Corrigé du contrôle de maths sup : arithmétique dans Z, groupes et anneaux

Barème du contrôle

Exercice	Points
Exercice 1 : Nombres premiers et lemme de Gauss	3 points
Exercice 2 : Algorithme d'Euclide étendu et équation diophantienne	4 points
Exercice 3 : Valuations p-adiques et congruences	5 points
Exercice 4 : Morphismes et groupe des inversibles	3 points
Exercice 5 : Problème – sous-groupes de Z et arithmétique	5 points
Total	**20 points**

Exercice 1 : Nombres premiers et lemme de Gauss (3 points)

a. Soit $n \geq 2$. L'ensemble des diviseurs $d \geq 2$ de n est non vide, car il contient n. Il admet donc un plus petit élément p. Si p n'était pas premier, il aurait un diviseur q avec $2 \leq q < p$, et q diviserait n : c'est contraire à la minimalité de p. **Donc p est un diviseur premier de n.**

Supposons maintenant qu'il n'y ait qu'un nombre fini de nombres premiers $p_1, \dots, p_r$. Posons $N = p_1 p_2 \dots p_r + 1 \geq 2$. D'après ce qui précède, N admet un diviseur premier, qui est l'un des p_i. Alors p_i divise $N - p_1 \dots p_r = 1$, ce qui est absurde. **L'ensemble des nombres premiers est infini.**

Téléchargé depuis https://mathovore.fr - Mathovore site de maths.

b. **Lemme de Gauss :** soient a, b, c des entiers. Si a divise bc et si $a \wedge b = 1$, alors a divise c.

Démonstration. Comme $a \wedge b = 1$, le théorème de Bézout fournit $u, v \in \mathbb{Z}$ tels que $au + bv = 1$. En multipliant par c : $c = acu + bcv$. Or a divise acu, et a divise bc donc bcv. **Ainsi a divise la somme, c'est-à-dire c.**

Barème : a) 1,5 point : 0,5 point pour l'existence d'un diviseur premier, 1 point pour l'argument d'Euclide ; b) 1,5 point : 0,5 point pour l'énoncé, 1 point pour la preuve.

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

a. Les divisions euclidiennes successives donnent :

$$\begin{aligned} 252 &= 1 \times 198 + 54 \\ 198 &= 3 \times 54 + 36 \\ 54 &= 1 \times 36 + 18 \\ 36 &= 2 \times 18 + 0 \end{aligned}$$

Le dernier reste non nul est 18 : $d = 252 \wedge 198 = 18$. Remontons les calculs :

$$\begin{aligned} 18 &= 54 - 36 = 54 - (198 - 3 \times 54) = 4 \times 54 - 198 \\ 18 &= 4 \times (252 - 198) - 198 = 4 \times 252 - 5 \times 198 \end{aligned}$$

Le couple $(u, v) = (4, -5)$ convient. Vérification : $1008 - 990 = 18$.

b. On divise par 18 : l'équation équivaut à $14x + 11y = 2$, avec $14 \wedge 11 = 1$. D'après a), $14 \times 4 - 11 \times 5 = 1$, donc $(x_0, y_0) = (8, -10)$ est une solution particulière.

Si (x, y) est solution, par différence $14(x - 8) = -11(y + 10)$. Ainsi 11 divise $14(x - 8)$ et $11 \wedge 14 = 1$. Par le lemme de Gauss, 11 divise $x - 8$: il existe $k \in \mathbb{Z}$ tel que $x = 8 + 11k$. En reportant, $14 \times 11k = -11(y + 10)$, donc $y = -10 - 14k$.

Réciproquement, $14(8+11k)+11(-10-14k)=112-110=2$. **Les solutions sont les couples** $\begin{matrix}(8+11k,\\ ,-10-14k)\end{matrix}$, $k\in\mathbb{Z}$.

c. Pour tous entiers x, y, 18 divise $252x+198y$. Or 18 ne divise pas 30. **L'équation n'a donc aucune solution entière.**

d. Pour des entiers naturels, le produit du PGCD et du PPCM vaut le produit des nombres. **Donc le PPCM vaut** $\frac{252\times 198}{18}=252\times 11=2772$.

