

Appui aux olympiades et compétitions de Mathématiques

Séminaire de formation des professeurs du 04 au 11 janvier 2023

ARITHMETIQUE

Horma Hamoud

Mahfoudh Mohamed Ammou

Table des matières

0) Introduction.....	Erreur ! Signet non défini.
1) Divisibilité dans \mathbb{Z}	5
Définition.....	5
Remarques.....	5
Propriétés.....	5
Exercice 1.....	6
Critères de divisibilité	6
Exercice 2.....	6
2) Division euclidienne dans \mathbb{N} et dans \mathbb{Z}	7
Division euclidienne dans \mathbb{N} :	7
Théorème 1	7
Exercice 3.....	7
Remarque	7
Division euclidienne dans \mathbb{Z}	7
Théorème	7
Remarque	7
Exercice 4.....	8
3) Congruences.	8
Définition1.....	8
Définition 2.....	8
Propriétés.....	8
Exercice 5.....	9
4) Nombres premiers.....	9
Définition 1.....	9
Définition 2.....	10
Remarques.....	10
Propriétés.....	10
Critère de primalité	10
Exercice 6.....	Erreur ! Signet non défini.
Crible d'Ératosthène :	11
Remarque	11
Record des nombres premiers connus.....	12
Décomposition en nombres premiers.....	12
Théorème	12
Corollaire	12
Propriétés.....	13
Exercice 7.....	13
5) PGCD	15
Définition.....	15
Remarque	15
Exercice 8.....	Erreur ! Signet non défini.
Remarque	15
Algorithme d'Euclide :	15
Exercice 9.....	16
Exercice 10.....	16
Remarque	16
Théorème	17
Propriétés.....	17
Exercice 11.....	17
Théorème	18

Théorème (de Bézout).....	18
Remarque	18
Théorème	18
Corollaire	18
Théorème (de Gauss)	18
Corollaire	18
Conséquences.....	18
Théorème (Petit théorème de Fermat).....	19
Corollaire	19
Exercice 12.....	19
6) PPCM.....	19
Définition	19
Propriétés	20
7) Equations diophantiennes	20
Théorème	20
Méthode de résolution.....	20
Exercice 13.....	20
8) Systèmes de numération	21
Système de numération décimal (ou « en base 10 ») :.....	21
Système binaire (ou « en base 2 ») :	22
Conversion décimal-binaire.....	22
Exercice 14.....	23
Système octal (ou « en base 8 ») :.....	23
Système hexadécimal (ou « en base 16 ») :	23
Exercice 15.....	24
Remarque	24
Exercice 16.....	24
Exercice 17.....	25
Généralisation	25
Propriété et définition :	25
Exercice 18.....	26
Exercice 19.....	26
Exercice 20.....	27
9) Enoncés des exercices corrigés.....	28
Exercice 21.....	28
Exercice 22.....	28
Exercice 23.....	28
Exercice 24.....	28
Exercice 25.....	31
Exercice 26.....	28
Exercice 27.....	29
Exercice 28.....	29
Exercice 29.....	29
Exercice 30.....	29
Exercice 31.....	30
Exercice 32.....	30
10) Corrigés des exercices.....	32
Corrigé 21	32
Corrigé 22	32
Corrigé 23	32
Corrigé 24	33
Corrigé 25	49

Corrigé 26	35
Corrigé 27	35
Corrigé 28	38
Corrigé 29	39
Corrigé 30	40
Corrigé 31	44
Corrigé 32	46

ARITHMETIQUE

Ce module de formation a pour objectif d'initier les professeurs de mathématiques de l'enseignement secondaire aux concepts de base en arithmétique en vue de préparer leurs élèves pour résoudre les exercices d'arithmétique de type olympique. Ce document présente les connaissances de base de l'arithmétique à savoir la divisibilité ; la congruence ; les nombres premiers ; les équations diophantiennes ainsi que les systèmes de numération.

1) Divisibilité dans \mathbb{Z}

Définition

Soient a et b deux entiers relatifs ($b \neq 0$), on dit que b divise a s'il existe un entier relatif k tel que $a = kb$. On note: $b \mid a$

Remarques

On dit aussi que a est un multiple de b ou que b est un diviseur de a .

1 et -1 divisent tous les nombres.

Un nombre $a \neq 0$ admet au minimum 4 diviseurs : $\{1 ; -1 ; a ; -a\}$.

Propriétés

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

$$(a \mid b \text{ et } b \mid a) \Leftrightarrow (a = b \text{ ou } a = -b)$$

$$(a \mid b \text{ et } b \mid c) \Rightarrow a \mid c \text{ (transitivité)}$$

$$(c \mid a \text{ et } c \mid b) \Rightarrow c \mid (ua + vb) ; u, v \in \mathbb{Z} \text{ (divisibilité par combinaison linéaire)}$$

$$a \mid b \Rightarrow -a \mid b$$

$$a \mid b \Rightarrow |a| \leq |b| ; b \neq 0$$

$$a \mid b \Rightarrow a \mid bc \text{ pour tout entier } c$$

$$a \mid b \Rightarrow ac \mid bc \text{ pour tout entier } c \text{ non nul.}$$

$$(a - b) \mid (a^n - b^n) ; n \in \mathbb{N}^*$$

$$\text{Si } n \text{ est impair alors } (a + b) \mid (a^n + b^n) ; n \in \mathbb{N}^*$$

Exercice 1

Montrer que le nombre $(5^{2023} - 1)$ est divisible par 4 ;

et le nombre $(5^{2023} + 1)$ est divisible par 6.

Solution

On utilise les propriétés 8 et 9.

Critères de divisibilité

Soit n un entier naturel

n	Critères de divisibilité par n (en écriture décimale)
10	Le chiffre des unités est 0.
2	Le chiffre des unités est paire :0, 2, 4, 6, 8.
5	Le chiffre des unités est 0 ou 5.
4	Le nombre formé par les deux derniers chiffres est divisible par 4
25	Le nombre formé par les deux derniers chiffres est divisible par 25.
8	Le nombre formé par les trois derniers chiffres est divisible par 8.
125	Le nombre formé par les trois derniers chiffres est divisible par 125.
3	La somme des chiffres qui le composent est divisible par 3.
9	La somme des chiffres qui le composent est divisible par 9.
11	La différence de la somme des chiffres de rang impair et de la somme des chiffres de rangs pair (en partant de la droite) est divisible par 11.
7	Le nombre de dizaines diminué du double du chiffre des unités est divisible par 7. Soustraction alternée des tranches de trois chiffres divisible par 7.
13	Le nombre de dizaines augmenté de 4 fois le chiffre des unités est divisible par 13. Soustraction alternée des tranches de trois chiffres divisible par 13.

Exercice 2

Appliquer les critères précédents pour tester la divisibilité de $A=25688865410$ par chacun des nombres 2 ,3 ,4,5,6,7,8 ,9,10,11,12,13,15,20,30 ;40,50,60 ;70,80 ;90.

