ARITHMÉTIQUE

1

Arithmétique

« *L'homme a toujours craint ce qu'il ne pouvait comprendre.* »

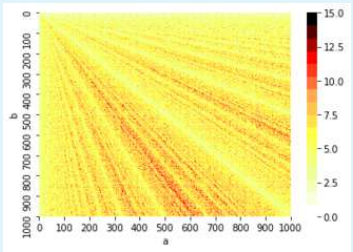
Magneto, *X-Men*, 2000

Introduction

Les entailles retrouvées sur l'os d'Ishango daté à plus de 20 000 ans avant notre ère, mis au jour par l'archéologue Jean de Heinzelin de Braucourt et antérieur à l'apparition de l'écriture (antérieur à 3 200 ans avant J.-C.), semblent isoler quatre nombres premiers 11, 13, 17 et 19. Certains archéologues l'interprètent comme la preuve de la connaissance des nombres premiers. Toutefois, il existe trop peu de découvertes permettant de cerner les connaissances réelles de cette période ancienne.

Chez les égyptiens, le calcul fractionnaire demandait des connaissances sur les opérations, les divisions d'entiers et les factorisations. Les Égyptiens ne notaient que les inverses d'entiers (1/2, 1/3, 1/4, 1/5, ...) ; l'écriture des fractions se faisait en additionnant des inverses d'entiers, si possible sans répétition (1/2 + 1/6 au lieu de 1/3 + 1/3). Disposer d'une liste des premiers nombres premiers devait être nécessaire.

La première trace incontestable de la présentation des nombres premiers remonte à l'Antiquité (vers -300 av. J.-C.), et se trouve dans les Éléments d'Euclide (tomes VII à IX). Euclide donne la définition des nombres premiers, la preuve de leur infinité, la définition du plus grand commun diviseur (PGCD) et du plus petit commun multiple (PPCM), et les algorithmes pour les déterminer, aujourd'hui appelés algorithmes d'Euclide. Les connaissances présentées lui sont toutefois bien antérieures.



Nombre d'étapes de l'algorithme d'Euclide en fonction des nombres entiers a et b (respectivement en abscisse et en ordonnées). Plus le point de coordonnées (a, b) est foncé, plus le calcul de PGCD(a, b) nécessite d'étapes.

On ne peut pas parler d'arithmétique et d'Euclide sans mentionner la *division euclidienne*. Le nom de division euclidienne est un hommage rendu à Euclide qui pose les fondements de l'arithmétique dans ses Éléments. Mais elle apparaît très tôt dans l'histoire des mathématiques, notamment dans les mathématiques égyptiennes où il s'agit par exemple de mesurer 30 avec l'unité 7. Une démarche analogue existe dans les mathématiques babyloniennes. On retrouve cette procédure décrite dans les mathématiques chinoises avec un algorithme proche du système actuel consistant à poser une division. Les Chinois ont un mot pour désigner le dividende, le diviseur et le quotient en cours de calcul.


EVCLIDIS
ELEMENTORVM
LIBRI XV. GRAE-
cè & Latiné,
Quibus, cùm ad omnem Mathematicæ scientiæ partem, tùm ad quamlibet Geometriæ tractationem facilis comparatur aditus.
Επίχειμιαπολαύει.
LVTETIAE,
Apud Gulielmum Cauellat, in pingui Gallina, ex aduerso collegij Cameracensis.
1558.

On a déjà parlé de plusieurs ensembles de nombres. On va s'arrêter quelques instants sur l'ensemble des entiers relatifs (les entiers positifs et négatifs). Même si cet ensemble semble d'apparence simple, on va voir qu'il est possible d'avoir des résultats intéressants. On va revenir sur les notions de *multiples* et *diviseurs*, peut-être vues au collège, mais également celles de nombres *pairs* et *impairs*. En définissant les *nombres premiers*, qui sont des espèces de "nombres que l'on ne peut pas casser", on va tomber sur des résultats intéressants. Notamment le fait qu'avec les nombres premiers, on peut représenter tous les autres nombres et ceci de façon unique ! Et ceci va nous simplifier la vie pour trouver le *PGCD* et le *PPCM* de deux entiers par exemple...

Auto-évaluation diagnotisque

coucou@coquillagesetpoincare.fr
pour toute(s) question(s) / remarque(s).

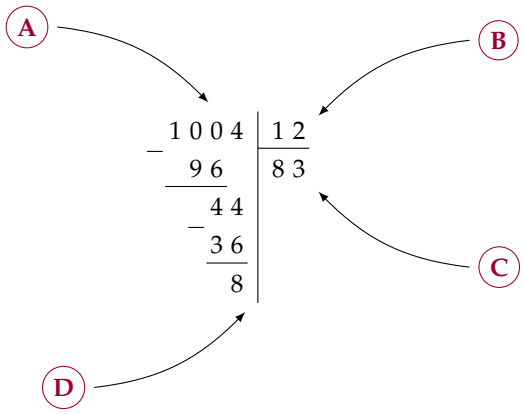
1 21 est un ... de -2100.

(a) multiple (b) diviseur (c) reste

2 L'ensemble des diviseurs positifs de 12 est

(a) $\{2;3;4;6\}$ (b) $\{2;3;4;6;12\}$ (c) $\{1;2;3;4;6;12\}$

Pour les questions 1 à 4, on considère la division euclidienne suivante :



1 Quel est le terme en (A) à indiquer l'extrémité de la flèche ?

(a) Quotient (b) Dividende (c) Diviseur

2 Quel est le terme en (B) à indiquer l'extrémité de la flèche ?

(a) Quotient (b) Dividende (c) Diviseur

3 Quel est le terme en (C) à indiquer l'extrémité de la flèche ?

(a) Quotient (b) Dividende (c) Diviseur

4 Quel est le terme en (D) à indiquer l'extrémité de la flèche ?

(a) Quotient (b) Résidu (c) Reste

3 99 est un ...

(a) nombre premier. (b) nombre pair. (c) multiple de 3.

4 Il existe une infinité de nombres premiers.

(a) Vrai. (b) Faux. (c) On ne sait pas.

➤➤➤ Voir solutions p. ??

Cours

1. Divisibilité dans $\mathbb{Z}$

A. Multiples et diviseurs

DÉFINITION : Multiple et diviseur

Soient a et b deux entiers relatifs.

- a est **multiple** de b s'il existe un entier relatif k tel que $a = k \times b$.
- • Pour $b \neq 0$, b est un **diviseur** de a (ou que b **divise** a) si a est un **multiple** de b. On note $b \mid a$.

NOTATION : $b \mid a$ se lit « b *divise* a ».

Exemple

$-42 = 6 \times (-7)$ donc :

- -42 est un multiple de -7 et de 6.
- $-7 \mid -42$ et $6 \mid -42$

REMARQUE :

- 0 est un multiple de tout entier relatif m car $0 = m \times 0$.
- 1 est un diviseur de tout entier relatif n car $n = 1 \times n$.

PRENONS DE LA HAUTEUR : L'ensemble des multiples d'un entier relatif a dans $\mathbb{Z}$ est noté $a\mathbb{Z}$ et l'ensemble des diviseurs de a est noté $D(a)$.
En utilisant les notations de la précédente définition, on a

$$b\mathbb{Z} \subset a\mathbb{Z} \text{ et } \text{Div}(b) \subset \text{Div}(a)$$

Par exemple, les multiples de 24 sont aussi des multiples de 3 : $24\mathbb{Z} \subset 3\mathbb{Z}$.
Les diviseurs de 12 sont des diviseurs de 24 :

$$\text{Div}(12) = \{-12; -6; -4; -3; -2; -1; 1; 2; 3; 4; 6; 12\}$$
$$\text{Div}(24) = \{-24; -12; -8; -6; -4; -3; -2; -1; 1; 2; 3; 4; 6; 8; 12; 24\}$$

On a bien $\text{Div}(12) \subset \text{Div}(24)$.

PROPOSITION

La somme de deux multiples d'un même entier relatif a est aussi un multiple de a.

PREUVE On va faire la démonstration pour les multiples de 5 (mais la démonstration est la même pour tout autre multiple !). On peut déjà remarquer que la proposition peut se réécrire :

« Si m et n sont deux multiples de 5, alors $m + n$ est un multiple de 5. »

Prenons donc ces deux entiers m et n : il existe donc deux entiers h et k tels que $m = 5h$ et $n = 5k$. On en déduit donc que

$$m + n = 5h + 5k = 5(h + k)$$

Comme h et k sont des entiers, alors $h + k$ est un entier. Donc $m + n$ est un multiple de 5. ■

PROPOSITION

Soit a un entier relatif non nul.

- Tout diviseur de a est compris entre $-|a|$ et $|a|$.
- Tout entier relatif non nul a a donc un nombre fini de diviseurs.

PROPOSITION

Soient a et b deux entiers relatifs. On a les équivalences suivantes :

$$b \mid a \;\Leftrightarrow\; (-b) \mid a \;\Leftrightarrow\; b \mid (-a) \;\Leftrightarrow\; (-b) \mid (-a)$$

PREUVE Pour démontrer cette équivalence, on verra qu'il s'agit principalement d'être assez malin en utilisant la multiplication par -1. On va également démontrer l'équivalence en suivant le schéma ci-après (et vous pourrez constater que l'on aura ainsi démontrer toutes les équivalences) :

$$\begin{array}{ccc} b \mid a & \Longrightarrow & (-b) \mid a \\ \Uparrow & & \Downarrow \\ (-b) \mid (-a) & \Longleftarrow & b \mid (-a) \end{array}$$

- Montrons que $b \mid a \;\Rightarrow\; (-b) \mid a$:
  On suppose donc que $b \mid a$ et ainsi qu'il existe un entier relatif k tel que $a = k \times b$. Or :
  $$a = k \times b = \underbrace{(-1) \times (-1)}_{=1} \times k \times b = (-1) \times k \times (-1) \times b = (-k) \times (-b)$$
  Comme k est un entier relatif, $-k$ est un encore entier relatif, donc on a bien $(-b) \mid a$.
- Montrons que $(-b) \mid a \;\Rightarrow\; b \mid (-a)$:
  On suppose donc que $(-b) \mid a$ et ainsi qu'il existe un entier relatif k tel que $a = k \times (-b)$. Or :
  $$a = k \times (-b) \;\Leftrightarrow\; a \times (-1) = k \times (-b) \times (-1) \;\Leftrightarrow\; -a = k \times b$$
  On a bien $b \mid (-a)$.
- Montrons que $b \mid (-a) \;\Rightarrow\; (-b) \mid (-a)$:
  On suppose donc que $b \mid (-a)$ et ainsi qu'il existe un entier relatif k tel que $-a = k \times b$. Or :
  $$-a = k \times b = \underbrace{(-1) \times (-1)}_{=1} \times k \times b = (-1) \times k \times (-1) \times b = (-k) \times (-b)$$
  Comme k est un entier relatif, $-k$ est un encore entier relatif, donc on a bien $(-b) \mid (-a)$.
- Montrons que $(-b) \mid (-a) \;\Rightarrow\; b \mid a$:
  On suppose donc que $(-b) \mid (-a)$ et ainsi qu'il existe un entier relatif k tel que $(-a) = k \times (-b)$. Or :
  $$-a = k \times (-b) \;\Leftrightarrow\; -a \times (-1) = k \times (-b) \times (-1) \;\Leftrightarrow\; a = k \times b$$
  On a bien $b \mid a$ ■

REMARQUE : a et $-a$ ayant les mêmes diviseurs dans $\mathbb{Z}$, on restreindra souvent l'étude à la divisibilité dans $\mathbb{N}$.

