*Journal de Théorie des Nombres*
*de Bordeaux* **12** (2000), 379–397

# Comptage exact de discriminants d'extensions abéliennes

par Henri COHEN

*Pour les 60 ans de Jacques Martinet, en témoignage de ma reconnaissance*

Résumé. Le but de cet article est d'expliquer comment calculer *exactement* le nombre de classes d'isomorphismes d'extensions abéliennes de $\mathbb{Q}$ en degré inférieur ou égal à 4 et de discriminant majoré par une borne donnée. On parvient par exemple à calculer le nombre de corps cubiques cycliques de discriminant inférieur ou égal à $10^{37}$.

Abstract. This paper explains how to compute *exactly* the number of isomorphism classes of Abelian extensions of $\mathbb{Q}$ in degree less than or equal to 4 having their discriminant bounded by a given integer. For example, we are able to compute the number of cyclic cubic fields of discriminant less than or equal to $10^{37}$.

## 1. Introduction

**1.1. But de l'article et notations.** Soit $K$ un corps de nombres, soit $G$ un sous-groupe transitif de $S_n$, et notons $\mathcal{F}_{K,n}(G)$ l'ensemble des $K$-isomorphismes d'extensions $L/K$ de degré $n$ telles que le groupe de Galois de la clôture galoisienne de $L/K$ dans une clôture algébrique $\overline{K}$ de $K$ fixée soit isomorphe à $G$. On notera $\mathcal{N}$ la norme absolue de $K/\mathbb{Q}$, et $\mathfrak{d}(L/K)$ l'idéal discriminant relatif de $L/K$.

On pose :

$$\Phi_{K,n}(G,s) = \sum_{L\in\mathcal{F}_{K,n}(G)} \frac{1}{\mathcal{N}(\mathfrak{d}(L/K))^s} \quad \text{et}$$
$$N_{K,n}(G,X) = |\{L \in \mathcal{F}_{K,n}(G),\ \mathcal{N}(\mathfrak{d}(L/K)) \le X\}| \quad .$$

Quand $K = \mathbb{Q}$, on omettra l'indice $K$, et on a bien entendu dans ce cas $\mathcal{N}(\mathfrak{d}(L/K)) = |d(L)|$, où $d(L)$ désigne le discriminant du corps de nombres $L$.

Manuscrit reçu le 29 février 2000.

C'est un problème important et hautement non trivial en général de calculer $\Phi_{K,n}(G,s)$ explicitement, ou de donner une évaluation asymptotique précise de $N_{K,n}(G,X)$ (voir [3] [4] [5] [6] [7] [8] [9]).

Dans le présent article, nous nous restreignons au cas où $K=\mathbb{Q}$, $G$ abélien et $n\le 4$ (ce qui ne laisse que les quatre cas $G=C_2$, $G=C_3$, $G=C_4$ et $G=V_4\simeq C_2\times C_2$), et notre but va être d'expliquer comment calculer *exactement* (par opposition à asymptotiquement) les nombres $N_n(G,X)$ pour de grandes valeurs de $X$ (nous atteindrons dans certains cas presque 40 chiffres décimaux). Je réfère à [4], [6] pour des tables étendues de $N_n(G,10^k)$. Des méthodes similaires peuvent être appliquées à tout groupe abélien $G$ de petit cardinal.

**Notations** Nous emploierons les notations suivantes. D'autres notations plus particulières seront introduites au fur et à mesure.

- La lettre $p$ désignera toujours un nombre premier.
- L'expression $v_p(n)$ désignera la valuation de $n$ en $p$, c'est-à-dire le plus grand entier $k$ tel que $p^k \mid n$.
- $\mu(m)$ est la fonction de Möbius en $m$, et $\omega(m)$ est le nombre de diviseurs premiers distincts de $m$ (donc $\mu(m)=(-1)^{\omega(m)}$ si $m$ est sans facteur carré, $\mu(m)=0$ sinon).
- Nous poserons $f_1(X)=\lfloor (X+1)/2\rfloor$. C'est le nombre d'entiers $n$ *impairs* tels que $1\le n\le X$.
- Soient $f$ et $g$ deux fonctions de la variable $X$, où $X$ va tendre vers $+\infty$. La notation $f=\widetilde{O}(g)$ (lire $f$ est un grand $O$ *mou* de $g$) signifie que pour tout $\varepsilon>0$ on a $f(X)=O(g(X)X^{\varepsilon})$ où le $O()$ a ici son sens habituel. Cette notation très pratique permet d'éviter de s'encombrer en permanence d'expressions du type $O(X^{\varepsilon})$.

**1.2. Résultats de théorie élémentaire des nombres.** Nous donnons ici deux résultats plus ou moins classiques dont nous aurons besoin. Le premier est connu sous le nom de "méthode de l'hyperbole". Sa démonstration est immédiate (voir par exemple [12] p. 38).

**Proposition 1.1.** *Soient $(a_n)_{n\ge1}$, $(b_n)_{n\ge1}$ deux suites, $c_n=\sum_{d\mid n} a_d b_{n/d}$ leur convolution arithmétique, et enfin soit $A(X)$, $B(X)$ et $C(X)$ les fonctions sommatoires de $a_n$, $b_n$, $c_n$ respectivement (donc $A(X)=\sum_{1\le n\le X} a_n$, etc...). Pour tout nombre réel $E$ (non nécessairement entier) tel que $1\le E\le X$ on a l'identité :*

$$C(X)=\sum_{1\le n\le E} a_n B(X/n)+\sum_{1\le n\le X/E} b_n A(X/n)-A(E)B(X/E)\ .$$

**Exemples**

(1) Si on choisit $a_n=b_n=1$, on a $c_n=d(n)$, le nombre de diviseurs de $n$, et d'autre part on a $A(X)=B(X)=\lfloor X\rfloor$. Il en résulte que l'on

peut calculer $\sum_{1\le n\le X} d(n)$ en temps $\widetilde{O}(X^{1/2})$, et en fait cela donne une estimation raisonnable de la fonction sommatoire de $d(n)$. C'est l'application la plus classique de la méthode de l'hyperbole.

(2) Si on prend $a_n = 1$ et $b_n = d(n)$, on a alors $c_n = d_3(n)$, nombre de manières d'écrire $n$ comme produit de 3 entiers positifs (et coefficient de $n^{-s}$ dans la série de Dirichlet pour $\zeta^3(s)$). Nous verrons plus loin que la méthode de l'hyperbole conduit au calcul de $\sum_{1\le n\le X} d_3(n)$ en temps $\widetilde{O}(X^{2/3})$. Je ne sais pas si on peut faire mieux en utilisant des méthodes élémentaires.

Le deuxième résultat que nous utiliserons est une variante d'un résultat démontré dans [11], mais probablement connu depuis longtemps.

Tout d'abord, introduisons la notation suivante :

$$M_i(X) = \sum_{\substack{1\le m\le X\\ 2\nmid m}} \mu(m) \enspace .$$

Cette fonction est liée à la fonction sommatoire habituelle $M(X)$ de la fonction de Möbius par l'identité $M(X) = M_i(X) - M_i(X/2)$ mais nous n'utiliserons pas ce résultat.

