Chapitre 12

Arithmétique dans $\mathbb{Z}$

Compétences attendues.

- ✓ Maitriser la notion de divisibilité et les écritures en termes de congruences.
- ✓ Calculer un PGCD, un PPCM, une relation de Bezout à l'aide de l'algorithme d'Euclide étendu.
- ✓ Exploiter la décomposition en facteurs premiers.

Mathieu Mansuy - Professeur en MP2I au Lycée Carnot (Dijon)
Page personnelle : `mathieu-mansuy.fr/`
E-mail : `mathieu.mansuy@ac-dijon.fr`

1 Relation de divisibilité

1.1 Diviseurs et multiples

Définition.

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

Notation.

Pour tout entier $b \in \mathbb{Z}$, on notera $\mathscr{D}(b)$ l'ensemble des diviseurs de b.
Pour tout entier $a \in \mathbb{Z}$, les multiples de a sont les éléments de $a\mathbb{Z} = \{ak,\ k \in \mathbb{Z}\}$.

Exemples.

- $\mathscr{D}(12) = \{1,-1,2,-2,3,-3,4,-4,6,-6,12,-12\}$, $\mathscr{D}(11) = \{1,-1,11,-11\}$.
- $0\mathbb{Z} = \{0\}$ et $\mathscr{D}(0) = \mathbb{Z}$, $(\pm 1)\mathbb{Z} = \mathbb{Z}$ et $\mathscr{D}(\pm 1) = \{-1,1\}$.

Propriété 1 ( )

Soient $a,b \in \mathbb{Z}$. Alors $a \mid b$ si, et seulement si, $b\mathbb{Z} \subset a\mathbb{Z}$.

Propriété 2 (Relation de divisibilité et relation d'ordre -)

- La relation de divisibilité est une relation d'ordre sur $\mathbb{N}$.
- La relation de divisibilité est réflexive et transitive sur $\mathbb{Z}$, mais pas antisymétrique :

$$\forall (a,b) \in \mathbb{Z},\quad a \mid b \text{ et } b \mid a \ \Leftrightarrow\ a\mathbb{Z} = b\mathbb{Z} \ \Leftrightarrow\ |a| = |b|.$$

Deux entiers a et b vérifiant l'une de ces propriétés équivalentes sont dits *associés*.

Propriété 3 (Divisibilité et opérations -)

Soient a,b,c,d des entiers.

(1) Si $a \mid b$ et $a \mid c$, alors $a \mid bu + cv$ pour tout $(u,v) \in \mathbb{Z}^2$.

(2) Si $a \mid b$ et $c \mid d$, alors $ac \mid bd$, et en particulier $a^k \mid b^k$ pour tout $k \in \mathbb{N}$.

(3) Si $ab \mid c$, alors $a \mid c$ et $b \mid c$.

Danger.

La réciproque du dernier point est fausse : 6 et 4 divisent 12, mais $24 = 6 \times 4$ ne divise pas 12.

Exercice 1 Montrer que pour tout entier naturel n, $2^{3n}-1$ est multiple de 7.

Exercice 2 Soit $(n,k)\in\mathbb{N}\times\mathbb{N}^*$. Montrer que k divise $n(n+1)(n+2)\dots(n+k-1)$.
Ainsi, le produit de k entiers consécutifs est toujours divisible par k.

1.2 Calcul modulaire

Soit $n\in\mathbb{N}^*$. On dispose d'une relation d'équivalence sur $\mathbb{Z}$ qui est la relation de congruence modulo n :

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

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

Propriété 4 (Propriété du calcul modulaire - ✎)

Soit $n\in\mathbf{N}^*$, et soient a,b,c,d des entiers.

(1) Si $a\equiv b\,[n]$ et $c\equiv d\,[n]$, alors $a+c\equiv b+d\,[n]$.

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

(3) Pour $m\in\mathbb{N}^*$, on a : $\quad a\equiv b\,[n] \;\Leftrightarrow\; am\equiv bm\,[mn]$.

Exercice 3 Montrer que $36^{2024}-13^{2024}$ est divisible par 7.

Exercice 4 On considère un entier naturel n dont l'écriture décimale est $n=\overline{a_p\dots a_1a_0}$, de sorte que :

$$n=a_p10^p+\dots+a_110^1+a_010^0.$$

Déterminer un critère de divisibilité de n par 3, par 9 et par 11.

1.3 Division euclidienne

Théorème 5 (✎)

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

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

On dit que q est le *quotient* et r le *reste* de la *division euclidienne de a par b*.

Remarque. Il est facile de constater que $q=\left\lfloor\frac{a}{b}\right\rfloor$. Par ailleurs, $a\equiv r\,[b]$.

