Nombres Premiers / composés

On désire disposer régulièrement *n* billes pour former un rectangle complet, non réduit à une ligne /colonne:

Si on y arrive, *n* est le produit de 2 nombres. Ci-dessus : 12 = 3 (lignes) x 4 (colonnes). On dit que *n* est un **nombre composé**.

Si on n'y arrive pas, *n* ne se décompose pas en produit de deux nombres, on dit que *n* est un **nombre premier**. On voit ci-dessous que 7 est un nombre premier.


→ Donc Un nombre premier est un entier naturel qui admet exactement deux diviseurs distincts entiers et positifs (qui sont alors 1 et lui-même car il n'est pas composé càd produit de deux nombres).

Les nombres premiers jusqu'à 100 :

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

→ *Tout entier naturel (plus grand que 1) qui n'est pas premier est décomposable d'une manière unique en un produit de nombres premiers.*

Exemple 1 : Décomposer 280 en un produit de facteurs premiers.

280	2
140	2
70	2
35	5
7	7
1	

280=2*2*2*5*7 (2 colonne contient des nombres premiers. Arret si quotient=1)

Exercice : Décomposer 7425 en un produit de facteurs premiers (7425=3*3*3*5*5*11)

PGCD *: Le plus grand commun diviseur*

Pour calculer le PGCD de deux nombres→ décomposer ces deux nombres en un produit de facteurs premiers. Le PGCD est alors le produit des facteurs premiers commun dans les deux décompositions :

Exercice: pgcd(170,578) ? 170 = **2***5***17** et 578 = **2*****17***17. Les facteurs communs sont 2 et 17, donc le PGCD(170, 578) = 2*17 = 34.

PPCM : Le plus petit commun multiple : deux méthode de calcul :

1. → Le PPCM de a et b est égal au produit de tous les facteurs premiers de a et de tous ceux de b, avec pour chacun d'eux l'exposant le plus grand de ceux qu'il a dans la décomposition de a et de b.

Exercice : $PPCM(675,360)=3^3\times5^2\times2^3=5400.$ car $675=3^3\times5^2$ et $360=2^3\times3^2\times5$

2. → PPCM (a,b) = a.b÷PGCD (a,b)

Entiers premiers entre eux : Deux entiers sont premiers entre eux lorsque leur PGCD est égal à 1.

Propriété :

Soient a et b des naturels non nuls et d un diviseur commun de a et b. On pose a = d a′ et b = d b′.
Le PGCD de a et b est d si et seulement si a′ et b′ sont premiers entre eux.

Preuve :

Si d est le PGCD de a et b alors d =pgcd(a ; b)=pgcd(d a′ ; d b′)=d pgcd(a′ ; b′). Comme d est non nul, pgcd(a ′ ; b′) = 1 donc a′ et b′ sont premiers entre eux.

Inversement si pgcd(a′ ; b′) = 1, alors pgcd(a ; b) = d pgcd(a′ ; b′) = d

La division euclidienne

Exemple : Avec 167 bouteilles, combien peut-on remplir de cartons de 6 bouteilles ?

167 = 6 × 27 + 5. On peut remplir 27 cartons, il reste 5 bouteilles. → division euclidienne de 167 par 6 → le quotient=27, le reste=5, le diviseur=6 et Dividende=167

Dans la division a÷b, le quotient est le nombre entier q tel que a=bq+r, où r est le reste < diviseur.

Arithmétique modulaire est un système arithmétique d'entiers modifiés, où les nombres sont « abaissés » lorsqu'ils atteignent une certaine valeur.

Définition : Deux entiers relatifs *a* et *b* sont dits **congrus modulo *n*** ($\mathbb{Z}/n\mathbb{Z}$) si leur différence est divisible par *n*, c'est-à-dire si *a* est de la forme *b* + *kn* avec *k* entier.
Exemple : $167 \equiv 5 \, mod(27) \equiv 5 \, mod(6)$ 167 est congru 5 modulo 27 et congru 5 modulo 6

Lemme d'Euclide (propriété fondamentale) : soit un couple d'entiers naturels non nuls (a,b), si des entiers naturels q et r, avec $r \neq 0$ a> b, sont tels que $a = bq + r$, alors : $PGCD(a,b) = PGCD(b,r)$.
autrement $PGCD(a,b) = PGCD(b, a \, mod(b))$.
Démonstration :

On note D(a) l'ensemble des diviseurs de a. soit $E = D(a) \cap D(b)$ et $F = D(b) \cap D(r)$, on montre que E est inclus dans F et que F est inclus dans E .

• Soit d ∈ E . Alors d divise b, donc d divise bq et comme d divise a, d divise a − bq = r , donc $d \in F$.

• Soit $d \in F$. . d divise b donc bq. Comme d divise r , d divise bq + r = a donc $d \in E$.

Les ensembles E et F sont égaux, donc ils ont le même plus grand élément. Ainsi : pgcd(a ; b)=pgcd(b ; r).

Exercice : Déterminer, selon les valeurs de n, le PGCD de A = 2n + 1 et de B = n − 5.
solution : Pour éliminer n, on calcule A−2B. A−2B = 2n+1−2(n−5) = 11 donc A = 2B+11.

PGCD(A ; B)=PGCD(B ; 11).

Comme 11 est un nombre premier, le PGCD de B et de 11 ne peut valoir que 1 ou 11.

→ PGCD(B ; 11) = 11 ⇔ 11 divise B → B ≡ 0 mod(11) ⇔ n − 5 ≡ 0 mod(11) ⇔ n ≡ 5 mod(11).

Donc le PGCD de A et B est 11 lorsque n est congru à 5 modulo 11 et à 1 dans les autres cas.

Ex n=16 → pgcd (A,B)=11 pour n=7 → pgcd (A,B)=1

Théorème de Bézout

Deux entiers a et b sont premiers entre eux si, et seulement si, il existe deux entiers relatifs u et v tels que au + bv = 1.

Exemple : -5 et 12 sont premiers entre eux car 7 × (−5) + 3 × 12 = 1.

Corollaire

Si d est le PGCD de deux entiers a et b, alors il existe des entiers u et v tels que au + bv = d .

Exercice 5 Montrer qu'un nombre premier est premier avec tous les nombres qu'il ne divise pas.

Sol. Soit p un nombre premier. Soit a un entier non divisible par p. On note d=pgcd(p, a).
d vaut 1 ou p car p est premier. d ne peut pas être égal à p, sinon p diviserait a. → d = 1

Algorithme d'Euclide

$a_0 = a$ → $a_{i+1} = b_i$

$b_0 = b$ $\quad b_{i+1} = a_i \, mod(b_i)$ On s'arrête dès que

$b_i = 0$ $\quad pgcd(a,b) = a \wedge b = a_i = b_{i-1}$

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

print(pgcd(170, 578))
```

```
def pgcd(a,b):
    if b==0 :
        return a
    else :
        return pgcd(b,a%b)

print(pgcd(170, 578))
```