Corrigé Devoir Surveillé MAT 309 n°2

Durée : 1h. Calculatrices et feuille manuscrite A4 recto-verso autorisées.
Toutes les réponses doivent être justifiées. La qualité de la rédaction sera prise en compte.

Exercice 1 : (*6 points*) On se place dans $\mathbb{Z}/13\mathbb{Z}$.

1. Quels sont les ordres possibles des éléments de $\mathbb{Z}/13\mathbb{Z}^*$.
2. Déterminer l'ordre de $\overline{10}$.
3. En déduire le reste dans la division euclidienne de 10^{139} par 13.
4. Montrer que $\overline{2}$ est un générateur de $\mathbb{Z}/13\mathbb{Z}^*$. Déterminer les autres générateurs.

Corrigé :

1. Le cardinal du groupe $\mathbb{Z}/13\mathbb{Z}^*$ vaut $\varphi(13) = 12$, donc par le théorème de Lagrange l'ordre d'un élément divise 12 : les ordres possibles sont $1, 2, 3, 4, 6, 12$.
2. Pour déterminer l'ordre de $\overline{10}$, on calcule les valeurs de $\overline{10}^k$ pour $k \in \{2, 3, 4, 6, 12\}$. On a
$$\overline{10}^2 = \overline{9},\ \overline{10}^3 = \overline{12},\ \overline{10}^4 = \overline{3},\ \overline{10}^6 = \overline{1}$$
donc l'ordre de $\overline{10}$ est 6.
3. On a $139 = 23 \cdot 6 + 1$ donc l'égalité suivante est vérifiée dans $\mathbb{Z}/13\mathbb{Z}$:
$$\overline{10}^{139} = (\overline{10}^6)^{23} \times \cdot\overline{10} = \overline{1}^{23} \cdot \overline{10} = \overline{10}$$
d'où l'on en déduit que le reste dans la division euclidienne de 10^{139} par 13 est 10.
4. D'après le cours, pour montrer que $\overline{2}$ est un générateur de $\mathbb{Z}/13\mathbb{Z}^*$, il suffit de vérifier que $\overline{2}^{\frac{12}{2}} \neq \overline{1}$ et $\overline{2}^{\frac{12}{3}} \neq 1$ puisque 2 et 3 sont les diviseurs premiers de 12. C'est le cas puisque $\overline{2}^4 = \overline{3}$ et $\overline{2}^6 = \overline{12}$.
Par propriété de cours, les autres générateurs sont de la forme $\overline{2}^k$ où k est un entier premier avec $\varphi(13) = 12$, d'où $k \in \{5, 7, 11\}$. Les autres générateurs sont donc
$$\overline{2}^5 = \overline{6},\ \overline{2}^7 = \overline{11},\ \overline{2}^{11} = \overline{7}.$$

Exercice 2 : (*6 points + Bonus*)

1. En utilisant l'algorithme d'exponentiation rapide, déterminer le reste dans la division euclidienne de 2^{90} par 91.
2. A quel test de primalité correspond ce résultat ? Quel témoin ou menteur vient-on d'exhiber pour 91 ?
3. (a) Montrer que le système de congruence
$$\begin{cases} x \equiv 1[7] \\ x \equiv 12[13] \end{cases}$$
équivaut à une unique congruence modulo $7 \times 13 = 91$ que l'on déterminera.
   (b) Vérifier que les restes dans les divisions euclidiennes de 2^{90} par 7 et 13 sont respectivement 1 et 12.
4. *Bonus :* On note $o(\overline{x})_n$ l'ordre d'un élément $\overline{x} \in \mathbb{Z}/n\mathbb{Z}^*$ pour $n \in \{7, 13, 91\}$. Montrer que
$$o(\overline{x})_{91} \mid \text{ppcm}(o(\overline{x})_7, o(\overline{x})_{13}).$$
En déduire que $\mathbb{Z}/91\mathbb{Z}^*$ n'admet pas de générateur.

