Chapitre

III Arithmétique, rudiments

L'arithmétique concerne l'étude des entiers naturels $\mathbb{N}$ ou relatifs $\mathbb{Z}$. Pourquoi $\mathbb{Z}$? Tout simplement car $\mathbb{Q}$ et $\mathbb{R}$ sont des corps trop grands et possédant trop de propriétés. Redescendre dans $\mathbb{Z}$ permettra donc de mieux discerner celles-ci et de mieux comprendre le lien entre la multiplication et l'addition.

Voyez donc les quelques lignes trops brèves qui vont suivre comme un retour aux origines des mathématiques, un retour en classe primaire mais avec la maturité d'un élève de prépa. Vos chères tables de multiplication, par exemple, apprises il y a longtemps vont ainsi prendre un peu de relief.

On commencera par accentuer notre compréhension de la relation de divisibilité. Quelques propriétés dégagées, nous nous intéresserons aux nombres *premiers*. Alors que leur définition semble ne receler aucun mystère, on échoue à trouver une régularité quelconque dans leur succession. Connus dès les débuts de l'arithmétique, les nombres premiers ont excité la curiosité de milliers de mathématiciens.

Ils sont au cœur de la science des nombres, car tout entier se décompose de façon unique en un produit de facteurs premiers. Ils sont aussi à l'origine de certains des problèmes les plus difficiles des mathématiques et ont acquis, avec les progrès de la cryptographie, une importance économique considérable.

La reconnaissance des nombres premiers et des nombres composés avec leur décomposition en facteurs premiers est connue pour être des plus importants et utiles en arithmétique.

Il a tant impliqué le zèle et la sagesse des géomètres anciens comme modernes qu'il serait superflu d'en discuter plus avant...

En plus, la dignité des sciences mêmes semble exiger que tous les moyens possibles soient explorés pour trouver la solution d'un problème si élégant et si célébré.

Karl Friedrich Gauss,

Disquisitiones Arithmeticae, 1801

À l'heure où j'écris ces pages, le plus grand nombre premier connu est $2^{82\ 589\ 933} - 1$ obtenu par Patrick Laroche dans le cadre du programme GIMPS et trouvé le 7 décembre 2018. Écrit en base 10, ce nombre comporte 24 862 048 chiffres, soit près d'un million de chiffres supplémentaires par rapport à l'ancien record qui datait de janvier 2018 .

Commençons !

CONTENU

I/ Rudiments d'arithmétique dans $\mathbb{N}$ et $\mathbb{Z}$

I.1 Divisibilité

Définition 1 (Divisibilité dans $\mathbb{Z}$) : Soient a et b des entiers relatifs.

On dit que a *divise* b, noté $a|b$, s'il existe un entier relatif k tel que $b = ka$.

On dit alors que :

— a est *un diviseur* de b. On note $\mathscr{D}(b)$ leur ensemble.
— b est *un multiple* de a. On note $a\mathbb{Z}$ leur ensemble.

Comme a et $-a$ ont les mêmes diviseurs dans $\mathbb{Z}$, on se restreindra le plus souvent, sans le dire, à l'étude de la divisibilité dans $\mathbb{N}$. C'est le parti pris par le programme donc, à partir de maintenant, sauf remarques intéressantes, on ne considèrera plus que la divisibilité dans $\mathbb{N}$.

Exemples 1 :

— $3|12$ et $5\not|12$.
— L'ensemble des diviseurs de 12 est $\mathscr{D}(12) = \{1, 2, 3, 4, 6, 12\}$.
— Tous les nombres divisent 0 *i.e.* 0 est multiple de tout entier : $\mathscr{D}(0) = \mathbb{N}$.
— 0 n'est diviseur d'aucun entier (non nul) : $0\mathbb{Z} = \{0\}$.

— $a|b \iff b\mathbb{Z} \subset a\mathbb{Z}$.

— Un multiple de 2 est aussi appelé un *nombre pair*. Ceux qui ne le sont pas sont appelés *nombre impair*. L'ensemble des nombres pairs est noté $2\mathbb{N}$. (*cf* le corollaire (2.1) pour les nombres impairs)

Exercice 1 : On appelle *nombre parfait* tout nombre égal à la somme de ses diviseurs stricts.

Par exemple $\mathscr{D}(6) = \{1, 2, 3, 6\}$ et $6 = 1 + 2 + 3$, donc 6 est parfait.

Montrer que 28 est parfait.

Méthode 1 :
Pour les problèmes donnés sous forme additive, on essaiera de se ramener à une forme multiplicative du type $A \times B = C$, où on connaît les diviseurs de C.

Exercice 2 : Déterminer les couples $(x\,;y)$ d'entiers naturels qui vérifient $x^2 = y^2 + 21$.

Proposition 1 (Relation de divisibilité) :

1. $\forall\, a \in \mathbb{N}, \quad a|a$ et $1|a$. ($\ll\, a|b\,\gg$ est réflexive)
2. $\forall\, a, b \in \mathbb{N}, \quad \begin{cases} a|b \\ b|a \end{cases} \implies a = b.$ ($\ll\, a|b\,\gg$ est antisymétrique sur $\mathbb{N}$)
3. $\forall\, a, b, c \in \mathbb{N}, \quad \begin{cases} a|b \\ b|c \end{cases} \implies a|c.$ ($\ll\, a|b\,\gg$ est transitive)

La relation « $a\mathscr{R}b \iff a|b$ », réflexive, antisymétrique et transitive est appelée une relation d'ordre sur $\mathbb{N}$. C'est un ordre non total.

ATTENTION

Sur $\mathbb{Z}$, la relation $a|b$ est seulement réflexive et transitive.

On perd l'antisymétrie :

$$\forall\, a, b \in \mathbb{Z}, \quad \begin{cases} a|b \\ b|a \end{cases} \iff |a| = |b|\,.$$

Preuve :

1. $a = a \times 1$, donc $1|a$ et $a|a$.
2. Si $b = ak$ et si $a = bl$ pour deux entiers k et l alors $b = bkl$.
   - Si $b = 0$ alors $a = bl = 0$ donc $|a| = |b|$.
   - Si $b \neq 0$ alors $kl = 1 \iff k = l = 1$ ou $k = l = -1$ *i.e.* $a = b$ ou $a = -b$ ou encore $|a| = |b|$.
3. Si a divise b, alors il existe k entier tel que $b = ka$.

   Si b divise c, alors il existe k' entier tel que $c = k'b$.

   Alors $c = k'b = k'(ka) = (k'k)a$ où $k'k \in \mathbb{Z}$, donc a divise c.

Proposition 2 (Compatibilité) :

1. $\begin{matrix} \forall\, a, b, c \in \mathbb{N} \\ \forall\, m, n \in \mathbb{N} \end{matrix}$, $\begin{cases} a|b \\ a|c \end{cases} \implies a|mb + nc$ (« $a|b$ » est compatible avec les combinaisons linéaires entières)
2. $\forall\, a, b, a', b', c \in \mathbb{N}, \quad \begin{cases} a|b \\ a'|b' \end{cases} \implies a|bc$ et $aa'|bb'$ (« $a|b$ » est compatible avec le produit)

   En particulier, $\forall\, a, b, n \in \mathbb{N}, \quad a|b \implies a^n|b^n$

Preuve :

1. Si a divise b et c alors il existe des entiers k et l tels que $b = ka$ et $c = la$.

   Alors, pour tout entier m et n, $mb + nc = \underbrace{(mk + nl)}_{\in\mathbb{N}} a$ *i.e.* a divise $mb + nc$.

2. De même, si $b = ka$ et $b' = la'$ pour deux entiers k et l alors $bc = kac$ et $bb' = \underbrace{(kl)}_{\in\mathbb{N}} aa'$ *i.e.* a divise bc et aa' divise bb'.

ATTENTION

- $\begin{cases} a|c \\ b|c \end{cases} \not\Longrightarrow ab|c$:

  $2|12$ et $4|12$ mais $2 \times 4 = 8 \not| 12$.

- $a|bc \not\Longrightarrow a|b$:

  $10|210 = 14 \times 15$ mais $10 \not| 14$.

  (et $10 \not| 15$)

Exemple 2 : Si $a \in \mathbb{Z}$ divise $3n + 2$ et $n - 3$ alors $a|11$.

