Arithmétique des nombres entiers relatifs

L'arithmétique ou théorie des nombres est sûrement la partie la plus fascinante des mathématiques. Elle permet d'énoncer très simplement des questions très difficiles. On pourra citer le très connu théorème des nombres premiers jumeaux. Gauss disait *"Die Mathematik ist die Königin der Wissenschaften, und die Arithmetik ist die Königin der Mathematik."* Comme quoi, c'est quand même super utile de parler allemand !
Nous allons voir les éléments de base : divisibilité entre entiers, primalité relative, calcul de PGCD, primalité.

1 Divisibilité

1.1 Définitions et premiers exemples

Définition 1
Soit $a, b \in \mathbb{Z}$.
a est un **multiple** de b s'il existe $q \in \mathbb{Z}$ tel que $a = qb$. a est un **diviseur** de b s'il existe $q \in \mathbb{Z}$ tel que $qa = b$.

Notation On note
$a\mathbb{Z} = \{ak \mid k \in \mathbb{Z}\}$ l'ensemble des multiples de a,
$\mathsf{div}(a) = \{k \in \mathbb{Z} \mid k|a\}$ l'ensemble des diviseurs de a

Exemple 1
$\mathsf{div}(0) = \mathbb{Z}$, $\mathsf{div}(1) = \{\pm 1\}$, $\mathsf{div}(-1) = \{\pm 1\}$, $\mathsf{div}(8) = \{\pm 1, \pm 2, \pm 4, \pm 8\}$, $\mathsf{div}(6) \cap \mathsf{div}(8) = \{\pm 1, \pm 2\}$.

Lien entre $\mid$ et $\leqslant$, Relation *divisibilité / ensemble des multiples*

Ainsi, un entier a est un diviseur d'un entier b si, et seulement si, b est un multiple de a. On note alors $a \mid b$ pour l'affirmation a divise b.
Pour tous $a, b \in \mathbb{N}^*$, $a \mid b \Longrightarrow a \leqslant b$. Relation très utile en pratique !
On a aussi $a \mid b \Longleftrightarrow b\mathbb{Z} \subset a\mathbb{Z}$.

Exemple 2
Comme $3 \mid 6$, on a $6\mathbb{Z} \subset 3\mathbb{Z}$.

Exemple 3
Résoudre dans $\mathbb{Z}$

① $x-1 \mid x+3$

$x=1$ n'est pas solution. Pour $x \neq 1$:
$x-1 \mid x+3 \iff \frac{x+3}{x-1} = 1 + \frac{4}{x-1} \in \mathbb{Z}$
$\iff x-1 \in \mathsf{div}(4) = \{1,2,4,-1,-2,-4\}$.
Ainsi $\mathcal{S} = \{2,3,5,0,-1,-3\}$.

② $x+2 \mid x^2+2$.

$x=-2$ n'est pas solution. Pour $x \neq -2$:
$x+2 \mid x^2+2 \iff \frac{x^2+2}{x+2} = x-2+\frac{6}{x+2} \in \mathbb{Z}$
$\iff x+2 \in \mathsf{div}(6) = \{1,2,3,6,-1,-2,-3,-6\}$
Ainsi $\mathcal{S} = \{-1,0,1,4,-3,-4,-5,-8\}$.

Proposition 1 : Propriétés de la relation de divisibilité

Soient $a,b,c,d \in \mathbb{Z}$.

① *La relation de divisibilité $\mid$ est réflexive et transitive sur $\mathbb{Z}$. C'est une relation d'ordre sur $\mathbb{N}$.*

② *Si $d \mid a$ et $d \mid b$, alors $d \mid (au+bv)$, pour tous $u,v \in \mathbb{Z}$.*

③ *Si $a \mid b$ et $c \mid d$, alors $ac \mid bd$.*
En particulier, si $a \mid b$, alors $a^k \mid b^k$ pour tout $k \in \mathbb{N}$.

Attention On n'invente pas de théorème !
$a \mid c$ et $b \mid c$ $\not\Longrightarrow$ $a+b \mid c$.
$3 \mid 6$ et $2 \mid 6$ mais $5 \nmid 6$.

Relation de divisibilité sur $\mathbb{N}$

On a, pour tout $k \in \mathbb{N}$, $1 \mid k$ et $k \mid 0$ donc $\mathbb{N}$ a pour plus petit élément 1 et pour plus grand élément 0, en prenant la relation de divisibilité comme relation d'ordre.
Mais ce n'est pas un ordre total. Par exemple, $2 \nmid 3$ et $3 \nmid 2$.

Preuve. Soient $a,b,c,d \in \mathbb{Z}$.

① **Transitivité** Si $b = ak$ et $c = bl$ pour certains $k,l \in \mathbb{Z}$, donc $c = bkl$.
Reflexivité On a $a = 1 \times a$.
Antisymétrie Sur $\mathbb{N}$, si $b = ak$ et $a = bl$ pour certains $k,l \in \mathbb{Z}$, donc $b = bkl$.
Si $b \neq 0$, alors $kl = 1$, donc $k = l = 1$ ou $k = l = -1$, , donc $a = b$, ou $a = -b$, , ce qui est absurde.

② On a $a = dk$ et $b = dl$ pour certains $k,l \in \mathbb{Z}$, donc $au+bv = d(ku+vl)$ avec $ku+vl \in \mathbb{Z}$ pour tous $u,v \in \mathbb{Z}$, donc enfin $d \mid (au+bv)$.

③ On a $b = ak$ et $d = cl$ pour certains $k,l \in \mathbb{Z}$, donc $bd = (ak)(cl) = (ac)(kl)$, avec $kl \in \mathbb{Z}$.

□

Attention La relation de divisibilité **n'est pas** une relation d'ordre sur $\mathbb{Z}$! En effet, pour $a,b \in \mathbb{Z}$,

$$a \mid b \text{ et } b \mid a \iff |a| = |b| \iff a = b \text{ ou } a = -b,$$

donc la relation n'est pas antisymétrique sur $\mathbb{Z}$.

1.2 La relation de congruence

Définition 2

Soit $n \in \mathbb{N}\backslash\{0\}$. La congruence modulo n est la relation binaire sur $\mathbb{Z}$ définie par la divisibilité de la différence par n.
Plus précisément, pour tous $a,b \in \mathbb{Z}$, $a = b \ [n]$ si $a-b \in n\mathbb{Z}$.

Notations La relation de congruence est également notée $\equiv$ même si on lui a préféré le symbole d'égalité dans ce cours.

Exemple 4
Montrons que, pour tout entier n impair, n^2-1 est un multiple de 8 .
En effet, en écrivant la relation $n=1\ [2]$, par sa définition $n=2k+1$ avec $k\in\mathbb{Z}$, on obtient $n^2-1=4k(k+1)$.
Or l'un des deux entiers consécutifs k ou $k+1$ est pair donc n^2-1 est un multiple de $4\times 2=8$.

Proposition 2
Soit $n\in\mathbb{N}\backslash\{0\}$. Soient $a,b,c,d\in\mathbb{Z}$.

(1) *Pour tout $a\in\mathbb{Z}$, $n\mid a \iff a\equiv 0[n]$.*

(2) *La congruence modulo n est une relation d'équivalence.*

(3) *Si $a=b[n]$ et $c=d[n]$. Alors, $a+c=b+d[n]$ et $ac=bd[n]$.*

(4) *Si $a=b[n]$. Alors, $a^k=b^k[n]$.*

(5) *Si $c\in\mathbb{N}\backslash\{0\}$, alors $a\equiv b[n]\Leftrightarrow ca\equiv cb[cn]$.*

Preuve. (1) vient de la définition.

(2) A vous !

(3) ▷ Si n divise $a-b$ et $c-d$ donc divise $(a+c)-(b+d)$.
▷ Si n divise $a-b$ et $c-d$ donc divise $(a-b)c+b(c-d)=ac-bd$.

(4) Conséquence immédiate de (3)

(5) Sous les hypothèses proposées, $a\equiv b[n]\Leftrightarrow\exists k\in\mathbb{Z}, b-a=kn\Leftrightarrow\exists k\in\mathbb{Z}, cb-ca=c(b-a)=kcn\Leftrightarrow cb\equiv ca[cn]$.

□

Exemple 5
On a $2^{345}+5^{432}\equiv(-1)^{345}+(-1)^{432}\equiv -1+1\equiv 0[3]$. Donc $2^{345}+5^{432}$ est divisible par 3.

Exemple 6
Montrons que, pour tout entier naturel n,

- $2^{3n}-1$ est un multiple de 7
  On a $2^3=1+7=1[7]$ donc $2^{3n}=1[7]$ et donc $2^{3n}-1=0[7]$.
  Plus généralement, montrez que
  si $a\in\mathbb{N}$ divise $b\in\mathbb{N}$, alors 2^a-1 divise 2^b-1.
  Le cas précédent correspond aux valeurs $a=3, b=3n$

- $10^{9n+2}+10^{6n+1}+1$ est un multiple de 111
  En effet, $10^3=1+9\times 111=1\ [111]$, on a donc

$$10^{9n+2}=\left(10^3\right)^{3n}10^2=100[111] \quad (1)$$
$$10^{6n+1}=\left(10^3\right)^{2n}10=10[111] \quad (2)$$
$$1=1[111] \quad (3)$$

  Donc,
  $10^{9n+2}+10^{6n+1}+1=100+10+1[111]=0[111]$.

