Agrégation interne. Cours P. Caldero.
Arithmétique.

L'ARITHMETIQUE DE $\mathbb{Z}[i]$

Dans la peau de Johann Carl Friedrich Gauss

L'idée de ce cours est de visiter les méthodes de l'arithmétique à travers des équations sur les entiers. L'outil principal de l'arithmétique est la divisibilité et tous ses avatars : idéaux, quotients... Effectivement, on peut définir la relation divise en disant que a divise b dans l'anneau commutatif A ssi b est dans l'idéal Aa, ou si $\bar{b}$ est nul dans A/Aa. En arithmétique, on travaille sur des anneaux, et un corps n'a que très peu d'intérêt puisqu'il n'a pas d'idéaux non triviaux.
Donnons tout de suite un exemple simple : on veut résoudre l'équation du second degré à inconnues entières $x^2 - y^2 = 15$, ou plus géométriquement on dit que l'on cherche les points entiers de l'hyperbole. La solution est simple si on pense à factoriser le membre de gauche et le membre de droite et si on connaît le théorème fondamental de l'arithmétique, théorème d'unicité de factorisation des nombres premiers. On trouve ainsi $(x+y, x-y) = (\epsilon, 15\epsilon)$, $(3\epsilon, 5\epsilon)$, $(5\epsilon, 3\epsilon)$, $(15\epsilon, \epsilon)$, avec $\epsilon = 1$ ou -1, et pour finir $(x, y) = (\pm 8, \pm 7)$, $(\pm 4, \pm 1)$.
On a donc appliqué la factorialité de $\mathbb{Z}$, qui dit qu'un nombre entier possède une unique factorisation en nombre premiers, mais il faut faire très attention à ce que signifie "unicité" et "nombre premiers". L'unicité n'est valable que si l'on considère un nombre premier *modulo les inversibles*. Par exemple, dans $\mathbb{Z}$, on a $3 \times 5 = (-3) \times (-5)$ et il n'y a vraiment unicité de la décomposition que si on assimile 3 et -3, 5 et -5. On voit donc que l'identité $(-1) \times (-1) = 1$ est génante pour l'application de notre théorème d'unicité, et c'est pour cela qu'il faudra comprendre un nombre premier comme une classe dont on choisit un représentant. Si on travaille sur l'anneau $\mathbb{Z}$, les inversibles sont 1 et -1, on choisit comme représentant un nombre positif. De la même manière, si on travaille sur l'anneau de polynômes $\mathbb{K}[X]$, où $\mathbb{K}$ est un corps, les inversibles sont les éléments de $\mathbb{K}^*$ et donc un polynôme premier (on dit irréductible) sera choisi unitaire.
Maintenant, si on veut résoudre l'équation $x^2 + y^2 = n$, où n est un paramètre, et appliquer la même méthode, il faut travailler dans l'anneau $\mathbb{Z}[i]$. Et on se posera de façon naturelle les questions : l'anneau $\mathbb{Z}[i]$ est-il factoriel ? Quelles sont ses unités (éléments inversibles) ? Quels sont ses éléments premiers ?
De même, si on veut résoudre l'équation $x^2 - 5y^2 = 2$, on sera amenés à travailler sur $\mathbb{Z}[\sqrt{5}]$, et si on veut résoudre l'équation $x^2 + 5y^2 = z^2$, on sera amenés à travailler sur $\mathbb{Z}[i\sqrt{5}]$, en se posant les mêmes questions. Dans la suite, nous allons nous intéresser tout particulièrement à l'anneau $\mathbb{Z}[i]$. Dans un premier temps, nous chercherons ses unités, nous montrerons qu'il est factoriel, à l'aide de la norme complexe. Puis nous donnerons deux applications de cette

étude. Une application concerne l'équation $x^2+y^2=n$, on la résoudra pour n premier et on verra que l'étude générale provient de ce cas particulier. Enfin, on regardera l'équation de Fermat $x^2+y^2=z^2$.

1 Généralités.

Soit A l'anneau $\mathbb{Z}[i]$ des entiers de Gauss.

La norme multiplicative

Il existe une application

$$N\ :\ \mathbb{Z}[i]\to\mathbb{N},\ \ z\mapsto N(z)=z\bar{z}$$

qui vérifie

$$N(zz')=N(z)N(z')$$

Elle va bien entendu nous servir à partir d'un ensemble $\mathbb{Z}[i]$ que l'on connait mal, pour arriver vers un $\mathbb{N}$ que l'on connaît bien, sans perdre ses propriétés multiplicatives.

