MATHEMATICS OF COMPUTATION
Volume 84, Number 294, July 2015, Pages 1933–1951
S 0025-5718(2015)02920-2
Article electronically published on January 12, 2015

EXACT COUNTING OF D_ℓ NUMBER FIELDS WITH GIVEN QUADRATIC RESOLVENT

HENRI COHEN

ABSTRACT. We give efficient numerical methods for counting exactly the number of D_ℓ number fields of degree ℓ with given quadratic resolvent, for calculating the constants occurring in their asymptotic expansions, and we give tables for typical cases.

1. Introduction and notation

In a previous paper [8], we have given asymptotic formulas for the number of cubic extensions of a number field with given quadratic resolvent, and even exact formulas in many cases, and in [9] these formulas have been made completely explicit in every case. In a more recent paper [10], we have generalized the results of [8] and [9] to D_ℓ-fields of degree ℓ having a given quadratic resolvent. The aim of the present paper is to solve efficiently the following two problems:

- Compute to high accuracy the constants occuring in the asymptotic expansions given in [10].
- Compute the *exact* number of D_ℓ number fields of degree ℓ and given quadratic resolvent, with absolute discriminant up to large bounds X.

We will give in detail the examples with tables of the first task for $3 \le \ell \le 11$, and for the second task for $3 \le \ell \le 7$.

We summarize the notation and results of [10] that we need. Let ℓ be an odd prime, let $K = \mathbb{Q}(\sqrt{D})$ be a quadratic field of discriminant $D \neq 1$.

We let $\mathcal{F}(K)$ be the set of (isomorphism classes of) D_ℓ number fields L of degree ℓ with quadratic resolvent isomorphic to K. We have $\mathrm{Disc}(L) = D^{(\ell-1)/2} f(L)^{\ell-1}$ for some positive integer $f(L)$ which by abuse of language we call the *conductor* of L, and we denote by $M_\ell(D;X)$ the number of such fields L with $f(L) \le X$.

A special case of the main result proved in [10] is as follows:

Theorem 1.1. *Set*

$$\Phi_{\ell,K}(s) = \frac{1}{\ell-1} + \sum_{L\in\mathcal{F}(K)} \frac{1}{f(L)^s} \ .$$

(1) *Set $r_2(D) = 0$ if $D > 0$ and $r_2(D) = 1$ if $D < 0$. We have*

$$\Phi_{\ell,K}(s) = \phi_{\ell,K}(s) + \frac{1}{(\ell-1)\ell^{1-r_2(D)}} L_\ell(s) \prod_{p\equiv\left(\frac{D}{p}\right)\equiv\pm1 \pmod{\ell}} \left(1+\frac{\ell-1}{p^s}\right) ,$$

Received by the editor August 20, 2013 and, in revised form, November 17, 2013.
2010 *Mathematics Subject Classification.* Primary 11R16, 11R20, 11R29.

with

$$L_\ell(s)=\begin{cases}1+(\ell-1)/\ell^{2s} & \text{if } \ell\nmid D\ ,\\ 1+(\ell-1)/\ell^{s} & \text{if } \ell\mid D \text{ and } \ell\ge 5\ ,\\ 1+(\ell-1)/\ell^{s} & \text{if } \ell=3 \text{ and } D\equiv 3 \pmod 9\ ,\\ 1+(\ell-1)/\ell^{s}+\ell(\ell-1)/\ell^{2s} & \text{if } \ell=3 \text{ and } D\equiv 6 \pmod 9\ ,\end{cases}$$

and where $\phi_{\ell,K}(s)$ can be extended to a holomorphic function in $\mathrm{Re}(s)>1/2$.

(2) *If $D<0$ and $\ell\nmid h(D)$ we have $\phi_{\ell,K}(s)=0$. In particular this is the case when $\ell\equiv 3 \pmod 4$ and $D=(-1)^{(\ell-1)/2}\ell=\ell^*$ (see below).*

(3) *Write*

$$\Phi_{\ell,K}(s)=\frac{1}{\ell-1}+\sum_{n\ge 1}\frac{a(n)}{n^s}$$

and $M_\ell(D;X)=\sum_{1\le n\le X}a(n)$, which counts the number of L such that $f(L)\le X$, and set $\ell^*=(-1)^{(\ell-1)/2}\ell$. In addition, set

$$c_1=1/((\ell-1)\ell^{1-r_2(D)})\ ,$$

$$c_2=\begin{cases}(\ell^2+\ell-1)/\ell^2 & \text{if } \ell\nmid D\ ,\\ 2-1/\ell & \text{if } \ell\mid D \text{ and } \ell\ge 5\ ,\\ 5/3 & \text{if } \ell=3 \text{ and } D\equiv 3 \pmod 9\ ,\\ 7/5 & \text{if } \ell=3 \text{ and } D\equiv 6 \pmod 9\ .\end{cases}$$

(a) *If $D\neq\ell^*$, there exists a constant $C_\ell(D)>0$ such that $M_\ell(D;X)=C_\ell(D)X+O(X^{1-2/(\ell+3)+\varepsilon})$ for all $\varepsilon>0$, and we have $C_\ell(D)=c_1c_2c_3$ with*

$$c_3=\mathrm{Res}_{s=1}\prod_{e(p)=f(p)=1}(1+(\ell-1)/p^s)\ ,$$

where $e(p)$ and $f(p)$ are the ramification and residual index of a prime number p in the extension $K'/\mathbb{Q}$, where $K'=\mathbb{Q}(\sqrt{D}(\zeta_\ell-\zeta_\ell^{-1}))$.

