Arithmétique dans $\mathbf{Z}$

L'arithmétique est une des plus anciennes branches des mathématiques, mais elle est loin d'être épuisée. Par exemple, ce n'est qu'en 1994 que A. Wiles démontre le grand théorème de Fermat (XVII^{e}) qui établit que pour $n \geqslant 3$ l'équation $x^n + y^n = z^n$ n'admet pas de solutions entières strictement positives.
De même, la conjecture de Goldbach (XVIII^{e}) selon laquelle tout entier pair $n \geqslant 4$ est somme de deux nombres premiers est non démontrée (et déchaîne les passions des amateurs, tous persuadés d'avoir trouvé LA preuve, mais d'être les victimes d'un affreux complot).

1 Division euclidienne

Le théorème de division euclidienne est **la propriété fondamentale** de ce chapitre. Toute l'arithmétique que vous verrons découle de cette propriété. Ainsi, lorsque nous définirons une division euclidienne sur l'ensemble des polynômes, nous aurons accès à toutes les propriétés arithmétiques de ce chapitre sans nécessité de les redémontrer.

Théorème 1.1 *(Rappel)*

Toute partie non vide de $\mathbf{N}$ admet un plus petit élément.

Preuve

On l'avait démontré à partir du principe de récurrence. ∎

Théorème 1.2 *(Division euclidienne)*

Soit $(a, b) \in \mathbf{Z} \times \mathbf{N}^*$, il existe un unique couple $(q, r) \in \mathbf{Z} \times \mathbf{N}$ tel que

1. $0 \leqslant r < b$,
2. $a = bq + r$.

a est le **dividende**, b est le **diviseur**, q est le **quotient** et r est le **reste.**

Explications

Il s'agit simplement de la division entière que vous avez apprise au primaire.
Pour $a \geqslant 0$, dans la division par b, on retire b autant de fois que l'on peut à la quantité a.
Par exemple, pour la division de 14 par 5, on voit que l'on peut retirer au plus deux fois 5 à 14 avant d'obtenir un négatif : $14 = 5 \times 2 + 4$.
Cela s'interprète comme un problème de partage : si vous avez la quantité 14 à partager en 5, alors chacun recevra 2 et il restera 4 à la fin que l'on ne peut plus partager de façon entière entre les 5 personnes.

Lorsque $a < 0$, il faut à présent ajouter b jusqu'à obtenir un positif.
Par exemple pour la division euclidienne de -14 par 5, il faut ajouter au minimum 3×5 pour avoir un reste positif. Ainsi $-14 = 5 \times (-3) + 1$.

Preuve

Existence : Si on pose $q = \left\lfloor \frac{a}{b} \right\rfloor \in \mathbf{N}$ et $r = a - bq \in \mathbf{Z}$, alors $\frac{a}{b} - 1 < q = \left\lfloor \frac{a}{b} \right\rfloor \leqslant \frac{a}{b}$ donc $0 \leqslant a - bq < b$, donc $r \in [\![0, b-1]\!]$.
Unicité : supposons que les couples (q, r) et (q', r') conviennent tous les deux.

$$a = bq + r$$
$$a = bq' + r'.$$

On réalise la différence, ce qui donne $0 = b(q - q') = r - r'$ c'est-à-dire $r - r' = b(q' - q)$.
Or $-b < r - r' < b$, donc en divisant par $b > 0$, on trouve $-1 < q - q' < 1$ qui est un

nombre entier, ce qui permet de conclure $q = q'$, donc $r = r'$. ■

Propriété 1.3 *(Extension au cas $b < 0$)*

On peut également réaliser une division euclidienne avec $b < 0$, elle s'énonce alors de la façon suivante :
Soit $(a, b) \in \mathbf{Z} \times \mathbf{Z}^*$, il existe un unique couple $(q, r) \in \mathbf{Z} \times \mathbf{N}$ tel que

1. $0 \leqslant r < |b|$,
2. $a = bq + r$.

Remarque : Cette situation est rarement utile car on s'arrange autant que possible à se ramener au cas $b > 0$ (comme le fait la preuve elle-même).

Preuve

Existence : on réalise la division euclidienne de a par $|b|$ ce qui donne $a = |b|\, q + r$ et $0 \leqslant r < |b|$.
Donc en affectant à q le signe de b, on trouve bien $a = bq' + r$ qui vérifie les hypothèses.
Unicité : exactement comme pour le cas $b > 0$. ■

Propriété 1.4 *(Caractérisation du quotient)*

Pour la division euclidienne $a = bq + r$, avec $b > 0$, on a

$$q = \left\lfloor \frac{a}{b} \right\rfloor \qquad \text{et} \qquad r = a - bq.$$

Remarque : Pour $b \in \mathbf{Z}^*$, on a $q = \operatorname{sgn}(b) \left\lfloor \frac{a}{|b|} \right\rfloor$.

2 Multiples et diviseurs

Définition 2.1

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

- a est un **diviseur** de b, ou a divise b s'il existe $c \in \mathbf{Z}$ tel que $ac = b$.
  On note parfois : $a|b$.
- b est un **multiple** de a si a divise b.

On remarquera que 0 se divise lui-même.
Un élément **inversible** est un diviseur de 1 : il n'y a que 1 et -1 qui soient inversibles dans $\mathbf{Z}$.

Propriété 2.2

Soit $(a, b, d, d') \in \mathbf{Z}^2$.

1. Si $d|a$ et $d|b$ alors $\forall (u, v) \in \mathbf{Z}^2$, $d|(au + bv)$.
2. Si $d|a$ et $d'|b$ alors $dd'|ab$.
3. Si $d|a$, alors $\forall k \in \mathbf{N}$, $d^k|a^k$.

Preuve

Il suffit de revenir à la définition.

1. Si $d|a$ et $d|b$, alors il existe $(k, k') \in \mathbf{Z}^2$ tel que $dk = a$ et $dk' = b$.
   Ainsi $au + bv = dku + dk'v = d(ku + k'v)$.
   Or, $ku + k'v \in \mathbf{Z}$, donc $d|(au + bv)$.
2. Si $d|a$ et $d'|b$, alors il existe $(k, k') \in \mathbf{Z}^2$ tel que $dk = a$ et $d'k' = b$.
   donc $dd'(kk') = ab$ ce qui montre que $dd'|ab$.
3. Conséquence du point précédent avec une récurrence immédiate sur $k \in \mathbf{N}$.

■

Propriété 2.3 *(Rappel)*

La relation de divisibilité est une relation d'ordre partielle sur $\mathbf{N}$, mais pas sur $\mathbf{Z}$.

Preuve

Voir la preuve dans le chapitre sur les nombres réels. ■

Définition 2.4 *(PGCD et PPCM)*

Soit $(a, b) \in \mathbf{Z}^2$,

- le **plus grand diviseur commun** à a et b – non tous les deux nuls – est le plus grand entier naturel qui divise à la fois a et b.
  On le note $a \wedge b$ ou $\operatorname{PGCD}(a, b)$.
- le **plus petit multiple commun** à a et b – tous les deux non nuls – est le plus petit entier naturel non nul qui est à la fois multiple de a et de b.
  On le note $a \vee b$ ou $\operatorname{PPCM}(a, b)$.

Preuve

Pour montrer que cette définition possède un sens, on montre l'existence du PGCD *et du* PPCM.

- PGCD
  Si on note D, l'ensemble des diviseurs communs à a et b ; $1 \in D \cap \mathbf{N}$, donc cette partie de $\mathbf{N}$ est non vide. Si $a \neq 0$ et $d|a$, alors $d \leqslant |a|$. Ainsi, pour prendre en compte le cas où a ou b est nul, on peut dire que $D \cap \mathbf{N}$ est majorée par $\max(|a|, |b|)$.
  Donc $D \cap \mathbf{N}$ est une partie non vide majorée de $\mathbf{N}$: elle contient un plus grand élément.

- PPCM
  Si on note M, l'ensemble des multiples communs à a et b ; alors, $M \cap \mathbf{N}^*$ est une partie non vide de $\mathbf{N}$.
  En effet, $|ab| \in M \cap \mathbf{N}^*$.
  Donc $M \cap \mathbf{N}^*$ contient bien un plus petit élément.

■

Définition 2.5 *(Entiers premiers entre eux)*

Deux entiers a et b sont dits **premiers entre eux**, si $a \wedge b = 1$.

3 Algorithme d'Euclide

Propriété 3.1

Soient $a \in \mathbf{N}^*$, $(b,\, d) \in (\mathbf{Z}^*)^2$.
Si $d|a$ et $d|b$ alors d divise le reste de la division euclidienne de a par b.

Preuve

Immédiat, si $d|a$ et $d|b$, alors $d|a - bq = r$. ■

Propriété 3.2

Soit $(a,\, b) \in \mathbf{Z}^2 \setminus \{(0,\, 0)\}$.
Si $a = bq + r$ avec $(q,\, r) \in (\mathbf{Z})^2$, alors $a \wedge b = b \wedge r$.

Remarque : Ce n'est pas nécessairement la division euclidienne car on n'impose pas à b d'être positif non nul ni à r d'être dans $[\![0,\, b-1]\!]$.

Preuve

Si $d|a$ et $d|b$ alors $d|a - bq$ donc $d|r$.
Réciproquement, si $d|b$ et $d|r$, alors $d|bq + r$. Ainsi les diviseurs communs à a et b sont les mêmes que ceux de b et r. ■

Méthode *(Algorithme d'Euclide)*

Soit $(a,\, b) \in (\mathbf{N}^*)^2$, on note $r_{-1} = a$ et $r_0 = b$, et on définit la suite $(r_n)_{n\in\mathbf{N}}$ par : $\forall n \in \mathbf{N}$,

- si $r_n \neq 0$, alors r_{n+1} est le reste de la division euclidienne de r_{n-1} par r_n.
- si $r_n = 0$, alors $r_{n+1} = 0$.