Mise en garde.

Attention aux nombres négatifs ! Par exemple, la division euclidienne de 131 par 7 est $131=18\times7+5$. D'où $-131=(-18)\times7-5$, qui n'est pas la division euclidienne de -131 par 7 puisque $-5\notin[\![0,6]\!]$. La division euclidienne de -131 par 7 est $-131=(-19)\times7+2$.

Algorithme de division euclidienne dans $\mathbb{N}$.

```
def div(a,b) :
    q = 0 ; r = a
    while r >= b :
        r = r-b
        q = q+1
    return(q,r)
```

On montre facilement que le nombre d'itérations dans cet algorithme lorsque $a > b$ est en $O\left(\ln\left(\frac{a}{b}\right)\right)$, et que sa complexité est en $O\left(\ln\left(\frac{a}{b}\right)\ln(b)\right)$.

Propriété 6 (✎)

Soient $(a,b) \in \mathbb{Z}$ et $n \in \mathbb{N}^*$.

- n divise a si, et seulement si, le reste de la division euclidienne de a par n est nulle.
- $a \equiv b\,[n]$ si, et seulement si, a et b ont même reste dans la division euclidienne par n.

Exercice 5 Déterminer le reste de la division euclidienne de 67^{2024} par 7.

Propriété 7 (✎)

Soit $n \in \mathbb{N}^*$. Il y a exactement n classes d'équivalence pour la congruence modulo n, qui sont $\overline{0}, \overline{1}, \ldots, \overline{n-1}$.

On s'intéresse dans l'exercice qui suit à la première *équation diophantienne* de ce chapitre. On appelle ainsi toute équation à inconnues entières construite à partir des seules opérations d'addition et de multiplication. Par exemple, les équations $2x + 3y = 5$ ou $x^3 + 2 = y^4$ d'inconnue $(x,y) \in \mathbb{Z}^2$.

Exercice 6 Soient $x, y, z \in \mathbb{Z}^3$ trois entiers solutions de l'*équation de Fermat* $x^3 + y^3 = z^3$. Montrer que l'un des entiers x, y ou z est divisible par 3.

1.4 Nombres premiers

Définition.

On dit qu'un entier naturel $p \geq 2$ est *premier* si ses seuls diviseurs sont ± 1 et $\pm p$.

✎ Notation.

On notera $\mathbb{P}$ l'ensemble des nombres premiers. Ainsi :

$$\mathbb{P} = \{2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, \ldots\}.$$

Remarques.

- 2 est le seul nombre premier pair.
- Un entier naturel $p \geq 2$ est premier si, et seulement si :

$$\forall (a,b) \in \mathbb{N}^2, \quad p = ab \;\Rightarrow\; (a = 1 \text{ ou } b = 1).$$

  Un entier naturel n n'est pas premier si $n = 0$ ou 1, ou s'il existe $a, b \geq 2$ tels que $n = ab$.

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.

Propriété 8 (Existence de la factorisation première - ✎)

Tout entier naturel non nul est produit de nombres premiers.

Théorème 9 (✎)

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

Crible d'Eratosthène (-276, -194)**.**

Le *crible d'Eratosthène* permet de dresser la liste de tous les nombres premiers inférieurs à un entier $n \geq 2$ donné. Il repose sur la remarque suivante : si n n'est pas premier, et si p est son plus petit diviseur premier, alors il existe $k \in \mathbb{N}$ tel que $n = pk$ avec $p \leq k$, de sorte que $p^2 \leq pk = n$. Ainsi :

un entier $n \geq 2$ non premier possède un diviseur premier inférieur à $\sqrt{n}$.

Partant de ce résultat, on procède comme suit :

(i) on écrit tous les nombres de 2 à n ;

(ii) on conserve le nombre premier 2 et on raye tous les multiples de 2 (qui ne sont donc pas premiers) ;

(iii) pour chaque nombre suivant p non rayé, on conserve p et on raye tous les multiples de p ;

(iv) on s'arrête dès que l'on dépasse strictement $\sqrt{n}$.

Tous les nombres non rayés sont les nombres premiers inférieurs ou égaux à n.

	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~~

Crible d'Eratosthène pour $n = 100$.

On en déduit un premier test de primalité : pour déterminer si un entier $n \geq 2$ est premier ou non, on teste sa divisibilité par tous les nombres premiers inférieurs à $\sqrt{n}$.

Le saviez-vous ?