(b) *If $\ell\equiv 1 \pmod 4$ and $D=\ell^*=\ell$, there exists a constant $C_\ell(D)>0$ such that $M_\ell(D;X)=C_\ell(D)X+O(X^{1-2/(\ell+3)+\varepsilon})$ for all $\varepsilon>0$, and we have $C_\ell(D)=c_1c_2c_3$ with*

$$c_3=\mathrm{Res}_{s=1}\prod_{p\equiv 1 \pmod\ell}(1+(\ell-1)/p^s)\ .$$

(c) *If $\ell\equiv 3 \pmod 4$ and $D=\ell^*=-\ell$, there exist constants $C_\ell(D)>0$ and $C'_\ell(D)$ such that $M_\ell(D;X)=C_\ell(D)(X\log(X)+C'_\ell(D)X)+O(X^{1-2/(\ell+3)+\varepsilon})$ for all $\varepsilon>0$, and we have $C_\ell(D)=c_1c_2c_3$ with*

$$c_3=\lim_{s\to 1}(s-1)^2\prod_{p\equiv\pm 1 \pmod\ell}(1+(\ell-1)/p^s)\ ,$$

and the constant $C'(D)$ can also be given explicitly if desired.

Note that when $\ell=3$ and $D\equiv 6 \pmod 9$ we include $p=\ell$ in the product for c_3, and compensate by setting $c_2=(7/3)/(1+2/3)=7/5$. In all other cases we have $e(\ell)>1$ so $p=\ell$ does not occur in the product for c_3.

Our goal is to compute for reasonably small D (say $|D| \leq 100$) and small ℓ (say $3 \leq \ell \leq 11$) the constants $C_\ell(D)$ to high accuracy (say 60 decimal digits) and the quantities $M_\ell(D; X)$ for rather large X (say $X \leq 10^{12}$, the upper bound here depending on ℓ). Although there are some similarities between the two problems, we consider them independently.

2. Computation of $C_\ell(D)$ in the general case

In [10], we have (easily) expressed c_3 as a product of four other constants, two of them being slowly convergent Euler products. However, the formula given above is the one we will use to compute c_3. As can be seen, the case $D = \ell^*$ leads to slightly different formulas, so we will first assume that $D \neq \ell^*$, which we will call the "general case".

2.1. **Splitting of primes in subfields of K'.** Recall that we have set $K' = \mathbb{Q}(\sqrt{D}(\zeta_\ell - \zeta_\ell^{-1}))$. It is immediate to see that the extension $K'/\mathbb{Q}$ is cyclic of degree $\ell - 1$, so for any $d \mid (\ell - 1)$ there exists a unique subfield K'_d such that $[K' : K'_d] = d$, or equivalently of degree $(\ell - 1)/d$.

For a prime p, denote by $\mathfrak{p}_d$ a prime ideal of K'_d above p, by $e(\mathfrak{p}_d)$, $f(\mathfrak{p}_d)$, and $g(\mathfrak{p}_d)$ the usual quantities linked to the splitting of primes in $K'_d/\mathbb{Q}$, abbreviate these quantities to $e(p)$, $f(p)$, and $g(p)$ when $d = 1$ (this being compatible with our previous notation). We first note the following lemma, which is Proposition 1.3 of [6], but which we prove again here in the form that we need:

Lemma 2.1. *Let $K'/\mathbb{Q}$ be a cyclic extension of degree n, and let K'_d, $\mathfrak{p}_d$, etc., be defined as above. Assume that p is unramified in $K'/\mathbb{Q}$, i.e., that $e(p) = 1$. We have $f(\mathfrak{p}_d) = f(p)/(f(p), d)$, where (u, v) is as usual an abbreviation for* $\gcd(u, v)$.

Proof. Let ρ be the canonical surjection from $\mathrm{Gal}(K'/\mathbb{Q})$ to $\mathrm{Gal}(K'_d/\mathbb{Q})$, and for simplicity write f instead of $f(p)$. We know that $D(\mathfrak{p}_d/p) = \rho(D(\mathfrak{p}_1/p))$ and denote by σ a generator of the cyclic group $\mathrm{Gal}(K'/\mathbb{Q})$. Since p is unramified in $K'/\mathbb{Q}$ we have

$$f(\mathfrak{p}_d) = |D(\mathfrak{p}_d/p)| = \frac{|D(\mathfrak{p}_1/p)|}{|\ker(\rho) \cap D(\mathfrak{p}_1/p)|} = \frac{f}{|\langle \sigma^{n/d} \rangle \cap \langle \sigma^{n/f} \rangle|} \ .$$

Now for a and b dividing n we evidently have

$$|\langle \sigma^a \rangle \cap \langle \sigma^b \rangle| = |\langle \sigma^{ab/(a,b)} \rangle| = m(a, b)/ab \ ,$$

so for $a = n/d$ and $b = n/f$, this is equal to

$$\frac{n(n/d, n/f)}{n^2/df} = (d, f) \ ,$$

proving the lemma. ∎

2.2. **Isolating the condition $e(p) = f(p) = 1$.** The following is essentially Theorem 2.16 of [5], which we also prove again in our context.

