

CHAPITRE 2

ARITHMÉTIQUE

Dans tout ce chapitre \mathbb{N} désigne l'ensemble des entiers naturels et \mathbb{Z} l'ensemble des entiers relatifs .

I. Divisibilité dans \mathbb{Z}

1. Définitions

Définition 1

- Soient a et b deux entiers relatifs tels que $a \neq 0$.

On dit que **a divise b** ou que **a est un diviseur de b** si et seulement si il existe un entier relatif q tel que $b = qa$. Il revient au même de dire que **a divise b** ou que **b est divisible par a** .

- Soient a et b deux entiers relatifs.

b est un multiple de a si et seulement si il existe un entier relatif q tel que $b = qa$.

Si de plus $a \neq 0$, alors b est multiple de a si et seulement si a divise b .

Notation :

- Quand a divise b on écrit $a|b$.
- La notation $a \nmid b$ signifie que a ne divise pas b .

Remarque :

– Dans la définition 1, on a imposé à a d'être non nul ou encore on n'écrira jamais une phrase du genre « 0 divise ... ». Néanmoins, puisque $0 = 0 \times 0$, on peut se permettre de dire que 0 est un multiple de 0.

– Si a est un entier relatif, les multiples de l'entier a sont les entiers relatifs de la forme $q \times a$ où q est un entier relatif. Ce sont donc les nombres : ... $-3a$ $-2a$ $-a$ 0 a $2a$ $3a$...

2. Propriétés de divisibilité

En utilisant la définition précédente, on a les propriétés suivantes :

Propriétés :

- Soit a un entier naturel non nul. Tout diviseur de a est inférieur ou égal à a .
- $\forall a \in \mathbb{Z}$, les diviseurs de a sont les diviseurs de $|a|$.
- $\forall a \in \mathbb{Z}$, les multiples de a sont les multiples de $|a|$.

Démonstration :

i. Soit b un entier naturel diviseur de $a > 0$. Alors par définition, il existe un entier naturel $k > 0$ tel que $a = kb$ $\Leftrightarrow b = \frac{a}{k}$. Or $k \in \mathbb{N}$ et $k > 0$ alors $k \geq 1$. On conclut alors que $a \geq b$.

ii. Soit a un entier relatif :

- Si $a \geq 0$, alors $|a| = a$ et le résultat est prouvé.
- Si $a < 0$ alors $|a| = -a$. Soit b un diviseur de a . Par définition, il existe un entier relatif k tel que $a = kb$. Alors $-a = -kb \Rightarrow |a| = k'b$. Par suite b est aussi un diviseur de $|a|$. Comme b est un diviseur quelconque de a , on conclut alors que tous les diviseurs de a sont aussi les diviseurs de $|a|$.

iii. Soit $a \in \mathbb{Z}$. Si $b = qa$ avec $q \in \mathbb{Z}$, alors $b = (sgn(a)q)|a|$ avec $(sgn(a)q) \in \mathbb{Z}$.

3. Nombres premiers

3-1. Définition

Définition 2 : Soit $p \in \mathbb{N}$.

On dit que p est un **nombre premier** ou plus simplement qu'il est premier si : il admet exactement 2 diviseurs entiers naturels distincts à savoir 1 et le nombre lui-même.

Remarque :

- La notion de nombre premier ne concerne que les entiers naturels.
- 0 a une infinité de diviseurs donc il n'est pas premier.
- 1 n'a qu'un seul diviseur, qui est lui-même donc 1 n'est pas premier.
- 2 a exactement 2 diviseurs : 1 et 2 donc 2 est le plus petit des nombres premiers.

Attention : Un nombre premier n'est pas forcément impair. Par exemple 2 est premier mais pair. Les notions de "parité" et de "primarité" sont bien distinctes.

3-2. Problématique de recherche de nombre premier

A ce jour, il n'existe toujours pas de critère ou de formule qui permet de dire instantanément si un nombre quelconque est premier.

Prenons un entier naturel n différent de 1, pour vérifier si ce nombre est premier ou pas, il suffit alors de partir de 2 et de tester tous les entiers jusqu'à $n - 1$. Si nous trouvons un entier naturel p , différent de 1 et de n , qui divise n alors par définition, n n'est pas premier. Sinon n est premier.

Mais prenons par exemple $n = 145237$. Est-il vraiment nécessaire de tester tous les entiers de 2 à 145237 jusqu'à ce que l'on trouve ou non un diviseur de 145237 ?

Nous allons voir des théorèmes qui nous permettent d'affiner nos recherches.

Théorème 3 :

Soit $n \in \mathbb{N}$, si $n \neq 1$, alors n admet au moins un diviseur premier.

Démonstration :

On va démontrer ce théorème en distinguant les différents cas possibles :

Cas 1 : Si $n = 0$, 2 divise 0 et par suite n admet au moins un diviseur premier.

Cas 2 : Supposons que $n \neq 0$.

- Si n est premier, ce diviseur est lui-même et la propriété est démontrée.
- Si n n'est pas premier, alors n possède au moins un diviseur différent de 1 et de lui-même.

Notons D l'ensemble des diviseurs de n autre que 1 et n . Par hypothèses, D est un sous ensemble non vide de \mathbb{N} , alors il possède un plus petit élément que nous noterons p . p n'est pas nul car 0 ne divise pas $n \neq 0$.

Montrons par absurdité que p est premier :

Si p n'est pas premier, par définition, on peut conclure que p a un diviseur k différent de 1 et de lui-même.

Puisque $k|p$ alors $k \leq p$ et comme $k \neq p$ alors $k < p$.

Or $p|n$ et $k|p \Rightarrow k|n$ avec $k < p < n$. Mais alors, k est dans D et $k < p$ ce qui contredit le fait que p est le plus petit élément de D . Par suite p est premier.

Conclusion : n admet dans tous les cas un diviseur premier.

Commentaire :

La conséquence immédiate de ce théorème est qu'au lieu de tester tous les entiers naturels compris 2 et $n - 1$, on ne va que tester parmi ces entiers, ceux qui sont premiers.

Inversement si $b = k|a|$ avec $k \in \mathbb{Z}$ alors $b = (sgn(a)k)a$. avec $(sgn(a)k) \in \mathbb{Z}$. D'où le résultat.

Théorème 1 :

- i. Pour $a \in \mathbb{Z}^*$, a divise 0. Pour tout $a \in \mathbb{Z}$, 0 est multiple de a .
- ii. Pour $a \in \mathbb{Z}$, 1 divise a . Pour tout $a \in \mathbb{Z}$, a est multiple de 1.

Démonstration :

- i. Soit $a \in \mathbb{Z}^*$, alors on peut écrire $0 = 0 \times a$. Et donc a divise 0 ou encore 0 est multiple de a . Cette dernière affirmation reste claire quand $a = 0$.
- ii. Soit $a \in \mathbb{Z}$. $a = a \times 1$ et donc $1|a$ ou encore a est multiple de 1.

Remarque :

Le théorème précédent dit que **tout entier relatif non nul divise 0** ou encore que **0 est multiple de tout entier relatif**. Cependant, **0 n'est pas le diviseur d'aucun entier relatif**.

Théorème 2 :

- i. Pour $a \in \mathbb{Z}^*$, a divise a (la relation de divisibilité dans \mathbb{Z}^* ou dans \mathbb{N}^* est réflexive).
- ii. Pour $(a, b) \in (\mathbb{N}^*)^2$, $a|b$ et $b|a \Leftrightarrow a = b$ (la relation de divisibilité dans \mathbb{N}^* est anti-symétrique).
- iii. Pour $(a, b) \in (\mathbb{Z}^*)^2$, $a|b$ et $b|a \Leftrightarrow a = b$ ou $a = -b$.
- iv. Pour $(a, b, c) \in \mathbb{Z}^* \times \mathbb{Z}^* \times \mathbb{Z}$, $a|b$ et $b|c \Rightarrow a|c$ (La transitivité)

Démonstration :

- i. Immédiat ($a = 1 \times a$)
- ii. Soit $(a, b) \in (\mathbb{N}^*)^2$. Si a divise b et b divise a , alors d'après les propriétés, $a \leq b$ et $b \leq a \Leftrightarrow a = b$. Réciproquement si $a = b$ alors a divise b et b divise a d'après i).
- iii. Soit $(a, b) \in (\mathbb{Z}^*)^2$ si $a|b$ et $b|a$ alors $|a|$ divise $|b|$ et $|b|$ divise $|a|$ puis on déduit que $|a| = |b|$ (d'après ii.). Ainsi $a = b$ ou $b = -a$. Réciproquement, si $a = b$ ou $b = -a$, alors a divise b et b divise a .
- iv. Soit $(a, b, c) \in \mathbb{Z}^* \times \mathbb{Z}^* \times \mathbb{Z}$ $\left\{ \begin{array}{l} a|b \Leftrightarrow \exists q \in \mathbb{Z} \text{ tel que } b = qa \\ b|c \Leftrightarrow \exists q' \in \mathbb{Z} \text{ tel que } c = q'b \end{array} \right. \Rightarrow c = qq'a \text{ et par suite } a|c.$

Théorème 3 : Soit $(a, b, c) \in \mathbb{Z} \times \mathbb{Z} \times \mathbb{Z}^*$

Si $c|a$ et $c|b$ alors $\forall (u, v) \in \mathbb{Z}^2$, $c|(au + bv)$

Démonstration :

- Soit $(a, b, c) \in \mathbb{Z} \times \mathbb{Z} \times \mathbb{Z}^*$ $\left\{ \begin{array}{l} c|a \Leftrightarrow \exists q \in \mathbb{Z} \text{ tel que } a = qc \\ c|b \Leftrightarrow \exists q' \in \mathbb{Z} \text{ tel que } b = q'c \end{array} \right. \Rightarrow \forall (u, v) \in \mathbb{Z}^2$, $au + bv = (qu + q'v)c$
Ainsi c divise aussi $au + bv$.

Commentaire :

Le théorème précédent peut être compris de la façon suivante : si a et b sont des multiples communs de c , alors tout entier de la forme $au + bv$ où u et v sont des entiers relatifs, est un multiple de c ou encore que si c est un diviseur commun à a et b , alors c divise tout entier du type $au + bv$, $(u, v) \in \mathbb{Z}^2$.

Exercice 1

Trouver tous les entiers naturels n tels que $2n + 3$ divise $3n + 7$.

Solution

Soit n un entier naturel tel que $2n + 3$ divise $3n + 7$. Puisque $2n + 3$ divise à la fois $2n + 3$ et $3n + 7$ alors $2n + 3$ divise $2(3n + 7) - 3(2n + 3) = 5$. Puisque $2n + 3$ est un entier naturel, on a donc nécessairement $2n + 3 = 1$ ou $2n + 3 = 5$ puis $n = -1$ ou $n = 1$ puis $n = 1$ car n est un entier naturel.

Réciproquement si $n = 1$ alors $2n + 3 = 5$ et $3n + 7 = 10$ et par suite $2n + 3$ divise $3n + 7$.

Il existe un et un seul entier naturel n tel que $2n + 3$ divise $3n + 7$ à savoir $n = 1$.

Le théorème suivant, qu'on va admettre, nous permettra d'alléger encore plus nos efforts de recherche de primalité d'un nombre.

Théorème 4 : Méthode de discrimination d'un nombre premier.

Soit n un entier naturel supérieur ou égale à 2.

Pour déterminer la primalité de n , il suffit de tester dans l'ordre croissant les nombres premiers inférieurs ou égaux \sqrt{n} .