**Proposition 1.2.** *Soit $u$ un nombre réel tel que $1 \le u \le X$. On a*

$$M_i(X) = M_i(u) - \sum_{\substack{1\le m\le u\\ 2\nmid m}} \mu(m) \sum_{\substack{u/m<n\le X/m\\ 2\nmid n}} M_i\left(\frac{X}{mn}\right) \enspace .$$

*Démonstration.* Nous calquons la démonstration de [11]. D'une part, on a

$$\sum_{\substack{1\le m\le u\\ 2\nmid m}} \mu(m) \sum_{\substack{1\le n\le u/m\\ 2\nmid n}} M_i(X/(mn)) = \sum_{\substack{1\le N\le u\\ 2\nmid N}} M_i(X/N) \sum_{m\mid N} \mu(m) = M_i(X) \enspace .$$

D'autre part, pour tout $Y \ge 1$, on a

$$\sum_{\substack{1\le m\le Y\\ 2\nmid m}} M_i(Y/m) = \sum_{\substack{1\le m\le Y\\ 2\nmid m}} \sum_{\substack{1\le n\le Y/m\\ 2\nmid n}} \mu(n) = \sum_{\substack{1\le N\le Y\\ 2\nmid N}} \sum_{n\mid N} \mu(n) = 1 \enspace ,$$

donc

$$\sum_{\substack{1\le m\le u\\ 2\nmid m}} \mu(m) \sum_{\substack{1\le n\le X/m\\ 2\nmid n}} M_i(X/(mn)) = \sum_{\substack{1\le m\le u\\ 2\nmid m}} \mu(m) = M_i(u) \enspace .$$

La proposition résulte de ces deux formules par soustraction. □

En combinant cette proposition avec la méthode de l'hyperbole et le calcul de $M(X)$ (ici de $M_i(X)$) par blocs, il est expliqué dans [11] comment en déduire une méthode de calcul de $M_i(X)$ en temps $\widetilde{O}(X^{2/3})$ et en espace $\widetilde{O}(X^{1/3})$. Ceci est un gain considérable par rapport à la méthode naïve.

**1.3. La méthode générale.** Ces préliminaires étant démontrés, nous allons passer au calcul exact des $N_n(G,X)$ pour les différents groupes abéliens $G$ énumérés ci-dessus. La stratégie de base utilisée dans chaque cas (et complétée cas par cas par des astuces complémentaires) va être tout d'abord d'écrire explicitement la fonction $\Phi_n(G,s)$ comme somme de produits
euleriens. Pour chacun de ces produits eulériens, on va remplacer éventuellement $s$ par $s/k$ pour le plus grand entier $k$ tel que cela reste une série de Dirichlet. On mettra ensuite en facteurs des produits eulériens correspondant à des suites $a_n$ dont les fonctions sommatoires sont les plus rapides à calculer (habituellement des variantes de $\zeta(s)$), de façon à faire apparaître un produit eulérien de la forme $\prod_p(1+O(p^{-vs}))$ avec $v$ (que nous appellerons la *valuation* du produit eulérien) le plus grand possible. Un calcul de convolution permet alors de calculer $N_n(G,X)$ en sommant sur des entiers $x \le O(X^{1/v})$ la fonction sommatoire des $a_n$ en $X/x^v$.

Ceci peut paraître compliqué, mais est en fait fort simple une fois qu'on en a pris l'habitude. Donnons un exemple, qui est en fait très voisin du cas $G = C_2$ que nous allons voir ci-dessous. Soit à calculer la fonction sommatoire $C(X)$ de la suite $c_n$ définie par $\prod_p(1+p^{-s}) = \sum_{n\ge1} c_n n^{-s}$. On a en fait $c_n = |\mu(n)|$ donc $C(X) = \sum_{1\le n\le X} |\mu(n)|$, mais le calcul direct de cette expression prendrait un temps $\widetilde{O}(X)$.

Or nous pouvons écrire $1+p^{-s} = (1-p^{-s})^{-1}(1-p^{-2s})$ donc

$$\prod_p(1+p^{-s}) = \zeta(s)\prod_p(1-p^{-2s})$$

(le deuxième produit est en fait égal à $\zeta(2s)^{-1}$, mais nous n'avons pas besoin de le savoir). On a donc mis en facteur un produit eulérien, à savoir $\zeta(s)$, dont la fonction sommatoire est immédiate à calculer, et on a fait apparaître un nouveau produit eulérien dont la valuation $v$ est cette fois-ci égale à 2 au lieu de 1 dans le produit initial. Ceci permet donc de calculer $C(X)$ en temps $\widetilde{O}(X^{1/2})$, grâce à la formule explicite

$$C(X) = \sum_{1\le n\le X} |\mu(n)| = \sum_{1\le m\le X^{1/2}} \mu(m)\left\lfloor\frac{X}{m^2}\right\rfloor \quad .$$

En d'autres termes, nous utilisons la formule

$$|\mu(n)| = \sum_{m^2\mid n} \mu(m) \quad .$$

## 2. Le cas $G = C_2$

Utilisant la caractérisation des discriminants de corps quadratiques, il est facile de montrer que

$$\begin{aligned}\Phi_2(C_2, s) &= -1 + \left(1 + \frac{1}{2^{2s}} + \frac{2}{2^{3s}}\right) \prod_{p\equiv 1 \pmod 2} \left(1 + \frac{1}{p^s}\right) \\ &= -1 + \left(1 - \frac{1}{2^s} + \frac{2}{2^{2s}}\right) \prod_p \left(1 + \frac{1}{p^s}\right) \\ &= -1 + \left(1 - \frac{1}{2^s} + \frac{2}{2^{2s}}\right) \frac{\zeta(s)}{\zeta(2s)} \\ &= -1 + \left(1 + \frac{1}{2^{2s}} + \frac{2}{2^{3s}}\right) \frac{\zeta_2(s)}{\zeta_2(2s)} \quad ,\end{aligned}$$

où pour tout nombre premier $\ell$ (ici $\ell = 2$)

$$\zeta_\ell(s) = \prod_{p\neq\ell} \left(1 - \frac{1}{p^s}\right)^{-1} = \left(1 - \frac{1}{\ell^s}\right) \zeta(s)$$

désigne la fonction $\zeta(s)$ privée de son facteur local en $\ell$. En pratique, c'est la dernière formule qui va s'avérer la plus rapide pour calculer $N_2(C_2, X)$. Si on pose

$$\frac{\zeta_2(s)}{\zeta_2(2s)} = \zeta_2(2s)^{-1}\zeta_2(s) = \sum_{2\nmid m} \frac{c(m)}{m^s} \quad ,$$

la fonction $c$ est la convolution arithmétique restreinte aux entiers impairs de la fonction constante 1 et de la fonction égale à $\mu(\sqrt{n})$ si $n$ est un carré et à 0 sinon. La fonction sommatoire de la suite définissant $\zeta_2(s)$ comme série de Dirichlet est égale à $f_1(X) = \lfloor (X+1)/2 \rfloor$, donc comme ci-dessus on obtient

$$C(X) = \sum_{\substack{1\leq n\leq X \\ 2\nmid n}} c(n) = \sum_{\substack{1\leq n\leq X \\ 2\nmid n \\ n=m^2}} \mu(m) f_1\left(\frac{X}{n}\right) = \sum_{\substack{1\leq m\leq X^{1/2} \\ 2\nmid m}} \mu(m) f_1\left(\frac{X}{m^2}\right) \quad .$$

D'après la formule pour $\Phi_2(C_2, s)$, il en résulte que

$$\begin{aligned}N_2(C_2, X) &= -1 + C(X) + C(X/4) + 2C(X/8) \\ &= -1 + \sum_{\substack{1\leq m\leq X^{1/2} \\ 2\nmid m}} \mu(m) f_2\left(\frac{X}{m^2}\right) \quad ,\end{aligned}$$

où $f_2(z) = f_1(z) + f_1(z/4) + 2f_1(z/8)$. Ceci donne une méthode tout à fait raisonnable de calcul de $N_2(C_2, X)$, nécessitant un temps en $\widetilde{O}(X^{1/2})$, mais nous allons montrer comment l'améliorer considérablement.

