Université Pierre et Marie Curie M1 théorie des nombres Année 2007-2008

Premiers de la forme $x^2 + ny^2$

Dans la première feuille d'exercices, nous avons traité le cas $n = 1$, i.e. un nombre premier p est somme de deux carrés si et seulement si $p \equiv 1 \mod 4$. La preuve découlait de l'étude de l'anneau euclidien $\mathbb{Z}[i]$. La même étude sur $\mathbb{Z}[i\sqrt{2}]$ et $\mathbb{Z}[i\sqrt{3}]$ donne de la même façon les résultats suivants :

$$\begin{aligned} p = x^2 + y^2 &\Leftrightarrow p \equiv 1 \mod 4 \\ p = x^2 + 2y^2 &\Leftrightarrow p \equiv 1, 3 \mod 8 \\ p = x^2 + 3y^2 &\Leftrightarrow p = 3 \text{ ou } p \equiv 1 \mod 3 \end{aligned}$$

Nous allons, suivant [**1**], présenter le résultat pour n quelconque en suivant plus ou moins l'historique des différentes techniques. Les dates de retour des devoirs sont indiquées dans le texte, un corrigé sera fourni au fur et à mesure pour que vous ne restiez pas bloqué : par ailleurs il vous est vivement conseillé de vous référer à [**1**].

1. Descente infinie à la Fermat

Nous allons présenter la preuve d'Euler du cas $n = 1$ dont on pense qu'elle était similaire à celle de Fermat. Celle-ci est basée sur les deux étapes suivantes :

- *descente* : si $p|x^2 + y^2$ avec $x \wedge y = 1$ alors p peut s'écrire sous la forme $a^2 + b^2$;
- *réciprocité* : si $p \equiv 1 \mod 4$ alors il existe $x \wedge y = 1$ tel que $p|x^2 + y^2$.

1.1. Preuve de la descente. —

(1) soit $N = x^2 + ny^2$ avec $x \wedge y = 1$ et soit $q = a^2 + nb^2$ un diviseur premier de N ; montrez que N/q s'écrit aussi sous la forme $c^2 + nd^2$ avec $c \wedge d = 1$.

(2) Soit p premier divisant $N = x^2 + y^2$ avec $x \wedge y = 1$.
   (i) Montrez que l'on peut se ramener à $N < p^2/2$.
   (ii) En utilisant (1), montrez par un raisonnement de descente, que si $p|N$ alors p peut s'écrire sous la forme $a^2 + b^2$.

1.2. Preuve de la réciprocité. — Soit $p = 4k + 1$, montrez en utilisant le théorème de Fermat qu'il existe x, y tels que $p|x^2 + y^2$.

Remarque : en suivant la même stratégie, Euler a montré les cas $n = 2$ et 3.

Remarque : l'étape qui causa le plus de difficultés à Euler fut celle de la réciprocité qui consiste à résoudre $p|x^2 + ny^2$ en termes de congruence sur p modulo $4n$. Cela le conduisit à la loi de réciprocité quadratique prouvée en toute généralité par Gauss : en effet $p|x^2 + ny^2$ est équivalent à $(\frac{-n}{p}) = 1$ et donc à des congruences sur p modulo $4n$.

Remarque : $p|x^2 + ny^2$ n'implique pas forcément que p soit de la forme $a^2 + nb^2$; prendre par exemple $3|21 = 1^2 + 5.2^2$ mais $3 \neq x^2 + 5y^2$. La résolution de ce problème est l'objet du paragraphe 2.2.

2. Travaux Lagrange et Legendre sur les formes quadratiques

Rappelons qu'une forme quadratique définie positive $f(x, y) = ax^2 + bxy + cy^2$ est dite *primitive* si $a \wedge b \wedge c = 1$. Dans la suite toutes les formes quadratiques considérées seront primitives. Un entier m est *représenté* par $f(x, y)$ si l'équation $m = f(x, y)$ a des solutions entières ; s'il existe une solution avec $x \wedge y = 1$, alors m est dit *proprement représenté* par $f(x, y)$.

