

Soit a et b deux entiers naturels non nuls de l'ensemble $E = \{ax - by \text{ avec } x \text{ et } y \text{ appartenant à } \mathbb{Z}\}$. On pose $E^+ = E \cap \mathbb{N}^*$

E^+ est donc l'ensemble des entiers naturels non nuls de la forme $ax - by$ avec x et y appartenant à $\mathbb{Z}$.

1. Démontrer que E^+ est non vide, en déduire qu'il admet un plus petit élément noté d , ainsi il existe deux entiers relatifs x_0 et y_0 tel que : $d = ax_0 - by_0$.
2. Démontrer que tout multiple de d est un élément de E
3. Soit n un élément de E et r le reste de la division euclidienne de n par d . Démontrer que r est, comme n , un élément de E . L'entier n peut-il appartenir à E^+ ? En déduire que $r = 0$ et que n est multiple de d
4. En déduire que E est l'ensemble des multiples de d (noté $d\mathbb{Z}$)
5. Démontrer que a et b appartiennent à E . En déduire que d est un diviseur commun de a et b
6. Démontrer que si d' est un diviseur commun positif de a et b alors d' divise d et par suite $d' \leq d$
(Indication : $d = ax_0 - by_0$)
7. Qu'en déduit-on sur d ?

CORRECTION

1. Si $a > 0$ et $x = 1$ et $y = 0$ alors $ax - by = a$ donc $a \in E^+$, E^+ est non vide.
Si $a < 0$ et $x = -1$ et $y = 0$ alors $ax - by = -a$ donc $-a \in E^+$, E^+ est non vide.
 E^+ est un ensemble non vide d'entiers naturels donc admet un plus petit élément strictement positif d , $d \leq |a|$
Il existe donc deux entiers relatifs x_0 et y_0 tel que : $d = ax_0 - by_0$.
2. Soit n un multiple de d , il existe donc un entier relatif p tel que $n = dp$ donc $dp = p(ax_0 - by_0)$ soit $n = a(px_0) - b(py_0)$
 $n = a(px_0) - b(py_0)$ avec (px_0) et (py_0) entiers relatifs donc $n \in E$. Tout multiple de d est un élément de E
3. Dans la division euclidienne de n par d , il existe deux entiers r et q tels que $n = dq + r$ avec $0 \leq r < d$
 $n \in E$ donc il existe u et v entiers relatifs tels que $n = au - bv$ or $d = ax_0 - by_0$ donc $r = au - bv - (ax_0 - by_0)$
 $r = a(u - x_0) - b(v - y_0)$ donc $r \in E$, $0 \leq r$ donc $r \in E^+$
 $r < d$ or d est le plus petit élément non nul de E^+ donc $r = 0$, donc $n = dq$, n est un multiple de d .
4. E contient tous les multiples de d (question 2) et tout élément de E est un multiple de d (question 3) donc E est l'ensemble des multiples de d .
5. Si $x = 1$ et $y = 0$ alors $ax - by = a$ donc $a \in E$ or donc E est l'ensemble des multiples de d donc a est donc un multiple de d
de même : si $x = 0$ et $y = -1$ alors $ax - by = b$ donc $b \in E$ donc b est donc un multiple de d
 d divise a et d divise b donc d est un diviseur commun de a et b
6. Si d' est un diviseur commun positif de a et b alors d' divise $ax_0 - by_0$, or $d = ax_0 - by_0$ donc d' divise d
 d est un entier strictement positif et d' divise d donc $d' \leq d$.
7. d est un diviseur commun de a et b donc d divise $\text{PGCD}(a; b)$
Tout diviseur commun positif de a et b divise d en particulier $\text{PGCD}(a; b)$ divise d
 d est un entier strictement positif et d divise $\text{PGCD}(a; b)$ et $\text{PGCD}(a; b)$ divise d donc $d = \text{PGCD}(a; b)$

Théorème de Bézout Brachet

Si a et b sont deux entiers naturels non nuls, si $d = \text{PGCD}(a; b)$ alors il existe deux entiers relatifs x_0 et y_0 tels que $d = ax_0 - by_0$.