Les entiers de Gauss

Ce problème porte sur les sommes de deux carrés de nombres entiers. On note

$$\Sigma = \left\{x^2 + y^2,\ (x, y) \in \mathbb{Z}^2\right\}$$

On appelle *entier de Gauss* un nombre complexe dont la partie réelle et la partie imaginaire sont des entiers relatifs. On note $\mathbb{Z}[i]$ l'ensemble des entiers de Gauss.

$$\mathbb{Z}[i] = \left\{x + yi, (x, y) \in \mathbb{Z}^2\right\}$$

Partie I: Question préliminaire.

Vérifier que $\mathbb{Z}[i]$ est un sous-anneau de $\mathbb{C}$ contenant $\mathbb{Z}$ c'est à dire que

$$\mathbb{Z} \subset \mathbb{Z}[i], \quad \forall (z, z') \in \mathbb{Z}[i]^2 :\ z + z' \in \mathbb{Z}[i] \text{ et } zz' \in \mathbb{Z}[i]$$

On introduit dans $\mathbb{Z}[i]$ des définitions arithmétiques analogues à celles de $\mathbb{Z}$; on convient de les noter en préfixant par un « G- ». Par exemple :

— Soit $u \neq 0$ et v deux entiers de Gauss, on dit que u *G-divise* v si et seulement si il existe $w \in \mathbb{Z}[i]$ tel que $v = uw$.

— Soit u un entier de Gauss, on note $\mathbb{Z}[i]u$ l'ensemble des *G-multiples* de u.

$$\mathbb{Z}[i]u = \{wu, w \in \mathbb{Z}[i]\}$$

Partie II: Arithmétique des entiers de Gauss.

1. (a) Montrer que
$$\forall z \in \mathbb{Z}[i],\ |z|^2 \in \mathbb{N}; \qquad \forall (z, z') \in \mathbb{Z}[i]^2,\ |zz'|^2 = |z|^2 |z'|^2$$
   (b) Montrer que, pour tout entier n,
$$n \in \Sigma \Leftrightarrow \exists u \in \mathbb{Z}[i] \text{ tel que } n = |u|^2$$
   En déduire que le produit de deux éléments de Σ est dans Σ.
   (c) Soit $u \neq 0$ et z dans $\mathbb{Z}[i]$. Montrer que si u G-divise z alors $|u|^2$ divise $|z|^2$. (divisibilité dans $\mathbb{Z}$)
2. Un entier de Gauss u est dit *G-inversible* si et seulement si il existe $v \in \mathbb{Z}[i]$ tel que $uv = 1$.
   (a) Montrer que 1, -1, i, $-i$ sont G-inversibles, préciser les entiers de Gauss inverses.
   (b) Soit u un entier de Gauss G-inversible, montrer que $|u|^2 = 1$. En déduire l'ensemble des éléments G-inversibles.
3. Un entier de Gauss non nul et non G-inversible z est dit *G-irréductible* si et seulement si, pour tout G-diviseur v de z, $|v| = 1$ ou $|v| = |z|$.
   (a) Étudier le caractère G-irréductible de $1 + i$, de 5, d'un élément de Σ.
   (b) Montrer que tout entier de Gauss non nul et non G-inversible est G-divisible par un entier de Gauss G-irréductible. En déduire qu'il est le produit d'un G-inversible et de G-irréductibles.
4. *G-division euclidienne.*
   (a) Montrer que, pour tout $x \in \mathbb{R}$, il existe $a \in \mathbb{Z}$ tel que $|x - a| \leq \frac{1}{2}$.
   (b) Soit $u \neq 0$ et z dans $\mathbb{Z}[i]$, montrer qu'il existe q et r dans $\mathbb{Z}[i]$ tels que
$$z = qu + r \text{ avec } |r|^2 < |u|^2$$
   (On pourra considérer le nombre complexe $\frac{z}{u}$.)

Partie III: Réseaux.

LES ENTIERS DE GAUSS

Dans ce problème, un *réseau* est une partie de $\mathbb{Z}[i]$ stable pour l'addition. Autrement dit, une partie $\mathcal{R}$ de $\mathbb{Z}[i]$ est un réseau si et seulement si

$$\forall (z,z') \in \mathcal{R}^2,\ -z \in \mathcal{R} \text{ et } z+z' \in \mathcal{R}$$

Il est évident que $\mathbb{Z}[i]$ est stable par conjugaison et multiplication par i. On définit les applications c, s et r de $\mathbb{Z}[i]$ dans $\mathbb{Z}[i]$ par :

$$\forall z \in \mathbb{Z}[i],\ c(z)=\overline{z},\ s(z)=i\,\overline{z},\ r(z)=iz$$

Un réseau $\mathcal{R}$ est dit 4-*symétrique* si et seulement si il est stable par r c'est à dire :

$$\forall z \in \mathcal{R},\ r(z)=iz \in \mathcal{R}$$

Soit $n \geq 2$ un entier naturel. On définit $\mathcal{S}_n$ et $\mathcal{T}_n$ par :

$$\mathcal{S}_n = \{z \in \mathbb{Z}[i] \text{ tq } \Re(z) \equiv \Im(z) \mod n\},\ \mathcal{T}_n = \{z \in \mathbb{Z}[i] \text{ tq } \Im(z) \equiv 0 \mod n\}$$

5. Vérifier que $s \circ c = -c \circ s = r$.
6. Soit $u \in \mathbb{Z}[i]$. Montrer que $\mathbb{Z}[i]u$ est un réseau et qu'il est 4-symétrique.
   Un réseau $\mathcal{R}$ est dit *carré* si et seulement si il existe $u \in \mathbb{Z}[i]$ tel que $\mathcal{R} = \mathbb{Z}[i]u$. Comment peut-on justifier ce terme ?
7. Soit $n \geq 2$ un entier naturel. Montrer que $\mathcal{S}_n$ et $\mathcal{T}_n$ sont des réseaux. Pour quelles valeurs de n le réseau $\mathcal{S}_n$ est-il 4-symétrique ?
8. On se propose de montrer que tout réseau 4-symétrique est carré.
   Soit $\mathcal{R}$ un réseau 4-symétrique non réduit à 0.
   (a) Soit $u \in \mathcal{R}$. Montrer que tout G-multiple de u est dans $\mathcal{R}$.
   (b) Montrer qu'il existe $u_0 \in \mathcal{R}$ non nul tel que
   $$\forall v \in \mathcal{R},\ v \neq 0 \Rightarrow |u_0|^2 \leq |v|^2$$
   (c) Montrer que $\mathcal{R} = \mathbb{Z}[i]u_0$. Dans quel cas a-t-on $|u_0| = 1$?

