Counting cubic extensions with given quadratic resolvent

Anna Morra
(joint work with Henri Cohen)

Université Bordeaux 1

Warwick, May 27th 2008

Definitions and notation

- Given $k \subset K$ two number fields, we denote by $\mathfrak{d}(K/k)$ the relative discriminant ideal of the extension.
- We define

$$N_{k,n}(X) = \sharp\{K | [K : k] = n, \mathcal{N}_{k/\mathbb{Q}}\mathfrak{d}(K/k) \le X\}/ \sim$$

Two main themes in the subject :

- Asymptotics as $X \to \infty$;
- Algorithmics.

Asymptotic results

- Asymptotic for relative quadratic extensions : Wright, Cohen-Diaz y Diaz-Olivier;
- Asymptotics for cubic extensions : Davenport-Heilbronn ($k = \mathbb{Q}$) Datskovsky-Wright (k arbitrary);
- Asymptotics for $n = 4, 5$ and $k = \mathbb{Q}$: Bhargava.

Let us focus on the case $n = 3$.

We may ask some more specific questions:

1. How many Galois (cyclic) extensions ?

   Then answer is given by Cohn for the rational case and by Cohen-Diaz y Diaz-Oliver for the general case.

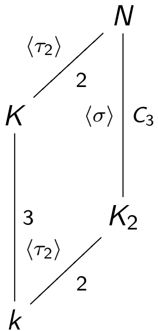
2. How many non-Galois extensions with a fixed quadratic resolvent K_2 ?

   We are going to answer to this question in this talk.

Let k be a number field, and fix K_2 a quadratic extension of k.

We define $\mathcal{F}(K_2)$ the set of cubic extensions K of k (modulo k-isomorphism) whose Galois closure N contains K_2 as quadratic subextension.

If we allow $[K_2 : k] = 1$ we can also describe cyclic cubic extensions.



Our goal

We look for an asymptotic formula for

$$N(K_2/k, X) = |\{K \in \mathcal{F}(K_2),\ \mathcal{N}_{k/\mathbb{Q}}(\mathfrak{d}(K/k)) \leq X\}| .$$

The conductor of the cyclic extension N/K_2 is of the form $\mathfrak{f}(N/K_2) = \mathfrak{f}(K/k)\mathbb{Z}_{K_2}$, where $\mathfrak{f}(K/k)$ is an ideal of k.

Since

$$\mathfrak{d}(K/k) = \mathfrak{d}(K_2/k)\mathfrak{f}(K/k)^2,$$

then we can reduce to study $M(K_2/k, X)$ where

$$M(K_2/k, X) = |\{K \in \mathcal{F}(K_2),\ \mathcal{N}_{k/\mathbb{Q}}(\mathfrak{f}(K/k)) \leq X\}|$$

Idea

We can study the fundamental Dirichlet series:

$$\Phi(s) = \frac{1}{2} + \sum_{K \in \mathcal{F}(K_2)} \frac{1}{\mathcal{N}_{k/\mathbb{Q}}(\mathfrak{f}(K/k))^s} ,$$

and thanks to a Tauberian theorem we can deduct asymptotic formulas for $M(K_2/k, X)$.

Outline of the work

1. Galois structure of the extensions (Kummer theory)

Outline of the work

1. Galois structure of the extensions (Kummer theory)
2. Conductor of the extensions (Hecke's Theorem)

Outline of the work

1. Galois structure of the extensions (Kummer theory)
2. Conductor of the extensions (Hecke's Theorem)
3. Study of the fundamental Dirichlet series

Outline of the work

1. Galois structure of the extensions (Kummer theory)
2. Conductor of the extensions (Hecke's Theorem)
3. Study of the fundamental Dirichlet series
4. Asymptotic formulas.

Galois theory

Let $\rho = \zeta_3$ a primitive cube root of unity.
Set $L = K_2(\rho)$ and $k_z = k(\rho)$.
Let

- τ be a generator of $\mathrm{Gal}(L/K_2)$,
- τ_2 a generator of $\mathrm{Gal}(K_2/k)$
- σ be a generator of the cyclic group of order 3 $\mathrm{Gal}(N/K_2) \simeq \mathrm{Gal}(N_z/L)$, where $N_z = N(\rho)$.