**Proposition 2.1.** *Soit $E$ un nombre réel tel que $1 \le E \le X$. On a*

$$N_2(C_2,X)=-1+\sum_{\substack{1\le m\le (X/(E+1))^{1/2}\\ 2\nmid m}}\mu(m)(f_2(X/m^2)-f_2(E))$$
$$+\sum_{1\le k\le E}M_i((X/k)^{1/2})(f_2(k)-f_2(k-1))\ .$$

Noter que

$$f_2(k)-f_2(k-1)=0,1,0,1,1,1,0,1,2,1,0,1,1,1,0,1$$

selon que $k \equiv 0,1,2,3,4,5,6,7,8,9,10,11,12,13,14,15 \pmod{16}$ respectivement.

*Démonstration.* En imitant la méthode de l'hyperbole, on a

$$N_2(C_2,X)=-1+\sum_{\substack{1\le m\le (X/(E+1))^{1/2}\\ 2\nmid m}}\mu(m)f_2\left(\frac{X}{m^2}\right)+S$$

avec

$$\begin{aligned}S&=\sum_{1\le k\le E}f_2(k)\sum_{\substack{(X/(k+1))^{1/2}<m\le (X/k)^{1/2}\\ 2\nmid m}}\mu(m)\\
&=\sum_{1\le k\le E}f_2(k)(M_i((X/k)^{1/2})-M_i((X/(k+1))^{1/2}))\\
&=\sum_{1\le k\le E}M_i((X/k)^{1/2})(f_2(k)-f_2(k-1))-f_2(E)M_i((X/(E+1))^{1/2})\ .\end{aligned}$$

Comme

$$M_i((X/(E+1))^{1/2})=\sum_{\substack{1\le m\le (X/(E+1))^{1/2}\\ 2\nmid m}}\mu(m)\ ,$$

on obtient la proposition. □

Si nous évaluons $M_i(X)$ naïvement, nous n'obtenons pas d'amélioration. En utilisant des formules classiques utilisées pour obtenir des majorations explicites de $M(X)$ de la forme $M(X) \le X/S$ pour de grandes valeurs de $S$ (voir [10]), on peut calculer $M_i(X)$ plus de 10 fois plus rapidement que par la méthode naïve, ce qui conduit à une amélioration notable du temps de calcul de $N_2(C_2,X)$, toutefois encore en $\widetilde{O}(X^{1/2})$. On peut faire nettement mieux et diminuer l'exposant de $X$ en utilisant la méthode de [11] basée sur la proposition 1.2, qui nous permet de calculer $M_i(X)$ en temps $\widetilde{O}(X^{2/3})$. En choisissant $E=\widetilde{O}(X^{1/7})$ (valeur optimale) dans la proposition 2.1, on voit facilement qu'on en déduit une méthode de calcul de $N_2(C_2,X)$ en temps $\widetilde{O}(X^{3/7})$ au lieu de $\widetilde{O}(X^{1/2})$. L'amélioration semble faible, mais en pratique elle est déjà considérable. Toutefois, on peut faire encore mieux en utilisant la proposition suivante.

**Proposition 2.2.** *Soit $E$ un nombre réel tel que $1 \le E \le X$. On a*

$$N_2(C_2, X) = N_2(C_2, E) + \sum_{\substack{1 \le m \le (X/(E+1))^{1/2} \\ 2 \nmid m}} \mu(m) \left( f_2\left(\frac{X}{m^2}\right) - f_2(E) \right)$$
$$- \sum_{1 \le N \le E} c(N) \sum_{\substack{(E/N)^{1/2} < n \le (X/N)^{1/2} \\ 2 \nmid n}} M_i\left(\frac{(X/N)^{1/2}}{n}\right) \quad ,$$

*où $c(N) = 0$ si $N$ possède un facteur carré impair plus grand que 1 ou si $v_2(N) \ge 4$, et sinon $c(N) = 1, 0, 1, 2$ selon que $v_2(N) = 0, 1, 2, 3$ respectivement.*

*Démonstration.* D'après la proposition 2.1, on a

$$N_2(C_2, X) = -1 + \sum_{\substack{1 \le m \le (X/(E+1))^{1/2} \\ 2 \nmid m}} \mu(m)(f_2(X/m^2) - f_2(E))$$
$$+ \sum_{1 \le k \le E} M_i((X/k)^{1/2})(f_2(k) - f_2(k-1)) \quad .$$

Dans la deuxième somme, remplaçons $M_i((X/k)^{1/2})$ par l'expression donnée par la proposition 1.2 avec $u = (E/k)^{1/2}$. On obtient

$$\sum_{1 \le k \le E} M_i((X/k)^{1/2})(f_2(k) - f_2(k-1))$$
$$= \sum_{1 \le k \le E} M_i((E/k)^{1/2})(f_2(k) - f_2(k-1)) - S$$

avec

$$S = \sum_{1 \le k \le E} (f_2(k) - f_2(k-1))$$
$$\sum_{\substack{1 \le m \le (E/k)^{1/2} \\ 2 \nmid m}} \mu(m) \sum_{\substack{\frac{(E/k)^{1/2}}{m} < n \le \frac{(X/k)^{1/2}}{m} \\ 2 \nmid n}} M_i\left(\frac{(X/k)^{1/2}}{mn}\right)$$
$$= \sum_{1 \le N \le E} c(N) \sum_{\substack{(E/N)^{1/2} < n \le (X/N)^{1/2} \\ 2 \nmid n}} M_i\left(\frac{(X/N)^{1/2}}{n}\right) \quad ,$$

où

$$c(N)=\sum_{\substack{m^2\mid N\\ 2\nmid m}}\mu(m)\left(f_2\left(\frac{N}{m^2}\right)-f_2\left(\frac{N}{m^2}-1\right)\right)\quad .$$

Comme $f_1(m)$ est la fonction sommatoire de la suite définie par la série de Dirichlet $\zeta_2(s)$, il en résulte que $f_2(m)$ est la fonction sommatoire de la suite définie par la série de Dirichlet $(1+2^{-2s}+2^{1-3s})\zeta_2(s)$, donc $f_2(m)-f_2(m-1)$ est la suite en question. Il en résulte que

$$\begin{aligned}\sum_{N\geq 1}\frac{c(N)}{N^s}&=\left(1+\frac{1}{2^{2s}}+\frac{2}{2^{3s}}\right)\frac{\zeta_2(s)}{\zeta_2(2s)}\\&=\left(1+\frac{1}{2^{2s}}+\frac{2}{2^{3s}}\right)\prod_{p\equiv 1\pmod 2}\left(1+\frac{1}{p^s}\right)\quad ,\end{aligned}$$

d'où la formule pour $c(N)$ donnée dans la proposition. Enfin, la proposition 2.1 appliquée à $X=E$ montre que

$$\sum_{1\leq k\leq E}M_i((E/k)^{1/2})(f_2(k)-f_2(k-1))=N_2(C_2,E)+1\quad ,$$

ce qui termine la démonstration de la proposition. Noter que l'on a

$$\sum_{N\geq 1}c(N)N^{-s}=1+\Phi_2(C_2,s)\quad .$$

□

En appliquant la méthode de l'hyperbole (en coupant la sommation à $(X/N)^{1/4}$), on obtient immédiatement le corollaire suivant.

