Fomesoutra.com
ça soutra!

COURS D'ARITHMÉTIQUE : 1SM-SIBM

PR. ABDELLAH AIT-CHEIKH

www.facebook.com/mathsly123

+212 600 69 49 61

Plan du cours

1. Divisibilité dans $\mathbb{Z}$ et congruences
2. PGCD et PPCM
3. Nombres premiers
4. Classes d'équivalence et l'ensemble $\mathbb{Z}/n\mathbb{Z}$

Pr. Abdellah AIT-CHEIKH

Capacités attendues

- Appliquer l'algorithme d'Euclide pour la détermination du PGCD de deux nombres entiers ;
- Utiliser la congruence modulo n dans l'étude de la divisibilité et inversement.
- Reconnaitre l'ensemble $\mathbb{Z}/n\mathbb{Z}$ et les règles de calcul modulo n ;

Divisibilité dans $\mathbb{Z}$

Pr. Abdellah AIT-CHEIKH

Définition

Soit a et b deux entiers relatifs. On dit que a divise b s'il existe un entier k tel que $b = a \times k$. Lorsque a divise b, on note $a \mid b$

On dit aussi que : a est un **diviseur** de b
b est **divisible** par a
b est un **multiple** de a

Remarque

0 est un multiple de tout entier : pour tout $n \in \mathbb{Z}, 0 \times n = 0$

Propriété

Soit a et b deux entiers

1. Si $a \mid b$ et $b \neq 0$ alors $|a| \leqslant |b|$
2. Tout entier b **non nul** a un nombre fini de diviseurs.

Exercice 1

Montrer par récurrence que pour tout entier naturel non nul n, $3^{4n-1} + 3$ est divisible par 5.

Corrigé 1

Montrons par récurrence que pour tout entier naturel non nul n, $3^{4n-1}+3$ est divisible par 5 :
On pose $P(n)$: $3^{4n-1}+3$ est divisible par 5

- Pour $n=1$, on a $3^{4\times 1-1}+3=30$.
  Or 30 est divisible par 5 alors $P(1)$ est vraie.
- Pour $n\geq 1$, on suppose que $P(n)$ est vraie et on démontre que $P(n+1)$ est vraie.
  C'est-à-dire on montre que $P(n+1)$: $3^{4(n+1)-1}+3$ est divisible par 5.
  On a :

$$\begin{aligned} 3^{4(n+1)}-1+3 &= 3^{4n-1}\times 3^4+3 \\ &= (3^{4n-1}+3)\times 3^4-3\times 3^4+3 \\ &= (3^{4n-1}+3)\times 3^4-240 \end{aligned}$$

CORRIGÉ 1 (SUITE)

Or $3^{4n-1}+3$ est divisible par 5 alors il existe un entier relatif k tel que $3^{4n-1}+3=5k$.
On en déduit que :

$$\begin{aligned} 3^{4(n+1)}-1+3 &= 5k\times 3^4-240 \\ &= 5k\times 81-5\times 48 \\ &= 5(81k-48) \end{aligned}$$

Puisque $81k-48$ est un entier relatif, alors $3^{4(n+1)-1}+3$ est divisible par 5.

- D'après le principe de récurrence pour tout entier naturel non nul n, $3^{4n-1}+3$ est divisible par 5.

Propriétés

Soit a,b et c trois entiers.

1. Si $a \mid b$ et $b \mid c$ alors $a \mid c$
2. $c \mid a$ si et seulement si $c \mid -a$
   (L'ensemble des diviseurs de a est égal à l'ensemble des diviseurs de $-a$)
3. Si $c \mid a$ alors $c \mid ab$
4. Si $c \mid a$ et $c \mid b$ alors :
   - $c \mid a+b$
   - $c \mid a-b$
   - $c \mid au+bv$ avec u et v entiers
5. Soit a et b non nuls. Si $b \mid a$ et $a \mid b$ alors $a=b$ ou $a=-b$

Exercice 2

Trouver tous les entiers relatifs n tels que $n+2$ divise $2n+7$.

