1 PGCD

A retenir

Lemme d'Euclide :
Soient a , b , q et r des entiers naturels non nuls tels que $a = bq + r$ avec $0 \leq r < b$.
Alors $PGCD(a; b) = PGCD(b; r)$

Le principe

On procède en deux temps : on va montrer par une double inclusion que l'ensemble des diviseurs communs de a et b est égal à l'ensemble des diviseurs communs de b et r.

La démonstration

- Posons les notations : On a donc $a = bq + r$.
  Soit D l'ensemble des diviseurs communs de a et b .
  Soit D' l'ensemble des diviseurs communs de b et r .
- Montrons que $D \subset D'$
  - Soit $d \in D$ alors d est un diviseur commun de a et b .
  - Par définition si d divise a et b alors d divise $a - bq = r$
  - Donc d divise à la fois r et b et donc $d \in D'$
  - Conclusion : $D \subset D'$
- Montrons que $D' \subset D$
  - Soit $d' \in D'$ alors d' est un diviseur commun de b et r .
  - Par définition , si d' divise b et r alors **d' divise** $bq + r = a$
  - d' est donc **un diviseur commun de a et b et** $d' \in D$
  - Conclusion : $D' \subset D$
- On a donc $D \subset D'$ **et** $D' \subset D$ **donc** $D = D'$

Astuce

1. Pour montrer que deux ensembles A et B sont égaux , on montre $A \subset B$ et $B \subset A$
2. Pour montrer que deux ensembles A et B sont tels que $A \subset B$, on prend un élément a de A et on montre que a appartient à B .

A retenir

1. $PGCD(a;b) = b \iff$ b divise a
2. Tout diviseur commun à a et b divise PGCD(a;b)
3. Soit k entier naturel , $PGCD(ka;kb) = kPGCD(a;b)$
4. Deux entiers a et b sont premiers entre eux si et seulement si $PGCD(a;b) = 1$
5. Un nombre premier est premier avec tous les entiers qu'il ne divise pas

Le principe

Pour la première , on applique les définitions . La deuxième et la troisième sont des conséquences d'Euclide . Les deux dernières utilisent les définitions .

Les démonstrations

1. On démontre la propriété en deux temps
   - Si $b = PGCD(a;b)$ alors par définition , b divise a .
   - Supposons que b divise a . Alors b est un diviseur commun de a et b et il est le plus grand diviseur possible de b . Donc par définition $PGCD(a;b) = b$
2. Soit d un diviseur commun de a et b .Par l'algorithme d'Euclide , d divise les restes successifs des divisions euclidiennes et donc également le dernier reste non nul qui est le PGCD de a et b .
3. On pose : $a = bq + r$. On applique l'algorithme d'Euclide en notant r_n le dernier reste non nul . Mais on peut écrire aussi $ka = kbq + kr$ et en appliquant l'algorithme d'Euclide , le dernier reste non nul ici sera kr_n . Par définition du PGCD , on a donc bien $PGCD(ka;kb) = kPGCD(a;b)$
4. On démontre en deux temps :
   - Si a et b sont premiers entre eux , leur seul diviseur commun est 1 donc $PGCD(a;b) = 1$
   - Si $PGCD(a;b) = 1$ alors le plus grand diviseur commun de a et b est 1 donc le seul diviseur commun est 1 . Et donc a et b sont premiers entre eux .
5. Soit p un nombre premier . Soit a un entier non multiple de p . Posons $d = PGCD(a;p)$
   Puisque p est premier , les diviseurs de p sont **1 et p** .
   Donc soit $d = 1$ **, soit** $d = p$
   Supposons que $d = p$. Alors par définition **p divise a . Contradiction . Donc** $d = 1$ **et a et p sont premiers entre eux**

A retenir

Soit $PGCD(a;b) = d$ alors il existe a' et b' deux entiers premiers entre eux tels que : $a = da'$ et $b = db'$

Le principe

On applique simplement les définitions

La démonstration

Soit $d = PGCD(a;b)$ alors d divise a et b donc **il existe a' et b' entiers tels que** $a = da'$ **et** $b = db'$
Montrons maintenant que a' et b' sont premiers entre eux :
$PGCD(a;b) = d \iff PGCD(da';db') = d \iff dPGCD(a';b') = d \iff PGCD(a';b') = 1$ **donc a' et b' sont bien premiers entre eux .**

2 Bézout

A retenir

Théorème de Bézout :
a et b sont premiers entre eux si et seulement s'il existe u et v entiers relatifs tels que $au + bv = 1$

Le principe

On doit montrer une double implication . On va utiliser l'ensemble des entiers qui s'écrivent $au + bv$ et montrer que 1 est dans cet ensemble si a et b sont premiers entre eux .