Partie IV: Armures et satins.

Dans cette partie [1], p désigne un nombre premier et $a \in \mathbb{Z}$. On définit $\mathcal{R}_a$ par

$$\mathcal{R}_a = \left\{xp + yip + z(1+ia), (x,y,z) \in \mathbb{Z}^3\right\}$$

9. (a) Montrer que $\mathcal{R}_a$ est un réseau.
   (b) Montrer [2] que $\mathcal{R}_0 = \mathcal{T}_p$ et que $\mathcal{R}_1 = \mathcal{S}_p$.
   (c) Soit a et b dans $\mathbb{Z}$, montrer que
   $$\mathcal{R}_a = \mathcal{R}_b \Leftrightarrow a \equiv b \mod p$$
10. On suppose que $a \not\equiv 0 \mod p$. On dit dans ce cas que $\mathcal{R}_a$ est un *satin*.
    (a) Montrer qu'il existe $a' \in \mathbb{Z}$ tel que $aa' \equiv 1 \mod p$.
    (b) Montrer que $c(\mathcal{R}_a) = \mathcal{R}_{-a}$ et que $s(\mathcal{R}_a) = \mathcal{R}_{a'}$.
    (c) Montrer que si $a' \equiv -a \mod p$ alors $\mathcal{R}_a$ est carré.
    (d) Le réseau de la figure **??** est un satin. Déterminer p et a et vérifier qu'il est bien carré.
11. (a) Montrer que
    $$\forall (z,z') \in \mathbb{Z}[i]^2,\ \Im(\overline{z}z') \in \mathbb{Z}$$

1. D'après La géométrie des tissus d'Édouard Lucas. L'armure est le mode d'entrecroisement des fils de chaîne et des fils de trame. Les armures peuvent être représentées par des réseaux $\mathcal{R}_a$.
2. Notations $\mathcal{T}$ pour *toile* et $\mathcal{S}$ pour *serge* : des types particuliers de tissus.

(b) Montrer que

$$\forall (u,u') \in \mathcal{R}_a^2,\ \Im(\overline{u}\,u') \equiv 0 \mod p$$

En déduire que $\mathcal{R}_a \neq \mathbb{Z}[i]$.

(c) Montrer que, dans un satin $\mathcal{R}_a$, il existe u et u' tels que $\Im(\overline{u}\,u') = p$.

12. On suppose qu'il existe $a \in \mathbb{Z}$ tel que $a^2+1 \equiv 0 \mod p$.

(a) Montrer que $\mathcal{R}_a$ est carré.

(b) Montrer que p est la somme de deux carrés d'entiers.

Partie V: Sommes de deux carrés.

Notons $\mathcal{P}_c$ l'ensemble des nombres premiers p pour lesquels -1 est un carré modulo p c'est à dire tels que

$$\exists a \in \mathbb{Z} \text{ tel que } a^2+1 \equiv 0 \mod p$$

Notons $\mathcal{P}'_c$ l'ensemble des nombres premiers qui ne vérifient pas cette propriété. On forme ainsi une partition de l'ensemble $\mathcal{P}$ de tous les nombres premiers.

13. (a) Montrer que $\mathcal{P}_c \subset \Sigma$.

(b) Soit n entier naturel non nul. On considère sa décomposition en facteurs premiers. Montrer que si les valuations $v_p(n)$ sont paires pour les diviseurs premiers dans $\mathcal{P}'_c$, alors $n \in \Sigma$.

14. Soit p un nombre premier dans Σ avec $p = x^2+y^2$ pour x et y non nuls dans $\mathbb{Z}$.

(a) Montrer qu'il existe λ et μ dans $\mathbb{Z}$ tels que $\lambda x - \mu y = 1$. On pose $a = \lambda y + \mu x$.

(b) Exprimer x et y en fonction de λ, μ, a.

(c) Montrer que $(\lambda^2+\mu^2)p = 1+a^2$. En déduire que $p \in \mathcal{P}_c$.

15. Montrer que tout $p \in \mathcal{P}'_c$ est G-irréductible. En déduire, pour tout nombre premier p, l'équivalence entre les trois propositions.

$$p \in \Sigma \Leftrightarrow p \in \mathcal{P}_c \Leftrightarrow p \text{ n'est pas G-irréductible}$$

16. (a) Présenter un G-algorithme d'Euclide et justifier sa terminaison.

(b) Définir une notion de G-pgcd et énoncer un G-théorème de Bezout.

(c) Calculer un G-pgcd de $5+5i$ et de $-3+4i$.

17. (a) Énoncer et démontrer un G-théorème de Gauss.

(b) Soit $n \in \Sigma$ et $p \in \mathcal{P}'_c$ un diviseur premier de n. Montrer p^2 divise n et que le quotient est dans Σ. En déduire que $v_p(n)$ est pair.

Partie VI: Congruences modulo 4.

Cette partie utilise la définition de $\mathcal{P}_c$ de la partie IV mais aucun des résultats démontrés dans les parties précédentes. Soit $p > 2$ un nombre premier et $I = [\![1, p-1]\!]$.

