Table des matières

Chapitre 1

ARITHMÉTIQUE

1.1 Divisibilité dans $\mathbb{Z}$

1.1.1 Diviseurs et Multiples d'un entier relatif

a) Définition

Soit a et b deux entiers relatifs tels que b soit non nul.

On dit que b est un diviseur de a si et seulement si il existe un entier k tel que $a = bk$.

On dit aussi que a est un multiple de b ou encore b divise a que l'on note b/a.

▷ L'ensemble des diviseurs de a se note $D(a)$.

▷ L'ensemble des multiples de b se note $b\mathbb{Z}$.

Exemple

$D(12) = \{-12; -6; -4; -3; -2; -1; 1; 2; 3; 4; 6; 12\}$

$3\mathbb{Z} = \{...; -9; -6; -3; 0; 3; 6; 9; ...\}$.

b) Propriétés

p_1) a/a ; $1/a$ et $a/0$.

p_2) Tout entier relatif a possède un nombre fini de diviseurs et une infinité de multiples.

p_3) Tout entier relatif non nul b a pour diviseurs au moins -1 ; 1 ; $-b$ et b.

p_4) Si b/a, alors $1 \leq |b| \leq |a|$.

p_5) Si b/a et a/b, alors $|a| = |b|$.

p_6) Si a/b et b/c, alors a/c.

p_7) Si ac/ab et $a \neq 0$ alors c/b.

p_8) Si a/b alors pour tout entier k ; a/bk.

p_9) Si a/b et a/c alors il existe deux entiers p et q tels que $a/(pb+cq)$

p_{10}) L'opposé d'un multiple de a est un multiple de a.

p_{11}) Le produit d'un multiple de a par un entier relatif est un multiple de a.

1.1.2 Division euclidienne dans $\mathbb{Z}$

Définition

Soit a et b deux entiers relatifs tels que b soit non nul.
Il existe un couple unique $(q;r)$ de $\mathbb{Z}\times\mathbb{N}$ tels que $a=bq+r$ où $0\leq r<|b|$.
Les nombres q et r s'appellent respectivement quotient et reste de la division euclidienne de a par b.

Remarque

Si $r=0$; on a : $a=bq$, on dit que a est divisible par b.

Exemple

$47=8\times5+7$; on a : $q=5$ et $r=7$.

1.1.3 Plus grand commun diviseur

a) Définition

Soit a et b deux entiers relatifs non nuls.
On appelle plus grand commun diviseur de a et b note $PGCD(a,b)$ où $a\wedge b$, le plus grand entier naturel de $D(a;b)$.

Exemple

$PGCD(24,30)=6$

b) Propriétés

p_1) $PGCD(a,b)=PGCD(b,a)=PGCD\left(|a|,|b|\right)$.

p_2) Si $PGCD(a,b)=d\Longrightarrow PGCD\left(\dfrac{a}{d},\dfrac{b}{d}\right)=1$.

p_3) $PGCD(ka, kb) = kPGCD(a, b)$ où $k \in \mathbb{Z}^*$.

p_4) Si b/a, $D(a, b) = D(b)$ où $D(a, b)$ est l'ensemble de diviseurs communs à a et b.

p_5) Si $a = bq + r$ avec $a > b > 0$

- $r \neq 0$, $D(a, b) = D(b, r)$ et $PGCD(a, b) = PCGD(b, r)$?
- $r = 0$, $D(a, b) = D(b)$ et $PGCD(a, b) = b$.

p_6) Si $PGCD(a, b) = d$, un entier m est multiple de d s'il existe deux entiers relatifs u et v tels que : $au + bv = m$

p_7) Si $PGCD(a, b) = d$, on a : $D(a, b) = D(d)$.

p_8) $PGCD(a; (b, c)) = PGCD((a, b); c)$.

p_9) $PGCD(a; 1) = 1$.

p_{10}) Si $a' = a/PGCD(a; b)$ et si $b' = b/PGCD(a; b)$, alors $PGCD(a'; b') = 1$.

c) Recherche du PGCD : Algorithme d'Euclide

Soit a et b deux entiers.

$a = bq_0 + r_0$

$b = r_0q_1 + r_1$

$r_0 = r_1q_2 + r_2$

$r_1 = r_2q_3 + r_3$

$\vdots$

$r_{n-2} = r_{n+1}q_n + r_n$

$r_{n-1} = r_nq_{n+1}$

On a : $PGCD(a, b) = r_n$. (le $PGCD$ de a et b est le dernier reste non nul).

Exemple

Déterminer le $PGCD(304939, 151097)$.

Solution

Déterminons le $PGCD(304939, 151097)$.

Dividende	304939	151097	2745	122
Diviseur	151097	2745	122	61
Reste	2745	122	61	0

D'où $PGCD(304939, 151097) = 61$

1.1.4 Nombres premiers entre eux

a) Définition

Soit a et b deux entiers relatifs non nuls.

On dit que a et b sont premiers entre eux si leur plus grand commun diviseur est égal à 1, c'est-à-dire $PGCD(a, b) = 1$.

Exemple

756 et 221 sont premiers entre eux.

b) Propriétés

p_1) $PGCD(a, b) = d \Longrightarrow \dfrac{a}{d}$ et $\dfrac{b}{d}$ sont premiers entre eux.

p_2) Si $PGCD(a, b) = d$, alors il existe deux entiers a' et b' premiers entre eux tels que : $a = da'$ et $b = db'$.