Barème : a) 1,5 point : 0,5 point pour les divisions, 0,5 point pour le PGCD, 0,5 point pour le couple de Bézout ; b) 1,5 point : 0,5 point pour la solution particulière, 0,5 point pour l'usage de Gauss, 0,5 point pour la réciproque ; c) 0,5 point ; d) 0,5 point.

Erreur fréquente : oublier de diviser par le PGCD avant d'appliquer le lemme de Gauss, ce qui donne une famille de solutions incomplète.

Exercice 3 : Valuations p-adiques et congruences (5 points)

a. On a $252=2^2\times 3^2\times 7$ et $198=2\times 3^2\times 11$. Le PGCD prend le minimum des valuations, le PPCM le maximum :

$$252\wedge 198=2^1\times 3^2=18$$
$$\text{ppcm}(252,198)=2^2\times 3^2\times 7\times 11=2772$$

On retrouve bien les résultats de l'exercice 2.

b. On a $v_p(n!)=\sum_{m=1}^{n} v_p(m)$. Or $v_p(m)$ est le nombre d'entiers $k\geq 1$ tels que p^k divise m. En échangeant les sommes, $v_p(n!)$ est la somme, sur $k\geq 1$, du nombre de multiples de p^k compris entre 1 et n. Ce nombre vaut $\left\lfloor \frac{n}{p^k}\right\rfloor$. **D'où la formule annoncée** (la somme est finie, car les termes sont nuls dès que $p^k>n$).

Téléchargé depuis https://mathovore.fr - Mathovore site de maths.

Pour $100!$:

$$v_5(100!) = 20 + 4 = 24$$
$$v_2(100!) = 50 + 25 + 12 + 6 + 3 + 1 = 97$$

Le nombre de zéros finaux est la plus grande puissance de $10 = 2 \times 5$ qui divise $100!$, soit $\min(97, 24)$. **L'écriture de $100!$ se termine par 24 zéros.**

c. Comme $7 \times 13 = 91 = 3 \times 30 + 1$, on a $7 \times 13 \equiv 1 \pmod{30}$. **L'inverse de 7 modulo 30 est 13.** En multipliant la congruence par 13, on obtient l'équivalence $7x \equiv 3 \Leftrightarrow x \equiv 39 \equiv 9 \pmod{30}$. **Les solutions sont les entiers $x = 9 + 30k$, $k \in \mathbb{Z}$.** Vérification : $7 \times 9 = 63 = 2 \times 30 + 3$.

d. Le nombre 11 est premier et ne divise pas 3. Le petit théorème de Fermat donne donc $3^{10} \equiv 1 \pmod{11}$. Comme $2026 = 202 \times 10 + 6$, on a $3^{2026} \equiv 3^6 \pmod{11}$. Or $3^5 = 243 = 22 \times 11 + 1$, donc $3^6 \equiv 3 \pmod{11}$. **Le reste de la division de 3^{2026} par 11 est 3.**

e. On a $42 = 2 \times 3 \times 7$.

Modulo 7, Fermat donne $n^7 \equiv n$. Modulo 3, Fermat donne $n^3 \equiv n$, donc $n^7 = (n^3)^2\, n \equiv n^3 \equiv n$. Modulo 2, n^7 et n ont la même parité.