**Corollaire 2.3.** *Soit $E$ un nombre réel tel que $1\leq E\leq X^{1/2}$. On a*

$$\begin{aligned}N_2(C_2,X)=N_2(C_2,E)&+\sum_{\substack{1\leq m\leq (X/(E+1))^{1/2}\\ 2\nmid m}}\mu(m)\left(f_2\left(\frac{X}{m^2}\right)-f_2(E)\right)\\&-\sum_{1\leq N\leq E}c(N)\sum_{\substack{(E/N)^{1/2}<n\leq (X/N)^{1/4}\\ 2\nmid n}}M_i\left(\frac{(X/N)^{1/2}}{n}\right)\\&-\sum_{1\leq N\leq E}c(N)\sum_{\substack{1\leq k\leq (X/N)^{1/4}\\ 2\nmid k}}M_i(k)g((X/N)^{1/2},k)\quad ,\end{aligned}$$

*où*

$$g(Y,k)=f_1(Y/k)-f_1(\max(Y/(k+2),Y^{1/2}))$$

*est égal au nombre d'entiers impairs $n>Y^{1/2}$ tels que $Y/(k+2)<n\leq Y/k$.*

En utilisant la même méthode que dans [11], on calcule les valeurs de $M_i(Y)$ pour $Y \leq (X/E)^{1/2}$ par blocs de taille $\widetilde{O}((X/E)^{1/4})$, ce qui nécessite un temps $\widetilde{O}((X/E)^{1/2})$. Au fur et à mesure de ces calculs, on peut évaluer la première somme pour $m \leq (X/(E+1))^{1/2}$, ce qui nécessite un temps similaire. Enfin, le calcul des deux dernières sommes nécessite un temps $\widetilde{O}(X^{1/4}E^{3/4})$. Le temps de calcul de $N(C_2, E)$ est plus petit que $\widetilde{O}(E^{1/2})$ et peut donc être négligé. La valeur de $E$ rendant minimale l'expression $\widetilde{O}((X/E)^{1/2}) + \widetilde{O}(X^{1/4}E^{3/4})$ est $E = \widetilde{O}(X^{1/5})$, ce qui donne un temps de calcul de $N_2(C_2, X)$ en $\widetilde{O}(X^{2/5})$ en utilisant une taille mémoire en $\widetilde{O}(X^{1/5})$. Ceci est donc encore un peu mieux que le temps $\widetilde{O}(X^{3/7})$ obtenu ci-dessus en appliquant directement la méthode de [11].

En pratique, on doit optimiser $E$ plus précisément. Ceci dépend bien entendu de l'implémentation, et se fait par expérimentation. D'autre part, pour calculer la première somme intervenant dans la formule ci-dessus, on peut choisir un nombre réel $D \geq E$ et utiliser la formule

$$\begin{aligned}
&\sum_{\substack{1\leq m\leq (X/(E+1))^{1/2} \\ 2\nmid m}} \mu(m)\left(f_2\left(\frac{X}{m^2}\right) - f_2(E)\right) \\
&= \sum_{\substack{1\leq m\leq (X/(D+1))^{1/2} \\ 2\nmid m}} \mu(m)\left(f_2\left(\frac{X}{m^2}\right) - f_2(E)\right) \\
&\qquad + \sum_{E+1\leq k\leq D} (f_2(k) - f_2(E)) \sum_{\substack{(X/(k+1))^{1/2}<m\leq (X/k)^{1/2} \\ 2\nmid m}} \mu(m).
\end{aligned}$$

Si $R$ est le rapport du temps moyen mis pour calculer une expression du type $\lfloor (X/k)^{1/2} \rfloor$ et du temps moyen mis pour calculer une expression du type $\lfloor X/m^2 \rfloor$, on trouve qu'en choisissant $D = (X/(16R^2))^{1/3}$ on minimise le temps de calcul (une valeur typique de $R$ est $R = 2$, ce qui donne $D = X^{1/3}/4$). En pratique, le gain est évidemment beaucoup plus marginal que celui obtenu en choisissant la constante $E$ de manière optimale, mais on peut gagner quelques pourcents.

Noter qu'une expression du type $\lfloor \sqrt{z} \rfloor$ ne se calcule *pas* en calculant approximativement la racine carrée de $z$ puis en prenant la partie entière, mais en calculant la partie entière de $z$ et en utilisant un algorithme spécifique pour calculer la racine carrée entière de $\lfloor z \rfloor$ (voir [1], Algorithme 1.7.1). D'autre part la fonction $f_2(k)$ s'évalue efficacement pour $k$ entier grâce à la formule $4f_2(k) = 3k + t(k)$, où

$$t(k) = 0, 1, -2, -1, 0, 1, -2, -1, 4, 5, 2, 3, 4, 5, 2, 3$$

selon que $k \equiv 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15 \pmod{16}$ respectivement.

En utilisant les formules données ci-dessus, on peut donc calculer

$$N_2(C_2, 10^{25}) = 6079271018540266286517795$$

en 43 jours de temps CPU (Pentium III à 600 Mhz).

## 3. Le cas $G = C_3$

Utilisant la caractérisation des discriminants de corps cubiques (voir par exemple [1], Section 6.4.2), il est facile de montrer que

$$\Phi_3(C_3, s) = -\frac{1}{2} + \frac{1}{2}\left(1 + \frac{2}{3^{4s}}\right) \prod_{p \equiv 1 \pmod 6} \left(1 + \frac{2}{p^{2s}}\right) \ .$$

Il en résulte que

$$N_3(C_3, X) = \frac{1}{2}(N(X^{1/2}) - 1) \ ,$$

où $N(X)$ est la fonction sommatoire des coefficients de la série de Dirichlet

$$\Phi(s) = \left(1 + \frac{2}{3^{2s}}\right) \prod_{p \equiv 1 \pmod 6} \left(1 + \frac{2}{p^{s}}\right) \ .$$