En effet, a divise alors $(3n + 2) - 3(n - 3) = 11$.

Exercice 3 : Trouver les entiers n pour lesquels $\dfrac{n + 15}{n + 2}$ est entier.

Correction : On simplifie d'abord un peu et on isole la variable n :

$n + 15 = n + 2 + 13$ donc $\dfrac{n + 15}{n + 2} = \dfrac{(n + 2) + 13}{n + 2} = 1 + \dfrac{13}{n + 2}$.

Le problème s'énonce alors de façon plus simple :

$$\frac{n + 15}{n + 2} \in \mathbb{Z} \iff \frac{13}{n + 2} \in \mathbb{Z},$$

c'est-à-dire si, et seulement si $n + 2$ est un diviseur de 13.

Les diviseurs de 13 sont -13, -1, 1 et 13. Il y a donc 4 équations à résoudre ($n + 2 = -13$, $n + 2 = ...$).

On obtient : $\mathscr{S} = \{-15;\ -3;\ -1;\ 11\}$.

D'une manière générale,

Méthode 2 :
Pour résoudre un problème du type $f(n)|g(n)$, on se ramène à un problème du type $h(n)|A$ où A est un entier *indépendant* de n. [1]

- On pourra développer une fraction en éléments simples comme à l' exercice (3) .
- On pourra aussi utiliser la *propriété (1.3)* pour rendre le dividende indépendant de n.

[1]. En d'autres termes, on isole la variable.

Corollaire 2.1 :
Les nombres impairs sont exactement les entiers de la forme $2p+1$ où $p \in \mathbb{Z}$.

Preuve : Il y a deux choses à prouver.

1. Tout nombre de la forme $2p+1$ où $p \in \mathbb{Z}$ est impair.

   En effet, $2|2p$ mais 2 ne divise pas 1, donc $2p+1$ n'est pas divisible par 2, donc est impair.
2. Tout nombre impair m s'écrit sous la forme $2p+1$ où $p \in \mathbb{Z}$ *i.e.* $m-1=2p$ est pair.

   Par l'absurde, supposons qu'il existe un nombre impair positif m tel que $m-1$ n'est pas pair.

   On note encore m le plus petit entier naturel vérifiant cette propriété et on va prouver qu'en fait $m-1$ vérifie aussi cette propriété.

   Observons que comme $2|(-2)$ alors $2|m$ est équivalent à ce que $2|(m-2)$.

   Or, par hypothèse m est impair *i.e.* 2 ne divise pas m. On obtient alors $m-2$ impair d'après l'observation précédente.

   Mais, par définition de m, $m-1$ est aussi un nombre impair qui, si on lui retranche 1, donne un nombre impair $m-2$.

   Ceci contredit que m est le plus petit impair vérifiant cette propriété.

   Ainsi tout nombre impair positif q est tel que $q-1$ soit pair *i.e.* $q-1=2p \iff q=2p+1$.

   Le raisonnement est identique avec les entiers relatifs négatifs en prenant un nombre impair m tel que $m+1$ ne soit pas pair.

Exercice 4 : Montrer que pour tout entier impair n, n^2-1 est multiple de 8.

I.2 Division euclidienne

Théorème 3 :
Pour tout $(a,b) \in \mathbb{N} \times \mathbb{N}^*$, il existe un unique couple $(q,r) \in \mathbb{N}^2$ tel que :

$$a = bq + r \quad \text{et} \quad 0 \leqslant r < b. \tag{III.1}$$

Lorsqu'on a obtenu cette écriture, on dit qu'on a effectué la *division euclidienne* de a par b.

Anodins en première lecture, les mots les plus importants de ce théorème sont « unique » et le symbole « $<$ ». Prêtez-y attention !

Rappel 1 (Vocabulaire) :

- q s'appelle le *quotient*,
- r s'appelle le *reste*,
- a s'appelle le *dividende*
- et b s'appelle le *diviseur*.

Preuve :

Existence :

Sans la partie entière :

1. Premier cas : Si $0 \leqslant a < b$ alors le couple $(q\,;r) = (0\,;a)$ convient.
2. Second cas : Si $a = b$ alors le couple $(1\,;a)$ convient.
3. Troisième cas : Supposons que $a > b$. En particulier, a et b sont donc tous deux strictement positifs.

   On note $\mathscr{M}(b)$ l'ensemble des multiples positifs de b inférieurs ou égaux à a :

   $$\mathscr{M}(b) = \{k \in \mathbb{N} \,/\, kb \leqslant a\}.$$

   $1 \in \mathscr{M}(b)$ donc $\mathscr{M}(b)$ une partie de $\mathbb{N}$, non vide et majorée. Elle admet donc un plus grand élément que l'on note q *i.e.* $qb \leqslant a$ avec $q+1 \notin \mathscr{M}(b)$ *i.e.* $(q+1)b > a$.

   On a donc :

   $$qb \leqslant a < (q+1)b. \tag{III.2}$$

   Posons alors $r = a - bq \in \mathbb{Z}$. D'après (III.2), on a alors :

   $$\begin{array}{rccl} \cancel{qb} - \cancel{qb} \leqslant & a - bq & < (\cancel{q} + 1)b - \cancel{bq} \\ 0 \leqslant & r & < b. \end{array}$$

Conclusion, dans tous les cas, il existe un couple $(q\,;r)$ vérifiant la relation (III.1).

Avec la partie entière : Tout repose sur les propriétés de la partie entière et l'inégalité stricte.

On pose $q = \left\lfloor \dfrac{a}{b} \right\rfloor$.

Par définition de la partie entière, $q \leqslant \dfrac{a}{b} < q+1$ d'où :

$$bq \leqslant a < bq + b \tag{III.3}$$

En posant, $r = a - bq$, on a bien $a = bq + r$.

D'après (III.3), on a aussi $0 \leqslant r < b$.

Unicité : Supposons qu'on ait $(q, r) \in \mathbb{N}^2$ et $(q', r') \in \mathbb{N}^2$ tels que : $\begin{cases} a = bq + r \\ 0 \leqslant r < b \end{cases}$ et $\begin{cases} a = bq' + r' \\ 0 \leqslant r' < b \end{cases}$.

On a donc $bq + r = bq' + r'$, *i.e.* $b(q - q') = r' - r$. Or $-b < r' - r < b$, d'où $-b < b(q - q') < b$ puis $-1 < q - q' < 1$.

Or, $q - q'$ est entier.

Donc, $q - q' = 0$ et $q = q'$. Enfin, $r = r'$.

Remarques :

— On peut étendre le théorème au cas où a est entier (relatif) et b entier non nul : $a = bq + r$, avec $0 \leqslant r < |b|$.

— Posant $q = \left\lfloor \frac{a}{b} \right\rfloor$, la division euclidienne doit plutôt être vue comme la recherche du plus grand multiple de b inférieur à a que comme un calcul de division.

Combien de fois peut-on soustraire 7 de 83 et combien reste-t-il ?

Réponse : autant de fois que l'on veut et il reste 76 à chaque fois.

Exercice 5 : Montrer que tout entier n non divisible par 5 a un carré de la forme $5p + 1$ ou $5p - 1$.

Proposition 4 :
Soient a et b deux entiers naturels avec b non nul.

$$b|a \iff \text{le reste dans la division euclidienne de } a \text{ par } b \text{ est nul.}$$

Remarque : En Python, le reste de la division euclidienne de a par b est obtenu par $a\%b$.

Preuve :

$\Longrightarrow$: Si b divise a, alors il existe $q \in \mathbb{N}$ tel que $a = bq + 0$.

Par unicité dans la division euclidienne, on en déduit que le reste de la division euclidienne de a par b est égal à 0.

$\Longleftarrow$: Supposons que le reste de la division euclidienne de a par b soit nul. Alors il existe q tel que $a = bq$ *i.e.* b divise a.

Exercice 6 : Le 1er mai 2022 tombait un dimanche. Quel jour tombe le 1er mai 2023 ?

I.3 Nombres premiers

Définition 2 : Un entier naturel est dit *premier* lorsqu'il admet exactement deux diviseurs (1 et lui-même).

On note $\mathbb{P}$ l'ensemble des nombres premiers.

Exemples 3 :

— $0 \notin \mathbb{P}$: il admet une infinité de diviseurs.

