LES ENTIERS DE LA FORME $a^2 + mb^2$

E. KOWALSKI

Soit $m \geqslant 1$ un entier. On pose

$$N(x) = |\{n \leqslant x \mid \text{il existe } (a,b) \text{ tels que } n = a^2 + mb^2\}|$$

et on veut évaluer asymptotiquement $N(x)$. Je note $N^\flat(x)$ le sous-ensemble des entiers sans facteurs carrés de la forme $a^2 + mb^2$. Pour simplifier je vais considérer $N^\flat(x)$ (donc au moins minorer $N(x)$).

Proposition 1. *Soit $m \geqslant 1$ tel que $\mathbf{Z}[\sqrt{-m}]$ est l'anneau des entiers de $\mathbf{Q}(\sqrt{-m})$. Alors il existe une constante $c_m > 0$ telle que*

$$N^\flat(x) \sim \frac{c_m x}{\sqrt{\log x}}$$

quand $x \to +\infty$.

Plus précisément soit

$$M(x) = |\{n \leqslant x \mid \text{ il existe un idéal } \mathfrak{a} \subset \mathbf{Z}[\sqrt{-m}] \text{ tel que } N\mathfrak{a} = x\}|$$

et $M^\flat(x)$ se restreignant aux idéaux sans facteurs carrés et divisibles uniquement par des idéaux premiers de degré un. Dans ce cas les valeurs de $n = N\mathfrak{a}$ intervenant sont sans facteurs carrés. On a donc évidemment $N(x) \leqslant M(x)$ et $N^\flat(x) \leqslant M^\flat(x)$. La proposition provient des deux suivantes :

Proposition 2. *On a*

$$N^\flat(x) \sim \frac{1}{h_2} M^\flat(x) \text{ quand } x \to +\infty,$$

où h_2 est l'ordre de la partie 2-primaire du groupe de classes de $\mathbf{Q}(\sqrt{-m})$.

Proposition 3. *Il existe une constante $c_m > 0$ telle que*

$$M^\flat(x) \sim \frac{c_m x}{\sqrt{\log x}}$$

quand $x \to +\infty$.

La partie « surprenante » est la Proposition 2, qui dit que (si l'ordre du groupe de classes était impair) que parmi les idéaux de norme n, on peut le plus souvent en trouver un qui est principal.

J'admets la Proposition 3 qui doit procéder comme Landau. Pour la Proposition 2, notons H le groupe de classes et écrivons

$$H = H_2 \oplus H_-,$$

où H_2 est la partie 2-primaire (d'ordre h_2) et H_- la partie impaire (d'ordre h_- disons). De plus décomposons H_- en facteurs cycliques (d'ordres impairs) :

$$H_- = H_{-,1} \oplus \cdots \oplus H_{-,\nu} \text{ avec } H_i \simeq \mathbf{Z}/d_i\mathbf{Z}. \tag{1}$$

D'après la théorie du genre, H_- est aussi l'image de l'application $a \mapsto 2a$ dans H. On note $a = a_2 + a_-$ la décomposition d'un élément $a \in H$ en ces deux composantes paires et impaires, et $a_- = a_{-,1} + \cdots + a_{-,\nu}$ celle de a_- suivant (1).

Pour chaque indice i, $1 \leqslant i \leqslant \nu$, on note $H_i^* \subset H$ le sous-ensemble des classes qui sont dans $H_{-,i}$ et qui engendrent $H_{-,i}$. On note $H_i^\sharp$ le complémentaire de H_i^* dans H. Si $H_- = 0$, on introduit (par convention) $H_{-,1} = 0$ et $H_1^* = \{0\}$, $H_1^\sharp = H_2 \setminus \{0\}$; on voit que les résultats ci-dessous restent alors valides. En particulier, remarquons que $H_i^\sharp \neq H$ dans tout les cas.