1.1.5 Théorèmes

a) Identité de Bézout

Soit a et b deux entiers relatifs non nuls et $PGCD(a, b) = d$. Il existe deux entiers relatifs u et v tels que $au + bv = d$.

b) Théorème de Bézout

Soit a et b deux entiers relatifs non nuls. a et b sont premiers entre eux si et seulement si il existe deux entiers relatifs u et v tels que $au + bv = 1$.

c) Théorème de Gauss

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

Si a divise bc et si a et b sont premiers entre eux, alors a divise c.

1.1.6 Application : Équation Diophantienne

a) Définition

Une équation diophantienne est une équation de la forme $ax + by = c$ avec a, b et c des entiers relatifs où a et b sont non nuls.

b) Résolution

Pour résoudre dans $\mathbb{Z}^2$ l'équation $ax + by = c$, on calculer le $PGCD(a, b)$.

Posons que $PGCD(a, b) = d$, on distingue deux cas :

▷ Premier cas :

Si d ne divise pas c, alors l'équation n'admet pas de solution.

▷ Deuxième cas :

Si d divise c, alors l'équation admet des solutions.

Exemple

Résoudre dans $\mathbb{Z}^2$ les équations suivantes : $(E) : 12x + 21y = 2$ et $(E') : 45x - 28y = 1$

Solution

Résolvons dans $\mathbb{Z}^2$ les équations suivantes : (E) et (E').

▷ Pour $(E) : 12x + 21y = 2$

Calculons le $PGCD(12, 21)$.

On a : $PGCD(12, 21) = 3$

Comme 3 ne divise pas 2, alors cette équation n'admet pas de solution.

D'où $S = \{\}$

▷ Pour $(E') : 45x - 28y = 1$

Calculons le $PGCD(45, 28)$.

On a : $PGCD(45, 28) = 1$

Comme $PGCD(45, 21)$ divise 1, l'équation admet des solutions

▷ Résolution de l'équation $(E'_0) : 45x - 28y = 0$

$45x - 28y = 0 \Longrightarrow 45x = 28y$

$45/28y$, comme $PGCD(45, 28) = 1$, donc d'après le théorème de Gauss $45/y$ donc il existe un entier relatif k tel que $y = 45k$.

$45x = 28y \Longrightarrow 45x = 28 \times 45k \Longrightarrow x = 28k$.

La solution de l'équation (E'_0) est $(28k, 45k)\,;\, k \in \mathbb{Z}$.

▷ Solution particulière de l'équation (E')

$45 = 28 \times 1 + 17$

$28 = 17 \times 1 + 11$

$11 = 6 \times 1 + 5$ $6 = 5 \times 1 + 1$

On a : $45(5) - 28(8) = 1$

La solution particulière de (E') est $(x_0; y_0) = (5, 8)$.

▷ Solution générale

$45x - 28y = 1$ et $45(5) - 28(8) = 1 \Longrightarrow 28k = x - 5$ et $45k = y - 8$

D'où $S = \{(5 + 28k; 8 + 45k)\,;\, k \in \mathbb{Z}\}$

1.1.7 Plus petit commun multiple

a) Définition

Soit a et b deux entiers non nuls.

On appelle plus petit commun multiple de a et b noté $PPCM(a, b)$ ou $a \vee b$ le plus petit élément strictement positif de $a\mathbb{Z} \cap b\mathbb{Z}$.

Exemple

$PPCM(7, 8) = 56$

b) Propriétés

Soit a, b et k trois entiers relatifs non nuls.

$p_1)$ $PPCM(a, b) = PPCM(b, a)$.

$p_2)$ $PPCM(ka, kb) = kPPCM(a, b)$.

$p_3)$ $PPCM(a, b) \times PGCD(a, b) = |a \times b|$.

1.1.8 Nombres premiers

a) Définition

Un nombre premier est un entier naturel qui admet deux diviseurs : 1 et lui-même.

Exemple

2 ; 3 ; 5 ; 7 ; 11 ; 13 ; 19 ; 23 ; 31 ; 37 sont des nombres premiers.

b) Théorèmes

T_1) Il existe une infinité de nombres premiers.

T_2) Tout entier naturel a supérieur ou égal à 2, admet au moins un diviseur premier.

T_3) Tout entier naturel a supérieur ou égal à 2 et non premier, admet au moins un diviseur premier p tel que : $2 \leq p \leq \sqrt{a}$.

T_4) Soit a un entier naturel supérieur ou égal à 2, alors il existe une famille de nombres premiers p_1, p_2, p_3,..., p_n et une famille d'entiers naturels α_1, α_2, α_3,..., α_n tels que : $a = p_1^{\alpha_1} \times p_2^{\alpha_2} \times ... \times p_n^{\alpha_n}$ avec $p_1 < p_2 < ... < p_n$.
On dit que a est décomposé en produit de facteurs premiers.
Cette décomposition est unique.

Exemple

$720 = 2^4 \times 3^2 \times 5$.

c) Nombre de diviseurs

Soit a un entier naturel supérieur ou égal à 2 admettant pour décomposition en facteurs premiers ; on désigne par N le nombre de diviseurs positifs de a.
$N = (\alpha_1 + 1) \times (\alpha_2 + 1) \times (\alpha_3 + 1) \times ... \times (\alpha_n + 1)$.

Exemple

$720 = 2^4 \times 3^2 \times 5$.
Déterminons le nombre de diviseurs positifs de 720
On a : $N = (4 + 1)(2 + 1)(1 + 1) = 30$

d) Diviseurs positifs d'un entier relatif

Les diviseurs positifs d'un entiers relatif a sont les termes de la somme, du développement du produit :
$S = (p_1^0 + p_1^1 + ... + p_1^{\alpha_1}) \times (p_2^0 + p_2^1 + ... + p_2^{\alpha_2}) \times ... \times (p_k^0 + p_k^1 + ... + p_k^{\alpha_k})$.