— $1 \notin \mathbb{P}$: il n'admet qu'un seul diviseur.

— $2 \in \mathbb{P}$: c'est le plus petit nombre premier, et il est pair. C'est le seul nombre premier pair.

— $2^{82\,589\,933} - 1$, qui comporte près de 25 millions de chiffres en écriture décimale est le plus grand nombre premier actuellement connu.

Il a été découvert le 7 décembre 2018 par le *Gimps* (Great Internet Mersenne Prime search)

— Une curiosité et un jeu des siècles passés, le polynôme $P(n) = n^2 - n + 41$ associé à Euler donne des nombres premiers pour n prenant les valeurs 0 à 39 mais $P(40) = 1681 = 41^2$!

Un mathématicien, un physicien, un informaticien et un littéraire sont devant un problème : montrer que tous les nombres impairs sont premiers.

Le mathématicien dit : « 3 est premier, 5 est premier, 7 est premier, 9 n'est pas premier, donc ça ne marche pas ».

Le physicien dit : « 3 est premier, 5 est premier, 7 est premier, donc en première approximation, ça marche ».

L'informaticien dit : « 3 est premier, 5 est premier, 7 est premier, 9 n'est pas premier, 9 n'est pas premier, 9 n'est pas premier, 9 n'est pas premier, …».

Le littéraire dit : « C'est quoi, un nombre premier ? ».

Théorème 5 (Critère d'arrêt) :

— Tout entier naturel n, $n \geqslant 2$, admet un diviseur premier.

— Si n n'est pas premier, alors il admet un diviseur premier p tel que :

$$2 \leqslant p \leqslant \sqrt{n}.$$

Preuve :

— Si n est premier, il admet donc un diviseur premier : lui-même.

— Sinon, l'ensemble des diviseurs d de n tel que $2 \leqslant d \leqslant n$ n'est pas vide (il contient n). Il admet donc un plus petit élément p. Si p n'était pas premier, il admettrait un diviseur strict d' tel que $2 \leqslant d' < p$ qui diviserait n. Ceci contredirait la définition de p.

Donc p est premier.

— On a donc p premier et $n = p \times q$ avec $p \leqslant q$. En multipliant cette inégalité par p, on obtient :

$$p^2 \leqslant pq = n \iff p \leqslant \sqrt{n}.$$

Exemple 4 (Comment montrer que 109 est un nombre premier) :

— On a $10 < \sqrt{109} < 11$.

On teste donc tous les nombres premiers strictement inférieurs à 11, soit : 2, 3, 5 et 7.

— Des règles de divisibilité, on déduit que 109 n'est divisible ni par 2, ni par 3, ni par 5.

— Soit, on se rappelle le critère de divisibilité par 7, soit on effectue la division euclidienne de 109 par 7, on obtient :

$$109 = 7 \times 15 + 4 \implies 109 \text{ n'est pas divisible par } 7.$$

— Conclusion : comme 109 n'est pas divisible par 2, 3, 5, et 7, il est premier.

Théorème 6 :
L'ensemble des nombres premiers est infini.

Preuve : Supposons le contraire *i.e.* qu'il existe un nombre fini de nombres premiers que l'on va noter p_1, p_2, ..., p_n et posons

$$\mathrm{N} = p_1 \times p_2 \times ... \times p_n + 1.$$

L'objectif de la cette démonstration [2] est de prouver que N est premier. Comme il est strictement plus grand que les p_i, on aura notre contradiction.

Si N est premier, la contradiction est déjà toute trouvée. Sinon, d'après le critère d'arrêt, N admet un diviseur premier. Soit p_i ce diviseur premier.

Par définition p_i divise donc $p_1 \times p_2 \times ... \times p_n$ et N donc divise aussi $\mathrm{N} - p_1 \times p_2 \times ... \times p_n = 1$.

Ceci est impossible, donc l'hypothèse qu'il existe un nombre fini de nombres premiers est absurde.

Crible d'Ératosthène :

Pour dresser la liste des nombres premiers entre 2 et 150, la méthode du crible d'Ératosthène [a] consiste à :

1. Écrire la liste des nombres entiers de 2 à 100.
2. Éliminer successivement les multiples propres de 2, de 3, ..., puis ceux de p, où p est le premier nombre non encore éliminé [b], etc...

a. **Ératosthène**, mathématicien, géographe, astronome et poète grec serait né en 276 avant J.C. à Cyrène (aujourd'hui en Libye). Il étudie quelques années à Athènes puis devient l'élève du poète grec Callimaque qui dirige la grande Bibliothèque d'Alexandrie.

Ayant ainsi accès à toutes les connaissances de l'époque, Ératosthène se lance dans différents travaux qui le rendront célèbre :

- En observant la position du Soleil à Syène (Assouan aujourd'hui) puis à Alexandrie au moment du solstice d'été, il parvient à déduire avec une bonne précision la circonférence de la Terre.
- Inventeur du mot géographie, il étudie les différentes zones climatiques, les altitudes des montagnes, la répartition des continents et des océans.
- Passionné d'astronomie, il réalise un catalogue de plus de 600 étoiles et 44 constellations. Il parvient aussi à calculer l'obliquité de l'écliptique (l'inclinaison de l'axe de la Terre par rapport à son axe de rotation autour du Soleil) avec une bonne précision.
- En mathématiques il invente un procédé (le crible d'Ératosthène) permettant de trouver les nombres premiers.

Devenu aveugle, Eratosthène se laisse mourir de faim en l'an 194 av. J-C.

b. donc premier

[2]. Connue d'Euclide himself !

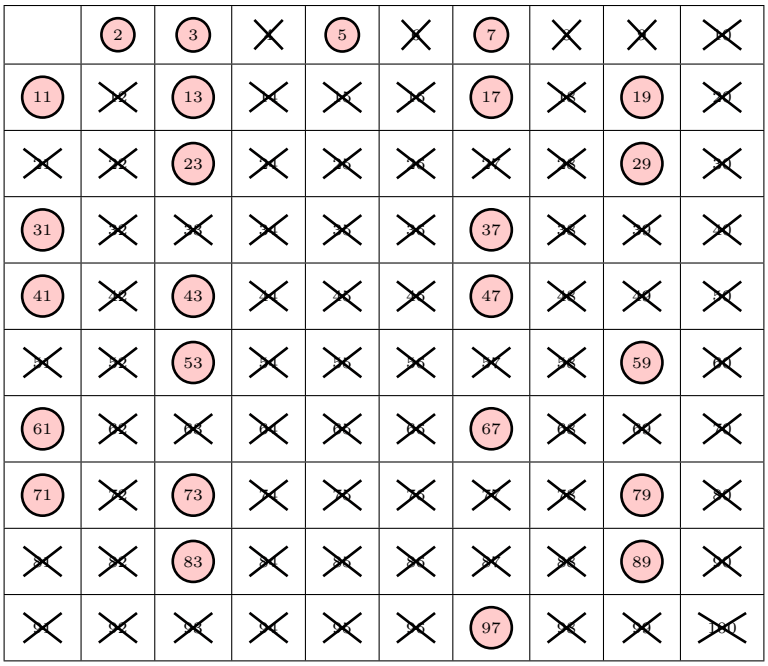


Figure III.1 – Les nombres premiers inférieurs à 100.

Les entiers barrés sont les entiers non premiers entre 2 et 100. Les entiers restant (en rouge) sont donc les nombres premiers inférieur à 100.

```python
def eratosthene(n):
    L = [ i for i in range(2,n+1) ]
    P = [ ]

    while len(L) != 0:
        P.append(L[0])
        i = L[0]
        for k in L:
            if k % i == 0:
                del(L[L.index(k)])

    return P
```

Figure III.2 – Crible d'Ératothène

Remarques :

— Pour éliminer les multiples propres de 7, commencer à 7^2, car les multiples inférieurs ont déjà été éliminés.

— D'après le théorème (5), il est possible de savoir à l'avance « jusqu'où aller ». En effet, tout entier composé n admet un diviseur premier p tel que : $2 \leqslant p \leqslant \sqrt{n}$.

Si $n \leqslant 150$, alors $12 < \sqrt{n} < 13$. Il suffira donc de tester au plus jusqu'aux multiples de 12 [3] et de les barrer, le cas échéant.