18. Soit $x \in I$. Préciser l'unique élément de I congru à $-x$ modulo p. Montrer qu'il existe dans I un unique élément noté x' tel que $xx' \equiv 1 \mod p$. Cette notation est valable dans toute la partie.

19. On définit dans I une relation $\bowtie$ par :

$$\forall (x,y) \in I^2,\ x \bowtie y \Leftrightarrow (x^4+1)y^2 \equiv (y^4+1)x^2 \mod p$$

Montrer que $\bowtie$ est une relation d'équivalence.

20. (a) L'équation $x \equiv -x \mod p$ admet-elle une solution dans I ?

(b) Déterminer les $x \in I$ tels que $x = x'$.

(c) On considère l'équation $x = p - x'$ avec $x \in I$. Déterminer l'ensemble des solutions dans le cas où il existe $a \in I$ tel que $a^2+1 \equiv 0 \mod p$.
Que se passe-t-il lorsqu'il n'existe pas un tel a ?

21. Factoriser

$$(x^4+1)y^2 - (y^4+1)x^2$$

En déduire la classe d'équivalence pour $\bowtie$ d'un $x \in I$.

22. Montrer que $p \in \mathcal{P}_c$ si et seulement si $p \equiv 1 \mod 4$.

LES ENTIERS DE GAUSS

Partie I: Question préliminaire

Pour tout entier n, on peut écrire $n = n + 0i \in \mathbb{Z}[i]$. Pour tout $(z, z') \in \mathbb{Z}[i]^2$, comme $\Re(z)$, $\Im(z)$, $\Re(z')$, $\Im(z')$ sont entiers,

$$z + z' = \underbrace{\Re(z) + \Re(z')}_{\in\mathbb{Z}} + \underbrace{(\Im(z) + \Im(z'))}_{\in\mathbb{Z}} i \in \mathbb{Z}[i]$$
$$zz' = \underbrace{\Re(z)\Re(z') - \Im(z)\Im(z')}_{\in\mathbb{Z}} + \underbrace{(\Re(z)\Im(z') + \Im(z)\Re(z'))}_{\in\mathbb{Z}} i \in \mathbb{Z}[i]$$

Partie II: Arithmétique des entiers de Gauss.

1. (a) Les parties réelles x et y d'un entier de Gauss z sont entières donc $|z|^2 = x^2 + y^2$ est un entier naturel. Il est même dans Σ. La deuxième relation est une propriété classique des modules des nombres complexes.

   (b) On a vu que $|u|^2 \in \Sigma$ pour $u \in \mathbb{Z}[i]$. Réciproquement, si $n = x^2 + y^2$ avec x et y entiers, alors $n = |u|^2$ avec $u = x + iy \in \mathbb{Z}[i]$.
   Si n et m sont dans Σ, il existe u et v dans $\mathbb{Z}[i]$ tels que

   $$\left.\begin{array}{l} n = |u|^2 \\ m = |v|^2 \end{array}\right\} \Rightarrow nm = |u|^2|v|^2 = |uv|^2 \in \Sigma \text{ car } uv \in \mathbb{Z}[i]$$

   (c) Si u G-divise z, il existe $v \in \mathbb{Z}[i]$ tel que $z = uv$ donc $|z|^2 = |u|^2\,|v|^2$. Comme il s'agit d'une relation entre entiers, on en déduit que $|u|^2$ divise $|z|^2$ au sens habituel de la divisibilité entière.

2. (a) Des produits élémentaires se traduisent par des G-inversibilités.

   $$1 \times 1 = 1 \Rightarrow 1 \text{ inversible d'inverse } 1$$
   $$(-1) \times (-1) = 1 \Rightarrow -1 \text{ inversible d'inverse } -1$$
   $$i \times (-i) = 1 \Rightarrow \begin{cases} i \text{ inversible d'inverse } -i \\ -i \text{ inversible d'inverse } i \end{cases}$$

   (b) Soit u un entier de Gauss G-inversible et v son inverse. On en tire la relation dans $\mathbb{N}$: $|u|^2|v|^2 = 1$ qui entraîne que $|u|^2 = 1$. Réciproquement, si $u = x + iz$ (avec x et y entiers) est de module 1, la relation $x^2 + y^2 = 1$ entraîne que $|x| = 1$ et $y = 0$ ou $x = 0$ et $|y| = 1$. On en déduit que les éléments G-inversibles sont seulement ceux de module 1 c'est à dire 1, -1, i, $-i$.

3. (a) Si v est un G-diviseur de $1 + i$, il existe $u \in \mathbb{Z}[i]$ tel que $uv = 1 + i$. On en déduit la relation entière $|u|^2|v|^2 = 2$. Comme 2 est premier, on doit avoir $|u|^2 = 1$ ou $|u|^2 = 2$. Ce qui assure que $1 + i$ est G-irréductible.
   En revanche, $5 = 1 + 2^2 = (1 + 2i)(1 - 2i)$ n'est pas G-irréductible. De même pour un élément de Σ. Soit il est un carré soit une somme de deux carrés non nuls donc de la forme $u\,\overline{u}$ pour un entier de Gauss u.

   (b) Soit z un entier de Gauss ni nul ni G-irréductible. Considérons l'ensemble D des $|u|^2$ pour les diviseurs u non inversibles de z. C'est une partie non vide de $\mathbb{N}$ car $|z|^2 \in D$. Elle admet un plus petit élément m et il existe un G-diviseur u de z tel que $|u|^2 = m$. Si w non inversible est un G-diviseur de u, il vérifie $|d|^2 \leq |u|^2$. Mais il G-divise aussi z donc $|d|^2 \in D$ et $|u|^2 = m \leq |d|^2$. On en déduit $|d| = |u|$ donc u est G-irréductible.
   Soit z un entier de Gauss non nul et non inversible. On raisonne algorithmiquement en posant $z_0 = z$. Tant que z_k n'est pas inversible, il admet un diviseur G-irreductible u_k. Il existe $z_{k+1} \in \mathbb{Z}[i]$ tel que $z_k = u_k z_{k+1}$. Cet algorithme se termine car $|z_k|^2$ est un entier qui diminue strictement à chaque étape. Lorsque l'algorithme se termine, le dernier z_p est inversible et z est le produit de z_p et des G-irréductibles u_k.

