Propriété des nombres entiers relatifs

I Division euclidienne

1) Division euclidienne sur les entiers naturels

$$\forall\, (\boldsymbol{a}\,,\boldsymbol{b}) \in \mathbb{N} \times\ \mathbb{N}^{*} :\ \exists\,!\ \ (\boldsymbol{q}\,,\boldsymbol{r}) \in \mathbb{N}^{\boldsymbol{2}} : \boldsymbol{a} = \boldsymbol{b}\,\boldsymbol{q} + \boldsymbol{r} \quad \textbf{et}\ \ \mathbf{0} \leq \mathbf{r} < b$$

Preuve :

existence de $(q\,,r)$

Considérons l'ensemble des nombres entiers naturels n tels que $b\,n$ soit inférieur ou égal à a. Notons q le plus grand élément de cet ensemble. Nous avons alors :

$$b\,q \leq a < b\,(q+1)$$

Soit, en soustrayant $b\,q$:

$$0 \leq a - b\,q < b$$

Posons alors :

$$r = a - b\,q$$

L'encadrement s'écrit alors :

$$0 \leq r < b$$

unicité de $(q\,,r)$

Supposons :

$$a = b\,q + r = b\,q' + r' \quad \text{et} \quad 0 \leq \mathrm{r} < b\,, 0 \leq \mathrm{r}' < b$$

Alors, en supposant par exemple $\mathrm{r} \leq \mathrm{r}'$:

$$b\,(q - q') = r' - r$$

Or :

$$0 \leq r' - r < b$$

Donc :

$$0 \leq b\,(q - q') < b$$

Il en résulte :

$$q - q' = 0$$

Donc :

$$q = q'$$

Puis :

$$r = r'$$

1) Division euclidienne sur les entiers relatifs

$$\forall\,(\boldsymbol{a}\,,\boldsymbol{b}) \in \mathbb{Z} \times\ \mathbb{Z}^* : \exists\,!\ \ (\boldsymbol{q}\,,\boldsymbol{r}) \in \mathbb{Z} \times \mathbb{N} : \boldsymbol{a = b\,q + r} \quad \textbf{et}\ \ \mathbf{0 \leq r < |b|}$$

Preuve :

Existence de $(q\,,r)$:

Procédons par disjonction de cas :

1er cas : $(a\,,b) \in \mathbb{N} \times\ \mathbb{N}^*$

C'est la division euclidienne sur les entiers naturels

2ème cas : $(a\,,b) \in (-\mathbb{N}) \times\ \mathbb{N}^*$

Alors : $(-a\,,b) \in \mathbb{N} \times\ \mathbb{N}^*$ donc :

$$\exists\ (q'\,,r') \in \mathbb{N} \times \mathbb{N} : -a = b\,q' + r' \quad \text{et}\ \ 0 \leq \mathrm{r}' < b$$

On en déduit :

$$a = b(-q') - r' = \ b(-q' - 1) + b - r\,'$$

Posons :

$$q = \ -q' - 1\,,\ \ r = b - r\,'$$

On en déduit :

$$a = b\,q + r \quad \text{et}\ \ 0 \leq \mathrm{r} < |\mathrm{b}|$$

3ème cas : $(a\,,b) \in \mathbb{N} \times\ (-\mathbb{N}^*)$

Alors : $(a\ , -b) \in \mathbb{N} \times\ \mathbb{N}^*$ donc :

$$\exists\ (q'\ , r') \in \mathbb{N} \times \mathbb{N} : a = (-b)\ q' + r' \quad \text{et} \quad 0 \leq \mathrm{r}' < -b$$

Posons :

$$q = \ -q'\ ,\ \ r = r\ '$$

On en déduit :

$$a = b\ q + r \quad \text{et} \quad 0 \leq \mathrm{r} < |\mathrm{b}|$$

<u>4ème cas</u> : $(a\ , b) \in (-\mathbb{N}) \times\ (-\mathbb{N}^*)$

Alors : $(-a\ , -b) \in \mathbb{N} \times\ \mathbb{N}^*$ donc :

$$\exists\ (q'\ , r') \in \mathbb{N} \times \mathbb{N} : -a = (-b)\ q' + r' \quad \text{et} \quad 0 \leq \mathrm{r}' < -b$$

On en déduit :

$$a = b\ q' - r' = \ \ b(q' + 1) - b - r\ '$$

Posons :

$q = \ q' + 1\ ,\ \ r = -b - r\ '$

On en déduit :

$$a = b\ q + r \quad \text{et} \quad 0 \leq \mathrm{r} < |\mathrm{b}|$$

<u>unicité de $(q\ , r)$</u>

Supposons :

$$a = b\ q + r = b\ q' + r' \quad \text{et} \quad 0 \leq \mathrm{r} < |\mathrm{b}|\ , 0 \leq \mathrm{r}' < |\mathrm{b}|$$

Alors , en supposant par exemple $\mathrm{r} \leq \mathrm{r}'$:

$$b\ (q - q') = r' - r$$

Or :

$$0 \leq r' - r < |\mathrm{b}|$$

Donc :

$$0 \leq b\ (q - q') < |\mathrm{b}|$$

Soit :

$$0 \leq |b|\ |q - q'| < |\mathrm{b}|$$

Il en résulte :

$$|q - q'| = 0$$

Donc :

$$q = q'$$

Puis :

$$r = r'$$

II Diviseur d'un nombre entier relatif

Etant donnéé un nombre entier relatif a, et un nombre entier relatif d non nul, on dit que d est un diviseur de a s'il existe un entier relatif a' tel que $a = d\ a'$.

Nous noterons $\mathfrak{D}(a)$ l'ensemble des diviseurs d'un nombre entier relatif a.

La définition s'écrit alors sous la forme plus compacte du langage mathématique:

$$\forall\ (\boldsymbol{d}, \boldsymbol{a}) \in \mathbb{Z} \times \mathbb{Z} :\ \boldsymbol{d} \in \mathfrak{D}(\boldsymbol{a}) \Leftrightarrow \boldsymbol{d} \neq \boldsymbol{0}\ \ \textbf{et}\ \ \exists\ \boldsymbol{a'} \in \mathbb{Z} : \boldsymbol{a} = \ \boldsymbol{d}\ \boldsymbol{a'}$$

Ainsi :

$\mathfrak{D}(0) = \mathbb{Z}$

$\mathfrak{D}(1) = \{-1; 1\}$

$\mathfrak{D}(2) = \{-2; -1; 1; 2\}$

Si nous notons $\mathfrak{D}_{\mathbb{N}}(a)$ les diviseurs entiers naturels d'un nombre entier relatif a, et $-\mathfrak{D}_{\mathbb{N}}(a)$ leurs opposés, alors nous avons :

$$\mathfrak{D}(\boldsymbol{a}) = \mathfrak{D}_{\mathbb{N}}(a) \cup (-\mathfrak{D}_{\mathbb{N}}(a))$$

La connaissance de $\mathfrak{D}_{\mathbb{N}}(a)$ est donc suffisante.