Corrigé 2

Soit n un entier naturel tel que $n+2$ divise $2n+7$.
Alors, comme $n+2$ divise $n+2$, $n+2$ divise aussi $(2n+7)-2(n+2)=3$ et donc $n+2 \in \{-3;-1;1;3\}$ puis $n \in \{-5;-3;-1,1\}$.
Réciproquement,

- si $n=-5$, $n+2=-3$ et $2n+7=-3$.
  Dans ce cas, $n+2$ divise $2n+7$.
- si $n=-3$, $n+2=-1$ et $2n+7=1$.
  Dans ce cas, $n+2$ divise $2n+7$.
- si $n=-1$, $n+2=1$ et $2n+7=5$.
  Dans ce cas, $n+2$ divise $2n+7$.
- si $n=1$, $n+2=3$ et $2n+7=9$.
  Dans ce cas, $n+2$ divise $2n+7$.

Les entiers relatifs n tels que $n+2$ divise $2n+7$ sont -5, -3, -1 et 1.

Théorème : Division Euclidienne

Soit a un entier et b un naturel non nul.
Il existe un unique entier q et un unique entier r tels que :

$$a = b \times q + r \text{ avec } 0 \leq r < b$$

Notation

- a est le dividende ;
- b est le diviseur ;
- q est le quotient ;
- r est le reste.

EXERCICE 3

Déterminer le quotient et le reste de la division euclidienne de a par b avec :

1. $a = 325, b = 7$
2. $a = -113, b = 7$

CORRIGÉ 3

1. On a : $325 = 7 \times 46 + 3$. D'où $q = 46, r = 3$
2. On a : $113 = 7 \times 16 + 1$ puis $-113 = -7 \times 16 - 1$
   Par suite $-113 = -7 \times 16 - 7 + 6$
   C'est-à-dire $-113 = -7 \times 17 + 6$
   D'où $q = -17, r = 6$

Congruence dans $\mathbb{Z}$

Pr. Abdellah AIT-CHEIKH

Définition

Soit a et b deux entiers et n un entier naturel non nul. On dit que a est **congru à** b **modulo** n si a et b ont le même reste dans la division euclidienne par n.
Il revient au même de dire qu'il existe un entier relatif k tel que $b = a + kn$ ou $b - a$ est un multiple de n.

Notation

a est congru à b modulo n se note au choix : $a \equiv b\,(n)$ ou $a \equiv b\,[n]$ ou $a \equiv b \bmod n$

Exemple

86 et 23 ont pour reste 2 dans la division euclidienne par 7 donc $86 \equiv 23\,(7)$

Théorème

Soit a, b, c et r entiers et n un entier naturel non nul.

1. $a \equiv b\,(n)$ si et seulement si $a - b$ est un multiple de n
2. Si $a \equiv r\,(n)$ et si $0 \leq r < n$ alors r est le reste de la division de a par n.
3. Si $a \equiv b\,(n)$ et $b \equiv c\,(n)$ alors $a \equiv c\,(n)$

Congruences et opérations

Soit a, b, c et d entiers et n un entier naturel non nul.

1. Si $a \equiv b\,(n)$ alors $ac \equiv bc\,(n)$
2. Si $a \equiv b\,(n)$ et $c \equiv d\,(n)$ alors :
   - $a + c \equiv b + d\,(n)$
   - $a - c \equiv b - d\,(n)$
   - $ac \equiv bd\,(n)$
3. Si $a \equiv b\,(n)$ alors, pour tout naturel p, on a : $a^p \equiv b^p\,(n)$