Exemple 7
Montrons que $17^{341}-2$ est un multiple de 5.
On a $17^4=2[5]$ donc $17^{341}=17^{340}\times 17=1\times 2[5]=2[5]$.
D'où $17^{341}-2\in 5\mathbb{Z}$.

Exemple 8
Cherchons le dernier chiffre de 13^{80} en base 10.
Comme $13 \equiv 3[10]$ alors $13^{80} \equiv 3^{80}[10]$. Mais $3^2 = 9 \equiv (-1)[10]$ donc $3^{80} = \left(3^2\right)^{40} \equiv (-1)^{40} \equiv 1[10]$.
Donc, le dernier chiffre de 13^{80} est un 1.

Corollaire 2.1 : Critères de divisibilités pour l'écriture en base 10

Soit $n = \sum_{k=0}^{r} a_k 10^k$ *avec, pour tout* $k \in [\![0, r]\!], a_k \in [\![0, 9]\!]$.

Diviseur	Critère
n *est un multiple de* 2	a_0 *est un multiple de* 2
n *est un multiple de* 3	*la somme des chiffres* $\sum_{k=0}^{r} a_k$ *est un multiple de* 3.
n *est un multiple de* 4	$10\ a_1 + a_0$ *est un multiple de* 4 .
n *est un multiple de* 5	a_0 *est un multiple de* 5 .
n *est un multiple de* 9	*la somme des chiffres* $\sum_{k=0}^{r} a_k$ *est un multiple de* 9 .
n *est un multiple de* 11	*la somme alternée des chiffres* $\sum_{k=0}^{r} a_k(-1)^k$ *est un multiple de* 11 .

Preuve. Il suffit de remarquer que $10 = 0[2], 10 = 1[3], 100 = 0[4], 10 = 0[5], 10 = 1[9]$ et $10 = -1[11]$ pour obtenir le reste de 10^k modulo le diviseur concerné. En utilisant les règles opératoires de la congruence, on obtient

- $n = a_0[2]$ car $10^k = 0\ [2]$ pour tout $k \geq 1$,
- $n = \sum_{k=0}^{r} a_k[3]$ car $10^k = 1[3]$ pour tout k,
- $n = 10a_1 + a_0[4]$ car $10^k = 0[4]$ pour tout $k \geq 2$,
- $n = a_0[5]$ car $10^k = 0[4]$ pour tout $k \geq 1$,
- $n = \sum_{k=0}^{r} a_k[9]$ car $10^k = 1[9]$ pour tout k,
- $n = \sum_{k=0}^{r} a_k(-1)^k[11]$ car $10^k = (-1)^k[11]$ pour tout k.

□

Exemple 9
L'entier 14146 est divisible par 11, *car* $1 - 4 + 1 - 4 + 6 = 0[11]$, mais pas par 3, *car* $1 + 4 + 1 + 4 + 6 = 1[3]$.

1.3 Division euclidienne

Proposition 3
Soit $(n, a) \in \mathbb{Z} \times \mathbb{N}\backslash\{0\}$. *Il existe un unique couple* $(q, r) \in \mathbb{Z} \times \mathbb{N}$ *tel que*

$$n = qa + r \quad 0 \leq r \leq a - 1 \ .$$

Les entiers q *et* r *sont respectivement appelés* ***quotient*** *et* ***reste*** *de la* ***division euclidienne*** *de* n *par* a.

Preuve. L'unicité est immédiate. En effet, si $n = qa + r$ et $n = q'a + r'$ avec $0 \leq r' \leq r < a$, alors $a > r - r' \geq 0$ et $r - r' = (q' - q)\, a$ est un multiple de a. par conséquent $r = r'$ et $q = q'$.

- Montrons l'existence pour un entier $n \in \mathbb{N}$ par récurrence forte.
  ▷ Le résultat est immédiat pour $n = 0$ avec $q = r = 0$.
  ▷ Soit $n \in \mathbb{N}$. Si l'existence est établie pour tout entier $k \in [\![1, n]\!]$, montrons-la pour $n + 1$. Si $n + 1 < a$, alors les entiers $q = 0$ et $r = n + 1$ conviennent. Sinon, $n + 1 - a \in [\![0, n]\!]$ et on conclut avec l'hypothèse de récurrence.
- Pour montrer l'existence pour $n < 0$, on applique le point précédent à $-n$: il existe $(q, r) \in \mathbb{Z} \times \mathbb{N}$ tel que $-n = qa + r$ et $0 \leq r \leq a - 1$. Ainsi, $n = -qa - r$ est la division euclidienne si $r = 0$ et $n = (-q - 1)a + (a - r)$ si $r \neq 0$.

□

Reste d'une division euclidienne et reformulation en terme de congruence

En fait, la preuve de ce résultat fournit une construction algorithmique du quotient et du reste. En effet, il suffit de retrancher a à n, jusqu'à obtenir un entier inférieur à a qui sera alors le reste r de notre division euclidienne.

On a aussi, par définition, $\boxed{q = \left\lfloor \frac{a}{b} \right\rfloor \text{ et } r = a[b]}$. On peut donc reformuler la proposition en termes de congruences

$$\forall n \in \mathbb{Z}, \quad \exists! r \in [\![0, a - 1]\!], \quad n \equiv r[a] \ ,$$

ce qui signifie que tout entier relatif n est congru modulo a à un unique entier r compris entre 0 et $a - 1$.
L'ensemble quotient de $\mathbb{Z}$ par la relation "$= \cdot[a]$" est donc l'ensemble $\{a\mathbb{Z}, a\mathbb{Z} + 1, \ldots, a\mathbb{Z} + a - 1\}$ à a éléments noté généralement $\mathbb{Z}/a\mathbb{Z}$. Par exemple, on peut ramener $n = 2348$ à l'un des entiers $0, 1, 2, 3$ ou 4 modulo $a = 5$.
Et effectivement, $2348 \equiv 3[5]$.

Exemple 10
Attention ! n et $-n$ n'ont pas les mêmes quotients et restes !
▷ Division euclidienne de 81 par 12 nous donne $81 = 12 \cdot 6 + 9$.
▷ Division euclidienne de -81 par 12 nous donne $-81 = 12 \cdot (-7) + 3$.

Exemple 11
Soient $x, y, z \in \mathbb{Z}$ solutions de l'équation $x^3 + y^3 = z^3$. Montrons que l'un des entiers x, y ou z est divisible par 3.
En effet, supposons par l'absurde que ni x ni y ni z n'est divisible par 3. Le reste de la division euclidienne de x, y et z par 9 est alors l'un des entiers $1, 2, 4, 5, 7, 8$. Regardons alors leurs puissances troisième :

▷ $x = 1[9] \implies x^2 = 1[9] \implies x^3 = 1[9]$,
▷ $x = 2[9] \implies x^2 = 4[9] \implies x^3 = -1[9]$,
▷ $x = 4[9] \implies x^2 = -2[9] \implies x^3 = 1[9]$,
▷ $x = 5[9] \implies x^2 = -2[9] \implies x^3 = -1[9]$,
▷ $x = 7[9] \implies x^2 = 4[9] \implies x^3 = 1[9]$,
▷ $x = 8[9] \implies x^2 = 1[9] \implies x^3 = -1[9]$.

Donc $x^3 = \pm 1[9]$ et de même pour $y^3 \equiv \pm 1[9]$ et $z^3 \equiv \pm 1[9]$.
Or, d'après l'équation, $x^3 + y^3 \equiv z^3[9]$. Mais il y a un problème ! Le nombre $x^3 + y^3$ peut seulement être congru à $1 + 1 = 2$, $1 - 1 = 0$, $-1 + 1 = 0$ ou $-1 - 1 = -2$. Absurde !

Exemple 12
Calculons le reste de la division euclidienne de 2^{65362} par 7. La résolution est très longue si on applique l'algorithme précédent comme un *bourrin*.
En se rappelant de ce que l'on a fait précédemment, on remarque que $2^3 = 8 = 1[7]$.
Trouver, si elle existe, la première puissance de 2 congrue à 1 ou -1 modulo 7, permet toujours de résoudre le problème.
Mais on a $65362 = 3 \times 21787 + 1$, donc $2^{65362} = \left(2^3\right)^{21787} \times 2^1 = 1^{21787} \times 2 = 2[7]$.

De même, Calculer le reste de la division euclidienne de 3^{12961} par 5.

Corollaire 3.1 : Écriture en base a

Soit a un entier supérieur ou égal à 2 . Pour tout $n \in \mathbb{N}\backslash\{0\}$, il existe un unique entier $N \in \mathbb{N}$ et un unique $(N+1)$-uplet $(d_0, \dots, d_N) \in [\![0, b-1]\!]^{N+1}$ tels que

$$n = \sum_{k=0}^{N} d_k a^k, \quad d_N \neq 0$$

*On note alors $n = \overline{d_N \dots d_0}^b$, que l'on appelle l'**écriture en base a** de n.*

Preuve. On montre l'existence par récurrence forte.

- Le résultat est immédiat pour $n = 1 = 1 \times a^0$.
- Soit $n \in \mathbb{N}\backslash\{0\}$. Supposons que la propriété est établie pour tout $k \in [\![1, n]\!]$.
  Considérons la division euclidienne de $n+1$ par a, qui donne $(q, d_0) \in \mathbb{Z}^2$ tel que $n+1 = qa + d_0$ avec $0 \leq d_0 < a$.
  Si $q = 0$, le résultat est établi. Sinon, $1 \leq q \leq n$ et l'hypothèse de récurrence entraîne qu'il existe $N' \in \mathbb{N}$ et un unique N'-uplet $(d_1, \dots, d_{N+1}) \in [\![0, a-1]\!]^{N'+1}$ tels que

$$q = \sum_{k=1}^{N+1} d_k a^{k-1}, \quad \text{avec } d_{N+1} \neq 0, \quad \text{soit} \quad n = \sum_{k=1}^{N+1} d_k a^k + d_0,$$

  ce qui donne le résultat.