Solution

A est divisible par 2, 5, 10, 13. A n'est pas divisible par 3, donc il en est de même pour 6, 9, 12, 15, 30, 60 et 90. A n'est pas divisible par 4, donc il en est de même pour 8, 12, 20, 40, 60, 80. A n'est pas divisible par 7, donc il en est de même pour 70. A n'est pas divisible par 25, donc il en est de même pour 50.

En effet A s'écrit $A = 2 \times 5 \times 13 \times 17 \times 11623921$ comme produit de facteurs premiers

2) Division euclidienne dans \mathbb{N} et dans \mathbb{Z} .

Division euclidienne dans \mathbb{N} :

Théorème 1

Soient a et b deux entiers naturels, avec $b \neq 0$. Il existe un unique couple $(q; r)$ d'entiers naturels tels que $a = bq + r$ avec $0 \leq r < b$.

a	b	q	r
dividende	diviseur	quotient	reste, $r \in \mathbb{N}$, $(r = 0 \Rightarrow b \mid a)$

Exercice 3

Effectuer la division euclidienne de 2022 par 7.

Solution

$2022 = 7 \times 288 + 6$ est la division euclidienne de 2022 par 7 mais par 288 aussi

Remarque

Si le reste est nul ($r = 0$), on dit que b divise a et on notera : $b \mid a$.

Division euclidienne dans \mathbb{Z}

Théorème

Pour deux entiers relatifs a et b avec $b \neq 0$, il existe un unique couple $(q; r)$ avec $q \in \mathbb{Z}, r \in \mathbb{N}$ tel que : $a = bq + r$ avec $0 \leq r < |b|$.

Remarque

Le reste est toujours positif.

Exercice 4

Effectuer les divisions euclidiennes de -2023 par 8 et de 2023 par -8 .

Solution

$-2023 = 8 \times (-253) + 1$ est la division euclidienne de -2023 par 8 .

$2023 = -8 \times (-252) + 7$ est la division euclidienne de 2023 par -8 .

3) Congruences.

Soient a et b deux entiers relatifs et n un entier naturel supérieur ou égal à 2 .

Définition 1

On dit que a et b sont congrus modulo n si et seulement si $a - b$ est divisible par n .

Définition 2

Les entiers a et b sont congrus modulo n si et seulement s'ils ont le même reste dans la division euclidienne par n .

Notation : On note $a \equiv b [n]$ ou $a \equiv b [\text{mod } n]$.

Exemples

$a = 25$ et $b = 7$ on a $a - b = 18$. On peut dire que : $a \equiv b [18]$; $a \equiv b [9]$; $a \equiv b [6]$
 $a \equiv b [3]$; $a \equiv b [2]$ car $a - b$ est divisible par chacun des nombres $18, 9, 6, 3$ et 2 .

Propriétés

Soient a, b, c, a' et b' des entiers relatifs, et n un entier naturel non nul.

$a \equiv b (n) \Leftrightarrow b \equiv a (n)$ $a \equiv b (n) \Leftrightarrow a - b \equiv 0 (n)$ $a \equiv b (n) \Leftrightarrow n \mid (a - b)$ $n \mid a \Leftrightarrow a \equiv 0 (n)$ $n \equiv 0 (n)$ $a \equiv a (n)$	$\left \begin{array}{l} a \equiv b (n) \\ b \equiv c (n) \end{array} \right. \Rightarrow a \equiv c (n)$ $\left \begin{array}{l} a \equiv b (n) \\ a' \equiv b' (n) \end{array} \right. \Rightarrow a + a' \equiv b + b' (n)$ $\left \begin{array}{l} a \equiv b (n) \\ a' \equiv b' (n) \end{array} \right. \Rightarrow a - a' \equiv b - b' (n)$	$\left \begin{array}{l} a \equiv b (n) \\ a' \equiv b' (n) \end{array} \right. \Rightarrow aa' \equiv bb' (n)$ $a \equiv b (n) \Rightarrow a^p \equiv b^p (n)$ pour tout p de \mathbb{N} , $a \equiv b (n) \Rightarrow ac \equiv bc (n)$ Si $a \times c \equiv b \times c [n]$ et si c est premier avec n , alors $a \equiv b [n]$
--	---	---

Exercice 5

Calculer le reste de la division euclidienne de 12^{2023} par 5.

Solution

$$12 \equiv 2[5]$$

$$\begin{cases} 2^0 \equiv 1[5] \\ 2^1 \equiv 2[5] \\ 2^2 \equiv 4[5] \\ 2^3 \equiv 3[5] \\ 2^4 \equiv 1[5] \end{cases}$$

Alors

$$2^{2020} \equiv 1[5] \text{ et } 2^3 \times 2^{2020} \equiv 3 \times 1[5] \text{ d'où } 2^{2023} \equiv 3[5] \text{ et } 12^{2023} \equiv 3[5].$$

Exercice 6

Trouver tous les entiers x tels que 7 divise $x^2 + x + 1$.

Solution

La condition équivaut $x^2 + x + 1 \equiv 0[7]$.

Reste de la division de x par 7	0	1	2	3	4	5	6
Reste de la division de x^2 par 7	0	1	4	2	2	4	1
Reste de la division de $x^2 + x + 1$ par 7	1	3	0	6	0	3	1

Il est clair que les seules solutions sont les entiers congrus à 2 ou 4 modulo 7.

4) Nombres premiers

Définition 1

Un entier naturel p est dit « premier » s'il admet exactement deux diviseurs dans \mathbb{N} : 1 et p lui-même.

Exemples et contre-exemples :

1) 0 n'est pas premier car il a une infinité de diviseurs.

2) 1 n'est pas premier car il n'a qu'un seul diviseur dans \mathbb{N} : 1 lui-même.

3) 2 est le premier nombre premier, et le plus petit. C'est le seul entier naturel premier qui soit pair.

4) Les nombres 3; 5; 7; 11; 13; 17; 19; ... sont premiers.

Définition 2

Deux entiers naturels a et b sont dits « premiers entre eux » s'ils n'ont en commun que 1 comme diviseur positif.

Exemples

9 et 14 sont premiers entre eux .

22, 27 et 35 sont premiers entre eux.

Remarques

1) Ne pas confondre « premier » avec « premiers entre eux »

2) Si p est un nombre premier et $n \in \mathbb{N}$, alors ou $p \mid n$ ou p est premier avec n .

3) Un entier naturel $n \geq 2$, non premier, est dit « composé ».

Propriétés

Soit $n \in \mathbb{N}$, $n \geq 2$

1) n admet au moins un diviseur premier.

2) Si n n'est pas premier, il admet au moins un diviseur premier p tel que $p \leq \sqrt{n}$.