4. (a) Tout réel x est dans l'intervalle défini par sa partie entière : $x \in [\lfloor x \rfloor, \lfloor x \rfloor[$. Suivant la place par rapport au milieu on prend pour a l'une ou l'autre des extrémités :

   $$a = \begin{cases} \lfloor x \rfloor & \text{si } \lfloor x \leq \rfloor x \lfloor x \leq \rfloor + \dfrac{1}{2} \\ \lfloor x \rfloor + 1 & \text{si } \lfloor x \rfloor + \dfrac{1}{2} < x < \lfloor x \rfloor + 1 \end{cases}$$

Un tel a est bien entier et vérifie $|x-a| \leq \frac{1}{2}$. On remarque que si x est demi-entier, deux entiers a sont possibles.

(b) Soit $u \neq 0$ et z deux entiers de Gauss. Notons x et y la partie réelle et la partie imaginaire du nombre complexe $\frac{z}{u}$ et a et b les nombres entiers relatifs dont l'existence est assurée par le a. et vérifiant

$$|x-a| \leq \frac{1}{2}, \quad |y-b| \leq \frac{1}{2}$$

Notons $q = a + ib$, c'est par définition un entier de Gauss. De plus,

$$\frac{z}{u} = x + iy = a + ib + (x-a) + i(y-b) \Rightarrow z = uq + r$$

avec $r = u((x-a) + i(y-b))$ donc $|r| \leq |u|\sqrt{\frac{1}{4}+\frac{1}{4}} = \frac{|u|}{\sqrt{2}} < |u|$ et $r = z - uq \in \mathbb{Z}[i]$. Cela prouve l'existence des q et r vérifiant la relation. On peut noter qu'il n'y a pas unicité du couple à cause des deux approximations possibles pour les nombres demi-entiers.

Partie III: Réseaux.

5. Pour tout $z \in \mathbb{Z}[i]$,
$$s \circ c(z) = s(\overline{z}) = i\,\overline{\overline{z}} = iz = r(z) = -\overline{i\overline{z}} = -c(s(z)) = -c \circ s(z)$$

6. Soit $u \in \mathbb{Z}[i]$ et z, z' deux G-multiples quelconques de u. Il existe w et w' dans $\mathbb{Z}[i]$ tels que $z = wu$, $z' = w'u$. Alors
$$-z = \underbrace{-w}_{\in\mathbb{Z}[i]}u, \quad z+z' = \underbrace{(w+w')}_{\in\mathbb{Z}[i]}u, \quad zz' = \underbrace{(ww'u)}_{\in\mathbb{Z}[i]}u, \quad iz = \underbrace{(iw)}_{\in\mathbb{Z}[i]}u$$
Donc $\mathbb{Z}[i]u$ est bien un réseau 4-symétrique.
Le terme carré est justifié par le fait que les points d'affixes dans $\mathbb{Z}[i]u$ sont ceux de coordonnées *entières* dans le repère $(O, \overrightarrow{u}, \overrightarrow{v})$ où $\overrightarrow{u}$ est le vecteur d'affixe u et $\overrightarrow{v}$ celui d'affixe iu.

7. Soit $n \in \mathbb{Z}^*$ et z, z' deux entiers de Gauss
$$\left.\begin{array}{rl} \Re(z) \equiv \Im(z) & \mod n \\ \Re(z') \equiv \Im(z') & \mod n \end{array}\right\} \Rightarrow \begin{cases} \Re(-z) \equiv \Im(-z) & \mod n \\ \Re(z+z') \equiv \Im(z+z') & \mod n \end{cases}$$
Donc $\mathcal{S}_n$ est un réseau. De même, les propriétés des congruences assurent que $\mathcal{T}_n$ est un réseau.
pour tout naturel $n \geq 2$, $1+i \in \mathcal{S}_n$. Si $\mathcal{S}_n$ est 4-symétrique, $i(1+i) = -1+i \in \mathcal{S}_n$. Donc
$$-1 \equiv 1 \mod n \Rightarrow 2 \equiv 0 \mod n \Rightarrow n = 2$$
Réciproquement, si $n = 2$, tout entier x est congru à son opposé modulo 2. Donc
$$\Re(z) \equiv \Im(z) \mod 2 \Rightarrow \Re(iz) = -\Im(z) \equiv \Re(z) = \Im(iz) \mod 2$$
Donc $\mathcal{S}_n$ est 4-symétrique si et seulement si $n = 2$.

8. Dans cette question, $\mathcal{R}$ est un réseau 4-symétrique.
(a) Soit $u \in \mathcal{R}$ et z un G-multiple de u. Il existe x et y dans $\mathbb{Z}$ tels que
$$z = (x+iy)u = xu + y(iu)$$
Exploitons les stabilités d'un réseau
$$xu = \left\{\begin{array}{ll} \underbrace{u+u+\cdots+u}_{x \text{ fois}} & \text{si } x \in \mathbb{N} \\ \underbrace{(-u)+(-u)+\cdots+(-u)}_{-x \text{ fois}} & \text{si } x \in \mathbb{Z}\setminus\mathbb{N} \end{array}\right\} \Rightarrow xu \in \mathcal{R}$$
Comme le réseau est 4-symétrique, on raisonne de même pour $iu \in \mathcal{R}$. En invoquant une dernière fois la stabilité pour l'addition, on peut conclure que $xu \in \mathcal{R}$. Ainsi $\mathbb{Z}[i]u \in \mathcal{R}$.

