

CB2 — CORRIGÉ DE L'ÉPREUVE SPÉCIFIQUE "MP"

Problème 1 — Une application des polynômes de Bernstein :

le théorème de Stone-Weierstraß

Partie I — Questions préliminaires

Les questions de cette partie sont indépendantes.

1/ Soit f une fonction continue sur $[0, 1]$ et à valeurs dans $\mathbb{R}$. D'après le théorème des bornes atteintes, la fonction f est bornée (et atteint ses bornes) sur le segment $[0, 1]$. Donc : $\exists M \in \mathbb{R}_+, \forall x \in [0, 1], |f(x)| \leq M$.

2/ Pour tout réel x on a : $\left(x - \frac{1}{2}\right)^2 \geq 0$. D'où : $x^2 - x + \frac{1}{4} \geq 0$. Par suite : $\forall x \in \mathbb{R}, x(1-x) \leq \frac{1}{4}$.

Par ailleurs, pour tout réel $x \in [0, 1]$, il est clair que : $x(1-x) \geq 0$.

On en déduit que : $\forall x \in [0, 1], 0 \leq x(1-x) \leq \frac{1}{4}$.

3/ D'après le cours, si X suit la loi binomiale de taille n et de paramètre x , on a :

$$E(X) = nx; \quad \text{Var}(X) = nx(1-x); \quad E\left(\frac{X}{n}\right) = x; \quad \text{Var}\left(\frac{X}{n}\right) = \frac{x(1-x)}{n}$$

Partie II — Théorème de Stone-Weierstraß

Soit f une fonction continue sur $[0, 1]$ et à valeurs dans $\mathbb{R}$. On note M un majorant de $|f|$ sur $[0, 1]$.*

Pour tout entier naturel n non nul et pour tout réel $x \in [0, 1]$, on pose :

$$B_{f,n}(x) = \sum_{k=0}^n \binom{n}{k} x^k (1-x)^{n-k} f\left(\frac{k}{n}\right)$$

On choisit un réel $x \in [0, 1]$ et un réel strictement positif ε , qui sont donc fixés tout au long de cette partie. Et on se propose d'établir que :

$$\boxed{\exists n_0 \in \mathbb{N}, [n \geq n_0] \implies [|f(x) - B_{f,n}(x)| < \varepsilon]}$$

4/ Puisque f est continue sur le segment $[0, 1]$, elle est uniformément continue sur ce segment en vertu du théorème de Heine. Par suite : $\boxed{\exists \alpha > 0, \forall (u, v) \in [0, 1]^2, [|v - u| < \alpha] \implies [|f(v) - f(u)| < \frac{\varepsilon}{2}]}$

5/ Soit n un entier naturel. D'après la formule du binôme de Newton : $\sum_{k=0}^n \binom{n}{k} x^k (1-x)^{n-k} = 1$.

Par suite : $f(x) = \sum_{k=0}^n \binom{n}{k} x^k (1-x)^{n-k} f\left(\frac{k}{n}\right)$.

*. L'existence d'un tel réel M est assurée par la question 1.

On en déduit que : $f(x) - B_{f,n}(x) = \sum_{k=0}^n \binom{n}{k} x^k (1-x)^{n-k} \left(f(x) - f\left(\frac{k}{n}\right) \right)$.

D'après l'inégalité triangulaire : $|f(x) - B_{f,n}(x)| \leq \sum_{k=0}^n \binom{n}{k} x^k (1-x)^{n-k} \left| f(x) - f\left(\frac{k}{n}\right) \right|$.