[3]. Plutôt 11 car les multiples de 12 seront déjà barrés en tant que multiples de 2 ou de 3.

```python
def isitPrime(k):
    if k==2 or k==3: return True
    if k%2==0 or k<2: return False
    for i in range(3, int(k**0.5)+1, 2):
        if k%i==0:
            return False

    return True
```

Figure III.3 – Algorithme optimisé testant la primalité d'un nombre : Sachant, qu'hormis 2 et 3, les nombres premiers peuvent s'écrire $6n \pm 1$, vérifier la divisibilité du nombre donné avec 2 et 3, puis vérifier chaque nombre qui a la forme $6n \pm 1$ est une solution plus efficace que tester chaque entier.

Un peu d'histoire : *En mathématiques, et plus précisément en théorie analytique des nombres, le théorème des nombres premiers, démontré indépendamment par Hadamard et La Vallée Poussin en 1896, est un résultat concernant la distribution asymptotique des nombres premiers.*

Théorème 7 :
La fonction π qui à un réel x associe $\mathcal{P}(x)$ le nombre de nombres premiers inférieurs ou égaux à x, est équivalente lorsque x tend vers $+\infty$, au quotient de x par son logarithme népérien :

$$\pi(x) \underset{x\to+\infty}{\sim} \frac{x}{\ln(x)}.$$

— *Le théorème des nombres premiers a été conjecturé dans la marge d'une table de logarithmes par Gauss en 1792 ou 1793 alors qu'il avait seulement 15 ou 16 ans (selon ses propres affirmations ultérieures) et par Adrien-Marie Legendre (ébauche en l'An VI du calendrier républicain, soit 1797-1798, conjecture précise en 1808).*

— *Le Russe Pafnouti Tchebychev a établi en 1851 que si x est assez grand, $\mathcal{P}(x)$ est compris entre $\dfrac{0,92129x}{\ln(x)}$ et $\dfrac{1,10556x}{\ln(x)}$.*

— *Le théorème a finalement été démontré indépendamment par Hadamard et La Vallée Poussin en 1896 à l'aide de méthodes d'analyse complexe, utilisant en particulier la fonction ζ de Riemann.*

— *Un approximant de $\pi(x)$ nettement meilleur que $\dfrac{x}{\ln(x)}$ est la fonction logarithme intégral*

$$li(x) = \int_0^x \frac{\mathrm{d}t}{\ln(t)}$$

ou sa variante, la fonction d'écart logarithmique intégrale

$$Li(x) = li(x) - li(2) = \int_2^x \frac{\mathrm{d}t}{\ln(t)}$$

$$\pi(x) \underset{x\to+\infty}{\sim} li(x) \underset{x\to+\infty}{\sim} Li(x).$$

— *En 1899, La Vallée Poussin a affiné son résultat en montrant que :*

$$\pi(x) \underset{x\to+\infty}{=} li(x) + \mathrm{O}\left(x\,\mathrm{e}^{-\sqrt{\frac{\ln(x)}{2\mathrm{V}}}}\right),$$

pour une certaine constante V.

Landau (en 1909) puis bien d'autres ont travaillé à réduire la taille admissible de cette constante V.

— *L'hypothèse de Riemann est même équivalente à l'estimation* $\pi(x) \underset{x\to+\infty}{=} li(x) + \mathrm{O}\left(\sqrt{x}\ln(x)\right)$. *Surprenant ! Magnifique ! et pourtant encore si loin ...*

Il y aurait encore beaucoup beaucoup à dire mais je m'arrête là et j'encourage les curieux à faire des recherches à partir des mots clés « théorème des nombres premiers ».

Exercice 7 : Soit $n \in \mathbb{N}$. On suppose $n \geqslant 2$.

Montrer qu'il n'existe aucun nombre premier entre $n! + 2$ et $n! + n$.

Correction : Par construction, $\forall\, k \in [\![2, n]\!], \quad k | n!$.

Donc $\forall\, k \in [\![2, n]\!], \quad k | n! + k$.

D'où $\forall\, k \in [\![2, n]\!], \quad n! + k \notin \mathbb{P}$.

Remarque : Il y a donc des « trous » aussi grands qu'on veut dans l'ensemble des nombres premiers.

Théorème 8 (Théorème fondamental de l'arithmétique) :
Tout entier n supérieur à 2 admet une et une seule (à l'ordre des facteurs près) décomposition en facteurs premiers.

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}, \text{ avec } p_i \in \mathbb{P} \text{ deux à deux distincts et } \alpha_i \in \mathbb{N}^*.$$

On l'appelle *décomposition primaire* de n et les exposants α_i s'appellent les valuations associées aux nombres premiers p_i.

Remarque : Le programme de PTSI spécifie que la démonstration est hors-programme mais pas le résultat qui est à connaître.

Preuve : Pour tout entier $n \geqslant 2$, posons :

$$\mathrm{H}(n) : \text{« L'entier } n \text{ peut s'écrire sous la forme d'un produit de nombres premiers. »}$$

On va démontrer cette propriété par une récurrence forte.

Comme 2 est premier, il peut s'écrire comme le produit de lui-même et $\mathrm{H}(2)$ est vérifiée.

Supposons alors que $\mathrm{H}(k)$ soit vérifiée pour tout entier k tel que $2 \leqslant k \leqslant n$ et considérons l'entier $n+1$:

— Si $n+1$ est premier, $\mathrm{H}(n+1)$ est vraie.

— Si $n+1$ n'est pas premier alors il admet un diviseur premier p et on a $n = p \times m$ où m est un entier tel que $2 \leqslant m \leqslant n$.

Il suffit alors d'appliquer l'hypothèse de récurrence à m pour avoir l'existence de la décomposition et la propriété $\mathrm{H}(n+1)$.

En conclusion, la propriété $\mathrm{H}(n)$ est donc héréditaire. Étant initialisée pour $n = 2$, elle est vraie pour tout entier $n \geqslant 2$.

Pour montrer l'unicité, on aura besoin d'un lemme qui est une application immédiate du théorème de Gauss (Hors-programme aussi) :

Lemme 1 :
Un nombre premier divise un produit si, et seulement si il divise l'un des facteurs du produit.

ATTENTION $4 | (14 \times 10)$ mais 4 ne divise ni 14, ni 10.

Comme toujours, supposons l'existence d'une autre décomposition :

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k} = q_1^{\beta_1} q_2^{\beta_2} \cdots q_l^{\beta_l}.$$

— p_1 premier divise $q_1^{\beta_1} q_2^{\beta_2} \cdots q_l^{\beta_l}$ donc divise l'un des q_i d'après le lemme (1) . Supposons que ce soit q_1 pour plus de commodité. Comme $q_1^{\beta_1}$ est le seul multiple de p_1, il est divisible par $p_1^{\alpha_1}$ et $\alpha_1 \leqslant \beta_1$. Par symétrie, on a aussi $\beta_1 \leqslant \alpha_1$ d'où l'égalité.
— On peut donc simplifier dans les deux membres par $p_1^{\alpha_1}$ et itérer le raisonnement. Comme tous les $p_i \geqslant 2$, ils ne divisent pas 1 et on ne peut avoir $k < l$. Par symétrie, on ne peut avoir non plus $l < k$ d'où l'égalité $k = l$.

En d'autres termes, l'unicité est prouvée à l'ordre près des facteurs.

Exemple 5 : Décomposons 16 758 en produit de facteurs premiers :

16758	2
8379	3
2793	3
931	7
133	7
19	19
1	

Pour décomposer un entier, on effectue des divisions successives par des nombres premiers dans l'ordre croissant.

On obtient :

$$16758 = 2 \times 3^2 \times 7^2 \times 19.$$

Exemples 6 :
— $510510 = 1001 \times 510 = (7 \times 11 \times 13) \times (2 \times 3 \times 5 \times 17) = (2)(3)(5)(7)(11)(13)(17)$
— $80000 = 8 \times 10^4 = (2)^7 (5)^4$.

Corollaire 8.1 :
Soient a et b deux entiers supérieurs à 2 dont les décompositions primaires s'écrivent $a = \prod_{p \in \mathbb{P}} p^{\alpha_p}$ et $b = \prod_{p \in \mathbb{P}} p^{\beta_p}$.

