en multipliant ces deux relations, il vient

$$1 = (au_1 + bv_1)(au_2 + cv_2) = a(u_1u_2 + u_1cv_2 + u_2bv_1) + bc(v_1v_2).$$

Et donc a et bc sont premiers entre eux. □

Corollaire 16.32 – *Soient $a, b_1, \dots, b_n$ des entiers. Alors a est premier avec le produit $b_1 \cdots b_n$ si et seulement si pour tout $i \in [\![1, n]\!]$, a est premier avec b_i.*

En abrégé

Un entier est premier avec un produit si et seulement si il est premier avec chacun de ses facteurs.

Démonstration. Par récurrence sur n. □

Proposition 16.33 (Lemme de Gauss) : *Si a divise bc et si a est premier avec b, alors a divise c.*

Démonstration. Il existe deux entiers u et v tels que $au + bv = 1$. Et donc $auc + bvc = c$.
Or, $a \mid auc$ et $a \mid bc$, donc $a \mid bvc$ et par conséquent $a \mid auc + bcv = c$. □

Corollaire 16.34 (Simplification dans des congruences) – *Soit $n \in \mathbf{N}^*$, et soient $a, b, k \in \mathbf{Z}$. Si $ak \equiv bk \pmod{n}$ et si $k \wedge n = 1$, alors $a \equiv b \pmod{n}$.*

Démonstration. Si $ak \equiv bk \pmod{n}$, alors $n \mid k(a-b)$.
Mais n étant premier avec k, n divise $a - b$, et donc $a \equiv b \pmod{n}$. □

Proposition 16.35 : *Soient a, b deux entiers, non tous deux nuls.*
Si on note $d = a \wedge b$ leur PGCD, alors il existe deux entiers a' et b' premiers entre eux tels que $a = da'$ et $b = db'$.
Réciproquement, s'il existe trois entiers $d, a', b' \in \mathbf{N} \times \mathbf{Z}^2$, avec $a' \wedge b' = 1$, tels que $a = da'$ et $b = db'$, alors $d = a \wedge b$

Démonstration. Le sens direct est facile : par définition, d divise à la fois a et b, donc il existe a' et b' tels que $a = da'$ et $b = db'$.
Si $n = a' \wedge b'$, alors dn divise à la fois a et b, donc divise d. Donc $dn \mid d \Leftrightarrow n \mid 1 \Leftrightarrow n = 1$.

Inversement, supposons l'existence de d, a', b' vérifiant les conditions de l'énoncé.
Alors $a \wedge b = d(a' \wedge b') = d$. □

Proposition-definition 16.36 Soit $r \in \mathbf{Q}$. Alors il existe un unique couple $(a, b) \in \mathbf{Z} \times \mathbf{N}^*$ avec a, b premiers entre eux et tel que $r = \dfrac{a}{b}$.
De plus, si $r = \dfrac{a'}{b'}$ avec $(a', b') \in \mathbf{Z} \times \mathbf{N}^*$, alors il existe $k \in \mathbf{Z}$ tel que $a' = ak$ et $b' = bk$.
L'écriture $r = \dfrac{a}{b}$ avec $a \wedge b = 1$ est appelée **forme irréductible** de r.

Démonstration. Pour l'existence, il suffit de noter que par définition de $\mathbf{Q}$, il existe $(u, v) \in \mathbf{Z} \times \mathbf{N}^*$ tels que $r = \dfrac{u}{v}$, et qu'alors, en posant $d = u \wedge v$, $u = du'$ et $v = dv'$, avec u' et v' premiers entre eux, alors $r = \dfrac{u'}{v'}$

Soit alors $r = \dfrac{a'}{b'}$, de sorte que $ab' = a'b$. Puisque a et b sont premiers entre eux, et que a divise $a'b$, a divise a'. Et de même, b divise b'.

Et alors $\frac{a'}{a} = \frac{b'}{b}$.
Enfin, si on a deux écritures de r sous forme irréductible, avec $r = \frac{a}{b} = \frac{c}{d}$, alors ce qui précède prouve que b divise d et d divise b. Mais b et d étant positifs, ils sont donc égaux. Et alors a divise c et c divise a, mais tous deux sont du même signe : celui de r. Donc $a = c$.
Et donc il y a bien unicité de la forme irréductible.