Soit $n = N\mathfrak{a}$ un entier compté par $M^\flat(x)$. On factorise

$$\mathfrak{a} = \mathfrak{p}_1 \cdots \mathfrak{p}_r$$

avec $r \geqslant 0$ et les $\mathfrak{p}_i$ sont les idéaux premiers (distincts et de degré 1) divisant $\mathfrak{a}$. Pour tout $\varepsilon = (\varepsilon_1, \ldots, \varepsilon_r) \in \{\pm 1\}^r$, on a $n = N\mathfrak{a}_\varepsilon$ avec

$$\mathfrak{a}_\varepsilon = \mathfrak{p}_1^{\varepsilon_1} \cdots \mathfrak{p}_r^{\varepsilon_r}$$

en notant (abusivement) $\mathfrak{b}^{-1}$ le conjugué d'un idéal $\mathfrak{b}$. Réciproquement toute solution de $N\mathfrak{b} = n$ est de la forme $b = \mathfrak{a}_\varepsilon$ pour un certain ε. Puisque $\varepsilon_i \in \pm\{1\}$, il découle aussitôt de cela que $[\mathfrak{a}]_2 = [\mathfrak{a}_\varepsilon]_2$ pour tout choix de ε. Une condition nécessaire pour que n soit norme d'un idéal principal est donc que n soit norme d'un idéal $\mathfrak{a}$ dont la classe dans H_2 est nulle. (C'est aussi évident en utilisant l'interprétation de H_- comme image de $a \mapsto 2a$). On va montrer que pour la plupart des n (ayant suffisamment de facteurs premiers en un certain sens), cette condition est suffisante. Notons dores et déjà que $M_2^\flat(x)$, le nombre d'entiers sans facteurs carrés représentables comme norme d'un idéal dont la classe dans H_2 est triviale, vérifie

$$M_2^\flat(x) \sim \frac{1}{h_2} M^\flat(x) \tag{2}$$

par équirépartition des classes d'idéaux (ou des « genres »).

Fixons maintenant $k \geqslant 1$ et faisons la décomposition suivante :

$$M_2^\flat(x) = M_1(x) + M_2(x)$$

où $M_2(x)$ correspond aux entiers qui sont norme d'un idéal $\mathfrak{a}$ tel que, pour $1 \leqslant i \leqslant \nu$, $\mathfrak{a}$ ait au moins k facteurs premiers dont la classe est dans H_i^*, et $M_1(x)$ correspond au complémentaire. Remarquons que les conditions imposées sont stables si on change un facteur premier par son conjugué, donc ces définitions sont raisonnables. De même on définit $N_1(x)$ et $N_2(x)$ puisque $N^\flat$ compte un sous-ensemble de $M^\flat$.

On a les lemmes suivants :

Lemme 4. *On a pour $x \geqslant 2$*

$$N_1(x), M_1(x) \ll \frac{x(\log\log x)^k}{(\log x)^{1-c}}$$

où $c < \frac{1}{2}$ est donnée par

$$2c = \max \frac{|H_i^\sharp|}{|H|}.$$

Lemme 5. *Il existe k_0, ne dépendant que de h, tel que si $k \geqslant k_0$, on a : pour $x \geqslant 2$,*

$$N_2(x) = M_2(x);$$

autrement dit, un $n \leqslant x$ sans facteurs carrés admettant au moins k facteur premiers primitifs est norme d'un idéal principal de $\mathbf{Z}[\sqrt{-m}]$ si et seulement si il est norme d'un idéal dont la classe dans H_2 est nulle.

Preuve du Lemme 4. Il s'agit d'un résultat standard. Il suffit de traiter M_1. Remarquons que par définition, si un entier n est compté par M_1, il existe i, $1 \leqslant i \leqslant \nu$, tel que $n = N\mathfrak{a}$ avec $\mathfrak{a}$ qui se factorise sous la forme

$$\mathfrak{a} = \mathfrak{p}_1 \cdots \mathfrak{p}_r \mathfrak{a}_1 = \mathfrak{a}_2 \mathfrak{a}_1 \tag{3}$$

où $r \leqslant k$, $\mathfrak{p}_i$ est dans H_i^* pour $1 \leqslant i \leqslant r$, et les facteurs premiers de $\mathfrak{a}_1$ sont tous dans $H_i^\sharp$. Notons $M_1'(x)$ le nombre des entiers de la forme $N\mathfrak{a}_1$, $M_1''(x)$ celui des entiers de la forme $N\mathfrak{a}_2$.

Pour $M_1'(x)$, on considère des entiers dont tout les facteurs premiers se trouvent dans un ensemble de nombres premiers de densité

$$c_i = \frac{|H_i^\sharp|}{2|H|} < \frac{1}{2}$$

(d'après l'équirépartition des idéaux premiers dans H). L'estimation

$$M_1'(x) \ll \frac{x}{(\log x)^{1-c_i}} \tag{4}$$

est alors un résultat standard de crible.