We have the following relations:

$$\tau^2 = \tau_2^2 = 1 \ , \quad \tau\tau_2 = \tau_2\tau \ , \quad \tau\sigma = \sigma\tau \ .$$

Five possible situations

1. K/k cyclic and $\rho \in k \Rightarrow \tau = \tau_2 = 1$.
2. K/k cyclic and $\rho \notin k \Rightarrow \tau_2 = 1,\ \tau(\rho) = \rho^{-1}$.
3. K/k non-cyclic and $\rho \in k \Rightarrow \tau = 1$ and $\tau_2(\rho) = \rho$.
4. K/k non-cyclic and $\rho \in K_2 \setminus k \Rightarrow \tau = 1$ and $\tau_2(\rho) = \rho^{-1}$.
5. K/k non-cyclic and $\rho \notin K_2 \Rightarrow \tau(\rho) = \rho^{-1}$ and $\tau_2(\rho) = \rho$.

Definition 1

- In cases (1) to (5) above, we set $T = \emptyset$, $\{\tau + 1\}$, $\{\tau_2 + 1\}$, $\{\tau_2 - 1\}$, $\{\tau + 1, \tau_2 + 1\}$, respectively, where T is considered as a subset of the group ring $\mathbb{Z}[\mathrm{Gal}(L/k)]$ or of $\mathbb{F}_3[\mathrm{Gal}(L/k)]$.

Definition 1

- In cases (1) to (5) above, we set $T = \emptyset$, $\{\tau + 1\}$, $\{\tau_2 + 1\}$, $\{\tau_2 - 1\}$, $\{\tau + 1, \tau_2 + 1\}$, respectively, where T is considered as a subset of the group ring $\mathbb{Z}[\mathrm{Gal}(L/k)]$ or of $\mathbb{F}_3[\mathrm{Gal}(L/k)]$.
- We define $\iota(\tau \pm 1) = \tau \mp 1$ and $\iota(\tau_2 \pm 1) = \tau_2 \mp 1$.

Definition 1

- In cases (1) to (5) above, we set $T = \emptyset$, $\{\tau + 1\}$, $\{\tau_2 + 1\}$, $\{\tau_2 - 1\}$, $\{\tau + 1, \tau_2 + 1\}$, respectively, where T is considered as a subset of the group ring $\mathbb{Z}[\mathrm{Gal}(L/k)]$ or of $\mathbb{F}_3[\mathrm{Gal}(L/k)]$.
- We define $\iota(\tau \pm 1) = \tau \mp 1$ and $\iota(\tau_2 \pm 1) = \tau_2 \mp 1$.
- For any group M on which T acts, we denote by $M[T]$ the subgroup of elements of M annihilated by all the elements of T.

Definition 1

- In cases (1) to (5) above, we set $T = \emptyset$, $\{\tau + 1\}$, $\{\tau_2 + 1\}$, $\{\tau_2 - 1\}$, $\{\tau + 1, \tau_2 + 1\}$, respectively, where T is considered as a subset of the group ring $\mathbb{Z}[\mathrm{Gal}(L/k)]$ or of $\mathbb{F}_3[\mathrm{Gal}(L/k)]$.
- We define $\iota(\tau \pm 1) = \tau \mp 1$ and $\iota(\tau_2 \pm 1) = \tau_2 \mp 1$.
- For any group M on which T acts, we denote by $M[T]$ the subgroup of elements of M annihilated by all the elements of T.

Lemma 2

Let M be an $\mathbb{F}_3[\mathrm{Gal}(L/k)]$-module. For any $t \in T$ we have $M[t] = \iota(t)(M)$, and conversely $M[\iota(t)] = t(M)$.