- Si l'un d'eux divise n alors n n'est pas premier.
- Sinon, n est premier.

Exemple

Prenons $n = 247$. Ce nombre est-il premier ?

Pour déterminer si 247 est un nombre premier ou pas, on utilise le théorème précédent.

On a $\sqrt{247} = 15.71$. On va alors tester pour voir s'il existe un nombre premier compris entre 2 et 15 qui divise 247. La liste des nombres premiers compris entre 2 et 15 est : $\{2, 3, 5, 7, 11, 13\}$.

On teste alors si l'un de ces nombres divise 247 à l'aide d'une calculatrice. On retrouve que $\frac{247}{13} = 19$.
Donc 247 n'est pas un nombre premier.

Exercice 2

En utilisant la démarche précédente, déterminer si les nombres suivants sont des nombres premiers ou pas :

1. $n = 569$ 2. $n = 437$ 3. $n = 881$

3-3. Décomposition d'un entier en produit de facteurs premiers

Nous avons vu que si $n \geq 2$ alors il possède au moins un diviseur premier p_1 . Ainsi $\exists q_1 \in \mathbb{N}$ tel que $n = q_1 \times p_1$. Si $q_1 \neq 1$ alors il possède à son tour au moins un diviseur premier p_2 (qui peut être éventuellement égal à p_1). Ainsi $\exists q_2 \in \mathbb{N}$ tel que $q_1 = q_2 \times p_2$ avec $q_2 < q_1$ car $p_2 \neq 1$.

On construit ainsi une suite (q_n) qui est décroissante et minorée par 1. Cette suite s'arrête donc « forcément » or elle ne peut s'arrêter que si l'un de ses termes vaut 1. Ainsi on peut écrire $n = p_1 \times p_2 \times \dots \times p_{k+1}$.

En écrivant les produits de nombres premiers égaux entre eux sous forme de puissance, on obtient donc le théorème suivant :

Théorème 5 : Soit n un entier naturel supérieur ou égale à 2. On peut alors décomposer l'entier n de façon unique sous la forme : $n = p_1^{\alpha_1} \times p_2^{\alpha_2} \times \dots \times p_m^{\alpha_m}$

Où p_1, p_2, \dots, p_m sont des nombres premiers tels que : $p_1 < p_2 < \dots < p_m$ et $\alpha_1, \alpha_2, \dots, \alpha_m$ sont des entiers naturels non nuls.

L'écriture de n sous cette forme est appelée **décomposition de n en produit de facteurs premiers**.

Remarques

- Ce théorème peut être montré de façon rigoureuse à l'aide d'un raisonnement par récurrence.
- L'ordre strict imposé sur les facteurs sert à garantir l'unicité de la décomposition.
- Quel que soit i : $\alpha_i \neq 0$ donc quel que soit i : $p_i | n$. De plus, il ne peut exister de nombre premier p différent des p_i qui divise n car sinon la décomposition ne serait pas unique.

Exemple de décomposition : technique et présentation.

Décomposons le nombre $n = 420$

		Méthode :
420	2	– On teste les nombres premiers par ordre croissant et on dispose les calculs comme dans cet exemple.
210	2	– Arriver à une étape i , si un entier premier ne divise pas le quotient trouvé à l'étape $i - 1$, il ne
105	3	peut plus être un diviseur dans les étapes suivantes.
35	5	– A la fin on fait le produit des diviseurs premiers trouvés affectés à leurs ordres de multiplicité.
7	7	– Dans notre exemple, $n = 420 = 2^2 \times 3 \times 5 \times 7$

Exercice 3

Donner la décomposition en facteurs premiers des nombres suivants :

1. $n = 2475$

2. $n = 1859$

3. $n = 18360$

II. Division euclidienne dans \mathbb{Z}

On admet le théorème suivant :

Théorème 6 : Soit $a \in \mathbb{Z}$ et $b \in \mathbb{N}^*$.

Il existe un couple (q, r) d'entiers relatifs et un seul tels que :

$$a = bq + r \quad \text{et } 0 \leq r < b$$

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

Exemple

Soit $n = 311$.

On peut écrire $n = 3 \times 103 + 2$. Dans ce cas :

- La division euclidienne de 311 par 3 a pour quotient $q = 103$ et pour reste $r = 2$.
- On peut aussi dire que la division euclidienne de 311 par 103 a pour quotient $q = 3$ et pour reste $r = 2$.

On a immédiatement le résultat suivant concernant la divisibilité d'un entier par un autre :

Propriété : Soient a et b deux entiers relatifs tels que $b \neq 0$.

b divise a si et seulement si le reste de la division euclidienne de a par b est nul.

III. PGCD - PPCM

On rappelle ce théorème important :

Théorème 7 :

- Toute partie non vide de \mathbb{N} admet un plus petit élément.
- Toute partie non vide et majorée de \mathbb{N} admet un plus grand élément.

A- PGCD**1. Introduction à la notion de pgcd**

Soient a et b deux entiers relatifs non nuls. On note par $D(a)$ l'ensemble des diviseurs de a qui sont des entiers positifs et par $D(b)$ celui des diviseurs de b qui sont des entiers positifs. L'ensemble de leurs diviseurs communs est noté : $D(a, b)$ avec $D(a, b) = D(a) \cap D(b)$.

$D(a, b)$ est non vide car on sait que pour tout entier relatif n , 1 divise n . En particulier 1 divise a et b donc $D(a, b)$ n'est pas vide.

De plus, a et b admettant un nombre fini de diviseurs et par conséquent leurs diviseurs communs sont en nombre fini. $D(a, b)$ étant un sous ensemble fini et non vide de \mathbb{N} , il admet donc un plus grand élément qu'on note d . d est donc par construction, le plus grand commun diviseur à a et b .

On a alors la définition suivante :

Définition 3 : Soit a et b deux entiers relatifs tous non nuls.

On dit que le nombre d est le **Plus Grand Commun Diviseur** de a et b lorsque d divise a , d divise b et qu'il n'y a pas un diviseur commun à ces deux nombres plus grands que d .

d est noté le plus souvent $PGCD(a, b)$ mais aussi $a \wedge b$

Remarque :

Si $a = b = 0$, la notion de PGCD de a et b n'a pas de sens car tout entier relatif non nul est un diviseur commun à a et b .

Exemple

Soient $a = -12$ et $b = 26$.

Alors $D(a) = \{1, 2, 3, 4, 6, 12\}$ et $D(b) = \{1, 2, 13, 26\}$. Alors $D(a, b) = \{1, 2\}$. On conclut que :
 $-12 \wedge 26 = 2$

Dans l'exemple précédent, on peut remarquer rechercher le $PGCD(-12, 26)$ revient à rechercher celui de $(12, 26)$. On généralise cette remarque dans le théorème suivant :

Théorème 8 :

Soient a et b deux entiers relatifs tels que $a \neq 0$ ou $b \neq 0$. Alors $PGCD(a, b) = PGCD(|a|, |b|)$.

Démonstration :

On a vu dans les propriétés de divisibilité que pour tout $a \in \mathbb{Z}$, les diviseurs de a sont les diviseurs de $|a|$. En utilisant cette propriété, on peut conclure que, les diviseurs communs à a et b sont aussi les diviseurs communs à $|a|$ et $|b|$. En particulier, le plus grand des diviseurs communs à a et b est aussi le plus grand des diviseurs communs à $|a|$ et $|b|$ ce qui démontre le résultat.

Commentaire :

Ce résultat ramène la recherche du PGCD de deux entiers relatifs à la recherche du PGCD de deux entiers naturels. Par exemple $PGCD(-35, 30) = PGCD(35, 30)$, $PGCD(-100, -25) = PGCD(100, 25)$ et le $PGCD(50, -60) = PGCD(50, 60)$.

2. Propriétés du PGCD

De la définition du PGCD et les propriétés de divisibilité, on déduit facilement les propriétés suivantes :

Propriétés : Soient a et b deux entiers relatifs tels que $a \neq 0$ ou $b \neq 0$:

i-a. $PGCD(a, a) = |a|$

b. $PGCD(a, 1) = 1$

c. $PGCD(a, 0) = |a|$.

ii-a. Si b divise a , alors $PGCD(a, b) = |b|$

b. Si a divise b , alors $PGCD(a, b) = |a|$.

iii-a. Pour tout entier naturel non nul k , $PGCD(ka, kb) = k \times PGCD(a, b)$

b. Pour tout entier relatif non nul k , $PGCD(ka, kb) = |k| \times PGCD(a, b)$

Exercice 4

Déterminer les PGCD suivants :

$$\begin{array}{lll} \text{1. } \text{PGCD}(24, 32) & \text{2. } \text{PGCD}(221, -187) & \text{3. } \text{PGCD}(-240, -32). \end{array}$$

3. Techniques de recherche du PGCD**3-1. Utiliser l'ensemble de diviseur**

Si on connaît l'ensemble des diviseurs positifs des deux entiers, on peut facilement déterminer le plus grand diviseur commun à ces deux nombres.

Application

Soient $a = 84$ et $b = 726$.

Alors $D(a) = \{1, 2, 3, 4, 6, 7, 12, 14, 21, 28, 42, 84\}$ et $D(b) = \{1, 2, 3, 6, 11, 22, 33, 66, 121, 242, 363, 726\}$.

On déduit facilement $a \wedge b = 6$.

3-2. Utilisation de la décomposition d'un nombre en facteur premiers

Si l'on possède les décompositions de a et de b , il est alors inutile de rechercher l'ensemble des diviseurs communs pour n'en garder que le plus grand. La méthode consiste à :

- décomposer chaque nombre en produit de facteurs premiers.
- Puis affecter aux facteurs premiers communs l'exposant le plus petit.

Reprenons $a = 84$ et $b = 726$.

- ♦ On décompose les entiers a et b en produits de facteurs premiers : $84 = 2^2 \times 3 \times 7$ et $726 = 2 \times 3 \times 11^2$.
- ♦ Et on affecte aux facteurs premiers communs l'exposant le plus petit :
 - En utilisant les décompositions, on voit 2 et 3 sont des facteurs premiers qui divisent 84 et 726.
 - Alors $\text{PGCD}(84, 726) = 2^1 \times 3^1 = 6$.

Les exemples suivants permettent de mieux comprendre cette technique :

i. Soient $a = 2^7 \times 5^3 \times 7^2 \times 11 \times 13$ et $b = 2^3 \times 5^5 \times 7^2 \times 11^2 \times 17^2$.

Alors le $\text{PGCD}(a, b) = 2^3 \times 5^3 \times 7^2 \times 11 = 539000$

ii. Soient $a = 2 \times 7^2 \times 11$ et $b = 3^3 \times 5^2 \times 17^2$. Dans ce cas, a et b n'ont pas de diviseur premier en commun.

Alors $\text{PGCD}(a, b) = 1$.

iii. Soient $a = 2^2 \times 3 \times 7^2 \times 17$ et $b = 2^2 \times 3 \times 5^5$. Alors le $\text{PGCD}(a, b) = 2 \times 3 = 12$.