  Pour l'unicité, Procédons par l'absurde. Si $\sum_{k=0}^{N} d_k a^k = \sum_{k=0}^{N} d'_k a^k$, avec $d_N \neq d'_N$ et tous les «chiffres» entre 0 et $a-1$, alors a^N divise $\sum_{k=0}^{N-1} (d'_k - d_k)\, a^k$.

  Or, ce dernier entier est inférieur en valeur absolue à $(a-1)\sum_{k=0}^{N-1} a^k = a^N - 1$, d'où la contradiction.

  On procède de la même manière pour tous les k en "descendant".

□

Autre preuve

L'étape d'existence dans l'hérédité peut être traitée différemment (ce qui donne une autre construction algorithmique). Soit $n \in \mathbb{N}\backslash\{0\}$. Supposons que la propriété est établie pour tout $k \in [\![1,\ n]\!]$. Définissons N comme le plus grand élément de l'ensemble non vide $\{k \in \mathbb{N} \mid b^k \leq n+1\}$ puis d_N comme le plus grand élément de l'ensemble non vide $\{l \in \mathbb{N} \mid lb^N \leq n+1\}$.
Ce dernier ensemble contient 1 mais pas b donc $d_N \in [\![1, b-1]\!]$. Appliquons l'hypothèse de récurrence à $n+1-d_N b^N \leq n$, donc il existe $(d_0, \dots, d_{N-1}) \in [\![0, b-1]\!]^N$ tels que

$$n + 1 - d_N b^N = \sum_{k=0}^{N-1} d_k b^k \quad \text{donc} \quad n + 1 = \sum_{k=0}^{N} d_k b^k \ .$$

Exemple 13

La numération en base 2 ou écriture binaire est essentielle (entre autres pour l'informatique).
Pour écrire 42 en base 2, on fait

$$\begin{aligned} 42 &= 2 \times 21 + 0 \\ 21 &= 2 \times 10 + 1 \\ 10 &= 2 \times 5 + 0 \\ 5 &= 2 \times 2 + 1 \\ 2 &= 2 \times 1 + 0 \\ 1 &= 2 \times 0 + 1 \end{aligned}$$

donc $\overline{101010}^2 = \overline{42}^{10} = 42$.

Exemple 14

L'écriture binaire de 108 est $\overline{1101100}^2$.
En utilisant l'idée de la démonstration, on calcule les divisions successives par 2 et l'écriture binaire est composée de la suite des restes (en la lisant de bas en haut sur notre illustration).

$$\begin{aligned} 108 &= 2\times 54+0\\ 54 &= 2\times 27+0\\ 27 &= 2\times 13+1\\ 13 &= 2\times 6+1\\ 6 &= 2\times 3+0\\ 3 &= 2\times 1+1\\ 1 &= 2\times 0+1 \end{aligned}$$

En utilisant l'idée de la remarque, on retranche à chaque étape la plus grande puissance possible.

$$\begin{aligned} 108 &= 2^6+44 = 2^6+2^5+12 = 2^6+2^5+2^3+2^2\\ &= 1\times 2^6+1\times 2^5+0\times 2^4+1\times 2^3+1\times 2^2+0\times 2^1+0\times 2^0 \end{aligned}$$

Nombres dyadiques

Les nombres dyadiques sont les nombres qui s'écrivent $\frac{k}{2^n}$, où k est un entier relatif et n est un entier naturel. Par exemple, $\frac{13}{4}$ est un nombre dyadique, mais $\frac{3}{10}$ ne l'est pas.
Tout nombre dyadique admet un développement dyadique fini, c'est-à-dire une écriture en base 2 ne comportant qu'un nombre fini de chiffres. Pour écrire le développement dyadique de $\frac{k}{2^n}$ on commence par écrire le développement dyadique de k, puis on insère une virgule juste après le n-ème chiffre en partant de la fin. Par exemple, on sait que 13 s'écrit en base 2 sous la forme 1101 et donc $\frac{13}{4}$ s'écrit 11,01.
Les nombres dyadiques jouent donc le même rôle pour la base 2 que les nombres décimaux pour la base 10. Ainsi, ils possèdent les mêmes propriétés. Par exemple, les nombres dyadiques sont denses dans $\mathbb{R}$!

1.4 Sous groupes de $\mathbb{Z}$

Définition 3 : Sous-groupe de $\mathbb{Z}$

On appelle sous-groupe de $\mathbb{Z}$, toute partie de $\mathbb{Z}$ stable par addition et qui contient l'opposé de tout ses nombres.

Proposition 4

Soit G un sous-groupe de $\mathbb{Z}$. Alors, il existe $n\in\mathbb{N}$ tel que

$$G = n\mathbb{Z} = \{kn \mid k\in\mathbb{Z}\}.$$

Preuve. Si $G=\{0\}$, alors $G=0\mathbb{Z}$.
Sinon, G contient un élément non nul, si $x<0$, l'élément $-x\in G$, donc G contient au moins un élément strictement positif.
Soit $n=\min G\cap\mathbb{N}\backslash\{0\}$. Comme G est stable par sommes et différences, $n\mathbb{Z}\subset G$.
Réciproquement, si $m\in G$, il existe $(q,r)\in\mathbb{Z}^2$ tel que $m=qn+r$ et $0\leq r<n$. Alors, $r=m-qn\in G$ et par minimalité de n, on a $r=0$. Ainsi, $m\in n\mathbb{Z}$.
Par double inclusion, $G=n\mathbb{Z}$. □

Quels avantages de cette vision ?

Cela nous donnent immédiatement les propriétés des diviseurs et des multiples d'un nombre entier. Aussi, il faut retenir l'argument utilisé en arithmétiques pour les parties de $\mathbb{N}$ $\longrightarrow$ Elles ont un plus petit élément !

2 PGCD, PPCM

2.1 Définitions

Définition 4 : Diviseurs communs, Multiples communs

Soit $a, b \in \mathbb{Z}$ non tous les deux nuls.
On dit que $d \in \mathbb{Z}$ est un diviseur commun de a et b s'il divise à la fois a et b.
Le PGCD de a et b est le **plus grand diviseur commun** à a et b.
On dit que $m \in \mathbb{Z}$ est un multiple commun de a et b si a et b divisent m.
Le PPCM de a et b est le **plus petit multiple commun** à a et b.

Notations Vous rencontrerez les notations suivantes :
$a \wedge b = \text{pgcd}(a, b) = \text{PGCD}(a, b)$
$a \vee b = \text{ppcm}(a, b) = \text{PPCM}(a, b)$

Pourquoi ces nombres existent et sont uniques ?

Les ensembles de tous les multiples et de tous les diviseurs à a et b sont des parties de $\mathbb{N}$, majorée pour la deuxième. On a vu donc qu'elles admettent respectivement un plus grand et un plus petit élément. Cela montre l'existence et l'unicité de ces deux nombres !

Exemple 15
Le PGCD de 39 et 42 est 3 car $3 = 3 \cdot 13$ et $42 = 3 \times 2 \cdot 7$. Le PPCM de 39 et 42 est 546.
Le PGCD de 121125 et 29835 est $3 \cdot 5 \cdot 17 = 255$ car $121125 = 3 \cdot 5 \cdot 5 \cdot 5 \cdot 17 \cdot 19$ et $29835 = 3 \cdot 3 \cdot 3 \cdot 5 \cdot 13 \cdot 17$.
Le PPCM de 121125 et 29835 est 14171625.

2.2 PGCD, PPCM et sous groupe de $\mathbb{Z}$

Proposition 5

Soit $a, b \in \mathbb{Z}$.
Le PGCD de a et b est l'unique entier naturel d tel que $a\mathbb{Z} + b\mathbb{Z} = d\mathbb{Z}$.
Le PPCM de a et b est l'unique entier naturel m tel que $a\mathbb{Z} \cap b\mathbb{Z} = m\mathbb{Z}$.

Pour les diviseurs

De manière équivalente, on a $\mathsf{div}(a) \cap \mathsf{div}(b) = \mathsf{div}(a \wedge b)$ et $\mathsf{div}(a) \cup \mathsf{div}(b) = \mathsf{div}(a \vee b)$.

Exemple 16
On a donc $39\mathbb{Z} + 42\mathbb{Z} = 3\mathbb{Z}$ et $39\mathbb{Z} \cap 42\mathbb{Z} = 546\mathbb{Z}$.