Corrigé :

1. La décomposition binaire de 90 est 1011010. Donc en partant de 1 et en lisant cette décomposition de la gauche vers la droite, on va multiplier par 2 et mettre au carré modulo 91 lorsqu'on a un 1, et mettre au carré modulo 91 lorsqu'on a un 0. Dans $\mathbb{Z}/91\mathbb{Z}$, on a :
$$\overline{2}^0 = \overline{1}, \quad \overline{2}^1 = \overline{2}, \quad \overline{2}^2 = \overline{4}, \quad \overline{2}^5 = \overline{2} \cdot (\overline{4}^2) = \overline{32}, \quad \overline{2}^{11} = \overline{2} \cdot (\overline{32})^2 = \overline{46},$$
$$\overline{2}^{22} = \overline{46}^2 = \overline{23}, \quad \overline{2}^{45} = \overline{2} \cdot (\overline{23})^2 = \overline{57}, \quad \overline{2}^{90} = \overline{57}^2 = \overline{64}.$$
Donc le reste dans la division euclidienne de 2^{90} par 91 est 64.
2. Puisque $\mathrm{pgcd}(2, 91) = 1$ mais que $\overline{2}^{90} = \overline{64} \neq \overline{1}$, l'entier 91 ne passe pas le test de Fermat et donc n'est pas premier, et 2 est un témoin de Fermat pour $n = 91$.
3. (a) Puisque 7 et 13 sont premiers entre eux, ce système admet des solutions d'après le théorème des restes chinois, égales modulo $7 \times 13 = 91$. Une identité de Bézout entre 7 et 13 est $2 \times 7 - 1 \times 13 = 1$ donc une solution particulière de ce système est $1 \times 13 \times (-1) + 12 \times 7 \times 2 = 155$, et la solution dans l'intervalle $[\![0, 90]\!]$ est $155 - 91 = 64$.

   (b) A partir du reste dans la division euclidienne de 2^{90} par 91 qui vaut 64, on retrouve les restes dans les divisions euclidiennes par 7 et 13 puisque $64 \equiv 1[7]$ et $64 \equiv 12[13]$.

   Autrement, on peut constater que par la bijection $f : \mathbb{Z}/91\mathbb{Z} \to \mathbb{Z}/7\mathbb{Z} \times \mathbb{Z}/13\mathbb{Z}$ donnée par les restes chinois, l'antécédant du couple $(\overline{1}, \overline{12})$ est $\overline{64}$, donc un élément dont le reste modulo 91 vaut 64 a pour reste 1 modulo 7 et 12 modulo 13.
4. Soit $\overline{x} \in \mathbb{Z}/91\mathbb{Z}^*$, notons a son ordre dans $\mathbb{Z}/7\mathbb{Z}^*$ et b son ordre dans $\mathbb{Z}/13\mathbb{Z}^*$, c'est à dire
$$\overline{x}^a = \overline{1} \text{ dans } \mathbb{Z}/7\mathbb{Z} \text{ et } \overline{x}^b = \overline{1} \text{ dans } \mathbb{Z}/13\mathbb{Z}.$$
Notons $c = \mathrm{ppcm}(a, b)$, d'où a divise c et b divise c : il existe des entiers a' et b' tels que $c = aa' = bb'$. Par la bijection des restes chinois, on a alors
$$\overline{x}^c = (\overline{x}^c, \overline{x}^c) = (\overline{x}^{aa'}, \overline{x}^{bb'}) = ((\overline{x}^a)^{a'}, (\overline{x}^b)^{b'}) = (\overline{1}^{a'}, \overline{1}^{b'}) = (\overline{1}, \overline{1})$$
et donc par bijection, puisque $\overline{1}$ est l'unique antécédent dans $\mathbb{Z}/91\mathbb{Z}$ du couple $(\overline{1}, \overline{1})$, on a $\overline{x}^c = \overline{1}$ dans $\mathbb{Z}/91\mathbb{Z}$. Donc l'ordre de $\overline{x}$ dans $\mathbb{Z}/91\mathbb{Z}^*$ divise c. Ainsi, on ne peut pas avoir d'élément d'ordre $\varphi(91) = 6 \cdot 12 = 72$ car si $\overline{x}$ est un élément d'ordre 6 dans $\mathbb{Z}/7\mathbb{Z}^*$ et $\overline{x}$ est un élément d'ordre 12 dans $\mathbb{Z}/13\mathbb{Z}^*$, alors l'ordre de $\overline{x}$ dans $\mathbb{Z}/91\mathbb{Z}^*$ divise $\mathrm{ppcm}(6, 12) = 12$ et donc sera plus petit que 12.

Exercice 3 : (*6 points*) Un professeur P décide d'envoyer ses notes par mail au secrétariat S de l'Université en utilisant un codage RSA. La clé publique de chiffrement est $(c = 3, n = 33)$.

1. Quel message chiffré correspond à la note 13 ?
2. Vérifier que la clé privée de déchiffrement est 7.
3. Si S reçoit le message chiffré "9", à quelle note cela correspond ?
4. Supposons désormais que la clé publique de chiffrement soit $(c = 3, n = 55)$. Quelle est alors la clé privée de déchiffrement ?