Alors :

$$a | b \quad \Longleftrightarrow \quad \forall\, p \in \mathbb{P},\ \alpha_p \leqslant \beta_p.$$

Preuve : Si $a|b$ alors il existe $c \in \mathbb{N}^*$ tel que $b = ac$.

Notons $c = \prod_{p \in \mathbb{P}} p^{\gamma_p}$ sa décomposition en facteurs premiers.

On a alors $\prod_{p \in \mathbb{P}} p^{\beta_p} = \prod_{p \in \mathbb{P}} p^{\alpha_p + \gamma_p}$.

Par unicité de la décomposition, $\forall\, p \in \mathbb{P},\ \beta_p = \alpha_p + \gamma_p \implies \alpha_p \leqslant \beta_p$.

Réciproquement, supposons que l'on ait, pour tout $p \in \mathbb{P}$, $\alpha_p \leqslant \beta_p$.

Il suffit de poser $c = \prod_{p\in\mathbb{P}} p^{\beta_p - \alpha_p}$ pour avoir $c \in \mathbb{N}$ et $b = ac$ *i.e.* $a|b$.

Un peu d'histoire : *On appelle* nombres de Mersenne [4], *les nombres* M_n *de la forme :*

$$\forall\, n \in \mathbb{N}^*,\ \mathrm{M}_n = 2^n - 1.$$

On a :

$$\mathrm{M}_1 = 2-1 = 1 \qquad \mathrm{M}_2 = 4-1 = 3$$
$$\mathrm{M}_3 = 8-1 = 7 \qquad \mathrm{M}_4 = 16-1 = 15$$
$$\mathrm{M}_5 = 32-1 = 31 \qquad \mathrm{M}_6 = 64-1 = 63$$

On remarque que M_2, M_3 *et* M_5 *sont premiers,* M_1, M_4 *et* M_6 *ne le sont pas. De cette observation est née une conjecture :*

$$n \text{ est premier} \iff \mathrm{M}_n \text{ est premier}.$$

Si celle-ci était vraie, cela permettrait de connaître un nombre premier aussi grand que l'on souhaite :

$$2 \text{ premier} \implies \mathrm{M}_2 \text{ premier} \implies \mathrm{M}_{\mathrm{M}_2} \text{ premier} \implies \mathrm{M}_{\mathrm{M}_{\mathrm{M}_2}} \text{ premier} \implies \ldots$$

Actuellement, le plus grand nombre premier trouvé est un nombre de Mersenne.

Malheureusement cette conjecture est fausse dans un sens.

En effet si $n = 11$, *premier donc, alors* $\mathrm{M}_{11} = 2^{11} - 1 = 2047 = 23 \times 89$.

M_{11} *n'est donc pas premier alors que 11 l'est.*

On peut cependant prouver que le sens direct est vrai en prouvant sa contraposée :

« Si n *n'est pas premier alors* M_n *ne l'est pas non plus ».*

Rappel 2 :

$$x^n - 1 = (x-1)(x^{n-1} + x^{n-2} + \ldots + x + 1).$$

Il suffit de développer le second membre et de simplifier ou de reconnaître dans le second membre, la somme des n *premiers termes de la suite géométrique de premier terme* 1 *et de raison* x.

Si n *n'est pas premier, alors il existe* d, *diviseur propre de* n *tel que* $n = dq$ *avec* $q > 1$.

D'où,

$$\begin{aligned}\mathrm{M}_n &= 2^n - 1 = (2^d)^q - 1\\ &= (2^d - 1)\Big((2^d)^{q-1} + (2^d)^{q-2} + \ldots + 2^d + 1\Big).\end{aligned}$$

[4]. **Marin Mersenne**, connu également sous son patronyme latinisé Marinus Mersenius, né le **8 septembre 1588** à Oizé, mort le **1er septembre 1648** à Paris, est un religieux français appartenant à l'ordre des Minimes, érudit, mathématicien et philosophe.

On lui doit les premières lois de l'acoustique, qui portèrent longtemps son nom. Il établit concomitamment avec Galilée la loi de la chute des corps dans le vide.

Donc $2^d - 1$ *est un diviseur propre de* M_n *qui n'est donc pas premier.*

Conclusion : Si n *n'est pas premier alors* M_n *non plus et la contraposée :*

Si M_n est premier alors n l'est également.

Corollaire 8.2 :
$n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$ admet $\prod_{i=1}^{k} (1 + \alpha_i)$ diviseurs.

Un peu d'histoire : *On appelle* nombres de Fermat [5], *les nombres* F_n *de la forme :*

$$\forall\, n \in \mathbb{N},\ F_n = 2^{2^n} + 1.$$

$$F_0 = 3, \quad F_1 = 5, \quad F_2 = 17, \quad F_3 = 257, \quad F_4 = 65\ 537, \quad \ldots$$

Fermat a montré que F_n *est premier pour* $n = 0, \ldots, 4$ *et a conjecturé que* $F_n \in \mathbb{P}$ *pour tout* n.

Cette conjecture s'est avérée fausse.

Euler montra que $F_5 = 4\ 294\ 967\ 297$ *est divisible par* 641.

Jusqu'à aujourd'hui, on n'a trouvé aucun autre nombre de Fermat premier et on ne sait même pas s'il y en a !

Exercice 8 : Trouver le nombre de diviseurs de 120 et déterminer tous ces diviseurs.

Correction :

— La décomposition de 120 en facteurs premiers est $120 = 2^3 \times 3 \times 5$.

Donc $\varphi(120) = (3+1) \times (1+1) \times (1+1) = 4 \times 2 \times 2 = 16$.

Il y a donc 16 diviseurs pour 120.

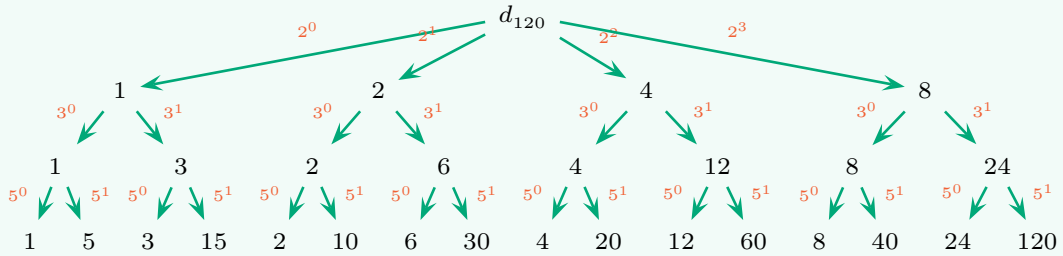
— Pour déterminer tous ces diviseurs, on peut utiliser un tableau double entrée en séparant les puissance de 2 et les puissance de 3 et 5.

On obtient alors :

$\times$	2^0	2^1	2^2	2^3
$3^0 5^0$	1	2	4	8
$3^1 5^0$	3	6	12	24
$3^0 5^1$	5	10	20	40
$3^1 5^1$	15	30	60	120

[5]. Pierre de Fermat, né dans la première décennie du XVIIe siècle près de Montauban, et mort le 12 janvier 1665 à Castres, est un magistrat, polymathe et surtout mathématicien français, surnommé par E.T. Bell « le prince des amateurs».
Il est aussi poète, habile latiniste et helléniste, et s'est intéressé aux sciences et en particulier à la physique. On lui doit notamment le principe de Fermat en optique. Il est particulièrement connu pour avoir énoncé le dernier théorème de Fermat, dont la démonstration n'a été établie que plus de 300 ans plus tard, par le mathématicien britannique Andrew Wiles en 1994.

— On peut aussi utiliser un arbre pondéré dont les coefficients sont les facteurs premiers possibles :



— Les 16 diviseurs de 120 sont donc :

$$d_{120} = \{1, 2, 3, 4, 5, 6, 8, 10, 12, 15, 20, 24, 30, 40, 60, 120\}.$$

II/ PGCD et PPCM

II.1 PGCD

Définition 3 : Soient a et b deux entiers naturels non nuls.

On appelle *PGCD de a et b*, noté $\text{pgcd}(a\,;b)$ ou $a \wedge b$, le plus grand diviseur commun à a et b.

Remarques :

— Comme 1 divise tous les nombres entiers $\text{pgcd}(a\,;b) \geqslant 1$.