(b) Considérons l'ensemble $\mathcal{N}$ des $|u|^2$ pour les $u \neq 0$ de $\mathcal{R}$. C'est une partie non vide de $\mathbb{N}$. Elle admet un plus petit élément m. Il existe donc un $u_0 \in \mathcal{R}$ tel que $m = |u_0|^2$. Il vérifie la propriété de minimalité demandée.

(c) Soit $z \in \mathcal{R}$. Écrivons la G-division euclidienne de z par u_0. Il existe des entiers de Gauss q et r tels que

$$z = qu_0 + r \text{ avec } |r|^2 < |u_0|^2$$

Comme $r = z - qu_0$ avec $z \in \mathcal{R}$ et $qu_0 \in \mathcal{R}$ d'après la question a., on en tire $r \in \mathcal{R}$. Mais comme $|r|^2 < |u_0|^2$, la minimalité de $|u_0|^2$ entraîne que $r = 0$. On en déduit

$$\mathcal{R} = \mathbb{Z}[i]u_0$$

Le cas $|u_0| = 1$ ne se produit que si u_0 est inversible ce qui revient à $\mathcal{R} = \mathbb{Z}[i]$.

Partie IV: Armures et satins.

9. (a) Chaque élément de $\mathcal{R}_a$ est une combinaison à coefficients entiers de p, ip et $1+ia$. L'opposé d'un tel élément ou la somme de deux est encore une combinaison à coefficients entiers. Cela traduit que $\mathcal{R}_a$ est un réseau.

(b) Pour tout élément $z \in \mathcal{T}_p$, il existe $\lambda \in \mathbb{Z}$ tel que $\Im(z) = \lambda p$. On en déduit que

$$z = \Re(z) + i\lambda p = 0\,p + \lambda\,(ip) + \Re(z)(1 + 0\,i) \in \mathcal{R}_0$$

Réciproquement, pour tout $z \in \mathcal{R}_0$, il existe x, y, z dans $\mathbb{Z}$ tels que

$$z = xp + yip + z(1 + 0i) = xp + z + ypi \Rightarrow \Im(z) = yp \equiv 0 \mod p \Rightarrow z \in \mathcal{T}_p$$

Donc $\mathcal{R}_0 = \mathcal{T}_p$. De même,

$$\forall z \in \mathcal{S}_p,\ \exists \lambda \in \mathbb{Z} \text{ tq } \Im(z) = \Re(z) + \lambda p \Rightarrow z = \lambda p + 0ip + \Re(z)(1 + i) \in \mathcal{R}_1$$

$$\forall z \in \mathcal{R}_1,\ \exists (x, y, z) \in \mathbb{Z}^3 \text{ tq } z = xp + yip + z(1 + i)$$
$$\Rightarrow \Re(z) = xp + z \equiv \Im(z) = yp + z \mod p \Rightarrow z \in \mathcal{S}_p$$

Donc $\mathcal{R}_1 = \mathcal{S}_p$.

(c) Supposons $\mathcal{R}_a = \mathcal{R}_b$. Comme $1 + ia \in \mathcal{R}_a$, il existe des entiers x, y, z tels que

$$1 + ia = xp + yip + z(1 + ib) \Rightarrow \begin{cases} 1 = xp + z \\ a = yp + zb \end{cases}$$
$$\Rightarrow a = yp + (1 - xp)b = b + (y - xb)p \equiv b \mod p$$

Supposons $a \equiv b \mod p$. Il existe alors $\lambda \in \mathbb{Z}$ tel que $b = a + \lambda p$. On en déduit

$$1 + ib = \lambda p + 0ip + 1(1 + ia) \in \mathcal{R}_a \Rightarrow \mathcal{R}_b \subset \mathcal{R}_a$$

avec les stabilités. De $a = b - \lambda p$, on déduit l'autre inclusion de la même manière. D'où $\mathcal{R}_a = \mathcal{R}_b$.

10. Dans cette question, $a \not\equiv 0 \mod p$. Donc a *est premier* avec p car p est premier.

(a) Comme a est premier avec p, le théorème de Bezout assure de l'existence d'entiers a' et λ tels que

$$a'a + \lambda p = 1 \Rightarrow aa' \equiv 1 \mod p$$

(b) Soit $z \in c(\mathcal{R}_a)$. Il existe x, y, z entiers tels que

$$z = \overline{xp + yip + z(1 + ia)} = xp + (-y)ip + z(1 - ia) \in \mathcal{R}_{-a}$$

On en tire $c(\mathcal{R}_a) \subset \mathcal{R}_{-a}$. L'autre inclusion est analogue d'où $c(\mathcal{R}_a) = \mathcal{R}_{-a}$.
Pour montrer que $s(\mathcal{R}_a) \subset \mathcal{R}_{a'}$. Il suffit (à cause des stabilités) de prouver que $s(1 + ia) \in \mathcal{R}_{a'}$.
Par définition de a', il existe un entier λ tel que $1 = aa' + \lambda p$. Cela permet d'écrire :

$$s(1 + ia) = i(1 - ia) = a + i = a + (aa' + \lambda p)i = 0\,p + \lambda ip + a(1 + a'i) \in \mathcal{R}_{a'}$$

Comme a et a' jouent des rôles symétriques, on a de même $s(\mathcal{R}_{a'}) \subset \mathcal{R}_a$ et on conclut en remarquant que s est une involution ($s \circ s = \mathrm{Id}$).

(c) On suppose ici que $a' \equiv -a \mod p$. On va montrer que $\mathcal{R}_a$ est carré en montrant d'abord qu'il est 4-symétrique puis en utilisant II.4. (tout réseau 4-symétrique est carré).

$$\forall z \in \mathcal{R}_a,\ iz = c(s(z))$$

D'après la question b. : $s(z) \in \mathcal{R}_{a'}$ et $c(s(z)) \in \mathcal{R}_{-a'}$. Or $\mathcal{R}_{-a'} = \mathcal{R}_a$ car $a' \equiv -a \mod p$. Donc $iz \in \mathcal{R}_a$ c'est à dire que le réseau est 4-symétrique.