Preuve.
Montrons le résultat pour le PGCD.
Remarquons que, si c est un diviseur de a et de b, alors $a\mathbb{Z} \subset c\mathbb{Z}$ et $b\mathbb{Z} \subset c\mathbb{Z}$ donc

$$a\mathbb{Z} + b\mathbb{Z} \subset c\mathbb{Z}$$

- $(a \wedge b) \mid a$ et $(a \wedge b) \mid b$, donc $a\mathbb{Z} + b\mathbb{Z} \subset (a \wedge b)\mathbb{Z}$. Mais $a\mathbb{Z} + b\mathbb{Z}$ est un sous groupe de $\mathbb{Z}$, donc de la forme $c\mathbb{Z}$, avec $c \in \mathbb{N}$. Donc $(a \wedge b) \mid c$.
  Mais $a\mathbb{Z} \subset c\mathbb{Z}$ et $b\mathbb{Z} \subset c\mathbb{Z}$ donc $c \mid a$ et $c \mid b$. Par maximalité de $a \wedge b$ dans $\mathsf{div}(a) \cap \mathsf{div}(b)$, alors $c \mid a \wedge b$. D'où $a \wedge b = c$.
- Soit c un diviseur de a et de b. Alors,
  $$d\mathbb{Z} = a\mathbb{Z} + b\mathbb{Z} \subset c\mathbb{Z}$$
  donc c est un diviseur de d. Donc d est le plus grand diviseur de a et b.

Montrons le résultat pour le PPCM.
Remarquons que, si c est un multiple de a et de b, alors $a\mathbb{Z} \supset c\mathbb{Z}$ et $b\mathbb{Z} \supset c\mathbb{Z}$ donc

$$a\mathbb{Z} \cap b\mathbb{Z} \supset c\mathbb{Z}$$

- On a donc $a\mathbb{Z} \cap b\mathbb{Z} \supset a \vee b\mathbb{Z}$. Mais $a\mathbb{Z} \cap b\mathbb{Z}$ est un sous groupe de $\mathbb{Z}$, donc de la forme $c\mathbb{Z}$, avec $c \in \mathbb{N}$. Donc $c \mid (a \vee b)$. Mais $a\mathbb{Z} \supset c\mathbb{Z}$ et $b\mathbb{Z} \supset c\mathbb{Z}$ donc $a \mid c$ et $b \mid c$. Par minimalité de $a \vee b$ dans $a\mathbb{Z} \cap b\mathbb{Z}$, alors $a \vee b \mid c$. D'où $a \vee b = c$.
- Soit c un multiple de a et de b. Alors,
$$c\mathbb{Z} \subset a\mathbb{Z} \cap b\mathbb{Z} = m\mathbb{Z}$$
donc c est un multiple de m. Donc $|c| \geqslant m$.

□

PGCD d'une famille d'entiers

Cette proposition permet de définir le PGCD d'une famille finie d'entiers. Le PGCD des entiers $a_1, \dots, a_n$ est l'unique entier naturel $a_1 \wedge \dots \wedge a_n$ tel que

$$a_1\mathbb{Z} + \dots + a_n\mathbb{Z} = (a_1 \wedge \dots \wedge a_n)\,\mathbb{Z}$$

On remarque en particulier «l'associativité du PGCD». Pour tous $a, b, c \in \mathbb{Z}$,

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

Les mêmes remarques restent valables pour le PPCM.

Exemple 17
Cherchons le PGCD de 28, 42 et 98. On a

$$\mathsf{div}(28) \cap \mathsf{div}(42) \cap \mathsf{div}(98) = \{\pm 1, \pm 2, \pm 7, \pm 14\}\ .$$

Donc $28 \wedge 42 \wedge 98 = 14$ et $28\mathbb{Z} + 42\mathbb{Z} + 98\mathbb{Z} = 14\mathbb{Z}$.

Bézout : Premier contact

La proposition de PGCD donne directement la propriété de Bézout. En effet, pour tous $a, b \in \mathbb{Z}$, il existe $u, v \in \mathbb{Z}$ tels que $ua + vb = a \wedge b$.
On remarque qu'il n'y a pas unicité de ces coefficients entiers u et v. Par exemple,

$$1 \times 3 + (-1) \times 2 = (-1) \times 3 + 2 \times 2 = 2 \wedge 3$$

Donc, dans les exercices, utiliser l'hypothèse "$d = a \wedge b$" revient à utiliser

$$d = a \wedge b \iff \begin{cases} \exists a' \in \mathbb{Z}, a = da' \\ \exists b' \in \mathbb{Z}, b = db' \\ a' \wedge b' = 1 \end{cases}$$

En effet,

$$d = a \wedge b \iff \exists u, v \in \mathbb{Z} \text{ tels que } ua + vb = d \iff \exists u, v \in \mathbb{Z} \text{ tels que } u\frac{a}{d} + v\frac{b}{d} = 1 \iff \frac{a}{d} \wedge \frac{b}{d} = 1\ .$$

Mais comment trouve-t-on ces coefficients u et v ? On a l'algorithme d'Euclide.

2.3 L'outil : l'algorithme d'Euclide

Proposition 6
Soit $a, b \in \mathbb{Z}$. Alors,

- $|a| \wedge |b| = a \wedge b \quad et \quad a \wedge 0 = |a|$
- $\forall k \in \mathbb{Z}, \quad (ka) \wedge (kb) = |k|(a \wedge b)$
- $\forall k \in \mathbb{Z}, \quad (ka) \vee (kb) = |k|(a \vee b)$
- ***Idée fondamentale l'algorithme d'Euclide***
$\forall k \in \mathbb{Z}, \quad a \wedge (b - ka) = a \wedge b$

Preuve. Il suffit de remarquer que $a\mathbb{Z} = |a|\mathbb{Z}$ et que $a\mathbb{Z} + (b - ka)\mathbb{Z} = a\mathbb{Z} + b\mathbb{Z}$. □

On est prêt pour l'algorithme d'Euclide !

Soient $a, b \in \mathbb{Z}$ tels que $a \geqslant b$ et $b \nmid a$. On obtient, par division euclidienne, $a = bq + r$, avec $q \in \mathbb{Z}$ et $r \in [\![0, b]\!]$.
Mais alors $a \wedge b = (bq + r) \wedge b = r \wedge b$, d'après la proposition précédente. On peut donc faire des division euclidiennes successive.
Par définition du reste, la suite des restes est strictement inférieure à $b - k$, où k est le nombre de division euclidienne. Donc le reste sera nul, à un certain rang.
Donc il y a au plus $b + 1$ divisions euclidiennes dans l'algorithme d'Euclide.

En pratique, voici les étapes :

1. On se ramène à des entiers naturels.
2. On retranche au plus grand des deux entiers le plus petit des deux et on recommence jusqu'à ce que l'un des deux entiers soit nul,
   OU
   On remplace le plus grand des deux entiers par le reste de la division euclidienne de celui-ci par le plus petit des deux et on recommence jusqu'à ce que l'un des deux entiers soit nul.
3. L'entier restant (celui qui n'est pas nul) est le PGCD.

En résumé, $a \wedge b$ est le **dernier reste non nul** de la suite des restes successifs .

Exemple 18
Calculons le PGCD de 1789 et 1515 avec l'algorithme d'Euclide.
La première étape est la division euclidienne de 1789 par 1515, soit $1789 = 1 \times 1515 + 274$. On effectue ensuite la division de 1515 par le premier reste 274, soit $1515 = 5 \times 274 + 145$ et on recommence $274 = 1 \times 145 + 129$, puis $145 = 1 \times 129 + 16$, et $129 = 8 \times 16 + 1$, pour obtenir enfin $16 = 16 \times 1 + 0$. Le PGCD est donc le dernier reste non nul 1.

Exemple 19
Calculons le PGCD $1542 \wedge 58$, avec l'algorithme d'Euclide. On a

$$1542 = 26 \times 58 + 34, \quad 58 = 1 \times 34 + 24, \quad 34 = 1 \times 24 + 10, \quad 24 = 2 \times 10 + 4, \quad 10 = 2 \times 4 + 2 \quad \text{et } 4 = 2 \times 2 + 0.$$

Donc $1542 \wedge 58 = 2$ et donc $1542\mathbb{Z} + 58\mathbb{Z} = 2\mathbb{Z}$.

Exemple 20
Soit $n \in \mathbb{Z}$. Calculons le pgcd de $(3n + 1)$ et $(2n + 5)$. On a

$$\begin{aligned}(3n + 1) \wedge (2n + 5) &= ((3n + 1) - (2n + 5)) \wedge (2n + 5) = (n - 4) \wedge (2n + 5) \\ &= (n - 4) \wedge ((2n + 5) - 2(n - 4)) = (n - 4) \wedge 13\end{aligned}$$

Donc $(3n + 1) \wedge (2n + 5) = \begin{cases} 13 & \text{si } n \equiv 4[13] \\ 1 & \text{sinon.} \end{cases}$

Exemple 21
Soit $n \in \mathbb{N}^*$. Calculons les PGCD de $\left(n^2 + n\right) \wedge (2n + 1) = 1$. On a

$$\begin{aligned}&n^2 + n = n(n + 1) \\ &1 \times (2n + 1) - 2 \times n = 1 \text{ donc } (2n + 1) \wedge n = 1 \\ &2 \times (n + 1) - 1 \times (2n + 1) = 1 \text{ donc } (2n + 1) \wedge (n + 1) = 1\end{aligned}$$

Par produit $(2n + 1) \wedge \left(n^2 + n\right) = 1$

Exemple 22
Soit $(F_n)_n$ une suite de Fibonacci définie par ses deux premiers termes et par la relation de récurrence

$$\forall n \in \mathbb{N}, \quad F_{n+2} = F_{n+1} + F_n$$

Les restes successifs de l'algorithme d'Euclide appliqué avec les arguments F_{n+1} et F_n sont les n termes de la suite de Fibonacci d'indices strictement inférieurs à n. En particulier, l'entier $F_{n+1} \wedge F_n$ ne dépend pas de n et se trouve donc être égal à $F_1 \wedge F_0$. Concrètement, pour tout $n \in \mathbb{N}$,

$$F_{n+1} \wedge F_n = F_n \wedge F_{n+1} = F_n \wedge (F_n + F_{n-1}) = F_n \wedge F_{n-1} \ .$$

Ce sont donc les premiers termes de la suite qui décident du PGCD entre 2 termes consécutifs de la suite !

