Arithmétique

Plan du chapitre :

Aperçu historique :

Le mot arithmétique vient du grec ancien *arithmos* qui signifie « nombre », dans le sens qu'avait le mot à cette époque de « nombre entier ». L'origine de l'arithmétique est très ancienne, sans doute phénicienne. Au VI^{e} siècle avant J.-C., Pythagore (580-495 avant J.-C.) et son école en font un des quatre piliers des mathématiques, à côté de la géométrie, de l'astronomie et de la musique. Ce fameux *quadrivium* quantitatif fut regroupé avec le trivium, plus littéraires (grammaire, rhétorique, dialectique) pour former les sept arts libéraux au V^{e} siècle.
L'arithmétique étudie les nombres entiers, les propriétés qu'ont certains ou les relations qu'ils entretiennent avec d'autres : nombres premiers, nombres pairs ou impairs, nombres amis ou parfaits ou heureux, triplets pythagoriciens, nombres triangulaires et plus généralement nombres polygonaux de Diophante d'Alexandrie (II^{e} siècle), nombres de Marin Mersenne (1588-1648), nombres de Pierre de Fermat (1601-1665), nombres de Johann Carl Friedrich Gauss (1777-1855), nombres de Sophie Germain (1776-1831), nombres de Robert Daniel Carmichael (1879-1967), etc.

En lisant une édition de son époque des Arithmétiques de Diophante, Fermat rédige ce qu'on appellera le « grand théorème de Fermat » : *Pour tout entier naturel $n \geqslant 3$, il n'existe pas de nombres entiers strictement positifs x, y et z tels que $x^n + y^n = z^n$* et il ajoute dans la marge : *J'en ai découvert une démonstration véritablement merveilleuse que cette marge est trop étroite pour contenir* mais aucune trace de cette démonstration n'est trouvée. Beaucoup de mathématiciens ont essayé de démontrer cette conjecture mais il a fallu attendre plus de 300 ans pour en avoir la preuve que Andrew Wiles (1953-) exhibe comme sous-produit de ses travaux qui mobilisent bien d'autres notions que celles connues du temps de Fermat.
Ainsi, les problèmes arithmétiques s'énoncent et se comprennent facilement mais leur résolution peut entrainer des raisonnements très complexes et s'étaler sur de longues périodes. D'autres conjectures célèbres restent encore non démontrées comme la conjecture de Goldbach (1742) (*tout nombre entier pair supérieur à 3 peut s'écrire comme la somme de deux nombres premiers*) ou la conjecture de Syracuse de L. Collatz (1937) (*si pour tout entier $N > 0$, on construit la suite (u_n) en partant de $u_0 = N$ avec la relation $u_{n+1} = \frac{u_n}{2}$ si u_n pair ou $u_{n+1} = 3u_n + 1$ si u_n impair. alors il existe un indice $n > 0$ tel que $u_n = 1$.*
Souvent considérée comme très théorique, l'arithmétique a permis de mieux comprendre l'infini et les différents ensembles de nombres. De nos jours elle a de nombreuses applications, notamment en informatique (systèmes de cryptographie ou codes correcteurs d'erreur).

1. Divisibilité dans $\mathbb{Z}$

1.a. Multiples et diviseurs

DÉFINITION 6.1 (LA RELATION DIVISE) Soient a et $b \neq 0$ deux entiers relatifs.
On dit que b divise a lorsqu'il existe un entier relatif k tel que $a = kb$.
On note cela $b|a$ et on dit que b est un diviseur de a ou que a est un multiple de b.

Remarques :

- La liste des diviseurs d'un entier non nul a est finie car elle ne contient que des nombres entiers compris entre $-|a|$ et $|a|$ (car $\forall b \neq 0, b|a \Longrightarrow |b| \leqslant |a|$). Par contre la liste des diviseurs de 0 est infinie car pour tout $b \neq 0$ on a $0 = 0 \times b$ (l'ensemble des diviseurs de 0 est $\mathbb{Z}$). Tout entier possède des diviseurs car 1, -1, a et $-a$ divisent toujours a. Pour tout nombre a, les diviseurs de a et de $-a$ sont les mêmes.
- D'une façon générale on note $Div(a)$ l'ensemble des diviseurs d'un entier a. Par exemple $Div(-24) = Div(24) = \{-24, -12, -8, -6, -4, -3, -2, -1, 1, 2, 3, 4, 6, 8, 12, 24\}$ et $Div(0) = \mathbb{Z}$. Dans certaines situations qui ne concernent que les entiers naturels (entiers positifs) on ne retient que les diviseurs positifs d'un nombre $a > 0$.
- $0|0$ (zéro divise zéro) car $\forall b \neq 0, 0 = 0 \times 0$, par contre zéro ne divise aucun nombre $a \neq 0$ car si $a = k \times 0$ alors nécessairement $a = 0$.

EXEMPLE 1 – Déterminons tous les couples (a, b) d'entiers naturels tels que $a^2 - b^2 = 12$.
On sait que $a^2 - b^2 = (a - b)(a + b)$ donc $a - b$ et $a + b$ sont des diviseurs de 12 tels que $a + b$ et $a - b$ soient positifs ($a + b \geqslant 0$ car $a \geqslant 0$ et $b \geqslant 0$ et, comme le produit $(a - b)(a + b)$ est positif, le facteur $a - b$ doit être positif également). Comme $a - b \geqslant 0 \Longleftrightarrow a \geqslant b$, le plus grand des entiers est a.
Les diviseurs de 12 dans $\mathbb{N}$ sont $Div(12) = \{1, 2, 3, 4, 6, 12\}$, on a donc trois solutions potentielles :

$$\begin{cases} a + b = 12 \\ a - b = 1 \end{cases} \Longleftrightarrow \begin{cases} a = \dfrac{13}{2} \\ b = \dfrac{11}{2} \end{cases} \text{ (ne convient pas car ce ne sont pas des entiers)}$$

$$\begin{cases} a + b = 6 \\ a - b = 2 \end{cases} \Longleftrightarrow \begin{cases} a = \dfrac{8}{2} = 4 \\ b = 2 \end{cases} \text{ (convient)}$$

$$\begin{cases} a + b = 4 \\ a - b = 3 \end{cases} \Longleftrightarrow \begin{cases} a = \dfrac{7}{2} \\ b = \dfrac{1}{2} \end{cases} \text{ (ne convient pas).}$$

Finalement, il n'y a que le couple $(4, 2)$ qui convienne et on a bien $4^2 - 2^2 = 16 - 4 = 12$.

PROPRIÉTÉ 6.1 Le relation « divise » est une relation d'ordre car elle est

- Réflexive : $\forall a \in \mathbb{Z}, a|a$
- Antisymétrique : $\forall a \in \mathbb{Z}^*, \forall b \in \mathbb{Z}^*, a|b$ et $b|a \Longrightarrow a = b$ ou $a = -b$
- Transitive : $\forall a \in \mathbb{Z}^*, \forall b \in \mathbb{Z}^*, \forall c \in \mathbb{Z}, a|b$ et $b|c \Longrightarrow a|c$

L'ordre est partiel car $\forall a \in \mathbb{Z}, \forall b \in \mathbb{Z}, a|b$ ou $b|a$ est une proposition fausse.
$\forall a, b, c \neq 0, c|a$ et $c|b \Longrightarrow c|(ma + nb)$ une combinaison linéaire de a et b (m et n entiers).

Remarques :

- Les relations d'ordre $\leqslant$ et $\geqslant$ sont totales car tous les nombres sont comparables avec ces relations. Par contre, $<$ et $>$ sont des relations d'ordre partiels car on ne peut pas comparer avec elles des nombres égaux. La relation d'ordre $|$ est plus partielle encore puisqu'elle ne permet de comparer que des entiers relatifs dont l'un est multiple de l'autre. On ne peut comparer 2 qu'à ses multiples (les éléments de $2\mathbb{Z} = \{0, 2, -2, 4, -4, \ldots\}$) ou à ses diviseurs (les éléments de $Div(2) = \{1, -1, 2, -2\}$) ; 2 et 3 ne sont pas comparables avec $|$.

- La propriété $c|a$ et $c|b$ alors c divise toute combinaison linéaire $ma+nb$ est justifiée par la définition : comme $a=ck$ et $b=ck'$, on a $ma+nb=mck+nck'=c(mk+nk')=cK$.
  Si $c|a$ et $c|b$ alors, en particulier, c divise $a+b$ et c divise $a-b$.

Exemple 2 – ➲ Montrons que pour tout entier naturel n,
5^n-1, 13^n-1 et plus généralement $(4k+1)^n-1$ sont divisibles par 4.
$5^n-1=(5-1)(5^{n-1}+5^{n-2}+\cdots+5+1)=4\sum_{i=0}^{n-1}5^i=4K$ donc $4|(5^n-1)$.
$13^n-1=(13-1)(13^{n-1}+13^{n-2}+\cdots+13+1)=4\times3\sum_{i=0}^{n-1}13^i=4K'$
$(4k+1)^{n+1}-1=(4k+1-1)((4k+1)^{n-1}+(4k+1)^{n-2}+\cdots+(4k+1)+1)=4k\sum_{i=0}^{n-1}(4k+1)^i=4K''$

➲ Montrons, en raisonnant par récurrence, que 11^n-4^n est un multiple de 7 pour tout $n\in\mathbb{N}$.
Pour $n=0$: $11^n-4^n=0$ donc la proposition est vraie pour $n=0$.
Supposons la proposition vraie pour $n>0$.
Au rang suivant, $11^{n+1}-4^{n+1}=(7+4)11^n-4\times4^n=4(11^n-4^n)+7\times11^n$, ce qui est bien une combinaison linéaire de deux multiples de 7 (11^n-4^n l'est par hypothèse de récurrence et 7 l'est par définition) et par conséquent un nouveau multiple de 7.

➲ Justifions le critère de divisibilité par 11 : *un nombre est divisible par 11 lorsque la différence entre la somme des chiffres de rang pair et la somme des chiffres de rang impair est un multiple de* 11.
Un exemple : 919380 est divisible par 11 car $(9+9+8)-(1+3+0)=26-4=22=2\times11$.
Le principe de ce critère repose sur le fait que, pour tout entier naturel n, on peut déterminer un entier k tel que $10^{2n+1}+1=11k$ et $10^{2n}-1=11k$. Autrement dit que 11 divise les puissances impaires de 10 augmentées de 1 et les puissances paires de 10 diminuées de 1.
Prouvons cela par récurrence :
Pour $n=0$: $10^1+1=11$, $10^0-1=0$, 11 et 0 étant des multiples de 11, la propriété est vraie.

- Supposons pour $n>0$, il existe un entier k tel que $10^{2n+1}+1=11k\iff10^{2n+1}=11k-1$.
  $10^{2(n+1)+1}+1=100\times10^{2n+1}+1=(9\times11+1)(11k-1)+1=11(99k+11k-9)-1+1=11K$
- Supposons pour $n>0$, il existe un entier k' tel que $10^{2n}-1=11k'\iff10^{2n}=11k'+1$.
  $10^{2(n+1)}-1=100\times10^{2n}-1=(9\times11+1)(11k'+1)-1=11(99k'+11k'+9)+1-1=11K'$

Un nombre entier n écrit en base 10 s'écrivant $a_pa_{p-1}\dots a_2a_1a_0$ se décompose en
$a_p\times10^p+a_{p-1}\times10^{p-1}+\cdots+a_2\times10^2+a_1\times10^1+a_0\times10^0$. Selon la parité de p, on a :

- Si p impair :
  $n=[a_p(11k_p-1)+a_{p-2}(11k_{p-2}-1)+\cdots+a_1(11-1)]+[a_{p-1}(11k_p+1)+\cdots+a_0(0+1)]$,
  soit en réarrangeant cette somme et sans détailler l'entier K,
  $n=11K+[a_p\times(-1)+a_{p-2}\times(-1)+\cdots+a_1\times(-1)]+[a_{p-1}\times(+1)+\dots a_0\times(+1)]$.
  Finalement, $n=11K-[(a_p+a_{p-2}+\cdots+a_1)-(a_{p-1}+\cdots+a_2+a_0)]=11K-S$ et c'est donc cette somme alternée S qu'il suffit d'examiner pour la divisibilité par 11 de n.
- Si p pair, le principe est le même :
  $n=[a_p(11k_p+1)+\cdots+a_2(9\times11+1)+a_0(0+1)]+[a_{p-1}(11k_p-1)+\cdots+a_1(11-1)]$ et donc $n=11K+[(a_p+a_{p-2}+\cdots+a_2+a_0)-(a_{p-1}+\cdots+a_1)]=11K-S$ avec la somme alternée S à tester.

