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 :

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

Le but de ce thème est de présenter le résultat pour n quelconque ; suivant [**1**], nous allons donner une présentation historique des différentes techniques.

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 $p|x^2 + y^2$.

Preuve de la descente : commençons par le lemme suivant que nous utiliserons dans le cas $n = 1$.

Lemme 0.1. — *Soit $N = x^2 + ny^2$ avec $x \wedge y = 1$ et soit $q = a^2 + nb^2$ un diviseur premier de N alors N/q s'écrit aussi sous la forme $c^2 + nd^2$ avec $c \wedge d = 1$.*

Preuve : Commençons par une analyse du problème : il s'agit donc de montrer que

$$N = x^2 + ny^2 = q(c^2 + nd^2) = (a^2 + nb^2)(c^2 + nd^2) = (ca + ndb)^2 + n(cb - da)^2$$

ce qui revient à montrer que $a|x + ndb$ où d est tel que $y = da + bc$ ce qui donne en éliminant c :

$$ay = a^2 d + bca = (q - nb^2)d + bca = qd + xb$$

i.e. $q|ay - xb$ le quotient s'appelant d. En résumé on va montrer que q divise $ay - xb = qd$ puis que $a|x + ndb = ac$.

Le nombre premier q divise $a^2N - x^2q = n(ay - xb)(xb + ay)$ et comme $q > n$, quitte à changer a en $-a$, q divise $xb - ay = dq$. En outre $x - ndb = ac$: en effet comme $a \wedge b = 1$ cela revient à montrer que a divise $(x - ndb)b = xb - ndb^2 = a(y - da)$ avec donc $y = bc + da$. Ainsi on a

$$N = x^2 + ny^2 = (ca + ndb)^2 + n(cb - da)^2 = (a^2 + nb^2)(c^2 + nd^2) = q(c^2 + nd^2)$$

et donc $N/q = c^2 + nd^2$. Par ailleurs on a

$$c \wedge d = (cb) \wedge (da) = (da - bc) \wedge c = y \wedge c = (ca) \wedge (ndb) = c \wedge x | x \wedge y = 1.$$

Soit donc p divisant $N = a^2 + b^2$ avec $a \wedge b = 1$. Quitte à ajouter des multiples de p à a et b, puis à diviser par leur pgcd toujours premiers à p, on peut supposer $|a|, |b| < p/2$ de sorte que $N < p^2/2$. Ainsi tous les diviseurs premiers $q \neq p$ de N sont strictement plus petit que p. Si tous les premiers $p \neq q|N$ sont somme de deux carrés alors d'après le lemme précédent il en est de même de p. Autrement dit si p n'est pas somme de deux carrés, il existe un premier $q < p$ tel que q n'est pas somme de deux carrés et divise $x^2 + y^2$ avec $x \wedge y = 1$. On peut alors appliquer le même raisonnement à q et ainsi construire une suite infinie de premiers strictement décroissante, ce qui ne se peut pas.

Preuve de la réciprocité : soit $p = 4k + 1$ d'après le théorème de Fermat on a

$$x^{4k} - 1 = (x^{2k} - 1)(x^{2k} + 1) \equiv 0 \mod p$$

et comme le polynôme $x^{2k}-1$ a au plus $2k$ racines dans le corps $\mathbb{F}_p$, il existe $x \in \mathbb{F}_p$ tel que $x^{2k}+1 \equiv 0 \mod p$ d'où le résultat.
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 prochain paragraphe et donnée par la proposition 0.5.
Lagrange, Legendre et 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 0.2. — 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 $\Gamma_f=\sqrt{A}\mathbb{Z}^2$.

Proposition 0.3. — ***(Gauss)*** *Deux formes quadratiques positives $f(x,y)$ et $g(x,y)$ sont géométriquement équivalentes si et seulement si elles sont arithmétiquement équivalentes.*

Preuve : S'il existe $P \in GL_2(\mathbb{Z})$ telle que $f(X)=g(PX)$ alors comme $P:\mathbb{Z}^2\to\mathbb{Z}^2$ est bijectif, f et g sont clairement arithmétiquement équivalentes.

