

CHAPITRE 2

ARITHMÉTIQUE

2.1. Rappel sur le principe de raisonnement par récurrence

Suite au chapitre 0 (Cours Préliminaire Intensif), nous allons compléter les raisonnements de logique par le raisonnement par récurrence.

Soit P_n une proposition qui dépend d'un entier n et soit n_0 un entier fixe.

Principe

Si la propriété $P(n_0)$ est vraie et si l'implication $P(n) \Rightarrow P(n+1)$ est vraie pour $n \geq n_0$

Alors la propriété $P(n)$ est vraie pour tout entier $n \geq n_0$

Méthodologie

On effectue deux étapes successives.

1^{er} Étape : Initialisation

On commence par vérifier que $P(n_0)$ est vraie

2^{ème} Étape : Hérédité

Ensuite, on montre que si $P(n)$ est vraie alors $P(n+1)$ est vraie.

Exemple pratique

1) Démontrer par récurrence que pour tout n entier naturel on a : $2^n \geq n + 1$

2) Montrer par récurrence que pour tout entier naturel non nul $(1 + 2 + \dots + n)^2 = 1^3 + 2^3 + \dots + n^3$

Méthode

1)

On désigne par P_n la proposition $2^n \geq n + 1$

Initialisation

- Pour $n = 0$
 $2^n = 2^0 = 1$ et $n + 1 = 0 + 1 = 1$

On a bien $1 \geq 1$

Alors la proposition P_n est vraie pour $n = 0$ (à l'ordre 0)

- Pour $n = 1$ on a $2^n = 2^1 = 2$ et $n + 1 = 1 + 1 = 2$
 $2 \geq 2$

Alors P_n est vraie à l'ordre 1

Hérédité

On suppose que la proposition P_n ($2^n \geq n + 1$) est vraie à l'ordre n (pour n fixé) c'est-à-dire $2^n \geq n + 1$

On cherche à démontrer que P_{n+1} est vraie autrement dit $2^{n+1} \geq (n + 1) + 1$ ou que $2^{n+1} \geq n + 2 \Rightarrow 2^{n+1} - n - 2 \geq 0$

P_n étant vraie $\Rightarrow 2^n \geq n + 1$

En multipliant l'inégalité par 2 on aura $2 \cdot 2^n \geq 2(n + 1)$

$2^{n+1} \geq 2n + 2$ en additionnant $-(n + 2)$, on aura

$$2^{n+1} - (n + 2) \geq 2n + 2 - (n + 2)$$

$$2^{n+1} - n - 2 \geq 2n - n - 2$$

$$2^{n+1} - n - 2 \geq n$$

$n \in \mathbb{N}$ C'est-à-dire que $0 \leq n \leq k$

On a : alors $2^{n+1} - n - 2 \geq n \geq 0$ Alors

$$2^{n+1} - n - 2 \geq 0 \Rightarrow 2^{n+1} \geq n + 2 \Rightarrow 2^{n+1} \geq (n + 1) + 1$$

Par suite P_{n+1} est vraie

On a : P_{n_0} vraie, P_n vraie, P_{n+1} vraie. Alors pour tout $n \in \mathbb{N}$

$$2^n \geq n + 1$$

2.2. Rappel sur les ensembles $\mathbb{N}$ et $\mathbb{Z}$ et Lois de composition internes

L'ensemble des nombres naturels est tel que

$\mathbb{N} = \{0, 1, 2, 3, 4, \dots\}$ et l'ensemble des entiers relatifs est tel que

$$\mathbb{Z} = \{\dots - 4, -3, -2, -1, 0, 1, 2, 3, 4, \dots\}$$

$\mathbb{N}$ est bien une partie de $\mathbb{Z}$

Lois de composition interne

Nous allons faire un cas général, le cas particulier peut être appliqué à l'addition et à la multiplication. Nous y ferons un accès lors de l'exposé du chapitre.

a) Définition

Étant donné un ensemble E non vide. Une loi interne T sur E est une application de $E \times E$ vers E qui à tout couple $(a; b)$ de $E \times E$ associe un élément c de E et on note aTb (Test un symbole appelé truc). Une loi de composition interne T possède les propriétés suivantes :

b) Associativité

La loi T est associative si $\forall a, b$ et $c \in E$

$$(aTb)Tc = aT(bTc)$$

c) Commutativité

La loi T est commutative si pour tout a et $b \in E$

$$aTb = bTa$$

d) Élément neutre

La loi T admet un élément neutre e si pour tout $a \in E$

$$aTe = eTa = a$$

e) Inverse

Si e est l'élément neutre de T , alors l'élément $a \in E$ admet un inverse (ou symétrique) noté $b \in E$ si $aTb = bTa = e$

f) Distributivité

La loi de composition x est distributive par rapport à T si pour tous a, b , et $c \in E$

$$ax(bTc) = (axb)T(axc)$$

g) Régularité

Pour tout $a, b, c \in E$

$$aTb = aTc \Rightarrow b = c$$

$$bTa = cTa \Rightarrow b = c$$

Soit T une loi de composition interne l'élément $a \in E$ est régulier pour T dans E si $\rightarrow$

h) Absorbance

Soit T une loi interne de E . Si pour $a \in E$

on a : $ax0 = 0xa = 0$, alors l'élément a est absorbant.

Remarque

Dans $\mathbb{N}$ l'addition (+) et la multiplication ($\times$) sont des lois de composition interne (associative, commutative et admet 0 ou 1 pour élément neutre). C'est-à-dire on remplace T par + ou $\times$ pour la vérification

Dans $\mathbb{N}$ ou dans $\mathbb{Z}$ la multiplication est associative, commutative et a pour élément neutre 1

Dans $\mathbb{N}$ et $\mathbb{Z}$ la multiplication est distributive par rapport à l'addition.

2.3. Groupes et sous groupes

1) Soit G un ensemble non vide muni d'une loi de composition interne T . (G, T) est un groupe si T est associative, possède un élément neutre et si tout élément de G est inversible.

Si de plus la loi T est commutatif alors on dit que (G, T) est un groupe commutatif ou abélien.

2) (G, T) est un groupe et H est un sous – ensemble non vide de G . si (H, T) est lui – même un groupe, alors il est appelé sous – groupe de (G, T) .

2.4. Caractères de divisibilités**a) Divisibilité par 2 et par 5****Théorème**

Étant donné un nombre a . Le nombre a est divisible par 2 (respectivement par 5) si le dernier chiffre des unités est divisible par 2 (respectivement par 5)

Exemple pratique

Vérifier la divisibilité respectivement par 2 et par 5 des réels 786 et 510.

Méthode

Pour 786 le dernier chiffres des unités est 6 et 6 est divisible par 2 alors 786 est divisible par 2

De même 510 a pour dernier chiffre d'unité 0 et 0 est divisible par 5 alors 510 est bien divisible par 5.

b) Divisible par 3 et par 9**Théorème**

Un nombre est divisible par 3 (respectivement par 9) si la somme de ses chiffres est divisible par 3 (respectivement la somme de ses chiffres est divisible par 9).

Exemple pratique

Vérifier la divisibilité de 522 et de 1821 par 3.

c) Divisibilité par 7

Un nombre est divisible par 7 si la différence entre le nombre des dizaines et le double du chiffre des unités est divisible par 7.

Exemple pratique

Montrer que 371 est divisible par 7.

d) Divisibilité par 11**Théorème**

Un nombre est divisible par 11, si la différence de la somme de ses chiffres de rang pair et la somme de ses chiffres de rang impair est divisible par 11.

Exemple pratique

Les nombres 45 et 132 sont – ils divisibles par 11.

e) Divisibilité par 4 et par 25

Théorème

Un nombre est divisible par 4 (respectivement par 25) si le nombre formé par les deux derniers chiffres est divisible par 4 (respectivement par 25)

Exemple pratique

Vérifier la divisibilité par 4 du réel 92 puis la divisibilité par 25 du réel 350.

2.5. Divisibilité**a) Définition**

Étant donnés deux entiers relatifs a et b tels qu'il existe un entier relatif k tel que $a = kb$

Alors on dit que $\begin{cases} b \text{ divise } a \\ b \text{ est un diviseur de } a \\ a \text{ est un multiple de } b \end{cases}$

On note b/a

Exemple

Soit l'égalité $21 = 7 \times 3$. Alors 3 est un diviseur de 21, de même 7 est un diviseur de 21. Alors 3 et 7 divisent 21

21 est un multiple de 7 et de 3 (l'ensemble des multiples de 7 et 3 sont respectivement de la forme $7k$ et $3k$ avec $k \in \mathbb{Z}$, et on note souvent $7\mathbb{Z}$ et $3\mathbb{Z}$).

b) Quelques propriétés de la divisibilité

a) Si a divise b et que b divise a , alors a et b sont tous égaux ou opposés

b) Si a divise b et b divise c alors a divise c

c) Si c divise a et c divise b , alors c divise toute combinaison linéaire de a et b de la forme $au + bv$ avec u et $v \in \mathbb{Z}$

d) a et $-a$ ont les mêmes diviseurs

e) 1 et -1 sont des diviseurs de tout entier relatif

f) 0 est un multiple de tout entier relatif

g) Étant donnés 2 entiers relatifs a et b ; si a divise b et si $b \neq 0$ alors $|a| \leq |b|$

h) Si a est un entier relatif non nul alors a possède un nombre fini de diviseurs.

i) Étant donnés $a, b, c \in \mathbb{Z}$

- Si a divise b alors a divise bc
- Si a divise b et si a divise c alors a divise $b + c$ et a divise $b - c$

Exemple d'application

Trouver les diviseurs de 30

$30 = 2 \times 15 = 6 \times 5 = 3 \times 10 = 30 \times 1$ Alors les diviseurs de 30 sont : 2, 5, 3, 15, 6, 10, 30 et 1.

c) Division euclidienne

Puisque $\mathbb{N} \subset \mathbb{Z}$ nous nous intéressons à la division euclidienne dans $\mathbb{N}$ puis dans $\mathbb{Z}$

i) Division euclidienne dans $\mathbb{N}$

Étant donnés a et b 2 entiers naturels avec $b \neq 0$, on peut trouver un couple unique (q, r) de $\mathbb{N}^2$ tel que $a = bq + r$ avec $R < b$

a se nomme le dividende, b le diviseur, q le quotient et r le reste. Le couple (q, r) est le résultat de la division euclidienne de a par b .