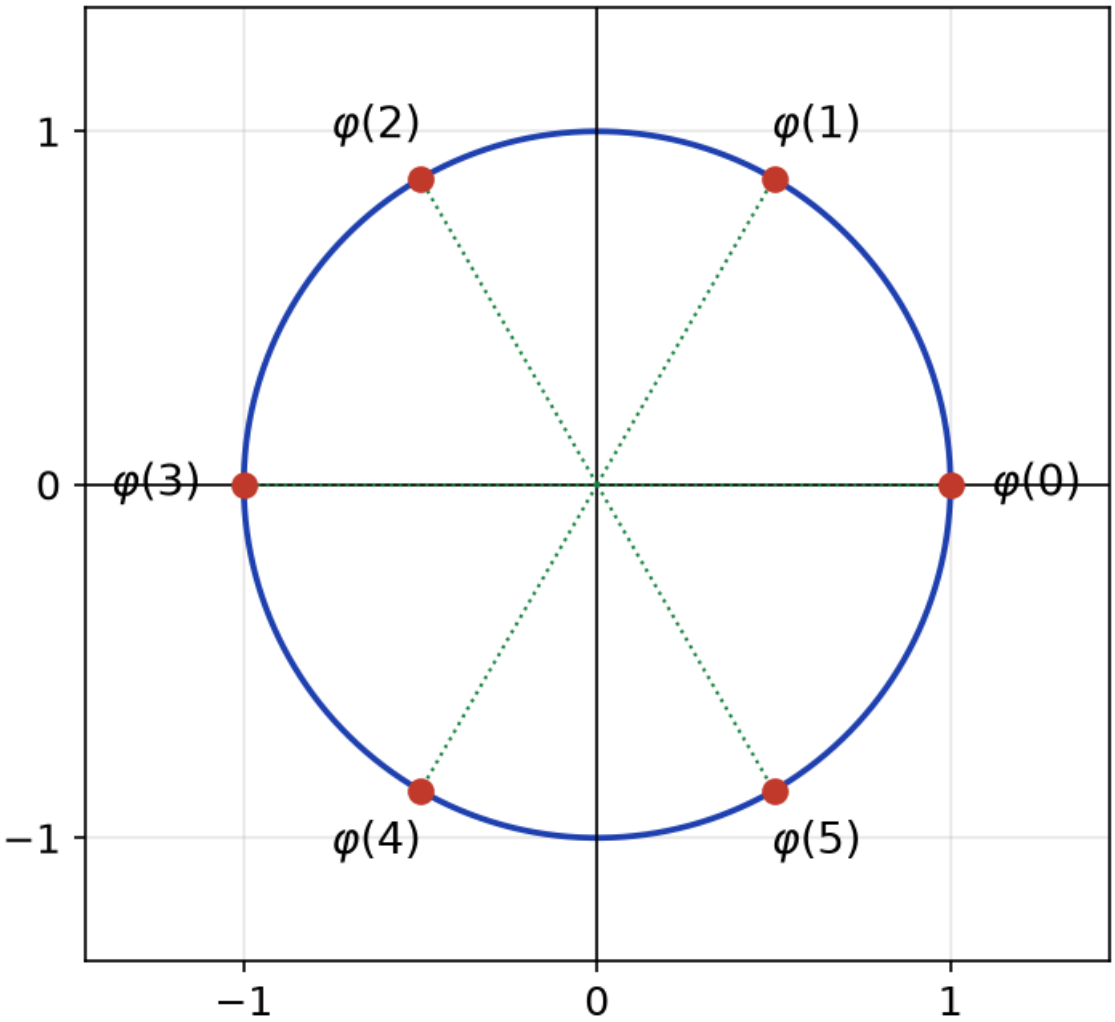
Ainsi 2, 3 et 7 divisent $n^7 - n$. Ils sont premiers entre eux deux à deux, donc leur produit divise $n^7 - n$. **Donc 42 divise $n^7 - n$.**

Barème : a) 1 point ; b) 1,5 point : 0,5 point pour la justification, 0,5 point pour les deux valuations, 0,5 point pour la conclusion ; c) 1 point : 0,5 point pour l'inverse, 0,5 point pour les solutions ; d) 1 point : 0,5 point pour Fermat, 0,5 point pour le reste ; e) 0,5 point.