La répartition des nombres premiers parmi l'ensemble des entiers naturels semble bien chaotique, presque aléatoire. On peut déjà le percevoir sur ce crible d'Eratosthène avec $n = 100$. Citons à ce sujet deux curiosités :

- certains nombres premiers ne sont distants que de 2, par exemple 11 et 13, 17 et 19, ou encore 71 et 73. De tels nombres premiers sont dits *jumeaux*. On connait des nombres premiers jumeaux à plus de 58000 chiffres. On ne sait cependant pas s'il en existe une infinité ou non.
- inversement, il semble y avoir des « trous » dans cette répartition, ici entre 89 et 97 par exemple. Plus généralement, pour tout $N \geq 1$, il existe des intervalles d'entiers de longueur N ne contenant aucun nombre premier (prendre par exemple $[\![(N+1)! + 2, (N+1)! + (N+1)]\!]$).

Donnons quelques résultats célèbres qui permettent de mieux appréhender (ou pas) cette répartition.

Le Théorème des nombres premiers démontré indépendamment par Hadamard et La Vallée Poussin en 1896. Il affirme que :

> Pour un entier naturel n, le nombre $\pi(n)$ de nombres premiers inférieurs ou égaux à n vérifie :
>
> $$\pi(n) \times \frac{\ln(n)}{n} \underset{n\to+\infty}{\longrightarrow} 1.$$

Une conséquence de ce résultat est que $\lim\limits_{n\to+\infty} \dfrac{\pi(n)}{n} = 0$. En d'autres termes, la densité des nombres premiers dans $\mathbb{N}$ est nulle.

Le Théorème de la progression arithmétique démontré par le mathématicien allemand Gustav Lejeune Dirichlet en 1838. Il s'énonce comme suit :

> Si a et b sont des entiers premiers entre eux, alors il existe une infinité de nombres premiers p vérifiant $p \equiv a\,[b]$.

Ainsi, il existe une infinité de nombres premiers de la forme $4k + 1$, ou encore une infinité de nombres premiers dont l'écriture décimale se termine par 2023 (2023 et 10000 étant premiers entre eux, il y a bien une infinité de nombres premiers dans $2023 + 10000\mathbb{N}$).

Le Théorème de Green-Tao. Peut-on trouver des progressions arithmétiques finies, mais de longueur arbitrairement grande, constituées uniquement de nombres premiers ? Par exemple des progressions arithmétiques :

- de longueur 3 : 3, 5, 7 ;
- de longueur 5 : 5, 11, 17, 23, 29 ;
- de longueur 6 : 7, 37, 67, 97, 127, 157 ;
- de longueur 26 (obtenue le 12 avril 2010 à l'aide de 75 ordinateurs) :

$$43\,142\,746\,595\,714\,191 + 23\,681\,770 \times 223\,092\,870 \times n \text{ pour } n \in [\![0, 25]\!].$$

Les mathématiciens Ben Green et Terence Tao sont parvenus à montrer en 2004 que :

> La suite des nombres premiers contient des progressions arithmétiques arbitrairement longues.

Autrement dit, pour un entier naturel k arbitraire, il existe une suite arithmétique de k termes formée de nombres premiers. Terence Tao a obtenu la médaille Fields en 2006 pour ces travaux.

2 Plus grand commun diviseur (PGCD), plus petit commun multiple (PPCM)

2.1 PGCD de deux entiers

Soit $(a,b) \in \mathbb{Z}^2$, $(a,b) \neq (0,0)$. L'ensemble $\mathscr{D}(a) \cap \mathscr{D}(b) \cap \mathbb{N}$ des diviseurs communs positifs de a et de b est une partie non vide (car elle contient 1) et majorée de $\mathbb{N}$ (par $|a|$ ou $|b|$ selon que $a \neq 0$ ou $b \neq 0$). Elle admet donc un plus grand élément.

Définition.

Soit $(a,b) \in \mathbb{Z}^2$, $(a,b) \neq (0,0)$. On appelle *plus grand commun diviseur* (en abrégé PGCD) de a et b, et on note $\mathrm{PGCD}(a,b)$ ou $a \wedge b$, l'entier $\max(\mathscr{D}(a) \cap \mathscr{D}(b) \cap \mathbb{N})$.

Par convention, on pose $0 \wedge 0 = 0$.

Exemple. $60 \wedge 18 = 6$ car $\mathscr{D}(60) \cap \mathscr{D}(18) \cap \mathbb{N} = \{1,2,3,6\}$.

Remarques.

