

Entiers de Gauss

- On note $\mathbb{Z}_i = \{a + ib, a \in \mathbb{Z}, b \in \mathbb{Z}\}$. Les éléments de \mathbb{Z}_i sont appelés *entiers de Gauss*.
 Dans suite, quand on dira soit $z = a + ib$ dans \mathbb{Z}_i , il sera sous-entendu que a, b sont dans \mathbb{Z} .
- Pour tout élément $z = a + ib$ de \mathbb{Z}_i , on note $\varphi(z) = z\bar{z} = |z|^2 = a^2 + b^2$.
 Bien sûr $\varphi(z)$ est dans \mathbb{N} et pour tous z, z' de \mathbb{Z}_i on a $\varphi(zz') = \varphi(z)\varphi(z')$.
- On note \mathbb{Z}_i^+ l'ensemble des $z = a + ib$ de \mathbb{Z}_i tels que $a \geq 1$ et $b \geq 0$.

Partie I. Divisibilité dans l'anneau \mathbb{Z}_i .

1. Montrer que $(\mathbb{Z}_i, +, \times)$ est anneau. Que dire de \mathbb{Z} relativement à \mathbb{Z}_i ? [S]
2. Montrer que les seuls éléments inversibles de l'anneau \mathbb{Z}_i sont $1, i, -1, -i$.
 Dans toute la suite, on notera $\mathcal{U} = \{1, i, -1, -i\}$. [S]
3. On dit que z divise z' dans \mathbb{Z}_i s'il existe q dans \mathbb{Z}_i tel que $z' = qz$.
 On note alors $z \parallel z'$ (on définit ainsi une relation réflexive et transitive sur \mathbb{Z}_i).
 Remarque : on note toujours $m \mid n$ la relation *divisibilité* dans \mathbb{Z} .
 - (a) Soient z, z' deux éléments de \mathbb{Z} , donc de \mathbb{Z}_i . Montrer que $z \mid z' \Leftrightarrow z \parallel z'$.
 Autrement dit la relation de divisibilité dans \mathbb{Z}_i "prolonge" celle de \mathbb{Z} . [S]
 - (b) Soient z et z' dans \mathbb{Z}_i . Montrer que $(z \parallel z' \text{ et } z' \parallel z) \Leftrightarrow \exists u \in \mathcal{U}, z' = uz$.
 On exprimera cette situation en disant que z et z' sont *associés* dans \mathbb{Z}_i .
 Dans toute la suite on notera $z \sim z'$ pour exprimer que z et z' sont associés. [S]
 - (c) Montrer que la relation \sim est une relation d'équivalence sur \mathbb{Z}_i .
 On notera \tilde{z} la classe d'équivalence d'un élément z de \mathbb{Z}_i .
 Quel est le cardinal de \tilde{z} ? Que représente géométriquement \tilde{z} ? [S]
 - (d) Soit $z \neq 0$ dans \mathbb{Z}_i . Montrer que \mathbb{Z}_i^+ contient un unique élément de \tilde{z} .
 Dans la suite du problème, cet élément sera noté z^+ . [S]
4. Dans cette question, z et z' sont deux éléments quelconques de \mathbb{Z}_i .
 On note $\mathcal{D}_i(z) = \{\omega \in \mathbb{Z}_i, \omega \parallel z\}$ l'ensemble des *diviseurs* de z dans \mathbb{Z}_i .
 On note $z\mathbb{Z}_i = \{z\omega, \omega \in \mathbb{Z}_i\}$ l'ensemble des *multiples* de z dans \mathbb{Z}_i .
 - (a) Montrer que $z\mathbb{Z}_i \subset z'\mathbb{Z}_i \Leftrightarrow z' \parallel z \Leftrightarrow \mathcal{D}_i(z') \subset \mathcal{D}_i(z)$.
 En déduire $z\mathbb{Z}_i = z'\mathbb{Z}_i \Leftrightarrow z' \sim z \Leftrightarrow \mathcal{D}_i(z) = \mathcal{D}_i(z')$. [S]
 - (b) Montrer que z divise $\varphi(z)$ dans \mathbb{Z}_i . [S]
 - (c) Montrer que $\begin{cases} z' \parallel z \Rightarrow \varphi(z') \mid \varphi(z) \\ z' \sim z \Rightarrow \varphi(z') = \varphi(z) \end{cases}$ et que les réciproques sont fausses. [S]
 - (d) Montrer que si $z' \parallel z$ et $\varphi(z) = \varphi(z')$, alors $z' \sim z$. [S]
 - (e) Déterminer $\mathcal{D}_i(4 + 7i) \cap \mathbb{Z}_i^+$, puis $\mathcal{D}_i(4 + 7i)$. [S]