(d) L'énoncé nous dit que le réseau présenté dans la figure est un satin. On peut trouver le p en comptant les points entres deux éléments sur une même colonne (par exemple celle d'abscisse 2. On trouve $p = 17$. Le a (appelé *décochement*) se trouve en examinant le premier point de la colonne d'abscisse 1. On trouve $a = 4$. Comme $17 = 4^2 + 1$,

$$4 \times (4) \equiv -1 \mod 17 \Rightarrow 4 \times (-4) \equiv 1 \mod 17 \Rightarrow a' \equiv -a \mod 17$$

La condition de la question c. est réalisée. Le satin est carré ce qui se voit bien sur la figure.

11. (a) Pour des entiers de Gauss z et z', notons $x = \Re(z)$, $y = \Im(z)$, $x' = \Re(z)$, $y' = \Im(z')$. Ils sont tous entiers et

$$\Im(\overline{z}\, z) = xy' - x'y \in \mathbb{Z}$$

(b) Soit u et u' dans $\mathcal{R}_a$, il existe des entiers x, y, z, x', y', z' tels que

$$\left.\begin{array}{l} u = xp + z + i(yp + za) \\ u' = x'p + z' + i(y'p + z'a) \end{array}\right\} \Rightarrow \Im(\overline{u}\, u') = (xp + z)(y'p + z'a) - (yp + za)(x'p + z') \equiv 0 \mod p$$

car, dans le développement, les termes en $az'a$ s'annulent et p se met en facteur dans tous les autres.
Comme dans $\mathbb{Z}[i]$, on peut trouver des u et v tels que $\Im(\overline{u}\, u')$ soit non congru à p, on en déduit que $\mathcal{R}_a \neq \mathbb{Z}[i]$; par exemple pour $u = 1$ et $u' = i$, $\Im(\overline{u}\, u') = 1$.

(c) Comme $\mathcal{R}_a$ est un satin, il existe $a' \in \mathbb{Z}$ tel que $aa' \equiv 1 \mod p$ donc il existe $\lambda \in \mathbb{Z}$ tel que $1 = aa' + \lambda p$. Considérons deux éléments particuliers de $\mathcal{R}_a$

$$\left.\begin{array}{l} u = a'p + (-\lambda p)\, ip \\ u' = 1 + ia \end{array}\right\} \Rightarrow \Im(\overline{u}\, u') = a'pa + \lambda p^2 = p(1 - \lambda p) + \lambda p^2 = 1$$

Ces éléments particuliers ont été trouvés après une analyse effectuée au brouillon avec des coefficients indéterminés.

12. Dans cette question, on suppose qu'il existe a tel que $a^2 + 1 \equiv 0 \mod p$. On peut aussi écrire cette relation comme

$$a(-a) \equiv 1 \mod p$$

(a) Avec les notations de la question 2, on peut donc écrire $a' = -a$. On a montré dans ces conditions en III.2.c. que $\mathcal{R}_a$ est carré.

(b) Comme $\mathcal{R}_a$ est carré, il est engendré par un de ses éléments. Notons $u_0 \in \mathcal{R}_a$ tel que $\mathcal{R}_a = \mathbb{Z}[i]u_0$.
D'après la question II.3.c., il existe u et u' dans $\mathcal{R}_a$ tels que $\Im(\overline{u}\, u') = p$. Comme le réseau est carré, il existe des entiers de Gauss z et z' tels que $u = zu_0$, $u' = z'u_0$. On en déduit

$$p = \Im(\overline{z\, u_0}\, z'\, u_0) = \underbrace{\Im(\overline{z}z')}_{\in\mathbb{Z}}\underbrace{|u_0|^2}_{\in\mathbb{Z}}$$

On en déduit que $|u_0|^2$ divise p.
Il est impossible que $|u_0| = 1$ car on aurait $\mathcal{R}_a = \mathbb{Z}[i]$ (d'après I.5.c.) en contradiction avec II.3.a. On doit donc avoir $|u_0|^2 = p$. Or u_0 est un entier de Gauss, sa partie réelle et sa partie imaginaire sont entières donc p est la somme de deux carrés d'entiers.

Partie V: Sommes de deux carrés.

13. (a) Cette question est une simple reformulation de III.4.b.

    (b) Soit n un entier naturel non nul. On suppose que, dans sa décomposition en facteurs premiers, tous les exposants des $p \in \mathcal{P}'_c$ sont pairs. On veut montrer que $n \in \Sigma$ c'est à dire qu'il est somme de deux carrés.
    Le point important est la stabilité de Σ par multiplication (question I.1.b).

    — Chaque diviseur premier $p \in \mathcal{P}_c$ est d'après 1.a. un élément de Σ. Peu importe donc sa valuation, le produit de tous ces facteurs sera encore une somme de deux carrés.

    — Pour les diviseurs $p \in \mathcal{P}'_c$, les valuations sont paires. Leur produit sera un carré donc une somme de deux carrés en prenant le deuxième carré de la somme nul.

    Le produit de tous les diviseurs premiers sera bien une somme de deux carrés.

14. Soit p un nombre premier avec $p = x^2 + y^2$ pour des entiers x et y non nuls.

    (a) Les entiers x et y sont forcément premiers entre eux car, à cause de $p = x^2 + y^2$, tout diviseur commun divise aussi p. Cette relation interdit à p d'être un diviseur commun car p^2 diviserait alors p.
    Comme il sont premiers entre eux, le théorème de Bezout prouve l'existence d'entiers λ et μ vérifiant la relation demandée.