Cours

PÉDAGOGIE 1 Un jeu pour les multiples et diviseurs : le jeu de Jupiner Green

Ce jeu a été créé par Richard Porteous, enseignant à l'école Juniper Green, d'où son nom. Vous pouvez retrouvez ce jeu en ligne ! Il a été développé par Julien Pavageau, professeur de mathématiques et référent RUPN (Ressources et Usages Pédagogiques Numériques) au collège Albert Camus de Frontenay Rohan (Académie de Poitiers).

Heuristique

Ce jeu se joue à deux, chaque joueur prenant un stylo de couleur différente.
On dispose d'une grille contenant les n entiers consécutifs $1, 2, 3, \ldots, n$.

1	2	3	4	5
6	7	8	9	10
11	12	13	14	15
16	17	18	19	20
21	22	23	24	25

Exemple avec $n = 25$

Règles :

1) *Le Joueur 1 choisit un nombre entre 1 et n, le barre sur la grille et note son choix.*
2) *A tour de rôle, chaque joueur choisit un nombre parmi les multiples ou les diviseurs du nombre choisi précédemment par son adversaire et inférieur à n, et le barre sur la grille.*
3) *Un nombre ne peut être joué qu'une seule fois.*

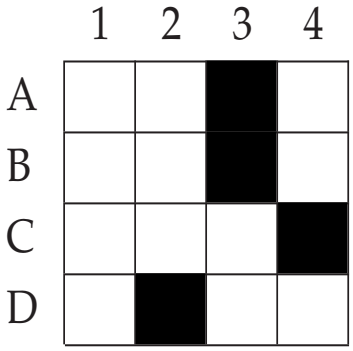
Il peut être intéressant de se poser quelques questions concernant ce jeu...

- Est-il possible de gagner à coup sûr à ce jeu et en très peu de coups ?
- Inversement, quel nombre doit-on initialement choisir pour cocher le plus possible de nombres sur la grille ?
- etc.

PÉDAGOGIE 2 Un autre jeu pour les multiples et diviseurs : les nombres croisés

Popularisés vers 1930, il s'agit de placer un chiffre par case libre d'une grille à partir de définitions qui permettent d'identifier des nombres horizontalement et verticalement. Les cases noires séparent les nombres au lieu des mots comme dans un Mots croisés.

Heuristique



Horizontalement

A - Multiple de 3 et de 5. • Diviseur de 25.
B - Multiple de 10. • Diviseur de tous les nombres.
C - Diviseur de 222 autre que lui-même.
D - Multiple de 5 (mais pas de 10) si on lui ajoute 1. • Multiple de 12 et 7.

Verticalement

1 - Nombre palindrome.
2 - Multiple de 100 si on lui enlève 1.
3 - Multiple de 2 et de 3.
4 - Multiple de 17.

B. Propriétés de la divisibilité

PROPOSITION : Propriété de transitivité

Soient a, b et c trois entiers relatifs. Si $a \mid b$ et $b \mid c$, alors $a \mid c$.

PREUVE

- $a \mid b$ signifie qu'il existe un entier relatif k tel que $a = k \times b$.
- $b \mid c$ signifie qu'il existe un entier relatif l tel que $c = l \times b$.

Par suite, $c = lb = l(ka) = lka$.
Or, comme lk est un entier relatif, on a donc $a \mid c$. ■

Exemple

Comme $17 \mid 51$ et $51 \mid 153$, alors on en déduit que $17 \mid 153$.

PROPOSITION

Soient a, b et c trois entiers relatifs.
1) Si $a \mid b$ et $a \mid c$, alors quels que soient les entiers u et v, on a $a \mid (ub + vc)$.
2) En particulier, si $a \mid b$, alors $a \mid (a + b)$ et $a \mid (a - b)$.

PREUVE

1) • $a \mid b$ signifie qu'il existe un entier relatif k tel que $b = k \times a$.
• $a \mid c$ signifie qu'il existe un entier relatif l tel que $c = l \times a$.
Par suite, pour tout entier u et v,

$$ub + vc = uka + vla = (uk + vl)a$$

Or, comme $uk + vl$ est un entier relatif, on a donc $a \mid ub + vc$.
2) On a $a \mid b$ et $a \mid a$, donc on a les résultats en prenant respectivement $u = 1$ et $v = 1$, puis $u = 1$ et $v = -1$). ■

Exemple

Déterminons les entiers relatifs n tels que $2n + 1$ divise $n + 13$.
L'idée est d'écrire une combinaison linéaire de $2n + 1$ et $n + 13$ indépendante de n :

$$2n + 1 - 2(n + 13) = -25$$

Donc si $2n + 1$ divise $n + 13$, $2n + 1$ divise -25.
Or $\text{Div}(25) = \{-25; -5, -1; 1; 5; 25\}$. On en déduit donc que :

$$\begin{cases} 2n+1 &= -25 \\ 2n+1 &= -5 \\ 2n+1 &= -1 \\ 2n+1 &= 1 \\ 2n+1 &= 5 \\ 2n+1 &= 25 \end{cases} \Leftrightarrow \begin{cases} n &= -13 \\ n &= -3 \\ n &= -1 \\ n &= 0 \\ n &= 2 \\ n &= 12 \end{cases}$$

Réciproquement, si $n = -13$, $2n + 1 = -25$ et $n + 13 = 0$, et -25 divise bien 0.
On vérifie de même les cinq autre valeurs trouvées pour n.
On conclut que les solutions sont les entiers -13, -3, -1, 0, 2 et 12.

C. Division euclidienne

PROPOSITION : La division euclidienne

Soient a entier relatif et b entier naturel non nul. Alors, il existe un unique couple d'entiers $(q;r)$ vérifiant la relation suivante

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

Cette relation est appelée **la division euclidienne de a par b.**
q est le **quotient de la division euclidienne** de a par b.
r est le **reste de la division euclidienne** de a par b.
a est le **dividende de la division euclidienne** de a par b.
b le **diviseur de la division euclidienne** de a par b.

Exemple

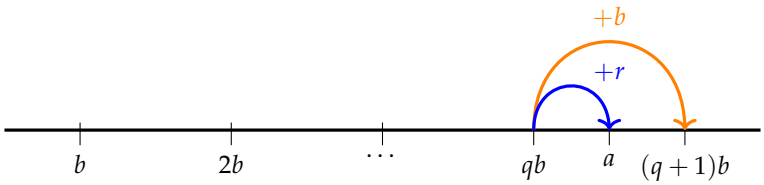
Dans la division euclidienne de -53 par 5 le quotient est de -11 et le reste est 2.
En effet, $5 \times (-11) < -53 < 5 \times (-10)$ donc le quotient euclidien est -11.
Et $-53 = 5 \times (-11) + 2$ et $0 \leqslant 2 < 5$ donc le reste est 2.

PÉDAGOGIE 3 Un schéma permettant de comprendre la division euclidienne

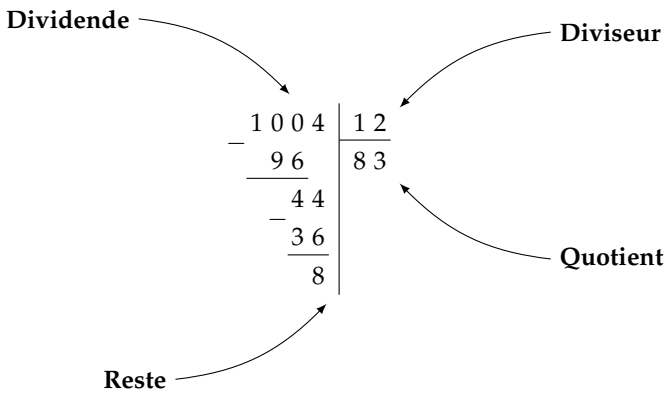
Il est important d'avoir en tête que **la division euclidienne n'est pas une définition, mais bien une proposition !** Elle se démontre donc !

Heuristique

L'idée de la démonstration repose essentiellement sur l'interprétation graphique qui nous illustre l'encadrement de a par deux entiers consécutifs.



REMARQUE : Cette division euclidienne est plus connue sous sa forme « *posée* ».



D. Nombres pairs et impairs

DÉFINITION

Un nombre entier n est **pair** si et seulement s'il existe un entier k tel que $n = 2k$.
Un nombre entier n est **impair** si et seulement s'il existe un entier k tel que $n = 2k + 1$.

REMARQUE :

- Un entier n est **pair** si et seulement son reste dans la division euclidienne par 2 vaut 0.
- Un entier n est **impair** si et seulement son reste dans la division euclidienne par 2 vaut 1.

ATTENTION : La parité de zéro est généralement une source de confusion. Dans des expériences qui mesurent le temps de réaction, la plupart des gens sont plus lents à déterminer que zéro est pair par rapport à 2, 4, 6 ou 8. Certains étudiants en mathématiques, et même certains professeurs pensent que la phrase « zéro est pair » est fausse (pensant donc que zéro est impair, à la fois pair et impair, ou aucun des deux).

