

Un corrigé du partielle du 18/10/2023

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

- a) Qu'est-ce qu'un nombre premier ?
- b) Qu'est-ce qu'un groupe ?

a) Un nombre premier est un entier positif qui a exactement deux diviseurs positifs

Ou : un entier > 1 dont les seuls diviseurs positifs sont 1 et lui-même.

b) Un groupe est un couple (G, \cdot) formé d'un ensemble G muni d'une application $\cdot : G \times G \rightarrow G$ dite loi du groupe tels que

1) la loi est associative : on a $(xy)z = x(yz)$, $\forall x, y, z \in G$;

2) il existe un élément neutre $e \in G$: $xe = x = ex$, $\forall x \in G$;

3) tout élément $x \in G$ admet un inverse $x' \in G$: on a

$$xx' = e = x'x.$$

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

On a $\text{pgcd}(33, 15) = 3$ et 3 divise 9. Donc il existe des solutions. L'équation est équivalente à

$$11x + 5y = 3.$$

Nous avons l'équation de Bézout

$$11 \cdot 1 + 5 \cdot (-2) = 1.$$

Donc $(x_0, y_0) = (3, -6)$ est une solution particulière.

La solution générale est

$$(x, y) = (x_0, y_0) + k \cdot (5, -11) = (3 + 5k, -6 - 11k), k \in \mathbb{Z}.$$

Exercice 3 (1+1 pts).

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

1. Nous avons $203 \equiv -1 \pmod{51}$ (car $4 \cdot 51 = 204$).

Donc $203^n \equiv (-1)^n \pmod{51}$ ne dépend que de la parité de n . Comme $n = 18032023$ est impair, nous avons $203^{18032023} \equiv -1 \pmod{51}$ et le reste recherché est 50.

2. Le dernier chiffre de l'écriture binaire d'un entier N vaut 1 ssi N est impair. Comme $2023 \equiv 1 \pmod{2}$, on a $2023^n \equiv 1 \pmod{2}$

pour tout entier $n \geq 1$. Donc 2023^n est impair
pour tout entier $n \geq 1$ et le dernier chiffre de
son écriture en binaire est 1.

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

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

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

Dans $3x \equiv 2 \pmod{7}$, nous avons $\text{pgcd}(3, 7) = 1$. Donc 3
est inversible modulo 7. En fait, 5 est inverse de 3
modulo 7. Donc on a, en multipliant des 2 côtés par 5,

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

Dans $2x \equiv 4 \pmod{6}$, on a $\text{pgcd}(2, 6) = 2$ et 2 divise 4.

La congruence est équivalente à $x \equiv 2 \pmod{3}$.

Dans $9x \equiv 9 \pmod{15}$, nous avons $\text{pgcd}(9, 15) = 3$ et
3 divise 9 donc il existe des solutions. La congruence
est équivalente à $3x \equiv 3 \pmod{5}$. Nous avons
 $\text{pgcd}(3, 5) = 1$ donc 3 est inversible modulo 5.

En fait, 2 est inverse à 3 modulo 5. En multipliant par 2, nous obtenons

$$3x \equiv 3 \pmod{5} \iff x \equiv 1 \pmod{5}.$$

b) Résoudre le système de congruences

$$\begin{cases} 3x \equiv 2 \pmod{7} \\ 2x \equiv 4 \pmod{16} \\ 9x \equiv 9 \pmod{15} \end{cases}$$

D'après a), ce système est équivalent au système

$$\begin{cases} (1) & x \equiv 3 \pmod{7} \\ (2) & x \equiv 2 \pmod{3} \\ (3) & x \equiv 1 \pmod{5} \end{cases}$$

Nous avons $\text{pgcd}(7, 3) = 1$ donc le système formé des congruences (1) et (2) admet une solution unique modulo $3 \cdot 7 = 21$. Nous avons l'équation de Bézout $(-2) \cdot 7 + 5 \cdot 3 = 1$.

$$\begin{aligned} \text{Donc (1) \& (2)} &\iff x \equiv 3 \cdot 15 + 2 \cdot (-14) \pmod{21} \\ &\iff x \equiv 17 \pmod{21} \quad (4) \end{aligned}$$

Il nous reste à résoudre le système

$$\begin{cases} (3) \quad x \equiv 1 \pmod{5} \\ (4) \quad x \equiv 17 \pmod{21} \end{cases}$$

Nous avons $\text{pgcd}(5, 21) = 1$ donc il existe une solution unique modulo $5 \cdot 21 = 105$. Nous avons l'équation de Bézout

$$(-4) \cdot 5 + 1 \cdot 21 = 1$$

$$\text{resp. } -20 + 21 = 1.$$

Donc le système est équivalent à

$$\begin{aligned} x &\equiv 1 \cdot 21 + 17 \cdot (-20) \pmod{105} \\ &\equiv 101 \pmod{105} \end{aligned}$$

Donc le système de congruences est équivalent à

$$x \equiv 101 \pmod{105}$$

et l'ensemble de ses solutions est

$$\{101 + 105 \cdot k \mid k \in \mathbb{Z}\}.$$

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

- a) Soit $n \geq 1$ un entier. Rappeler la définition du groupe $(\mathbb{Z}/n\mathbb{Z})^\times$.
 b) Dresser la liste des éléments du groupe $(\mathbb{Z}/18\mathbb{Z})^\times$.

a) Le groupe $(\mathbb{Z}/n\mathbb{Z})^\times$ est l'ensemble des classes " \bar{x} modulo n , où x est inversible modulo n (i.e. $\text{pgcd}(x, n) = 1$). Sa loi de groupe est la multiplication des classes modulo n :

$${}^n\bar{x} \cdot {}^n\bar{y} = {}^n\bar{xy}.$$

b) Éléments de $(\mathbb{Z}/18\mathbb{Z})^\times$:

$$\bar{1}, \bar{5}, \bar{7}, \bar{11}, \bar{13}, \bar{17}.$$

Notons que nous avons

$$\begin{aligned} |(\mathbb{Z}/18\mathbb{Z})^\times| &= \varphi(18) = \varphi(2 \cdot 9) = \varphi(2 \cdot 3^2) \\ &= \varphi(2) \varphi(3^2) = (2-1)(3^2 - 3) = 1 \cdot 6. \end{aligned}$$

Donc la liste est complète.