- Par définition du pgcd de $(a,b) \in \mathbb{Z}^2$, $a \wedge b = b \wedge a$ (commutativité du PGCD) et $a \wedge b = |a| \wedge |b|$ (invariance du PGCD par changement de signe).
- Si $b = 0$, alors $\mathscr{D}(a) \cap \mathscr{D}(b) \cap \mathbb{N} = \mathscr{D}(a) \cap \mathbb{N}$ et donc $a \wedge 0 = |a|$.
- Si $b \mid a$, alors $\mathscr{D}(b) \subset \mathscr{D}(a)$ et donc $\mathscr{D}(a) \cap \mathscr{D}(b) \cap \mathbb{N} = \mathscr{D}(b) \cap \mathbb{N}$, de sorte que $a \wedge b = |b|$.

2.2 L'algorithme d'Euclide

Nous présentons dans cette section 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.

Propriété 10 (✎)

Soient a et b deux entiers naturels avec $b > 0$. Si r désigne le reste de la division de a par b, alors :

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

Algorithme d'Euclide. Soient a et b deux entiers naturels[1] non nuls. On définit la suite (r_k) par :

- $r_0 = a$, $r_1 = b$;
- supposons avoir défini les termes r_{k-1} et r_k pour un certain rang $k \geq 1$. Si $r_k > 0$, on effectue la division euclidienne de r_{k-1} par r_k : il existe un unique couple d'entiers (q_{k+1}, r_{k+1}) tels que

$$r_{k-1} = q_{k+1} r_k + r_{k+1} \quad \text{avec} \quad 0 \leq r_{k+1} < r_k.$$

Par construction, $(r_k)_{k \geq 1}$ est une suite strictement décroissante d'éléments de $[\![0, \max(a,b)]\!]$. Elle est donc nécessairement finie : il existe $N \in \mathbb{N}$ tel que $r_N \neq 0$ et $r_{N+1} = 0$.

[1] On peut s'y ramener quitte à remplacer a et b par $|a|$ et $|b|$, ce qui ne changera pas leur PGCD.

Propriété 11 (Première caractérisation du PGCD - ✎)

Soient $(a,b) \in \mathbb{Z}^2 \setminus \{(0,0)\}$. Alors $a \wedge b$ est le dernier reste non nul quand on effectue les divisions euclidiennes successives dans l'algorithme d'Euclide.

On en déduit la fonction suivante pour le calcul du PGCD de deux entiers.

```
def euclide(a,b) :
    r0 = a ; r1 = b
    while r1 > 0 :
        r2 = div(r0,r1)[1]
        r0 = r1
        r1 = r2
    return r0
```

Lorsque $a > b$, on peut montrer que le nombre d'itérations dans cet algorithme est en $O(\ln(b))$, et que sa complexité est en $O(\ln(a)^2)$.

Exercice 7 Calculer $162 \wedge 207$.

Corollaire 12 (✎)

Soient $(a,b) \in \mathbb{Z}^2$ et $d \in \mathbb{Z}$. Alors :

$$(d \mid a \text{ et } d \mid b) \Leftrightarrow d \mid a \wedge b.$$

Autrement dit, $\mathscr{D}(a) \cap \mathscr{D}(b) = \mathscr{D}(a \wedge b)$.

Propriété 13 (Deuxième caractérisation du PGCD -✎)

Soient $(a,b) \in \mathbb{Z}^2$ et $d \in \mathbb{N}$. Alors :

$$d = a \wedge b \Leftrightarrow \begin{cases} d \mid a \text{ et } d \mid b \\ \forall n \in \mathbb{N},\ (n \mid a \text{ et } n \mid b) \Rightarrow n \mid d \end{cases}.$$

Remarque. Soient $a, b \in \mathbb{Z}$. La proposition précédente affirme que :

- $a \wedge b$ appartient à $\mathscr{D}(a) \cap \mathscr{D}(b) \cap \mathbb{N}$;
- $a \wedge b$ est plus grand au sens de la relation de divisibilité (qui, rappelons le, est une relation d'ordre sur $\mathbb{N}$) que tout élément de $\mathscr{D}(a) \cap \mathscr{D}(b) \cap \mathbb{N}$.

Ainsi, $a \wedge b$ est le plus grand élément de $\mathscr{D}(a) \cap \mathscr{D}(b) \cap \mathbb{N}$ pour la relation de divisibilité dans $\mathbb{N}$.

Propriété 14 (✎)

Soient $(a,b,c) \in \mathbb{Z}^3$.

- *Associativité du PGCD* : $(a \wedge b) \wedge c = a \wedge (b \wedge c)$.
- *Homogénéité du PGCD* : $\forall k \in \mathbb{Z},\ (ak) \wedge (bk) = |k|(a \wedge b)$.