Corrigé :

1. Pour chiffrer la note 13, on calcule $13^3[33] = 19$.
2. La clé privée de déchiffrement d doit vérifier $ed \equiv 1[\varphi(n)]$. Or $n = 33 = 3 \cdot 11$ donc $\varphi(n) = 2 \cdot 10 = 20$ et $3 \cdot 7 = 21 \equiv 1[20]$ donc la clé privée est bien 7.
3. Pour déchiffrer le message 9, on calcule $9^7[33] = 15$ en utilisant par exemple l'algorithme d'exponentiation rapide.
4. Supposons maintenant que la clé publique est $(c = 3, n = 55)$, on a alors $\varphi(n) = 4 \cdot 10 = 40$ et on cherche donc l'inverse de 3 dans $\mathbb{Z}/40\mathbb{Z}$ (qui existe car 3 est premier avec 40). Pour ceci, on détermine une égalité de Bézout entre 3 et 40 :
$$1 = 1 \times 40 - 13 \times 3$$
donc l'inverse est $\overline{-13} = \overline{27}$ dans $\mathbb{Z}/40\mathbb{Z}$. Dans ce cas, la clé privée est donc 27.

Exercice 4 : (*6 points*)

1. Montrer que pour tout $n \in \mathbb{N}$, on a
   (a) $n^5 \equiv n[2]$,
   (b) $n^5 \equiv n[3]$,
   (c) $n^5 \equiv n[5]$.

   Indication : Pour chacune de ces questions, on pourra séparer les cas $\overline{n} = \overline{0}$ et $\overline{n} \neq \overline{0}$ dans $\mathbb{Z}/2\mathbb{Z}$, $\mathbb{Z}/3\mathbb{Z}$ et $\mathbb{Z}/5\mathbb{Z}$ respectivement.
2. En déduire que pour tout $n \in \mathbb{N}$,
$$n^5 \equiv n[30].$$

Corrigé :

1. (a) Soit $\overline{n} \in \mathbb{Z}/2\mathbb{Z}$. Si $\overline{n} = 0$, alors $\overline{n}^5 = \overline{0}$ et donc $n^5 \equiv n[2]$. Sinon, alors $\overline{n} = \overline{1}$, et on a alors $\overline{1}^5 = \overline{1}$.
   (b) Soit $\overline{n} \in \mathbb{Z}/3\mathbb{Z}$. Si $\overline{n} = 0$, alors $\overline{n}^5 = \overline{0}$ et donc $n^5 \equiv n[3]$. Sinon, alors $\overline{n} = \overline{1}, \overline{2}$ est inversible dans $\mathbb{Z}/3\mathbb{Z}$ et d'après le théorème de Euler-Fermat on a alors $\overline{n}^{\varphi(3)} = \overline{n}^2 = \overline{1}$. D'où $\overline{n}^5 = (\overline{n}^2)^2 \cdot \overline{n} = \overline{n}$, ce qui implique que $n^5 \equiv n[3]$.
   (c) Soit $\overline{n} \in \mathbb{Z}/5\mathbb{Z}$. Si $\overline{n} = 0$, alors $\overline{n}^5 = \overline{0}$ et donc $n^5 \equiv n[5]$. Sinon, alors $\overline{n}$ est inversible dans $\mathbb{Z}/5\mathbb{Z}$ et d'après le théorème de Euler-Fermat on a alors $\overline{n}^{\varphi(5)} = \overline{n}^4 = \overline{1}$. D'où $\overline{n}^5 = \overline{n}^4 \cdot \overline{n} = \overline{n}$, ce qui implique que $n^5 \equiv n[5]$.
2. Puisque 2,3 et 5 sont premiers entre eux deux à deux, d'après le théorème des restes chinois on a une fonction bijective $f : \mathbb{Z}/30\mathbb{Z} \to \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}$, $\overline{n} \mapsto (\overline{n}, \overline{n}, \overline{n})$.
   Soit $n \in \mathbb{N}$, alors on a
$$\begin{aligned} f(\overline{n}^5) &= (\overline{n}^5, \overline{n}^5, \overline{n}^5) \in \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z} \\ &= (\overline{n}, \overline{n}, \overline{n}) \text{ d'après la question 1.} \end{aligned}$$
   Or $\overline{n}$ est un antécédent du triplet $(\overline{n}, \overline{n}, \overline{n})$ par f et donc, par bijection, on en déduit que $\overline{n}^5 = \overline{n}$. Ceci étant vrai pour tout n, on obtient $n^5 \equiv n[30]$.