Proposition 2.2. *Keep the notation of Lemma* 2.1*, in particular, $K'/\mathbb{Q}$ is cyclic of degree n. Set*

$$Z(s) = \prod_{d \mid n} \zeta_{K'_d}(ds)^{\mu(d)} \ .$$

Then $Z(s)=Z_R(s)L(s)$, *with*

$$Z_R(s)=\prod_{e(p)>1}\prod_{d\mid n}(1-1/p^{f(\mathfrak{p}_d)ds})^{-\mu(d)g(\mathfrak{p}_d)}\ ,$$
$$L(s)=\prod_{e(p)=f(p)=1}\prod_{d\mid n}(1-1/p^{ds})^{-\mu(d)n/d}\ .$$

Note that we will apply this proposition with $n=\ell-1$ in the general case and also in the special case when $\ell\equiv 1 \pmod 4$, and with $n=(\ell-1)/2$ in the special case when $\ell\equiv 3 \pmod 4$.

Proof. Both sides being Euler products, we prove the result for each Euler factor at p. The Euler factor at p of $\zeta_{K'_d}(s)$ is by definition equal to $(1-1/p^{f(\mathfrak{p}_d)s})^{-g(\mathfrak{p}_d)}$. It follows that the result is immediate when $e(p)>1$, and also when $e(p)=f(p)=1$, since for $d\mid n$ we have $e(\mathfrak{p}_d)=f(\mathfrak{p}_d)=1$, hence $g(\mathfrak{p}_d)=n/d$.

Thus assume that $e(p)=1$ and $f(p)>1$. If we denote by $Z_p(s)$ the Euler factor at p of $Z(s)$ we must show that $Z_p(s)=1$. Since $e(p)=1$ we have $g(\mathfrak{p}_d)=((\ell-1)/d)/f(\mathfrak{p}_d)$, so

$$Z_p(s)=\prod_{d\mid n}(1-q^{df(\mathfrak{p}_d)})^{-\mu(d)(n/d)/f(\mathfrak{p}_d)}\ ,$$

where for simplicity we set $q=1/p^s$. Using the above lemma and setting for simplicity $f=f(p)$, we thus have

$$Z_p(s)=\prod_{d\mid n}(1-q^{df/(d,f)})^{-\mu(d)n(d,f)/(df)}\ .$$

By definition of the cyclotomic polynomials Φ_m we have

$$q^{df/(d,f)}-1=\prod_{m\mid df/(d,f)}\Phi_m(q)\ ,$$

so that

$$Z_p(s)=\pm\prod_{d\mid n}\prod_{m\mid df/(d,f)}\Phi_m(q)^{-\mu(d)n(d,f)/(df)}=\pm\prod_{m\mid n}\Phi_m(q)^{h(m)}\ ,$$

with

$$h(m)=-n\sum_{d\mid n,\ m\mid df/(d,f)}\mu(d)(d,f)/(df)\ .$$

Setting $d_1=df/(d,f)$, which is equal to the LCM of d and f, hence divides n, we have

$$h(m)=-n\sum_{\substack{f\mid d_1\mid n\\ m\mid d_1}}(1/d_1)\sum_{\substack{d\mid d_1\\ \mathrm{lcm}(d,f)=d_1}}\mu(d)=-n\sum_{m_1\mid d_1\mid n}(1/d_1)I(d_1,f)\ ,$$

where we set $m_1=\mathrm{lcm}(f,m)$ and

$$I(d_1,f)=\sum_{\substack{d\mid d_1\\ \mathrm{lcm}(d,f)=d_1}}\mu(d)\ .$$

Set $d'=d_1/d$ and $f'=d_1/f$. We have

$$(d',f')=(d_1f,d_1d)/(df)=d_1(d,f)/(df)\ ,$$

so the condition $\mathrm{lcm}(d,f)=d_1$ is equivalent to $d'\mid d_1$ and $(d',f')=1$. Thus,

$$\begin{aligned}I(d_1,f)&=\sum_{\substack{d'\mid d_1\\(d',f')=1}}\mu(d_1/d')=\sum_{d'\mid d_1}\mu(d_1/d')\sum_{e\mid(d',f')}\mu(e)\\&=\sum_{e\mid f'}\mu(e)\sum_{e\mid d'\mid d_1}\mu(d_1/d')=\sum_{e\mid f'}\mu(e)\sum_{d''\mid(d_1/e)}\mu((d_1/e)/d'')\end{aligned}$$

since $f'\mid d_1$. The inner sum vanishes unless $d_1/e=1$, so that $I(d_1,f)=\mu(d_1)$ if $d_1\mid f'$ and $I(d_1,f)=0$ otherwise. However, since $f'=d_1/f$, we have $d_1\mid f'$ if and only if $f=1$. We deduce that $I(d_1,f)=0$ for all d_1 when $f>1$, and otherwise $I(d_1,f)=\mu(d_1)$. Thus $h(m)=0$ if $f>1$, so that $Z_p(s)=\pm1$, and of course since the constant term in $q=p^{-s}$ of $Z_p(s)$ is equal to 1 we have $Z_p(s)=1$, proving the result. □

2.3. **The folklore trick.** See for instance Section 10.3.6 of [4] or [3]. This "trick" is completely general, but we apply it to our case:

Proposition 2.3. *Set*

$$a(k)=\frac{1}{k}\sum_{\substack{n\mid k\\(k/n,\ell-1)=1}}(-1)^{n-1}\mu(k/n)(\ell-1)^{n-1}\;.$$