□

16.2.5 PPCM de deux entiers

Définition 16.37 – Soient $a, b \in \mathbf{Z}$ non nuls. On appelle **plus petit commun multiple de a et b**, et on note $a \vee b$ le plus petit[16] élément strictement positif multiple de a et b, c'est-à-dire $a \vee b = \min(a\mathbf{Z} \cap b\mathbf{Z} \cap \mathbf{N}^*)$.
Pour $a \in \mathbf{Z}$, on pose $a \vee 0 = 0 \vee a = 0$.

[16] Au sens de la relation d'ordre usuelle.

Proposition 16.38 : *Soient $a, b \in \mathbf{Z}$.*

1. *Les multiples communs de a et b sont exactement les multiples de $a \vee b$. Autrement dit, $a\mathbf{Z} \cap b\mathbf{Z} = (a \vee b)\mathbf{Z}$.*
2. $(a \vee b) \times (a \wedge b) = ab \Leftrightarrow (a \vee b) = \dfrac{ab}{a \wedge b}$.
3. *Pour tout $k \in \mathbf{Z}$, $(ak) \vee (bk) = |k|(a \vee b)$.*

Démonstration. Supposons que a et b sont positifs.
Notons $a = (a \wedge b)a'$ et $b = (a \wedge b)b'$, avec a' et b' premiers entre eux.
Alors $\frac{ab}{a \wedge b} = ab' = a'b$. Donc déjà, $\frac{ab}{a \wedge b}$ est un multiple commun à a et b.
Tout multiple de $a \vee b$ est un multiple de a et de b, donc $(a \vee b)\mathbf{Z} \subset a\mathbf{Z} \cap b\mathbf{Z}$.

Réciproquement, soit m un multiple commun à a et à b.
Alors $m = au = bv$. Après division par $a \wedge b$, on a $a'u = b'v$, avec $a' \wedge b' = 1$.
Donc $a' \mid b'v$, et donc par le théorème de Gauss, $a' \mid v$. Donc $v = a'v'$.
Et alors $m = (a \wedge b)b'v = (a \wedge b)b'a'v' = ba'v' = v'\dfrac{ab}{a \wedge b}$.
Donc m est un multiple de $\dfrac{ab}{a \wedge b}$.
Ainsi, $a\mathbf{Z} \cap b\mathbf{Z} \subset \dfrac{ab}{a \wedge b}\mathbf{Z}$.
Nous venons donc de prouver que $\dfrac{ab}{a \wedge b}$, qui est un multiple commun de a et b, divise tout multiple commun de a et b.
C'est le plus petit[17] multiple commun de a et b : par définition du PPCM, c'est $a \vee b$.
Ceci prouve à la fois les points 1) et 2).
Le dernier est évident : $(ak) \vee (bk) = \dfrac{k^2ab}{(ka) \wedge (kb)} = \dfrac{k^2ab}{|k|(a \wedge b)} = |k|(a \vee b)$.

[17] Au sens de la relation d'ordre $\leqslant$.

□

16.2.6 Familles de n entiers

Définition 16.39 – Soient $a_1, \dots, a_n$ des entiers non tous nuls. On appelle PGCD de $a_1, \dots, a_n$ le plus grand diviseur commun des a_i, c'est-à-dire $\max\left(\bigcap_{i=1}^{n} \mathcal{D}(a_i)\right)$.

Proposition 16.40 : *Avec les notations ci-dessus, si d est le PGCD de $a_1, \dots, a_n$, alors*

$$\mathcal{D}(d) = \bigcap_{i=1}^{n} \mathcal{D}(a_i).$$

Autrement dit, un entier divise à la fois $a_1, \dots, a_n$ si et seulement si il divise leur PGCD.