Des chercheurs en enseignement des mathématiques prétendent que ces idées fausses peuvent être source d'apprentissage. L'étude d'égalités telles que $0 \times 2 = 0$ peuvent aider les étudiants à dissiper leurs doutes sur le fait que zéro est un nombre et leur permettre de l'utiliser en arithmétique. Parler de la parité de zéro en classe peut leur faire comprendre les principes de base du raisonnement mathématique, ainsi que l'importance des définitions.

Déterminer la parité de ce nombre particulier est un premier exemple d'un thème omniprésent en mathématiques : l'abstraction d'un concept familier et son application à un cas qui l'est moins.

PROPOSITION

Le carré d'un nombre impair est un nombre impair.

PREUVE Soit n un nombre impair. On sait donc qu'il existe un entier k tel que $n = 2k + 1$.
Alors :

$$n^2 = (2k+1)^2 = (2k)^2 + 2 \times 2k \times 1 + 1^2$$

(on a utilisé l'identité remarquable $(a+b)^2 = a^2 + 2ab + b^2$ avec $a = 2k$ et $b = 1$). On obtient donc, en simplifiant,

$$n^2 = 4k^2 + 4k + 1$$

Comme on doit montrer que n^2 est impair, il faut écrire n^2 sous la forme $2h + 1$ pour un certain entier h ... Allons-y !

$$n^2 = 4k^2 + 4k + 1 = 2(\underbrace{2k^2 + 2k}_{:=h}) + 1 = 2h + 1$$

On a posé $h = 2k^2 + 2k$ (qui est bien un entier !).
On en déduit donc que n^2 est un nombre impair.

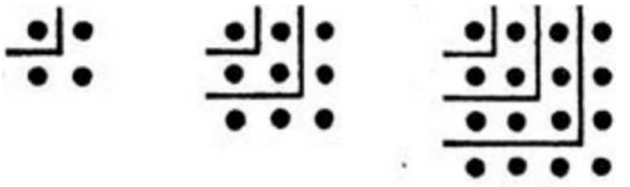
■

PÉDAGOGIE 4 Preuve sans mots

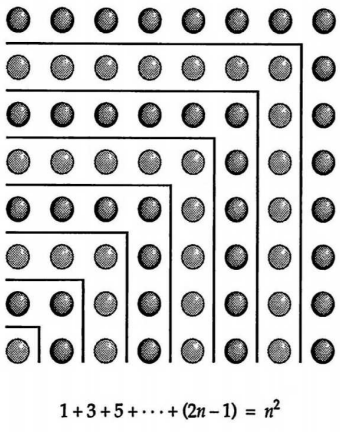
En mathématiques, une preuve sans mots (ou une démonstration visuelle) est une démonstration d'une identité (ou d'une affirmation mathématique plus générale) à l'aide d'un diagramme ou d'un dessin la rendant évidente, sans qu'un texte plus explicite le commentant soit nécessaire. Malgré les risques qu'elles présentent, ces démonstrations sont souvent considérées comme plus élégantes que des preuves mathématiquement plus rigoureuses.

Heuristique

Il s'agit d'une "démonstration" de la somme des nombres impairs trouvé par Nicomaque de Gérase en (l'an) 100. Une telle représentation graphique permet de démontrer d'un seul coup d'œil que la somme des nombres impairs est égale à la suite des nombres carrés ...



$1+3=2^2,$ $1+3+5=3^2,$ $1+3+5+7=4^2$



UN PEU D'HISTOIRE :

Nicomaque de Gérase, né à Gérase (actuelle Jerash, en Jordanie), vécut en 150 (d'autres sources donnent 50 - 120) est un mathématicien et philosophe néo-pythagoricien. Il est mort en 196 selon le philosophe John M. Dillon - ou en 142 (selon Andrew H. Criddle).
Dans son ouvrage *Introduction à l'arithmétique*, il étudie les nombres et cherche leurs propriétés métaphysiques. Ce n'est donc pas une œuvre en arithmétique au sens où on l'entendrait de nos jours. Il définit néanmoins les nombres pairs et impairs, les nombres premiers et composés, les nombres parfaits et remarques plusieurs propriétés intéressantes ...

E. Critères de divisibilté

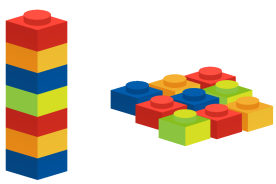
Une critère ou une règle de divisibilité est un moyen « *rapide* » de vérifier si un nombre donné est divisible par un diviseur fixe sans effectuer la division, généralement en examinant ses chiffres.

Divisibilité par	Énoncé du critère	Exemple
1	Tout nombre entier est divisible par 1.	1, 2, 3,4 sont divisibles par 1.
2	Un nombre est divisible par 2 si et seulement si son dernier chiffre est un chiffre pair (0, 2, 4, 6, 8).	1548 est divisible par 2 car son dernier chiffre est pair (8).
3	Un nombre est divisible par 3 si et seulement si la somme de ses chiffres est divisible par 3.	864 est divisible par 3 car $8+6+4=18$ (divisible par 3).
4	Un nombre est divisible par 4 si et seulement si le nombre formé par ses 2 derniers chiffres est divisible par 4.	2588 est divisible par 4 ($88=22\times 4$).
5	Un nombre est divisible par 5 si et seulement si son chiffre des unités est 0 ou 5.	1254410 est divisible par 5 car son dernier chiffre est 0.
6	Un nombre est divisible par 6 si et seulement s'il est à la fois divisible par 2 **et** par 3.	24186 est divisible par 6 car 6 est un chiffre pair **et** $2+4+1+8+6=21(3\times 7)$
8	Un nombre est divisible par 8 si et seulement si le nombre formé par ses 3 derniers chiffres est divisible par 8.	636136 est divisible par 8 car 136 est divisible par 8 (17×8).
9	Un nombre est divisible par 9 si et seulement si la somme de ses chiffres est divisible par 9	423 est divisible par 9 car $4+2+3=9$.
10	Un nombre est divisible par 10 si et seulement si son chiffre des unités est 0.	211055460 est divisible par 10 car son chiffre des unités est 0.
11	La différence entre la somme de ses chiffres de rangs pairs et la somme de ses chiffres de rangs impairs est un multiple de 11	80927 est un multiple de 11 car : $(8+9+7)-(0+2)=22\ \ (2\times 11)$
13	SUn nombre est divisible par 13 si son nombre de dizaines plus quatre fois le chiffre des unités est divisible par 13.	$156 : 15+(4\times 6)=39=3\times 13$ donc divisible par 13.
25	Un nombre est divisible par 25 si et seulement s'il se termine par 00 ; 25 ; 50 ; 75.	215375 est divisible par 25 car il se termine par 75.

Exemple

Jane joue avec des blocs.
Elle veut mettre ses 49 blocs en piles avec le même nombre de blocs dans chaque pile.

Combien de blocs pourrait-elle mettre dans chaque pile ?



2. Nombres premiers

A. Définition d'un nombre premier

DÉFINITION

Un nombre entier naturel est un **nombre premier** s'il admet exactement deux diviseurs positifs (qui sont 1 et lui-même).

Exemple

Les nombres premiers inférieurs à 100 sont :

$$2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97$$

REMARQUE :

- 1 n'est pas un nombre premier car il n'admet qu'un seul diviseur positif : lui-même.
- 0 n'est pas non plus un nombre premier car il admet une infinité de diviseurs.

REMARQUE : Pour une liste plus grande des nombres premiers (inférieurs à 10 000), on pourra la trouver en fin de cours dans la partie *Récréation, énigmes*.

PRENONS DE LA HAUTEUR : Dans un passé encore proche, on considérait autrefois que 1 est premier. Ce n'est qu'au tout début des années 1960, avec l'introduction des mathématiques dites *modernes* que 1 perd son statut de nombre premier (Lebossé et Hémery, 1947).

B. Le crible d'Ératosthène

Chercher des nombres premiers est un problème très ancien ! Eratosthène (276 av. J.-C. - 194 av. J.-C.) proposait une méthode afin de les trouver. On va l'illustrer sur un exemple : prenons la liste des entiers naturels jusqu'à 50 et barrons 1 (car 1 n'est pas premier !).

~~1~~	2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50

Puis Eratosthène eu l'idée suivante : "*Mais si je barre tous les multiples de* 2 *(autres que* 2*), bah c'est sûr que les nombres barrés ne sont pas premiers puisqu'un nombre premier n'a que* 1 *et lui-même en diviseur !* " Donc il barre tous les multiples de 2 :

~~1~~	2	3	~~4~~	5	~~6~~	7	~~8~~	9	~~10~~
11	~~12~~	13	~~14~~	15	~~16~~	17	~~18~~	19	~~20~~
21	~~22~~	23	~~24~~	25	~~26~~	27	~~28~~	29	~~30~~
31	~~32~~	33	~~34~~	35	~~36~~	37	~~38~~	39	~~40~~
41	~~42~~	43	~~44~~	45	~~46~~	47	~~48~~	49	~~50~~

"*Nom de Zeus !*" dit Eratosthène (bon en fait, c'est Doc dans "Retour dans le futur" qui dit ça ...) Eratosthène constate qu'il s'est débarassé d'un bon paquet de nombres qui ne sont pas premiers ! Il continue en se disant : "*Mais maintenant si je barre tous les multiples de* 3 *(autres que* 3*), bah c'est sûr que les nombres barrés ne sont pas premiers puisqu'un*

nombre premier n'a que 1 *et lui-même en diviseur !* " Donc il barre tous les multiples de 3 :

~~1~~	2	3	~~4~~	5	~~6~~	7	~~8~~	~~9~~	~~10~~
11	~~12~~	13	~~14~~	~~15~~	~~16~~	17	~~18~~	19	~~20~~
~~21~~	~~22~~	23	~~24~~	25	~~26~~	~~27~~	~~28~~	29	~~30~~
31	~~32~~	~~33~~	~~34~~	35	~~36~~	37	~~38~~	~~39~~	~~40~~
41	~~42~~	43	~~44~~	~~45~~	~~46~~	47	~~48~~	49	~~50~~