Cas particulier

- Si $r \neq 0$ on dit que a n'est pas divisible par b
- Si $r = 0$, on dit que a est divisible par b .

Exemple d'application

$$\begin{array}{r|l} 29 & 7 \\ \hline 1 & 4 \end{array}$$

$q = 4$ et $r = 1$

$$\begin{array}{r|l} 42 & 6 \\ \hline 0 & 7 \end{array}$$

$q = 7$ et $r = 0$

ii) Division euclidienne dans $\mathbb{Z}$

Étant donnés deux entiers relatifs avec $b \neq 0$. Alors il existe un et un seul couple $(q, r) \in \mathbb{Z}^2$ tel que $a = bq + r$

et $0 \leq r < |b|$ avec q et r respectivement le quotient et le reste de la division euclidienne de a par b .

Exemple pratique

$$\begin{array}{r|l} -14 & 3 \\ \hline 1 & -5 \end{array}$$

On a : $-14 = 3 \times (-5) + 1$ et $0 \leq 1 < 3$

2.6. Notation de congruence modulo

a) Définition

Étant donnés $k \in \mathbb{N}$ et α, β deux entiers relatifs.
On dit que α est congru à β modulo k et on note

$\alpha \equiv \beta [\text{modulo } k]$ ou simplement $\alpha \equiv \beta [k]$, si α et β ont le même reste dans la division euclidienne par k

Exemple

$20 \equiv 38[3]$ c'est-à-dire 20 et 38 ont tous 2 comme reste de la division par 3

$$\begin{array}{r|l} 20 & 3 \\ \hline & 6 \\ \hline \end{array} \quad \begin{array}{r|l} 38 & 3 \\ \hline & 12 \\ \hline \end{array}$$

b) Propriétés de la congruence

Étant donnés $k \in \mathbb{N}$ et α, β et $\gamma \in \mathbb{Z}$

- $\alpha \equiv \beta [k] \Leftrightarrow \beta - \alpha$ est un multiple de k
- Si $\alpha \equiv \beta [k]$ et si $\beta \equiv \gamma [k]$ alors $\alpha \equiv \gamma [k]$
- Si $\alpha \equiv \beta [k]$ et si $\alpha' \equiv \beta' [k]$ alors
 $\alpha + \alpha' \equiv \beta + \beta' [k]$
 $\alpha\alpha' \equiv \beta\beta' [k]$ et $\alpha - \alpha' \equiv \beta - \beta' [k]$
- $\alpha^n \equiv \beta^n [k]$ pour $n \in \mathbb{N}^*$
- Si $\alpha \equiv \beta [k]$ alors $\forall \gamma \in \mathbb{Z}$
 $\alpha + \gamma \equiv \beta + \gamma [k]$
 $\alpha - \delta \equiv \beta - \gamma [k]$ et $\alpha\gamma \equiv \beta\gamma [k]$
- $\alpha \equiv \beta [k] \Leftrightarrow \beta \equiv \alpha [k]$
- $\alpha \equiv 0 [k] \Leftrightarrow \alpha$ est divisible par k
- Si $\alpha \equiv \beta [k]$ et si $0 \leq \beta < k$ alors β est le reste de la division euclidienne de α par k
- Si r est le reste de la division euclidienne de α par β
alors $\begin{cases} r \equiv \alpha [\beta] \\ 0 \leq r < |\beta| \end{cases}$

c) Calcul du reste de la division euclidienne à l'aide de la congruence**Exemple pratique 1**

Déterminer le reste de la division euclidienne de 2009^{2009} par 5

Méthode

On a : $2009 \equiv -1[5]$

Car $2009 + 1 = 2010$ qui est divisible par 5 donc
 $2009^{2009} \equiv (-1)^{2009}[5]$ soit $2009^{2009} \equiv -1[5]$ et

$-1 \equiv 4[5]$ alors $2009^{2009} \equiv 4[5]$

On a bien $0 \leq 4 < 5$ alors le reste de la division euclidienne de 2009^{2009} par 5 est 4.

Exemple pratique 2

Soit n un entier naturel. Démontrer que $n(n^4 - 1)$ est divisible par 5

2.7. Système de numération

Dans la numération on utilise les chiffres de 0 à 9 pour écrire tous les nombres dans le système décimal.

Par exemple les enfants ont amené deux cent quatre vingt trois oiseaux.

Deux cent quatre vingt trois oiseaux peut s'écrire en chiffre 283, qui peut être décomposé ainsi :

$$283 = 200 + 80 + 3 = 2 \times 100 + 8 \times 10 + 3$$

On sait que $100 = 10^2$ alors $283 = 2 \times 10^2 + 8 \times 10 + 3 \times 1$ et on sait que $10^0 = 1$ par suite $283 = 2 \times 10^2 + 8 \times 10^1 + 3 \times 10^0$

On a pu décomposer 283 en une somme de puissance de 10. On a le théorème suivant :

a) Théorème de décomposition

Étant donné un entier $\beta \in \mathbb{N}^*$. Pour tout $a \in \mathbb{N}$, on peut confirmer l'existence d'une suite $\alpha_0, \alpha_1, \alpha_2, \dots, \alpha_n$ et une seule appartenant à $\mathbb{N}$ vérifiant les conditions suivantes :

- 1) Pour tout i tel que $0 \leq i \leq n-1$, $0 \leq \alpha_i < \beta$
- 2) Pour tout i tel que $0 \leq i \leq n-1$, $0 \leq \alpha_n < \beta$
- 3) a peut s'écrire $a = \alpha_0 + \alpha_1\beta + \alpha_2\beta^2 + \dots + \alpha_n\beta^n$

Exemple pratique

Décomposer le nombre 25

Méthode

$$25 = 20 + 5$$

$$25 = 2 \times 10 + 5 \times 1 = 2 \times 10^1 + 5 \times 10^0$$

b) Notation de base**Définition**

On nomme base, le nombre de chiffres nécessaires dans un système de numération pour exprimer tout nombre dans cette base.

Nous venons d'écrire le nombre a tel que

$$a = \alpha_0 + \alpha_1\beta + \alpha_2\beta^2 + \dots + \alpha_n\beta^n$$

La suite d'entiers $(\alpha_0, \alpha_1, \dots, \alpha_n)$ existe et est unique on peut écrire :

$$a = \overline{\alpha_n \alpha_{n-1} \alpha_{n-2} \dots \alpha_1 \alpha_0}^\beta$$

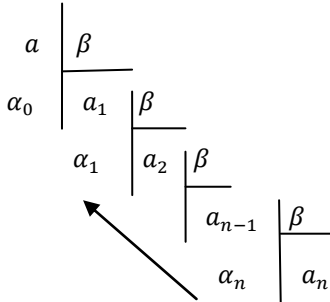
Cette écriture se nomme écriture du nombre a en base β .

Et la lecture est telle que $\alpha_n \alpha_{n-1} \alpha_{n-2} \dots \alpha_1 \alpha_0$

c) Méthode théorique de détermination de la suite d'entier
 $(\alpha_0, \alpha_1, \dots, \alpha_n)$

Déterminer la suite associée au nombre a dans la base β

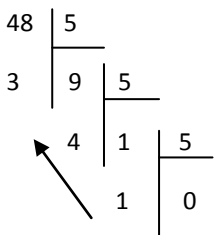
On procède ainsi par la disposition pratique suivante



Alors on écrit $a = \overline{\alpha_n \dots \alpha_0}^\beta$

Exemple pratique

Écrire le nombre 48 dans la base 5



On a $\alpha_0 = 3, \alpha_1 = 4$ et $\alpha_2 = 1$ alors $48 = \alpha_2 \alpha_1 \alpha_0$ soit $48 = \overline{143}^5$

Remarque

On doit effectuer la division euclidienne jusqu'à obtenu un reste nul.

Jusque là nous opérons dans un système de numération appelé « système de **numération décimale** ».

Il existe d'autres systèmes de numération tels que : la **numération binaire** (couramment appelé en base 2), utilisant les chiffres 0 et 1 uniquement est beaucoup pratique en informatique et en électronique. Dans ce système, tout nombre se décompose en une puissance de 2 contrairement à la numération décimale dans laquelle, tout nombre se décompose en une puissance de 10.

La **numération hexadécimale** (ou numération de base 16) utilise 16 caractères qui sont : les chiffres de 0 à 9 et les lettres de A à F c'est-à-dire 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, A, B, C, D, E, F. Dans la numération hexadécimale, tout nombre se décompose suivant une puissance de 16.