Partie II. Division et pgcd dans \mathbb{Z}_i .

1. Division euclidienne

 (a) Soit ω un élément de \mathbb{C} .

 Montrer qu'il existe de un à quatre éléments z de \mathbb{Z}_i tel que $|z - \omega| < 1$.

 Montrer qu'il existe au moins un élément z de \mathbb{Z}_i tel que $|z - \omega| \leq \frac{1}{2}$. [S]

 (b) Soient z, z' deux éléments de \mathbb{Z}_i , z étant non nul.

 Montrer qu'il existe de un à quatre couples (q, r) de \mathbb{Z}_i^2 tels que
$$\begin{cases} z' = qz + r \\ \varphi(r) < \varphi(z) \end{cases}$$

 Cette écriture est appelée *une division de z' par z dans \mathbb{Z}_i* .

 Dans une telle division, q est appelé le *quotient* et r est appelé le *reste*. [S]

 (c) Ecrire toutes les divisions possibles dans \mathbb{Z}_i de $z' = 1 + 11i$ par $z = 3 + 4i$.

Quelle est la meilleure division (celle donnant le reste de module minimum)? [S]

 (d) Soient z' dans \mathbb{Z} et z dans \mathbb{N}^* . Vérifier que la division euclidienne de z' par z dans \mathbb{Z} (donc au sens habituel) est aussi une division de z' par z dans \mathbb{Z}_i . [S]

 (e) Ecrire une procédure Maple, sur le modèle `div :=proc(z1,z2)...end`, prenant en argument deux nombres complexes z_1 et z_2 (écrits sous la forme $x + iy$) et renvoyant la liste $[q, r]$ représentant une division de z_1 par z_2 dans \mathbb{Z}_i .

 Pour choisir q , on utilisera la fonction `round` qui accepte un complexe $x + iy$ et renvoie le complexe obtenu par arrondi de x, y aux entiers les plus proches. [S]

2. Algorithme d'Euclide

Dans cette question, on va prouver la proposition suivante :

Proposition

 Soient z et z' deux éléments de \mathbb{Z}_i , non tous les deux nuls.

 Il existe un unique élément d de \mathbb{Z}_i^+ tel que $\mathcal{D}_i(z) \cap \mathcal{D}_i(z') = \mathcal{D}_i(d)$.

 Autrement dit, pour tout ω de \mathbb{Z}_i , on a $(\omega \parallel z \text{ et } \omega \parallel z') \Leftrightarrow \omega \parallel d$.

 On dit que d est le *pgcd* de z et z' dans \mathbb{Z}_i . On note $d = \text{pgcd}(z, z')$ ou $d = z \wedge z'$.

 Il existe un couple u, v d'éléments de \mathbb{Z}_i tels que $zu + z'v = d$.

 On dit que (u, v) est un couple de *coefficients de Bezout* du couple (z, z') .

 On complète cette définition en posant $0 \wedge 0 = 0$.

Pour démontrer cette proposition, on va mettre en œuvre un algorithme d'Euclide.

 Les éléments z et z' jouant un rôle symétrique, on peut supposer $z \neq 0$.

 – On pose $r_0 = z'$ et $r_1 = z$. On note $r_0 = q_1 r_1 + r_2$ une division de r_0 par r_1 dans \mathbb{Z}_i .

 – Si $r_2 \neq 0$, on note $r_1 = q_2 r_2 + r_3$ une division de r_1 par r_2 dans \mathbb{Z}_i .