Exercice 4

Trouver le reste de la division par 13 du nombre 100^{1000}

Corrigé 4

Soit r le reste de la division par 13 du nombre 100^{1000}.
Alors $100^{1000} \equiv r[13]$.
On a $100 \equiv 9[13]$ (*) c'est-à-dire $100^2 \equiv 81[13]$.
Or $81 \equiv 3[13]$ alors $100^2 \equiv 3[13]$ (**) .
De (*) et (**) on a $100^3 \equiv 27[13]$. D'où $100^3 \equiv 1[13]$ car $27 \equiv 1[13]$.
Par suite $100^{3\times 333} \equiv 1[13]$. Soit $100^{999} \equiv 1[13]$ (***).
En utilisant (*) et (***) on obtient $100^{1000} \equiv 9[13]$.
Donc le reste de la division par 13 du nombre 100^{1000} est 9.

Résolution de congruences

Pr. Abdellah AIT-CHEIKH

On se donne n un entier naturel et a, b et x trois entiers relatifs et on veut résoudre la congruence $ax + b \equiv 0[n]$ d'inconnue x. On va apprendre à " faire passer a et b de l'autre côté" quand cela est possible. On va voir que la multiplication est beaucoup plus délicate à gérer que l'addition.

Résolution de congruences

Pr. Abdellah AIT-CHEIKH

Résolution de $x + a \equiv 0[n]$

Soient n un entier naturel et a et x deux entiers relatifs.

- Si $x + a \equiv 0[n]$, on a $x + a - a \equiv 0 - a[n]$ ou encore $x \equiv -a[n]$.
- Si $x \equiv -a[n]$, alors $x + a \equiv a - a[n]$ et donc $x + a \equiv 0[n]$.

En résumé, $x + a \equiv 0[n] \Leftrightarrow x \equiv -a[n]$.

Résolution de congruences

Pr. Abdellah AIT-CHEIKH

Résolution de $ax \equiv b[n]$

Soient n un entier naturel et a, b et x trois entiers relatifs. Supposons il existe un entier relatif a' tel que $a \times a' \equiv 1[n]$ (on dit dans ce cas que a est inversible modulo n), alors on peut écrire :

- si $ax \equiv b[n]$, on a : $aa'x \equiv ba'[n]$ ou encore $1 \times x \equiv ba'[n]$ ou enfin $x \equiv ba'[n]$
- si $x \equiv ba'[n]$, alors $ax \equiv baa'[n]$ ou encore $ax \equiv b \times 1[n]$ et donc $ax \equiv b[n]$.

En résumé, s'il existe un entier relatif a tel que $a \times a' \equiv 1[n]$, alors $ax \equiv b[n] \Leftrightarrow x \equiv ba'[n]$.

Exercice 5

Résoudre dans $\mathbb{Z}$ la congruence $2x + 5 \equiv 0[7]$.

CORRIGÉ 5

Soit x un entier relatif.
On a : $2x + 5 \equiv 0[7] \Leftrightarrow 2x \equiv -5[7]$.
On note alors que $2 \times 4 = 8 = 1 + 7$
Donc $2 \times 4 \equiv 1[7]$.
Par suite $2x + 5 \equiv 0[7] \Leftrightarrow 2x \equiv -5[7] \Leftrightarrow x \equiv -20[7]$.
Comme $-20 \equiv 1[7]$ car $-20 - 1 = -21 = (-3) \times 7$
Enfin, $2x + 5 \equiv 0[7] \Leftrightarrow x \equiv 1[7]$.
D'où les entiers relatifs x tels que $2x + 5 \equiv 0[7]$ sont les entiers relatifs de la forme $1 + 7k$ où k est un entier relatif.

EXERCICE 6

Montrer que la congruence $2x \equiv 1[6]$ n'a pas de solution dans $\mathbb{Z}$.

CORRIGÉ 6

Supposons qu'il existe un entier relatif x tel que $2x \equiv 1[6]$. Alors, il existe un entier relatif k tel que $2x = 1 + 6k = 1 + 2 \times (3k)$.
Le membre de gauche de cette égalité est un entier pair et le membre de droite est un entier impair. Ceci est impossible et donc la congruence $2x \equiv 1[6]$ n'a pas de solution dans $\mathbb{Z}$.