With a slight abuse of notation, we have

$$c_3(s):=\prod_{e(p)=f(p)=1}(1+(\ell-1)/p^s)=\prod_{k\geq1}L(ks)^{a(k)}\;.$$

In particular

$$c_3=\mathrm{Res}_{s=1}L(s)\prod_{k\geq2}L(k)^{a(k)}\;.$$

Proof. I claim that there exist unique exponents $a(k)$ such that

$$c_3(s)=\prod_{k\geq1}L(ks)^{a(k)}\;,$$

and that they are given by the formula of the proposition. Indeed, setting $q=p^{-s}$ and taking logarithms of the Euler factors at p, this is equivalent to the equality

$$\sum_{n\geq1}(-1)^{n-1}\frac{(\ell-1)^n}{n}q^n=\sum_{k\geq1}a(k)\sum_{d\mid(\ell-1)}\mu(d)\frac{(\ell-1)}{d}\sum_{m\geq1}\frac{1}{m}q^{kdm}\;,$$

hence setting $n=kdm$ this gives the identities

$$\begin{aligned}(-1)^{n-1}(\ell-1)^{n-1}&=\sum_{kdm=n,\ d\mid(\ell-1)}ka(k)\mu(d)=\sum_{k\mid n}ka(k)\sum_{d\mid(n/k,\ell-1)}\mu(d)\\&=\sum_{k\mid n,\ (n/k,\ell-1)=1}ka(k)=\sum_{k\mid n}ka(k)\delta(n/k)\;,\end{aligned}$$

where $\delta(n)=1$ if $(n,\ell-1)=1$ and $\delta(n)=0$ otherwise. Now $\sum_{n\ge1}\delta(n)/n^s=\sum_{(n,\ell-1)=1}1/n^s$, which implies that $\left(\sum_{n\ge1}\delta(n)/n^s\right)^{-1}=\sum_{(n,\ell-1)=1}\mu(n)/n^s$, so

$$ka(k)=\sum_{\substack{n\mid k\\(k/n,\ell-1)=1}}(-1)^{n-1}\mu(k/n)(\ell-1)^{n-1}\ ,$$

proving the proposition. □

For any Euler product $P(s)$, write $P_{>B}(s)$ (resp., $P_{\le B}(s)$) for the Euler product limited to primes $p>B$ (resp., $p\le B$). In practice, we will use the proposition through the following corollary, whose immediate proof is left to the reader:

Corollary 2.4. *For all $B\ge1$ we have*

$$\begin{aligned}
c_3&=\prod_{\substack{e(p)=f(p)=1\\p\le B}}(1+(\ell-1)/p)\operatorname{Res}_{s=1}L_{>B}(s)\prod_{k\ge2}L_{>B}(k)^{a(k)}\ ,\\
L_{>B}(k)&=\prod_{e(p)=f(p)=1,\ p\le B}\ \prod_{d\mid(\ell-1)}(1-1/p^{dk})^{\mu(d)(\ell-1)/d}Z(k)/Z_R(k)\ ,\\
\operatorname{Res}_{s=1}L_{>B}(s)&=\prod_{e(p)=f(p)=1,\ p\le B}\ \prod_{d\mid(\ell-1)}(1-1/p^{d})^{\mu(d)(\ell-1)/d}\operatorname{Res}_{s=1}Z(s)/Z_R(1)\ ,\\
\operatorname{Res}_{s=1}Z(s)&=\operatorname{Res}_{s=1}\zeta_{K'}(s)\prod_{\substack{d\mid(\ell-1)\\d>1}}\zeta_{K'_d}(d)^{\mu(d)}\ .
\end{aligned}$$

2.4. **Implementation.** We will see below how to compute $\zeta_{K'_d}(k)$. The main problem in the use of the above corollary is the computation of $L_{>B}(k)^{a(k)}$: if k is not small, say $k=100$, then $L_{>B}(k)$ is extremely close to 1, and $a(k)$ is large, so we will have quite a loss of accuracy. Let us quantify this: since primes such that $e(p)=f(p)=1$ are common, we will have very roughly $L_{>B}(k)\approx(1-1/B^k)^{-(\ell-1)}$. On the other hand, $a(k)$ will be of the order of $(\ell-1)^{k-1}/k\approx(\ell-1)^{(k-1)}$. Thus, $|L_{>B}(k)^{a(k)}-1|\le e^{-D}$ is essentially equivalent to $a(k)\log(L_{>B}(k))<e^{-D}$, hence to $(\ell-1)^k/B^k<e^{-D}$; in other words $k>D/\log(B/(\ell-1))$ (which of course implies that we must take B considerably larger than $\ell-1$). This gives roughly the value of k that we will need, but is not the whole story: given this value of k, we must compute $L_{>B}(k)^{a(k)}$ to accuracy (absolute or relative, here it is the same since this quantity is close to 1) less than e^{-D}. Thus, it is necessary to perform the computation of $L_{>B}(k)$ to precision less than $e^{-D}/a(k)=e^{-D'}$, with

$$D'\approx D+k\log(\ell-1)=D+D\log(\ell-1)/\log(B/\ell-1)=D\log(B)/\log(B/(\ell-1))\ .$$

For instance, if we choose $B=(\ell-1)^2$, we simply have $D'=2D$.

