PGCD ET NOMBRES PREMIERS	
Cours	*Terminale maths expertes*

Objectifs :
- *Déterminer le PGCD de deux entiers.*
- *Établir et utiliser des tests de divisibilité, étudier la primalité de certains nombres, étudier des problèmes de chiffrement.*

1. PGCD de deux entiers

Tous les diviseurs de 36 sont : ……………………………………………………..

Tous les diviseurs de 48 sont : ……………………………………………………..

Les diviseurs communs à 36 et 48 sont : ……………………………………………………..

Le plus grand diviseur commun à 36 et 48 est …... On le nomme le PGCD de 36 et 48.

Définition 1. *Plus grand diviseur commun*

On appelle plus grand commun diviseur des entiers naturels non nuls a et b, l'entier naturel dont l'ensemble des diviseurs est égal à l'ensemble des diviseurs de a et de b. On le note PGCD (a ; b).

Remarque : On peut généraliser la définition 1 aux entiers quelconques : soit a et b des entiers naturels non nuls simultanément. Comme l'ensemble des diviseurs de (- a) est l'ensemble des diviseurs de a, et que, l'ensemble des diviseurs de (- b) est l'ensemble des diviseurs de b, $PGCD(a\ ;\ a) = PGCD(|a|\ ;\ |b|)$.

Exercice 1

Déterminer PGCD(105 ; 45), en dressant la liste des diviseurs de chacun de ces entiers.

Propriété 1. *PGCD*

Soit a et b des entiers naturels non nuls.

1. PGCD (a ; b) = ……………..

2. PGCD (a ; a) = ……

3. PGCD (1 ; a) = ……

4. PGCD (a ; 0) = ……

Démonstrations : 1. Chercher les diviseurs communs à a et à b revient à chercher les diviseurs communs à ………………

2. Conséquence de la définition.

3. Le seul diviseur de 1 est ….. Donc le plus grand diviseur commun à 1 et à a est …..

4. L'ensemble des diviseurs de 0 est $\mathbb{N}$; donc PGCD (a ; 0) = ……

5. Si b divise a alors tous diviseurs de b sont des diviseurs de a. Donc le plus grand diviseur de b est un diviseur de a.

http://fr.wikipedia.org/wiki/Euclide

Euclide a vécu au 3ème siècle avant notre ère en Grèce. Il est considéré comme le "père de la géométrie". Son ouvrage le plus célèbre, les Éléments, comprenant 13 tomes est un des plus anciens traités connus présentant de manière systématique, à partir d'axiomes et de postulats et avec des démonstrations, un large ensemble de théorèmes sur la géométrie et l'arithmétique. Ce traité est, paraît-il, le livre qui s'est le plus vendu au monde après la bible.

Théorème 1.

Soient a et b deux entiers naturels non nuls.
Soit r le reste de la division euclidienne de a par b.

Alors PGCD (a ; b) = …………………

Démonstration :
Si a n'est pas multiple de b, alors $a = bq + r$ avec $0 \leq r < b$.

Tout diviseur commun de a et de b divise alors a et bq, donc divise aussi leur différence r.
Réciproquement, tout diviseur commun de b et de r divise aussi $a = bq + r$ alors tout diviseur commun de b et de r est un diviseur commun de a et de b.

Exemple : Déterminer le PGCD de 65 et de 80.

On applique l'algorithme d'Euclide :
$80 = 1 \times 65 + 15$
$65 = 4 \times 15 + 5$
$15 = 3 \times 5 + 0$
Le dernier reste non nul est …… donc PGCD (65 ; 80) = ……
En effet, d'après la propriété précédente :
PGCD (80 ; 65) = PGCD (65 ; 15) = PGCD (15 ; 5) = PGCD (5 ; 0) = …..

Avec une TI 83 :

Avec Python :

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

Exercice 2
Déterminer le PGCD de 252 et de 360.

