

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 nombre¹, 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 richesse² 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 $\mathcal{D}(n) = \{a \in \mathbf{Z} \mid a \text{ divise } n\}$ 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 $|k| \geq 1$. Et donc $|a| \leq |n|$, de sorte que $a \in \llbracket -n, n \rrbracket$.

Donc $\mathcal{D}(n) \subset \llbracket -n, n \rrbracket$, qui est un ensemble fini, donc $\mathcal{D}(n)$ est lui-même fini. \square

Exemple 16.3

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

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 $n \mid ab$.

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 $ab = knb$, donc $n \mid ab$.

□

 La réciproque au second point est fautive : n peut diviser un produit ab sans diviser ni a ni b . Par exemple, 4 divise $12 = 2 \times 6$, mais ne divise ni 2 ni 6.

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 :

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

Notons qu'en particulier, n divise a si et seulement si $a \equiv 0 \pmod{n}$.

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

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

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 $a + c \equiv b + d \pmod{n}$.

2. Avec les mêmes notations :

$$ac = (b + nk_1)(d + nk_2) = bd + n(k_1d + k_2b + nk_1k_2) \Leftrightarrow ac - bd = n \underbrace{(k_1d + k_2b + nk_1k_2)}_{\in \mathbf{Z}}.$$


Donc $ac \equiv bd \pmod{n}$.

La relation sur les puissances en découle directement, par récurrence sur k .

3. On a

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

□

 La relation de congruence modulo α , avec $\alpha \in \mathbf{R} \setminus \mathbf{Z}$ (on pensera notamment à $\alpha = 2\pi \dots$) est encore compatible avec l'addition, mais pas avec la multiplication³.

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

Exemples 16.7

► $36^{2022} - 13^{2022}$ est divisible par 7. En effet, on a

$$36^{2022} - 13^{2022} \equiv 1^{2022} - (-1)^{2022} \equiv 1 - 1 \equiv 0 \pmod{7}.$$

► $117^{119} - 8$ est divisible par 17.

On a $117 = 7 \times 17 - 2 \equiv -2 \pmod{17}$. Et donc $117^{119} \equiv (-2)^{119} \pmod{17}$.

Or, par élévations au carré successives, on a

$$(-2)^2 \equiv 4 \pmod{17}, (-2)^4 \equiv 4^2 \equiv 16 \equiv -1 \pmod{17}, (-2)^8 \equiv (-1)^2 \equiv 1 \pmod{17}.$$

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

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

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

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

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 $0 \leq r_1 < b$ et $0 \leq r_2 < b$.

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 $a \geq 0$ 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 $r \geq b$, 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 $0 \leq r < b$. \square

Remarques. ► La méthode qu'on vous a expliquée au primaire⁴ pour trouver q et r reste valable, et on ne peut pas faire beaucoup mieux !

► L'idée de base étant⁵ 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 $q = \left\lfloor \frac{a}{b} \right\rfloor$ (et alors $r = a - bq$).

► Attention aux nombres négatifs ! Nous avons dit précédemment que $131 = 18 \times 7 + 5$. 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 $-131 = -19 \times 7 + 2$.

► Le résultat est encore valable si b est un entier strictement négatif si on impose au reste de vérifier $0 \leq r < |b|$.

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 $0 \leq r < n$. 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 .

Remarque

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

⁴ «Poser» la division.

⁵ Au moins si a et b sont positifs.

Exercice

Le prouver.

- Démonstration.* 1. C'est immédiat en utilisant la compatibilité de la congruence avec l'addition et la multiplication : $a \equiv nq + r \equiv 0 + r \equiv r \pmod{n}$.
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 : $a \equiv b \pmod{n}$.
 Et donc par le point 1), $r_1 \equiv r_2 \pmod{n}$. 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 $a \equiv r_1 \equiv r_2 \equiv b \pmod{n}$. □

Exemple 16.10

Déterminons le reste de la division euclidienne de 67^{2024} par 7.
 Cela revient à trouver $r \in \llbracket 0, 6 \rrbracket$ tel que $67^{2024} \equiv r \pmod{7}$.
 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 de 2024 par 3. Mais nous n'avons pas besoin de cette division euclidienne : 2022 est divisible⁶ par 3, donc il existe $k \in \mathbf{N}$ tel que $2022 = 3k$ donc $2024 = 3k + 2$. Le reste cherché est 2.
 On a donc $67^{2024} \equiv 4^{2024} \equiv 4^{3k} \times 4^2 \pmod{7} \equiv 2 \pmod{7}$.
 Et donc le reste de la division euclidienne de 67^{2020} par 2 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 $\sum_{k=0}^p a_k \equiv 0 \pmod{3}$.

Rappelons que pour $k \in \mathbf{Z}$, la classe d'équivalence de k pour la relation de congruence modulo n est $\bar{k} = \{qn + k, q \in \mathbf{Z}\}$.

La division euclidienne permet de dénombrer les classes d'équivalence pour cette relation :

Proposition 16.11 : Il y a exactement n classes d'équivalence pour la congruence modulo n , qui sont $\bar{0}, \bar{1}, \dots, \bar{n-1}$.

Démonstration. Par la proposition 16.9 deux entiers sont dans la même classe modulo n si et seulement si ils ont même reste dans la division euclidienne par n .