Exercice 5

En utilisant la décomposition en produits de facteurs premiers, déterminer les PGCD suivants :

$$\begin{array}{lll} \text{1. } \text{PGCD}(96, 252) & \text{2. } \text{PGCD}(1470, 252) & \text{3. } \text{PGCD}(1815, 98). \end{array}$$

3-3. Utilisation de l'algorithme d'Euclide

Avant d'exposer cette méthode, On commence par le lemme d'Euclide qu'on va admettre :

Lemme d'Euclide : Soit a, b, q et r des entiers relatifs tels $a \neq 0, b \neq 0, r \neq 0$ et $a = bq + r$.

$$\text{PGCD}(a, b) = \text{PGCD}(b, r) \quad (a \wedge b = b \wedge r)$$

En utilisant ce lemme, on peut énoncer le théorème de l'algorithme d'Euclide :

Théorème de l'algorithme d'Euclide : Soient a et b deux entiers naturels non nuls :

- Si b divise a alors $\text{PGCD}(a, b) = b$.
- Sinon $\text{PGCD}(a, b)$ est le dernier reste non nul dans les divisions euclidiennes successives du diviseur par le reste.

Donc l'algorithme d'Euclide consiste donc à :

- effectuer les divisions successives de l'algorithme d'Euclide.
- le dernier reste non nul est le PGCD de a et de b .

Remarque :

- Il faut toujours faire la division euclidienne du "grand nombre" par le "petit nombre".
- Si une des divisions a un reste égal à 1 alors $\text{PGCD}(a, b) = 1$ car le reste suivant strictement inférieur à 1 ne peut être que nul.

Application

Soient $a = 7260$ et $b = 2574$.

$$7260 = 2 \times 2574 + 2112$$

$$2574 = 1 \times 2112 + 462$$

$$2112 = 4 \times 462 + 264$$

$$462 = 1 \times 264 + 198$$

$$264 = 1 \times 198 + 66$$

$$198 = 3 \times 66 + 0$$

D'où $\text{PGCD}(2574, 7260) = 66$

NB : Il faut bien noter que dans l'algorithme d'Euclide, on prend le **dernier reste non nul** comme PGCD.

Exercice 6

En utilisant la méthode d'algorithme d'Euclide, déterminer les PGCD suivants :

1. $\text{PGCD}(66248, 9438)$
2. $\text{PGCD}(1122, 5915)$
3. $\text{PGCD}(343, 539)$.

A partir, de l'algorithme d'Euclide, on obtient une propriété importante du PGCD qu'on va admettre.

Théorème 9 : Soit a et b deux entiers relatifs non nuls.

- Il existe u et v deux entiers relatifs tel que : $a \wedge b = au + bv$.
- Les diviseurs communs à a et à b sont les diviseurs de leur PGCD .

B- PPCM

1. Introduction à la notion de PPCM

Notons Θ l'ensemble des entiers $m \in \mathbb{N}^*$ tel que m est multiple de a et b ou encore $\Theta = \{m \in \mathbb{N}^* / a|m \text{ et } b|m\}$. Θ est une partie non vide de \mathbb{N} car $|ab| \in \Theta$. D'après le théorème 7, on peut déduire que Θ admet un plus petit élément qui est par définition un entier naturel non nul, multiple commun à a et à b et plus petit que tout multiple commun à a et à b qui est strictement positif. On a alors la définition suivante du *PPCM*.

Définition 4 : On dit que le nombre entier naturel m est le Plus Petit Multiple Commun de deux entiers relatifs a et b lorsque m est un multiple strictement positif de a et de b et qu'il n'y a pas d'autre plus petit multiple non nuls de ces deux nombres. On note : $m = \text{PPCM}(a, b) = a \vee b$

D'une manière pratique, pour déterminer le *PPCM* de deux entiers relatifs, on considère leurs valeurs absolues qu'on décompose par la suite en produit de facteurs premiers. Une fois les décompositions trouvées, le *PPCM* est obtenu en faisant le produit $m_1 \times m_2$ avec :

- m_1 produit des facteurs premiers figurant à la fois dans la décomposition de $|a|$ et celle de $|b|$ affectés aux exposants les plus grands,
- m_2 produit de tous les facteurs premiers figurant dans la décomposition de $|a|$ et celle de $|b|$ affectés à leurs exposants et qui ne sont pas intervenus dans le calcul de m_1 .

Cernons bien ce qui a été dit à l'aide d'exemples :

Exemple

i) Soient $a = 440$ et $b = 2100$. On a : $a = 440 = 2^3 \times 5 \times 11$ et $b = 2100 = 2^2 \times 3 \times 5^2 \times 7$.

Application de la méthode :

– On repère les facteurs premiers communs à ces deux puis on fait un premier produit des facteurs communs ayant le plus grand exposant.

– A ce premier produit, on multiplie avec le reste des autres facteurs restants des deux nombres.

En appliquant la méthode, on conclue que $PPCM(440, 2100) = 2^3 \times 5^2 \times 3 \times 11 \times 7 = 46200$.

ii) Soient $a = 2^7 \times 3^2 \times 13$ et $b = 2 \times 3^2 \times 7 \times 11$.

Alors on a $PPCM(a, b) = 2^7 \times 3^2 \times 7 \times 11 \times 13 = 1153152$.

iii) Soient $a = 2^2 \times 3 \times 5$ et $b = 7^2 \times 11$ alors $PPCM(a, b) = 2^2 \times 3 \times 7^2 \times 11 \times 5 = 32340$.

Exercice 7

Déterminer les PPCM suivants :

$$1. \quad PPCM(66, 660)$$

$$2. \quad PGCD(294, 325)$$

$$3. \quad PGCD(5775, 1365).$$

2. Propriétés du PPCM

De la définition du PPCM on a immédiatement le théorème suivant :

Théorème 10 :

i. Pour tout entier relatif a non nul, $a \vee a = |a|$. En particulier si $a \in \mathbb{N}^*$ alors $a \vee a = a$.

ii. Pour tout $(a, b) \in (\mathbb{Z}^*)^2$, $PPCM(a, b) = PPCM(|a|, |b|)$

iii. Pour tout $a \in \mathbb{Z}^*$ alors $a \vee 1 = |a|$.

iv. Pour tout $(a, b) \in (\mathbb{Z}^*)^2$, si b divise a alors $a \vee b = |a|$.

Commentaire :

Le théorème 10 permet ramener la recherche du $PPCM$ de deux entiers relatifs à la recherche du $PPCM$ de deux entiers naturels comme dans le cas du $PGCD$.

On peut également mentionner d'autres propriétés du $PPCM$.

Autre propriétés du PPCM :

Soit $(a, b) \in (\mathbb{Z}^*)^2$

i. Pour $(a, b) \in (\mathbb{Z}^*)^2$ et pour tout $k \in \mathbb{Z}^*$, $PPCM(ka, kb) = |k| \times PPCM(a, b)$

En particulier si $k \in \mathbb{N}^*$ alors $PPCM(ka, kb) = k \times PPCM(a, b)$.

ii. Pour tout $(a, b) \in (\mathbb{Z}^*)^2$, $a|(a \vee b)$, $b|(b \vee a)$ et $(a \vee b)|ab$.

Lien entre PPCM et le PGCD

Théorème 11 :

Soient a et b deux entiers relatifs non nuls :

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

Commentaire :

Ce théorème nous donne une autre méthode pour calculer le $PPCM$ de deux nombres connaissant leur $PGCD$. Il est le plus souvent facile de déterminer le $PGCD$ que le $PPCM$ ou vice versa.

NB : Le $PPCM$ et le $PGCD$ sont toujours des **entiers naturels strictement positifs**.

IV. Nombres premiers entre eux. Théorème de Bézout et Gauss

1. Nombres premiers entre eux

Définition 5 : Soient a et b deux entiers relatifs non nuls.

On dit que a et b sont premiers entre eux si $PGCD(a, b) = 1$.

Par exemple le $PGCD$ de 10 et 5 est 5. Donc 10 et 5 ne sont pas premiers entre eux.

Le $PGCD$ de 11 et 12 est égale à 1. Donc 12 et 11 sont premiers entre eux.

Commentaire :

- Deux nombres premiers entre eux ont donc 1 pour seul diviseur commun.
- Si a est un nombre premier et que a ne divise pas b alors a et b sont premiers entre eux.

En appliquant le théorème 9 pour deux nombres premiers entre eux, on a le théorème de Bézout :

Théorème de Bézout : Soient a et b deux entiers relatifs non nuls.

a et b sont premiers entre eux si et seulement si il existe deux entier relatif u et v tels que : $au + bv = 1$

Commentaire :

- Le couple (u, v) n'est pas forcément unique.
- Ce couple peut être trouvé en « remontant » les divisons de l'algorithme d'Euclide. Cette technique sera vue dans le paragraphe sur les équations diophantiennes.

Le théorème suivant est une application du théorème de Bézout.

Théorème 12 : Soient a , b et c trois entiers relatifs non nuls.

Si c est premier avec a et b alors c est premier avec $a \times b$

Démonstration :

c est premier avec a et $b \Leftrightarrow \begin{cases} \exists(u, v) \in \mathbb{Z}^2 \text{ tel que } au + cv = 1 \\ \exists(u', v') \in \mathbb{Z}^2 \text{ tel que } bu' + cv' = 1 \end{cases}$ En multipliant membre à membre ces deux égalités, on obtient : $abuu' + c(auv' + bvu' + cvv') = 1$. D'où le résultat d'après le théorème de Bézout.

2. Théorème de Gauss

Le théorème suivant est une conséquence du théorème de Bézout.

Théorème de Gauss :

Soient a , b et c trois entiers relatifs tels que $a \neq 0$ et $b \neq 0$. Si a divise bc et si a et b sont premiers entre eux, alors a divise c .

Démonstration :

Soient a , b et c trois entiers relatifs tels que $a \neq 0$ et $b \neq 0$:

- a divise $bc \Leftrightarrow \exists q$ tel que $bc = qa$.
- a et b sont premiers entre eux $\Leftrightarrow \exists (u, v) \in (\mathbb{Z})^2$ tels que $au + bv = 1$.

On multiplie les deux membres de cette dernière égalité par c et on obtient :

$acu + cbv = c \Rightarrow acu + qav = c \Rightarrow a(cu + qv) = c$. Ainsi a divise alors c .

3. Équations diophantiennes

Une équation diophantine est une équation d'inconnues relatifs x et y du type : (E) : $ax + by = c$ avec a , b et c des entiers relatifs tels que $a \neq 0$ ou $b \neq 0$.

3-1. Étapes de résolution des équations du type (E) : $ax + ay = c$

- Condition nécessaire et suffisante d'existence de solution :

Notons $d = PGCD(a, b)$. Si (E) admet au moins une solution alors il existe u et v entiers relatifs tels que : $au + bv = c$. Puisque d divise a et b donc d divise toute combinaison linéaire de a et de b . Par conséquent $d|c$. Réciproquement supposons que $d|c$, alors $\exists k \in \mathbb{Z}$ tel que $c = kd$. Puisque $d = PGCD(a, b)$ alors il existe des entiers relatifs a' et b' premiers entre eux tels que $a = d \times a'$ et $b = d \times b'$.

En utilisant le théorème de Bézout, on déduit qu'il existe u' et v' deux entiers relatifs tels que $a'u' + b'v' = 1$. D'où : $kda'u' + kdb'v' = kd$ Soit : $aku' + bkv' = c$. On pose $u = ku'$ et $v = kv'$. Le couple (u, v) est bien une solution de (E) .

Conclusion : L'équation (E) admet une solution si et seulement si $d = pgcd(a, b)$ divise c .

- Recherche de solution particulière :

La solution particulière de l'équation peut être évidente.

Cependant, si la solution particulière n'est pas évidente, on peut obtenir une solution de l'équation (E) en remontant l'algorithme d'Euclide comme on va le voir dans l'exemple qui suit.

Exemple

Retrouvons la solution particulière de l'équation (E) : $63x + 55y = 1$.

