ARITHMETIQUE PARTIE 2

Chapitre 3

PGCD, PPCM, théorème de Bézout, théorème de Gauss

Arithmétique partie 2

PGCD, PPCM, THEOREME DE BEZOUT, THEOREME DE GAUSS

I. PGCD

1. Définition

Soit a et b deux nombres entiers non nuls. Alors le plus grand diviseur commun des deux nombres a et b est noté $PGCD(a;b)$.

Exemple

$PGCD(4;16) = 4$
$PGCD(34;112) = 2$

Pour trouver le $PGCD$ de deux nombres on peut dresser la liste des diviseurs des deux nombres. Alors le $PGCD$ de ces deux nombres est le plus grand diviseur commun à ces deux nombres.

Propriété (Démonstration hors programme)

Soit k un entier naturel non nul, alors on a : $PGCD(ka;kb) = k \times PGCD(a;b)$

2. Nombres premiers entre eux

Définition

On dit que deux nombres a et b sont premiers entre eux si et seulement si :

$$PGCD(a;b) = 1$$

Remarque

Il ne faut pas confondre nombres premiers entre eux et nombres premiers. En effet, 32 et 33 ne sont pas premiers car ils sont respectivement divisibles par 2 et 3. En revanche, 32 et 33 sont premiers entre eux car leur PGCD vaut 1.

3. Algorithme d'Euclide

L'algorithme d'Euclide permet de trouver « à la main » le PGCD de deux entiers. On souhaite déterminer le PGCD de 32 et 44. Alors on fait la division euclidienne du plus grand nombre par le plus petit :

$$44 = 32 \times 1 + 12$$

On réalise ensuite la division euclidienne du diviseur de cette première division par son reste :

$$32 = 12 \times 2 + 8$$

On répète la dernière opération jusqu'à trouver un reste nul :

$$12 = 8 \times 1 + \mathbf{4}$$
$$8 = 4 \times 2 + 0$$

Dès lors le $PGCD(32;44) = 4$

II. PPCM

Définition

Soient a et b deux entiers non nuls. Alors le $PPCM$ de a et b noté $PPCM(a;b)$ est le plus petit multiple commun à a et b.

Exemple

$PPCM(18,12) = 36$
$PPCM(24; 40) = 120$

Propriété (Démonstration hors programme)

$$\boldsymbol{ab = PPCM(a; b) \times PGCD(a; b)}$$

Illustration

D'une part, nous avons : $PGCD(8; 12) = 4$ et $PPCM(8; 12) = 24$ d'où $4 \times 24 = 96$

D'autre part, nous avons $8 \times 12 = 96$.

Ainsi, nous pouvons dire que la propriété est vérifiée dans ce cas particulier. On admettra qu'elle est vraie pour tous les entiers a et b.

III. THEOREME DE BEZOUT

1. Egalité de Bézout

Soient a et b deux entiers non nuls. On pose $D = PGCD(a; b)$. Dès lors il existe un couple d'entiers $(u; v)$ tels que :

$$\boldsymbol{au + bv = D}$$

Remarque IMPORTANTE

L'égalité de Bézout est une implication seulement, cela signifie que la réciproque est fausse.

Démonstration (importance : haute)

- Soient a et b deux entiers non nuls.
  On note E un ensemble constitué des nombres entiers strictement positifs sous la forme : $ma + nb$ où m et n sont des entiers relatifs quelconques.
  On peut donc dire que E est une partie de $\mathbb{N}$ qui est non vide, c'est-à-dire qu'il y a forcément au moins un élément dans E. Pour vérifier que E est non vide, on peut vérifier qu'il y existe au moins un élément.
  En effet on peut aisément vérifier que $|b| \in E$.
  Donc E admet un plus petit élément. Ce plus petit élément, on l'appelle $\boldsymbol{d = au + bv}$. En fait, d est atteint pour $m = u$ et $n = v$.
  Soit $D = PGCD(a\,; b)$ donc D/a et D/b donc D divise TOUTE combinaison linéaire de a et de b on a donc :
  $\boldsymbol{D/(au + bv)}$ **donc** $\boldsymbol{D/d}$ **ce qui veut dire que** $\boldsymbol{D}$ **est un diviseur de** $\boldsymbol{d}$ **donc** $\boldsymbol{D \leq d}$
- Montrons maintenant que d/a. Effectuons alors la division euclidienne de a par d, on a :
  $a = dq + r$ où $0 \leq r < d$.