 – Soit n un entier de \mathbb{N}^* . On suppose qu'on a formé r_k et que r_k est non nul.

 On note alors $r_{k-1} = q_k r_k + r_{k+1}$ une division de r_{k-1} par r_k dans \mathbb{Z}_i .

 – Si $r_{k+1} \neq 0$, on poursuit l'algorithme, sinon on arrête, et r_k est le dernier reste non nul obtenu par cette méthode.

- (a) Montrer que l'algorithme se termine au bout d'un nombre fini de divisions. [S]
- (b) Il existe donc un entier n tel que $r_n \neq 0$ et $r_{n+1} = 0$. On pose $d = r_n^+$.
 Prouver $\forall k \leq n, \mathcal{D}_i(z) \cap \mathcal{D}_i(z') = \mathcal{D}_i(r_k) \cap \mathcal{D}_i(r_{k+1})$, puis $\mathcal{D}_i(z) \cap \mathcal{D}_i(z') = \mathcal{D}_i(d)$.
 Montrer que d est le seul élément de \mathbb{Z}_i^+ à vérifier cette propriété. [S]
- (c) Montrer que : $\forall k \in \{0, \dots, n\}, \exists (u_k, v_k) \in \mathbb{Z}_i^2, zu_k + z'v_k = r_k$.
 En déduire qu'il existe (u, v) dans \mathbb{Z}_i^2 tels que $zu + z'v = d$.
 Ceci achève la démonstration de la proposition. [S]
- (d) Montrer que parmi les diviseurs communs de z et z' , l'élément $z \wedge z'$ et ses trois associés sont ceux qui ont le plus grand module. [S]
- (e) Montrer que si $z, z' \in \mathbb{Z}$, leur pgcd (au sens habituel) est $z \wedge z'$ au sens de \mathbb{Z}_i . [S]

3. Un peu de programmation

Les procédures Maple demandées ici prennent en argument un ou deux éléments de \mathbb{Z}_i , qui sont supposés écrits sous la forme $z = x + iy$, avec x, y entiers relatifs. On ne procédera donc à aucune vérification de la validité des arguments.

On rappelle d'autre part que Maple évalue automatiquement les expressions arithmétiques (sommées, produits, quotients, puissances, ...) formées à partir de nombres complexes donnés explicitement sous la forme $z = x + iy$.

- (a) Ecrire une procédure Maple, sur le modèle `zpos :=proc(z) ...end`, prenant en argument un élément z de \mathbb{Z}_i , et renvoyant z^+ . [S]
- (b) Ecrire une procédure Maple, sur le modèle `pgcd :=proc(z1, z2) ...end`, calculant le pgcd de deux entiers de Gauss z_1 et z_2 , de manière itérative. [S]
- (c) Ecrire une procédure Maple, sur le modèle `rpgcd :=proc(z1, z2) ...end`, calculant le pgcd de deux entiers de Gauss z_1 et z_2 , de manière récursive. [S]
- (d) Ecrire une procédure Maple, sur le modèle `bezout :=proc(z1, z2) ...end`, calculant un couple de coefficients de Bezout de z_1, z_2 . Le résultat sera une liste $[u, v]$ telle que $zu + z'v = z \wedge z'$. La procédure `bezout` calculera u, v de manière itérative. [S]
- (e) Ecrire une procédure Maple, sur le modèle `rbezout :=proc(z1, z2) ...end`, et qui effectue le même calcul que `bezout` mais de manière récursive. [S]

4. Entiers de Gauss premiers entre eux

On dit que deux éléments z, z' de \mathbb{Z}_i sont premiers entre eux dans \mathbb{Z}_i si $z \wedge z' = 1$.

Remarque : il découle de II.2.e que si z et z' sont dans \mathbb{Z} , alors ils sont premiers entre eux en tant qu'éléments de \mathbb{Z} si et seulement si ils le sont en tant qu'éléments de \mathbb{Z}_i .

Dans les questions suivantes z, z' et z'' sont des éléments de \mathbb{Z}_i .