Notons également que :

$$\mathfrak{D}(\boldsymbol{a}) = \mathfrak{D}(-\boldsymbol{a})$$

Exemple de détermination des diviseurs entiers naturels d'un nombre entier naturel : 12

On décompose d'abord ce nombre en produit de facteurs premiers :

$$12 = 2 \times 2 \times 3$$

Les diviseurs entiers naturels de 12 sont alors, 1, chaque facteur premier pris individuellement, puis tous les produits possibles de facteurs premiers, c'est-à-dire, les produits deux à deux , 2×2 et 2×3, puis le produit des trois $2 \times 2 \times 3$

Ainsi :

$\mathfrak{D}_{\mathbb{N}}(12) = \{1; 2; 3; 4; 6; 12\}$

Propriétés des ensembles de diviseurs :

Propriété 1 :

$$\forall\ (\boldsymbol{a}, \boldsymbol{b}, \boldsymbol{z}) \in \mathbb{Z}^{\boldsymbol{3}} :\ \mathfrak{D}(\boldsymbol{a} + \boldsymbol{z}\ \boldsymbol{b}) \cap \mathfrak{D}(\boldsymbol{b}) = \mathfrak{D}(\boldsymbol{a}) \cap \mathfrak{D}(\boldsymbol{b})$$

Preuve :

Soit $d \in \mathfrak{D}(a + z\ b) \cap \mathfrak{D}(b)$ alors :

$$\exists\ z' \in \mathbb{Z} : a + z\ b = \ d\ z'$$

$$\exists\ b' \in \mathbb{Z} :\ b = \ d\ b'$$

On en déduit :

$$a + z\ d\ b' = \ d\ z'$$

$$a = \ d\ (z' - z\ b')$$

Donc :

$$d \in \mathfrak{D}(a)$$

D'où :

$$\mathfrak{D}(a + z\ b) \cap \mathfrak{D}(b) \subset \mathfrak{D}(a) \cap \mathfrak{D}(b)$$

Réciproquement, soit $d \in \mathfrak{D}(a) \cap \mathfrak{D}(b)$ alors :

$$\exists\ a' \in \mathbb{Z} : a = \ d\ a'$$

$$\exists\ b' \in \mathbb{Z} :\ b = \ d\ b'$$

On en déduit :

$$a + z\ b = d\ (a' + z\ b')$$

Donc :

$$d \in \mathfrak{D}(a + z\ b)$$

D'où :

$$\mathfrak{D}(a) \cap \mathfrak{D}(b) \subset \mathfrak{D}(a + z\ b) \cap \mathfrak{D}(b)$$

D'où finalement l'égalité.

Propriété 2 :

En notant $z\ \mathfrak{D}(a) = \{n \in \mathbb{Z} : \exists\ d \in \mathfrak{D}(a) :\ n = z\ d\}$

$$\forall\ (\boldsymbol{a}, \boldsymbol{b}, \boldsymbol{z}) \in \mathbb{Z}^{\boldsymbol{3}} :\ \boldsymbol{z}\ \mathfrak{D}(\boldsymbol{a}) \cap \boldsymbol{z}\ \mathfrak{D}(\boldsymbol{b}) \subset \mathfrak{D}(\boldsymbol{z}\ \boldsymbol{a}) \cap \mathfrak{D}(\boldsymbol{z}\ \boldsymbol{b})$$

Preuve :

Soit $d \in z\ \mathfrak{D}(a) \cap z\ \mathfrak{D}(b)$ alors :

$$\exists\ (d', a') \in \mathbb{Z}^2 : d = z\ d' \quad \text{et} \quad a = d'\ a'$$

$$\exists\ (d'', b') \in \mathbb{Z}^2 : d = z\ d'' \quad \text{et} \quad b = d''\ b'$$

Donc :

$$z\ a = z\ d'\ a' = d\ a'$$

$$z\ b = z\ d''\ b' = d\ b'$$

Donc :

$$d \in z\ \mathfrak{D}(z\ a) \cap z\ \mathfrak{D}(z\ b)$$

D'où l'inclusion

Attention, il n'y a pas égalité comme le montre l'exemple :

$\mathfrak{D}(2) = \{-2; -1; 1; 2\}$

$\mathfrak{D}(3) = \{-3; -1; 1; 3\}$

$\mathfrak{D}(3 \times 2) = \{-6; -3; -2; -1; 1; 2; 3; 6\}$

$\mathfrak{D}(3 \times 3) = \{-9; -3; -1; 1; 3; 9\}$

$$3\ \mathfrak{D}(2) \cap 3\ \mathfrak{D}(3) = \{-3; 3\}$$

$$\mathfrak{D}(3 \times 2) \cap \mathfrak{D}(3 \times 3) = \{-3; -1; 1; 3\}$$

III Le théorème de Bezout

1) Pour deux nombres

Etant donnés deux nombres entiers relatif a et b ayant 1 pour seul diviseur entier naturel commun (on les qualifie de premiers entre eux), alors, il existe deux entiers relatifs u et v tels que :

$$\boldsymbol{a\,u + b\,v = 1}$$

Soit en écriture plus mathématique :

$$\forall\,(\boldsymbol{a},\boldsymbol{b}) \in \mathbb{Z}^{\mathbf{2}} :\ \mathfrak{D}_{\mathbb{N}}(\boldsymbol{a}) \cap \mathfrak{D}_{\mathbb{N}}(\boldsymbol{b}) = \{\mathbf{1}\} \Rightarrow\ \exists\,(\boldsymbol{u},\boldsymbol{v}) \in \mathbb{Z}^{\mathbf{2}} : \boldsymbol{a\,u + b\,v = 1}$$

Preuve :

Nous allons proposer une démonstration ne faisant pas appel aux propriétés des sous-ensembles de $\mathbb{Z}$ appelés idéaux et sur lesquels nous reviendrons un peu plus loin, ce qui sera ptécisément l'occasion d'introduire le concept d'idéal d'un anneau.

Cas entier naturel :

Nous supposerons dans un premier temps $(a, b) \in \mathbb{N}^2$

Le fait que ces deux nombres n'aient pas de diviseur commun autre que 1 impose qu'ils soient tous deux non nuls.

Considérons les nombres entiers naturels non nuls de la forme $a\,u - b\,v$ ou $b\,v - a\,u$, u et v étant deux entiers naturels.

Cet ensemble, que nous appellerons $\mathbb{E}$, est un sous ensemble de $\mathbb{N}$ non vide car il contient a. Il admet donc un plus petit élément, que nous noterons d.

Nous allons alors prouver que d est à la fois un diviseur de a et de b.

Sans nuire à la généralité, nous supposerons que d est de la première forme, soit :

$$d = a\,u_0 - b\,v_0 \quad , \qquad (u_0, v_0) \in \mathbb{N}^{\mathbf{2}}$$

1ère étape : Montrons que d est diviseur de a

La division euclidienne de a par d donne :

$$\exists\,!\ \ (q\,, r) \in \mathbb{N}^2 : a = d\,q + r \quad \text{et} \quad 0 \leq \mathrm{r} < d$$

Donc :

$$r = a - d\,q$$

$$r = a - (a\,u_0 - b\,v_0)\,q$$

$$r = b\,(v_0\,q) - a\,(u_0\,q - 1\,)$$

Soit, en posant : $v = v_0\,q\ \ ,\ u = \ u_0\,q - 1$:

$$r = b\,v - a\,u$$

Montrons par l'absurde que : $u_0\,q \neq 0$

Supposons $u_0\,q = 0$ alors deux cas peuvent se présenter :

1er cas : $u_0 = 0$, mais alors $d = -b\,v_0 \leq 0$, ce qui est absurde car $d > 0$

2ème cas : $q = 0$, mais alors $r = a$, or $a \in \mathbb{E}$ et $d = min(\mathbb{E})$ donc : $d \leq a$ cela contredit $r < d$

u et v sont donc tous deux des entiers naturels.

Supposons alors par l'absurde que $r > 0$. Alors $r \in \mathbb{E}$ et $r < d,$ cela contredit $d = min(\mathbb{E})$

Donc $r = 0$, il en résulte : $a = d\,q$ et donc que d est un diviseur de a

2ème étape : Montrons que d est diviseur de b

La division euclidienne de b par d donne :

$$\exists\,!\ \ (q\,,r) \in \mathbb{N}^2 : b = d\,q + r \quad \text{et} \quad 0 \leq \mathrm{r} < b$$

Donc :

$$r = b - d\,q$$

$$r = b - (a\,u_0 - b\,v_0)\,q$$

$$r = b\,(1 + v_0\,q) - a\,u_0\,q$$

Soit, en posant : $v = 1 + v_0\,q\ \ ,\ u = \ u_0\,q$:

$$r = b\,v - a\,u$$

u et v sont donc tous deux des entiers naturels.

Supposons alors par l'absurde que $r > 0$ alors $r \in \mathbb{E}$ et $< d$, cela contredit $d = min(\mathbb{E})$

Donc $r = 0$, il en résulte : $b = d\,q$ et donc que d est un diviseur de b

d est donc un diviseur commun à a et b, donc :

$$d = 1$$

Cela prouve la propriété

Cas général :

Ce cas se déduit trivialement du précédent par disjonction de cas. Nous ne traiterons que le cas $(a, b) \in \mathbb{N} \times (-\mathbb{N})$, les autres étant analogues.