Soit

$$L(s) = \prod_p \left(1 - \left(\frac{-3}{p}\right) p^{-s}\right)^{-1} = \sum_{n \geq 1} \frac{\left(\frac{-3}{n}\right)}{n^s}$$

la série de Dirichlet associée au caractère quadratique $\left(\frac{-3}{n}\right)$. En utilisant la notation $\zeta_\ell(s)$ déjà utilisée ci-dessus pour $\ell = 2$, on a :

$$\frac{\zeta_3(s)}{\zeta_3(2s)} L(s) = \prod_{p \neq 3} (1 + p^{-s}) \prod_p \left(1 - \left(\frac{-3}{p}\right) p^{-s}\right)^{-1} = \prod_{p \equiv 1 \pmod 6} \frac{1 + p^{-s}}{1 - p^{-s}} \ .$$

Il en résulte que

$$\prod_{p \equiv 1 \pmod 6} (1 + 2p^{-s}) = \frac{\zeta_3(s)}{\zeta_3(2s)} L(s) \prod_{p \equiv 1 \pmod 6} \frac{(1 + 2p^{-s})(1 - p^{-s})}{1 + p^{-s}} \ .$$

Toutefois, il est préférable d'écrire ceci sous la forme :

$$\prod_{p\equiv 1 \pmod 6}(1+2p^{-s}) = \zeta_3(s)L(s)\prod_{p\equiv 2 \pmod 3}\left(1-\frac{1}{p^{2s}}\right)$$
$$\times\prod_{p\equiv 1 \pmod 6}\left(1+\frac{2}{p^s}\right)\left(1-\frac{1}{p^s}\right)^2$$
$$= \zeta_3(s)L(s)\prod_{p\equiv 2 \pmod 3}\left(1-\frac{1}{p^{2s}}\right)\prod_{p\equiv 1 \pmod 6}\left(1-\frac{3}{p^{2s}}+\frac{2}{p^{3s}}\right) \ .$$

Posons

$$\left(1+\frac{2}{3^{2s}}\right)\prod_{p\equiv 2 \pmod 3}\left(1-\frac{1}{p^{2s}}\right)\prod_{p\equiv 1 \pmod 6}\left(1-\frac{3}{p^{2s}}+\frac{2}{p^{3s}}\right) = \sum_{n\geq 1}\frac{b(n)}{n^s} \ .$$

Il est clair que $b(n)\neq 0$ si et seulement si $n=x^2y^3$ avec $x$ et $y$ sans facteur carré, premiers entre eux, et tel que les diviseurs premiers de $y$ sont tous congrus à 1 modulo 6. Pour un tel $n=x^2y^3$, il est clair qu'on a

$$b(n)=\mu(x)(-2)^{v_3(x)}3^{\omega_6(x)}2^{\omega_6(y)}$$

où $v_3(x)$ désigne l'exposant de 3 dans la factorisation de $x$ (donc 0 ou 1) et $\omega_6(x)$ est le nombre de diviseurs premiers de $x$ congrus à 1 modulo 6. Si

$$\zeta_3(s)L(s)=\sum_{3\nmid n}\frac{a_n}{n^s}$$

et si on pose $A(X)=\sum_{1\leq n\leq X}a_n$, on a donc comme ci-dessus

$$N(X)=\sum_{n\leq X}b(n)A(X/n)$$
$$=\sum_{\substack{y\leq X^{1/3}\\ |\mu(y)|=1\\ p|y\implies p\equiv 1 \pmod 6}}2^{\omega_6(y)}\sum_{\substack{x\leq (X/y^3)^{1/2}\\ (x,y)=1}}\mu(x)(-2)^{v_3(x)}3^{\omega_6(x)}A(X/(x^2y^3)) \ .$$

Pour calculer $A(Y)$, nous allons appliquer la méthode de l'hyperbole, c'est-à-dire la Proposition 1.1. On écrit

$$\zeta_3(s)L(s)=\zeta(s)\left(1-\frac{1}{3^s}\right)\sum_{n\geq 1}\frac{\left(\frac{-3}{n}\right)}{n^s}=\zeta(s)\sum_{n\geq 1}\frac{\left(\frac{-3}{n}\right)-\left(\frac{-3}{n/3}\right)}{n^s} \ ,$$

où il est entendu que le terme $\left(\frac{-3}{n/3}\right)$ est omis quand $3\nmid n$. Posons $\chi(n)=\left(\frac{-3}{n}\right)-\left(\frac{-3}{n/3}\right)$. C'est une fonction périodique de période 9 dont les valeurs sont $0,1,-1,-1,1,-1,1,1,-1$ quand $n \equiv 0,1,2,3,4,5,6,7,8 \pmod 9$ respectivement. Si on note $\psi(n)$ sa fonction sommatoire, c'est également une fonction périodique de période 9 dont les valeurs correspondantes aux entiers sont $0,1,0,-1,0,-1,0,1,0$ (si $z$ n'est pas entier on a évidemment $\psi(z) = \psi(\lfloor z \rfloor)$). Appliquant donc la proposition 1.1 aux suites 1 et $\chi(n)$, on en déduit donc que pour tout réel $E$ tel que $1 \le E \le Y$ on a

$$A(Y) = \sum_{1 \le n \le E} \psi(Y/n) + \sum_{1 \le n \le Y/E} \chi(n) \lfloor Y/n \rfloor - \lfloor E \rfloor \psi(Y/E) \ .$$

Comme les fonctions $\psi$ et $\chi$ sont périodiques de période 9, leur calcul se fait en lisant une simple table, donc ne prend pas de temps. Il faut donc calculer approximativement $E + Y/E$ fois une quantité de la forme $\lfloor Y/n \rfloor$, et ceci prend un temps minimal quand $E = Y^{1/2}$ (rappelons que $E$ n'est pas nécessairement un entier). On utilise donc la formule

$$A(Y) = \sum_{1 \le n \le Y^{1/2}} (\chi(n) \lfloor Y/n \rfloor + \psi(Y/n)) - \lfloor Y^{1/2} \rfloor \psi(Y^{1/2}) \ .$$

Le calcul de $A(Y)$ prend donc un temps $\widetilde{O}(Y^{1/2})$.

**Remarque.** Il était préférable, comme nous l'avons fait, d'appliquer la méthode de l'hyperbole à $\zeta(s)$ et $(1-3^{-s})L(s)$ plutôt qu'à $(1-3^{-s})\zeta(s) = \zeta_3(s)$ et $L(s)$, car la fonction sommatoire de $\zeta_3(s)$ est $\lfloor X \rfloor - \lfloor X/3 \rfloor$, donc est plus longue à calculer.

Il résulte de la formule pour $N(X)$ ci-dessus que le temps de calcul de $N(X)$ est de

$$\begin{aligned} \sum_{y \le X^{1/3}} \sum_{x \le (X/y^3)^{1/2}} \widetilde{O}((X/(x^2y^3))^{1/2}) &= \widetilde{O}(X^{1/2}) \sum_{y \le X^{1/3}} y^{-3/2} \log(X/y^3) \\ &= \widetilde{O}(X^{1/2}) \ , \end{aligned}$$

donc le temps de calcul de $N_3(C_3, X)$ est en $\widetilde{O}(X^{1/4})$. Cela explique pourquoi nous pouvons aller beaucoup plus loin que pour $C_2$. Par exemple, en utilisant les formules données ci-dessus, nous avons pu calculer

$$N_3(C_3, 10^{37}) = 501310370031289126$$

en une quarantaine d'heures CPU (Pentium III à 600 Mhz).