Eratosthène se frotte les mains et il continue en se disant : "*Mais maintenant si je barre tous les multiples de* 5 *(autres que* 5*), bah ...* ! " Oui, c'est bon, on a compris ... Donc il barre tous les multiples de 5 :

~~1~~	2	3	~~4~~	5	~~6~~	7	~~8~~	~~9~~	~~10~~
11	~~12~~	13	~~14~~	~~15~~	~~16~~	17	~~18~~	19	~~20~~
~~21~~	~~22~~	23	~~24~~	~~25~~	~~26~~	~~27~~	~~28~~	29	~~30~~
31	~~32~~	~~33~~	~~34~~	~~35~~	~~36~~	37	~~38~~	~~39~~	~~40~~
41	~~42~~	43	~~44~~	~~45~~	~~46~~	47	~~48~~	49	~~50~~

Puis les multiples de 7 (sauf 7) :

~~1~~	2	3	~~4~~	5	~~6~~	7	~~8~~	~~9~~	~~10~~
11	~~12~~	13	~~14~~	~~15~~	~~16~~	17	~~18~~	19	~~20~~
~~21~~	~~22~~	23	~~24~~	~~25~~	~~26~~	~~27~~	~~28~~	29	~~30~~
31	~~32~~	~~33~~	~~34~~	~~35~~	~~36~~	37	~~38~~	~~39~~	~~40~~
41	~~42~~	43	~~44~~	~~45~~	~~46~~	47	~~48~~	~~49~~	~~50~~

Et voilà le travail ! Il ne reste que des nombres premiers ! Bien évidemment, si on prend un nombre plus grand que 50 et que l'on regarde les nombres premiers qui lui sont inférieurs, il ne faudra pas s'arrêter à 7 comme diviseur mais aller au-delà. La proposition qui suit peut nous aider à ne pas faire trop de calculs ...

C. Test de primalité

PROPOSITION

Soit n un entier supérieur ou égal à 2.
Si n n'admet pour diviseur aucun des nombres premiers inférieurs ou égaux à $\sqrt{n}$, alors n est un nombre premier.

ATTENTION : Cette proposition repose sur la proposition suivante tout aussi importante :

« Tout entier naturel supérieur ou égal à 2 est divisible par un nombre premier. »

REMARQUE : On pourrait se demander en quoi ce théorème est si intéressant que ça. Il est très efficace pour décider si un nombre est premier ou non ! Par exemple, si l'on doit utiliser le crible d'Eratosthène pour savoir si 101 est premier, ça peut être un peu long (et encore plus si l'on ne connait pas ses tables de multiplications ...). Tandis qu'avec cette proposition, voici comment on procède :

Exemple

On prend la racine carré de 101 (qui vaut environ 10,05). Puis on regarde les nombres premiers inférieurs à $\sqrt{101}$. Cool ! Il y en a pas beaucoup : 2, 3, 5, 7. Enfin, on regarde si ces 4 nombres premiers divisent 101 : ça n'est pas le cas ! Donc, d'après le test de primalité, on en déduit que 101 est premier. Simple, rapide, élégant !

REMARQUE : 2022 et 2023 ne sont pas des nombres premiers. La prochaine année première sera 2027. Et les suivantes : 2029, 2039, 2053, 2063, 2069, 2081, 2083, 2087, 2089, 2099 ...

UN PEU D'HISTOIRE :

Ératosthène de Cyrène, ou simplement Ératosthène, est un astronome, géographe, philosophe et mathématicien grec du iiie siècle av. J.-C. (Cyrène, v. -276 – Alexandrie, Égypte, v. -194).
Il est surtout connu pour avoir mesuré la circonférence de la Terre avec ... un bâton et un chameau ... Il trouva environ 39500 km. En sachant qu'aujourd'hui, avec les techniques modernes, on sait que la circonférence de la Terre est 40075 km. Il s'est trompé seulement de 575 km ... soit une erreur d'environ 1,5% ... Calcul fait, il y a plus de 2200 ans avec un bâton et un chameau !

D. Une infinité de nombres premiers

PROPOSITION : Théorème d'Euclide

Il existe une infinité de nombres premiers.

ATTENTION : Cette démonstration est très classique et élémentaire ! Vous devez savoir la faire et surtout ... la comprendre !

PREUVE Supposons le contraire (*i.e.*) qu'il existe un nombre fini de nombres premiers, que nous noterons p_1, p_2,..., p_k. Considérons le nombre

$$N = p_1 p_2 ... p_k + 1$$

Si N est premier, alors on a trouvé un nombre premier plus grand que p_k, et on a donc une contradiction.
Si N est composé, alors N est divisible un nombre premier (*i.e.*) qu'il existe $i \in \{1, ..., k\}$ tel que $p_i \mid N$, mais alors on aurait $p_i \mid 1$. Absurde.

■

ATTENTION : Attention, les entiers

$$M_k = p_1 p_2 ... p_k + 1$$

ne sont pas tous premiers. En effet, $M_6 = 30031 = 59 \times 509$. De nos jours, on ne sait pas si la suite $(M_k)_{k \in \mathbb{N}}$ contient une infinité de nombres premiers ...

REMARQUE : Ce résultat est énoncé et démontré dans les Éléments d'Euclide, c'est la proposition 20 du livre IX. Il y prend cependant une forme différente : « *les nombres premiers sont plus nombreux que n'importe quelle multitude de nombres premiers proposée* », plus compatible avec la conception de l'infini de l'auteur.

E. Décomposition d'un entier en produit de facteurs premiers

PROPOSITION : Théorème fondamental de l'arithmétique

Tout entier naturel supérieur ou égal à 2 s'écrit soit comme une puissance d'un nombre premier, soit comme un produit de puissances de nombres premiers.

Plus précisement, tout nombre naturel $n > 1$ peut s'écrire de façon unique sous la forme

$$n = p_1^{a_1} p_2^{a_2} ... p_r^{a_r}$$

où les p_i sont des nombres premiers distincts et où les p_i sont des entiers positifs.
Cette écriture est unique, à l'ordre des facteurs près.

Exemple

- $25 = 5^2$
- $1116 = 2^2 \times 3^3 \times 31$

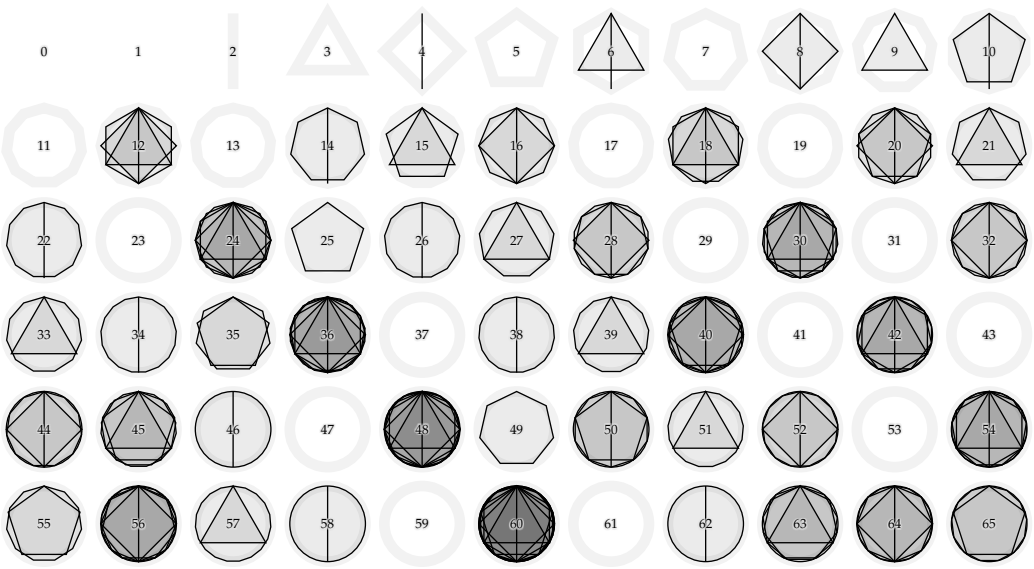
PÉDAGOGIE 5 Approche polygonale

Il existe plusieurs approches permettant de visualer la décomposition d'un entier en produit de facteurs premiers. Les moins connues restent les approches dites *géométriques*, et parmi celles-ci, il y a une approche très intéressante qualifiée de *polygonale*.

Heuristique

L'idée est très simple, dans un premier temps, on liste les nombres et on représente le polygone régulier avec le nombre de côtés correspondant.
Dans un second temps, on superpose sur ces les susdits polygones, les polygones correspondants à leur décomposition.

Par exemple, pour le nombre 6, on a un hexagone. On superpose sur cet hexagone un segment et un triangle équilatéral (car $6 = 2 \times 3$).



PÉDAGOGIE 6 Différentes approches de la décomposition d'un entier en produit de facteurs premiers

Ce théorème est loin d'être évident... Je vous conseille d'aller voir un exemple assez particulier dans la partie *Récréation, énigmes*...
On voit là l'intérêt des nombres premiers : ils permettent une « *décomposition atomique* » où les *atomes* seraient justement les nombres premiers (car "on ne peut plus casser" en des nombres plus petits).

Afin de trouver la décomposition d'un entier en produit de facteurs premiers, il peut être très intéressant de varier les approches.

Heuristique

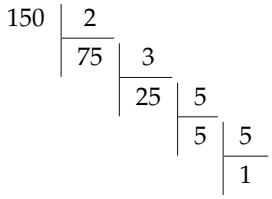
- **La méthode classique :**

$$150 = 2 \times 75$$
$$150 = 2 \times 3 \times 25$$
$$150 = 2 \times 3 \times 5 \times 5$$
$$150 = 2 \times 3 \times 5^2$$

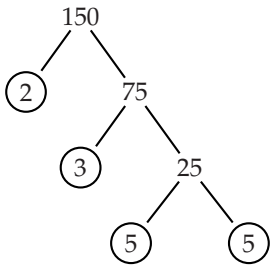
- **La barre verticale :** où l'on écrit la décomposition sous la forme d'un tableau présentant la décomposition sur le côté droit du tableau.