Démonstration. La preuve se fait par récurrence sur n, l'idée étant que si $d' = a_1 \wedge \cdots \wedge a_n$, alors

$$\bigcap_{i=1}^{n+1} \mathcal{D}(a_i) = \left(\bigcap_{i=1}^{n} \mathcal{D}(a_i)\right) \cap \mathcal{D}(a_{n+1}) = \mathcal{D}(d') \cap \mathcal{D}(d' \wedge a_{n+1}).$$

Mais $d' \wedge a_{n+1}$ est le plus grand élément de $\mathcal{D}(d' \wedge a_{n+1})$, et donc est le PGCD de $a_1, \cdots, a_{n+1}$. □

Remarque. Notons que cette preuve montre que le PGCD de $a_1, \cdots, a_{n+1}$ est égal au PGCD de $a_1, \cdots, a_n$ et de a_{n+1}, et qu'on peut donc le calculer par récurrence.
Le PGCD de $a_1, \dots, a_n$ est donc $a_1 \wedge (a_2 \wedge \cdots \wedge (a_{n-1} \wedge a_n))$.
Et comme nous avons déjà prouvé l'associativité du PGCD, les parenthèses ne sont pas indispensables, on peut noter $a_1 \wedge \cdots \wedge a_n$.

Proposition 16.41 (Identité de Bézout) : *Soient $a_1, \dots, a_n$ non tous nuls. Alors il existe $u_1, \cdots, u_n \in \mathbf{Z}$ tels que* $\sum_{i=1}^{n} a_i u_i = \bigwedge_{i=1}^{n} a_i$.

Démonstration. Par récurrence sur n : notons $d = a_1 \wedge \cdots \wedge a_n$, et supposons que $d = \sum_{i=1}^{n} a_i u_i$, alors $\bigwedge_{i=1}^{n+1} a_i = d \wedge a_{n+1}$.
Et donc l'identité de Bézout, il existe $u, v \in \mathbf{Z}$ tels que

$$d \wedge a_{n+1} = du + a_{n+1}v = d\left(\sum_{i=1}^{n} a_i u_i\right)u + a_{n+1}v = \sum_{i=1}^{n} a_i d u_i + a_{n+1}v.$$

□

Définition 16.42 – Soient $a_1, \dots, a_n$ des entiers non tous nuls. On dit que $a_1, \dots, a_n$ sont **premiers entre eux dans leur ensemble** si leur PGCD vaut 1 (ou de manière équivalente, si leurs seuls diviseurs communs sont ± 1).

⚠ Si des entiers $a_1, \dots, a_n$ sont deux à deux premiers, alors ils sont premiers entre eux dans leur ensemble. En effet, on a déjà $a_1 \wedge a_2 = 1$, donc $a_1 \wedge a_2 \wedge \cdots \wedge a_n = 1$.
En revanche la réciproque est fausse : par exemple les entiers 6, 10 et 15 sont premiers entre eux dans leur ensemble puisque

$$6 \wedge 10 \wedge 15 = (6 \wedge 10) \wedge 15 = 2 \wedge 15 = 1.$$

Pourtant ils ne sont pas deux à deux premiers puisque $6 \wedge 10 = 2$, $6 \wedge 15 = 3$ et $10 \wedge 15 = 5$.

Proposition 16.43 : *Des entiers $a_1, \dots, a_n$ non tous nuls sont premiers entre eux dans leur ensemble si et seulement si il existe des entiers $u_1, \dots, u_n$ tels que* $\sum_{i=1}^{n} a_i u_i = 1$.

16.3 FACTORISATION PREMIÈRE ET APPLICATIONS

Dans la suite, on note $\mathscr{P}$ l'ensemble des nombres premiers.

16.3.1 Quelques propriétés des nombres premiers

Proposition 16.44 : *Soit p un nombre premier, et soit $n \in \mathbf{Z}$ non divisible par p. Alors p et n sont premiers entre eux.*

Démonstration. Notons $d = p \wedge n$. Alors $d \mid p$, et donc $d = 1$ ou $d = p$.
Si $d = p$, cela signifie que $p \mid n$, ce qui est contraire à notre hypothèse.
Donc $d = 1$ et donc p et n sont premiers entre eux. □

Notons en particulier que deux nombres premiers distincts sont toujours premiers entre eux puisqu'aucun ne divise l'autre.