On a alors : $(a, -b) \in \mathbb{N} \times \mathbb{N}$ et a et – b sont premiers entre eux. Donc :

$$\exists\, (u, v) \in \mathbb{Z}^2 : a\, u - b\, v = 1$$

D'où :

$$a\, u + b\, (-v) = 1$$

Soit en posant : $u' = u$, $v' = -v$:

$$a\, u' + b\, v' = 1$$

Ce qui prouve la propriété.

2) Pour n nombres

Etant donnés n nombres entiers relatif $a_1, a_2, \dots, a_n$ ayant 1 pour seul diviseur entier naturel commun (on les qualifie de premiers entre eux dans leur ensemble), alors, il existe n entiers relatifs $u_1, u_2, \dots, u_n$ tels que :

$$\boldsymbol{a_1 u_1 + a_2\, u_2 + \cdots + a_n\, u_n = 1}$$

Soit en écriture plus mathématique :

$$\forall\, (\boldsymbol{a_1, a_2, \dots, a_n}) \in \mathbb{Z}^{\boldsymbol{n}} :$$

$$\mathfrak{D}_{\mathbb{N}}(a_1) \cap \mathfrak{D}_{\mathbb{N}}(a_2) \cap \dots \cap \mathfrak{D}_{\mathbb{N}}(a_n) = \{\boldsymbol{1}\} \Rightarrow \exists\, (\boldsymbol{u_1, u_2, \dots, u_n}) \in \mathbb{Z}^{\boldsymbol{n}} : \boldsymbol{a_1 u_1 + a_2\, u_2 + \cdots + a_n\, u_n = 1}$$

Preuve : Par récurrence sur n pour $n \geq 2$

Qualifions de $P(n)$ la propriété précédente.

La propriété a déjà été initialisée pour $n = 2$, voyons son caractère héréditaire.

Soit donc un entier naturel $n \geq 2$ pour lequel $P(n)$ est vraie, et soit $n + 1$ nombres entiers relatifs $a_1, a_2, \ldots, a_n, a_{n+1}$ n'ayant que 1 pour seul diviseur entier naturel commun, notons alors d le plus grand entier naturel diviseur commun à $a_1, a_2, \ldots, a_n$. On a alors :

$$a_1 = d\, b_1, a_2 = d\, b_2, \ldots, a_n = d\, b_n$$

$b_1, b_2, \ldots, b_n$ sont alors n nombres entiers relatifs n'ayant que 1 pour seul diviseur entier naturel commun. D'après l'hypothèse de récurrence, on en déduit :

$$\exists\, (u_1, u_2, \ldots, u_n) \in \mathbb{Z}^n : b_1 u_1 + b_2\, u_2 + \cdots + b_n\, u_n = 1$$

Donc, en multipliant par d :

$$d\ b_1\ u_1 + d\, b_2\, u_2 + \cdots + d\ b_n\ u_n = d$$

soit :

$$a_1\ u_1 + a_2\, u_2 + \cdots + a_n\ u_n = d$$

Or d et a_{n+1} sont deux nombres entiers relatifs n'ayant que 1 pour seul diviseur entier naturel commun. D'après l'initialisation, on en déduit :

$$\exists\, (u, v) \in \mathbb{Z}^2 : d\, u + a_{n+1}\, v = 1$$

Soit :

$$(a_1\ u_1 + a_2\, u_2 + \cdots + a_n\ u_n)\, u + a_{n+1}\, v = 1$$

D'où :

$$a_1\ (u_1\, u) + a_2\, (u_2\, u) + \cdots + a_n\ (u_n\, u) + a_{n+1}\, v = 1$$

Soit en posant : $v_1 = u_1\, u, v_2 = u_2\, u, \ldots, v_n = u_n\, u,\ v_{n+1} = v$

$$a_1\ v_1 + a_2\, v_2 + \cdots + a_n\ v_n + a_{n+1}\, v_{n+1} = 1$$

Ce qui prouve que $P(n + 1)$ est vraie

$P(n)$ est donc vraie pour tout $n \geq 2$

IV Plus Grand Commun Diviseur

3) Définition pour deux nombres

Le plus grand commun diviseur (PGCD) de deux nombres entiers relatifs a et b est, comme son nom l'indique, le plus grand des diviseurs entiers naturels communs à ces deux nombres. Nous le noterons $a \wedge b$. Ainsi :

$$\boldsymbol{a \wedge b = Max\left(\mathfrak{D}_{\mathbb{N}}(a) \cap \mathfrak{D}_{\mathbb{N}}(b)\right)}$$

Exemple :

$\mathfrak{D}_{\mathbb{N}}(12) = \{1; 2; 3; 4; 6; 12\}$

$\mathfrak{D}_{\mathbb{N}}(15) = \{1; 3; 5; 15\}$

$$12 \wedge 15 = 3$$

4) propriétés

Propriété 1

$$a \wedge b = |a| \wedge |b|$$

Cette propriété, évidente, montre que le calcul du PGCD de deux nombres relatifs se ramène à celui de nombres entiers naturels.

Propriété 2

$$a \wedge b = (a - b) \wedge b$$

Preuve :

Nous avons :

$$\mathfrak{D}(a - b) \cap \mathfrak{D}(b) = \mathfrak{D}(a) \cap \mathfrak{D}(b)$$

Il en découle :

$$(a - b) \wedge b = a \wedge b$$

A noter que nous avons également :

$$\mathfrak{D}(a+b) \cap \mathfrak{D}(b) = \mathfrak{D}(a) \cap \mathfrak{D}(b)$$

Donc :

$$a \wedge b = (a+b) \wedge b$$

Propriété 3 :

Effectuons la division euclidienne de a par b :

$$\exists\,!\ \ (q\,, r) \in \mathbb{Z} \times \mathbb{N} : a = b\,q + r \quad \text{et} \ \ 0 \leq \mathrm{r} < |\mathrm{b}|$$

En prenant $z = -q$ nous en déduisons :

$$a \wedge b = (a - b\,q) \wedge b = r \wedge b$$

Cette propriété conduit à l'algorithme d'Euclide pour la détermination du PGCD

Propriété 4 :

$$\forall\, (\boldsymbol{a}, \boldsymbol{b}, \boldsymbol{z}) \in \mathbb{Z}^{\boldsymbol{3}} :\ (\boldsymbol{z}\,\boldsymbol{a}) \wedge (\boldsymbol{z}\,\boldsymbol{b}) = |\boldsymbol{z}|\ (\boldsymbol{a} \wedge \boldsymbol{b})$$

Preuve :

Il suffit de se ramener au cas $z > 0$:

Notons : $d = a \wedge b\ ,\ d' = (z\,a) \wedge (z\,b)$ alors :

$$\exists\, a' \in \mathbb{Z} : a = d\,a'$$

$$\exists\, b' \in \mathbb{Z} : b = d\,b'$$

$$a' \wedge b' = 1$$

Donc :

$$z\,a = z\,d\,a'$$

$$z\,b = z\,d\,b'$$

Donc :

$$z\,d \in \mathfrak{D}_{\mathbb{N}}(z\,a) \cap \mathfrak{D}_{\mathbb{N}}(z\,b)$$

D'où :

$$z\,d \leq (z\,a) \wedge (z\,b) = d'$$

Inversement :

$$\exists\, z' \in \mathbb{Z} : z\, a = d' z'$$

$$\exists\, z" \in \mathbb{Z} : z\, b = d'\, z"$$

Donc :

$$z\, d\, a' = d' z'$$

$$z\, d\, b' = d'\, z"$$

Or d'après le théorème de Bezout :

$$\exists (u, v) \in \mathbb{Z}^2 :\ a' u + b' v = 1$$

On en déduit :

$$z\, d\, a' u + z\, d\, b' v = z\, d$$

$$d' z' u + d'\, z"\, v = z\, d$$

$$d' (z' u +\ z"\, v) = z\, d$$

Donc $d' \in \mathfrak{D}_{\mathbb{N}}(z\, d)$

Donc :

$$d' \leq z\, d$$

D'où l'égalité

Propriété 5 :

$$\forall\, (\boldsymbol{a}, \boldsymbol{b}) \in \mathbb{Z}^{\boldsymbol{2}} : \exists\, (\boldsymbol{u}, \boldsymbol{v}) \in \mathbb{Z}^{\boldsymbol{2}} :\ \boldsymbol{a} \wedge \boldsymbol{b} = \boldsymbol{a}\, \boldsymbol{u} + \boldsymbol{b}\, \boldsymbol{v}$$