2.5. **Computation of $\zeta_{K'_d}(k)$.** To compute c_3, it remains to compute $\operatorname{Res}_{s=1}\zeta_{K'}(s)$ and $\zeta_{K'_d}(k)$ for $k\ge2$. For the first quantity, we can use Dirichlet's class number formula, and for the others the preprogrammed functions `zetakinit` and `zetak` of `Pari/GP`. However, as mentioned in the manual, these functions are very inefficient especially when the degree $\ell-1$ is not tiny, so it is highly preferable instead to use Dirichlet characters.

Indeed, if we denote by ω a generator of the group of characters modulo ℓ and by χ_D the quadratic character $\left(\frac{D}{\cdot}\right)$, we have

$$\zeta_{K'_d}(s) = \prod_{0\le j<(\ell-1)/d} L((\omega\chi_D)^{dj}, s)\ ,$$

where we recall that the product of characters is taken in the group of characters, meaning, in particular, that when dj is even we have $(\omega\chi_D)^{dj} = \omega^{dj}$. In particular, we have

$$\mathrm{Res}_{s=1}\,\zeta_{K'}(s) = \prod_{1\le j<\ell-1} L((\omega\chi_D)^{j}, 1)\ .$$

The quantities $L((\omega\chi_D)^{dj}, s)$ can in turn be computed using the approximate functional equation, which here involves the incomplete gamma function. We omit the details, which are classical, but simply note that for a given value of s the quantities $L((\omega\chi_D)^{dj}, s)$ for $1 \le j < (\ell-1)/d$ can be computed simultaneously for essentially the same cost as a single value, since the incomplete gamma function arguments will be the same.

3. Computation of $C_\ell(D)$ in the special case

We now assume that we are in the "special case", i.e., that $D = \ell^* = (-1)^{(\ell-1)/2}\ell$. In view of Theorem 1.1, we will need to distinguish $\ell \equiv 1 \pmod 4$ and $\ell \equiv 3 \pmod 4$. In fact, nothing much needs to be changed compared to the general case.

Assume first that $\ell \equiv 1 \pmod 4$. The condition $p \equiv 1 \pmod \ell$ is equivalent to p splitting completely in the cyclotomic field $\mathbb{Q}_z = \mathbb{Q}(\zeta_\ell)$, which is again cyclic of order $\ell - 1$. If in this case we set $K' = \mathbb{Q}(\zeta_\ell)$, then Lemma 2.1, Proposition 2.2, Proposition 2.3, and Corollary 2.4 are valid as such (with again $n = [K' : \mathbb{Q}] = \ell-1$), and the only change is that the formula for $\zeta_{K'_d}(s)$ is replaced by

$$\zeta_{K'_d}(s) = \prod_{0\le j<(\ell-1)/d} L(\omega^{dj}, s)\ .$$

Assume now that $\ell \equiv 3 \pmod 4$. The condition $p \equiv \pm 1 \pmod \ell$ is equivalent to p splitting completely in the totally real subfield $\mathbb{Q}_z^+ = \mathbb{Q}(\zeta_\ell + \zeta_\ell^{-1})$ of $\mathbb{Q}_z = \mathbb{Q}(\zeta_\ell)$ which is now cyclic of order $(\ell-1)/2$. Thus we set $K' = \mathbb{Q}_z^+$. Here the results change slightly. Lemma 2.1 and Proposition 2.2 are now used with $n = (\ell-1)/2$, and the formula for $\zeta_{K'_d}(s)$ is now

$$\zeta_{K'_d}(s) = \prod_{0\le j<(\ell-1)/(2d)} L(\omega^{2dj}, s)\ .$$

However, we must now change Proposition 2.3 (hence also Corollary 2.4). The new formulas are as follows:

Proposition 3.1. *Keep the above notation, in particular $K' = \mathbb{Q}_z^+$, and set*

$$a(k) = \frac{2}{k} \sum_{\substack{n\mid k \\ (k/n,(\ell-1)/2)=1}} (-1)^{n-1}\mu(k/n)(\ell-1)^{n-1}\ .$$

We have

$$c_3(s) := \prod_{e(p)=f(p)=1} (1 + (\ell - 1)/p^s) = \prod_{k \geq 1} L(ks)^{a(k)}\ .$$

In particular,

$$c_3 = (\mathrm{Res}_{s=1} L(s))^2 \prod_{k \geq 2} L(k)^{a(k)}\ .$$

Proof. The proof is identical to the one in the general case, except that we must now use the formula of Proposition 2.2 with $n = (\ell - 1)/2$, which implies that the GCD of k/n is now taken with respect to $(\ell - 1)/2$, and we must replace the factor $1/k$ by $2/k$ in the formula for $a(k)$. In particular note that $a(1) = 2$. $\square$