Corollaire 16.45 – *Un nombre premier p divise un produit si et seulement si il divise l'un des facteurs.*

Démonstration. Prouvons le résultat pour un produit de deux facteurs, une récurrence facile permettant ensuite de généraliser à un produit de n facteurs, n quelconque.
Soient donc a et b deux entiers tels que $p \mid ab$.
Soit $p \mid a$, auquel cas il n'y a rien à prouver.
Soit p ne divise pas a, et donc est premier avec a.
Par le lemme de Gauss, p divise donc b.
Ainsi, $p \mid ab \Rightarrow p \mid a$ ou $p \mid b$. □

Remarque
Notons que ce résultat est évidemment faux si p n'est pas premier : $4 \mid 12 = 2 \times 6$, mais $4 \nmid 2$ et $4 \nmid 6$.

16.3.2 Valuation p-adique

Définition 16.46 – Soit p un nombre premier, et soit $n \in \mathbf{Z}$ un entier non nul. Alors le maximum de l'ensemble $\{k \in \mathbf{N} \mid p^k \text{ divise } n\}$ est appelé valuation p-adique de n, et noté $v_p(n)$.

Démonstration. Il y a tout de même quelque chose à prouver : que le maximum en question existe.
Pour ce faire, prouvons que $\{k \in \mathbf{N}, p^k \mid n\}$ est une partie non vide et majorée de $\mathbf{N}$.
Elle est clairement non vide car elle contient 0 : $p^0 = 1$ divise toujours n.
Elle est majorée car si p^k divise n, alors $k \leqslant p^k \leqslant |n|$. □

Par définition, $v_p(n)$ est la plus grande puissance de p qui divise n.
Notons que n est premier avec p si et seulement si $v_p(n) = 0$. Par exemple, $v_2(12) = 2$ car $2^2 = 4$ divise 12 et $2^3 = 8$ ne divise pas 12 (et donc aucune puissance plus grande de 2 ne peut diviser 12).

Lemme 16.47. Soit $p \in \mathscr{P}$, soit $a \in \mathbf{Z}$ non nul, et soit $n \in \mathbf{N}$. Alors $n = v_p(a)$ si et seulement si il existe $a' \in \mathbf{Z}$, premier à p, tel que $a = p^n a'$.

Démonstration. Si $n = v_p(a)$, alors p^n divise a : il existe $a' \in \mathbf{Z}$ tel que $a = p^n a'$. Et alors p ne peut pas diviser a', car alors a serait au moins divisible par p^{n+1}. Par conséquent, a' est premier avec a.
Inversement, si $a = p^n a'$, avec $a' \wedge p = 1$, alors p^n divise a, et p ne divisant pas a', p^{n+1} ne divise pas a, donc $v_p(a) = n$. □

Proposition 16.48 : *Soit p un nombre premier. Si a et b sont deux entiers non nuls, alors $v_p(ab) = v_p(a) + v_p(b)$.*

Démonstration. $p^{v_p(a)}$ divise a et $p^{v_p(b)}$ divise b, donc $p^{v_p(a)+v_p(b)} = p^{v_p(a)}p^{v_p(b)}$ divise ab.
Par définition de $v_p(a)$, $a = p^{v_p(a)}a'$, où p ne divise pas a'. Puisque p est premier, on a donc $p \wedge a' = 1$.
De même, $b = p^{v_p(b)}b'$, où $p \wedge b' = 1$.
Et donc $ab = p^{v_p(a)+v_p(b)}a'b'$, où $a'b'$ est premier avec p.
Et donc, par le lemme précédent, $v_p(ab) = v_p(a) + v_p(b)$. □

Il n'existe pas de règle générale pour la valuation d'une somme (voir TD pour quelques cas particuliers).

16.3.3 Décomposition en produit de facteurs premiers

Théorème 16.49 : *Soit $n \in \mathbf{N}^*$. Alors il existe une unique suite finie $(p_1, \alpha_1), \cdots, (p_k, \alpha_k)$ de couples de $\mathcal{P} \times \mathbf{N}^*$ telle que :*

1. *pour $i < j$, $p_i < p_j$*
2. $n = \prod_{i=1}^{k} p_i^{\alpha_i}$

Plus simplement : tout entier non nul se décompose de manière unique[18] comme produit de facteurs premiers.

[18] À l'ordre des facteurs près.