Or, il y a exactement n restes possible : $0, 1, 2, \dots, n-1$.

Donc il y a n classes d'équivalence. □

Enfin, ajoutons un corollaire de la division euclidienne qui sert souvent :

Proposition 16.12 : Pour $n, k \in \mathbf{N} \times \mathbf{N}^*$, k divise $n(n+1)(n+2) \cdots (n+k-1)$.
 Autrement dit, le produit de k entiers consécutifs est toujours divisible par k .

Démonstration. L'idée est tout simplement que l'un au moins des k entiers consécutifs $n, n+1, \dots, n+k-1$ est divisible par k .

Notons $n = kq + r$ la division euclidienne de n par k , avec $0 \leq r < k$.

Si $r = 0$ alors $n \equiv 0 [k]$ et donc $n(n+1) \cdots (n+k-1) \equiv 0 [k]$.

Et si $r \neq 0$, alors $n+k-r = k(q+1) \equiv 0 [k]$, et donc $n(n+1) \cdots (n+k-r) \cdots (n+k-1) \equiv 0 [k]$. \square

Exemples 16.13

- Pour tout $n \in \mathbf{N}$, $n(n+1)$ est pair.
 - Pour tout $n \in \mathbf{N}$, $n^3 - n = (n-1)n(n+1)$ est divisible par 3.
 - On peut en réalité faire beaucoup mieux : un produit de k entiers consécutifs est toujours divisible par $k!$.
- En effet, pour $n \in \mathbf{N}$, on a

$$n(n+1) \cdots (n+k-1) = \frac{(n+k-1)!}{(n-1)!} = k! \binom{n+k-1}{n-1}.$$

Puisque nous avons prouvé que les coefficients binomiaux sont toujours entiers⁷, alors $k!$ divise $n(n+1) \cdots (n+k-1)$.

⁷ Ce qui n'est pas complètement trivial, et ne découle pas directement de divisibilités, mais plutôt de l'identité de Pascal.

16.1.4 Nombres premiers

Définition 16.14 – Un **nombre premier** est un entier naturel 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 nul⁸, ne peut pas non plus être égal à 1 (qui ne possède que lui-même comme diviseur positif).

Et puisqu'un entier $n \geq 2$ 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, $p \geq 2$ 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 16.15

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.

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 16.16 : *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 $n \geq 2$ 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 $\llbracket 2, n \rrbracket$ soit produit de nombres premiers.

Si $n+1$ est premier alors il n'y a rien à prouver : c'est le produit d'un nombre premier.

Sinon, il existe $a, b \in \mathbf{N}^*$, tous deux plus grands que 2 tels que $n+1 = ab$.

Rappel

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

Notons que puisque $b > 1$, alors $a < n + 1$, et donc $a \leq n$, et de même $b \leq n$. Donc par hypothèse de récurrence, il existe $p_1, \dots, p_k, q_1, \dots, q_r$ premiers tels que $a = p_1 \cdots p_k$ et $b = q_1 \cdots q_r$, si bien que

$$n + 1 = p_1 \cdots p_k q_1 \cdots q_r$$

est produit de nombres premiers.

Par le principe de récurrence forte, tout entier supérieur ou égal à 2 est produit de nombres premiers. \square

Théorème 16.17 : *Il existe une infinité de nombres premiers.*

Démonstration. Raisonnons par l'absurde en supposant 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 $i \in \llbracket 1, N \rrbracket$ 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 fautive, et donc il existe une infinité de nombres premiers. \square

Pour déterminer les nombres premiers inférieurs à un entier n fixé, on utilise le crible d'Ératosthène rencontré en terminale (voir ci-dessous).

Mentionnons que le problème de déterminer si un grand nombre est premier est difficile, au sens où il est coûteux en calculs.

C'est plutôt une bonne nouvelle, puisque c'est sur ce principe que reposent *la plupart* des algorithmes cryptographiques utilisés aujourd'hui.

En revanche, avec un ordinateur quantique, factoriser un entier en produit de premiers devient bien plus facile.

Non parce qu'un ordinateur quantique est «plus puissant⁹», mais parce que pour ce problème précis, on dispose d'un algorithme quantique, appelé algorithme de SHOR, qui est bien plus efficace¹⁰. Cela signifie que si les ordinateurs quantiques venaient à se démocratiser, alors il faudra rapidement changer nos habitudes en matière de cryptographie.

Relativisons un peu : à l'heure actuelle, le plus grand entier factorisé par un ordinateur quantique à l'aide de l'algorithme de Shor est 15.

⁹ Pour certains problèmes, les ordinateurs quantiques ne sont pas meilleurs que les ordinateurs classiques.
¹⁰ Il factorise N en $O((\log N)^3)$.

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

16.2.1 PGCD de deux entiers

Définition 16.18 – Soient $(a, b) \in \mathbb{Z}^2$, $(a, b) \neq (0, 0)$ deux entiers non simultanément nuls¹¹. 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 $0 \wedge 0 = 0$.

Remarque. 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 \mathbb{Z} , elle admet bien un plus grand élément.

¹¹ 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 \leq) nombre qui divise à la fois a et 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.