PGCD et PPCM

Pr. Abdellah AIT-CHEIKH

Définition

- L'ensemble des diviseurs communs à a et b admet un plus grand élément noté $\text{pgcd}(a;b)$ ou $a \wedge b$
- L'ensemble des multiples communs à a et b admet un plus petit élément noté $\text{ppcm}(a;b)$ ou $a \vee b$
- On désigne par $n\mathbb{Z}$ l'ensemble des multiples de n dans $\mathbb{Z}$

Propriétés du PGCD

Soit a, b et r entiers non nuls.

1. $\mathrm{pgcd}(a;b) \geq 1$
2. $\mathrm{pgcd}(a;b) = \mathrm{pgcd}(b;a)$
3. $\mathrm{pgcd}(a;a) = |a|$
4. $\mathrm{pgcd}(a;b) = \mathrm{pgcd}(-a;b) = \mathrm{pgcd}(a;-b)$
5. Si $b \mid a$, $\mathrm{pgcd}(a;b) = |b|$
6. Si $a = bq + r$ alors, $\mathrm{pgcd}(a;b) = \mathrm{pgcd}(b;r)$

Principe de l'algorithme d'Euclide pour calculer le pgcd

Soit a et b deux entiers naturels non nuls tels que b ne divise pas a. Alors $\text{pgcd}(a;b)$ est le **dernier reste non nul** de la suite des divisions de l'algorithme d'Euclide.
Si $r_1, r_2, ..., r_n$ est la suite de restes non nuls et si on note r_n le dernier reste non nul dans cet algorithme, on a :
$\text{pgcd}(a;b) = \text{pgcd}(b;r_1) = ... = \text{pgcd}(r_{n-1};r_n) = r_n$

Exercice 7

Calculer $\operatorname{pgcd}(8820;3150)$

CORRIGÉ 7

L'algorithme d'Euclide appliqué à 8820 et 3150 s'écrit :

$$\begin{aligned} 8820 &= 2 \times 3150 + 2520 \\ 3150 &= 1 \times 2520 + 630 \\ 2520 &= 4 \times 630 + 0 \end{aligned}$$

Le dernier reste non nul est 630, donc

$\operatorname{pgcd}(8820;3150) = 630$

Propriétés

Soit a et b deux entiers non nuls et $d = pgcd(a;b)$

1. L'ensemble des diviseurs communs à a et b est l'ensemble des diviseurs de d
2. Il existe des entiers u et v tels que : $d = au + bv$
3. Pour $k \in \mathbb{N}^*, pgcd(ka;kb) = k \times pgcd(a;b)$

EXERCICE 8

1. Déterminer le PGCD de 12642 et 2382.
2. En déduire les diviseurs communs à 12642 et 2382 qui sont des entiers naturels.

Corrigé 8

1. Déterminons le PGCD de 12642 et 2382.
   L'algorithme d'Euclide appliqué à 12642 et 2382 s'écrit :
   $$\begin{aligned} 12642 &= 5 \times 2382 + 732 \\ 2382 &= 3 \times 732 + 186 \\ 732 &= 3 \times 186 + 174 \\ 186 &= 1 \times 174 + 12 \\ 174 &= 14 \times 12 + 6 \\ 12 &= 2 \times 6 + 0 \end{aligned}$$
   Le dernier reste non nul est 6 et donc $\mathrm{PGCD}(12642; 2382) = 6$.

2. Les diviseurs communs à 12642 et 2382 sont les diviseurs de leur PGCD à savoir 6.
   Les diviseurs communs à 12642 et 2382 qui sont des entiers naturels sont 1, 2, 3 et 6.