2.3 Théorème de Bezout

Théorème 15 (*Identité de Bezout* - ✎)

Soient $a, b \in \mathbb{Z}$. Alors il existe un couple $(u, v) \in \mathbb{Z}^2$ tels que :

$$a \wedge b = au + bv.$$

Un tel couple (u, v) est appelé **un** couple de Bezout, et une telle relation **une** *relation de Bezout*.

Mise en garde.

- L'identité de Bézout nous donne une implication, mais pas une équivalence : si $d = au + bv$, alors $a \wedge b$ divise d, mais on n'a pas nécessairement $d = a \wedge b$. 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 :

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

Algorithme d'Euclide étendu. Soient a et b deux entiers naturels non nuls. En conservant les notations de l'algorithme d'Euclide, on a obtenu dans la preuve précédente l'existence de deux suites $(u_k)_{0 \leq k \leq N}$ et $(v_k)_{0 \leq k \leq N}$ satisfaisant :

$$\forall k \in [\![0, N]\!], \quad r_k = au_k + bv_k.$$

Elles sont définies récursivement par $(u_0, v_0) = (1, 0)$, $(u_1, v_1) = (0, 1)$ et pour tout $k \in [\![0, N-2]\!]$:

$$(u_{k+2}, v_{k+2}) = (u_k - q_{k+2}u_{k+1}, v_k - q_{k+2}v_{k+1}).$$

On en déduit la fonction suivante pour l'obtention du PGCD de deux entiers naturels non nuls et d'un couple de Bezout associé. Sa complexité est la même que pour l'algorithme d'Euclide, à savoir $O\left(\ln(\max(a, b))^2\right)$.

```
def euclide_etendu(a,b) :
      u0 = 1 ; u1 = 0 ; v0 = 0 ; v1 = 1 ; r0 = a ; r1 = b
      while r1>0 :
            (q2,r2) = div(r0,r1);
            r0 = r1 ; r1 = r2
            u2 = u0-q2*u1 ; v2 = v0-q2*v1
            u0 = u1 ; v0 = v1
            u1 = u2 ; v1 = v2
      return (r0,u0,v0)
```

Exercice 8 Déterminer un couple de Bezout associé aux entiers $a = 207$ et $b = 162$.

2.4 Entiers premiers entre eux

Définition.

Soit $(a, b) \in \mathbb{Z}^2$. On dit que a et b sont *premiers entre eux* si $a \wedge b = 1$, autrement dit si les seuls diviseurs communs à a et b sont 1 et -1.

Exemples.

- 4 et 5 sont premiers entre eux, de même que 6 et 35. En revanche, 4 et 10 ne sont pas premiers entre eux, de même que 21 et 35.
- Deux nombres premiers distincts sont toujours premiers entre eux.

Théorème 16 (*de Bezout* (1730-1783) - ✎)

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

Propriété 17 (✎)

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.

Corollaire 18 (✎)

Soient $a, b_1, \ldots, b_n$ des entiers. Alors a est premier avec le produit $b_1 \times \cdots \times b_n$ si pour tous $i \in [\![1, n]\!]$, a est premier avec b_i.

Propriété 19 (Lemme de Gauss (1777-1855) - ✎)

Soient a, b et c des entiers. Si a divise bc et si a est premier avec b, alors a divise c.

Corollaire 20 (✎)

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

Application au calcul modulaire. Soit $n \in \mathbb{N}^*$, et soient $a, b, k \in \mathbb{Z}$.

- Si $k \wedge n = 1$, et si $(u, v) \in \mathbb{Z}^2$ sont tels que $ku + bn = 1$, alors $ku \equiv 1\,[n]$. On dit alors que u est un *inverse de k modulo n*.
- Si $ak \equiv bk\,[n]$ et si $k \wedge n = 1$, alors $a \equiv b\,[n]$ (puisque $a \equiv aku \equiv bku \equiv b\,[n]$).

Danger.

L'hypothèse $k \wedge n = 1$ est indispensable pour effectuer une simplification. Ce résultat est faux sinon : par exemple $2 \times 3 \equiv 2 \times 0\,[6]$, mais $3 \not\equiv 0\,[6]$.

Propriété 21 (Troisième caractérisation du PGCD - ✎)

Soient $(a,b) \in \mathbb{Z}^2 \setminus \{(0,0)\}$ et $d \in \mathbb{N}^*$. Alors :

$$d = a \wedge b \;\Leftrightarrow\; \exists\,(a',b') \in \mathbb{Z}^2,\; \begin{cases} a = da' \\ b = db' \\ a' \wedge b' = 1 \end{cases}.$$

Propriété 22 (✎)

Soit $r \in \mathbb{Q}$. Il existe un unique $(a,b) \in \mathbb{Z} \times \mathbb{N}^*$ tel que $r = \dfrac{a}{b}$ avec a, b premiers entre eux.
L'écriture $r = \dfrac{a}{b}$ avec $(a,b) \in \mathbb{Z} \times \mathbb{N}^*$ et $a \wedge b = 1$ est appelée *forme irréductible de* r.