4. Tables of $C_\ell(D)$

Using the methods explained above, we have computed to 80 decimal digits a number of values of $C_\ell(D)$ for $\ell = 3$, 5, 7, and 11. The `Pari/GP` programs used to compute them as well as extensive tables are available from the author. Here is a short sample:

$$\begin{aligned}
C_3(-4) &= 0.1362190676241212841449867354342013681519368439930712\cdots \\
C_3(-15) &= 0.1763719187254720659991236662528459282731234960996698\cdots \\
C_3(5) &= 0.0818840074459636358232037502298557955922438940548390\cdots \\
C_3(12) &= 0.0803828977056554045622405320212726495945956846819225\cdots
\end{aligned}$$

$$\begin{aligned}
C_5(-3) &= 0.0507853244497800993782016760188293630841512728322622\cdots \\
C_5(-15) &= 0.0788048138013829128282439800292179771995450785328207\cdots \\
C_5(8) &= 0.0134747747475919140437863334316374195138193286084845\cdots \\
C_5(40) &= 0.0209091332290219355851856898077132371766161995648898\cdots
\end{aligned}$$

$$\begin{aligned}
C_7(-3) &= 0.0296332163247300745247219282260715878558066725943508\cdots \\
C_7(-56) &= 0.0476482546822832432485663400482260513425675409153078\cdots \\
C_7(5) &= 0.0064676733264714100259068107168272139045182602157945\cdots \\
C_7(21) &= 0.0092561380479824845096549623915860255741312857684523\cdots
\end{aligned}$$

$$\begin{aligned}
C_{11}(-3) &= 0.0147492212096080611979142320145680269303157592953914\cdots \\
C_{11}(-55) &= 0.0262064374769044759545849551388248215923277698284101\cdots \\
C_{11}(5) &= 0.0015062181029612487738633338522967418184629721573614\cdots \\
C_{11}(33) &= 0.0030220320861762508020132258509009135197011333981156\cdots
\end{aligned}$$

We also give the constants $C_\ell(D) = C_\ell(\ell^*)$ in the special case, as well as the constants $C'_\ell(-\ell)$ when $\ell \equiv 3 \pmod 4$:

$$
\begin{aligned}
C_3(-3) &= 0.066907733301378371291841632984295637501344096955 9\cdots\\
C'_3(-3) &= 2.450222797830591962790711919671110418268850425298 0\cdots\\
C_5(5) &= 0.020378187055903714655893604338351682058377927048 1\cdots\\
C_7(-7) &= 0.012105263421451229801857880331290147832963231442 8\cdots\\
C'_7(-7) &= 4.589110939732976665087912619030795401506560583619 8\cdots\\
C_{11}(-11) &= 0.005935464188743864527830659018560284360416869029 2\cdots\\
C'_{11}(-11) &= 4.940758664573022462245757323617522646548920262317 8\cdots
\end{aligned}
$$

5. Computation of $M_\ell(D;X)$

5.1. **Reduction to $\zeta_{K'}(s)$.** Recall from Theorem 1.1 that if $\phi_{\ell,K}(s)$ is identically zero, we have

$$\Phi_{\ell,K}(s) = \frac{1}{\ell-1} L_\ell(s) \prod_{e(p)=f(p)=1,\ p\neq\ell} (1+(\ell-1)/p^s)\ ,$$

where $L_\ell(s)$ is a polynomial of degree less than or equal to 2 in $1/\ell^s$ given in Theorem 1.1, so that if we write $\Phi_{\ell,K}(s) = 1/(\ell-1) + \sum_{n\ge1} a(n)/n^s$, we have $M_\ell(D;X) = \sum_{1\le n\le X} a(n)$. Note that the condition $e(p)=f(p)=1$, $p\neq\ell$, is equivalent to $p \equiv \left(\frac{D}{p}\right) \equiv \pm1 \pmod{\ell}$ so it is immediate to test without doing any work in the field K'.

Now we write

$$\mathcal{A}_1(s) := \prod_{e(p)=f(p)=1,\ p\neq\ell} (1+(\ell-1)/p^s) = \sum_{\substack{n\ge1\\ n \text{ squarefree}}} a_1(n)/n^s\ ,$$

with $a_1(n) = (\ell-1)^{\omega_1(n)}$, where $\omega_1(n)$ is the number of distinct prime divisors p of n such that $e(p)=f(p)=1$ and $p\neq\ell$, and set $A_1(X) = \sum_{1\le n\le X} a_1(n)$; we have

$$
\begin{aligned}
&(\ell-1)M_\ell(D;X)+1\\
&\quad= \begin{cases} A_1(X) + (\ell-1)A_1(X/\ell^2) & \text{if } \ell \nmid D\ ,\\ A_1(X) + (\ell-1)A_1(X/\ell) & \text{if } \ell \mid D \text{ and } \ell \ge 5\ ,\\ A_1(X) + (\ell-1)A_1(X/\ell) & \text{if } \ell = 3 \text{ and } D \equiv 3 \pmod 9\ ,\\ A_1(X) + (\ell-1)A_1(X/\ell) + 2\ell A_1(X/\ell^2) & \text{if } \ell = 3 \text{ and } D \equiv 6 \pmod 9\ . \end{cases}
\end{aligned}
$$

We are thus evidently reduced to the computation of $A_1(X)$. A straightforward method to do this is to use the explicit formula for $a_1(n)$: since $\omega_1(n)$ can be computed in $O(n^\varepsilon)$ time for any $\varepsilon > 0$, this gives a $O(X^{1+\varepsilon})$ method for computing $A_1(X)$, hence $M_\ell(D;X)$.

By using once again the Dedekind zeta function of the field K' it is, however, possible to improve this to a $O(X^{1-1/(\ell-1)+\varepsilon})$ method. In particular, this is $O(X^{1/2+\varepsilon})$ for $\ell = 3$ and $O(X^{3/4+\varepsilon})$ for $\ell = 5$.

We will assume from now on that we are in the general case, the modifications that are needed for the special case being immediate and mentioned at the end.

