



I – Division dans \mathbb{Z}

1– Multiples et diviseurs d'un entier relatif

Définition

Soit a et d deux nombres entiers relatifs tel que $d \neq 0$.

- ▲ On dit que d divise a , ou que d est un diviseur de a si et seulement si il existe un entier relatif q tel que $a = d \times q$. On note $d \mid a$
- ▲ On dit que a est un multiple de d si et seulement si d est un diviseur de a

Exemple

- $3 \mid 51$ car $51 = 3 \times 17$
- 243 est un multiple de 9 car $243 = 9 \times 27$

Remarque

- ◆ Un nombre entier relatif x est pair si et seulement si x est divisible par 2.
Autrement dit : Un nombre entier x est pair si et seulement si il existe $k \in \mathbb{Z}$ tel que $x = 2k$
- ◆ Un nombre entier relatif x est impair si et seulement si x n'est pas divisible par 2.
Autrement dit : Un nombre entier x est impair si et seulement si il existe $k \in \mathbb{Z}$ tel que $x = 2k + 1$

Propriétés

Soient a, b, c, d, n et m des nombres entiers relatifs et $p \in \mathbb{N}^*$

- ★ Si $b \neq 0$ on a : $b \mid a \Leftrightarrow \frac{a}{b} \in \mathbb{Z}$
- ★ Si $d \neq 0$ on a : $d \mid 0$
- ★ $1 \mid a$; $(-1) \mid a$; $a \mid a$ et $(-a) \mid a$
- ★ Si $a \mid b$ et $b \mid c$ alors $a \mid c$
- ★ Si $a \mid b$ et $a \mid c$ alors $a \mid n \times b + m \times c$ pour tout $(n, m) \in \mathbb{Z}^2$
- ★ Si $a \mid b$ et $b \mid a$ alors $a = \pm b$
- ★ Si $a \mid b$ et $b \neq 0$ alors $|a| \leq |b|$
- ★ Si $a \neq 0$, on a : $a^p \mid b^p \Leftrightarrow a \mid b$

Exemples

1) Soient x et y des entiers relatifs. Montrer que $7 \mid (2x + 3y) \Leftrightarrow 7 \mid (5x + 4y)$

Réponse

$$\begin{aligned} \Rightarrow) 7 \mid (2x + 3y) &\Rightarrow 7 \mid 6(2x + 3y) \text{ et } 7 \mid 7(x + 2y) \\ &\Rightarrow 7 \mid [6(2x + 3y) - 7(x + 2y)] \\ &\Rightarrow 7 \mid (5x + 4y) \end{aligned}$$

$$\begin{aligned} \Leftarrow) 7 \mid (5x + 4y) &\Rightarrow 7 \mid 6(5x + 4y) \text{ et } 7 \mid 7(4x + 3y) \\ &\Rightarrow 7 \mid [6(5x + 4y) - 7(4x + 3y)] \\ &\Rightarrow 7 \mid 2x + 3y \end{aligned}$$

$$\text{Donc } 7 \mid (2x + 3y) \Leftrightarrow 7 \mid (5x + 4y)$$

2) Déterminer les nombres entiers naturels n tels que $(n^2 + 1) \mid (n + 1)$.

Réponse

Soit $n \in \mathbb{N}$ tel que $(n^2 + 1) \mid (n + 1)$. Comme $(n^2 + 1) > 0$ et $(n + 1) > 0$ alors $(n^2 + 1) \leq (n + 1)$ ce qui est vérifié que pour $n = 1$. Alors $(n^2 + 1) \mid (n + 1) \Leftrightarrow n = 1$

2 – Division euclidienne dans \mathbb{Z}

Proposition

Soient a et b deux entiers relatifs tels que $b \neq 0$. Il existe un unique couple $(q, r) \in \mathbb{Z} \times \mathbb{N}$ tel que :

$$\begin{cases} a = bq + r \\ 0 \leq r < |b| \end{cases}$$

L'entier q s'appelle le **quotient** et l'entier r s'appelle le **reste** de la division euclidienne de a par b .

Exemples

- Effectuer la division euclidienne de 427 par 9 puis celle de -427 par 9.

$$\text{On a : } 427 = 9 \times 47 + 4 \text{ donc } -427 = 9 \times (-47) - 4 = 9 \times (-48) + 5$$

$$\text{D'où } -427 = 9 \times (-48) + 5$$

- Déterminer les entiers naturels n pour lesquels $3n^2 + 15n + 1$ soit divisible par $n + 1$.

$$\text{On a : } 3n^2 + 15n + 1 = (n+1)(3n+12) - 11$$

$$\text{Donc } (n+1) \mid (3n^2 + 15n + 1) \Leftrightarrow (n+1) \mid (n+1)(3n+12) - 11$$

$$\Leftrightarrow (n+1) \mid 11$$

$$\Leftrightarrow n+1 \in \{1, 11\}$$

$$\Leftrightarrow n \in \{0, 10\}$$

- Résoudre dans \mathbb{Z} l'équation : $x^2 - y^2 = 35$

$$\text{On a : } x^2 - y^2 = 35 \Leftrightarrow (x-y)(x+y) = 35 \text{ et comme on a : } 35 = 1 \times 35 = (-1) \times (-35) = 5 \times 7 = (-5) \times (-7)$$

$$\text{Alors : } x^2 - y^2 = 35 \Leftrightarrow \begin{cases} x-y=1 \\ x+y=35 \end{cases} \text{ ou } \begin{cases} x-y=35 \\ x+y=1 \end{cases} \text{ ou } \begin{cases} x-y=-1 \\ x+y=-35 \end{cases} \text{ ou } \begin{cases} x-y=-35 \\ x+y=-1 \end{cases}$$

$$\text{ou } \begin{cases} x-y=5 \\ x+y=7 \end{cases} \text{ ou } \begin{cases} x-y=7 \\ x+y=5 \end{cases} \text{ ou } \begin{cases} x-y=-5 \\ x+y=-7 \end{cases} \text{ ou } \begin{cases} x-y=-7 \\ x+y=-5 \end{cases}$$

$$\Leftrightarrow \begin{cases} x=18 \\ y=17 \end{cases} \text{ ou } \begin{cases} x=18 \\ y=-17 \end{cases} \text{ ou } \begin{cases} x=-18 \\ y=-17 \end{cases} \text{ ou } \begin{cases} x=-18 \\ y=17 \end{cases} \text{ ou } \begin{cases} x=6 \\ y=1 \end{cases} \text{ ou } \begin{cases} x=6 \\ y=-1 \end{cases}$$

$$\begin{cases} x=-6 \\ y=-1 \end{cases} \text{ ou } \begin{cases} x=-6 \\ y=1 \end{cases}$$

$$\text{Alors } S = \{(18,17); (18,-17); (-18,-17); (-18,17); (6,1); (6,-1); (-6,-1); (-6,1)\}$$