3) Si un nombre premier divise un produit alors il divise au moins l'un des facteurs de ce produit.

Critère de primalité

Si un entier naturel $n \geq 2$ n'est divisible par aucun nombre premier inférieur ou égal à \sqrt{n} , alors n est premier.

Exemple :

Pour tester la primalité de 103, on a $\sqrt{103} \approx 10$.

Le nombre 103 n'est divisible par aucun nombre premier inférieur ou égal à $\sqrt{103} \approx 10$ (les nombres 2, 3, 5 et 7). Alors il est premier.

Crible d'Ératosthène :

Le test de primalité permet de concevoir le crible d'Ératosthène, qui donne la liste de tous les nombres premiers compris entre 1 et un nombre entier donné :

1	2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50
51	52	53	54	55	56	57	58	59	60
61	62	63	64	65	66	67	68	69	70
71	72	73	74	75	76	77	78	79	80
81	82	83	84	85	86	87	88	89	90
91	92	93	94	95	96	97	98	99	100

On vérifie les règles suivantes :

- 1) Pour obtenir tous les nombres premiers entre 1 et 100, on prend le premier nombre premier, c'est-à-dire 2, on barre tous les multiples de 2, le premier nombre suivant non barré est premier puis on barre tous les multiples de celui-ci, et ainsi de suite. . .
- 2) Quand on arrive à un nombre premier p , le premier nombre suivant non premier à barrer doit être supérieur à p^2 .
- 3) Quand on aura barré tous les multiples des nombres premiers inférieurs strictement à 11 (car $\sqrt{100} < 11$), les nombres non barrés sont tous des nombres premiers entre 1 et 100.

$\{2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97\}$.

Remarque

Deux nombres premiers sont dits jumeaux lorsque leur différence est 2 .

Exemples : $(3, 5); (5, 7); (11, 13) \dots$ Sont-ils en nombre fini (conjecture)?

Théorème d'Euclide

Il existe une infinité de nombres premiers.

Record des nombres premiers connus

Les derniers plus grands nombres premiers connus sont :

$M = 2^{57885151} - 1$, trouvé en janvier 2013 avec 17325421 chiffres en écriture décimale,

$M = 2^{74207281} - 1$, trouvé en janvier 2016 avec 22338618 chiffres en écriture décimale,

$M = 2^{82598933} - 1$, trouvé en décembre 2018 avec 24862048 chiffres en écriture décimale.

Ceux sont des nombres de Mersenne (nombres de la forme $M_n = 2^n - 1$).

En septembre 2016, le couple record $(p, p+2)$ des nombres premiers jumeaux est

$2996863034895 \times 2^{1290000} \pm 1$. Ces deux nombres possèdent 388 342 chiffres.

Décomposition en nombres premiers

Théorème (théorème fondamental de l'arithmétique)

Tout entier naturel $n > 1$ s'écrit de façon unique sous la forme d'un produit de facteurs :

$$n = p_1^{\alpha_1} \times p_2^{\alpha_2} \times p_3^{\alpha_3} \times \dots \times p_r^{\alpha_r}$$

où $p_1, p_2, p_3, \dots, p_r$ sont des nombres premiers et $\alpha_1, \alpha_2, \alpha_3, \dots, \alpha_r$ des entiers naturels.

On note $n = \prod_{k=1}^r p_k^{\alpha_k}$.

Cette décomposition est unique, à l'ordre des facteurs près.

Corollaire

Un entier naturel d divise un entier naturel n si et seulement si les nombres premiers de la décomposition en facteurs premiers de d figurent dans celle de n avec des exposants inférieurs ou égaux à ceux de la décomposition de n .

Exemple

$n = 2^3 \times 5^2 \times 11^3 \times 19$. $a = 2^2 \times 5 \times 11^2$ divise n .

Tandis que $b = 2^5 \times 5 \times 11^2$ et $c = 2^2 \times 7 \times 11^2$ ne divisent pas n .

Propriétés

Soit n un entier naturel non nul, tel que $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$ où pour tout $i \in [1, k]$, p_i est un entier naturel premier et α_i un entier naturel non nul.

1) Le nombre de diviseurs de n est donné par la formule:

$$N = (\alpha_1 + 1)(\alpha_2 + 1) \times \dots \times (\alpha_k + 1).$$

2) La somme de ces diviseurs est donnée par la formule:

$$S = (1 + p_1 + p_1^2 + \dots + p_1^{\alpha_1})(1 + p_2 + p_2^2 + \dots + p_2^{\alpha_2}) \dots (1 + p_k + p_k^2 + \dots + p_k^{\alpha_k})$$

ou encore

$$S = \frac{p_1^{\alpha_1+1} - 1}{p_1 - 1} \times \frac{p_2^{\alpha_2+1} - 1}{p_2 - 1} \times \dots \times \frac{p_k^{\alpha_k+1} - 1}{p_k - 1}.$$

3) Le produit de ces diviseurs est : $P = \sqrt{n^N}$.

Exercice 7

1) Décomposer le nombre $n = 180$ en facteurs premiers.

2) Déterminer le nombre de diviseurs et la somme des diviseurs de n .

Solution

1) On procède à des divisions successives de n par les nombres premiers en ordre croissant jusqu'à l'obtention d'un quotient égal à 1.

180	2
90	2
45	3
15	3
5	5
1	

On trouve: $n = 2^2 \times 3^2 \times 5^1$

2) Le nombre de diviseurs de n est : $(2+1)(2+1)(1+1) = 18$.

La somme de ces diviseurs est : $S = \frac{2^3-1}{2-1} \times \frac{3^3-1}{3-1} \times \frac{5^3-1}{5-1} = 2821$.

Valuation p-adique

Si p est un nombre premier, et n un entier non nul, la valuation p -adique de n est le plus grand entier k tel que p^k divise n . On la note $v_p(n)$. Si $n = 0$, on convient que $v_p(0) = +\infty$ pour tout nombre premier p .

Exemple

Calculer $v_2(360)$, $v_3(360)$, $v_5(360)$.

Solution

On a $360 = 2^3 \times 3^2 \times 5^1$. Donc $v_2(360) = 3$; $v_3(360) = 2$ et $v_5(360) = 1$.

Formule de Legendre

Si p est un nombre premier et n est un entier positif, on a :

$$v_p(n!) = \sum_{i=1}^{\infty} \left[\frac{n}{p^i} \right] = \left[\frac{n}{p} \right] + \left[\frac{n}{p^2} \right] + \left[\frac{n}{p^3} \right] + \dots$$

A noter que si $p^i > n$; $\left[\frac{n}{p^i} \right] = 0$.

Exercice 8

Par combien de zéros se termine le nombre $1000!$?