    (b) Exprimons les relation comme un système aux inconnues x et y puis résolvons le par les formules de Cramer.

$$\begin{cases} \lambda x - \mu y = 1 \\ \mu x + \lambda y = a \end{cases} \Rightarrow \begin{cases} x = \dfrac{\begin{vmatrix} 1 & -\mu \\ a & \lambda \end{vmatrix}}{\begin{vmatrix} \lambda & -\mu \\ \mu & \lambda \end{vmatrix}} = \dfrac{\lambda + a\mu}{\lambda^2 + \mu^2} \\ y = \dfrac{\begin{vmatrix} \lambda & 1 \\ \mu & a \end{vmatrix}}{\begin{vmatrix} \lambda & -\mu \\ \mu & \lambda \end{vmatrix}} = \dfrac{\lambda a - \mu}{\lambda^2 + \mu^2} \end{cases}$$

    (c) On remplace dans $p = x^2 + y^2$:

$$p = \frac{(\lambda + a\mu)^2 + (\lambda a - \mu)^2}{(\lambda^2 + \mu^2)^2} = \frac{(1 + a^2)\lambda^2 + (1 + a^2)\mu^2}{(\lambda^2 + \mu^2)^2} \Rightarrow p(\lambda^2 + \mu^2) = 1 + a^2$$

    On en déduit $1 + a^2 \equiv 0 \mod p$ c'est à dire $p \in \mathcal{P}_c$.

15. Soit p un nombre premier qui n'est pas G-irréductible. Il existe alors $u \in \mathbb{Z}[i]$ un G-diviseur de p tel que $|u|^2$ divise $|p|^2 = p^2$ (divisibilité dans $\mathbb{Z}$) avec $1 < |u|^2 < p^2$. On peut envisager seulement trois possibilités : $|u|^2 = 1$, $|u|^2 = p$, $|u|^2 = p^2$.
    Seule la deuxième est compatible avec les hypothèses sur u. On en déduit que $p \in \Sigma$. Par contraposition :

$$p \notin \Sigma \Rightarrow p \text{ G-irréductible}$$

    D'après la question 2. $p \in \Sigma$ entraîne $p \in \mathcal{P}_c$. Or $p \in \mathcal{P}'_c$ signifie $p \notin \mathcal{P}_c$ donc $p \notin \Sigma$. Avec la première implication on a bien montré

$$p \in \mathcal{P}'_c \Rightarrow p \text{ G-irréductible}$$

    On a montré en IV.1 que $p \in \mathcal{P}_c$ entraîne $p \in \Sigma$. On a montré en I.3. que $p \in \Sigma$ entraine que p n'est pas G-irréductible. On peut compléter la boucle d'implications car

$$(p \in \mathcal{P}'_c \Rightarrow p \text{ G-irréductible}) \Leftrightarrow (p \text{ non G-irréductible} \Rightarrow p \in \mathcal{P}_c)$$

    car $\mathcal{P}'_c$ est le complémentaire de $\mathcal{P}_c$ dans l'ensemble des nombres premiers.

16. (a) Les algorithmes d'Euclide (simple ou étendu) s'adaptent sans modification dans l'anneau des entiers de Gauss. On se donne deux entiers de Gauss non nuls u_0 et u_1 puis, tant que u_k est non nul, on divise u_{k-1} par u_k en nommant u_{k+1} le reste obtenu. Le seul point nouveau est qu'il n'y a pas unicité du reste et du quotient. Pour l'algorithme étendu, on utilise le quotient pour calculer deux suites, convenablement initialisée et permettant d'exprimer u_k comme combinaison de u_0 et u_1. La validité de l'algorithme est justifiée par le fait que l'ensemble des diviseurs communs à u_k et u_{k+1} est un invariant et que $|u_k|^2$ est une fonction de terminaison. Il faut noter que l'on doit prendre le carré du module pour rester dans $\mathbb{N}$.

(b) Soit u_0 et u_1 deux entiers de Gauss non nuls et u_p le dernier reste non nul du G-algorithme d'Euclide. L'ensemble des diviseurs communs à u_0 et u_1 est aussi l'ensemble des diviseurs de u_p qui est donc aussi celui dont le carré du module est le plus grand. On convient de le désigner comme un G-pgcd des deux. En multipliant u_p par un élément G-inversible on obtient un autre Gpgcd avec les mêmes propriétés.
En utilisant la version étendue du G-algorithme d'Euclide, on obtient λ et μ dans $\mathbb{Z}[i]$ tels que $u_p = \lambda u_0 + \mu u_1$.
Deux entiers de Gauss seront dits G-premiers entre eux si et seulement si leurs G-pgcd sont G-inversibles.
Si u et v sont G-premiers entre eux, en multipliant par l'inverse du G-pgcd, on obtient :

$$\exists(\lambda,\mu) \in \mathbb{Z}[i]^2 \text{ tq } \lambda u + \mu v = 1$$

(c) Division euclidienne de $u_0 = 5+5i$ par $u_1 = -3+4i$. On calcule le quotient complexe puis on l'approche au mieux par un entier de Gauss.

$$\frac{5+5i}{-3+4i} = \frac{(5+5i)(-3-4i}{25} = \frac{5-35i}{25} = \frac{1-7i}{5} = -i + \frac{1-2i}{5}$$

Comme aucun nombre demi-entier ne figure, une seule division euclidienne est possible : quotient $q_1 = i$, reste

$$u_2 = (-3+4i)\frac{1-2i}{5} = \frac{5+10i}{5} = 1+2i$$

Division euclidienne de u_1 par u_2.

$$\frac{u_1}{u_2} = \frac{-3+4i}{1+2i} = \frac{(-3+4i)(1-2i)}{5} = \frac{5+10i}{5} = 1+2i \in \mathbb{Z}[i]$$

Le reste est nul. Un G-pgcd est $1+2i$.