Démonstration. Nous avons déjà vu l'existence à la proposition 16.15. Il s'agit donc de prouver ici que cette décomposition est unique.
Supposons donc qu'il existe deux décompositions de n en produits de facteurs premiers :

$$n = \prod_{i=1}^{k} p_i^{\alpha_i} = \prod_{j=1}^{\ell} q_i^{\beta_i}$$

où $p_1 < p_2 < \cdots < p_k$ et $q_1 < \cdots < q_\ell$ sont des nombres premiers et $\alpha_1, \ldots, \alpha_k, \beta_1, \ldots, \beta_\ell$ des entiers strictement positifs.
Notons que pour tout nombre premier p, $p^0 = 1$, et donc quitte à ajouter des termes de la forme q_i^0, à la première décomposition et des termes de la forme p_i^0 à la seconde, on peut supposer que ces deux décompositions contiennent les mêmes facteurs premiers, à des puissances positives[19].

[19] Mais éventuellement nulles.

Autrement dit : $n = \prod_{i=1}^{k} p_i^{\alpha_i} = \prod_{i=1}^{k} p_i^{\beta_i}$, où les α_i, β_i sont dans $\mathbf{N}$.

Alors, pour tout $i \in [\![1, k]\!]$, $p_i^{\alpha_i}$ divise $n = p_i^{\beta_i} \prod_{\substack{j=1 \\ j\neq i}}^{k} p_j^{\beta_j}$.

Étant premier avec $\prod_{\substack{j=1 \\ j\neq i}}^{k} p_j^{\beta_j}$ (car premier avec chacun de ses facteurs), $p_i^{\alpha_i}$ divise donc $p_i^{\beta_i}$.
Et par conséquent, $\alpha_i \leqslant \beta_i$.
On prouve de manière similaire que $\beta_i \leqslant \alpha_i$ et donc que $\alpha_i = \beta_i$.
Et donc la décomposition est unique. □

Notons que dans cette écriture, α_i est la plus grande puissance de p_i divisant n, et donc autrement dit, $\alpha_i = v_{p_i}(n)$.
Un moyen pratique d'écrire la décomposition en produit de facteurs premiers de n est donc $n = \prod_{p\in\mathcal{P}} p^{v_p(n)}$.
Il y a tout de même des précautions à prendre puisque ce produit comporte un nombre infini de termes. Seulement, il n'existe qu'un nombre fini de premiers p pour lesquels $v_p(n) \neq 0$, et donc pour lesquels $p^{v_p(n)} \neq 1$.
Autrement dit, le produit est bien infini, mais seuls un nombre fini de termes ne valent pas 1. Nous pourrions donc tout aussi bien écrire

$$n = \prod_{\substack{p\in\mathcal{P} \\ v_p(n)\neq 0}} p^{v_p(n)}$$

mais il faut bien reconnaître que cette écriture est moins élégante !

16.3.4 Application aux diviseurs, au PGCD et au PPCM

Proposition 16.50 : *Soient a et b deux entiers naturels. Alors $a \mid b$ si et seulement si pour tout $p \in \mathcal{P}$, $v_p(a) \leqslant v_p(b)$.*

Démonstration. Si a divise b, soit $k \in \mathbf{N}$ tel que $b = ak$. Alors pour tout premier p, $v_p(b) = v_p(a) + v_p(k) \geqslant v_p(a)$.
Inversement, supposons que pour tout $p \in \mathcal{P}$, $v_p(a) \leqslant v_p(b)$, et soit $k = \prod_{p\in\mathcal{P}} p^{v_p(b)-v_p(a)}$.

Alors k est un entier et

$$ak = \prod_{p\in\mathcal{P}} p^{v_p(a)} \times \prod_{p\in\mathcal{P}} p^{v_p(b)-v_p(a)} = \prod_{p\in\mathcal{P}} p^{v_p(b)} = b.$$

Donc $a \mid b$. □

Proposition 16.51 : *Soient $a, b \in \mathbf{N}$. Alors :*

1. $a \wedge b = \prod_{p\in\mathcal{P}} p^{\min(v_p(a),v_p(b))}$.
   Autrement dit, pour tout $p \in \mathcal{P}$, $v_p(a \wedge b) = \min(v_p(a), v_p(b))$.
2. $a \vee b = \prod_{p\in\mathcal{P}} p^{\max(v_p(a),v_p(b))}$.
   Autrement dit, pour tout $p \in \mathcal{P}$, $v_p(a \vee b) = \max(v_p(a), v_p(b))$.
3. *a et b sont premiers entre eux si et seulement si pour tout $p \in \mathcal{P}$, $v_p(a) = 0$ ou $v_p(b) = 0$.*

Démonstration.