De plus on a trivialement

$$M_1''(x) \ll \frac{x(\log\log x)^{k-1}}{\log x}, \tag{5}$$

puisque les entiers du type n_2 ont au plus k facteurs premiers.

Soit enfin $n = N\mathfrak{a} \leqslant x$ un entier avec $\mathfrak{a}$ du type (3), $n_i = N\mathfrak{a}_i$. L'un des entiers n_1, n_2 est $\leqslant \sqrt{x}$. On estime séparément le nombres $Q_1(x)$ des $n \leqslant x$ tels que $n_1 \leqslant \sqrt{x}$ et $R_1(x)$ de ceux tels que $n_2 \leqslant \sqrt{x}$.

D'abord

$$Q_1(x) \leqslant \sum_{n_1 \leqslant \sqrt{x}} M_1''\Big(\frac{x}{n_1}\Big) \ll \frac{x(\log\log x)^{k-1}}{\log x} \sum_{n_1 \leqslant \sqrt{x}} \frac{1}{n_1} \ll \frac{x(\log\log x)^{k-1}}{(\log x)^{1-c_i}}$$

par sommation par partie en utilisant (4).

Finalement,

$$R_1(x) \leqslant \sum_{n_2 \leqslant \sqrt{x}} M_1'\Big(\frac{x}{n_2}\Big) \ll \frac{x}{(\log x)^{1-c_i}} \sum_{n_2 \leqslant \sqrt{x}} \frac{1}{n_2} \ll \frac{x(\log\log x)^{k}}{(\log x)^{1-c_i}}$$

de même à partir de (5).

Prenant le « pire » des c_i, on obtient la proposition. □

Ce lemme implique aussi que

$$M_2(x) \sim \frac{c_m x}{\sqrt{\log x}}$$

d'après la Proposition 3. Le Lemme 5 implique donc alors la Proposition 2.

Pour le Lemme 5, soit n compté par $M_2(x)$. On a donc $n = N\mathfrak{a}$ pour un idéal de la forme

$$\mathfrak{a} = \mathfrak{b}(\mathfrak{p}_{1,1} \cdots \mathfrak{p}_{1,k})(\mathfrak{p}_{2,1} \cdots \mathfrak{p}_{2,k}) \cdots (\mathfrak{p}_{\nu,1} \cdots \mathfrak{p}_{\nu,k})$$

où $\mathfrak{p}_{i,j} \in H_i^*$ pour $1 \leqslant j \leqslant k$, et $\mathfrak{b}$ est le produit des autres facteurs premiers.

Maintenant, pour tout choix de $\varepsilon = (\varepsilon_{i,j}) \in \{\pm 1\}^{\nu k}$, on a aussi

$$n = N\mathfrak{a}_\varepsilon$$

avec

$$\mathfrak{a}_\varepsilon = \mathfrak{b}(\mathfrak{p}_{1,1}^{\varepsilon_{1,1}} \cdots \mathfrak{p}_{1,k}^{\varepsilon_{1,k}})(\mathfrak{p}_{2,1}^{\varepsilon_{2,1}} \cdots \mathfrak{p}_{2,k}^{\varepsilon_{2,k}}) \cdots (\mathfrak{p}_{\nu,1}^{\varepsilon_{\nu,1}} \cdots \mathfrak{p}_{\nu,k}^{\varepsilon_{\nu,k}}).$$

If suffit de trouver des signes ε tels que $[\mathfrak{a}_\varepsilon] = 0$ dans H. Pour la composante paire, c'est vrai par hypothèse. La composante selon $H_{-,i}$ vaut

$$[\mathfrak{a}_\varepsilon]_{-,i} = [\mathfrak{b}]_{-,i} + \varepsilon_{i,1}[\mathfrak{p}_{i,1}] + \cdots + \varepsilon_{i,k}[\mathfrak{p}_{i,k}]$$

par définition de H_i^*.