2.5 PPCM de deux entiers

Soient $a, b \in \mathbb{Z}$ non nuls. L'ensemble $a\mathbb{Z} \cap b\mathbb{Z} \cap \mathbb{N}^*$ des multiples communs strictement positifs de a et de b est une partie non vide de $\mathbb{N}$ (car elle contient par exemple $|ab|$). Elle admet donc un plus petit élément (au sens de la relation d'ordre usuelle sur $\mathbb{N}$).

Définition.

Soient $a, b \in \mathbb{Z}^*$ non nuls. On appelle *plus petit commun multiple* (en abrégé PPCM) de a et b, et on note $\mathrm{PPCM}(a,b)$ ou $a \vee b$, l'entier $\min(a\mathbb{Z} \cap b\mathbb{Z} \cap \mathbb{N}^*)$.
Pour $a \in \mathbb{Z}$, on pose $a \vee 0 = 0 \vee a = 0$.

Exemple. $6 \vee 8 = 24$ car $6\mathbb{Z} \cap \mathbb{N}^* = \{6, 12, 18, 24, 30, \dots\}$ et $8\mathbb{Z} \cap \mathbb{N}^* = \{8, 16, 24, 32, \dots\}$.

Remarque. Comme pour le PGCD, le PPCM est commutatif ($a \vee b = b \vee a$) et est invariant par changement de signe : $a \vee b = |a| \vee |b|$.

Propriété 23 (Caractérisation du PPCM - ✎)

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

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

Remarque. Soient $a, b \in \mathbb{Z}$. Pour la relation de divisibilité, $a \vee b$ est donc le plus petit élément de $a\mathbb{Z} \cap b\mathbb{Z} \cap \mathbb{N}^*$.

Propriété 24 (Homogénéité du PPCM - ✎)

Soit $(a,b) \in \mathbb{Z}^2$. Pour tout $k \in \mathbb{Z}$, $(ak) \vee (bk) = |k|(a \vee b)$.

Propriété 25 (✎)

Pour tout $(a,b) \in \mathbb{N}^2$, $(a \wedge b) \times (a \vee b) = ab$.

Remarque. On dispose de l'algorithme d'Euclide pour calculer le PGCD de deux entiers. Grâce à cette formule, on obtient également leur PPCM.

2.6 Généralisation à une famille de n entiers

Définition.

Soient $n \geq 2$ et $a_1, \dots, a_n$ des entiers naturels.

- Supposons $(a_1, \dots, a_n) \neq (0, \dots, 0)$. On appelle PGCD de $a_1, \dots, a_n$, et on note $a_1 \wedge \cdots \wedge a_n$, le plus grand diviseur commun positif des a_i, c'est-à-dire $\max\left(\mathbb{N} \cap \bigcap_{i=1}^{n} \mathscr{D}(a_i)\right)$.
- Supposons $a_1, \dots, a_n$ tous non nuls. On appelle PPCM de $a_1, \dots, a_n$, et on note $a_1 \vee \cdots \vee a_n$, le plus petit commun multiple positif des a_i, c'est-à-dire $\min\left(\mathbb{N}^* \cap \bigcap_{i=1}^{n} a_i\mathbb{Z}\right)$.

Propriété 26 (✎)

Avec les notations ci-dessus :

$$\bigcap_{i=1}^{n} \mathscr{D}(a_i) = \mathscr{D}\left(\bigwedge_{i=1}^{n} a_i\right) \quad \text{et} \quad \bigcap_{i=1}^{n} a_i\mathbb{Z} = \left(\bigvee_{i=1}^{n} a_i\right)\mathbb{Z}.$$

Remarque. Ainsi :

$$\bigwedge_{i=1}^{n} a_i = \max\left(\mathbb{N} \cap \left(\bigcap_{i=1}^{n-1} \mathscr{D}(a_i)\right) \cap \mathscr{D}(a_n)\right) = \max\left(\mathbb{N} \cap \mathscr{D}\left(\bigwedge_{i=1}^{n-1} a_i\right) \cap \mathscr{D}(a_n)\right)$$

de sorte que $a_1 \wedge \cdots \wedge a_{n-1} \wedge a_n = (a_1 \wedge \cdots \wedge a_{n-1}) \wedge a_n$, et en itérant ce processus :

$$a_1 \wedge \cdots \wedge a_{n-1} \wedge a_n = (\dots((a_1 \wedge a_2) \wedge a_3) \wedge \cdots \wedge a_{n-1}) \wedge a_n.$$

Le calcul du PGCD de n entiers se ramène de cette manière à $n-1$ calculs de PGCD de deux entiers. De plus, cette égalité permet d'étendre les propriétés établies pour le PGCD de deux entiers à celui de n entiers (associativité, commutativité, homogénéité). Tout ceci vaut également pour le PPCM par les mêmes arguments.