La suite est stationnaire à 0.
Ainsi, il existe un rang $n_0 \geqslant 1$ tel que $r_{n_0-1} \neq 0$ et $r_{n_0} = 0$. On a alors

$$a \wedge b = r_{n_0-1}.$$

Remarque : On voit que si $a < b$, alors la première étape consiste à échanger a et b.

Preuve

On montre par récurrence immédiate que $\forall n \in \mathbf{N}$, $r_n \in \mathbf{N}$ et que la suite est décroissante.
Ainsi, l'ensemble de ses valeurs est une partie non vide de $\mathbf{N}$ qui admet donc un plus petit élément. Cet élément ne peut pas être strictement positif (car si $r_n \geqslant 1$, alors $r_{n+1} < r_n$), donc la suite atteint 0 et elle est donc stationnaire à 0.
Si on note n_0 le plus petit entier n tel que $r_n = 0$ (partie non vide minorée de $\mathbf{N}$), alors $n_0 \geqslant 1$ (car $r_0 = b > 0$).
Montrons alors que $r_{n_0-1} = a \wedge b$.
Par récurrence immédiate et d'après la propriété précédente, $\forall n \leqslant n_0$, $a \wedge b = r_{n-1} \wedge r_n$.
En particulier $a \wedge b = r_{n_0-1} \wedge r_{n_0} = r_{n_0-1} \wedge 0 = r_{n_0-1}$. ■

Exemple *(Informatique)*

Pour $b \geqslant 2$, un entier, la division euclidienne permet d'obtenir simplement l'écriture d'un entier en base b. Comment procède-t-on ?
Si besoin, on pourra commencer par $b = 10$ et généraliser ensuite.

Solution :

Voyons sur un exemple avec $b = 10$.
Il s'agit d'écrire un nombre $a = 1487\cdots869$ en écriture décimale, ce qui revient à « extraire » chacun de ses chiffres pour l'écrire

$$a = 9 \times 10^0 + 6 \times 10^1 + 8 \times 10^2 \cdots$$

On procède par étapes.

1	4	8	7	$\cdots$	8	6	9
			q_1				a_0
1	4	8	7	$\cdots$	8	6	9
			q_2			a_1	
			$\vdots$				
1	4	8	7	$\cdots$	8	6	9
q_n		a_{n-1}					
1	4	8	7	$\cdots$	8	6	9
q_{n+1}	a_n						

La première étape extrait le premier chiffre : $a = 10q_1 + a_0$, puis on réitère à la seconde étape : $q_0 = 10q_1 + a_1$ ce qui donne $a = 10^2 q_1 + 10a_1 + a_0$... et ainsi de suite jusqu'à épuisement.
Formalisons :
Pour $a \in \mathbf{N}$, on construit la suite des restes des divisions successives par b.
On pose $q_0 = a$ et pour tout $n \in \mathbf{N}$, on effectue la division euclidienne de q_n par b : $q_n = bq_{n+1} + a_n$ avec $a_n \in [\![0,\, b-1]\!]$.
On construit ainsi les suites $(q_n)_{n\in\mathbf{N}}$ et $(a_n)_{n\in\mathbf{N}}$.
$(q_n)_{n\in\mathbf{N}}$ est une suite décroissante et à valeurs entières donc elle est stationnaire (et ne peut l'être qu'à 0). Ceci montre que la suite $(a_n)_{n\in\mathbf{N}}$ est également stationnaire à 0.
Les deux suites sont donc stationnaires à 0.
Ensuite, on montre par récurrence que pour tout $n \in \mathbf{N}$, $a = q_n b^n + \sum_{k=0}^{n-1} a_k b^k$.

Initialisation : vraie par définition de q_0 (la somme est vide).

Hérédité : on suppose la relation au rang $n \in \mathbf{N}$, alors,

$$a = q_n b^n + \sum_{k=0}^{n-1} a_k b^k = (q_{n+1}b + a_n)b^n + \sum_{k=0}^{n-1} a_k b^k = q_{n+1}b^{n+1} + \sum_{k=0}^{n} a_k b^k.$$

Ce qui prouve l'égalité par récurrence.
Or la suite $(q_n)_{n\in\mathbf{N}}$ est stationnaire à 0,
donc il existe un rang n_0 tel que pour tout $n \geqslant n_0$,

$$a = \sum_{k=0}^{n} a_k b^k = \sum_{k=0}^{+\infty} a_k b^k.$$

On remarque que pour tout $n \in \mathbf{N}$, $q_n = \left\lfloor \frac{a}{b^n} \right\rfloor$.

Propriété 3.3

Pour a et b de signe quelconque, $a \wedge b = |a| \wedge |b|$, donc on peut appliquer l'algorithme d'Euclide avec les entiers positifs.

Preuve

Les diviseurs de a sont les mêmes que ceux de $-a$. ■

Exemple *(Méthode « basique »)*

Utiliser l'algorithme d'Euclide pour donner $258 \wedge 145$ et en déduire un couple $(u, v) \in \mathbf{Z}^2$ tel que $258u + 145v = 1$.

Solution :

On écrit l'algorithme d'Euclide en conservant les résultats, et on le remonte ensuite à l'envers.

$$\begin{aligned} 258 &= 145 \times 1 + 113 \\ 145 &= 113 \times 1 + 32 \\ 113 &= 32 \times 3 + 17 \\ 32 &= 17 \times 1 + 15 \\ 17 &= 15 \times 1 + 2 \\ 15 &= 2 \times 7 + 1 \\ 2 &= 1 \times 2 + 0 \end{aligned}$$

n	r_{n-1}	r_n	q_n	r_{n+1}
0	258	145	1	113
1	145	113	1	32
2	113	32	3	17
3	32	17	1	15
4	17	15	1	2
5	15	2	7	1
6	2	1	2	0

On obtient donc $\text{PGCD}(258, 145) = 1$.
À présent, pour obtenir l'égalité cherchée, on remonte l'algorithme précédent en remplaçant à chaque fois le dernier r_k avec la relation précédente.

$$\begin{aligned} 1 &= 15 - 2 \times 7 \\ &= 15 - (17 - 15 \times 1) \times 7 = 17 \times (-7) + 15 \times 8 \\ &= 17 \times (-7) + (32 - 17 \times 1) \times 8 = 32 \times 8 + 17 \times (-15) \\ &= 32 \times 8 + (113 - 32 \times 3) \times (-15) = 113 \times (-15) + 32 \times 53 \\ &= 113 \times (-15) + (145 - 113 \times 1) \times 53 = 145 \times 53 + 113 \times (-68) \\ &= 145 \times 53 + (258 - 145 \times 1) \times (-68) = 258 \times (-68) + 145 \times 121. \end{aligned}$$

Donc $(u, v) = (-68, 121)$ convient.
On verra plus loin comment trouver tous les autres couples solution.

L'algorithme d'Euclide, tel que présenté dans l'exemple précédent permet de trouver la relation de Bézout[1] mais il est long et demande une mémoire importante pour retenir tous les résultats intermédiaires avant de faire la « remontée ».
Il existe un méthode optimisée, qui permet de construire directement la relation de Bézout, on la préférera dans le cadre d'une implémentation en informatique.
Pour trouver cette méthode, on se contente de réaliser l'algorithme en essayant de construire en même temps la relation : déterminer à chaque étape, le reste en fonction des deux valeurs a et b du début.
Si on suppose l'avoir fait à l'étape n, voici ce que ça donne en continuant :

$$\begin{array}{rcccccccc} r_{n-1} & = & a & \times & u_{n-1} & + & b & \times & v_{n-1} \\ r_n & = & a & \times & u_n & + & b & \times & v_n \end{array}$$

r_{n+1} s'obtient par la division euclidienne de r_{n-1} par r_n qui donne donc

$$r_{n-1} = r_n q + r_{n+1}.$$

Ainsi, pour écrire a et b en fonction de r_{n+1}, on trouve

$$\begin{aligned} r_{n+1} &= r_{n-1} - q r_n \\ &= a \times u_{n-1} + b \times v_{n-1} - q\,(a \times u_n + b \times v_n) \\ &= a \times (u_{n-1} - q u_n) + b \times (v_{n-1} - q v_n)\,. \end{aligned}$$

On obtient donc une récurrence linéaire d'ordre 2 en le couple (u_n, v_n). Il reste simplement à initialiser avec deux rangs.
Le plus simple pour cela est de commencer en écrivant :

$$\begin{array}{rcccccccc} r_0 & = & a & \times & 1 & + & b & \times & 0 \\ r_1 & = & a & \times & 0 & + & b & \times & 1 \end{array}$$

Puis on établit la suite des restes successifs par récurrence, avec les termes (u_n, v_n).
À chaque étape de l'algorithme, on a donc en mémoire 6 termes : deux pour la suite u, deux pour la suite v et deux restes.
L'algorithme se termine lorsque l'on obtient un reste nul.
En Python, voilà ce que ça donne (pour les restes, on a conservé les noms de variables a et b) :

1. Ici, intervient une difficulté portant sur l'orthographe de ce nom. Faut-il écrire Bézout ou Bezout ? Des recherches acharnées du savant Cosinus lui-même ont établi avec une certitude absolue qu'il n'y avait aucune certitude, ou plutôt, que les deux orthographes ont eu cours, de la main du mathématicien éponyme lui-même. Rappelons que l'homme qu'on ne peut nommer vécut de 1730 à 1783, époque où l'orthographe des noms propres était sujette à fluctuations. Le site Gallica propose ainsi un certains nombre de cours de mathématiques imprimés vers les années 1810-1840, certains par Bézout et d'autres par Bezout (ici, l'usage des lettres capitales ne justifie pas l'absence de l'accent, mis par ailleurs au terme mathématiques). La similarité très grande des sujets porte à croire qu'il s'agit du même personnage et que les deux orthographes sont donc utilisées également par les imprimeurs au début du XIXème. Selon le dictionnaire Alfonsi aux éditions L'Harmattan (2011), Bezout aurait utilisé les deux écritures, mais avec une préférence pour l'orthorgraphe accentuée (je n'ai pas eu accès à l'ouvrage directement).
Il semble également que le XXème siècle ait privilégié l'écriture sans accent, alors que le XXIème, en rupture totale, ait préféré largement l'écriture avec accent.
En homme de mon temps, je me soumets donc et utiliserai préférentiellement Bézout dans ce cours ; veuille bien Bezout me pardonner.