La démonstration

- Montrons que si $au + bv = 1$ alors a et b sont premiers entre eux .
  Soit $d = PGCD(a;b)$ alors d divise $au + bv = 1$ donc $d = 1$ et a et b premiers entre eux

- Montrons maintenant que si a et b premiers entre eux , alors il existe u et v tels que $au + bv = 1$

  - Soit $E = \{au + bv, (u;v) \in \mathbb{Z}^2\}$. On va montrer que 1 est dans E .

  - $a = a \times 1 + b \times 0$ et $-a = a \times -1 + b \times 0$ donc E n'est pas vide et contient au moins un élément positif . On note d le plus petit élément positif de E . On peut écrire : $d = au_0 + bv_0$.

– On applique la division euclidienne de a par d , alors il existe q et r tels que $a = dq + r$ avec $0 \leq r < d$.
Donc $r = a - dq = a - (au_0 + bv_0)q = a(1 - u_0q) + b(-v_0q)$ et donc $r \in E$.

– Mais d est le plus petit élément de E et r lui est strictement inférieur donc $r = 0$. Donc d divise a .

– On démontre de la même façon que d divise b . Donc d divise PGCD(a;b) et puisque a et b sont premiers entre eux , alors $d = 1$

– On a donc : $1 = d = au_0 + bv_0$

A retenir

1. Si $d = PGCD(a; b)$ alors il existe des entiers relatifs u et v tels que $au + bv = d$
2. Une équation de la forme $ax + by = m$ avec a , b , x , y et m entiers admet des solutions si et seulement si m est un multiple de PGCD(a;b)
3. Si un nombre est premier avec deux entiers , il est premier avec leur produit .

Le principe

Ce sont des conséquences du théorème de Bézout .

Les démonstrations

1. Si $d = PGCD(a; b)$ alors il existe des entiers relatifs a' et b' premiers entre eux tels que $a = da'$ et $b = db'$. Par Bézout , on a donc : **il existe u et v tels que** $a'u + b'v = 1 \iff da'u + db'v = d \iff au + bv = d$

2. Démontrons le en deux temps :

   - Supposons m est un multiple de $d = PGCD(a; b)$ donc il existe **k entier tel que** $m = kd$ et par la propriété précédente , **il existe u et v tels que** $au + bv = d \iff aku + bkv = kd = m$ **et le couple** $(ku; kv)$ **est donc solution**
   - Supposons maintenant que l'équation $au + bv = m$ admet au moins une solution , le couple (u;v) . Notons $d = PGCD(a; b)$. Alors il existe a' et b' premiers entre eux tels que $da'u + db'v = m \iff d(a'u + b'v) = m$ **donc d divise m**

3. Supposons a et b premiers entre eux , alors par Bézout , **il existe u et v tels que** $au + bv = 1$
   Supposons a et c premiers entre eux , alors par Bézout **il existe u' et v' tels que** $au' + cv' = 1$
   On a donc : $(au + bv)(au' + cv') = 1 \iff a(auu' + bvu' + ucv') + bc(vv') = 1$ **et donc par Bézout , a et** bc **sont premiers entre eux .**

3 Gauss

A retenir

Théorème de Gauss :
Si a est premier avec b et a divise bc alors a divise c .

Le principe

On utilise Bézout .

La démonstration

Supposons que a divise bc . Puisque a et b sont premiers entre eux , par le théorème de Bézout , il existe u et v entiers tels que $au + bv = 1$.
On a donc : $auc + bvc = c$.
Or , a divise auc **et a divise** bcv **donc a divise** $auc + bvc = c$

A retenir

1. Soient a et b premiers entre eux . Si a divise n et b divise n , alors ab divise n .
2. Si p premier divise ab alors p divise a ou p divise b .

Le principe

Ce sont des conséquences de Gauss .

La démonstration

1. Si a divise n alors **il existe k entier tel que** $n = ka$
   Si b divise n alors **il existe k' entier tel que** $n = k'b$
   On a donc $k'b = ka$ donc a divise $k'b$. Mais a et b sont premiers entre eux , donc **d'après Gauss , a divise k'** . Donc il existe p tel que $k' = pa$ et donc $n = pab$ et ab divise n .

2. Supposons p divise ab , on a donc deux cas :
   - Soit p divise a et la propriété est démontrée .
   - Soit p ne divise pas a . Alors puisque p est premier , il est premier avec a et donc par Gauss , p divise b .