Nombres d'étapes pour l'informatique

Ce dernier calcul peut fournir davantage d'informations. Une récurrence sur n permet de montrer que si l'algorithme d'Euclide pour calculer le PGCD des entiers naturels a et $b > a$ requiert n étapes, alors les minorations $b \geq F_{n+2}$ et $a \geq F_{n+1}$ sont vérifiées.
Un corollaire de ces inégalités est que l'on peut majorer le nombre d'étapes pour calculer le PGCD d'entiers a et b en se ramenant à la suite de Fibonacci connue explicitement. Plus précisément, le théorème de Lamé indique le nombre d'étapes dans l'algorithme d'Euclide pour deux entiers naturels est majoré par cinq fois le nombre de chiffres dans l'écriture décimale du plus petit des deux entiers.

2.4 Nombres premiers entre eux

Définition 5
Deux entiers sont premiers entre eux si leur PGCD est égal à 1 .

⚠ Attention On ne confond pas $a \nmid b$ et $a \wedge b = 1$.
On a seulement $(a \nmid b) \Leftarrow (a \wedge b = 1)$, mais attention, $6 \nmid 9$, mais $6 \wedge 9 = 3 \neq 1$.

Vocabulaire On dit aussi bien que deux entiers a et b sont premiers entre eux ou que a est premier avec b. Remarquons que la notion «d'entiers premiers entre eux» est définie sans avoir recours aux nombres premiers.

Écriture unique d'un nombre rationnel

Tout nombre rationnel a donc une écriture unique de la forme

$$\frac{p}{q} \qquad \text{tel que } (p,q) \in \mathbb{Z} \times \mathbb{N}^* \text{ et } p \wedge q = 1 \ .$$

Exemple 23
La forme unique d'un rationnel s'utilise parfois pour trouver les solutions d'une équation polynomiale sur $\mathbb{Q}$. Montrons, par exemple, que l'équation $x^3 - x^2 + x + 1 = 0$ n'a pas de solutions dans $\mathbb{Q}$.
Par l'absurde, admettons qu'il existe une solution rationnelle $x = p/q$, avec $p \wedge q = 1$ et $q > 0$. Alors, remplaçant x par p/q dans l'équation et multipliant tout par q^3, on obtient

$$p^3 - p^2q + pq^2 + q^3 = 0$$

Puisque $q \mid p^2q + pq^2 + q^3$, on obtient $q \mid p^3$ et donc $q = 1$ puisque p et q sont premiers entre eux. En effectuant le même raisonnement avec p, on obtient $p = \pm 1$. Or 1 et -1 ne sont pas solutions de l'équation. Il y a donc contradiction.

Théorème 1 : Bézout

Deux entiers a et b sont premiers entre eux si, et seulement si, il existe $u, v \in \mathbb{Z}$ tels que

$$ua + vb = 1.$$

Preuve. Le sens direct est une simple conséquence de la définition du PGCD. Pour le sens retour, remarquons que le PGCD divise à la fois a et b donc $ua + vb = 1$; par conséquent, il est égal à 1 . □

Méthode : algorithme d'Euclide étendu

On trouve des entiers u et v satisfaisant cette relation en «remontant» les calculs dans l'algorithme d'Euclide.

Exemple 24

Reprenons l'exemple 18. Essayons de remonter. On avait

$$\begin{aligned}
1789 &= 1 \times 1515 + 274\\
1515 &= 5 \times 274 + 145\\
274 &= 1 \times 145 + 129\\
145 &= 1 \times 129 + 16\\
129 &= 8 \times 16 + 1\\
16 &= 16 \times 1 + 0.
\end{aligned}$$

$$\begin{aligned}
1 &= 94 \times (1789 - 1 \times 1515) - 17 \times 1515 = \underline{94 \times 1789 - 111 \times 1515}\\
&\uparrow_{274=1789-1\times1515}\\
1 &= 9 \times 274 - 17 \times (1515 - 5 \times 274) = 94 \times 274 - 17 \times 1515\\
&\uparrow_{145=1515-5\times274}\\
1 &= 9 \times (274 - 1 \times 145) - 8 \times 145 = 9 \times 274 - 17 \times 145\\
&\uparrow_{129=274-1\times145}\\
1 &= 129 - 8 \times (145 - 1 \times 129) = 9 \times 129 - 8 \times 145\\
&\uparrow_{16=145-1\times129}\\
1 &= 129 - 8 \times 16
\end{aligned}$$

D'où $1 = 94 \times 1789 - 111 \times 1515$.

⚠ Attention (u, v) n'est pas unique !

Méthode : Retrouver tous les coefficients de Bézout

Soit a et b deux entiers premiers entre eux et $u, v \in \mathbb{Z}$ tels que $ua + vb = 1$. Alors, pour tout $k \in \mathbb{Z}$, $(u - kb)a + (v + ka)b = ua + vb + abk - abk = ua + vb = 1$. On peut donc retrouver les autres relations de Bézout et choisir k de sorte à obtenir certaines propriétés (par exemple la positivité) pour l'un des coefficients.

Exemple 25

On a dans l'exemple précédent,
$1 = 94 \times 1789 - 111 \times 1515 = (94 - 1515) \times 1789 - (111 - 1789) \times 1515 = \underline{-1421 \times 1789 + 1678 \times 1515}$,
ce qui nous donne une nouvelle décomposition de Bézout.
On peut bien sûr en obtenir à l'infini : $1 = 94 \times 1789 - 111 \times 1515 = (94 - 1515k) \times 1789 - (111 - 1789k) \times 1515$, pour tout $k \in \mathbb{Z}$. Donc les coefficients de Bézout pour 1789 et 1515 sont les couple (u, v) du produit cartésien

$$(94 - 1515\mathbb{Z}) \times (111 - 1789\mathbb{Z}) = \Big\{(94 - 1515k\ ,\ 111 - 1789k) \mid k \in \mathbb{Z}\Big\}\ .$$

Corollaire 1.1

Soient $a, b, c \in \mathbb{Z}$.

1. *Si $a \wedge b = 1$ et $a \wedge c = 1$, alors $a \wedge (bc) = 1$.*
2. *Si $a \wedge b = 1$, alors $a^p \wedge b^q = 1$ pour tous $p, q \in \mathbb{N}$.*
3. *Si a et b divisent c et $a \wedge b = 1$. Alors, ab divise c.*
4. ***Lemme de Gauss*** *Si a divise bc et $a \wedge b = 1$. Alors a divise c.*

Preuve.

1. D'après le théorème de Bézout, il existe $u, v, u', v' \in \mathbb{Z}$ tels que $ua + vb = 1$, $u'a + v'c = 1$.
   D'où $1 = ua + vb\,(u'a + v'c) = (u + vbu')\,a + (vv')\,bc$.
   D'après le théorème de Bézout, $a \wedge (bc) = 1$.
2. Conséquence de 1.
3. D'après le théorème de Bézout, il existe $u, v \in \mathbb{Z}$ tel que $ua + vb = 1$ donc $uac + vbc = c$. L'entier b divise c donc ab divise ac; de même, ab divise bc. Ainsi, ab divise $uac + vbc = c$.
4. D'après le théorème de Bézout, il existe $u, v \in \mathbb{Z}$ tels que $ua + vb = 1$ donc $uac + vbc = c$. a divise les deux termes du premier membre donc divise c.

□

Exemple 26

On utilise souvent le Lemme de Gauss pour montrer la divisibilité de certains coefficients binomiaux.

Montrons par exemple que $n + 1 \Big| \binom{2n}{n}$.

Tout d'abord, $2 \times (n+1) - 1 \times (2n+1) = 1$ donc $(n+1) \wedge (2n+1) = 1$. De plus, par une formule connue

$$(n+1)\binom{2n+1}{n+1} = (2n+1)\binom{2n}{n} .$$

Puisque $\binom{2n+1}{n+1} \in \mathbb{Z}$, on a $(n+1) \mid (2n+1)\binom{2n}{n}$.

Or $(n+1) \wedge (2n+1) = 1$, donc $(n+1) \mid \binom{2n}{n}$.

Exemple 27

Considérons un polynôme à coefficients entiers de degré n

$$P(X) = \sum_{k=0}^{n} \alpha_k X^k$$

Montrons que si la fraction irréductible $\frac{p}{q}$ est une racine de P, alors p divise α_0 et q divise α_n. En effet,

$$\sum_{k=0}^{n} \alpha_k p^k q^{n-k} = 0$$

soit

$$\alpha_0 q^n = -\sum_{k=1}^{n} \alpha_k p^k q^{n-k}$$

On applique alors le lemme de Gauss : p divise tous les termes $\alpha_k p^k q^{n-k}$ pour $k \geq 1$ donc divise $\alpha_0 q^n$. Or on sait que p est premier avec q donc avec q^n, et p divise α_0.
On procède de même avec q et α_n.
Ce critère permet une recherche facile des racines rationnelles d'un polynôme à coefficients entiers en donnant une

condition nécessaire qui limite à un nombre fini de cas : il suffit ensuite de tester ces quelques valeurs pour vérifier si elles sont racines.
Par exemple, d'après le critère précédent, les racines rationnelles de $X^4-9X^3+13X^2+X+2$ sont parmi $\{-2,-1,1,2\}$; on vérifie rapidement que 2 est la seule racine rationnelle.