150	2
75	3
25	5
5	5
1	

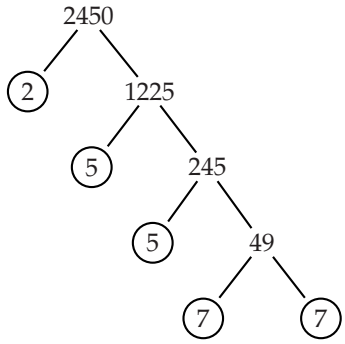
- **La potence :** où l'on écrit la décomposition sous la forme d'une suite de « divisions ».



- **L'arbre :**



Remarque : On pourrait donc très bien imaginer une rédaction de la sorte :
Écrire la décomposition en produit de facteurs premiers du nombre 2 450.
On décompose 2 450 :



$$2\,450 = 2 \times 1\,225$$
$$2\,450 = 2 \times 5 \times 245$$
$$2\,450 = 2 \times 5 \times 5 \times 49$$
$$2\,450 = 2 \times 5 \times 5 \times 7 \times 7$$

Par conséquent, on écrit :

$$2\,450 = 2 \times 5^2 \times 7^2$$

F. Application à la détermination du PGCD et du PPCM

DÉFINITION

Soient a et b sont deux entiers non nuls.
On appelle **plus grand diviseur commun** de a et de b, et on note $\text{PGCD}(a;b)$, le plus grand des diviseurs communs positifs de a et de b.
On appelle **plus petit multiple commun** de a et de b, et on note $\text{PPCM}(a;b)$, le plus petit des multiples communs positifs de a et de b.

REMARQUE :

- On a $\text{PGCD}(a;0) = |a|$ et, par convention, $\text{PGCD}(0;0) = 0$.
- Un nombre entier et son opposé ont les mêmes diviseurs. On se restreint donc au cas des entiers naturels.

PROPOSITION

Soient a et b deux entiers relatifs non simultanément nuls.

- $\text{PGCD}(a;b) \geq 1$; $\text{PGCD}(0;a) = a$; $\text{PGCD}(1;a) = 1$.
- a divise b si, et seulement si, $\text{PGCD}(a;b) = a$
- $\text{PGCD}(a;b) = \text{PGCD}(a-b;b)$ (Méthode de la soustraction).
- $\text{PGCD}(a;b)$ divise $\text{PPCM}(a;b)$
- $\text{PGCD}(a;b) \times \text{PPCM}(a;b) = a \times b$
- Si k est un entier naturel non nul, on a $\text{PPCM}(ka;kb) = k\text{PPCM}(a;b)$ (Homogénéité)

Exemple

$\text{PGCD}(229;225) = \text{PGCD}(229-225;225) = \text{PGCD}(4;225) = 1$ car 1 est le seul diviseur positif commun à 4 et 225.

PROPOSITION

Soient m et n deux entiers naturels supérieurs ou égaux à 2. On suppose, quitte à utiliser des exposants nuls, que m et n peuvent s'écrire sous forme de produit de facteurs premiers de la manière suivante :

$$n = p_1^{\alpha_1} \times p_2^{\alpha_2} \times \ldots \times p_k^{\alpha_k} \text{ et } m = p_1^{\beta_1} \times p_2^{\beta_2} \times \ldots \times p_k^{\beta_k}$$

On a alors :

$$\text{PGCD}(m;n) = p_1^{\min(\alpha_1;\beta_1)} \times p_2^{\min(\alpha_2;\beta_2)} \times \ldots \times p_k^{\min(\alpha_k;\beta_k)}$$
$$\text{PPCM}(m;n) = p_1^{\max(\alpha_1;\beta_1)} \times p_2^{\max(\alpha_2;\beta_2)} \times \ldots \times p_k^{\max(\alpha_k;\beta_k)}$$

NOTATION : On peut réécrire la proposition précédente comme suit :
Si $n = \prod_{i=1}^{r} p_i^{\alpha_i}$ et $m = \prod_{i=1}^{r} p_i^{\beta_i}$, avec $\alpha_i > 0$ et $\beta_i > 0$ pour chaque i, sont les représentations canoniques de n et m, alors :

$$\text{PGCD}(n,m) = \prod_{i=1}^{r} p_i^{\min(\alpha_i,\beta_i)} \quad \text{et} \quad \text{PPCM}(n,m) = \prod_{i=1}^{r} p_i^{\max(\alpha_i,\beta_i)}$$

MÉTHODE 1 Trois méthodes pour trouver le PPCM de deux nombres

À ce stade, nous avons donc trois méthodes pour déterminer le PPCM de deux nombres.

Nous allons donc calculer $PGCD(72,132)$ de trois manières différentes :

- **Méthode 1 : Énumération des multiples**

  Les multiples de 132 sont :

  $0\,;\,132\,;\,264\,;\,396\,;\,528\,;\,660\,;\,792\,;\,924\,;\,\ldots$ (liste infinie)

  Les multiples de 72 sont :

  $0\,;\,72\,;\,144\,;\,216\,;\,288\,;\,360\,;\,432\,;\,504\,;\,576\,;\,648\,;\,720\,;\,792\,;\,\ldots$ (liste infinie)

  Les multiples communs sont : $0\,;\,792\,;\,\ldots$ (On trouverait ensuite : $1584\,;\,2372\,;\,\ldots$)

  Le plus petit multiple commun non nul est 792.

  REMARQUE : Les multiples communs sont les multiples du PPCM.

- **Méthode 2 : Avec la formule PGCD$(a;b)\times$ PPCM$(a;b) = a \times b$**

  Le produit de deux nombres entiers (non nuls) est toujours égal au produit de leur PGCD par leur PPCM.

  On peut commencer par calculer le PGCD de 72 et 132. On trouve : $\text{PGCD}(72;132) = 12$.

  Donc :

  $$\text{PPCM}(72;132) = \frac{72 \times 132}{\text{PGCD}(72;132)} = 792$$

  REMARQUE : À ce propos, il existe une « *blague de mathématicien·ne* » sous la forme d'une fausse proposition :

  PROPOSITION : Blague de mathématicien·ne

  - Le PGCD de deux nombres est utilisé pour trouver le PPCM de ces deux nombres.
  - Le PPCM de deux nombres est utilisé pour trouver le PGCD de ces deux nombres.

- **Méthode 3 : Décomposition d'un entier en produit de facteurs premiers**

  $$72 = 2 \times 2 \times 2 \times 3 \times 3 = 2^3 \times 3^2$$
  $$132 = 2 \times 2 \times 3 \times 11 = 2^2 \times 3^1 \times 11^1$$

  Prenons tous les facteurs qui figurent dans l'un au moins de ces produits ; s'ils ont des exposants, nous leur attribuons leur plus grand exposant ; effectuons ensuite le produit :

  $$\text{PPCM}(72;132) = 2^3 \times 3^2 \times 11^1 = 8 \times 9 \times 11 = 792$$

MÉTHODE 2 Trois méthodes pour trouver le PGCD de deux nombres

À ce stade, nous avons donc trois méthodes pour déterminer le PGCD de deux nombres.

Nous allons donc calculer $PGCD(72, 132)$ de trois manières différentes :

- **Méthode 1 : Énumération de tous les diviseurs**

  On énumère tous les diviseurs des deux nombres.
  Les diviseurs de 72 sont : $1; 2; 3; 4; 6; 8; 9; 12; 18; 24; 36; 72$.
  En effet : $72 = 1 \times 72 = 2 \times 36 = 3 \times 24 = 4 \times 18 = 6 \times 12 = 8 \times 9$.
  Les diviseurs de 132 sont : $1; 2; 3; 4; 6; 11; 12; 22; 33; 44; 66; 132$.
  En effet : $132 = 1 \times 132 = 2 \times 66 = 3 \times 44 = 4 \times 33 = 6 \times 22 = 11 \times 12$.

  Les diviseurs communs (présents dans les deux listes) sont : $1; 2; 3; 4; 6; 12$. **Le plus grand diviseur commun est donc :** 12.

- **Méthode 2 : Méthode de la soustraction**

  On réalise des soustractions successives, en utilisant le fait que Principe : si $a < b$, alors : $\text{PGCD}(a; b) = \text{PGCD}(a - b; b)$.
  Il est donc permis de remplacer le plus grand des deux nombres par la différence des deux nombres (car ceci ne change pas le PGCD).

  $\text{PGCD}(72, 132) = \text{PGCD}(72, 132 - 72) = \text{PGCD}(72, 60)$
  $\text{PGCD}(72, 60) = \text{PGCD}(72 - 60, 60) = \text{PGCD}(12, 60)$
  $\text{PGCD}(12, 60) = \text{PGCD}(12, 60 - 12) = \text{PGCD}\ (12, 48)$
  $\text{PGCD}(12, 48) = \text{PGCD}(12, 48 - 12) = \text{PGCD}(12, 36)$
  $\text{PGCD}(12, 36) = \text{PGCD}(12, 36 - 12) = \text{PGCD}(12, 24)$
  $\text{PGCD}(12, 24) = \text{PGCD}(12, 24 - 12) = \text{PGCD}(12, 12)$.

  À partir de là, la solution est évidente : le PGCD est 12.

- **Méthode 3 : Décomposition d'un entier en produit de facteurs premiers**

  On décompose les deux nombres en produits de facteurs premiers.

  $$72 = 2 \times 2 \times 2 \times 3 \times 3 = 2^3 \times 3^2$$
  $$132 = 2 \times 2 \times 3 \times 11 = 2^2 \times 3^1 \times 11^1$$

  Pour calculer le PGCD, on sélectionne les facteurs communs (présents dans les deux produits) ; s'ils figurent avec des exposants, nous leur attribuons leur plus petit exposant ; ensuite nous effectuons le produit :

  $$PGCD(72, 132) = 2^2 \times 3^1 = 4 \times 3 = 12$$

REMARQUE : En général, l'algorithme d'Euclide est plus efficace pour calculer le PGCD.

G. Algorithme d'Euclide

PROPOSITION

On note q et r le quotient et le reste de la division euclidienne de a par b.
Avec ces notations, PGCD$(a;b)$ =PGCD$(b;r)$.

Exemple

$546 = 60 \times 9 + 6$ donc PGCD$(546;60)$ = PGCD$(60;6)$ = PGCD$(6 \times 10;6) = 6$.