## 4. Le cas $G = C_4$

L'étude des extensions $C_4$ de $\mathbb{Q}$ n'est pas difficile, mais un peu moins facile tout de même que celle des extensions $C_2$ et $C_3$. Quoi qu'il en soit, on trouve (voir [4] [6]) que

$$\Phi_4(C_4,s)=\frac{\zeta(2s)}{2\zeta(4s)(1+1/2^{2s})}$$
$$\times\left(\left(1+\frac{1}{2^{4s}}+\frac{2}{2^{6s}}+\frac{4}{2^{11s}}\right)\prod_{p\equiv 1 \pmod 4}\left(1+\frac{2}{p^{3s}+p^s}\right)-\left(1+\frac{1}{2^{4s}}+\frac{2}{2^{6s}}\right)\right)\ .$$

D'après la formule du paragraphe 2, on a

$$\frac{\zeta(2s)}{2\zeta(4s)(1+1/2^{2s})}\left(1+\frac{1}{2^{4s}}+\frac{2}{2^{6s}}\right)=\frac{1}{2}\left(1+\Phi_2(C_2,2s)\right)\ .$$

Il en résulte que

$$N_4(C_4,X)=\frac{1}{2}\left(N(X)-N_2(C_2,X^{1/2})-1\right)\ ,$$

où $N(X)$ est la fonction sommatoire des coefficients de la série de Dirichlet

$$\Phi(s)=\frac{\zeta_2(2s)}{\zeta_2(4s)}\left(1+\frac{1}{2^{4s}}+\frac{2}{2^{6s}}+\frac{4}{2^{11s}}\right)\prod_{p\equiv 1 \pmod 4}\left(1+\frac{2}{p^{3s}+p^s}\right)\ .$$

On peut écrire

$$\Phi(s)=\zeta_2(2s)\left(1+\frac{1}{2^{4s}}+\frac{2}{2^{6s}}+\frac{4}{2^{11s}}\right)$$
$$\prod_{p\equiv 1 \pmod 4}\left(1+\frac{2}{p^{3s}}-\frac{1}{p^{4s}}-\frac{2}{p^{5s}}\right)\prod_{p\equiv 3 \pmod 4}\left(1-\frac{1}{p^{4s}}\right)\ .$$

Ceci est donc le produit de la série de Dirichlet $\zeta_2(2s)$ dont la fonction sommatoire se calcule en temps $\widetilde{O}(1)$ par un produit eulérien de valuation égale à 3, donc en appliquant directement la formule donnant la fonction sommatoire du produit des deux séries, on obtient une méthode de calcul de $N(X)$ (et donc de $N_4(C_4,X)$) en temps $\widetilde{O}(X^{1/3})$. Je ne vois pas comment ramener ceci à un temps $\widetilde{O}(X^{1/4})$ en utilisant les méthodes que nous avons utilisées ci-dessus.

Bien que la formule obtenue donne une méthode en $\widetilde{O}(X^{1/3})$, il est préférable d'utiliser une formule différente, qui sera toujours en $\widetilde{O}(X^{1/3})$, mais qui sera en pratique plus rapide.

Pour cela, nous écrivons $\zeta_2(2s)/\zeta_2(4s)=\prod_{p>2}(1+p^{-2s})$, et on obtient :

$$\Phi(s)=\left(1+\frac{1}{2^{4s}}+\frac{2}{2^{6s}}+\frac{4}{2^{11s}}\right)\prod_{p\equiv 1 \pmod 4}\left(1+\frac{1}{p^{2s}}+\frac{2}{p^{3s}}\right)$$
$$\times\prod_{p\equiv 3 \pmod 4}\left(1+\frac{1}{p^{2s}}\right)\ .$$

Il en résulte que

$$N(X) = S(X) + S(X/16) + 2S(X/64) + 4S(X/2048)$$

où $S$ est la fonction sommatoire de la suite $b(n)$ définie par la série de Dirichlet $\Phi(s)$ dont on omet le facteur local en 2 (ceci est bien entendu indépendant de la manière dont on écrit $\Phi(s)$). Or il est clair que $b(n) \neq 0$ si et seulement si $n$ est de la forme $n = x^3y^2$ avec $x$ et $y$ sans facteur carré et premiers entre eux, $y$ impair, et $x$ divisible seulement par des premiers congrus à 1 modulo 4. Pour un tel $n$, on a $b(n) = 2^{\omega(x)}$.

Pour alléger les notations, notons $\mathcal{X}$ l'ensemble des $x$ sans facteur carré divisible seulement par des premiers congrus à 1 modulo 4 et $\mathcal{Y}$ l'ensemble des entiers $y$ impairs sans facteur carré. On a donc la formule

$$S(X) = \sum_{\substack{x \le X^{1/3} \\ x \in \mathcal{X}}} 2^{\omega(x)} \sum_{\substack{y \le (X/x^3)^{1/2} \\ y \in \mathcal{Y} \\ (x,y)=1}} 1 \ .$$

L'astuce supplémentaire mentionnée ci-dessus consiste à remarquer que l'on peut calculer rapidement la somme intérieure. Posons

$$T(Y, x) = \sum_{\substack{y \le Y \\ y \in \mathcal{Y} \\ (x,y)=1}} 1 \ .$$

Comme nous l'avons vu ci-dessus, la formule pour $\zeta(s)/\zeta(2s) = \prod_p (1+p^{-s})$ équivaut à la formule

$$|\mu(y)| = \sum_{m^2 | y} \mu(m) \ .$$

On a donc :

$$T(Y, x) = \sum_{\substack{y \le Y \\ (y,2x)=1}} |\mu(y)| = \sum_{\substack{y \le Y \\ (y,2x)=1}} \sum_{m^2 | y} \mu(m) = \sum_{\substack{m \le Y^{1/2} \\ (m,2x)=1}} \mu(m) \sum_{\substack{a \le Y/m^2 \\ (a,2x)=1}} 1 \ .$$

Pour calculer la présente somme intérieure, posons enfin

$$U(Z, x) = \sum_{\substack{a \le Z \\ (a,2x)=1}} 1 \ .$$

Ecrivons la division euclidienne de $Z$ par $2x$, disons $Z = 2xq + r$ avec $0 \le r \le 2x - 1$, où on a bien entendu $q = \lfloor Z/2x \rfloor$ et $r = Z \bmod 2x$. Si d'autre part on écrit la division euclidienne de $a$ par $2x$, soit $a = q_1(2x) + r_1$, il est clair que $a \le Z$ équivaut à $q_1 < q$ ou $q_1 = q$ et $r_1 \le r$, et d'autre part que $(a,2x)=(r_1,2x)$. On a donc

$$U(Z,x)=\sum_{0\le q_1<q}\sum_{\substack{1\le r_1\le 2x-1\\(r_1,2x)=1}}1+\sum_{\substack{1\le r_1\le r\\(r_1,2x)=1}}1=q\varphi(2x)+\sum_{\substack{1\le r_1\le r\\(r_1,2x)=1}}1\ .$$