[corrigé en vidéo]

Propriété 2. *Ensemble des diviseurs communs de deux entiers*

Soit a et b deux entiers naturels non nuls.
L'ensemble des diviseurs communs de a et b est l'ensemble des diviseurs de leur PGCD.

Exercice 3
Déterminer les diviseurs communs de 2 730 et 5 610.

[corrigé en vidéo]

Exercice 4
Déterminer l'ensemble des diviseurs communs à 390 et 525.

Exercice 5
Soient a et b deux entiers naturels non nuls. Soient $x = 7a + 5b$ et $y = 4a + 3b$.
Montrer que le PGCD de x et de y est égal au PGCD de a et de b.

Propriété 3. *PGCD*

Soit a et b deux entiers naturels non nuls.
Pour tout entier naturel k, PGCD (ka ; kb) = ….. $\times$ PGCD (a ; b).

Exemple : PGCD (420 ; 540) = PGCD (…… ; ……) car $420 = 20 \times ......$ et $540 = 20 \times ......$.
Or PGCD (21 ; 27) = …… ; d'où PGCD (420 ; 540) = $20 \times ...... = ...$.

2. Théorème de Bézout et théorème de Gauss

Définition 2. *Nombres premiers entre eux*

Deux entiers naturels non nuls sont dits premiers entre eux lorsque leur PGCD est égal à ……

Exemple : 35 et 23 sont deux entiers naturels premiers entre eux car $35 = 7 \times 5$ et $23 = 23 \times 1$ ont pour PGCD l'entier …….

Exercice 6
Démontrer que 153 et 104 sont premiers entre eux.

Remarque : Il ne faut pas confondre les nombres premiers et les nombres premiers entre eux. 153 et 104 ne sont pas premiers, mais ils sont premiers entre eux. Mais deux nombres premiers distincts sont premiers entre eux car les diviseurs positifs d'un nombre premier sont 1 et lui-même.

Propriété 4. ***Identité de Bézout***

Soient a et b deux entiers naturels non nuls et d leur PGCD.

Il existe deux entiers relatifs u et v tels que $au + bv = ...$.

Démonstration : Soit l'ensemble E des entiers positifs de la forme $au + bv$, avec u et v entiers relatifs. Cet ensemble n'est pas vide, car il contient a $(a = 1 \times a + 0 \times b)$.
E contient alors un plus petit élément noté d qui s'écrit sous la forme $au_0 + bv_0$.
Le but de la démonstration est de montrer que d est le PGCD de a et b.

La division euclidienne de a par d s'écrit : $a = qd + r$ avec $0 \leq r < d$.
Supposons que $r > 0$; alors $r = a - qd = a - q(au_0 + bv_0) = a(1 - qu_0) + b(-qv_0)$. D'où r appartient à E, et est plus petit que d. C'est impossible car d est le plus petit élément de E : il y a une contradiction. Par conséquent, $r = 0$, et par suite, d divise a.

On montre de même que d divise b. Par conséquent, d est un diviseur commun à a et à b.
On en déduit que $d \leq \text{PGCD}(a ; b)$.

De plus, $\text{PGCD}(a ; b)$ divise a et b donc divise toute combinaison linéaire de a et de b.
Par suite, $\text{PGCD}(a ; b)$ divise d. D'où $\text{PGCD}(a ; b) \leq d$.
Par conséquent, $d = \text{PGCD}(a ; b)$.

Exemple : On sait que PGCD (65 ; 80) = ….. Il existe donc deux entiers relatifs u et v tels que $65u + 80v = ...$.

Le couple $(5 ; -4)$ convient car $65 \times 5 + 80 \times (-4) = 5$.

Théorème 2. ***Théorème de Bézout***

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

Démonstration : • Si a et b sont premiers entre eux alors le résultat est immédiat d'après l'identité de Bézout.