Algorithme d'Euclide :

$$63 = 1 \times 55 + 8$$

$$55 = 6 \times 8 + 7$$

$$8 = 1 \times 7 + 1$$

$$7 = 7 \times 1$$

$$\text{Ainsi } PGCD(63, 55) = 1$$

Recherche d'une solution de (E) à l'aide de l'algorithme d'Euclide

- On exprime 1 en fonction de 7 et 8 à partir de la dernière égalité : $1 = 8 - 7$.
- On exprime ensuite 7 en fonction de 8 et 55 et donc 1 en fonction de 8 et 55 à partir de l'égalité précédente : $1 = 8 - 7 = 8 - (55 - 6 \times 8) = 7 \times 8 - 55$.
- On exprime enfin 8 en fonction de 55 et 63 et donc 1 en fonction de 55 et 63 à partir de la première égalité : $1 = 8 - 7 = 8 - (55 - 6 \times 8) = 7 \times 8 - 55 = 7 \times (63 - 55) - 55 = 63 \times 7 + 55 \times (-8)$

Le couple $(x_0, y_0) = (7, -8)$ est un couple solution de l'équation $63x + 55y = 1$.

- Résolution complète de l'équation (E)

Soit $(a, b) \in (\mathbb{Z}^*)^2$ et soit l'équation diophantine (E) : $ax + by = c$.

On vient de voir que (E) admet une solution si et seulement si le $PGCD(a, b)$ divise c . Quitte à diviser les deux membres de l'équation (E) par le $PGCD(a, b)$, on peut transformer l'équation (E) en une équation du type : $a'x + b'y = c'$ avec $a = da'$, $b = db'$ et $c = dc'$ et de sorte que $a' \wedge b' = 1$.

Par la suite, on peut donc considérer l'équation (E) : $ax + by = c$ avec $a \wedge b = 1$.

Soit $(x, y) \in \mathbb{Z}^2$ et soit le couple (x_0, y_0) , une solution particulière de (E) .

$$(x, y) \text{ solution de } (E) \Leftrightarrow ax + by = c \Leftrightarrow ax + by = ax_0 + by_0 \Leftrightarrow a(x - x_0) = b(y_0 - y).$$

– Puisque $a(x - x_0) = b(y_0 - y)$ alors nécessairement b divise $a(x - x_0)$ et comme $a \wedge b = 1$, d'après le théorème de Gauss, b divise $x - x_0$. Donc $\exists k \in \mathbb{Z}$ tel que $x - x_0 = kb$ ou encore $x = x_0 + kb$.

– De même $a(x - x_0) = b(y_0 - y)$ alors a divise $b(y_0 - y)$ et puisque $a \wedge b = 1$, d'après le théorème de Gauss, a divise $y_0 - y$. Donc $\exists k' \in \mathbb{Z}$ tel que $y_0 - y = k'a$ ou encore $y = y_0 - k'a$.

Réciproquement, soient $(k, k') \in \mathbb{Z}^2$ puis $(x, y) = (x_0 + kb, y_0 - k'a)$.

Si le couple (x, y) vérifie : $ax + by = c$ alors, $a(x_0 + kb) + b(y_0 - k'a) = c \Rightarrow ab(k - k') = 0$.

Or $ab \neq 0$ on déduit alors que $k' = k$. (On vient de montrer maintenant, l'égalité entre les deux variables)

Conclusion : Les solutions de (E) si elles existent, sont des couples (x, y) de la forme :

$$(x, y) = (x_0 + kb, y_0 - ka) \text{ avec } k \in \mathbb{Z}$$

3-2. Exemples de résolution des équations diophantiennes

Dans ces exercices, on va détailler les différents points abordés dans le cas général.

Exemple

Soit l'équation diophantienne (E) : $616x + 585y = 12$.

- **On calcul le PGCD de 616 et 585 :** (Pour facilement les choses, il faut toujours chercher le PGCD à l'aide de l'algorithme d'Euclide pour pouvoir utiliser cet algorithme et retrouver une solution particulière)

$$616 = 1 \times 585 + 31$$

$$585 = 18 \times 31 + 27$$

$31 = 1 \times 27 + 4$ Alors le $\text{PGCD}(616, 585) = 1$. Le $\text{PGCD}(616, 585)$ divise $c = 12$. Par suite l'équation

$27 = 6 \times 4 + 3$ (E) admet au moins une solution.

$$4 = 1 \times 3 + 1$$

$$3 = 3 \times 1 + 0$$

- **Recherche de solution particulière :** Une solution n'est pas évident ici.

On utilise la technique de remonter d'algorithme d'Euclide :

$$1 = 4 - 3$$

$$3 = 27 - 6 \times 4 \Rightarrow 1 = 4 - (27 - 6 \times 4) \Rightarrow 1 = -27 + 7 \times 4$$

$$4 = 31 - 27 \Rightarrow 1 = -27 + 7(31 - 27) \Rightarrow 1 = 7 \times 31 - 8 \times 27$$

$$27 = 585 - 18 \times 31 \Rightarrow 1 = -8 \times 585 + 151 \times 31$$

$$31 = 616 - 585 \Rightarrow 1 = 151 \times 616 - 159 \times 585$$

$$\text{Ainsi } 151 \times 616 - 159 \times 585 = 1$$

– Pour les étapes de calculs, il ne faut pas donner les résultats des opérations mais les écrire sous forme de produit. Écrire par exemple $1 = -27 + 7 \times 4$ au lieu de $1 = -27 + 28$

– Et vue la probabilité de se tromper dans ce genre de manipulation, il est conseillé de vérifier le résultat trouvé

On a donc $151 \times 616 - 159 \times 585 = 1$, pour avoir une solution particulière de (E), il suffit de multiplier les deux membres par 12. Ainsi $1812 \times 616 + (-1908) \times 585 = 12$.

Par suite le couple $(x_0, y_0) = (1812, -1908)$ est une solution de (E).

Solution générale de l'équation (E) :

Notons $(x_0, y_0) = (1812, -1908)$ la solution particulière et $(x, y) \in \mathbb{Z}^2$.

(x, y) est solution de (E) $\Leftrightarrow 616x + 585y = 12 = 616x_0 + 585y_0 \Rightarrow 616(x - x_0) = 585(y_0 - y)$.

– Puisque $616(x - x_0) = 585(y_0 - y)$, alors 616 divise $585(y_0 - y)$. Comme $616 \wedge 585 = 1$ alors d'après le théorème de Gauss, on conclut que 616 divise $y_0 - y$. Par suite $\exists k \in \mathbb{Z}$ tel que $y_0 - y = 616k \Rightarrow y = y_0 - 616k$.

– En remplaçant dans l'égalité $616(x - x_0) = 585(y_0 - y)$, y par $y_0 - 616k$ on tire que $x = x_0 + 585k$.

Ainsi si un couple (x, y) est solution de (E) alors $\exists k \in \mathbb{Z}$ tel que : $\begin{cases} x = 1812 + 585k \\ y = -1908 - 616k \end{cases}$

Réiproquement, soit un couple $(x, y) \in \mathbb{Z}^2$ tel que : $\begin{cases} x = 1812 + 585k \\ y = -1908 - 616k \end{cases}$

Alors $616x + 585y = 616(1812 + 585k) + 585(-1908 - 616k) = 12$ et le couple (x, y) est solution de (E).

Conclusion : Les solutions de (E) sont les couples de la forme : $(x, y) = (1812 + 585k, -1908 - 616k)$ $k \in \mathbb{Z}$

Exemple

Soit l'équation diophantienne (E) : $731x - 204y = 68$.

- **On calcul le PGCD de 731 et 204 avec l'algorithme d'Euclide :**

- **Situation 2** : Les coefficients a et b sont premiers entre eux .
- **Situation 3** : Les coefficients a et b ne sont pas premiers entre eux . Dans ce cas, il faut alors simplifier l'équation par leur pgcd sinon on ne peut pas appliquer le théorème de Gauss.

Exercice 8

Déterminer, si elles existent, les solutions des équations suivantes dans $\mathbb{Z} \times \mathbb{Z}$.

1. $(E_1) : 323x - 391y = 612$.
2. $(E_2) : 42x + 45y = 4$.
3. $(E_3) : 212x + 45y = 3$.
4. $(E_4) : 162x + 207y = 27$
5. $(E_5) : 221x + 247y = 15$

Solution :

1. L'ensemble des solutions de (E_1) est : $S_1 = \{(-216 + 23k, -180 + 19k), k \in \mathbb{Z}\}$.
2. Le $PGCD(42, 45) = 3$. Or 3 ne divise pas 4. Donc l'équation (E_2) n'a pas de solution.
3. L'ensemble des solutions de (E_3) est : $S_3 = \{(-21 + 45k, 99 - 212k), k \in \mathbb{Z}\}$.
4. L'ensemble des solutions de (E_4) est : $S_4 = \{(27 - 23k, -21 + 18k), k \in \mathbb{Z}\}$.
5. Le pgcd de 221 et 247 est 13. Or, 13 ne divise pas 15. L'équation n'admet donc pas de solutions !

V. Congruences

1. Définition

Définition 6 : Soit n un entier naturel. Soient a et b deux entiers relatifs.

On dit que **a est congru à b modulo n** et on écrit $a \equiv b[n]$ si et seulement si $b - a$ est un multiple de n . Il revient au même de dire qu'il existe un entier relatif k tel que $b = a + kn$.

Commentaire :

- On dit aussi que a et b sont égaux modulo n .
- La congruence modulo 1 ne présente aucun intérêt car dans la division euclidienne par 1, tout nombre a pour reste 0. Et donc deux nombres quelconques sont égaux modulo 1.

Exemple

- $17 = 4 \times 4 + 1 \Rightarrow 17 \equiv 1[4]$.
- $24 = 9 + 3 \times 5$ donc on peut écrire $9 \equiv 24[5]$
- Puisque $-3 = 11 - 2 \times 7$ donc $11 \equiv -3[7]$

Un résultat immédiat est :

Théorème 13 : Soit n un entier naturel non nul. Soit a un entier relatif. Soit r le reste de la division euclidienne de a par n . Alors, $a \equiv r[n]$.

$a \equiv 0[n] \Leftrightarrow n$ divise a .

2. Propriétés de la congruence

Théorème 14 : Soit n un entier naturel.

- i. Pour tout entier relatif a , $a \equiv a[n]$ (réflexivité)
- ii. Pour tous entiers relatifs a et b , si $a \equiv b[n]$, alors $b \equiv a[n]$ (symétrie) .
- iii. Pour tous entiers relatifs a , b et c , si $a \equiv b[n]$ et $b \equiv c[n]$ alors $a \equiv c[n]$ (transitivité)

$$\begin{aligned}
 731 &= 3 \times 204 + 119 && \text{Alors le } PGCD(616, 585) = 17. \\
 204 &= 1 \times 119 + 85 \\
 119 &= 1 \times 85 + 34 \\
 85 &= 2 \times 34 + 17 \\
 34 &= 2 \times 17 + 0 && \text{On divise les deux membre de (E) par le } PGCD(731, 204) \text{ et on a l'équation (E') :} \\
 &&& 43x - 12y = 4.
 \end{aligned}$$

Alors résoudre (E) revient à résoudre (E') : $43x - 12y = 4$. On considère désormais l'équation simplifiée (E')

- **Recherche de solution particulière :** Une solution de (E') n'est pas évident ici.
On exécute l'algorithme d'Euclide de 43 et 12 puis on refait le chemin inverse pour trouver la solution particulière

$$\begin{array}{ll}
 43 = 3 \times 12 + 7 & 1 = 5 - 2 \times 2 \\
 12 = 1 \times 7 + 5 & 2 = 7 - 5 \Rightarrow 1 = -2 \times 7 + 3 \times 5 \\
 7 = 1 \times 5 + 2 & 5 = 12 - 7 \Rightarrow 1 = 3 \times 12 - 5 \times 7 \\
 5 = 2 \times 2 + 1 & 7 = 43 - 3 \times 12 \Rightarrow 1 = -5 \times 43 + 18 \times 12 \\
 2 = 2 \times 1 + 0 &
 \end{array}$$

On a donc $-5 \times 43 + 18 \times 12 = 1 \Rightarrow 43 \times (-5) - 12 \times (-18) = 1$, pour avoir une solution particulière de (E'), il suffit de multiplier les deux membres par 4. Ainsi $43 \times (-20) - 12 \times (-72) = 4$.