Proposition 7 : Lien PGCD-PPCM

Soient $a,b\in\mathbb{Z}$.

$$(a\wedge b)\cdot(a\vee b)=|ab|\ .$$

Preuve. D'après la remarque précédente, $\dfrac{ab}{a\wedge b}=a\dfrac{b}{a\wedge b}=\dfrac{a}{a\wedge b}b$. Donc $a\mid\frac{ab}{a\wedge b}$ et $b\mid\frac{ab}{a\wedge b}$. Donc $\dfrac{ab}{a\wedge b}$ est un multiple commun à a et b.
Soit $m\in a\mathbb{Z}\cap b\mathbb{Z}$. Par définition $m=au=bv$ pour certains $u,v\in\mathbb{Z}$, donc $ua'=vb'$ après division par $a\wedge b\neq 0$. En particulier, $a'\mid vb'$, mais par ailleurs, $a'\wedge b'=1$.
Donc $a'\mid v$ d'après le théorème de Gauss, et on obtient $v=a'k$ pour un certain $k\in\mathbb{Z}$. Finalement, $m=bv=ba'k=k\frac{ab}{a\wedge b}$, , donc $m\in\left(\frac{ab}{a\wedge b}\right)\mathbb{Z}$ et tout multiple commun de a et b et un multiple de $\frac{ab}{a\wedge b}$, d'où

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

□

Exemple 28
Et si on se donnait seulement le PGCD et PPCM de deux nombres $x,y\in\mathbb{Z}$? Trouverait on les nombres x et x ? Par exemple, résolvons dans $\mathbb{N}^2$ le système $\begin{cases}\text{pgcd}(x,y)=5,\\ \text{ppcm}(x,y)=60\ .\end{cases}$
On a d'abord $\text{pgcd}(x,y)=5$, donc $x=5x'$ et $y=5y'$ avec $x'\wedge y'=1$.
On a alors $\text{ppcm}(x,y)=5x'y'=60$ donc $x'y'=12$ d'où

$$(x',y')\in\{(1,12),(2,6),(3,4),(4,3),(6,2),(12,1)\}$$

Les couples $(2,6)$ et $(6,2)$ sont à éliminer car 2 et 6 ne sont pas premiers entre eux. On obtient donc

$$(x,y)\in\{(5,60),(15,20),(20,15),(60,5)\}$$

On vérifie que les solutions fonctionnent. Finalement $\mathcal{S}=\{(5,60),(15,20),(20,15),(60,5)\}$.

Proposition 8 : Nombres premiers entre eux - Divisibilité et congruences

Soient $a_1,a_2,\dots,a_r,b\in\mathbb{Z}$ *et* $n\in\mathbb{N}$.

(1) $a_1b\equiv a_2b[n]$ *et* $b\wedge n=1\implies a_1\equiv a_2[n]$.

(2) *Si chacun des entiers* $a_1,\dots,a_r$ *est premier avec* n, *leur produit* $a_1\dots a_r$ *l'est aussi.*

(3) *Si les entiers* $a_1,\dots,a_r$ *divisent* n *et sont* ***premiers entre eux deux à deux***, *leur produit* $a_1\dots a_r$ *divise* n.

Nombres premiers entre eux dans leur ensemble

⚠ $a_1,a_2,\dots,a_r$ sont premiers entre eux deux à deux n'est pas équivalent à $a_1\wedge\ldots\wedge a_r=1$. On a seulement l'implication directe.
On dit que $a_1,a_2,\dots,a_r$ sont **premiers entre eux deux à deux** si et seulement si $a_i\wedge a_j=1$, pour tout $i,j\in[\![1,r]\!]$, avec $i\neq j$,
et $a_1\wedge\ldots\wedge a_r=1$ si et seulement si $a_1,a_2,\dots,a_r$ sont **premiers entre eux dans leur ensemble**.
Ne pas confondre ces deux expressions ! Par exemple, $6\wedge 3\wedge 8=1$, car ils n'ont que ±1 comme diviseurs communs, mais 6, 3 et 8 sont sont clairement pas premiers entre eux deux à deux.

Exemple 29
Pour démontrer que des entiers sont premiers entre eux, on peut utiliser l'absurde, car on peut utiliser le fait que les deux nombres aient un diviseur premier, ce qui nous facilite la vie !
Par exemple, soit $n \in \mathbb{N}$. Montrons que, pour $i \in \{1, \dots, n+1\}$, les entiers $a_i = i.n! + 1$ sont deux à deux premiers entre eux.
Par l'absurde, supposons que a_i et a_j, avec $i, j \in \{1, \dots, n+1\}$, ne soient pas premiers entre eux. Considérons d un diviseur premier commun à a_i et a_j.
L'entier d est diviseur de $a_i - a_j$ donc de $(i-j) \cdot n!$. Puisque d est premier et diviseur de $i - j$ ou de $n!$, il est nécessairement inférieur à n et donc assurément diviseur de $n!$. Or d divise aussi $a_i = i \cdot n! + 1$ et donc d divise 1. Absurde.

2.5 Utilisation d'un inverse modulo n

Proposition 9
Soit $(a, n) \in \mathbb{Z} \times \mathbb{N} \setminus \{0\}$. Si $a \wedge n = 1$, alors,

$$\exists b \in \mathbb{Z}, ab \equiv 1[n]$$

*b s'appelle **l'inverse de a modulo n**, et peut être trouvé par l'algorithme de Bézout.*

Preuve. Sera démontré en théorie des groupes. □
Cette propriété est très utile pour résoudre les équations du type $ax \equiv c[n]$. Il suffit alors de multiplier par b pour obtenir le résultat.

Exemple 30
Résoudre les équations suivantes d'inconnue $x \in \mathbb{Z}$,

- $2x \equiv 3[125]$
  On a $2 \cdot 63 = 126 = 125 + 1$, donc $2 \cdot 63 = 1$ [125] et on obtient
  $2x \equiv 3[125] \iff 2x \cdot 63 \equiv 3 \cdot 63[125] \iff x \equiv 189[125] \equiv 64[125]$
  $S = \{64 + 125k \mid k \in \mathbb{Z}\}$
- $8x \equiv 4[13]$
  On a $8 \cdot 5 = 40 = 13 \cdots 3 + 1$, donc $8 \cdot 5 = 1$ [13] et on obtient
  $8x \equiv 4[13] \iff 8x \cdot 5 \equiv 4 \cdot 5[13] \iff x \equiv 20[13] \equiv 7[13]$
  $S = \{7 + 13k \mid k \in \mathbb{Z}\}$

Attention Il n'existe pas toujours d'inverse si $a \wedge n \neq 1$!
2 n'a pas d'inverse modulo 6 !

3 Nombres premiers

3.1 Définitions

Définition 6
Un entier $p \in \mathbb{N}\setminus\{0, 1\}$ est premier si les seuls diviseurs positifs de p sont 1 et p.
Donc quatre diviseurs si on n'impose pas la positivité.

Attention L'entier 1 n'est pas un nombre premier.
Il n'y a qu'un seul nombre premier pair : 2 .

Exemple 31
Comment utilise-t-on le fait qu'un nombre est premier.
Soient $a, b \in \mathbb{N}\backslash\{0,1\}$ et $n \in \mathbb{N}$ pair. Montrons que si $a^n + b^n$ est un nombre premier, alors n est une puissance de 2 ou 0.

- Remarquons que si $n = 0$, $a^n + b^n = 2$ est bien premier.
- On peut écrire $n = 2^k(2p+1)$ avec $k, p \in \mathbb{N}$ et l'enjeu est d'établir $p = 0$. Posons $\alpha = a^{2^k}$ et $\beta = b^{2^k}$. On a $a^n + b^n = \alpha^{2p+1} + \beta^{2p+1} = \alpha^{2p+1} - \left(-\beta^{2p+1}\right)$
  On peut alors factoriser par $\alpha - (-\beta) = \alpha + \beta$ et puisque $a^n + b^n$ est un nombre premier, on en déduit que $\alpha + \beta = 1$ ou $\alpha + \beta = a^n + b^n$. Puisque $\alpha, \beta \geq 1$, le cas $\alpha + \beta = 1$ est à exclure et puisque $\alpha \leq a^n$ et $\beta \leq b^n$, le cas $\alpha + \beta = a^n + b^n$ entraîne $\alpha = a^n$ et $\beta = b^n$.
  Puisque $a \geq 2$, l'égalité $\alpha = a^n = \alpha^{2p+1}$ entraîne $p = 0$ et finalement n est une puissance de 2 .

Proposition 10
Soit p un nombre premier. Alors, pour tout entier n, $n \wedge p \in \{1, p\}$.

Preuve. Les seuls diviseurs positifs de p sont 1 et p donc $n \wedge p$ est égal à l'un de ces entiers.
Les entiers sont donc, soit premiers avec p, soit des multiples de p. □

Corollaire 10.1
Pour tout nombre premier p et tout entier $k \in [\![1, p-1]\!]$, p divise $\binom{p}{k}$.

Preuve. En effet, $p\binom{p-1}{k-1} = k\binom{p}{k}$ donc p divise $k\binom{p}{k}$. Par ailleurs, comme k n'est pas un multiple de p, donc p est premier avec k. D'après le théorème de Gauss, p divise $\binom{p}{k}$. □

Proposition 11 : Fermat
Soit p un nombre premier et $n \in \mathbb{Z}$. Alors,

(1) $n^p = n[p]$.