6/ On a :

$$\Delta_n(x) = \underbrace{\sum_{k \in E} \binom{n}{k} x^k (1-x)^{n-k} \left(f(x) - f\left(\frac{k}{n}\right) \right)}_{=S_1(x)} + \underbrace{\sum_{k \in \bar{E}} \binom{n}{k} x^k (1-x)^{n-k} \left(f(x) - f\left(\frac{k}{n}\right) \right)}_{=S_2(x)}$$

D'après l'inégalité triangulaire : $|\Delta_n(x)| \leq |S_1(x)| + |S_2(x)|$ (♠)

Par définition de l'ensemble E , et d'après la question précédente, on a :

$$|S_1(x)| \leq \sum_{k \in E} \binom{n}{k} x^k (1-x)^{n-k} \frac{\varepsilon}{2} \leq \frac{\varepsilon}{2} \underbrace{\sum_{k \in E} \binom{n}{k} x^k (1-x)^{n-k}}_{\leq 1}$$

D'où : $|S_1(x)| \leq \frac{\varepsilon}{2}$ (♣)

Par ailleurs, pour tout couple de réels (u, v) dans $[0, 1]$, on a : $|f(v) - f(u)| \leq 2M$, puisque la valeur absolue de f est majorée par M . En particulier pour tout entier n non nul on a :

$$\left| f(x) - f\left(\frac{k}{n}\right) \right| \leq 2M.$$

Il s'ensuit que : $|S_2(x)| \leq 2M \sum_{k \in \bar{E}} \binom{n}{k} x^k (1-x)^{n-k}$ (♡)

On déduit de (♠), (♣) et (♡) que : $|\Delta_n(x)| \leq \frac{\varepsilon}{2} + 2M \sum_{k \in \bar{E}} \binom{n}{k} x^k (1-x)^{n-k}$.

7/ Soit X une variable aléatoire suivant la loi binomiale de taille n et de paramètre x . On a, par définition de l'ensemble E (et de la loi binomiale) :

$$P\left(\left|\frac{X}{n} - x\right| \geq \alpha\right) = \sum_{k \in \bar{E}} P(X = k) \text{ d'où : } P\left(\left|\frac{X}{n} - x\right| \geq \alpha\right) = \sum_{k \in \bar{E}} \binom{n}{k} x^k (1-x)^{n-k}.$$

8/ D'après l'inégalité de Bienaymé-Tchebychev : $P(|X - E(X)| \geq \alpha) \leq \frac{\text{Var}(X)}{\alpha^2}$ (pour tout réel $\alpha > 0$). En appliquant cette propriété à la variable aléatoire X/n , on obtient (d'après les rappels faits au cours de la question 3) :

$$P\left(\left|\frac{X}{n} - x\right| \geq \alpha\right) \leq \frac{x(1-x)}{n\alpha^2}$$

On en déduit, avec la question précédente, que : $\sum_{k \in \bar{E}} \binom{n}{k} x^k (1-x)^{n-k} \leq \frac{x(1-x)}{n\alpha^2}$

9/ D’après les questions 6 et 8, on a : $|\Delta_n(x)| \leq \frac{\varepsilon}{2} + \frac{2Mx(1-x)}{n\alpha^2}$.

Or : $0 \leq x(1-x) \leq \frac{1}{4}$ (d’après la question 2). On en déduit : $|\Delta_n(x)| \leq \frac{\varepsilon}{2} + \frac{M}{2n\alpha^2}$.

10/ Dans l’inégalité précédente, les réels M et α sont indépendants de n , et il est donc immédiat que $\frac{M}{2n\alpha^2}$ tend vers 0 lorsque n tend vers $+\infty$.

Comme il est également clair que le réel $\frac{M}{2n\alpha^2}$ est positif, on peut affirmer qu’à partir d’un certain rang, on a : $0 \leq \frac{M}{2n\alpha^2} \leq \frac{\varepsilon}{2}$.

On en déduit, grâce à la question précédente, qu’à partir d’un certain rang : $|\Delta_n(x)| \leq \varepsilon$.

Il s’ensuit que toute fonction continue sur le segment $[0, 1]$ peut être approchée arbitrairement près par une fonction polynomiale. Autrement dit, le sev des fonctions polynomiales sur $[0, 1]$ est dense dans l’ev des fonctions continues sur $[0, 1]$.