Exercice

On donne $A = 72$

1. Décomposer A en produit de facteurs premiers.
2. Quel est le nombre de diviseurs positifs de A ?
3. Déterminer l'ensemble de diviseurs positifs de A.

Corrigé

1. Décomposition de A
   $A = 2^3 \times 3^2$
2. Nombre de diviseur de A
   Soit N ce nombre.
   On a : $N = (3+1)(2+1) = 12$
3. Ensemble de diviseurs positifs de A
   $D(A) = \{1, 2, 3, 4, 6, 8, 9, 12, 18, 24, 36, 72\}$

Remarque

On dit que deux nombres sont amis si la somme des diviseurs positifs autres que lui-même de chacun de ces deux nombres est égale à l'autre nombre.

Exercice

Soit deux entiers relatifs α et β définis par : $\alpha = 220$ et $\beta = 284$.

1. Déterminer l'ensemble des diviseurs positifs de α et β.
2. Montrer que α et β sont amis.

Corrigé

1. Ensemble des diviseurs positifs de α et β.
   $D(\alpha) = \{1, 2, 4, 5, 10, 11, 20, 22, 44, 55, 110, 220\}$
   $D(\beta) = \{1, 2, 4, 71, 142, 284\}$
2. Preuve que α et β sont amis.
   Pour $\alpha = 220$;
   $N = 1 + 2 + 4 + 5 + 10 + 11 + 20 + 22 + 44 + 55 + 110 = 284$

Et pour $\beta = 284$;

$N = 1 + 2 + 4 + 71 + 142 = 220$

Donc α et β sont amis.

e) PGCD et PPCM Connaissant la décomposition

Soit a et b deux entiers supérieurs ou égal à 2 tels que :

$a = p_1^{\alpha_1} \times p_2^{\alpha_2} \times ... \times p_n^{\alpha_n}$ et $b = p_1^{\beta_1} \times p_2^{\beta_2} \times ... \times p_n^{\beta_n}$ avec $p_1 < p_2 < ... < p_n$.

▷ $PGCD(a, b) = p_1^{\gamma_1} \times p_2^{\gamma_2} \times ... \times p_n^{\gamma_n}$ où $\gamma_i = min(\alpha_i, \beta_i)$.

▷ $PPCM(a, b) = p_1^{\delta_1} \times p_2^{\delta_2} \times ... \times p_n^{\delta_n}$ où $\delta_i = max(\alpha_i, \beta_i)$.

Exercice

On donne les nombres suivants : $\alpha = 220$ et $\beta = 568$

1. Décomposer ces nombres en produit de facteur premiers.
2. Déterminer le $PGCD$ et $PPCM$ de α et β.

Corrigé

1. Décomposition en éléments simples.
   $\alpha = 2^2 \times 5 \times 11$ et $\beta = 2^3 \times 71$
2. Le PGCD(220, 568)=$2^2 \times 1$ et PPCM(220, 568)=$2^3 \times 5 \times 11 \times 71$

1.2 Congruence modulo n avec $n \in \mathbb{N}$

1.2.1 Définition

Soit n un entier naturel non nul, a et b deux entiers relatifs.

On dit que a est congru à b modulo n si et seulement si a et b ont le même reste dans leurs divisions euclidienne par n ou si $a - b$ est un multiple de n.

On écrit $a \equiv b[n]$.

1.2.2 Propriétés

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

P_1) $a \equiv a[n]$.

P_2) Si $a \equiv b[n]$, alors $b \equiv a[n]$.

P_3) Si $a \equiv b[n]$ et $b \equiv c[n]$, alors $a \equiv c[n]$.

P_4) Soit a' un entier relatif, r et r' les restes respectifs de la division euclidienne de a et a' par n.
On a : $a \equiv a'[n] \Leftrightarrow r = r'$.

$P_{(5)}$) Si $a \equiv a'[n]$ et $b \equiv b'[n]$, alors
▷ $ab \equiv a'b'[n]$;
▷ $a + b \equiv a' + b'[n]$;
▷ $a^k \equiv a'^k[n]$ où $b' \in \mathbb{Z}$ et $k \in \mathbb{N}$.

Exercice

1. Écrire le nombre 200 en modulo 3
2. Calculer le nombre a tel que $203 = a[4]$

Corrigé

1. Preuve que $27 = 1[2]$
   On a : $200 = 3(66) + 2 \Longrightarrow$ r=2 donc $200 \equiv 2[3]$
2. Calcul de a
   On a : $203 = 4 \times 50 + 3 \Longrightarrow r = 3$

1.2.3 Ordre modulo n

Définition

Soit n et a deux entiers naturels non nuls tel que a non divisible par n.
On appelle ordre de a modulo n, le plus petit entier naturel non nul k tel que $a^k \equiv 1[n]$.

Exemple

2 est l'ordre modulo 5 de 2004, car $2004^2 \equiv 1[5]$.

1.2.4 Petit théorème de Fermat

Si a est un entier naturel et p un nombre premier, alors $a^p \equiv a[p]$.
Si de plus a et p sont premiers entre eux, c'est-à-dire $PGCD(a, p) = 1$, alors $a^{p-1} \equiv 1[p]$

Exercice

Montrer d'après le petit théorème de Fermat que $3^4 \equiv 1[5]$

Corrigé

Il s'agit de chercher la période de k tel que $3^{k-1} \equiv 1[k]$. Comme 5 est un nombre premier et que $PGCD(3,5) = 1$ alors d'après le petit théorème de de Fermat on a : $3^4 \equiv 1[5]$

1.3 Ensemble quotient $\mathbb{Z}/n\mathbb{Z}$

1.3.1 Classe de congruence modulo

Définition

Soit n un entier naturel non nul et x un entier relatif strictement inférieur à n.
La classe de congruence de x modulo n est l'ensemble des entiers relatifs a tels que : $a \equiv x[n]$.
On le note $\dot{x} = \{a \in \mathbb{Z}/a \equiv x[n]\}$.
$\dot{x} = \{a \in \mathbb{Z}/a = nk + x; k \in \mathbb{Z}\}$.

