Mathématiques : 1Bac SM

Séance 14-1 : Arithmétique dans $\mathbb{Z}$ (Cours)

Professeur : Mr CHEDDADI Haitam

Sommaire

I- Divisibilité dans l'ensemble $\mathbb{Z}$

1-1/ Divisibilité dans $\mathbb{Z}$

1-2/ Division euclidienne dans $\mathbb{N}$

1-3/ Division euclidienne dans $\mathbb{Z}$

II- Nombres premiers

2-1/ Nombres premiers

2-2/ Détermination des nombres premiers

2-3/ Décomposition en produit de facteurs premiers

III- Plus grand commun diviseur - Plus petit commun multiple

3-1/ Plus grand commun diviseur

3-2/ Calcul pratique du P.G.C.D : L'algorithme d'Euclide

3-3/ Plus petit commun multiple

3-4/ Nombre de diviseurs d'un entier naturel non nul

IV- Congruence module n

4-1/ Congruences module n

4-2/ Propriétés de la relation « congruence modulo »

V- L'ensemble $\mathbb{Z}/n\mathbb{Z}$

5-1/ Classes d'équivalence

5-2/ Opérations dans l'ensemble $\mathbb{Z}/n\mathbb{Z}$

I- Divisibilité dans l'ensemble $\mathbb{Z}$

1-1/ Divisibilité dans $\mathbb{Z}$

Définition

Soit a et b deux entiers relatifs.

On dit que a divise b, et on écrit a/b s'il existe $k \in \mathbb{Z}$ tel que $b = ak$.

Autrement dit : $a/b \Leftrightarrow [(\exists k \in \mathbb{Z}) : \ b = ka]$

On dit aussi que b est divisible par a, ou que b est un multiple de a, ou encore que a est un diviseur de b.

Applications

Soit a et b deux entiers relatifs non nuls.

1. Montrer que : $b/a \Leftrightarrow |b| \leq |a|$

Soit x et y deux éléments de $\mathbb{Z}^*$, et n un entier naturel non nul.

2. a- Montrer l'équivalence suivante : $xy = 1 \Leftrightarrow (x = y = 1 \ ou \ x = y = -1)$
2. b- Montrer que si x divise y, alors : x/y^n et x^n/y^n

Proposition

Soit a, b, c et d des éléments de $\mathbb{Z}$.

Alors :

$$\boxed{1} \ a/a \ et \ a/-a \ et \ a/ab$$
$$\boxed{2} \ a/b \Leftrightarrow a/-b$$
$$\boxed{3} \ (a/b \ et \ b/c) \Rightarrow a/c$$
$$\boxed{4} \ (a/b \ et \ a/c) \Rightarrow (a/b+c \ et \ a/b-c)$$
$$\boxed{5} \ (a/b \ et \ b/a) \Rightarrow |a| = |b|$$
$$\boxed{6} \ (a/b \ et \ c/d) \Rightarrow ac/bd$$
$$\boxed{7} \ \left(\forall (\alpha;\beta) \in \mathbb{Z}^2\right) : \ (a/b \ et \ a/c) \Rightarrow a/\alpha b + \beta c$$

Applications

Soit a, b, c, x et y des éléments de $\mathbb{Z}$ tels que $a/x-y$ et $a/b-c$.

1. Montrer que : $a/bx-cy$

Soit d et n deux entiers relatifs.

2. Établir l'implication : $\begin{cases} d/n^2+3 \\ d/2n-1 \end{cases} \Rightarrow d/13$
3. Déterminer toutes les valeurs de l'entier relatif n pour lesquelles : $n-17/n-1$

Soit $(x;y) \in \mathbb{Z}^2$ et d un diviseur commun des entiers x et y.

4. Déterminer les valeurs possibles de d sachant que : $4x - 13y = 5$
5. Résoudre dans $\mathbb{Z}^2$ l'équation suivante : $(x+1)(y+2) = 2xy$

1-2/ Division euclidienne dans $\mathbb{N}$

Théorème

Soit a et b deux entiers naturels tels que $a \neq 0$.

Il existe un unique couple $(q;r) \in \mathbb{N}^2$ tel que $b = aq + r$ et $0 \leq r < a$.