Remarques

- Effectuer une division euclidienne de a par b consiste à déterminer le quotient q et le reste r tels que

$$\begin{cases} a = bq + r \\ 0 \leq r < |b| \end{cases}$$

- $b \mid a \Leftrightarrow r = 0$

II - Plus grand diviseur commun – Plus petit multiple commun

1 – Plus grand commun diviseur de deux entiers

Définition

Soient a et b deux entiers relatifs non nuls.

On appelle le **plus grand commun diviseur** de a et b , et on note $PGCD(a,b)$ ou $a \wedge b$, le plus grand diviseur positif de a et de b .

Exemples

1) Déterminer $PGCD(84,130)$.

Réponse

Déterminons tous les diviseurs de 84 et ceux de 130.

$$\text{On a : } 84 = 1 \times 84 = 2 \times 42 = 3 \times 28 = 4 \times 21 = 6 \times 14 = 7 \times 12. \text{ Donc } D_{84} = \{1, 2, 3, 4, 6, 7, 12, 14, 21, 28, 42, 84\}$$

$$\text{Et } 130 = 1 \times 130 = 2 \times 65 = 5 \times 26 = 10 \times 13. \text{ Donc } D_{130} = \{1, 2, 5, 10, 13, 26, 65, 130\}$$

$$\text{On a aussi : } D_{84} \cap D_{130} = \{1, 2\}. \text{ Alors } PGCD(84,130) = 2$$

2) Déterminer $PGCD(120,111)$ Proposition 1

Soient a et b deux entiers relatifs non nuls.

Tous les diviseurs communs de a et b sont des diviseurs du $PGCD(a,b)$.

Autrement dit : Si $\begin{cases} d|a \\ d|b \end{cases}$ alors $d|a \wedge b$

Remarque

Pour déterminer $a \wedge b$, lorsqu'on connaît a et b , on utilise :

- * Les diviseurs communs
- * L'algorithme d'Euclide
- * La décomposition en produit de facteurs premiers

Proposition 2

Soient a, b et c trois entiers relatifs non nuls. Alors :

- ★ $a \wedge a = |a|$; $a \wedge 1 = 1$; $a \wedge b = b \wedge a$; $a \wedge (b \wedge c) = (a \wedge b) \wedge c$
- ★ Si $d|a$ alors $a \wedge d = |d|$; Si $a \neq 0$ alors $a \wedge 0 = |a|$; $a \wedge b = |b| \Leftrightarrow b|a$
- ★ $1 \leq a \wedge b \leq \min(a,b)$

Proposition 3

Soient a, b et k trois entiers relatifs non nuls. Alors :

$$PGCD(ka, kb) = |k| \times PGCD(a, b)$$

Proposition 4

Soient a et b deux entiers relatifs et $d = a \wedge b$. Alors il existe (a', b') un couple d'entiers relatifs tels que :

$$\begin{cases} a = da' \\ b = db' \\ a' \wedge b' = 1 \end{cases}$$

Définition

Soient a et b deux entiers relatifs non nuls.

On dit que a et b sont **premiers entre eux** si et seulement si $a \wedge b = 1$

2 - Algorithme d'EuclideProposition 1

Soient a et b deux entiers naturels non nuls tels que $a > b$ et soit r le reste de la division euclidienne de a par b

Alors : $a \wedge b = b \wedge r$

Exemples

Déterminer $a \wedge b$ dans chacun des cas suivants :

1) $a = 1986, b = 936$; 2) $a = 2700, b = 909$; 3) $a = 9680, b = 4690$

Réponses

- On a :

$$1986 = 936 \times 2 + 114$$

$$936 = 114 \times 8 + 24$$

$$114 = 24 \times 4 + 18$$

$$24 = 18 \times 1 + 6$$

$$18 = 6 \times 3 + 0$$

$$\text{Donc } PGCD(1986, 936) = 6$$

- On a :

$$2700 = 909 \times 2 + 882$$

$$909 = 882 \times 1 + 27$$

$$882 = 27 \times 32 + 18$$

$$27 = 18 \times 1 + 9$$

$$18 = 9 \times 2 + 0$$

$$\text{Donc } PGCD(2700, 909) = 9$$

Proposition 2

Soient a et b deux entiers naturels non nuls tels que $a > b$.

Si b ne divise pas a , alors le $PGCD(a,b)$ est le dernier reste non nul obtenu par l'algorithme d'Euclide.



Autrement dit :

Si on a :

$$a = b \times q_1 + r_1 \quad ; r_1 \neq 0$$

$$b = r_1 \times q_2 + r_2 \quad ; r_2 \neq 0$$

$$r_1 = r_2 \times q_3 + r_3 \quad ; r_3 \neq 0$$

.....

$$r_n = r_{n+1} \times q_{n+2} + r_{n+2} \quad ; r_{n+2} \neq 0$$

$$r_{n+1} = r_{n+2} \times q_{n+3} + 0$$

$$\text{Alors } \text{PGCD}(a, b) = r_{n+2}$$

3 - Plus petit commun multiple de deux entiers

Définition

Soient a et b deux entiers non nuls.

Le plus petit multiple commun positif non nul de a et b est appelé **le plus petit multiple commun de a et b** .