Exemple

1. La classe de congruence de 2 modulo 5 est :
   $\dot{2} = \{a \in \mathbb{Z}/a \equiv 2[5]\}$.
   $\dot{2} = \{...., -13, -8, -3, 2, 7, 12, 17, ...\}$.
2. La classe de congruence de 3 modulo 4 est :
   $\dot{3} = \{a \in \mathbb{Z}/a \equiv 3[4]\}$.
   $\dot{3} = \{...., -9, -5, -1, 3, 7, 11, 15, ...\}$.

1.3.2 Définition de l'ensemble quotient

L'ensemble quotient $\mathbb{Z}/n\mathbb{Z}$ est l'ensemble des classes de congruences modulo n.
On a : $\mathbb{Z}/n\mathbb{Z} = \left\{\dot{0}; \dot{1}; \dot{2}; ...; \widehat{\dot{n-1}}\right\}$.

1.3.3 Opérations dans $\mathbb{Z}/n\mathbb{Z}$

a) Addition

Soit $\dot{a} \in \mathbb{Z}/n\mathbb{Z}$ et $\dot{b} \in \mathbb{Z}/n\mathbb{Z}$.
On a : $\dot{a} + \dot{b} = \widehat{\dot{a+b}}$.

b) Multiplication

Soit $\dot{a} \in \mathbb{Z}/n\mathbb{Z}$ et $\dot{b} \in \mathbb{Z}/n\mathbb{Z}$.
On a : $\dot{a} \times \dot{b} = \widehat{\dot{a \times b}}$.

Application

Exercice

1. Définir l'ensemble $\mathbb{Z}/4\mathbb{Z}$.
2. Donner la table d'addition et de la multiplication dans $\mathbb{Z}/4\mathbb{Z}$.
3. Résoudre dans $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$ et dans $\mathbb{Z}/4\mathbb{Z}$
   (a) le système suivant : $\begin{cases} \dot{2}x + y = \dot{1} \\ x + \dot{2}y = \dot{2} \end{cases}$
   (b) L'équation suivante : $\dot{3}x + \dot{2} = \dot{3}$.

Corrigé

1. Ensemble $\mathbb{Z}/4\mathbb{Z}$
   $\mathbb{Z}/4\mathbb{Z} = \{\dot{0}, \dot{1}, \dot{2}, \dot{3}\}$
2. Table d'addition et de multiplication.

Addition

$+$	$\dot{0}$	$\dot{1}$	$\dot{2}$	$\dot{3}$
$\dot{0}$	0	1	2	3
$\dot{1}$	1	2	3	0
$\dot{2}$	2	3	0	1
$\dot{3}$	3	0	1	2

Multiplication

$\times$	$\dot{0}$	$\dot{1}$	$\dot{2}$	$\dot{3}$
$\dot{0}$	0	0	0	0
$\dot{1}$	0	1	2	3
$\dot{2}$	0	2	0	2
$\dot{3}$	0	3	2	1

3. Résolution dans $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$ et dans $\mathbb{Z}/4\mathbb{Z}$

   a. $\begin{cases} \dot{2}x + y = \dot{1} \ (1) \\ x + \dot{2}y = \dot{2} \ (2) \end{cases}$

   En faisant (1)+(2), on trouve : $\dot{3}x + \dot{3}y = \dot{3}$ (3)

   Ensuite, en faisant (1)+(3), on obtient : $\dot{5}x + \dot{4}y = \dot{4}$, or $\dot{4} = \dot{0}$ et $\dot{5} = \dot{1}$, alors $x = \dot{0}$ (4)

   En remplaçant (4) dans (2), on trouve : $\dot{2}y = \dot{2}$

   Soit $y = \dot{1}$ ou $y = \dot{3}$

   D'où $S = \{(\dot{0}, \dot{1}); (\dot{0}, \dot{3})\}$

   b. Résolution de $\dot{3}x + \dot{2} = \dot{3}$

   $\dot{3}x + \dot{2} = \dot{3} \Longrightarrow \dot{3}x = \dot{1}$

x	0	1	2	3
$3x$	0	3	2	1

   $3x = 1 \Longleftrightarrow x = 3 \Longleftrightarrow S = \{3\}$

1.4 Équations modulaires

1.4.1 Inverse modulo n

Définition

Soit a un entier relatif non nul et n un entier naturel.

On appelle inverse modulo n de a l'entier relatif a' tel que $a \times a' \equiv 1[n]$.

On le note $a' \equiv a^{-1}[n]$.

Exemple

$2 \times 3 \equiv 1[5]$

Donc l'inverse de 2 modulo 5 est 3

$3 \equiv 2^{-1}[5]$.

1.4.2 Recherche de l'inverse

Théorème

Un entier a est inversible modulo n, si et seulement si a et n sont premiers entre eux.

1.4.3 Application

$aa' \equiv 1[n] \Leftrightarrow aa' = 1 + kn \Leftrightarrow aa' - kn = 1\,;\, k \in \mathbb{Z}$

On se sert de l'algorithme d'Euclide.

Exemple

Trouver l'inverse module 55 de 24.