L'opération qui permet la détermination du couple $(q;r)$ est appelée la division euclidienne de l'entier b par l'entier a dans $\mathbb{N}$.

Les entiers b, a, q et r sont appelés respectivement le dividende, le diviseur, le quotient et le reste.

1-2/ Division euclidienne dans $\mathbb{Z}$

Soit a et b deux entiers naturels tels que $a \neq 0$.

Il existe un unique couple $(q;r) \in \mathbb{Z} \times \mathbb{N}$ tel que $b = aq + r$ et $0 \leq r < a$.

L'opération qui permet la détermination du couple $(q;r)$ est appelée la division euclidienne de l'entier b par l'entier a dans $\mathbb{Z}$.

Les entiers b, a, q et r sont appelés respectivement le dividende, le diviseur, le quotient et le reste.

Applications

1. Déterminer le quotient et le reste de la division euclidienne de b par a dans chacun des cas suivants :

$\boxed{1}\ a = 5 \ \ et \ \ b = 67$ $\boxed{2}\ a = 5 \ \ et \ \ b = -67$ $\boxed{3}\ a = -5 \ \ et \ \ b = 67$	$\boxed{4}\ a = -5 \ \ et \ \ b = -67$ $\boxed{5}\ a = 29 \ \ et \ \ b = -314$ $\boxed{6}\ a = -13 \ \ et \ \ b = -76$

Les restes de la division euclidienne des nombres 4294 et 3512 par un entier naturel non nul a sont respectivement 10 et 12.

2. Déterminer la valeur de a.

La division euclidienne de l'entier 1517 par un entier naturel x donne 75 comme quotient et r comme reste.

3. Déterminer les valeurs des nombres x et r.

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

On désigne par q et r le quotient et le reste de la division euclidienne de 125 par n respectivement.

4. Déterminer les valeurs de q et r sachant que $r = q^2$.

II- Nombres premiers

2-1/ Nombres premiers

Définition

Soit $p \in \mathbb{Z}$

On dit que p est un nombre premier si $|p| \neq 1$ et $D_p = \{-1; 1; -p - p\}$, où D_p désigne l'ensemble des diviseurs de p.

Remarque

Si p est premier dans $\mathbb{N}$, alors $-p$ est premier dans $\mathbb{Z}$.

Plus précisément :

(p est premier dans $\mathbb{Z}$)$\Leftrightarrow$ $CardD_p = 4$; (p est premier dans $\mathbb{N}$)$\Leftrightarrow$ $CardD_p = 2$

C'est pour cette raison qu'on va se contenter dans la suite du ce chapitre du traitement des nombres positifs, et l'ensemble des nombres premiers positifs sera noté $\mathbb{P}$.

On a donc l'équivalence : $x \in \mathbb{P}$ $\Leftrightarrow$($x \in \mathbb{N}$ et x premier)

Applications

1. Montrer que les nombres suivants ne sont pas premiers :

$$4825 \ - \ 7281 \ - \ 2501 \ - \ 111 \ - \ 111111 \ - \ 25008$$

2. Montrer que tout nombre premier positif et distinct de 2 et 3 s'écrit sous la forme $6p+1$ ou $6p+5$.

Pour tout $n \in \mathbb{N}$, on pose : $P\left(n\right) = 10n + 7$

3. Déterminer les valeurs de n inférieur à 10 et pour lesquelles $P\left(n\right)$ n'est pas un nombre premier.

2-2/ Détermination des nombres premiers

Proposition

Soit a un nombre non premier et différent de 1.

Le plus petit diviseur propre de a (c'est-à-dire distinct de 1 et a) est un nombre premier.