Méthode *(Algorithme d'Euclide étendu en informatique)*

```
def euclide(a,b):
    (u0,v0) = (1,0)   # a = a*1+b*0
    (u1,v1) = (0,1)   # b = a*0+b*1
    while b > 0 :
        (q,r) = (a//b, a%b)   # division euclidienne
        (u0,v0,u1,v1)=(u1,v1,u0-q*u1,v0-q*v1)
        (a,b) = (b,r)
    return (a,u0,v0)          # (pgcd, u, v)
```

Preuve

Si on note a_0, b_0 les deux valeurs dont on cherche une décomposition, alors, en conservant les notations de l'algorithme Python, on montre par récurrence double qu'à la fin de chaque étape (boucle) : $a = a_0u_0 + b_0v_0$ et $b = a_0u_1 + b_0v_1$.
Lorsque l'algorithme s'arrête (il s'arrête nécessairement par décroissance de r), on a alors $r = 0$ et a qui est égal au reste précédent, c'est-à-dire au PGCD.
On choisit donc u_0, v_0 pour la relation. ■

Théorème 3.4 *(Relation de Bézout)*

Soient a et b deux entiers non tous les deux nuls,

$$\exists (u,\, v) \in \mathbf{Z}^2,\ au + bv = a \wedge b.$$

⚠ Les entiers u et v ne sont pas définis de façon unique.

Preuve

Grâce à l'algorithme d'Euclide étendu tel que décrit précédemment. ■

La théorème suivant donne une forme de réciproque lorsque a et b sont premiers entre eux.

Théorème 3.5 *(Théorème de Bézout)*

Soient a et b deux entiers non tous les deux nuls,

$$a \wedge b = 1 \iff \exists (u,\, v) \in \mathbf{Z}^2,\ au + bv = 1.$$

Remarque : D'après cette même relation u et v sont premiers entre eux.

Preuve

Le sens direct a été montré au théorème précédent.
Le sens réciproque est immédiat : $a \wedge b | a$ et $a \wedge b | b$, donc $a \wedge b | au + bv = 1$,
donc $a \wedge b = 1$. ■

Exemple

Montrer que cette réciproque est fausse si $d \neq 1$.

Solution :

Par exemple pour $a = 2$ et $b = 3$, en prenant $u = v = 1$, alors $au + bv = 5$, mais $a \wedge b = 1$.

Par contre, on voit alors que le PGCDdivise d dans la relation. Le cas du théorème de Bézout fonctionne bien car pour $d = 1$, il n'y a pas d'autre diviseurs positifs que lui-même : c'est ce qui permet de conclure.

⚠ Il ne faut pas confondre la relation de Bézout qui est valable quel que soit le PGCD, et le théorème, qui donne la réciproque lorsque les entiers sont **premiers entre eux.**

Propriété 3.6 *(Caractérisation du PGCD)*

Soient a et b deux entiers relatifs non tous les deux nuls.

$a \wedge b$ est le plus grand diviseur commun à a et b pour la relation d'ordre de divisibilité sur $\mathbf{N}$.

En particulier, tous les diviseurs communs à a et b le divisent.

Autrement écrit :

Soit $d \in \mathbf{N}$, $d = a \wedge b$ si, et seulement si les deux conditions suivantes sont vérifiées :

1. $d|a$ et $d|b$,
2. $\forall \delta \in \mathbf{Z}$, $(\delta|a$ et $\delta|b) \Rightarrow \delta|d$.

ou écrit en français :

1. d divise a et b,
2. tout diviseur commun à a et b est aussi un diviseur de d.

Preuve

(sens direct) soit δ un diviseur commun à a et b, pour tout $(u,\, v) \in \mathbf{Z}^2$, on a $\delta | au + bv$.
Ainsi, d'après la relation de Bézout, $\delta|d$.
(sens réciproque) évident. ■

Propriété 3.7 *(Caractérisation du PPCM)*

Soient a et b deux entiers relatifs non tous les deux nuls.

$a \vee b$ est le plus petit multiple commun à a et b pour la relation d'ordre de divisibilité sur $\mathbf{N}$.

En particulier, il divise tous les multiples communs à a et b.

Autrement écrit :

Soit $m \in \mathbf{N}$,
$m = a \vee b$ si, et seulement si les deux conditions suivantes sont vérifiées :

1. $a|m$ et $b|m$,
2. $\forall \mu \in \mathbf{Z}$, $(a|\mu$ et $b|\mu) \Rightarrow m|\mu$.

ou écrit en français :

1. m est multiple de a et b,
2. tout multiple commun à a et b est aussi un multiple de m.

Preuve

(sens direct) si $m = a \vee b$, alors par définition m est un multiple commun à a et b.
De plus, si μ est un autre multiple commun, alors si on réalise la division euclidienne de μ par m, le reste est aussi un multiple commun à a et b. Or, il est strictement inférieur à m, donc il est nul. Ainsi m divise μ, ou autrement dit, μ est un multiple de m.
(sens réciproque) évident. ■

Concrètement on utilise souvent le sens réciproque des caractérisations précédentes :

Corollaire 3.8

1. Si $d|a$ et $d|b$, alors $d|(a \wedge b)$.
2. Si $a|m$ et $b|m$, alors $(a \vee b)|m$.

Propriété 3.9

Si $d = a \wedge b$, alors il existe $(a', b') \in \mathbf{Z}^2$ tel que $a = da'$ et $b = db'$.
Dans ce cas $a' \wedge b' = 1$.

Preuve

D'après Bézout, il existe $(u, v) \in \mathbf{Z}^2$ tel que $au + bv = d$, donc en divisant par $d \neq 0$, on obtient $a'u + b'v = 1$ ce qui prouve que $a \wedge b = 1$. ■

Théorème 3.10

Soient $(a, b) \in (\mathbf{N}^*)^2$

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

Preuve

On utilise la relation précédente pour écrire $a = (a \wedge b)a'$ et $b = (a \wedge b)b'$.
Alors $(a \wedge b) \times (a \wedge b)a'b' = ab$.
Or, $(a \wedge b)a'b'$ est évidemment un multiple commun à a et à b et donc un multiple du PPCM.
Ainsi, il existe $k \in \mathbf{N}$ tel que $k(a \vee b) = (a \wedge b)a'b'$.
$a \vee b$ étant un multiple de a, on peut diviser la relation par a et obtenir que $k|b'$. On obtient de la même manière que $k|a'$.
Donc $k|(a' \wedge b') = 1$, donc $k = 1$.
Ainsi $a \vee b = (a \wedge b)a'b'$ et on obtient la relation voulue. ■

Propriété 3.11 *(Propriétés du PGCD et du PPCM)*

Si a et b sont deux entiers non tous les deux nuls, alors

1. (commutativité)
$$a \wedge b = b \wedge a \quad \text{et} \quad a \vee b = b \vee a.$$
2. (insensible au signe)
$$(-a) \wedge b = a \wedge b \quad \text{et} \quad (-a) \vee b = a \vee b.$$
3. (homogénéité)
$$\forall k \in \mathbf{Z}^*, \qquad (ka) \wedge (kb) = |k|\,(a \wedge b) \quad \text{et} \quad (ka) \vee (kb) = |k|\,(a \vee b)\,.$$

Preuve

Trivial pour les deux premières relations.
Pour la dernière relation avec le PGCD, on applique l'algorithme d'Euclide (on prend, a, b, k positifs) et on remarque que si $a = bq + r$, alors $ka = kbq + kr$ avec $r \leqslant b - 1$, donc $kr \leqslant kb - k \leqslant kb - 1$.
Par unicité dans la division euclidienne, le reste est multiplié par k.
Ainsi, par récurrence immédiate, la suite des restes de l'algorithme d'Euclide est aussi multipliée terme à terme par k, donc le dernier reste non nul l'est aussi. C'est le PGCD. Pour le PPCM, cela découle de la propriété précédente. ■

4 Nombres premiers

Définition 4.1

Un nombre entier naturel est **premier** s'il admet exactement deux diviseurs distincts dans $\mathbf{N}$ (1 et lui-même).
On notera $\mathcal{P}$ l'ensemble des nombres premiers.

Remarque : 1 n'est pas premier (les diviseurs ne sont pas distincts).

Exemple *(Crible d'Eratosthène)*

Le crible d'Eratosthène est une méthode algorithmique simple pour trouver facilement tous les nombres premiers inférieurs ou égaux à une certaine valeur.
Par exemple, si on cherche tous les nombres premiers inférieurs à 100, on les place dans une grille.

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

L'idée est ensuite de rayer tous les nombres qui ne sont pas premiers, c'est-à-dire ceux qui ont des diviseurs strictement compris entre 1 et eux-mêmes.
On barre donc 1, puis 2 est premier, mais tous ses multiples ne le sont pas, donc on les barre tous en avançant de 2 en 2 dans le tableau.

~~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 trouve alors que 3 est premier et on barre tous ses multiples (en avançant de 3 en 3 dans le tableau).

~~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~~

La case suivante non barrée est 5 qui est premier, et on barre tous ses multiples... et ainsi de suite jusqu'à la fin du tableau.
On remarque qu'il n'est pas nécessaire de s'occuper des multiples de 4 car il est barré. Cela veut dire qu'il est lui-même multiple d'un nombre premier plus petit (2) et que les multiples de 4 sont donc tous également multiples de ce nombre (2) : ils ont donc déjà été barrés.
On trouve à la fin :

~~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~~

Exemple

Soit $n \in \mathbf{N}^*$. Montrer que si n n'admet pas de diviseur inférieur à $\sqrt{n}$, alors, il est premier.
Ainsi, pour le crible d'Eratosthène avec 100, on n'a plus rien à barrer à partir des multiples de 10.

