Chapitre 3 : PGCD et théorèmes fondamentaux de l'arithmétique

1. PGCD :

1.1. Définition : Soient a et b deux entiers relatifs non nuls. L'ensemble des diviseurs communs à a *et* b admet un plus grand élément δ, appelé PGCD de a et b. On le note $\boldsymbol{PGCD(a,b)}$ ou $\boldsymbol{PGCD(b,a)}$.

Remarques importantes :

- $b|a$ si et seulement si $PGCD(a,b)=b$. (*démonstration à connaître*).
- Pour démontrer que $PGCD(a,b)=PGCD(m,n)$, on peut par exemple démontrer que l'ensemble des diviseurs communs à a et b est le même que celui de m et n.
- A la calculatrice, on utilise la touche « gcd ».

1.2. Algorithme d'Euclide, calcul du PGCD :

Soient a et b deux entiers naturels non nuls. La suite des divisions euclidiennes :

- de a par b : $a=bq_0+r_0$;
- de b par r_0 (si $r_0\neq 0$) : $b=r_0q_1+r_1$;
- de r_0 par r_1(si $r_1\neq 0$) : $r_0=r_1q_2+r_2$;
- ….
- de r_{n-1} par r_n (si $r_n\neq 0$) : $r_{n-1}=r_nq_{n+1}+r_{n+1}$.

finit par s'arrêter, l'un des restes r_i étant nul.

Le dernier reste non nul est alors le PGCD de a et b.

Démonstration :

Lemme : Soient a,b,q,r des entiers relatifs non nuls tels que $a=bq+r$.
Alors $PGCD(a,b)=PGCD(b,r)$.

Démonstration du lemme : on va montrer que les ensembles de diviseurs des deux couples sont les mêmes.

- Soit d un diviseur commun à a et b. Alors d divise toute combinaison linéaire de a et b, et en particulier $a-bq$. Donc $d|r$. d est donc un diviseur commun à b *et* r.
- Réciproquement, soit d' un diviseur commun à b *et* r. Alors d' divise $a=bq+r$, comme combinaison linéaire de b et r. Donc d' est un diviseur commun à b *et* a.
- Les ensembles des diviseurs communs aux deux couples étant les mêmes, ces deux couples ont le même PGCD.

Démonstration du théorème : Les propriétés liées à la division euclidienne imposent que $b>r_0>r_1>\cdots>r_i>\cdots\geq 0$. La suite (r_i) est donc une suite d'entiers strictement décroissante d'entiers naturels, elle est donc finie. Elle possède donc un plus petit élément strictement positif (le dernier reste non nul), notons-le r_n.

D'après le lemme, on a : $PGCD(a,b)=PGCD(b,r_0)=PGCD(r_0,r_1)=\cdots=PGCD(r_{n-2},r_{n-1})=PGCD(r_{n-1},r_n)$

Or $r_{n-2}=r_{n-1}q_n+r_n$ et $r_{n-1}=r_nq_{n+1}$ (car r_n est le dernier reste non nul). Donc $r_n|r_{n-1}$ et $PGCD(r_{n-1},r_n)=r_n$.

D'où $PGCD(a,b)=r_n$.

1.3. Propriétés du PGCD, nombres premiers entre eux : (DAC)

- L'ensemble des **diviseurs communs à a et b** est l'ensemble des **diviseurs de leur PGCD.**
- Pour tous entiers naturels a,b et k non nuls, on a $\boxed{PGCD(ka,kb)=kPGCD(a,b)}$.

Csq : Pour tous entiers naturels a,b et k non nuls, avec k diviseur de a et b on a $PGCD\left(\frac{a}{k},\frac{b}{k}\right)=\frac{1}{k}PGCD(a,b)$.

- Les deux entiers relatifs non nuls a et b sont dits **premiers entre eux** ou **étrangers**, lorsque leur PGCD est 1.

Soit $(a,b)\in\mathbb{Z}^*\times\mathbb{Z}^*$. Si $d=PGCD(a,b)$ alors il existe deux entiers relatifs a'et b' premiers entre eux tels que $a=d\times a'$et $d=d\times b'$.

2. Etienne Bézout (1730 – 1783) :

Génie précoce, Bézout était à 19 ans adjoint de l'Académie des sciences. Sa plus grande œuvre, *Théorie générale des équations algébriques*, un traité clair et détaillé, témoigne de sa volonté de rendre parfaitement accessibles ses découvertes. Toutes ses publications restent encore très largement usitées pendant tout le XIX^{ème} siècle.