Problème 2 — Entiers sommes de deux carrés

Notations : tout au long du problème, on notera $\mathbb{Z}[i]$ l’anneau des **entiers de Gauss**, c’est-à-dire l’anneau des nombres complexes à parties réelle et imaginaire entières. Explicitement :

$$\mathbb{Z}[i] = \{a + ib \mid (a, b) \in \mathbb{Z}^2\}$$

Par ailleurs, on définit une “norme” sur $\mathbb{C}$, l’application
$$\begin{array}{l} N : \mathbb{C} \longrightarrow \mathbb{R}_+ \\ z \longmapsto z\bar{z} \end{array}$$

Partie I — Quelques propriétés de l’anneau des entiers de Gauss

1) Description des inversibles de $\mathbb{Z}[i]$.

a) Soient u et v dans $\mathbb{Z}[i]$. On a : $N(uv) = uv\bar{u}\bar{v} = u\bar{u}v\bar{v} = N(u)N(v)$.

En outre : $\forall u \in \mathbb{Z}[i], \exists (a, b) \in \mathbb{Z}^2, u = a + ib$. D’où : $N(u) = a^2 + b^2 \in \mathbb{N}$.

Conclusion. $\forall (u, v) \in \mathbb{Z}[i] \times \mathbb{Z}[i], N(uv) = N(u)N(v)$ et $\forall u \in \mathbb{Z}[i], N(u) \in \mathbb{N}$.

b) Si $u \in \mathbb{Z}[i]$ est inversible, alors il existe $v \in \mathbb{Z}[i]$ tel que : $N(uv) = 1$. D’après la question précédente, on en déduit que $N(u)$ est un diviseur entier naturel de 1, ce qui implique : $N(u) = 1$.

Par conséquent, les entiers de Gauss u inversibles sont à rechercher parmi ceux vérifiant : $N(u) = 1$. Or $N(u) = 1 \implies \operatorname{Re}^2(u) + \operatorname{Im}^2(u) = 1$. Par suite : u est inversible si et seulement si $\operatorname{Re}(u) = \pm 1$ et $\operatorname{Im}(u) = 0$; ou $\operatorname{Re}(u) = 0$ et $\operatorname{Im}(u) = \pm 1$. En résumé : $\mathbb{Z}[i]^* = \{\pm 1; \pm i\}$.

2) **Divisibilité dans $\mathbb{Z}[i]$.** Soient u et v dans $\mathbb{Z}[i]$, tels que u divise v dans $\mathbb{Z}[i]$. Alors il existe $s \in \mathbb{Z}[i]$ tel que : $v = us$. D’après la question 1-a, on en déduit que : $N(v) = N(u)N(s)$, ce qui signifie que $N(u)$ divise $N(v)$ dans $\mathbb{Z}$.

Conclusion. $\forall (u, v) \in \mathbb{Z}[i] \times \mathbb{Z}[i], (u|v) \implies (N(u)|N(v))$.

3) a) Soit $z \in \mathbb{C}$. Posons $a = \lfloor \operatorname{Re}(z) \rfloor$ et $a' = a + 1$. On a alors : $|\operatorname{Re}(z) - a| \leq \frac{1}{2}$ ou (non exclusif) $|\operatorname{Re}(z) - a'| \leq \frac{1}{2}$. Appelons A un des deux entiers relatifs (a ou a') vérifiant cette condition.

De même, appelons B l'un des deux entiers relatifs b ou b' vérifiant $|\operatorname{Im}(z) - b| \leq \frac{1}{2}$ ou $|\operatorname{Im}(z) - b'| \leq \frac{1}{2}$.

Alors le nombre complexe $u = A + iB$ est un entier de Gauss tel que : $N(z - u) \leq \left(\frac{1}{2}\right)^2 + \left(\frac{1}{2}\right)^2 = \frac{1}{2}$ d'où en particulier : $N(z - u) < 1$. **Conclusion.** $\forall z \in \mathbb{C}, \exists u \in \mathbb{Z}[i], N(z - u) < 1$.