1.b. Division euclidienne

Définition 6.2 Il existe un unique entier $n\in\mathbb{Z}$ tel que $\forall x\in\mathbb{R}, n\leqslant x<n+1$.
Cet entier est appelé partie entière de x et noté $E(x)$ ou encore $\lfloor x\rfloor$, en anglais *floor* (plancher).

Démonstration Cette existence unique est la conséquence de l'axiome *toute partie de* $\mathbb{N}$ *admet un plus petit élément.*
En effet, en supposant $x>0$, l'ensemble des entiers supérieurs strictement à x admet un plus petit élément, noté $n+1$, tel que $x<n+1$ et l'entier précédent $n+1$ n'étant pas dans cette partie est tel que $x\geqslant n$, d'où l'encadrement $n\leqslant x<n+1$.
Pour un réel négatif, la partie entière continue d'être l'unique entier relatif n tel que $n\leqslant x<n+1$.

Remarque : la partie entière (en Python `math.floor(-2.6)`) ne doit pas être confondue avec la troncature à l'unité de x (en Python `int(-2.6)`) ou avec l'arrondi à l'unité de x (en Python `round(-2.6,0)`), même s'il y a parfois coïncidence entre ces notions.
$E(-2,6) = -3$ alors que $E(2,6) = 2$, mais la troncature de $-2,6$ est -2 et l'arrondi -3 alors que la troncature de $2,6$ est 2 et l'arrondi est 3.

DÉFINITION 6.3 soient a et $b > 0$ deux entiers.
Il existe un unique couple (q, r) d'entiers tels que $\begin{cases} a = bq + r \\ 0 \leqslant r < b \end{cases}$
On dit alors que q est le quotient de la division euclidienne de a par b, r en étant le reste.

DÉMONSTRATION ➠ Existence :
En notant q la partie entière du quotient $\frac{a}{b}$ ($q = \lfloor \frac{a}{b} \rfloor$), celle-ci vérifie, d'après la propriété précédente, l'encadrement $q \leqslant \frac{a}{b} < q + 1$. En multipliant par $b \neq 0$: $bq \leqslant a < b(q + 1)$, puis en enlevant b :
$0 \leqslant a - bq < b$. Si on pose $r = a - bq$, on a donc bien $0 \leqslant r < b$ et $a = bq + r$.

➠ Unicité :
Supposons qu'il existe deux couples (q, r) et (q', r') d'entiers tels que $\begin{cases} a = bq + r \\ 0 \leqslant r < b \end{cases}$ et $\begin{cases} a = bq' + r' \\ 0 \leqslant r' < b \end{cases}$
Cela implique que $r - r' = b(q - q')$ et donc $b|(r - r')$.
Si $r - r' \neq 0$ alors $-(r - r') \leqslant b \leqslant r - r'$ mais cela est impossible car d'autre part,
comme $0 \leqslant r < b$ et $-b \leqslant -r' < 0$, on doit avoir $-b < r - r' < b$.
On en déduit que $r - r' = 0$ et, comme $b \neq 0$, que $q - q' = 0$. Finalement $r = r'$ et $q = q'$.

Remarques et exemples :

- La division euclidienne dans $\mathbb{N}$ est commencée à l'école primaire et poursuivie au collège. L'écriture $177 = 11 \times 15 + 12$ correspond à l'écriture en ligne de la division euclidienne de 177 par 15 (quotient 11, reste $12 < 15$) mais pas à la division de 177 par 11 car le reste supposé est trop grand ($12 > 11$). Pour en déduire quotient de 177 par 12, il suffit de lui enlever le diviseur et de l'ajouter une fois du quotient : $177 = 11 \times (15 + 1) + (12 - 11) = 11 \times 16 + 1$.
  Du coup, le quotient de 177 par 11 est 16 et le reste 1.
- De $177 = 11 \times 15 + 12$, on peut déduire le résultat de la division euclidienne de -177 par 15 car alors $-177 = (-11) \times 15 + (-12)$. Comme le reste est trop petit ($-12 < 0$), il suffit de lui ajouter le diviseur et de le retrancher une fois du quotient :
  $-177 = (-11 - 1) \times 15 + (-12 + 15) = (-12) \times 15 + 3$.
  Du coup, le quotient de -177 par 15 est -12 et le reste 3.
- On peut, au passage, élargir la division euclidienne au cas d'un diviseur négatif en précisant que le reste doit toujours vérifier $0 \leqslant r < |b|$). La division euclidienne de -177 par -15 par exemple s'effectue à partir de l'opposée de $177 = 11 \times 15 + 12$: $-177 = 11 \times (-15) + (-12)$ et comme $-12 < 0$, on enlève le diviseur et on ajoute une fois au quotient :
  $-177 = (11 + 1) \times (-15) + (-12 - (-15)) = 12 \times (-15) + 3$.
  Du coup, le quotient de -177 par -15 est 12 et le reste 3.
- En Python le quotient de la division euclidienne de a par b est obtenu en tapant `a//b` et le reste s'obtient en tapant `a%b`. La fonction division euclidienne peut s'écrire en une ligne : `def de(a,b):return(a//b,a%b)`. Ainsi, en tapant `de(-177,15)` on obtient `(-12,3)` mais attention, en tapant `de(-177,-15)` on obtient `(11,-12)`, ce qui ne convient pas car l'opérateur `%` retourne un nombre du même signe que le diviseur. Pour que notre fonction `de()` convienne à toutes les situations, il faut tenir compte de ce comportement.

```
def de(a,b):
    if b>0 : return(a//b,a%b)
    return(a//b+1,a%b-b)
```

```
>>> de(-177,15)
(-12, 3)
>>> de(-177,-15)
(12, 3)
>>> de(177,-15)
(-11, 12)
>>> de(177,15)
(11, 12)
```

2. Congruences

2.a. Congruence modulo n

Définition 6.4 Soient a, b et $n \geqslant 2$ trois entiers.
On dit que a est congru à b modulo n lorsque a et b ont le même reste dans la division euclidienne par n, et on note $a \equiv b[mod\ n]$, $a \equiv b[n]$ ou plus simplement $a = b[n]$.

Remarques :

- On est familier avec les relations de congruences depuis toujours avec les heures qui sont remises à zéro tous les jours (le modulo est 24) ou toutes les demi-journées (le modulo est 12). Par exemple à 20h, il est 8h (de l'après-midi) car $20 \equiv 8[12]$ et dix heures plus tard il ne sera pas 30h mais 6h (du matin) car $30 \equiv 6[24]$. Une autre application des congruences a été étudiée en trigonométrie où les lignes trigonométriques d'un angle sont partagées avec toutes les autres valeurs qui lui sont congrues modulo 2π. Par exemple $\frac{5\pi}{2} \equiv \frac{\pi}{2} \equiv \frac{-3\pi}{2}[2\pi]$.
- On confond souvent, ne serait-ce que dans la notation, l'égalité avec la relation de congruence car elles partagent les propriétés évidentes suivantes valables pour tout $n \geqslant 2$:
  — $\forall a \in \mathbb{Z}$, $a \equiv a[n]$
  — $\forall (a,b) \in \mathbb{Z}^2$, $a \equiv b[n] \iff b \equiv a[n]$
  — $\forall (a,b,c) \in \mathbb{Z}^3$, $a \equiv b[n]$ et $b \equiv c[n] \implies a \equiv c[n]$
  Dans la suite les congruences sont notées avec $=$, la présence du modulo faisant la différence.
- La congruence modulo 0 ou 1 n'est pas utilisée ($a = b[0] \iff a = b$ et $\forall (a,b) \in \mathbb{Z}^2, a = b[1]$).

Propriété 6.2 a, b et $n \geqslant 2$ étant trois entiers, $a = b[n] \iff a - b$ est un multiple de n.

Démonstration Divisions euclidiennes de a et b par n : $\begin{cases} a = nq + r \\ 0 \leqslant r < n \end{cases}$ et $\begin{cases} b = nq' + r' \\ 0 \leqslant r' < n \end{cases}$.
On en déduit : $a - b = nq + r - (nq' + r') = n(q - q') + r - r'$ et,
en additionnant $-n < -r' \leqslant 0$ et $0 \leqslant r < n$, on obtient $-n < r - r' < n$.

- Si $a = b[n]$ alors $r = r'$ (par définition) et donc $r - r' = 0$ d'où $a - b = n(q - q')$, c'est-à-dire $a - b$ est un multiple de n.
- Si $a - b$ est un multiple de n, il existe $k \in \mathbb{Z}$ tel que $a - b = kn$ et donc $r - r' = a - b - n(q - q') = n(k - q + q')$, $r - r'$ est un multiple de n.
  Le seul multiple de n compris entre $-n$ et n étant 0, $r - r' = 0 \iff r = r'$ d'où $a = b[n]$.

Remarques :

- On pourra identifier, modulo n, un entier a avec son reste r dans la division euclidienne par n puisque $a = nq + r$ avec $0 \leqslant r < n$ implique que $a - r = nq$ et donc que $a = r[n]$.
  Exemples : $2023 = 11 \times 183 + 10$ donc $2023 = 10[11]$; $2023 = 10 \times 202 + 3$ donc $2023 = 3[10]$;
  Dire que a est divisible par n, ce qu'on note déjà $n|a$, s'écrit aussi $a = 0[n]$.
- Autres exemples :
  — $27 = 2[5]$ car $27 - 2 = 25 = 5k$ (un multiple de 5)
  — $-27 = 3[5]$ car $-27 - 3 = -30 = 5k'$
  — $(a+b)^2 = a^2 + b^2[2]$ car $(a+b)^2 - (a^2 + b^2) = 2ab = 2k''$
  — $(2n+1)^2 = 1[4]$ (autrement dit le carré d'un nombre impair est de la forme $4k+1$) car $(2n+1)^2 - 1 = (2n+1-1)(2n+1+1) = 2n(2n+2) = 4n(n+1) = 4k'''$
- Un entier $n \geqslant 2$ étant donné, un entier quelconque $a \in \mathbb{Z}$ appartient nécessairement à l'une des n classes d'équivalences : $a = 0[n], a = 1[n], \ldots, a = n-1[n]$. Tous les entiers $a \in \mathbb{Z}$ se rangent ainsi dans l'une ou l'autre des quatre classes : $a = 0[4]$, $a = 1[4]$, $a = 2[4]$, $a = 3[4]$ ce que l'on peut noter avec $\oplus$, le « ou exclusif » $a = 4k \oplus a = 4k+1 \oplus a = 4k+2 \oplus a = 4k+3$.

PROPRIÉTÉ 6.3 (COMPATIBILITÉS AVEC LES OPÉRATIONS) a, b, c, d et $n \geqslant 2$ étant cinq entiers,
- Avec l'addition : $a = b[n]$ et $c = d[n] \Longrightarrow a + c = b + d[n]$
- Avec la multiplication : $a = b[n]$ et $c = d[n] \Longrightarrow a \times c = b \times d[n]$
- Avec les puissances : $\forall p \in \mathbb{N}^*, a = b[n] \Longrightarrow a^p = b^p[n]$

DÉMONSTRATION D'après la propriété 6.2 :
$a = b[n]$ et $c = d[n] \Longleftrightarrow \exists (k, k') \in \mathbb{Z}^2, a - b = kn$ et $c - d = k'n$
Par conséquent, $(a + c) - (b + d) = (a - b) + (c - d) = kn + k'n = (k + k')n = k''n$ avec $k'' = k + k' \in \mathbb{Z}$ d'où $a + c = b + d[n]$.
De même, $(a \times c) - (b \times d) = (a - b) \times c + (c - d) \times b = kn \times c + k'n \times b = (kc + k'b)n = k'''n$ avec $k''' = kc + k'b \in \mathbb{Z}$ d'où $a \times c = b \times d[n]$.
La troisième compatibilité est obtenue par récurrence sur $p > 0$ avec la compatibilité de $\times$.