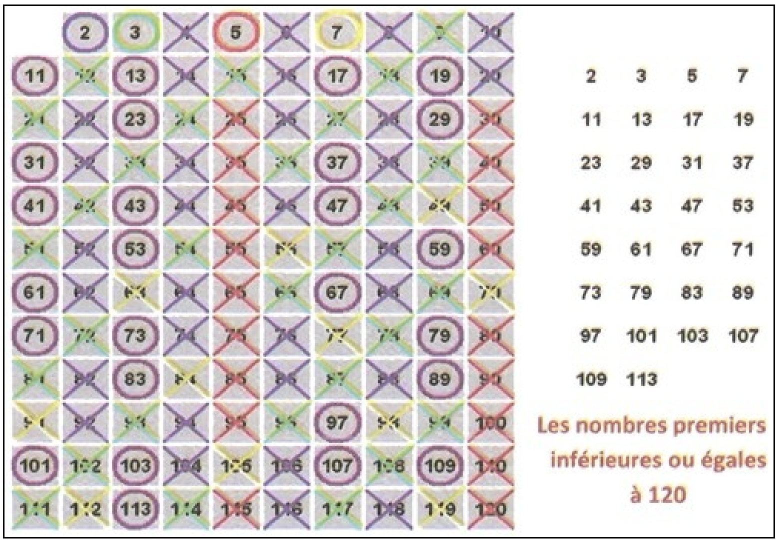
Théorème

Soit n un entier non premier et supérieur ou égal à 2.

Alors, il existe au moins un diviseur premier p du nombre n et vérifiant $p^2 \leq n$.

En d'autres termes :

(n est un nombre premier)$\Leftrightarrow$(n n'admet pas de diviseur premier dans $\left[2; \sqrt{n}\right] \cap \mathbb{N}$)



Applications

1. Parmi les nombres suivants, lesquels sont des nombres premiers :

$$127 \ - \ 1979 \ - \ 2017 \ - \ 13957 \ - \ 3599 \ - \ 2309$$

2. En utilisant le crible d'Eratosthène, déterminer les nombres premiers qui existent entre 100 et 150.

Pour tout $n \in \mathbb{N}$, on pose : $M_n = \frac{3^n - 1}{2}$

3. Montrer que si M_n est premier, alors n est un nombre premier.

Théorème

L'ensemble $\mathbb{P}$ des nombres premiers positifs est infini.

2-3/ Décomposition en produit de facteurs premiers

Tout entier relatif n distinct de 1 et -1 peut s'écrire et de façon unique sous la forme $n = \varepsilon p_1{}^{\alpha_1} p_2{}^{\alpha_2} \ldots . p_k{}^{\alpha_k}$ où $p_1, p_2, \ldots . p_k$ des nombres premiers positifs et distincts, $\alpha_1, \alpha_2, \ldots . \alpha_k$ des éléments de $\mathbb{N}^*$ et $\varepsilon = \pm 1$.

Cette écriture est appelée la décomposition de n en produit de facteurs premiers.

Technique

420	2
210	2
105	3
35	5
7	7
1	

Applications

1. Décomposer les nombres suivants en produit de facteurs premiers :

$$10000 \ ; \ 8200 \ ; \ 1332 \ ; \ 1777 \ ; \ \ -1032 \ ; \ 111333 \ ; \ \ -51480$$

2. Décomposer en produit de facteurs premiers le nombre $a = 6^6 + 1$.
3. Décomposer en produit de facteurs premiers le nombre $x = 100^{2n}$ où $n \in \mathbb{N}^*$.

Proposition

Soit n un entier naturel supérieur ou égal à 2 et tel que sa décomposition en produit de facteurs premiers est : $n = p_1{}^{\alpha_1} p_2{}^{\alpha_2} \ldots . p_k{}^{\alpha_k}$

- Pour qu'un entier naturel d soit un diviseur de n, il faut et il suffit que sa décomposition en produit de facteurs premiers s'écrit sous la forme $d = p_1{}^{\beta_1} p_2{}^{\beta_2} \ldots . p_k{}^{\beta_k}$ avec $0 \leq \beta_i \leq \alpha_i$ pour tout $i \in \{1; 2; \ldots ; k\}$.

- Pour qu'un entier naturel m soit un multiple de n, il faut et il suffit que sa décomposition en produit de facteurs premiers s'écrit sous la forme $m = p_1{}^{\gamma_1} p_2{}^{\gamma_2} \ldots . p_k{}^{\gamma_k} \times a$ avec $\alpha_i \leq \gamma_i$ pour tout $i \in \{1; 2; \ldots ; k\}$ et a est produit des facteurs premiers distincts de $p_1, p_2, \ldots . p_k$.