Preuve :

Notons $d =\ a \wedge b$ alors :

$$\exists\, (a', b') \in \mathbb{Z}^2 :\ a = d\, a', \qquad b = d\, b', \qquad a' \wedge b' = 1$$

D'après le théorème de Bezout :

$$\exists\, (u, v) \in \mathbb{Z}^2 :\ a' u + b' v = 1$$

Donc, en multipliant par d :

$$d\, a' u + d\, b' v = d$$

Soit :

$$a\, u + b\, v = d$$

5) Définition pour n nombres

Le plus grand commun diviseur (PGCD) de n nombres entiers relatifs $a_1, a_2, \dots, a_n$ est, comme son nom l'indique, le plus grand des diviseurs entiers naturels communs à tous ces nombres. Nous le noterons $a_1 \wedge a_2 \wedge \dots \wedge a_n$. Ainsi :

$$\boldsymbol{a_1 \wedge a_2 \wedge \dots \wedge a_n = Max\left(\mathfrak{D}_{\mathbb{N}}(a_1) \cap \mathfrak{D}_{\mathbb{N}}(a_2) \cap \dots \cap \mathfrak{D}_{\mathbb{N}}(a_n)\right)}$$

Propriété 6 :

$$\forall\, (\boldsymbol{a_1, a_2, \dots, a_n}) \in \mathbb{Z}^{\boldsymbol{n}} :$$

$$\exists\, (\boldsymbol{u_1, u_2, \dots, u_n}) \in \mathbb{Z}^{\boldsymbol{n}} : \boldsymbol{a_1 \wedge a_2 \wedge \dots \wedge a_n = a_1 u_1 + a_2 u_2 + \dots + a_n u_n}$$

Preuve :

Analogue à celle de la propriété 5

V Nombres premiers

Un nombre premier est un nombre entier naturel qui possède exactement deux diviseurs distincts, 1 et lui-même.

La définition mathématique est donc la suivante en notant $\mathcal{P}_{\mathbb{N}}$ l'ensemble des nombres premiers :

$$\boldsymbol{p \in \mathcal{P}_{\mathbb{N}} \Leftrightarrow p \neq 1 \ \text{ et } \ \mathfrak{D}_{\mathbb{N}}(p) = \{1; p\}}$$

Le crible d'Eratosthène permet de déterminer les nombres premiers inférieurs à un entier naturel donné (voir fiche à ce sujet)

Nous verrons plus loin qu'il existe une infinité de nombres premiers, dont voici les premiers :

$$\mathcal{P}_{\mathbb{N}} = \{2; 3; 5; 7; 11; 13; 17; 19; 23; 29; 31; 37; 41; 43; 47; 53; 59; 61; 67; 71; 73; 79; 83; 89; 97; \dots\}$$

Propriété :

Si p est un nombre premier et a un nombre entier relatif alors :

Si $p \in \mathfrak{D}_{\mathbb{N}}(a)$: $p \wedge a = p$

Si $p \notin \mathfrak{D}_{\mathbb{N}}(a)$: $p \wedge a = 1$

Preuve :

Si $p \in \mathfrak{D}_{\mathbb{N}}(a)$: $\exists\, a' \in \mathbb{Z} : a = p\ a'$ et $p \wedge a = (p\ a') \wedge p = p\ (a'\ \wedge 1) = p$

Si $p \notin \mathfrak{D}_{\mathbb{N}}(a)$: notons $d = p \wedge a$ alors d divise p , maist $d \neq p$ car d divise a, donc $d = 1$

VI Nombres premiers entre eux

1) Deux nombres

Deux nombres entiers relatifs a et b sont dits premiers entre eux si leur PGCD est 1 , autrement dit :

a et b premiers entre eux $\Leftrightarrow$ $a \wedge b = 1$

Une caractérisation découlant de la propriété 5 est :

a et b premiers entre eux $\Leftrightarrow$: $\exists\, (u, v) \in \mathbb{Z}^2 : a\,u + b\,v = 1$

Propriété 7 :

$$\forall\, (a, b, c) \in \mathbb{Z}^3 : \left.\begin{matrix} a \wedge b = 1 \\ a \wedge c = 1 \end{matrix}\right\} \Leftrightarrow a \wedge (b\,c) = 1$$

Preuve :

Si $a \wedge b = 1$ et $a \wedge c = 1$ alors d'après le théorème de Bezout :

$$\exists\, (u, v) \in \mathbb{Z}^2 : a\,u + b\,v = 1$$

$$\exists\, (u', v') \in \mathbb{Z}^2 : a\,u' + c\,v' = 1$$

Par produit :

$$(a\,u + b\,v)\,(a\,u' + c\,v') = 1$$

Soit en développant :

$$a\,(a\,u' + c\,v') + a\,(b\,v\,u') + b\,c\,v\,v' = 1$$

Donc :

$$a\,(a\,u' + c\,v' + b\,v\,u') + (b\,c)\,v\,v' = 1$$

En posant : $u" = a\,u' + c\,v' + b\,v\,u'$, $v = v\,v'$:

$$a\,u" + (b\,c)\,v" = 1$$

Donc

$$a \wedge (b\,c) = 1$$

Propriété 8 : Pour n entier naturel supérieur ou égal à deux

$$\forall\,(\boldsymbol{a, b_1, b_2}\,, \ldots, \boldsymbol{b_n}) \in \mathbb{Z}^{\boldsymbol{n+1}} :\ \boldsymbol{a \wedge b_1 = a \wedge b_2 = \cdots = a \wedge b_n = 1 \Leftrightarrow a \wedge (b_1\,b_2\,\ldots b_n) = 1}$$

Preuve :

Par récurrence et en utilisant la propriété 7

2) n nombres

n nombres entiers relatifs $a_1, a_2\,, \ldots, a_n$ sont premiers entre eux dans leur ensemble si leur PGCD est 1, autrement dit :

$$\boldsymbol{a_1, a_2\,, \ldots, a_n}\ \textbf{premiers entre eux dans leur ensemble} \Leftrightarrow\ \boldsymbol{a_1 \wedge\ a_2 \wedge \ldots \wedge\ a_n = 1}$$

Une caractérisation découlant de la propriété 6 est :

$$\boldsymbol{a_1, a_2\,, \ldots, a_n}\ \textbf{premiers entre eux dans leur ensemble}$$

$$\Leftrightarrow\ \exists\,(\boldsymbol{u_1, u_2\,, \ldots, u_n}) \in \mathbb{Z}^{\boldsymbol{n}} : \boldsymbol{a_1 u_1 + a_2\,u_2 + \cdots +\ a_n\,u_n = 1}$$

3) Applications aux nombres premiers

Si $\boldsymbol{p}$ **et** $\boldsymbol{q}$ **sont deux nombres premiers distincts alors :**

$$\forall\,(\boldsymbol{n, m}) \in \mathbb{N}^{\boldsymbol{2}} :\ \boldsymbol{p^n \wedge q^m = 1}$$

Preuve :

1er cas : $n = 0$ ou $m = 0$

la propriété est triviale

2ème cas : $n = 1$ et $m = 1$

la propriété est encore triviale

3ème cas : $n = 1$ et $m > 0$

la propriété est une conséquence immédiate de la propriété 8 avec

$$a = p, b_1 = b_2 = \cdots = b_n = q$$

4ème cas : $n > 0$ et $m > 0$

la propriété est encore une conséquence immédiate de la propriété 8 et de la précédente avec :

$$a = p^n, b_1 = b_2 = \cdots = b_m = q$$

Généralisation :