Nombres premiers

Pr. Abdellah
AIT-CHEIKH

Définition

Un entier naturel est dit **premier** s'il admet exactement deux diviseurs positifs (1 et lui-même)

Remarque

1 n'est pas premier.

Théorème

Tout $n \in \mathbb{N}$ avec $n \geq 2$ admet au moins un diviseur premier.
Si n n'est pas premier et $n \geq 2$ alors il admet un diviseur premier compris entre 2 et $\sqrt{n}$

Remarque

On utilise ce théorème de la manière suivante :
Si un naturel $n \geq 2$ n'admet pas de diviseur premier compris entre 2 et $\sqrt{n}$ alors n est premier.

EXERCICE 9

Démontrer que 331 est un nombre premier.

CORRIGÉ 9

On a : $\sqrt{331} = 18,....$ Les nombres premiers inférieurs ou égaux à $\sqrt{331}$ sont 2, 3, 5, 7, 11, 13 et 17.

- $\dfrac{331}{2} = 165,5$
- $\dfrac{331}{3} = 110,3..$
- $\dfrac{331}{5} = 66,2$
- $\dfrac{331}{7} = 47,2..$
- $\dfrac{331}{11} = 30,09..$
- $\dfrac{331}{13} = 25,4..$
- $\dfrac{331}{17} = 19,47..$

Finalement, 331 n'est divisible par aucun nombre premier inférieur ou égal à sa racine et donc 331 est un nombre premier.

Théorème

Il existe une infinité de nombres premiers.

Théorème

Tout entier naturel strictement supérieur à 1 admet une décomposition, unique à l'ordre des facteurs près, en produit de nombres premiers.

Exemple

$72 = 2^3 \times 3^2$

Propriété

Si $\begin{cases} a = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_n^{\alpha_n} \\ b = p_1^{\beta_1} p_2^{\beta_2} \dots p_n^{\beta_n} \end{cases}$ alors $\begin{cases} \text{PGCD}(a,b) = p_1^{m_1} p_2^{m_2} \dots p_n^{m_n} \\ \text{PPCM}(a,b) = p_1^{M_1} p_2^{M_2} \dots p_n^{M_n} \end{cases}$ où $m_i = \min(\alpha_i, \beta_i)$ et $M_i = \max(\alpha_i, \beta_i)$

EXERCICE 10

Soient $a = 4116$ et $b = 6300$.
Déterminer $a \vee b$ et $a \wedge b$.

CORRIGÉ 10

On a : $a = 4116 = 2^2 \times 3 \times 7^3 = 2^2 \times 3 \times 5^0 \times 7^3$ et $b = 6300 = 2^2 \times 3^2 \times 5^2 \times 7$.

Alors, $a \wedge b = 2^2 \times 3 \times 5^0 \times 7 = 84$ et $a \vee b = 2^2 \times 3^2 \times 5^2 \times 7^3 = 308700$.

Classes d'équivalence et l'ensemble $\mathbb{Z}/n\mathbb{Z}$

Définition

Soit $n \in \mathbb{N}$.
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 modulo n, on la note $\bar{r}$.
Et on a : $\bar{r} = \{x \in \mathbb{Z} \ / \ x \equiv r[n]\} = \{r + kn \ / \ k \in \mathbb{Z}\}$

Exemples

- $\bar{0} = \{kn \ / \ k \in \mathbb{Z}\}$, pour $n = 2$ on a $\bar{0} = \{2k \ / \ k \in \mathbb{Z}\}$ donc $\bar{0}$ est l'ensemble des nombres pairs.
- $\bar{1} = \{kn + 1 \ / \ k \in \mathbb{Z}\}$, pour $n = 2$ on a $\bar{1} = \{2k + 1 \ / \ k \in \mathbb{Z}\}$ donc $\bar{1}$ est l'ensemble des nombres impairs.