III- Plus grand commun diviseur - Plus petit commun multiple

3-1/ Plus grand commun diviseur

Définition

Soit a et b deux entiers relatifs non nuls.

Le plus grand commun diviseur de a et b, noté $a \wedge b$ ou $PGCD\,(a, b)$ ou $\Delta\,(a, b)$, est le plus grand des diviseurs strictement positifs communs à a et b.

Remarques

- On convient que pour tout $a \in \mathbb{Z}$: $a \wedge 0 = |a|$

- La définition précédente peut être encore formulée par l'équivalence suivante :

$$\delta = a \wedge b \Leftrightarrow \begin{cases} \delta/a \; et \; \delta/b \\ (\forall d \in D_a \cap D_b) : \; d \leq \delta \end{cases}$$

- Soit a et b deux entiers relatifs non nuls.

Si $\delta = a \wedge b$ alors :

- $\delta \geq 1$ et δ/a et δ/b.
- Pour tout $d \in \mathbb{Z}^*$: $(d/a \; et \; d/b) \Rightarrow d/\delta$

Proposition

Soit a, b et c des entiers relatifs non nuls et n un entier naturel non nul.

Alors :

$$\boxed{1}\; a \wedge b = |a| \wedge |b|$$
$$\boxed{2}\; a \wedge b = b \wedge a$$
$$\boxed{3}\; a \wedge a = a \wedge 0 = |a|$$
$$\boxed{4}\; a \wedge 1 = 1$$
$$\boxed{5}\; (a \wedge b) \wedge c = a \wedge (b \wedge c)$$
$$\boxed{6}\; a/b \Leftrightarrow a \wedge b = |a|$$
$$\boxed{7}\; a^n \wedge a = |a|$$

3-2/ Calcul pratique du P.G.C.D : L'algorithme d'Euclide

Soit a et b deux entiers relatifs non nuls.

Si $a = bq + r$ et $0 < r < b$, alors : $a \wedge b = b \wedge r$

En d'autres termes : Lorsque b ne divise pas a, le plus grand commun diviseur des entiers a et b est égal au dernier reste non nul obtenu grâce à l’algorithme d'Euclide.

Explication de l'algorithme d'Euclide

On considère deux entiers $a \in \mathbb{Z}^*$ et $b \in \mathbb{N}^*$.

- On effectue la division euclidienne de a par b : $a = bq_1 + r_1$ avec $0 \leq r_1 < b$

  - Si $r_1 = 0$, on arrête l’algorithme en déduisant que $a \wedge b = b$.

- Si $r_1 \neq 0$, on continue.

- On effectue la division euclidienne de b par r_1 : $b = r_1 q_2 + r_2$ avec $0 \leq r_2 < r_1$

- Si $r_2 = 0$, on arrête l'algorithme en déduisant que $a \wedge b = r_1$.
- Si $r_2 \neq 0$, on continue.

- Etc.

Notons que le processus engagé va s'arrêter, car sinon, on construirait une suite d'entiers naturels strictement décroissante, ce qui est impossible.

Il existe donc un entier $p \in \mathbb{N}$ tel que $r_p \neq 0$ et $r_{p+1} = 0$.

Par conséquent : $a \wedge b = r_p$

Applications

1. En utilisant l'algorithme d'Euclide, déterminer le plus grand commun diviseur des entiers relatifs a et b dans chacun des cas suivants :

$$\boxed{1}\ a = 134\ et\ b = 25$$
$$\boxed{2}\ a = 336\ et\ b = 124$$
$$\boxed{3}\ a = -74\ et\ b = -24$$
$$\boxed{4}\ a = 21384\ et\ b = 613$$
$$\boxed{5}\ a = -1074\ et\ b = 323$$

Soit n un entier naturel supérieur ou égal à 2.

2. En utilisant l'algorithme d'Euclide, montrer que :

$$\left(n^3 + 3n^2 + n + 1\right) \wedge n^2 = n^2 \wedge (n+1)$$

Proposition

Soit a, b et c des entiers relatifs non nuls.