- (a) Montrer que $z \wedge z' = 1 \Leftrightarrow \exists (u, v) \in \mathbb{Z}_i^2, zu + z'v = 1$ (Bezout.) [S]
- (b) Montrer que si $z \parallel (z'z'')$ dans \mathbb{Z}_i , et si $z \wedge z' = 1$, alors $z \parallel z''$ (Gauss.) [S]
- (c) Montrer que si $z \wedge z' = 1$ et $z \wedge z'' = 1$ alors $z \wedge (z'z'') = 1$. Généraliser. [S]
- (d) Montrer que si $z \parallel z''$ et $z' \parallel z''$, et si $z \wedge z' = 1$, alors $(zz') \parallel z''$. [S]

Partie III. Entiers de Gauss irréductibles

Définition

On dit que z est irréductible dans \mathbb{Z}_i si z est non nul, non inversible, et si ses seuls diviseurs sont les éléments de $\mathcal{U} = \{1, i, -1, -i\}$ et les associés de z c'est-à-dire $z, iz, -z, -iz$.

On note \mathcal{P}_i l'ensemble des éléments irréductibles de \mathbb{Z}_i .

On note comme d'habitude \mathcal{P} l'ensemble des entiers naturels premiers.

 1. Quelques propriétés des éléments de \mathcal{P}_i

(a) Montrer $z \in \mathcal{P}_i \Leftrightarrow z^+ \in \mathcal{P}_i$. On pose $\mathcal{P}_i^+ = \mathcal{P}_i \cap \mathbb{Z}_i^+ = \{a + ib \in \mathcal{P}_i, a \geq 1, b \geq 0\}$. Les éléments de \mathcal{P}_i^+ seront appelés *facteurs irréductibles normalisés*. [S]

(b) Soient p dans \mathcal{P}_i et z dans \mathbb{Z}_i . Montrer que si p ne divise pas z , alors $p \wedge z = 1$. En déduire que si p et q sont distincts dans \mathcal{P}_i^+ , alors $p \wedge q = 1$. [S]

(c) Soit p un élément de \mathcal{P}_i . Montrer que si $p \parallel (zz')$, alors $p \parallel z$ ou $p \parallel z'$.

Plus généralement, montrer que si $p \parallel \prod_{k=1}^n z_k$, alors $\exists k \in \{1, \dots, n\}, p \parallel z_k$. [S]

(d) Montrer que si $\varphi(z)$ est dans \mathcal{P} , alors z est dans \mathcal{P}_i . [S]

2. Factorisation en produit de facteurs irréductibles normalisés

Soit z un élément de \mathbb{Z}_i , non nul et non inversible (donc tel que $\varphi(z) > 1$.)

(a) Montrer que z est divisible par au moins un élément p de \mathcal{P}_i^+ . [S]

(b) Montrer que z peut s'écrire sous la forme $z = u \prod_{k=1}^m p_k^{n_k}$, où :

– u est un élément de $\mathcal{U} = \{1, i, -1, -i\}$. ; m est un élément de \mathbb{N}^*

– pour tout k de $\{1, \dots, m\}$, p_k est dans \mathbb{Z}_i^+ et n_k dans \mathbb{N}^* .

[S]

(c) Montrer que l'écriture précédente de z est unique à l'ordre près des facteurs. [S]

 3. Irréductibilité des éléments de \mathbb{N}^* .

Il est clair que si $n \geq 2$ est un entier non premier, il n'est pas irréductible dans \mathbb{Z}_i (ses diviseurs dans \mathbb{N} étant aussi des diviseurs dans \mathbb{Z}_i). Il reste donc à comprendre quand un entier premier p est irréductible dans \mathbb{Z}_i . Pour cela on va démontrer le résultat suivant :

Proposition

Soit p un nombre premier. Les conditions suivantes sont équivalentes :

– p n'est pas irréductible dans \mathbb{Z}_i .

– Il existe a et b dans \mathbb{N}^* tels que $p = a^2 + b^2$.

– $p = 2$, ou p est congru à 1 modulo 4.