De même, il est évident que si a et b sont non nuls, $\text{pgcd}(a\,;b) \leqslant a$ et $\text{pgcd}(a\,;b) \leqslant b$.

— $\text{pgcd}(a\,;b) = \text{pgcd}(b\,;a)$

— Si $a > 0$, $\text{pgcd}(a\,;0) = a$. Par convention, on posera $\text{pgcd}(0\,;0) = 0$.

— En d'autres termes $a \wedge b = \max\left(\mathscr{D}(a) \cap \mathscr{D}(b)\right)$. Plus tard, quand vous saurez que $\mathbb{Z}$ est un anneau *principal*, vous démontrerez que le $\text{pgcd}(a\,;b)$ est le générateur de l'idéal $a\mathbb{Z} + b\mathbb{Z}$:

$$d\mathbb{Z} = a\mathbb{Z} + b\mathbb{Z}, \quad \text{où } d = \text{pgcd}(a\,;b)\,.$$

Preuve : Avant de donner un nom à quelque chose, il faut montrer que ce quelque chose existe et avant de l'appeler « le », il faut montrer qu'il est unique.

Existence : L'ensemble $\mathcal{D}(a) \cap \mathcal{D}(b)$ des diviseurs communs à a et b est un ensemble fini car intersection de deux ensembles finis.

De plus 1 divise a et b donc l'ensemble des diviseurs communs à a et b est non vide.

Or, tout ensemble d'entiers fini non vide admet un plus grand élément que l'on peut appeler $\text{pgcd}(a\,;b)$.

Unicité : Le fait que $\text{pgcd}(a\,;b)$ ait été choisi comme le plus grand élément d'un ensemble fini impose son unicité…s'il en existait un plus grand, on prendrait celui-là.

Dans la pratique, on se bornera souvent au cas où a et b sont dans $\mathbb{N}^*$ et tels que $a > b$. Cette condition n'est pas restrictive car les diviseurs d'un nombre et de son opposé sont les mêmes, donc $\text{pgcd}(a\,;b) = \text{pgcd}(|a|\,;|b|)$ pour a et b dans $\mathbb{Z}$.

Et, par ailleurs, parmi deux entiers naturels a et b, il y en a toujours un qui est plus grand que l'autre. Il suffira donc de commencer par diviser le plus grand par le plus petit.

Exemple 7 :

- $\text{pgcd}\,(24\,;18) = 6$.
- $\text{pgcd}\,(60\,;84) = 12$.
- $\text{pgcd}\,(150\,;240) = 30$.
- $\text{pgcd}\,(27\,;140) = 1$.
- $\text{pgcd}\,(6\,;72) = 6$.
- $\text{pgcd}\,(31\,;45) = 1$.
- $\text{pgcd}\,(5\,;7) = 1$.

Exercice 9 : Pour tout entier n non nul, on définit la suite $(u_n)_{n\in\mathbb{N}}$ par :

$$u_n = \frac{1}{n}\text{pgcd}\,(24\,;n)\,.$$

La suite $(u_n)_{n\in\mathbb{N}}$ est-elle convergente ?

La remarque qui suit exploite dans le domaine de l'arithmétique le vocabulaire des relations d'ordre que nous avons déjà développé :

La première chose dont il faut se rappeler est que la relation de divisibilité est une relation d'ordre sur $\mathbb{N}$ MAIS PAS SUR $\mathbb{Z}$.

Pour cette raison, nous ne parlerons ci-dessous que d'entiers naturels. Le mot « diviseur », en particulier, est à comprendre au sens restreint de « diviseur positif », mais nous omettrons la précision « positif » pour alléger.

Les lettres a, b désignent des entiers NATURELS.

- Dire que a DIVISE b, c'est dire que a est PLUS PETIT QUE b au sens de la divisibilité.
- Les DIVISEURS COMMUNS POSITIFS de a et b sont exactement les MINORANTS de $\{a, b\}$ au sens de la divisibilité.
- Nous avons défini le PGCD de a et b comme le plus grand élément de $\mathscr{D}(a) \cap \mathscr{D}(b)$ au sens de la relation $|$

  Conclusion : $a \wedge b$ est le plus grand minorant de $\{a, b\}$ au sens de la divisibilité *i.e.* sa borne inférieure.

Proposition 9 :

- $\text{pgcd}\,(a\,;a) = |a|$ et $\text{pgcd}\,(1\,;a) = 1$.
- Si $b|a$ alors $\text{pgcd}\,(a\,;b) = |b|$.

Théorème 10 (Fondamental) :
Soient a et b deux entiers non nuls tels et un couple d'entiers $(q\,;r)$ tels que $a = bq + r$. Alors,

$$\text{pgcd}\,(a\,;b) = \text{pgcd}\,(b\,;r).$$

Remarques :

- Même si l'énoncé du théorème (10) fait fortement penser à la division euclidienne de a par b, il n'est nullement besoin que ce soit le cas pour que ce théorème soit vrai.
- En d'autre terme, le théorème (10) s'écrit :

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

Preuve : Posons $\mathrm{D} = \mathrm{pgcd}\,(a\,;b)$ et $d = \mathrm{pgcd}\,(b\,;r)$.

- Comme D divise a et b, il divise aussi $a - bq = r$. Donc D est un diviseur de a et r et $\mathrm{D} \leqslant d$.
- De la même manière, d divise b et r donc divise $bq + r = a$ et $d \leqslant \mathrm{D}$.
- On conclue à $\mathrm{D} = d$.

Méthode 3 (Égalité entre deux nombres) :
Soit d et D, deux quantités. Pour montrer que $d = \mathrm{D}$, il suffit :

- de montrer successivement que $d \leqslant \mathrm{D}$ puis $\mathrm{D} \leqslant d$.
- dans le cas de nombres entiers positifs, on pourra aussi montrer que $d|\mathrm{D}$ puis $\mathrm{D}|d$.

Ce théorème est fondamental par ses applications et notamment dans l'algorithme d'Euclide du paragraphe (II.2) .

Exercice 10 : Soient a et b deux entiers naturels non nuls. Soient $x = 7a + 5b$ et $y = 4a + 3b$.

Montrer que $\mathrm{pgcd}\,(x\,;y) = \mathrm{pgcd}\,(a\,;b)$.

Correction :

Première méthode : On applique le même raisonnement qu'à l'exercice précédent avec des combinaisons linéaires judicieusement choisies afin d'utiliser le théorème (10).

$$\begin{aligned} x = 7a + 5b &= (4a + 3b) + (3a + 2b) \\ &= y + (3a + 2b) \end{aligned} \implies \begin{aligned} \mathrm{pgcd}\,(x\,;y) &= \mathrm{pgcd}\,(7a + 5b\,;4a + 3b) \\ &= \mathrm{pgcd}\,(4a + 3b\,;3a + 2b)\,. \end{aligned}$$

$$\text{Or, } 3a + 2b = 2(a + b) + a \implies \mathrm{pgcd}\,(4a + 3b\,;3a + 2b) = \mathrm{pgcd}\,(a + b\,;a) = \mathrm{pgcd}\,(a\,;b)\,.$$

On en déduit que : $\mathrm{pgcd}\,(x\,;y) = \mathrm{pgcd}\,(a\,;b)$.

Deuxième méthode : En revenant à la définition du pgcd, on applique la méthode (3) en montrant, en deux temps, que $\mathrm{pgcd}\,(x\,;y)\,|\mathrm{pgcd}\,(a\,;b)$ puis $\mathrm{pgcd}\,(a\,;b)\,|\mathrm{pgcd}\,(x\,;y)$.

Pour se simplifier les notations, on pose $d = \mathrm{pgcd}\,(a\,;b)$ et $d' = \mathrm{pgcd}\,(x\,;y)$.

- d divise a et b, donc d divise aussi $x = 7a + 5b$ et $y = 4a + 3b$. On en déduit que $d|d'$.
- De même, si d' divise $7a + 5b$ et $4a + 3b$ alors d' divise aussi $7(4a + 3b) - 4(7a + 5b) = b$ et $3(7a + 5b) - 5(4a + 3b) = a$. Donc $d'|d$.

Comme d divise d' et d' divise d, on a donc $d = d'$.