Si $\boldsymbol{p}, \boldsymbol{p_1}, \boldsymbol{p_2}, \ldots, \boldsymbol{p_n}$ **sont des nombres premiers deux à deux distincts alors :**

$$\forall\, (\boldsymbol{m}, \boldsymbol{\alpha_1}, \boldsymbol{\alpha_2}, \ldots, \boldsymbol{\alpha_n}) \in \mathbb{N}^{\boldsymbol{n+1}} :\ \boldsymbol{p^m} \wedge \boldsymbol{{p_1}^{\alpha_1}}\, \boldsymbol{{p_2}^{\alpha_2}} \ldots \boldsymbol{{p_n}^{\alpha_n}} = \boldsymbol{1}$$

Preuve :

On applique la propriété 8 avec :

$$a = p^m, b_1 = {p_1}^{\alpha_1}, b_2 = {p_2}^{\alpha_2} \ldots = b_n = {p_n}^{\alpha_n}$$

VII Théorème de Gauss

Si un entier relatif divise un produit d'entiers relatifs et qu'il est premier avec l'un des facteurs du produit alors il divise le second facteur

En version mathématique :

$$\forall\, (\boldsymbol{a}, \boldsymbol{b}, \boldsymbol{c}) \in \mathbb{Z}^{\boldsymbol{3}} : \left.\begin{matrix} \boldsymbol{a} \in \mathfrak{D}(\boldsymbol{b}\, \boldsymbol{c}) \\ \boldsymbol{a} \wedge \boldsymbol{b} = \boldsymbol{1} \end{matrix}\right\} \Rightarrow\ \boldsymbol{a} \in \mathfrak{D}(\, \boldsymbol{c})$$

Preuve :

a et b étant premiers entre eux, le théorème de Bezout permet d'écrire :

$$\exists\,(u,v)\in\mathbb{Z}^2 : a\,u+b\,v=1$$

Donc, en multipliant par c :

$$a\,c\,u+b\,c\,v=c$$

a étant un diviseur de $b\,c$, on en déduit :

$$\exists\,k\in\mathbb{Z} : b\,c=k\,a$$

Donc :

$$a\,c\,u+k\,a\,v=c$$

D'où :

$$a\,(c\,u+k\;\,v)=c$$

Donc :

$$a\in\mathfrak{D}(\,c)$$

<u>Corollaire</u> :

Si deux entiers relatifs premiers entre eux divisent un même troisième, alors leur produit divise ce dernier.

Soit, en version mathématique :

$$\forall\,(\boldsymbol{a},\boldsymbol{b},\boldsymbol{c})\in\mathbb{Z}^{\boldsymbol{3}} : \left.\begin{matrix}(\boldsymbol{a},\boldsymbol{b})\in\mathfrak{D}(\,\boldsymbol{c})^{\boldsymbol{2}}\\ \boldsymbol{a}\wedge\boldsymbol{b}=\boldsymbol{1}\end{matrix}\right\}\Rightarrow\ \boldsymbol{a}\,\boldsymbol{b}\in\mathfrak{D}(\,\boldsymbol{c})$$

<u>Preuve</u>

Nous nous contenterons du cas où a et b sont des entiers naturels, le cas général s'en déduisant trivialement

La division euclidienne de c par $a\,b$ s'écrit :

$$\exists\,!\ \ (q\,,r)\in\mathbb{N}^2 : c=a\,b\,q+r\quad\text{ et }\ 0\leq \mathrm{r}<b$$

Donc :

$$r=c-a\,b\,q$$

a divise c et a divise $a\,b\,q$ donc il divise la différence $r=c-a\,b\,q$

De la même façon, b divise r. On en déduit :

$$\exists\ r_1\in\mathbb{N}:\ \ r=a\,r_1$$

b divise $a\,r_1$ et $a\wedge b=1$, d'après le théorème de Gauss, b divise r_1 donc :

$$\exists\ r_2 \in \mathbb{N} :\ r_1 = b\, r_2$$

Donc :

$$r = a\, b\, r_2$$

D'où :

$$0 \leq a\, b\, r_2 < a\, b$$

Soit, en divisant par $a\ b$ qui est un entier naturel non nul :

$$0 \leq\ r_2 < 1$$

Donc :

$$r_2 = 0$$

D'où

$$r = 0$$

Puis :

$$c = a\, b\, q$$

Finalement :

$$a\ b \in \mathfrak{D}(\ c)$$

VIII Décomposition en produits de facteurs premiers

Tout nombre entier naturel supérieur ou égal à 2 se décompose de façon unique en produit de facteurs premiers

Mathématiquement :

$$\forall\ \boldsymbol{m} \in \mathbb{N}\backslash\{\mathbf{0},\mathbf{1}\} :\ \exists\,!\,\boldsymbol{n} \in \mathbb{N}\ \exists\,!\ \ (\boldsymbol{\alpha_1}, \boldsymbol{\alpha_2}\ , \ldots , \boldsymbol{\alpha_n}) \in (\mathbb{N}^*)^{\boldsymbol{n}}\ , \exists\,!\ \ (\boldsymbol{p_1}, \boldsymbol{p_2}\ , \ldots , \boldsymbol{p_n}) \in (\boldsymbol{\mathcal{P}}_{\mathbb{N}})^{\boldsymbol{n}} :$$

$$\forall\ (\boldsymbol{i}, \boldsymbol{j}) \in (\llbracket \mathbf{1}; \boldsymbol{n} \rrbracket)^{\mathbf{2}} : \boldsymbol{p_i} \neq\ \boldsymbol{p_j}\ \ \textbf{et}\ \ \boldsymbol{m} = \boldsymbol{p_1}^{\boldsymbol{\alpha_1}}\, \boldsymbol{p_2}^{\boldsymbol{\alpha_2}} \ldots\ \boldsymbol{p_n}^{\boldsymbol{\alpha_n}}$$

Preuve :

Existence de la décomposition :

Notons $P(m)$ le prédicat suivant :

$$\exists\, n \in \mathbb{N}\ \exists\ (\alpha_1, \alpha_2\ , \dots , \alpha_n) \in (\mathbb{N}^*)^n\ , \exists\ (p_1, p_2\ , \dots , p_n) \in (\mathcal{P}_{\mathbb{N}})^n :$$

$$\forall\ (i,j) \in ([\![1; n]\!])^2 : p_i \neq\ p_j\ \text{ et }\ m = {p_1}^{\alpha_1}\ {p_2}^{\alpha_2} \dots\ {p_n}^{\alpha_n}$$

Et démontrons que $P(m)$ est vraie pour tout entier $m \geq 2$ par une récurrence forte.

Initialisation : pour $m = 2$

$$2 = 2^1$$

Donc $P(2)$ est vraie

Hérédité : Soit $m \in \mathbb{N}\backslash\{0,1\}$ tel que : $\forall\ k \in [\![2; m]\!]$: $P(k)$ vraie, alors par disjonction de cas :

1er cas : $m + 1$ est un nombre premier noté p et :

$$m + 1 = p^1$$

Donc $P(m + 1)$ est vraie

2er cas : $m + 1$ n'est pas un nombre premier et il possède un diviseur k distinct de 1 et de lui-même, donc :

$$\exists\ (k\ k') \in \mathbb{N}^2 :\ m + 1 = k\ k'\ \text{ et }\ \ 2 \leq k \leq m\ \ ,\ 2 \leq k' \leq m$$

L'hypothèse de récurrence s'applique donc à k et à k' et s'écrit :

Pour k :

$$\exists\, n \in \mathbb{N}\ \exists\ (\alpha_1, \alpha_2\ , \dots , \alpha_n) \in (\mathbb{N}^*)^n\ , \exists\ (p_1, p_2\ , \dots , p_n) \in (\mathcal{P}_{\mathbb{N}})^n :$$

$$\forall\ (i,j) \in ([\![1; n]\!])^2 : p_i \neq\ p_j\ \text{ et }\ k = {p_1}^{\alpha_1}\ {p_2}^{\alpha_2} \dots\ {p_n}^{\alpha_n}$$

Pour k' :

$$\exists\ l \in \mathbb{N}\ \exists\ (\beta_1, \beta_2\ , \dots , \beta_l) \in (\mathbb{N}^*)^l\ , \exists\ (q_1, q_2\ , \dots , q_l) \in (\mathcal{P}_{\mathbb{N}})^l :$$

$$\forall\ (i,j) \in ([\![1; l]\!])^2 : q_i \neq\ q_j\ \text{ et }\ k' = {q_1}^{\beta_1}\ {q_2}^{\beta_2} \dots\ {q_l}^{\beta_l}$$

Ainsi :

$$m + 1 = {p_1}^{\alpha_1}\ {p_2}^{\alpha_2} \dots\ {p_n}^{\alpha_n}\ {q_1}^{\beta_1}\ {q_2}^{\beta_2} \dots\ {q_l}^{\beta_l}$$

En regroupant les nombres premiers qui sont communs aux décompositions de k et de k' sous une même puissance, on obtient que $P(m + 1)$ es vraie.

