

Partiel du samedi 18 mars 2023

Durée : 2 heures.

Les documents, calculatrices, téléphones portables et montres connectées sont interdits.

Pour obtenir une très bonne note, il n'est pas nécessaire de résoudre tous les exercices.

Toutes les réponses devront être soigneusement justifiées.

Exercice 1 (1+3 pts). Questions de cours.

- Qu'est-ce qu'un nombre premier ?
- Qu'est-ce qu'un groupe ?

Exercice 2 (2 pts). Déterminer les solutions $(x, y) \in \mathbb{Z}^2$ de l'équation $33x + 15y = 9$.

Exercice 3 (1+1 pts).

- Quel est le reste dans la division euclidienne par 51 de 203^{180323} ?
- L'écriture en binaire de $2023^{14071789}$ se termine-t-elle par 0 ou par 1 ?

Exercice 4 (1+1+1+2 pts).

- Pour chacune des congruences suivantes, trouver une congruence équivalente de la forme $x \equiv a \pmod{n}$.

$$3x \equiv 2 \pmod{7}, \quad 2x \equiv 4 \pmod{6}, \quad 9x \equiv 9 \pmod{15}.$$

- Résoudre le système de congruences

$$\begin{cases} 3x \equiv 2 \pmod{7} \\ 2x \equiv 4 \pmod{6} \\ 9x \equiv 9 \pmod{15} \end{cases}$$

Exercice 5 (1+1+2+2+2 pts).

- Soit $n \geq 1$ un entier. Rappeler la définition du groupe $(\mathbb{Z}/n\mathbb{Z})^\times$.
- Dresser la liste des éléments du groupe $(\mathbb{Z}/18\mathbb{Z})^\times$.
- Calculer les ordres des groupes $(\mathbb{Z}/8\mathbb{Z})^\times$, $(\mathbb{Z}/27\mathbb{Z})^\times$ et $(\mathbb{Z}/216\mathbb{Z})^\times$.
- Déterminer l'ordre de la classe de 2 et celui de la classe de 8 dans le groupe $(\mathbb{Z}/27\mathbb{Z})^\times$.
Ce groupe est-il cyclique ?
- Montrer qu'il existe un unique morphisme de groupes de $(\mathbb{Z}/12\mathbb{Z}, +)$ vers $(\mathbb{Z}/27\mathbb{Z})^\times$ qui envoie la classe de 1 sur celle de 8. Déterminer son noyau et son image.

Exercice 6 (2 pts). Soit G un groupe. Soient x et y deux éléments de G qui sont d'ordres finis a et b . Supposons que $xy = yx$. Montrer que l'ordre de xy divise $\text{ppcm}(a, b)$.

VÉRIFICATION DES APTITUDES
ET DES CONNAISSANCES

DATE : 18/03

ECUE OU UE : Mathématiques

Après avoir rempli l'en-tête, rabattre et coller le coin noir ci-dessous

Nom : TANG
 Prénom : Thank Long
 N° d'étudiant : 22110569
 N° de place : Info 4

N.B. - Il est interdit aux candidats, sous peine d'exclusion, de signer leur composition ou d'y apporter un signe distinctif quelconque.

Correcteurs

Nom :	NOTE	Nom :	NOTE
Appréciations :	14,5/20	Appréciations :	
Note définitive :	Ex2: 2/2		

Ex2: 2/2

$$33x + 15y = 9$$

On calcule d'abord le pgcd(33, 15) = 3

$$33 = 2 \times 15 + 3$$

On constate que 3 | 9 donc l'équation admet dans des solutions

15 = 5 × 3 + 0

On cherche la solution particulière à l'équation

$$33x + 15y = 3$$

On remonte la division Euclidienne :