Propriété 4.2

Tout entier supérieur ou égal à 2 admet au moins un diviseur premier (éventuellement lui-même).

Preuve

Par récurrence forte.

Initialisation : 2 est premier et se divise lui-même.

Hérédité : Pour $n \geqslant 2$.

Si n est premier, alors il admet un diviseur premier (lui-même), sinon, il admet un diviseur d avec $2 \leqslant d \leqslant n-1$.

Or, par hypothèse de récurrence forte, d admet un diviseur premier, qui est donc aussi diviseur premier de n. ■

Théorème 4.3

Il existe une infinité de nombres premiers.

Preuve

Supposons par l'absurde qu'il existe un nombre fini de nombres premiers que l'on nomme $p_1, p_2, \cdots, p_n$.

On pose $p = 1 + \prod_{k=1}^{n} p_k$. p admet un diviseur premier (car $p \geqslant 2$), ainsi, il existe $i \in [\![1, n]\!]$ tel que $p_i | p$.

Or, $p_i | \prod_{k=1}^{n} p_k$, donc $p_i | p - \prod_{k=1}^{n} p_k = 1$. C'est absurde. ■

Théorème 4.4 *(Lemme de Gauss)*

Soit $(a, b, c) \in (\mathbf{Z}^*)^3$.

$$\text{Si } a|bc \text{ et } a \wedge c = 1, \text{ alors } a|b.$$

Preuve

Si $a|bc$, alors il existe $k \in \mathbf{Z}$ tel que $ak = bc$.

De plus, $a \wedge c = 1$, donc en appliquant l'égalité de Bézout, on trouve $(u, v) \in \mathbf{Z}^2$ tel que $au + cv = 1$.

Ainsi, en multipliant la première relation par v, on trouve :

$$akv = bcv = b(1 - au).$$

Ce qui est équivalent à $a(kv + bu) = b$, ainsi $a|b$. ■

Théorème 4.5

Soit $(a, a', c) \in (\mathbf{Z}^*)^3$. Si $a|c$, $a'|c$ et si $a \wedge a' = 1$, alors $aa'|c$.

Preuve

$a \wedge a' = 1$, donc il existe $(u, v) \in \mathbf{Z}^2$ tel que $au + a'v = 1$.

Or $a|c$ donc $aa'|ca$ et de la même manière $aa'|ca'$.

Donc $aa'|cau + ca'v = c(au + a'v) = c$. ■

Exemple

Si $5|a$ et $12|a$ alors $60|a$.

Les équations diophantiennes (équations à coefficients entiers et solutions entières) sont très difficiles à résoudre en général. Cependant, celles qui sont sous la forme d'une relation de Bézout se résolvent aisément.

Exemple *(Une équation diophantienne simple)*

Trouver toutes les solutions dans $\mathbf{Z}$ de l'équation $5x + 7y = 1$.

Solution :

1. *Solution particulière.*
   On trouve une solution particulière avec l'algorithme d'Euclide.
   $7 = 5 + 2$ et $5 = 2 \times 2 + 1$.
   Donc $1 = 5 - 2 \times 2 = 5 - (7 - 5) \times 2 = 5 \times 3 + 7 \times (-2)$.
   Le couple $(x_0, y_0) = (3, -2)$ est donc une solution particulière à cette équation.
2. *Solution générale*
   - Forme des solutions : (x, y) solution si, et seulement si $5x + 7y = 1 = 5x_0 + 7y_0$, si, et seulement si $5(x - x_0) + 7(y - y_0) = 0$.
     Donc chercher les solutions générales se ramène à la résolution de l'équation homogène :
     $$5u + 7v = 0.$$
   - Analyse : Si (u, v) solution, alors, $5|7v$.
     Or, $5 \wedge 7 = 1$, donc en appliquant le lemme de Gauss, $5|v$.
     Ainsi, il existe $k \in \mathbf{Z}$ tel que $v = 5k$.
     Dans ce cas, $5u = -7 \times 5k$, donc $u = -7k$.
   - Synthèse : Soit $k \in \mathbf{Z}$, on note $u = -7k$ et $v = 5k$.
     Alors $5u + 7v = -5 \times 7k + 7 \times 5k = 0$, donc le couple est solution de l'équation homogène.
3. *Conclusion :*
   $$\mathscr{S} = \{(-7k + 3, 5k - 2), k \in \mathbf{Z}\}.$$

Exemple

Pour $(a, b, d) \in \mathbf{Z}^3$, avec a et b non tous les deux nuls, l'équation d'inconnues $(x, y) \in \mathbf{Z}^2$:

$$ax + by = d$$

admet des solutions si, et seulement si $a \wedge b | d$.

En effet, si x et y sont solution, alors $a \wedge b | a$ et $a \wedge b | b$ donc $a \wedge b | ax + by = d$.

Réciproquement, si $a \wedge b | d$, alors on peut écrire $a = (a \wedge b)a'$, $b = (a \wedge b)b'$ et $d = (a \wedge b)d'$ où $a' \wedge b' = 1$.

L'équation s'écrit alors $a'x + b'y = 1$ ce qui admet des solutions (une infinité) d'après le théorème de Bézout.

Théorème 4.6 *(Théorème fondamental de l'arithmétique)*

Soit $a \in \mathbf{N}^*$.
Il existe $n \in \mathbf{N}$,
$(p_1, \cdots, p_n)$ sont n nombres premiers distincts deux à deux,
$(\alpha_1, \cdots, \alpha_n) \in (\mathbf{N}^*)^2$,

tels que

$$a = \prod_{k=1}^{n} p_k^{\alpha_k}.$$

Cette décomposition est unique (à l'ordre près).
Tout entier naturel non nul se décompose de façon unique comme produit de facteurs premiers.

Explications

Ce théorème traduit que les nombres premiers sont les « *briques élémentaires* » à partir desquelles on peut reconstruire tous les nombres entiers.
Ainsi, chaque nombre entier peut se décomposer en produit de nombres premiers (si le nombre est négatif, on multiplie par $\lambda = -1$).
En outre, cette décomposition est unique et permet donc d'identifier parfaitement le nombre en question : ainsi deux nombres sont égaux si, et seulement s'ils ont la même décomposition.
Chaque nombre premier peut intervenir plusieurs fois dans la décomposition (d'où la puissance).
Remarques :
- Lorsque $n = 0$, on obtient un produit vide qui vaut 1.
- On voit que les puissances α_k doivent être non nulles (sinon, on pourrait rajouter des facteurs premiers à la puissance 0, sans modifier la valeur du produit, ce qui contredirait l'unicité).
- 1 n'est pas un nombre premier (sinon, on n'aurait plus unicité de cette décomposition).
- il est évident qu'une telle décomposition n'est pas valable pour $a = 0$.

Preuve

L'existence se montre par récurrence forte, l'unicité par le lemme de Gauss.

- *Existence :*
  procédons par récurrence forte sur $a \geqslant 1$.
  Initialisation : la propriété est vraie au rang $a = 1$ avec un produit vide.
  Hérédité : soit $a \geqslant 2$.
  Si a est premier, alors la décomposition est immédiate.
  Sinon, on peut alors écrire a sous la forme $a = bc$, avec b et c deux entiers naturels non nuls et strictement inférieurs à a.
  Par hypothèse de récurrence, ils peuvent tous les deux être décomposés en produit de facteurs premiers, ce qui donne, par produit, une décomposition pour a.
- *Unicité :* supposons par l'absurde qu'il existe deux décompositions pour a sous la forme

$$a = \prod_{p \in \mathcal{P}} p^{\alpha_p} = \prod_{p \in \mathcal{P}} p^{\beta_p}.$$

Supposons qu'il existe $p_0 \in \mathcal{P}$ tel que $\alpha_{p_0} \neq \beta_{p_0}$.
Par exemple, on suppose $\alpha_{p_0} \geqslant \beta_{p_0} + 1$.
Alors en divisant de part et d'autre de l'égalité par $p_0^{\beta_{p_0}}$, on obtient

$$p_0^{\alpha_{p_0} - \beta_{p_0}} \prod_{p \in \mathcal{P} \setminus \{p_0\}} p^{\alpha_p} = \prod_{p \in \mathcal{P} \setminus \{p_0\}} p^{\beta_p}.$$

Ainsi $p_0 | \prod_{p \in \mathcal{P} \setminus \{p_0\}} p^{\beta_p}$, mais il est premier avec chacun des facteurs premiers du produit.
Par application successive du lemme de Gauss, $p_0 | 1$ ce qui est absurde.
Donc la décomposition est unique.

■

Remarque : Pour les entiers négatifs, ils suffit de mettre un facteur -1.

Exemple

Donner la décomposition en facteurs premiers de 1980.
Solution :
On factorise simplement par tous les facteurs auxquels on pense (que l'on décompose ensuite à leur tour) jusqu'à n'avoir que des nombres premiers $1980 = 10 \times 198 = 2 \times 5 \times 198 = 2 \times 5 \times 2 \times 99 = 2^2 \times 5 \times 9 \times 11 = 2^2 \times 5 \times 3^2 \times 11 = 2^2 \times 3^2 \times 5 \times 11$.

Notation

Pour A un ensemble contenant 0 et I un ensemble d'indices (a priori infini), On note $A^{(I)}$ l'ensemble des familles d'éléments de A indicées par I et *presque nulles*, c'est-à-dire telles qu'il n'existe qu'un nombre **fini** d'éléments non nuls.

Exemple

$\mathbf{R}^{(\mathbf{N})}$ désigne l'ensemble des suites stationnaires à 0.