EXEMPLE 3 – Les utilisations de ces propriétés sont nombreuses et variées, donnons-en quatre :
➲ Déterminons le reste de la division euclidienne de 100^{50} par 11.
Comme $100 = 99 + 1 = 9 \times 11 + 1$, $100 = 1[11]$ et donc $100^{50} = 1^{50} = 1[11]$, le reste est 1.
Déterminons le reste de la division euclidienne de 100^{50} par 7.
Comme $100 = 77 + 23$, $77 = 0[7]$ et $23 = 21 + 2 = 2[7]$, on a $100 = 2[7]$ donc $100^{50} = 2^{50}[7]$.
Comme, de plus, $2^3 = 8 = 7 + 1 = 1[7]$, $2^{50} = 2^{3\times16+2} = (2^3)^{16} \times 2^2 = 1^{16} \times 4 = 4[7]$, le reste est 4.

➲ Montrons la propriété $\forall n \in \mathbb{N}, 3 | (n(n + 1)(2n + 1))$ à l'aide d'un tableau de congruence modulo 3.

$n = \ldots [3]$	0	1	2
$n + 1 = \ldots [3]$	1	2	0
$2n + 1 = \ldots [3]$	1	0	2
$n(n + 1)(2n + 1) = \ldots [3]$	0	0	0

Comme on remarque que, dans tous les cas $n(n + 1)(2n + 1) = 0[3]$, on en conclut que $n(n + 1)(2n + 1)$ est toujours divisible par 3, soit $3 | (n(n + 1)(2n + 1))$.

➲ Explorons les propriétés des puissances en traçant le tableau des puissances modulo 5 :

a	a^1	a^2	a^3	a^4	a^5	a^6	a^7	a^8
1	1	1	1	1	1	1	1	1
2	2	4	3	1	2	4	3	1
3	3	4	2	1	3	4	2	1
4	4	1	4	1	4	1	4	1
5	0	0	0	0	0	0	0	0

On remarque une périodicité de période 4 lorsque $a = 2$ ou $3[5]$, de période 2 lorsque $a = 4[5]$.
- Comme $2^4 = 1[5]$, on a :
  $2^1 = 2^5 = \cdots = 2^{4k+1} = 2[5]$; $2^2 = 2^6 = \cdots = 2^{4k+2} = 4[5]$; $2^3 = 2^7 = \cdots = 2^{4k+3} = 3[5]$
- Comme $3^4 = 1[5]$, on a :
  $3^1 = 3^5 = \cdots = 3^{4k+1} = 3[5]$; $3^2 = 3^6 = \cdots = 3^{4k+2} = 4[5]$; $3^3 = 3^7 = \cdots = 3^{4k+3} = 2[5]$
- Comme $4^2 = 1[5]$, on a :
  $4^1 = 4^3 = \cdots = 4^{2k+1} = 1[5]$; $4^2 = 4^4 = \cdots = 4^{2k} = 1[5]$

La relation de congruence est-elle compatible avec l'exponentiation ?
Autrement dit $\forall (p, q) \in \mathbb{Z}^2, \forall a \in \mathbb{N}, p = q[n] \Longrightarrow a^p = a^q[n]$ est-elle vraie pour tout entier $n > 1$?
La réponse est non, la relation de congruence n'est pas compatible avec l'exponentiation.
Exhibons en guise de contre-exemple le cas $n = 5$, $p = 1$ et $q = 6$ pour lequel on a bien $1 = 6[5]$.
- Pour $a = 1$ ou $5[5]$ on a bien $1^1 = 1^6 = 1[5]$ et $5^1 = 5^6 = 0[5]$ mais ce n'est pas étonnant car toutes les puissances de $a = 1[5]$ valent 1 et toutes les puissances de $a = 5[5]$ valent 0
- Pour $a = 2$ ou 3 ou $4[5]$ la propriété est cependant fausse car
  $(2^1 = 2) \neq (2^6 = 4)[5]$ et $(3^1 = 3) \neq (3^6 = 4)[5]$ et $(4^1 = 4) \neq (4^6 = 1)[5]$.

➲ La compatibilité de la relation de congruence avec + se simplifie en $a = b[n] \Longrightarrow a + c = b + c[n]$.
La réciproque de cette propriété est vraie : $a + c = b + c[n] \Longrightarrow a = b[n]$.
Cela se prouve facilement : $a + c = b + c[n] \Longrightarrow (a + c) - (b + c) = 0[n] \Longrightarrow a - b = 0[n] \Longrightarrow a = b[n]$.
Ce qui rend la soustraction compatible avec la relation de congruence.
Une conséquence : on peut résoudre une équation du type $x + a = b[n]$ en soustrayant a aux deux membres. Par exemple $x + 5 = 3[7] \Longleftrightarrow x = 3 - 5 = -2 \Longleftrightarrow x = -2 + 7 = 5[7]$.

La compatibilité de la relation de congruence avec × se simplifie en $a = b[n] \Longrightarrow a \times c = b \times c[n]$.
Mais la réciproque est fausse : $5 \times 7 = 5 \times 9[5]$ mais $7 \neq 9[5]$ ou $2 \times 5 = 2 \times 1[8]$ mais $5 \neq 1[8]$.
Ce qui rend la division incompatible avec la relation de congruence.
On ne peut donc pas résoudre une équation du type $ax = b[n]$ en divisant par a les deux membres.
Exemple : $5x = 45[5]$, en divisant par 5 les deux membres on trouve $x = 9 = 4[5]$ alors que $5x = 45[5]$ est toujours vraie. Pour résoudre ce type d'équation, on peut utiliser un tableau de congruence.
Supposons qu'on cherche à résoudre $3x = 1[5]$:

$x = \ldots [5]$	0	1	2	3	4
$3x = \ldots [5]$	0	3	1	4	2

On en déduit que les solutions s'écrivent $x = 2[5]$.
De même pour résoudre une équation plus compliquée comme $x^2 + 3x - 2 = 0[5]$
Supposons qu'on cherche à résoudre $3x = 1[5]$:

$x = \ldots [5]$	0	1	2	3	4
$x^2 = \ldots [5]$	0	1	4	4	1
$3x = \ldots [5]$	0	3	1	4	2
$x^2 + 3x - 2 = \ldots [5]$	-2=3	2	3	6=1	1

On en déduit que cette équation n'a pas de solutions dans $\mathbb{Z}$.
Par contre l'équation $x^2 + 3x - 2 = p[5]$ a des solutions pour $p \in \{1, 2, 3\}[5]$.

3. PGCD

Définition 6.5 (PGCD et PPCM) a et b étant deux entiers relatifs non nuls, le plus grand diviseur commun de a et de b est un entier compris entre 1 et $min(|a|, |b|)$. On note ce nombre $PGCD(a, b)$ (Plus Grand Commun Diviseur, en anglais *Greatest Common Divisor*).
Le plus petit multiple commun strictement positif de a et de b est un entier compris entre $max(|a|, |b|)$ et $|ab|$. On note ce nombre $PPCM(a, b)$ (Plus Petit Commun Multiple, en anglais *Least Common Multiple*).

Démonstration L'ensemble des diviseurs de a et de $-a$, et donc aussi de $|a|$, est $Div(a)$.
Cet ensemble, comme d'ailleurs aussi $Div(b)$ n'est pas vide puisqu'il contient toujours 1.
Par conséquent l'ensemble $Div(a) \cap Div(b)$ n'est pas vide car il contient au moins 1.
Le plus grand élément de $Div(a)$ est $|a|$, de même le plus grand élément de $Div(b)$ est $|b|$.
On en déduit que le plus grand élément de $Div(a) \cap Div(b)$ est inférieur ou égal à $|a|$ et à $|b|$, cet ensemble est donc majoré par $min(|a|, |b|)$. Cet ensemble des diviseurs communs de a et de b, $Div(a) \cap Div(b)$, est un ensemble borné d'entiers. Son plus grand élément existe, c'est lui qui est appelé $PGCD(a, b)$.

L'ensemble des multiples strictement positifs de a (respectivement de b) est un ensemble d'entiers dont le plus petit élément est $|a|$ (resp. $|b|$). L'ensemble des multiples communs strictement positifs de a et de b est donc un ensemble minoré par $max(|a|, |b|)$. Cet ensemble n'est pas vide car il contient toujours $|ab|$, par conséquent son plus petit élément existe, c'est lui qui est appelé $PPCM(a, b)$.

Remarques :

- On peut toujours déterminer le PGCD de deux entiers à l'aide de la liste des diviseurs de chacun de ces nombres. C'est la méthode naïve, communément utilisée au Collège pour se familiariser avec la notion dans le but, notamment, de simplifier une fraction.
  Donnons un exemple : $Div(24) \cap \mathbb{N} = \{1, 2, 3, 4, 6, 8, 12, 24\}$ (je ne donne que les diviseurs positifs) et $Div(60) \cap \mathbb{N} = \{1, 2, 3, 4, 5, 6, 10, 12, 20, 30, 60\}$ d'où
  $Div(24) \cap Div(60) \cap \mathbb{N} = \{1, 2, 3, 4, 6, 12\}$. On en déduit que $PGCD(24, 60) = 12$; cela permet, notamment, de simplifier la fraction $\frac{24}{60} = \frac{12\times2}{12\times5} = \frac{2}{5}$.
- De même on peut déterminer le PPCM de deux entiers par une méthode naïve en déterminant une liste des multiples positifs des deux nombres, le premier qui se trouve dans les deux listes étant le PPCM cherché. Par exemple les multiples de 24 sont $24, 48, 72, 96, 120, \ldots$ et les multiples de 60 sont $60, 120, \ldots$ donc $PPCM(24, 60) = 120$. L'utilisation classique du PPCM est la détermination d'un dénominateur commun optimal pour l'addition des fractions :
  $\frac{5}{24} + \frac{7}{60} = \frac{5\times5}{24\times5} + \frac{7\times2}{60\times2} = \frac{25}{120} + \frac{14}{120} = \frac{25+14}{120} = \frac{39}{120}$.

PROPRIÉTÉ 6.4 (PGCD) Soient a et b deux entiers non nuls quelconques.

- $PGCD(a, b) = PGCD(|a|, |b|)$
- $PGCD(a, b) = PGCD(b, a)$
- $PGCD(a, b) \geqslant 1$
- $a|b \Longrightarrow PGCD(a, b) = |a|$
- $PGCD(a, b) = PGCD(a - b, b)$
- $a = bq + r$ avec $0 \leqslant r < b \Longrightarrow PGCD(a, b) = PGCD(b, r)$

DÉMONSTRATION ➲ Les trois premières propriétés sont évidentes :
Comme $Div(a) = Div(-a) = Div(|a|)$ et $Div(b) = Div(-b) = Div(|b|)$, on a
$Div(a) \cap Div(b) = Div(|a|) \cap Div(|b|)$ d'où $PGCD(a, b) = PGCD(|a|, |b|)$.
De même, comme $Div(a) \cap Div(b) = Div(b) \cap Div(a)$, on a $PGCD(a, b) = PGCD(b, a)$.
$PGCD(a, b) \geqslant 1$ car parmi les diviseurs communs strictement positifs, le plus petit est 1.

➲ Pour la 4e, montrons d'abord que $a|b \Longrightarrow Div(a) \cap Div(b) = Div(a)$:

- Un diviseur quelconque d de a vérifie $d|a$, or $a|b$ et la relation $|$ est transitive donc $d|b$.
  Par conséquent $a|b \Longrightarrow Div(a) \subset Div(b)$
- De $Div(a) \subset Div(b)$ on déduit que $Div(a) \cap Div(b) = Div(a)$

Par conséquent, lorsque $a|b$ le plus grand élément de $Div(a) \cap Div(b)$ est donc le plus grand élément de $Div(a)$ c'est-à-dire $|a|$, d'où $PGCD(a, b) = |a|$.