Write $\zeta_{K'}(s) = P_R P_F P_1$, where

$$P_R(s) = \prod_{e(p)>1 \text{ or } p=\ell} (1 - 1/p^{f(p)s})^{-(\ell-1)/(e(p)f(p))} \ ,$$

$$P_F(s) = \prod_{e(p)=1,\ f(p)>1,\ p\neq\ell} (1 - 1/p^{f(p)s})^{-(\ell-1)/f(p)} \ ,$$

$$P_1(s) = \prod_{e(p)=f(p)=1,\ p\neq\ell} (1 - 1/p^{s})^{-(\ell-1)} \ .$$

Thus $\mathcal{A}_1(s) = Q_1(s)P_1(s)$ with

$$Q_1(s) = \prod_{e(p)=f(p)=1,\ p\neq\ell} ((1 + (\ell-1)/p^s)(1 - 1/p^s)^{\ell-1}) \ ,$$

hence $\mathcal{A}_1(s) = P_R(s)^{-1}\mathcal{A}_2(s)$, with

$$\mathcal{A}_2(s) = Q_1(s)P_F(s)^{-1}\zeta_{K'}(s) \ .$$

Set

$$\mathcal{A}_2(s) = \sum_{n\geq 1} a_2(n)/n^s \quad \text{and} \quad A_2(X) = \sum_{1\leq n\leq X} a_2(n).$$

Since $P_R(s)^{-1}$ is a Dirichlet polynomial of reasonably small degree d, if we write $P_R(s)^{-1} = \sum_{1\leq n\leq d} r(n)/n^s$ we have $A_1(X) = \sum_{1\leq n\leq d} r(n)A_2(X/n)$.

Now note that $Q_1(s)$ and $P_F(s)^{-1}$ are Euler products of power series in $1/p^s$ of the form $1 + O(1/p^{2s})$. Thus, we can set

$$Q_1(s)P_F(s)^{-1} = \sum_{n\geq 1} c(n)/n^s \ ,$$

and the n such that $c(n) \neq 0$ are *powerful* numbers, i.e., such that if a prime p divides n, then $p^2 \mid n$ also. Hence if we set $\zeta_{K'}(s) = \sum_{n\geq 1} a_3(n)/n^s$ and $A_3(X) = \sum_{1\leq n\leq X} a_3(n)$, we have

$$A_2(X) = \sum_{1\leq n\leq X,\ c(n)\neq 0} c(n)A_3(X/n) \ .$$

The point of this formula is that the number of powerful $n \leq X$ is asymptotic to $c_p \cdot X^{1/2}$ (with $c_p = \zeta(2)\zeta(3)/\zeta(6)$), so that the above sum involves only $O(X^{1/2})$ terms. More precisely, if $A_3(X)$ can be computed in time $O(X^{\alpha+\varepsilon})$ for all $\varepsilon > 0$ with $\alpha \geq 1/2$, then $A_2(X)$ can be computed in time $O(X^{\alpha+\varepsilon}S)$, with $S = \sum_{n \text{ powerful}} 1/n^{\alpha+\varepsilon}$, which is a convergent series for $\alpha \geq 1/2$.

Remarks 5.1. (1) The same reasoning shows that if $\alpha < 1/2$ the computation time is $O(X^{1/2+\varepsilon})$, so there is no real improvement compared to the case $\alpha = 1/2$. This is because we use Euler products in $1 + O(1/p^{2s})$, and not $1 + O(1/p^{ms})$ for some $m \geq 3$. Using these more rapidly convergent Euler products would considerably complicate the combinatorics and not gain any time in practice.

(2) The formula given above for $A_2(X)$ must of course not be used as written, since it would involve factoring all $n \leq X$, and even if factoring could be done in time $O(1)$, this would take time $O(X)$. Instead, note that the Euler factors of $Q_1(s)$ and of P_F^{-1} have degree less than or equal to ℓ ($\ell - 1$ for

P_F^{-1}), so any n with $c(n) \neq 0$ can be written $n = \prod_{2\leq k\leq \ell} x_k^k$ for some integers x_k, and the summation over $n \leq X$ is written as

$$\sum_{x_\ell \leq X^{1/\ell}} \sum_{x_{\ell-1}\leq (X/x_\ell^\ell)^{1/(\ell-1)}} \cdots .$$

The number of terms in this multiple sum is less than or equal to the number of powerfull numbers up to X, hence $O(X^{1/2})$.

Thus the computation time of $A_2(X)$ is of the same order of magnitude as that of $A_3(X)$ (for $\alpha \geq 1/2$, which is what we will have in practice), so we are reduced to studying the summatory function of the Dirichlet series coefficients of $\zeta_{K'}(s)$. In actual practice, the computation of this latter function takes more than 99% of the time.

5.2. **Summatory function of $\zeta_{K'}(s)$.** Recall from Section 2.5 that in the general case we have

$$\zeta_{K'}(s) = \prod_{0\leq j<\ell-1} L((\omega\chi_D)^j, s) = \sum_{n\geq 1} a_3(n)/n^s ,$$

and we want to compute $A_3(X) = \sum_{1\leq n\leq X} a_3(n)$ (in the special case the formulas are slightly different (see above), but the method will be identical).

