•ARITHMETIQUE•

L'arithmétique est un des secteurs scientifiques les plus anciens et les plus féconds. Fondée essentiellement par les pythagoriciens pour qui tout était nombre, elle a connu de grands progrès sous l'impulsion de Fermat, Euler, Lagrange, Gauss et Legendre.

Longtemps considérée comme la branche la plus abstraite et la moins utile des mathématiques, elle connaît aujourd'hui de nombreuses applications en informatique, en électronique et en cryptographie. Voici de façon presque détaille le plan du chapitre :

•Table des matières•

I NUMERATION

I.1 Division euclidienne dans $\mathbb{N}$

Définition

Soit a et b deux entiers naturels non nuls. Il existe un unique couple (q,r) d'entiers naturels tels que $a = bq + r$ avec $0 \leq r < b$.

L'opération qui permet de trouver q et r connaissant a et b est appelée la **division euclidienne** de a par b.

a est le **dividende**, b est le **diviseur**, q le **quotient** et r le **reste**.

Exemple :

$23 = 7 \times 3 + 2$; $15 = 7 \times 2 + 1$; $10 = 10 \times 1 + 0$

I.2 Ordre dans $\mathbb{N}$

Dans $\mathbb{N}$, il est défini une relation notée $\leq$ par : $\forall (a,b) \in \mathbb{N}^2$, $(a \leq b \iff \exists c \in \mathbb{N}, b = a + c)$.

Cette relation est une **relation d'ordre** car elle possède les caractéristiques suivantes :

Propriété$_1$

$\forall a, b, c \in \mathbb{N}$, on a :

- $a \leq a$. On dit que la relation $\leq$ est **réflexive**.
- si $a \leq b$ et $b \leq a$, alors $a = b$. On dit que la relation $\leq$ est **antisymétrique**.
- si $a \leq b$ et $b \leq c$, alors $a \leq c$. On dit que la relation $\leq$ est **transitive**.

De plus deux entiers naturels a et b sont toujours comparables, c'est à dire on a toujours $a \leq b$ ou $b \leq a$; on dit alors que $\leq$ dans est une **relation d'ordre total**.

Propriété$_2$

Toute partie non vide de $\mathbb{N}$ admet un plus petit élément.

Exemple :

- 0 est le plus petit élément de $\mathbb{N}$.
- Le plus petit élément de l'ensemble $\{5n+2, n \in \mathbb{N}\}$ est 2.

I.3 Système de numération

On appelle **système de numération** un mode de représentation de tous les entiers naturels à l'aide d'un nombre fini de symboles. Ces symboles sont appelés **chiffres**.

Théorème

Soit b un entier naturel supérieur ou égal à 2.

Tout entier naturel x non nul peut s'écrire de façon unique $x = \sum_{k=0}^{p} a_k b^k$, où les a_k sont des entiers naturels tels que $0 \leq a_k < b$ et $a_p \neq 0$.

Il convient d'écrire $x = \overline{a_p a_{p-1} \cdots a_2 a_1 a_0}^b$. Cette écriture est appelée **écriture de x en base b**.

Par convention, les écritures sans "barre" sont en base 10.

Comment écrire un nombre en base b ?

Soit $x = \overline{a_p a_{p-1} \cdots a_2 a_1 a_0}^b$.

Cette écriture équivaut aussi à $x = a_p b^p + a_{p-1} b^{p-1} + \cdots + a_2 b^2 + a_1 b + a_0$.

$\star$ $x = b(a_p b^{p-1} + a_{p-1} b^{p-2} + \cdots + a_2 b + a_1) + a_0$. Donc $q_0 = \overline{a_p a_{p-1} \cdots a_2 a_1}^b$ et a_0 sont respectivement le quotient et le reste de la division euclidienne de x par b.

$\star$ On a $q_0 = b(a_p b^{p-2} + a_{p-1} b^{p-3} + \cdots + a_2) + a_1$. Donc $q_1 = \overline{a_p a_{p-1} \cdots a_2}^b$ et a_1 sont respectivement le quotient et le reste de la division euclidienne de x par b.

on peut ainsi déterminer de proche en proche l'écriture de x en base b.

