PGCD et applications

1) Plus grand commun diviseur

Définition 1

Parmi les diviseurs communs de deux entiers a et b (ceux qui divisent à la fois a et b), le plus grand est appelé $pgcd(a;b)$

Propriété 2 (pgcd et division euclidienne)

Soit $a = bq + r$ la division euclidienne de a par b.
Alors $pgcd(a;b) = pgcd(b;r)$

La propriété précédente permet de déterminer le pgcd de deux nombres en effectuant des divisions euclidiennes successives :

Méthode 3 (Algorithme d'Euclide)

On considère deux entiers naturels $a \geq b$, et on définit la suite (r_n) par :

- $r_0 = b$
- r_1 est le reste de la division euclidienne de a par b
- pour $n \geq 1$,
  - Si $r_n = 0$, alors $r_{n+1} = 0$
  - Si $r_n \neq 0$, alors r_{n+1} est le reste de la division euclidienne de r_{n-1} par r_n.

Alors il existe un rang p au-delà duquel tous les termes de la suite (r_n) sont nuls, et on a $pgcd(a;b) = r_p$.

Savoir-Faire :

Déterminer le pgcd de 36 et 128.

Propriété 4 (simplifications de calculs)

Pour tous a, b, k entiers, on a :

$$pgcd(ka;kb) = k \times pgcd(a;b)$$

2) Entiers premiers entre eux

Propriété 5

Lorsque le pgcd de deux nombres vaut 1, on dit qu'ils sont premiers entre eux.
Ils n'ont alors aucun diviseur commun autre que 1

Remarque :

Si a et b sont premiers entre eux, alors la fraction $\frac{a}{b}$ est irréductible.

3) Théorème de Bézout

Propriété 6 (Combinaison linéaire et pgcd)

Soit g le pgcd de eux entiers a et b.
Alors il existe deux entiers u et v tels que $au + bv = g$.

Propriété 7 (théorème de Bézout)

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

Remarque :

Attention, la première propriété est une équivalence et la seconde est une implication ;
Par exemple, $3 \times 4 + 5 \times 8 = 52$ alors que 52 n'est pas le pgcd de 3 et 5

4) Théorème de Gauss

Propriété 8

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

Savoir-Faire : (*Équation $au = bv$*)

Résoudre dans $\mathbb{Z}^2$ l'équation ***(E)*** $34u = 22v$

5) Démonstration(s)

- « Si g divise a et b, alors il divise tout combinaison linéaire de a et b (du type $au + bv$ avec u et v deux entiers relatifs) »

  g divise a donc il existe un entier k tel que $a = kg$;

  g divise b donc il existe un entier k' tel que $b = k'g$;

  $$au + bv = kgu + k'gv = (ku + k'v)g$$

  donc g divise $au + bv$.

- « Les diviseurs communs à deux nombres sont les diviseurs de leur *pgcd*. »

  D'après la démonstration précédente, on peut conclure dans l'algorithme d'Euclide, que $\mathscr{D}(a;b) = \mathscr{D}(r_n;0) = \mathscr{D}(r_n)$, où r_n est le dernier reste non nul de l'algorithme, c'est-à-dire $r_n = pgcd(a;b)$.

  D'où le résultat $\mathscr{D}(a;b) = \mathscr{D}(pgcd(a;b))$.

- « $pgcd(ka;kb) = k \times pgcd(a;b)$ »

  Soit $g = pgcd(a;b)$ et $G = pgcd(ka;kb)$. On souhaite montrer que $G = kg$.

  g divise a et b, donc kg divise ka et kb, donc kg divise G (cf démonstration précédente).

  Donc il existe un entier l tel que $G = lkg$

  lkg divise ka et kb donc lg divise a et b, donc lg divise g.

  Donc $lg \leq g$, soit $l \leq 1$, c'est-à-dire $l = 1$.

  Donc $G = kg$, ce qui prouve le résultat.

Propriété 6 (Combinaison linéaire et pgcd)

Soit g le pgcd de eux entiers a et b.
Alors il existe deux entiers u et v tels que $au + bv = g$.

On va considérer l'ensemble des combinaisons linéaires non nulles de a et b ($E = \{am + bn, m \in \mathbb{Z}, n \in \mathbb{Z}\}$, et leur plus petit élément d, qui s'écrit $d = au + bv$.

Puis, on va montrer que $d = pgcd(a; b)$ en montrant successivement que $d \leq pgcd(a; b)$ puis $pgcd(a; b) \leq d$.

- Montrons que $pgcd(a; b) \leq d$:

  Comme le $pgcd(a; b)$ divise a et b, il divise toute combinaison linéaire de a et b, donc il divise en particulier d, ce qui prouve que $pgcd(a; b) \leq d$.

- Montrons que $d \leq pgcd(a; b)$:

  La division euclidienne de a par d donne deux nombres entiers q et $0 \leq r < d$ tels que $a = dq + r$.

  On va prouver que r vaut 0, et donc que d divise a :

  On a

  $$r = a - dq = a - (au + bv) = a(1 - u) + b(-v),$$

  Donc r est une combinaison linéaire de a et b, donc soit r est nul, soit r appartient à E.

  Or, comme $r < d$ et que d est le plus petit élément de E, alors r ne peut appartenir à E et donc on a $r = 0$.

  Donc $a = dq$, et d divise a.

  On montre de la même manière que d divise b, et on en déduit que d divise $pgcd(a; b)$.

  Ce qui prouve que $d \leq pgcd(a; b)$

Les deux résultats prouvent que $d = pgcd(a; b)$ et qu'il existe une combinaison linéaire $au + bv$ égale au $pgcd(a; b)$.

Propriété 8 (Théorème de Gauss)

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

On appliquera le théorème de Bézout pour prouver le théorème de Gauss.

a divise bc donc il existe un entier k tel que $bc = ka$.

Puisque a et b sont premiers entre eux, alors il existe, d'après le théorème de Bézout, deux entiers u et v tels que $au + bv = 1$.

En multipliant toute l'égalité par c, on obtient $auc + bvc = c$ et en remplaçant bc parka, on obtient : $auc + kav = c$, soit $a(uc + kv) = c$, ce qui prouve que a divise c.

6) Algorithme

Coefficients de Bézout (Python et traduction en français)

```
a=int(input("a= ?"))
b=int(input("b= ?"))
r0=a
r1=b
u0=1
u1=0
v0=0
v1=1
u=0
v=0
while r1!=0 :
    q=r0//r1
    r=r0
    u=u0-u1*(r0//r1)
    v=v0-v1*(r0//r1)
    print(u,v)
    r0=r1
    r1=r
    u0=u1
    u1=u
    v0=v1
    v1=v
print("résultat : ",a, " x ", u0,
" + ",b, " x ",v0, " = 1")
```

Saisir a
Saisir b
r_0 prend la valeur a
r_1 prend la valeur b
u_0 prend la valeur 1
u_1 prend la valeur 0
v_0 prend la valeur 0
v_1 prend la valeur 1
u prend la valeur 0
v prend la valeur 0
Tant que $r_1 \neq 0$, Faire :
    q est le quotient de la division de r_0 par r_1
    r est le reste de la division de r_0 par r_1
    u prend la valeur $u_0 - u_1 \times q$
    v prend la valeur $v_0 - v_1 \times q$
    Afficher u et v
    r_0 prend la valeur r_1
    r_1 prend la valeur r
    u_0 prend la valeur u_1
    u_1 prend la valeur u
    v_0 prend la valeur v_1
    v_1 prend la valeur v
Afficher : "résultat : $a \times u_0 + b \times v_0 = 1$"