(2) *Si en plus $n \notin p\mathbb{Z}$, alors $n^{p-1} = 1[p]$.*

Preuve. Soit p premier fixé.

(1)
- Pour $n = 1$, le résultat est évident.
- Soit $n \in \mathbb{N}$ tel que $n^p = n[p]$. Alors,

$$\begin{aligned}(n+1)^p &= \sum_{j=0}^{p} \binom{p}{j} n^j = n^p + \sum_{j=1}^{p-1} \binom{p}{j} n^j + 1[p] \\ &= n + 0 + 1[p] \\ &= n + 1[p],\end{aligned}$$

d'après l'hypothèse de récurrence.
On a ainsi établi le résultat pour $n \in \mathbb{N}$. En séparant les cas,
▷ $p = 2$ pour lequel $(-n)^2 = n^2[2] = n[2] = -n[2]$ pour tout $n \in \mathbb{N}$,
▷ p impair pour lequel $(-n)^p = -n^p = -n[p]$ pour tout $n \in \mathbb{N}$, on obtient le résultat pour tout $n \in \mathbb{Z}$.

(2) On a déjà que p divise $n^p - n = n\left(n^{p-1} - 1\right)$. Or, p et n sont premiers entre eux, donc d'après le théorème de Gauss, p divise $n^{p-1} - 1$, soit $n^{p-1} = 1[p]$.

□

Exemple 32
Ce théorème est utile en pratique ! Montrons que si, pour tout entier $n \geq 2$,

$$\forall a \in \{1, \ldots, n-1\}, a^{n-1} \equiv 1 \quad [n] \ , \qquad (*)$$

alors n est un nombre premier.
Mais $(*)$ voudrait dire que tout diviseur tout diviseur commun à a et n est diviseur de $a^{n-1} - 1$ et donc de 1, car

$a \mid a^{n-1}$. Donc, pour tout $a \in \{1, \dots, n-1\}$, $a \wedge n = 1$. D'où n est premier puisque premier avec chaque naturel strictement inférieur à lui-même.

3.2 Théorème fondamental de l'arithmétique

Proposition 12 : Euclide

Soit p un nombre premier et des entiers $a_1, \dots, a_n$. Si p divise $\prod_{k=1}^{n} a_k$, alors il existe $k \in [\![1, n]\!]$ tel que p divise a_k.

Preuve. Raisonnons par l'absurde. Si p ne divise aucun de ces entiers, alors aucun des a_k n'est multiple de p donc le produit n'est pas non plus multiple de p. Absurde □

Proposition 13

Tout entier de valeur absolue supérieure ou égale à 2 admet un diviseur premier.

Preuve. On procède par récurrence forte.

- 2 admet le nombre premier 2 comme diviseur.
- Soit $n \geq 2$. Supposons que le résultat est vrai pour tout entier $k \in [\![2, n]\!]$. Si $n+1$ est premier, alors $n+1$ est un diviseur premier de $n+1$. Sinon, $n+1 = a.b$ avec $a, b \in [\![2, n]\!]$ et on applique l'hypothèse de récurrence à a ou b.

□

Théorème 2

Pour tout entier $n \geq 2$, il existe un entier $m \geq 1$, des nombres premiers $p_1 > \dots > p_m$ et des entiers non nuls $r_1, \dots, r_m$ tels que :

$$n = \prod_{k=1}^{m} p_k^{r_k}$$

Preuve. Un preuve par récurrence forte arrivera à bout du théorème. □

Remarque

Cette décomposition est en fait unique (à l'ordre près des facteurs).

En effet, si $n = \prod_{k=1}^{m} p_k^{r_k} = \prod_{k=1}^{m} p_k^{s_k}$ avec $r_1 < s_1$, alors $p_1^{s_1 - r_1}$ divise $\prod_{k=2}^{m} p_k^{r_k}$ et est premier avec ce nombre. Absurde !

Le nombre d'applications de ce théorème est élevé. C'est notre *bazooka* de l'arithmétique.

Exemple 33

Montrons que si le produit de 2 nombres a et b, premiers entre eux, est un carré parfait, alors a et b sont deux carrés parfaits.

Décomposons a, b et ab en produit de facteurs premiers,

$$a = p_1^{\alpha_1} \dots p_r^{\alpha_r} \quad , \quad b = p_1^{\beta_1} \dots p_r^{\beta_r} \quad \text{et} \quad ab = p_1^{2\gamma_1} \dots p_r^{2\gamma_r} \ .$$

On a utilisé le fait que ab est un carré parfait.

Pour tout j, on a la relation $2\gamma_j = \alpha_j + \beta_j$. De plus, puisque $a \wedge b = 1$, si α_j est non-nul, alors $\beta_j = 0$, et réciproquement.

On a alors $\alpha_j = 2\gamma_j$ et $\beta_j = 0$, ou $\beta_j = 2\gamma_j$ et $\alpha_j = 0$. Dans tous les cas, α_j et β_j sont tous les deux pairs.

Ainsi, a et b sont des carrés parfaits.

Définition 7 : Valuation p-adique

Soit p un nombre premier. La **valuation p-adique** d'un entier n non nul est l'entier $v_p(n)$ défini comme l'exposant de p dans la décomposition de n en facteurs premiers avec, par convention, la valeur 0 si le nombre premier p n'apparaît pas.

Exemple 34
Comme $120 = 2^3 \times 3 \times 5, v_2(120) = 3, v_3(120) = 1, v_5(120) = 1$ et $v_7(120) = 0$.

Proposition 14
Soit p un nombre premier. Soient $m, n \in \mathbb{Z} \setminus \{0\}$ et $k \in \mathbb{N}$.

$v_p(mn) = v_p(m) + v_p(n)$ $\qquad$ $v_p\left(n^k\right) = kv_p(n)$

Exemple 35
Soit $n \in \mathbb{N}$. Montrons que $\sqrt{n} \in \mathbb{Q}$ si, et seulement si, n est le carré d'un entier. Le sens retour est évident. Pour le sens direct, supposons que $\sqrt{n}$ soit égale à la fraction irréductible $\frac{a}{b}$. Alors, $a^2 = nb^2$. En écrivant les décompositions en facteurs premiers de a, b et n, on obtient que, pour tout facteur premier $p, v_p(n) = 2v_p(a) - 2v_p(b)$ est pair. Donc, n est un carré.

Proposition 15
Soient $a, n \in \mathbb{Z}$. Si a est un diviseur de n, on a

$$n = \prod_{k=1}^{m} p_k^{r_k} \quad \Longrightarrow \quad a = \prod_{k=1}^{m} p_k^{\alpha_k} \text{ avec pour tout } k \in [\![1, m]\!], \alpha_k \leq r_k.$$

Donc, pour tout nombre premier p, $v_p(a) \leq v_p(n)$.

Exemple 36
Soient $a, b, c \in \mathbb{N}^*$ et soit $n \in \mathbb{N}^*$. Démontrons que $c|ab \Longrightarrow c|(a \wedge c)(b \wedge c)$.
On écrit les décompositions

$$a = p_1^{\alpha_1} \dots p_r^{\alpha_r}, b = p_1^{\beta_1} \dots p_r^{\beta_r}, c = p_1^{\gamma_1} \dots p_r^{\gamma_r}.$$

La condition $c \mid ab$ signifie que $\gamma_j \leq \alpha_j + \beta_j$ pour tout j. De plus, on a

$$a \wedge c = p_1^{\min(\alpha_1, \gamma_1)} \dots p_r^{\min(\alpha_r, \gamma_r)}$$
$$b \wedge c = p_1^{\min(\beta_1, \gamma_1)} \dots p_r^{\min(\beta_r, \gamma_r)}$$

et donc on a $c \mid (a \wedge c)(b \wedge c)$ si et seulement si, pour tout j de $1, \dots, r$, on a

$$\gamma_j \leq \min(\alpha_j, \gamma_j) + \min(\beta_j, \gamma_j)$$

Mais si $\min(\alpha_j, \gamma_j) = \gamma_j$ ou $\min(\beta_j, \gamma_j) = \gamma_j$, c'est trivial. Sinon on a

$$\min(\alpha_j, \gamma_j) + \min(\beta_j, \gamma_j) = \alpha_j + \beta_j \geq \gamma_j$$

par hypothèse. Ceci prouve le résultat.

Corollaire 15.1
L'entier naturel de décomposition en facteurs premiers $\prod_{k=1}^{m} p_k^{r_k}$ admet exactement $\prod_{k=1}^{m} (r_k + 1)$ diviseurs positifs.

La somme de tous ses diviseurs est

$$\prod_{k=1}^{m} \frac{p_k^{r_k+1} - 1}{p_k - 1}$$

Exemple 37
Les entiers qui admettent un nombre impair de diviseurs positifs sont les carrés d'un entier. En effet, il faut que tous les facteurs $r_k + 1$ soient impairs et donc que les r_k soient pairs.