Le système de **numération octet** est peu utilisé. Dans ce système les chiffres utilisés sont : de 0 à 7.

Exemple pratique

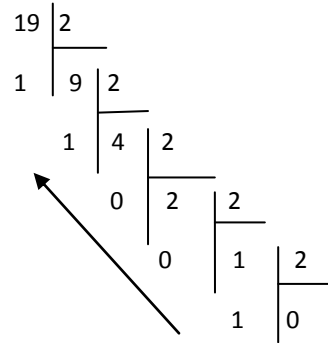
1) Écrire le nombre réel 19 en système binaire.

2) Écrire le nombre 3234 en numération hexadécimale.

Méthode

1) Écrivons le nombre 19 en système binaire.

Le système binaire est la base 2. On effectue la division de 19 par 2, puis la division du quotient obtenu par 2, puis à nouveau jusqu'à obtenir un reste ou un quotient nul. On s'intéresse aux restes en remontent.

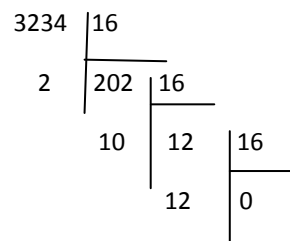


Alors on aura $19 = \overline{10011}^2$

Autre méthode

$$19 = 1 \times 2^4 + 0 \times 10^3 + 0 \times 10^2 + 0 \times 10^1 + 1 \times 10^0$$

2) Écrivons le nombre 3234 en base 16



$3234 = \overline{12102}^{16}$

Remarque

En base hexadécimale :

- le chiffre 10 représente la lettre A
- le chiffre 11 représente la lettre B
- le chiffre 12 représente la lettre C
- le chiffre 13 représente la lettre D
- le chiffre 14 représente la lettre la lettre E
- et le chiffre 15 représente la lettre F.

Ainsi le nombre 3234 s'écrit dans la base 16

$$3234 = \overline{12102}^{16} \text{ soit } 3234 = \overline{CA2}^{16}$$

d) Comment passer du système décimal au système binaire ou hexadécimal et vice versa

Exemple pratique 1

1) Écrire en base 2 le nombre 23

2) Écrire en base 16 le nombre entier 312

Méthode

1) Écrivons en base 2 (binaire) le nombre 23
on a

$$\begin{array}{r}
 23 \mid 2 \\
 1 \mid 11 \mid 2 \\
 \quad 1 \mid 5 \mid 2 \\
 \quad \quad 1 \mid 2 \mid 2 \\
 \quad \quad \quad 0 \mid 1 \mid 2 \\
 \quad \quad \quad \quad 1 \mid 0
 \end{array}$$

Alors on a $23 = \overline{10111}^2$

2) Écrivons 312 en hexadécimal (ou base 16)

$$\begin{array}{r}
 312 \mid 16 \\
 8 \mid 19 \mid 16 \\
 \quad 3 \mid 1 \mid 16 \\
 \quad \quad 1 \mid 0
 \end{array}$$

$312 = \overline{138}^{16}$

Exemple pratique 2

Écrire les nombres suivants dans le système décimal

a) $\overline{10111}^2$ b) $\overline{138}^{16}$

Solution

Écrivons en système décimal les nombres suivants

a) $\overline{10111}^2 = 1x2^4 - 0x2^3 + 1x2^2 + 1x2^1 + 1x2^0$

$\overline{1011}^2 = 16 + 0 + 4 + 2 + 1$, soit $\overline{1011}^2 = 23$

On a procédé ainsi $\overline{10111}^2$ on a $n = 5$ chiffre (1,0,1,1,1) qui représente les suites de nombre associés et la base utilisée 2

La plus grande puissance serait $n - 1$ soit $5 - 1 = 4$
Alors $\overline{10111}^2 = 1x2^4 + 0x2^3 + 1x2^2 + 1x2^1 + 1x2^0$

D'où $\overline{10111}^2 = 23$

b) $\overline{138}^{16} = 1x16^2 + 3x16^1 + 8x16^0$

$\overline{138}^{16} = 256 + 48 + 8$

$\overline{138}^{16} = 312$

2.8. Multiples et ensemble des multiples d'un entier relatif

Soit l'opération

$$\begin{array}{r}
 40 \mid 5 \\
 0 \mid 8
 \end{array}$$

On peut écrire que $40 = 5 \times 8$.

Alors 40 est appelé un multiple de 5 et également un multiple de 8

a) Résumé

Étant donné un entier β . l'entier α est appelé un multiple de α si et seulement si, il existe un nombre entier k tel que $\alpha = k\beta$

Par exemple certains multiples du nombre entier 3 sont :

$$3 \times 0 = 0$$

$$3 \times 1 = 3$$

$$3 \times 2 = 6$$

$$3 \times 3 = 9$$

$$3 \times 4 = 12$$

etc.....

C'est-à-dire de la forme $3k$ avec $k \in \mathbb{Z}$.

Les entiers 0, 3, 6, 9, 12, etc... sont les multiples de 3 appelés ensemble des multiples de 3.

b) Généralisation

Soit α un entier relatif. L'ensemble des multiples de α sont de la forme $k\alpha$ avec $k \in \mathbb{Z}$ c'est-à-dire $\{\dots, -3\alpha, -2\alpha, -\alpha, 0, \alpha, 2\alpha, 3\alpha, \dots\}$

On note $\alpha\mathbb{Z}$ l'ensemble des multiples de α et on a plus généralement : $\alpha\mathbb{Z} = \{\beta \in \mathbb{Z} / \exists k \in \mathbb{Z}, \beta = \alpha k\}$

Remarque

- ✓ 0 est multiple de tous les nombres
- ✓ L'entier α est un multiple de l'entier β (avec β non nul) si β/α c'est-à-dire que le reste de la division de α par β est nul
- ✓ Si $m \in \mathbb{N}$ alors 2 divise $m(m+1)$ c'est-à-dire que $m(m+1)$ est un multiple de 2

c) Propriétés du multiple et de l'ensemble multiples

- Pour tout $\alpha \in \mathbb{Z}$ $\alpha\mathbb{Z} \neq \emptyset$
- Pour tout α_1 et $\alpha_2 \in \mathbb{Z}$

On a $\alpha_1 + \alpha_2 \in \alpha\mathbb{Z}$ et $\alpha_1 - \alpha_2 \in \alpha\mathbb{Z}$

- Pour tous α et $\beta \in \mathbb{Z}$
si $\alpha = \beta$ alors $\alpha\mathbb{Z} = \beta\mathbb{Z}$
si $\alpha = -\beta$ alors $\alpha\mathbb{Z} = \beta\mathbb{Z}$ c'est-à-dire que $\alpha\mathbb{Z} = \beta\mathbb{Z}$ ssi $\alpha = \beta$ ou $\alpha = -\beta$

- Pour tous α et $\beta \in \mathbb{Z}$ si α est un multiple de β alors $\alpha\mathbb{Z} \subset \beta\mathbb{Z}$
- Pour tout m et $\alpha \in \mathbb{Z}$ si $m \in \alpha\mathbb{Z} \Leftrightarrow -m \in \alpha\mathbb{Z}$

Exemple pratique

Trouver l'ensemble des multiples de 8

Méthode

Trouvons l'ensemble des multiples de 8
L'ensemble des multiples de 8 est de la forme

$$8\mathbb{Z} = \{x \in \mathbb{Z} / \exists k \in \mathbb{Z}, x = 8k\}$$

$$\mathbb{Z} = \{\dots -4, -3, -2, -1, 0, 1, 2, 3, 4, \dots\}$$

$$\text{Alors } 8\mathbb{Z} = \{\dots, -32, -24, -16, -8, 0, 8, 16, 24, 32, \dots\}$$

2.9. Diviseurs et ensemble des diviseurs d'un entier relatif

Soit l'opération

$$\begin{array}{r|l} 48 & 6 \\ \hline 0 & 8 \end{array}$$

On a alors $48 = 6 \times 8$

6 est un diviseur de 48 de même 8 est également un diviseur de 48. On dit que 6 et 8 divisent 48.

a) Définition

Étant donné α un entier relatif. L'entier relatif non nul β est un diviseur de α (ou que β divise α ou que α est divisible par β) s'il existe un entier relatif k tel que $\alpha = k\beta$.
Autrement dit β est un diviseur de α si α est un multiple de β .

Dans ce qui précède on a trouvé

$$48 = 6 \times 8$$

$$48 = 4 \times 12$$

$$48 = 3 \times 16$$

$$48 = 2 \times 24 \text{ etc.}$$

Les entiers 6, 8, 4, 12, 3, 16, 2, 24, ... sont appelés l'ensemble des diviseurs de 48

b) Généralisation

Soit $\alpha \in \mathbb{Z}$, l'ensemble des diviseurs de α est noté D_α et est tel que $D_\alpha = \{-|\alpha|, \dots, -1, 1, \dots, |\alpha|\}$.

c) Note

α est tel que si $\beta \in \mathbb{Z}^*$ divise α alors il existe un entier relatif k tel que $\alpha = k\beta$ alors $|\alpha| = |k\beta|$ ainsi :

$$D_\alpha = \{-|k\beta|, \dots, -1, 1, \dots, |k\beta|\} \text{ avec } k \in \mathbb{Z} \text{ et } \beta \text{ un diviseur de } \alpha$$

Exemple pratique

Déterminer l'ensemble des diviseurs de 32

Méthode

Déterminerons l'ensemble des diviseurs de 32

On sait que

$$32 = 2 \times 16$$

$$32 = 4 \times 8$$

$$32 = 1 \times 32$$

Alors les diviseurs positifs sont 1, 2, 4, 8, 16, 32

L'ensemble des diviseurs de 32 sont :

$$D_{32} = \{-32, -16, -8, -4, -2, -1, 1, 2, 4, 8, 16, 32\}$$

2.10. Propriétés de la divisibilité

Nota bene

Toutes les démonstrations ou preuves du cours sont renvoyées aux Travaux Encadrés(Exercices).