Proposition 3

1. *There exists a bijection between :*
   - *isomorphism classes of extensions K/k having quadratic resolvent isomorphic to K_2 (i. e. elements of $\mathcal{F}(K_2)$), and*
   - *elements $\overline{\alpha} \in (L^*/{L^*}^3)[T]$, $\overline{\alpha} \neq \overline{1}$, modulo the equivalence relation identifying $\overline{\alpha}$ with its inverse.*
2. *If $\alpha \in L^*$ is some representative of $\overline{\alpha}$, the extension K/k corresponding to α is the fixed field under $\mathrm{Gal}(L/k)$ of the field $N_z = L(\sqrt[3]{\alpha})$.*

Definition 4

We denote by $V_3(L)$ the group of 3-*virtual units* of L, in other words the group of $u \in L^*$ such that $u\mathbb{Z}_L = \mathfrak{q}^3$ for some ideal $\mathfrak{q}$ of L. We define the 3-*Selmer group* $S_3(L)$ of L by $S_3(L) = V_3(L)/{L^*}^3$.

Proposition 5

1. *There exists a bijection between isomorphism classes of cubic extensions K/k with given quadratic resolvent field K_2 and equivalence classes of triples $(\mathfrak{a}_0, \mathfrak{a}_1, \overline{u})$ such that*
   1. *The $\mathfrak{a}_i$ are coprime integral squarefree ideals of L such that $\overline{\mathfrak{a}_0\mathfrak{a}_1^2} \in Cl(L)^3$ and $\mathfrak{a}_0\mathfrak{a}_1^2 \in (I/I^3)[T]$, where I is the group of fractionals ideals of L.*
   2. *$\overline{u} \in S_3(L)[T]$, and $\overline{u} \neq 1$ when $\mathfrak{a}_0 = \mathfrak{a}_1 = \mathbb{Z}_L$.*

   modulo the equivalence relation $(\mathfrak{a}_0, \mathfrak{a}_1, \overline{u}) \sim (\mathfrak{a}_1, \mathfrak{a}_0, 1/\overline{u})$
2. *If $(\mathfrak{a}_0, \mathfrak{a}_1)$ is a pair of ideals satisfying (1.1) there exist an ideal $\mathfrak{q}_0$ and an element α_0 of L such that $\mathfrak{a}_0\mathfrak{a}_1^2\mathfrak{q}_0^3 = \alpha_0\mathbb{Z}_L$ with $\alpha_0 \in (L^*/{L^*}^3)[T]$. The cubic extensions K/k corresponding to such a pair $(\mathfrak{a}_0, \mathfrak{a}_1)$ are given as follows: for any $\overline{u} \in S_3(L)[T]$ the extension is the cubic subextension of $N_z = L(\sqrt[3]{\alpha_0 u})$ (for any lift u of $\overline{u}$).*

Lemma 6

1. *The condition* $\mathfrak{a}_0\mathfrak{a}_1^2 \in (I/I^3)[T]$ *is equivalent to* $\mathfrak{a}_1 = \tau(\mathfrak{a}_0)$, $\mathfrak{a}_1 = \tau_2(\mathfrak{a}_0)$, $\mathfrak{a}_0 = \tau_2(\mathfrak{a}_0)$ *and* $\mathfrak{a}_1 = \tau_2(\mathfrak{a}_1)$, *and* $\mathfrak{a}_1 = \tau(\mathfrak{a}_0) = \tau_2(\mathfrak{a}_0)$ *in cases (2), (3), (4), and (5), respectively.*

Lemma 6

1. *The condition* $\mathfrak{a}_0\mathfrak{a}_1^2 \in (I/I^3)[T]$ *is equivalent to* $\mathfrak{a}_1 = \tau(\mathfrak{a}_0)$, $\mathfrak{a}_1 = \tau_2(\mathfrak{a}_0)$, $\mathfrak{a}_0 = \tau_2(\mathfrak{a}_0)$ *and* $\mathfrak{a}_1 = \tau_2(\mathfrak{a}_1)$, *and* $\mathfrak{a}_1 = \tau(\mathfrak{a}_0) = \tau_2(\mathfrak{a}_0)$ *in cases (2), (3), (4), and (5), respectively.*
2. *The ideal* $\mathfrak{a}_0\mathfrak{a}_1$ *of* L *comes from an ideal* $\mathfrak{a}_\alpha$ *of* K_2 *(in other words* $\mathfrak{a}_0\mathfrak{a}_1 = \mathfrak{a}_\alpha\mathbb{Z}_L$*), and in cases (1), (2), and (3) it comes from an ideal of* k*, while in cases (4) and (5),* $\mathfrak{a}_\alpha$ *is an ideal of* K_2 *invariant by* τ_2*.*

