Pgcd et Ppcm de deux nombres entiers.

On s'intéresse ici aux diviseurs des entiers relatifs, et plus particulièrement aux diviseurs positifs.

Pour $n \in \mathbb{Z}$ on notera D_n l'ensemble des diviseurs positifs de n.

1) Plus grand diviseur commun à deux entiers :

Définition 1 : Soit a et b deux entiers relatifs non tous les deux nuls.

L'ensemble des diviseurs communs à a et b est fini et non vide, il possède donc un **unique** plus grand élément, appelé **plus grand commun diviseur** de a et b, et noté $\boldsymbol{pgcd}(\boldsymbol{a}, \boldsymbol{b})$.

preuve de l'existence :

$D_0 = \mathbb{N}^*$, et si $a \neq 0$ alors D_a est fini,
car si d est un entier positif qui divise a alors $1 \leqslant d \leqslant |a|$.

Donc $D_a \cap D_b$ est un ensemble fini, et non vide puisqu'il contient 1.
Alors cet ensemble possède un plus grand élément, qui est unique.

Exemple : Pour trouver le pgcd de deux nombres, il suffit de regarder leurs diviseurs positifs.

$30 = 1\times30 = 2\times15 = 3\times10 = 5\times6$ et $72 = 1\times72 = 2\times36 = 3\times24 = 4\times18 = 6\times15 = 8\times9$

donc leur plus grand diviseur commun est $6 = pgcd(30, 72)$

Propriétés 1 : Soit a et b deux entiers relatifs non simultanément nuls.

i) $pgcd(a, b) \geqslant 1$

ii) $pgcd(a, b) = pgcd(b, a) = pgcd(-a, b)$

iii) $pgcd(a, 0) = |a|$ et $pgcd(a, 1) = 1$

iv) si b divise a alors $pgcd(a, b) = |b|$

Exemples :

Un diviseur positif est toujours supérieur ou égal à 1, on ne s'intéresse qu'aux diviseurs positifs donc peu importe les signes de a et b, avec 0 le plus grand diviseur est la valeur absolu du nombre, et avec 1 c'est 1, puis $pgcd(13, 39) = 13$ pour finir.

preuves :

i) $D_a \cap D_b = D_b \cap D_a$ et $1 \in D_a \cap D_b$ donc $pgcd(a,b) \geqslant 1$.

ii) et iii) évidents.

iiv Si b divise a alors : si c divise b alors c divise a donc $D_b \subset D_a$ et $D_a \cap D_b = D_b$.

2) Algorithme d'Euclide :

L'existence de la division euclidienne entre les entiers est fondamentale pour prouver la plupart des résultats d'arithmétique.

Propriété 2 : Soit a et b deux entiers naturels non nuls tels que b ne divise pas a.

La succession des divisions euclidiennes suivantes finit par s'arrêter.
Le dernier reste non nul est alors le $pgcd(a,b)$.

a par b	$a = bq_0 + r_0$	avec $b > r_0 \geqslant 0$
b par r_0	$b = r_0 q_1 + r_1$	avec $r_0 > r_1 \geqslant 0$
r_0 par r_1	$r_0 = r_0 q_2 + r_2$	avec $r_1 > r_2 \geqslant 0$
.....	.....	.....
.....	.....	.....
r_{n-2} par r_{n-1}	$r_{(n-2)} = r_{n-1} q_n + r_n$	avec $r_{n-1} > r_n \geqslant 0$
r_{n-1} par r_n	$r_{n-1} = r_n q_{n+1} + r_{n+1}$	avec $r_n > r_{n+1} = 0$

On a alors $pgcd(a,b) = r_n$, le **dernier reste non nul**.

preuve :

La suite des restes est une suite strictement décroissante dans $\mathbb{N}$ car $r_0 > r_1 > r_2 > \ldots > r_n$.
Cette suite est donc finie. Alors il existe n tel que $r_{n+1} = 0$.

i) Montrons que $pgcd(a,b) = pgcd(b, r_0)$:

Soit alors $D = pgcd(a,b)$ et $d = pgcd(b, r_0)$;