Par suite le couple $(x_0, y_0) = (-20, -72)$ est une solution de (E').

- **Solution générale de l'équation (E) :**

Notons $(x_0, y_0) = (-20, 72)$ la solution particulière et $(x, y) \in \mathbb{Z}^2$.

(x, y) est solution de (E') $\Leftrightarrow 43x - 12y = 4 = 43x_0 - 12y_0 \Rightarrow 43(x - x_0) = 12(-y_0 + y)$.

– Puisque $43(x - x_0) = 12(-y_0 + y)$, alors 43 divise $12(-y_0 + y)$. Comme $43 \wedge 12 = 1$ alors on conclut, d'après le théorème de Gauss, que 43 divise $y - y_0$. Par suite $\exists k \in \mathbb{Z}$ tel que $y - y_0 = 43k \Rightarrow y = y_0 + 43k$.

– En remplaçant dans l'égalité $43(x - x_0) = 12(-y_0 + y)$, y par $y_0 + 43k$ on tire que $x = x_0 + 12k$.

Ainsi si un couple (x, y) est solution de (E') alors $\exists k \in \mathbb{Z}$ tel que : $\begin{cases} x = -20 + 12k \\ y = -72 + 43k \end{cases}$

Réiproquement, soit un couple $(x, y) \in \mathbb{Z}^2$ tel que : $\begin{cases} x = -20 + 12k \\ y = -72 + 43k \end{cases}$

Alors $43x - 12y = 43(-20 + 12k) - 12(-72 + 43k) = 4$ et le couple (x, y) est solution de (E').

NB : (E) et (E') ont les mêmes solutions car c'est la même équation.

Conclusion : Les solutions de (E) sont les couples de la forme : $(x, y) = (-20 + 12k, -72 + 43k)$ $k \in \mathbb{Z}$

Exemple 3

Soit l'équation diophantienne (E) : $84x - 66y = 13$.

Existence d'une solution :

$84 = 3 \times 2^2 \times 7$ et $66 = 3 \times 2 \times 11$. Alors le $PGCD(84, 66) = 3 \times 2 = 6$.

Puisque 6 ne divise pas 13, alors on conclut l'équation (E) proposé n'admet pas de solution.

Récapitulatif :

Soit à résoudre dans \mathbb{Z} , l'équation (E) : $ax + by = c$ avec a et b des entiers relatifs non nuls.

3 Situations peuvent se présenter :

- **Situation 1 :** Le $PGCD(a, b)$ ne divise pas c et dans ce cas, (E) n'admet aucune solution.

En résumé, si 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 10

Résoudre dans \mathbb{Z} les congruences :

1-a. $6x + 5 \equiv 2[9]$

b. $6x + 5 \equiv 1[9]$

2. $2x + 5 \equiv 0[7]$ et $3x + 5 \equiv 4[7]$

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

Solution :

1-a. Soit x un entier relatif tel que : $6x + 5 \equiv 2[9]$ alors $6x + 5 - 5 \equiv 2 - 5[9]$ puis $6x \equiv -3[9]$

$$6x \equiv -3[9] \Leftrightarrow \exists k \in \mathbb{Z} / 6x = -3 + 9k \Leftrightarrow \exists k \in \mathbb{Z} / 2x = -1 + 3k.$$

$$\Leftrightarrow 2x \equiv -1[3].$$
 Puisque $2 \times 2 = 4 \equiv 1[3]$ alors $2 \times 2 \equiv 2 \times (-1)[3]$

$$\Leftrightarrow x \equiv -2[3] \Leftrightarrow x \equiv 1[3].$$

D'où l'ensemble solution est : $S = \{1 + 3k, k \in \mathbb{Z}\}$

b. Soit x un entier relatif tel que $6x + 5 \equiv 1[9]$ alors $6x + 5 - 5 \equiv 1 - 5[9] \Leftrightarrow 6x \equiv -4[9] \Leftrightarrow 6x \equiv 5[9]$. Par suite : $6x + 5 \equiv 1[9] \Leftrightarrow \exists k \in \mathbb{Z} / 6x = -4 + 9k \Leftrightarrow \exists k \in \mathbb{Z} / 6x - 9k = -4$

Or l'entier $6x - 9k$ est divisible par 3 alors que 3 ne divise pas -4.

Par suite on conclut que la congruence $6x + 5 \equiv 1[9]$ n'a pas de solution dans \mathbb{Z} .

2. – Soit x un entier relatif tel que $2x + 5 \equiv 0[7]$ alors $2x \equiv -5[7]$. Or $2 \times 4 = 8 \equiv 1[7]$. Alors :

$$2x + 5 \equiv 0[7] \Leftrightarrow x \equiv -20[7] \Leftrightarrow x \equiv 1[7]$$

L'ensemble solution est alors $S = \{1 + 7k, k \in \mathbb{Z}\}$

– Soit x un entier relatif tel que $3x + 5 \equiv 4[7]$ alors $3x \equiv -1[7]$ or $3 \times 5 = 15 \equiv 1[7]$. Par suite :

$$3x + 5 \equiv 4[7] \Leftrightarrow x \equiv -5[7] \Leftrightarrow x \equiv 2[7]$$

L'ensemble solution est alors $S = \{2 + 7k, k \in \mathbb{Z}\}$

3. Soit x un entier relatif tel que : $2x \equiv 1[6]$ alors $\exists k \in \mathbb{Z}$ tel que $2x = 1 + 6k \Leftrightarrow 2x = 1 + 2 \times 3k$.

$2x$ est un multiple de 2 alors $1 + 2 \times 3k$ ne l'est pas. D'où la congruence $2x \equiv 1[6]$ n'a pas de solution dans \mathbb{Z} .

4-3. Les classes d'équivalence

Soit n un entier naturel non nul. On peut regrouper les entiers relatifs dont la division euclidienne par n a un certain même reste r dans une classe.

Cette classe s'appelle la classe d'équivalence de r et se note : \bar{r} .

$$\bar{r} = \{m \in \mathbb{Z} / m \equiv r[n]\} = \{nk + r \text{ où } k \in \mathbb{Z}\}.$$

L'ensemble qui contient toutes les classes d'équivalence modulo n est noté : $\mathbb{Z}/n\mathbb{Z}$

$$\mathbb{Z}/n\mathbb{Z} = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \dots, \bar{n-2}, \bar{n-1}\}$$

Dans $\mathbb{Z}/n\mathbb{Z}$, on définit la somme et le produit des classes, de la façon suivante : $\begin{cases} \bar{a} + \bar{b} = \overline{a+b} \\ \bar{a} \times \bar{b} = \overline{ab} \end{cases}$

Par exemple si on désire résoudre dans $\mathbb{Z}/24\mathbb{Z}$: $\bar{9}\bar{x} = \bar{6}$ est équivalent à résoudre dans \mathbb{Z} ; $9x \equiv 6[24]$.

On sait résoudre dans \mathbb{Z} cette équation. L'ensemble solution est dans \mathbb{Z} :

$$S = \{6 + 8k, k \in \mathbb{Z}\} = \{6 + 24k, 14 + 24k, 22 + 24k, k \in \mathbb{Z}\}.$$

Alors dans $\mathbb{Z}/24\mathbb{Z}$, l'équation $\bar{9}\bar{x} = \bar{6}$ a pour solution $S = \{\bar{6}, \bar{14}, \bar{22}\}$.

4. Applications de la congruence

4-1. Recherche du reste d'une division euclidienne

Exercice 9

- 1-a. Déterminer, suivant les puissances de $n \in \mathbb{N}$, le reste de la division euclidienne de 2^n par 5.
- b. En déduire le reste de la division euclidienne de 2^{2022} par 5.
2. Quel est le reste de la division par 5 de 1357^{2022} .
3. Déterminer suivant l'entier naturel n le reste de la division euclidienne de 5^n par 13.
En déduire les entiers naturels n tels que : $5^n \equiv -1[13]$.
4. Déterminer les entiers naturels n tels que 13 divise $5^{2n} + 5^n$.

Solution :

1-a. Cherchons le premier entier $k \geq 1$ tel que $2^k \equiv 1[5]$ ou à défaut on trouve un $k \geq 1$ à partir duquel un cycle apparaît.

$$2^0 \equiv 1[5], \quad 2^1 \equiv 2[5] \quad 2^2 \equiv 4[5] \quad 2^3 \equiv 3[5] \quad 2^4 \equiv 1[5].$$

Ainsi en utilisant les propriétés de congruence, on peut donc classer les entiers n modulo 4 : En effet, si $n = 4k+r$, alors sachant que $2^{2k} \equiv 1^k[5]$ soit $2^{2k} \equiv 1[5]$ et on retrouve que $2^n \equiv 2^r[5]$

- Si $n = 4k$, alors $2^n \equiv 1[5]$
- Si $n = 4k+1$, alors $2^n \equiv 2[5]$
- Si $n = 4k+2$, alors $2^n \equiv 4[5]$
- Si $n = 4k+3$, alors $2^n \equiv 3[5]$

b. Puisque $2022 = 505 \times 4 + 2$. D'après la question 1-a), on conclut que le reste de la division euclidienne de 2^{2022} par 5 est 4.

3. Même technique qu'en 1-a). on a :

$$5^0 \equiv 1[13], \quad 5^1 \equiv 5[13] \quad 5^2 \equiv -1[13] \text{ (ou } 5^2 \equiv 12[13] \text{)} \quad 5^3 \equiv -5[13] \text{ (ou } 5^3 \equiv 8[13] \text{)} \quad 5^4 \equiv 1[13].$$

On déduit à l'aide des propriétés de congruence (comme en 1-a) que :

- Si $n = 4k$, alors $5^n \equiv 1[13]$
- Si $n = 4k+1$, alors $5^n \equiv 5[13]$
- Si $n = 4k+2$, alors $5^n \equiv -1[13]$
- Si $n = 4k+3$, alors $5^n \equiv -5[13]$

En utilisant ce qui précède, on conclut $5^n \equiv -1[13]$ si $n = 4k+2$ avec $k \in \mathbb{N}$.

4. On peut écrire $5^{2n} + 5^n = 5^n(5^n + 1)$. Or $5 \wedge 13 = 1$, d'après Gauss, 13 divise $5^n(5^n + 1)$ si 13 divise $5^n + 1$.
13 divise $5^n + 1 \Leftrightarrow 5^n \equiv -1[13]$. En utilisant la question précédente, on conclut que $n = 4k+2$ avec $k \in \mathbb{N}$

D'où 13 divise $5^{2n} + 5^n$ si $n = 4k+2$, $k \in \mathbb{N}$

4-2. Résolution de la congruence

• Résolution de $x + a \equiv 0[n]$.