Donc $P(m)$ est vraie pout tout entier naturel $m \geq 2$

Unicité de la décomposition.

Soit deux décompositions en facteurs premiers d'un même nombre m. Quitte à ajouter des facteurs premiers manquant à la puissance 0, nous pouvons supposer que les deux décompositions ont les mêmes facteurs premiers et partir de :

$$m = {p_1}^{\alpha_1}\ {p_2}^{\alpha_2} \dots\ {p_n}^{\alpha_n} = {p_1}^{\beta_1}\ {p_2}^{\beta_2} \dots\ {p_n}^{\beta_n}$$

Sans nuire à la généralité nous pouvons supposer $\alpha_1 \geq \beta_1$

On a alors :

$${p_1}^{\alpha_1-\beta_1}\ {p_2}^{\alpha_2} \dots\ {p_n}^{\alpha_n} =\ {p_2}^{\beta_2} \dots\ {p_n}^{\beta_n}$$

Donc :

${p_1}^{\alpha_1-\beta_1}$ est un diviseur de ${p_2}^{\beta_2} \dots\ {p_n}^{\beta_n}$

Or :

$${p_1}^{\alpha_1-\beta_1} \wedge {p_2}^{\beta_2} = \dots = {p_1}^{\alpha_1-\beta_1} \wedge {p_n}^{\beta_n} = 1$$

Donc :

$${p_1}^{\alpha_1-\beta_1} \wedge \left({p_2}^{\beta_2} \dots\ {p_n}^{\beta_n}\right) = 1$$

D'où :

$${p_1}^{\alpha_1-\beta_1} = 1$$

Il en résulte :

$$\alpha_1 = \beta_1$$

et

$${p_2}^{\alpha_2} \dots\ {p_n}^{\alpha_n} =\ {p_2}^{\beta_2} \dots\ {p_n}^{\beta_n}$$

En réitérant le procédé, on obtient :

$$\alpha_2 = \beta_2\ , \dots , \alpha_n = \beta_n$$

Ce qui prouve l'unicité de la décomposition.

IX Plus Petit Commun multiple

1) Définition pour deux nombres

Le plus petit commun multiple (PPCM) de deux nombres entiers relatifs a et b est, comme son nom l'indique, le plus petit des multiples entiers naturels communs à ces deux nombres. Nous le noterons $a \vee b$. Ainsi en notant $\mathfrak{M}_{\mathbb{N}}(a)$ l'ensemble des multiples entiers naturels non nuls d'un nombre entier relatif a, la définition s'écrit mathématiquement :

$$\boldsymbol{a \vee b = Min\left(\mathfrak{M}_{\mathbb{N}}(a) \cap \mathfrak{M}_{\mathbb{N}}(b)\right)}$$

Exemple :

$\mathfrak{M}_{\mathbb{N}}(12) = \{12; 24; 36; 48; 60; 72; 84; \dots\}$

$\mathfrak{M}_{\mathbb{N}}(15) = \{15; 30; 45; 60; 75; \dots\}$

$$12 \vee 15 = 60$$

2) Définition pour deux nombres

Le plus petit commun multiple (PPCM) de de n nombres entiers relatifs $a_1, a_2, \dots, a_n$ est, comme son nom l'indique, le plus petit des multiples entiers naturels communs à tous ces nombres. Nous le noterons $a_1 \vee a_2 \vee \dots \vee a_n$. Ainsi :

$$\boldsymbol{a_1 \vee a_2 \vee \dots \vee a_n = Min\left(\mathfrak{M}_{\mathbb{N}}(a_1) \cap \mathfrak{M}_{\mathbb{N}}(a_2) \cap \dots \cap \mathfrak{M}_{\mathbb{N}}(a_n)\right)}$$

X Propriétés du PGCD et du PPCM

1) pour deux nombres

Soit deux entiers naturels a et b dont les décompositions en facteurs premiers sont éventuellement enrichies de facteurs premiers à la puissance 0 de telle sorte que les deux décompositions aient les mêmes facteurs premiers :

$$\boldsymbol{a = {p_1}^{\alpha_1} {p_2}^{\alpha_2} \dots {p_n}^{\alpha_n}}$$

$$\boldsymbol{b = p_1^{\beta_1}\, p_2^{\beta_2} \ldots\, p_n^{\beta_n}}$$

alors :

$$\boldsymbol{a \wedge b = p_1^{\gamma_1}\, p_2^{\gamma_2} \ldots\, p_n^{\gamma_n}}$$

$$\boldsymbol{a \vee b = p_1^{\delta_1}\, p_2^{\delta_2} \ldots\, p_n^{\delta_n}}$$

avec :

$$\forall\, \boldsymbol{i} \in [\![\mathbf{1}; \boldsymbol{n}]\!] \;:\; \boldsymbol{\gamma_i = \min(\alpha_i\ , \beta_i)}\ \ ,\ \ \boldsymbol{\delta_i = \max(\alpha_i\ , \beta_i)}$$

De cette propriété, on déduit :

$$\boldsymbol{(a \wedge b\ ) \times\ (a \vee b) = a \times b}$$

2) pour n nombres :

Des formules analogues s'établissent pour n nombres

$$\boldsymbol{(a_1 \wedge\ a_2 \wedge \ldots \wedge\ a_n)\ \times\ \ (a_1 \vee\ a_2 \vee \ldots \vee\ a_n) = a_1 \times\ a_2 \times \ldots \times\ a_n}$$

X Notion d'idéal d'un anneau

1) Approche

Rappelons que $(\mathbb{Z}, +, \times)$ a une structure d'anneau commutatif. Considérons alors, pour deux entiers relatifs a et b, les sous-ensembles d'entiers relatifs de la forme :

$$\mathbb{E}_{a,b} = \{a\, u + b\, v :\ (u, v) \in \mathbb{Z}^2\}$$

Nous voyons que ces ensembles sont stables pour l'addition et l'opposé. En effet :

La somme de deux de ces nombres est du même type que ces nombres

$$(a\, u + b\, v) + (a\, u' + b\, v') = a(u + u'\,) + b\, (v + v')$$

et l'opposé d'un de ces nombres est du même type que ce dernier :

$$-(a\, u + b\, v) = a(-u\,) + b\, (-v)$$

Ces deux propriétés suffisent à faire de $(\mathbb{E}_{a,b}, +)$ un groupe commutatif qualifié de sous groupe de $(\mathbb{Z}, +)$ car l'associativité de l'addition dans $\mathbb{Z}$ se retrouve assurée sur tout sous-ensemble, et l'élément neutre de l'addition, 0, est nécessairement dans $\mathbb{E}_{a,b}$ car somme d'un élément de $\mathbb{E}_{a,b}$ et de son opposé.

De même, le produit de deux éléments de $\mathbb{E}_{a,b}$ est du même type , mais il y a mieux, le produit d'un élément de $\mathbb{E}_{a,b}$ par un élément de $\mathbb{Z}$ (à gauche ou à droite car la multiplication est commutative) est du même type, car :

$$(a\,u + b\,v) \times z = a(u\,z) + b\,(v\,z')$$

On dit alors que $\mathbb{E}_{a,b}$ est un **idéal** de $(\mathbb{Z}, +, \times)$.

En revanche, l'élément neutre multiplicatif, 1, n'est dans $\mathbb{E}_{a,b}$ que si a et b sont premiers entre eux.

