Grands théorèmes de l'arithmétique

I- PGCD , algorithme d'Euclide

1) PGCD : P*lus Grand Commun Diviseur*

Définition : Soient a et b deux entiers non nuls
L'ensemble des diviseurs communs à a et à b possède un plus grand élément noté PGCD(a,b)

Propriétés :
1) PGCD (a , b) = PGCD($|a|$, $|b|$)
2) PGCD(a,b) = $|b|$ $\Leftrightarrow$ b divise a
3) **Propriété d'homogénéité**
Soit k un entier naturel non nul. $\text{PGCD}(k\times a, k\times b) = k\times\text{PGCD}(a,b)$

Démonstration :

1) C'est une conséquence de la définition
2) Si b divise a alors b est un diviseur commun à a et b d'où comme $|b|$ est le plus grand diviseur positif de b on a PGCD(a,b) = $|b|$. Réciproquement, si PGCD(a,b) = $|b|$ alors $|b|$ divise a donc b divise a.
3) Soit d le PGCD de a et b et D le PGCD de ka et kb
Comme d divise a et b , kd divise ka et kb donc kd ≤ D
Comme k divise ka et kb, k divise D, il existe donc un entier n tel que D = kn
Comme D divise ka et kb, n divise a et b donc n ≤ d d'où kn ≤ kd cad D ≤ kd
Conclusion : D = kd

2) Calcul effectif du PGCD

Lemme d'Euclide Soient a et b deux entiers naturels non nuls Si a = bq+r alors PGCD (a , b) = PGCD (b , r)

Démonstration : Voir l'activité

Théorème (algorithme d'Euclide) :
L'itération du théorème précédent permet de trouver le PGCD de a et b comme le dernier reste non nul .

Démonstration : on a successivement PGCD(a,b)= PGCD(b, r_0) puis PGCD (b, r_0)=PGCD (r_0 , r_1) puis PGCD(r_0 , r_1) = PGCD(r_1 , r_2) etc... La suite (r_k) des restes est strictement décroissante (car un reste est strictement inférieur au diviseur) ; elle s'arrête donc. Notons r_{n-1} le dernier reste non nul. Par égalités successives, on a donc PGCD(a,b) = PGCD(b, r_0)= ... = PGCD(r_{n-2} , r_{n-1}) Or $r_{n-2}=qr_{n-1}+r_n = qr_{n-1}$ donc r_{n-1} divise r_{n-2}
Le PGCD recherché est donc r_{n-1} dernier reste non nul

3) Nombre premiers entre eux

Définition : Soit a et b deux entiers relatifs non nuls.
Les entiers a et b sont dits premiers entre eux si et seulement si $\text{PGCD}(a,b)=1$

Remarques

- En d'autres termes, deux entiers premiers entre eux n'admettent que deux diviseurs communs : 1 et -1
- Une conséquence de cette définition est une caractérisation des fractions irréductibles :
Soit a et b deux entiers relatifs non nuls.
La fraction $\frac{a}{b}$ est irréductible si et seulement si a et b sont premiers entre eux
- $\text{PGCD}(a,b)=d$ si et seulement si $\begin{cases} a=d\times a' \\ b=d\times b' \end{cases}$ avec a' et b' premiers entre eux

II- Grands théorèmes de l'arithmétique

1) Le Théorème de Bezout

a) Identité de Bezout

Identité de Bezout

a et b désignent deux entiers relatifs non nuls.

Si d = PGCD(a;b) alors il existe des entiers relatifs u et v tels que **au + bv = d**

Démonstration : voir livre p 144

Remarque :

- Le couple (u ; v) n'est pas unique
  Par exemple, pour $a=3$ et $b=2$, on obtient PGCD$(2;3)=1$ et $1\times 3-1\times 2=1$ ou encore $-1\times 3+2\times 2=1$
- **La réciproque est fausse**
  Pour a = 4 et b = 5 , on a $3\times 4-2\times 5=2$ et pourtant PGCD(4;5) ≠ 2

b) Conséquences de l'identité de Bezout

Conséquence 1 : L'ensemble des diviseurs de deux entiers a et b est l'ensemble des diviseurs de leur PGCD

Démonstration : C'est une conséquence de l'identité de Bezout. Soit D = PGCD(a,b)

- Soit d un diviseur de D alors comme D divise a et b alors d divise a et b
- D = PGCD(a,b) donc d'après l'identité de Bezout il existe u et v tels que $au+bv=$D d'où si d est un diviseurs de a et b alors d divise au+bv c'est à dire d divise D

Conséquence 2 : Le Théorème de Bezout

Soient a et b deux entiers relatifs

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

- Si a et b sont premiers entre eux, PGCD(a;b) = 1 et l'identité de Bezout permet de dire qu'il existe deux entiers relatifs u et v tels que au + bv = 1
- Réciproquement, s'il existe des entiers relatifs u et v tels que au + bv = 1, tout diviseur commun à a et b divise au et bv donc divise au + bv c'est à dire 1 donc PGCD(a;b) est un entier positif qui divise 1 d'où PGCD(a;b) = 1 et a et b sont premiers entre eux.