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

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

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

Ainsi $x + a \equiv 0[n] \Leftrightarrow x \equiv -a[n]$

• Résolution de $ax \equiv b[n]$.

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 a :

Si $ax \equiv b[n]$ alors $a \times a'x \equiv b \times a'[n]$ ou encore $1 \times x \equiv ba'[n]$ ou enfin $x \equiv ba'[n]$.

et si $x \equiv ba'[n]$ alors $a \times x \equiv ba' \times a[n]$ ou encore $ax \equiv b[n]$.

Démonstration :

- i. Pour tout entier relatif a , $a = 0 \times n + a$ et par définition $a \equiv a[n]$.
- ii. Pour les entiers relatifs a et b , si $a \equiv b[n]$ alors par définition $(a - b)$ est un multiple de n et par conséquent, $(b - a)$ est aussi un multiple de n . D'où $b \equiv a[n]$.
- iii. Soient trois entiers relatifs a , b et c . $a \equiv b[n]$ alors $(a - b)$ est d'un multiple de $n \Rightarrow \exists k \in \mathbb{Z}$ tel que $a = b + kn$. De plus $b \equiv c[n]$ alors $(b - c)$ est d'un multiple de $n \Rightarrow \exists k' \in \mathbb{Z}$ tel que $b = c + k'n$. Par suite $a = b + kn \Rightarrow a = c + (k' + k)n$. D'où $a - c$ est un multiple de n . Ainsi $a \equiv c[n]$.

3. Calculs avec des congruences

Opérations sur la congruence :

Théorème 15 : (compatibilité avec l'addition). Soit n un entier naturel

- i. Soient a , b et c des entiers relatifs. Si $a \equiv b[n]$ alors $a + c \equiv b + c[n]$.
- ii. Soient a , b , c et d des entiers relatifs. Si $a \equiv b[n]$ et $c \equiv d[n]$ alors $a + c \equiv b + d[n]$.

Remarque :

- Ainsi, on peut additionner membre à membre des congruences
- L'écriture $a + c \equiv a + b[n]$ pouvait être écrite $a + c \equiv (a + b)[n]$

Théorème 16 : (compatibilité avec la multiplication). Soit n un entier naturel

- i. Soient a , b et c des entiers relatifs. Si $a \equiv b[n]$ alors $ac \equiv bc[n]$.
- ii. Soient a , b , c et d des entiers relatifs. Si $a \equiv b[n]$ et $c \equiv d[n]$ alors $ac \equiv bd[n]$.
- iii. Pour tout $(a, b) \in \mathbb{Z}^2$, $\forall k \in \mathbb{N}$, Si $a \equiv b[n] \Rightarrow a^k \equiv b^k[n]$.

Ainsi, on peut multiplier membre à membre des congruences.

Commentaires :

Grâce à ces propriétés nous allons pouvoir manipuler la congruence de façon assez intuitive mais attention :

- **La congruence n'est pas compatible avec la division !** c'est-à-dire que si $a \equiv b[n]$ et $a' \equiv b'[n]$ alors on ne peut pas écrire que : $\frac{a}{a'} \equiv \frac{b}{b'}[n]$ pour le simple fait que la congruence est une notion qui s'applique à des nombres relatifs et que le rapport de deux relatifs n'est pas toujours un relatif.
- **Il faudra se méfier des simplifications abusives en particulier lors de la résolution d'équations modulo n.** Plus précisément $ka \equiv kb[n]$ n'implique pas forcement que $a \equiv b[n]$.

En effet :

45 et 63, multiples de 3 sont congrus à 0 modulo 3 donc : $63 \equiv 45[3]$.

En simplifiant par 9, on obtiendrait : $7 \equiv 5[3]$ or $7 - 5 = 2$ qui n'est pas un multiple de 3 et donc on ne peut pas écrire : $7 \equiv 5[3]$

On va maintenant analyser le principal problème des congruences : la possibilité de simplifier un même nombre de part et d'autre d'une congruence.

Théorème 17 : (Simplification). Soit n un entier naturel non nul.

- i. Soient $(a, b, c) \in \mathbb{Z}^3$, $a + c \equiv b + c[n] \Rightarrow a \equiv b[n]$ (tout entier relatif est simplifiable pour l'addition).
- ii. Soient a et b des entiers relatifs, Si $ac \equiv bc[n]$ et $c \wedge n = 1$ alors $a \equiv b[n]$.
- iii. Si $n \geq 2$, les entiers relatifs simplifiables modulo n sont les entiers non nuls et premiers à n .

De plus : $-10 \times 105 + 13 \times 81 = 3$; on peut donc prendre : $(u; v) = (-10, 13)$; on aura alors : $\beta'mu + \alpha'nv = 2106$.

D'où l'ensemble des solutions du système : $S = \{2106v + 2835k / k \in \mathbb{Z}\}$

6. Petit théorème de Fermat

Petit théorème de Fermat :

Soient p un nombre premier et a un entier naturel non nul.

- i. Pour tout $a \in \mathbb{N}$, $a^p \equiv a[p]$
- ii. Pour tout $a \in \mathbb{N}$, si $\text{PGCD}(a, p) = 1$ alors $a^{p-1} \equiv 1[p]$.

Remarques :

La démonstration de ce théorème, assez technique, est ici admise.

7. Numération de base a

7-1. Le système de base 10

Dans la base 10, on dispose de dix symboles, les dix chiffres 0, 1, 2, 3, 4, 5, 6, 7, 8, 9.

Tout nombre s'écrit dans le système de numération à l'aide de ces 10 chiffres.

Par exemple 48603 dans la base 10 peut être vu comme $4 \times 10^4 + 8 \times 10^3 + 6 \times 10^2 + 0 \times 10^1 + 3 \times 10^0$.

D'une manière générale, un entier naturel n s'écrivant en base 10 sous la forme $c_nc_{n-1}c_{n-2}\dots c_1c_0$ peut être vu comme $c_n \times 10^n + c_{n-1} \times 10^{n-1} + \dots + c_1 \times 10^1 + c_0 \times 10^0$. On a la définition suivante :

Définition 7 : Soit n un entier naturel non nul.

Il existe c_p, c_{p-1}, \dots, c_1 et c_0 tels que n se note sous la forme $n = c_pc_{p-1}\dots c_1c_0$ ou encore n s'écrit $n = c_p \times 10^p + c_{p-1} \times 10^{p-1} + \dots + c_1 \times 10^1 + c_0 \times 10^0$.

Pour dire que nous sommes dans la base 10, on peut aussi noter $n = \overline{c_pc_{p-1}\dots c_1c_0}^{10}$. Le système décimal est le système de numération usuelle.

7-2. Le système de base $a \geq 2$

En analogie avec le système décimal, pour écrire un entier n dans un système de numération de base $a \geq 2$, on aura besoin de a objets. Par exemple :

- Quand $a = 2$, on a besoin de deux chiffres. On choisit les symboles 0 et 1 : c'est le **système binaire**
- Quand $a = 3$, on a besoin de deux chiffres. On choisit les symboles 0, 1 et 3.
- Quand $a = 16$, on a besoin de seize (16) chiffres. On choisit les symboles 0, 1, 3, 3, 4, 5, 6, 7, 8, 9, A, B, C, D, E et F. C'est l'**hexadécimale**
- D'une manière générale, si $a > 10$, on utilise, en plus des 10 chiffres, des lettres pour compléter la base.

Si un entier naturel n s'écrit dans la base $a \geq 2$ sous la forme $c_pc_{p-1}\dots c_1c_0$ alors la valeur de n dans la base 10 est alors : $n = c_p \times a^p + c_{p-1} \times a^{p-1} + \dots + c_1 \times a^1 + c_0 \times a^0$.

On a alors la définition suivante :

Définition 8 : Soit n un entier naturel non nul et a un entier naturel supérieur ou égal à 2 donné.

Écrire n dans la base a revient à trouver les chiffres c_p, c_{p-1}, \dots, c_1 et c_0 se trouvant dans la base a tels que n s'écrit dans le système décimal sous la forme $n = c_p \times a^p + c_{p-1} \times a^{p-1} + \dots + c_1 \times a^1 + c_0 \times a^0$.

Dans ce cas, on dit que n s'écrit $c_pc_{p-1}\dots c_1c_0$ dans la base a .

Pour dire que nous sommes dans la base a , on peut aussi noter $n = \overline{c_pc_{p-1}\dots c_1c_0}^a$.

5. Théorème Chinois (en exercice)

Exercice 11

Théorème chinois :

Soient m et n deux entiers naturels non nuls. On note $\delta = m \wedge n$ et $\mu = m \vee n$.

1. Démontrer que pour tous entiers a et b , on a : $\begin{cases} a \equiv b[m] \\ a \equiv b[n] \end{cases} \Leftrightarrow a \equiv b[\mu]$

2. Soient α, β deux entiers. On se propose de résoudre le système : $\begin{cases} x \equiv \alpha[m] \\ x \equiv \beta[n] \end{cases}$ (2)

Démontrer que si $\alpha - \beta$ n'est pas multiple de δ , alors le système n'a pas de solution.

3. On suppose désormais que α et β sont multiples de δ et on désigne par α' et β' leurs quotients respectifs par δ .

a. Justifier l'existence d'un couple d'entiers (u, v) tels que : $mu + nv = \delta$.

b. Justifier que : $\begin{cases} mu \equiv 0[m] \\ mu \equiv \delta[n] \end{cases}$ et $\begin{cases} nv \equiv 0[m] \\ nv \equiv \delta[n] \end{cases}$

c. En déduire que $\beta'mu + \alpha'nv$ est une solution particulière de l'équation (2).

4. Résoudre l'équation (2).

5. Application : Résoudre le système suivant : $\begin{cases} x \equiv 0[105] \\ x \equiv 6[81] \end{cases}$

Solution :

1. – Soient a et b deux entiers relatifs et supposons que $\begin{cases} a \equiv b[m] \\ a \equiv b[n] \end{cases}$ alors $a - b$ est un multiple de m et n donc de leur PPCM. D'où $a \equiv b[\mu]$.

– Réciproquement, supposons que : $a \equiv b[\mu]$ alors $a - b$ est multiple de μ et μ est multiple de m et n donc, par transitivité, $a - b$ est multiple de m et n . D'où $\begin{cases} a \equiv b[m] \\ a \equiv b[n] \end{cases}$

2. Supposons par absurdité que (2) admet une solution qu'on note x mais que $\alpha - \beta$ n'est pas un multiple de δ .

Alors il existe k et k' tel que $\begin{cases} x = \alpha + km \\ x = \beta + k'n \end{cases}$ et par suite on déduit que $\alpha + km = \beta + k'n \Rightarrow \alpha - \beta = k'n - km$.

m et n étant des multiples de δ , alors $k'n - km$ l'est aussi et donc $\alpha - \beta$ est aussi un multiple de δ ce qui est absurde .

On conclut alors que si $\alpha - \beta$ n'est pas multiple de δ , alors le système (2) n'a pas de solution.

3-a. On sait que $\delta = m \wedge n$ alors il existe un couple (u, v) tel que $mu + nv = \delta$ (résultat du cours)

b. mu est multiple de m donc : $mu \equiv 0[m]$. D'après la question précédente, $mu - \delta$ est multiple de n , donc :

$\begin{cases} mu \equiv 0[m] \\ mu \equiv \delta[n] \end{cases}$. On établit de même que : $\begin{cases} nv \equiv \delta[m] \\ nv \equiv 0[n] \end{cases}$

c. Par produits par α' et par β' , on en déduit que : $\begin{cases} \beta'mu \equiv 0[m] \\ \beta'mu \equiv \beta[n] \end{cases}$ et $\begin{cases} \alpha'nv \equiv \alpha[m] \\ \alpha'nv \equiv 0[n] \end{cases}$

puis par sommes, il vient : $\begin{cases} \beta'mu + \alpha'nv \equiv \alpha[m] \\ \beta'mu + \alpha'nv \equiv \beta[n] \end{cases}$

Par suite $\beta'mu + \alpha'nv$ est une solution particulière de l'équation (2).