Exemples 16.19

- ▶ $60 \wedge 18 = 6$ car $\mathcal{D}(60) \cap \mathcal{D}(18) = \{\pm 1, \pm 2, \pm 3, \pm 6\}$.
- ▶ Si $b = 0$, alors $\mathcal{D}(a) \cap \mathcal{D}(b) = \mathcal{D}(a)$ et donc $a \wedge 0 = |a|$.
- ▶ Plus généralement, si $b \mid a$, $\mathcal{D}(b) \subset \mathcal{D}(a)$, et donc $\mathcal{D}(a) \cap \mathcal{D}(b) = \mathcal{D}(b)$, de sorte que $a \wedge b = |b|$.
- ▶ Le PGCD est insensible aux signes : $a \wedge b = |a| \wedge |b|$.

Proposition 16.20 : 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 16.21. Soient $(a, b) \in \mathbf{Z}^2$. Alors, pour tout $k \in \mathbf{Z}$, $a \wedge b = (a + kb) \wedge b$.

Terminologie

◀ Ce résultat est souvent appelé lemme d’Euclide.

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 $a \wedge b = (a + kb) \wedge b$. □

Corollaire 16.22 – 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 remarquer 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 diviseurs de ces deux entiers.

Soient donc a et b deux entiers naturels¹² non nuls.

Notons r_1 le reste de la division euclidienne de a par b . On a donc $0 \leq r_1 < b$.

Par le corollaire 16.22, $a \wedge b = r_1 \wedge b$.

Notons alors r_2 le reste de la division euclidienne de b par r_1 . On a alors $0 \leq r_2 < r_1$.

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 $r_k \neq 0$ (car on n'a pas défini la division euclidienne par 0).

On obtient alors une suite strictement décroissante (car $r_{k+1} < r_k$) d'éléments de $\llbracket 0, b - 1 \rrbracket$. Cette suite est donc nécessairement finie¹³, puisque $\llbracket 0, b - 1 \rrbracket$ est fini.

Autrement dit, il existe un rang n tel que $r_n = 0$.

Et alors, par applications successives du corollaire 16.22,

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

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

¹² Changer le signe de a et/ou de b ne change pas le PGCD.

¹³ Et même de cardinal au plus b .

Exemple 16.23

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 $1540 \wedge 882 = 14$.

Proposition 16.24 : Soit $(a, b) \in \mathbf{Z}^2$. 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.

Si $(a, b) = (0, 0)$, alors $\mathcal{D}(a) \cap \mathcal{D}(b) = \mathbf{N} = \mathcal{D}(0)$.

Si $a = 0$, alors $\mathcal{D}(a) \cap \mathcal{D}(b) = \mathcal{D}(b) = \mathcal{D}(0 \wedge b)$.

Nous supposons donc a et b non nuls. En reprenant les notations de l'algorithme d'Euclide, on a¹⁴

$$\mathcal{D}(a) \cap \mathcal{D}(b) = \mathcal{D}(r_1) \cap \mathcal{D}(b) = \dots = \mathcal{D}(r_{n-1}) \cap \mathcal{D}(r_n) = \mathcal{D}(r_{n-1}) \cap \underbrace{\mathcal{D}(0)}_{=\mathbf{Z}} = \mathcal{D}(r_{n-1}) = \mathcal{D}(a \wedge b).$$

□

¹⁴ Cf la preuve 16.21.

Proposition 16.25 : Soient $(a, b) \in \mathbf{Z}^2$ et soit $d \in \mathbf{N}$.
 Alors $d = a \wedge b$ si et seulement si $\begin{cases} d \mid a \\ d \mid b \\ \forall n \in \mathbf{N}, (n \mid a \text{ et } n \mid b) \Rightarrow n \mid d \end{cases}$

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

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

Alors par le sens direct, $d \mid (a \wedge b)$ et en prenant $n = a \wedge b$, qui divise a et b , on a donc $a \wedge b \mid d$.

Donc $d = a \wedge b$. □

Remarque. Pour a, b positifs, la proposition précédente affirme que $a \wedge b$ est plus petit à la fois que a et b au sens de la relation de divisibilité¹⁵ et qu'il est plus grand (toujours pour la divisibilité) que tout diviseur commun de a et b , c'est-à-dire que tout minorant de $\{a, b\}$. Autrement dit, $a \wedge b$ est le plus grand des minorants de $\{a, b\}$: c'est donc $\inf\{a, b\}$.

¹⁵ Qui est une relation d'ordre sur \mathbf{N} .

Proposition 16.26 : Soient $(a, b, c) \in \mathbf{Z}^3$.

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

Démonstration. 1. Il s'agit de noter que

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

2. Prouvons le résultat pour $k \in \mathbf{N}$ puisque le PGCD est insensible aux signes.
Puisque $a \wedge b$ divise à la fois a et b , $k(a \wedge b)$ divise à la fois ak et bk et donc divise $(ak) \wedge (bk)$.

Inversement, k divise ak et bk , donc divise leur PGCD : il existe $d \in \mathbf{N}$ tel que $|k|d = (ak) \wedge (bk)$.

Donc kd divise ak , et donc d divise a . De même, d divise b . Donc d divise $a \wedge b$.

Et après multiplication par k , $kd = (ak) \wedge (bk)$ divise $k(a \wedge b)$.

