

Corrigé du contrôle de maths L1 : arithmétique, Bézout, Gauss et congruences

Barème du contrôle

Exercice	Points
Exercice 1 : Question de cours : le lemme de Gauss	3 points
Exercice 2 : Algorithme d'Euclide étendu et équation diophantienne	6 points
Exercice 3 : Décomposition en facteurs premiers	3 points
Exercice 4 : Congruences et petit théorème de Fermat	3 points
Exercice 5 : Problème : un trésor et des restes	5 points
Total	20 points

Exercice 1 : Question de cours : le lemme de Gauss (3 points)

- a. **Théorème de Bézout.** Deux entiers a et b sont premiers entre eux si et seulement s'il existe des entiers u et v tels que $au + bv = 1$. Plus généralement, pour tous entiers a et b non tous deux nuls, il existe $u, v \in \mathbb{Z}$ tels que $au + bv = \text{pgcd}(a, b)$.
- b. **Lemme de Gauss.** Si a divise bc et si a est premier avec b , alors a divise c .

Démonstration. Comme a et b sont premiers entre eux, le théorème de Bézout fournit $u, v \in \mathbb{Z}$ tels que $au + bv = 1$. En multipliant par c , on obtient :

$$c = a (u c) + (b c) v.$$

Or a divise $a (u c)$, et a divise $b c$ par hypothèse, donc a divise $(b c) v$. Ainsi a divise la somme, c'est-à-dire c . **Donc** $a \mid c$.

Barème : a) 1 point (0,5 pour l'équivalence, 0,5 pour la forme générale avec le pgcd) ; b) 0,5 point pour l'énoncé, 1,5 point pour la démonstration (relation de Bézout multipliée par c , conclusion).

Exercice 2 : Algorithme d'Euclide étendu et équation diophantienne (6 points)

- a. On part des lignes $r_0 = 255$ avec $(u_0, v_0) = (1, 0)$ et $r_1 = 141$ avec $(u_1, v_1) = (0, 1)$. À chaque étape, q_k est le quotient de r_{k-1} par r_k , puis $r_{k+1} = r_{k-1} - q_k r_k$, et les coefficients suivent la même relation.

k	r_k	q_k	u_k	v_k
0	255		1	0
1	141	1	0	1
2	114	1	1	-1
3	27	4	-1	2
4	6	4	5	-9
5	3	2	-21	38
6	0			

Les divisions successives sont $255 = 1 \times 141 + 114$, $141 = 1 \times 114 + 27$,
 $114 = 4 \times 27 + 6$, $27 = 4 \times 6 + 3$ et $6 = 2 \times 3 + 0$. Le dernier reste non nul est 3,
donc $\text{pgcd}(255, 141) = 3$.

Vérification de la dernière ligne : $255 \times (-21) + 141 \times 38 = -5355 + 5358 = 3$. **On peut prendre** $(u, v) = (-21, 38)$.

- b. Comme 3 divise 12, on divise l'équation par 3 : elle équivaut à $85x + 47y = 4$. La relation précédente divisée par 3 donne $85 \times (-21) + 47 \times 38 = 1$, donc $85 \times (-84) + 47 \times 152 = 4$. Pour travailler avec des nombres plus petits, on remarque que $(x_0, y_0) = (10, -18)$ est aussi solution : $850 - 846 = 4$.

Soit (x, y) une solution. En soustrayant $85x_0 + 47y_0 = 4$, on obtient :

$$85(x - 10) = -47(y + 18).$$

Ainsi 47 divise $85(x - 10)$. Or $\text{pgcd}(85, 47) = \text{pgcd}(255, 141)/3 = 1$: 47 est premier avec 85. D'après le lemme de Gauss, 47 divise $x - 10$: il existe $k \in \mathbb{Z}$ tel que $x = 10 + 47k$. En reportant, $85 \times 47k = -47(y + 18)$, d'où $y = -18 - 85k$.