Néanmoins voici comment se passe quelques démonstrations pour les propriétés suivantes.

- Étant donnés α, β, γ trois entiers relatifs, si α divise β alors pour tout entier relatif δ , α divise $\beta\gamma$

Preuve

α divise β alors $\exists k \in \mathbb{Z}$ tel que $\beta = k\alpha$

En multipliant par γ

$$\beta\alpha = k\alpha\gamma \Rightarrow \beta\gamma = \alpha(k\gamma), \text{ c'est-à-dire que } \alpha \text{ divise } \beta\gamma$$

- Étant donnés α, β, γ , trois entiers relatifs
Si α divise β alors $\alpha\gamma$ divise $\beta\gamma$

Preuve

α divise $\beta \Leftrightarrow \beta$ peut s'écrire $\beta = k\alpha$ pour $k \in \mathbb{Z} \Leftrightarrow$

$$\beta\alpha = \alpha\beta\gamma = (\alpha\gamma)k \Leftrightarrow \alpha\gamma \text{ divise } \beta\gamma$$

- Étant donnés $\alpha, \beta, \gamma \in \mathbb{Z}$

Si α divise β et que α divise γ alors pour tous a et $b \in \mathbb{Z}$

α divise $a\beta + b\gamma$.

Autrement dit si α divise β et γ alors α divise également toute combinaisons linéaire entre β et γ (c'est-à-dire la somme et la différence de β et γ)

Preuve

$$\alpha \text{ divise } \beta \Leftrightarrow \beta = k\alpha$$

$$\alpha \text{ divise } \gamma \Leftrightarrow \gamma = k'\alpha$$

Pour tous a et $b \in \mathbb{Z}$

$$\begin{cases} a\beta = ak\alpha \\ b\gamma = bk'\alpha \end{cases}$$

$$a\beta + b\gamma = ak\alpha + bk'\alpha$$

$$a\beta + b\gamma = \alpha(ak + bk') \text{ alors } \alpha \text{ divise } a\beta + b\gamma$$

- Étant donnés α et $\beta \in \mathbb{Z}$ si α divise β et que β divise α alors soit $a = b$ ou $a = -b$

Preuve

$$\alpha \text{ divise } \beta \text{ alors } |\alpha| \leq |\beta|$$

$$\beta \text{ divise } \alpha \text{ alors } |\beta| \leq |\alpha| \text{ alors on a } |\alpha| = |\beta| \text{ alors } \begin{cases} \alpha = \beta \\ \text{ou} \\ \alpha = -\beta \end{cases}$$

- Étant donnés deux entiers relatifs α et β , si β divise α on a : $|\beta| \leq |\alpha|$ avec $\alpha \neq 0$

Preuve

$$\beta/a, \text{ on a alors } \alpha = k\beta$$

$$\text{Alors } |\alpha| = |\alpha\beta| = |\alpha||\beta|$$

Puis que $\alpha \neq 0$ par suite $|k| \in \{1, 2, \dots\}$ alors on a bien $|\alpha| \geq |\beta|$ soit $|\beta| \leq |\alpha|$

- Étant donnés α et $\beta \in \mathbb{Z}$ si β divise α alors $-\beta$ divise α

Preuve

$$\beta/\alpha \text{ alors } \exists k \in \mathbb{Z} \text{ tel que } \alpha = k\beta.$$

$$\text{Don } \alpha = (-k)(-b) \text{ avec } -k \in \mathbb{Z}$$

$$\text{Soit } \alpha = -\beta.(-k) \text{ alors } -\beta \text{ divise } \alpha$$

- pour tout $\alpha \in \mathbb{Z}$ α divise α (la réflexivité de la relation de divisibilité).

Preuve

$$a = a \times 1 \text{ Alors } a \text{ divise } a$$

- Pour tous $\alpha, \beta, \gamma \in \mathbb{Z}$. Si α divise β et β divise γ alors α divise γ (la transitivité de la relation de divisibilité).

Preuve

$$\frac{\alpha}{\beta} \Leftrightarrow \exists k \in \mathbb{Z} \text{ tel que } \beta = k\alpha$$

$$\beta/\gamma \Leftrightarrow \exists k' \in \mathbb{Z} \text{ tel que } \gamma = k'\beta$$

$$\text{On a } \gamma = k'\beta = k'(k\alpha) = kk'\alpha$$

$$\gamma = (kk')\alpha, \text{ c'est-à-dire } \alpha \text{ divise } \gamma$$

Remarque

Pour tout $\alpha \in \mathbb{Z}$

1 divise α

-1 divise α

a divise α et $-a$ divise α

c'est-à-dire que pour tout $\alpha \in \mathbb{Z}$

α admet au minimum 4 diviseurs. Ces quatre diviseurs sont : $-1, 1, -a$ et a

2.11. Propriétés de la multiplicité

Les propriétés de la divisibilité peuvent être interprétées en termes de multiplicité.

- Étant donnés α et $\beta \in \mathbb{Z}$. Si β est un multiple de α alors on a $|\beta| \geq |\alpha|$
- Étant donnés α, β et $\gamma \in \mathbb{Z}$. Si β est un multiple de α alors $\beta\gamma$ est un multiple de α .
- Soit $\alpha, \beta, \gamma \in \mathbb{Z}$. Si β et γ sont des multiples de α alors $\exists a$ et $b \in \mathbb{Z}$ tel que $a\beta + b\gamma$ soit un multiple de α .
- Pour tout $\alpha \in \mathbb{Z}$, tout multiple d'un multiple de α est un multiple de α .

2.12. Anneaux $(\mathbb{Z}/n\mathbb{Z}, +, \times)$

Notation de classe modulo n

Étant données n et q deux entiers relatifs. Soit k un reste de la division euclidienne de n par q . On nomme classe de k l'ensemble des entiers relatifs qui ont k pour reste. On note $\bar{k}$.

On désigne par $\mathbb{Z}/n\mathbb{Z}$ l'ensemble des classes modulo n et est telle que $\mathbb{Z}/n\mathbb{Z} = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \dots, \overline{(n-1)}\}$

Exemple pratique

$$\text{On a : } \mathbb{Z}/4\mathbb{Z} = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}\} \text{ et } \mathbb{Z}/6\mathbb{Z} = \{\bar{0}, \bar{1}, \bar{2}, \bar{4}, \bar{5}\}$$

$$\text{Ainsi dans } \mathbb{Z}/3\mathbb{Z} = \{\bar{0}, \bar{1}, \bar{2}\} \text{ on a}$$

$$\dot{0} = \{\dots, -6, -3, 0, 3, 6, \dots\}$$

$$\dot{1} = \{\dots, -5, -2, 1, 4, 7, \dots\}$$

$$\dot{2} = \{\dots, -4, -1, 2, 5, 8, \dots\}$$

Calcul dans $\mathbb{Z}/n\mathbb{Z}$

Pour tout $\alpha, \beta \in \mathbb{Z}/n\mathbb{Z}$

$$\dot{\alpha} + \dot{\beta} = \overline{\alpha + \beta}$$

$$\dot{\alpha}\dot{\beta} = \overline{\alpha\beta}$$

On retient que $(\mathbb{Z}/n\mathbb{Z}, +, \times)$ est un groupe commutatif, la multiplication est associative et commutative dans $(\mathbb{Z}/n\mathbb{Z})$, la multiplication est distributive par rapport à l'addition dans $(\mathbb{Z}/n\mathbb{Z})$.

Exemple pratique

Résoudre dans $(\mathbb{Z}/7\mathbb{Z})$ l'équation $x^2 - \dot{2}x + \dot{6} = \dot{0}$

2.13. Plus grand commun diviseur, plus petit commun multiple

La notion de PGCD et de PPCM a été abordé en classe de 8^{ème} année fondamentale. Cette année nous allons faire une étude approfondie sur cette notion.

1) PGCD

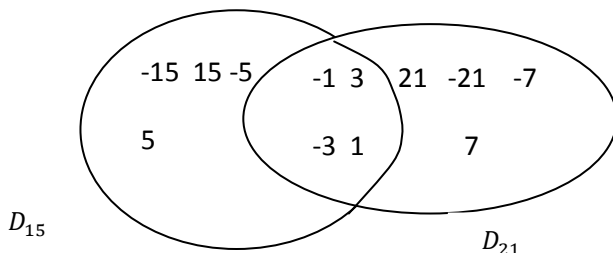
a) Activité

L'ensemble des diviseurs de 15 et 21 sont respectivement

$$D_{15} = \{-15, -5, -3, -1, 1, 3, 5, 15\} \text{ et}$$

$$D_{21} = \{-21, -7, -3, -1, 1, 3, 7, 21\}$$

On peut les représenter ainsi



-1, 1, -3 et 3 sont les diviseurs communs à 15 et à 21

On peut les noter $D_{15} \cap D_{21} = \{-1, 1, -3, 3\}$

Le plus petit est -3 et le plus grand commun diviseur des deux nombres 15 et 21 est 3

3 est appelé le plus grand commun diviseur (PGCD) de 15 et 21 et on note $3 = \text{PGCD}(15, 21)$

b) Définitions

Diviseur commun

Étant donnés α et β deux entiers relatifs. Si l'entier γ divise à la fois α et β alors γ se nomme diviseur commun de α et β .