Le groupe des unités $\mathbb{Z}[i]^*$

On note $\mathbb{Z}[i]^*$ l'ensemble de éléments inversibles de $\mathbb{Z}[i]$ (il faut que leur inverse soit dans $\mathbb{Z}[i]$!). On vérifie facilement que c'est un groupe pour la multiplication. On a

$$\mathbb{Z}[i]^*=\{z\in\mathbb{Z}[i],\ N(z)=1\}=\{1,i,-1,-i\}$$

Prouvons ces égalités.
Une inclusion est claire : si z vérifie $N(z)=1$, alors $z\bar{z}=1$ et donc z est bien inversible dans $\mathbb{Z}[i]$ puisque $\bar{z}\in\mathbb{Z}[i]$.
Pour l'inclusion inverse, supposons z inversible dans $\mathbb{Z}[i]$, alors il existe z' dans $\mathbb{Z}[i]$ tel que $zz'=1$, en prenant la norme, on obtient $N(z)N(z')=1$, donc $N(z)$ est un inversible de $\mathbb{N}$, d'où $N(z)=1$.
Pour la seconde égalité, il suffit de remarquer que $N(z)=1$, $z=a+ib$ donne $a^2+b^2=1$ et donc a ou b vaut zero par positivité du carré.

L'anneau $\mathbb{Z}[i]$ est principal donc factoriel

C'est surtout factoriel qui va nous servir, mais on va montrer plus : $\mathbb{Z}[i]$ est muni d'une division euclidienne, donc principal,... et donc factoriel. Cette preuve est très classique et est à bien connaître
Preuve : Soit I un idéal de A et z_0 un élément de I de norme minimale non nulle.
Montrons que $I=Az_0$.
L'inclusion inverse est claire puisque z_0 est dans I et que I est un idéal.
Réciproquement, soit z dans I, montrons que z_0 divise z. Pour cela, on pose $x=\frac{z}{z_0}$. x appartient a priori à $\mathbb{Q}[i]$, mais il faut montrer qu'il est en fait dans $\mathbb{Z}[i]$. En faisant un petit dessin, on voit que tout complexe se situe à une distance inférieure à $\sqrt{2}/2$ d'un élément de $\mathbb{Z}[i]$. Donc, il existe un q de $\mathbb{Z}[i]$ tel que $N(x-q)\leq\sqrt{2}/2<1$. Posons $r=x-q$ de sorte

que $\frac{z}{z_0} - q = r$ et $N(r) < 1$. Il en résulte que

$$N(z - z_0 q) = N(rz_0) = N(r)N(z_0) < N(z_0)$$

Or $z - z_0 q \in I$ et par minimalité, $N(z - z_0 q) = 0$, d'où $z = z_0 q \in Az_0$. Conclusion tout idéal est principal.

On vient donc de voir que $\mathbb{Z}[i]$ est principal, car euclidien, et donc factoriel. Notons un grand classique : le passage d'euclidien à factoriel passe par l'identité de Bezout, puis le lemme de Gauss, et enfin la preuve besogneuse de l'unicité de la décomposition en irréductibles, l'existence de la décomposition étant une simple formalité.

Peut-être serait il bien de rappeler quelques propriétés des anneaux factoriels :

• Dans un anneau factoriel, tout élément se décompose de façon "unique" en éléments irréductibles.
• Dans un anneau factoriel, un élément est premier ssi il est irréductible. (irréductible=ne se décompose pas en produit d'éléments non inversibles, p premier=si p divise ab alors p divise soit a, soit b. Attention, premier et irréductible excluent que le nombre soit inversible !)
• Dans un anneau factoriel, si deux premiers distincts (à unité près) divisent a alors leur produit divise a.