Définition 2.1. — Deux formes quadratiques $f(x,y)$ et $g(x,y)$ sont dites géométriquement équivalentes (resp. proprement géométriquement équivalentes) s'il existe $\begin{pmatrix} p & q \\ r & s \end{pmatrix} \in GL_2(\mathbb{Z})$ (resp. $SL_2(\mathbb{Z})$) telle que $f(x,y) = g(px+qy, rx+sy)$. Elles sont dites arithmétiquement équivalentes si elles représentent les mêmes entiers avec la même multiplicité, i.e. si les multi-ensembles

$$\{(m, n_f(m)) \in \mathbb{Z} \times \mathbb{N} :\ n_f(m) = \mathrm{card}\{(x,y) \in \mathbb{Z}^2 :\ m = f(x,y)\}\} =$$
$$\{(m, n_g(m)) \in \mathbb{Z} \times \mathbb{N} :\ n_g(m) = \mathrm{card}\{(x,y) \in \mathbb{Z}^2 :\ m = g(x,y)\}\}.$$

Remarque : soit A la matrice de f, i.e. $f(x,y) = {}^tXAX$ avec ${}^tX = (x,y)$. Notons $\sqrt{A}$ la racine carrée positive de A de sorte que, comme $f(x,y) = |\sqrt{A}X|^2$, les entiers représentés par f sont les carrés des longueurs des éléments du réseau $\Gamma_f = \sqrt{A}\mathbb{Z}^2$.

2.1. Un théorème de Gauss. — Le but de cette partie est de montrer le résultat suivant du à Gauss : *deux formes quadratiques positives $f(x,y)$ et $g(x,y)$ sont géométriquement équivalentes si et seulement si elles sont arithmétiquement équivalentes.*

(1) Montrez que si f, g sont géométriquement équivalentes alors elles sont arithmétiquement équivalentes.
(2) Réciproquement, soient $\Gamma_f = \sqrt{A}\mathbb{Z}^2$ et $\Gamma_g = \sqrt{B}\mathbb{Z}^2$ les réseaux associés à f et g. Montrez que l'aire $\mu(\Gamma_f)$ d'un domaine fondamental de Γ_f est égale à $\mu(\Gamma_g)$.
(3) Montrez qu'il existe une isométrie u telle que $\Gamma_g = u(\Gamma_f)$.
(4) Montrez le résultat de Gauss énoncé plus haut.

2.2. Nombres représentés par des formes quadratiques. —

(1) Montrez qu'une forme quadratique $f(x,y)$ représente proprement $m \in \mathbb{N}$ si et seulement s'il existe $b, c \in \mathbb{Z}$ tels que $f(x,y)$ est proprement géométriquement équivalente à la forme quadratique $mx^2 + bxy + cy^2$.
(2) Soient n un entier et p premier ne divisant pas n. Montrez que $-n$ est un carré modulo p si et seulement si p est représenté par une forme quadratique primitive de discriminant $-4n$.

A rendre pour le 22 février

2.3. Formes réduites. — En vue de généraliser l'énoncé de descente, on est amené à considérer les formes quadratiques de discriminant fixé. Pour se ramener à un nombre fini, Lagrange a introduit la notion de forme quadratique réduite.

Définition 2.2. — Une forme quadratique primitive, donc définie positive, $ax^2 + bxy + cy^2$ est dite *réduite* si

$$|b| \leq a \leq c, \text{ et } b \geq 0 \text{ si } |b| = a \text{ ou } a = c.$$

Remarque : $x^2 + ny^2$ est une forme réduite de discriminant $-4n$. Plus généralement pour $D \equiv 0 \mod 4$ (resp. $D \equiv 1 \mod 4$), la forme $x^2 - \frac{D}{4}y^2$ (resp. $x^2 + xy + \frac{1-D}{4}y^2$) est une forme réduite de discriminant D que l'on appelle **la forme principale** de discriminant D.

(1) Montrez que toute forme quadratique primitive définie positive est proprement équivalente à une unique forme réduite.
(2) Pour $D < 0$, on note $h(D)$ *le nombre de formes quadratiques primitives positives définies réduites de discriminant D*. Montrez que $h(D)$ est fini.

(3) Il s'agit de prouver le **théorème de Landau** : pour $n \in \mathbb{N}$, on a $h(-4n) = 1 \Leftrightarrow n = 1, 2, 3, 4, 7$.
   (i) Montrez que pour $n = 1, 2, 3, 4, 7$, on a $h(-4n) = 1$.
   (ii) Supposons que n n'est pas la puissance d'un nombre premier, i.e. $n = ac$ avec $1 < a < c$ et $a \wedge c = 1$; montrez que la forme $ax^2 + cy^2$ est réduite de discriminant $-4ac = -4n$.
   (iii) Pour $n = 2^r$ et $r \geq 4$, montrez que $4x^2 + 4xy + (2^{r-2} + 1)y^2$ est primitive, réduite et de discriminant $4^2 - 4.4(2^{r-2} + 1) = -16.2^{r-2} = -4n$.
   (iv) Pour $n = 8$, montrez que $h(-32) = 2$.
   (v) Pour $n = p^r \neq 3, 7$ avec p premier impair, montrez que si on a $n + 1 = ac$ avec $1 < a < c$ et $a \wedge c = 1 =$, alors $ax^2 + 2xy + cy^2$ est réduite de discriminant $2^2 - 4ac = 4 - 4(n + 1) = -4n$.
   (vi) Pour $n = p^r$ et $n + 1 = 2^s$, montrez que $8x^2 + 6xy + (2^{s-3} + 1)y^2$ est primitive réduite de discriminant $-4n$.
   (vii) Concluez, en admettant que $h(-4.31) = 3$.