Exemple 38
Déterminons tous les entiers naturels dont le produit des diviseurs positifs est égal à 45^{42}.
Remarquons d'abord que 45^{42} se décompose en facteurs premiers sous la forme $3^{84}5^{42}$. Ainsi, un entier n dont le produit des diviseurs est égal à 45^{42} est de la forme 3^p5^q, sinon, on aurait un autre facteur premier dans la décomposition de 45^{42}.
Maintenant, les diviseurs d'un tel entier sont tous les nombres de la forme 3^k5^l avec $0 \leq k \leq p$ et $0 \leq l \leq q$. Ainsi, le produit de ces diviseurs est égal à $\prod_{k=0}^{p}\prod_{l=0}^{q} 3^k5^l$ et on veut que cela soit égal à $3^{84}5^{42}$. On a alors

$$v_3\left(\prod_{k=0}^{p}\prod_{l=0}^{q} 3^k5^l\right) = \sum_{k=0}^{p}\sum_{l=0}^{q} v_3\left(3^k5^l\right) = \sum_{k=0}^{p}\sum_{l=0}^{q} k = (q+1)\frac{p(p+1)}{2}$$

et

$$v_5\left(\prod_{k=0}^{p}\prod_{l=0}^{q} 3^k5^l\right) = \sum_{k=0}^{p}\sum_{l=0}^{q} v_5\left(3^k5^l\right) = \sum_{k=0}^{p}\sum_{l=0}^{q} l = (p+1)\frac{q(q+1)}{2}\ .$$

D'où p et q sont donc solutions du système

$$\begin{cases} p(p+1)(q+1) = 168 \\ q(q+1)(p+1) = 84 \end{cases}$$

Si on fait le quotient de ces deux équations, on obtient $p = 2q$, ce qui donne encore

$$q(q+1)(2q+1) = 84$$

La seule solution est $q = 3$ et donc $p = 6$. Ainsi, il y a un unique entier naturel dont le produit des diviseurs est 45^{42}. Il s'agit de 3^65^3.

Corollaire 15.2
Considérons les entiers naturels a, b de décompositions en facteurs premiers

$$a = \prod_{k=1}^{m} p_k^{\alpha_k}, \quad b = \prod_{k=1}^{m} p_k^{\beta_k}.$$

Alors,

$$a \wedge b = \prod_{k=1}^{m} p_k^{\min(\alpha_k,\beta_k)}, \quad a \vee b = \prod_{k=1}^{m} p_k^{\max(\alpha_k,\beta_k)}$$

Autrement dit, pour tout premier p,

$$v_p(a \wedge b) = \min\left(v_p(a), v_p(b)\right) \qquad \text{et} \qquad v_p(a \vee b) = \max\left(v_p(a), v_p(b)\right)\ .$$

Calculs de PGCD et PPCM

Cette proposition ne fournit pas un calcul aussi efficace que l'algorithme d'Euclide pour déterminer le PGCD de deux entiers.

On vérifie grâce à cette propriété que $(a \wedge b) \cdot (a \vee b) = |a \cdot b|$.

Proposition 16
L'ensemble des nombres premiers est infini.

Preuve. Raisonnons par l'absurde. Supposons que l'ensemble des nombres premiers est fini $\{p_1, \dots, p_N\}$. L'entier $\prod_{k=1}^{N} p_k + 1$ n'est divisible par aucun des entiers premiers et donc n'a aucun diviseur premier. Absurde. □

Résultats sur les nombres premiers

C'est une grande part des mathématiques, qui est celle de connaître la répartition des nombres premiers dans l'ensembles des entiers.
On connaît des résultats plus fins sur cet ensemble. Par exemple, $\pi(n)$, le cardinal de l'ensemble des nombres premiers inférieurs à n vérifie :

$$\pi(n) \times \frac{\ln n}{n} \underset{n\to+\infty}{\longrightarrow} 1 \ ,$$

résultat souvent appelé le *Théorème des nombres premiers*, démontré indépendamment par Hadamard et La Vallée Poussin.
Beaucoup de conjectures restent non démontrées à ce jour concernant cette répartition, comme *l'hypothèse de Riemann* ou *l'infinité des nombres premiers jumeaux.*

Exemple 39
Il existe toujours un nombre premier strictement compris entre n et $n! + 2$, pour tout $n \in \mathbb{N}$. *Cela montre autrement que l'ensemble des nombres premiers est infini*
Considérons l'entier $n! + 1$. Celui-ci est divisible par un nombre premier p inférieur à $n! + 1$. Si ce nombre premier p est aussi inférieur à n alors il divise $n!$, car il apparaît comme l'un des facteurs de ce produit, et donc il divise aussi $1 = (n! + 1) - n!$. Ceci est absurde et donc le nombre premier en question est au moins égal à $n + 1$. Finalement, il est strictement compris entre n et $n! + 2$.

Exemple 40
L'ensemble des nombres premiers de la forme $4n - 1$ est infini.

Raisonnons par l'absurde. Supposons que cet ensemble est fini $\{p_1, \dots, p_N\}$. Soit M l'entier $4\prod_{k=1}^{N} p_k - 1$. Tous les nombres premiers, sauf 2, sont impairs, donc ils s'écrivent $4k + 1$ ou $4k - 1$.
Comme $M = -1[4]$, il admet un diviseur premier de la forme $4n_0 - 1$. Mais M est premier avec $p_1, \dots, p_N$, par construction, donc $4n_0 - 1 \in\notin \{p_1, \dots, p_N\}$. Absurde.

4 Systèmes congruentiels

Une **équation diophantienne** est une équation (c'est-à-dire équation à inconnues parmi les entiers) congruentielles d'inconnues x et y. Les autres lettres désignent des entiers paramètres.

Exemple 41
Par définition, l'ensemble des entiers x tels que $x = a[n]$ est $a + n\mathbb{Z}$.

Exemple 42
Notons S l'ensemble des entiers x tels que $ax = b[n]$.

- Si $a \wedge n = 1$, alors il existe $u, v \in \mathbb{Z}$ tels que $ua + vn = 1$ et $S = bu + n\mathbb{Z}$.
- Si $a \wedge n \neq 1$, alors
- si $a \wedge n \mid b$, alors, on divise par $a \wedge n$ et on se ramène au cas précédent.
- sinon, $S = \varnothing$.

4.1 Cas des modulos premiers entre eux

Notons S l'ensemble des entiers x solutions de $\left\{\begin{array}{ll} x & = a[p] \\ x & = b[q] \end{array}\right.$ avec $p \wedge q = 1$.
D'après le théorème de Bézout, il existe $u, v \in \mathbb{Z}$ tels que $up + vq = 1$. L'entier $avq + bup$ est alors solution du système et on en déduit que l'ensemble des solutions est : $S = avq + bup + pq\mathbb{Z}$.
On remarque, en particulier, qu'il n'y a qu'une solution dans $[\![0, pq-1]\!]$. Pour résoudre un système congruentiel de plus de deux équations, on regroupe les équations deux par deux.

4.2 Cas général

Pour résoudre le système diophantien $\left\{\begin{array}{ll} x & = a[m] \\ x & = b[n] \end{array}\right.$ avec des entiers $m = \prod_i p_i^{m_i}$ et $n = \prod_i p_i^{n_i}$ non nécessairement premiers entre eux donnés par leurs décompositions en facteurs premiers, on utilise le protocole suivant:

(1) on se ramène à des «modulos » deux à deux premiers entre eux en écrivant chacune des équations sous la forme du système correspondant :

$$\left\{\begin{array}{ll} x & = a\left[p_1^{m_1}\right] \\ x & = a\left[p_2^{m_2}\right] \\ & \vdots \end{array}\right., \quad \left\{\begin{array}{l} x = \\ x = \\ \vdots \\ b\left[p_2^{n_1}\right] \\ \vdots \end{array}\right.$$

(2) on étudie, pour tout i, le système composé des deux équations correspondant au même facteur premier

$$\left\{\begin{array}{l} x = a\left[p_i^{m_i}\right] \\ x = b\left[p_i^{n_i}\right] \end{array}\right.$$

On obtient l'aternative suivante: soit le système n'admet pas de solution, soit les solutions forment une classe de congruence modulo $p_i^{\max(m_i, n_i)}$.

(3) On conclut comme précédemment. Le résultat obtenu est alors une classe modulo $m \vee n$.

Remarque

Dans la deuxième étape, on a utilisé que si $x = b\,[p^n]$, alors $x = b\,[p^m]$ pour tout $m \leq n$ ce qui est élémentaire en réécrivant la définition de congruence. Pour le dire en d'autres termes, une classe modulo p^m pour $m \leq n$ est une réunion de classes modulo p^n.

Exemple 43

Le système $\left\{\begin{array}{ll} x & = 17[28] \\ x & = 3[98] \end{array}\right.$ est équivalent à

$$\left\{\begin{array}{lll} x & = 17\left[2^2\right] & = 1\left[2^2\right] \\ x & = 17[7] & = 3[7] \\ x & = 3[2] & = 1[2] \\ x & = 3\left[7^2\right] & = 3\left[7^2\right] \end{array}\right.$$

qui équivaut, à son tour, à

$$\left\{\begin{array}{l} x = 1\left[2^2\right] \\ x = 3\left[7^2\right] \end{array}\right.$$

Comme $-12.2^2 + 1.7^2 = 1$, les solutions sont d'après le point précédent, $101 + 196\mathbb{Z}$.

Exemple 44

Le système $\begin{cases} x = 7[12] \\ x = 5[15] \end{cases}$ est équivalent à

$$\begin{cases} x = 7[4] & = 3[4] \\ x = 7[3] & = 1[3] \\ x = 5[3] & = 2[3] \\ x = 5[5] & = 0[5] \end{cases}$$

Il n'y a pas de solutions car les deuxième et troisième équations ne sont pas compatibles.