Solution

Trouvons l'inverse module 55 de 24.

Soit a' l'inverse l'inverse module 55 de 24, c'est-à-dire $24a' \equiv 1[55]$ ou $a' \equiv 24^{-1}[55]$.

Comme 55 et 24 sont premiers entre eux, d'après le théorème de Bezout, il existe deux entiers relatifs u et v tels que : $55u + 24v = 1$

D'après l'algorithme d'Euclide, on a :

$55 = 24 \times 2 + 7 \Longrightarrow 7 = 55 - 24 \times 2$ (1)

$24 = 7 \times 3 + 3 \Longrightarrow 3 = 24 - 7 \times 3$ (2)

$7 = 3 \times 2 + 1 \Longrightarrow 7 - 3 \times 2 = 1$ (3)

(1) et (2) dans (3) ; $55 - 24 \times 2 - 2 \times (24 - 7 \times 3) = 1$

$55 - 24 \times 4 + 7 \times 6) = 1 \Longrightarrow 55 - 24(4) + 55(6) - 24(12) = 1$

$24(-16) = 1 - 55(7) \Longrightarrow 24(-16) \equiv 1[55] \Longrightarrow 24^{-1}[55] = -16$

Ou

$-16 \equiv 39[55] \Longrightarrow 24^{-1}[55] = 39$

D'où $a' = 39$

1.5 Équations linéaires modulo n

1.5.1 Définition

Soit n un entier naturel non nul.

On appelle équation linéaire modulo n, toute expression de la forme $ax \equiv b[n]$ où a et b sont des entiers et x l'inconnue.

1.5.2 Résolution

Pour résoudre l'équation $ax \equiv b[n]$, on distingue deux cas :

▷ Premier cas : si a et n sont premiers entre eux

On a : $ax \equiv b[n] \Longrightarrow x = a^{-1}b[n]$

La solution de cette équation est $x = a^{-1}b + kn, k \in \mathbb{Z}$ où a^{-1} est l'inverse module n de a.

▷ Deuxième cas : si a et n ne sont pas premiers entre eux

Posons $PGCD(a, n) = d$;

• Si d divise b, il existe des entiers a', b' et n' tels que : $a = a'd$; $b = b'd$ et $n = n'd$.

L'équation devient

$a'dx \equiv b'd[dn'] \Longrightarrow a'x \equiv b'[n']$.

On se ramène au cas précèdent.

• Si d ne divise pas b, alors l'équation n'a pas des solutions.

1.5.3 Application

Exercice

Résoudre dans $\mathbb{Z}$ les équations suivantes : $(E) : 5x \equiv 3[7]$ et $(E') : 60x \equiv 36[144]$

Solution

Résolvons dans $\mathbb{Z}$ les équations suivantes : $(E) : 5x \equiv 3[7]$ et $(E') : 60x \equiv 36[144]$

▷ Pour $(E) : 5x \equiv 3[7]$

Cherchons le $PGCD(5, 7)$

On a : $PGCD(7, 5) = 1$, alors 5 et 7 sont premiers entre eux

Cherchons l'inverse modulo 7 de 5

On a :

x	0	1	2	3	4	5	6
$5x$	0	5	3	1	6	4	2

On a : $5^{-1}[7] = 3$

$x \equiv 3 \times 3[7]$

$x \equiv 9[7]$

$x \equiv 2[7]$

D'où $S = \{2 + 7k; k \in \mathbb{Z}\}$

▷ Pour $(E') : 60x \equiv 36[144]$

Cherchons le $PGCD(60, 144)$

On a : $PGCD(60, 144) = 12$

Comme 12 divise 36, alors l'équation devient : $5x \equiv 3[12]$

Cherchons l'inverse modulo 12 de 5

On a : $5^{-1}[12] = 5$

$x \equiv 3 \times 5[12]$

$x \equiv 15[12]$

$x \equiv 3[12]$

D'où $S = \{3 + 12k; k \in \mathbb{Z}\}$

1.6 Système d'équations linéaires modulo n

1.6.1 Définition

Soit n_1, n_2,..., n_p des entiers supérieurs à 2, deux à deux premiers entres eux.

On appelle système d'équations linéaires modulo n tout système de congruence de la forme

$$(S) : \begin{cases} x \equiv a_1[n_1] \\ x \equiv a_2[n_2] \\ \vdots \\ x \equiv a_p[n_p] \end{cases} \quad \text{où } x \in \mathbb{Z} \text{ est l'inconnue.}$$

1.6.2 Résolution

a) Méthode de substitution

Pratique d'un exemple

Résoudre dans $\mathbb{Z}$ le système suivant $\begin{cases} 2x \equiv 1[5] \\ 3x \equiv 2[7] \end{cases}$

Solution

Résolvons dans $\mathbb{Z}$ le système suivant $\begin{cases} 2x \equiv 1[5] \\ 3x \equiv 2[7] \end{cases}$

Transformons le système

$\triangleright$ $2x \equiv 1[5]$

Cherchons l'inverse modulo 5 de 2

On a : $2^{-1}[5] = 3$

$2x \equiv 1[5] \Longrightarrow x \equiv 3[5]$

$\triangleright$ $3x \equiv 2[7]$

Cherchons l'inverse modulo 7 de 3

On a : $3^{-1}[7] = 5$

$3x \equiv 2[7] \Longrightarrow x \equiv 10[7] \Longrightarrow x \equiv 3[7]$

Le système devient : $\begin{cases} x \equiv 3[5] \ (1) \\ x \equiv 3[7] \ (2) \end{cases}$