(a) Montrer que si p n'est pas irréductible, alors $\exists (a, b) \in (\mathbb{N}^*)^2, p = a^2 + b^2$ (utiliser un diviseur de p dans \mathbb{Z}_i , non inversible et non associé à p .) [S]

- (b) Inversement, si $p = a^2 + b^2$ (avec a, b dans \mathbb{N}^*) montrer que p n'est pas irréductible et écrire la factorisation de p en produit de facteurs irréductibles normalisés.
En déduire que la paire $\{a, b\}$ de $(\mathbb{N}^*)^2$ telle que $p = a^2 + b^2$ est unique. [S]
- (c) Montrer que $p = 2$ n'est pas irréductible dans \mathbb{Z}_i . [S]
- (d) On rappelle le théorème de Wilson : p premier $\Leftrightarrow (p-1)! \equiv -1 \pmod{p}$.
On suppose que $p \equiv 1 \pmod{4}$. Il existe donc n dans \mathbb{N}^* tel que $p = 4n + 1$.
Montrer que $(p-1)! \equiv (2n)!^2$. Ainsi, en posant $m = (2n)!$, on a $m^2 \equiv -1 \pmod{p}$.
Par l'absurde, on suppose que p est irréductible.
Montrer que p divise $m+i$ ou $m-i$ et aboutir à une contradiction.
Donc si p est premier et congru à 1 modulo 4, il n'est pas irréductible. [S]
- (e) Montrer que si $p \equiv 3 \pmod{4}$, alors p est irréductible (raisonner par l'absurde.)
Autrement si, si p n'est pas irréductible, il est égal à 2, ou congru à 1 modulo 4.
Ceci termine la démonstration de la proposition.
Le résultat de cette question peut être résumé ainsi : *Un entier $n \geq 1$ est irréductible dans \mathbb{Z}_i si et seulement si* $\begin{cases} n \text{ est premier} \\ n \equiv 3 \pmod{4} \end{cases}$ [S]

4. Éléments irréductibles normalisés de \mathbb{Z}_i .

La question précédente indique quels éléments de \mathbb{N}^* sont irréductibles.

Pour ce qui est des éléments de \mathbb{Z}_i^+ , il reste à établir le résultat suivant :

Proposition

Soit $z = a + ib$, avec $a \in \mathbb{N}^*$ et $b \in \mathbb{N}^*$.
 z est irréductible si et seulement si $\varphi(z) = a^2 + b^2$ est un entier premier.
De plus cet entier premier est égal à 2, ou est congru à 1 modulo 4.

On sait déjà que si $\varphi(z)$ est un entier premier, alors z est irréductible (cf III.1.d.)

La question III.3.e) a également montré qu'un entier premier congru à 3 modulo 4 (donc qui n'est ni égal à 2 ni congru à 1 modulo 4) n'est jamais la somme de deux carrés.

Il reste donc à supposer que $z = a + ib$ ($a, b \geq 1$) est dans \mathcal{P}_i et à montrer que $\varphi(z) \in \mathcal{P}$.

- (a) En considérant la décomposition de $\varphi(z)$ en produits de facteurs premiers dans \mathbb{N} , montrer qu'il existe un entier premier p tel que $z \parallel p$. [S]
- (b) Avec les notations précédentes, montrer que $\varphi(z) = p$. [S]

On a ainsi obtenu la caractérisation des éléments irréductibles normalisés de \mathbb{Z}_i :

Proposition

Un élément de $z = a + ib$ de \mathbb{Z}_i^+ ($a \geq 1, b \geq 0$) est irréductible si et seulement si :
– Ou bien : $b = 0$ et a est un nombre premier congru à 3 modulo 4.
– Ou bien : $b \geq 1$ et $a^2 + b^2$ est un nombre premier non congru à 3 modulo 4.

Corrigé du problème

Partie I. Divisibilité dans l'anneau \mathbb{Z}_i .