On en déduit¹⁶ que $(ak) \wedge (bk) = k(a \wedge b)$. □

¹⁶ C'est l'antisymétrie de la relation de divisibilité sur \mathbf{N}

16.2.3 Théorème de Bézout

Théorème 16.27 (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 $b \geq 1$.

Plus précisément, nous allons prouver par récurrence forte sur $b \in \mathbf{N}^*$ la propriété $\mathcal{P}(b)$: «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 $1 \leq r < b$.

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 $\mathcal{P}(b)$ est vraie, et par le principe de récurrence, elle est vraie pour tout $b \geq 1$. □



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 (car a et b sont tous deux multiples de $a \wedge b$).

Par exemple, $4 \wedge 6 = 2$, et $8 = 14 \times 4 - 6 \times 8$.



Il n'y a pas unicité d'un couple (u, v) tel que $au + bv = a \wedge b$.

Par exemple, $18 \wedge 30 = 6 = (-3) \times 18 + 2 \times 30 = 2 \times 18 + (-1) \times 30$.

Terminologie

Une telle relation est appelée relation de Bézout.

Plus généralement, si $d = a \wedge b$ et si $au + bv = d$ est une relation de Bézout, alors pour tout $k \in \mathbf{Z}$, $a\left(u + k\frac{b}{d}\right) + b\left(v - k\frac{a}{d}\right) = d$ est une autre 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 \mathcal{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 \mathcal{R}_{n-1} , on obtient une relation de Bézout pour le couple (r_{n-3}, r_{n-2}) , relation que l'on notera \mathcal{R}_{n-2} .

De proche en proche, on finit donc par arriver à une relation de Bézout (\mathcal{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 16.28

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 16.29 – Soient $(a, b) \in \mathbf{Z}^2$. 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 16.30

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

Théorème 16.31 (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 $a \wedge b = 1$. \square

⚠ 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 16.32 : Soient a, b, c trois entiers non nuls. Alors a est premier avec bc si et seulement si a est premier à la fois avec b et 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 Bézout¹⁷, il existe deux couples d'entiers (u_1, v_1) et (u_2, v_2) tels que $1 = au_1 + bv_1$ et $1 = au_2 + cv_2$.

Alors, en multipliant ces deux relations, il vient

$$1 = (au_1 + bv_1)(au_2 + cv_2) = a(au_1u_2 + u_1cv_2 + u_2bv_1) + bc(v_1v_2).$$

Et donc¹⁸ a et bc sont premiers entre eux. \square

Corollaire 16.33 – 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 $i \in \llbracket 1, n \rrbracket$, a est premier avec b_i .

Démonstration. Par récurrence sur n . \square

Proposition 16.34 (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 $a \mid auc + bvc = c$. \square

Corollaire 16.35 – Soient a, b, n trois entiers. Si a et b sont premiers entre eux, et divisent tous les deux n , alors leur produit ab divise n .

Démonstration. Puisque $a \mid n$, il existe $d \in \mathbf{Z}$ tel que $n = ad$.

Mais alors $b \mid ad$ et b est premier avec a , donc b divise d .

Par conséquent, il existe $d' \in \mathbf{Z}$ tel que $d = bd'$, et donc $n = ad = (ab)d'$, si bien que $ab \mid n$. \square

Corollaire 16.36 (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 $a \equiv b \pmod{n}$. \square

¹⁷ En fait, ici on n'utilise que le sens «identité de Bézout».

¹⁸ C'est Bézout.

En abrégé

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

⚠ Attention !

Vous noterez bien la différence avec la proposition 16.6 : ici on n'a que des congruences modulo le même n .

Proposition 16.37 : 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 $b = db'$.

Et alors on sait que $d = (da') \wedge (db') = d(a' \wedge b')$, donc $a' \wedge b' = 1$.

Inversement, supposons l'existence de d, a', b' vérifiant les conditions de l'énoncé.

Alors $a \wedge b = (da') \wedge (db') = d(a' \wedge b') = d$. □

Proposition-définition 16.38 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 $r = \frac{a}{b}$.

De plus, si $r = \frac{a'}{b'}$ avec $(a', b') \in \mathbf{Z} \times \mathbf{N}^*$, alors il existe $k \in \mathbf{N}$ tel que $a' = ak$ et $b' = bk$.

L'écriture $r = \frac{a}{b}$ 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 $r = \frac{u}{v}$, et qu'alors, en posant $d = u \wedge v$, $u = da$ et $v = db$, avec a et b premiers entre eux, alors $r = \frac{a}{b}$

Soit alors $r = \frac{a'}{b'}$ une autre écriture de r , 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 $\frac{a'}{a} = \frac{b'}{b}$. Si on pose $k = \frac{a'}{a} \in \mathbf{N}$, alors $a' = ka$ et $b' = kb$.

On a alors $a' \wedge b' = k$, si bien que $a' \wedge b' = 1 \Leftrightarrow k = 1$, et donc il y a unicité de la forme irréductible. □

16.2.5 PPCM de deux entiers

Définition 16.39 – 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 petit¹⁹ 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 $a \vee 0 = 0 \vee a = 0$.

Remarques. ► Ce minimum existe bien car si $a \neq 0$ et $b \neq 0$, alors $a\mathbf{Z} \cap b\mathbf{Z} \cap \mathbf{N}^*$ est une partie non vide de \mathbf{N} , car elle contient $|ab|$.