• S'il existe des entiers u et v tels que $au + bv = ...$, alors, si d est le PGCD de a et b, il divise a et b, donc ……………., c'est-à-dire ……. Par suite, d vaut ……., et a et b sont premiers entre eux.

Remarque : La relation $au+bv=1$ est parfois appelée relation de Bézout relative aux entiers a et b.

Exemples : • 35 et 12 sont premiers entre eux, car on a l'égalité $35\times......+12\times......=1$.

• Soit n un entier. Alors, n et $n+1$ sont premiers entre eux, car on peut écrire

$......\times(n+1)+......\times n=1$. Ainsi, deux entiers consécutifs sont toujours premiers entre eux.

Exercice 7

Démontrer que pour tout entier naturel n, $2n+3$ et $5n+7$ sont premiers entre eux.

corrigé en vidéo

Exercice 8

Démontrer que pour tout entier naturel n, $2n+1$ et $3n+1$ sont premiers entre eux.

Exercice 9

Montrer que 99 et 56 sont premiers entre eux, puis déterminer des entiers u et v tels que $99u+56v=1$.

Exercice 10

Montrer que 59 et 27 sont premiers entre eux, puis déterminer deux entiers x et y tels que $59x+27y=1$.

Propriété 5. ***Corollaire du théorème de Bézout***

Soit un entier naturel n tel que $n\geq 2$.

Un entier a est inversible modulo n si, et seulement si, a et n sont ………………..

…………….

Exercice 11

1) Déterminer un inverse de 5 modulo 16.

2) En déduire les solutions de l'équation $5x\equiv 7\ [16]$.

corrigé en vidéo

Exercice 12

Déterminer tous les entiers inversibles modulo n, et préciser leur inverse, pour :

1) $n=8$; 2) $n=11$; 3) $n=24$.

Claude-Gaspard Bachet

(Source : Wikipédia)

Ce théorème est parfois appelé théorème de Bachet-Bézout.
C'est en fait Bachet de Méziriac qui a établi ce théorème en 1621.
Étienne Bézout (1730-1783) a généralisé ce résultat.

Étienne Bézout

(Source : Wikipédia)

Johann Carl Friedrich Gauss

(Source : Wikipédia)

Carl Fiedrich Gauss (1777-1855), surnommé « le prince des mathématiques », publia dès 1801 un important ouvrage de théorie des nombres « Disquisitiones arithmeticae ».

Théorème 3. ***Théorème de Gauss***

Soient a, b et c trois entiers non nuls. Si a divise le produit bc et s'il est premier avec b, alors a divise ……

Démonstration : Soit a, b et c trois entiers naturels non nuls. Supposons que a divise bc et PGCD (a ; b) = 1.

Si PGCD (a ; b) = 1, alors PGCD (ac ; bc) = ……

Il est évident que a divise ac et, par hypothèse, a divise bc donc a divise …………………,

c'est-à-dire a divise ……

Exemple : Soient a et b deux entiers tels que 3a = 4b. Ici, 4 divise le produit 3a, et les entiers 3 et 4 sont premiers entre eux. D'après le théorème de Gauss, 4 divise a.

Théorème 4. ***Corollaire du théorème de Gauss***

Soient a, b et c trois entiers naturels non nuls.
Si a et b divisent c, et si a et b sont premiers entre eux alors ab divise ……

L'hypothèse « a et b premiers entre eux » est fondamentale.
Par exemple, 4 et 6 divisent 36, mais leur produit 24 ne divise pas 36.

Démonstration : Comme n est divisible par a et b, il existe des entiers k et k' tels que : $n = ka = k'b$. Cette égalité montre que a divise $k'b$; comme a et b sont premiers entre eux, le théorème de Gauss assure que a divise k', donc il existe un entier q tel que $k' = qa$.
On en déduit : $n = qab$, donc n est divisible par ab.

Exemple : 6 et 11 divisent 660, et 6 et 11 sont premiers entre eux, donc 66 divise 660.