PGCD

Étant donnés α et β deux entiers naturels. Le plus grand élément de l'ensemble des diviseurs communs à α et β se nomme plus grand commun diviseur de α et β et se note $\text{PGCD}(\alpha, \beta)$.

Exemple pratique

Trouver le $\text{PGCD}(16, 64)$

Méthode

$$D_{16} = \{-16, -8, -4, -2, -1, 1, 2, 4, 8, 16\}$$

$$\text{et } D_{16} \cap \mathbb{N} = \{1, 2, 4, 8, 16\}.$$

$$D_{64} \cap \mathbb{N} = \{1, 2, 4, 8, 16, 32, 64\}$$

$$(D_{16} \cap \mathbb{N}) \cap (D_{64} \cap \mathbb{N}) = \{1, 2, 4, 8, 16\}$$

le plus grand de l'ensemble $\{1, 2, 4, 8, 16\}$ est 16 alors $\text{PGCD}(16, 64) = 16$.

Remarque de notation particulière

On note souvent $\text{PGCD}(\alpha, \beta) = \alpha \wedge \beta$

c) Propriété sur le PGCD

- ❖ Étant donnés α et β des entiers relatifs non nuls. On a $\text{PGCD}(\alpha, \beta) = \text{PGCD}(|\alpha|, |\beta|)$.
- ❖ Étant donnés α et β deux entiers relatifs non nuls. Si β divise α alors $\text{PGCD}(\alpha, \beta) = \beta$
- ❖ Pour tous α et $\beta \in \mathbb{Z}^*$ on a :

$$\text{PGCD}(\alpha, \beta) \leq \alpha \wedge \beta \leq \beta$$

$$\text{et } \text{PGCD}(\alpha, \beta) = \text{PGCD}(\beta, \alpha)$$

- ❖ Étant donnés α et $\beta \in \mathbb{Z}$. On a : $1 \leq \text{PGCD}(\alpha, \beta) \leq \min(\alpha, \beta)$
- ❖ Étant donnés α et $\beta \in \mathbb{Z}^*$. L'ensemble des diviseurs communs à α et β est égal à l'ensemble des diviseurs communs du plus petit et de la différence des deux nombres, c'est-à-dire si $\alpha > \beta$ alors $D(\alpha, \beta) = D(\beta, \alpha - \beta)$
- ❖ Étant donnés $\alpha \in \mathbb{Z}^*$. L'ensemble des diviseurs communs entre α et 0 est égal à l'ensemble des diviseurs de α c'est-à-dire $D(\alpha, 0) = D_c$
- ❖ Étant donnés α et $\beta \in \mathbb{Z}^*$. Soient Q et R respectivement le quotient et le reste de la division euclidienne de α par β (c'est-à-dire $\alpha = \beta Q + R$)
 - Si le reste $R \neq 0$ alors $\text{PGCD}(\alpha, \beta) = \text{PGCD}(\beta, R)$
 - Si le reste $R = 0$ alors $\text{PGCD}(\alpha, \beta) = \beta$

❖ Étant donnés α, β et $\gamma \in \mathbb{Z}^*$

$$PGCD(\gamma\alpha, \gamma\beta) = \gamma PGCD(\alpha, \beta)$$

❖ Étant donnés α et $\beta \in \mathbb{Z}^*$. L'ensemble des diviseurs communs à α et à β est égal à l'ensemble des diviseurs de leur $PGCD$.

❖ Étant donnés α et β deux entiers relatifs non nuls. Soit R_n la suite d'entiers naturels telle que $R_0 = \beta, R_1$ est le reste de la division de α par β

Pour tout $n \in \mathbb{N}^*$

- Si $R_n = 0$ alors $R_{n+1} = 0$
- Si $R_n \neq 0$ alors R_{n+1} est le reste de la division de R_{n-1} par R_n . Alors il existe $n_0 \in \mathbb{N}$ tel que $R_{n_0} \neq 0$ et $\forall n > n_0, R_n = 0$ alors on a $PGCD(\alpha, \beta) = R_{n_0}$

Cette propriété est connue sous le nom d'algorithme d'Euclide

❖ Étant donnés α et β deux entiers positifs et soit $d = PGCD(\alpha, \beta)$. On a les équivalences suivantes $PGCD(\alpha, \beta) = d \Leftrightarrow d/\alpha$ et d/β alors

$PGCD\left(\frac{\alpha}{d}, \frac{\beta}{d}\right) = 1 \Leftrightarrow d/\alpha$ et d/β alors il existe a et $b \in \mathbb{Z}$ tels que $a\alpha + b\beta = d$ cette propriété est la caractérisation du $PGCD$.

- ❖ Étant donné α et β deux entiers positifs des diviseurs du $PGCD$ et soit $d = PGCD(\alpha, \beta)$. Alors pour tout $\gamma \in \mathbb{N}$ $PGCD(\alpha\gamma, \beta\gamma) = d\gamma$. Cette propriété est appelée la multiplicativité du $PGCD$.
- ❖ Étant donnés α et $\beta \in \mathbb{Z}^*$, si $d = PGCD(\alpha, \beta)$ alors l'ensemble des diviseurs de α et β est aussi l'ensemble des diviseurs du $PGCD$.

d) Détermination du $PGCD$ de deux entiers relatifs

Nous avons vu dans une propriété qu'étant donnés α et $\beta \in \mathbb{Z}^*$ tel que $\alpha \neq \beta$ alors $PGCD(\alpha, \beta) = PGCD(\beta, \alpha - \beta)$

Nous allons utiliser cette propriété.

Exemple pratique

Trouver le $PGCD(584, 64)$. On procède successivement :

$$\alpha = 584 \text{ et } \beta = 64$$

$$\begin{aligned} \alpha \neq \beta \text{ alors } PGCD(584, 64) &= PGCD(64, 520) \\ &= PGCD(64, 456) \\ &= PGCD(64, 392) \\ &= PGCD(64, 328) \\ &= PGCD(64, 264) \\ &= PGCD(64, 200) \end{aligned}$$

$$= PGCD(64, 136)$$

$$= PGCD(64, 72)$$

$$= PGCD(64, 8)$$

Alors on conclut que $PGCD(584, 64) = PGCD(64, 8) = 8$.

C'est à dire le $PGCD$ est la dernière valeur non nulle de $\alpha - \beta$. On peut résumer ceci dans un tableau pratique.

Étape k	0	1	2	3	4	5	6	7	8	9	10
α_k	584	520	456	392	328	264	200	136	72	64	8
β_k	64	64	64	64	64	64	64	64	64	8	56
$\alpha_k - \beta_k$	520	456	392	328	264	200	136	72	8	56	8

e) Recherche du $PGCD$ par l'algorithme d'Euclide

Étant donnés α et $\beta \in \mathbb{Z}^*$

- ❖ Si β divise α alors d'après les propriétés précédentes $PGCD(\alpha, \beta) = \beta$
- ❖ Si β ne divise pas α alors on utilise nécessairement l'algorithme d'Euclide.

Détails

Cherchons $PGCD(\alpha, \beta)$. Puisque β ne divise pas α alors il existe un couple (Q, R) tel que $\alpha = \beta Q + R$ avec Q et R respectivement le quotient et le reste de la division euclidienne de α , par β avec $0 \leq R \leq \beta$. Nous savons que l'ensemble des diviseurs de α , et $\beta, D(\alpha, \beta)$ est égal à l'ensemble des diviseurs de β et $R, D(\beta, R)$ car $\beta < \alpha$ et $R < \beta$ alors $PGCD(\alpha, \beta) = PGCD(\beta, R)$. Nous recommençons encore si R ne divise pas β . Soit le couple (Q_1, R_1) tel que $\beta = RQ_1 + R_1$ ou Q_1 et R_1 sont respectivement le quotient et le reste de la division euclidienne de β par R .

$$\text{Alors } D(\beta, R) = D(R, R_1)$$

$$\text{C'est-à-dire } PGCD(\beta, R) = PGCD(R, R_1)$$

Nous poursuivons la division et nous s'arrêtons au moment, ou nous obtenons un reste nul alors le dernier reste non nul R_k est le $PGCD$ de α et β soit $PGCD(\alpha, \beta) = R_k$

Exemple pratique

Trouver par l'algorithme d'Euclide $PGCD(712, 114)$

Méthode

114 ne divise pas 712 alors, on utilise l'algorithme d'Euclide

$$\begin{array}{r|l} 712 & 114 \\ 28 & 6 \end{array}$$

$$\text{Alors } 712 = 114 \times 6 + 28$$

$$\text{alors } PGCD(712, 114) = PGCD(114, 28)$$

$$\begin{array}{r|l} 114 & 28 \\ 2 & 4 \end{array}$$

$$114 = 28 \times 4 + 2$$

$$PGCD(114, 28) = PGCD(28, 2)$$

$$\begin{array}{r|l} 28 & 2 \\ 0 & 14 \end{array}$$

$$28 = 2 \times 14 + 0$$

Dans ce cas le reste est nul, car 2 divise 28 et le reste non nul est $R = 2$ alors $PGCD(114, 28) = 2$

Soit par le tableau.