PROPOSITION : Algorithme d'Euclide

Soient a et b deux entiers naturels non nuls, avec $a > b$.
On divise a par b.

$$a = bq_1 + r_1, \text{ avec } 0 \leqslant r_1 < b.$$

- Si $r_1 = 0$, alors PGCD$(a\ ;\ b) = b$ puisque b divise a.
- Si $r_1 \neq 0$, PGCD$(a\ ;\ b)$=PGCD$(b\ ;\ r_1)$. On effectue alors la division de b par r_1.

On a :

$$b = r_1q_2 + r_2, \text{ avec } 0 \leqslant r_2 < r_1.$$

- Si $r_2 = 0$, alors PGCD$(a\ ;\ b)$=PGCD$(b\ ;\ r_1) = r_1$.
- Si $r_2 \neq 0$, PGCD$(b\ ;\ r_1)$=PGCD$(r_1\ ;\ r_2)$.

On continue la suite de divisions euclidiennes en divisant un reste par le reste suivant. On obtient une suite de restes $r_1, r_2, \ldots, r_n$, avec $r_1 > r_2 > r_3 \cdots \geqslant 0$. Comme ce sont des entiers, il existe un reste qui est nul.
Notons r_n le dernier reste non nul. Alors :

$$\text{PGCD}(a\ ;\ b)=\text{PGCD}(b\ ;\ r_1)=\text{PGCD}(r_1\ ;\ r_2) = \cdots =\text{PGCD}(r_{n-1}\ ;\ r_n) = r_n$$

car r_n divise r_{n-1}

NOTATION : On peut visualiser l'algorithme de la manière suivante :

Etape	Division	Dividende	Diviseur	Reste
1	$a = bq_1 + r_1$	a	b	$0 \leqslant r_1 < b$
2	$b = r_1q_2 + r_2$	b	r_1	$0 \leqslant r_2 < r_1$
$\ldots$	$\ldots$	$\ldots$	$\ldots$	$\ldots$
n	$r_{n-1} = r_nq_{n+1} + 0$	r_{n-1}	r_n	$0 \leqslant r_{n-1} < r_n$

REMARQUE : Cet algorithme fut décrit par Euclide au IIIème siècle avant J.-C.

Exemple

Calculons par l'algorithme d'EUCLIDE le PGCD des nombres 753 et 345.

$$753 = 345 \times 2 + 63$$
$$345 = 63 \times 5 + 30$$
$$63 = 30 \times 2 + 3$$
$$30 = 3 \times 10 + 0$$

Le PGCD des nombres 753 et 345 est le dernier reste non nul du procédé, c'est-à-dire 3.

Remarque : Malgré sa simplicité (relative), c'est un algorithme très efficace, même en partant avec de très grands nombres comme le montre l'exemple ci-dessous :

$$
\begin{aligned}
2220690239027589097 &= 2 \times 8169486210102119257 + 5868007818823350583\\
8169486210102119257 &= 1 \times 5868007818823350583 + 2301478391278768674\\
5868007818823350583 &= 2 \times 2301478391278768674 + 1265051036265813235\\
2301478391278768674 &= 1 \times 1265051036265813235 + 1036427355012955439\\
1265051036265813235 &= 1 \times 1036427355012955439 + 228623681252857796\\
1036427355012955439 &= 4 \times 228623681252857796 + 121932630001524255\\
228623681252857796 &= 1 \times 121932630001524255 + 106691051251333541\\
121932630001524255 &= 1 \times 106691051251333541 + 15241578750190714\\
106691051251333541 &= 6 \times 15241578750190714 + 15241578750189257\\
15241578750190714 &= 1 \times 15241578750189257 + 1457\\
15241578750189257 &= 10460932567048 \times 1457 + 321\\
1457 &= 4 \times 321 + 173\\
321 &= 1 \times 173 + 148\\
173 &= 1 \times 148 + 25\\
148 &= 5 \times 25 + 23\\
25 &= 1 \times 23 + 2\\
23 &= 11 \times 2 + 1\\
2 &= 2 \times 1 + 0
\end{aligned}
$$

H. Nombres premiers entre eux

DÉFINITION

Soient a et b deux entiers relatifs non nuls.
a et b sont **premiers entre eux** lorsque leurs seuls diviseurs communs sont 1 et -1.
Autrement dit, a et b sont premiers entre eux lorsque $\text{PGCD}(a;b) = 1$.

Remarque : Deux nombres premiers distincts sont premiers entre eux.

Exemple

18 et 35 sont premiers entre eux car 35 est un multiple de 1;5;7 et 35 alors que 18 n'est divisible par aucun de ces nombres autres que 1. Donc le PGCD de 18 et 35 vaut 1.

PROPOSITION

Si a et b sont deux nombres premiers entre eux, on a $\text{PPCM}(a;b) = a \times b$.

PROPOSITION

Soient a et b deux entiers relatifs non nuls.
Soient $d = \text{PGCD}(a;b)$ et a',b' les entiers tels que $a = da'$ et $b = db'$.
Alors a' et b' sont premiers entre eux.
Réciproquement, s'il existe $d \in \mathbb{N}$ et a', b' des entiers premiers entre eux tels que $a = da'$ et $b = db'$, alors d est le PGCD de a et b.

Exemple

$36 = 12 \times 3$ et $60 = 12 \times 5$. Puisque 3 et 5 sont premiers entre eux, alors $\text{PGCD}(60;36) = 12$.

Je teste mes connaissances

À la fin de ce chapitre, je dois être capable de :

- Déterminer si un nombre est premier ou non.
- Dresser la liste des nombres premiers inférieurs à un nombre entier donné.
- Décomposer un nombre en produit de facteurs premiers.
- Déterminer les diviseurs d'un nombre entier.
- Déterminer le PGCD et le PPCM de deux nombres entiers à l'aide d'une décomposition en produit de facteurs premiers.
- Modéliser et résoudre des problèmes mobilisant les notions de multiple, de diviseur, de nombre pair, de nombre impair, de nombre premier.

QCM d'auto-évaluation

coucou@coquillagesetpoincare.fr
pour toute(s) question(s) / remarque(s).

Voici un QCM d'auto-évaluation pour vous tester. Vous avez quelques questions reprenant l'ensemble des notions abordées dans ce cours.

5 L'ensemble des diviseurs positifs de 14 est

(a) $\{2;7\}$ (b) $\{2;7;14\}$ (c) $\{1;2;7;12\}$

6 La division euclidienne de 30 par 8 s'écrit

(a) $30 = 8 \times 3 + 6$ (b) $30 = 8 \times 4 - 2$ (c) $30 = 8 \times 3 + 0,75$

7 Un entier n est impair si et seulement son reste dans la division euclidienne par 2 vaut

(a) 0. (b) 1. (c) 2.

8 La courbe de f est

(a) une droite (b) une parabole (c) autre

9 Soient a et b deux entiers relatifs non simultanément nuls. Alors $a \times b =$

(a) $\text{PGCD}(a;b) \div \text{PPCM}(a;b)$ (b) $\text{PGCD}(a;b) \times \text{PPCM}(a;b)$ (c) $\text{PGCD}(a;b) + \text{PPCM}(a;b)$

10 $\text{PGCD}(28;77) =$

(a) 308 (b) 153 (c) 7

11 $\text{PPCM}(18;42) =$

(a) 126 (b) 73 (c) 6

Multiples et diviseurs

12 Multiple ou diviseur ?

CORRIGÉ

Recopier les phrases suivantes et les compléter par *multiple* ou *diviseur* :

1) 250 est un ... de 50.
2) 0 est un ... de 15.
3) 2023 est un ... de 0.
4) 21 est un ... de -2100.
5) 1 est un ... de 4.
6) 37 est un ... de 37.

13 Pour tout entier n

CORRIGÉ

On considère un entier naturel n.
Démontrer que $3n-1$ divise $6n^2-2n$.

14 VRAI/FAUX I

CORRIGÉ

Les propositions suivantes sont-elles vraies ou fausses ? Justifier.

1) La somme de trois entiers consécutifs est un multiple de 3.
2) La somme de quatre entiers consécutifs est un multiple de 4.
3) La somme de cinq entiers consécutifs est un multiple de 5.

15 VRAI/FAUX II

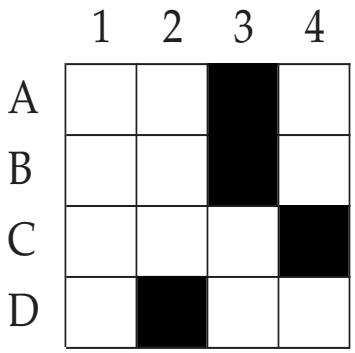
CORRIGÉ

Les propositions suivantes sont-elles vraies ou fausses ? Justifier.

- Le produit de deux multiples de 3 est un multiple de 9.
- Le produit d'un multiple de 4 et d'un multiple de 6 est un multiple de 24.

16 Nombres croisés

CORRIGÉ



Horizontalement

A - Multiple de 3 et de 5. • Diviseur de 25.
B - Multiple de 10. • Diviseur de tous les nombres.
C - Diviseur de 222 autre que lui-même.
D - Multiple de 5 (mais pas de 10) si on lui ajoute 1. • Multiple de 12 et 7.

Verticalement

1 - Nombre palindrome.
2 - Multiple de 100 si on lui enlève 1.
3 - Multiple de 2 et de 3.
4 - Multiple de 17.

Nombre pair et impair

17 Impair + Impair

CORRIGÉ

Démontrer que la somme de deux nombres impairs est un nombre pair.

18 Entiers consécutifs

CORRIGÉ

Soit $n \in \mathbb{N}$.

1) Démontrer que si n est pair, alors $n(n+1)$ est pair.
2) Démontrer que si n est impair, alors $n(n+1)$ est pair.
3) Que peut-on conclure sur $n(n+1)$?

19 Quatre entiers consécutifs

CORRIGÉ

Montrer que la somme de quatre nombres consécutifs est paire.

20 Carré et parité

CORRIGÉ

Démontrer que si a est un entier, a^2-a est pair.

S'entraîner

Nombres premiers

21 Décomposons

CORRIGÉ

Décomposer en produit de facteurs premiers les nombres suivants :

1) 27
2) 49
3) 100
4) 24

22 VRAI/FAUX III

CORRIGÉ

Les propositions suivantes sont-elles vraies ou fausses ? Justifier.