Exemple

Ecrire le nombre 432 en base 7.

Ecrire le nombre $\overline{423}^4$ en base 10.

Remarque

Dévélopper un entier naturel x suivant les puissances de b revient à mettre x sous la forme $x = a_p b^p + a_{p-1} b^{p-1} + \cdots + a_1 b + a_0$.

Exemple

Développer 2837 suivant les puissances de 5.

II DIVISIBILITE DANS $\mathbb{Z}$

II.1 Division euclidienne

Théorème

Soit $a \in \mathbb{Z}$ et $b \in \mathbb{Z}^*$, il existe un unique entier relatif q et un unique entier naturel r tels qu $a = bq + r$ où $0 \leq r < |b|$

Exemple

$47 = 9 \times 5 + 2$; $-47 = 5 \times (-10) + 3$; $47 = (-5)(-9) + 2$.

Attention ! Le reste d'une division euclidienne est toujours positif. Donc éviter d'écrire par exemple $-47 = 5(-9) - 2$.

II.2 Multiple d'un entier

Soit $n \in \mathbb{Z}$. On appelle **multiple** de n tout entier relatif x tel que $x = kn$ où $k \in \mathbb{Z}$. C'est à dire le reste de la division euclidienne de x par n est 0.

On dit aussi que n est un diviseur de x si $n \neq 0$ ou que n divise x et on note n/x.

Soit n un entier relatif. On note $n\mathbb{Z}$ l'ensemble des multiples de n.

Ainsi $x \in n\mathbb{Z} \Longleftrightarrow \exists k \in \mathbb{Z}/x = kn$

Remarques

- Tout entier relatif est multiple de 1 et -1
- 0 est multiple de tout entier relatif
- $\forall x \in n\mathbb{Z}, \forall y \in \mathbb{Z}, xy \in n\mathbb{Z}$

Théorème

La relation $\mathscr{R}$ définie dans $\mathbb{Z}$ par $\forall (x,y) \in \mathbb{Z}^2$, $x\mathscr{R}y \Longleftrightarrow x - y \in n\mathbb{Z}$ est une relation d'équivalence.

Preuve :

$\star$ $\forall x \in n\mathbb{Z}$, $x - x = 0$ or $0 \in n\mathbb{Z}$ donc $\underline{x\mathscr{R}x}$ (***Reflexivité***)

$\star$ $\forall (x,y) \in \mathbb{Z}^2$, $x\mathscr{R}y \Longleftrightarrow x - y \in n\mathbb{Z}$

$\Longleftrightarrow \exists k \in \mathbb{Z}/x-y=nk$

$\Longleftrightarrow y-x=-nk=n(-k)=nk',k' \in \mathbb{Z}$

$\Longleftrightarrow \underline{y\mathscr{R}x}$ (***Symétrie***)

$\star$ Soit x,y,z trois entiers tels que $x\mathscr{R}y$ et $y\mathscr{R}z$.

$x\mathscr{R}y \Longleftrightarrow \exists k \in \mathbb{Z}/x-y=nk$

$y\mathscr{R}z \Longleftrightarrow \exists k' \in \mathbb{Z}/y-z=nk'$

Ainsi, $(x-y)+(y-z)=nk+nk'$ donc $x-z=n(k+k')=nk''$, $k'' \in \mathbb{Z}$ d'où $\underline{x\mathscr{R}z}$ (***Transitivité***)

II.3 Congruence modulo n

a) Définition

Soit $n \in \mathbb{N}^*$, a et b deux entiers relatifs. On dit que a est **congru à** b **modulo** n si $(a-b)$ est un multiple de n. On note $a \equiv b[n]$.

Exemple : $9 \equiv 1[2]$; $21 \equiv 6[5]$

Propriété$_1$:

La relation de congruence modulo est une relation d'équivalence.

Preuve : il suffit de remplacer dans le théorème ci-dessus $\mathscr{R}$ par $\equiv$

Propriété$_2$:

Soit n un entier naturel non nul, x et y deux entiers relatifs, r et r' les restes des divisions euclidiennes de x et y par n. On a : $x \equiv y[n] \Longleftrightarrow r=r'$.

Preuve :

On a $x=nk+r$ et $y=nk'+r'$.