On le note **PPCM** (a, b) ou $a \vee b$,

Exemple

Déterminer $a \vee b$ dans chacun des cas suivants :

$$1) a = 2, b = 3 \quad ; \quad 2) a = 5, b = 7 \quad ; \quad 3) a = 13, b = 17$$

Réponses

1) Notons $M(a)$ l'ensemble des multiples positifs de a .

$$\text{On a : } M(2) = 2\mathbb{Z}^+ = \{0, 2, 4, 6, 8, 10, 12, \dots\} \text{ et } M(3) = 3\mathbb{Z}^+ = \{0, 3, 6, 9, 12, \dots\}.$$

$$\text{D'où } M(2) \cap M(3) = \{0, 6, 12, \dots\} \text{ Par suite } 2 \vee 3 = 6$$

Proposition 1

Soient a et b deux entiers non nuls. Alors : $|a \times b| = (a \wedge b) \times (a \vee b)$

Remarque

$$\text{On a : } (a \vee b) = \frac{|a \times b|}{(a \wedge b)}$$

Propriétés

Soient a, b et c trois entiers relatifs non nuls. Alors :

- ★ $a \vee a = |a|$
- ★ $a \vee b = b \vee a$
- ★ $a \vee 1 = |a|$
- ★ $(a \vee b) \vee c = a \vee (b \vee c)$
- ★ $a | (a \vee b)$, $b | (a \vee b)$, $(a \vee b) | a \times b$
- ★ Si $b | a$, alors $a \vee b = |a|$
- ★ Si M est un multiple commun de a et b , alors $(a \vee b) | M$.

III- Théorème de Bézout

1 - Théorème de Bézout

Proposition

Soient a et b deux entiers relatifs non nuls et $d \in \mathbb{N}^*$. Alors :

$$a \wedge b = d \Rightarrow (\exists (u, v) \in \mathbb{Z}^2); d = au + bv$$

Remarques

- ♦ La réciproque n'est pas vraie : En effet on a : $2 \times 24 + (-2) \times 18 = 12$ mais $24 \wedge 18 = 6 \neq 12$
- ♦ Le couple (u, v) n'est pas unique : En effet on a : $24 \wedge 18 = 6$ donc $1 \times 24 + (-1) \times 18 = (-2) \times 24 + 3 \times 18 = 6$

Théorème de Bézout

Soient a et b deux entiers relatifs non nuls. Alors :

$$a \wedge b = 1 \Leftrightarrow (\exists (u, v) \in \mathbb{Z}^2); 1 = au + bv$$

Exemples

1) Montrer que : $(\forall n \in \mathbb{Z}); (7n+2) \wedge (3n+1) = 1$.

En effet, on a : $7(3n+1) - 3(7n+2) = 1$, donc si on pose $u = 7$ et $v = -3$ on a : $(3n+1)u + (7n+2)v = 1$

D'après le théorème de Bézout $(7n+2) \wedge (3n+1) = 1$

2) En utilisant les égalités de Bézout, montrer que : $(\exists (u, v) \in \mathbb{Z}^2): au + bv = 18$

Posons $a = 360$ et $b = 234$. En appliquant l'algorithme d'Euclide, on a :

$$a = b + 126 \quad \Rightarrow 126 = a - b$$

$$b = 126 + 108 \quad \Rightarrow 108 = b - 126$$

$$126 = 108 + 18 \quad \Rightarrow 18 = 126 - 108$$

$$108 = 18 \times 6 + 0 \quad \Rightarrow 360 \wedge 234 = 18$$

$$\text{Alors } 18 = 126 - (b - 126) = 2 \times 126 - b = 2(a - b) - b = 2a - 3b$$

$$\text{Donc } 2a + (-3)b = 18$$

En posant $u = 2$ et $v = -3$, on a : $(\exists (u, v) \in \mathbb{Z}^2): au + bv = 18$

2 - Applications du théorème de BézoutThéorème de Gauss

Soient a, b et c trois entiers relatifs non nuls. On a : $\begin{cases} c | ab \\ a \wedge c = 1 \end{cases} \Rightarrow c | b$

Preuve

On a $a \wedge c = 1$, donc d'après le théorème de Bézout $(\exists (u, v) \in \mathbb{Z}^2): au + cv = 1$ donc $(\exists (u, v) \in \mathbb{Z}^2): abu + cbv = b$

Et comme $c | ab$ donc $\exists k \in \mathbb{Z}: ab = ck$. D'où $cku + cbv = b$ donc $c(ku + bv) = b$ alors $c | b$

Corollaire

Soient a, b et c trois entiers relatifs non nuls. On a : $\begin{cases} a | c \\ b | c \\ a \wedge b = 1 \end{cases} \Rightarrow ab | c$

Preuve

On a $a | c$ et $b | c$, donc $\exists (k, h) \in \mathbb{Z}^2: c = ak$ et $c = bh$

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

Donc $c = cau + cbv = hbau + kabv = ab(hu + kv)$. Alors $ab | c$

Proposition

Soient a, b et c trois entiers relatifs non nuls et soit $(n, m) \in \mathbb{N}^{*2}$.

$$\star \begin{cases} a \wedge b = 1 \\ a \wedge c = 1 \end{cases} \Leftrightarrow a \wedge bc = 1$$

$$\star a \wedge b = 1 \Leftrightarrow a \wedge b^n = 1$$

$$\star a \wedge b = 1 \Leftrightarrow a^m \wedge b^n = 1$$

IV - Equation diophantienneDéfinition

Toute équation de la forme $ax + by = c$, où a, b et c sont des entiers relatifs, est appelée une **équation diophantienne**.

Théorème 1

L'équation $ax + by = c$ admet une solution si et seulement si $(a \wedge b) | c$

Preuve

\Rightarrow Supposons que l'équation $ax + by = c$ admet une solution (x_0, y_0) donc $ax_0 + by_0 = c$; posons $d = a \wedge b$ donc $d | a$ et $d | b$ par suite $d | ax_0$ et $d | by_0$ d'où $d | ax_0 + by_0$, alors $d | c$ donc $(a \wedge b) | c$.