On remarque que pour $n = 2$ on a : $\mathbb{Z} = \bar{0} \cup \bar{1}$

Propriété

- $(\forall a \in \mathbb{Z}) \quad \overline{a} = \{x \in \mathbb{Z} / \quad x \equiv a[n]\}$
- $x \in \overline{a} \Leftrightarrow x \equiv a[n]$
- $x \in \overline{a} \Leftrightarrow n$ divise $x - a$
- $\mathbb{Z} = \overline{0} \cup \overline{1} \cup \overline{2} \cup \cdots \cup \overline{(n-1)}$
- $\mathbb{Z}/n\mathbb{Z} = \{\overline{0}, \overline{1}, \overline{2}, \cdots, \overline{(n-1)}\}$
- Soient x et y deux éléments de $\{0;1;2;\cdots;(n-1)\}$. On a :
  - $\overline{x} = \overline{y} \quad \Leftrightarrow \quad x = y$
  - $\overline{x} \cap \overline{y} = \emptyset \quad \Leftrightarrow \quad x \neq y$
  - $\overline{x} + \overline{y} = \overline{x+y}$
  - $\overline{x} \times \overline{y} = \overline{x \times y}$

EXERCICE 11

Déterminer la classe d'équivalence modulo 12 de chacun des nombres : 116 et 2019

Corrigé 11

- On a $\overline{116} = \{116 + kn \ / \ k \in \mathbb{Z}\}$.
  Alors pour $n = 12$, on a $\overline{116} = \{116 + 12k \ / \ k \in \mathbb{Z}\}$
  $\overline{116} = \{8 + 12k \ / \ k \in \mathbb{Z}\} = \overline{8}$.
- On a $\overline{2019} = \{2019 + kn \ / \ k \in \mathbb{Z}\}$.
  Alors pour $n = 12$, on a $\overline{2019} = \{2019 + 12k \ / \ k \in \mathbb{Z}\}$
  $\overline{2019} = \{3 + 12k \ / \ k \in \mathbb{Z}\} = \overline{3}$

Exercices à faire

Exercice 12

1. Écrire l'ensemble des entiers relatifs diviseurs de 6.
2. Déterminer les entiers relatifs n tels que $n-4$ divise 6.
3. Déterminer les entiers relatifs n tels que $n-4$ divise $n+2$.
4. Déterminer les entiers relatifs n tels que $n+1$ divise $3n-4$.
5. Quel est le nombre de diviseurs de 2880 ?
6. Trouvez le PGCD des nombres 1640 et 492 en utilisant la décomposition en facteurs premiers, puis en utilisant l'algorithme d'Euclide.

Exercices à faire

Exercice 13

1. a est un entier naturel. Montrez que $a^5 - a$ est divisible par 10.
2. Montrer que les nombres entiers $A_n = 3^{2n} - 1$, sont divisibles par 8.
3. Soit l'entier $a_n = 4^n - 1\,; n \in \mathbb{N}$
    1. Montrer par récurrence que pour tout entier naturel n, on a : a_n est divisible par 3.
    2. En déduire que $4^{n+1} - 4$ est divisible par 3.
    3. Déterminer alors le reste de la division euclidienne par 3 du nombre 2^{102}.

Exercices à faire

Pr. Abdellah AIT-CHEIKH

Exercice 14

1. Effectuer la division euclidienne de -283 par 19
2.
   1. Traduire en terme de congruence la division euclidienne de 11 par 7.
   2. Prouver que, pour tout entier naturel n, le nombre $2^{3n+1} + 3^{6n} + 11^{3n+1}$ est divisible par 7.
3. On considère le nombre A défini pour tout entier naturel n par $A = 9^{n+1} + 2^{6n+1}$.
   Démontrer que A est divisible par 11 pour tout n de $\mathbb{N}$:
   1. en utilisant les congruences
   2. en raisonnant par récurrence.
4. Déterminer le reste de la division euclidienne de $(1429^{2009} + 2008^{1430})$ par 9