Solution

L'entier 10 n'est pas premier : on ne peut donc pas appliquer directement la formule de Legendre. Le plus grand exposant n tel que 10^n divise $1000!$ est le plus petit des deux nombres $v_2(1000!)$ et $v_5(1000!)$. La formule de Legendre prouve directement que c'est $v_5(1000!)$

$$v_5(1000!) = \sum_{i=1}^{\infty} \left[\frac{1000}{5^i} \right] = \left[\frac{1000}{5} \right] + \left[\frac{1000}{5^2} \right] + \left[\frac{1000}{5^3} \right] + \left[\frac{1000}{5^4} \right]$$

$$v_5(1000!) = 200 + 40 + 8 + 1 = 249$$

Le nombre $1000!$ se termine donc par 249 zéros.

5) PGCD

Définition

Soient a et b deux entiers naturels non nuls. Le plus grand élément des diviseurs communs de a et b est appelé Plus Grand Commun Diviseur de a et b et se note $\text{PGCD}(a;b)$ ou $a \wedge b$.

Cette définition s'applique aussi au cas où a et b sont des entiers relatifs non nuls : $\text{PGCD}(a;b) = \text{PGCD}(|a|;|b|)$. On se limitera aux entiers naturels.

Remarque

Notons $D(a)$ l'ensemble des diviseurs d'un entier a . L'ensemble des diviseurs communs à a et b n'est pas vide : il contient au moins 1.

Exemple

Trouver le PGCD de 42 et de 36.

Solution

$D(42) = \{1 ; 2 ; 3 ; 6 ; 7 ; 14 ; 21 ; 42\}$ et $D(36) = \{1 ; 2 ; 3 ; 4 ; 6 ; 9 ; 12 ; 18 ; 36\}$.

L'ensemble des diviseurs communs à 42 et 36 est $D(42) \cap D(36) = \{1;2;3;6\}$.

Donc $\text{PGCD}(42;36) = 42 \wedge 36 = 6$.

En d'autres termes :

$42 = 2^1 \times 3^1 \times 7^1$ et $36 = 2^2 \times 3^2$ implique que $\text{PGCD}(42;36) = 2^1 \times 3^1 = 6$

Remarque

Tous les diviseurs communs de a et b divisent leur PGCD. On peut de manière générale démontrer que $D(a) \cap D(b) = D(\text{PGCD}(a;b))$

Algorithme d'Euclide :

a et b étant deux entiers naturels non nuls tels que $a > b$ et $a = qb + r$ avec $0 \leq r < b$. Si $r = 0$ alors $\text{PGCD}(a;b) = b$, sinon $\text{PGCD}(a;b) = \text{PGCD}(b;r)$.

La réitération de cette propriété lors de la recherche du PGCD de deux nombres s'appelle l'Algorithme d'Euclide.

La réitération est forcément finie car on construit une suite décroissante d'entiers naturels.

Exemple

$$42 = 36 \times 1 + 6$$

$$36 = 6 \times 6 + 0$$

Exercice 9

Calculer le PGCD de 42 et de 150 par l'algorithme d'Euclide.

Solution

$$150 = 42 \times 3 + 24$$

$$42 = 24 \times 1 + 18$$

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

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

Le PGCD est le dernier reste non nul, c'est-à-dire 6.

Nous avons donc $\text{PGCD}(150; 42) = \text{PGCD}(42; 24) = \text{PGCD}(24; 18) = \text{PGCD}(18; 6) = 6$.

Exercice 10

En utilisant l'exercice précédent, exprimer 6 comme combinaison linéaire de 150 et 42.

Solution

On remonte l'algorithme d'Euclide

$$\begin{aligned} 6 &= 24 - 1 \times 18 \\ &= 24 - 1 \times (42 - 1 \times 24) \\ &= 24 - 1 \times 42 + 1 \times 24 \\ &= -1 \times 42 + 2 \times 24 \\ &= -1 \times 42 + 2 \times (150 - 3 \times 42) \\ &= -1 \times 42 + 2 \times 150 - 6 \times 42 \\ &= 2 \times 150 - 7 \times 42 \end{aligned}$$

A chaque fois qu'on remplace un reste, on consacre une ou deux lignes pour le regroupement avant de remplacer le reste suivant, ça évite les erreurs.

On a donc obtenu : $150 \times 2 + 42 \times (-7) = 6$.

Remarque

On peut aussi trouver le PGCD(42;150) en utilisant les décompositions en facteurs premiers.

On a : $42 = 2 \times 3 \times 7$ et $150 = 2 \times 3 \times 5^2$. Le produit des facteurs communs élevés aux puissances les plus petites. Ici $6 = 2 \times 3$.

Théorème

Soient a et b deux entiers naturels et $d = \text{PGCD}(a; b)$. Il existe deux entiers relatifs x et y tels que : $ax + by = d$.

On peut trouver un tel couple (x, y) en remontant l'algorithme d'Euclide (comme dans l'exercice précédent).

Propriétés

a, b et c étant trois entiers naturels non nuls.

1. $c | a$ et $c | b \Leftrightarrow c | \text{PGCD}(a; b)$
2. $b | a \Rightarrow b = \text{PGCD}(a; b)$
3. $\text{PGCD}(a; b) = \text{PGCD}(b; a)$ soit $a \wedge b = b \wedge a$
4. $\text{PGCD}(a; \text{PGCD}(b; c)) = \text{PGCD}(\text{PGCD}(a; b); c)$ soit
 $a \wedge (b \wedge c) = (a \wedge b) \wedge c$
5. $a \text{PGCD}(b; c) = \text{PGCD}(ab; ac)$ soit $a(b \wedge c) = ab \wedge ac$
6. a, b et g sont trois entiers positifs.

$$g = \text{PGCD}(a, b) \Leftrightarrow \begin{cases} \bullet g | a \text{ et } g | b \\ \bullet \frac{a}{g} \wedge \frac{b}{g} = 1 \end{cases} \Leftrightarrow \begin{cases} \bullet g | a \text{ et } g | b \\ \bullet \text{il existe } u \text{ et } v \\ \text{tels que } ua + vb = g \end{cases}$$

Exercice 11

On dispose de 959 billes rouges et 685 billes vertes. Quel est le nombre maximum de paquets identiques qu'on peut former en utilisant toutes les billes ? Quel est alors le contenu de chaque paquet ?

Solution

Pour qu'il ne reste pas de billes le nombre de paquets doit être un diviseur commun de 959 et 685. Pour que le nombre de paquets soit maximal ce diviseur doit être le plus grand et donc le PGCD.

L'algorithme d'Euclide donne : $959 = 685 \times 1 + 274$. $685 = 274 \times 2 + 137$ et $274 = 137 \times 2 + 0$.
 Donc $959 \wedge 685 = 137$. Le nombre maximum de paquets identiques est 137 et chaque paquet contient 12 billes dont 7 sont rouges et 5 vertes : $959 = 137 \times 7$ et $685 = 137 \times 5$.