17. (a) Formulation du G-théorème de Gauss. Soit u, v, w non nuls dans $\mathbb{Z}[i]$. Si u est G-premier avec v et s'il G-divise vw alors il G-divise w. La démonstration est exactement la même que dans $\mathbb{Z}$ ou dans un anneau de polynômes.

(b) Soit $n \in \Sigma$ et $p \in \mathcal{P}'_c$ un diviseur premier de n. D'après la question 3., on sait que p est G-irréductible. Comme n est un carré d'entiers, il existe x et y entiers tels que $n = x^2+y^2 = z\,c(z)$ avec $z = x+iy$.
Comme p divise n, on peut dire aussi que p G-divise $zc(z)$.
Remarquons d'abord que, si p G-divise l'un des deux z ou $c(z)$, on montre qu'il G-divise aussi l'autre en conjuguant la relation de divisibilité.
Comme p est G-irréductible, s'il ne divise pas z il doit diviser $c(z)$ d'après le G-théorème de Gauss ce qui est absurde. Ainsi p G-divise z, il existe $\lambda \in \mathbb{Z}[i]$ tel que

$$\left.\begin{array}{l} z = \lambda p \\ c(z) = \overline{\lambda}\, p \end{array}\right\} \Rightarrow n = |\lambda|^2 p^2$$

Donc p^2 divise n et le quotient $|\lambda|^2$ est encore dans Σ.
Tant que le quotient admet au moins un diviseur premier dans $\mathcal{P}'_c$, on peut le diviser par le carré de ce diviseur. Cela prouve que la valuation d'un élément de Σ en un de ces diviseurs premiers doit être paire.

Partie VI: Congruences modulo 4.

18. Dans I chaque classe de congruence modulo p admet un unique représentant et tous les éléments de I sont premiers avec p.
Le seul représentant de la classe de $-x$ est $p-x$. On a déjà montré (théorème de Bezout) l'existence d'entiers z tels que $xz \equiv 1 \mod p$. Cette classe de congruence a un unique représentant dans I, on le note x'.

19. La réflexivité et la symétrie de $\bowtie$ sont évidentes d'après la définition de la relation. La transitivité devient aussi évidente lorsque l'on multiplie la définition par $(x'y')^2$:

$$x \bowtie y \Leftrightarrow (x^4+1)x'^2 \equiv (y^4+1)y'^2$$

LES ENTIERS DE GAUSS

20. (a) L'équation n'a pas de solution.

$$x \equiv -x \mod p \Rightarrow 2x \equiv 0 \mod p \Rightarrow p \text{ divise } 2x$$

Ce qui est impossible car p est premier avec 2 et x.

(b) L'équation admet deux solutions 1 et $p-1$. En effet 1 et $p-1$ sont bien solutions et

$$x = x' \Rightarrow x^2 \equiv 1 \mod p \Rightarrow (x-1)(x+1) \equiv 0 \mod p$$

d'où $x \equiv 1 \mod p$ ou $x \equiv -1 \mod p$.

(c) Dans le cas où il existe a tel que $a^2 + 1 \equiv 0 \mod p$, les solutions sont a et $p-a$.
En effet, on a alors

$$a^2 + 1 \equiv 0 \mod p \Rightarrow a(-a) \equiv 1 \mod p \Rightarrow a' \equiv -a \mod p \Rightarrow a' = p - a$$

Réciproquement

$$x = p - x' \Rightarrow x^2 \equiv -1 \mod p \Rightarrow x^2 \equiv a^2 \mod p$$

donc $x \equiv a \mod p$ ou $x \equiv -a \mod p$.
On a vu dans le calcul précédent que si x est solution alors $x^2 \equiv -1 \mod p$. Donc, s'il n'existe pas de a tel que $a^2 + 1 \equiv 0 \mod p$, l'équation n'a pas de solutions.

21. Factorisation :

$$(x^4+1)y^2 - (y^4+1)x^2 = x^2y^2(x^2-y^2) + y^2 - x^2 = (x^2-y^2)(x^2y^2-1)$$

On en déduit que la classe de x est l'ensemble des y annulant (modulo p) l'expression du dessus. Elle est donc formée par x et $p-x$ (qui annulent le x^2-y^2) et de x' et $p-x'$ (qui annulent le x^2y^2-1).

22. Le cœur de cette question est l'examen de la partition de I en classes d'équivalence. D'après la question précédente, chaque classe semble être formée de 4 éléments de la forme

$$x, \quad p-x, \quad x', \quad p-x'$$

Or ces éléments ne sont pas toujours deux à deux distincts. Les équations de la question 3. permettent de préciser les classes particulières avec moins de 4 éléments.

— La relation $x = p - x$ ne peut pas se produire.

— La relation $x = x'$ ne peut se produire que si $x = 1$ ou $p-1$. Cela conduit à une classe particulière $\{1, p-1\}$.

— La relation $x = p - x'$ ne peut se produire que si $p \in \mathcal{P}_c$. Dans ce cas elle conduit à une seule classe particulière : $\{a, p-a\}$.

En conclusion :

— Si $p \notin \mathcal{P}_c$. Il existe une seule classe particulière à deux éléments $\{1, p-1\}$. Toutes les autres (disons m) sont à 4 éléments. Par le principe du berger, on en déduit

$$p - 1 = 2 + m \times 4 \Rightarrow p \equiv 3 \mod p$$

— Si $p \in \mathcal{P}_c$. Il existe deux classes particulières à deux éléments $\{1, p-1\}$ et $\{a, p-a\}$. Toutes les autres (disons m) sont à 4 éléments. Par le principe du berger, on en déduit

$$p - 1 = 2 + 2 + m \times 4 \Rightarrow p \equiv 1 \mod p$$

On a bien démontré que si $p > 2$ est un nombre premier, -1 est un carré modulo p si et seulement si p est congru à 1 modulo 4.