$$3 = 33 - 2 \times 15$$

On a alors $(x_0, y_0) = (1, -2)$

On cherche ensuite la solution particulière dans l'équation

$$33x + 15y = 3$$

$$\Leftrightarrow 33x + 15(-2) + 3 = 3$$

$$\Leftrightarrow 33x + 3 + 15(-6) = 3$$

$$\Rightarrow (x_0, y_0) = (3, -6) \leftarrow \text{Solution particulière}$$

NE RIEN ÉCRIRE ICI

page 2/10

Sait $a', b' \in \mathbb{Z}$, On a l'équation sous la forme

$$ax + by = d \quad \text{avec } a = 33 \quad b = 15$$

$$a = \text{pgcd}(a, b) \times a' \quad b = \text{pgcd}(a, b) \times b'$$

$$33 = 3 \times a' \quad 15 = 3 \times b'$$

$$a' = 11$$

$$b' = 5$$

✓ Solution générale : $\{(3 + 5k, -6 - 11k) | k \in \mathbb{Z}\}$

Ex 3 2/2

$$14203 \mod 51$$

$$203 = 3 \times 51 + 5 \quad \textcircled{B}$$

$$\text{Danc } 203 \equiv -1 \mod 51 \equiv 50 \mod 51$$

$$\Leftrightarrow (203)^2 \equiv (-1)^2 \mod 51 \\ \equiv 1 \mod 51$$

Alors 180323 est un nombre impair. Alors un k tel que $180323 = 2k + 1$

On a alors

$$203^{180323} = (203^2)^k 203$$

$$\Rightarrow 203^{180323} \mod 51$$

$$\Leftrightarrow (203^2)^k 203 \mod 203^{2k+1} \mod 5$$

$$\Leftrightarrow (203^2)^k 203 \equiv 1^k \times (-1) \mod 51 \mod 5$$

$$\equiv -1 \mod 51$$

Le reste de la division euclidienne est 50 ✓

du 2023 14071789

On constate que 2023 est un nombre impair donc

$$2023 \equiv 1 \pmod{2}$$

$$\Leftrightarrow 2023^{14071789} \equiv 1^{14071789} \pmod{2}$$

$$\equiv 1 \pmod{2}$$

Donc le chiffre unité est 1 ✓

merci!

Ex 4 4.5/5. bien.

~~$$3x \equiv 2 \pmod{4}$$~~

~~$$\text{pgcd}(3, 4) = 1$$~~

On constate que le ~~$\text{pgcd}(3, 4) : 2 \nmid 2$~~ dans l'équation n'admet pas de solution

~~$$3x \equiv 2 \pmod{4}$$~~

fait à la page 8

$$2x \equiv 4 \pmod{6}$$

$$\text{pgcd}(2, 6) = 2$$

$$6 = 3 \times 2 + 0$$

On voit que le ~~$\text{pgcd}(2, 6) : 2 \mid 4$~~ dans l'équation admet au moins une solution et est équivalente à :

$$x \equiv 2 \pmod{3} \quad \checkmark$$

On cherche à inverser le mod 2 mod 6

$$\text{Dans } S = \exists 3k + 2 \mid k \in \mathbb{Z} \exists$$

$$9x \equiv 9 \pmod{15}$$

$$\text{pgcd}(9, 15) = 3$$

$$15 = 1 \times 9 + 6$$

$$9 = 1 \times 6 + 3$$

$$3 = 2 \times 3 + 0$$

On cherche à inverser le 3 mod 5

$$3 \times 7 = 21 \equiv 1 \pmod{5}$$

On a donc :

$$3x \equiv 3 \pmod{5}$$

$$\Leftrightarrow 3x \times 7 \equiv 3 \times 7 \pmod{5}$$

$$\Leftrightarrow 21x \equiv 21 \pmod{5}$$

$$\Leftrightarrow x \equiv 21 \pmod{5}$$

$$\Leftrightarrow x \equiv 1 \pmod{5} \quad \checkmark$$

$$S = \exists 5k + 11 \mid k \in \mathbb{Z} \exists$$

Rappel n° de place :

c'est faire $\text{pgcd}(3, 6) = 3$

394

Ex 1: 0.5.

point

est toujours = 1

ax Un nombre premier est un nombre qui a seulement les diviseurs qui sont 1 ou lui-même donc son pgcd avec n'importe quel autre nombre

bx Un groupe est un ensemble G , une loi $G \times G \xrightarrow{*} G$ qui doit vérifier

- o * associativité : $\forall x, y, z \in G$ tel que $(a+b)+c = a+(b+c)$
- o \exists un élément neutre, $e \in G$ tel que $\forall a \in G \quad a + e = e + a = a$
- o $\forall a \exists b$ un inverse a^{-1} tel que $a + b = b + a = e$
 $x * y = y * x$