Donc $x-y=(k-k')n+r-r'$, avec $-n<r-r'<n$

$x \equiv y \Longleftrightarrow x-y \in n\mathbb{Z}$

$\Longleftrightarrow (k-k')n+r-r' \in n\mathbb{Z}$

$\Longleftrightarrow r-r' \in n\mathbb{Z}$

$\Longleftrightarrow r-r'=0$ car $r-r'<n$

$\Longleftrightarrow r=r'$

Propriété$_3$:

Soit $n \in \mathbb{N}^*$. Soit $(x,y,z,t) \in \mathbb{Z}^4$.

- si $x \equiv y[n]$ et $z \equiv t[n]$ alors $x+z \equiv y+t[n]$
- si $x \equiv y[n]$ et $z \equiv t[n]$ alors $xz \equiv yt[n]$

Il en résulte que la congruence modulo n est compatible avec l'addition et la multiplication dans $\mathbb{Z}$.

Preuve

- $x \equiv y[n] \Longleftrightarrow x-y \in n\mathbb{Z}$ et $z \equiv t[n] \Longleftrightarrow z-t \in n\mathbb{Z}$

Ainsi, $(x-y)+(z-t) \in n\mathbb{Z}$. D'où $(x+z)-(y+t) \in n\mathbb{Z}$

Et par conséquent $x+z \equiv y+t[n]$

- $x \equiv y[n] \Longleftrightarrow \exists k \in \mathbb{Z}, x = nk+y$ et $z \equiv t[n] \Longleftrightarrow \exists k' \in \mathbb{Z}, z = nk'+t$

$xz = (nk+y)(nk'+t) = n^2kk' + nkt + nyk' + yt = n(nkk' + kt + yk') + yt$

Donc $xz - yt = n(nkk' + kt + yk')$. D'où $xz - yt \in n\mathbb{Z}$ et par conséquent $xz \equiv yt[n]$.

Remarque : Si $k \in \mathbb{Z}^*$, on a : $x \equiv y[n] \Longleftrightarrow x^k \equiv y^k[n]$.

b) Définition

Soit a un entier relatif. On appelle **classe d'équivalence** de a, l'ensemble des entiers relatifs qui sont congrus à a modulo n. Il est noté $\overline{a}$. Ainsi, $\overline{a} = \{x \in \mathbb{Z}/x \equiv a[n]\}$.

$$\begin{aligned} x \in \overline{a} &\Longleftrightarrow x \equiv a[n] \\ &\Longleftrightarrow \exists k \in \mathbb{Z}/x-a = kn \\ &\Longleftrightarrow x = kn+a \end{aligned}$$

Ainsi, $\overline{a} = \{x \in \mathbb{Z}/\exists k \in \mathbb{Z}, x = nk+a\}$

On a :

$\overline{0} = \{x \in \mathbb{Z}/\exists k \in \mathbb{Z}, x = nk\} = n\mathbb{Z}$

$\overline{1} = \{x \in \mathbb{Z}/\exists k \in \mathbb{Z}, x = nk+1\}$

$\overline{2} = \{x \in \mathbb{Z}/\exists k \in \mathbb{Z}, x = nk+2\}$

$\vdots$

$\overline{n-1} = \{x \in \mathbb{Z}/\exists k \in \mathbb{Z}, x = nk+n-1\}$

$\overline{n} = \{x \in \mathbb{Z}/\exists k \in \mathbb{Z}, x = nk+n = n(k+1) = nk'\} = n\mathbb{Z} = \overline{0}$

Il existe n classes d'équivalence. On note $\mathbb{Z}/n\mathbb{Z}$ l'ensemble des classes d'équivalence.

$\mathbb{Z}/n\mathbb{Z} = \{\overline{0}, \overline{1}, \overline{2}, \cdots, \overline{n-1}\}$

Exemple : $\mathbb{Z}/3\mathbb{Z} = \{\overline{0}, \overline{1}, \overline{2}\}$; $\mathbb{Z}/6\mathbb{Z} = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}, \overline{5}\}$

III PDCD et PPCM

Soit a et b deux entiers relatifs non nuls.