Exercice 4 : Morphismes et groupe des inversibles (3 points)

a. Pour $k, l \in \mathbb{Z}$, $\varphi(k+l) = e^{2i(k+l)\pi/n} = e^{2ik\pi/n}\, e^{2il\pi/n} = \varphi(k)\varphi(l)$. **Donc φ est un morphisme de groupes.**

Ensuite, $\varphi(k) = 1$ équivaut à $\frac{2k\pi}{n} \in 2\pi\mathbb{Z}$, soit $n \mid k$. **Donc $\ker\varphi = n\mathbb{Z}$ et $\mathrm{Im}\varphi = \mathbb{U}_n$**, groupe des racines n-ièmes de l'unité. Le noyau n'est pas réduit à $\{0\}$, donc φ **n'est pas injectif**.



b. Pour $z, w \in \mathbb{Z}[i]$, $N(zw) = |zw|^2 = N(z)N(w)$, et $N(a+ib) = a^2 + b^2$ est un entier naturel.

Si z est inversible, il existe $w \in \mathbb{Z}[i]$ tel que $zw = 1$. Alors $N(z)N(w) = N(1) = 1$ avec des entiers naturels, donc $N(z) = 1$. Ainsi $a^2 + b^2 = 1$, d'où $(a, b) \in \{(\pm 1, 0), (0, \pm 1)\}$.

Téléchargé depuis https://mathovore.fr - Mathovore site de maths.

Réciproquement, $1 \times 1 = 1$, $(-1)(-1) = 1$ et $i \times (-i) = 1$. **Le groupe des inversibles de $\mathbb{Z}[i]$ est $\{1, -1, i, -i\} = \mathbb{U}_4$.**

c. Comme a commute avec 1, un calcul télescopique donne :

$$(1 - a)(1 + a + \ldots + a^{m-1}) = 1 - a^m = 1,$$

et de même dans l'autre sens. **Donc $1 - a$ est inversible, d'inverse $\sum_{k=0}^{m-1} a^k$.**

Barème : a) 1 point : 0,5 point pour le morphisme, 0,5 point pour noyau et image ; b) 1,5 point : 0,5 point pour la multiplicativité de N, 0,5 point pour N(z) = 1, 0,5 point pour la réciproque ; c) 0,5 point.

Exercice 5 : Problème – sous-groupes de Z et arithmétique (5 points)

1. On a $0 = n \times 0 \in n\mathbb{Z}$. Pour nk et nl dans $n\mathbb{Z}$, $nk - nl = n(k - l) \in n\mathbb{Z}$. **Par la caractérisation des sous-groupes, $n\mathbb{Z}$ est un sous-groupe de $\mathbb{Z}$.**

2. Si $H = \{0\}$, alors $H = 0\mathbb{Z}$. Sinon, H contient un $h \neq 0$ et son opposé, donc $H \cap \mathbb{N}^*$ est non vide. Cette partie de $\mathbb{N}$ admet un plus petit élément n.

   Comme H est un sous-groupe contenant n, il contient tous les multiples nk, $k \in \mathbb{Z}$. Ainsi $n\mathbb{Z} \subset H$.

   Soit $h \in H$. La division euclidienne donne $h = qn + r$ avec $0 \leq r < n$. Alors $r = h - qn \in H$. Si r était non nul, ce serait un élément de $H \cap \mathbb{N}^*$ strictement inférieur à n, ce qui est impossible. Donc $r = 0$ et $h \in n\mathbb{Z}$.

Ainsi $H = n\mathbb{Z}$ **.** L'entier $n \geq 0$ est unique, car c'est 0 si $H = \{0\}$ et le plus petit élément de $H \cap \mathbb{N}^*$ sinon.

3. La partie $a\mathbb{Z} + b\mathbb{Z}$ contient 0, et la différence de deux de ses éléments $au + bv$ et $au' + bv'$ vaut $a(u - u') + b(v - v')$. C'est donc un sous-groupe. D'après 2, il s'écrit $\delta\mathbb{Z}$ avec $\delta \geq 0$, et $\delta \neq 0$ car a ou b est non nul.