II.2 Algorithme d'Euclide

Théorème 11 (Le pgcd est le dernier reste non nul) :
Soient a et b deux naturels non nuls tels que b ne divise pas a. La suite des divisions euclidiennes suivantes finit par s'arrêter.

Le dernier reste non nul est alors le pgcd $(a\,;b)$.

$$\begin{array}{lll} a \text{ par } b & a = bq_0 + r_0 & \text{avec} \quad b > r_0 \geqslant 0 \\ b \text{ par } r_0 & b = r_0q_1 + r_1 & \text{avec} \quad r_0 > r_1 \geqslant 0 \\ r_0 \text{ par } r_1 & r_0 = r_1q_2 + r_2 & \text{avec} \quad r_1 > r_2 \geqslant 0 \\ & \vdots & \\ r_{n-2} \text{ par } r_{n-1} & r_{n-2} = r_{n-1}q_n + r_n & \text{avec} \quad r_{n-1} > r_n \geqslant 0 \\ r_{n-1} \text{ par } r_n & r_{n-1} = r_nq_{n+1} + 0. & \end{array}$$

On a alors pgcd $(a\,;b) = r_n$.

Preuve :

- La suite des restes r_0, r_1, r_2, ..., r_n est une suite strictement décroissante dans $\mathbb{N}$. Elle est donc nécessairement finie. Il existe, de plus, un certain rang n tel que $r_{n+1} = 0$.
- En appliquant le théorème (10) de proche en proche, on obtient alors :

$$\text{pgcd}\,(a\,;b) = \text{pgcd}\,(b\,;r_0) = \text{pgcd}\,(r_0\,;r_1) = \ldots = \text{pgcd}\,(r_{n-1}\,;r_n)\,.$$

- Or, $r_{n-1} = r_nq_{n+1} + 0$ *i.e.* r_n divise r_{n-1}.

  Donc pgcd $(r_{n-1}\,;r_n) = r_n$.
- Conclusion : pgcd $(a\,;b) = r_n$. Le dernier reste non nul est le PGCD.

Exemple 8 : Calculer le pgcd $(4539\,;1958)$. On effectue les divisions euclidiennes suivantes :

$$\begin{aligned} 4539 &= 1958 \times 2 + 623 \\ 1958 &= 623 \times 3 + 89 \\ 623 &= 89 \times 7 + 0 \end{aligned}$$

Conclusion : pgcd $(4539\,;1958) = 89$.

Remarque : Le petit nombre d'étapes montre la performance de cet algorithme. Celui-ci porte le nom d'un père des mathématiques car il était effectivement connu d'Euclide six siècles avant notre ère !!!

Exercice 11 : Calculer le pgcd de 162 et 207.

Correction :

$$\begin{aligned} 207 &= 162 \times 1 + 45 \\ 162 &= 45 \times 3 + 27 \\ 45 &= 27 \times 1 + 18 \\ 27 &= 18 \times 1 + 9 \\ 18 &= 9 \times 2 + 0 \end{aligned} \qquad \Longrightarrow \ \text{pgcd}\,(162\,;207) = 9.$$

Voici un algorithme d'Euclide que l'on peut proposer pour trouver le PGCD de deux nombres.

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

Figure III.4 – Algorithme d'Euclide

Théorème 12 :
Soient a et b deux entiers non nuls.

Les diviseurs communs de a et b sont **exactement** les diviseurs de $\text{pgcd}\,(a\,;b)$:

$$d|\text{pgcd}\,(a\,;b) \iff \begin{cases} d|a \\ d|b \end{cases}$$

De manière équivalente : $\mathscr{D}(a \wedge b) = \mathscr{D}(a) \cap \mathscr{D}(b)$.

Remarque : Avant ce théorème, nous n'avions que l'inclusion $\mathscr{D}(a \wedge b) \subset \mathscr{D}(a) \cap \mathscr{D}(b)$.

Preuve : On démontre les deux implications séparément :

Condition nécessaire : Si $d|\text{pgcd}\,(a\,;b)$ alors $d|a$ et $d|b$ par transitivité.

Condition suffisante : Soit d divisant a et b. Appliquons l'algorithme d'Euclide à a et b et considérons la suite finie des r_n apparaissant dans celui-ci.

À la première étape, $r_0 = a - bq$ *i.e.* $d|r_0$. On déroule alors en appliquant le théorème (10) fondamental :

$$\begin{cases} d|a \\ d|b \end{cases} \Longrightarrow \begin{cases} d|b \\ d|r_0 \end{cases} \Longrightarrow \begin{cases} d|r_0 \\ d|r_1 \end{cases} \Longrightarrow \ldots \Longrightarrow \begin{cases} d|r_{n-1} \\ d|r_n \end{cases}.$$

Or, $r_n = \text{pgcd}\,(a\,;b)$.

Donc $d|\text{pgcd}\,(a\,;b)$.

Proposition 13 :
Pour tout entier naturel k non nul, $\text{pgcd}\,(ka\,;kb) = k \times \text{pgcd}\,(a\,;b)$.

Preuve : Ici aussi, on applique l'algorithme d'Euclide à a et b. Partant de $a = b \times q + r_0$ avec $0 \leqslant r_0 < b$, on a

$$ka = kb \times q + kr_0, \quad \text{avec } 0 \leqslant kr_0 < kb \tag{III.4}$$

i.e. (III.4) est bien l'expression de la division euclidienne de ka par kb et, dans l'algorithme d'Euclide appliqué à ka et kb, la suite des restes est formée des kr_n. Le dernier reste non nul sera donc $kr_n = k\text{pgcd}\,(a\,;b)$.

Donc $\text{pgcd}\,(ka\,;kb) = k \times \text{pgcd}\,(a\,;b)$.

Exemple 9 :

- $\text{pgcd}\,(800\,;500) = \text{pgcd}\,(100\times 8\,;100\times 5) = 100\times\text{pgcd}\,(8\,;5) = 100$.
- $\text{pgcd}\,(36\,;24) = \text{pgcd}\,(12\times 3\,;12\times 2) = 12\times\text{pgcd}\,(3\,;2) = 12$.

Proposition 14 :
Soient a et b deux entiers supérieurs à 2 dont les décompositions primaires s'écrivent $a = \prod_{p\in\mathbb{P}} p^{\alpha_p}$ et $b = \prod_{p\in\mathbb{P}} p^{\beta_p}$.

Alors,

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

Preuve : Comme $\min(\alpha_p,\beta_p) \leqslant \alpha_p$ et $\min(\alpha_p,\beta_p) \leqslant \beta_p$, $d = \prod_{p\in\mathbb{P}} p^{\min(\alpha_p,\beta_p)}$ est bien un diviseur de a et b.

Soit alors $d' = \prod_{p\in\mathbb{P}} p^{\delta_p}$ un diviseur de a et b. Le corollaire (8.1) entraîne que $\delta_p \leqslant \alpha_p$ et $\delta_p \leqslant \beta_p$ *i.e.* $\delta_p \leqslant \min(\alpha_p,\beta_p)$.

Donc $d'|d$ et $d = \text{pgcd}\,(a\,;b)$.

Dans le cas de deux nombres a et b pas trop grands, on pourra ainsi réviser ses tables de multiplication et décomposer les deux nombres a et b en facteurs premiers et trouver, « à la main », le plus grand diviseur commun. [6]

Exemples 10 :

- $510510 \wedge 80000 = (2)(3)(5)(7)(11)(13)(17) \wedge (2)^7(5)^4 = (2)(5) = 10$.
- $9100 \wedge 1848 = (2)^2(5)^2(7)(13) \wedge (2)^3(3)(7)(11) = (2)^2(7) = 28$.

Exercice 12 : Déterminer le PGCD de 1960 et de 34300.

Correction : On a : $1960 = 2^3 \times 5^1 \times 7^2$ et $34300 = 2^2 \times 5^2 \times 7^3$.

On en déduit que $\text{pgcd}\,(1960\,;34300) = 2^2 \times 5^1 \times 7^2 = 980$.

[6]. Cette décomposition en facteurs premiers proprement dite est, en fait, un problème extrêmement difficile pour des nombres élevés. Pour trouver le pgcd de tels nombres nous aurons besoin d'un algorithme plus puissant (*cf* plus loin).

II.3 PPCM

Définition 4 : Soient a et b deux entiers naturels non nuls.