Propriété 27

Avec les notations ci-dessus, pour tout $d, m \in \mathbb{N}$:

- $d = a_1 \wedge \cdots \wedge a_n \Leftrightarrow \begin{cases} d \mid a_1, \dots, d \mid a_n \\ \forall k \in \mathbb{N},\ (\forall i \in [\![1, n]\!],\ k \mid a_i) \ \Rightarrow\ k \mid d \end{cases}$.
- $m = a_1 \vee \cdots \vee a_n \Leftrightarrow \begin{cases} a_1 \mid m, \dots, a_n \mid m \\ \forall k \in \mathbb{N},\ (\forall i \in [\![1, n]\!],\ a_i \mid m) \ \Rightarrow\ m \mid k \end{cases}$.

Propriété 28 (Identité de Bezout - ✎)

Soient $a_1, \dots, a_n$ non tous nuls. Alors il existe $u_1, \dots, u_n \in \mathbb{Z}$ tels que $\sum_{i=1}^{n} u_i a_i = \bigwedge_{i=1}^{n} a_i$.

Exercice 9 Calculer $6 \wedge 10 \wedge 15$ et déterminer une relation de Bezout.

Définition.

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 $a_1 \wedge \cdots \wedge a_n = 1$, autrement dit si leurs seuls diviseurs communs sont 1 et -1.

Mise en garde.

Si des entiers $a_1, \dots, a_n$ sont deux à deux premiers entre eux, alors ils sont premiers entre eux dans leur ensemble. En effet, on a déjà $a_1 \wedge a_2 = 1$, donc $a_1 \wedge a_2 \wedge \cdots \wedge a_n = 1$.

En revanche la réciproque est fausse : par exemple, les entiers 6, 10 et 15 sont premiers entre eux dans leur ensemble, mais ils ne sont pas deux à deux premiers entre eux puisque $6 \wedge 10 = 2$, $6 \wedge 15 = 3$ et $10 \wedge 15 = 5$.

Propriété 29

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

3 Factorisation première et applications

3.1 Valuation p-adique

Soit p un nombre premier, et soit $n \in \mathbb{Z}$ un entier non nul. Le sous-ensemble $\{k \in \mathbb{N} \mid p^k \text{ divise } n\}$ de $\mathbb{N}$ est non vide (car il contient 0) et majoré (car si p^k divise n, alors $k \leq p^k \leq |n|$). Il admet donc un plus grand élément.

Définition.

Soit p un nombre premier, et soit $n \in \mathbb{Z}$ un entier non nul.

On appelle *valuation p-adique de n*, et on note $v_p(n)$, le maximum de l'ensemble $\{k \in \mathbb{N} \mid p^k \text{ divise } n\}$.

Exemple. $v_2(12) = 2$ car $2^2 \mid 12$ et $2^k \nmid 12$ pour $k \geq 3$, $v_3(12) = 1$ et $v_p(12) = 0$ pour tout $p \in \mathbb{P} \setminus \{2, 3\}$.

Propriété 30 (✎)

Soit p un nombre premier, et soient $a, b \in \mathbb{Z}$.

- Si $p \nmid a$, alors p et a sont premiers entre eux.
- Si $p \mid ab$, alors $p \mid a$ ou $p \mid b$.

Propriété 31 (✎)

Soit p un nombre premier. Si a et b sont deux entiers non nuls, alors :

$$v_p(ab) = v_p(a) + v_p(b).$$

Exemple. Pour tous $p, q \in \mathbb{P}$ et $k \in \mathbb{N}$, $v_p(q^k) = kv_p(q) = \begin{cases} k & \text{si } q = p \\ 0 & \text{sinon} \end{cases}$.

3.2 Décomposition en produit de facteurs premiers

Théorème 32 (Théorème fondamental de l'arithmétique - ✎)

Tout entier naturel n non nul se décompose de manière unique (à l'ordre des facteurs près) comme un produit de nombres premiers :

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

où $r \in \mathbb{N}$, $p_1, \ldots, p_r$ des nombres premiers deux à deux distincts et $\alpha_1, \ldots, \alpha_r$ des entiers naturels non nuls.