(4) Montrez que

$$p = x^2 + 7y^2 \Leftrightarrow (\frac{-n}{7}) = 1 \Leftrightarrow p \equiv 1, 9, 11, 15, 23, 25 \mod 28.$$

2.4. Genre d'une forme quadratique. —

Définition 2.3. — (**Lagrange**) Deux formes quadratiques primitives définies positives de discriminant D sont dites de même genre si elles représentent les mêmes valeurs dans $(\mathbb{Z}/D\mathbb{Z})^\times$.

Exemples : pour $D = -20$, $x^2 + 5y^2$ représente $1, 9 \in (\mathbb{Z}/20\mathbb{Z})^\times$ et $2x^2 + 2xy + 3y^2$ représente $3, 7 \in (\mathbb{Z}/20\mathbb{Z})^\times$. Pour $D = -56$, on a

$$\begin{array}{rll} x^2 + 14y^2,\ 2x^2 + 7y^2 & \text{représentent} & 1, 9, 14, 23, 25, 29 \in (\mathbb{Z}/56\mathbb{Z})^\times \\ 3x^2 \pm 2xy + 5y^2 & \text{représentent} & 3, 5, 13, 19, 27, 45 \in (\mathbb{Z}/56\mathbb{Z})^\times \end{array}$$

On observe donc que les genres ne sont pas forcément réduit à un élément. Cependant il semble que les valeurs représentées forment des ensembles disjoints ce que nous allons montrer.

(1) Soit $D < 0$ tel que $D \equiv 0, 1 \mod 4$. On note $\chi : (\mathbb{Z}/D\mathbb{Z})^\times \to \{\pm 1\}$ l'homomorphisme défini par le symbole de Jacobi, i.e. $\chi(\bar{n}) = (\frac{D}{n})$ où $n \in \bar{n}$ est impair [(1)].
   (i) Soit m premier à D qui est représenté par une forme $f(x, y)$ de discriminant D : montrez que $\bar{m} \in \operatorname{Ker} \chi$.
   (ii) Montrez que les valeurs de $(\mathbb{Z}/D\mathbb{Z})^\times$ représentées par la forme principale de discriminant D est un sous groupe $H \subset \operatorname{Ker} \chi$.

(2) Soit $f(x, y)$ une forme quadratique et M un entier ; montrez que $f(x, y)$ représente proprement un nombre premier à M.

(3) Montrez que les valeurs de $(\mathbb{Z}/D\mathbb{Z})^\times$ représentées par une forme primitive définie positive de discriminant D forment une classe dans $\operatorname{Ker} \chi / H$.

Remarque : pour H' une classe dans $\operatorname{Ker} \chi / H$, le genre de H' est l'ensemble des formes quadratiques réduites de discriminant D dont les valeurs représentées sont $H' \subset \operatorname{Ker} \chi \subset (\mathbb{Z}/D\mathbb{Z})^\times$. Si le genre de la forme principale est réduit à un seul élément, l'étape de descente se résoud alors simplement en terme de congruences. On a déjà vu que c'était le cas pour

[(1)] Le point essentiel est de voir que le symbole de Jacobi ne dépend que de la classe modulo D

$n = 5$ et on peut montrer que ce cas favorable se produit pour $n = 6, 10, 13, 15, 21, 22, 30$, ce qui donne les résultats suivants :

$$\begin{aligned}
p = x^2 + 5y^2 &\Leftrightarrow p \equiv 1, 9 \mod 20 \\
p = x^2 + 6y^2 &\Leftrightarrow p \equiv 1, 7 \mod 24 \\
p = x^2 + 10y^2 &\Leftrightarrow p \equiv 1, 9, 11, 19 \mod 40 \\
p = x^2 + 13y^2 &\Leftrightarrow p \equiv 1, 9, 17, 25, 29, 49 \mod 52 \\
p = x^2 + 15y^2 &\Leftrightarrow p \equiv 1, 19, 31, 49 \mod 60 \\
p = x^2 + 21y^2 &\Leftrightarrow p \equiv 1, 25, 37 \mod 84 \\
p = x^2 + 22y^2 &\Leftrightarrow p \equiv 1, 9, 15, 23, 25, 31, 47, 49, 71, 81 \mod 88 \\
p = x^2 + 30y^2 &\Leftrightarrow p \equiv 1, 31, 49, 79 \mod 120
\end{aligned}$$