Alors :

$$\boxed{1}\ \left(c/a\ et\ c/b\right) \Leftrightarrow c/a \wedge b$$
$$\boxed{2}\ (ca) \wedge (cb) = |c|\,(a \wedge b)$$
$$\boxed{3}\ \begin{cases} c/a \\ c/b \end{cases} \Rightarrow \left(\frac{a}{c}\right) \wedge \left(\frac{b}{c}\right) = \frac{a \wedge b}{|c|}$$

Soit $(a;b) \in \left(\mathbb{N}^*\right)^2$ tel que $a = {p_1}^{\alpha_1}{p_2}^{\alpha_2} \ldots . {p_k}^{\alpha_k}$ et $b = {p_1}^{\beta_1}{p_2}^{\beta_2} \ldots . {p_k}^{\beta_k}$ avec $p_1, p_2, \ldots . p_k$ des nombres premiers positifs et distincts et $\beta_i = 0$ si p_i n'apparaît pas dans la décomposition de b et $\alpha_i = 0$ si p_i n'apparaît pas dans la décomposition de a.

Alors :

$$a \wedge b = {p_1}^{\gamma_1}{p_2}^{\gamma_2} \ldots . {p_k}^{\gamma_k} \text{ avec } \gamma_i = inf\left(\alpha_i; \beta_i\right) \text{ pour tout } i \in \{1; 2; \ldots; k\}$$

3-3/ Plus petit commun multiple

Définition

Soit a et b deux entiers relatifs non nuls.

Le plus petit commun multiple de a et b, noté $a \vee b$ ou $PPCM\,(a,b)$ ou $M\,(a,b)$, est le plus petit des multiples strictement positifs communs à a et b.

Remarques

- On convient que pour tout $a \in \mathbb{Z}$: $a \vee 0 = 0$

- En notant $a\mathbb{Z}$ l'ensemble des multiples de a, on a :
$a\mathbb{Z} = \{\ldots; -3a; -2a; -a; 0; a; 2a; 3a; \ldots\}$
Le plus petit élément de l'ensemble $(a\mathbb{Z} \cap b\mathbb{Z}) \cap \mathbb{N}^*$ est donc $a \vee b$.

- Soit a et b deux entiers relatifs non nuls.

Si $m = a \vee b$, alors :

- $m \geq 1$ et a/m et b/m.
- Pour tout $c \in \mathbb{Z}$: $(a/c\; et\; b/c) \Rightarrow m/c$

Proposition

Soit a, b et c des entiers relatifs non nuls.

Alors :

$$\boxed{1}\; a \vee b = |a| \vee |b|$$
$$\boxed{2}\; a \vee b = b \vee a$$
$$\boxed{3}\; a \vee a = |a|$$
$$\boxed{4}\; a \vee 1 = |a|$$
$$\boxed{5}\; (a \vee b) \vee c = a \vee (b \vee c)$$
$$\boxed{6}\; a/b \Leftrightarrow a \vee b = |b|$$
$$\boxed{7}\; a \vee b/ab$$

Soit $(a;b) \in (\mathbb{N}^*)^2$ tel que $a = {p_1}^{\alpha_1}{p_2}^{\alpha_2}\ldots.{p_k}^{\alpha_k}$ et $b = {p_1}^{\beta_1}{p_2}^{\beta_2}\ldots.{p_k}^{\beta_k}$ avec $p_1, p_2, \ldots.p_k$ des nombres premiers positifs et distincts et $\beta_i = 0$ si p_i n'apparaît pas dans la décomposition de b et $\alpha_i = 0$ si p_i n'apparaît pas dans la décomposition de a.

Alors :

$$a \vee b = {p_1}^{\gamma_1}{p_2}^{\gamma_2}\ldots.{p_k}^{\gamma_k} \text{ avec } \gamma_i = sup\,(\alpha_i;\beta_i) \text{ pour tout } i \in \{1;2;\ldots;k\}$$

Soit a, b et c des entiers relatifs non nuls.

Alors :

$$\boxed{1}\; (ca) \vee (cb) = |c|\,(a \vee b)$$
$$\boxed{2}\; \begin{cases} c/a \\ c/b \end{cases} \Rightarrow \left(\frac{a}{c}\right) \vee \left(\frac{b}{c}\right) = \frac{a \vee b}{|c|}$$
$$\boxed{3}\; (a \wedge b).\,(a \vee b) = |ab|$$

Applications

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

$$\boxed{1}\; a \wedge b = 13\; et\; ab = 221$$
$$\boxed{2}\; a \wedge b = 17\; et\; ab = -578$$

Soit $(a;b;c;d) \in (\mathbb{Z}^*)^4$.

