

Corrigé du contrôle de maths L2 : arithmétique et anneau $\mathbb{Z}/n\mathbb{Z}$

Barème du contrôle

Exercice	Points
Exercice 1 : Question de cours : inversibles de $\mathbb{Z}/n\mathbb{Z}$	3 points
Exercice 2 : Algorithme d'Euclide étendu	4 points
Exercice 3 : Grandes puissances modulo n	4 points
Exercice 4 : Lemme chinois	4 points
Exercice 5 : Problème : le chiffrement RSA	5 points
Total	20 points

Exercice 1 : Question de cours : inversibles de $\mathbb{Z}/n\mathbb{Z}$ (3 points)

- a. Supposons $k \wedge n = 1$. D'après le théorème de Bézout, il existe $u, v \in \mathbb{Z}$ tels que $ku + nv = 1$. En passant aux classes modulo n , on obtient $\bar{k}\bar{u} = \bar{1}$, car $\bar{nv} = \bar{0}$. Donc $\bar{k}$ est inversible, d'inverse $\bar{u}$.

Réciproquement, supposons qu'il existe u tel que $\bar{k}\bar{u} = \bar{1}$. Alors n divise $ku - 1$: il existe $v \in \mathbb{Z}$ tel que $ku - 1 = nv$, soit $ku - nv = 1$. Tout diviseur commun de k et n divise donc 1 . Par conséquent, **$\bar{k}$ est inversible si et seulement si $k \wedge n = 1$** .

- b. L'anneau $\mathbb{Z}/n\mathbb{Z}$ est commutatif et non nul car $n \geq 2$. C'est donc un corps si et seulement si toute classe non nulle $\bar{k}$, avec $1 \leq k \leq n-1$, est inversible.

Si n est premier, tout k compris entre 1 et $n - 1$ vérifie $k \wedge n = 1$, car les seuls diviseurs positifs de n sont 1 et n . D'après a, $\bar{k}$ est inversible : $\mathbb{Z}/n\mathbb{Z}$ est un corps.

Si n n'est pas premier, on écrit $n = ab$ avec $1 < a, b < n$. Alors $\bar{a} \neq \bar{0}$ et $\bar{a}\bar{b} = \bar{0}$ avec $\bar{b} \neq \bar{0}$. Ainsi $\bar{a}$ est un diviseur de zéro, donc il n'est pas inversible. $\mathbb{Z}/n\mathbb{Z}$ **est un corps si et seulement si n est premier.**

Barème : a) 0,75 point par implication, Bézout cité ; b) 0,75 point pour le sens direct, 0,75 point pour le contre-exemple de diviseur de zéro.

Exercice 2 : Algorithme d'Euclide étendu (4 points)

a. On effectue les divisions euclidiennes successives :

$$97 = 2 \times 35 + 27$$

$$35 = 1 \times 27 + 8$$

$$27 = 3 \times 8 + 3$$

$$8 = 2 \times 3 + 2$$

$$3 = 1 \times 2 + 1$$

Le dernier reste non nul vaut 1, donc $97 \wedge 35 = 1$.

b. On remonte les égalités en partant de la dernière :

$$1 = 3 - 2 = 3 - (8 - 2 \times 3) = 3 \times 3 - 8$$

$$1 = 3 \times (27 - 3 \times 8) - 8 = 3 \times 27 - 10 \times 8$$

$$1 = 3 \times 27 - 10 \times (35 - 27) = 13 \times 27 - 10 \times 35$$

$$1 = 13 \times (97 - 2 \times 35) - 10 \times 35 = 13 \times 97 - 36 \times 35$$

Donc $u = 13$ et $v = -36$ conviennent. Vérification : $13 \times 97 = 1261$ et $36 \times 35 = 1260$.

- c. En réduisant modulo 97, on obtient $-36 \times 35 \equiv 1 \pmod{97}$. Ainsi $\overline{35}^{-1} = \overline{-36} = \overline{61}$ dans $\mathbb{Z}/97\mathbb{Z}$. Ensuite, $35x \equiv 4 \pmod{97}$ équivaut à $x \equiv 4 \times 61 = 244 \pmod{97}$, car on peut multiplier par l'inverse. Or $244 = 2 \times 97 + 50$. Les solutions sont donc **les entiers** $x = 50 + 97k$, $k \in \mathbb{Z}$. Vérification : $35 \times 50 = 1750 = 18 \times 97 + 4$.
- d. Soit (u, v) une solution. En soustrayant $97 \times 13 + 35 \times (-36) = 1$, on obtient $97(u - 13) = -35(v + 36)$. Donc 35 divise $97(u - 13)$; comme $35 \wedge 97 = 1$, le lemme de Gauss donne $35 \mid u - 13$. On écrit $u = 13 + 35k$, puis $v = -36 - 97k$. Réciproquement, ces couples sont solutions, car $97 \times 35k - 35 \times 97k = 0$. **Les solutions sont les couples** $(13 + 35k, -36 - 97k)$, $k \in \mathbb{Z}$.