Conductors

Definition 7

Let $\overline{\alpha} \in (L^*/{L^*}^3)[T]$ as above, let p be an ideal of k above 3, let $\mathfrak{p}$ be an ideal of K_2 above p, let $\mathfrak{p}_z$ be an ideal of L above $\mathfrak{p}$, and denote by C_k the congruence $x^3/\alpha \equiv 1 \pmod{{}^*\mathfrak{p}_z^k}$ in L. If this congruence is soluble for $k = 3e(\mathfrak{p}_z/3)/2$ we set $A_\alpha(p) = 3e(\mathfrak{p}_z/3)/2 + 1$. Otherwise, if $k < 3e(\mathfrak{p}_z/3)/2$ is the largest exponent for which it has a solution, we set $A_\alpha(p) = k$. In both cases we set

$$a_\alpha(p) = \frac{A_\alpha(p) - 1}{e(\mathfrak{p}_z/p)} .$$

Theorem 8

Let N correspond to α as above, write uniquely $\alpha\mathbb{Z}_L = \mathfrak{a}_0\mathfrak{a}_1^2\mathfrak{q}^3$ with $\mathfrak{a}_0$ and $\mathfrak{a}_1$ integral coprime squarefree ideals, and let $\mathfrak{a}_\alpha$ be the ideal of K_2 such that $\mathfrak{a}_0\mathfrak{a}_1 = \mathfrak{a}_\alpha\mathbb{Z}_L$. Then

$$\mathfrak{f}(N/K_2) = \frac{3\mathfrak{a}_\alpha \prod_{p\mid 3\mathbb{Z}_k}(p\mathbb{Z}_{K_2})^{e(p/3)/2} \prod_{\substack{p\mid 3\mathbb{Z}_k \\ e(\mathfrak{p}/3)\ odd}} (p\mathbb{Z}_{K_2})^{1/2}}{\prod_{\substack{p\mid 3\mathbb{Z}_k \\ p\nmid\mathfrak{a}_\alpha}}(p\mathbb{Z}_{K_2})^{\lceil a_\alpha(p)e(\mathfrak{p}/p)\rceil/e(\mathfrak{p}/p)}} .$$

Definition 9

- If $\mathfrak{a}$ is an ideal of k, we set $\mathcal{N}(\mathfrak{a}) = \mathcal{N}_{k/\mathbb{Q}}(\mathfrak{a})$,
- if $\mathfrak{a}$ is an ideal of K_2, we set $\mathcal{N}(\mathfrak{a}) = \mathcal{N}_{K_2/\mathbb{Q}}(\mathfrak{a})^{1/[K_2:k]}$.

Remark

This notation is consistent, in fact if $\mathfrak{a}$ is an ideal of k we have $\mathcal{N}(\mathfrak{a}) = \mathcal{N}(\mathfrak{a}\mathbb{Z}_{K_2})$.

Definition 10

The fundamental Dirichlet series is defined by

$$\Phi(s)=\frac{1}{2}+\sum_{K\in\mathcal{F}(K_2)}\frac{1}{\mathcal{N}(\mathfrak{f}(K/k))^s}\;.$$

By the fundamental bijection

$$\Phi(s)=\frac{1}{2}\sum_{(\mathfrak{a}_0,\mathfrak{a}_1)\in J}\quad\sum_{\overline{u}\in S_3(L)[T]}\frac{1}{\mathcal{N}(\mathfrak{f}(N/K_2))^s}\;,$$

where J is the set of pairs $(\mathfrak{a}_0,\mathfrak{a}_1)$ of coprime integral squarefree ideals of L such that $\mathfrak{a}_0\mathfrak{a}_1^2\in(I/I^3)[T]$ and $\overline{\mathfrak{a}_0\mathfrak{a}_1^2}\in Cl(L)^3$, and where $\mathfrak{f}(N/K_2)$ is the conductor of the extension N/K_2 corresponding to the triple $(\mathfrak{a}_0,\mathfrak{a}_1,\overline{u})$.