Ex 5 2.5/8

ax $(\mathbb{Z}/n\mathbb{Z})^*$ et l'ensemble des éléments de $\mathbb{Z}/n\mathbb{Z}$, qui sont inversibles, un élément a est inversible par la multiplication si et seulement si a et n sont premiers entre eux

bx $(\mathbb{Z}/18\mathbb{Z})^* = \{\bar{1}, \bar{5}, \bar{7}, \bar{11}, \bar{13}, \bar{17}\}$

 ob
y

il est à aussi
divisible →
par -1, et
par -P.
oh mais
attention aux
énuméros 2/3/4/5/6/7

Ex: $f: (\mathbb{Z}/8\mathbb{Z}) \rightarrow (\mathbb{Z}/2\mathbb{Z})$ tel que $f(1) = \bar{8}$

Puisque $f(1) = \bar{8}$, on peut définir f pour chaque élément de $\mathbb{Z}/8\mathbb{Z}$ en multipliant 8 par l'élément de $\mathbb{Z}/8\mathbb{Z}$

On définit donc $f(a) = 8a \text{ mod } 2^4$ $f(a) = \bar{8}^a$

Pour que $f: (\mathbb{Z}/8\mathbb{Z}) \rightarrow (\mathbb{Z}/2\mathbb{Z})$ soit un unique morphisme, il doit vérifier les propriétés suivantes:

$f(a+b \text{ mod } 8) = f(a) + f(b) \text{ mod } 2^4$ pour tous les éléments a, b de $\mathbb{Z}/8\mathbb{Z}$

Soit a et b des éléments de $\mathbb{Z}/8\mathbb{Z}$. On a

$$f(a+b \text{ mod } 8) = 8(a+b \text{ mod } 8) \text{ mod } 2^4$$

$$\text{Ainsi: } f(a) + f(b) = 8(a+b) \text{ mod } 2^4$$

$$\begin{aligned} \text{Ainsi } f(a) + f(b) \text{ mod } 2^4 &= (8a \text{ mod } 2^4 + 8b \text{ mod } 2^4) \text{ mod } 2^4 \\ &= (8a + 8b) \text{ mod } 2^4 \end{aligned}$$

$$\text{On a } 8(a+b) \text{ mod } 2^4 = (8a + 8b) \text{ mod } 2^4$$

$$\text{Donc } f(a+b \text{ mod } 8) = f(a) + f(b) \text{ mod } 2^4$$

Supposons qu'il y a un autre morphisme de groupe

$$g: \mathbb{Z}/8\mathbb{Z} \rightarrow \mathbb{Z}/2^4 \mathbb{Z} \text{ tel que } g(1) = \bar{8}$$

Alors pour chaque élément a de $\mathbb{Z}/8\mathbb{Z}$ on a

$$g(a) = g(a \times 1) = a \times g(1) = a \times 8 \text{ mod } 2^4 \Rightarrow g = f$$

Cela montre que $g(a) = 5a \text{ (mod } 2^4)$ pour un unique morphisme de groupe $f: \mathbb{Z}/8\mathbb{Z} \rightarrow \mathbb{Z}/2^4 \mathbb{Z}$ tel que $f(1) = \bar{8}$

$$f(1) = \bar{8}$$

On cherche son noyau :

$$\ker = \{a \in \mathbb{Z}/8\mathbb{Z} \mid f(a) = 0 \text{ mod } 2^4\}$$

Pour déterminer le noyau, on cherche les valeurs de a pour que $f(a) = 8a \equiv 0 \pmod{2^4}$

Dans $\mathbb{Z}/8\mathbb{Z}$, les éléments possibles sont $\{1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11\}$

$$f(0) = 8 \times 0 = 0 \pmod{2^4}$$

Donc $\ker f = \{0\}$



On cherche ensuite l'image de f :

$$\text{Im } f = \{f(a) \mid a \in \mathbb{Z}/18\mathbb{Z}\}$$

a	$\mod 18$
0	0
1	8
2	16
3	24
4	8
5	13
6	21
7	2
8	
9	
10	
11	
12	
13	
14	
15	
16	
17	

$$\text{Danc } \text{Im } f = \{f(0), f(1), \dots\}$$

$$\{0, 8, 16, 24, 25, 13, 5, 21, 2\}$$

O.S

$$Cyc (\mathbb{Z}/18\mathbb{Z})^*, (\mathbb{Z}/12\mathbb{Z})^*, (\mathbb{Z}/16\mathbb{Z})^*$$