Les questions en suspens sont alors de savoir caractériser tous les n pour lesquels le genre de la forme principale est réduite à un élément puis de trouver une autre idée pour traiter les autres cas.

A rendre pour le 14 mars

3. Composition à la Gauss des formes quadratiques

Commençons par citer le résultat suivant prouvé par Lagrange :

$$p, q \equiv 3, 7 \mod 20 \Rightarrow pq = x^2 + 5y^2$$

La démonstration est la suivante : on a vu que p et q peuvent s'écrire sous la forme $2x^2 + 2xy + 3y^2$, le résultat découle alors directement de l'identité remarquable :

$$(1) \qquad (2x^2 + 2xy + 3y^2)(2z^2 + 2zw + 3w^2) = (2xz + xw + yz + 3yw)^2 + 5(xw - yz)^2$$

Inspiré par ce résultat, Gauss a introduit la notion suivante :

Définition 3.1. — Soient $f(x, y)$ et $g(x, y)$ des formes quadratiques primitives définies positives de discriminant D alors une forme quadratique $F(x, y)$ de même type est leur composée si

$$f(x,y)g(z,w) = F\Big(B_1(x,y;z,w), B_2(x,y;z,w)\Big) \qquad B_i(x,y;z,w) = a_i xz + b_i xw + c_i yz + d_i yw.$$

Remarque : deux formes peuvent être composées de plusieurs façons et les formes obtenues ne sont pas forcément proprement équivalentes. L'idée est de restreindre cette opération de sorte à obtenir une structure de groupe abélien sur l'ensemble des formes de discriminant fixé d'élément neutre la forme principale. Dans [**1**] §3, l'auteur présente les constructions de Gauss et de Dirichlet, pour notre part nous allons utiliser la notion de groupe de classes d'idéaux.

Définition 3.2. — Soit $f(x, y) = ax^2 + bxy + cy^2$ une forme quadratique primitive définie positive de discriminant D. On lui associe l'idéal fractionnaire $I_f :=< 1, \tau_f >$, où $\tau_f = \frac{-b+i\sqrt{-D}}{2a} >$, de l'anneau des entiers $\mathcal{O}_K$ du corps quadratique imaginaire $K = \mathbb{Q}(i\sqrt{-D})$.

(1) Montrez que l'application $f \mapsto I_f$ induit une bijection de l'ensemble des classes d'équivalence sous $SL_2(\mathbb{Z})$ des formes quadratiques définies positives de discriminant D avec les classes d'idéaux fractionnaires de $\mathcal{O}_K$.

(2) Comme les classes d'idéaux fractionnaires de K est muni d'une structure de groupe, alors l'ensemble $C(D)$ des classes des formes quadratiques primitives définies positives de discriminant donnée aussi et on vérifie que cette loi correspond à celle définie par Gauss, cf. [**1**] théorème 5.30 p.112. On note en particulier que l'élément neutre correspond à la forme principale et que l'opposée de $ax^2+bxy+cy^2$ est $ax^2-bxy+cy^2$: en particulier elle est réduite d'ordre ≤ 2 si et seulement si $b=0$, $a=b$ ou $a=c$. En utilisant le fait que l'addition de deux formes est un composé au sens de la définition de Gauss, montrez le résultat suivant :

Soit $\Phi : C(D) \to \mathrm{Ker}\,\chi/H$ l'application qui à une forme quadratique primitive définie positive associe son genre, alors cette application est un morphisme de groupe.

(3) Soit $D<0$ tel que $D \equiv 0,1 \mod 4$ montrez que tous les genres des formes quadratiques de discriminant D ont le même cardinal qui est une puissance de 2.

Remarque : on peut en fait montrer que le genre de la forme principale est égal à $C(D)^2$. En particulier, en rapport avec la fin du paragraphe précédent, on peut en déduire, cf. [**1**] théorème 3.22 p.59, que le genre de la forme principale est réduite à un seul élément si et seulement si $C(D)^2=\{1\}$ et donc que tous les éléments de $C(D)$ sont d'ordre ≤ 2, autrement dit tels que le nombre de classes h_K de $K=\mathbb{Q}(i\sqrt{-D})$ est une puissance de 2.