2.1. Identité de Bézout :

> Soient a et b deux entiers **relatifs** non nuls et D leur PGCD. Alors il existe deux entiers **relatifs** u et v tels que :
> $$au + bv = D$$

Démonstration :

- Soit E l'ensemble des entiers naturels non nuls de la forme $ax + by$, où x, y sont des entiers relatifs. Cet ensemble est une partie non vide de $\mathbb{N}$ (il contient $a = a \times 1 + b \times 0$ si $a > 0$ ou $-a = -1 \times a + 0 \times b$ si $a < 0$). E possède donc un plus petit élément, n.non nul. Par définition, il existe deux entiers relatifs u, v tels que $n = au + bv$.
  Or, D divise a et b, donc D divise n.
- On montre alors que n divise a : la division euclidienne de a par n s'écrit $a = nq + r$ avec $0 \leq r < n$. Alors $r = a - nq = a - (au + bv)q = a(1 - uq) - b(vq)$. Donc r est de la forme $ax + by$. Mais $r < n$. Donc $r = 0$. D'où n divise a.
- De même, n divise b. Par suite, n divise D.
- On en déduit que $n = D$ et donc $D = au + bv$ pour deux entiers relatifs u et v.

2.2. Théorème de Bézout :

> Deux entiers **relatifs** non nuls a et $b$sont premiers entre eux si et seulement si il existe deux entiers **relatifs** u et v tels que :
> $$au + bv = 1$$

Démonstration : à vous de la faire !

2.3. Exemple de détermination des coefficients de Bézout :

Soient $a = 62$ et $b = 43$. L'algorithme d'Euclide s'écrit :

$$62 = 43 \times 1 + 19 \quad (1)$$
$$43 = 19 \times 2 + 5 \quad (2)$$
$$19 = 5 \times 3 + 4 \quad (3)$$
$$5 = 4 \times 1 + 1 \quad (4)$$

Il s'agit de remonter l'algorithme en éliminant les restes, sauf le PGCD :
On a : $5 - 4 \times 1 = \mathbf{1}$ (4)
Or, $19 - 5 \times 3 = 4$ (3) donc $5 - (19 - 5 \times 3) \times 1 = \mathbf{1}$ soit $-19 \times 1 + 5 \times 4 = 1$.
Avec (2) : $5 = 43 - 19 \times 2$, d'où $-19 \times 1 + (43 - 19 \times 2) \times 4 = \mathbf{1}$
ie $-19 \times 1 + 43 \times 4 - 19 \times 8 = \mathbf{1}$ ie $-19 \times 9 + 43 \times 4 = \mathbf{1}$.
Avec (1) : $19 = 62 - 43 \times 1$, donc $-(62 - 43 \times 1) \times 9 + 43 \times 4 = \mathbf{1}$
Soit $-62 \times 9 + 43 \times 13 = \mathbf{1}$.
Une solution est donc $(-9\,;13)$.

3. Johann Carl Friedrich Gauss (1777 – 1855) :

Mathématicien, physicien, astronome allemand, il n'est pas un seul domaine des sciences que Gauss n'ait pas abordé. On lui doit, entre autres, la première étude complète des congruences en 1801, des travaux sur les nombres complexes, le magnétisme, l'algèbre, et bien sûr l'arithmétique. Depuis son plus jeune âge, il avait une affinité particulière avec les nombres, et calcula de tête, grâce à une ruse de sioux, et presque immédiatement la somme des cent premiers nombres entiers vers 5 ou 6 ans :

$$1 + 2 + 3 + \cdots + 99 + 100 = (1 + 100)(2 + 99) \ldots (50 + 51) = 50 \times 101 = 5050\ldots$$

3.1. Théorème de Gauss :

Théorème :

> Soient a, b, c trois entiers naturels. Si a divise bc et si a est premier avec b, alors a divise c.

Remarques : Tout élève sérieux ne saurait oublier l'hypothèse « a est premier avec b ». On remarquera également que la réciproque de cette propriété est fausse…

Démonstration : ROC

On a par hypothèse a divise bc, donc il existe un entier k tel que $bc = ak$.