$(\mathbb{E}_{a,b}, +, \times)$ ne sera alors un anneau, qualifié de sous anneau de $(\mathbb{Z}, +, \times)$ que si a et b sont premiers entre eux.

Nous arrivons donc à la définition générale suivante :

Etant donné un anneau commutatif $(\mathbb{A}, +, *)$, un sous-ensemble $\mathbb{I}$ de $\mathbb{E}$ est un idéal si :

a) $(\mathbb{I}, +)$ **est un sous-groupe de** $(\mathbb{A}, +)$ **c'est-à-dire que :**
- $\mathbb{I}$ **est stable pour la première loi :**

$$(\boldsymbol{x}, \boldsymbol{y}) \in \mathbb{I}^{\mathbf{2}} \Rightarrow \boldsymbol{x} + \boldsymbol{y} \in \mathbb{I}$$

- $\mathbb{I}$ **est stable pour le passage à l'opposé :**

$$\boldsymbol{x} \in \mathbb{I} \Rightarrow -\boldsymbol{x} \in \mathbb{I}$$

b) $\mathbb{I}$ **est stable par opération avec la seconde loi sur un élément quelconque de** $\mathbb{A}$ **:**

$$(\boldsymbol{x}, \boldsymbol{y}) \in \mathbb{I} \times \mathbb{A} \Rightarrow \boldsymbol{x} * \boldsymbol{y} \in \mathbb{I}$$

Propriété des idéaux :

Si $\mathbb{I}$ et $\mathbb{J}$ sont deux idéaux d'un anneau commutatif $(\mathbb{A}, +, *)$ alors les sous ensembles $\mathbb{I} + \mathbb{J}$ et $\mathbb{I} \cap \mathbb{J}$ sont des idéaux de $\mathbb{A}$

Preuve :

Facile à faire et laissée au soin du lecteur

2) Les idéaux de $\mathbb{Z}$

Nous avons vu que les sous-ensembles $\mathbb{E}_{a,b}$ étaient des idéaux de $\mathbb{Z}$. Voyons plus précisément leur nature. Notons $d = a \wedge b$. Nous avons vu :

$$\exists\, (u,v) \in \mathbb{Z}^{\,2} :\ d = a\,u + b\,v$$

Donc : $d \in \mathbb{E}_{a,b}$

$\mathbb{E}_{a,b}$ étant un idéal, nous en déduisons :

$$\forall\, z \in \mathbb{Z}\ :\ d\,z\ \in \mathbb{E}_{a,b}$$

Donc , en notant $d\,\mathbb{Z}$ l'ensemble des multiples entiers relatifs de d :

$$d\,\mathbb{Z}\ \subset \mathbb{E}_{a,b}$$

Or nous avons également :

$$\exists\, (a',b') \in \mathbb{Z}^{\,2} :\ a = d\,a', b = d\,b'$$

Donc :

$$\forall\, (u,v) \in \mathbb{Z}^{\,2} :\ a\,u + b\,v = d\,a'\,u + d\,b'\,v = d\,(a'\,u + b'\,v)$$

Cela prouve que tout nombre de $\mathbb{E}_{a,b}$ est un multiple entier relatif de d et donc :

$$\mathbb{E}_{a,b} \subset d\,\mathbb{Z}$$

d'où l'égalité :

En résumé, nous avons montré :

$$\{a\,u + b\,v :\ (u,v) \in \mathbb{Z}^2\} = d\,\mathbb{Z}$$

Soit encore :

$$\boldsymbol{a}\,\mathbb{Z} + \boldsymbol{b}\,\mathbb{Z} = (\boldsymbol{a} \wedge \boldsymbol{b}\,)\mathbb{Z}$$

L'ensemble des nombres entiers relatifs qui sont la somme de multiples de deux nombres est un idéal qui est l'ensemble des multiples de leur PGCD

De façon plus générale , pour n entiers relatifs quelconques :

$$\boldsymbol{a_1}\,\mathbb{Z} + \boldsymbol{a_2}\,\mathbb{Z} + \cdots \boldsymbol{a_n}\,\mathbb{Z} = (\boldsymbol{a_1} \wedge\, \boldsymbol{a_2} \wedge \ldots \wedge\, \boldsymbol{a_n})\,\mathbb{Z}$$

La démonstration se décalque sur la précédente

Il est alors trivial de vérifier que tous les sous ensembles d'entiers relatifs qui sont de la forme $d\,\mathbb{Z}$, d étant un entier relatif quelconque, sont des idéaux. Se pose alors la question : sont ils les seuls ? La réponse est oui :

Les idéaux de $\mathbb{Z}$ sont les sous-ensembles de la forme $d\,\mathbb{Z}$, où d est un entier relatif quelconque.

Preuve :

Soit $\mathbb{I}$ un idéal de $\mathbb{Z}$, notons :

$$\mathbb{I}^+ = \mathbb{I} \cap \mathbb{N}^*$$

1er cas : $\mathbb{I} = \{0\}$

alors : $\mathbb{I} = 0\,\mathbb{Z}$

2ème cas : $\mathbb{I} \neq \{0\}$

Alors : $\mathbb{I}^+ \neq \emptyset$

$\mathbb{I}^+$ possède donc un plus petit élément d qui est un entier naturel non nul.

On a alors :

$$\forall\, z \in \mathbb{Z} : d\,z \in \mathbb{I}$$

Donc :

$$d\,\mathbb{Z} \subset \mathbb{I}$$

Soit alors $x \in \mathbb{I}$, la division euclidienne de $|x|$ par d donne :

$$\exists\, (q,r) \in \mathbb{Z}^2 : |x| = d\,q + r \ , \quad 0 \leq r < d$$

Supposons par l'absurde : $r \neq 0$ alors :

$$r = |x| - d\,q \in \mathbb{I}^+$$

$r < d$ fournit alors une contradiction.

Donc : $r = 0$ et donc :

$$|x| = d\,q$$

On en déduit que x est un multiple entier relatif de d et donc :

$$\mathbb{I} \subset d\,\mathbb{Z}$$

D'où l'égalité.

3) Idéaux intersections dans $\mathbb{Z}$

L'ensemble des nombres entiers relatifs qui sont multiples de deux nombres est un idéal qui est l'ensemble des multiples de leur PPCM

Soit mathématiquement :

$$\boldsymbol{a}\,\mathbb{Z} \cap \boldsymbol{b}\,\mathbb{Z} = (\boldsymbol{a} \vee \boldsymbol{b})\mathbb{Z}$$

Preuve :

Notons : $m = a \vee b$ alors :

$$\exists\,(a', b') \in \mathbb{Z}^2 : \; a\,a' = m \;\; , \qquad b\,b' = m$$

Donc :

$$\forall\, z \in \mathbb{Z} : m\,z = a\,a'z = b\,b'z$$

D'où : $z\,m \in a\,\mathbb{Z} \cap b\,\mathbb{Z}$ et donc :

$$m\,\mathbb{Z} \subset a\,\mathbb{Z} \cap b\,\mathbb{Z}$$

Soit alors : $x \in a\,\mathbb{Z} \cap b\,\mathbb{Z}$:

La division euclidienne de $|x|$ par m donne :

$$\exists\,(q, r) \in \mathbb{Z}^2 : \; |x| = m\,q + r \;\; , \quad 0 \leq r < m$$

Supposons par l'absurde : $r \neq 0$ alors $r = |x| - m\,q$ est un multiple commun à a et à b et c'est un entier naturel

$r < m$ fournit alors une contradiction.

Donc : $r = 0$ et donc :

$$|x| = m\,q$$

On en déduit que x est un multiple entier relatif de m et donc :

$$a\,\mathbb{Z} \cap b\,\mathbb{Z} \subset m\,\mathbb{Z}$$

D'où l'égalité.