1. Il suffit de vérifier que \mathbb{Z}_i est un sous-anneau de $(\mathbb{C}, +, \times)$.
 Tout d'abord \mathbb{Z}_i contient $1 = 1 + 0i$ (le neutre multiplicatif de l'anneau \mathbb{C}).
 Si $z = a + ib$ et $z' = c + id$ sont dans \mathbb{Z}_i , il en est de même de :
 - $z - z' = (a - c) + i(b - d)$ car $a - c$ et $b - d$ sont éléments de \mathbb{Z} .
 - $zz' = (ac - bd) + i(ad + bc)$ car $ac - bd$ et $ad + bc$ sont éléments de \mathbb{Z} .
 Conclusion : \mathbb{Z}_i est un sous-anneau de $(\mathbb{C}, +, \times)$.
 L'anneau $(\mathbb{Z}, +, \times)$ est bien sûr un sous-anneau de \mathbb{Z}_i . [Q]
2. Si $z = a + ib$ est inversible dans \mathbb{Z}_i , il existe $z' = c + id$ dans \mathbb{Z}_i tel que $zz' = 1$.
 On a alors l'égalité $1 = \varphi(1) = \varphi(zz') = \varphi(z)\varphi(z')$.
 $\varphi(z)$ et $\varphi(z')$ étant des entiers naturels, cela implique $\varphi(z) = 1$.
 Réciproquement, si $\varphi(z) = a^2 + b^2 = 1$, alors $\bar{z} = a - ib \in \mathbb{Z}_i$ et $z\bar{z} = 1$.
 Conclusion : un élément $z = a + ib$ de \mathbb{Z}_i est inversible $\Leftrightarrow \varphi(z) = a^2 + b^2 = 1$.
 Il y a quatre solutions, qui sont les points à coordonnées entières du cercle unité.
 Les seuls éléments inversibles de \mathbb{Z}_i sont donc $1, i, -1, -i$. [Q]
3. (a) Soient z et z' deux éléments de \mathbb{Z} , donc deux éléments de \mathbb{Z}_i .
 - Supposons que z divise z' dans \mathbb{Z} , c'est-à-dire qu'il existe q dans \mathbb{Z} tel que $z' = qz$.
 Alors z divise z' dans \mathbb{Z}_i car q est aussi un élément de \mathbb{Z}_i .
 - Réciproquement, supposons que z' divise z dans \mathbb{Z}_i .
 Il existe donc un élément q de \mathbb{Z}_i tel que $z' = qz$.
 Si $z = 0$, alors $z' = 0$ et z divise z' dans \mathbb{Z} ($z' = mz$ pour tout m de \mathbb{Z}).
 Si $z \neq 0$, alors $q = \frac{z'}{z}$ est un entier relatif. Donc z divise z' dans \mathbb{Z} .
 - Finalement, si $z, z' \in \mathbb{Z}$, z divise z' dans $\mathbb{Z} \Leftrightarrow z$ divise z' dans \mathbb{Z}_i .
 En ce sens, la relation de divisibilité dans \mathbb{Z}_i prolonge celle de \mathbb{Z} .
 [Q]
- (b) Soient z et z' deux éléments de \mathbb{Z}_i .
 - S'il existe u dans \mathcal{U} tel que $z' = uz$, alors $z = \bar{u}z'$ (et $\bar{u} \in \mathcal{U}$).
 Autrement dit $z \parallel z'$ et $z' \parallel z$.
 - Réciproquement, supposons $z \parallel z'$ et $z' \parallel z$.
 Il existe donc deux éléments q, q' de \mathbb{Z}_i tels que $z' = qz$ et $z = q'z'$.
 On en déduit $z(qq' - 1) = 0$ donc $z = 0$ ou $qq' = 1$.
 Si $z = 0$, alors $z' = 0$ et on peut bien écrire $z' = uz$ pour tout u de \mathcal{U} .
 Sinon $qq' = 1$ montre que q et q' sont deux éléments de \mathcal{U} , inverses l'un de l'autre.
 - Conclusion : pour tous z, z' de \mathbb{Z}_i , $(z \parallel z' \text{ et } z' \parallel z) \Leftrightarrow \exists u \in \mathcal{U}, z' = uz$.
 [Q]