Les éléments du groupe $\mathbb{Z}/18\mathbb{Z}$ sont $\{1, 2, 3, 5, 7\}$

~~0, c'est élément neutre de $(\mathbb{Z}/18\mathbb{Z})^*$, on a 0 est autre~~

* On calcule leurs ordres:

1 est l'élément neutre de $(\mathbb{Z}/18\mathbb{Z})^*$, il est donc d'ordre 1 dans $(\mathbb{Z}/18\mathbb{Z})^*$

Ex 4

ap $3x \equiv 2 \pmod{7}$

$\text{pgcd}(3, 7) = 1$

On constate que 112 , l'équation admet donc au moins une solution

On cherche à inverser $3 \pmod{7}$

$3 \times 5 = 15 \equiv 1 \pmod{7}$

On a donc

$3x \equiv 2 \pmod{7}$

$\Leftrightarrow 5 \times 3x \equiv 5 \times 2 \pmod{7}$

$\Leftrightarrow 15x \equiv 10 \pmod{7}$

$\Leftrightarrow x \equiv 3 \pmod{7} \quad \checkmark$

$S = \{ \ldots, 7k + 3 \mid k \in \mathbb{Z} \}$

à b) $S \left\{ \begin{array}{l} 3x \equiv 2 \pmod{7} \\ 2x \equiv 4 \pmod{6} \\ 9x \equiv 9 \pmod{15} \end{array} \right.$

D'après la question précédente (a), on obtient donc un nouveau système de congruences

$S \left\{ \begin{array}{l} x \equiv 3 \pmod{7} \\ x \equiv 2 \pmod{3} \\ x \equiv 1 \pmod{5} \end{array} \right.$

On choisit 2 équations

$S' \left\{ \begin{array}{l} x \equiv 3 \pmod{3} \\ x \equiv 1 \pmod{5} \end{array} \right.$

On cherche ~~donc~~ le pgcd $(3, 5) = 1$

Comme $1 \mid 2-1$, le système admet des solutions

On applique l'algorithme Euclide à $(3, 5)$



Rappel n° de place :

page 9, 0

Ex 2

by

On applique l'algo Euclide à (3, 5)

$$3u + 5v = \text{pgcd}(3, 5)$$

$$3u + 5v = 1$$

$$m' = \frac{m}{\text{pgcd}(a, b)} = \frac{3}{1} = 3$$

$$n' = \frac{n}{\text{pgcd}(a, b)} = \frac{5}{1} = 5$$

solution particulière $x = bum' +avn'$

$$\begin{aligned} &= 1 \times 2 \times 3 + 2 \times (-1) \times 5 \\ &= 6 - 10 \\ &= -4 \end{aligned}$$

$$\text{ppcm}(3, 5) = 15$$

\Rightarrow Solution générale $\underline{-4 + x} \equiv -4 \pmod{15}$
 $\forall k \in \mathbb{Z}$

On obtient donc un nouveau système de S

$$\begin{cases} x \equiv 3 \pmod{7} \\ x \equiv -4 \pmod{15} \end{cases}$$

$$\text{pgcd}(7, 15) = 1$$

On constate que $\text{pgcd}(7, 15) : 1 \mid -4 - 3$, l'équation admet des solutions

On applique l'algo Euclide à (7, 15)

$$7u + 15v = \text{pgcd}(7, 15)$$

$$7u + 15v = 1$$

$$u = (-2) \quad v = +1$$

$$m' = \frac{m}{\text{pgcd}(a, b)} = \frac{7}{1} = 7$$

$$n' = \frac{n}{\text{pgcd}(a, b)} = \frac{15}{1} = 15$$



$$\begin{aligned}
 \text{solution particulière : } x &= bu_1' + av_1' \\
 &= (-4)x - 2x + \cancel{+} \cancel{-3 \times 1 \times 15} \\
 &= -56 + 45 \\
 &= -11 \quad 101
 \end{aligned}$$

$$\text{PPCM}(f, 5) = 105$$

\Rightarrow Solution générale de S est $\left\{ \begin{array}{l} y = -11 + 105k \\ k \in \mathbb{Z} \end{array} \right\}$

propre \nearrow correct, à put une erreur de calcul

1.5/2