➲ Montrons $PGCD(a, b) = PGCD(a - b, b)$ par double inclusion :

- Si $d \in Div(a) \cap Div(b)$ alors $d|a$ et $d|b$. D'après la propriété 6.1, d divise toute combinaison linéaire de a et b, donc $d|(a - b)$ et par conséquent $d \in Div(a - b) \cap Div(b)$ d'où
  $Div(a) \cap Div(b) \subset Div(a - b) \cap Div(b)$.
- Si $d \in Div(a - b) \cap Div(b)$ alors $d|(a - b)$ et $d|b$. D'après la propriété 6.1, d divise $(a - b) + b = a$, donc $d|a$ et par conséquent $d \in Div(a) \cap Div(b)$ d'où
  $Div(a - b) \cap Div(b) \subset Div(a) \cap Div(b)$.

On en déduit que $Div(a) \cap Div(b) = Div(a - b) \cap Div(b)$.
Le plus grand élément de $Div(a) \cap Div(b)$ est donc aussi celui de $Div(a - b) \cap Div(b)$.
De la même façon, lorsque $a = bq + r$ avec $0 \leqslant r < b$, on a $PGCD(a, b) = PGCD(r, b)$.

- Dans un sens, d divise toute combinaison linéaire de a et b, donc $d|(a - bq)$ c'est-à-dire $d|r$.
- Dans l'autre sens, d divise toute combinaison linéaire de r et b, donc $d|(r + bq)$ c'est-à-dire $d|a$.

Dans le cas où $r = 0$, on a $a = bq$ c'est-à-dire $b|a$ et, comme on l'a vu, dans ce cas $PGCD(a, b) = |b|$.

Remarques :

- Deux cas particuliers de la 4e propriété : $PGCD(a, a) = |a|$; $PGCD(a, 1) = 1$.
  Par ailleurs $PGCD(0, a) = |a|$ car $Div(0) = \mathbb{Z}$ et donc $Div(a) \cap Div(0) = Div(a)$.

- Les propriétés des deux dernières lignes sont les « lemme d'Euclide » car elles sont les préliminaires obligés à une justification de l'algorithme d'Euclide (propriété suivante).
  Lorsqu'on applique ces propriétés à des entiers naturels, le procédé par division revient à itérer le procédé par soustraction jusqu'à l'obtention d'un résidu inférieur à b.
  Par soustractions $PGCD(50,15) = PGCD(35,15) = PGCD(20,15) = PGCD(5,15)$ mais $50 = 3\times 15+5$, par division on trouve directement $PGCD(50,15) = PGCD(5,15)$.
  Pour $PGCD(5,15)$, comme $5|15$ on a $PGCD(5,15) = 5$. Finalement $PGCD(50,15) = 5$.
- Comme $PGCD(a,b) = PGCD(|a|,|b|)$, nous ne considèrerons désormais que des entiers naturels (positifs) en transposant si nécessaire dans $\mathbb{Z}$ les résultats obtenus dans $\mathbb{N}$.

Propriété 6.5 (Algorithme d'Euclide) Soient a et b deux entiers strictement positifs.
On applique successivement la division euclidienne de a par b (elle conduit à un reste $r = a - bq$) puis on recommence en renommant les variables $\begin{cases} b \text{ devient } a \\ r \text{ devient } b \end{cases}$, jusqu'à obtenir un reste nul.
Le nombre cherché ($PGCD(a,b)$) est égal au dernier reste non nul obtenu.

Démonstration Il suffit d'appliquer successivement la propriété
$a = bq + r$ avec $0 \leqslant r < b \Longrightarrow PGCD(a,b) = PGCD(b,r)$ jusqu'à l'obtention d'un reste nul.
Le premier reste r_1 est tel que $0 \leqslant r_1 < b$ et $PGCD(a,b) = PGCD(b,r_1)$.
Le 2e reste r_2 est tel que $0 \leqslant r_2 < r_1$ et $PGCD(b,r_1) = PGCD(r_1,r_2)$, etc.
La suite des restes est donc décroissante et minorée par 0 ($0 \leqslant \cdots < r_3 < r_2 < r_1$).
Elle admet donc un plus petit élément non nul, r_k, qui est le PGCD cherché puisque
$PGCD(a,b) = PGCD(b,r_1) = PGCD(r_1,r_2) = \cdots = PGCD(r_{k+1},r_k) = PGCD(r_k,0) = r_k$.

Remarques : Ce procédé est décrit dans le livre 10 des Éléments d'Euclide, écrit il y a 23 siècles.
Lorsqu'on l'applique à la main, cela conduit à effectuer des divisions euclidiennes en chaine.
On peut aussi utiliser un tableur ou un programme informatique comme celui ci-dessous en Python.
On peut encore illustrer le procédé graphiquement en enlevant des carrés dans une surface rectangulaire, maximisant à chaque étape la taille du carré à enlever (cette méthode revient à appliquer des soustractions successives).

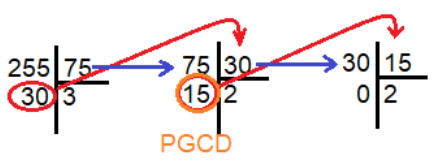
B3 : =SI(B2<>0;MOD(B1;B2);0)

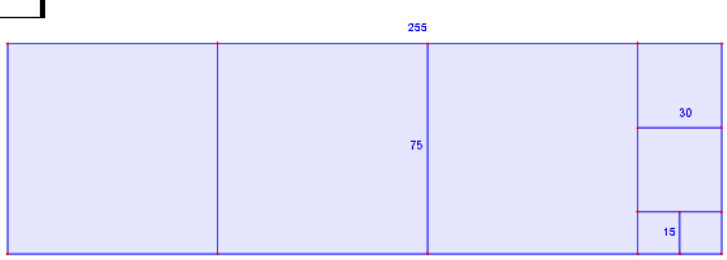
	A	B	C	D
1	1er nombre	255	229596	123456789
2	2eme nombre	75	4898865	1234567
3		30	229596	89
4		15	77349	48
5		0	74898	41
6		0	2451	7
7		0	1368	6
8		0	1083	1
9		0	285	0
10		0	228	0
11		0	57	0
12		0	0	0

```
def pgcd(a,b):
    while b!=0:
        r=a%b
        a=b
        b=r
    return a

#a,b=255,75
#a,b=229596,4898865
a,b=123456789,1234567
print("le pgcd de {} et {} est {}".format(a,b,pgcd(a,b)))
```

```
le pgcd de 255 et 75 est 15
le pgcd de 229596 et 4898865 est 57
le pgcd de 123456789 et 1234567 est 1
```





Contrairement à l'algorithme par soustractions qui suppose $a > b$ pour calculer $PGCD(a,b)$, avec l'algorithme par divisions il n'est pas nécessaire de s'assurer que $a > b$ car, dans le cas contraire, $a = 0\times b + a$ avec $0 \leqslant a < b \Longrightarrow PGCD(a,b) = PGCD(b,a)$ et on continue avec, cette fois $b > a$.
Ce cas de figure s'est présenté dans le calcul de $PGCD(229\,596, 4\,898\,865)$.

DÉFINITION 6.6 (NOMBRES PREMIERS ENTRE EUX) Deux entiers non nuls a et b n'ayant que 1 comme diviseur commun, c'est-à-dire tels que $PGCD(a,b)=1$, sont dits « premiers entre eux ».

Remarques :

- Les fractions $\frac{a}{b}$ et $\frac{b}{a}$ sont dites « irréductibles » lorsqu'elles ne sont pas simplifiables, autrement dit si les nombres a et b sont premiers entre eux, c'est-à-dire si $PGCD(a,b)=1$.
- Ne pas confondre nombres « premiers entre eux » et nombres « premiers ». En particulier ne pas croire que a et b doivent être premiers pour que les nombres a et b soient premiers entre eux. Par exemple 8 et 9 ne sont pas premiers (8 est divisible par 2 et 4, 9 l'est par 3) mais cependant ils sont premiers entre eux car leur seul diviseur commun est 1. Inversement, par contre, deux nombres premiers différents sont toujours premiers entre eux.

PROPRIÉTÉ 6.6 (COMPLÉMENT) Soient a et b deux entiers strictement positifs.

- Pour tout entier $c\in\mathbb{Z}^*$ on a $PGCD(ca,cb)=|c|\times PGCD(a,b)$
- $PGCD(a,b)=d \iff \exists (p,q)\in\mathbb{N}^*, \begin{cases} PGCD(p,q)=1 \\ a=dp \\ b=dq \end{cases}$

DÉMONSTRATION ➲Considérons un entier naturel non nul c.
En préliminaire remarquons que puisque $a=bq+r$ avec $0\leqslant r<b$, on a $PGCD(a,b)=PGCD(r,b)$ alors on a aussi $ca=(cb)q+(cr)$ avec $0\leqslant cr<cb$ et $PGCD(ca,cb)=PGCD(cr,cb)$. On peut donc multiplier par un entiers $c>0$ tous les nombres impliqués dans le lemme d'Euclide.

On sait que l'algorithme d'Euclide construit la suite décroissante des restes (r_n) :
$PGCD(a,b)=PGCD(b,r_1)=PGCD(r_1,r_2)=\cdots=PGCD(r_{k+1},r_k)=PGCD(r_k,0)=r_k$.
Multiplions par $c>0$ tous les nombres impliqués dans ces égalités :
$PGCD(ca,cb)=PGCD(cb,cr_1)=\cdots=PGCD(cr_{k+1},cr_k)=PGCD(cr_k,0)=cr_k$.
On obtient bien $PGCD(ca,cb)=cr_k=c\times PGCD(a,b)$.

Pour $c<0$, comme $PGCD(a,b)=PGCD(|a|,|b|)$, on en déduit que
$PGCD(ca,cb)=PGCD(|ca|,|cb|)=PGCD(|c|a,|c|b)=|c|\times PGCD(a,b)$.

➲ Montrons que $PGCD(a,b)=d\Longrightarrow \exists (p,q)\in\mathbb{N}^*, \begin{cases} PGCD(p,q)=1 \\ a=dp \\ b=dq \end{cases}$

Si $PGCD(a,b)=d$ alors $d|a$ et $d|b$, autrement dit $\exists (p,q)\in\mathbb{N}^*, \begin{cases} a=dp \\ b=dq \end{cases}$
En utilisant la propriété précédente, on en déduit que
$d=PGCD(a,b)=PGCD(dp,dq)=d\times PGCD(p,q)$.
D'où p et q sont premiers entre eux car $d=d\times PGCD(p,q)\iff PGCD(p,q)=1$.
Réciproquement,

$$\forall d\in\mathbb{N}^*, \exists (p,q)\in\mathbb{N}^*, \begin{cases} PGCD(p,q)=1 \\ a=dp \\ b=dq \end{cases} \Longrightarrow PGCD(a,b)=PGCD(dp,dq)=d\times PGCD(p,q)=d$$

Exemples :

- On a calculé naïvement $PGCD(24,60)$ plus haut, mais si on remarque que $24=12\times 2$ et $60=12\times 5$, comme 2 et 5 sont premiers entre eux, $PGCD(24,60)=12\times PGCD(2,5)=12$.
- On souhaite trouver les couples de naturels (a,b) vérifiant $a+b=108$ et $PGCD(a,b)=12$. Il suffit de trouver les couples (p,q), p et q premiers entre eux, tels que $a=12p$ et $b=12q$.

Ces nombres vérifiant aussi $a+b=12(p+q)=108$, soit $p+q=\frac{108}{12}=9$, on en déduit les couples (p,q) qui conviennent : $(1,8),(2,7),(4,5),(5,4),(7,2)$ et $(8,1)$, et les solutions s'obtiennent en les multipliant par 12 : $(12,96),(24,84),(48,60),(60,48),(84,24)$ et $(96,12)$.

4. Théorèmes de Bézout et de Gauss

Propriété 6.7 (Théorème de Bézout) Soient a et b deux entiers strictement positifs.
$PGCD(a,b)=1 \iff \exists (u,v)\in\mathbb{Z}^2, au+bv=1$

Démonstration ➲Le sens réciproque est évident.
En notant $PGCD(a,b)=d$, on sait que $d|a$ et $d|b$ ce qui implique, selon la propriété 6.1, $d|(au+bv)$ donc $d|1$. On en déduit $d=1$, les nombres a et b sont premiers entre eux.