   D'une part, a et b appartiennent à $\delta\mathbb{Z}$, donc δ est un diviseur commun de a et b. D'autre part, $\delta \in a\mathbb{Z} + b\mathbb{Z}$ s'écrit $\delta = au + bv$, donc tout diviseur commun de a et b divise δ. **Ainsi** $\delta = a \wedge b = d$**.**

   On retrouve la relation de Bézout : il existe $u, v \in \mathbb{Z}$ tels que $au + bv = a \wedge b$.

4. L'intersection de deux sous-groupes est un sous-groupe. D'après 2, $a\mathbb{Z} \cap b\mathbb{Z} = \mu\mathbb{Z}$ avec $\mu \geq 0$. De plus ab est un élément non nul de l'intersection, donc $\mu > 0$. Les éléments de l'intersection sont exactement les multiples communs de a et b. Ainsi μ est un multiple commun strictement positif, et tout multiple commun est multiple de μ. **Donc** μ **est le PPCM :** $a\mathbb{Z} \cap b\mathbb{Z} = m\mathbb{Z}$**.**

5. Soit f un morphisme de $(\mathbb{Z}, +)$ dans lui-même, et $a = f(1)$. Comme en 1 et 2, une récurrence et l'imparité donnent $f(k) = f(k \times 1) = k\, f(1) = ak$ pour tout $k \in \mathbb{Z}$. Réciproquement, $k \to ak$ est un morphisme.

   Les morphismes sont les applications $k \to ak$**,** $a \in \mathbb{Z}$**.** Le noyau est $\{0\}$ si et seulement si $a \neq 0$: ces morphismes sont injectifs exactement pour $a \neq 0$. L'image est $a\mathbb{Z}$, égale à $\mathbb{Z}$ si et seulement si $1 \in a\mathbb{Z}$, c'est-à-dire $a = \pm 1$.

   Le groupe des automorphismes de $(\mathbb{Z}, +)$ **est** $\{\mathrm{id}, -\mathrm{id}\}$, isomorphe à $\{1, -1\}$ muni de la multiplication.

6. L'entier k est inversible modulo n s'il existe x tel que $kx \equiv 1 \pmod{n}$, c'est-à-dire s'il existe $x, y \in \mathbb{Z}$ tels que $kx + ny = 1$. Cela revient à dire que $1 \in k\mathbb{Z} + n\mathbb{Z} = (k \wedge n)\mathbb{Z}$, soit $k \wedge n = 1$, d'après la question 3.

   Modulo 12**, les entiers inversibles de** $\begin{Bmatrix} 0, \\ fs4\ldots\}, 11 \end{Bmatrix}$ **sont** $1, 5, 7$ **et** 11**.**

Téléchargé depuis https://mathovore.fr - Mathovore site de maths.

Barème : 1) 0,5 point ; 2) 1,5 point : 0,5 point pour l'existence de n, 0,5 point pour l'inclusion, 0,5 point pour la division euclidienne ; 3) 1 point : 0,5 point pour le sous-groupe, 0,5 point pour l'identification du PGCD ; 4) 0,5 point ; 5) 1 point : 0,5 point pour la forme des morphismes, 0,5 point pour injectivité, surjectivité et automorphismes ; 6) 0,5 point.

Revenir à l'énoncé du contrôle

Après le corrigé du contrôle : arithmétique dans Z, groupes et anneaux

Pour consolider ce que le corrigé vous a appris, relisez le cours « Arithmétique dans Z » en maths sup et « Groupes, anneaux et corps » en maths sup puis entraînez-vous avec les **exercices corrigés** arithmétique dans z, groupes, anneaux et corps.

Retrouvez tous les **contrôles de maths sup** classés par chapitre, ou choisissez un autre niveau sur la page contrôles de maths du CP au post-bac.