Théorème

Soit a et b deux entiers naturels non nuls et $d = \text{PGCD}(a; b)$ tels que $a = a' \times d$ et $b = b' \times d$. Les entiers a' et b' premiers entre eux.

Théorème (de Bézout)

Les nombres a et b sont premiers entre eux si et seulement si, il existe deux entiers relatifs x et y tels que $ax + by = 1$.

Remarque

Le couple $(x; y)$ n'est pas unique. En effet, 4 et 3 sont premiers entre eux, on a : $4 \times 4 + (-5) \times 3 = 1$ et on a aussi : $1 \times 4 + (-1) \times 3 = 1$.

Théorème

Si a , entier naturel, est premier avec b_1, b_2, \dots, b_n , entiers naturels, alors a est premier avec leur produit.

Corollaire

Si a et b sont premiers entre eux alors a^p est premier avec b^q pour $(p, q) \in \mathbb{N}^2$.

Théorème (de Gauss)

Etant donnés trois entiers relatifs a , b et c non nuls, si a et b sont premiers entre eux et si $a \mid bc$ alors $a \mid c$.

Corollaire

Si a , entier naturel, est divisible par b_1, b_2, \dots, b_n , entiers naturels, et si ces entiers sont premiers entre eux deux à deux, alors a est divisible par leur produit.

Conséquences

Soit a , b , c et p des entiers naturels non nuls.

$$1) \quad \left. \begin{array}{l} \bullet a \mid c, \\ \bullet b \mid c, \\ \bullet \text{PGCD}(a, b) = 1. \end{array} \right\} \Rightarrow \boxed{ab \mid c}$$

$$2) \quad \left. \begin{array}{l} \bullet p \text{ est premier}, \\ \bullet p \mid ab. \end{array} \right\} \Rightarrow \boxed{p \mid a \text{ ou } p \mid b}$$

$$3) \left| \begin{array}{l} \bullet p \text{ est premier,} \\ \bullet \text{PGCD}(p,a) = 1, \\ \bullet \text{PGCD}(p,b) = 1. \end{array} \right. \Rightarrow \boxed{\text{PGCD}(p,ab) = 1}$$

Théorème (Petit théorème de Fermat)

Si l'entier naturel p est premier, alors, pour tout entier naturel a , $(a^p - a)$ est divisible par p .

Corollaire

Si l'entier naturel p est premier, alors, pour tout entier naturel a non multiple de p , $(a^{p-1} - 1)$ est divisible par p . (ie $a^{p-1} \equiv 1 [p]$)

Exercice 12

Montrer que pour tout $n \in \mathbb{N}^*$; le nombre $A = n^{13} - n$ est divisible par 13, 7, 5, et 2.

Solution

On écrit A sous plusieurs formes et on utilise le petit théorème de Fermat

$$A = n((n^6)^2 - 1) = n(n^6 - 1)(n^6 + 1) = n(n^3 - 1)(n^3 + 1)(n^6 + 1)$$

6) PPCM

Définition

Soit a et b deux entiers naturels non nuls. L'ensemble des multiples positifs communs à a et b admet un plus petit élément. On appelle Plus Petit Commun Multiple de a et de b le plus petit entier strictement positif commun à a et à b . On note $\text{PPCM}(a ; b)$ ou $a \vee b$

Exemple

Recherche du PPCM de 12 et de 8.

Multiples positifs de 8 : 8 ; 16 ; 24 ; 32 ; ...

Multiples positifs de 12 : 12 ; 24 ; 36 ; ... On a donc $\text{PPCM}(8,12) = 24$.

Propriétés

1. $a|b \Rightarrow \text{PPCM}(a;b) = b$
2. $\text{PGCD}(a;b) = 1 \Rightarrow \text{PPCM}(a;b) = ab$
3. $\text{PPCM}(a;b) = \text{PPCM}(b;a)$ soit $a \vee b = b \vee a$
4. $\text{PPCM}(a; \text{PPCM}(b;c)) = \text{PPCM}(\text{PPCM}(a;b); c)$ soit $a \vee (b \vee c) = (a \vee b) \vee c$
5. $a \text{PPCM}(b;c) = \text{PPCM}(ab;ac)$ soit $a(b \vee c) = ab \vee ac$
6. $\text{PPCM}(a;b) \times \text{PGCD}(a;b) = ab$ soit $(a \vee b)(a \wedge b) = ab$

7) Equations diophantiennes

Théorème

a, b et c étant trois entiers naturels. L'équation $ax + by = c$ admet des solutions entières si et seulement si c est un multiple du $\text{PGCD}(a;b)$.

Méthode de résolution

Les équations de la forme (E) : $ax + by = c$ où a, b et c sont dans \mathbb{Z} se résolvent en général de la façon suivante:

- Si a et b sont premiers entre eux, on cherche une solution particulière (x_0, y_0) . On utilise, par exemple, l'Algorithme d'Euclide. Toute autre solution (x, y) doit alors vérifier : $a(x - x_0) + b(y - y_0) = 0$ donc : $a(x - x_0) = -b(y - y_0)$. Comme a et b sont premiers entre eux, cette dernière relation implique (d'après le Théorème de Gauss) que a divise $(y - y_0)$, donc qu'il existe un entier k dans \mathbb{Z} tel que $y - y_0 = ka$. En remplaçant dans l'équation précédente, on obtient alors $a(x - x_0) = -bka$ d'où $x - x_0 = -kb$.
 - Toute solution est donc de la forme : $(x = x_0 - kb; y = y_0 + ka)$ où k est un entier relatif.
 - On vérifie alors sans problème que ces couples sont bien des solutions (la réciproque).
- Si a et b ne sont pas premiers entre eux, on note d le PGCD de a et b .
 - Si d divise c , on sait alors qu'il existe A, B et C tels que $a = Ad, b = Bd$ et $c = Cd$ où A et B sont premiers entre eux. L'équation (E) s'écrit alors : $Ax + By = C$. On est alors dans le cas précédent.
 - Si d ne divise pas c , alors l'équation (E) n'admet aucune solution dans \mathbb{Z}^2 .

Exercice 13

Résoudre l'équation (E) : $24x + 35y = 1$ dans \mathbb{Z}^2

Solution

On a $24 = 2^3 \times 3$ et $35 = 5 \times 7$ donc $24 \wedge 35 = 1$ et $1 | 1$. L'équation admet des solutions entières.

Recherche d'une solution particulière.

$$\begin{aligned}35 &= 24 \times 1 + 11 \\24 &= 11 \times 2 + 2 \\11 &= 2 \times 5 + 1 \\2 &= 1 \times 2 + 0\end{aligned}$$

Remontons l'algorithme d'Euclide.

$$\begin{aligned}1 &= 11 - 5 \times 2 \\&= 11 - 5 \times (24 - 2 \times 11) \\&= 11 - 5 \times 24 + 10 \times 11 \\&= -5 \times 24 + 11 \times 11 \\&= -5 \times 24 + 11 \times (35 - 1 \times 24) \\&= -5 \times 24 + 11 \times 35 - 11 \times 24 \\&= 11 \times 35 - 16 \times 24\end{aligned}$$

On a obtenu : $24 \times (-16) + 35 \times 11 = 1$, c'est-à-dire que le couple $(-16, 11)$ est une solution particulière de (E).