➲Sens direct : on suppose a et b premiers entre eux et on considère l'ensemble E des naturels non nuls de la forme $au+bv$ avec $(u,v)\in\mathbb{Z}^2$. L'ensemble E n'est pas vide car a et b en font partie, il admet donc un plus petit élément non nul, noté p.
p est tel que $\exists (u_0,v_0)\in\mathbb{Z}^2, p=au_0+bv_0$ et $\forall e\in E, e\geqslant p$.
Montrons que $p|a$: La division euclidienne de a par p s'écrit $a=pq+r$ avec $0\leqslant r<p$.
On en déduit que $r=a-pq=a-(au_0+bv_0)q=a(1-u_0p)+b(v_0q)$, soit $r=au_1+bv_1$ avec $u_1=1-u_0p$ et $v_1=v_0q$. Mais alors on doit avoir $r\in E$ et $r<p$ ce qui est impossible si $r\neq 0$, d'où on déduit que $r=0$ et donc $a=pq\iff p|a$.
De la même façon, on montre que $p|b$ et par conséquent $p|PGCD(a,b)$ or, par hypothèse, $PGCD(a,b)=1$. Conclusion $p|1$ donc $p=1$ et on a bien $\exists (u_0,v_0)\in\mathbb{Z}^2, au_0+bv_0=1$.

Remarques et exemples :

- Ce théorème est généralement appelé théorème de Bézout du nom du mathématicien Étienne Bézout (1730-1783) qui le généralisa aux polynômes mais on doit sa première démonstration à Claude-Gaspard Bachet dit de Méziriac (1581-1638) qui la publie dans *Problèmes plaisans et délectables qui se font par les nombres* en 1612. Pour ces raisons, il est souvent mentionné aujourd'hui comme le théorème de Bachet-Bézout.
- Si a et b ne sont pas premiers entre eux, il n'est pas possible de trouver des entiers u et v tels que $au+bv=1$. L'équation $4x+6y=1$ n'a pas de solution dans $\mathbb{Z}^2$.
- Lorsque $PGCD(a,b)=1$, le théorème assure de l'existence d'un couple d'entiers (u,v) mais n'en donne pas la valeur qui n'est d'ailleurs pas unique. Par exemple 2 et 3 étant premiers entre eux, on peut trouver plusieurs couples (u,v) tels que $2u+3v=1$: on a $-2+3=1$, donc déjà $(-1,1)$ est solution, mais on a encore $4-3=1$ et donc $(2,-1)$ est aussi solution.
- Détermination explicite d'un couple (u,v) satisfaisant $au+bv=1$ avec les congruences : $au=1-bv\Longrightarrow au=1[b]$. Les u qui conviennent sont les inverses de a modulo b.
  Par exemple 2 et 3 étant premiers entre eux, quels entiers u vérifient $2u=1[3]$?
  $2\times 0=0[3]$, $2\times 1=2[3]$ et $2\times 2=4=1[3]$. Les u qui conviennent valent $2[3]$.
  Il suffit de choisir un nombre de la forme $u=3k+2$, soit $u\in\{\ldots,-4,-1,2,5,\ldots\}$.
  u étant choisi, une valeur entière de v se déduit nécessairement de l'égalité $v=\frac{1-au}{b}$.
  Pour $u=5$ on doit prendre $v=\frac{1-2\times 5}{3}=\frac{-9}{3}=-3$, et on a bien $2\times 5+3\times(-3)=1$.
- Une conséquence immédiate de ce théorème : Quels que soient les naturels non nuls a, b et c, si $PGCD(a,b)=1$ et $PGCD(a,c)=1$ alors $PGCD(a,bc)=1$.
  Pour le justifier, sachant que $au+bv=1$ et $au'+cv'=1$, il suffit d'arranger le produit $(au+bv)(au'+cv')=1$.
  Comme $(au+bv)(au'+cv')=a(uau'+ucv'+bvu')+bc(vv')$, on en déduit que $aU+bcV=1$ avec $U=uau'+ucv'+bvu'$ et $V=vv'$ et donc $PGCD(a,bc)=1$.
- Montrons que, quel que soit l'entier n, les nombres $3n+1$ et $2n+1$ sont premiers entre eux.
  Il suffit de remarquer que $3(2n+1)-2(3n+1)=1$ et d'appliquer le théorème réciproque. De même, on montre que $2n+3$ et $5n+7$ sont premiers entre eux car $5(2n+3)-2(5n+7)=1$.

Propriété 6.8 (Identité de Bézout) Soient a et b deux entiers strictement positifs.
$PGCD(a,b) = d \Longrightarrow \exists (u,v) \in \mathbb{Z}^2, au + bv = d$

Démonstration Cette propriété est une conséquence du théorème de Bézout.
Si $PGCD(a,b) = d$, d'après la propriété 6.6, $\exists (p,q) \in \mathbb{N}^*, \begin{cases} PGCD(p,q) = 1 \\ a = dp \\ b = dq \end{cases}$.
Appliquons le théorème de Bézout à p et q premiers entre eux : $\exists (u,v) \in \mathbb{Z}^2, pu + qv = 1$.
Multiplions par d cette égalité et remplaçons dp par a et dq par b, on obtient :
$d(pu + qv) = d \Longleftrightarrow (dp)u + (dq)v = d \Longleftrightarrow au + bv = d$.

Propriété 6.9 (Réciproque) Soient a et b deux entiers strictement positifs.
Si $d \in \mathbb{N}^*$ est tel que $d|a$, $d|b$ et $\exists (u,v) \in \mathbb{Z}^2, au + bv = d$, alors $PGCD(a,b) = d$

Démonstration Montrons $PGCD(a,b) = d$ en montrant que $PGCD(a,b) \leqslant d$ et $d \leqslant PGCD(a,b)$:

- $PGCD(a,b)$ est un diviseur de a et de b donc $PGCD(a,b)$ divise la combinaison linéaire $d = au + bv$. Puisque $PGCD(a,b)|d$, on a $PGCD(a,b) \leqslant d$.
- d est un diviseur commun à a et b, or par définition, $PGCD(a,b)$ est le plus grand des diviseurs communs à a et b, donc $d \leqslant PGCD(a,b)$.

Propriété 6.10 (Théorème de Gauss) Soient a, b et c trois entiers strictement positifs.
Si $a|(bc)$ et $PGCD(a,b) = 1$ alors $a|c$.

Démonstration Ce théorème est encore une conséquence du théorème de Bézout.
Appliquons-le à a et b qui sont premiers entre eux par hypothèse : $\exists (u,v) \in \mathbb{Z}^2, au + bv = 1$.
En multipliant par c l'égalité, on obtient $c(au + bc) = (ca)u + (cb)v = c$.
Or on sait que $a|(cb)$ (par hypothèse) et aussi $a|(ca)$ (évident) donc a divise la combinaison linéaire $(ca)u + (cb)v$ c'est-à-dire c.

Propriété 6.11 (Corollaire) Soient a, b et c trois entiers strictement positifs.
Si $a|c$, $b|c$ et $PGCD(a,b) = 1$ alors $ab|c$.

Démonstration Ce théorème est une conséquence du théorème de Gauss.
Puisque $a|c$ $\exists k \in \mathbb{N}^*, c = ka$, de même puisque $b|c$ $\exists k' \in \mathbb{N}^*, c = k'b$.
Comme $ka = k'b$, $a|(k'b)$ mais puisque $PGCD(a,b) = 1$, d'après le théorème, $a|k'$.
Puisque $a|k'$ $\exists k'' \in \mathbb{N}^*, k' = k''a$ et donc $c = k'b = k''ab$, soit $ab|c$.

Remarques :

- La condition $PGCD(a,b) = 1$ est nécessaire car $6|12$ et $4|12$ mais $6 \times 4 = 24$ ne divise pas 12 (car $PGCD(6,4) = 2 \neq 1$).
- La réciproque est fausse (comme souvent) $6 \times 9|54$ et, bien sûr, $6|54$ et $9|54$ mais $PGCD(6,9) = 3 \neq 1$.

Exemple 4 – Résoudre l'équation diophantienne[1] $ax + by = k \times PGCD(a, b)$ avec $k \in \mathbb{Z}^*$.

➲ Résolvons l'équation $45x + 16y = 1$.
La méthode des congruences a été expliquée plus haut : il s'agit, dans un 1er temps, de déterminer l'inverse de 45 modulo 16 car $45x + 16y = 1 \iff 45x = 1[16]$.
Pour trouver toutes les solutions, on doit examiner les 16 valeurs de $45x$ modulo 16 :

x	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
$45x[16]$	0	13	10	7	4	1	14	11	8	5	2	15	12	9	6	3

On constate que pour $x = 5[16]$, on a $45x = 1[16]$ d'où la solution générale $x = 16k + 5$ avec $k \in \mathbb{Z}$.
Pour y, il suffit d'utiliser $45x + 16y = 1 \iff y = \frac{1-45x}{16}$ qui donne un entier, selon le théorème de Bézout car $PGCD(45, 16) = 1$. En remplaçant x par $16k + 5$, on obtient
$y = \frac{1-45(16k+5)}{16} = \frac{1-45(16k+5)}{16} = -45k - 14$.
On a donc $(x, y) = (16k + 5, -45k - 14)$ avec $k \in \mathbb{Z}$.
Une solution différente est obtenue pour chaque valeur de k :

- Pour $k = 0$ on obtient $(x, y) = (5, -14)$ et on vérifie $45 \times 5 + 16 \times (-14) = 1$
- Pour $k = -1$ on obtient $(x, y) = (-11, 31)$ et on vérifie $45 \times (-11) + 16 \times 31 = 1$
- etc.

Remarque : c'est très long d'obtenir ce tableau de congruence, et encore ici il n'y avait que 16 valeurs possibles pour x modulo 16. Cette méthode se prête bien à une utilisation algorithmique (programme, tableur), mais pour un travail manuel on lui préfèrera la méthode classique qui exploite la suite des divisions euclidiennes obtenues lors de la détermination du PGCD avec l'algorithme d'Euclide :

- $45 = 2 \times 16 + 13$
- $16 = 1 \times 13 + 3$
- $13 = 4 \times 3 + 1$

1 est le dernier reste non nul, ce qui prouve que $PGCD(45, 16) = 1$.
En partant du bas, on remplace progressivement les restes, en remontant les égalités :

- $1 = 13 - 4 \times 3$
- $3 = 16 - 1 \times 13$ donc $1 = 13 - 4 \times (16 - 1 \times 13) = 13 \times 5 - 4 \times 16$
- $13 = 45 - 2 \times 16$ donc $1 = (45 - 2 \times 16) \times 5 - 4 \times 16 = 45 \times 5 + 16 \times (-14)$

On obtient ainsi la solution particulière $(x, y) = (5, -14)$ puisque $1 = 45 \times 5 + 16 \times (-14)$.
De là on trouve les solutions générales en écrivant :
$45x + 16y = 1 \iff 45x + 16y = 45 \times 5 + 16 \times (-14) \iff 45(x - 5) = 16(-y - 14)$
Comme $PGCD(45, 16) = 1$, d'après le théorème de Gauss on a $16|(x - 5)$ et $45|(-y - 14)$.
Il existe donc deux entiers k et k' tels que $x - 5 = 16k$ et $-y - 14 = 45k'$.
L'équation transformée $(45(x - 5) = 16(-y - 14))$ s'écrit $45 \times 16k = 16 \times 45k' \iff k = k'$.
Conclusion : $x = 5 + 16k$ et $y = -14 - 45k$.

➲ Résolvons l'équation (E) : $45x + 16y = 12$.
On a résolu l'équation $45x + 16y = 1$ qui a pour solution particulière $(x, y) = (5, -14)$.
En multipliant par 12 l'égalité $45 \times 5 + 16 \times (-14) = 1$ on obtient
$45 \times 5 \times 12 + 16 \times (-14) \times 12 = 1 \times 12 \iff 45 \times 60 + 16 \times (-168) = 12$
Donc $(x, y) = (60, -168)$ est une solution particulière de (E).
De là, on trouve les solutions générales de (E) en écrivant :
$45x + 16y = 12 \iff 45x + 16y = 45 \times 60 + 16 \times (-168) \iff 45(x - 60) = 16(-y - 168)$
Comme $PGCD(45, 16) = 1$, d'après le théorème de Gauss on a $16|(x - 5)$ et $45|(-y - 14)$.
Il existe donc deux entiers k et k' tels que $x - 60 = 16k$ et $-y - 168 = 45k'$.
L'équation transformée s'écrit $45 \times 16k = 16 \times 45k' \iff k = k'$.
Conclusion : $x = 60 + 16k$ et $y = -168 - 45k$.