Barème : a) 1 point ; b) 0,5 point pour la remontée, 0,5 point pour le couple vérifié ; c) 0,5 point pour l'inverse, 0,5 point pour les solutions ; d) 0,5 point pour Gauss, 0,5 point pour la réciproque et la conclusion.

Exercice 3 : Grandes puissances modulo n (4 points)

- a. Pour $n \geq 1$, $\varphi(n)$ est le nombre d'entiers $k \in \{1, \dots, n\}$ premiers avec n . C'est aussi le cardinal de $(\mathbb{Z}/n\mathbb{Z})^\times$. Comme $100 = 2^2 \times 5^2$, la formule $\varphi(n) = n \prod_{p \mid n} \left(1 - \frac{1}{p}\right)$ donne $\varphi(100) = 100 \times \frac{1}{2} \times \frac{4}{5}$, soit $\varphi(100) = 40$.
- b. **Théorème d'Euler** : si $a \wedge n = 1$, alors $a^{\varphi(n)} \equiv 1 \pmod{n}$. Comme $7 \wedge 100 = 1$, on a

$7^{40} \equiv 1 \pmod{100}$. Par ailleurs $7^2 = 49$ et $7^4 = 49^2 = 2401$, donc $7^4 \equiv 1 \pmod{100}$. De plus $7^1 \equiv 7$, $7^2 \equiv 49$ et $7^3 = 343 \equiv 43$ ne valent pas 1 modulo 100. **L'ordre de 7 est donc 4**, qui divise bien 40 comme le veut le théorème de Lagrange.

c. On effectue la division $2026 = 4 \times 506 + 2$. Alors

$7^{2026} = (7^4)^{506} \times 7^2 \equiv 1 \times 49 \pmod{100}$. **Les deux derniers chiffres de 7^{2026} sont 4 et 9.**

d. Le nombre 13 est premier et ne divise pas 2. D'après le petit théorème de Fermat,

$2^{12} \equiv 1 \pmod{13}$. Or $2026 = 12 \times 168 + 10$, donc $2^{2026} \equiv 2^{10} \pmod{13}$. Ensuite $2^4 = 16 \equiv 3$, donc $2^8 \equiv 9$ et $2^{10} \equiv 9 \times 2 = 18 \equiv 5 \pmod{13}$. **Le reste cherché est 5.** Vérification : $2^{10} = 1024 = 78 \times 13 + 5$.

Erreur fréquente : réduire l'exposant modulo 100 au lieu de le réduire modulo l'ordre de la classe, ou modulo $\varphi(100)$.

Barème : a) 0,5 point pour la définition, 0,5 point pour la valeur ; b) 0,5 point pour Euler, 0,5 point pour l'ordre ; c) 1 point ; d) 0,5 point pour Fermat et la réduction de l'exposant, 0,5 point pour le reste.

Exercice 4 : Lemme chinois (4 points)

a. **Théorème chinois :** si m_1, m_2, m_3 sont deux à deux premiers entre eux et $m = m_1 m_2 m_3$, l'application

$$\mathbb{Z}/m\mathbb{Z} \rightarrow \mathbb{Z}/m_1\mathbb{Z} \times \mathbb{Z}/m_2\mathbb{Z} \times \mathbb{Z}/m_3\mathbb{Z}, x \bmod m \rightarrow (x \bmod m_1, x \bmod m_2, x \bmod m_3)$$

est bien définie et c'est un **isomorphisme d'anneaux**.

b. Les nombres 3, 5, 7 sont premiers deux à deux, donc le système admet une unique solution modulo 105. Les conditions $x \equiv 2 \pmod{3}$ et $x \equiv 2 \pmod{7}$ signifient que 3 et 7 divisent $x - 2$. Comme $3 \wedge 7 = 1$, elles équivalent à $21 \mid x - 2$, c'est-à-dire $x = 2 + 21k$ avec $k \in \mathbb{Z}$.

Ensuite, $2 + 21k \equiv 3 \pmod{5}$ équivaut à $k \equiv 1 \pmod{5}$, car $21 \equiv 1 \pmod{5}$. On pose $k = 1 + 5j$, d'où $x = 23 + 105j$.