2. a- Établir les égalités suivantes : $(ab) \vee (ac) = (a \wedge c)\,((ab) \vee c)$
2. b- Montrer que si $b \wedge c = a \wedge d = 1$, alors : $(ab) \vee (cd) = (a \vee c)\,(b \vee d)$

Soit a et b deux éléments de $\mathbb{N}^*$.

3. Montrer que : $\left(\exists\,(a';b') \in \mathbb{N}^2\right)$: $\frac{1}{a} + \frac{1}{b} = \frac{a'+b'}{a \vee b}$

3-4/ Nombre de diviseurs d'un entier naturel non nul

Proposition

Soit $a = {p_1}^{\alpha_1}{p_2}^{\alpha_2}.\ldots{p_k}^{\alpha_k}$ la décomposition d'un entier naturel non nul en produit de facteurs premiers.

Le nombre de diviseurs positifs de a vaut : $(1+\alpha_1)\,(1+\alpha_2)\ldots(1+\alpha_n)$

Applications

On considère le nombre $a = p^2 q^3$ avec p et q deux nombres premiers distincts.

1. Déterminer le nombre de diviseurs de a puis donner ces diviseurs.
2. Montre que :

   (p est premier dans $\mathbb{N}$)⇔(la somme des diviseurs de p est $p+1$)

IV- Congruence module n

4-1/ Congruences module n

Définition

Soit n un entier naturel non nul.

On dit que deux entiers relatifs a et b sont congrus modulo n si n divise $b-a$, c'est-à-dire s'il existe un entier $k \in \mathbb{Z}$ tel que $b = a + kn$.

On écrit : $a \equiv b \ [n]$

Applications

1. Compléter chacune des égalités suivantes par un entier naturel convenable :

   $5 \equiv 0 \ [\_\_] \ ; \ 5 \equiv -5 \ [\_\_] \ ; \ -7 \equiv \_\_\_ \ [4] \ ; \ -1 \equiv \_\_\_ \ [3]$

2. Déterminer la valeur de vérité de chacune des propositions suivantes $(n \in \mathbb{N}^*)$:

   P : « $3 \equiv -11 \ [7]$ » ; Q : « $193 \equiv 193 \ [2018]$ » ; R : « $2n \equiv -3n \ [5]$ »

3. Déterminer les valeurs de l'entier relatif x vérifiant l'égalité suivante : $5x \equiv x \ [5]$

4-2/ Propriétés de la relation « congruence modulo »

Proposition

Soit n un entier naturel non nul.

La relation « de congruence » est une relation d'équivalence sur $\mathbb{Z}$, c'est-à-dire :

1) Elle est réflexive : $(\forall a \in \mathbb{Z})\ a \equiv a\ [n]$

2) Elle est symétrique : $\left(\forall (a;b) \in \mathbb{Z}^2\right)\ (a \equiv b\ [n] \Rightarrow b \equiv a\ [n])$

3) Elle est transitive : $\left(\forall (a;b;c) \in \mathbb{Z}^3\right)\ (a \equiv b\ [n]\ et\ b \equiv c\ [n]) \Rightarrow a \equiv c\ [n]$

Soit n un entier naturel non nul et $(a;b;c;d) \in \mathbb{Z}^4$.

Alors :

1) $a \equiv b\ [n]$ $\Leftrightarrow$(Les restes respectifs des divisions euclidiennes de a et de b par n sont égaux).

2) Si $a \equiv b\ [n]$ et $c \equiv d\ [n]$, alors : $a + c \equiv b + d\ [n]$ et $ac \equiv bd\ [n]$

3) Si $a \equiv b\ [n]$ et $k \in \mathbb{Z}$, alors : $ka \equiv kb\ [n]$

4) Si $a \equiv b\ [n]$ et $p \in \mathbb{N}$, alors : $a^p \equiv b^p\ [n]$

Applications

Soit a et b deux entiers relatifs tels que 17 est le reste de la division euclidienne de a par 19, et 15 est le reste de la division euclidienne de b par 19.