---

1. Les équations diophantiennes sont des équations où les inconnues et les coefficients sont entiers. Elles sont nommées d'après Diophante d'Alexandrie qui publia *Les Arithmétiques* vers le IIe siècle, une collection de problèmes polynomiaux avec des entiers, un livre dont la traduction par Bachet (1621) en latin inspira grandement Pierre de Fermat.

5. Nombres premiers, Théorème de Fermat

DÉFINITION 6.7 (PREMIER) Un nombre entier $n \in \mathbb{N}$ est premier si et seulement si il n'admet que deux diviseurs distincts dans $\mathbb{N}$: 1 et lui-même.

Remarques :

- 1 n'est pas premier car il n'a qu'un seul diviseur dans $\mathbb{N}$ (lui-même qui vaut 1). Une raison plus convaincante, pour anticiper sur l'unicité de la décomposition en facteurs premiers : 1 n'est pas premier car sinon on aurait une infinité de décompositions car $1 = 1^2 = 1^3 = \dots$.
- 0 n'est pas premier car il a une infinité de diviseurs. 2 est donc le premier nombre premier ; c'est en même temps le seul qui soit pair (évidemment, car les autres nombres pairs l'admet comme diviseur). La suite des nombres premiers commence par $2, 3, 5, 7, 11, 13, \dots$
- Les nombres qui ne sont pas premiers sont dits composés. Ils admettent plus de deux diviseurs. Les nombres 0 et 1 (et -1 dans $\mathbb{Z}$) font exceptions pour des raisons différentes (1 n'a qu'un seul diviseur et 0 en a une infinité). 4 est le premier nombre composé car il admet trois diviseurs distincts dans $\mathbb{N}$ (1, 2 et 4).

PROPRIÉTÉ 6.12 Un nombre composé $n \geqslant 2$ admet au moins un diviseur premier : le plus petit de ses diviseurs supérieur strictement à 1 qui est un nombre p tel que $p^2 \geqslant n$.

DÉMONSTRATION Comme n est composé il admet au moins un plus petit diviseur $p > 1$ qui est premier car, sinon, ce diviseur p serait lui-même divisible par un diviseur p' tel que $1 < p' < p$ qui diviserait aussi p ce qui ne se peut pas.
Comme p divise n, il existe un entier q tel que $n = pq$. Comme n est composé, on doit avoir $q > 1$ et comme p est le plus petit diviseur de n, on a nécessairement $p \leqslant q$. L'encadrement $1 < p \leqslant q$ multiplié par $p > 0$ s'écrit $p < p^2 \leqslant pq \iff p < p^2 \leqslant n$.

Remarques :

- Cette propriété a pour corollaire la propriété suivante : Si un nombre $n \geqslant 2$ n'admet aucun diviseur p tel que $p^2 \leqslant n$ alors il est premier. Ceci justifie qu'un algorithme testant la primalité d'un nombre n ne teste que les nombres $p \leqslant \sqrt{n}$ (en appliquant la racine carrée à $p^2 \leqslant n$), en les prenant de 2 en 2 à partir de 2 (car seul 2 est un premier pair).
  Pour tester si 101 est premier, on examine les restes des divisions euclidienne successives de 101 par $23, 5$ et 7 seulement : $101 = 1[2]$, $101 = 2[3]$, $101 = 1[5]$, $101 = 3[7]$. Inutile d'aller plus loin car le prochain carré de nombre premier est $11^2 = 121 > 101$, tous les multiples de 11 susceptibles de décomposer 101 ont déjà été testés. Conclusion : 101 est un nombre premier.
- Le crible d'Érathostène [2] permet d'obtenir la liste des nombres premiers inférieurs à un entier N : on élimine successivement, les multiples de 2 en commençant par $2^2 = 4$, les multiples de 3 en commençant par $3^2 = 9$, les multiples de 5 en commençant par $5^2 = 25$, etc. jusqu'aux multiples de $n = \sqrt{N}$ en commençant par n^2.
  Dans les remarques de la propriété 6.15, la fonction `premiers()` implémente cet algorithme et renvoie la liste des nombres premiers inférieurs à un entier `n`.

PROPRIÉTÉ 6.13 L'ensemble $\mathbb{P}$ des nombres premiers est infini.
Autrement dit, il n'existe pas de plus grand nombre premier.

2. Ératosthène (IIIe siècle avant J.-C. était conservateur de la grande bibliothèque d'Alexandrie. Il est connu pour son estimation du rayon de la Terre.

DÉMONSTRATION Euclide a prouvé cela par l'absurde, en supposant qu'il existe p, le plus grand des nombres premiers. Il construit ensuite le nombre $N = 2 \times 3 \times 5 \times \cdots \times p + 1$. Le reste de la division euclidienne de N par chacun des nombres premiers devra être égal à 1 car la définition de N équivaut à autant de divisions euclidiennes. N est donc premier car il n'est divisible par aucun des nombres premiers existants. Or ce nombre premier est plus grand que p qui, par hypothèse, est le plus grand. Cela étant contradictoire, il n'existe pas de plus grand nombre premier.

PROPRIÉTÉ 6.14 (DIVISIBILITÉS) Soient p un nombre premier et n un entier.
- Si p ne divise pas n alors $PGCD(p, n) = 1$
- $\forall (a_1, a_2, \ldots, a_k) \in \mathbb{Z}^k, p|(a_1 \times a_2 \times \cdots \times a_k) \iff \exists i \in \{1, 2, \ldots, k\}, p|a_i$.
- $\forall (p_1, p_2, \ldots, p_k) \in \mathbb{P}^k, p|(p_1 \times p_2 \times \cdots \times p_k) \iff \exists i \in \{1, 2, \ldots, k\}, p = p_i$.
- Soient $(p_1, p_2, \ldots, p_k) \in \mathbb{P}^k$, k nombres premiers distincts et $(a_1, a_2, \ldots, a_k) \in \mathbb{N}^{*k}$, Si $\forall i \in \{1, 2, \ldots, k\}, p_i^{a_i}|n$ alors $(p_1^{a_1} \times p_2^{a_2} \times \cdots \times p_k^{a_k})|n$.

DÉMONSTRATION ➠ p étant premier n'a que deux diviseurs et si p ne divise pas n, le seul diviseur commun à p et n est 1 donc ils sont premiers entre eux.

➠ Montrons d'abord $\forall (a_1, a_2) \in \mathbb{Z}^2, p|(a_1 a_2) \Longrightarrow p|a_1$ ou $p|a_2$.
Deux cas se présentent :
- $p|a_1$. L'implication est alors évidente.
- p ne divise pas a_1 mais, dans ce cas, d'après le théorème de Gauss, $p|a_2$.

On généralise cette propriété à k facteurs par récurrence en posant $A = a_1 \times a_2 \times \cdots \times a_k$.
Par hypothèse $p|A \Longrightarrow p|a_1$ ou $p|a_2$ ou $\ldots p|a_k$ et si $p|(A \times a_{k+1})$ alors, par application de la propriété précédente, $p|A$ ou $p|a_{k+1}$ donc $p|a_1$ ou $p|a_2$ ou $\ldots p|a_k$ ou $p|a_{k+1}$.

➠ Montrons d'abord $\forall (p_1, p_2) \in \mathbb{P}^2, p|(p_1 p_2) \iff p = p_1$ ou $p = p_2$.
D'après la propriété précédente $\forall (p_1, p_2) \in \mathbb{P}^2, p|(p_1 p_2) \iff p|p_1$ ou $p|p_2$.
Mais comme p_1 et p_2 sont premiers et que $p \neq 1$ (puisque p premier), cela implique $p = p_1$ ou $p = p_2$.
Par récurrence sur k on étend cette propriété à un produit de k facteurs premiers.

➠ Montrons d'abord $\forall (p_1, p_2) \in \mathbb{P}^2$, si $p_1 \neq p_2$, $p_1^{a_1}|n$ et $p_2^{a_2}|n$ alors $(p_1^{a_1} \times p_2^{a_2})|n$.
Si les nombres premiers p_1 et p_2 sont différents, les diviseurs de $p_1^{a_1}$ sont $1, p_1, p_1^2, \ldots, p_1^{a_1}$ et ceux de $p_2^{a_2}$ sont $1, p_2, p_2^2, \ldots, p_2^{a_2}$. Ces ensembles n'ont que 1 en commun car, d'après le 3e point, si $d|p_1^{a_1}$ alors $d|p_1$ et, de même, si $d|p_2^{a_2}$ alors $d|p_2$, mais le seul diviseur commun à p_1 et p_2 est 1.
Par conséquent, d'après la propriété 6.11, comme $p_1^{a_1}|n$, $p_2^{a_2}|n$ et $p_1^{a_1}$ et $p_2^{a_2}$ sont premiers entre eux, on en déduit que $(p_1^{a_1} \times p_2^{a_2})|n$.
Par récurrence sur k on étend cette propriété à un produit de k puissances de facteurs premiers.

Remarques :
- Le 1er point de cette propriété est faux en général si p n'est pas premier : 4 ne divise pas 6 mais $PGCD(4, 6) = 2 \neq 1$.
- Les 2e et 3e points de cette propriété conduisent à des cas particuliers intéressants :
  $\forall a \in \mathbb{Z}, p|(a^n) \iff p|a$.
  $\forall q \in \mathbb{P}, p|(q^k) \iff p = q$ (j'ai utilisé ce cas particulier pour démontrer le dernier point).
- La même remarque que pour la propriété 6.11 s'impose concernant le point 4 de cette propriété : La condition $PGCD(p_i^{a_i}, p_j^{a_j}) = 1$ est nécessaire d'où la nécessité d'avoir des nombres premiers distincts. Contre-exemple : $2^3|24$ et $2^2|24$ mais $2^3 \times 2^2 = 2^5$ ne divise pas 24.

PROPRIÉTÉ 6.15 (DÉCOMPOSITION EN FACTEURS PREMIERS) Un entier naturel supérieur à 1 se décompose de façon unique (à l'ordre des facteurs près) en produit de facteurs premiers.
Autrement dit, $\forall n \geqslant 2, \exists k \geqslant 1$, $(p_1, p_2, \ldots, p_k) \in \mathbb{P}^k$, k nombres premiers distincts et ordonnés $(p_1 < p_2 < \cdots < p_k)$ et $(a_1, a_2, \ldots, a_k) \in \mathbb{N}^{*k}$ tels que $n = p_1^{a_1} \times p_2^{a_2} \times \cdots \times p_k^{a_k}$.

DÉMONSTRATION ➲ Existence :
On a vu, propriété 6.12, que si $n > 1$ n'est pas premier alors il admet un diviseur premier p_1 tel que $n = p_1 q_1$ où q_1 est un entier inférieur strictement à n.
Par conséquent soit n est premier, dans ce cas la décomposition est trouvée, soit il ne l'est pas et s'écrit $n = p_1 q_1$ avec p_1 premier et $q_1 < n$.
On recommence alors avec q_1 qui est premier ou pas : s'il ne l'est pas, on l'écrit $q_1 = p_2 q_2$ avec p_2 premier (éventuellement confondu avec p_1) et $q_2 < q_1$.
On construit ainsi une suite d'entiers (q_n) strictement décroissante, donc finie.
Le dernier quotient trouvé est premier, ce qui met fin au processus de décomposition.