\Leftarrow Posons $d = a \wedge b$ et supposons que $(a \wedge b) | c$ donc $d | c$ alors $\exists k \in \mathbb{Z} : c = dk$

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

Donc $c = kd = k(au + bv) = a(ku) + b(kv)$; en posant $x_0 = ku$ et $y_0 = kv$ on a : $ax_0 + by_0 = c$ donc (x_0, y_0) est une solution de l'équation $ax + by = c$

Exemple

Montrer que les équations suivantes admettent des solutions dans chacun des cas suivants :

$$1) 265x + 180y = 30 \quad ; \quad 1230x - 480y = 750 \quad ; \quad 378x - 564y = 90$$

Théorème 2

Si l'équation $(E) : ax + by = c$ admet des solutions et si (x_0, y_0) est une solution de l'équation (E) , alors :

L'ensemble des solutions de l'équation (E) est $S = \left\{ \left(x_0 + \frac{kb}{a \wedge b}, y_0 - \frac{ka}{a \wedge b} \right) / k \in \mathbb{Z} \right\}$.

Preuve**Exemple**

On considère l'équation $(E) : 272x - 180y = 44$

1) Montrer que l'équation (E) admet des solutions

2) Déterminer une solution particulière de l'équation (E)

3) Résoudre l'équation (E)

V - Congruences dans \mathbb{Z} **Définition**

Soit $n \in \mathbb{N}^*$.

Deux entiers relatifs a et b sont dits congrus modulo n si et seulement si $a - b$ est divisible par n . On note $a \equiv b[n]$.

Autrement dit : $a \equiv b[n] \Leftrightarrow n | (a - b) \Leftrightarrow \exists k \in \mathbb{Z} : a - b = nk$

Proposition

Soit $n \in \mathbb{N}^*$.

Soient a et b deux entiers relatifs tels que $a = nq + r$ où $(q, r) \in \mathbb{Z} \times \mathbb{N}$ avec $0 \leq r < n$ et $b = nq' + r'$ où $(q', r') \in \mathbb{Z} \times \mathbb{N}$ avec $0 \leq r' < n$. Alors : $a \equiv b[n] \Leftrightarrow r = r'$

Exemple

On a : $785 = 14 \times 56 + 1$ et $407 = 14 \times 29 + 1$ donc $785 \equiv 1[14]$ et $407 \equiv 1[14]$. Alors $785 \equiv 407[14]$

Propriétés

Soit $n \in \mathbb{N}^*$. Alors :

★ $a \equiv a[n]$ pour tout entier relatif a

★ $\forall (a, b) \in \mathbb{Z}^2 : a \equiv b[n] \Leftrightarrow b \equiv a[n]$

★ $\forall (a, b, c) \in \mathbb{Z}^3 : \begin{cases} a \equiv b[n] \\ b \equiv c[n] \end{cases} \Rightarrow a \equiv c[n]$ (relation de transitivité)

Propriétés (congruence et opérations)Soit $n \in \mathbb{N}^*$.Soient a, a', b et b' quatre entiers relatifs tels que : $a \equiv b[n]$ et $a' \equiv b'[n]$. Alors :

- ★ $a + a' \equiv b + b'[n]$
- ★ $a - a' \equiv b - b'[n]$
- ★ $a \times a' \equiv b \times b'[n]$
- ★ $\forall k \in \mathbb{Z} : k \times a \equiv k \times b[n]$
- ★ $\forall p \in \mathbb{N}^* : a^p \equiv b^p[n]$

Exemples1) Soient x et y deux entiers relatifs tels que $x \equiv 4[7]$ et $y \equiv 3[7]$ alors : $x + y \equiv 4 + 3[7]$ et $5 \times x - 2 \times y \equiv 5 \times 4 - 2 \times 3[7]$ donc $x + y \equiv 0[7]$ et $5 \times x - 2 \times y \equiv 0[7]$ 2) Déterminer le reste de la division euclidienne de 2^{456} par 5 et 2^{437} par 7

* On sait que toute puissance de 1 est égale à 1. Cherchons une puissance de 2 qui est congrue à 1 modulo 5.

On a : $2^4 \equiv 16 \equiv 1[5]$ et $456 = 4 \times 114$ donc $2^{456} \equiv 2^{4 \times 114}[5]$

$$\equiv (2^4)^{114}[5]$$

$$\equiv 1^{114}[5]$$

$$\equiv 1[5]$$

Donc le reste de la division euclidienne de 2^{456} par 5 est 13) Déterminer les entiers relatifs x tels que : $x + 6 \equiv 5[3]$ On a : $x + 6 \equiv 5[3] \Leftrightarrow 6 + x - 6 \equiv 5 - 6[3]$

$$\Leftrightarrow x \equiv -1[3]$$

$$\Leftrightarrow x \equiv 2[3]$$

Donc $S = \{2 + 3k / k \in \mathbb{Z}\}$ 4) Résoudre dans \mathbb{Z} , l'équation : $3x \equiv 5[4]$ On a : $3x \equiv 5[4] \Leftrightarrow 3x \equiv 1[4]$ car $4 \equiv 0[4]$

$x \equiv \dots[4]$	0	1	2	3
$3x \equiv \dots[4]$	0	3	2	1

Donc on déduit à partir du tableau que $3x \equiv 1[4] \Leftrightarrow x \equiv 3[4]$ D'où $S = \{3 + 4k / k \in \mathbb{Z}\}$ ThéorèmeSoit $n \in \mathbb{N}^*$.Soient a, b et c trois entiers relatifs non nuls tels que $d = c \wedge n$. Alors :

$$ac \equiv bc[n] \Leftrightarrow a \equiv b \left[\frac{n}{d} \right]$$

PreuvePropositionSoit n et p deux entiers naturels non nuls.Soient a, b et c trois entiers relatifs non nuls tels que $c \wedge n = 1$. Alors :

- ★ $ac \equiv bc[n] \Leftrightarrow a \equiv b[n]$



$$\star \begin{cases} a \equiv b[n] \\ p | n \end{cases} \Rightarrow a \equiv b[p]$$

$$\star \begin{cases} ac \equiv bc[n] \\ p \text{ premier} \\ p \text{ ne divise pas } n \end{cases} \Rightarrow a \equiv b[p]$$

Exemple

Résoudre dans \mathbb{Z} , l'équation : (E): $2x \equiv 6[14]$

En posant $a = x$, $b = 3$, $c = 2$ et $n = 14$; on a : (E) $\Leftrightarrow ac \equiv bc[n]$ et comme $d = c \wedge n = 2$, alors :

D'après le théorème précédent, on a : $a \equiv b \left[\frac{n}{d} \right]$ soit $x \equiv 3[7]$ D'où $S = \{3 + 7k / k \in \mathbb{Z}\}$

VI – Les nombres premiers**1 Définitions et propriétés****Définition**

Soit p un entier relatif non nul.

