# Corrigé Examen Mai 2019

**Exercice 1.**

1. On a de façon immédiate

$$\sigma^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 \\ 8 & 6 & 3 & 10 & 1 & 2 & 4 & 5 & 12 & 11 & 7 & 9 \end{pmatrix}.$$

2. La décomposition de $\sigma$ en cycles à supports disjoints est la suivante :

$$\sigma = \begin{pmatrix} 1 & 5 & 8 \end{pmatrix} \begin{pmatrix} 2 & 6 \end{pmatrix} \begin{pmatrix} 4 & 7 & 11 & 10 \end{pmatrix} \begin{pmatrix} 9 & 12 \end{pmatrix}.$$

3. Puisque des cycles à supports disjoints commutent deux à deux, on a pour tout entier naturel $n$,

$$\sigma^n = \begin{pmatrix} 1 & 5 & 8 \end{pmatrix}^n \begin{pmatrix} 2 & 6 \end{pmatrix}^n \begin{pmatrix} 4 & 7 & 11 & 10 \end{pmatrix}^n \begin{pmatrix} 9 & 12 \end{pmatrix}^n.$$

Ainsi, le plus petit entier naturel $n$ non nul vérifiant $\sigma^n = \mathrm{id}$ est le plus petit entier naturel $n$ non nul tel qu'on ait simultanément

$$\begin{cases} \begin{pmatrix} 1 & 5 & 8 \end{pmatrix}^n = \mathrm{id} \\ \begin{pmatrix} 2 & 6 \end{pmatrix}^n = \mathrm{id} \\ \begin{pmatrix} 4 & 7 & 11 & 10 \end{pmatrix}^n = \mathrm{id} \\ \begin{pmatrix} 9 & 12 \end{pmatrix}^n = \mathrm{id}, \end{cases}$$

c'est à dire le ppcm des ordres des quatre cycles sus-mentionnés.
L'ordre de $\sigma$ est donc égal à $\mathrm{ppcm}(2, 3, 4) = 12$.

4. Puisque $\sigma$ est d'ordre 12, on écrit la division euclidienne de 2019 par 12 :

$$2019 = 12 \times 168 + 3.$$

On a donc

$$\begin{aligned} \sigma^{2019} &= (\sigma^{12})^{168}\sigma^3 \\ &= \mathrm{id}^{168} \begin{pmatrix} 1 & 5 & 8 \end{pmatrix}^3 \begin{pmatrix} 2 & 6 \end{pmatrix}^3 \begin{pmatrix} 4 & 7 & 11 & 10 \end{pmatrix}^3 \begin{pmatrix} 9 & 12 \end{pmatrix}^3 \\ &= \begin{pmatrix} 2 & 6 \end{pmatrix} \begin{pmatrix} 4 & 10 & 11 & 7 \end{pmatrix} \begin{pmatrix} 9 & 12 \end{pmatrix}. \end{aligned}$$

**Exercice 2.**

1. Pour résoudre l'équation $48x + 66y = 8$, on doit d'abord calculer le pgcd de 48 et 66. Pour cela, on utilise l'algorithme d'Euclide :

$$\begin{aligned} 66 &= 48 \times 1 + 18 \\ 48 &= 18 \times 2 + 12 \\ 18 &= 12 \times 1 + 6 \\ 12 &= 6 \times 2 + 0. \end{aligned}$$

Le pgcd est le dernier reste non nul qui est donc 6. Or, 6 ne divise pas 8 donc cette équation n'a pas de solution.

2. L'équation $48x + 66y = 6$ admet des solutions puisque $\text{pgcd}(48, 66) = 6$ divise 6.
   En divisant par 6, on obtient une nouvelle équation qui lui est équivalente :
$$8x + 11y = 1.$$
   On trouve une solution évidente $(x_0, y_0) = (-4, 3)$.
   Soit $(x, y)$ un autre couple de solutions. Alors on a
$$\begin{cases} 8x + 11y = 1 \\ 8x_0 + 11y_0 = 1. \end{cases}$$
   On soustrait les deux lignes et on obtient
$$8(x - x_0) + 11(y - y_0) = 0,$$
   ou encore
$$8(x - x_0) = 11(y_0 - y).(*)$$
   En particulier, 11 divise $8(x - x_0)$. Or, 11 et 8 sont premiers entre eux donc d'après le lemme de Gauss, 11 divise $x - x_0$.
   Il existe donc un entier relatif $k$ tel que
$$11k = x - x_0.$$
   En injectant ceci dans l'égalité (*), on trouve
$$8 \times 11k = 11(y_0 - y),$$
   i.e.
$$8k = y_0 - y.$$
   Finalement, on trouve les solutions
$$\begin{cases} x = x_0 + 11k \\ y = y_0 - 8k. \end{cases}, k \in \mathbb{Z},$$
   ou encore
$$\begin{cases} x = -4 + 11k \\ y = 3 - 8k. \end{cases}, k \in \mathbb{Z}$$