Exercice 13

1) Soit n un entier naturel. On suppose que $5n$ est un multiple de 3. Quelles sont les valeurs possibles pour n ?

2) Soit n un entier naturel multiple de 7 et de 11. Quelles sont les valeurs possibles pour n ?

corrigé en vidéo

Propriété 6. *Équation diophantienne*

Soit l'équation l'équation $ax + by = c$, d'inconnues entières x et y.

• Si PGCD(a ; b) ne divise pas c, alors l'équation n'a aucune solution.

• Si PGCD(a ; b) divise c, alors l'équation a une infinité de solution.

Exemple : PGCD(21 ; 15) = 3 ; ainsi l'équation diophantienne $21x + 15y = 4$ n'a aucune solution.

Exercice 14

a) Déterminer les entiers x et y tels que $5x + 7y = 1$.

b) Déterminer les entiers x et y tels que $5x + 7y = 12$.

corrigé en vidéo

Exercice 15

1) Déterminer les entiers x et y tels que $2x + 3y = 1$.

2) Déterminer les entiers x et y tels que $2x + 3y = 5$.

Exercice 16

Déterminer les entiers x et y tels que $15x + 6y = 18$.

Exercice 17

Déterminer les entiers x et y tels que $5x = 3y$.

Exercice 18

Lors d'un trek, un marcheur a effectué des réservations dans deux types de gîtes : le gîte A et le gîte B.
Une nuit dans le gîte A coûte 24 € et une nuit dans le gîte B coûte 45 €.
Il se rappelle que le coût total de sa réservation est de 885 €.
On souhaite retrouver les nombres x et y de nuitées passées respectivement dans le gîte A et dans le gîte B.

1) Montrer que les nombres x et y sont respectivement inférieurs ou égaux à 36 et 19.
2) Justifier que le coût total de la réservation est un multiple de 3.
3) a) Justifier que l'équation $8x + 15y = 1$ admet pour solution au moins un couple d'entiers relatifs. En déterminer un.
b) En déduire une solution $(x_0\ ;\ y_0)$ de l'équation $8x + 15y = 295$.
c) Démontrer que $(x\ ;\ y)$ est solution de $8x + 15y = 295$ si, et seulement si, $8(x - x_0) = -15(y - y_0)$.

d) En déduire l'ensemble des solutions de l'équation $8x+15y=295$.

e) Expliquer pourquoi résoudre le problème revient à résoudre l'équation $8x+15y=295$ où x et y sont des nombres entiers relatifs vérifiant $0 \leqslant x \leqslant 36$ et $0 \leqslant y \leqslant 19$.

f) Compléter le programme Python suivant afin qu'il retourne une solution du problème.

```
def bezout() :
    for x in range(...............) :
       for y in range(................) :
           if ...................................... :
                 return(x,y)
```

g) Programmer la fonction `bezout` puis déterminer une solution possible du problème.

4) Le randonneur se souvient avoir passé entre 10 et 20 nuits dans le gîte A. Déterminer le nombre exact de nuits passées dans le gîte A et celui des nuits passées dans le gîte B.

3. Nombres premiers

Définition 3. *Nombre premier*

Un nombre premier est un entier naturel qui admet exactement deux diviseurs : 1 et lui-même.

Exemples : 1 n'est pas premier. 2 est premier : c'est le plus petit nombre premier, et c'est le seul qui soit pair.
Les nombres premiers inférieurs à 50 sont : 2 ; 3 ; 5 ; 7 ; 11 ; 13 ; 17 ; 19 ; 23 ; 29 ; 31 ; 37 ; 41 ; 43 et 47.