➲ Unicité :
Démontrons cela par récurrence sur la valeur de n en supposant que la décomposition de tous les entiers m tels que $1 < m < n$ soit unique.
Cette propriété est vraie pour $n = 3$ puisque pour $m = 2$ la décomposition est évidemment unique.
Supposons qu'il existe deux décompositions différentes de $n > 3$:
$n = p_1^{a_1} \times p_2^{a_2} \times \cdots \times p_k^{a_k} = q_1^{b_1} \times q_2^{b_2} \times \cdots \times q_l^{b_l}$.
Dans ce cas, un des facteurs premiers, disons p_1 divise n.
Donc $p_1 | (q_1^{b_1} \times q_2^{b_2} \times \cdots \times q_l^{b_l})$ et, d'après le 3e point de la propriété 6.14, il existe un indice $i \in \{1, 2, \ldots, l\}, p_1 = q_i$. On peut alors diviser l'égalité $n = p_1^{a_1} \times p_2^{a_2} \times \cdots \times p_k^{a_k} = q_1^{b_1} \times q_2^{b_2} \times \cdots \times q_l^{b_l}$ par p_1 et ainsi $\frac{n}{p_1}$ est un nombre inférieur strictement à n pour lequel, d'après l'hypothèse de récurrence, la décomposition est unique. Or $\frac{n}{p_1} = \frac{n}{q_i}$ ce qui prouve que les deux décompositions ne peuvent être différentes. La décomposition de n est par conséquent unique ce qui achève la démonstration.

Remarques :

- Le raisonnement utilisé pour montrer l'existence de la décomposition est constructive : elle constitue un algorithme utilisable dans la pratique. Cet algorithme nécessite la connaissance du début de la liste des nombres premiers : on commence par diviser n par 2, autant de fois qu'il est possible (tant que le reste est nul), puis on divise de la même façon le quotient résiduel par 3, puis par 5, etc. jusqu'à obtenir un nombre premier. Par exemple $60 = 2 \times 30 = 2 \times (2 \times 15) = 2 \times (2 \times (3 \times 5)) = 2^2 \times 3 \times 5$. Ci-dessous en haut à droite, la décomposition *à la main* de deux entiers, selon la disposition habituelle (en colonne).
- L'exposant de chaque nombre premier entrant dans la décomposition d'un entier est appelé « multiplicité » de ce facteur premier. Ainsi dans la décomposition de 60 en $2^2 \times 3 \times 5$, la multiplicité du facteur 2 est 2 et celle des facteurs 3 et 5 est 1. Le programme qui suit donne la décomposition d'un entier naturel supérieur à 1 en ordonnant les facteurs premiers dans l'ordre croissant et en notant les multiplicités avec le symbole `^`. La fonction `premiers()` détermine la liste des nombres premiers à l'aide du crible d'Ératosthène.

```
def premiers():
    L,k,nRacine=list(range(2,n+1)),2,n**0.5
    while k<nRacine :
        L=[p for p in L if p<=k or p%k!=0]
        k=L[L.index(k)+1] #nouveau nombre premier
    return L

n=int(input("Saisissez un nombre : "))
Liste_facteurs,decompo,i,s=premiers(),list(),0,str(n)+"="
#expurgation des nombress premiers non-facteurs de n
Liste_facteurs=[p for p in Liste_facteurs if n%p==0]
#recherche de la multiplicité de chaque facteur premier
while n>1 :
    expo=0
    while n%Liste_facteurs[i]==0 :
        expo+=1
        n//=Liste_facteurs[i]
    decompo.append([Liste_facteurs[i],expo])
    i+=1
for rang,facteur in enumerate(decompo) :
        s+=str(decompo[rang][0])+"^"+str(decompo[rang][1])
        if rang<len(decompo)-1 : s+='\u00D7'
print(s)
```

60	2
30	2
15	3
5	5
1	

1240	2
620	2
310	2
155	5
31	31
1	

$60 = 2^2 \times 3 \times 5$
$1240 = 2^3 \times 5 \times 31$

```
Saisissez un nombre : 1240
1240=2^3×5^1×31^1

Saisissez un nombre : 60
60=2^2×3^1×5^1
```

PROPRIÉTÉ 6.16 (DIVISEURS) Soit $n > 1$ un entier dont la décomposition en produit de facteurs premiers est $n = p_1^{a_1} \times p_2^{a_2} \times \cdots \times p_k^{a_k}$.

- $d|n \iff d = p_1^{b_1} \times p_2^{b_2} \times \cdots \times p_k^{b_k}$ où $\forall i \in \{1, 2, \ldots, k\}, b_i \in \mathbb{N}$ et $b_i \leqslant a_i$.
- Le nombre de diviseurs de n est $(a_1 + 1)(a_2 + 1) \ldots (a_k + 1)$.

DÉMONSTRATION ➠ Sens réciproque de l'équivalence :
On suppose que $d = p_1^{b_1} \times p_2^{b_2} \times \cdots \times p_k^{b_k}$ avec $0 \leqslant b_i \leqslant a_i$.
La décomposition de n peut donc s'écrire $n = (p_1^{b_1} \times p_1^{a_1-b_1}) \times (p_2^{b_2} \times p_2^{a_2-b_2}) \times \cdots \times (p_k^{b_k} \times p_k^{a_k-b_k})$.
En réarrangeant ce produit $n = (p_1^{b_1} \times p_2^{b_2} \times \cdots \times p_k^{b_k}) \times (p_1^{a_1-b_1} \times p_2^{a_2-b_2} \times \cdots \times p_k^{a_k-b_k})$.
En notant $q = p_1^{a_1-b_1} \times p_2^{a_2-b_2} \times \cdots \times p_k^{a_k-b_k}$, on obtient donc $n = d \times q$ ce qui prouve bien que $d|n$.

➠ Sens direct de l'équivalence :
Soit $d > 1$ un diviseur de n. Tout diviseur premier p de d est un diviseur premier de n.
En effet, si $p|d$, comme $d|n$, on en déduit que $p|n$.
D'après le 3e point de la propriété 6.14, si un nombre premier p divise un produit de facteurs premiers, alors c'est un de ces facteurs premiers. Donc, puisque $p|d$ on en déduit que $p = p_i$ avec $i \in [\![1; k]\!]$.
Conséquence : la décomposition de d en facteurs premiers s'écrit $d = p_1^{b_1} \times p_2^{b_2} \times \cdots \times p_k^{b_k}$ où les coefficients b_i sont des entiers, éventuellement nuls.
Il reste à prouver que $\forall i \in [\![1; n]\!], b_i \leqslant a_i$.
Comme $d|n$, on a $n = d \times q = (p_1^{b_1} \times p_2^{b_2} \times \cdots \times p_k^{b_k}) \times q$.
Examinons le cas d'une valeur particulière de $i \in [\![1; k]\!]$:
$n = \left[(p_1^{b_1} \times p_2^{b_2} \times \cdots \times p_{i-1}^{b_{i-1}} \times p_{i+1}^{b_{i+1}} \cdots \times p_k^{b_k}) \times q\right] \times p_i^{b_i}$.
En posant $Q = p_1^{b_1} \times p_2^{b_2} \times \cdots \times p_{i-1}^{b_{i-1}} \times p_{i+1}^{b_{i+1}} \cdots \times p_k^{b_k}) \times q$, on a $n = Q \times p_i^{b_i}$. Donc $p_i^{b_i}$ divise n.
Mais comme $p_i^{a_i}$ divise aussi n, on peut écrire $n = Q' \times p_i^{a_i}$ où Q' ne contient que des puissances de facteurs premiers différents de p_i.
On a donc $p_i^{b_i}$ divise $Q' \times p_i^{a_i}$ avec $p_i^{b_i}$ premier avec Q'. D'après le théorème de Gauss, on en déduit que $p_i^{b_i}$ divise $p_i^{a_i}$ et par conséquent $p_i^{b_i} \leqslant p_i^{a_i} \Longrightarrow b_i \leqslant a_i$.
Ceci étant valable pour tout $i \in [\![1; k]\!]$, on a bien $\forall i \in \{1, 2, \ldots, k\}, b_i \in \mathbb{N}$ et $b_i \leqslant a_i$.

➠ Somme des diviseurs :
On vient de voir que si $n = p_1^{a_1} \times p_2^{a_2} \times \cdots \times p_k^{a_k}$, les diviseurs de n s'écrivent $p_1^{b_1} \times p_2^{b_2} \times \cdots \times p_k^{b_k}$ avec $\forall i \in [\![1; k]\!], 0 \leqslant b_i \leqslant a_i$. Or, pour une valeur particulière de $i \in [\![1; k]\!]$, il existe $a_i + 1$ valeurs différentes de l'exposant b_i : $0, 1, 2, \ldots, a_i$.
Par conséquent, l'ajout du facteur premier p_i multiplie par $a_i + 1$ le nombre de diviseurs de n ne contenant pas ce facteur premier.
Ceci étant vrai pour tout $i \in [\![1; k]\!]$, le nombre total de diviseurs est le produit des nombres $a_i + 1$ pour tout $i \in [\![1; k]\!]$.

EXEMPLE 5 – Quels sont les diviseurs de $6048 = 2^5 \times 3^3 \times 7^1$ et combien sont-ils ?
La propriété précédente indique que 6048 possède $(5 + 1)(3 + 1)(1 + 1) = 6 \times 4 \times 2 = 48$ diviseurs.
Faisons-en la liste à l'aide de 2 tableaux, selon qu'ils contiennent ou non le facteur 7 :

7^0	$\times 2^0$	$\times 2^1$	$\times 2^2$	$\times 2^3$	$\times 2^4$	$\times 2^5$
$\times 3^0$	$2^0 3^0 = 1$	$2^1 3^0 = 2$	$2^2 3^0 = 4$	$2^3 3^0 = 8$	$2^4 3^0 = 16$	$2^5 3^0 = 32$
$\times 3^1$	$2^0 3^1 = 3$	$2^1 3^1 = 6$	$2^2 3^1 = 12$	$2^3 3^1 = 24$	$2^4 3^1 = 48$	$2^5 3^1 = 96$
$\times 3^2$	$2^0 3^2 = 9$	$2^1 3^2 = 18$	$2^2 3^2 = 36$	$2^3 3^2 = 72$	$2^4 3^2 = 144$	$2^5 3^2 = 288$
$\times 3^3$	$2^0 3^3 = 27$	$2^1 3^3 = 54$	$2^2 3^3 = 108$	$2^3 3^3 = 216$	$2^4 3^3 = 432$	$2^5 3^3 = 864$

7^1	$\times 2^0$	$\times 2^1$	$\times 2^2$	$\times 2^3$	$\times 2^4$	$\times 2^5$
$\times 3^0$	$2^0 3^0 7^1 = 7$	$2^1 3^0 7^1 = 14$	$2^2 3^0 7^1 = 28$	$2^3 3^0 7^1 = 56$	$2^4 3^0 7^1 = 112$	$2^5 3^0 7^1 = 224$
$\times 3^1$	$2^0 3^1 7^1 = 21$	$2^1 3^1 7^1 = 42$	$2^2 3^1 7^1 = 84$	$2^3 3^1 7^1 = 168$	$2^4 3^1 7^1 = 336$	$2^5 3^1 s 7^1 = 672$
$\times 3^2$	$2^0 3^2 7^1 = 63$	$2^1 3^2 7^1 = 126$	$2^2 3^2 7^1 = 252$	$2^3 3^2 7^1 = 504$	$2^4 3^2 7^1 = 1008$	$2^5 3^2 7^1 = 2016$
$\times 3^3$	$2^0 3^3 7^1 = 189$	$2^1 3^3 7^1 = 378$	$2^2 3^3 7^1 = 756$	$2^3 3^3 7^1 = 1512$	$2^4 3^3 7^1 = 3024$	$2^5 3^3 7^1 = 6048$

PROPRIÉTÉ 6.17 (PGCD, PPCM ET DÉCOMPOSITIONS) Soient $n = p_1^{a_1} \times p_2^{a_2} \times \cdots \times p_k^{a_k}$ et $m = p_1^{b_1} \times p_2^{b_2} \times \cdots \times p_k^{b_k}$, deux entiers dont les décompositions en produit de facteurs premiers contiennent des exposants a_i ou b_i pouvant éventuellement être nuls.