(1) $x \equiv 3[5] \Leftrightarrow x = 3 + 5p$, $p \in \mathbb{Z}$

(2) $x \equiv 3[7] \Leftrightarrow x = 3 + 7q,\ q \in \mathbb{Z}$

On a : $3 + 5p = 3 + 7q \Longrightarrow 5p = 7q$

Or $PGCD(5; 7) = 1$, d'après le théorème de Gauss ; 5 divise q

5 divise $q \Leftrightarrow$ il existe $k \in \mathbb{Z}$, tel que $q = 5k$

(2) $x = 3 + 7(5k) \Longrightarrow x = 3 + 35k$

D'où $S = \{3 + 35k; k \in \mathbb{Z}\}$

b) Méthode des restes chinois

Le système (S) admet une solution x_0 modulo N tel que : $x_0 = \left(\sum_{i=1}^{p} a_i N_i y_i\right)[N]$

où $N = n_1 \times n_2 \times n_3 \times ... \times n_p$; $N_i = \dfrac{N}{n_i}$ et $y_i = N_i^{-1}[n_i]$.

Pratique d'un exemple

Résoudre dans $\mathbb{Z}$ le système suivant $\begin{cases} 2x \equiv 1[5] \\ 3x \equiv 2[7] \end{cases}$

Solution

Résolvons dans $\mathbb{Z}$ le système suivant $\begin{cases} 2x \equiv 1[5] \\ 3x \equiv 2[7] \end{cases}$

Transformons le système

▷ $2x \equiv 1[5]$

Cherchons l'inverse modulo 5 de 2

On a : $2^{-1}[5] = 3$

$2x \equiv 1[5] \Longrightarrow x \equiv 3[5]$

▷ $3x \equiv 2[7]$

Cherchons l'inverse modulo 7 de 3

On a : $3^{-1}[7] = 5$

$3x \equiv 2[7] \Longrightarrow x \equiv 10[7] \Longrightarrow x \equiv 3[7]$

Le système devient : $\begin{cases} x \equiv 3[5]\ (1) \\ x \equiv 3[7]\ (2) \end{cases}$

$N = 5 \times 7 = 35$

$N_1 = \dfrac{N}{n_1} = \dfrac{35}{5} = 7$

$N_2 = \dfrac{N}{n_2} = \dfrac{35}{7} = 5$
$y_1 = N_1^{-1}[n_1] = 7^{-1}[5] \Longrightarrow y_1 = 3$
$y_2 = N_2^{-1}[n_2] = 5^{-1}[7] \Longrightarrow y_2 = 3$
$x_0 = \left(\sum_{i=1}^{2} a_i N_i y_i\right)[N] \Longrightarrow x_0 = (3 \times 7 \times 3) + (3 \times 5 \times 3)[35]$
$x_0 = 108[35]$
$x_0 = 3[35] \Longrightarrow x_0 = 3 + 35k,\ k \in \mathbb{Z}$
D'où $S = \{3 + 35k; k \in \mathbb{Z}\}$

1.7 Autres systèmes d'équations

Systèmes de types $\begin{cases} \text{PGCD}(x,y) = \alpha \\ x + y = \beta \end{cases}$; $\begin{cases} \text{PPCM}(x,y) = \alpha' \\ x \times y = \beta' \end{cases}$ ou $\begin{cases} \text{PPCM}(x,y) = \alpha'' \\ x + y = \beta'' \end{cases}$

Application

Résoudre dans $\mathbb{N}^2$ les systèmes suivantes : $(S) : \begin{cases} \text{PGCD}(x,y) = 354 \\ x + y = 5664 \end{cases}$

Corrigé

Résolution dans $\mathbb{N}^2$ du système : $\begin{cases} \text{PGCD}(x,y) = 354 \ \ (1) \\ x + y = 5664 \ \ (2) \end{cases}$

$(1) \Longrightarrow \exists x'$ et y' premiers entre eux tels que $x = 354x'$ et $y = 354y'$. En remplaçant x et y dans l'équation (2) on obtient : $354(x' + y') = 5664 \Longrightarrow x' + y' = 16$

On trouve : $\begin{cases} x' = 1 \\ y' = 15 \end{cases}$ ou $\begin{cases} x' = 15 \\ y' = 1 \end{cases}$; $\begin{cases} x' = 3 \\ y' = 13 \end{cases}$ ou $\begin{cases} x' = 13 \\ y' = 3 \end{cases}$;

$\begin{cases} x' = 5 \\ y' = 11 \end{cases}$ ou $\begin{cases} x' = 11 \\ y' = 5 \end{cases}$; $\begin{cases} x' = 9 \\ y' = 7 \end{cases}$ ou $\begin{cases} x' = 7 \\ y' = 9 \end{cases}$

En remplaçant x' et y' par leur valeur dans x et y on trouve

$S = \{(354, 5310); (5310, 354); (1062, 4602); (4602, 1062); (1770, 3894);$
$(3894, 1770); (2478, 3186); (3186, 2478)\}$

1.8 Systèmes de numérotations

1.8.1 Définition

Un système de numérotation est une manière de représenter un entier naturel.

On distingue :

▷ Le système de numérotation binaire ou système de base 2, l'ensemble de chiffres utilisés est $\{0 : 1\}$;

▷ Le système de numérotation décimal ou système de base 10, l'ensemble de chiffres utilisés est $\{0 : 1; 2; 3; 4; 5; 6; 7; 8; 9\}$;

▷ Le système de numérotation hexadécimal ou système de base 16, l'ensemble de chiffres utilisés est $\{0 : 1; 2; 3; 4; 5; 6; 7; 8; 9; 10; 11; 12; 13; 14; 15\}$ ou $\{0 : 1; 2; 3; 4; 5; 6; 7; 8; 9; A; B; C; D; E; F\}$ avec $A; B; C; D; E; F$ représentent respectivement 10 ; 11 ; 12 ; 13 ; 14 et 15.