α	712	114	28
β	114	28	2
Q	6	4	14
R	28	2	0

2) Plus Petit Commun Multiple (PPCM)

a) Activité

Déterminer $6\mathbb{Z}$, $3\mathbb{Z}$, $6\mathbb{Z} \cap 3\mathbb{Z}$ et $6\mathbb{Z} \cap 3\mathbb{Z} \cap \mathbb{N}^*$

Méthode

$6\mathbb{Z}$ est l'ensemble des multiples de 6, c'est à dire

$$6\mathbb{Z} = \{x \in \mathbb{Z} / \exists k \in \mathbb{Z} \text{ tel que } x = 6k\}$$

C'est-à-dire $6\mathbb{Z} = \{\dots, -18, -12, -6, 0, 6, 12, 18, \dots\}$

$$3\mathbb{Z} = \{\dots, -9, -6, -3, 0, 3, 6, 9, \dots\}$$

$$6\mathbb{Z} \cap 3\mathbb{Z} = \{\dots, 18, -12, -6, 0, 12, 18\}$$

$$6\mathbb{Z} \cap 3\mathbb{Z} = \{\dots, 18, -12, -6, 0, 6, 12, 18\} \text{ et}$$

$6\mathbb{Z} \cap 3\mathbb{Z} \cap \mathbb{N}^* = \{6, 12, 18\}$ le plus petit de ces trois nombres est 6. Il est appelé plus petit commun multiple de 3 et 6 et est noté $PPCM(3, 6)$

b) Définitions

Étant données α et $\beta \in \mathbb{N}^*$

On nomme plus petit multiple commun de α et β noté $PPCM(\alpha, \beta)$ le plus petit élément de l'ensemble des multiples strictement positifs communs à α et à β .

Exemple pratique

Calculer $PPCM(4, 12)$

Méthode

On sait que

$$4\mathbb{Z} = \{\dots, -16, -12, -8, -4, 0, 4, 8, 12, 16, \dots\} \text{ et}$$

$$6\mathbb{Z} = \{\dots, -24, -18, -12, -6, 0, 6, 12, 18, \dots\}$$

Les entiers strictement positifs de $4\mathbb{Z} \cap 6\mathbb{Z}$ sont : 12, 24, ... et le plus petit de ces éléments est 12.

Alors on a $PPCM(4, 6) = 12$

Propriétés

- ❖ Étant donnés deux entiers naturels α et β non nuls. L'ensemble des multiples communs à α et à β est l'ensemble des multiples de leur PPCM.

Remarque de notation

On note souvent $PPCM(\alpha, \beta) = \alpha \vee \beta$

2.14. Relation entre PPCM et PGCD

- Étant donnés α et $\beta \in \mathbb{N}^*$. Si β est un multiple de α alors
 $PPCM(\alpha, \beta) = \beta$ et
 $PGCD(\alpha, \beta) = \alpha$
- Étant donnés α et $\beta \in \mathbb{N}^*$

$$PGCD(\alpha, \beta) \text{ divise } PPCM(\alpha, \beta)$$

- Étant donnés α et $\beta \in \mathbb{N}^*$.
 $PGCD(\alpha, \beta) \times PPCM(\alpha, \beta) = \alpha \beta$
- Étant donnés α, β et γ trois entiers naturels non nuls on a : $PPCM(\gamma\alpha, \gamma\beta) = \gamma \cdot PPCM(\alpha, \beta)$
- Pour tous α et $\beta \in \mathbb{N}^*$ on a
 $Max(\alpha, \beta) \leq PPCM(\alpha, \beta) \leq \alpha \beta$
- Étant donnés $\alpha, \beta \in \mathbb{Z}^*$ on a
 $PPCM(\alpha, \beta) = PPCM(|\alpha|, |\beta|)$
- Étant donnés α et $\beta \in \mathbb{Z}^*$.
 Si $d = PGCD(\alpha, \beta)$ et $m = PPCM(\alpha, \beta)$ alors on a l'équivalence suivante :

$$m = PPCM(\alpha, \beta) \Leftrightarrow \begin{cases} m \text{ est multiple de } \alpha \text{ et } \beta \\ \frac{m}{\alpha} \text{ et } \frac{m}{\beta} \text{ sont premiers entre eux} \end{cases}$$

- Étant donnés α, β des entiers. Si α et β sont premiers entre eux alors $PPCM(\alpha, \beta) = \alpha \beta$

Cette relation est la relation de caractérisation du PPCM. On abordera la notation de nombre premier plus tard. On retiendra enfin que

- Étant donnés α et $\beta \in \mathbb{Z}^*$ et $\gamma \in \mathbb{N}^*$ un diviseur commun de α , et de β .

$$\text{Alors } PPCM\left(\frac{\alpha}{\gamma}, \frac{\beta}{\gamma}\right) = \frac{PPCM(\alpha, \beta)}{\gamma}$$

Exemple pratique

Résoudre dans $\mathbb{N}^{*2}$ l'équation : $\begin{cases} x + y = 56 \\ x \vee y = 105 \end{cases}$

Méthode

Réolvons cette équation :

On pose $x\Lambda y = d$ alors l'équation devient

$$\begin{cases} x + y = 56 \\ x\vee y = 105 \end{cases} \Rightarrow$$

$$\exists (x', y') \in \mathbb{N}^{*2} \begin{cases} (x' + y')d = 56 \\ x'y'd = 105 \\ x'\Lambda y' = 1 \end{cases} \Rightarrow \begin{cases} x' + y' = 8 \\ x'y' = 15 \\ x'\Lambda y' = 1 \end{cases}$$

Par suite x' et y' sont solutions de l'équation

$$X^2 - 8X + 15 = 0$$

On a : $(x', y') \in (5, 3)$ alors on a également

$$(x', y') \in (35, 21) \text{ d'où}$$

$$S = \{(21, 35); (35, 21)\}$$

2.15. Nombres premiers entre eux et nombre premiers**a) Activité**

Trouvons le $PGCD(8, 13)$

Le plus grand commun diviseur de 8 et 13 est 1 c'est-à-dire $PGCD(8, 13) = 1$

Ou encore 8 ne divise pas 13. En d'autre terme, on ne peut pas simplifier $\frac{8}{13}$ et $\frac{13}{8}$. Alors on dit que 8 et 13 sont premiers entre eux.

b) Définition

Étant donnés α et $\beta \in \mathbb{Z}^*$.

Les entiers α et β sont premiers entre eux si leur $PGCD$ est égal à 1

On dit souvent que α et β sont **étrangers**.

Remarque sur la définition

- ❖ Dire que α est premier avec β équivaut à dire que β est premier avec α
- ❖ α et β sont premiers entre eux signifie qu'ils admettent seulement comme diviseurs communs 1 et -1
- ❖ Si α et β sont premiers entre eux alors tout diviseur de α est premiers avec β .

d) Propriétés des nombres premiers entre eux

- ❖ Étant donnés α et $\beta \in \mathbb{Z}^*$ et γ un nombre premier. Si δ divise le produit $\alpha\beta$ de α et β alors γ divise à la fois α et β (on verra plus tard la notion de nombre premier)
- ❖ Étant donnés α et $\beta \in \mathbb{Z}^*$ premiers entre eux et soit $\gamma \in \mathbb{N}$ un entier divisible à la fois par α et β alors γ est divisible par leur produit $\alpha\beta$

- ❖ Étant donnés α et $\beta \in \mathbb{Z}^*$ et $\gamma \in \mathbb{N}^*$ tel que $PGCD(\alpha, \beta) = \gamma \Leftrightarrow \frac{\alpha}{\gamma}$ et $\frac{\beta}{\gamma} \in \mathbb{Z}^*$ sont premiers entre eux $\Leftrightarrow$ il existe α' et β' tels que $\alpha = \gamma\alpha'$ et $\beta = \gamma\beta'$

2.16. Théorème de Fermat

Étant donné k un nombre premier. α étant un entier non multiple de k alors $\alpha^{k-1} - 1$ est divisible par k

2.17. Théorème de Bézout

Étant donnés α et $\beta \in \mathbb{Z}^*$

α et β sont premiers entre eux si et seulement si il existe deux entiers relatifs a et b tels $a\alpha + b\beta = 1$

Preuve

Supposons qu'il existe deux entiers relatifs a et b tels que

$a\alpha + b\beta = 1$ et prouvons que α et β sont premiers entre eux. Pour tout γ tel que α/γ et α/β alors γ divise toute combinaison linéaire entre ces deux nombres c'est-à-dire $\gamma/a\alpha + b\beta$. On a $a\alpha + b\beta = 1$ d'où $\gamma/1$ alors $\gamma = 1$

Aucun autre nombre que γ ne divise à la fois

α et β alors α et β sont premiers entre eux. Puisque α et β sont premiers entre eux montrons que : $a\alpha + b\beta = 1$

Désignons par E l'ensemble des nombres de la forme $a\alpha + b\beta$ avec a et $b \in \mathbb{Z}$. On a bien $E \neq \emptyset$ et contient des éléments de $\mathbb{Z}_+$ et un de ceux-ci est le plus petit que l'on désigne par k c'est-à-dire qu'il existe α' et $\beta' \in \mathbb{Z}$ tels que $\alpha\alpha' + \beta\beta' = k$ alors on doit prouver que k/α et k/β

Si k/α alors $\exists (q, r)$ tel que $\alpha = kq + r$.