► Comme pour le PGCD, le PPCM est commutatif ($a \vee b = b \vee a$) et insensible au signe puisque $|a| \vee |b| = a \vee b$.

Proposition 16.40 : Soient $(a, b) \in \mathbf{Z}^2$, et soit $m \in \mathbf{N}$. Alors

$$m = a \vee b \Leftrightarrow \begin{cases} a \mid m \\ b \mid m \\ \forall n \in \mathbf{N}, (a \mid n \text{ et } b \mid n) \Rightarrow m \mid n \end{cases}$$

Démonstration. Si $m = a \vee b$, alors m est divisible à la fois par a et par b .

De plus, si n est un multiple commun de a et b , notons $n = mq + r$ la division euclidienne de n par m , avec $0 \leq r < m$.

¹⁹ Au sens de la relation d'ordre usuelle.

Autrement dit

Pour la relation de divisibilité, $a \vee b$ est le plus petit des majorants de $\{a, b\}$, donc $\sup\{a, b\}$.

Alors $r = n - mq$ est divisible à la fois par a et par b , donc est un multiple commun de a et b . Étant strictement inférieur à m , il ne peut pas être strictement positif²⁰ et donc est nul. Donc $m \mid n$.

²⁰ m est le plus petit multiple commun strictement positif de a et b .

Inversement, si m est un multiple commun de a et b divisant tout autre multiple commun de a et b , alors en particulier, il divise $a \vee b$.

Or, nous venons de prouver que $a \vee b \mid m$, et donc $m = a \vee b$. \square

Proposition 16.41 : Soient $(a, b) \in \mathbf{Z}^2$. Alors $\forall k \in \mathbf{Z}, (ka) \vee (kb) = |k|(a \vee b)$.

Démonstration. Supposons a, b et k non nuls. Encore une fois, on peut supposer $k \in \mathbf{N}$. Alors $k(a \vee b)$ est un multiple commun de ka et de kb .

Par ailleurs, si n est un multiple commun de ka et de kb , alors n est divisible par k , donc il existe $c \in \mathbf{Z}$ tel que $n = kc$.

Mais $ka \mid kc$ et $k \neq 0$, donc $a \mid c$. Et de même $b \mid c$. Donc $(a \vee b) \mid c$.

Et par conséquent, $k(a \vee b) \mid n$.

Nous reconnaissons là la caractérisation de $(ka) \vee (kb)$ donnée par la proposition précédente, donc $k(a \vee b) = (ka) \vee (kb)$. \square

Le PGCD et le PPCM sont reliés par la formule suivante :

Proposition 16.42 : Pour tout $(a, b) \in \mathbf{N}^2$, on a $(a \vee b) \times (a \wedge b) = ab$.

Remarque

Il suffit donc de savoir calculer l'un des deux nombres $a \vee b$ ou $a \wedge b$ pour déterminer l'autre.

Démonstration. Commençons par supposer a et b premiers entre eux, et prouvons qu'alors $a \vee b = ab$.

Soit m un multiple commun de a et b . Alors il existe deux entiers u et v tels que $m = au = bv$.

Alors $a \mid bv$, et puisque $a \wedge b = 1$, $a \mid v$, de sorte que $ab \mid bv$ et donc $ab \mid m$.

Puisque ab est évidemment un multiple commun de a et b , on a donc $ab = a \vee b$.

Dans le cas général, notons $d = a \wedge b$, de sorte qu'il existe deux entiers a' et b' , premiers entre eux tels que $a = da'$ et $b = db'$. Et alors

$$a \vee b = (da') \vee (db') = d(a' \vee b') = da'b' = ab'.$$

Et donc après multiplication par $a \wedge b$, $(a \wedge b) \times (a \vee b) = adb' = ab$. \square

16.2.6 Familles de n entiers

Définition 16.43 – 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 16.44 : 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 $d' = a_1 \wedge \dots \wedge a_n$, alors

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

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, \dots, a_{n+1} . \square

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

Proposition 16.45 (Identité de Bézout) : Soient a_1, \dots, a_n non tous nuls. Alors il

existe $u_1, \dots, u_n \in \mathbf{Z}$ tels que $\sum_{i=1}^n a_i u_i = \bigwedge_{i=1}^n a_i$.

Démonstration. Par récurrence sur n : notons $d = a_1 \wedge \dots \wedge a_n$, 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 par l'identité de Bézout, il existe $u, v \in \mathbf{Z}$ tels que

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

□

Définition 16.46 – 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 $a_1 \wedge a_2 \wedge \dots \wedge a_n = 1$. En revanche la réciproque est fautive : 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 16.47 : 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 $\sum_{i=1}^n a_i u_i = 1$.

Démonstration. Si $a_1 \wedge a_2 \wedge \dots \wedge a_n = 1$, alors c'est l'identité de Bézout.

Inversement, supposons qu'il existe u_1, \dots, u_n tels que $\sum_{i=1}^n a_i u_i = 1$.

Alors $d = \bigwedge_{i=1}^n a_i$ divise chacun des a_i et donc divise $\sum_{i=1}^n a_i u_i = 1$, et donc $d = 1$. □

16.3 FACTORISATION PREMIÈRE ET APPLICATIONS

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

16.3.1 Quelques propriétés des nombres premiers

Proposition 16.48 : Soit p un nombre premier, et soit $n \in \mathbf{Z}$ non divisible par p . Alors p et n sont premiers entre eux.