Comme $q=\lfloor Z/2x\rfloor$ et que $x$ est impair, on a donc finalement

$$U(Z,x)=\varphi(x)\left\lfloor\frac{Z}{2x}\right\rfloor+\sum_{\substack{1\le r_1\le r\\(r_1,2x)=1}}1=\varphi(x)\left(1+\left\lfloor\frac{Z}{2x}\right\rfloor\right)-\sum_{\substack{r<r_1\le 2x-1\\(r_1,2x)=1}}1\ .$$

Nous avons donc trois formules pour calculer $U(Z,x)$. La définition initiale nécessite $Z$ calculs de PGCD avec $2x$. La première formule ci-dessus, outre le calcul de $\varphi(x)$ (qui pourrait être négligé puisque $x$ est la variable de la somme externe) nécessite 1 division et $r$ PGCD. Enfin, la deuxième formule ci-dessus nécessite 1 division et $2x-r$ PGCD. Puisqu'on a toujours $r\le Z$, il en résulte que l'on utilisera la définition initiale si $Z=r\le 2x-r$ (pour éviter une division), c'est-à-dire si $Z\le x$, la première formule ci-dessus quand $r\le x$ et enfin la deuxième quand $r>x$. Il est à noter que le cas $Z\le x$ arrive en fait très fréquemment et n'est donc pas à négliger. En effet, on a $Z=Y/m^2\le Y=(X/x^3)^{1/2}$ donc $Z\le x$ dès que $x\ge X^{1/5}$, c'est-à-dire pour presque toutes les valeurs de $x$.

Pour résumer, on a donc

$$N_4(C_4,X)=\frac{1}{2}\Big(S(X)+S(X/16)+2S(X/64)+4S(X/2048)\\ -N_2(C_2,X^{1/2})-1\Big)\ ,$$

où

$$S(X)=\sum_{\substack{x\le X^{1/3}\\x\in\mathcal{X}}}2^{\omega(x)}T((X/x^3)^{1/2},x)\ ,$$

$$T(Y,x)=\sum_{\substack{m\le Y^{1/2}\\(m,2x)=1}}\mu(m)U(Y/m^2,x)\ ,$$

$$U(Z,x)=\begin{cases}\sum_{\substack{1\le r_1\le Z\\(r_1,2x)=1}}1 & \text{si } Z\le x\\ \varphi(x)\lfloor Z/2x\rfloor+\sum_{\substack{1\le r_1\le r\\(r_1,2x)=1}}1 & \text{si } Z>x \text{ et } r\le x\\ \varphi(x)\left(1+\lfloor Z/2x\rfloor\right)-\sum_{\substack{r<r_1\le 2x-1\\(r_1,2x)=1}}1 & \text{si } r>x\ ,\end{cases}$$

où $r=Z \bmod 2x$.

Cette formule donne un moyen efficace en $\widetilde{O}(X^{1/3})$ de calculer $N_4(C_4,X)$ (nettement plus efficace que l'utilisation directe du produit eulérien, bien que du même ordre de grandeur). Par exemple, en utilisant les formules données ci-dessus, nous avons pu calculer

$$N_4(C_4, 10^{30}) = 122051516492357$$

en environ 8 jours de temps CPU (Pentium III à 600 Mhz).

## 5. Le cas $G = V_4 = C_2 \times C_2$

L'étude des extensions $V_4 = C_2 \times C_2$ est très facile, et on trouve (voir [4] [6]) que

$$\begin{aligned}\Phi_4(V_4, s) = &\frac{1}{6}\left(1 + \frac{3}{2^{4s}} + \frac{6}{2^{6s}} + \frac{6}{2^{8s}}\right) \prod_{p \equiv 1 \pmod 2} \left(1 + \frac{3}{p^{2s}}\right) \\ &- \frac{1}{2}\left(1 + \frac{1}{2^{4s}} + \frac{2}{2^{6s}}\right) \prod_{p \equiv 1 \pmod 2} \left(1 + \frac{1}{p^{2s}}\right) + \frac{1}{3} \ .\end{aligned}$$

Il en résulte que

$$\begin{aligned}N_4(V_4, X) &= \frac{1}{6}(N(X^{1/2}) - 3(N_2(C_2, X^{1/2}) + 1) + 2) \\ &= \frac{1}{6}(N(X^{1/2}) - 3N_2(C_2, X^{1/2}) - 1) \ ,\end{aligned}$$

où $N(X)$ est la fonction sommatoire de la fonction arithmétique définie par la série de Dirichlet

$$\Phi(s) = \left(1 + \frac{3}{2^{2s}} + \frac{6}{2^{3s}} + \frac{6}{2^{4s}}\right) \prod_{p \equiv 1 \pmod 2} \left(1 + \frac{3}{p^s}\right) \ .$$

Le produit eulérien dont le comportement se rapproche le plus de celui de $\Phi(s)$ est le produit eulérien associé à $\zeta_2(s)^3$. On écrit donc

$$\Phi(s) = \left(1 + \frac{3}{2^{2s}} + \frac{6}{2^{3s}} + \frac{6}{2^{4s}}\right) \zeta_2(s)^3 \prod_{p \equiv 1 \pmod 2} \left(1 - \frac{6}{p^{2s}} + \frac{8}{p^{3s}} - \frac{3}{p^{4s}}\right) \ .$$

Définissons la fonction arithmétique $b(n)$ comme la fonction multiplicative vérifiant pour tout nombre premier $p$ impair $b(p) = 0$, $b(p^2) = -6$, $b(p^3) = 8$, $b(p^4) = -3$ et $b(p^v) = 0$ pour $v \geq 5$. Ecrivons d'autre part $\zeta_2(s)^3 = \sum_{n \text{ impair}} d_3(n) n^{-s}$, et soit $D(X)$ la fonction sommatoire des $d_3(n)$ pour $n$ impair. On aura donc

$$N(X) = S(X) + 3S(X/4) + 6S(X/8) + 6S(X/16) \qquad \text{avec} \quad S(X) = \sum_{n \leq X} b(n) D(X/n) \ .$$

De plus, on a $b(n) \neq 0$ si et seulement si $n$ est impair de la forme $n = x^3y^2$ avec $x$ sans facteur carré, $y$ sans facteur cubique et $(x, y) = 1$, et on a dans ce cas

$$b(x^3y^2) = 2^{3\omega(x)}b_1(y)$$

où $b_1(y)$ est la fonction arithmétique multiplicative vérifiant pour tout nombre premier impair $b_1(p) = -6$, $b_1(p^2) = -3$ et $b_1(p^v) = 0$ pour tout $v \geq 3$. Il en résulte que

$$S(X) = \sum_{\substack{x \leq X^{1/3} \\ |\mu(2x)|=1}} 2^{3\omega(x)} \sum_{\substack{y \leq (X/x^3)^{1/2} \\ (y,2x)=1}} b_1(y)D(X/(x^3y^2)) \ .$$

Il nous reste à donner un moyen efficace de calculer $D(Y)$.