Théorème 4.7 *(Autre formlation)*

Pour tout $n \in \mathbf{N}^*$, il existe un unique $(\alpha_p)_{p \in \mathcal{P}} \in \mathbf{N}^{(\mathcal{P})}$ tel que

$$n = \prod_{p \in \mathcal{P}} p^{\alpha_p}.$$

En d'autres termes

$$\varphi : \left\{ \begin{array}{ccc} \mathbf{N}^{(\mathcal{P})} & \to & \mathbf{N}^* \\ \alpha & \mapsto & \prod_{p \in \mathcal{P}} p^{\alpha_p} \end{array} \right.$$

est une bijection.

Définition 4.8 *(Valuation p−adique)*

Soit $n \in \mathbf{N}^*$, il existe une unique famille $(v_p(n))_{p\in\mathcal{P}}$, à termes presque tous nuls (seul un nombre fini d'entre eux est non nul) telle que

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

$v_p(n)$ s'appelle la **valuation p-adique** de n.
Pour tout $p \in \mathcal{P}$, $v_p(n)$ est l'élément d'indice p de $\varphi^{-1}(n)$ avec la notation du théorème précédent.

Remarque : L'existence et l'unicité de la famille provient du théorème fondamental de l'arithmétique.

Exemple

Donner les valuations 2, 3, 5-adiques de 12.
Solution :
$12 = 2^2 \times 3$, donc la valuation 2-adique de 12 est 2, la valuation 3-adique est 1 et la valuation 5-adique est 0.

Théorème 4.9 *(Propriétés de la valuation p-adique)*

Soient $(a, b) \in (\mathbf{N}^*)^2$, $p \in \mathcal{P}$.

1. $v_p(ab) = v_p(a) + v_p(b)$.
2. $a|b \iff \forall p \in \mathcal{P},\ v_p(a) \leqslant v_p(b)$.
3. $v_p(a \wedge b) = \min(v_p(a), v_p(b))$.
4. $v_p(a \vee b) = \max(v_p(a), v_p(b))$.

Preuve

Immédiat en décomposant a et b en produit de nombres premiers. ■

Exemple

Calculer $84 \vee 18$ et $84 \wedge 18$ en utilisant leurs décompositions en facteurs premiers.

Solution :
On pourrait bien sûr appliquer l'algorithme d'Euclide pour trouver le PGCD puis utiliser la relation $(a \wedge b) \times (a \vee b) = ab$ pour en déduire le PPCM.
Mais nous disposons à présent d'une autre méthode (pas nécessairement plus efficace, en particulier quand les nombres sont grands) que nous allons utiliser ici.
$84 = 2 \times 42 = 2^2 \times 21 = 2^2 \times 3 \times 7$ et $18 = 2 \times 9 = 2 \times 3^2$.
Ainsi, pour trouver le PGCD on ne conserve que les facteurs premiers communs (avec la plus grande puissance possible).

$$84 \wedge 18 = 2 \times 3 = 6.$$

Pour le PPCM, on part d'une des deux décompositions et on « ajoute » les facteurs manquants dans l'autre décomposition.
Par exemple, on a $84 = 2^2 \times 3 \times 7$, mais pour 18, il faut un 3^2 dans la décomposition, on obtient donc

$$84 \vee 18 = 2^2 \times 3^2 \times 7 = 84 \times 3 = 252.$$

On remarque bien que

$$(84 \wedge 18) \times (84 \vee 18) = 2 \times 3 \times 2^2 \times 3^2 \times 7 = 2^2 \times 3 \times 7 \times 2 \times 3^2 = 84 \times 18.$$

Exemple

Trouver tous les diviseurs positifs de 28.
Solution :
$28 = 4 \times 7 = 2^2 \times 7$.
Les diviseurs positifs sont donc 1, 2, 2^2, 7, 2×7, $2^2 \times 7$.

Corollaire 4.10

Si $a = \prod_{k=1}^{n} p_k^{\alpha_k}$ (avec les p_k premiers, et α_k entiers naturels non nuls), alors les diviseurs entiers naturels de a forment l'ensemble

$$\left\{ \prod_{k=1}^{n} p_k^{\beta_k},\ \forall k \in [\![1, n]\!],\ 0 \leqslant \beta_k \leqslant \alpha_k \right\}.$$

Remarque : Pour « éliminer » un facteur premier, on prend $\beta_k = 0$.

Propriété 4.11

$\forall (a, b) \in (\mathbf{N}^*)^2$,

$$a \wedge b = 1 \iff (\forall p \in \mathcal{P},\ v_p(a)v_p(b) = 0).$$

En d'autres termes, si une des valuations p-adique est non nulle, alors l'autre doit l'être, sinon, cela forme un diviseur commun.

Théorème 4.12 *(Écriture d'un nombre rationnel)*

Tout nombre rationnel $a \in \mathbf{Q}$, s'écrit de manière unique sous la forme $a = \frac{p}{q}$ avec $p \in \mathbf{Z}$, $q \in \mathbf{N}^*$ et $p \wedge q = 1$.

Explications

C'est ce que l'on vous a appris à faire dès le collège : simplifier un quotient jusqu'à obtenir une fraction irréductible, c'est-à-dire telle que le numérateur et le dénominateur soient premiers entre eux. S'ils ne sont pas premiers entre eux, alors on peut simplifier par un facteur commun.
p est un entier relatif pour « porter le signe » de a, et bien sûr, $q \neq 0$ (on n'autorise pas $q < 0$ pour garder l'unicité de l'écriture).

Preuve

Existence : Pour $a \geqslant 0$, par définition, un nombre rationnel s'écrit comme un quotient donc il existe $(p, q) \in (\mathbf{N}^*)^2$ tel que $a = \frac{p}{q}$.
On pose alors $p' = \frac{p}{p \wedge q}$ et $q' = \frac{q}{p \wedge q}$.
Alors on a évidemment $a = \frac{p'}{q'}$ avec $(p, q) \in (\mathbf{N}^*)^2$.
Et par homogénéité du PGCD (ou d'après la propriété 3.9), on obtient $p' \wedge q' = 1$.
Si $a < 0$, alors il suffit de multiplier p' par -1.
Unicité : Si $a = \frac{p}{q} = \frac{p'}{q'}$.
Alors $pq' = p'q$, donc $q'|p'q$, or par hypothèse $p' \wedge q' = 1$ donc d'après le lemme de Gauss, $q'|q$.
Par symétrie, on a aussi, $q|q'$ et par antisymétrie de la relation de divisibilité sur $\mathbf{N}$, $q = q'$.
Donc on a également $p = p'$. ■

5 Généralisation à plusieurs entiers entre eux

On étend les définitions vues pour deux entiers relatifs à un plus grand nombre.

Définition 5.1

Soit $(a_1, \cdots, a_n) \in \mathbf{Z}^n$.

1. d est un diviseur commun à $a_1, \cdots, a_n$ s'il divise à la fois $a_1, a_2, \cdots a_n$.
2. m est un multiple commun à $a_1, \cdots, a_n$ s'il est multiple à la fois de $a_1, a_2, \cdots a_n$.
3. Le PGCD de $(a_1, a_2, \cdots, a_n)$ – non tous nuls – est leur plus grand diviseur commun.
   Il se note $a_1 \wedge a_2 \wedge \cdots \wedge a_n = \bigwedge_{i=1}^{n} a_i$.
4. Le PPCM de $(a_1, a_2, \cdots, a_n)$ – tous non nuls – est leur plus petit multiple commun positif.
   Il se note $a_1 \vee a_2 \vee \cdots \vee a_n = \bigvee_{i=1}^{n} a_i$.

Explications

La relation de divisibilité est une relation d'ordre sur $\mathbf{N}$.

- un diviseur commun positif à $a_1, \cdots, a_n$ est un minorant dans $\mathbf{N}$ de $\{a_1, \cdots, a_n\}$ pour la relation d'ordre $|$.
  Cet ensemble des minorants admet un plus grand élément que l'on nomme son PGCD.
- un multiple commun positif à $a_1, \cdots, a_n$ est un majorant dans $\mathbf{N}$ de $\{a_1, \cdots, a_n\}$ pour la relation d'ordre $|$.
  Cet ensemble des majorants admet un plus petit élément que l'on nomme son PPCM.

Preuve

La preuve de l'existence du PGCD et du PPCM est la même que celle pour deux réalisée plus haut. ■

Propriété 5.2 *(valuations p-adiques du PGCD et du PPCM)*

Pour $(a_1, a_2, \cdots, a_n) \in \mathbf{N}^n$ tous non nuls,
$\forall p \in \mathcal{P}$,

$$v_p\left(\bigwedge_{i=1}^{n} a_i\right) = \min\left\{v_p(a_i),\, i \in [\![1, n]\!]\right\}.$$

$$v_p\left(\bigvee_{i=1}^{n} a_i\right) = \max\left\{v_p(a_i),\, i \in [\![1, n]\!]\right\}.$$

Preuve

- Pour le PGCD.
  On pose $d = \prod_{p \in \mathcal{P}} p^{\min\left\{v_p(a_i),\, i \in [\![1, n]\!]\right\}}$.
  On voit donc que $\forall j \in [\![1, n]\!]$, $d|a_i$ (car ses valuations $p-$adiques sont inférieures).
  De plus si δ est un diviseur commun dans $\mathbf{N}^*$, alors $\forall p \in \mathcal{P}$, $\forall i \in [\![1, n]\!]$, $v_p(\sigma) \leqslant v_p(a_i)$ car c'est un diviseur de a_i.
  Ainsi $v_p(\delta) \leqslant \min\left\{v_p(a_i),\, i \in [\![1, n]\!]\right\}$.
  On obtient alors que $\delta \leqslant d$ ce qui prouve bien que d est le plus grand diviseur commun (et aussi que tout autre diviseur commun est un diviseur de d).
- Pour le PPCM.
  On fait de même (en exercice).