⚠ Attention !

La notation est bien pratique pour la suite du cours, mais n'a rien de standard, donc si vous décidez de noter \mathbf{P} l'ensemble des nombres premiers dans une copie, signalez-le clairement.

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. \square

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

Corollaire 16.49 – 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 $p \mid b$. \square

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 16.50 – 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 $k \leq p^k \leq |n|$. \square

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 16.51. Soit $p \in \mathbf{P}$, 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 p .

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 $v_p(a) = n$. \square

Proposition 16.52 : 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 .

Mais $a = p^{v_p(a)} a'$, avec $a' \wedge p = 1$.

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, $v_p(ab) = v_p(a) + v_p(b)$. \square

Rappel

Un entier est premier à un produit si et seulement si il est premier à chacun des facteurs.

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 16.53 : Soit $n \in \mathbf{N}^*$. Alors il existe une unique suite finie $(p_1, \alpha_1), \dots, (p_k, \alpha_k)$ de couples de $\mathbf{P} \times \mathbf{N}^*$ 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 unique²¹ comme produit de facteurs premiers.

²¹ À l'ordre des facteurs près.

Démonstration. Nous avons déjà vu l'existence à la proposition 16.16. 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 :

$$n = \prod_{i=1}^k p_i^{\alpha_i} = \prod_{j=1}^{\ell} q_j^{\beta_j}$$

où $p_1 < p_2 < \dots < p_k$ et $q_1 < \dots < q_{\ell}$ sont des nombres premiers et $\alpha_1, \dots, \alpha_k, \beta_1, \dots, \beta_{\ell}$ des entiers strictement positifs.

Commençons par prouver que ces deux décompositions contiennent les mêmes nombres premiers, et supposons par l'absurde qu'il existe $i \in \llbracket 1, k \rrbracket$ tel que $p_i \notin \{q_1, \dots, q_{\ell}\}$. Alors p_i est premier avec chacun des q_j , et donc est premier avec $n = \prod_{j=1}^{\ell} q_j^{\beta_j}$.

C'est absurde car $p_i \mid n$.

Donc les deux décompositions contiennent les mêmes nombres premiers :

$$n = \prod_{i=1}^k p_i^{\alpha_i} = \prod_{i=1}^k p_i^{\beta_i}.$$

De plus, pour $i \in \llbracket 1, k \rrbracket$, $n = p_i^{\alpha_i} \prod_{\substack{j=1 \\ j \neq i}}^k p_j^{\alpha_j}$, et p_i étant premier avec chacun²² des p_j , $j \neq i$, il

est premier avec $\prod_{\substack{j=1 \\ j \neq i}}^k p_j^{\alpha_j}$.

Donc par le lemme 16.51 $\alpha_i = v_{p_i}(n)$. Et de même, $\beta_i = v_{p_i}(n)$.

Donc l'écriture est bien unique. \square

Nous venons de prouver que dans cette écriture, $\alpha_i = v_{p_i}(n)$.

Un moyen pratique d'écrire la décomposition en produit de facteurs premiers de n est donc $n = \prod_{p \in \mathbf{P}} p^{v_p(n)}$.

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

$$n = \prod_{\substack{p \in \mathbf{P} \\ v_p(n) \neq 0}} p^{v_p(n)} \text{ ou encore } n = \prod_{\substack{p \in \mathbf{P} \\ p \mid n}} p^{v_p(n)}$$

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

Détails

Deux nombres premiers distincts sont toujours premiers entre eux.

²² Deux nombres premiers distincts sont toujours premiers entre eux.

16.3.4 Application aux diviseurs, au PGCD et au PPCM

Proposition 16.54 : Soient a et b deux entiers naturels non nuls. Alors $a \mid b$ si et seulement si pour tout $p \in \mathbf{P}$, $v_p(a) \leq v_p(b)$.

Démonstration. Si a divise b , soit $k \in \mathbf{N}$ tel que $b = ak$.

Alors pour tout premier p , $v_p(b) = v_p(a) + v_p(k) \geq v_p(a)$.

Inversement, supposons que pour tout $p \in \mathbf{P}$, $v_p(a) \leq v_p(b)$, et soit $k = \prod_{p \in \mathbf{P}} p^{v_p(b) - v_p(a)}$.

Alors k est un entier (car les $v_p(b) - v_p(a)$ sont tous positifs) et

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

Donc $a \mid b$. □

Proposition 16.55 : Soient $a, b \in \mathbf{N}^*$. Alors :

1. $a \wedge b = \prod_{p \in \mathbf{P}} p^{\min(v_p(a), v_p(b))}$.

Autrement dit, pour tout $p \in \mathbf{P}$, $v_p(a \wedge b) = \min(v_p(a), v_p(b))$.

2. $a \vee b = \prod_{p \in \mathbf{P}} p^{\max(v_p(a), v_p(b))}$.

Autrement dit, pour tout $p \in \mathbf{P}$, $v_p(a \vee b) = \max(v_p(a), v_p(b))$.

3. a et b sont premiers entre eux si et seulement si pour tout $p \in \mathbf{P}$, $v_p(a) = 0$ ou $v_p(b) = 0$.