On aura $\alpha = kq + r$ en remplaçons k par son expression ($\alpha = \alpha\alpha' + \beta\beta'$) $q + r$ c'est-à-dire

$$r = (1 - \alpha'q)\alpha - \beta'q\beta \text{ avec } 0 \leq r \leq k \text{ c'est-à-dire}$$

$$r = A\alpha + B\beta \text{ Avec } A = 1 - \alpha'q \text{ et } B = -\beta'q, A, B \in \mathbb{Z}$$

Alors $r \in E$

$r \leq k$ c'est-à-dire que r ne peut être que 0 ($r = 0$) alors $\alpha = kq$ c'est-à-dire m/α . De même par le même raisonnement, on montre que m/β

k est le seul diviseur commun à α et à β forcément $k = 1$ par suite on a $a\alpha + b\beta = 1$ d'où la démonstration.

2.18. Théorème de Gauss

Étant donné α, β et $\gamma \in \mathbb{Z}$

Si α divise $\beta\gamma$ et si α est premier avec β alors α divise γ

Preuve

α divise $\beta\gamma$ équivaut à dire que $\beta\gamma = \alpha q$ et

$$\alpha \wedge \beta = 1 \Leftrightarrow \exists a \text{ et } b \in \mathbb{Z} \text{ tels que } a\alpha + b\beta = 1$$

Par multiplication par γ de l'égalité précédente, on a

$$a\alpha\gamma + b\beta\gamma = \gamma. \text{ Or on sait que } \beta\gamma = \alpha q \text{ alors on aura } a\alpha\gamma + b\alpha q = \gamma. \text{ Soit } a\gamma\alpha + bqa = \gamma$$

Par fini on a : $\alpha(\gamma a + bq) = \gamma$ c'est-à-dire que α divise γ d'où la démonstration.

Corollaire de gauss

Étant donnés α, β et $k \in \mathbb{Z}$

Si k est divisible par α et par β premier entre eux, alors il est divisible par leur produit c'est-à-dire

$$\left. \begin{array}{l} \alpha/k \\ \beta/k \\ \alpha \wedge \beta = 1 \end{array} \right\} \Rightarrow \alpha\beta/k$$

Preuve

Rapidement on a $\alpha/k \Rightarrow k = \alpha q_1$

$$\beta/k \Rightarrow k = \beta q_2$$

$$\alpha q_1 = \beta q_2, \text{ on déduit que } \alpha \text{ divise } \beta q_2$$

α et β étant premiers entre eux par le théorème de Gauss on conclut que α divise q_2 . Alors on confirme l'existence d'un entier u tel que $q_2 = \alpha u$ donc $k = \beta q_2 = \beta \alpha u$ par suite on a bien $\beta \alpha$ divise k .

2.19. Nombres premiers

a) Définition

Étant donné k un entier naturel strictement supérieur à 1 c'est-à-dire $k \in \mathbb{N} - \{0,1\}$. On nomme nombre premier k , si l'ensemble de ses diviseurs dans $\mathbb{Z}^*$ sont $-1, 1, -k$ et k . Autrement dit si l'ensemble de ses diviseurs dans $\mathbb{N}$ sont 1 et k .

Si le nombre k n'est pas premier, alors on l'appelle nombre composé.

Exemple de nombre premier

2,3,5,7,11, ... sont des exemples de nombres premiers

Attention

Le nombre 1 n'est pas premier par convention car le nombre premier $k \in \mathbb{N} - \{0,1\}$

Exemple d'application

Préciser si les nombres suivants sont premier ou non 4, 8, 13, 30, 37.

Méthode

Un nombre $k \in \mathbb{N} - \{0,1\}$ est premier si ses seuls diviseurs sont $-1, 1, k$ et $-k$.

Les diviseurs de 4 sont : $-1, 1, 4, -4, 2, -2$.

Alors 4 n'est pas premier.

Les diviseurs de 8 sont : $-1, 1, -8, 8, -2, 2, 4, -4$, alors 8 n'est pas premier.

Les diviseurs de 13 sont $-1, 1, -13$ et 13 alors les nombres 13 est premier.

Les diviseurs de 30 sont $-1, 1, -30, 30, -2, 2, -5, 5,$

$-6, 6, -10, 10, -3, 3, -15, 15$.

Alors 30 n'est pas premiers.

Les diviseurs de 37 sont $-1, 1, 37$ et -37 alors 37 est premier.

b) Propriété des nombres premiers

- ✓ Dans l'ensemble des entiers naturels $\mathbb{N}$ il ya une infinité de nombres premiers.
- ✓ Étant donné $k \in \mathbb{N} - \{0,1\}$
 k possède au moins un diviseur premier.
 Si k n'est pas premier alors au moins un des diviseurs premiers de k est inférieur à $\sqrt{k}$

c) Détermination d'un nombre premier

Pour déterminer le caractère premier d'un nombre k on procède ainsi :

- On remarque si le nombre k est divisible par un nombre premier inférieur (ou égal) à $\sqrt{k}$
- Si l'un des nombres premiers inférieurs (ou égaux) à $\sqrt{k}$ divise k , on conclut que k n'est pas premier.
- Dans le cas contraire c'est-à-dire si aucun des nombres premiers inférieurs (ou égaux) à $\sqrt{k}$ ne divise k on conclut que k est premier.

d) Méthode d'obtention de nombres premiers

Par exemple pour chercher tous les nombres premiers inférieurs ou égaux à 50 on procède ainsi :

- Dans le tableau de 1 à 50
- On hachure 1 qui n'est pas premier
- On hachure tous les multiples de 2 supérieurs à 2
- On hachure tous les multiples de 3 supérieurs à 3
- On hachure les multiples de 5 supérieurs à 5
- On hachure les multiples de 7 supérieurs à 7 on s'arrête à 7 car $7 > \sqrt{50}$

Alors dans le tableau, les nombres non hachurés sont premiers.

1	2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50

Les nombres premiers inférieurs à 50 sont :

2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43 et 47.

Cette méthode se nomme le **crible d’Eratosthène**

2.20. Décomposition d’un nombre en produit de facteurs premiers

a) Activité

Soit le nombre 600.

On a les opérations suivantes :

$$600 = 300 \times 2$$

$$300 = 100 \times 3$$

$$100 = 2 \times 50$$

$$50 = 5 \times 10$$

$$10 = 5 \times 2$$

Alors 600 peut s’écrire $600 = 2 \times 3 \times 2 \times 5 \times 5 \times 2$

$$600 = 2 \times 2 \times 2 \times 3 \times 5 \times 5$$

$$600 = 2^3 \times 3 \times 5^2$$

Les nombre 2, 3 et 5 sont premiers et $600 = 2^3 \times 3 \times 5^2$ est appelé décomposition du nombre 600 en produit de facteurs premiers.

b) Définition et propriété

- ❖ Étant donné un entier k supérieur (ou égal) à 2 On appelle décomposition k toute écriture de la forme $k = a_1^{b_1} \cdot a_2^{b_2} \cdot \dots \cdot a_i^{b_i}$ avec $a_1, a_2, \dots, a_i$ des nombres premiers tels que $a_1 < a_2 < \dots < a_i$ et $b_1, b_2, \dots, b_i \in \mathbb{N}^*$
- ❖ Cette décomposition est unique et tout diviseur premier de k est l’un des nombres $b_1, b_2, \dots, b_i$
- ❖ Étant donné k un entier supérieur (ou égal à 2) admettant une décomposition unique telle que $k = a_1^{b_1} a_2^{b_2} \dots a_i^{b_i}$.
L’ensemble des diviseurs naturels de k est l’ensemble des entiers h s’écrivant sous la forme $h = a_1^{c_1} a_2^{c_2} \dots a_i^{c_i}$ avec $c_1, c_2, \dots, c_i$ des entiers naturels tels que $0 \leq c_1 \leq b_1, 0 \leq c_2 \leq b_2, \dots, 0 \leq c_i \leq b_i$
- ❖ Étant donné $k \in \mathbb{N} - \{0, 1\}$ et soit la décomposition de $k = a_1^{b_1} a_2^{b_2} \dots a_i^{b_i}$.

Alors le nombre de diviseurs naturels de k est $(b_1 + 1)(b_2 + 1) \dots (b_i + 1)$

- ❖ Étant donné k et $h \in \mathbb{N} - \{0, 1\}$ admettant les décompositions respectives $k = a_1^{b_1} a_2^{b_2} \dots a_i^{b_i}$ et $h = a_1^{c_1} a_2^{c_2} \dots a_i^{c_i}$ avec $a_1, a_2, \dots, a_i$ des nombres premiers et $b_1, b_2, \dots, b_i, c_1, c_2, \dots, c_i \in \mathbb{N}^*$
Pour tout $p \in \{1, \dots, i\}$ en posant $\alpha_p = \min(b_i, c_i)$ et $\beta_p = \max(b_i, c_i)$ alors on a
 $PGCD(k, h) = a_1^{\alpha_1} a_2^{\alpha_2} \dots a_i^{\alpha_i}$ et
 $PPCM(k, h) = a_1^{\beta_1} a_2^{\beta_2} \dots a_i^{\beta_i}$

Exemple pratique des propriétés

En utilisant la décomposition trouver $PGCD(2250, 4725)$ et $PPCM(2250, 4725)$ puis trouver le nombre de diviseurs naturel de 2250.