■

Propriété 5.3 *(Associativité)*

$\wedge$ et $\vee$ sont associatives :

$$\forall (a, b, c) \in \mathbf{Z}^3,\ (a \wedge b) \wedge c = a \wedge (b \wedge c) = a \wedge b \wedge c.$$

$$\forall (a, b, c) \in \mathbf{Z}^3,\ (a \vee b) \vee c = a \vee (b \vee c) = a \vee b \vee c.$$

Preuve

Avec les caractérisations à partir des valuations p-adiques, on remarque simplement que $\forall (\alpha, \beta, \delta) \in \mathbf{N}^3$, $\min(\min(\alpha, \beta), \delta) = \min(\alpha, \min(\beta, \delta))$ et de même pour le maximum.
On applique ensuite aux valuations $p-$adiques (les PGCD et PPCM sont invariant par changement de signe, donc on peut travailler avec les valeurs absolues des a_i).
Pour le PGCD, on traite à part le cas où l'un est nul (immédiat) car alors ses valuations p-adiques ne sont pas définies. ■

Exemple

Calculer $12 \wedge 42 \wedge 15$.

Solution :

En utilisant l'associativité, on peut calculer $12 \wedge 42$ puis $(12 \wedge 42) \wedge 15$.
Si on applique l'algorithme d'Euclide à 12 et 42, on trouve $42 = 12 \times 3 + 6$, puis $12 = 6 \times 2 + 0$.
Donc $12 \wedge 42 = 6$.
Ensuite pour $6 \wedge 15$: $15 = 6 \times 2 + 3$, et $6 = 3 \times 2 + 0$, donc $6 \wedge 15 = 3$.
Ainsi $12 \wedge 42 \wedge 15 = 3$.
Autre méthode : on peut aussi décomposer les trois nombres en facteurs premiers puis ne garder que ceux qui sont communs.
$12 = 2^2 \times 3$, $42 = 2 \times 21 = 2 \times 3 \times 7$ et $15 = 3 \times 5$.
Donc on remarque un seul facteur commun : 3.
$12 \wedge 42 \wedge 15 = 3$.

Théorème 5.4 *(Relation de Bézout)*

Soit $(a_1, a_2, \cdots, a_n) \in \mathbf{Z}^n$, non tous nuls.

$\exists (u_1, u_2, \cdots, u_n) \in \mathbf{Z}^n$, tel que $a_1u_1 + a_2u_2 + \cdots + a_nu_n = a_1 \wedge a_2 \wedge \cdots \wedge a_n$.

Preuve

Preuve par récurrence sur $n \in \mathbf{N}$

Pour $n = 0$ ou $n = 1$, la relation a peu d'intérêt.
Pour $n = 2$, elle a été montrée plus haut avec l'algorithme d'Euclide étendu.
Hérédité : supposons qu'on l'ai démontré pour un $n-$uplet.
On considère alors un $(n+1)$-uplet de $\mathbf{Z}^n$: $(a_1, \cdots, a_n, a_{n+1})$.
Par associativité, on sait que $\bigwedge_{i=1}^{n+1} a_i = \left(\bigwedge_{i=1}^{n} a_i\right) \wedge a_{n+1}$.
D'après le cas $n = 2$ montré à part, il existe donc (v, u_{n+1}) dans $\mathbf{Z}^2$ tel que

$$\left(\bigwedge_{i=1}^{n} a_i\right) v + a_{n+1}u_{n+1} = \bigwedge_{i=1}^{n+1} a_i.$$

En appliquant l'hypothèse de récurrence à $(a_1, \cdots, a_n)$, on a l'existence de $(v_1, \cdots v_n) \in \mathbf{Z}^n$ tel que $\bigwedge_{i=1}^{n} a_i = \sum_{i=1}^{n} a_i v_i$.
Alors, en notant pour tout $i \in [\![1, n]\!]$, $u_i = v \times v_i$, on trouve

$$\bigwedge_{i=1}^{n+1} a_i = \sum_{i=1}^{n+1} a_i u_i.$$

Autre preuve plus algébrique :

On note $E = a_1\mathbf{Z} + a_2\mathbf{Z} + \cdots + a_n\mathbf{Z}$ l'ensemble des nombres qui s'écrivent sous la forme $a_1u_1 + a_2u_2 + \cdots + a_nu_n$, avec $(u_1, u_2, \cdots, u_n) \in \mathbf{Z}^n$.
On cherche donc à montrer que $\bigwedge_{i=1}^{n} a_i \in E \cap \mathbf{N}^*$.
$E \cap \mathbf{N}^*$ est une partie non vide de $\mathbf{N}$ et elle admet donc un plus petit élément que l'on note d.
Montrons que $d = \bigwedge_{i=1}^{n} a_i$.
On remarque tout d'abord que $\bigwedge_{i=1}^{n} a_i | d$ car il divise chacun des a_i.
Montrons réciproquement que d divise tous les a_i, donc leur PGCD.
Pour cela, si on note la division euclidienne $a_i = dq_i + r_i$.
alors $r_i = a_i - dq_i \in E \cap \mathbf{N}$, donc par minimalité de d, $r_i = 0$.
Ce qui permet de conclure : $\forall i \in [\![1, n]\!]$, $d|a_i$, donc $d| \bigwedge_{i=1}^{n} a_i$. Or on a aussi montré que $\bigwedge_{i=1}^{n} a_i | d$, ainsi, par antisymétrique de la relation de divisibilité sur $\mathbf{N}$, $d = \bigwedge_{i=1}^{n} a_i$.
Or, $d = \min(E \cap \mathbf{N}^*)$, et en particulier $d \in E$.
Ce qui prouve l'existence de $u_1, u_2, \cdots, u_n \in \mathbf{Z}^n$ tel que $\bigwedge_{i=1}^{n} a_i = \sum_{i=1}^{n} a_i u_i$.

En fait, on définit souvent le PGCD *à partir de l'ensemble E.*
On peut définir de même le PPCM *comme le plus petit élément de $(a_1\mathbf{Z} \cap a_2\mathbf{Z} \cap \cdots \cap a_n\mathbf{Z}) \cap \mathbf{N}^*$. C'est beaucoup plus simple que pour le* PGCD.
■

Propriété 5.5 *(Homogénéité du* PGCD *et du* PPCM*)*

Si $(a_1, \cdots, a_n)$ sont des entiers non tous nuls, alors

$$\forall k \in \mathbf{Z}^*, \quad \bigwedge_{i=1}^{n} (ka_i) = |k| \bigwedge_{i=1}^{n} a_i \quad \text{et} \quad \bigvee_{i=1}^{n} (ka_i) = |k| \bigvee_{i=1}^{n} a_i.$$

Preuve

Par récurrence en utilisant l'associativité. ■

Définition 5.6 *(Entiers premiers deux à deux ou dans leur ensemble)*

Soit $(a_1, a_2, \cdots, a_n) \in \mathbf{Z}^n$.

1. Les entiers sont **premiers entre eux deux à deux** si
$$\forall (i, j) \in [\![1, n]\!]^2, \quad i \neq j \Rightarrow a_i \wedge a_j = 1.$$
2. Les entiers sont **premiers entre eux dans leur ensemble** si
$$\bigwedge_{i=1}^{n} a_i = 1.$$

Explications

La notion d'entiers premiers deux à deux est simple à comprendre : dès que l'on prend deux entiers parmi les n, alors ils sont entiers entre eux.
La notion « premiers dans leur ensemble » est beaucoup plus faible. Elle dit simplement qu'ils n'ont pas de diviseur *commun à tous*, autre que 1 et -1. Mais rien n'empêche que deux d'entre eux ne soient pas premiers entre eux. On a immédiatement

premiers entre eux deux à deux $\Rightarrow$ premiers entre eux dans leur ensemble.

Mais la réciproque est fausse.

Exemple

Si la famille contient 1 ou -1, alors les entiers sont premiers dans leur ensemble (mais pas nécessairement deux à deux).
Par exemple $(1, 6, 9)$: $1 \wedge 6 \wedge 9 = 1$, mais $6 \wedge 9 = 3$.

Exemple

1. Trouver trois entiers premiers entre eux deux à deux.
2. Trouver trois entiers premiers entre eux dans leur ensemble, mais tels qu'aucun des trois ne soit premier avec un autre.

Solution :

1. Par exemple $(2, 5, 7)$: s'ils sont premiers distincts, ils sont a fortiori premiers deux à deux. Mais on peut aussi prendre $(2, 9, 35)$ ou encore beaucoup d'autres exemples.
2. Par exemple $(6, 14, 21)$.
   Pour trouver cet exemple, on s'est appuyé sur la décomposition en nombres premiers de telle sorte que chaque nombre ait au moins un facteur en commun avec un autre, mais qu'il n'y ait aucun facteur commun aux trois.

Propriété 5.7

Soient $n \in \mathbf{Z}$ et $(a_1, a_2, \cdots, a_k) \in \mathbf{Z}^k$.

1. Si pour tout $i \in [\![1, k]\!]$, $a_i \wedge n = 1$, alors $a_1 a_2 \cdots a_k \wedge n = 1$.
2. Si $\forall i \in [\![1, k]\!]$, $a_i | n$, et si les a_i sont premiers entre eux **deux à deux**, alors $a_1 a_2 \cdots a_k | n$.

Preuve

On travaille avec les valeurs absolues des nombres (car les propriétés sont invariantes par changement de signe), ce qui permet d'utiliser les valuations p-adiques.