Démonstration. 1. Soit $p \in \mathbf{P}$. Alors $p^{\min(v_p(a), v_p(b))}$ divise a et b , donc divise $a \wedge b$.

Ainsi, $v_p(a \wedge b) \geq \min(v_p(a), v_p(b))$.

Inversement, si p^k divise $a \wedge b$, alors p^k divise a et p^k divise b , donc $v_p(a) \geq k$ et $v_p(b) \geq k$, de sorte que $k \leq \min(v_p(a), v_p(b))$.

Et alors $v_p(a \wedge b) \leq \min(v_p(a), v_p(b))$.

2. Il suffit d'utiliser $a \vee b = \frac{ab}{a \wedge b}$, et de noter que pour tous entiers²³ m et n ,

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

Et donc en particulier, pour p premier,

$$v_p(a) + v_p(b) - \min(v_p(a), v_p(b)) = \max(v_p(a), v_p(b)).$$

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. □

²³ Et même réels.

16.3.5 Petit théorème de Fermat

Théorème 16.56 : Soit p un nombre premier, et soit $a \in \mathbf{Z}$. Alors $a^p \equiv a \pmod{p}$.
De plus, si a n'est pas divisible par p , alors $a^{p-1} \equiv 1 \pmod{p}$.

Démonstration. Commençons par remarquer que pour $k \in \llbracket 1, p-1 \rrbracket$, p divise $\binom{p}{k}$.

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, $\binom{p}{k} \equiv 0 \pmod{p}$.

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

$$(u+v)^p = \sum_{k=0}^p \binom{p}{k} u^k v^{p-k} \equiv u^p + v^p \pmod{p}.$$

Prouvons à présent par récurrence sur $a \in \mathbf{N}$ que $a^p \equiv a \pmod{p}$.

Pour $a = 0$ ou $a = 1$, c'est évident. Supposons que $a^p \equiv a \pmod{p}$.

Alors $(a+1)^p \equiv a^p + 1 \equiv a + 1 \pmod{p}$.

Par le principe de récurrence, pour tout $a \in \mathbf{N}$, $a^p \equiv a \pmod{p}$.

Et si $a < 0$, alors il existe $b \in \mathbf{N}$ tel que $a \equiv b \pmod{p}$.

Et donc $a^p \equiv b^p \equiv b \equiv a \pmod{p}$.

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 $a^{p-1} \equiv 1 \pmod{p}$. □

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).

Exemple 16.57

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

En effet, soit $p \in \mathbf{P}$ 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 $(n^2)^{\frac{p-1}{2}} \equiv 1 \pmod{p}$.

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 $\frac{p-1}{2}$ est pair : il existe $k \in \mathbf{Z}$ tel que $\frac{p-1}{2} = 2k \Leftrightarrow p = 4k + 1$.

Détails

Puisque $p \geq 3$, -1 n'est pas congru à 1 modulo p .

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 $\llbracket 0, n-1 \rrbracket$.

Autrement dit, si on note $\bar{r} = \{k \in \mathbf{Z} \mid k \equiv r \pmod{n}\} = \{r + kn, k \in \mathbf{Z}\}$ la classe d'équivalence de r pour la relation de congruence modulo n , alors $\bar{0}, \bar{1}, \dots, \overline{n-1}$ est une partition de \mathbf{Z} . Les classes d'équivalence de la relation de congruence modulo n sont appelées **classes de congruence modulo n** .

Définition 16.58 – Soit $n \in \mathbf{N}^*$. On note $\mathbf{Z}/n\mathbf{Z}$ l'ensemble des classes de congruence modulo n : $\mathbf{Z}/n\mathbf{Z} = \{\bar{0}, \bar{1}, \dots, \overline{n-1}\}$.

Pour $x \in \mathbf{Z}/n\mathbf{Z}$, on appelle **représentant de x** tout élément de x (qui rappelons-le, est un ensemble).

Ainsi, les représentants de $\bar{0}$ sont tous les entiers divisibles par n , les représentants de $\bar{1}$ sont les entiers congrus à 1 modulo n , etc.

Rappelons qu'une classe d'équivalence est entièrement caractérisée par la donnée d'un seul de ses éléments, et donc qu'un représentant de $x \in \mathbf{Z}/n\mathbf{Z}$ caractérise entièrement x .

On définit une loi de composition interne sur $\mathbf{Z}/n\mathbf{Z}$ en posant $\overline{k} + \overline{\ell} = \overline{k + \ell}$.

Le point clé est que la classe d'équivalence de $x + y$ ne dépend pas des représentants x et y choisis.

Plus précisément : si $k \equiv k' \pmod{n}$ et si $\ell \equiv \ell' \pmod{n}$, alors $k + \ell \equiv k' + \ell' \pmod{n}$.

Et donc $\overline{k + \ell} = \overline{k' + \ell'}$.

Remarque

$\mathbf{Z}/n\mathbf{Z}$ n'est donc pas une partie de \mathbf{Z} , mais un ensemble d'ensembles de nombres. Ou encore une partie de $\mathcal{P}(\mathbf{Z})$.

Autrement dit, il n'y a pas d'ambiguïté dans la définition de $\overline{k + \ell}$: tout choix de représentants de \overline{k} et $\overline{\ell}$ conduit à la même classe d'équivalence.