Réciproquement, pour tout $k \in \mathbb{Z}$:

$$85(10 + 47k) + 47(-18 - 85k) = 850 - 846 + 85 \times 47k - 47 \times 85k = 4.$$

Les solutions sont les couples $(10 + 47k, -18 - 85k)$, **avec** $k \in \mathbb{Z}$.

- c. Pour tous entiers x et y , 3 divise $255x + 141y$ puisque 3 divise 255 et 141. Or 3 ne divise pas 10. **L'équation n'a donc aucune solution entière.**

Erreur fréquente : oublier la réciproque en b), ou appliquer le lemme de Gauss sans avoir divisé l'équation par le pgcd (85 et 47 sont premiers entre eux, mais 255 et 141 ne le sont pas).

Barème : a) 2,5 points : 1,5 point pour le tableau correct, 0,5 point pour le pgcd, 0,5 point pour le couple vérifié ; b) 3 points : 0,5 point pour la simplification par 3, 0,5 point pour une solution particulière, 1,5 point pour l'usage justifié du lemme de Gauss, 0,5 point pour la réciproque et la conclusion ; c) 0,5 point.

Exercice 3 : Décomposition en facteurs premiers (3 points)

- a. $3600 = 36 \times 100 = 2^2 \times 3^2 \times 2^2 \times 5^2$, donc $n = 2^4 \times 3^2 \times 5^2$. De même $756 = 4 \times 189 = 4 \times 27 \times 7$, donc $m = 2^2 \times 3^3 \times 7$.

Un diviseur positif de n s'écrit de façon unique $2^\alpha 3^\beta 5^\gamma$ avec $0 \leq \alpha \leq 4$, $0 \leq \beta \leq 2$ et $0 \leq \gamma \leq 2$ (unicité de la décomposition). Il y a donc $5 \times 3 \times 3 = 45$ choix : **n possède 45 diviseurs positifs.**

- b. Le pgcd s'obtient avec les exposants minimaux et le ppcm avec les exposants maximaux :

$$\text{pgcd}(n, m) = 2^2 \times 3^2 = 36, \quad \text{ppcm}(n, m) = 2^4 \times 3^3 \times 5^2 \times 7 = 75\,600.$$

Contrôle : $36 \times 75\,600 = 2\,721\,600 = 3600 \times 756$. **Le pgcd vaut 36 et le ppcm vaut 75 600.**

- c. L'entier $n k$ est un cube si et seulement si chaque exposant de sa décomposition est un multiple de 3. Il faut donc que k contienne au moins 2^2 (pour passer de 2^4 à 2^6), 3^1 (pour passer de 3^2 à 3^3) et 5^1 (pour passer de 5^2 à 5^3). Le plus petit choix est $k = 2^2 \times 3 \times 5 = 60$. On vérifie : $3600 \times 60 = 216\,000 = 60^3$. **Le plus petit entier cherché est $k = 60$.**

Barème : a) 1 point (0,5 pour les deux décompositions, 0,5 pour le nombre de diviseurs justifié) ; b) 1 point (0,5 chacun) ; c) 1 point (0,5 pour la condition sur les exposants, 0,5 pour la valeur).

Exercice 4 : Congruences et petit théorème de Fermat (3 points)

- a. **Petit théorème de Fermat.** Si p est premier et a un entier non divisible par p , alors $a^{p-1} \equiv 1 \pmod{p}$. Pour tout entier a , on a aussi $a^p \equiv a \pmod{p}$.

Ici 7 est premier et ne divise pas 2 , donc $2^6 \equiv 1 \pmod{7}$. Comme $100 = 6 \times 16 + 4$:

$$2^{100} = (2^6)^{16} \times 2^4 \equiv 1 \times 16 \equiv 2 \pmod{7}.$$

Le reste de la division de 2^{100} par 7 est 2.

b. On a $42 = 2 \times 3 \times 7$. Montrons que 2, 3 et 7 divisent $n^7 - n$.