D divise a et b donc D divise $a - bq_0 = r_0$, donc D divise b et r_0 donc : $D \leqslant d$;
d divise b et r_0 donc d divise $bq_0 + r_0 = a$, donc d divise a et b donc : $d \leqslant D$.

ii) De proche en proche on en déduit :

$$pgcd(a,b)=pgcd(b,r_0)=pgcd(r_0,r_1)=\ldots=pgcd(r_{n-2},r_{n-1})=pgcd(r_{n-1},r_n)$$

or r_n divise r_{n-1} puisque $r_{n+1}=0$, donc $pgcd(r_{n-1},r_n)=r_n$.

iii) Conclusion : $pgcd(a,b)=r_n$ le dernier reste non nul.

Exemple : Calculons le pgcd(4 539, 1 958).

On effectue les divisions euclidiennes suivantes :

$$4\,539 = 1\,958\times 2 + 263$$
$$1\,958 = 623\times 3 + 89$$
$$623 = 89\times 7$$

Conclusion : pgcd(4 539, 1 958) = 89

Le peu d'étapes nécessaire montre l'efficacité de cet algorithme.

Calculatrices : Déterminons le pgcd(252,360).

T.I. : menu Maths puis Num et pgcd(252,360)
Casio : menu Option puis Num et PGCD(252,360)

Algorithme :

demander a et b
    tant que $b\neq 0$ faire :
        r prend la valeur du reste
        a prend la valeur de b
        b prend la valeur de r
    afficher a

```
# pgcd de deux entiers
from math import sqrt
a = int(input("donner l'entier a:"))
b = int(input("donner l'entier b:"))
while b != 0:
    r = a % b
    a, b = b, r
print(a)
```

On peut également intégrer ce calcul du pgcd au sein d'une fonction :

```
# fonction classique pgcd
def pgcd(a,b):
    while b!=0:
        a,b = b,reste(a,b)
    return abs(a)
```

```
# fonction pgcd récursive
def pgcd_rec(a,b):
    if b==0:
        return abs(a)
    else:
        return pgcd_rec(b,reste(a,b))
```

Propriété 3 : Soit a et b deux entiers relatifs non tous les deux nuls.

L'ensemble des diviseurs communs à a et b est l'ensemble des diviseurs de leur pgcd.

Autrement dit : d divise a et b $\Leftrightarrow$ d divise $pgcd(a,b)$.

preuve :

L'ensemble des diviseurs communs à a et b est égal à l'ensemble des diviseurs de b et r dans la division euclidienne, et ainsi de suite en recommençant les divisions.
Finalement, l'ensemble des diviseurs communs à a et b est l'ensemble des diviseurs du dernier reste non nul r_n, qui n'est autre que leur pgcd.

Exemple : Rechercher les diviseurs communs à deux nombres revient à chercher les diviseurs de leur pgcd.

Ainsi $pgcd(2\,730,5\,610)=30$ à la calculatrice, et $D_{30}=\{1,2,3,5,6,10,15,30\}$ qui sont les diviseurs communs à $2\,730$ et $5\,610$.

Propriété 4 : Soit a et b deux entiers relatifs non tous les deux nuls et $k\in\mathbb{N}^*$.

i) $pgcd(ka\,,kb)=k\,pgcd(a\,,b)$.

ii) si k divise a et b, $pgcd\left(\frac{a}{k},\frac{b}{k}\right)=\frac{1}{k}\,pgcd(a\,,b)$.

preuve :

i) $pgcd(ka,kb)=pgcd(kb,kr_0)=pgcd(kr_0,kr_1)=\ldots=pgcd(kr_n,0)=kr_n=k\,pgcd(a,b)$.

ii) si k divise a et b alors il divise leur reste et leur pgcd, donc on peut diviser l'égalité $a=bq+r$ par k, ce qui donne : $a/k=b/k\times q+r/k$ puis on poursuit les divisions.

Exemple : On peut simplifier des recherches de pgcd si l'on voit une factorisation.

Ainsi $pgcd(420,540)=20\times pgcd(21,27)=20\times 3=60$.

3) Nombres premiers entre eux :

Définition 2 : Soit a et b deux entiers relatifs non nuls.