Par exemple, modulo 6, $3 \equiv 9$ et $4 \equiv 16$.
Et alors $\overline{3 + 4} = \overline{7} = \overline{1}$ et $\overline{9 + 16} = \overline{25} = \overline{1}$. Donc $\overline{3} + \overline{4} = \overline{1}$.

Donnons par exemple la table d'addition de $\mathbf{Z}/5\mathbf{Z}$.

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

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

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

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 la loi +.

Ainsi, $(\mathbf{Z}/n\mathbf{Z}, +)$ est un groupe abélien.

Soit alors $\zeta = e^{i\frac{2\pi}{n}}$, de sorte que $\mathbf{U}_n = \{\zeta^k, k \in \llbracket 0, n-1 \rrbracket\}$.

Considérons alors l'application $\varphi : \begin{cases} \mathbf{Z}/n\mathbf{Z} & \longrightarrow & \mathbf{U}_n \\ \overline{k} & \longmapsto & \zeta^k \end{cases}$.

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

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

Ce morphisme est surjectif, car si $z \in \mathbf{U}_n$, alors il existe $k \in \llbracket 0, n-1 \rrbracket$ tel que $z = \zeta^k = \varphi(\overline{k})$.

De plus, $\overline{k} \in \text{Ker } \varphi \Leftrightarrow \varphi(\overline{k}) = 1 \Leftrightarrow \zeta^k = 1$.

Si on note $k = nq + r$ la division euclidienne de k par n , on a alors $\zeta^k = \zeta^r = 1$, et donc, puisque les $\zeta^j, 0 \leq j \leq n-1$ sont deux à deux distincts, nécessairement $r = 0$.

Donc n divise k , de sorte que $\overline{k} = \overline{0}$.

Ceci prouve donc que $\text{Ker } \varphi = \{\overline{0}\}$, 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.

L'élément neutre de $\mathbf{Z}/n\mathbf{Z}$ pour la loi \times est alors $\overline{1}$.

Remarque

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

⚠ Attention !

Je n'ai pas dit qu'il s'agissait d'un sous-anneau de \mathbf{Z} , puisque $\mathbf{Z}/n\mathbf{Z}$ n'est pas une partie de \mathbf{Z} , mais toutes les propriétés d'associativité, distributivité, etc. découlent de celles des lois de \mathbf{Z} .

Proposition 16.59 : Soit $n \in \mathbf{N}^*$. L'application $\pi : \begin{cases} \mathbf{Z} & \longrightarrow & \mathbf{Z}/n\mathbf{Z} \\ k & \longmapsto & \overline{k} \end{cases}$, qui à un entier associe sa classe de congruence modulo n est un morphisme d'anneaux surjectif.

Démonstration. On a déjà $f(1) = \bar{1}$, qui est le neutre multiplicatif de $\mathbf{Z}/n\mathbf{Z}$.

Par ailleurs, nous avons déjà prouvé²⁴ que pour $k, \ell \in \mathbf{Z}$, $\overline{k + \ell} = \bar{k} + \bar{\ell}$.

Soit encore $f(k + \ell) = f(\bar{k}) + f(\bar{\ell})$.

Et de même pour le produit, donc f est bien un morphisme d'anneaux.

Il est évidemment surjectif, puisque les éléments de $\mathbf{Z}/n\mathbf{Z}$ sont tous de la forme $\bar{k} = f(k)$, pour $0 \leq k \leq n - 1$. \square

Proposition 16.60 : Soit $n \in \mathbf{N}^*$ et $a \in \mathbf{Z}$. Alors \bar{a} est un inversible de $\mathbf{Z}/n\mathbf{Z}$ si et seulement si $a \wedge n = 1$.

Démonstration. \bar{a} est inversible si et seulement si il existe $\bar{u} \in \mathbf{Z}/n\mathbf{Z}$ 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 $a \wedge n = 1$. \square

Proposition 16.61 : 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 $\bar{0} = \bar{n} = \bar{a}\bar{b}$.

Mais $2 \leq a < n$, donc $\bar{a} \neq \bar{0}$ et de même $\bar{b} \neq \bar{0}$.

Donc \bar{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.

Inversement, si n est premier, alors pour tout $k \in \llbracket 1, n - 1 \rrbracket$, $n \wedge k = 1$, et donc \bar{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. \square

Notons qu'une fois ces résultats établis, si l'on connaît un peu de théorie des groupes (au moins le fait que dans un groupe fini tout élément est d'ordre divisant le cardinal du groupe²⁵), il est facile de donner une démonstration du petit théorème de Fermat.

Soit p un nombre premier, et soit $a \in \mathbf{Z}$, non divisible par p .

Alors \bar{a} est un élément non nul du groupe $((\mathbf{Z}/p\mathbf{Z})^\times, \times)$, qui est de cardinal $p - 1$ (car tous les éléments non nuls de $\mathbf{Z}/p\mathbf{Z}$ sont inversibles).

Et donc est d'ordre divisant $p - 1$, si bien que $\bar{a}^{p-1} = \bar{1} \Leftrightarrow a^{p-1} \equiv 1 \pmod{p}$.

²⁴ C'est la définition de l'addition sur $\mathbf{Z}/n\mathbf{Z}$.

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).

²⁵ Voir le DM 11.