Il suffit de trouver des signes $\varepsilon_{i,j}$ tels que ceci vaille 0 dans $H_{-,i}$. Puisque $H_{-,i}$ est cyclique d'ordre impair et que les composantes $\mathfrak{p}_{i,j}$ engendrent $H_{-,i}$, le lemme suivant est ad-hoc :

Lemme 6. *Soit h un nombre impair, $G = \mathbf{Z}/h\mathbf{Z}$. Il existe un entier $k_0 \geqslant 1$ avec la propriété suivante : pour tout $k \geqslant k_0$ et tout choix de b, a_1, …, $a_k \in G$, avec a_i un générateur de G pour $1 \leqslant i \leqslant k$, il existe $\varepsilon_1, \ldots, \varepsilon_k \in \{\pm 1\}$ tel que*

$$b + \varepsilon_1 a_1 + \cdots + \varepsilon_k a_k = 0 \in G. \tag{6}$$

Démonstration. Pour k fixé quelconque, soit $N = N(k)$ le nombre de solutions $\varepsilon = (\varepsilon_1, \ldots, \varepsilon_k)$ de l'équation (6). On veut $N \geqslant 1$. On a

$$N = \frac{1}{h} \sum_{\alpha \,(\mathrm{mod}\, h)} e\Big(\frac{\alpha b}{h}\Big) \sum_{\varepsilon_1, \ldots, \varepsilon_k} \cdots \sum e\Big(\frac{\alpha(\varepsilon_1 a_1 + \cdots + \varepsilon_k a_k)}{h}\Big).$$

Cela donne

$$N = \frac{2^k}{h} \sum_{\alpha \,(\mathrm{mod}\, h)} e\Big(\frac{\alpha b}{h}\Big)\Big(\cos\frac{2\pi\alpha a_1}{h}\Big) \cdots \Big(\cos\frac{2\pi\alpha a_k}{h}\Big).$$

La contribution de $\alpha = 0$ vaut $2^k/h$. Pour $\alpha \neq 0$, on a $\alpha a_i \neq 0 \,(\mathrm{mod}\, h)$ puisque a_i est supposé primitif dans G. Comme de plus h est impair, $\frac{\alpha a_i}{h} \neq \frac{1}{2} \,(\mathrm{mod}\, 1)$, donc

$$\Big|\cos\frac{2\pi\alpha a_i}{h}\Big| \leqslant \Big|\cos\frac{2\pi}{h}\Big| = \beta, \text{ disons.}$$

Chaque terme avec $\alpha \neq 0$ est donc majoré par β^k, et la contribution totale est

$$\leqslant 2^k \beta^k.$$

Comme $\beta < 1$ et que le terme principal est $2^k/h$, il suffit de choisir k_0 tel que $\beta^{k_0} < h^{-1}$ pour avoir $N > 0$ donc $N \geqslant 1$ puisque c'est un entier. □

Remarque 7. (1) On voit facilement que la preuve donne $k_0 \simeq h^2 \log h$. L'argument élémentaire suivant, dû à K. Bellabas fait mieux : si $\ell \geqslant 1$, et parmi les a_i il y en a ℓ égaux à a fixé, les permutations de signes limitées à ℓ telles valeurs permettent d'obtenir tout les éléments du type $b' + (\ell - 2t)a$ où $0 \leqslant t \leqslant \ell$ (b' vaut b plus la sommes des autres a_i). Si $\ell \geqslant h$, une telle « orbite » est égale à G puisque a est inversible. Par le principe des tiroirs, si on a $h\varphi(h)$ éléments a_i, chacun valant l'un des $\varphi(h)$ éléments primitifs, il existe une valeur au moins répétées $\geqslant h$ fois.

(2) Le terme d'erreur final est limité par la constante c dans le Lemme 4 (on gagne $(\log x)^{\frac{1}{2}-c}$; pour avoir le « vrai » terme d'erreur, il faut aussi regarder celui de la Proposition 3 qui est $\ll x(\log x)^{-3/2}$ je crois, mais je n'ai pas regardé sa dépendance en m). Dans la preuve ici, il dépend donc assez finement de la structure du groupe de classes. Lorsque la partie impaire est cyclique, d'ordre h_-, c vaut $\frac{1}{2} - \varphi(h_-)/2h$, ce qui donne un terme d'erreur qui est

$$\ll \frac{x(\log\log x)^{h_-^2}}{(\log x)^{\frac{1}{2}+\varphi(h_-)/2h}},$$

pour $x \geqslant 2$, la constante implicite étant absolue.