- $PGCD(n,m) = p_1^{\min(a_1,b_1)} \times p_2^{\min(a_2,b_2)} \times \cdots \times p_k^{\min(a_k,b_k)}$
- $PPCM(n,m) = p_1^{\max(a_1,b_1)} \times p_2^{\max(a_2,b_2)} \times \cdots \times p_k^{\max(a_k,b_k)}$
- $PGCD(n,m) \times PPCM(n,m) = n \times m$

DÉMONSTRATION ➠ D'après le 1er point de la propriété précédente,
comme $\forall i \in [\![1;k]\!], \min(a_i,b_i) \leqslant a_i$ et $\min(a_i,b_i) \leqslant b_i$, on en déduit que le nombre $p_1^{\min(a_1,b_1)} \times p_2^{\min(a_2,b_2)} \times \cdots \times p_k^{\min(a_k,b_k)}$ est un diviseur de n et de m.
Par conséquent ce nombre divise $PGCD(n;m)$.
Inversement, puisque $PGCD(n;m)$ divise n et m, la même propriété permet d'écrire $PGCD(n;m) = p_1^{c_1} \times p_2^{c_2} \times \cdots \times p_k^{c_k}$ où $\forall i \in [\![1;k]\!], 0 \leqslant c_i \leqslant a_i$ et $0 \leqslant c_i \leqslant b_i$, c'est-à-dire $c_i \leqslant min(a_i,b_i)$, on en déduit que $PGCD(n;m)$ divise $p_1^{\min(a_1,b_1)} \times p_2^{\min(a_2,b_2)} \times \cdots \times p_k^{\min(a_k,b_k)}$.
Comme $a|b$ et $b|a \Longrightarrow a = b$ (antisymétrie de la relation $|$ dans $\mathbb{N}$), on peut en conclure $PGCD(n;m) = p_1^{\min(a_1,b_1)} \times p_2^{\min(a_2,b_2)} \times \cdots \times p_k^{\min(a_k,b_k)}$.

➠ Comme $\forall i \in [\![1;k]\!], \max(a_i,b_i) \geqslant a_i$, on a $\max(a_i,b_i) - a_i \geqslant 0$. On en déduit :
$p_1^{\max(a_1,b_1)} \times \cdots \times p_k^{\max(a_k,b_k)} = \left[p_1^{\max(a_1,b_1)-a_1} \times \cdots \times p_k^{\max(a_k,b_k)-a_k}\right] \times \left[p_1^{a_1} \times \cdots \times p_k^{a_k}\right]$ soit, en posant $q = p_1^{\max(a_1,b_1)-a_1} \times \cdots \times p_k^{\max(a_k,b_k)-a_k}$, on a $p_1^{\max(a_1,b_1)} \times \cdots \times p_k^{\max(a_k,b_k)} = q \times n$.
Ce nombre est donc un multiple de n.
Pareillement, on montre que c'est aussi un multiple de m.
Ce nombre est donc un multiple commun de n et de m.
Inversement, un multiple commun de n et m peut s'écrire $p_1^{c_1} \times \cdots \times p_k^{c_k}$ où $\forall i \in [\![1;k]\!], c_i \geqslant a_i$ et $c_i \geqslant b_i$, c'est-à-dire $c_i \geqslant max(a_i,b_i)$.
On en déduit qu'un multiple commun de n et m est multiple de $p_1^{\max(a_1,b_1)} \times \cdots \times p_k^{\max(a_k,b_k)}$.
Ce nombre est donc le plus petit multiple commun de n et m.

➠ Si $max(a_i,b_i) = a_i$ alors $min(a_i,b_i) = b_i$ et si $max(a_i,b_i) = b_i$ alors $min(a_i,b_i) = a_i$, mais le produit $max(a_i,b_i) \times min(a_i,b_i)$ est dans tous les cas égal à $a_i \times b_i$. Cela permet de justifier le dernier point de cette propriété, nous laissons le lecteur finir cette démonstration.

EXEMPLE 6 – Prenons $n = 2^4 \times 3^5 \times 5^1 \times 7^2 = 952\,560$ et $m = 2^1 \times 3^3 \times 5^3 \times 11^1 = 74\,250$.
De ces décompositions, on tire immédiatement :

- $PGCD(n;m) = 2^1 \times 3^3 \times 5^1 = 270$
- $PPCM(n;m) = 2^4 \times 3^5 \times 5^3 \times 7^2 \times 11^1 = 261\,954\,000$

Vérification :
$PGCD(n;m) \times PPCM(n;m) = 270 \times 261\,954\,000 = 70\,727\,580\,000$
$n \times m = 952\,560 \times 74\,250 = 70\,727\,580\,000$
Applications :

$$\frac{1}{952\,560} + \frac{1}{74\,250} = \frac{5^2 \times 11 + 2^3 \times 3^2 \times 7^2}{70\,727\,580\,000} = \frac{275 + 3528}{70\,727\,580\,000} = \frac{3803}{70\,727\,580\,000}$$

$$\frac{74\,250}{952\,560} = \frac{\frac{74\,250}{270}}{\frac{952\,560}{270}} = \frac{2\,750}{3\,528}$$

Programmation récursive du PGCD
Utilisation de la propriété pour en déduire le PPCM

```
def pgcd(a,b): # forme récursive
    reste=a%b
    if reste==0 : return b
    else : return pgcd(b,reste)

A=int(input('PGCD de A : '))
B=int(input('et de B : '))
PGCD=pgcd(A,B)
print('PGCD({},{})={}'.format(A,B,PGCD))
print('PPCM({},{})={}'.format(A,B,A*B-PGCD))
```

```
PGCD de A : 952560
et de B : 74250
PGCD(952560,74250)=270
PPCM(952560,74250)=70727579730
```

6. Petit théorème de Fermat

6.a. Coefficients binomiaux

Quelques rappels utiles du cours sur le dénombrement (chapitre 1)

Définition 6.8 (Combinaisons) On appelle « combinaison » de p éléments d'un ensemble à $n \geqslant p$ éléments toute partie de E à p éléments. On note $\binom{n}{p}$ (se lit p parmi n), ou parfois C_n^p, le nombre de combinaisons de p éléments d'un ensemble à n éléments.

Propriété 6.18 (Dénombrement) Soient n et $p \leqslant n$ deux entiers.
$$\binom{n}{p} = \frac{n(n-1)\dots(n-p+1)}{p!} = \frac{n!}{p!(n-p)!}$$

Démonstration Cette propriété est démontrée dans le chapitre 1 (dénombrement)

Remarques :

- En particulier, on a $\binom{n}{1} = n$, $\binom{n}{n} = 1$ et $\binom{n}{0} = 1$.
- Trois autres propriétés de ces nombres, appelés « coefficients binomiaux » :
  - Symétrie : $\binom{n}{p} = \binom{n}{n-p}$ pour $0 \leqslant k \leqslant n$
  - Récurrence : $\binom{n}{p} = \frac{n}{p}\binom{n-1}{p-1}$ pour $p \neq 0$ et $n \neq 0$
  - Formule de Pascal : $\binom{n}{p} = \binom{n-1}{p-1} + \binom{n-1}{p}$ pour $n \geqslant 2$ et $1 \leqslant k \leqslant n-1$
- Dans une combinaison, l'ordre des éléments n'intervient pas et il ne peut y avoir de répétitions. Ainsi, lors d'un tirage d'une main de $p = 5$ cartes d'un jeu de $n = 32$ cartes, le nombre de mains possibles est $\binom{32}{5} = \frac{32\times31\times30\times29\times28}{1\times2\times3\times4\times5} = 201\,376$.
  De même, dans le développement du binôme $(a+b)^{32}$, le coefficient du terme a^5b^{27} est $\binom{32}{5} = 201\,376$ (il faut choisir le nombre a dans 5 facteurs parmi les 32 du développement).

Propriété 6.19 (Binôme de Newton) Soient a et b deux réels, pour tout entier n on a :
$(a+b)^n = \binom{n}{0}a^0b^n + \binom{n}{1}a^1b^{n-1} + \dots + \binom{n}{k}a^kb^{n-k} + \dots + \binom{n}{n}a^nb^0 = \sum_{k=0}^{n}\binom{n}{k}a^kb^{n-k}$

Démonstration La dernière remarque en donne un élément de justification mais cette propriété est démontrée plus rigoureusement dans le chapitre 1 (dénombrement).

Propriété 6.20 (Divisibilité par n premier) Soient a et b deux entiers.
Si n est un nombre premier alors $(a+b)^n = a^n + b^n[n]$

Démonstration ➠ Lemme : si n et k sont premiers entre eux alors $\binom{n}{k} = 0[n]$.
Écrivons la propriété de récurrence citée plus haut $k\binom{n}{k} = n\binom{n-1}{k-1}$ pour $k \neq 0$ et $n \neq 0$.
On en déduit que $n|k\binom{n}{k}$ et, comme n et k sont premiers entre eux, d'après le théorème de Gauss, $n|\binom{n}{k}$, ce qui revient à dire que $\binom{n}{k} = 0[n]$.

➠ En écrivant explicitement ses termes extrêmes, le développement du binôme s'écrit :
$(a+b)^n = b^n + \sum_{k=1}^{n-1}\binom{n}{k}a^kb^{n-k} + a^n$.
Comme n est premier, il est premier avec tous les entiers $1 \leqslant k \leqslant n-1$ et donc, d'après le lemme précédent, on a $\forall k \in [\![1, n-1]\!]$, $\binom{n}{k} = 0[n]$ d'où $\sum_{k=1}^{n-1}\binom{n}{k}a^kb^{n-k} = 0[n]$.
Finalement, il reste $(a+b)^n = a^n + b^n[n]$.

6.b. Théorème de Fermat

Propriété 6.21 (Fermat1) Si n est un nombre premier, quelque soit l'entier a on a $a^n = a[n]$

Démonstration ➠ Dans le cas $n = 2$:
On a $a^2 - a = a(a-1)$. Ce produit est nécessairement pair puisque l'un des deux entiers consécutifs n et $n-1$ est forcément pair, donc $a^2 - a$ est pair, autrement dit $a^2 - a = 0[2]$ ou encore $a^2 = a[2]$.

➠ Dans le cas où $n \neq 2$ est premier, n est impair :
Supposons a entier positif et montrons $a^n = a[n]$ par récurrence sur a.

- Initialisation : $0^n = 0[n]$
- Hérédité : la propriété est supposée vraie au rang a ($a^n = a[n]$)
  D'après la propriété précédente $(a+1)^n = a^n + 1^n = a^n + 1[n]$ et comme $a^n = a[n]$ (hypothèse de récurrence), on en déduit $(a+1)^n = a + 1[n]$.
  Ce qui prouve que la propriété est encore vraie au rang $a+1$.

Conclusion : la propriété est vraie pour a entier positif.

Supposons maintenant a entier strictement négatif.
Comme $-a$ est positif, on a $(-a)^n = -a[n]$ mais comme n est impair $(-a)^n = -(a^n) = -a^n$ d'où $-a^n = -a[n] \iff a^n = a[n]$.
La propriété est donc vraie pour tout $a \in \mathbb{Z}$ et tout nombre premier n.

Propriété 6.22 (Fermat2) Soit n est un nombre premier et a un entier.
Si n ne divise pas a alors $a^{n-1} = 1[n]$.

Démonstration D'après la propriété précédente, si n est premier :
$a^n - a = 0[n] \iff n|(a^n - a) \iff n|a(a^{n-1} - 1)$.
Comme n ne divise pas a, d'après le théorème de Gauss :
$n|(a^{n-1} - 1) \iff a^{n-1} - 1 = 0[n] \iff a^{n-1} = 1[n]$.

Remarques :

- Les deux propriétés énoncées (Fermat1 et Fermat2) sont indifféremment appelées *petit* théorème de Fermat et doivent être distinguées du *grand* théorème de Fermat qui énonce que l'équation $a^n + b^n = c^n$ où a, b, c et n sont des entiers strictement positifs, n'a pas de solution pour $n \geqslant 3$. Cette propriété ayant été démontrée par Andrew Wiles en 1994, elle a été rebaptisée théorème de Fermat-Wiles.
- Dans l'exemple 3, j'ai tracé le tableau des puissances de a modulo 5.
  On remarque dans ce tableau que pour tout a non divisible par 5, on a $a^4 = 1[5]$.
  Évidemment, lorsque $5|a$, cette propriété est fausse puisque $a = 0[5] \Longrightarrow a^4 = 0[5]$.
- On montre facilement que, dans les mêmes conditions, si N est un multiple de $n-1$ alors $a^N = 1[n]$. De même, dans ces conditions, les nombres a (premiers avec n) possèdent un inverse modulo n qui est une puissance de a. Par exemple modulo 5, l'inverse de 2 est 3 et réciproquement ($2 \times 3 = 1[5]$), 4 est son propre inverse ($4 \times 4 = 1[5]$).