1. S'il existe $i \in [\![1, k]\!]$ tel que $a_i = 0$, alors le résultat est immédiat car on obtient $n = 1$.
   Sinon, on considère $p \in \mathcal{P}$. $\forall i \in [\![1, k]\!]$, $v_p(a_i)v_p(n) = 0$ car $a_i \wedge n = 1$.
   Donc $\sum_{i=1}^{k} v_p(a_i)v_p(n) = 0$, ce qui donne

$$v_p\left(\prod_{i=1}^{k} a_i\right) v_p(n) = \left(\sum_{i=1}^{k} v_p(a_i)\right) v_p(n) = \sum_{i=1}^{k} v_p(a_i)v_p(n) = 0.$$

   Donc $(a_1 a_2 \cdots a_k) \wedge n = 1$.
2. Si l'un des a_i est nul, alors $n = 0$, donc la propriété est évidente.
   Sinon, on sait que pour tout $p \in \mathcal{P}$, $\forall i \in [\![1, k]\!]$ $v_p(a_i) \leqslant v_p(k)$.
   Or, les a_i sont premiers deux à deux entre eux, donc il existe au plus une valeur non nulle parmi $v_p(a_1), v_p(a_2), \cdots, v_p(a_k)$ (sinon, les deux en question ne seraient pas premiers entre eux).
   Ainsi, $\sum_{k=1}^{k} v_p(a_i) = \max\{v_p(a_i),\ i \in [\![1, k]\!]\} \leqslant v_p(n)$.
   Ce qui prouve que $a_1 a_2 \cdots a_k | n$.

■

6 Relation de congruence

Définition 6.1 *(Congruence modulo n)*

Soient $n \in \mathbf{N}^*$, $(a, b) \in \mathbf{Z}^2$.
On dit que a est **congru** à b modulo n si il existe $k \in \mathbf{Z}$ tel que $a = b + kn$.
On note $a \equiv b\ [n]$.
Autrement dit :

$$a \equiv b\ [n] \iff a - b \in n\mathbf{Z}.$$

Remarque : $a - b \in n\mathbf{Z}$ peut aussi s'écrire : $n|(a - b)$ ce qui nous amène à la propriété suivante :

Propriété 6.2

Soient $n \in \mathbf{N}^*$, $(a, b) \in \mathbf{Z}^2$.
$a \equiv b\ [n]$ si, et seulement si a et b ont le **même reste** dans la division par n.

En particulier, a est congru à son reste par la division euclidienne.

Plus généralement,

$$a \equiv b\ [n] \iff \exists (k, k') \in \mathbf{Z}^2,\ r \in \mathbf{Z},\ \text{ tel que } a = kn + r \text{ et } b = k'n + r.$$

Preuve

Caractérisation avec le reste de la division euclidienne :
On note $a = nq + r$ et $b = nq' + r'$.

$$a \equiv b\ [n] \iff a - b \in n\mathbf{Z} \iff n(q - q') + r - r' \in n\mathbf{Z} \iff r - r' \in n\mathbf{Z}.$$

Or $r - r' \in [\![-n + 1, n - 1]\!]$, donc la seule possibilité est $r - r' = 0$.
Cas général :
Le sens direct est immédiat en prenant la division euclidienne : a et b ont le même reste.
Le sens réciproque n'est pas plus dur : $a - b = n(k - k') \in n\mathbf{Z}$. ■

Exemple

Dire à chaque fois si les nombres a et b sont congrus modulo n.

1. $a = 5$, $b = 12$, $n = 3$.
2. $a = 5$, $b = 12$, $n = 7$.
3. $a = -5$, $b = 2$, $n = 7$.

Solution :

1. $5 = 3+2$ et $12 = 3\times 4$, donc les restes par la division euclidienne par 3 sont différents : $5 \not\equiv 12$ [3].
2. $5 = 7-2$ et $12 = 7\times 2 - 2$ ce qui permet de voir que $5 \equiv 12$ [7].
   Certes, -2 n'est pas le reste de la division euclidienne, mais le fait d'avoir la même valeur montre que si on soustrait les deux, le résultat est bien un multiple de 7.
3. $-5 = -7+2$ et $2 = 0\times 7 + 2$, donc $-5 \equiv 2$ [7].

Exemple

Caractériser tous entiers $a \equiv 0$ $[n]$.

Solution :

$a \equiv 0$ $[n]$ si, et seulement si le reste de la division euclidienne de a par n est 0, c'est-à-dire si, et seulement si $n|a$.
Les solutions forment l'ensemble des multiples de n : $n\mathbf{Z}$.

Exemple *(Informatique)*

Réaliser un modulo 2^n en informatique revient à ne conserver que les n bits de poids faibles.
L'opération est donc très simple réaliser.

Théorème 6.3

$\equiv$ $[n]$ forme une relation d'équivalence sur $\mathbf{Z}$.

Preuve

1. *reflexivité* évidente $\forall a \in \mathbf{Z}$, $a - a = 0 \in n\mathbf{Z}$.
2. *symétrie* évidente car si $a - b \in n\mathbf{Z}$, alors $b - a \in n\mathbf{Z}$ (le facteur multiplicatif de n est changé en son opposé).
3. *transitivité.*
   Si $a \equiv b$ $[n]$ et $b \equiv c$ $[n]$ alors, $a - c = a - b + b - c \in n\mathbf{Z} + n\mathbf{Z} = n\mathbf{Z}$.

■

L'idée des congruences modulo n est de *classer* les entiers selon leur divisibilité par n.
Deux entiers sont congrus lorsque le reste de leur division par n est le même.
Cette idée de classification nous conduit aux classes d'équivalence modulo n.
Une classe d'équivalence contient tous les éléments qui ont le même reste modulo n : la valeur de ce reste est donc ce qui décrit naturellement la classe.

Propriété 6.4 *(Classes d'équivalence)*

Les classes d'équivalence modulo n sont les ensembles :

$$r + n\mathbf{Z} \qquad \text{pour } r \in [\![0, n-1]\!].$$

Ainsi la relation contient exactement n classes d'équivalence distinctes.
La classe $r + n\mathbf{Z}$ est souvent notée $\overline{r}$ ou $\dot{r}$.

Exemple

Les classes d'équivalence modulo 3 sont exactement : $\overline{0}$, $\overline{1}$, $\overline{2}$.
$\overline{0}$ désigne l'ensemble de tous les entiers dont le reste de la division euclidienne par 3 est nul. Ce sont tous les multiples de 3.

$$\overline{0} = \{\cdots, -9, -6, -3, 0, 3, 6 \cdots\}.$$

$\overline{1} = \{\cdots -8, -5, -2, 1, 4, 7 \cdots\}$.
C'est l'ensemble $\overline{0}$ translaté de 1 pour que le reste de la division soit 1.
Enfin $\overline{2} = \{\cdots, -7; -4, -1, 2, 4, 8, \cdots\}$.
On voit que ces trois classes forment bien une partition de $\mathbf{Z}$.

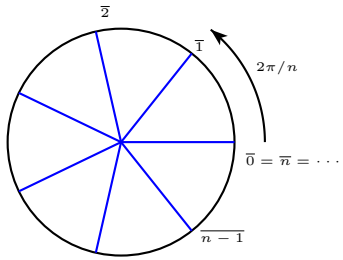
Chercher le reste de la division euclidienne de a par n revient à chercher le plus petit « représentant » positif de la classe de a modulo n.

Explications

Interprétation géométrique des nombres congrus entre eux.
Nous avons vu dans le chapitre sur les nombres complexes que les solutions complexes de $z^n = 1$ s'écrivent

$$\left\{ e^{2ik\frac{\pi}{n}},\ k \in \mathbf{Z}\right\} = \left\{\xi_1^k,\ k \in \mathbf{Z}\right\},$$

en notant $\xi_1 = e^{2i\frac{\pi}{n}}$.



Ces racines consistent à tourner le long du cercle trigonométrique en augmentant (ou diminuant) l'angle d'un nombre entier de fois $2\frac{\pi}{n}$.
On peut donc numéroter les points obtenus selon k et on voit que l'on retombe sur le même point tous les n.
Ainsi, 0, n, $2n$, $\cdots$ correspondent au même point, de même pour 1, $n+1$, $\cdots$
Ces points representent donc les classes d'équivalence modulo n : le point $\overline{k}$ contient toutes les valeurs $k + n\mathbf{Z}$, c'est-à-dire k et tous les autres points obtenus par l'ajout d'un ou plusieurs tours de cercle.
Chercher le reste d'un nombre revient à « supprimer » les tours de cercle complet, et deux nombres sont congrus, lorsqu'ils correspondent au même point.

Propriété 6.5 *(Compatibilité avec somme et produit)*

La relation de congruence est compatible avec la somme et le produit.

1. Si $a \equiv r_1$ $[n]$ et $b \equiv r_2$ $[n]$, alors $a + b \equiv r_1 + r_2$ $[n]$.
2. Si $a \equiv r_1$ $[n]$ et $b \equiv r_2$ $[n]$, alors $ab \equiv r_1 r_2$ $[n]$.
3. Si $a \equiv r_1$ $[n]$, et si $k \in \mathbf{N}$, alors $a^k \equiv r_1^k$ $[n]$.

Preuve

1. Si $a \equiv r_1$ $[n]$, alors il existe $k \in \mathbf{Z}$ tel que $a - r_1 = kn$.
   De même, si $b \equiv r_2$ $[n]$, alors il existe $k' \in \mathbf{Z}$ tel que $b - r_2 = k'n$.
   Donc $(a+b) - (r_1 + r_2) = (k + k')n \in n\mathbf{Z}$, donc $a + b \equiv r_1 + r_2$ $[n]$.

2. De même, on a $ab = (r_1 + kn)(r_2 + k'n) = r_1r_2 + n(kr_2 + k'r_1 + kk'n)$, d'où le résultat.
3. C'est un cas particulier du cas précédent (récurrence immédiate).

■

Exemple

Donner le reste de la division euclidienne de $2^{1239875}$ par 7.