Les solutions sont les entiers $x = 23 + 105j$, $j \in \mathbb{Z}$. Vérification :
 $23 = 7 \times 3 + 2 = 4 \times 5 + 3 = 3 \times 7 + 2$.

- c. Un isomorphisme d'anneaux envoie les inversibles sur les inversibles. De plus, un triplet est inversible dans l'anneau produit si et seulement si chacune de ses composantes l'est. Donc $(\mathbb{Z}/105\mathbb{Z})^\times$ est en bijection avec $(\mathbb{Z}/3\mathbb{Z})^\times \times (\mathbb{Z}/5\mathbb{Z})^\times \times (\mathbb{Z}/7\mathbb{Z})^\times$. Ainsi $\mathbb{Z}/105\mathbb{Z}$ possède $2 \times 4 \times 6 = 48$ **éléments inversibles**, c'est-à-dire $\varphi(105) = 48$.

Barème : a) 1 point ; b) 0,5 point pour la réduction modulo 21, 1 point pour $x \equiv 23$, 0,5 point pour l'ensemble des solutions ; c) 0,5 point pour la justification, 0,5 point pour le résultat.

Exercice 5 : Problème : le chiffrement RSA (5 points)

- a. Les nombres 11 et 17 sont premiers et distincts, donc $\varphi(187) = 10 \times 16 = 160$. Comme $160 = 2^5 \times 5$ et que 7 est premier, on a $7 \wedge 160 = 1$, donc $\bar{7}$ est inversible dans $\mathbb{Z}/160\mathbb{Z}$. Enfin $7 \times 23 = 161 = 160 + 1$. Donc $d = 23$.
- b. On a $ed = 1 + k\varphi(n) = 1 + k(p-1)(q-1)$ avec $k \geq 0$; ici $ed = 161$ et $k = 1$.

Si p divise m , alors $m^{ed} \equiv 0 \equiv m \pmod{p}$.

Sinon, le petit théorème de Fermat donne $m^{p-1} \equiv 1 \pmod{p}$. Donc
 $m^{ed} = m \times (m^{p-1})^{k(q-1)} \equiv m \times 1 \pmod{p}$. Dans les deux cas,
 $m^{ed} \equiv m \pmod{p}$.

- c. Par symétrie des rôles, on a aussi $m^{ed} \equiv m \pmod{q}$. Ainsi p et q , premiers entre eux, divisent $m^{ed} - m$, donc leur produit n le divise aussi. Par conséquent,
 $m^{ed} \equiv m \pmod{n}$. Alice calcule alors $c^d \equiv m^{ed} \equiv m \pmod{n}$. Comme
 $0 \leq m < n$, **le message m est le reste de c^d modulo n** : Alice le retrouve grâce à sa

clé secrète d .

d. On a $2^7 = 128 < 187$, donc $c = 128$.

Modulo 11 : $128 = 11 \times 11 + 7$, donc $c \equiv 7$. Par Fermat, $7^{10} \equiv 1$, d'où
 $7^{23} \equiv 7^3 = 343 = 31 \times 11 + 2$. Ainsi $c^{23} \equiv 2 \pmod{11}$.

Modulo 17 : $128 = 7 \times 17 + 9$, donc $c \equiv 9$. Par Fermat, $9^{16} \equiv 1$, d'où $9^{23} \equiv 9^7$.
Or $9^2 = 81 \equiv -4$ et $9^4 \equiv 16 \equiv -1$, donc
 $9^7 \equiv (-1) \times (-4) \times 9 = 36 \equiv 2 \pmod{17}$.

Ainsi $c^{23} - 2$ est divisible par 11 et par 17, donc par 187 : $c^d \equiv 2 \pmod{187}$, et Alice retrouve bien le message de Bob.

Barème : a) 0,5 point pour $\varphi(n)$, 0,5 point pour d ; b) 0,5 point pour le cas $p \mid m$, 1 point pour le cas général avec Fermat ; c) 0,5 point pour le passage à n , 0,5 point pour le déchiffrement ; d) 0,5 point pour c , 0,5 point par module.

[Revenir à l'énoncé du contrôle](#)

Après le corrigé du contrôle : arithmétique et anneau $\mathbb{Z}/n\mathbb{Z}$

Pour consolider ce que le corrigé vous a appris, relisez le cours « [Arithmétique et \$\mathbb{Z}/n\mathbb{Z}\$ en L2](#) puis entraînez-vous avec les **exercices corrigés** [arithmétique et \$\mathbb{Z}/n\mathbb{Z}\$](#) .

Retrouvez tous les [contrôles de maths de L2 classés par chapitre](#), ou choisissez un autre niveau sur la page [contrôles de maths du CP au post-bac](#).