Recherche des solutions générales.

Soit (x, y) une solution quelconque de (E). On a : $24x + 35y = 24 \times (-16) + 35 \times 11 \Leftrightarrow$

$24(x + 16) = 35(11 - y) \quad (*)$. On voit que 24 divise $35(11 - y)$ et que $24 \wedge 35 = 1$ donc d'après Gauss 24 doit diviser $11 - y$. Il existe $k \in \mathbb{Z}$ tel que $11 - y = 24k$. En remplaçant dans $(*)$ on trouve : $24(x + 16) = 35 \times 24k$, soit $x + 16 = 35k$. Les solutions de (E) sont :

$$S = \{(-16 + 35k, 11 - 24k) / k \in \mathbb{Z}\}.$$

8) Systèmes de numération

L'écriture d'un nombre entier en utilisant les chiffres 0, 1, 2, ... 8, 9, n'a pas été de tout temps ni en tout lieu un usage commun. Un des premiers systèmes d'écriture est né vers 2000 avant J-C et utilisait la base 60. Il nous en est resté le système horaire (1 heure = 60 minutes, 1 minute = 60 secondes...).

Système de numération décimal (ou « en base 10 ») :

Dans notre système habituel de numération, on dispose de 10 symboles (chiffres) : 0, 1, 2, 3, ... 9 pour écrire tous nos nombres.

Tout nombre peut donc se décomposer en une somme de puissances de 10.

Exemples

Le nombre 2023, est composé de 2 milliers, 0 centaine, 2 dizaines et 3 unités:

$$2023 = 2 \times 1000 + 0 \times 100 + 2 \times 10 + 3 = 2 \times 10^3 + 0 \times 10^2 + 2 \times 10 + 3$$

$$65743 = 6 \times 10^4 + 5 \times 10^3 + 7 \times 10^2 + 4 \times 10^1 + 3 \times 10^0$$

On « regroupe par paquets de 10 ».

Système binaire (ou « en base 2 ») :

Ce système ne se compose que de deux symboles : 0 et 1 ; ce qui est très pratique pour toute l'électronique puisqu'il n'y a que deux possibilités : le courant passe ou ne passe pas. Tout nombre se décompose donc ici en « paquets de 2 » au lieu de « paquets de 10 », et donc en puissances de 2.

Ainsi, un nombre exprimé en base 2 pourra se présenter de la manière suivante : $(10110)_2$.

Exemple

$$(10110)_2 = 1 \times 2^4 + 0 \times 2^3 + 1 \times 2^2 + 1 \times 2^1 + 0 \times 2^0$$

$$(10110)_2 = 1 \times 16 + 0 \times 8 + 1 \times 4 + 1 \times 2 + 0 \times 1$$

Le nombre représenté par 10110 en base deux est le même nombre qui est représenté par 22 en base 10

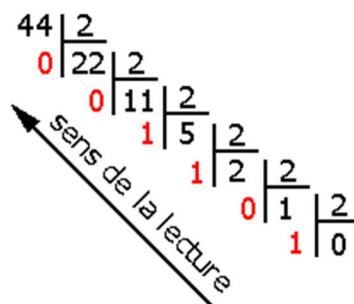
Conversion décimal-binaire

Pour obtenir l'expression binaire d'un nombre exprimé en décimal, il suffit de diviser successivement ce nombre par 2 jusqu'à ce que le quotient obtenu soit égal à 0.

Les restes de ces divisions lus de bas en haut représentent le nombre binaire.

Exemple

Pour convertir le nombre 44 exprimé en décimal en base 2, on procède aux divisions successives :



$$(44)_{10} = (101100)_2$$

Exercice 14

Ecrire 17 (décimal) en base 2.

Solution

On a : $17 = 8 \times 2 + 1$, $8 = 4 \times 2$, $4 = 2 \times 2$, $2 = 1 \times 2$. Donc

$$17 = 8 \times 2 + 1 = (4 \times 2) \times 2 + 1 = 4 \times 2^2 + 1 = (2 \times 2) \times 2^2 + 1 = 2 \times 2^3 + 1 = 1 \times 2^4 + 0 \times 2^3 + 0 \times 2^2 + 0 \times 2^1 + 1$$

D'où l'écriture de 17 en base 2 : $(17)_{10} = (10001)_2$ ou bien $17 = \overline{10001}^2$.

Divisions successives

17	2
1	8
	2
	0
	4
	2
	0
	2
	2
	0
	1
	2
	1
	0

Système octal (ou « en base 8 ») :

Le système octal utilise un système de numération ayant comme base 8 (octal => latin octo = huit). Il faut noter que dans ce système nous avons 8 symboles seulement : 0, 1, 2, 3, 4, 5, 6, 7.

Cette base obéira aux mêmes règles que la base 10, vue précédemment, ainsi on peut décomposer $(745)_8$ de la façon suivante :

$$(745)_8 = 7 \times 8^2 + 4 \times 8^1 + 5 \times 8^0$$

$$(745)_8 = 7 \times 64 + 4 \times 8 + 5 \times 1$$

$$(745)_8 = 448 + 32 + 5 = 485. \text{ Nous venons de voir que : } (745)_8 = (485)_{10}$$

Système hexadécimal (ou « en base 16 ») :

On dispose ici de 16 symboles et on décompose selon les puissances de 16. Les chiffres s'écrivent

ainsi : 0 ; 1 ; 2 ; 3 ; 4 ; 5 ; 6 ; 7 ; 8 ; 9 ; A ; B ; C ; D ; E ; F.

Un nombre exprimé en base 16 pourra se présenter de la manière suivante : $(5AF)_{16}$

Le nombre $(5AF)_{16}$ peut se décomposer comme suit :

$$(5AF)_{16} = 5 \times 16^2 + A \times 16^1 + F \times 16^0$$

En remplaçant A et F par leur équivalent en base 10, on obtient :

$$(5AF)_{16} = 5 \times 16^2 + 10 \times 16^1 + 15 \times 16^0$$

$$(5AF)_{16} = 5 \times 256 + 10 \times 16 + 15 \times 1$$

$$\text{donc } (5AF)_{16} = (1455)_{10}$$

Exercice 15

Ecrire le nombre 2023 dans les systèmes binaire, octal et hexadécimal.

Solution

On procède aux divisions successives :

$$(2023)_{10} = (11111100111)_2$$

$$(2023)_{10} = (3747)_8$$

$$(2023)_{10} = (7E7)_{16}$$

Remarque

Il y a une équivalence entre :

chaque chiffre octal et chaque groupe de 3 chiffres binaires ;

chaque chiffre hexadécimal et chaque groupe de 4 chiffres binaires.

