Université d'Évry Val d'Essonne 2011-2012

M54 algèbre et arithmétique 2

Devoir à la maison — théorème des deux carrés

Le but du devoir est de montrer le résultat suivant, connu sous le nom de théorème des deux carrés (Fermat, 1640), en utilisant les propriétés de l'anneau $\mathbf{Z}[i]$*, appelé anneau des entiers de Gauss. On dit qu'un nombre entier* n *est somme de deux carrés s'il existe deux entiers* a *et* b *tels que* $n = a^2 + b^2$*.*

Théorème 1. *Soit* p *un nombre premier impair. Alors* p *est somme de deux carrés si et seulement si* $p = 1 \mod 4$*.*

Plus généralement, un entier $n \geqslant 1$ *est somme de deux carrés si et seulement si les exposants de tous les nombres premiers congrus à* -1 *modulo* 4 *sont pairs dans sa décomposition en facteurs premiers.*

1 Généralités sur $\mathbf{Z}[i]$

On note $\mathbf{Z}[i]$ le sous-anneau de $\mathbf{C}$ engendré par le nombre complexe i et N l'application de $\mathbf{Z}[i]$ dans $\mathbf{R}_+$ définie par $N(z) = z\bar{z} = |z|^2$.

1.1 Montrer que $\mathbf{Z}[i] = \{a + ib \text{ avec } (a, b) \in \mathbf{Z}^2\}$. Calculer $N(a + ib)$ et en déduire que l'image de N est l'ensemble des entiers qui sont somme de deux carrés. (En particulier, N prend en fait ses valeurs dans $\mathbf{N}$.)

1.2 Montrer que pour tous x et y dans $\mathbf{Z}[i]$ on a $N(xy) = N(x)N(y)$.

1.3 En déduire que si $x \in \mathbf{Z}[i]^\times$ est inversible, alors $N(x) = 1$.

1.4 Réciproquement, si $N(x) = 1$, en déduire que x est inversible dans $\mathbf{Z}[i]$. (*Indication : dans* $\mathbf{C}$*, exprimer* z^{-1} *en fonction de* $\bar{z}$ *et* $|z|$.)

1.5 En déduire que $\mathbf{Z}[i]^\times = \{1, -1, i, -i\}$.

1.6 Déduire de la question 1.2 que, si $N(x)$ est un nombre premier, alors x est irréductible dans $\mathbf{Z}[i]$.

1.7 Soient x et $y \neq 0$ dans $\mathbf{Z}[i]$. On considère le nombre complexe $z = x/y$ (qui n'appartient en général pas à $\mathbf{Z}[i]$) et les deux réels a et b tels que $z = a + ib$. On note a' l'entier le plus proche de a et b' l'entier le plus proche de b, puis $z' = a' + ib'$.

Montrer que $N(z - z') < 1$ et en déduire qu'il existe q et r dans $\mathbf{Z}[i]$ tels que $x = qy + r$ et $N(r) < N(y)$.

1.8 En déduire que $\mathbf{Z}[i]$ est principal et factoriel.

2 Décomposition des premiers dans $\mathbf{Z}[i]$

Le but de cette section est de montrer la proposition suivante. (On dit que x est un carré dans $\mathbf{F}_p$ s'il existe $y \in \mathbf{F}_p$ tel que $x = y^2$ dans $\mathbf{F}_p$.)

Proposition 2. *Soit p un nombre premier, alors p est irréductible dans $\mathbf{Z}[i]$ si et seulement si -1 n'est pas un carré dans $\mathbf{F}_p$.*

De plus, si p est réductible dans $\mathbf{Z}[i]$, sa décomposition est de la forme $p = q\bar{q}$ où q est irréductible dans $\mathbf{Z}[i]$.

2.1 Montrer que -1 est un carré dans $\mathbf{F}_2$. Calculer $N(1+i)$ et déduire de la question 1.6 que la proposition est vraie pour $p = 2$.

Désormais, p désignera un nombre premier impair (c'est-à-dire différent de 2).

2.2 On admet que $\mathbf{Z}[i]/(p) \approx \mathbf{F}_p[X]/(X^2+1)$. En déduire que l'idéal (p) de $\mathbf{Z}[i]$ est maximal si et seulement si l'idéal (X^2+1) de $\mathbf{F}_p[X]$ est maximal.

2.3 En déduire, en utilisant la question 1.8, que p est irréductible dans $\mathbf{Z}[i]$ si et seulement si X^2+1 est irréductible dans $\mathbf{F}_p[X]$.