On appelle *PPCM de a et b*, noté $\text{ppcm}(a\,;b)$ ou $a \vee b$, le plus petit multiple commun de a et b.

Remarques :

— Le seul multiple de 0 est 0 donc, pour tout entier a, $\text{ppcm}(a\,;0) = 0$.

— Comme tous les entiers sont multiples de 1, $\text{ppcm}(a\,;b) \geqslant 1$.

De même, il est évident que si a et b sont non nuls, $\text{ppcm}(a\,;b) \geqslant a$ et $\text{ppcm}(a\,;b) \geqslant b$.

— $\text{ppcm}(a\,;b) = \text{ppcm}(b\,;a)$.

— En d'autres termes, $a \vee b = \min(a\mathbb{Z} \cap b\mathbb{Z})$ ou encore $\text{ppcm}(a\,;b)$ engendre l'idéal $a\mathbb{Z} \cap b\mathbb{Z}$.

Preuve : La démonstration est identique à celle du pgcd :

— L'ensemble des multiples strictement positifs à a et à b n'est pas vide puisqu'il contient au moins ab.

Comme toute partie non vide de $\mathbb{N}$ admet un plus petit élément, $\text{ppcm}(a\,;b)$ existe.

— Comme on a pris le plus petit des candidats par définition, $\text{ppcm}(a\,;b)$ est unique.

Au collège, pour additionner deux fractions, on recherchait le dénominateur commun le plus petit qui n'était rien d'autre que $\text{ppcm}(a\,;b)$.

Exemple 11 :

— $\text{ppcm}(18\,;12) = 36$.

— $\text{ppcm}(24\,;40) = 120$.

— $\text{ppcm}(11\,;17) = 11 \times 17 = 187$.

— $\text{ppcm}(19\,;5) = 19 \times 5 = 195$.

Proposition 15 :
Soient a et b deux entiers naturels non nuls.

— $\text{ppcm}(a\,;a) = a$ et $\text{ppcm}(1\,;a) = a$.

— Si $b|a$ alors $\text{ppcm}(a\,;b) = a$.

Théorème 16 :
Soient a et b deux entiers non nuls.

Les multiples communs de a et b sont **exactement** les multiples de $\text{ppcm}(a\,;b)$:

$$\text{ppcm}(a\,;b)\,|m \iff \begin{cases} a|m \\ b|m \end{cases}$$

De manière équivalente : $(a \vee b)\mathbb{Z} = a\mathbb{Z} \cap b\mathbb{Z}$.

Au sens de la divisibilité, $a \vee b$ est le plus petit majorant de $\{a, b\}$ *i.e.* sa borne supérieure.

Preuve : On démontre les deux implications séparément :

Condition nécessaire : Si m est un multiple de $\text{ppcm}\,(a\,;b)$ alors m est un multiple de a et b par définition.

Condition suffisante : Soit m un multiple de a et b. Posons $\text{M} = \text{ppcm}\,(a\,;b)$.

La division euclidienne de m par M s'écrit $m = \text{M}q + r$ avec $0 \leqslant r < \text{M}$.

Or, $r = m - \text{M}q$ est alors aussi un multiple de a et b et strictement plus petit que $\text{M} = \text{ppcm}\,(a\,;b)$. Ceci n'est possible qu'à la condition que $r = 0$ *i.e.* $m|\text{M}$. $\text{ppcm}\,(a\,;b)$ est donc un multiple de m.

En pratique, on sait calculer le PGCD de deux nombres mais moins leur PPCM. Le théorème (17) donne un moyen de le calculer :

Théorème 17 :
Soient a et b deux entiers naturels.

$$ab = \text{ppcm}\,(a\,;b) \times \text{pgcd}\,(a\,;b)\,.$$

Preuve : Si $a = 0$ ou $b = 0$, la relation est clairement vérifiée.

Supposons à présent a et b non nuls et posons $\delta = a \wedge b$ et $\mu = a \vee b$.

Montons que $ab = \delta\mu$ par divisibilité réciproque :

$\delta\mu|ab$ **:** Par définition de δ, $\delta|a$ et $\delta|b$ donc il existe $a', b' \in \mathbb{N}$ tels que $a = \delta a'$ et $b = \delta b'$

On pose $m = \delta a'b' = ab' = a'b$.

m est donc un multiple de a et b donc un multiple de μ d'après le théorème (16).

Par conséquence, $ab = \delta m$ est un multiple de $\delta\mu$ *i.e.* $\delta\mu|ab$.

$ab|\delta\mu$ **:** Par définition de μ, il existe $n \in \mathbb{N}$ tel que $ab = \mu n$.

Or, μ est aussi un multiple de a donc il existe $c \in \mathbb{N}$ tel que $\mu = ac$.

Alors $ab = \mu n = acn \implies b = cn$ (car a $a \neq 0$) *i.e.* $n|b$.

On montre de la même manière que $n|a$. L'entier n est donc un diviseur commun à a et b, il divise donc le plus grand d'entre eux δ d'après le théorème (12)

En conclusion $ab = n\mu$ divise $\delta\mu$.

Par antisymétrie de la relation de divisibilité sur $\mathbb{N}$, on en déduit que $\delta\mu = ab$.

Remarque : La notion de PPCM peut aisément s'étendre aux entiers relatifs en prenant comme définition, le plus petit multiple de $|a|$ et $|b|$. Dans ce cas, on aurait également :

$$|ab| = \text{ppcm}\,(a\,;b) \times \text{pgcd}\,(a\,;b)\,.$$

Exemple 12 : Le PGCD de 42 et 60 est 6. Si on note m leur PPCM, alors $6m = 42 \times 60$ et $m = 420$.

Corollaire 17.1 :

$$\forall\, k \in \mathbb{N}, \quad \text{ppcm}\,(ka\,;kb) = k \times \text{ppcm}\,(a\,;b)\,.$$

Preuve : Si k, a ou b est nul, c'est évident.

Sinon, supposons a, b et k non nuls.

Toujours d'après la proposition (17) , $\text{ppcm}\,(ka\,;kb) \times \text{pgcd}\,(ka\,;kb) = ka \times kb$.

Or, $\text{pgcd}\,(ka\,;kb) = k \times \text{pgcd}\,(a\,;b)$.

Après simplification, on a le résultat escompté.

Exercice 13 : Déterminer $m = 44100 \vee 36036$.

Correction : On commence par déterminer $44100 \wedge 36036$ l'algorithme d'Euclide :

$$44100 \wedge 36036 = 36036 \wedge 8064 = 8064 \wedge 3780 = 3780 \wedge 504 = 504 \wedge 252 = 252.$$

D'après la relation (17), on a alors $252 \times m = 44100 \times 36036$.

D'où $m = \dfrac{44100 \times 36036}{252} = 6306300$.

Proposition 18 :
Soient a et b deux entiers supérieurs à 2 dont les décompositions primaires s'écrivent $a = \prod_{p\in\mathbb{P}} p^{\alpha_p}$ et $b = \prod_{p\in\mathbb{P}} p^{\beta_p}$.

Alors,

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

Preuve : La démonstration est quasi-identique à celle de la proposition (14) .

Comme $\max(\alpha_p,\beta_p) \geqslant \alpha_p$ et $\max(\alpha_p,\beta_p) \geqslant \beta_p$, $m = \prod_{p\in\mathbb{P}} p^{\max(\alpha_p,\beta_p)}$ est bien un multiple de a et b.

Soit alors $m' = \prod_{p\in\mathbb{P}} p^{\delta_p}$ un multiple de a et b. Le corollaire (8.1) entraîne que $\delta_p \geqslant \alpha_p$ et $\delta_p \geqslant \beta_p$ *i.e.* $\delta_p \geqslant \max(\alpha_p,\beta_p)$.

Donc $m|m'$ et $m = \text{ppcm}\,(a\,;b)$.

Méthode 4 (Trouver un PPCM) :
Pour des entiers a et b pas « trop grands », une méthode enfantine mais souvent suffisante est de décomposer a et b en facteurs premiers.

Le ppcm de a et b est alors égal au produit de tous les facteurs premiers de a et b pris avec l'exposant le plus grand apparaissant dans les décompositions.

Exercice 14 : Déterminer $\text{ppcm}\,(240\,;756)$.