So from the theorem above,

$$\Phi(s) = \frac{1}{2 \cdot 3^{(3/2)[k:\mathbb{Q}]s} \prod_{\substack{p \mid 3\mathbb{Z}_k, \\ e(\mathfrak{p}/3) \text{ odd}}} \mathcal{N}(p)^{s/2}} \sum_{(\mathfrak{a}_0, \mathfrak{a}_1) \in J} \frac{S_{\alpha_0}(s)}{\mathcal{N}(\mathfrak{a}_\alpha)^s},$$

where

$$S_{\alpha_0}(s) = \sum_{\overline{u} \in S_3(L)[T]} \prod_{\substack{p \mid 3\mathbb{Z}_k \\ p \nmid \mathfrak{a}_\alpha}} \mathcal{N}(p)^{\lceil a_{\alpha_0 u}(p) e(\mathfrak{p}/p) \rceil s / e(\mathfrak{p}/p)},$$

and where α_0 is any element of L such that there exists an ideal $\mathfrak{q}_0$ such that $\mathfrak{a}_0 \mathfrak{a}_1^2 \mathfrak{q}_0^3 = \alpha_0 \mathbb{Z}_L$ and $\alpha_0 \in (L^*/{L^*}^3)[T]$.

Definition 11

For $\alpha_0 \in L^*$ and $\mathfrak{b}$ an ideal of K_2 we introduce the function

$$f_{\alpha_0}(\mathfrak{b}) = \left|\{\overline{u} \in S_3(L)[T], x^3/(\alpha_0 u) \equiv 1 \pmod{{}^*\mathfrak{b}\mathbb{Z}_L} \text{ soluble in } L\}\right|$$

with the convention that $f_{\alpha_0}(\mathfrak{b}) = 0$ if $\mathfrak{b}\mathbb{Z}_L \nmid 3\sqrt{-3}$.

There exist a set $\mathcal{B}'$ of ideals $\mathfrak{b} = \prod_{\mathfrak{p}_i | 3\mathbb{Z}_{K_2}} \mathfrak{p}_i^{b_i}$ of K_2 (where $b_i \in \mathbb{Z}$ or sometimes $b_i \in \mathbb{Z}/2$ if $\mathfrak{p}_i$ ramifies in L/K_2) such that

$$\sum_{(\mathfrak{a}_0,\mathfrak{a}_1)\in J} \frac{S_{\alpha_0}(s)}{\mathcal{N}(\mathfrak{a}_\alpha)^s} = \sum_{\mathfrak{b}\in\mathcal{B}'} \lceil\mathcal{N}\rceil(\mathfrak{b})^s P_{\mathfrak{b}}(s) \sum_{(\mathfrak{a}_0,\mathfrak{a}_1)\in J'} \frac{f_{\alpha_0}(\mathfrak{b})}{\mathcal{N}(\mathfrak{a}_\alpha)^s},$$

where J' is "some" subset of J, $P_{\mathfrak{b}}(s)$ is "some" (totally explicit) function with values in $\mathbb{Q}$, and
$\lceil\mathcal{N}\rceil(\mathfrak{b}) = \prod_{\mathfrak{p}_i | 3\mathbb{Z}_{K_2}} \mathcal{N}\left(\mathfrak{p}_i^{\lceil b_i \rceil}\right)$.

Computation of $f_{\alpha_0}(\mathfrak{b})$

Let $\mathfrak{b} \in \mathcal{B}'$, $\mathfrak{b}_z = \mathfrak{b}\mathbb{Z}_L$ and $Cl_{\mathfrak{b}}(L)$ the ray class group.

Definition 12

$S_{\mathfrak{b}}(L)[T] = \{\overline{u} \in S_3(L)[T],\ x^3 \equiv u \pmod{^*\mathfrak{b}_z} \text{ soluble}\}$, where u is any lift of $\overline{u}$ coprime to $\mathfrak{b}_z$, and the congruence is in L.