- ▲ On dit que p est **premier** s'il admet exactement deux diviseurs positifs **1 et $|p|$**
- ▲ Si p n'est pas premier et $p \geq 2$, on dit qu'il est composé
- ▲ L'ensemble des entiers naturels premiers est noté **P**

Conséquences

- Le nombre 1 n'est pas premier (car il ne possède qu'un seul diviseur)
- Un entier naturel premier p est supérieur ou égal à 2 : $p \geq 2$
- Les nombres premiers positifs inférieurs à 100 sont :
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.

Remarque

Les entiers p et $-p$ tels que $|p| \geq 2$ ont la même primalité (sont premiers tous les deux ou ils ne le sont pas tous les deux). Pour cela on va se limiter dans l'étude des nombres premiers aux entiers naturels.

Proposition 1 (Critère d'arrêt)

- ★ Tout entier naturel n tel que $n \geq 2$, admet au moins un diviseur premier.
- ★ Si n n'est pas premier, alors il admet un diviseur premier p tel que $2 \leq p \leq \sqrt{n}$

Méthode

Pour montrer qu'un entier naturel n est premier ou non, on suit les étapes suivantes :

- On calcule \sqrt{n}
- On détermine tous les nombres premiers p tel que $2 \leq p \leq \sqrt{n}$
- On teste la divisibilité de n par ses nombres
- Conclusion :
 - Si n n'admet aucun diviseur premier p tel que $2 \leq p \leq \sqrt{n}$, alors on affirme que n est premier.
 - Si on trouve qu'un entier premier p tel que $2 \leq p \leq \sqrt{n}$ est un diviseur de n , on arrête la recherche et on affirme que n n'est pas premier.

Exemple

Déterminer parmi les nombres entiers suivants ceux qui sont premiers :

109 ; 203 ; 601.

- On a $\sqrt{109} \approx 10,4$. Les entiers premiers qui sont inférieurs à $\sqrt{109}$ sont : 2 ; 3 ; 5 et 7
Aucun de ses entiers ne divise 109. Alors 109 est premier
- On a $\sqrt{203} \approx 14,2$. Les entiers premiers qui sont inférieurs à $\sqrt{203}$ sont : 2 ; 3 ; 5 ; 7 ; 11 et 13
Et on a : $7 | 203$. Donc 203 n'est pas premier

Proposition 2

Soit $n \in \mathbb{N}$ tel que $n \geq 2$ et non premier. Alors le plus petit diviseur positif de n différent de 1 est premier.

**Proposition 3**

L'ensemble \mathbf{P} des entiers naturels premiers est un ensemble infini.

Crible d'Eratosthène

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
51	52	53	54	55	56	57	58	59	60
61	62	63	64	65	66	67	68	69	70
71	72	73	74	75	76	77	78	79	80
81	82	83	84	85	86	87	88	89	90
91	92	93	94	95	96	97	98	99	100
101	102	103	104	105	106	107	108	109	110
111	112	113	114	115	116	117	118	119	120
121	122	123	124	125	126	127	128	129	130
131	132	133	134	135	136	137	138	139	140
141	142	143	144	145	146	147	148	149	150

Proposition 4

- ★ Si p et q sont deux entiers premiers positifs distincts, alors ils sont premiers entre eux.

Autrement dit : $\forall (p, q) \in \mathbf{P}^2, p \neq q \Rightarrow p \wedge q = 1$

- ★ Si p est premier, alors p est premier avec tous les entiers qu'il ne divise pas.

Autrement dit : $(\forall n \in \mathbb{Z})(\forall p \in \mathbf{P}), (p \text{ ne divise pas } n) \Rightarrow p \wedge n = 1$

Proposition 5 (Théorème de Gauss et nombres premiers)

- ★ Un nombre premier divise un produit de facteurs si, et seulement si, il divise l'un de ces facteurs.

Autrement dit : $(\forall (a, b) \in \mathbb{Z}^2)(\forall p \in \mathbf{P}): p \mid ab \Leftrightarrow p \mid a \text{ ou } p \mid b$

- ★ $(\forall p \in \mathbf{P})(\forall a \in \mathbb{Z})(\forall k \in \mathbb{N}): p \mid a^k \Leftrightarrow p \mid a$

- ★ $\forall (p, p_1, p_2, \dots, p_n) \in \mathbf{P}^{n+1}: p \mid \prod_{i=1}^n p_i \Leftrightarrow [\exists i \in \{1, 2, \dots, n\} / p = p_i]$

2 – Décomposition en produit de facteurs premiers**Théorème fondamental de l'arithmétique**

Tout entier $n \geq 2$, peut se décomposer de façon unique en un produit de facteurs premiers.