4. On déduit de 3-c. et de 1. que :

(2) $\Leftrightarrow \begin{cases} x \equiv \beta'mu + \alpha'nv[m] \\ x \equiv \beta'mu + \alpha'nv[n] \end{cases} \Leftrightarrow x \equiv \beta'mu + \alpha'nv[\mu]$

D'où il vient l'ensemble des solutions de (2) : $S = \{\beta'mu + \alpha'nv + k\mu/k \in \mathbb{Z}\}$

5. Application : $\begin{cases} x \equiv 0[105] \\ x \equiv 6[81] \end{cases}$

On a donc : $(m, n) = (105, 81)$; $(\delta, \mu) = (3, 2835)$; $(\alpha, \beta) = (0, 6)$; $(\alpha', \beta') = (0, 2)$.

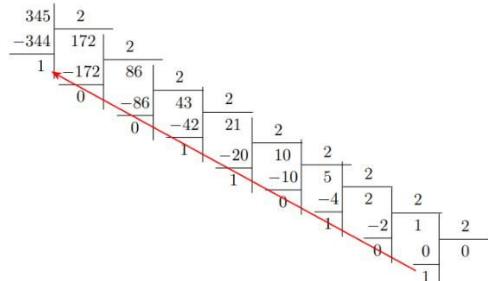
Quelques exemples de bases et de décomposition

a. La base 2 : les deux chiffres utilisés sont 0, 1.

Soit $n = 345$ écrit dans le système décimal (base 10). Cherchons l'écriture de n dans la base 2. Comme la **définition 8** nous l'indique, il faut chercher le c_p , c_{p-1}, \dots, c_1 et c_0 tels que : $n = c_p \times 2^p + c_{p-1} \times 2^{p-1} + \dots + c_1 \times 2^1 + c_0 \times 2^0$. Pour ce faire, on peut utiliser la méthode suivante :

On effectue les divisions successives des dividendes par la base a , comme dans l'exemple ci-contre. L'écriture dans la base a s'obtient en écrivant les restes du bas vers le haut (dans la direction de la flèche indiquée)

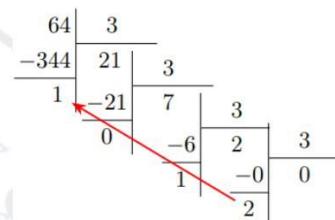
Ainsi n s'écrit dans la base 2 sous la forme $\overline{101011001}_2$



b. La base 3 : les deux chiffres utilisés sont 0, 1 et 2.

Soit $n = 64$ écrit dans le système décimal (base 10). Cherchons l'écriture de n dans la base 3.

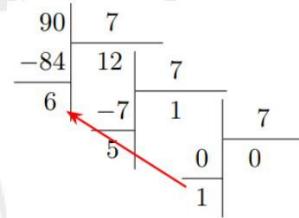
Ainsi l'écriture de $n = 64$ dans la base 3 est : $\overline{2101}_3$



c. La base 7

Soit $n = 90$ dans le système décimal. Écrivons ce nombre dans le système de numération de base 7.

Donc $n = 90$ s'écrit en base 7 sous la forme : $\overline{156}_7$

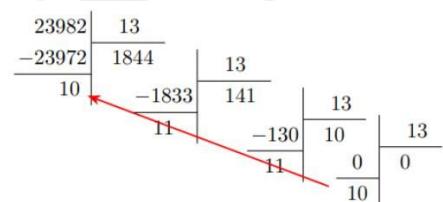


d. La base 13

Soit $n = 23982$ dans la base 10. Écrivons n dans le système de base 13.

Si la base est supérieure à 10, on utilise les lettres avec les correspondances $A = 10, B = 11, C = 12, \dots$ et ainsi de suite.

Alors n s'écrit en base 13 sous la forme de \overline{ABBA}^{13}



Exercice 12

1-a. Soient $n_1 = 124$, $n_2 = 11$ et $n = 227$ dans la base 10. Écrire ces nombres dans les bases 5 et 11.

b. Soit $n = \overline{21000220}^3$, $n_2 = \overline{27A3}^{11}$ et $n_3 = \overline{BAC}^{2021}$. Écrire ces nombres dans la base 9, 5 et 20.

2. Ecrire $n = 2199$ (écrit dans la base 10) respectivement dans les bases 11, 17 et 19.

3. Déterminer dans la base 10 les nombres suivants : $n_1 = \overline{101101}^2 + \overline{362}^7$ et $n_2 = \overline{A15CD}^{15} + \overline{2054}^7$.

4. Soient, dans le système décimal, les nombres $n_1 = 2009$, $n_2 = 2000$ et $n_3 = 2020$. Écrire ces nombres dans le système de numération de base 2, 8 et 15.

5. Soit, dans le système décimal, le nombre $n_1 = 44993556$. Écrire ce nombre dans le système de numération de base 2022.

- c. Donner alors les solutions du systèmes : $\begin{cases} \bar{3}x + \bar{2}y = \bar{1} \\ \bar{2}x + \bar{4}y = \bar{3} \end{cases}$
5. En utilisant la technique de la question précédente, résoudre dans $\mathbb{Z}/37\mathbb{Z}$ le système : $\begin{cases} \bar{3}x + \bar{7}y = \bar{3} \\ \bar{6}x - \bar{7}y = \bar{0} \end{cases}$

Exercice 5

On considère dans \mathbb{Z}^2 l'équation : $(E) : 35u - 96v = 1$.

1. Montrer que cette équation admet au moins une solution.

Montrer que le couple $(11; 4)$ est une solution particulière de (E) .

2. Déterminer l'ensemble solution de l'équation (E) .

On considère dans \mathbb{Z} l'équation $(F) : x^{35} \equiv 2[97]$

3. Soit x une solution de l'équation (F) .

a. Montrer que le nombre 97 est premier et que les nombres x et 97 sont premiers entre eux.

b. Montrer que : $x^{96} \equiv 1[97]$

c. Montrer que : $x \equiv 2^{11}[97]$

4. Montrer que si le nombre entier x vérifie la condition $x \equiv 2^{11}[97]$, alors x est solution de l'équation (F) .

5. Montrer que l'ensemble solution de l'équation (F) est l'ensemble des nombres entiers naturels de la forme $11 + 97k$ avec $k \in \mathbb{N}$

Problèmes

Problème 1

Partie A :

1. On considère dans \mathbb{Z} l'équation suivante d'inconnue x : $(E) : 3x^2 + 6x + 5 \equiv 0[7]$.

a. Montrer que l'équation (E) est équivalente à l'équation (E') où : $(E') : 3x(x+2) \equiv 2[7]$.

b. Recopier et compléter le tableau des congruences modulo 7 suivant :

x	0	1	2	3	4	5	6
$3x$							
$x + 2$							
$3x(x+2)$							

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

2. Moyennant la démarche précédente, résoudre dans \mathbb{Z} l'équation $(E_2) : x^2 - 4x + 3 \equiv 0[12]$.

3. Un entier naturel A s'écrit $\overline{361}^\beta$ dans le système de numération de base β et a pour reste 3 dans la division euclidienne par 7.

a. Démontrer que : $3\beta^2 + 6\beta - 2 \equiv 0[7]$.

b. En déduire l'ensemble des valeurs possibles de β .

4. Vérifier que 8 est une valeur possible de β .

Partie B

1. On se propose de résoudre dans $\mathbb{Z} \times \mathbb{Z}$ l'équation d'inconnue (x, y) suivante : $(F) : x^2 + 10x = y^2 + 46$.

a. Vérifier que l'équation (F) est équivalente à : $(x+5)^2 - y^2 = 71$.

b. Démontrer que 71 est premier.

c. Déterminer alors l'ensemble des solutions de (F) .

Exercices

Exercice 1

1. Montrer que pour tout entier naturel n , les entiers naturels n et $n + 1$ sont premiers entre eux.
2. Soit n un entier naturel. Démontrer que $n(n^4 - 1)$ est multiple de 5.
- 3- a. Soit n un entier naturel. Démontrer que le reste de la division euclidienne de n^2 par 8 est 0, 1 ou 4.
b. En déduire que les nombres de la forme : $8k + 7$, $k \in \mathbb{Z}$ ne sont pas la somme de trois carrés parfaits.
4. Déterminer les entiers relatifs n tels que $n + 2$ divise $3n + 1$.
5. Démontrer que, pour tout entier naturel n , $3^{2n+1} + 2^{4n+2}$ est divisible par 7.
6. Montrer que le produit de quatre entiers consécutifs, augmenté de 1, est un carré parfait.

Exercice 2

Le but de ce exercice est de trouver le chiffre des unités du nombre $n = 7^{7^{7^{7^7}}}$.

- 1- a. Pour tout entier naturel n , déterminer le reste de la division euclidienne de 7^n par 10.
b. En déduire le chiffre des unités de l'entier 7^{2022} .
- 2- a. Pour tout entier naturel n , déterminer le reste de la division euclidienne de 7^n par 4.
b. En déduire le reste de la division euclidienne de 7^{2024} par 4.
3. En utilisant les propriétés de la congruence, en déduire alors le chiffre des unités de l'entier : $n = 7^{7^{7^{7^7}}}$. Vérifier que ce nombre est impair.
4. En déduire de même le chiffre des unités de $n = 4^{4^{4^4}}$.
On considère l'ensemble des classes d'équivalence modulo 9 noté $\mathbb{Z}/9\mathbb{Z}$.
- 5- a. Pour tout entier naturel n , déterminer le reste de la division euclidienne de 7^n par 9.
b. En déduire le reste de la division euclidienne de 7^{2023} par 9.
6. Donner alors la classe de l'entier $n = 7^{7^{7^{7^7}}}$ dans $\mathbb{Z}/9\mathbb{Z}$.

Exercice 3

1. Résoudre dans \mathbb{N} , l'équation suivante : $3^n + 5n + 1 \equiv 0[8]$.
2. Montrer que : 4^n est congru à $1 + 3n$ modulo 9. En déduire que $2^{2n} + 15n - 1$ est toujours divisible par 9.
On se propose de déterminer l'ensemble de solution de l'équation (E) : $567x + 2854y = 5$.
- 3- a. Démontrer, en utilisant l'algorithme d'Euclide, que 567 et 2854 sont premiers entre eux .
b. Utiliser les calculs effectués à la question précédente pour déterminer deux entiers relatifs u et v tels que : $567u + 2854v = 5$.
c. En déduire l'ensemble de solution de cette équation.
4. Moyennant la question 3., déterminer les solutions dans \mathbb{Z} de l'équation (E_0) : $143x - 195y = 52$.