1. Soit $p \in \mathcal{P}$. Alors $p^{\min(v_p(a),v_p(b))}$ divise a et b, donc divise $a \wedge b$.
   Ainsi, $v_p(a \wedge b) \geqslant \min(v_p(a), v_p(b))$.
   Inversement, si p^k divise $a \wedge b$, alors p^k divise a et p^k divise b, donc $v_p(a) \geqslant k$ et $v_p(b) \geqslant k$, de sorte que $k \leqslant \min(v_p(a), v_p(b))$.
   Et alors $v_p(a \wedge b) \leqslant \min(v_p(a), v_p(b))$.
2. Il suffit d'utiliser $a \vee b = \dfrac{ab}{a \wedge b}$, et de noter que pour tous entiers[20] m et n,

   $$m + n - \min(m, n) = \max(m, n).$$

   [20] Et même réels.
3. Utiliser le point 1) et le fait que le minimum de deux nombres positifs est nul si et seulement si l'un de ces nombres est nul.

□

16.3.5 Petit théorème de Fermat

Théorème 16.52 : *Soit p un nombre premier, et soit $a \in \mathbf{Z}$. Alors $a^p \equiv a \quad [p]$.*
De plus, si a n'est pas divisible par p, alors $a^{p-1} \equiv 1 \quad [p]$.

Démonstration. Commençons par remarquer que pour $k \in [\![1, p-1]\!]$, $\binom{p}{k}$ est divisible par p.
En effet, on a $k\binom{p}{k} = p\binom{p-1}{k-1}$.
Donc p divise $k\binom{p}{k}$ et est premier avec k, de sorte que par le lemme de Gauss, il divise $\binom{p}{k}$.
Autrement dit, $\binom{p}{k} \equiv 0 \quad [p]$.

Ainsi, quels que soient les entiers u et v, on a

$$(u+v)^p = \sum_{k=0}^{p} \binom{p}{k} u^k v^{n-k} \equiv u^p + v^p \quad [p].$$

Prouvons à présent par récurrence sur $a \in \mathbf{N}$ que $a^p \equiv a \quad [p]$.
Pour $a = 0$ ou $a = 1$, c'est évident. Supposons que $a^p \equiv a \quad [p]$.
Alors $(a+1)^p \equiv a^p + 1 \equiv a + 1 \quad [p]$.
Par le principe de récurrence, pour tout $a \in \mathbf{N}$, $a^p \equiv a \quad [p]$.
Et si $a < 0$, alors il existe $b \in \mathbf{N}$ tel que $a \equiv b \quad [p]$.
Et donc $a^p \equiv b^p \equiv b \equiv a \quad [p]$.

Détails

Par exemple, on peut prendre pour b le reste de la division euclidienne de a par p (ce n'est pas du tout la seule solution, mais c'est la plus petite).

Enfin, si a n'est pas divisible par p, alors il est premier avec p. Or, ce que nous venons de prouver, c'est que $a^p - a$ est divisible par p.
Mais $a^p - a = a(a^{p-1} - 1)$, avec $a \wedge p = 1$, donc p divise $a^{p-1} - 1$.
Soit encore $a^{p-1} \equiv 1 \quad [p]$. □

Exemple 16.53

Pour tout $n \in \mathbf{Z}$, tout diviseur premier impair de $n^2 + 1$ est congru à 1 modulo 4.
Soit donc $p \in \mathcal{P}$ un nombre premier impair divisant $n^2 + 1$.
Alors n n'est pas divisible par p, puisque n^2 ne l'est pas non plus.
Donc $n^{p-1} \equiv 1 \pmod{p}$.
Soit encore $\left(n^2\right)^{\frac{p-1}{2}} \equiv 1 \pmod{p}$.
Mais $n^2 \equiv -1 \pmod{p}$, donc $(-1)^{\frac{p-1}{2}} \equiv 1 \pmod{p}$.
Mais puisque $(-1)^{\frac{p-1}{2}} = \pm 1$, la congruence donnée plus tôt est nécessairement une égalité : $(-1)^{\frac{p-1}{2}} = 1$.
Et donc $\dfrac{p-1}{2}$ est pair : il existe $k \in \mathbf{Z}$ tel que $\dfrac{p-1}{2} = 2k \Leftrightarrow p = 4k + 1$.