Si $\boldsymbol{pgcd(a\,,b)=1}$ on dit que a et b sont **premiers entre eux**.
Ils n'ont que -1 et 1 comme diviseurs communs.

Remarques :

- Il ne font pas confondre des nombres premiers et des nombres premiers entre eux.
  Par exemple $pgcd(14,15)=1$ mais 14 et 15 ne sont pas premiers.
- En revanche, deux nombres premiers distincts sont nécessairement premiers entre eux.

Exercice : Nombres de Fermat

4) Plus petit multiple commun à deux entiers :

Définition 3 : Soit a et b deux entiers relatifs non nuls.

L'ensemble des multiples positifs communs à a et b est non vide, donc il possède un unique plus petit élément, appelé **plus petit commun multiple** de a et b, et noté $\boldsymbol{ppcm(a\,,b)}$.

preuve de l'existence :

L'ensemble des multiples positifs de a et b n'est pas vide puisqu'il contient $|a\,b|$.
Toute partie non vide de $\mathbb{N}$ possède un plus petit élément, donc le ppcm existe bien.

Exemple : $ppcm(18,12)=36$ et $ppcm(24,40)=120$

Pour additionner des fractions, on recherche le dénominateur commun le plus petit, qui n'est autre que le ppcm des deux nombres.

Propriété 5 : Soit a et b deux entiers relatifs non nuls.

i) $ppcm(a\,,b)=ppcm(b\,,a)=ppcm(-a\,,b)\geqslant 1$ et $ppcm(a\,,1)=|a|$

ii) si b divise a alors $ppcm(a\,,b)=|a|$

iii) $pgcd(a\,,b)\times ppcm(a\,,b)=|a\;b|$ et si $pgcd(a\,,b)=1$ alors $ppcm(a\,,b)=|a\,b|$.

5) Théorème de Bézout :

Propriété 6 : **Égalité** de Bézout

Soit a et b deux entiers relatifs non nuls et $d = pgcd(a, b)$.

Alors il existe deux entiers relatifs u et v tels que $d = au + bv$.

preuve :

- Soit E l'ensemble des nombres entiers positifs qui peuvent s'écrire sous la forme $au + bv$ avec $u, v \in \mathbb{Z}$; mathématiquement, on écrirait $E = \{au + bv \in \mathbb{N}^* / u, v \in \mathbb{Z}\}$.

Comme $|a| \in E$, E est une partie non vide de $\mathbb{N}$, donc E possède un plus petit élément d, d'après l'axiome de $\mathbb{N}$.
On a donc bien l'existence d'un entier positif $d = au + bv$ avec u et v entiers relatifs.

- Puisque le $pgcd(a, b)$ divise a et b, alors il divise $d = au + bv$. Donc $pgcd(a, b) \leqslant d$.

- Montrons maintenant que d divise a :

- Dans la division de a par d on obtient : $a = dq + r$ avec $0 \leqslant r < d$;
alors $r = a - dq = a - (au + bv)q = a - auq - bvq = a(1 - uq) + b(-vq)$

- Donc soit $r = 0$ et d divise a, soit $r \neq 0$ et alors $r \in E$.

Mais comme $r < d$, cela est impossible puisque d est le plus petit élément positif de E.
Donc r ne peut pas être non nul.

- De manière analogue, on démontre que d divise b, donc il divise a et b,
et donc nécessairement leur pgcd, ce qui prouve que $d \leqslant pgcd(a, b)$.

Finalement, on a démontré que $d = pgcd(a, b)$, et il existe bien une combinaison linéaire $au + bv = pgcd(a, b)$ où $(u, v) \in \mathbb{Z}^2$.

Propriété 7 : **Théorème** de Bézout

Deux entiers relatifs non nuls a et b sont premiers entre eux si et seulement s'il existe deux nombres relatifs u et v tels que $au + bv = 1$.

Les entiers relatifs u et v sont alors eux-mêmes premiers entre eux.

preuve :

CN : si $pgcd(a,b)=1$ alors $1=au+bv$ d'après l'égalité de Bézout.