III.1 PPCM

Un entier M est un multiple commun de a et b si et seulement si $M \in a\mathbb{Z} \cap b\mathbb{Z}$. Le plus petit élément strictement positif de $a\mathbb{Z} \cap b\mathbb{Z}$ est appelé **plus petit commun multiple de** a **et** b. On le note $ppcm(a,b)$.

Exemple : $ppcm(12,15) = 60$

Propriété

Posons $\mu = ppcm(a,b)$. On a donc $a\mathbb{Z} \cap b\mathbb{Z} = \mu\mathbb{Z}$. En effet, si a/M et si b/M alors μ/M.

Propriétés

- $ppcm(a,b) = ppcm(b,a)$
- $\forall k \in \mathbb{N}^*$, $ppcm(ka,kb) = kppcm(a,b)$
- $\mu = ppcm(a,b) \Longrightarrow \exists (u,v) \in \mathbb{Z}^2$, $\mu = au + bv$

III.2 PGCD

L'ensemble des diviseurs communs de a et b noté $\mathscr{D}(a,b)$ contient 1 et est fini. Il admet donc un plus grand élément strictement positif.

On appelle **plus grand commun diviseur** de a et b et on note $pgcd(a,b)$, le plus grand élément de $\mathscr{D}(a,b)$.

Propriétés

- $pgcd(a,b) = pgcd(b,a)$
- $\forall k \in \mathbb{N}^*$, $pgcd(ka,kb) = kpgcd(a,b)$
- Si $\delta = pgcd(a,b)$ alors $\delta\mathbb{Z} = \{au + bv; (u,v) \in \mathbb{Z}^2\}$
- $\mathscr{D}(a,b) = \mathscr{D}(\delta)$

III.3 Recherche du *pgcd*

Théorème : Algorithme d'Euclide

Soit a et b deux entiers relatifs et r le reste de la division euclidienne de a par b.

$\star$ Si $r = 0$ alors $pgcd(a,b) = b$

$\star$ Si $r \neq 0$ alors $pgcd(a,b) = pgcd(b,r)$

Preuve

♦ Si $r = 0$ alors $b/a \Longrightarrow b/b$ et b/a. donc $pgcd(a,b) = b$.

♦ Si $r \neq 0$, alors $a = bq + r \Longrightarrow r = a - bq$.

Soit d un diviseur commun de a et b. on a $a = da'$ et $b = db'$. Ainsi, $r = da' - db'q = d(a' - b'q)$. donc d/r. Ainsi, $pgcd(a,b) = pgcd(b,r)$.

Exemple : Trouver le $pgcd(12,48)$ et $pgcd(50,70)$.

Propriétés

• Si d/a et d/b alors d divise toute combinaison linéaire de a et b.

En effet, $\forall (u,v) \in \mathbb{Z}^2$, $au + bv = a'du + b'dv = d(a'u + b'v)$

• b/a si et seulement si $a\mathbb{Z} \subset b\mathbb{Z}$

En effet, $b/a \Longrightarrow \forall M \in a\mathbb{Z}, M = ka = ka'b$ donc $M \in b\mathbb{Z}$ d'où $a\mathbb{Z} \subset b\mathbb{Z}$.

Ensuite, $a\mathbb{Z} \subset b\mathbb{Z} \Longrightarrow \forall M \in a\mathbb{Z}, b/M$. Or $a \in a\mathbb{Z}$ donc b/a.

Par conséquent, $b/a \Longleftrightarrow a\mathbb{Z} \subset b\mathbb{Z}$

IV NOMBRES PREMIERS ENTRE EUX

IV.1 Définition

Deux entiers relatifs a et b sont dits premiers entre eux si $pgcd(a,b) = 1$.

$pgcd(a,b) = 1 \Longleftrightarrow \mathscr{D}(a,b) = \{-1,1\}$

IV.2 Théorème de Bezout

Soit a et b deux entiers relatifs non nuls.