Autrement dit : $(\forall n \in \mathbb{N}^* - \{1\})(\exists!(p_1, p_2, \dots, p_k) \in \mathbf{P}^k)(\exists!(\alpha_1, \alpha_2, \dots, \alpha_k) \in \mathbb{N}^{*k}): n = p_1^{\alpha_1} \times p_2^{\alpha_2} \times \dots \times p_k^{\alpha_k}$

Exemple

Décomposer en un produit de facteurs premiers les entiers suivants :

$$a = 12375 \quad ; \quad b = 5096$$

12375	3
4125	3
1375	5
275	5
55	5
11	11
1	

5096	2
2548	2
1274	2
637	7
91	7
13	13
1	

$$\text{Donc : } 12375 = 3^2 \times 5^3 \times 11$$

$$\text{Donc : } 5096 = 2^3 \times 7^2 \times 13$$

Proposition 1

Soit n un entier naturel tel que $n \geq 2$ dont la décomposition en produit de facteurs premiers est :

$n = p_1^{\alpha_1} \times p_2^{\alpha_2} \times \dots \times p_n^{\alpha_n}$ où p_1, p_2, \dots, p_n sont des entiers naturels premiers et $\alpha_1, \alpha_2, \dots, \alpha_n$ sont des entiers naturels. Alors :

★ Tout diviseur d de n a pour décomposition en produit de facteurs premiers :

$$d = p_1^{\beta_1} \times p_2^{\beta_2} \times \dots \times p_n^{\beta_n} \quad \text{avec } 0 \leq \beta_i \leq \alpha_i \text{ pour tout } i \in \{1, 2, \dots, n\}$$

★ Le nombre de diviseurs de n est : $N = (1 + \alpha_1)(1 + \alpha_2) \dots (1 + \alpha_n)$

Exemple

Trouver le nombre de diviseurs de 120 puis déterminer tous ses diviseurs.

On vérifie que $120 = 2^3 \times 3 \times 5$

On a alors $(1+3)(1+1)(1+1) = 16$. Donc 120 possède 16 diviseurs.

Pour déterminer les diviseurs de 120 on peut utiliser le tableau suivant
Donc l'ensemble des diviseurs de 120 est:

$$D_{120} = \{1, 2, 3, 4, 5, 6, 8, 10, 12, 15, 20, 24, 30, 40, 60, 120\}$$

\times	2^0	2^1	2^2	2^3
$3^0 5^0$	1	2	4	8
$3^1 5^0$	3	6	12	24
$3^0 5^1$	5	10	20	40
$3^1 5^1$	15	30	60	120

Proposition 2

Soient a et b deux entiers naturels dont les décompositions en produit de facteurs premiers sont :

$a = p_1^{\alpha_1} \times p_2^{\alpha_2} \times \dots \times p_n^{\alpha_n}$ et $b = p_1^{\beta_1} \times p_2^{\beta_2} \times \dots \times p_n^{\beta_n}$ où $\forall i \in \{1, 2, \dots, n\} : p_i \in \mathbf{P}$ et $(\alpha_i, \beta_i) \in \mathbb{N}^2$. Alors :

★ $a \wedge b = p_1^{\inf(\alpha_1, \beta_1)} \times p_2^{\inf(\alpha_2, \beta_2)} \times \dots \times p_n^{\inf(\alpha_n, \beta_n)}$

★ $a \vee b = p_1^{\sup(\alpha_1, \beta_1)} \times p_2^{\sup(\alpha_2, \beta_2)} \times \dots \times p_n^{\sup(\alpha_n, \beta_n)}$

Exemple

Déterminer $a \wedge b$ et $a \vee b$ dans les cas suivants :

1) $a = 198, b = 256$; 2) $a = 168, b = 204$; 3) $a = 4294, b = 3521$

3 – Petit théorème de Fermat**Théorème (Petit théorème de Fermat)**

Soit p un nombre premier et a un entier naturel non divisible par p , alors $a^{p-1} \equiv 1[p]$ ou encore $p \mid (a^{p-1} - 1)$

Corollaire du petit théorème de Fermat

Soit p un nombre premier et a un entier naturel, alors $a^p \equiv a[p]$.

Théorème de Wilson

Soit p un entier naturel tel que : $p \geq 2$. Alors :

p est premier $\Leftrightarrow (p-1)! + 1$ est divisible par p .

VII – L'ensemble $\mathbb{Z}/n\mathbb{Z}$ **1 – Classe d'équivalence**

Soit $n \in \mathbb{N}^*$.

★ L'ensemble des entiers relatifs qui ont le même reste r de la division euclidienne par n , est appelée **La classe d'équivalence de r** et est notée \bar{r} .

Autrement dit : $\bar{r} = \{x \in \mathbb{Z} / x \equiv r[n]\} = \{r + nk / k \in \mathbb{Z}\}$

★ Plus généralement : Si $a \in \mathbb{Z}$ et $n \in \mathbb{N}^*$.

La classe d'équivalence de a modulo n est l'ensemble défini par :

$$\bar{a} = \{x \in \mathbb{Z} / x \equiv a[n]\} = \{a + nk / k \in \mathbb{Z}\}$$

Exemple



♦ Si $n = 2$, on a : $\bar{0} = \{x \in \mathbb{Z} / x \equiv 0[2]\} = \{2k / k \in \mathbb{Z}\} = 2\mathbb{Z}$

Et $\bar{1} = \{x \in \mathbb{Z} / x \equiv 1[2]\} = \{1 + 2k / k \in \mathbb{Z}\}$

Donc $\bar{0}$ est l'ensemble des entiers relatifs pairs et $\bar{1}$ est l'ensemble des entiers relatifs impairs, par suite :

Pour $n = 2$, on a : $\bar{0} \cup \bar{1} = \mathbb{Z}$

♦ Si $n = 3$, on a : $\bar{0} = \{x \in \mathbb{Z} / x \equiv 0[3]\} = \{3k / k \in \mathbb{Z}\}$, $\bar{1} = \{x \in \mathbb{Z} / x \equiv 1[3]\} = \{3k + 1 / k \in \mathbb{Z}\}$

Et $\bar{2} = \{x \in \mathbb{Z} / x \equiv 2[3]\} = \{3k + 2 / k \in \mathbb{Z}\}$. De plus on a : $\mathbb{Z} = \bar{0} \cup \bar{1} \cup \bar{2}$

♦ Modulo 9, on a : $\overline{77} = \bar{5} = \{5 + 9k / k \in \mathbb{Z}\}$; $\overline{204} = \bar{6} = \{6 + 9k / k \in \mathbb{Z}\}$.

Proposition

Soit $n \in \mathbb{N}^*$.