2 Deux applications classiques.

Soit p un nombre premier différent de 2.

$$\boxed{p \text{ est somme de deux carrés ssi } p \equiv 1\,[4]}$$

"$\Longrightarrow$"
C'est la partie simple si on connait le symbole de Legendre. Supposons donc $p = a^2 + b^2$, avec $0 < a, b < p$, on a alors $\bar{a}^2 + \bar{b}^2 = 0$ dans $\mathbb{Z}/p\mathbb{Z}$ et $\bar{a}$, $\bar{b}$ sont tous deux non nuls dans le corps $\mathbb{Z}/p\mathbb{Z}$ donc inversibles. Il vient $(\bar{a}\bar{b}^{-1})^2 = -1$, donc -1 est un carré et donc avec le symbole de Legendre

$$(-1)^{\frac{p-1}{2}} = \left(\frac{-1}{p}\right) = 1$$

Ceci implique que $(p-1)/2$ est pair et donc $p \equiv 1\,[4]$.
"$\Longleftarrow$"
On suppose que p est congru à 1 modulo 4 et donc que -1 est un carré modulo p d'après ce qui précède. Il existe donc un $\bar{\omega}$ dans $\mathbb{Z}/p\mathbb{Z}$ tel que $\bar{\omega}^2 = -1$ et on peut choisir un représentant ω dans $\mathbb{Z}$ tel que $|\omega| \leq p/2$. On a donc $-1 = \omega^2 - kp$, avec k dans $\mathbb{Z}$ et il vient $kp = (\omega - i)(\omega + i)$. En prenant la norme, on obtient $N(\omega \pm i) = \omega^2 + 1 \leq p^2/4 + 1 < p$, donc $\omega \pm i \notin p\mathbb{Z}[i]$, alors que leur produit $(\omega + i)(\omega - i) \in Ap$. Il en résulte que p n'est pas premier, or dans un anneau factoriel, un nombre est irréductible ssi il est premier, donc p est réductible. Dit autrement, p peut donc se décomposer en produit de deux entiers de Gauss non inversibles, $p = zz'$.
Soit α un facteur irréductible de z, montrons que α et $\bar{\alpha}$ sont deux premiers distincts (modulo

les inversibles) de A. Il suffit de montrer que $\frac{\alpha}{\bar{\alpha}} \neq 1, i, -1, -i$ et on voit facilement que cela revient à montrer que α n'est ni dans $\mathbb{Z}$, ni dans $i\mathbb{Z}$, ni multiple de $(1+i)$. Les deux premiers sont impossibles car p est premier dans $\mathbb{Z}$ (on aurait $p = k.k'z'$, où k est un entier et $N(z') > 1$), le dernier est impossible car en prenant la norme on aurait que 2 divise p^2. Conclusion, α et $\bar{\alpha}$ sont bien deux premiers distincts (à unité près).
Ceci permet de conclure puisque dans un anneau factoriel, on obtient que $\alpha\bar{\alpha}$ divise p mais cette divisibilité est cette fois-ci dans $\mathbb{Z}$ et donc c'est une égalité (au signe près) puisque p est premier. Il vient $p = (a+ib)(a-ib) = a^2 + b^2$.

Remarque : L'ensemble des entiers qui peuvent s'écrire sous forme de somme de deux carrés est une partie de $\mathbb{N}$ stable par multiplication car

$$(a^2+b^2)(c^2+d^2) = (ac-bd)^2 + (ad+cb)^2$$

Cette formule que l'on peut facilement vérifier à la main, provient aussi de la multiplicativité de la norme complexe $N(z)N(z') = N(zz')$.

On en déduit ensuite sans trop de difficulté qu'un entier positif n est somme de deux carrés ssi $n = \prod p_i^{\alpha_i}$ avec α_i pair lorsque $p_i \equiv 3\,[4]$.

Résolution de l'équation $x^2 + y^2 = z^2$ dans $\mathbb{Z}$

C'est une équation déjà résolue par Pythagore puisque les solutions (x, y, z) sont appelées "triplets pythagoriciens". Une méthode géométrique consiste à diviser par z pour obtenir l'équation $X^2 + Y^2 = 1$, et se ramener à chercher les points rationnels d'un cercle par projection sur la tangente. Ici, c'est la méthode arithmétique que l'on va utiliser. L'idée étant de factoriser le membre de gauche en $(x+iy)(x-iy) = z^2$ et d'utiliser l'unicité de la décomposition en facteurs premiers dans $\mathbb{Z}[i]$.