En général, on n'a pas unicité de l'entier de Gauss u : pour le complexe $z = \frac{1+i}{2}$, les quatre entiers de Gauss $0, 1, i$ et $1+i$ conviennent.

b) Soient $u \in \mathbb{Z}[i]$ et $v \in \mathbb{Z}[i]^*$. On pose $z = \frac{u}{v}$, et on choisit $q \in \mathbb{Z}[i]$ tel que : $N\left(\frac{u}{v} - q\right) < 1$. On pose alors : $r = u - qv$. On a : $u = qv + r$, et $N(r) = N\left(\frac{u}{v} - q\right) N(v)$ donc $N(r) < N(v)$ (l'inégalité est stricte puisque $N(v)$ ne peut être nul).

Conclusion. $\forall (u, v) \in \mathbb{Z}[i] \times \mathbb{Z}[i]^*, \exists (q, r) \in \mathbb{Z}[i] \times \mathbb{Z}[i], [(u = vq + r) \wedge (N(r) < N(v))]$.

Remarque : on a ainsi prouvé qu'il existe une “pseudo”-division euclidienne dans $\mathbb{Z}[i]$. L'originalité de cette division par rapport à celle de $\mathbb{Z}$ ou de $\mathbb{K}[X]$ est que l'on n'a pas unicité du quotient ni du reste, en vertu de la question précédente.

Partie II — PGCD dans l'anneau des entiers de Gauss

4) L'ensemble $A = \{N(w) / w \in I(u, v) \setminus \{0\}\}$ est non vide sous réserve que $(u, v) \neq (0, 0)$. En effet, dès lors que $u \neq 0$ on a $u \in I(u, v)$ et $N(u) > 0$ (de même si $v \neq 0$). De plus, A est une partie de $\mathbb{N}^*$; elle possède donc un plus petit élément $\min A$. On pose alors : $d = \min A > 0$.

5) Soient u et v deux entiers de Gauss, non simultanément nuls. Notons δ un élément de $I(u, v)$ tel que $N(\delta) = d$. Notons que $\delta \neq 0$ puisque $(u, v) \neq (0, 0)$.

Montrons que : $\delta\mathbb{Z}[i] \subset I(u, v)$. Puisque δ est un élément de $I(u, v)$, il existe un couple d'entiers de Gauss (a, b) tel que : $\delta = au + bv$. Considérons alors un élément x quelconque de $\delta\mathbb{Z}[i]$. Il existe $c \in \mathbb{Z}[i]$ tel que : $x = c\delta$. Par suite : $x = acu + bcv$, d'où : $x \in I(u, v)$. D'où : $\delta\mathbb{Z}[i] \subset I(u, v)$.

Réciproquement, montrons que : $I(u, v) \subset \delta\mathbb{Z}[i]$. Soit x un élément de $I(u, v)$. D'après la question 3-b, il existe un couple d'entiers de Gauss (q, r) tel que : $x = q\delta + r$, avec $N(r) < N(\delta)$.

Raisonnons par l'absurde et supposons que $r \neq 0$. Alors r est un élément de $I(u, v)$ (puisque $r = x - q\delta$ et que x et δ sont dans $I(u, v)$), pour lequel : $0 < N(r) < N(\delta)$. Ce qui contredit la minimalité de $N(\delta)$. Par suite : $r = 0$. Donc : $x = q\delta$, ce qui assure que $x \in \delta\mathbb{Z}[i]$. D'où : $I(u, v) \subset \delta\mathbb{Z}[i]$.

D'après la règle de double inclusion : $I(u, v) = \delta\mathbb{Z}[i]$.

Remarque : ce résultat permet de montrer que tout idéal de $\mathbb{Z}[i]$ est monogène; on dit que l'anneau des entiers de Gauss est principal. On peut observer que le résultat tient encore dans le cas où u et v sont simultanément nuls, puisqu'alors : $I(u, v) = 0\mathbb{Z}[i] = \{0\}$.