CS : si $au+bv=1$ alors $pgcd(a,b)$ divise a et b, donc il divise 1, donc $pgcd(a,b)=1$.

Exemple : Deux entiers consécutifs quelconques sont toujours premiers entre eux.
En effet, $1\times(n+1)-1\times n=1$ pour tout $n\in Z$.

Exercice : Montrer que $2n+1$ et $3n+2$ sont premiers entre eux $\forall n\in\mathbb{N}$.

Propriété 8 : Soit un entier $n\geqslant 2$ et $a\in\mathbb{Z}^*$.

1) L'entier a possède un inverse dans la congruence modulo n ssi $pgcd(a,n)=1$.

Un inverse de a modulo n est un nombre b tel que $ab\equiv 1[n]$

2) Si $ac\equiv bc[n]$ et $pgcd(c,n)=1$, alors $a\equiv bn[n]$ (on peut simplifier)

preuve :

1) - si $ab\equiv 1[n]$ alors $ab=1+\alpha n$ donc $ab-\alpha n=1$ donc $pgcd(a,n)=1$.

- si $pgcd(a,n)=1$ alors $\alpha a+\beta n=1$ et $\alpha a=1+(-\beta)n$ donc $\alpha a\equiv 1[n]$.

2) Si $pgcd(c,n)=1$ alors il existe d tel que $cd\equiv 1[n]$.

Et comme $ac\equiv bc[n]$, alors on a $acd\equiv bcd[n]$ et donc $a\equiv b[n]$.

Propriété 9 : Corollaire de l'égalité de Bézout.

L'équation $ax+by=c$ admet des solutions entières si et seulement si c est un multiple de $pgcd(a,b)$.

preuve :

CN : Si (x_0,y_0) est une solution entière alors $c=ax_0+by_0$.
Le pgcd de a et b divise donc c.

CS : Si $c = k\,d$ où $d = pgcd(a\,,b)$ alors l'égalité de Bézout nous permet d'écrire que :
$au + bv = d \quad \Leftrightarrow \quad a\,ku + b\,kv = k\,d = c \quad \Leftrightarrow \quad ax_0 + b\,y_0 = c$ en posant $x_0 = ku$ et $y_0 = kv$.

Exemples :

L'équation $4x + 9y = 2$ admet des solutions entières car $pgcd(4\,,9) = 1$,
et 2 est multiple de 1 .

L'équation $9x - 15y = 2$ n'admet pas de solution entières car $pgcd(9\,,15) = 3$,
et 2 n'est pas multiple de 3 .

Algorithme de Bézout : Soient a et b deux entiers premiers entre eux.

Il s'agit de déterminer les coefficients de Bézout u et v tels que $au + bv = 1$.

On cherche d'abord u .

Pour cela, on regarde les multiples de a sous la forme $a\,u$ en commençant par $u = 1$,
puis on regarde leur reste dans la division par b ,
ce qui donne $a\,u = bq + r$ avec un reste non nul au début.
On recommence en faisant augmenter u , tant que le reste ne vaut pas 1 .

A ce moment là, on obtient $a\,u = b\,q + 1$, et donc $a\,u + b(-q) = 1$,
ce qui donne $v = -q = (1 - a\,u)/b$.

En langage naturel :

demander a et b
u prend la valeur 0
r prend la valeur 0
tant que $r \neq 1$ faire :
    u prend la valeur u + 1
    r prend la valeur du reste de a*u par b
v prend la valeur (1 - a*u) / b
afficher u et v

En Python :

```
# fonction coefficient de Bézout
def coeff_bezout(a, b):
    r, u = 0, 0
    while r != 1:
        u = u + 1
        r = (a*u) % b
    v = (1 - a*u)/b
    return u, v
# programme principal
p = int(input("donner a:"))
q = int(input("donner b:"))
print(coeff_bezout(p, q))
```

Exercice :

En utilisant l'algorithme d'Euclide, montrer que 64 et 27 sont premiers entre eux.
En remontant les divisions en partant de 1, déterminer un couple $(x\,,y)$ tel que $64x + 27y = 1$.

6) Lemme de Gauss et conséquences :

Propriété 10 : Lemme de Gauss

Soit trois entiers relatifs non nuls a , b et c .