- c) Calculer les ordres des groupes $(\mathbb{Z}/8\mathbb{Z})^\times$, $(\mathbb{Z}/27\mathbb{Z})^\times$ et $(\mathbb{Z}/216\mathbb{Z})^\times$.

Nous avons $|(\mathbb{Z}/n\mathbb{Z})^\times| = \varphi(n)$, $\varphi(nm) = \varphi(n)\varphi(m)$ si $\text{pgcd}(n, m) = 1$ et $\varphi(p^e) = p^e - p^{e-1}$ si p est

premier et $e \geq 1$ un entier. Donc

$$|(\mathbb{Z}/18\mathbb{Z})^\times| = \varphi(18^3) = 18^3 - 18^2 = 8 - 4 = 4$$

$$|(\mathbb{Z}/27\mathbb{Z})^\times| = \varphi(27^3) = 27^3 - 27^2 = 27 - 6 = 21$$

$$\begin{aligned} |(\mathbb{Z}/216\mathbb{Z})^\times| &= \varphi(216) = \varphi(8 \cdot 27) \stackrel{\substack{\varphi(18) \cdot \varphi(27) \\ \text{pgcd}(18, 27) = 1}}{=} \\ &= 4 \cdot 21 = 84. \end{aligned}$$

- d) 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 ?

Calculons les puissances de $\bar{2}^{27}$ dans $(\mathbb{Z}/27\mathbb{Z})^\times$:

k	1	2	3	4	5	6	7	8	9
$\bar{2}^k$	$\bar{2}$	$\bar{4}$	$\bar{8}$	$\bar{16}$	$\bar{32} = \bar{5}$	$\bar{10}$	$\bar{20}$	$\bar{40} = \bar{13}$	$\bar{1}$

k	10	11	12	13	14	15	16	17	18
$\bar{2}^k$	$-\bar{2}$	$-\bar{4}$	$-\bar{8}$	$-\bar{16}$	$-\bar{5}$	$-\bar{10}$	$-\bar{20}$	$-\bar{13}$	$\bar{1}$

Il s'ensuit que $\bar{2}$ est d'ordre 18. Dans ce

tableau nous voyons aussi les puissances

$$\bar{8}^m = \bar{2}^{3m} :$$

k	1	2	3	4	5	6
$\bar{8}^k$	$\bar{8}$	$\bar{10}$	$-\bar{1}$	$-\bar{8}$	$-\bar{10}$	$\bar{1}$

Il s'ensuit que $\bar{8}$ est d'ordre 6.

Comme $\bar{2}$ est d'ordre 18 et $|(\mathbb{Z}/12\mathbb{Z})^\times| = 18$, le groupe $(\mathbb{Z}/12\mathbb{Z})^\times$ est formé des puissances de $\bar{2}$. Donc $\bar{2}$ est un générateur de ce groupe et $(\mathbb{Z}/12\mathbb{Z})^\times$ est bien un groupe cyclique.

- e) 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.

Nous avons vu dans d) que nous avons $\bar{8}^6 = \bar{1}$ dans $(\mathbb{Z}/12\mathbb{Z})^\times$. Donc nous avons $\bar{8}^{12} = (\bar{8}^6)^2 = \bar{1}$ dans $(\mathbb{Z}/12\mathbb{Z})^\times$. Par le lemme 2.26 du cours, il existe un unique morphisme de groupes

$$f: (\mathbb{Z}/12\mathbb{Z}, +) \rightarrow (\mathbb{Z}/27\mathbb{Z})^\times$$

tel que $f(12\bar{1}) = 27\bar{8}$ et nous avons $f(k) = \bar{8}^k$ pour tout $k \in \mathbb{Z}$. Nous obtenons le tableau

\mathbb{Z}	0	1	2	3	4	5	6	7	8	9	10	11
$f(k)$	7	8	10	-7	-8	-10	7	8	10	-7	-8	-10

Il s'ensuit que

$$\text{Im } f = \{7, 8, 10, -7, -8, -10\}$$

$$\text{Ker } f = \{0, 6\}.$$

Notons que nous avons $|\text{Im } f| \cdot |\text{Ker } f| = |Z/12Z|$.

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 $\text{ppcm}(a, b)$.

Disons que $M = \text{ppcm}(a, b) = ua = vb$. Comme G

est commutatif, nous avons

$$(xy)^M = \underbrace{(xy)(xy) \dots (xy)}_{M \text{ facteurs}} = \underbrace{(x \cdots x)(y \cdots y)}_{M \text{ facteurs}} = x^M y^M$$

Nous avons

$$x^M = x^{ua} = (x^a)^u = e^u = e \quad \text{et}$$

$$y^M = y^{vb} = (y^b)^v = e^v = e.$$

Donc $(xy)^M = x^M y^M = e$ et $\text{ord}(xy)$ divise M .