1.8.2 Propriété

Soit b un entier naturel supérieur ou égal à 2.

Tous entier naturel non nul x peut s'écrire de façon unique $x = \sum_{k=0}^{n} a_k b^k$ où a_k sont des entiers tels que $0 \leq a_k < b$ et $a_n \neq 0$.

On note alors $x = \overline{a_n a_{n-1} a_{n-2} ... a_1 a_0}^b$.

Cette écriture est appelée écriture de x en base b.

Remarque

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

1.8.3 Changement de base de numérotation

a) Passage de la base décimal en base a

Exercice

Écrire les nombres 87 en base 2.

Corrigé

On effectue les divisions successives (euclidiennes) de 87 par 2.

Soit $87 = \overline{1010111}^2$

b) Passage de la base a en base 10

Exercice

Écrire les nombres $\overline{10100111001}^2$ en base 10.

Corrigé

On a : $\overline{10100111001}^2 = 1 \times 2^{10} + 0 \times 2^9 + 1 \times 2^8 + 0 \times 2^7 + 0 \times 2^6 + 1 \times 2^5 + 1 \times 2^4 + 1 \times 2^3 + 0 \times 2^2 + 0 \times 2^2 + 0 \times 2^1 + 1 \times 2^0) = 1337$

c) Passage de la base 10 en base 16

Exercice

Écrire le nombre suivant 64206 en base 16.

Corrigé

On effectue les divisions successives (euclidiennes) de 64206 par 16.
Soit $64206 = \overline{FACE}^{16}$

EXERCICES D'APPLICATIONS

Exercice 1

Trouver le reste le reste de la division euclidienne de $(2004)^{2021}$ par 5.

Exercice 2

1. Vérifier que 999 est divisible par 27.
2. En déduire que pour tout entier naturel n, $10^{3n} \equiv 1[27]$.
3. On donne $\alpha = 10^{100} + 100^{10}$. Quel est le reste de la division euclidienne de α par 27.

Exercice 3

On considère dans $\mathbb{Z}^2$ l'équation : $(E) : 148x - 97y = 1$.

1. Énoncer le théorème de Bézout.
2. a) Montrer que $(-19, -29)$ est une solution particulière de (E).
   b) Résoudre dans $\mathbb{Z}^2$, l'équation (E).
3. a) Déterminer l'inverse modulo 148 de l'entier naturel 97.
   b) Prouver que 149 est un nombre premier.
   c) Soit p un entier naturel non nul tel que : $p \leq 148$.
   Montrer, en utilisant le petit théorème de Fermat que : $p^{148} \equiv 1[149]$.
4. Soit $a \in \{2, 3, 4, ..., 148\}$. On pose $S(a) = 1 + a + a^2 + ... + a^{147}$.
   a) Montrer que a^{148} et $a - 1$ sont premier entre eux.
   b) Montrer que 149 divise $S(a)$.

Exercice 4

1. a) Quel est le reste de la division euclidienne de 6^{10} par 11 ?

   b) Quel est le reste de la division euclidienne de 6^4 par 5 ?

   c) En déduire que $6^{40} \equiv 1[11]$ et que $6^{40} \equiv 1[5]$.

   d) Démontrer que $6^{40} - 1$ est divisible par 55.

2. Soit (S) et (S') deux systèmes définis par : $(S) : \begin{cases} a \equiv 3[65] \\ a \equiv 4[40] \end{cases}$ et $(S') : \begin{cases} b \equiv 3[17] \\ b \equiv 4[40] \end{cases}$

   (a) Montrer que les systèmes (S) et (S') sont équivalents respectivement aux équations $(E) : 65x - 40y = 1$ et $(E') : 17x - 40y = 1$ avec $(x, y) \in \mathbb{Z}^2$.

   (b) Montrer que l'équation (E) n'admet pas de solution dans $\mathbb{Z}^2$.

   (c) Montrer que l'équation (E') admet au moyen une solution dans $\mathbb{Z}^2$.

3. (a) Montrer que l'équation (E') est équivalente à l'équation $(E'') : 17x \equiv 1[40]$.

   (b) Donner l'inverse modulo 40 de 17.

   (c) En déduire les solutions de l'équation de (E'').

   (d) Déterminer les solutions de l'équation (E').

Exercice 5

On considère l'équation $(E) : 24x + 36y = 60$; où x et y sont des entiers relatifs.

1. Déterminer le $PGCD$ de 24 et 36, puis simplifier l'équation (E).
2. Trouver une solution évidente pour l'équation (E) et résoudre cette équation. On appellera S l'ensemble des couples (x, y) solutions de l'équation (E).
3. Énumérer tous les couples de S tels que $-10 \leq x \leq 10$.
4. Donner ceux parmi eux, pour lesquels x et y sont multiples de 5.

Exercice 6

1. Trouver tous les diviseurs positifs de 21.
2. Trouver tous les couples $(a; b)$ d'entiers naturels tels que : $a^2 - b^2 = 21$

Exercice 7

Soit $n \in \mathbb{N}^*$ un, on considère les nombres a et b définis par : $a = 2n + 3$ et $b = 5n - 2$.

1. Montrer que tout diviseur de a et b est diviseur de 19.
2. En utilisant le théorème de Gauss, déterminer les entiers naturels n pour lesquels $PGCD(a; b) = 19$.