Ce qui permet de passer facilement d'un système à base 8 ou 16 à un système à base 2 et vice versa.

Exercice 16

Effectuer les conversions suivantes sans passer par le système décimal:

101111100001 du binaire en octal

362 de l'octal au binaire

110100001100 du binaire en hexadécimal

1AF3 de l'hexadécimal au binaire

Solution

$$\begin{array}{ccccccc} \text{Binaire} & (101) & (111) & (100) & (001) &)_2 \\ \downarrow \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \\ \text{Octal} & (5) & (7) & (4) & (1) &)_8 \end{array}$$

$$\begin{array}{ccccccc} \text{Octal} & (3) & (6) & (2) &)_8 \\ \downarrow \downarrow & \downarrow & \downarrow & \downarrow & \\ \text{Binaire} & (011) & (110) & (010) &)_2 \end{array}$$

$$\begin{array}{ccccccc} \text{Binaire} & (1101) & (0000) & (1100) &)_2 \\ \downarrow \downarrow & \downarrow & \downarrow & \downarrow & \\ \text{Hexadécimal} & (D) & (0) & (C) &)_{16} \end{array}$$

$$\begin{array}{ccccccc} \text{Hexadécimal} & (1) & (A) & (F) & (3) &)_{16} \\ \downarrow \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \\ \text{Binaire} & (0001) & (1010) & (1111) & (0011) &)_2 \end{array}$$

Exercice 17

Effectuer les opérations suivantes dans le système indiqué :

Binaire	Octal	Hexadécimal
1101011101 +1101110011	754 +462	A34D +4671

Solution

Binaire	Octal	Hexadécimal
1101011101 <u>+1101110011</u> =11011010000	754 <u>+462</u> =1436	A34D <u>+4671</u> = E9BE

Généralisation

Un système de numération repose sur le principe de la division Euclidienne:

"Pour tout a et tout b entiers supérieurs strictement à 0, il existe q et r entiers uniques tels que $a = bq + r$ avec $0 \leq r < b$. q est le quotient et r le reste.

D'une façon plus générale:

Si b et a sont des entiers tels que $b \geq 2$ et $a > 0$, la division euclidienne de a par b s'écrit:
 $a = q_0b + a_0$ où $0 \leq a_0 < b$.

Effectuons alors la division euclidienne de q_0 par b : $q_0 = q_1b + a_1$ avec $0 \leq a_1 < b$

On peut alors continuer ce principe de division tant que le quotient obtenu n'est pas nul.

On construit ainsi deux suites (q_n) et (a_n) où (q_n) décroît.

Comme c'est une suite d'entiers naturels, il y a un terme q_n qui est inférieur à b , donc égal à son reste a_n dans la division euclidienne par b .

En reportant les calculs effectués, on constate alors que: $a = a_nb^n + a_{n-1}b^{n-1} + \dots + a_1b + a_0$

C'est le développement de a suivant les puissances de b .

Propriété et définition

Soient b et a deux entiers naturels tels que $b \geq 2$ et $a > 0$. Il existe une suite unique

a_0, a_1, \dots, a_n d'entiers naturels tels que : $a = a_0 + a_1b + a_2b^2 + \dots + a_nb^n = \sum_{k=0}^n a_kb^k$ avec

$0 \leq k \leq n$, $0 \leq a_k < b$ et $a_n \neq 0$. L'écriture de a en base b est alors par convention:

$a = \overline{a_na_{n-1}\dots a_2a_1a_0}^b$ ou $a = (a_na_{n-1}\dots a_2a_1a_0)_b$. La suite de chiffres a_0, a_1, \dots, a_n est la suite de chiffres de a dans la base b .

La représentation symbolique du nombre a dans la base b nécessite b symboles, appelés chiffres. Les premiers symboles utilisés sont $0, 1, 2, \dots, 9$ puis les 26 lettres de l'alphabet : A, B, \dots, Z

Exemple

Prenons un exemple: $a = 115$ et $b = 7$, ces nombres étant pris dans leur écriture "classique" de numération en base 10.

On a alors $115 = 16 \times 7 + 3$. Le quotient est $q = 16$ et le reste est $r = 3$.

Effectuons alors la division euclidienne du quotient 16 par 7.

$16 = 2 \times 7 + 2$. Le reste est $r = 2$ et le quotient est $q = 2$, et enfin le reste de division de 2 par 7 est $r = 2$

On peut alors écrire : $115 = 16 \times 7 + 3 = (2 \times 7 + 2) \times 7 + 3 = 2 \times 7^2 + 2 \times 7 + 3$

115 peut alors s'écrire $(115)_{10} = (223)_7$. C'est son écriture en base 7.

Exercice 18

Ecrire 65 exprimé en décimal, en base 6.

Solution

On a : $65 = 10 \times 6 + 5$, $10 = 1 \times 6 + 4$

Donc $65 = 10 \times 6 + 5 = (1 \times 6 + 4) \times 6 + 5 = 1 \times 6^2 + 4 \times 6 + 5$.

D'où l'écriture de 65 en base 6 : $(65)_{10} = (145)_6$

$$\begin{array}{r|l} 65 & 6 \\ 5 & \overline{10} \quad 6 \\ & 4 \quad \overline{1} \quad 6 \\ & & 1 \quad \overline{0} \end{array}$$

Exercice 19

Ecrire 1690 exprimé en décimal, en base 12.

Solution

Si on veut écrire un nombre en base 12, on doit introduire d'autres symboles d'écriture en plus des chiffres usuels 0, 1, 2, ..., 9. Posons alors $A = 10$ et $B = 11$.

Les chiffres disponibles sont alors 0, 1, 2, ..., 9, A, B.. Les divisions successives permettent de trouver facilement cette écriture

$$(1690)_{10} = (B8A)_{12}$$

On range les restes du dernier à gauche au droite.

1690	12	
A	140	12
8	11	12
B	0	premier à

Exercice 20

Calculer dans le système de base 13 :

$$BAC + 2023$$

Solution

$$\begin{array}{r} BAC \\ + 2023 \\ \hline = 2C02 \end{array}$$

9) Enoncés des exercices

Exercice 21

- 1) Décomposer le nombre $n = 4678128$ en facteurs premiers.
- 2) Déterminer le nombre de diviseurs et la somme des diviseurs de n .

Exercice 22

Soit $a = 2645$ et $b = 321$ représentés en base 7.

Calculer $a + b$ et axb en base 7.

Exercice 23

Montrer que pour tout $n \in \mathbb{N}$, le nombre $A = n^2(n^4 - 1)$ est divisible par 60.

Exercice 24

Par combien de zéros se termine le nombre $2023!$?