De plus, a est premier avc b donc d'après le théorème de Bezout, il existe deux entiers relatifs u, v tels que $au + bv = 1$. En multipliant cette égalité par c, il vient $auc + bcv = c$, soit $auc + akv = c$ ie $a(uc + kv) = c$. Or $uc + kv$ est un entier relatif. Donc a divise bien c.

- **Corollaire :** Comme tout bon théorème, celui de Gauss a son corollaire :

> Si n est divisible par a et par b et si a et b sont premiers entre eux, alors n est divisible par leur produit ab.

Démonstration :R♥C

(1) Avec Bezout : On a $n = ak$ et $n = bk'$ pour des entiers k, k'. De plus, d'après le théorème de Bezout, il existe deux entiers relatifs u, v tels que $au + bv = 1$. En multipliant cette égalité par n, il vient : $nau + nbv = n$. Donc $bk'au + akbv = n$ *ie* $ab(k'u + kv) = n$. Or $k'u + kv$ est un entier relatif. D'où ab divise bien n.

(2) Avec Gauss : On a $n = ak$ et $n = bk'$ pour des entiers k, k'. Donc $ak = bk'$. D'où $a|bk'$, mais a est premier avec b, donc d'après le théorème de Gauss, $a|k'$. Il existe alors un entier p tel que $k' = ap$. D'où $n = bap$. Or p est un entier, donc ab divise bien n.

- **Application : démonstration du lien entre PGCD et PPCM :**

> Pour tous entiers naturels non nuls a et b,
> $$PGCD(a;b) \times PPCM(a;b) = a \times b$$

Démonstration :

Soient a et b deux entiers naturels non nuls.

- *1er cas : a et b sont premiers entre eux.*

$a|PPCM(a,b)$ donc il existe un entier k tel que $PPCM(a,b) = ka$. Alors $b|PPCM(a,b)$ soit $b|ka$. Or b est premier avec a. Donc $b|k$ d'après le théorème de Gauss. D'où $b \leq k$ et donc $ab \leq ka$ ie $ab \leq PPCM\ (a,b)$.
Or, il est clair que $PPCM(a,b) \leq ab$. D'où l'égalité, avec $PGCD(a,b) = 1$.

- *2ème cas : a et b ne sont pas premiers entre eux. On nomme $\delta = PGCD(a,b)$.On a vu qu'alors $PPCM(a,b) = \delta\ PPCM\left(\frac{a}{\delta}, \frac{b}{\delta}\right)$. Mais $\frac{a}{\delta}$ et $\frac{b}{\delta}$ sont premiers entre eux. Donc d'après le cas précédent : $PPCM\left(\frac{a}{\delta}, \frac{b}{\delta}\right) = \frac{a}{\delta}\frac{b}{\delta} = \frac{ab}{\delta^2}$.*

D'où $PPCM(a,b) = \delta\ \frac{ab}{\delta^2} = \frac{ab}{\delta}$ ie $\mu = \frac{ab}{\delta}$ et $\mu\delta = ab$.

3.2. Application à la résolution d'équations diophantiennes :

Diophante d'Alexandrie, vers les années 250 de notre ère, recherchait déjà systématiquement les solutions en nombres entiers (ou rationnels) d'une équation ou d'un système d'équations. D'où le nom d'équations diophantiennes pour des équations polynomiales à coefficient entiers et dont on recherche les solutions entières (ou rationnelles).

Exemple : Etudions l'équation $8x + 5y = 1$.

- Elle a pour solution « évidente » $x_0 = 2$, $y_0 = -3$.
- Par suite, un couple $(x\,;y)$ est solution de l'équation ssi $8(x - x_0) + 5(y - y_0) = 0$.
  D'où $8(x - x_0) = -5(y - y_0)$.
  On en déduit que $8 \mid 5(y - y_0)$, mais 8 est premier avec 5. D'après le th de Gauss, $8 \mid y - y_0$. Il existe donc un entier k tel que $y - y_0 = 8k$, soit $y = -3 + 8k$. Alors, $x - x_0 = -5k$ et donc $x = 2 - 5k$, $k \in \mathbb{Z}$.

Pour trouver la solution particulière, on peut notamment utiliser les coefficients de Bézout…

Rqe : Les équations diophantiennes n'ont pas toutes de solution dans $\mathbb{Z} \times \mathbb{Z}$: il n'y a pas de solution à $ax + by = c$ lorsque c n'est pas un multiple du $PGCD(a,b)$.