Lemma 13

Let $\mathfrak{a}_0, \mathfrak{a}_1$ as in condition (1) of Proposition 5. Then

$$f_{\alpha_0}(\mathfrak{b}) = \begin{cases} |S_{\mathfrak{b}}(L)[T]| & \text{if } \overline{\mathfrak{a}_0\mathfrak{a}_1^2} \in Cl_{\mathfrak{b}}(L)^3 \\ 0 & \text{otherwise.} \end{cases}$$

Lemma 14

Set $Z_{\mathfrak{b}} = (\mathbb{Z}_L/\mathfrak{b}_z)^*$. *Then*

$$|S_{\mathfrak{b}}(L)[T]| = \frac{|(U(L)/U(L)^3)[T]||(Cl_{\mathfrak{b}}(L)/Cl_{\mathfrak{b}}(L)^3)[T]|}{|(Z_{\mathfrak{b}}/Z_{\mathfrak{b}}^3)[T]|}.$$

Remark 15

We can compute explicitly $|(U(L)/U(L)^3)[T]|$ *and* $|(Z_{\mathfrak{b}}/Z_{\mathfrak{b}}^3)[T]|$*, but we can't compute* $|(Cl_{\mathfrak{b}}(L)/Cl_{\mathfrak{b}}(L)^3)[T]|$*. Luckily it is not necessary, because this term will disappear in subsequent computations.*

Final form of the Dirichlet series

Theorem 16

We have

$$\Phi(s) = \frac{|(U(L)/U(L)^3)[T]|}{2 \cdot 3^{(3/2)[k:\mathbb{Q}]s} \prod_{\substack{p|3\mathbb{Z}_k, \\ e(\mathfrak{p}/3) \text{ odd}}} \mathcal{N}(p)^{s/2}} \cdot$$

$$\cdot \sum_{\mathfrak{b} \in \mathcal{B}'} \left(\frac{\lceil \mathcal{N} \rceil (\mathfrak{b})}{\mathcal{N}(\mathfrak{r}^e(\mathfrak{b}))} \right)^s \frac{P_{\mathfrak{b}}(s)}{|(Z_{\mathfrak{b}}/Z_{\mathfrak{b}}^3)[T]|} \sum_{\chi \in \widehat{G_{\mathfrak{b}}}} F(\mathfrak{b}, \chi, s) \, .$$

Where

$$G_{\mathfrak{b}} = (Cl_{\mathfrak{b}}(L)/Cl_{\mathfrak{b}}(L)^3)[T], \quad \mathfrak{r}^e(\mathfrak{b}) = \prod_{\substack{\mathfrak{p}|3\mathbb{Z}_{K_2}, \mathfrak{p} \nmid \mathfrak{b} \\ e(\mathfrak{p}/3) \text{ even}}} \mathfrak{p} .$$

Thanks to the theorem, we can now expand $\Phi(s)$ around the pole $s = 1$:

1. In cases (1) and (4) we get

$$\Phi(s) = \frac{C(K_2/k)}{(s-1)^2} + \frac{C(K_2/k)D(K_2/k)}{(s-1)} + O(1),$$

2. while in the other cases we get

$$\Phi(s) = \frac{C(K_2/k)}{(s-1)} + O(1),$$

where the formulas for $C(K_2/k)$ and $D(K_2/k)$ are totally explicit.

Asymptotic formulas

Thanks to a Tauberian theorem we get

1. In cases (1) and (4) :

$$M(K_2/k, X) = C(K_2/k)X(\log(X) + D(K_2/k) - 1) + O(X^{1/2+\varepsilon}).$$

2. In the other cases :

$$M(K_2/k, X) = C(K_2/k)X + O(X^{1/2+\varepsilon}).$$

Examples

Cyclic cubic extensions of $\mathbb{Q}$

In this case we obtain

$$\sum_{K/\mathbb{Q} \text{ cyclic cubic}} \frac{1}{f(K)^s} = -\frac{1}{2}+\frac{1}{2}\left(1+\frac{2}{3^{2s}}\right)\prod_{p\equiv 1 \pmod 3}\left(1+\frac{2}{p^s}\right),$$

and so

$$M(\mathbb{Q},X) = C(\mathbb{Q})X + O(X^{1/2+\varepsilon}),$$

with

$$C(\mathbb{Q}) = \frac{11\sqrt{3}}{36\pi}\prod_{p\equiv 1 \pmod 3}\left(1-\frac{2}{p(p+1)}\right)$$
$$= 0.1585282583961420602835078203575\ldots$$