Exercice 25

- 1) Trouvez, suivant les valeurs de l'entier naturel n , le reste de la division euclidienne de 5^n par 7.
- 2) Trouvez le reste de la division euclidienne de 2021^{2020} par 7.
- 3) Soit $X = 2011^{2n+1} + 2014^{2n+1}$.
 - a) Montrez que pour tout entier naturel n , X est divisible par 7.
 - b) Montrez que pour tout entier naturel n , X est divisible par 25.
 - c) X est-il divisible par 175 ? Justifier.

Exercice 26

En rangeant les n pièces de son puzzle, un enfant constate que :

S'il les range par groupe de 5, il lui reste 3 pièces.

S'il les range par groupe de 7, il lui reste 2 pièces.

S'il les range par groupe de 9, il lui reste 1 pièce.

S'il les range par groupe de 11, il ne lui reste plus de pièces.

Sa mère affirme qu'alors $2n-11$ est divisible par 5, 7, 9 et 11.

1) A-t-elle raison ?

2) Combien ce puzzle contient de pièces sachant que ce nombre est inférieur à 2020 ?

Exercice 27

1) On considère l'équation (E) :, où x et y sont des entiers relatifs $25x - 49y = 5$

a) Déterminer le pgcd de 49 et 25 à l'aide de l'algorithme d'Euclide et en déduire que l'équation (E) admet des solutions entières.

b) Vérifier que le couple (10 ; 5) est une solution particulière de (E). Résoudre l'équation (E).

c) Montrer qu'il existe un unique entier p compris entre 1960 et 2018 tel que : $25p \equiv 5[49]$.

2.a) Justifier que si (x,y) est une solution de (E) alors $5x \equiv 1[7]$ et $y \equiv 0[5]$.

b) Montrer que $5x \equiv 1[7]$ si et seulement si $x \equiv 3[7]$.

3.a) Soit x un entier relatif. Quels sont les restes de x^2 dans la division euclidienne par 7 ?

b) Existe-t-il un couple (x,y) d'entiers relatifs tels que (x^2, y^2) soit solution de (E) ?

Exercice 28

Quels sont les entiers n tels que $n^6 - 1$ soit divisible par 9 ?

Exercice 29

On considère l'équation (E) :, où x et y sont des entiers relatifs. $11x - 7y = 25$

1.a) Justifier que l'équation (E) admet des solutions entières et vérifier que le couple (8,9) est une solution particulière de (E).

b) Déterminer l'ensemble des solutions de (E).

2) Soit (x,y) une solution de (E).

a) Montrer que si x est un diviseur de y , alors x est un diviseur de 25.

b) Soit m un entier relatif. Existe-t il des valeurs de m telles que le quotient $\frac{20+11m}{15+7m}$ soit un entier relatif ?

Exercice 30

Pour tout entier naturel supérieur ou égal à 5, on considère les nombres $a_n = n^3 - n^2 - 12n$ et $b_n = 2n^2 - 7n - 4$.

1) Montrer, après factorisation, que a_n et b_n sont des entiers naturels divisibles par $n-4$.

2) On pose $\alpha = 2n+1$ et $\beta = n+3$. On note d le PGCD de α et β .

a) Etablir une relation entre α et β indépendante de n .

b) Démontrer que d est un diviseur de 5.

c) Démontrer que les nombres α et β sont multiples de 5 si et seulement si $n-2$ est un multiple de 5

- 3) Montrer que $2n + 1$ et n sont premiers entre eux.
- 4-a) Déterminer, suivant les valeurs de n et en fonction de n , le PGCD de a_n et b_n .
- b) Vérifier les résultats obtenus dans les cas particuliers $n = 11$ et $n = 7$.
- c) Résoudre dans \mathbb{Z}^2 l'équation $1078x + 161y = 35$.

Exercice 31

On considère les équations dont les inconnues sont des entiers (E): $35u - 96v = 1$ et (F): $x^{35} \equiv 2 \pmod{97}$.

- 1.a) En appliquant le test de primalité vérifier que 97 est un nombre premier.
- b) Montrer que le couple (11;4) est solution de l'équation (E).
- c) Résoudre dans \mathbb{Z}^2 l'équation (E).
- 2) Soit x une solution de l'équation (F).
- a) Prouver que les nombres x et 97 sont premiers entre eux.
- b) Montrer que $x^{96} \equiv 1 \pmod{97}$ puis que $x \equiv 2^{11} \pmod{97}$
- 3) Soit n un entier. Montrer que si $n \equiv 2^{11} \pmod{97}$ alors n est solution de (F).
- 4) Montrer que les solutions de (F) sont tous les entiers $x = 11 + 97k$; $k \in \mathbb{Z}$

Exercice 32

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

- 1.a) Déterminer le PGCD de 109 et 226. Que peut-on conclure pour l'équation (E) ?
- b) Donner une solution particulière de (E). Déterminer alors l'ensemble des solutions de (E).
- c) En déduire qu'il existe un unique entier naturel d inférieur ou égal à 226 et un unique entier naturel e tels que $109d = 1 + 226e$. On précisera les valeurs de d et e .
- 2) Montrer que 227 est premier.
- 3) On note A l'ensemble des entiers naturels a tels que $a \leq 226$.
- On considère les deux fonctions f et g définies de A dans A de la manière suivante :
- $f(a) = r$ où r est le reste de la division euclidienne de a^{109} par 227 et $g(a) = r'$ où r' est le reste de la division euclidienne de a^{141} par 227.
- a) Vérifier que $g \circ f(0) = 0$.
- b) Justifier que, quelque soit l'entier non nul a de A , $a^{226} \equiv 1 \pmod{227}$.
- c) En déduire que, quelque soit l'entier non nul a de A , $g[f(a)] = a$.
- Que peut-on dire de $f[g(a)]$?

Exercice 33

1) On considère l'équation (E) :, où x et y sont des entiers relatifs $2017x + 41y = 1$

a) Vérifier que 2017 est un nombre premier puis montrer que l'équation (E) admet des solutions entières.

b) Vérifier que le couple $(-5; 246)$ est une solution particulière de (E). Résoudre l'équation (E).

c) Dédire qu'il existe un unique entier y inférieur ou égal à 2016 tel que : $41y \equiv 1[2017]$

Pour la suite de l'exercice on rappelle qu'un entier a est l'inverse de b modulo 2017 si $ab \equiv 1[2017]$.

2) Soient a et b deux entiers relatifs.

a) Montrer que : si $ab \equiv 0[2017]$ alors $(a \equiv 0[2017] \text{ ou } b \equiv 0[2017])$

b) Dédire que : si $a^2 \equiv 1[2017]$ alors $(a \equiv 1[2017] \text{ ou } a \equiv -1[2017])$

c) Quels sont donc les entiers de l'intervalle $[1; 4033]$ qui sont égaux à leurs inverses modulo 2017 ?