Pour tout $x \in \mathbb{Z}$, on désigne par \bar{x} la classe d'équivalence de x modulo n . Alors :

★ $(\forall a \in \mathbb{Z})(\exists! r \in \{0, n-1\}) : a = \bar{r}$

★ Si $0 \leq r < n$ et $0 \leq r' < n$, alors :

1) $\bar{r} = \bar{r}' \Leftrightarrow r = r'$

2) $r \neq r' \Leftrightarrow \bar{r} \cap \bar{r}' = \emptyset$

★ $(\forall a \in \mathbb{Z})(\exists! r \in \{0, n-1\}) : a \in \bar{r}$

★ $\mathbb{Z} = \bar{0} \cup \bar{1} \cup \dots \cup \overline{(n-1)}$

Notation

Soit $n \in \mathbb{N}^*$.

L'ensemble des classes d'équivalence modulo n est noté : $\mathbb{Z} / n\mathbb{Z}$.

On a : $\mathbb{Z} / n\mathbb{Z} = \{\bar{0}, \bar{1}, \bar{2}, \dots, \overline{(n-1)}\}$. Donc : $card(\mathbb{Z} / n\mathbb{Z}) = n$.

Exemple

On a : $\mathbb{Z} / 2\mathbb{Z} = \{\bar{0}, \bar{1}\}$; $\mathbb{Z} / 3\mathbb{Z} = \{\bar{0}, \bar{1}, \bar{2}\}$; $\mathbb{Z} / 7\mathbb{Z} = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}, \bar{6}\}$

2 - Opérations dans l'ensemble $\mathbb{Z} / n\mathbb{Z}$

Définition

Soit $n \in \mathbb{N}^*$.

▲ L'addition $+$ dans $\mathbb{Z} / n\mathbb{Z}$ est définie, pour tout \bar{x} et \bar{y} de $\mathbb{Z} / n\mathbb{Z}$ par : $\overline{\bar{x} + \bar{y}} = \overline{x + y}$.

▲ La multiplication \times dans $\mathbb{Z} / n\mathbb{Z}$ est définie, pour tout \bar{x} et \bar{y} de $\mathbb{Z} / n\mathbb{Z}$ par : $\overline{\bar{x} \times \bar{y}} = \overline{x \times y}$

Exemples

▪ On définit l'addition dans $+$ $\mathbb{Z} / 5\mathbb{Z}$ par :

+	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$
$\bar{0}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$
$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{0}$
$\bar{2}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{0}$	$\bar{1}$
$\bar{3}$	$\bar{3}$	$\bar{4}$	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{4}$	$\bar{4}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$

\times	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$
$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$
$\bar{1}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$
$\bar{2}$	$\bar{0}$	$\bar{2}$	$\bar{4}$	$\bar{1}$	$\bar{3}$
$\bar{3}$	$\bar{0}$	$\bar{3}$	$\bar{1}$	$\bar{4}$	$\bar{2}$
$\bar{4}$	$\bar{0}$	$\bar{4}$	$\bar{3}$	$\bar{2}$	$\bar{4}$

▪ Résoudre dans $\mathbb{Z} / 5\mathbb{Z}$, les équations suivantes :

$\bar{3}x = \bar{2}$; $\bar{2}x^2 + \bar{3}x + \bar{1} = \bar{0}$; $(\bar{3}x - \bar{1})(\bar{2}x + \bar{3}) = \bar{0}$

1) $\bar{3}x = \bar{2}$

x	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$
$\bar{3}x$	$\bar{0}$	$\bar{3}$	$\bar{1}$	$\bar{4}$	$\bar{2}$

$$\text{Donc } S = \bar{4} = \{4 + 5k / k \in \mathbb{Z}\}$$

$$2) \bar{2}x^2 + \bar{3}x + \bar{1} = \bar{0}$$

x	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$
x^2	$\bar{0}$	$\bar{1}$	$\bar{4}$	$\bar{4}$	$\bar{1}$
$\bar{2}x^2$	$\bar{0}$	$\bar{2}$	$\bar{3}$	$\bar{3}$	$\bar{2}$
$\bar{3}x$	$\bar{0}$	$\bar{3}$	$\bar{1}$	$\bar{4}$	$\bar{2}$
$\bar{2}x^2 + \bar{3}x + \bar{1}$	$\bar{1}$	$\bar{1}$	$\bar{0}$	$\bar{3}$	$\bar{0}$

$$\text{Donc : } S = \bar{2} \cup \bar{4} = \{2 + 5k, 4 + 5k / k \in \mathbb{Z}\}$$

Proposition

Soit p un nombre premier positif. Alors :

- ★ $(\forall \bar{x} \in \mathbb{Z} / p\mathbb{Z} - \{\bar{0}\})(\exists \bar{y} \in \mathbb{Z} / p\mathbb{Z} - \{\bar{0}\}) : \bar{x} \times \bar{y} = \bar{1}$
- ★ $(\forall \bar{x} \in \mathbb{Z} / p\mathbb{Z})(\forall \bar{y} \in \mathbb{Z} / p\mathbb{Z}) : \bar{x} \times \bar{y} = \bar{0} \Leftrightarrow (\bar{x} = \bar{0} \text{ ou } \bar{y} = \bar{0})$

VIII – Système de numération

1- Bases de numération

Les bases de numération sont un concept fondamental en mathématiques, elles représentent la manière dont les nombres sont exprimés en fonction d'un système de nombres élémentaires. Les bases les plus courantes sont la base 10 (le système décimal), la base 2 (le système binaire), la base 8 (le système octal), la base 16 (le système hexadécimal) et la base 60 (le système sexagésimal). Voici un aperçu des bases les plus courantes :

- ✚ Base 10 (Décimale) :

Utilise les chiffres 0,1,2,3,4,5,6,7,8 et 9

$$\text{Par exemple : } 3526 = \overline{3526}^{(10)} = 3 \times 10^3 + 5 \times 10^2 + 2 \times 10^1 + 6 \times 10^0$$

- ✚ Base 2 (Binaire) :

Utilise les chiffres : 0 et 1

$$\text{Par exemple : } \overline{110101}^{(2)} = 1 \times 2^5 + 1 \times 2^4 + 0 \times 2^3 + 1 \times 2^2 + 0 \times 2^1 + 1 \times 2^0$$

- ✚ Base 8 (Octale) :

Utilise les chiffres 0,1,2,3,4,5,6 et 7

$$\text{Par exemple : } \overline{2715}^{(8)} = 2 \times 8^3 + 7 \times 8^2 + 1 \times 8^1 + 5 \times 8^0$$

Moins utilisée que la base 2 et la base 10

- ✚ Base 16 (Hexadécimale) :

Utilise les chiffres 0,1,2,3,4,5,6,7,8,9 et les lettres A,B,C,D,E,F (représentant 10,11,12,13,14,15)

$$\text{Par exemple : } \overline{1A9D2F}^{(16)} = 1 \times 16^5 + 10 \times 16^4 + 9 \times 16^3 + 13 \times 16^2 + 2 \times 16^1 + 15 \times 16^0$$

Souvent utilisée en informatique pour représenter des adresses mémoire et des valeurs binaires de manière plus compacte.