1. Déterminer le reste de la division euclidienne de chacun des nombres suivants par 19 :

$a + b\ ;\ ab\ ;\ 2a - 5b\ ;\ a^2b^3\ ;\ a^2 + b^2\ ;\ 2a + 3b$

2. Montrer que le reste de la division euclidienne du nombre $N = (2018)^{102}$ par 5 est égale à 4.
3. Déterminer que le reste de la division euclidienne du nombre 2^{2018} par 7.
4. a- Déterminer les restes de la division euclidienne par 7 des nombres suivants :

$$5\ ;\ 5^2\ ;\ 5^3\ ;\ 5^4\ ;\ 5^5\ ;\ 5^6\ ;\ 5^7$$

4. b- En déduire, selon les valeurs de l'entier naturel n, le reste de la division euclidienne de 5^n par 7.
5. Déterminer l'ensemble des entiers naturels n pour lesquels 3 divise le nombre $45671^n + 11569^n$.

V- L'ensemble $\mathbb{Z}/n\mathbb{Z}$

5-1/ Classes d'équivalence

Définition

Soit n un élément de $\mathbb{N}$*.

- L'ensemble des entiers relatifs qui ont le même reste r de la division euclidienne par n est appelé la classe d'équivalence de r, et on la note $\bar{r}$.

C'est la classe d'équivalence de r modulo n dans $\mathbb{Z}$.

- Généralisation : soit $a \in \mathbb{Z}$ et $n \in \mathbb{N}$*.

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

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

Applications

1. Déterminer la classe d'équivalence modulo 12 de chacun des nombres :

$$116 \ ; \ 1979 \ ; \ 2018$$

Proposition

Soit n un entier naturel non nul.

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

Alors :

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

2) Si $0 \leq r < n$ et $0 \leq r' < n$, alors : $\bar{r} = \overline{r'} \Leftrightarrow r = r'$ et $r \neq r' \Leftrightarrow \bar{r} \cap \overline{r'} = \emptyset$.

3) $(\forall x \in \mathbb{Z}) \ (\exists! r \in \{0; 1; ...; n-1\}) \ x = \bar{r}$ (r étant le reste de la division euclidienne de x par n)

4) $\mathbb{Z} = \bar{0} \cup \bar{1} \cup \bar{2} \cup .... \cup \overline{n-1}$

5) Par définition $\mathbb{Z}/n\mathbb{Z} = \left\{\bar{0}; \bar{1}; \bar{2}; ....; \overline{n-1}\right\}$. On a : $Card\left(\mathbb{Z}/n\mathbb{Z}\right) = n$

5-2/ Opérations dans l'ensemble $\mathbb{Z}/n\mathbb{Z}$

Définition

Soit n un entier naturel non nul.

- On définit l'addition dans $\mathbb{Z}/n\mathbb{Z}$ comme suit : Pour tous $\bar{x}$ et $\bar{y}$ de $\mathbb{Z}/n\mathbb{Z}$:
$\bar{x} + \bar{y} = \overline{x+y}$

- On définit la multiplication dans $\mathbb{Z}/n\mathbb{Z}$ comme suit : Pour tous $\bar{x}$ et $\bar{y}$ de $\mathbb{Z}/n\mathbb{Z}$:
$\bar{x} \times \bar{y} = \overline{x \times y}$

Applications

1. Montrer que pour tout $n \in \mathbb{N}^*$:

$$\boxed{1} \ (n+1)^{2018} - 1 \equiv 0 \ [n]$$
$$\boxed{2} \ 4^{2n+2} \equiv 1 \ [15]$$

2. Résoudre dans $\mathbb{Z}/6\mathbb{Z}$ les équations :

$\boxed{1} \ \bar{4}x = \bar{2}$ $\boxed{2} \ \bar{3}x^2 + x + \bar{1} = \bar{0}$	$\boxed{3} \ \left(\bar{4}x - \bar{1}\right)\left(\bar{2}x + \bar{3}\right) = \bar{0}$ $\boxed{4} \ x^3 = x$