$pgcd(a,b) = 1 \Longleftrightarrow \exists (u,v) \in \mathbb{Z}^2, au + bv = 1.$

Exemple :

- Montrer que 23 et 16 sont premiers entre eux
- trouver deux entiers relatifs u et v tels que $23u+16v=1$

IV.3 Théorème de Gauss

Soient a,b et c trois entiers relatifs. Si a et b sont premiers entre eux et si a/bc alors a/c. C'est à dire $(pgcd(a,b)=1 \text{ et } a/bc) \Longrightarrow a/c$

Preuve

$a/bc \Longrightarrow bc=ka$ et $pgcd(a,b)=1 \Longrightarrow au+bv=1$

$$\begin{aligned} 1=au+bv &\Longrightarrow c=cau+cbv \\ &\Longrightarrow c=cau+kav \\ &\Longrightarrow c=a(cu+kv) \\ &\Longrightarrow a/c \end{aligned}$$

Propriétés

Soit a, b et c trois entiers relatifs.

• $(pgcd(a,b)=1 \text{ et } pgcd(a,c)) \Longrightarrow pgcd(a,bc)=1$

En effet, on a : $au+bv=1$ et $ax+cy=1$.

$$\begin{aligned} (au+bv)(ax+cy)=1 &\Longleftrightarrow a^2ux+acy+abvx+bcvy=1 \\ &\Longleftrightarrow a(aux+cy+bvx)+bc(vy)=1 \\ &\Longleftrightarrow a\alpha+bc\beta=1 \\ &\Longleftrightarrow pgcd(a,bc)=1. \end{aligned}$$

Conséquence :

$$\begin{aligned} pgcd(a,b)=1 &\Longrightarrow pgcd(a,b^2)=1 \\ &\Longrightarrow pgcd(a^2,b)=1 \end{aligned}$$

• Si $pgcd(a,b)=1$ alors $ppcm(a,b)=ab$

• Soit a et b deux entiers relatifs non nuls tels que $pgcd(a,b)=\delta$. Il existe deux entiers relatifs a' et b' non nuls et premiers entre eux tels que $a=a'\delta$ et $b=b'\delta$.

• Si a/c et b/c et si $pgcd(a,b)=1$ alors ab/c.

• Si $\delta=pgcd(a,b)$ et $\mu=ppcm(a,b)$ alors $\delta\mu=|ab|$

Exemple :

$\star$ Trouver deux entiers naturels a et b tels que : $\begin{cases} a+b=20 \\ pgcd(a,b)=4 \end{cases}$

Solution

$$\begin{cases} a+b=20 \\ pgcd(a,b)=4 \end{cases} \iff \begin{cases} a=4a' \ et \ b=4b' \\ pgcd(a',b')=1 \\ a'+b'=5 \end{cases}$$

Donc $(a',b') \in \{(1,4);(2,3);(3,2);(4,1)\}$.

Ainsi, $(a,b) \in \{(4,16);(8,12);(12,8);(16,4)\}$

$\star$ Trouver deux entiers naturels a et b tels que : $\begin{cases} a+b=30 \\ pgcd(a,b)=5 \end{cases}$

IV.4 Equations du type $ax+by=c$

Théorème

Soit l'équation $(E) : ax+by=c$ où $(a,b) \in \mathbb{Z}^*$ et $c \in \mathbb{Z}$.

L'équation (E) admet une solution dans $\mathbb{Z}^2$ si et seulement si $pgcd(a,b)$ divise c.

Théorème

Si $pgcd(a,b)=\delta$ divise c alors l'équation (E) a une infinité de solution de la forme : $\begin{cases} x=x_0-\frac{b}{\delta}t \\ y=y_0+\frac{a}{\delta}t \end{cases}$ $t \in \mathbb{Z}$ où (x_0,y_0) est une solution particulière de l'équation (E)

Preuve

Soit l'équation $(E) : ax+by=c$ et (x_0,y_0) une solution particulière de (E).

$$\begin{cases} ax+by=c \\ ax_0+by_0=c \end{cases} \iff a(x-x_0)+b(y-y_0)=0$$

$$\iff \frac{a}{\delta}(x-x_0)+\frac{b}{\delta}(y-y_0)=0$$

$$\iff \frac{a}{\delta}(x-x_0)=-\frac{b}{\delta}(y-y_0)$$

$\Longleftrightarrow \frac{a}{\delta}/\frac{b}{\delta}(y-y_0)$ et $\frac{b}{\delta}/\frac{a}{\delta}(x-x_0)$ or $\frac{a}{\delta}$ et $\frac{b}{\delta}$ sont premiers entre eux. Donc $\frac{a}{\delta}/(y-y_0)$ et $\frac{b}{\delta}/(x-x_0)$