Solution :

On remarque que $2^3 = 8$, donc $2^3 \equiv 1\ [7]$.
Ensuite, on réalise la division euclidienne de 1239875 par 3 et on trouve $1239875 = 413291 \times 3 + 2$ donc $2^{1239875} = \left(2^3\right)^{413291} \times 2^2 \equiv 1^{413291}2^2 \equiv 4\ [7]$.
Le reste de la division est donc 4.
Remarque : on peut même aller un peu plus vite.
On voit donc que $2^3 \equiv 1\ [7]$ et on s'intéresse donc au reste de 1239875 par 3. Plutôt que de faire la division euclidienne complète, on peut donc simplement travailler modulo 3, ce qui donne

$$\overline{\underbrace{12}\,39875} = \overline{\underbrace{039}\,875} = \overline{875} = \overline{5} = \overline{2}.$$

on trouve don bien $2^{1239875} \equiv 2^2 \equiv 4\ [7]$.

Exemple

Montrer que $\forall n \in \mathbf{N}$, $3^{n+3} - 4^{4n+2}$ est divisible par 11.

Solution :

$3^3 = 27 \equiv 5\ [11]$ et $4^2 = 16 \equiv 5\ [11]$ donc

$$3^{n+3} - 4^{4n+2} \equiv 5 \times 3^n - 5 \times 4^{4n} \equiv 5 \times \left(3^n - \left(4^4\right)^n\right)\ [11].$$

Or, $4^4 \equiv 16^2 \equiv 5^2 \equiv 3\ [11]$.
On obtient donc $3^{n+3} - 4^{4n+2} \equiv 5 \times (3^n - 3^n) \equiv 0\ [11]$.
Donc $11 | 3^{n+3} - 4^{4n+2}$.

Exemple *(Méthode)*

Trouver tous les entiers relatifs $n \in \mathbf{Z}$ tels que

$$\begin{cases} n \equiv 6\ [17] \\ n \equiv 4\ [15] \end{cases}$$

Solution :

1. On commence par chercher une solution particulière.
   Pour cela on dispose de différentes méthodes.
   - *Avec Bézout :*

$$\begin{aligned} x \text{ solution} &\iff \exists (k,k') \in \mathbf{Z}^2, \begin{cases} x &= 6 + 17k \\ x &= 4 + 15k' \end{cases} \\ &\iff \exists (k,k') \in \mathbf{Z}^2, \begin{cases} x &= 4 + 15k' \\ 6 + 17k &= 4 + 15k' \end{cases} \\ &\iff \exists (k,k') \in \mathbf{Z}^2, \begin{cases} x &= 4 + 15k' \\ -17k + 15k' &= 2. \end{cases} \end{aligned}$$

On cherche un couple (k, k') qui convient grâce à Bézout.
Pour cela on commence par chercher une relation de Bézout avec le PGCD. On applique l'algorithme d'Euclide :
$17 = 15 + 2$ et $15 = 7 \times 2 + 1$,
donc $1 = 15 - 7 \times 2 = 15 - 7 \times (17 - 15) = 8 \times 15 - 7 \times 17$.
On trouve donc la relation de Bézout :

$$17 \times (-7) + 15 \times 8 = 1.$$

On multiplie par 2 pour avoir (k, k') :

$$17 \times (-14) + 15 \times 16 = 2,$$

donc $(k, k') = (14, 16)$ convient La solution la plus simple s'obtient avec

$$n_0 = 15 \times k' + 4 = 244.$$

- *Idem en plus rapide :*
  $15 \wedge 17 = 1$ et on cherche une relation de Bézout.
  $17 = 15 + 2$ et $15 = 7 \times 2 + 1$ ce qui donne

$$1 = 15 - 7 \times 2 = 15 - 7 \times (17 - 15) = 8 \times 15 - 7 \times 17.$$

$$8 \times 15 - 7 \times 17 = 1.$$

  - *Modulo* 17
    $8 \times 15 \equiv 8 \times 15 - 7 \times 17 \equiv 1$.
    Donc en multipliant par 6 : $6 \times 8 \times 15 \equiv 6$.
  - *Modulo* 15
    $-7 \times 17 \equiv 8 \times 15 - 7 \times 17 \equiv 1$.
    Donc en multipliant par 4 : $4 \times (-7) \times 17 \equiv 4$.

  On fait la somme

$$n_0 = 6 \times 8 \times 15 - 4 \times 7 \times 17 = 244.$$

- Ici, on peut aller plus vite :
  on remarque que $17 - 15 = 2$,
  - *Modulo* 17
    $(-1) \times 15 \equiv 17 - 15 \equiv 2$.
    Donc en multipliant par 3 : $(-3) \times 15 \equiv 6$.
  - *Modulo* 15
    $17 \equiv 17 - 15 \equiv 2$.
    Donc en multipliant par 2 : $2 \times 17 \equiv 4$.

  On obtient par somme

$$n_0 = -3 \times 15 + 2 \times 17 \times 2 = -11.$$

- Par l'intuitition : si on y arrive, ça peut réduire les calculs.
  $n \equiv 6 - 17 \equiv -11\ [17]$ et $n \equiv 4 - 15 \equiv -11\ [15]$ donc $n_0 = -11$ convient.

2. On recherche ensuite les solutions générales.
   n est une solution si, et seulement si $\begin{cases} n - n_0 \equiv 0\ [17] \\ n - n_0 \equiv 0\ [15] \end{cases}$,
   ce qui revient à $17|n - n_0$ et $15|n - n_0$.
   Or $15 \wedge 17 = 1$ donc $15 \times 17 | n - n_0$ et il existe $k \in \mathbf{Z}$ tel que $n - n_0 = 15 \times 17k = 255k$.
   La réciproque est évidente

On en conclut que les solutions sont $\{n_0 + 255k,\ k \in \mathbf{Z}\}$.
On remarque bien que -11+255 = 244.

Propriété 6.6

Si $a \equiv b\ [n]$ et $m \in \mathbf{N}^*$, alors $ma \equiv mb\ [mn]$.

Mais on a également $ma \equiv mb\ [n]$ d'après la propriété précédente.

Preuve

Trivial : $n|a - b \Rightarrow mn|ma - mb$. ■

Définition 6.7 *(Inverse modulo n)*

On dit qu'un entier k admet un **inverse** modulo n, s'il existe k' tel que $kk' \equiv 1\ [n]$.

Propriété 6.8

Soit $n \geqslant 1$.
k est inversible modulo n si, et seulement si $k \wedge n = 1$.

Preuve

$kk' \equiv 1\ [n] \iff \exists u \in \mathbf{Z},\ kk' + un = 1$.
D'après le théorème de Bézout, les inversibles sont exactement les entiers premiers avec n. ■

Exemple

Résoudre $4x \equiv 5\ [9]$.
Solution :
Méthode 1 : on remarque que $4 \wedge 9 = 1$, donc 4 est inversible modulo 9.
Immédiatement, on voit que $9 = 4 \times 2 + 1$, donc $4 \times (-2) \equiv 1\ [9]$: donc -2 est un inverse de 4 modulo 9.
On a donc

$$4x \equiv 5\ [9] \iff x \equiv -10\ [9].$$

La multiplication par un inversible permet de garder l'équivalence.
Or $-10 \equiv -1\ [9]$, donc l'équation s'écrit $x \equiv -1\ [9]$, ainsi les solutions sont

$$\{-1 + 9k,\ k \in \mathbf{Z}\}.$$

Méthode 2 : Comme il n'y a que 9 valeurs modulo 9, on peut se permettre de toutes les tester.

x	0	1	2	3	4	5	6	7	8
$4x$	0	4	8	3	7	2	6	1	5

Ainsi l'ensemble des solutions est

$$\{8 + 9k,\ k \in \mathbf{Z}\}.$$

Théorème 6.9 *(Petit théorème de Fermat)*

Soit $p \in \mathcal{P}$, $a \in \mathbf{Z}$,

$$a^p \equiv a\ [p],$$

et si a n'est pas divisible par p, alors $a^{p-1} \equiv 1\ [p]$.

Remarque : Ce théorème n'est pas à confondre avec le grand théorème de Fermat qui dit que pour tout $n \geqslant 3$, il n'existe aucune solution non triviale dans $\mathbf{N}$ à l'équation $x^n + y^n = z^n$.

Preuve

- Commençons par traiter le cas $a \geqslant 0$, par récurrence.
  Initialisaton : pour $a = 0$, comme $p \geqslant 2$ on a $a^p = 0 \equiv 0\ [p]$.
  Hérédité : supposons la relation vraie au rang $a \geqslant 0$ et montrons là au rang $a + 1$.
  D'après le binôme de Newton :

$$(a+1)^p = \sum_{k=0}^{p} \binom{p}{k} a^k = a^p + 1 + \sum_{k=1}^{p-1} \binom{p}{k} a^k.$$

  Montrons à présent que $\forall k \in [\![1, p-1]\!],\ p|\binom{p}{k}$.
  On sait que $k \geqslant 1$ et $p \geqslant 2$, donc $k\binom{p}{k} = p\binom{p-1}{k-1}$.
  Ainsi $p|k\binom{p}{k}$, or, $k \in [\![1, p-1]\!]$ et p premier, donc $p \wedge k = 1$,
  le lemme de Gauss donne alors $p|\binom{p}{k}$.
  Ainsi, en passant aux congruences et avec l'hypthèse de récurrence :

$$(a+1)^p \equiv a^p + 1 + \sum_{k=1}^{p-1} 0 \times a^k \equiv a + 1\ [p].$$

- Pour $a < 0$, $-a > 0$ donc $(-a)^p \equiv -a\ [p]$, donc $(-1)^{p-1} a^p \equiv a\ [p]$.
  Si $p = 2$, alors $(-1)^{p-1} = -1 \equiv 1\ [p]$ et si $p \geqslant 3$, alors p est impair et donc $(-1)^{p-1} = 1$.
- À présent, si $p \not| a$, alors $a \wedge p = 1$.
  Or, $p|(a^p - a) = a\left(a^{p-1} - 1\right)$ et par application du lemme de Gauss, $p|a^{p-1} - 1$, donc $a^{p-1} \equiv 1\ [p]$.

■