1) Il y a plus de nombres premiers entre 20 et 30 qu'entre 40 et 50.
2) Un diviseur d'un nombre premier est forcément premier.

23 La bonne paire

CORRIGÉ

On dit que deux nombres premiers forment une paire s'ils s'écrivent avec les mêmes chiffres mais en sens inverse. Par exemple, 1933 et 3391 forment une paire.

1) Expliquer pourquoi le premier chiffre d'un entier d'une paire ne peut être que 1, 3, 7 ou 9.
2) Trouver toutes les paires de nombres premiers à deux chiffres.

24 Avec une fonction

CORRIGÉ

Pour tout entier naturel m, on considère la fonction f définie par

$$f(m) = m^2 + m + 41$$

Pour tout entier naturel m, $f(m)$ est-il un nombre premier ?

PGCD & PCCM

25 Pour s'échauffer

1) Déterminer le PGCD de 4480 et 400 à l'aide de la décomposition en facteurs premiers.
2) Déterminer le PPCM de 4480 et 400.
3) Déterminer le PGCD de 3045 et 300 à l'aide de l'algorithme d'Euclide.
4) Déterminer le PPCM de 3045 et 300.

26 Mixité dans l'e-sport

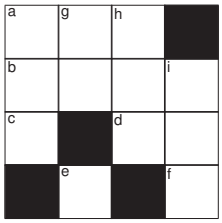
CORRIGÉ

Lors d'une convention d'e-sport, il y a 80 gameurs et 60 gameuses inscrits. L'organisation veut constituer un maximum d'équipes mixtes contenant le même nombre d'hommes et le même nombre de femmes.

Combien d'équipes peuvent être constituées ?

27 Nombres croisés II

CORRIGÉ



Horizontal

a $PGCD(125;250)$.
b Ce nombre est un multiple de 9.
c Le chiffre des unités d'un nombre divisible par 10.
d Ce nombre est divisible par 5.
e Le reste de la division euclidienne de 121 par 8.
f Le quotient dans celle de 245 par 112.

Vertical

a Le plus petit multiple de 24 à trois chiffres.
g Le quotient de la division euclidienne de 274 par 10.
e Diviseur commun à tous les entiers.
h $PGCD(1542;3598)$
i 3 est un diviseur de ce nombre.

Vu au CRPE

28 Groupement 2 - CRPE 2020 CRPE

Indiquer si les affirmations suivantes sont vraies ou fausses **en justifiant la réponse**.

Une réponse exacte mais non justifiée ne rapporte aucun point. Une réponse fausse, incorrecte ou une absence de réponse n'enlève pas de point.

1) **Affirmation 1 :** « le nombre 4 700 001 est un nombre premier »
2) **Affirmation 2 :** « les nombres 32^{12} et $16^{15}+3$ sont égaux »
3) **Affirmation 3 :** « La somme des carrés de deux nombres entiers naturels consécutifs est toujours un nombre impair. »

29 Groupement 5 - CRPE 2020 CRPE

Pour chacune des affirmations ci-dessous, indiquer si elle est vraie ou fausse en justifiant la réponse.
Une réponse non justifiée ne rapporte aucun point.

1) **Affirmation 1 :** « Le nombre $\frac{27}{45}$ est un nombre décimal. »
2) **Affirmation 2 :** « Si a et b sont deux nombres décimaux positifs non nuls, alors le résultat de la division de a par b est plus petit que a. »
3) **Affirmation 3 :** « La somme de trois entiers consécutifs est toujours un multiple de 3. »
4) **Affirmation 4 :** « 42 possède exactement 7 diviseurs positifs. »

30 Groupement 3 - CRPE 2019 CRPE

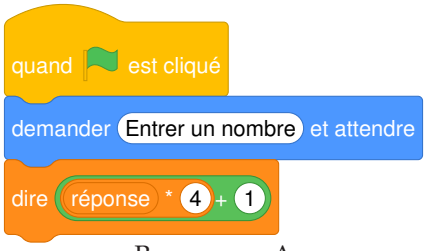
1) Pour tout nombre entier n, montrer que $30n+25$ est divisible par 5 .
2) Voici un programme de calcul :

- Choisir un nombre entier
- Multiplier par 3
- Ajouter 5
- Élever au carré
- Soustraire 9 fois le carré du nombre de départ

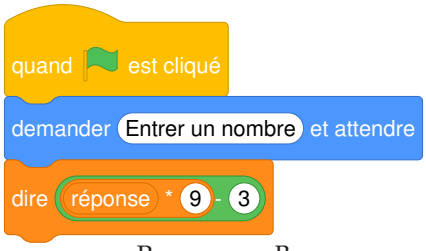
   a) Montrer que ce programme a pour résultat 265 si le nombre entier choisi est 8. Les calculs seront détaillés.
   b) Quel résultat obtient-on si le nombre entier choisi est (-56) ?
   c) Montrer que le résultat de ce programme de calculs, quel que soit le nombre de départ, est divisible par 5.

31 Groupement 4 - CRPE 2019 CRPE

On dispose des deux programmes de calcul ci-dessous :



Programme A



Programme B

1) Différents nombres sont entrés dans le programme A.
   a) Montrer que quand on entre le nombre 5, la réponse obtenue est le nombre 27.
   b) Quel nombre est obtenu quand on entre le nombre $\frac{7}{10}$? Justifier la réponse.
2) Quel nombre faut-il entrer dans le programme B pour que le résultat affiché soit égal à 0,69 ?
3) Prouver que quand on entre un nombre impair dans le programme B, le nombre obtenu est toujours un multiple de 6.
4) Existe-t-il des nombres qui permettent d'avoir le même résultat affiché avec les deux programmes ? Si oui, déterminer tous ces nombres.

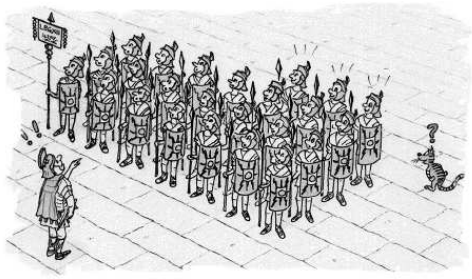
La liste des nombres premiers inférieurs à 10 000