Dans les années 1950 le géologue belge Jean de Heinzelin de Braucourt découvrit ces ossements dans des couches de cendres volcaniques au bord du lac Édouard dans la région d'Ishango au Congo belge (aujourd'hui République démocratique du Congo), près de la frontière ougandaise. Il s'agit de deux os d'approximativement 10 cm et 14 cm, provenant d'animaux non identifiés (on pense à des os humains, de singe ou de lion). Ces os portent plusieurs incisions sur chacune de leurs faces. Le plus petit porte plusieurs incisions, organisées en groupes de trois colonnes. La colonne de gauche peut être divisée en 4 groupes. Chaque groupe possède respectivement 19, 17, 13 et 11 entailles. Ce sont les quatre nombres premiers successifs compris entre 10 et 20.

http://fr.wikipedia.org/wiki/Os_d'Ishango

Exercice 19

1) Montrer que le nombre $f(n)=n^2+18n+77$ n'est premier pour aucune valeur de l'entier naturel n. On pourra factoriser $f(n)$ ...

2) Peut-on trouver un entier négatif n tel que $f(n)$ soit premier ?

Exercice 20

Soit p un nombre premier impair. Déterminer les entiers naturels x et y tels que $x^2-y^2=p$.

Propriété 7. *Critère d'arrêt*

Tout entier naturel n supérieur ou égal à 2 admet un diviseur premier.
Si n n'est pas premier, alors il admet un diviseur p premier tel que $2 \leq p \leq \sqrt{n}$.

Démonstration : • Soit n un entier strictement supérieur à 1.
→ Si n est premier, il admet lui-même comme diviseur premier.
→ Si n est composé, il admet d'autres diviseurs que 1 et n : soit p le plus petit d'entre eux.
Alors, p est premier ; sinon, il serait composé et il admettrait un diviseur d tel que $1 < d < p$; mais d serait alors un diviseur de n plus petit que p, ce qui est impossible. Donc, p est premier et n admet p comme diviseur premier.

• On peut écrire que $n = p \times q$ avec $p \leq q$ car p est le plus petit élément de l'ensemble des diviseurs de n autre que 1 et n.
En multipliant cette inégalité par p, on obtient : $p \times p \leq q \times p$, c'est-à-dire $p^2 \leq n$.
On en déduit que : $p \leq \sqrt{n}$.

Exemple : 247 est-il premier ? Comme $\sqrt{247} \approx 15{,}7$, il suffit d'examiner si 247 est divisible par ……………………………. Puisque 247 est divisible par ……, alors 247 n'est pas un nombre premier.

Exercice 21
323 et 139 sont-ils des nombres premiers ?

Exercice 22

La fonction ci-contre renvoie le plus petit diviseur premier d'un entier naturel n supérieur ou égal à 2, en utilisant le principe du critère d'arrêt.
Si elle renvoie n, l'entier n est premier.
Compléter les pointillés.

```
from math import*

def plus_petit_diviseur_premier(n):
    r=int(floor(sqrt(n)))
    d=2
    while n%d!=0 and d<=r:
        d+=1
    if d<=r:
        return ...
    else :
        return ...
```

La fonction ci-contre renvoie la liste des nombres premiers inférieurs ou égaux à un entier naturel n supérieur ou égal à 2.
La compléter.
La dernière ligne doit être sur la même ligne que l'avant-dernière ; il y a eu un saut pour des raisons de place.

```
from math import*

def liste_nb_premiers_inferieurs_ou_egaux_a_(n):
    return [plus_petit_diviseur_premier(i) for i in range(2,n+1)
    if plus_petit_diviseur_premier(i)==...]
```

Théorème 5. ***Infinité des nombres premiers***

Il existe une infinité de nombres premiers.

Démonstration : Raisonnons par l'absurde en supposant qu'il existe un nombre fini d'entiers premiers. Soit p le plus grand d'entre eux et soit N le produit de tous ces nombres premiers : $2\times3\times5\times...\times p$.

Soit à présent l'entier $N' = N + 1$: le reste de la division euclidienne de N' par 2, 3, 5, … ou p est ….., donc N' n'est divisible par aucun des entiers 2, 3, 5, …, p.

→ Si N' est premier, il est ………………. à p, ce qui est absurde.