**Exercice 3.**

1. Calculons le reste de $3^{2019}$ dans la division euclidienne par 21.
   Pour cela, on remarque que modulo 21,
   $3^3 \equiv 6[21]$, $3^4 \equiv -3[21]$, $3^5 \equiv 12[21]$, $3^6 \equiv -6[21]$, $3^7 \equiv 3[21]$.
   Par une récurrence immédiate, on voit que pour tout entier naturel $n$,
$$3^{6n+1} \equiv 3[21].$$
   Effectuons la division euclidienne de 2019 par 6 :
$$2019 = 6 \times 336 + 3.$$
   Ainsi,
$$\begin{aligned} 3^{2019} &\equiv 3^{6\times 336+1} \times 3^2[21] \\ &\equiv 3 \times 3^2[21] \\ &\equiv 6[21]. \end{aligned}$$

Le reste de $3^{2019}$ dans la division euclidienne par 21 est donc 6.
Calculons maintenant le reste de $3^{2019}$ dans la division euclidienne par 80.
On remarque que $3^4 \equiv 1[80]$ donc par une récurrence immédiate, pour tout entier naturel $n$,

$$3^{4n} \equiv 1[80].$$

On effecute la division euclidienne de 2019 par 4 :

$$2019 = 4 \times 504 + 3.$$

Ainsi,

$$\begin{aligned} 3^{2019} &\equiv (3^4)^{504} 3^3 [80] \\ &\equiv 1 \times 3^3 [80] \\ &\equiv 27[80]. \end{aligned}$$

Le reste de $3^{2019}$ dans la division euclidienne par 80 est donc 27.

2. Puisque 21 et 80 sont premiers entre eux, d'après le théorème chinois, ce système admet une unique solution modulo $21 \times 80 = 1680$.
   On remarque facilement que $x = 27$ convient. La solution de ce système est donc

$$x \equiv 27[1680]$$

.

3. D'après la question 1, on a simultanément

$$\begin{cases} 3^{2019} \equiv 6[21] \\ 3^{2019} \equiv 27[80] \end{cases}.$$

   Or, d'après la question 2, ceci équivaut à dire que

$$3^{2019} \equiv 27[1680].$$

   Le reste de la division euclidienne de $3^{2019}$ par 1680 est donc 27.

**Exercice 4.**

1. On rappelle que pour tout $k \in \mathbb{Z}$, l'ordre de $\overline{k}$ dans $(\mathbb{Z}/n\mathbb{Z}, +)$ est donné par $\dfrac{n}{\text{pgcd}(n,k)}$.
   Ainsi, l'ordre de $\overline{16}$ dans $(G, +)$ est égal à $\dfrac{20}{\text{pgcd}(20,16)} = \dfrac{20}{4} = 5$.
2. On sait que $G^\times = \{\overline{k} \in G | \text{pgcd}(20,k) = 1\}$.
   Or, $\text{pgcd}(20,16) = 4$ donc $\overline{16} \notin G^\times$.
3. 17 et 20 sont premiers entre eux (puisque 17 est lui-même premier), donc $\overline{17} \in G^\times$.
   Pour déterminer l'inverse de $\overline{17}$ dans $G^\times$, il suffit d'établir une relation de Bézout entre 17 et 20.
   On a

$$6 \times 20 - 7 \times 17 = 1.$$

   Lue dans $\mathbb{Z}/20\mathbb{Z}$, cette égalité donne

$$-\overline{7} \times \overline{17} = \overline{1},$$

   donc l'inverse de $\overline{17}$ dans $G^\times$ est $\overline{-7}$=$\overline{13}$.