Remarque : Un théorème qui permet de montrer facilement que deux entiers sont premiers entre eux
Par exemple, pour tout entier naturel n non nul, n et 2n+1 sont premiers entre eux car $(2n+1)\times 1 - n\times 2 = 1$

Conséquence 3 : Existence de solutions à une équation diophantienne

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

L'équation diophantienne $ax+by=c$ où les inconnues x et y sont des entiers relatifs admet des solutions si et seulement si c est un multiple du PGCD de a et b

Remarque : Diophante d'Alexandrie est un mathématicien grec du III^{ème} siècle qui fut le premier à s'intéresser à ce genre d 'équation

Exemple : $2x+3y=7$ est une équation diophantienne

Démonstration

- Supposons que l'équation admette une solution $(x_0;y_0)$. On a donc $ax_0+by_0=c$.
  Si on note d le $PGCD(a;b)$ alors d divise a et divise b donc toute combinaison linéaire de a et b en particulier ax_0+by_0 c'est à dire c
- réciproquement, soit d le $PGCD(a;b)$. Comme c divise d, il existe un entier k tel que c=kd.
  L'identité de Bezout permet aussi d'écrire qu'il existe deux entiers u et v tels que au+bv = d d'où en multipliant cette égalité par k il vient : $kau+kbv=kd$ c'est à dire a(ku)+b(kv)=c et on a ainsi trouvé un couple solution à notre équation : le couple $(x;y)=(ku;kv)$

2) Le théorème de Gauss

a) Le théorème

Théorème de Gauss

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

Si **a divise le produit bc** et si **a est premier avec b** alors **a divise c**

Démonstration : a est premier avec b donc d'après le théorème de Bezout, il existe deux entiers relatifs u et v tels que $au+bv=1$. En multipliant par $c\neq 0$, on obtient : $acu+bcv=c$ d'où comme par hypothèse, a divise bc, a divise acu+bcv cad a divise c

b) Conséquences

Propriété: a , b et c désignent trois entiers relatifs non nuls

Si **b et c sont premiers entre eux et divisent a** alors **bc divise a**

Démonstration

- b divise a donc il existe un entier relatif d tel que a = db
- c divise a donc il existe un entier relatif d' tel que a = d'c. On a donc a = db = d'c
  c divise donc db or c et b sont premiers entre eux donc d'après le théorème de Gauss, c divise d et il existe un entier relatif d'' tel que d = d''c
  a = db devient donc a = d''cb et bc divise a

Exemple : Le nombre 1 573 875 est divisible par 5 puisqu'il se termine par 5 et il est divisible par 9 car la somme de ses chiffres est divisible par 9. Or 5 et 9 sont premiers entre eux donc 1 573 875 est divisible par 9×5 cad 45

c) Une application : Résolution d'une équation diophantienne $ax+by=c$

Deux exemples pour comprendre

Exemple 1 : Résoudre l'équation diophantienne (E) : $17x-33y=1$

1) Cette équation admet une solution particulière évidente le couple (2;1). En effet, $17\times 2-33\times 1=1$

2) On a donc $\begin{cases} 17x-33y=1 \\ 17\times 2-33\times 1=1 \end{cases}$.

Par soustraction il vient : $17(x-2)-33(y-1)=0$ c'est à dire $17(x-2)=33(y-1)$ (E')

3) 17 divise donc $33(y-1)$ or 17 et 33 sont premiers entre eux donc **d'après le théorème de Gauss,** 17 divise $y-1$ et on a donc $y=1+17k$. En remplaçant dans (E'), on obtient alors $x=2+33k$

Les couples solutions sont donc de la forme $\begin{cases} x=2+33k \\ y=1+17k \end{cases}$ avec $k\in\mathbb{Z}$.

4) On vérifie alors que ce couple convient (car la raisonnement précédent ne se fait pas par équivalence) :
$17x-33y=17(2+33k)-33(1+17k)=34+17\times 33k-33-33\times 17k=1$

Exemple 2 : Résoudre l'équation diophantienne (E) $15x+8y=5$

1) 15 et 8 sont premiers entre eux donc cette équation admet des solutions

2) On peut alors rechercher une solution particulière à l'équation $15x+8y=1$ **(souvent plus simple à trouver)**
Cette équation admet une solution particulière évidente le couple (-1;2).
En effet, $15\times(-1)+8\times2=-15+16=1$.
Il ne reste alors qu'à multiplier par 5 pour obtenir une solution à l'équation (E) : le couple (-5;10)

3) On a donc $\begin{cases} 15x+8y=5 \\ 15\times(-5)+8\times10=5 \end{cases}$

Par soustraction il vient : $15(x+5)+8(y-10)=0$ c'est à dire $15(x+5)=8(10-y)$ (E')

3) 15 divise donc $8(10-y)$ or 15 et 8 sont premiers entre eux donc **d'après le théorème de Gauss**, 15 divise $10-y$ et on a donc $y=10-15k$. En remplaçant dans (E') , on obtient alors $x=-5+8k$

Les couples solutions sont donc de la forme $\begin{cases} x=-5+8k \\ y=10-15k \end{cases}$ avec $k \in \mathbb{Z}$.

4) On vérifie alors que ce couple convient (car le raisonnement précédent ne se fait pas par équivalence) :
$15x+8y=15(-5+8k)+8(10-15k)=-75+15\times8k+80-8\times15k=5$

Conclusion

- On cherche une solution particulière à l'équation
- On recherche ensuite l'ensemble des solutions en soustrayant termes à termes l'équation et l'égalité de la solution particulière
- On applique **le théorème de Gauss** puis on vérifie que les solutions trouvées vérifient bien l'équation