16.4 Une brève introduction à $\mathbf{Z}/n\mathbf{Z}$.

Nous avons mentionné précédemment que pour $n \in \mathbf{N}^*$, tout entier $k \in \mathbf{Z}$ est congru à un et un seul entier de $[\![0, n-1]\!]$.
Autrement dit, si on note $\overline{r} = \{k \in \mathbf{Z},\ k \equiv r \pmod{n}\} = \{r + kn,\ k \in \mathbf{Z}\}$ la classe d'équivalence de r pour la relation de congruence modulo n, alors $\overline{0}, \overline{1}, \ldots, \overline{n-1}$ est une partition de $\mathbf{Z}$.

On note alors $\mathbf{Z}/n\mathbf{Z}$ l'ensemble de ces classes d'équivalence : $\mathbf{Z}/n\mathbf{Z} = \{\overline{0}, \overline{1}, \ldots, \overline{n-1}\}$.
On définit une loi de composition interne sur $\mathbf{Z}/n\mathbf{Z}$ en posant $\overline{x} + \overline{y} = \overline{x+y}$.
Le point clé est que la classe d'équivalence de $x + y$ ne dépend pas des éléments x et y qu'on a choisi dans une classe d'équivalence.
Plus précisément : si $x \equiv x' \pmod{n}$ et si $y \equiv y' \pmod{n}$, alors $x + y \equiv x' + y' \pmod{n}$.
Et donc $\overline{x+y} = \overline{x'+y'}$.
Par exemple, modulo 5, $3 \equiv 8$ et $4 \equiv 14$.
Et alors $\overline{3+4} = \overline{7} = \overline{2}$ et $\overline{8+14} = \overline{22} = \overline{2}$.
Ainsi, l'addition est bien définie sans ambiguïté sur $\mathbf{Z}/n\mathbf{Z}$.

	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$
$\overline{0}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{0}$
$\overline{2}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{0}$	$\overline{1}$
$\overline{3}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{4}$	$\overline{4}$	$\overline{5}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{5}$	$\overline{5}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$

Elle est associative car si $\overline{x}, \overline{y}, \overline{z}$ sont trois éléments de $\mathbf{Z}/n\mathbf{Z}$,

$$\overline{x} + \overline{y} + \overline{z} = \overline{x+y} + \overline{z} = \overline{(x+y)+z} = \overline{x+(y+z)} = \overline{x} + \overline{y+z} = \overline{x} + (\overline{y} + \overline{z}).$$

Remarque

Nous avons en fait utilisé ici l'associativité de l'addition sur $\mathbf{Z}$.

De même, en utilisant la commutativité de l'addition d'entiers, on prouve que + est commutative sur $\mathbf{Z}/n\mathbf{Z}$.
La classe d'équivalence de 0 (qui est formée des multiples de n) est élément neutre, puisque pour tout $\overline{k} \in \mathbf{Z}/n\mathbf{Z}$, on a

$$\overline{0} + \overline{k} = \overline{0+k} = \overline{k}.$$

Enfin, pour tout $\overline{k} \in \mathbf{Z}/n\mathbf{Z}$, on a $\overline{k} + \overline{-k} = \overline{k+(-k)} = \overline{0}$, et donc $\overline{-k}$ est l'inverse de $\overline{k}$ pour +.
Ainsi, $(\mathbf{Z}/n\mathbf{Z}, +)$ est un groupe abélien.