Pour cela, nous utilisons tout d'abord la méthode de l'hyperbole appliquée à la série de Dirichlet $\zeta_2(s)^2$. Rappelons que nous avons noté $f_1(x) = \lfloor (x + 1)/2 \rfloor$ la fonction sommatoire de la suite définie par la série de Dirichlet $\zeta_2(s)$. Si on appelle $B(X)$ la fonction sommatoire associée à $\zeta_2(s)^2$, on a donc, en choisissant $E = X^{1/2}$ :

$$B(X) = 2 \sum_{\substack{1 \leq n \leq X^{1/2} \\ 2 \nmid n}} f_1(X/n) - f_1(X^{1/2})^2 \ .$$

On en déduit :

$$\begin{aligned} D(X) &= 2 \sum_{\substack{1 \leq n \leq X \\ 2 \nmid n}} \sum_{\substack{1 \leq m \leq (X/n)^{1/2} \\ 2 \nmid m}} f_1(X/(nm)) - \sum_{\substack{1 \leq n \leq X \\ 2 \nmid n}} f_1((X/n)^{1/2})^2 \\ &= 2 \sum_{\substack{m^2 n \leq X \\ 2 \nmid mn}} f_1(X/nm) - \sum_{\substack{1 \leq n \leq X \\ 2 \nmid n}} f_1((X/n)^{1/2})^2 \\ &= 2 \sum_{\substack{1 \leq m \leq X^{1/2} \\ 2 \nmid m}} I_{1,m}(X) - I_2(X) \ , \end{aligned}$$

avec

$$I_{1,m}(X) = \sum_{\substack{1 \leq n \leq X/m^2 \\ 2 \nmid n}} f_1(X/nm) \quad \text{et} \quad I_2(X) = \sum_{\substack{1 \leq n \leq X \\ 2 \nmid n}} f_1((X/n)^{1/2})^2 \ .$$

Pour calculer efficacement $I_{1,m}(X)$, nous allons appliquer une variante de la méthode de l'hyperbole. Soit $E$ un nombre réel tel que $1 \leq E \leq X/m^2$.

On a :

$$\begin{aligned}
I_{1,m}(X) &= \sum_{\substack{1\le n\le E\\ 2\nmid n}} f_1(X/nm) + \sum_{f_1(m)\le k\le f_1(X/Em)} k \sum_{\substack{f_1(X/nm)=k\\ 2\nmid n}} 1\\
&= \sum_{\substack{1\le n\le E\\ 2\nmid n}} f_1(X/nm) + \sum_{f_1(m)\le k\le f_1(X/Em)} k \sum_{\substack{X/(m(2k+1))<n\le X/(m(2k-1))\\ n>E\\ 2\nmid n}} 1\\
&= \sum_{\substack{1\le n\le E\\ 2\nmid n}} f_1(X/nm)\\
&+ \sum_{f_1(m)\le k\le f_1(X/Em)} k(f_1(X/(m(2k-1))) - f_1(\max(X/(m(2k+1)),E)))\ .
\end{aligned}$$

Puisque $m$ est impair, $f_1(m)=(m+1)/2$. En posant $n=2k-1$ et utilisant une sommation d'Abel on obtient :

$$\begin{aligned}
I_{1,m}(X) = \sum_{\substack{1\le n\le E\\ 2\nmid n}} f_1(X/nm) &+ \sum_{\substack{m<n\le X/Em\\ 2\nmid n}} f_1(X/nm)\\
&+ f_1(m)f_1(X/m^2) - f_1(X/Em)f_1(E)\ .
\end{aligned}$$

Notons que la définition de $I_{1,m}$ nécessite un temps $\widetilde{O}(X/m^2)$, alors que l'utilisation de la présente formule en nécessite $\widetilde{O}(E+X/Em-m)$. Le minimum est atteint pour $E=(X/m)^{1/2}$, mais comme nous devons avoir $E\le X/m^2$, cela implique que $m\le X^{1/3}$. En résumé, pour calculer $I_{1,m}(X)$, on utilise la définition

$$I_{1,m}(X) = \sum_{\substack{1\le n\le X/m^2\\ 2\nmid n}} f_1(X/nm)$$

quand $m>X^{1/3}$ et la formule

$$\begin{aligned}
I_{1,m}(X) = \sum_{\substack{1\le n\le m\\ 2\nmid n}} f_1(X/nm) &+ 2\sum_{\substack{m<n\le (X/m)^{1/2}\\ 2\nmid n}} f_1(X/nm)\\
&+ f_1(m)f_1(X/m^2) - f_1((X/m)^{1/2})^2
\end{aligned}$$

quand $m\le X^{1/3}$.

Reste enfin à calculer $I_2(X)$. On applique à nouveau le principe de l'hyperbole, et on choisit cette fois-ci $E=X^{1/3}$. Je laisse le détail des calculs (faciles) au lecteur, et on trouve :

$$I_2(X) = \sum_{\substack{n \le X^{1/3} \\ 2 \nmid n}} (f_1((X/n)^{1/2})^2 + n f_1(X/n^2)) - f_1(X^{1/3})^3 \ .$$

Ces formules, jointes aux formules ci-dessus, donnent une méthode en $\widetilde{O}(X^{1/3})$ pour calculer $N_4(V_4, X)$. Nous avons pu par exemple calculer

$$N_4(V_4, 10^{35}) = 6894524058812256194$$

en moins de 15 jours de temps CPU (Pentium III à 600 Mhz).

## Bibliographie


[1] H. Cohen, *A course in computational algebraic number theory (third printing)*. Graduate Texts in Math. **138**, Springer-Verlag (1996).

[2] H. Cohen, *Advanced topics in computational number theory*. Graduate Texts in Math **193**, Springer-Verlag (2000).

[3] H. Cohen, F. Diaz y Diaz, M. Olivier, *Densité des discriminants des extensions cycliques de degré premier*, C.R. Acad. Sci. Paris **330** (2000), 61–66.

[4] H. Cohen, F. Diaz y Diaz, M. Olivier, *Counting discriminants of number fields of degree up to four*. proceedings ANTS IV Leiden (2000), Lecture Notes in Comp. Sci. **1838**, Springer-Verlag, 269–283.

[5] H. Cohen, F. Diaz y Diaz, M. Olivier, *Counting discriminants of number fields*. MSRI preprint **2000-026** (2000), 9p.

[6] H. Cohen, F. Diaz y Diaz, M. Olivier, *Asymptotic and exact enumeration of discriminants of number fields*. En préparation.

[7] H. Cohen, F. Diaz y Diaz, M. Olivier, *Enumerating quartic dihedral extensions of* $\mathbb{Q}$. Submitted.

[8] H. Cohen, F. Diaz y Diaz, M. Olivier, *On the density of discriminants of cyclic extensions of prime degree*. En préparation.

[9] H. Cohen, F. Diaz y Diaz, M. Olivier, *On the density of discriminants of quartic number fields*. En préparation.

[10] H. Cohen, F. Dress, M. El Marraki, *Explicit estimates for summatory functions linked to the Möbius $\mu$-function*. Preprint (1996), soumis.

[11] M. Deléglise, J. Rivat, *Computing the summation of the Möbius function*. Exp. Math. **5** (1996), 291–295.

[12] G. Tenenbaum, *Introduction à la théorie analytique et probabiliste des nombres*. Cours Spécialisé S.M.F. **1**, Paris (1996).



Henri Cohen
Laboratoire A2X
U.M.R. 5465 du C.N.R.S.
Université Bordeaux I
351 Cours de la Libération
33405 Talence Cedex
France
*E-mail* : cohen@math.u-bordeaux.fr