Exercice 8

1. Déterminer les diviseurs positifs de 85.
2. On considère dans $\mathbb{N}\times\mathbb{N}$ le système d'équations (S) suivant : $(S) : \begin{cases} x^2 - y^2 = 5440 \\ \text{PGCD}(x, y) = 8 \end{cases}$
   (a) Montrer que qu'il existe deux entiers naturels a et b premiers entre eux tels que le système (S) soit équivalent au système (S') : $(S) : \begin{cases} a^2 - b^2 = 85 \\ \text{PGCD}(a, b) = 1 \end{cases}$.
   (b) Résoudre le système (S').
   (c) En déduire les couples $(x; y)$, solution de système (S).

Exercice 9

Dans tout l'exercice, x et y désignent des entiers naturels non nuls avec $x < y$.
S est l'ensemble des couples (x, y) tels que $PGCD(x; y) = y - x$.

1. (a) Calculer le plus grand commun diviseur de 363 et 484.
   (b) Le couple $(363; 484)$ appartient-il à S ?
2. Soit n un entier naturel non nul. Le couple $(n; n + 1)$ appartient-il à S ? Justifier votre réponse.
3. (a) Démontrer que $(x; y)$ appartient à S si et seulement si il existe un entier naturel non nul k tel que $\begin{cases} x = k(y - x) \\ y = (k + 1)(y - x) \end{cases}$.
   (b) En déduire que $PPCM(x; y) = k(k + 1)(y - x)$.
4. (a) Déterminer l'ensemble des entiers naturels diviseurs de 228.
   (b) En déduire l'ensemble des couples $(x; y)$ de S tels que $PPCM(x; y) = 228$.

Exercice 10

Soit l'équation $(E) : 109x - 226y = 1$ où x et y sont des entiers naturels.

1. Déterminer le $PGCD(109; 226)$. Que peut-on en déduire pour (E).
2. (a) Vérifier que le couple $(141; 68)$ est une solution particulière de (E).
   (b) En déduire la solution générale de l'équation (E).
3. Dans la suite, A est l'ensemble des entiers naturels inférieurs ou égaux à 226.
   Pour tout $a \in A$, f et g sont deux fonctions définies de la manière suivante : f associe le reste de la division euclidienne de a^{109} par 227 et g le reste de la division euclidienne de a^{141} par 227.

(a) Vérifier que $g[f(0)] = 0$.

(b) Montrer que 227 est un nombre premier.

(c) En déduire que pour $a \neq 0$, $a^{226} \equiv 1[227]$.

4. En déduire que pour $a \neq 0$, $g[f(a)] = a$.

Exercice 11

On donne $B_n = 3^{2n+1} + 2^{n+2}$ où $n \in \mathbb{N}$.

1. Montrer que B_n est divisible par 7.
2. En déduire le reste de la division euclidienne de B_{2020} par 7.
3. (a) Déterminer suivant les valeurs de n le reste de la division de 5^n par 7.

   (b) En déduire le reste de la division de 5^{2020} et 5^{2021} par 7.

Exercice 12

Étant donné deux entiers a et b et un entier naturel n non nuls.

1. (a) Démontrer que si $a \equiv b[n]$ et $c \equiv d[n]$, alors $ac \equiv bd[n]$.

   (b) En déduire que pour tout entier k, $a^k \equiv b^k[n]$.
2. Soit a un entier naturel non divisible par 7.

   (a) Quel est l'ordre modulo 7 de 5 et de 4 ?

   (b) Montrer que $a^6 - 1$ est divisible par 7.

   (c) Montrer que le reste r de la division euclidienne de 6 par k vérifie $a^r \equiv 1[7]$.

   (d) En déduire que k divise 6.
3. On donne $A_n = 4^n + 5^n$. Montrer que $A_{2020} \equiv 6[7]$.

Exercice 13

Résoudre dans $\mathbb{N}^2$ les systèmes suivantes :

$$(S_1) : \begin{cases} \text{PPCM}(x, y) = 168 \\ x \times y = 1008 \end{cases} ; (S_2) : \begin{cases} \text{PGCD}(x, y) = 354 \\ x + y = 5664 \end{cases} ; (S_3) : \begin{cases} \text{PPCM}(x, y) = 504 \\ x + y = 135 \end{cases}$$

et $(S_4) : \begin{cases} \text{PGCD}(x, y) = 42 \\ \text{PPCM}(x, y) = 1680 \end{cases}$

Corrigé de l'exercice 1

On a : $2004 = 5(400) + 4 \Longrightarrow 2004 \equiv 4[5]$

On trouve la période de 2021.

En effet ;

$4^0 \equiv 1[5]$

$4^1 \equiv 4[5]$

$4^2 \equiv 16[5] \Longrightarrow 4^2 \equiv 1[5]$. Alors la période $k = 2$

Ainsi, $2021 = (2 \times 1010) + 1$

D'où $(2004)^{2021} = 4^{2021} = 4^{2(1010)+1} = 4^{2(1010)} \times 4 = 4[5]$

Finalement, le reste de la division euclidienne de $(2004)^{2021}$ par 5 est 4

Corrigé de l'exercice 2

1. Vérifions que 999 est divisible par 27
   On a : $999 = 27 \times 37 \Longrightarrow r = 0$ c'est à dire $999 = 0[27]$
2. $10^{3n} = 1[27] \Longrightarrow [10^3]^n (1000)^n = (99 + 1)^n = 1^n = 1[27] \Longrightarrow (10^3)^n = 1[27]$
3. $\alpha = 10^{1300} + 100^{10}[27] = 10^{3\times 99+1} + 10^{20} = 10^{3\times 99} \times + 10^{3\times\times 10^2} = 10 + 10^2 = 110[27] = 2[27] \Longrightarrow r = 2$