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

preuve :

Si a est premier avec b alors $au+bv=1$ d'après le théorème de Bézout.
Alors $auc+bvc=c$.
Comme a divise bc , il divise bvc , et aussi auc , donc il divise c .

autre preuve ne nécessitant pas le théorème de Bézout :

Comme a divise ac et bc il divise leur $pgcd(ac,bc)=c\,pgcd(a,b)=c$.

Exemple : Déterminons les solutions entières de l'équation $5(x-1)=7y$.

D'après l'équation, 5 divise $7y$, or $pgcd(5,7)=1$, donc d'après le lemme de Gauss, 5 divise y, donc $y=5k$, pour $k\in\mathbb{Z}$.
En remplaçant dans l'équation, on obtient $x=7k+1$.

Les solutions sont donc nécessairement de la forme $\begin{cases} x=7k+1 \\ y=5k \end{cases}$ pour $k\in\mathbb{Z}$.

On doit maintenant vérifier que cela est suffisant, en vérifiant que tous les nombres de cette forme sont bien solutions de l'équation de départ. Ce qui est bien le cas.

Exercice :

1) Déterminer les solution de l'équation $5x+7y=1$, en commençant par en trouver une solution particulière..

2) Déterminer les solutions de l'équation $5x+7y=12$.

Propriété 11 : Corollaire au lemme de Gauss

Si b et c divisent a, et si b et c sont premiers entre eux, alors bc divise a.

preuve :

Si b divise a, alors $a = k\,b$ et si c divise $k\,b$, comme $pgcd(b,c) = 1$ alors c divise k, d'après le lemme de Gauss, donc $a = k\,b = k'\,c\,b$.
Ce qui prouve que bc divise a.

Remarque : Attention, si deux nombres en divisent un même troisième, ce n'est pas en général le cas pour du produit de ces deux nombres.

En conséquences des théorèmes de Bézout et de Gauss, on a la propriété suivante.

Propriété 12 : Soit a et b deux nombres relatifs non nuls.

On note $d = pgcd(a,b)$ et $m = ppcm(a,b)$.

i) Alors il existe deux entiers a' et b' premiers entre eux tels que $\begin{cases} a = d \times a' \\ b = d \times b' \end{cases}$.

ii) On a les relations suivantes : $m = d \times a'b'$ et $ab = md$.

Exercice : Chiffrement affine

Chiffrement

Afin de coder un message on assimile chaque lettre de l'alphabet à un nombre entier comme l'indique le tableau ci-dessous :

A	B	C	D	E	F	G	H	I	J	K	L	M
0	1	2	3	4	5	6	7	8	9	10	11	12
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
13	14	15	16	17	18	19	20	21	22	23	24	25

Le chiffrement ou cryptage consiste à coder un message. Le déchiffrement consiste à décoder une message codé.

Etienne Bézout (1730-1783)

Carl Friedrich Gauss (1777-1855)

Application

Un chiffrement élémentaire est le chiffrage affine. On se donne une fonction de codage affine f, par exemple : $f(x) = 11x + 8$.
À une lettre du message :

- on lui associe un entier x entre 0 et 25 suivant le tableau ci-dessus
- on calcule $f(x) = 11x + 8$ et l'on détermine le reste y de la division euclidienne de $f(x)$ par 26
- On traduit y par une lettre d'après le tableau ci-dessus

Exemple : Si l'on veut coder par exemple la lettre G par la fonction $f(x) = 11x + 8$

$$\text{G} \Rightarrow x = 6 \Rightarrow 11 \times 6 + 8 = 74 \Rightarrow 74 \equiv 22\ (26) \Rightarrow y = 22 \Rightarrow \text{W}$$

La lettre G est donc codée par la lettre W.

Remarques

- Pour la fonction de déchiffrage f^{-1}, vous n'aurez qu'à vous laisser guider par l'énoncé. Dans l'exemple $f^{-1}(y) = 19y + 4$.
- D'autres chiffrements existent comme le chiffrement de Hill où l'on prend les lettres par paquet de 2. Là encore laissez-vous guider par l'énoncé.