2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97, 101, 103, 107, 109, 113, 127, 131, 137, 139, 149, 151, 157, 163, 167, 173, 179, 181, 191, 193, 197, 199, 211, 223, 227, 229, 233, 239, 241, 251, 257, 263, 269, 271, 277, 281, 283, 293, 307, 311, 313, 317, 331, 337, 347, 349, 353, 359, 367, 373, 379, 383, 389, 397, 401, 409, 419, 421, 431, 433, 439, 443, 449, 457, 461, 463, 467, 479, 487, 491, 499, 503, 509, 521, 523, 541, 547, 557, 563, 569, 571, 577, 587, 593, 599, 601, 607, 613, 617, 619, 631, 641, 643, 647, 653, 659, 661, 673, 677, 683, 691, 701, 709, 719, 727, 733, 739, 743, 751, 757, 761, 769, 773, 787, 797, 809, 811, 821, 823, 827, 829, 839, 853, 857, 859, 863, 877, 881, 883, 887, 907, 911, 919, 929, 937, 941, 947, 953, 967, 971, 977, 983, 991, 997, 1009, 1013, 1019, 1021, 1031, 1033, 1039, 1049, 1051, 1061, 1063, 1069, 1087, 1091, 1093, 1097, 1103, 1109, 1117, 1123, 1129, 1151, 1153, 1163, 1171, 1181, 1187, 1193, 1201, 1213, 1217, 1223, 1229, 1231, 1237, 1249, 1259, 1277, 1279, 1283, 1289, 1291, 1297, 1301, 1303, 1307, 1319, 1321, 1327, 1361, 1367, 1373, 1381, 1399, 1409, 1423, 1427, 1429, 1433, 1439, 1447, 1451, 1453, 1459, 1471, 1481, 1483, 1487, 1489, 1493, 1499, 1511, 1523, 1531, 1543, 1549, 1553, 1559, 1567, 1571, 1579, 1583, 1597, 1601, 1607, 1609, 1613, 1619, 1621, 1627, 1637, 1657, 1663, 1667, 1669, 1693, 1697, 1699, 1709, 1721, 1723, 1733, 1741, 1747, 1753, 1759, 1777, 1783, 1787, 1789, 1801, 1811, 1823, 1831, 1847, 1861, 1867, 1871, 1873, 1877, 1879, 1889, 1901, 1907, 1913, 1931, 1933, 1949, 1951, 1973, 1979, 1987, 1993, 1997, 1999, 2003, 2011, 2017, 2027, 2029, 2039, 2053, 2063, 2069, 2081, 2083, 2087, 2089, 2099, 2111, 2113, 2129, 2131, 2137, 2141, 2143, 2153, 2161, 2179, 2203, 2207, 2213, 2221, 2237, 2239, 2243, 2251, 2267, 2269, 2273, 2281, 2287, 2293, 2297, 2309, 2311, 2333, 2339, 2341, 2347, 2351, 2357, 2371, 2377, 2381, 2383, 2389, 2393, 2399, 2411, 2417, 2423, 2437, 2441, 2447, 2459, 2467, 2473, 2477, 2503, 2521, 2531, 2539, 2543, 2549, 2551, 2557, 2579, 2591, 2593, 2609, 2617, 2621, 2633, 2647, 2657, 2659, 2663, 2671, 2677, 2683, 2687, 2689, 2693, 2699, 2707, 2711, 2713, 2719, 2729, 2731, 2741, 2749, 2753, 2767, 2777, 2789, 2791, 2797, 2801, 2803, 2819, 2833, 2837, 2843, 2851, 2857, 2861, 2879, 2887, 2897, 2903, 2909, 2917, 2927, 2939, 2953, 2957, 2963, 2969, 2971, 2999, 3001, 3011, 3019, 3023, 3037, 3041, 3049, 3061, 3067, 3079, 3083, 3089, 3109, 3119, 3121, 3137, 3163, 3167, 3169, 3181, 3187, 3191, 3203, 3209, 3217, 3221, 3229, 3251, 3253, 3257, 3259, 3271, 3299, 3301, 3307, 3313, 3319, 3323, 3329, 3331, 3343, 3347, 3359, 3361, 3371, 3373, 3389, 3391, 3407, 3413, 3433, 3449, 3457, 3461, 3463, 3467, 3469, 3491, 3499, 3511, 3517, 3527, 3529, 3533, 3539, 3541, 3547, 3557, 3559, 3571, 3581, 3583, 3593, 3607, 3613, 3617, 3623, 3631, 3637, 3643, 3659, 3671, 3673, 3677, 3691, 3697, 3701, 3709, 3719, 3727, 3733, 3739, 3761, 3767, 3769, 3779, 3793, 3797, 3803, 3821, 3823, 3833, 3847, 3851, 3853, 3863, 3877, 3881, 3889, 3907, 3911, 3917, 3919, 3923, 3929, 3931, 3943, 3947, 3967, 3989, 4001, 4003, 4007, 4013, 4019, 4021, 4027, 4049, 4051, 4057, 4073, 4079, 4091, 4093, 4099, 4111, 4127, 4129, 4133, 4139, 4153, 4157, 4159, 4177, 4201, 4211, 4217, 4219, 4229, 4231, 4241, 4243, 4253, 4259, 4261, 4271, 4273, 4283, 4289, 4297, 4327, 4337, 4339, 4349, 4357, 4363, 4373, 4391, 4397, 4409, 4421, 4423, 4441, 4447, 4451, 4457, 4463, 4481, 4483, 4493, 4507, 4513, 4517, 4519, 4523, 4547, 4549, 4561, 4567, 4583, 4591, 4597, 4603, 4621, 4637, 4639, 4643, 4649, 4651, 4657, 4663, 4673, 4679, 4691, 4703, 4721, 4723, 4729, 4733, 4751, 4759, 4783, 4787, 4789, 4793, 4799, 4801, 4813, 4817, 4831, 4861, 4871, 4877, 4889, 4903, 4909, 4919, 4931, 4933, 4937, 4943, 4951, 4957, 4967, 4969, 4973, 4987, 4993, 4999, 5003, 5009, 5011, 5021, 5023, 5039, 5051, 5059, 5077, 5081, 5087, 5099, 5101, 5107, 5113, 5119, 5147, 5153, 5167, 5171, 5179, 5189, 5197, 5209, 5227, 5231, 5233, 5237, 5261, 5273, 5279, 5281, 5297, 5303, 5309, 5323, 5333, 5347, 5351, 5381, 5387, 5393, 5399, 5407, 5413, 5417, 5419, 5431, 5437, 5441, 5443, 5449, 5471, 5477, 5479, 5483, 5501, 5503, 5507, 5519, 5521, 5527, 5531, 5557, 5563, 5569, 5573, 5581, 5591, 5623, 5639, 5641, 5647, 5651, 5653, 5657, 5659, 5669, 5683, 5689, 5693, 5701, 5711, 5717, 5737, 5741, 5743, 5749, 5779, 5783, 5791, 5801, 5807, 5813, 5821, 5827, 5839, 5843, 5849, 5851, 5857, 5861, 5867, 5869, 5879, 5881, 5897, 5903, 5923, 5927, 5939, 5953, 5981, 5987, 6007, 6011, 6029, 6037, 6043, 6047, 6053, 6067, 6073, 6079, 6089, 6091, 6101, 6113, 6121, 6131, 6133, 6143, 6151, 6163, 6173, 6197, 6199, 6203, 6211, 6217, 6221, 6229, 6247, 6257, 6263, 6269, 6271, 6277, 6287, 6299, 6301, 6311, 6317, 6323, 6329, 6337, 6343, 6353, 6359, 6361, 6367, 6373, 6379, 6389, 6397, 6421, 6427, 6449, 6451, 6469, 6473, 6481, 6491, 6521, 6529, 6547, 6551, 6553, 6563, 6569, 6571, 6577, 6581, 6599, 6607, 6619, 6637, 6653, 6659, 6661, 6673, 6679, 6689, 6691, 6701, 6703, 6709, 6719, 6733, 6737, 6761, 6763, 6779, 6781, 6791, 6793, 6803, 6823, 6827, 6829, 6833, 6841, 6857, 6863, 6869, 6871, 6883, 6899, 6907, 6911, 6917, 6947, 6949, 6959, 6961, 6967, 6971, 6977, 6983, 6991, 6997, 7001, 7013, 7019, 7027, 7039, 7043, 7057, 7069, 7079, 7103, 7109, 7121, 7127, 7129, 7151, 7159, 7177, 7187, 7193, 7207, 7211, 7213, 7219, 7229, 7237, 7243, 7247, 7253, 7283, 7297, 7307, 7309, 7321, 7331, 7333, 7349, 7351, 7369, 7393, 7411, 7417, 7433, 7451, 7457, 7459, 7477, 7481, 7487, 7489, 7499, 7507, 7517, 7523, 7529, 7537, 7541, 7547, 7549, 7559, 7561, 7573, 7577, 7583, 7589, 7591, 7603, 7607, 7621, 7639, 7643, 7649, 7669, 7673, 7681, 7687, 7691, 7699, 7703, 7717, 7723, 7727, 7741, 7753, 7757, 7759, 7789, 7793, 7817, 7823, 7829, 7841, 7853, 7867, 7873, 7877, 7879, 7883, 7901, 7907, 7919, 7927, 7933, 7937, 7949, 7951, 7963, 7993, 8009, 8011, 8017, 8039, 8053, 8059, 8069, 8081, 8087, 8089, 8093, 8101, 8111, 8117, 8123, 8147, 8161, 8167, 8171, 8179, 8191, 8209, 8219, 8221, 8231, 8233, 8237, 8243, 8263, 8269, 8273, 8287, 8291, 8293, 8297, 8311, 8317, 8329, 8353, 8363, 8369, 8377, 8387, 8389, 8419, 8423, 8429, 8431, 8443, 8447, 8461, 8467, 8501, 8513, 8521, 8527, 8537, 8539, 8543, 8563, 8573, 8581, 8597, 8599, 8609, 8623, 8627, 8629, 8641, 8647, 8663, 8669, 8677, 8681, 8689, 8693, 8699, 8707, 8713, 8719, 8731, 8737, 8741, 8747, 8753, 8761, 8779, 8783, 8803, 8807, 8819, 8821, 8831, 8837, 8839, 8849, 8861, 8863, 8867, 8887, 8893, 8923, 8929, 8933, 8941, 8951, 8963, 8969, 8971, 8999, 9001,

9007, 9011, 9013, 9029, 9041, 9043, 9049, 9059, 9067, 9091, 9103, 9109, 9127, 9133, 9137, 9151, 9157, 9161, 9173, 9181, 9187, 9199, 9203, 9209, 9221, 9227, 9239, 9241, 9257, 9277, 9281, 9283, 9293, 9311, 9319, 9323, 9337, 9341, 9343, 9349, 9371, 9377, 9391, 9397, 9403, 9413, 9419, 9421, 9431, 9433, 9437, 9439, 9461, 9463, 9467, 9473, 9479, 9491, 9497, 9511, 9521, 9533, 9539, 9547, 9551, 9587, 9601, 9613, 9619, 9623, 9629, 9631, 9643, 9649, 9661, 9677, 9679, 9689, 9697, 9719, 9721, 9733, 9739, 9743, 9749, 9767, 9769, 9781, 9787, 9791, 9803, 9811, 9817, 9829, 9833, 9839, 9851, 9857, 9859, 9871, 9883, 9887, 9901, 9907, 9923, 9929, 9931, 9941, 9949, 9967, 9973

Le problème du centurion

Le centurion ordonne à ses légionnaires :
« *Rangez-vous par 4 !* ». Les soldats s'exécutent, mais le dernier rang est incomplet : il ne compte que 3 soldats.
« *Mettez-vous par 5 !* », hurle alors le centurion ; mais au dernier rang, incomplet, on compte encore 3 soldats.
« *Eh bien, rangez-vous par 7 !* ». Encore une fois, le dernier rang reste incomplet : on y compte toujours 3 soldats.



Le problème est d'aider le centurion à ranger ses légionnaires pour que tous les rangs soient complets.

Une décomposition en produits de facteurs premiers pas comme les autres...

Alors revenons un peu sur la décomposition en nombres premiers... Elle peut paraître très simple, naturel, voire enfantine. Par exemple, $12 = 3 \times 4$ ou $24 = 2^3 \times 3$... Et il parait "évident" que cette décomposition soit unique... Que nenni !
Prenons par exemple l'ensemble des nombres pairs et appelons le $\mathcal{P}$. Donc on a

$$\mathcal{P} = \{0; 2; 4; 6; 8; 10; 12; 14; 16; 18; 20; 22; 24...\}$$

On va supposer que l'on ne connaît QUE ces nombres : les nombres pairs (et que l'on a jamais entendu parlé de notre vie des nombres impairs). Vous allez voir qu'il va se passer des choses étranges...
Prenons 60. Incontestablement, $60 \in \mathcal{P}$. De plus, on a

$$60 = 10 \times 6$$
$$60 = 30 \times 2$$

Mais vous me direz "Ouais et ?". Eh bah, DANS $\mathcal{P}$, 30, 10, 6 sont des nombres premiers ! Vous allez me dire "Bah non ! On a bien $30 = 15 \times 2$ par exemple !". Oui mais 15 n'appartient pas à $\mathcal{P}$, et rappelez vous, on n'a dit que l'on ne connaissait que les nombres pairs ! Idem pour 10 qui s'écrit 5×2 ($5 \notin \mathcal{P}$) et pour 6 qui s'écrit 3×2 ($3 \notin \mathcal{P}$).
Donc, ce qui est incroyable ici, c'est que l'on n'a pas une décomposition unique en nombres premiers...

Quelques questions...

- Existe-t-il une infinité de nombres premiers de la forme $n^2 + 1$, $n \in \mathbb{N}$?
- Existe-t-il une infinité de nombres premiers de la forme $n! + 1$, $n \in \mathbb{N}$?
- Existe-t-il une infinité de nombres premiers jumeaux, c'est à dire des nombres premiers p_n et p_{n+1} tels que $p_{n+1} - p_n = 2$? Cousins ($p_{n+1} - p_n = 4$) ? Sexys ($p_{n+1} - p_n = 6$) ?