De façon plus générale , pour n entiers relatifs quelconques :

$$\boldsymbol{a_1}\,\mathbb{Z} \cap \boldsymbol{a_2}\,\mathbb{Z} \cap \ldots \cap \boldsymbol{a_n}\,\mathbb{Z} = (\boldsymbol{a_1} \vee \boldsymbol{a_2} \vee \ldots \vee \boldsymbol{a_n})\,\mathbb{Z}$$

La démonstration se décalque sur la précédente

XI Arithmétique modulaire

1) Congruences - Définition

Etant donnés deux entiers relatifs a et b et un entier naturel n, on dit que a et b sont congrus modulo n si leur distance est un multiple de n, ce qui mathématiquement s'écrit :

$$a \equiv b \ [n] \ \Leftrightarrow \ \exists q \in \mathbb{Z} : a = b + q\,n$$

Un premier exemple simple avec la division euclidienne :

Si a et n sont deux entier naturels et n non nul alors, en notant r le reste de la division euclidienne de a par n nous avons : $a \equiv r \ [n]$

L'intérêt, comme nous le verrons dans les applications, est bien souvent de trouver le nombre congru le plus proche de 0. Ainsi :

En enlevant trois fois 5 à 13 :

$$13 \equiv -2 \ [5]$$

En enlevant deux fois 5 à 11 :

$$11 \equiv 1 \ [5]$$

2) Congruences-propriétés

Dans la suite a, b, c, d désignent des entiers relatifs quelconques et n un entier naturel

a) Produit par un entier :

$$a \equiv b \ [n] \ \Rightarrow a\,c \equiv b\ c\ [n]$$

Preuve :

Si $a \equiv b \ [n]$ alors : $\exists\, q \in \mathbb{Z} : a = b + q\,n$ donc : $a\,c = b\,c + (q\,c)\,n$ d'où : $a\,c \equiv b\ c\ [n]$

b) Somme

$$\left.\begin{matrix} \boldsymbol{a \equiv b} \ \ [\boldsymbol{n}] \\ \boldsymbol{c \equiv d} \ \ [\boldsymbol{n}] \end{matrix}\right\} \Rightarrow \boldsymbol{a + c \equiv b + d} \ \ [\boldsymbol{n}]$$

Preuve

Si $a \equiv b \ \ [n]$ et $c \equiv d \ \ [n]$ alors : $\exists\, (q, q') \in \mathbb{Z}^2 : a = b + q\, n$ et $c = d + q'\, n$ donc :

$$a + c = b + d + (q + q')\, n$$

Et donc :

$$a + c \equiv b + c \ \ [n]$$

c) Différence

$$\left.\begin{matrix} \boldsymbol{a \equiv b} \ \ [\boldsymbol{n}] \\ \boldsymbol{c \equiv d} \ \ [\boldsymbol{n}] \end{matrix}\right\} \Rightarrow \boldsymbol{a - c \equiv b - d} \ \ [\boldsymbol{n}]$$

Preuve

Il suffit de noter que $-c \equiv -d \ \ [n]$ et d'ajouter à $a \equiv b \ \ [n]$

d) Produit

$$\left.\begin{matrix} \boldsymbol{a \equiv b} \ \ [\boldsymbol{n}] \\ \boldsymbol{c \equiv d} \ \ [\boldsymbol{n}] \end{matrix}\right\} \Rightarrow \boldsymbol{a\, c \equiv b\, d} \ \ [\boldsymbol{n}]$$

Preuve

Si $a \equiv b \ \ [n]$ et $c \equiv d \ \ [n]$ alors : $\exists\, (q, q') \in \mathbb{Z}^2 : a = b + q\, n$ et $c = d + q'\, n$ donc :

$$a\, c = b\, d + (d\, q + b\, q' + q\, q')\, n$$

Et donc :

$$a\, c \equiv b\, d \ \ [n]$$

e) Puissance

$$\forall\, \boldsymbol{m} \in \mathbb{N} : \ \ \boldsymbol{a \equiv b} \ \ [\boldsymbol{n}] \ \Rightarrow \boldsymbol{a^m \equiv b^m} \ \ [\boldsymbol{n}]$$

Preuve :

Par récurrence évidente sur m en se servant de la propriété produit.

Toutes les propriétés présentées sont des implications et non des équivalences. Des exemples simples permettent de s'en convaincre, par exemple pour la première :

$2 \times 3 \equiv 2 \times 4 \ [2]$ mais $3 \not\equiv 2 \ [2]$

3) Exemple d'application

Sot à déterminer le reste de la division de 37^{14} par 13 en faisant le moins de calculs possibles :

En enlevant trois fois 13 :

$$37 \equiv -2 \ [13]$$

Donc :

$$37^{14} \equiv (-2)^{14} \ [13]$$

Mais :

$$(-2)^{14} = 2^{2\times 7} = (2^7)^2 = 128^2$$

Or en enlevant dix fois 13 à 128 :

$$128 \equiv -2 \ [13]$$

Donc :

$$128^2 \equiv (-2)^2 \ [13]$$

Finalement :

$$37^{14} \equiv 4 \ [13]$$

Donc :

$$\exists\, q \in \mathbb{Z} \ : \ 37^{14} = 13\, q + 4$$

L'unicité du couple quotient –reste dans la division euclidienne prouve que le reste de la division de 37^{14} par 13 est 4.

4) Le théorème de Fermat

Si p est un nombre premier et a un entier relatif non divisible par p donc premier avec p, alors :

$$\boldsymbol{a^{p-1} \equiv 1 \ [p]}$$

Et donc :

$$\boldsymbol{a^{p} \equiv a \ [p]}$$

Preuve

Notons r_1 , r_2 , … , r_{p-1} les restes respectivement de $1\ a$, $2\ a$, … , $(p-1\ )a$

Montrons d'abord qu'aucun de ces restes n'est nul par l'absurde.

Soit $k \in [\![1; p-1]\!]$, supposons : $\exists\ q \in \mathbb{N}$: $k\ a = q\ p$ alors p divise $k\ a$ mais puisque p est premier avec a, p divise k, ce qui est absurde car $k < p$

Montrons ensuite que ces restes sont deux à deux distincts, encore par l'absurde :

Soit $(k, k') \in [\![1; p-1]\!]^2$, supposons $r_k = r_k$, alors $k\ a \equiv k' a\ \ [p]$ donc :

$\exists\ q \in \mathbb{Z}$: $(k-k')a = q\ p$ d'où : $\exists\ q' \in \mathbb{N}$: $|k-k'|a = q'\ p$

En notant : $k" = |k-k'|$, $k" \in [\![1; p-1]\!]$ et $k"\ a = q'\ p$, d'après ce qui précède : $k" = 0$ d'où :

$$k = k'$$

La contraposée de ce que nous avons montré est :

$$\forall\ (k, k') \in [\![1; p-1]\!]^2\ :\ k \neq k' \Rightarrow r_k \neq r_{k'}$$

Ce qui prouve que les restes sont deux à deux distincts.

Or nous avons :

$$1\ a \equiv r_1\ \ [p]$$

$$2\ a \equiv r_2\ \ [p]$$

$$\vdots$$

$$(p-1)\ a \equiv r_{p-1}\ \ [p]$$

Soit par produit :

$$1\ a \times 2\ a \times \ldots \times (p-1)\ a \equiv r_1 \times r_2 \times \ldots \times r_{p-1}\ \ [p]$$

Mais l'ensemble formé par les restes étant le même que celui formé par les entiers de $[\![1; p-1]\!]$, nous avons :

$$(p-1)!\ a^{p-1} \equiv (p-1)!\ \ [p]$$

On en déduit :

$$\exists\ q \in \mathbb{Z}$: $(p-1)!\ a^{p-1} - (p-1)!\ = q\ p$$

p divise donc le nombre :

$$(p-1)!\ a^{p-1} - (p-1)! = (p-1)!\ (a^{p-1} - 1\ )$$

Or p est premier avec chacun des facteurs de $(p-1)!$ donc avec $(p-1)!$

On en déduit que p divise le nombre $a^{p-1} - 1$ et donc

$$a^{p-1} - 1 \equiv 0 \ \ [p]$$

Soit

$$a^{p-1} \equiv 1 \ \ [p]$$

Puis par multiplication par p :

$$a^p \equiv a \ \ [p]$$

Exemple concret :

$$75^{37} \equiv 75 \ \ [37] \equiv 1 \ \ [37]$$

Donc le reste de la division de 75^{37} par 37 est 1