2.4 En déduire la première partie de la proposition.

On suppose désormais que p est un nombre premier impair réductible dans $\mathbf{Z}[i]$ et on note $q = a + ib$ un diviseur de p irréductible dans $\mathbf{Z}[i]$.

2.5 Montrer que $\bar{q}$ est aussi un diviseur de p dans $\mathbf{Z}[i]$ et qu'il est aussi irréductible dans $\mathbf{Z}[i]$.

2.6 Si $q = \bar{q}$, montrer que $q = \pm p$. Pourquoi est-ce absurde ? De même, montrer qu'il n'est pas possible d'avoir $q = -\bar{q}$.

2.7 Si $q = i\bar{q}$, en déduire que $a = b$ puis que $N(q) = 2N(a)$ divise p. Pourquoi est-ce absurde ? De même, montrer qu'il n'est pas possible d'avoir $q = -i\bar{q}$.

2.8 Déduire des deux questions précédentes et de la question 1.5 que q et $\bar{q}$ ne sont pas associés.

2.9 En déduire que $q\bar{q}$ divise p dans $\mathbf{Z}[i]$.

2.10 Soit $r \in \mathbf{Z}[i]$ tel que $p = rq\bar{q}$. En calculant $N(p)$ de deux façons différentes, montrer que $N(r) = 1$ puis que $r = 1$.

3 Carrés dans $\mathbf{F}_p$

Le but de cette section est de montrer la proposition suivante. (On dit que x est un carré dans $\mathbf{F}_p$ s'il existe $y \in \mathbf{F}_p$ tel que $x = y^2$ dans $\mathbf{F}_p$.)

Proposition 3. *Soit p un nombre premier, alors -1 est un carré dans $\mathbf{F}_p$ si et seulement si $p \neq -1 \mod 4$.*

3.1 Montrer que la proposition est vraie pour $p = 2$.

On suppose désormais que p est un nombre premier impair et on note $q = (p-1)/2$ qui est donc un entier. On note C_p l'ensemble des carrés dans $\mathbf{F}_p^\times$.

3.2 Résoudre l'équation $x^2 = 1$ dans $\mathbf{F}_p$.

3.3 On considère l'application c de $\mathbf{F}_p^\times$ dans lui-même définie par $c(x) = x^2$. Montrer que c'est un morphisme de groupes, que $\ker c = \{1, -1\}$ et que $\operatorname{im} c = C_p$.

3.4 En déduire que $\operatorname{Card} C_p = q$.

3.5 Montrer que si x est un carré dans $\mathbf{F}_p^\times$, alors $x^q = 1$ dans $\mathbf{F}_p$.

3.6 Montrer que l'équation $x^q = 1$ a au plus q solutions dans $\mathbf{F}_p$. En déduire que x est un carré dans $\mathbf{F}_p^\times$ si et seulement si $x^q = 1$ dans $\mathbf{F}_p$.

3.7 En déduire la proposition.

4 Théorème des deux carrés

4.1 Déduire des deux propositions la première partie du théorème.

4.2 Soit $n \geqslant 1$ un entier et $n = p_1^{r_1} \cdots p_k^{r_k}$ sa décomposition en facteurs premiers dans $\mathbf{Z}$. On suppose les p_i numérotés de telle sorte que, pour un certain l, on a $p_1, \ldots, p_l$ non congrus à -1 modulo 4 et $p_{l+1}, \ldots, p_k$ congrus à -1 modulo 4.

Déduire des deux propositions que la décomposition de n en facteurs irréductibles dans $\mathbf{Z}[i]$ est de la forme $n = q_1^{r_1}(\bar{q}_1)^{r_1} \cdots q_l^{r_l}(\bar{q}_l)^{r_l} \cdot p_{l+1}^{r_{l+1}} \cdots p_k^{r_k}$.

4.3 En conservant les notations de la question précédente, on suppose que $r_{l+1}, \cdots, r_k$ sont pairs. Montrer qu'il existe $x \in \mathbf{Z}[i]$ tel que $n = N(x)$.

4.4 Réciproquement, montrer que s'il existe $x \in \mathbf{Z}[i]$ tel que $n = N(x)$, alors $r_{l+1}, \cdots, r_k$ sont pairs. (*Indication : considérer la décomposition de x et celle de $\bar{x}$, qui s'en déduit.*)

4.5 Conclure.