Réciproquement soient $\Gamma_f=\sqrt{A}\mathbb{Z}^2$ et $\Gamma_g=\sqrt{B}\mathbb{Z}^2$ les réseaux associés à f et g avec les notations de la remarque précédente. Par hypothèses les vecteurs de norme donnée sont de même cardinal dans Γ_f et Γ_g. En particulier l'aire d'un domaine fondamental, cf. **??**, est le même pour Γ_f et Γ_g : en effet le nombre de vecteurs de norme inférieur ou égal à n dans un réseau Γ est asymptotiquement équivalent à $\pi n^2/\mu(\Gamma)$ (considérer un domaine fondamental centré en l'origine). Rappelons qu'en dimension 2, un domaine fondamental peut s'obtenir comme suit : on choisit un vecteur de norme minimal u puis un autre v de norme minimal parmi ceux qui ne sont pas colinéaire à u. Soient donc (u_f,v_f) et (u_g,v_g) les bases respectives de Γ_f et Γ_g ainsi construites. Comme $|u_f|=|u_g|$, soit alors une rotation r qui envoie u_f sur u_g. En outre comme le nombre de vecteurs de norme donnée dans Γ_f et Γ_g sont égaux, on en déduit que $|v_f|=|v_g|$; en utilisant que $\mu(\Gamma_f)=\mu(\Gamma_g)$ on en déduit que $|<u_f|v_f>|=|<u_g|v_g>|$ i.e. qu'étant donnée $u_f=u_g$ et v_f alors v_g est l'image de v_f par l'une des cas isométries suivantes : l'identité, la symétrie par rapport à l'origine ou la droite des x ou celle des y.

Ainsi il existe une matrice orthogonale $O \in O_2(\mathbb{R})$ telle que $\Gamma_g = O.\Gamma_f$ et donc $O\sqrt{B}(\sqrt{A})^{-1}$ est un automorphisme de $\Gamma_f \simeq \mathbb{Z}^2$, i.e. un élément de $GL_2(\mathbb{Z})$. Soit alors $P \in GL_2(\mathbb{Z})$ telle que $\sqrt{A} = O\sqrt{B}P$ de sorte que ${}^tXAX = {}^tX{}^tP\sqrt{B}{}^tOO\sqrt{B}PX$ et donc $A = {}^tPBP$, d'où le résultat.

Lemme 0.4. — *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 $mx^2 + bxy + cy^2$.*

Preuve : Si $m = f(p,q)$ avec $p \wedge q = 1$ alors pour r, s tels que $ps - qr = 1$ on a $f(px+ry, qx+sy) = f(p,q)x^2 + bxy + cy^2$ avec $b = 2apr + bps + brq + 2cqs$ et $c = f(r,s)$. Réciproquement $mx^2 + bxy + cy^2$ représente proprement m pour $(x,y) = (1,0)$.
Remarque : rappelons que le discriminant de $ax^2+bxy+cy^2$ est $D = b^2-4ac$ avec $4af(x,y) = (2ax + by)^2 - Dy^2$ de sorte que si $D < 0$, f ne peut représenter que des valeurs positives. La réponse apportée à la dernière remarque du paragraphe précédent est alors donnée par la proposition suivante.

Proposition 0.5. — *Soient n un entier et p premier ne divisant pas n. Alors $(\frac{-n}{p}) = 1$ si et seulement si p est représenté par une forme quadratique primitive de discriminant $-4n$.*

Preuve : Si $f(x,y)$ représente proprement p alors on peut d'après le lemme précédent supposer que $f(x,y) = px^2 + bxy + cy^2$ avec $D = b^2 - 4pc$ qui est donc un carré modulo p. Pour b pair, on a $D = -4n$ avec $(\frac{-4n}{p}) = (\frac{-n}{p}) = 1$.

Réciproquement si $(\frac{-4n}{p}) = (\frac{-n}{p}) = 1$ alors $D = -4n \equiv b^2 \mod p$; quitte à remplacer b par $b + p$, on peut supposer que D et b ont la même parité de sorte qu'il existe $c \in \mathbb{Z}$ tel que $D = b^2 - 4pc$ et $p^2 + bxy + cy^2$ est une forme de discriminant $D = -4n$ qui représente proprement p.

Références

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