6) Notons que $u \in I(u, v)$. D’après la question précédente, on a donc : $u \in \delta\mathbb{Z}[i]$. Par suite, il existe un entier de Gauss a tel que : $u = \delta a$. En particulier : $\delta|u$. Le raisonnement s’appliquant également à v , on peut conclure : $\delta|u$ et $\delta|v$.

Soit w un entier de Gauss. Supposons que $w|\delta$. Puisqu’en outre $\delta|u$, la transitivité de la divisibilité permet d’affirmer que : $w|u$. On montre de façon analogue que $w|v$. Par suite : $[w|\delta] \implies [w|u \wedge w|v]$.

Réciproquement, supposons que $w|u$ et $w|v$. Alors il existe deux entiers de Gauss a et b tels que : $u = aw$ et $v = bw$. De plus, $\delta \in \delta\mathbb{Z}[i]$ donc d’après la question précédente, $\delta \in I(u, v)$; il existe donc deux entiers de Gauss c et d tels que $\delta = cu + dv$. Par suite : $\delta = caw + dbw$ d’où $\delta = w(ca + db)$ donc : $w|\delta$. En résumé : $[w|u \wedge w|v] \implies [w|\delta]$.

Conclusion. $[w|u \wedge w|v] \iff [w|\delta]$.

Partie III — Entiers de Gauss premiers entre eux

7) Supposons que z et z' soient deux entiers de Gauss premiers entre eux. En reprenant les notations de la partie précédente, on a donc $\delta = \pm 1$ ou $\pm i$.

Par ailleurs, puisque $I(u, v) = \delta\mathbb{Z}[i]$ et que $\delta \in \delta\mathbb{Z}[i]$, il existe deux entiers de Gauss a et b tels que : $\delta = au + bv$.

En multipliant cette dernière égalité par $\bar{\delta}$ on obtient : $a(\bar{\delta}u) + b(\bar{\delta}v) = 1$. Il reste à voir que $\bar{\delta}u$ et $\bar{\delta}v$ sont deux entiers de Gauss, d’une part car l’anneau $\mathbb{Z}[i]$ est stable par conjugaison, et d’autre part car il est stable par produit (le produit étant une loi de composition interne dans $\mathbb{Z}[i]$).

En posant donc : $z = \bar{\delta}u$ et $z' = \bar{\delta}v$, on peut conclure :

Si u et v sont deux entiers de Gauss premiers entre eux, alors : $\exists (z, z') \in \mathbb{Z}[i]^2, uz + vz' = 1$.

8) Soit w un entier de Gauss tel que $u|vw$. D’après la question précédente, il existe un couple (z, z') d’entiers de Gauss tel que : $uz + vz' = 1$. D’où : $uwz + vwz' = w$. Il est immédiat que $u|uwz$, et par hypothèse on peut affirmer que $u|vwz'$. Donc u divise la somme de ces deux entiers, c’est à dire : $u|w$.

Conclusion. Si u et v sont deux entiers de Gauss premiers entre eux, alors : $[u|vw] \implies [u|w]$.

Remarque : ce résultat est à mettre en parallèle avec le lemme de Gauss dans $\mathbb{Z}$: “soient a, b et c trois entiers. Si $a|bc$ et a est premier avec b , alors $a|c$ ”.

Partie IV — Entiers de Gauss irréductibles

9) Soit d un entier de Gauss, diviseur commun à u et v . Puisque d est en particulier un diviseur de u , et que u est irréductible, on a : $d = \pm 1$ ou $\pm i$ ou $\pm u$ ou $\pm iu$.

Supposons que : $d = \pm u$ ou $\pm iu$. Alors $\pm u$ ou $\pm iu$ serait un diviseur de v (puisque $d|v$), ce qui impliquerait $u|v$: contradiction. Par suite : $d = \pm 1$ ou $\pm i$; u et v sont donc premiers entre eux.

Conclusion. Si u est un entier de Gauss irréductible, et si u ne divise pas $v \in \mathbb{Z}[i]$, alors u et v sont premiers entre eux.

Remarque : énoncé à mettre en parallèle avec celui connu dans $\mathbb{Z}$: “un nombre premier est premier avec tout entier qu’il ne divise pas”.