Méthode

Commençons par décomposer ces nombres

2250	2
1125	5
225	5
45	5
9	3
3	3
1	

Ainsi $2250 = 2 \times 5 \times 5 \times 5 \times 3 \times 3$

$$2225 = 2^1 \times 5^3 \times 3^2 \text{ ou } 2225 = 2^1 \times 3^2 \times 5^3$$

4725	5
945	5
189	3
63	7
9	3
3	3
1	

Alors $4725 = 3 \times 3 \times 3 \times 5 \times 5 \times 7$

$$4725 = 3^3 \times 5^2 \times 7^1$$

En utilisant les mêmes facteurs premiers pour les nombres 2250 et 4725 et en autorisant l’usage d’exposants nuls on a

$$2250 = 2^1 \times 3^2 \times 5^3 \times 7^0 \text{ et } 4725 = 2^0 \times 3^3 \times 5^2 \times 7^1$$

- Pour les exposants de 2, le plus petit est 2^0
- Pour les exposants de 3, le plus petit est 3^2
- Pour les exposants de 5, le plus petit est 5^2 et
- Pour les exposants de 7 le plus petit est 7^0

$$\text{Donc } PGCD(225, 4725) = 2^0 \cdot 3^2 \cdot 5^2 \cdot 7^0$$

$$PGCD(2250, 4725) = 225$$

- Pour les puissances de 2, le plus grand est 2^1
- Pour les puissances de 3, le plus grand est 3^3
- Pour les puissances de 5, le plus grand est 5^3
- Et pour les puissances de 7, le plus grand est 7^1

$$\text{Alors } PPCM(225, 4725) = 2^1 \cdot 3^3 \cdot 5^3 \cdot 7^1$$

$$PPCM(2250, 4725) = 47250$$

Trouvons le nombre de diviseurs naturels de 2250

$2250 = 2^1 \cdot 3^3 \cdot 5^3$ qui est la décomposition de 2250 en facteurs premiers alors on a

$a_1 = 2, a_2 = 3$ et $a_3 = 5$ et $b_1 = 1, b_2 = 2$ et $b_3 = 3$
Le nombre de diviseur est

$$(b_1 + 1)(b_2 + 1)(b_3 + 1) = (1 + 1)(2 + 1)(3 + 1) = 24$$

2.21. Résolution d'équation dans $\mathbb{Z} \times \mathbb{Z}$

On s'intéresse à la résolution des équations de la forme $ax + by = c$ avec a, b et $c \in \mathbb{Z}$ tel que $ab \neq 0$.

Cette équation admet un couple de solution dans $\mathbb{Z}^2$. Ces types d'équations sont appelées **équation diophantienne**.

Méthode générale de résolution de l'équation du type $ax + by = c$ avec $a, b, c \in \mathbb{Z}$ et $ab \neq 0$

On recherche à résoudre l'équation $ax + by = c$ avec a, b , et $c \in \mathbb{Z}$

En désignant par $d = PGCD(a, b)$ alors $\exists \alpha$ et $\beta \in \mathbb{Z}$ tels que $a = \alpha d$ et $b = \beta d$ avec α et β premiers entre eux ; c'est-à-dire $PGCD(\alpha, \beta) = 1$

On distingue deux cas sur d

1^{er} cas

Si d ne divise pas c alors l'équation $ax + by = c$ n'admet pas de solution dans $\mathbb{Z} \times \mathbb{Z}$ c'est-à-dire $S = \emptyset$

2^{ème} cas

Si d divise c alors il existe $\gamma \in \mathbb{Z}$ tel que $c = \gamma d$.

Alors on a $ax + by = c \Leftrightarrow \alpha dx + \beta dy = \gamma d$

c'est-à-dire $ax + by = c \Leftrightarrow \alpha x + \beta y = \gamma$

Désignons par x_0 et y_0 la solution particulière de l'équation (solution par évidence). L'équation devient $ax + \beta y = \gamma$ et $\alpha x_0 + \beta y_0 = \gamma$

On le système
$$\begin{cases} \alpha x + \beta y = \gamma \\ \alpha x_0 + \beta y_0 = \gamma \end{cases}$$

C'est-à-dire $\alpha(x - x_0) = \beta(y_0 - y)$ cela signifie que β divise $x - x_0$, c'est-à-dire qu'il existe $k \in \mathbb{Z}$ tel que $x - x_0 = \beta k \Rightarrow x = \beta k + x_0$ en remplaçant x par son expression dans $\alpha(x - x_0) = \beta(y_0 - y)$, on a $y = -\alpha k + y_0$.

On dira alors que les solutions de l'équation sont les couples $(x, y) \in \mathbb{Z}^2$ tels que $(x, y) = (\beta k + x_0, -\alpha k + y_0)$ avec $k \in \mathbb{Z}$.

Exemple pratique 1

Résoudre dans $\mathbb{Z} \times \mathbb{Z}$ l'équation $8x - 5y = 3$

Méthode

Cette équation est de la forme $ax + by = c$ avec

$$\begin{cases} a = 8 \\ b = -5 \\ c = 3 \end{cases}$$

$$\begin{array}{r|l} 8 & 5 \\ 3 & 1 \end{array}$$

$$8 = 5 \times 1 + 3$$

$$8 - 5 \times 1 = 3$$

C'est-à-dire $8 \times 1 - 5 \times 1 = 3$ c'est-à-dire la solution particulière est $\begin{cases} x_0 = 1 \\ y_0 = 1 \end{cases}$

On sait que $PGCD(8, 5) = 1$ alors 1 divise $8x - 5y$ et 1 divise 3, c'est à dire que

$$8 = 8 \times 1 \quad \text{et} \quad 5 = 5 \times 1$$

Alors $3 = 3 \times 1$ alors $8x - 5y = 3$ on a donc le système

$$\begin{cases} 8x - 5y = 3 & (1) \\ 8x_1 - 5y_1 = 3 & (2) \end{cases}$$

Pour soustraction membre par membre, on a

$$8(x - 1) - 5(y - 1) = 0$$

$$8(x - 1) = 5(y - 1)$$

C'est-à-dire que 5 divise $x - 1$ et 8 divise $y - 1$, c'est-à-dire qu'il existe un $k \in \mathbb{Z}$ tel que $x - 1 = 5k$ et $y - 1 = 8k$ c'est-à-dire $x = 5k + 1$ et $y = 8k + 1$ (application direct du théorème de Gauss). Alors la solution finale est

$$S = \{(5k + 1, 8k + 1) | k \in \mathbb{Z}\}$$

Exemple d'application 2

Résoudre l'équation diophantienne $5x - 7y = 4$

Méthode

On cherche d'abord une solution particulière de l'équation.
On peut trouver deux entiers α et β tels que

$$5\alpha - 7\beta = 1 \text{ si } \alpha = 3 \text{ et } \beta = 2$$

$$5 \times 3 - 7 \times 2 = 1$$

En multipliant par 4

$$5 \times 3 \times 4 - 7 \times 2 \times 4 = 1 \times 4 \Rightarrow 5 \times 12 - 7 \times 8 = 4$$

Alors une solution particulière de l'équation est

$\begin{cases} x_0 = 12 \\ y_0 = 8 \end{cases}$ et $PGCD(5,7) = 1$, autrement dit 5 et 7 sont premiers entre eux. L'équation est toujours égale à elle-même $5x - 7y = 4$

On forme le système

$$\begin{cases} 5x - 7y = 4 \\ 5 \times 12 - 7 \times 8 = 4 \end{cases}$$

$$5(x - 12) - 7(y - 8) = 0$$

$$5(x - 12) - 7(y - 8) = 0$$

Par application du théorème de Gauss, on trouve que

$$x - 12 = 7k \text{ et } y - 8 = 5k \text{ Avec } k \in \mathbb{Z}$$

alors $x = 7k + 12$ et $y = 5k + 8$. Doù

$$S = \{(7k + 12, 5k + 8), k \in \mathbb{Z}\}$$

2.22. Histoire des mathématiciens**a) Gauss**

Gauss, Carl Friedrich vécu entre 1777 et 1855, mathématicien, physicien, et astronome Allemand. Il est né à Brunswick. On l'appelle le prince des mathématiciens. Il a apporté sa contribution dans la plus part des branches scientifiques.

b) Euclide

Euclide, (III^e siècle av. J.-C.), mathématicien grec, auteur du plus célèbre ouvrage de l'histoire des mathématiques, les *Éléments*. Euclide se distingue également en théorie des nombres, démontrant notamment que l'ensemble des nombres premiers est infini. Il est aussi le premier à pratiquer la division avec le reste, appelée aujourd'hui division euclidienne.

c) Bézout

Étienne Bézout, né à Nemours en 1730 et mort à Avon en 1783, est un mathématicien français.

Il est l'auteur d'une Théorie générale des équations algébriques, publiée en 1779, sur la théorie de l'élimination et des fonctions symétriques sur les racines d'une équation.

Élu adjoint de mécanique à l'Académie des sciences en 1758, il y devient associé en 1768, puis pensionnaire en 1770.

d) Fermat

Pierre de Fermat, né dans la première décennie du 17^e siècle, à Beaumont-de-Lomagne, près de Montauban, et mort le en 1665 à Castres, est un juriste et mathématicien français, surnommé « le prince des amateurs ». Il est en même temps un habile helléniste. Il s'est aussi intéressé aux sciences physiques ; on lui doit notamment le principe de Fermat en optique.

Note

L'arithmétique a eu aujourd'hui son application grâce à la révolution technologique. Son domaine d'application est la Cryptologie. La Cryptologie est essentiellement fondée sur les nombres et surtout les nombres premiers.

Pour plus d'info sur cette partie en bref, consulter une encyclopédie (Wikipédia ou Encarta).