Arithmetique — CM: 4

Par Lorenzo

27 septembre 2024

0.1 Arithmétique élémentaire dans $\mathbb{Z}$

Définition 0.1. *Soient x et y dans $\mathbb{Z}$. On dit que x divise y s'il existe $k \in \mathbb{Z}$ tel que $y = kx$. La notation associée est $x \mid y$. x est un diviseur de y ou y est un multiple de x*

Remarques 0.1. *tout entier relatif divise 0.*
0 divise uniquement 0.
si x est un diviseur de y alors (-x) est un diviseur de y
1 et -1 sont les diviseurs de tout entier relatifs.
les diviseurs de 1 et -1 sont 1 et -1
$\forall x, y \in \mathbb{N}^* \implies (x \mid y \implies x \leq y)$

Définition 0.2. *On dit que $p \in \mathbb{N},\ p \geq 2$ est un nombre premier si les seuls diviseurs positifs de p sont 1 et p.*

Remarques 0.2. *Une autre définition est tout nombre qui a exactement 2 diviseurs.*

Remarques 0.3. *Pour vérifier qu'un nombre est premier, on peut regarde pour chaque $\forall k \in \mathbb{N}, k \leq \sqrt{p}$ si k divise p.*

Définition 0.3. *Soit $n \in \mathbb{Z}^*$, on appelle décomposition en facteurs premiers de n une écriture de la forme*
$n = cmultip_i = c(p_1 \times ... \times p_k)$
où $c \in +-1, k \in \mathbb{N}, p_1, ..., p_k$ sont premiers

Proposition 0.1.

Tout $n \in \mathbb{Z}^*$ admet une décomposition en facteurs premier.

Démonstration 0.1.

Il suffit de le démontrer pour $n \in \mathbb{N}^*$ et $c = 1$ et pour les négatifs on se ramène à $\mathbb{N}^*$ en posant $c = -1$

Démonstration par récurrence forte.

Initialisation: *$n = 1$, on pose $c = 1, k = 0$, c'est un produit vide.*

Initialisation: *Soit $n \in \mathbb{N}^*, \forall d \leq n$, on ait une telle décomposition. Si n + 1 est premier, on pose $k = 1 \quad P_1 = n + 1$. Si n + 1 n'est pas premier il admet un diviseur $d \in [2, n]$. Par hypothèse de récurrence $d = c \times p_1 \times ... \times p_k$. De même $d' = \dfrac{n+1}{d} \in [2; n]$ $d' = p'_1 \times ... \times p'_k$.*

Donc $n + 1 = d \times d' = p_1 \times ... \times p_k \times p'_1 \times ... \times p'_k$

$\square$

Corollaire: Tout entier $n \geq 2$ admet au moins un diviseur premier

Proposition 0.2.

L'ensemble des nombre premiers est infini.

Démonstration 0.2.

Supposons (par l'absurde) qu'il y ait un nombre fini de nombres premiers $p_1, ..., p_m$
On pose $N = p_1 \times ... \times p_m + 1$
Alors N admet un diviseur premier $p_i(i \in [i; m])$ *i.e.* $N = p_i N' \implies N = multip_j + 1 \implies p_i N' - p_i multi_{i \neg j} p_j = 1 \implies p_i(N' - multi_{j \neg i} p_j) = 1$

$\square$

Théorème 0.1. *Soient* $a \in \mathbb{Z}, b \in \mathbb{N}*$.
Alors il existe un unique couple $(q, r) \in \mathbb{Z} \times \mathbb{N}, a = bq + r$ *avec* $b > r \geq 0$

Démonstration 0.3.

Existence: *Pour* $a \in \mathbb{N}$*, raisonnement par récurrence.*
Initialisation: $a = 0$*: On pose* $q = 0$ *et* $r = 0 \implies 0 = b \times 0 + 0$
Hérédité: *Si* $a = bq + r$ *avec* $(b > r \geq 0)$
Alors $a+1 = bq+(r+1)$*, C'est une division euclidienne lorsque* $r+1 < b \implies r < l-1$
Lorsque $r = b - 1$
$a + 1 = bq + ((b - 1) + 1) = bq + b = b(q + 1) + 0$*, C'est une division euclidienne.*
Si $a < 0$ *alors* $(-a) > 0$ *Donc* $\exists(q, r) \in \mathbb{Z} \times \mathbb{N}, -a = bq + r \implies a = b \times (-q) + (-r)$ *avec* $(b > r \geq 0)$
Si r = 0, c'est une division euclidienne.
Sinon $-b < -r < 0 \implies 0 < -r + b < b$
Donc $a = b \times (-q) + (-r+b) - b = b \times (-q-1) + (-r+b)$ *C'est un division euclidienne.*
Unicité: *Si* $a = bq + r$ *et* $a = bq' + r'$ *avec* $b > r, r' \geq 0$
Par soustraction: $0 = b(q - q') + r - r' \implies r' - r = b(q - q')$
$b - 1 \geq r' - r \geq -b - 1$ *Donc* $r' - r = 0 \implies r = r'$
Ainsi $bq + r = bq' + r' \implies bq = bq' \implies q = q'$

$\square$

Définition 0.4. *le **pgcd** de deux nombres* $a, b \in \mathbb{Z}^*$ *est le plus grand diviseur commun à a et b. Il est noté* $PGCD(a, b)$ *(ou encore* $a \wedge b$*)*
*On dit que a et b sont **premiers entre eux** si PGCD(a, b) = 1.*
*Le **ppcm** de deux nombres* $a, b \in \mathbb{Z}^*$ *est le plus petit multiple strictement positif commun à a et b. Il est noté PPCM(a, b) (ou encore* $a \vee b$*)*

Proposition 0.3.

$\forall a, b \in \mathbb{Z}^*, PGCD(a, b) \times PPCM(a, b) = |ab|$

Démonstration 0.4.

Si on remplace a et b par leurs valeurs absolues: $||a||b|| = |ab|$
Les multiples et les diviseurs de —a— et de a sont les mêmes.
Donc $PGCD(a, b) = PGCD(|a|, |b|)$ *et* $PPCM(a, b) = PPCM(|a|, |b|)$
Ainsi il suffit de montrer le résultat pour $a, b \in \mathbb{N}^*$

On pose $d = PGCD(a,b)$
$\exists a', b' \in \mathbb{N}^*, a = da'$ *et* $b = db'$
$\dfrac{ab}{d} = \dfrac{da'b}{d} = a'b$ $\dfrac{ab}{d} = \dfrac{adb'}{d} = ab'$

$\square$

Méthode 0.1.

L'algorithme d'Euclide:
Le PGCD peut se calculer avec l'algorithme d'Euclide:

1. *(Eventuellement) remplacer a et b par* $|a|$ *et* $|b|$

2. *De manière récursive:*

2.1 *Calculer la division euclidienne de a par b:* $a = bq + r$

2.2 *Si* $r \neq 0$*: recommencer en remplcaçant (a, b) par (b, r) Sinon sortir de la récursion*

3. *Le pgcd est le dernier reste non-nul calculé.*

Proposition 0.4.

Si d est un diviseur commun à a et b alors $d \mid PGCD(a,b)$

Corollaire:
Le PGCD est aussi le plus grand diviseur commun au sens de la divisibilité.