10) Soit u un entier de Gauss irréductible, et soit v un entier de Gauss. Prouvons la propriété de l'énoncé par disjonction des cas.

Si $u|v$: l'assertion est prouvée.

Si u ne divise pas v : d'après la question précédente, u et v sont premiers entre eux. D'après la question 7, il existe alors deux entiers de Gauss z et z' tels que : $uz + vz' = 1$. D'où : $uwz + vwz' = w$. Il est alors immédiat que $u|uwz$, et $u|vwz'$ (par hypothèse). Donc $u|uwz + vwz'$, soit : $u|w$.

Conclusion. Soient v et w dans $\mathbb{Z}[i]$. Si u est un entier de Gauss irréductible, et si $u|vw$, alors $u|v$ ou $u|w$.

Remarque : énoncé à mettre en parallèle avec celui connu dans $\mathbb{Z}$: “soient a et b deux entiers, et p un nombre premier. Si $p|ab$, alors $p|a$ ou $p|b$ ”.

Partie V — Entiers sommes de deux carrés

On note $S = \{a^2 + b^2 / (a, b) \in \mathbb{Z}^2\}$. L'ensemble S est donc l'ensemble des entiers (naturels) s'écrivant comme sommes de deux carrés. L'objet de cette partie est de donner une description de S .

Questions 11) & 12) : triviales.

13) Si $p \in S$, alors il existe deux entiers naturels a et b tels que $p = a^2 + b^2$. Or les valeurs possibles modulo 4 pour a^2 (ou b^2) sont 0 et 1. On en déduit que $a^2 + b^2$ est congru à 0, 1 ou 2 modulo 4. L'entier p étant supposé impair, on a donc nécessairement : $p \equiv 1 \pmod{4}$.

14) a) Puisque $p \equiv 3 \pmod{4}$, alors p est irréductible dans $\mathbb{Z}[i]$. Puisqu'en outre p divise $n = (a + ib)(a - ib)$, on en déduit que p divise $(a + ib)$ ou $(a - ib)$ (d'après la question 10). Il reste à observer que p divise $(a + ib)$ ou $(a - ib)$ dès lors qu'il divise l'un de ces deux entiers de Gauss pour conclure.

b) D'après la question précédente, il existe un entier de Gauss u tel que : $pu = a + ib$. On a alors : $p\bar{u} = a - ib$. Par suite : $p^2 N(u) = n$. Donc p^2 divise n dans $\mathbb{Z}$.

15) On peut déjà s'assurer que tout entier de la forme décrite dans l'énoncé est effectivement dans S . Cela provient des observations suivantes :

- $2 = 1^2 + 1^2 \in S$. Par suite, d'après la question 12 : $2^n \in S$ pour tout entier naturel n .
- Si p_i est un nombre premier tel que $p_i \equiv 1 \pmod{4}$, alors $p_i \in S$ d'après l'indication de l'énoncé. Par suite, d'après la question 12 : $p_i^n \in S$ pour tout entier naturel n .
- Si p_i est un nombre premier tel que $p_i \equiv 3 \pmod{4}$ et α_i pair. Alors il existe un entier naturel β_i tel que $\alpha_i = 2\beta_i$, d'où : $p_i^{\alpha_i} = (p_i^2)^{\beta_i}$. Or : $p_i^2 = p_i^2 + 0^2 \in S$. Par suite, d'après la question 12 : $p_i^{\alpha_i} \in S$ pour tout entier naturel n .

On en déduit que si n est de la forme proposée dans l'énoncé, alors $n \in S$.

Réciproquement, soit $n \in S$, avec $n \geq 1$. L'entier n admet une décomposition en facteurs premiers, que l'on peut écrire : $\prod_{i=1}^m p_i^{\alpha_i}$.

Le point à prouver est que la valuation p_i -adique de n est paire pour tout p_i est congru à 3 modulo 4. Ceci provient de la question précédente, puisque si un tel premier p_i divise n , alors p_i^2 divise n ...