Remarque : comme le genre de la classe principale est $C(D)^2$, il doit exister une généralisation de l'identité remarquable 1 pour les formes de discriminant $-4n$, la voilà :

$$(ax^2+2bxy+cy^2)(az^2+2bzw+cw^2)=(axz+bxw+byz+cyw)^2+n(xw-yz)^2.$$

4. Résolution du cas général via le corps de classes de Hilbert

Pour simplifier, considérons n sans facteurs carré tels que $n \not\equiv 3 \mod 4$ de sorte que l'anneau des entiers de $K=\mathbb{Q}(i\sqrt{n})$ est $\mathcal{O}_K=\mathbb{Z}[i\sqrt{n}]$. Nous allons utiliser la théorie du corps de classe de Hilbert et on renvoie le lecteur à tout bon ouvrage sur le thème ; le résumé donné dans [**1**] est plus léger et suffit amplement pour une première lecture. Soit donc H_K **le corps de classe de Hilbert** : il s'agit d'une extension galoisienne abélienne non ramifiée maximale de groupe de Galois le groupe de classe $C(\mathcal{O}_K)$: un idéal premier $\mathfrak{P}$ de $\mathcal{O}_K$ est alors totalement décomposé dans H_K si et seulement s'il est principal.

(1) Montrez les équivalences suivantes

$$\begin{aligned} p=x^2+ny^2 &\Leftrightarrow p\mathcal{O}_K=\mathfrak{P}\bar{\mathfrak{P}},\ \mathfrak{P}\neq\bar{\mathfrak{P}} \text{ et } \mathfrak{P} \text{ principal} \\ &\Leftrightarrow \mathfrak{P} \text{ est totatlement décomposé dans } H_K \\ &\Leftrightarrow p \text{ est totalement décomposé dans } H_K \end{aligned}$$

(2) Soient K un corps quadratique imaginaire et L une extension finie de K galoisienne sur $\mathbb{Q}$ montrez que :

(i) il existe α un entier algébrique réel tel que $L=K(\alpha)$;

(ii) soit $\mu_\alpha \in \mathbb{Z}[X]$ le polynôme minimal de α ; soit un premier p ne divisant pas le discriminant de $f(X)$ alors

$$p \text{ est totalement décomposé dans } L \Leftrightarrow \begin{cases} (\frac{D_K}{p})=1 \text{ et } f(x)\equiv 0 \mod p \\ \text{a une solution entière} \end{cases}$$

(3) Soit $n>0$ un entier sans facteur carré tel que $n \not\equiv 3 \mod 4$. Montrez qu'il existe un polynôme irréductible unitaire $f_n(X) \in \mathbb{Z}[X]$ de degré $h(-4n)$ tel que si p premier impair

ne divisant pas n ni le discriminant de $f_n(X)$ alors

$$p = x^2 + ny^2 \Leftrightarrow \begin{cases} (\frac{-n}{p}) = 1 \text{ et } f_n(x) \equiv 0 \mod p \\ \text{a une solution entière} \end{cases}$$

Remarque : en ce qui concerne les entiers n tel que $\mathbb{Z}[i\sqrt{n}] \subsetneq \mathcal{O}_K$, en utilisant la notion d'ordre, on peut reprendre les arguments précédents et obtenir un résultat analogue qui fait intervenir un corps de classe associé à l'ordre $\mathbb{Z}[i\sqrt{n}]$, cf. [**1**] théorème 9.2.
Remarque : pour $p = 14$, on calcule $H_K = K(\alpha)$ avec $\alpha = \sqrt{2\sqrt{2} - 1}$ de polynôme minimal $(x^2 + 1)^2 - 8$ de sorte que pour $p \neq 7$ premier on a

$$p = x^2 + 14y^2 \Leftrightarrow \begin{cases} (\frac{-14}{p}) = 1 \text{ et } (x^2 + 1)^2 \equiv 8 \mod p \\ \text{a une solution entière.} \end{cases}$$

Dans le chapitre 3, via la théorie de la multiplication et l'utilisation de la forme modulaire j, l'auteur présente un algorithme pour calculer le polynôme $f_n(X)$.

A rendre pour le 27 mars

Références

[1] D. Cox. *Primes of the form $x^2 + ny^2$*. Pure and applied mathematics. 1989.