Remarque. Nous avons de plus obtenu que pour tout $k \in [\![1, r]\!]$, $\alpha_k = v_{p_k}(n)$. Et puisque $v_p(n) = 0$ pour tout $p \in \mathbb{P} \setminus \{p_1, \ldots, p_r\}$, on peut récrire la décomposition de n en produits de facteurs premiers :

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

Mise en garde.

Ce produit comporte un nombre infini de termes, mais seuls un nombre fini d'entre eux ne valent pas 1 : il n'existe qu'un nombre fini de $p \in \mathbb{P}$ pour lesquels $v_p(n) \neq 0$, et donc pour lesquels $p^{v_p(n)} \neq 1$.

Exercice 10 Soit $n \geq 2$. Montrer que $\sqrt{n}$ est un irrationnel si, et seulement si, n n'est pas un carré.

Propriété 33 (✎)

Soient $a, b \in \mathbb{N}^*$.

(1) $a \mid b \Leftrightarrow \forall p \in \mathbb{P}, v_p(a) \leq v_p(b)$.

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

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

(4) $a \wedge b = 1 \Leftrightarrow \forall p \in \mathbb{P}, v_p(a) = 0$ ou $v_p(b) = 0$.

Exemple. Puisque $9100 = 2^2 \cdot 5^2 \cdot 7 \cdot 13$ et $1848 = 2^3 \cdot 3 \cdot 7 \cdot 11$, on obtient $9100 \wedge 1848 = 2^2 \cdot 7$ et $9100 \vee 1848 = 2^3 \cdot 3 \cdot 5^2 \cdot 7 \cdot 11 \cdot 13$.

Exercice 11 Soit $n \geq 2$. Déterminer le nombre de diviseurs dans $\mathbb{N}$ de n.

Le saviez-vous ?

Obtenir la factorisation d'un entier en produit de nombres premiers n'est pas un problème algorithmique simple : bien qu'il existe des algorithmes performants pour calculer $p \times q$ même pour de très grands entiers, on ne sait pas à partir d'un produit $p \times q$ de deux grands nombres premiers p et q, déterminer p et q facilement (les algorithmes les plus performants ont une complexité exponentielle ou sous-exponentielle au mieux, et restent donc très lents).

On a ici un exemple de ce qu'on appelle une *fonction à sens unique*, à savoir une application $f : E \to F$ telle que :

- il est possible de calculer simplement $f(x)$ pour tout $x \in E$;
- pour la plupart des éléments $y \in f(E)$, il n'est pas possible de trouver un élément $x \in E$ tel que $f(x) = y$, à moins d'exécuter un nombre prohibitif d'opérations, ou d'avoir une chance sur laquelle il est déraisonnable de compter.

C'est sur cette fonction à sens unique que repose la sécurité d'un grand nombre de systèmes de cryptage, tel que le chiffrement RSA qui date de 1977 et qui est encore très utilisé aujourd'hui dans le commerce électronique, et plus généralement pour échanger des données confidentielles sur internet.

3.3 Petit théorème de Fermat

Théorème 34 (Petit théorème de Fermat (1601 - 1665) -)

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

Exercice 12 Montrer que pour tout $n \in \mathbb{Z}$, tout diviseur premier impair de $n^2 + 1$ est congru à $1\,[4]$.

Le saviez-vous ?

La dénomination de « petit théorème de Fermat » sous-entend l'existence d'un grand théorème de Fermat. En voici l'énoncé :

> Il n'existe pas de nombres entiers strictement positifs x, y et z tels que :
> $$x^n + y^n = z^n$$
> dès que n est un entier supérieur strictement à 2.

Ce résultat a été énoncé par Pierre de Fermat dans une note marginale de son exemplaire de l'*Arithmetica* de Diophante, lors d'un passage consacré au théorème de Pythagore (qui correspond au cas $n = 2$ pour lequel cette équation a une infinité de solutions, les triplets pythagoriciens). Il y précise, quelques lignes plus bas :

> « J'ai une démonstration véritablement merveilleuse de cette proposition, que cette marge est trop étroite pour contenir ».

On ne retrouva jamais la « preuve » de Fermat (tout indique qu'il n'en avait d'ailleurs pas), et il fallut plus de trois siècles pour qu'une telle preuve soit établie par le mathématicien britannique Andrew Wiles en 1994. Mais c'est surtout par les idées qu'il a fallu mettre en œuvre pour le démontrer, par les outils qui ont été mis en place pour ce faire, que ce résultat a pris une valeur considérable.