Exercice 4 : (Anneau $\mathbb{Z}/n\mathbb{Z}$)

- 1- a. Déterminer le $PGCD(49, 18)$ à l'aide de l'algorithme d'Euclide. En déduire le $PPCM(49, 18)$.
En déduire deux entiers relatifs u et v tels que $18u + 49v = 1$.
b. Moyennant la question précédente, Est-ce que $\bar{18}$ est inversible dans $\mathbb{Z}/49\mathbb{Z}$? Si oui, quel est son inverse ?
- 2- a. En raisonnant comme dans la question précédente, donner l'inverse de $\bar{7}$ dans $\mathbb{Z}/37\mathbb{Z}$.
b. Résoudre alors dans $\mathbb{Z}/37\mathbb{Z}$ l'équation : $\bar{7}y = \bar{2}$.
- 3- a. Préciser l'ensemble $\mathbb{Z}/4\mathbb{Z}$.
b. Moyennant la question 3-a., montrer que l'équation : $\bar{2}x = \bar{3}$ n'admet pas de solutions dans $\mathbb{Z}/4\mathbb{Z}$.
c. En utilisant 3-a., résoudre dans $\mathbb{Z}/4\mathbb{Z}$ les équations (E_1) : $x^2 + \bar{3}x = \bar{0}$ et (E_2) : $\bar{2013}x^3 + \bar{2}x = \bar{k}$.
- 4- a. En précisant l'ensemble $\mathbb{Z}/5\mathbb{Z}$, donner les solutions de l'équation $\bar{3}x + \bar{2}y = \bar{1}$ dans $\mathbb{Z}/5\mathbb{Z}$. (on pourra s'aider du tableau de congruence modulo 5 à double entrées)
b. En déduire de même la résolution dans $\mathbb{Z}/5\mathbb{Z}$ de l'équation : $\bar{2}x + \bar{4}y = \bar{3}$.

2. On considère à présent l'équation (G) : $13x + 7y = 16$. On cherche à résoudre (E) dans \mathbb{Z} .
- Déterminer le $PPCM(13, 7)$ et le $PGCD(13, 7)$. En déduire que (G) admet au moins une solution.
 - Vérifier que le couple $(5, -7)$ est une solution de l'équation (G) .
 - Déterminer alors les couples (x, y) d'entiers relatifs vérifiant (G) .

Problème 2

On rappelle ici le petit théorème de Fermat : Pour tout nombre premier p et pour tout entier naturel non nul a , si $a \wedge p = 1$ alors $a^{p-1} \equiv 1[p]$.

On souhaite déterminer les couples de (x, y) de $\mathbb{N}^* \times \mathbb{N}^*$ vérifiant l'équation (E_0) : $px + y^{p-1} = 2017$ avec p un nombre premier supérieur ou égal à 5.

I- Préliminaire

Soit a un élément de \mathbb{N}^* .

- Montrer que si a et 13 sont premiers entre eux alors : $a^{2016} \equiv 1[13]$.
On considère dans \mathbb{N}^* l'équation (E_1) : $x^{2015} \equiv 2[13]$.
 - Montrer que x et 13 sont premiers entre eux.
 - Montrer que : $x \equiv 7[13]$
 - En déduire les solutions de (E_1) .
- Montrer que 2017 est un nombre premier et donner la décomposition primaire de 2016.

II- Résolution de (E_0)

- Vérifier que $p < 2017$ et montrer que p ne divise pas y .
- Montrer que : $y^{p-1} \equiv 1[p]$ puis en déduire que p divise 2016.
- En déduire alors que $p = 7$.
- Résoudre alors l'équation (E_0) .

Problème 3

Les trois parties sont totalement indépendantes.

Partie A

- On considère l'équation (E) : $25x - 49y = 5$, où x et y sont des entiers relatifs.
 - Déterminer le $PGCD$ de 25 et 49 à l'aide de l'algorithme d'Euclide . Déduire alors le $PPCM$ de 25 et 49 à partir de leur $PGCD$.
 - Montrer que l'équation (E) admet au moins une solution. Déterminer une solution de (E) .
 - Résoudre l'équation (E) .
 - Montrer qu'il existe un unique entier p compris entre 1960 et 2018 tel que : $25p \equiv 5[49]$.
- Justifier que si (x, y) est solution de (E) alors $5x \equiv 1[7]$ et $y \equiv 0[5]$.
 - Montrer que $5x \equiv 1[7]$ si et seulement si $x \equiv 3[7]$.
- Soit x un entier relatif. Quels sont les restes possibles de x^2 dans la division euclidienne par 7.
 - Existe-t-il un couple (x, y) d'entiers relatifs tels que (x^2, y^2) soit solution de (E) ?

Partie B

Dans cette partie, on pourra utiliser le résultat suivant :

« Étant donnés deux entiers naturels a et b non nuls, si $PGCD(a, b) = 1$ alors $PGCD(a^2, b^2) = 1$ ».

On considère la suite (S_n) est définie pour $n > 0$ par : $S_n = \sum_{k=1}^n k^3$. On se propose de calculer, pour tout entier naturel non nul n , le plus grand commun diviseur de S_n et S_{n+1} .

- 3.** On se propose de démontrer que si p n'est pas premier, alors N_p n'est pas premier.

On rappelle que pour tout nombre réel x et tout entier naturel n non nul,

$$x^n - 1 = (x - 1)(x^{n-1} + x^{n-2} + \cdots + x + 1)$$

- On suppose que p est pair et on pose $p = 2q$, où q est un entier naturel plus grand que 1. Montrer que N_p est divisible par $N_2 = 11$.
- On suppose que p est multiple de 3 et on pose $p = 3q$, où q est un entier naturel plus grand que 1. Montrer que N_p est divisible par $N_3 = 111$.
- On suppose p non premier et on pose $p = kq$ où k et q sont des entiers naturels plus grands que 1. En déduire que N_p est divisible par N_k .

- 4.** Énoncer une condition nécessaire pour que N_p soit premier. Cette condition est-elle suffisante ?

Problème 5

Partie A

- a. Vérifier que : 503 est entier premier.
b. Montrer que $7^{502} \equiv 1[503]$. En déduire que $7^{2008} \equiv 1[503]$.
- Soit dans \mathbb{Z}^2 , l'équation $(E) : 49x - 6y = 1$.
 - A l'aide de l'algorithme d'Euclide, déterminer le PGCD de 49 et 6. Déterminer ainsi le PPCM de 49 et 6 en utilisant leur PGCD. Justifier que l'équation (E) admet au moins une solution.
 - sachant que le couple $(8; 1)$ est une solution particulière de l'équation (E) , résoudre dans \mathbb{Z}^2 (E) .
- On pose $N = 1 + 7 + 7^2 + \cdots + 7^{2007}$.
 - Montrer que le couple $(7^{2006}, N)$ est solution de l'équation (E) .
 - Montrer que : $N \equiv 0[4]$ et $N \equiv 0[503]$
 - En déduire que N est divisible par 2012.

Partie B

On considère dans \mathbb{Z}^2 , l'équation $(E) : 143x - 195y = 52$.

- a. Déterminer le PGCD de 143 et 195 , en déduire que l'équation (E) admet au moins une solution dans \mathbb{Z}^2 .
b. Déterminer une solution particulière de (E) . Déterminer alors la solution générale de (E) dans \mathbb{Z}^2 .
- Soit n un entier naturel non nul et premier avec 5 , montrer que $\forall k \in \mathbb{N}$, $n^{4k} \equiv 1[5]$.
- Soient x et y deux nombres entiers non nuls tels que $x \equiv y[4]$.
 - Montrer que : $\forall n \in \mathbb{N}^* ; n^x \equiv n^y[5]$.
 - En déduire que : $\forall n \in \mathbb{N}^* ; n^x \equiv n^y[10]$.
- Soient x et y deux entiers naturels non nuls tels que le couple (x, y) soit solution de l'équation (E) .
Montrer que quel que soit n de \mathbb{N}^* : les nombres n^x et n^y ont le même chiffre des unités dans le système de numération décimal.

1. Démontrer que, pour tout $n > 0$, on a : $S_n = \left(\frac{n(n+1)}{2}\right)^2$.
2. Étude du cas où n est pair. Soit k l'entier naturel non nul tel que $n = 2k$.
 - a. Démontrer que $\text{PGCD}(S_{2k}, S_{2k+1}) = (2k+1)^2 \text{PGCD}(k^2, (k+1)^2)$.
 - b. Calculer $\text{PGCD}(k, k+1)$.
 - c. Calculer $\text{PGCD}(S_{2k}, S_{2k+1})$.
3. Étude du cas où n est impair. Soit k l'entier naturel non nul tel que $n = 2k+1$.
 - a. Démontrer que les entiers $2k+1$ et $2k+3$ sont premiers entre eux.
 - b. Calculer $\text{PGCD}(S_{2k+1}, S_{2k+2})$.
4. Déduire des questions précédentes qu'il existe une unique valeur de n , que l'on déterminera, pour laquelle S_n et S_{n+1} sont premiers entre eux.

Partie C

Soit dans \mathbb{Z} le système (S) suivant : $\begin{cases} x \equiv a[p] \\ x \equiv b[q] \end{cases}$ où a, b, p et q des entiers relatifs tels que $p \wedge q = 1$.

- 1- a. Montrer qu'il existe un couple de (u_0, v_0) de \mathbb{Z}^2 vérifiant : $pu_0 + qv_0 = 1$.
b. Montrer que $x_0 = bpu_0 + aqv_0$ est une solution du système (S).
2. Soit x une solution du système (S), montrer que le nombre pq divise le nombre $x - x_0$.
3. Soit x un entier relatif tel que pq divise le nombre $x - x_0$, montrer que x est solution du système (S).
4. En déduire l'ensemble solution du système (S).
5. Résoudre dans le système : $\begin{cases} x \equiv 1[8] \\ x \equiv 3[13] \end{cases}$

Problème 4

On se propose dans ce problème d'étudier le problème (P) suivant :

« Les nombres dont l'écriture décimale n'utilise que le seul chiffre 1 peuvent-ils être premiers ? »

On rappelle dès lors que : $N_p = 10^{p-1} + 10^{p-2} + \dots + 10^0$.

Partie I : Quelques résultats dans la base 10

On désigne x un entier naturel non nul et $\overline{a_n a_{n-1} \dots a_0}$ avec $a_n \neq 0$ son écriture décimale.

On a : $x = a_n 10^n + a_{n-1} 10^{n-1} + \dots + a_0$.

1. Vérifier que : $\forall p \in \mathbb{N}^*$, $10^p \equiv 0[5]$. En déduire que : $x \equiv a_0[5]$.
2. Montrer que : $\forall p \in \mathbb{N} \setminus \{0, 1\}$, $10^p \equiv 0[4]$. Conclure que $x \equiv \overline{a_1 a_0}[4]$.
3. Montrer que : $\forall p \in \mathbb{N}$, $10^p \equiv 1[9]$. Conclure que $x \equiv \sum_{p=0}^n a_p[9]$.
Soit x un nombre entier naturel tel que : $10^x \equiv 2[19]$
- 4- a. Vérifier que : $10^{x+1} \equiv 1[19]$. En déduire que 10^{x+1} et 19 sont premiers entre eux.
b. Montrer que $10^{18} \equiv 1[19]$. (On pourra utiliser le petit théorème de Fermat)
En déduire que 10^{18} et 19 sont premiers entre eux.
5. Soit d un diviseur commun de $x+1$ et 18.
 - a. Montrer que $10^d \equiv 1[19]$. Que dire des nombres 10^d et 19 ?
 - b. Montrer que $d = 18$. (On pourra considérer l'ensemble des diviseurs de 18)
 - c. En déduire que : $x \equiv 17[18]$.

Partie II : Retour au problème (P)

1. Les nombres $N_2 = 11$, $N_3 = 111$ et $N_4 = 1111$ sont-ils premiers ?
2. Prouver que $N_p = \frac{10^p - 1}{9}$. Peut-on être certain que $10^p - 1$ est divisible par 9 ?