- Divisibilité par 7 : 7 est premier, donc $n^7 \equiv n \pmod{7}$ par le petit théorème de Fermat.
- Divisibilité par 3 : par Fermat, $n^3 \equiv n \pmod{3}$. Alors
 $n^7 = n^3 \times n^3 \times n \equiv n \times n \times n = n^3 \equiv n \pmod{3}$.
- Divisibilité par 2 : $n^2 \equiv n \pmod{2}$ par Fermat, donc de proche en proche
 $n^7 \equiv n \pmod{2}$ (ou : n^7 et n ont la même parité).

Ainsi $n^7 - n$ est multiple de 2 et de 3, premiers entre eux, donc de 6 (corollaire du lemme de Gauss). Puis il est multiple de 6 et de 7, premiers entre eux, donc de 42. **Pour tout entier n , 42 divise $n^7 - n$.**

Erreur fréquente : conclure qu'un entier divisible par 6 et par 7 l'est par 42 sans invoquer que 6 et 7 sont premiers entre eux (12 est divisible par 4 et par 6, mais pas par 24).

Barème : a) 1 point (0,25 pour l'énoncé, 0,75 pour le calcul) ; b) 2 points (0,5 par nombre premier, 0,5 pour la conclusion par Gauss).

Exercice 5 : Problème : un trésor et des restes (5 points)

- a. 5 et 7 sont deux nombres premiers distincts, donc leurs seuls diviseurs positifs communs se réduisent à 1 : ils sont premiers entre eux. On a $5 \times 3 + 7 \times (-2) = 15 - 14 = 1$. **On peut prendre $u = 3$ et $v = -2$.**

- b. Sens réciproque : si $N \equiv 17 \pmod{35}$, alors $N = 17 + 35j$. Comme 35 est multiple de 5 et de 7, $N \equiv 17 \equiv 2 \pmod{5}$ et $N \equiv 17 \equiv 3 \pmod{7}$.

Sens direct : supposons $N \equiv 2 \pmod{5}$ et $N \equiv 3 \pmod{7}$. Puisque 17 vérifie les deux mêmes congruences, $N - 17$ est divisible par 5 et par 7. Comme 5 et 7 sont premiers entre eux, le lemme de Gauss donne : $N - 17 = 5a$ et $7 \mid 5a$, donc $7 \mid a$, puis $35 \mid N - 17$.

Les deux conditions équivalent à $N \equiv 17 \pmod{35}$. (Les coefficients de a) expliquent d'où vient 17 : $2 \times 7 \times (-2) + 3 \times 5 \times 3 = -28 + 45 = 17$.)

- c. Le nombre N de pièces vérifie $N \equiv 17 \pmod{35}$, donc $N \in \{17 + 35j\}$. Entre 300 et 400, on trouve $17 + 35 \times 9 = 332$ et $17 + 35 \times 10 = 367$ (car $297 < 300$ et $402 > 400$).

Il reste la condition $N \equiv 1 \pmod{3}$: $332 = 3 \times 110 + 2$ ne convient pas, tandis que $367 = 3 \times 122 + 1$ convient.

Vérification : $367 = 5 \times 73 + 2 = 7 \times 52 + 3 = 3 \times 122 + 1$. **Le trésor compte 367 pièces.**

Barème : a) 1 point (0,5 pour la justification, 0,5 pour le couple) ; b) 2 points (0,5 pour la réciproque, 1,5 pour le sens direct avec le lemme de Gauss) ; c) 2 points (1 pour les candidats 332 et 367, 0,5 pour la condition modulo 3, 0,5 pour la vérification et la phrase-réponse).

[Revenir à l'énoncé du contrôle](#)

Après le corrigé du contrôle : arithmétique, Bézout, Gauss et congruences

Pour consolider ce que le corrigé vous a appris, relisez le cours « [Arithmétique dans \$\mathbb{Z}\$](#) » en L1 puis entraînez-vous avec les **exercices corrigés** [arithmétique dans \$\mathbb{Z}\$](#) .

Retrouvez tous les [contrôles de maths de L1 classés par chapitre](#), ou choisissez un autre niveau sur la page [contrôles de maths du CP au post-bac](#).

Autres contrôles de maths de L1 sur ce thème

- [Contrôle de maths L1 : polynômes, arithmétique et nombres complexes](#)