Pure cubic fields over $\mathbb{Q}$

Case (4) : $K_2 = \mathbb{Q}(\rho)$ and $L = K_2$, so $K/\mathbb{Q}$ is a *pure cubic field* i. e. $K = \mathbb{Q}(\sqrt[3]{m})$. We get

$$\sum_{K/\mathbb{Q} \text{ pure cubic}} \frac{1}{f(K)^s} = -\frac{1}{2} + \frac{1}{6}\left(1 + \frac{2}{3^s} + \frac{6}{3^{2s}}\right) \prod_{p \neq 3} \left(1 + \frac{2}{p^s}\right) + \frac{1}{3} \prod_{p \equiv \pm 1 \pmod 9} \left(1 + \frac{2}{p^s}\right) \prod_{p \not\equiv \pm 1 \pmod 9} \left(1 - \frac{1}{p^s}\right).$$

and so

$$M(\mathbb{Q}(\sqrt{-3}), X) = C \cdot X \cdot (\log(X) + D - 1) + O(X^{1/2+\varepsilon}),$$

where

$$C = C(\mathbb{Q}(\sqrt{-3})) = \frac{7}{30} \prod_p \left(1 - \frac{3}{p^2} + \frac{2}{p^3}\right)$$
$$= 0.066907733301378371291841632984295\dots$$
$$D = D(\mathbb{Q}(\sqrt{-3})) = 2\gamma - \frac{16}{35}\log(3) + 6\sum_p \frac{\log(p)}{p^2+p-2}$$
$$= 3.4502227978305919627907119196711 10\dots,$$

and γ is Euler's constant.

Case (5) : $K_2 = \mathbb{Q}(\sqrt{D})$ **with** $D \neq -3$

There exists a function $\phi_D(s)$ holomorphic for $\mathrm{Re}(s) > 1/2$ such that

$$\sum_{K \in \mathcal{F}(K_2)} \frac{1}{f(K)^s} = \phi_D(s) + \frac{3^{r_2(D)}}{6} L_3(s) \prod_{\left(\frac{-3D}{p}\right)=1} \left(1 + \frac{2}{p^s}\right),$$

where

$$L_3(s) = \begin{cases} 1 + 2/3^{2s} & \text{if } 3 \nmid D, \\ 1 + 2/3^s & \text{if } D \equiv 3 \pmod{9}, \\ 1 + 2/3^s + 6/3^{2s} & \text{if } D \equiv 6 \pmod{9}. \end{cases}$$

$r_2(D) = 1$ for $D < 0$, $r_2(D) = 0$ otherwise.

Set $D' = -3D$ if $3 \nmid D$ and $D' = -D/3$ if $3 \mid D$, and denote as usual by $\chi_{D'}$ the character $\left(\frac{D'}{.}\right)$. Then if $D \neq -3$ is a fundamental discriminant, for all $\varepsilon > 0$ we have

$$M(\mathbb{Q}(\sqrt{D}), X) = C(\mathbb{Q}(\sqrt{D}))X + O(X^{1/2+\varepsilon}),$$

with

$$C(\mathbb{Q}(\sqrt{D})) = \frac{3^{r_2(D)}\ell_3 L(\chi_{D'}, 1)}{\pi^2} \prod_{p \mid D'} \left(1 - \frac{1}{p+1}\right) \cdot \prod_{\left(\frac{D'}{p}\right)=1} \left(1 - \frac{2}{p(p+1)}\right), \quad \text{where}$$

$$\ell_3 = \begin{cases} 11/9 & \text{if } 3 \nmid D, \\ 5/3 & \text{if } D \equiv 3 \pmod 9, \\ 7/5 & \text{if } D \equiv 6 \pmod 9. \end{cases}$$