Supposons que $r \neq 0$. Maintenant, on isole r et dans le même temps on remplace d par $au + bv$. On obtient donc :

$$r = a - (au + bv) \times q = a - auq - bvq = \boldsymbol{a(1 - uq) + b(-vq)}$$

En posant $1 - uq = M$ et $-vq = N$, nous venons de montrer ainsi que $r = Ma + Nb$. Donc $r \in E$. Or cela est **ABSURDE.** En effet nous savons que le plus petit élément de E est d or $r < d$. Donc on en déduit que la seule valeur possible pour r est $r = 0$. **Donc d divise a.**

En effectuant exactement la division euclidienne de b par d, on démontre exactement de la même manière que **d divise b.**

Ainsi d divise a et d divise b. Donc d est un diviseur commun de a et b. Or D est le plus grand des diviseurs communs, donc $d \leq D$.

Finalement, nous avons montré d'une part que $D \leq d$, d'autre part que $d \leq D$ donc il en résulte : $\boldsymbol{d = D}$. En d'autres termes :

$$\boldsymbol{au + bv = D}$$

2. Théorème de Bézout (équivalence)

Soient a et b deux entiers. Alors a et b sont premiers entre eux si et seulement s'il existe deux entiers u et v tels que :

$$\boldsymbol{au + bv = 1}$$

Remarque IMPORTANTE

Le théorème de Bézout est une équivalence, c'est-à-dire que la réciproque est vraie. Il faut donc démontrer le théorème dans les deux sens : « ⇒ » et « ⇐ »

Démonstration ROC (importance : haute)

- Dans le sens ⇒ :

Les nombres a et b sont deux entiers qui sont premiers entre eux. C'est-à-dire que $PGCD(a; b) = 1$. D'après l'égalité de Bézout il existe deux entiers u et v tels que $au + bv = 1$.

- Dans le sens ⇐ :

On suppose qu'il existe deux entiers tels que $au + bv = 1$. Notons alors D le $PGCD$ de a et de b, i.e $PCGD(a; b) = D$. Dès lors, D est le plus grand diviseur **commun** à a et à b. Donc D/a et D/b. Donc D divise **toute** combinaison linéaire de a et b. Ainsi : $D/(au + bv)$ donc $D/1$ donc $d = 1$.

3. Corollaire du théorème de Bézout (équivalence)

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

Démonstration (importance : haute)

- Dans le sens ⇒ :

L'équation $ax + by = c$ admet des solutions entières que l'on note $(x_0; y_0)$ on a donc $ax_0 + by_0 = c$.

Soit $D = PGCD(a; b)$. Ainsi D/a et D/b donc D divise toute combinaison linéaire de a et de b ainsi :

$D/(\ ax_0 + by_0)$. Donc D/c, en d'autres terme, c est un multiple de D.

- Dans le sens ⇐ :

D'une part, c est un multiple de $PGCD(a; b) = D$. Il existe donc il entier k tel que $c = Dk$.

D'autre part, d'après l'égalité de Bézout, il existe un couple $(u; v)$ tel que :

$$au + bv = D$$

En multipliant les deux membres de cette égalité par k, on obtient :

$$auk + bvk = Dk \Leftrightarrow a(uk) + b(vk) = c$$

On pose maintenant $x_0 = uk$ et $y_0 = vk$ on obtient finalement : $ax_0 + by_0 = c$.

IV. THEOREME DE GAUSS

Théorème (implication, réciproque fausse)

Soient a, b et c trois entiers non nuls. Si a divise bc et si a et b sont premiers entre eux alors a divise c.

Démonstration ROC (importance : très haute)

D'une part, a divise bc donc il existe un entier k tel que $bc = ka$.

D'autre part a et b sont premiers entre eux donc d'après le théorème de Bézout, il existe un couple $(u; v)$ tel que : $au + bv = 1$. En multipliant cette égalité par c, on a :

$auc + bvc = c$ on se souvient ici que $bc = ka$ d'où :
$a \times uc + a \times kv = c$ on factorise par a :

$$a(uc + kv) = c$$

Comme $uc + kv$ est un entier, on peut dire que a divise c.

Corollaire du théorème de Gauss

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

Démonstration ROC (importance : haute)

Nous savons que b et c divisent a. Ainsi, des entiers k et k' tels que $a = kb$ et $a = k'c$. Par transitivité :

$$kb = k'c$$

Donc $b/k'c$ et d'ailleurs b et c sont premiers entre eux donc d'après le théorème de Gauss, b divise k'. Il existe donc un entier k'' tel que $k' = bk''$. Cela nous permet d'écrire que :

$$\boldsymbol{a = k'c = bk''c = k''bc}$$

Donc bc divise a.