$\frac{a}{\delta}/(y-y_0) \Longleftrightarrow y-y_0 = \frac{a}{\delta}t, t \in \mathbb{Z}$

$\Longleftrightarrow \boxed{y = y_0 + \frac{a}{\delta}t}$

$\frac{a}{\delta}(x-x_0) = -\frac{b}{\delta}(y-y_0) \Longleftrightarrow \frac{a}{\delta}(x-x_0) = -\frac{b}{\delta}(y_0+\frac{a}{\delta}t-y_0)$

$\Longleftrightarrow \frac{a}{\delta}(x-x_0) = -\frac{b}{\delta}\frac{a}{\delta}t$

$\Longleftrightarrow x-x_0 = -\frac{b}{\delta}t$

$\Longleftrightarrow \boxed{x = x_0 - \frac{b}{\delta}t}$

Exemple :

Résoudre dans $\mathbb{Z}$ les équations $3x+8y=8$ et $1045x+561y=33$.

Trouvons d'abord deux entiers relatifs x_0 et y_0 tels que $3x_0+8y_0=8$.

Après division euclidienne, on a :

$8 = 3(2)+2$ et $3 = 2(1)+1$

$3 = 2(1)+1 \Longleftrightarrow 1 = 3-2$

$\Longleftrightarrow 1 = 3-(8-3(2))$

$\Longleftrightarrow 1 = 3-8+3(2)$

$\Longleftrightarrow 1 = 3(3)+8(-1)$

$\Longleftrightarrow 8 = 3(24)+8(-8)$

$\Longleftrightarrow 3(24)+8(-8)=8$. Donc $x_0 = 24$ et $y_0 = -8$.

Ainsi, $(24,-8)$ sont des solutions particulières de $3x+8y=8$.

Comme $pgcd(3,8)=1$ alors les solutions de l'équation sont :

$\boxed{\boxed{(x,y) \in \{(24-8t, -8+3t); t \in \mathbb{Z}\}}}$

V NOMBRES PREMIERS

Définition

Un nombre entier naturel p est premier s'il possède exactement deux diviseurs positifs qui sont 1 et p.

Propriétés

$\star$ Soit p un nombre premier. L'ensemble des diviseurs positifs de p est $\{1, p\}$.
$\star$ Soit p un nombre premier et d un entier relatif. Si d/p alors $d \in \{-p, -1, 1, p\}$.
$\star$ Soit p un nombre premier et a un entier relatif. Si a ne divise pas p, alors $pgcd(a, p) = 1$ ou $pgcd(a, p) = p$.
$\star$ Pour tout entier naturel X, il existe un p-uplet $(p_1, p_2, \cdots, p_n)$ d'entiers naturels premiers tel que $X = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_n^{\alpha_n}$, $\alpha_i \in \mathbb{N}$. Cette écriture est la décomposition de X en produit de facteurs premiers.

Théorème

Soit $X = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_n^{\alpha_n}$ la décomposition de X en produit de facteurs premiers. X admet exactement $(\alpha_1 + 1)(\alpha_2 + 1) \cdots (\alpha_n + 1)$ diviseurs positifs.

Exemple

Donner le nombre de diviseurs positifs de 60 et déterminer ces diviseurs.
$60 = 2^2 \times 3 \times 5$. Donc 60 a exactement $(2+1)(1+1)(1+1)$ diviseurs positifs c'est à dire 12.

$$\begin{aligned}(2^0 + 2^1 + 2^2)(3^0 + 3^1)(5^0 + 5^1) &= (1+2+4)(1+3)(1+5) \\ &= (1+3+2+6+4+12)(1+5) \\ &= 1{+}5{+}3{+}15{+}2{+}10{+}6{+}30{+}4{+}20{+}12{+}60.\end{aligned}$$

Ainsi, les diviseurs positifs de 60 sont : $1, 2, 3, 4, 5, 6, 10, 12, 15, 20, 30, 60$