4. Par définition,
$$G^\times = \{\overline{k} \in G | \mathrm{pgcd}(20, k) = 1\}.$$
Il s'ensuit que
$$|G^\times| = |\{1 \leq k \leq 20 | \mathrm{pgcd}(20, k) = 1\}|,$$
ce qui est égal à $\varphi(20)$ par définition, où $\varphi$ désigne l'indicatrice d'Euler.
Or, 4 et 5 étant premiers entre eux,
$\varphi(20) = \varphi(4)\varphi(5) = 2 \times 4 = 8$.
Le cardinal de $G^\times$ est donc égal à 8.
5. Puisque 4 et 5 sont premiers entre eux, d'après le théorème chinois, on a un isomorphisme de groupes
$$\mathbb{Z}/20\mathbb{Z} \simeq \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}.$$
L'isomorphisme est donné explicitement par la formule suivante
$$k \bmod 20 \mapsto (k \bmod 4, k \bmod 5).$$
6. Puisque $G \simeq \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}$, on a
$$G^\times \simeq (\mathbb{Z}/4\mathbb{Z})^\times \times (\mathbb{Z}/5\mathbb{Z})^\times.$$
Or, $(\mathbb{Z}/4\mathbb{Z})^\times = \{\overline{1}, \overline{3}\} \simeq \mathbb{Z}/2\mathbb{Z}$.
D'autre part,
$$(\mathbb{Z}/5\mathbb{Z})^\times = \{\overline{1}, \overline{2}, \overline{3}, \overline{4}\}.$$
C'est un groupe à 4 éléments qui contient un élément d'ordre 4 : en effet, $\overline{2}$ est d'ordre 4 dans $(\mathbb{Z}/5\mathbb{Z})^\times$ puisque $\overline{2}^1 = \overline{2}$, $\overline{2}^2 = \overline{4}$, $\overline{2}^3 = \overline{8}$ et $\overline{2}^4 = \overline{16} = \overline{1}$.
$(\mathbb{Z}/5\mathbb{Z})^\times$ est cyclique d'ordre 4 et est donc isomorphe à $\mathbb{Z}/4\mathbb{Z}$.
Finalement, on a bien
$$G^\times \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}.$$
7. $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$ est un groupe d'ordre 8 mais n'est pas cyclique car il ne contient pas d'élément d'ordre 8. En effet, pour tout $(\overline{a}, \overline{b}) \in \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$, on a
$$4.(\overline{a}, \overline{b}) = (4\overline{a}, 4\overline{b}) = (\overline{0}, \overline{0}),$$
donc tout élément est d'ordre au plus 4.
$G^\times$ n'est donc pas cyclique.

**Exercice 5.** Soit $(a, b)$ et $(a', b')$ deux couples d'entiers.
On a
$$\begin{aligned} f((a,b) + (a',b')) &= f(a + a', b + b') \\ &= a + a' + (b + b')\sqrt{5} \\ &= (a + b\sqrt{5}) + (a' + b'\sqrt{5}) \\ &= f(a,b) + f(a',b'), \end{aligned}$$
ce qui prouve que $f$ est un morphisme de groupes d'image $H$ (qui est donc bien un sous-groupe de $\mathbb{R}$ comme image d'un groupe par un morphisme de groupes) et de noyau
$K = \{(a, b) \in \mathbb{Z}^2 | a + b\sqrt{5} = 0\} = \{(0, 0)\}$. (En effet, si $b \neq 0$ et $a + b\sqrt{5} = 0$, $a$ ne peut pas être un entier...)

**Exercice 6.**

1. Soit $d \in \mathbb{Z}$ premier avec $(p-1)(q-1)$. Alors d'après le théorème de Bézout, il existe $(e, f) \in \mathbb{Z}^2$ tels que
$$de + (p-1)(q-1)f = 1,$$
ce qui donne
$$de \equiv 1[(p-1)(q-1)].$$

2. Soit $t \in \mathbb{Z}$. Si $t$ est divisible par $p$, alors le résultat est trivial.
Supposons que $t$ ne soit pas divisible par $p$. Puisque $p$ est premier, cela revient à dire que $t$ et $p$ sont premiers entre eux.
D'après le petit théorème de Fermat, on a donc
$$t^{p-1} \equiv 1[p].$$
Or, d'après la question 1, on sait que $p-1$ divise $de-1$ donc il existe $k \in \mathbb{Z}$ tel que $k(p-1) = de-1$.
Ainsi, $t^{de-1} = (t^{p-1})^k$. Il s'ensuit que
$$t^{de-1} \equiv (t^{p-1})^k [p],$$
i.e.
$$t^{de-1} \equiv 1[p],$$
d'où
$$t^{de} \equiv t[p].$$
Finalement, on a bien montré que pour tout $t \in \mathbb{Z}$,
$$t^{de} \equiv t[p].$$

3. De façon similaire, on trouve que pour tout $t \in \mathbb{Z}$,
$$t^{de} \equiv t[q].$$
Ainsi, $p$ et $q$ divisent $t^{de} - t$ pour tout $t \in \mathbb{Z}$ et sont premiers entre eux (puisque ce sont deux nombres premiers distincts).
D'après le lemme d'Euclide, on en déduit que $n = pq$ divise $t^{de} - t$ pour tout $t \in \mathbb{Z}$.
On peut donc conclure que pour tout $t \in \mathbb{Z}$,
$$t^{de} \equiv t[n].$$