- ✚ Base 60 (Sexagésimale)

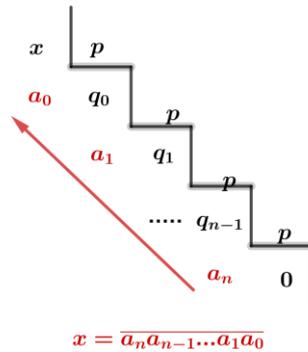
Théorème

Soit p un entier naturel tel que $p \geq 2$.

Tout entier naturel x s'écrit d'une façon unique : $x = \sum_{k=0}^n a_k p^k$ où les a_k sont des entiers naturels tels que

$$0 \leq a_k < p \text{ avec } a_n \neq 0 \text{ si } x \neq 0 \text{ et } n = 0 \text{ si } x = 0.$$

La suite a_0, a_1, \dots, a_n est appelée développement de x en base p et l'on écrit : $x = \overline{a_n a_{n-1} \dots a_1 a_0}^{(p)}$



Remarque

En base 10, on utilise la notation habituelle de l'écriture des nombres par exemple 5427 au lieu de $\overline{5427}^{(10)}$

Exemple

1) Ecrire 3654 en base 7.

Donc :

$$3654 = \overline{13440}^{(7)}$$

2) Ecrire $\overline{1010001}^{(2)}$ e, base 10

On a : $\overline{1010001}^{(2)} = 1 \times 2^6 + 1 \times 2^4 + 1 = 81$

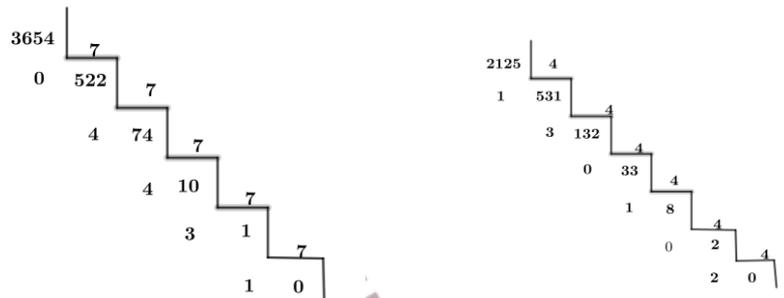
3) Ecrire $\overline{6124}^{(7)}$ en base 4.

On a : $\overline{6124}^{(7)} = 6 \times 7^3 + 1 \times 7^2 + 2 \times 7 + 4 = 2125$

Et on a :

$$2125 = \overline{201031}^{(4)}$$

D'où : $\overline{6124}^{(7)} = \overline{201031}^{(4)}$



[HTTPS://WWW.DIMAMATH.COM](https://www.dimamath.com)
 Smail Eljaafari
 ✨ ✨

Proposition

Soit p un entier naturel tel que $p \geq 2$.

Soient x et y deux entiers naturels tels que : $x = \overline{a_n a_{n-1} \dots a_1 a_0}^{(p)}$ et $y = \overline{c_m c_{m-1} \dots c_1 c_0}^{(p)}$.

- ★ Si $m > n$, alors $y > x$.
- ★ Si $m = n$ et $c_n = a_n, c_{n-1} = a_{n-1}, \dots, c_{i+1} = a_{i+1}$ et $c_i > a_i$, alors $y > x$
- Et si $c_i < a_i$, alors $y < x$.

Exemples

• On pose $x = \overline{23615}^{(8)}$ et $y = \overline{7926}^{(8)}$

Le nombre de chiffres formant x est 5 et le nombre de chiffres formant y est 4 et puisque $5 > 4$ alors $x > y$

• On pose : $x = \overline{32410}^{(5)}$ et $y = \overline{32432}^{(5)}$

Les entiers x et y sont formés par le même nombre de chiffres 5. Et comme $3 > 2$, alors $y > x$.

2 – Addition et multiplication dans le même système de numération

Exemples

Calculer 1) $\overline{3514}^{(6)} + \overline{532}^{(6)}$ et 2) $\overline{251}^{(6)} \times \overline{132}^{(6)}$.

1) Calculons $\overline{3514}^{(6)} + \overline{532}^{(6)}$

1^{ère} méthode

On a : $\overline{3514}^{(6)} = 3 \times 6^3 + 5 \times 6^2 + 1 \times 6 + 4$ et $\overline{532}^{(6)} = 5 \times 6^2 + 3 \times 6 + 2$



On a : $a_0 = 0$ donc $x \equiv 0[2]$ et $a_0 + a_1 + a_2 + a_3 + a_4 = 5 + 9 + 4 = 18$, donc $18 \equiv 0[3]$ donc $x \equiv 0[3]$
Et $18 \equiv 0[9]$ donc $x \equiv 0[9]$. Puisque $a_0 = 0$ donc $x \equiv 0[5]$. Comme $a_1 a_0 = 00 \equiv 0[4]$ alors $x \equiv 0[4]$.
De même $a_1 a_0 = 00 \equiv 0[25]$ donc $x \equiv 0[25]$.
On a aussi $a_4 - a_3 + a_2 - a_1 + a_0 = 4 - 9 + 5 - 0 + 0 = 0 \equiv 0[11]$ donc $x \equiv 0[11]$.