→ Si N' n'est pas premier, il a au moins un diviseur premier qui est ………………. à p, ce qui est absurde.

Théorème 6. ***Théorème fondamental de l'arithmétique***

Tout entier naturel n strictement supérieur à 1 se décompose en produit de facteurs premiers. Cette décomposition est unique à l'ordre près des facteurs. On note $n = p_1^{\alpha_1}\times p_2^{\alpha_2}\times...\times p_m^{\alpha_m}$ avec $p_1, p_2, ..., p_m$ des nombres premiers distincts et $\alpha_1, \alpha_2, ..., \alpha_m$ des entiers naturels non nuls.

Exemple : Décomposer en facteurs premiers le nombre 924.

On teste comme diviseurs les nombres premiers successifs 2, 3, 5, …
On obtient : $924 = 2^2\times3\times7\times11$.

Théorème 7. ***Nombre de diviseurs d'un entier***

Soit un entier naturel n, supérieur ou égal à 2, dont la décomposition en facteurs premiers est $n = p_1^{\alpha_1}\times p_2^{\alpha_2}\times...\times p_m^{\alpha_m}$.
Tout diviseur d de n admet une décomposition en produit de facteurs premiers de la forme $d = p_1^{\beta_1}\times p_2^{\beta_2}\times...\times p_m^{\beta_m}$, avec $0\le\beta_i\le\alpha_i$ pour tout $1\le i\le m$.
Le nombre de diviseurs de n est alors égal à $(\alpha_1+1)(\alpha_2+1)...(\alpha_m+1)$.

Exemple : $924 = 2^2\times3\times7\times11$ alors $2^1\times3^0\times7^0\times11 = 22$ est un diviseur de 924.

Exercice 23
1) Décomposer 17 640 et 411 600 en produits de facteurs premiers.
2) En déduire le PGCD de ces deux nombres.

corrigé en vidéo

Exercice 24
Décomposer 21 168 en produit de nombres premiers.

21 168 = $2^4 \times 3^3 \times 7^2$

Exercice 25
Déterminer tous les diviseurs de 132.

corrigé en vidéo

Exercice 26
Trouver le nombre de diviseurs de 120, puis déterminer tous ces diviseurs.

Exercice 27
Un entier naturel n a 15 diviseurs. On sait de plus que n est divisible par 6 mais pas par 8. Déterminer cet entier n.

Exercice 24
1) À l'aide de la décomposition en facteurs premiers de 84, résoudre dans $\mathbb{N}$ l'équation :
$x(x+1)(2x+1)=84$.

Exercice 29
Un annuaire comportant 999 991 noms a entre 100 et 1 000 pages et plus de 1 000 noms par page. On trouve le même nombre de noms sur toutes les pages.
Combien a-t-il de pages ?

Théorème 8. ***Petit théorème de Fermat***

Soit p un nombre premier.
Pour tout entier naturel a non multiple de p, $a^{p-1} \equiv 1 \ [p]$.

Exercice 30
Démontrer que pour tout entier naturel n, 7 divise $3^{6n}-1$.

corrigé en vidéo

Exercice 31
1) Vérifier que 761 est un nombre premier.
2) L'entier n est un entier naturel composé de 760 chiffres tous égaux à 9 : $n = \underbrace{999...99}_{760 \text{ fois}}$.

a) Calculer $n+1$.
b) Montrer que 761 divise n.

Théorème 9. ***Corollaire du petit théorème de Fermat***

Si p est un nombre premier et si a est un entier, alors $a^p \equiv ......\ [p]$.

Exercice 32

Soit n un entier naturel non nul ; on note $a = n^{13} - n$.

1) Montrer que a est divisible par 13 et 7.
2) En déduire que a est divisible par 182.

Pierre de Fermat (1601-1655) a rédigé peu de ses démonstrations, mais la plupart des résultats arithmétiques qu'il a annoncés étaient vrais.

C. Lainé