Arithmetique | CM: 5

Par Lorenzo

04 octobre 2024

1 Arithmétique avancée dans $\mathbb{Z}$

1.1 Bézout, Gauss

Proposition 1.1 (Bézout)**.**

Soient $a, b \in \mathbb{Z}^*$. Il existe $u, v \in \mathbb{Z}$ tels que
$au + bv = PGCD(a, b)$

Méthode 1.1.

Pour trouver une relation de Bezout, il suffit de remonter l'algorithme d'Euclide. Que l'on appelle ***l'algorithme d'Euclide étendu****.*

1. *Faire l'algorithme d'Euclide*

2. *Réecrire le reste avec les autres valeurs*

Lemme 1.1. *Les sous-groupes de $\mathbb{Z}$ sont les $n\mathbb{Z} := \{nk \mid k \in \mathbb{Z}\}$ avec $n \in \mathbb{Z}$*

Démonstration 1.1.

- *$n\mathbb{Z}$ sous groupe de $(\mathbb{Z}, +)$ (cf TD1)*
- *Soit H un sous groupe de $(\mathbb{Z}, +)$ alors $0 \in H$*
  - *Si $H = \{0\}$ alors $H = 0\mathbb{Z}$*
  - *Sinon il existe un x non nuls dans H, alors $(-x) \in H$ "A completer"*

□

Corollaire 1.1. *Soient $a, b \in \mathbb{Z}$ alors $a\mathbb{Z} + b\mathbb{Z} = \{au + bv | u, v \in \mathbb{Z}\} = \delta\mathbb{Z}$ où $\delta =$* PGCD(a, b)

Démonstration 1.2.

Soient $u, v \in \mathbb{Z}$ et $c = au + bv$. Comme δa et δb alors δc.

Réciproquement, soit $c \in \delta\mathbb{Z}$, il existe un c' dans $\mathbb{Z}$ tel que $c = \delta c'$. Par Bézout, il existe $u', v' \in \mathbb{Z}$ tels que $au' + bv' = \delta$, en multipliant par c' on a $au'c' + bv'c' = \delta c' = c$. Il suffit alors de poser $u = u'c'$ et $v = v'c'$.

On dit alors que le sous groupe ***engendré par*** *a et b coïncide avec le sous groupe engendré par leurs PGCD.*

$\square$

Proposition 1.2 (Gauss)**.**

Soient $n, a, b \in \mathbb{Z}^*$ *tels que* $n|ab$ *et* $\mathrm{PGCD}(n, a) = 1$. *Alors* $n|b$.

Démonstration 1.3.

Par Bezout, il existe u *et* v *tels que* $nu + av = 1$. *Donc* $nub + abv = b$. *De* $ab = nk$ *(pour un* $k \in \mathbb{Z}$*), on déduit* $n(ub + kv) = b$. *Donc* $n|b$.

$\square$

1.2 Unicité de la décomposition en facteurs premiers

Lemme 1.2.

1. *Soient* $a, b, c \in \mathbb{Z}^*$

$$\left.\begin{array}{l}\mathrm{PGCD}(c, a) = 1 \\ \mathrm{PGCD}(c, b) = 1\end{array}\right\} \implies \mathrm{PGCD}(c, ab) = 1$$

2. *Soient* p *un nombre premier et* $a, b \in \mathbb{Z}^*$
   (a) *On a* $\mathrm{PGCD(a, p)} = 1$ *ou* $p|a$
   (b) *On a* $[p|ab \implies (p|aoup|b)]$

Démonstration 1.4.

À faire

$\square$

Proposition 1.3.

Une décomposition en facteurs premier est unique à l'ordre des facteurs près.

Démonstration 1.5.

À faire

$\square$

1.3 Résolution des équations diophantiennes

Soient $a, b \in \mathbb{Z}^*$ et $c \in \mathbb{Z}$.

On cherche à résoudre l'équation suivante d'inconnues entères u, v

$$au + bv = c$$

Méthode 1.2.

1. *Posant* $\delta = \mathrm{PGCD(a, b)}$*, on a* $a = \delta a'$, $b = \delta b'$ *et* $c = \delta c'$ *avec* $a', b', c' \in \mathbb{Z}$ *on a donc*

$$a'u + b'v = c'$$

   Soit $d = \mathrm{PGCD(a', b')}$ *alors* $d\delta$ *est un diviseur commun à* $a = \delta a'$ *et* $b = \delta b'$*. Par maximalité du diviseur commun* δ*, on a* $d = 1$*. Donc a' et b' sont premier entre eux.*

2. *Bézout nous fournit une solution à l'équation* $a'u + b'v = 1$*, qu'il suffit de multiplier par c' pour avoir une solution particulière* (u_0, v_0)*.*

3. *Soit* $(u, v) \in \mathbb{Z}^2$ *une solution.* $a'u + b'v = c'$ *et* $a'u_0 + b'v_0 = c'$ *donc* $a'(u - u_0) + b'(v - v_0) = 0$*. On a* $\mathrm{PGCD(a', b')} = 1$ *donc, d'après Gauss,* $a'|(v - v_0)$*. Donc* $\exists k \in \mathbb{Z}$ *tel que* $v - v_0 = ka' \implies v = v_0 + ka'$ *donc* $u = u_0 - b'k$*.*

4. *L'ensemble des solutions est donc contenu dans* $\{u_0 - b'k, v_0 + a'k \mid k \in \mathbb{Z}\}$