Soit alors $\zeta = e^{i\frac{2\pi}{n}}$, de sorte que $\mathbf{U}_n = \{\zeta^k,\ k \in [\![0, n-1]\!]\}$.
Considérons alors l'application $\varphi : \left| \begin{array}{ccc} \mathbf{Z}/n\mathbf{Z} & \longrightarrow & \mathbf{U}_n \\ \overline{k} & \longmapsto & \zeta^k \end{array} \right.$.
Elle est bien définie car ζ^k ne dépend pas du représentant de $\overline{k}$ choisi. Plus précisément : si $\overline{k'} = \overline{k}$, alors $\exists p \in \mathbf{Z}$ tel que $k' = pn + k$, et donc $\zeta^{k'} = \zeta^{np+k} = (\zeta^n)^p \zeta^k = \zeta^k$.
De plus, φ est un morphisme de groupes, puisque pour $\overline{k}, \overline{k'} \in \mathbf{Z}/n\mathbf{Z}$, on a

$$\varphi(\overline{k} \cdot \overline{k'}) = \varphi(\overline{kk'}) = \zeta^{kk'} = \zeta^k \zeta^{k'}.$$

Il est clairement surjectif, et si $\varphi(\overline{k}) = 1$, alors $\zeta^k = 1$. Si on note $k = nq + r$ la division euclidienne de k par n, on a alors $\zeta^k = \zeta^r = 1$, et donc $r = 0$, de sorte que $\overline{k} = \overline{0}$.
Ceci prouve donc que $\operatorname{Ker}\varphi = \{\overline{0}\}$, et donc φ est injectif.
Donc φ est un isomorphisme de groupes entre $(\mathbf{Z}/n\mathbf{Z}, +)$ et $\mathbf{U}_n$.

A l'instar de ce qui a été fait pour la loi +, on peut définir une seconde loi $\times$ sur $\mathbf{Z}/n\mathbf{Z}$ en posant $\overline{k} \times \overline{k'} = \overline{kk'}$.
Elle est bien définie car la congruence modulo n est compatible à la multiplication.
On prouve alors que $(\mathbf{Z}/n\mathbf{Z}, +, \times)$ est un anneau commutatif, en utilisant le fait que $\mathbf{Z}$ en est un.

Remarque

Nous avons déjà dit que nous pouvions simplifier par a modulo n si $a \wedge n = 1$. Nous pouvons désormais le formuler différemment : tout élément inversible de $\mathbf{Z}/n\mathbf{Z}$ est régulier (pour la multiplication).

Proposition 16.54 : *Soit $n \in \mathbf{N}^*$. Alors $\overline{a}$ est un inversible de $\mathbf{Z}/n\mathbf{Z}$ si et seulement si $a \wedge n = 1$.*

Démonstration. $\overline{a}$ est inversible si et seulement si il existe $\overline{u} \in \mathbf{Z}/n\mathbf{Z}$ tel que $\overline{au} = 1$, soit si et seulement si il existe $(u, v) \in \mathbf{Z}^2$ tels que $au + nv = 1$.
Donc si et seulement si $a \wedge n = 1$. □

Proposition 16.55 : *L'anneau $\mathbf{Z}/n\mathbf{Z}$ est intègre si et seulement si n est premier. Dans ce cas, $\mathbf{Z}/n\mathbf{Z}$ est un corps.*

Démonstration. Si n est composé, $n = ab$, avec a, b positifs, tous deux distincts de 1.
Alors $\overline{0} = \overline{n} = \overline{a}\overline{b}$.
Mais $2 \leqslant a < n$, donc $\overline{a} \neq \overline{0}$ et de même $\overline{b} \neq \overline{0}$.
Donc $\overline{a}$ est un diviseur de 0 : $\mathbf{Z}/n\mathbf{Z}$ n'est pas intègre.
Par contraposée, si $\mathbf{Z}/n\mathbf{Z}$ est intègre, alors n est premier.

En revanche, si n est premier, alors pour tout $k \in [\![1, n-1]\!]$, $n \wedge k = 1$, et donc $\overline{k}$ est inversible dans $\mathbf{Z}/n\mathbf{Z}$.
Donc tout élément non nul de $\mathbf{Z}/n\mathbf{Z}$ est inversible : $\mathbf{Z}/n\mathbf{Z}$ est un corps, et en particulier est intègre. □