Commençons par se ramener au cas où x et y sont premiers entre eux. Pour cela, soit d le pgcd de x et y, on a alors en divisant par d^2 l'équation $(\frac{x}{d})^2 + (\frac{y}{d})^2 = (\frac{z}{d})^2$. $\frac{x}{d}$ et $\frac{y}{d}$ sont des entiers, donc $(\frac{z}{d})^2$ est un entier, or le carré d'un rationnel n'est entier que si ce rationnel est lui-même entier, donc $\frac{z}{d}$ est entier et d divise z. On peut donc poser $X = \frac{x}{d}$, $Y = \frac{y}{d}$, $Z = \frac{z}{d}$ et on doit maintenant résoudre $X^2 + Y^2 = Z^2$, où cette fois X et Y sont premiers entre eux. On factorise donc dans $\mathbb{Z}[i]$: $(X+iY)(X-iY) = Z^2$. Maintenant, si on arrive à montrer que $(X+iY)$ et $(X-iY)$ n'ont pas de facteurs commun dans A, alors ceci impliquera, en décomposant les deux membres en facteurs premiers, que $(X+iY)$ est un carré.
Supposons donc que α est un diviseur premier commun à $(X+iY)$ et $(X-iY)$. Alors $\bar{\alpha}$ divise aussi $(X+iY)$ et $(X-iY)$. Montrons tout d'abord que α et $\bar{\alpha}$ sont deux premiers distincts (à unité près), c'est à dire que $\frac{\alpha}{\bar{\alpha}} \neq 1, i, -1, -i$ et cela revient à montrer comme précédemment que α n'est ni dans $\mathbb{Z}$, ni dans $i\mathbb{Z}$, ni multiple de $(1+i)$. Or, α ne peut pas être dans $\mathbb{Z}$ ni dans $i\mathbb{Z}$ puisque α est non inversible, divise $(X+iY)$ et X, Y sont premiers entre eux.
Montrons par l'absurde que α ne peut pas être multiple de $(1+i)$. On aurait donc $(1+i)$ divise $(X+iY)$ et en prenant la norme cela donne que 2 divise X^2+Y^2, donc 2 divise Z^2, donc 2 divise Z, du coup, 4 divise Z^2 et donc 4 divise X^2+Y^2. Cela implique que X et Y sont de même parité, et comme ils sont premiers entre eux, il vient que X et Y sont tous deux

impairs. Posons $X = 2k+1, Y = 2l+1$, alors 4 divise $(2k+1)^2+(2l+1)^2 = 4k^2+4l^2+4k+4l+2$, ce qui est impossible.
Conclusion, α et $\bar{\alpha}$ sont deux premiers distincts (à unité près) et comme ils divisent tous deux $X + iY$, leur produit $\alpha\bar{\alpha}$ divise $X + iY$ également. Mais $\alpha\bar{\alpha}$ est non inversible dans $\mathbb{Z}$ et ceci est encore une fois impossible puisque X et Y sont premiers entre eux. Nous avons donc montré par l'absurde que $(X + iY)$ et $(X - iY)$ n'ont pas de facteur commun et donc $X + iY$ est bien un carré.
On a donc $X + iY = u(a + ib)^2$, où $u = 1, i, -1, -i$.
Cela donne au final : $(x, y, z) = (d(a^2 - b^2), 2dab, d(a^2 + b^2))$, $(2dab, d(a^2 - b^2), d(a^2 + b^2))$, où a,b,d décrivent $\mathbb{Z}$.

Remarque. L'équation $x^2+2y^2 = z^2$ dans $\mathbb{Z}$ impose de travailler dans $\mathbb{Z}[i\sqrt{2}]$ qui est encore principal (faire un dessin pour représenter le réseau $\mathbb{Z}[i\sqrt{2}]$ et reproduire la preuve pour $\mathbb{Z}[i]$). Si on pense à la célèbre équation de Fermat $x^n+y^n = z^n$ qui a donné tant de fil à retordre aux mathématiciens des deux siècles derniers, on voit bien l'angle d'attaque naturel du problème : travailler dans l'anneau $\mathbb{Z}[\omega]$ où ω est une racine primitive n-ième de -1 et factoriser le membre de gauche. Malheureusement, l'anneau $\mathbb{Z}[\omega]$ n'est en général pas factoriel. Ce n'est pas un crime de lèse-mathématicien, ni une élucubration fumeuse à la Da Vinci Code, de supposer qu'il s'agit là de l'erreur originale de Fermat ("ma preuve inouye qui ne tiendrait pas dans la marge") d'avoir cru naïvement à la factorialité de cet anneau. On voit donc là toute la subtilité de la notion d'anneau factoriel qui n'a pas échappé au prince des mathématiciens Johann Carl Friedrich Gauss.