For this, we will make use of the method of the hyperbola in the following form:

Proposition 5.2. *Assume that c is the arithmetic convolution of a and b, and denote by $A(X)$, $B(X)$, and $C(X)$ the summatory functions of a, b, and c, respectively. For any $E \in \mathbb{R}$ such that $1 \leq E \leq X$ we have*

$$C(X) = \sum_{1\leq n\leq E} a(n)B(X/n) + \sum_{1\leq n\leq X/E} b(n)A(X/n) - A(E)B(X/E) .$$

Corollary 5.3. *Assume that the functions $a(n)$ and $b(n)$ can be computed in time $O(n^\varepsilon)$, and that $A(X)$ and $B(X)$ can be computed in time $O(X^{\alpha+\varepsilon})$ and $O(X^{\beta+\varepsilon})$ respectively, with $\alpha < 1$ and $\beta < 1$. Then, using the proposition, $C(X)$ can be computed in time $O(X^{\gamma+\varepsilon})$ with $\gamma = (1-\alpha\beta)/(2-\alpha-\beta)$ by choosing $E = X^{(1-\beta)/(2-\alpha-\beta)}$.*

Proof. Immediate and left to the reader. $\square$

Now note that for $j \not\equiv 0 \pmod{\ell - 1}$ the functions $(\omega\chi_D)^j$ as well as their summatory functions are periodic of period dividing $(\ell-1)|D|$, and since we assume ℓ and D small they can be tabulated once and for all. Although not periodic, for $j = 0$ the function 1 and its summatory function $\lfloor X\rfloor$ also take negligible time to compute. Thus, splitting the product of L-functions by pairs, we have to compute the product of $(\ell-1)/2$ Dirichlet series, whose coefficients take negligible time to compute, and summatory functions taking time $O(X^{1/2+\varepsilon})$. Continuing by taking products by pairs, it is easy to see that the global time will be $O(X^{1-1/(\ell-1)+\varepsilon})$.

5.3. **The Case $\ell = 3$.** We summarize the reductions made above in this case:

$$2M_3(D;X) + 1 = \begin{cases} A_1(X) + 2A_1(X/9) & \text{if } 3 \nmid D ,\\ A_1(X) + 2A_1(X/3) & \text{if } D \equiv 3 \pmod 9 ,\\ A_1(X) + 2A_1(X/3) + 6A_1(X/9) & \text{if } D \equiv 6 \pmod 9 . \end{cases}$$

Since

$$P_R(s)^{-1} = L_3(s) \prod_{p \mid D,\ p \neq 3} (1 - 1/p^s) = L_3(s) \sum_{n \mid D,\ 3 \nmid n} \mu(n)/n^s$$

with $L_3(s) = 1 - 1/3^s$, $1 - 1/3^{2s}$, or $1 - 2/3^s + 1/3^{2s}$ according to the three cases, we have

$$A_1(X) = \begin{cases} A_2'(X) - A_2'(X/3) & \text{if } 3 \nmid D\ , \\ A_2'(X) - A_2'(X/9) & \text{if } D \equiv 3 \pmod 9\ , \\ A_2'(X) - 2A_2'(X/3) + A_2'(X/9) & \text{if } D \equiv 6 \pmod 9\ , \end{cases}$$

and

$$A_2'(X) = \sum_{n \mid D,\ 3 \nmid n} \mu(n) A_2(X/n)\ .$$

We have

$$Q_1(s) = \prod_{\left(\frac{-3D}{p}\right)=1} (1 - 3/p^{2s} + 2/p^{3s}) \quad \text{and} \quad P_F(s)^{-1} = \prod_{\left(\frac{-3D}{p}\right)=-1} (1 - 1/p^{2s})\ .$$

Thus $Q_1(s)P_F(s)^{-1} = \sum_{n \geq 1} c(n)/n^s$, and we have $c(n) \neq 0$ if and only if $3 \nmid n$ and $n = x^2y^3$, where x and y are coprime and squarefree and $p \mid y$ implies $\left(\frac{-3D}{p}\right) = 1$, in which case

$$c(n) = 2^{\omega(y)}(-3)^{\omega^+(x)}(-1)^{\omega^-(x)}\ ,$$

where $\omega^{\pm}(m)$ is the number of $p \mid m$ with $\left(\frac{-3D}{p}\right) = \pm 1$. It follows that

$$A_2(X) = \sum_{\substack{y \leq X^{1/3},\ 3 \nmid y \\ y \text{ squarefree} \\ p \mid y \implies \left(\frac{-3D}{p}\right)=1}} 2^{\omega(y)} \sum_{\substack{x \leq (X/y^3)^{1/2},\ 3 \nmid x \\ (x,y)=1 \\ x \text{ squarefree}}} (-3)^{\omega^+(x)}(-1)^{\omega^-(x)} A_3(X/(x^2y^3))\ .$$

Finally, if we set $D^* = -3D$ if $3 \nmid D$ and $D^* = -D/3$ if $3 \mid D$, we have

$$\zeta_{K'}(s) = \zeta_{\mathbb{Q}(\sqrt{D^*})}(s) = \zeta(s) L(\left(\tfrac{D^*}{.}\right), s) = \sum_{n \geq 1} a_3(n)/n^s\ .$$

To compute $A_3(X)$, we use the method of the hyperbola (Proposition 5.2), where, as mentioned above, we set $a(n) = 1$ and $b(n) = \left(\frac{D^*}{n}\right)$. Thus $A(X) = \lfloor X \rfloor$, and $B(X) = B(X - |D^*| \lfloor (X/|D^*|) \rfloor)$ is a periodic function of period $|D^*|$ which we tabulate, since D is quite small. Thus

$$A_3(X) = \sum_{1 \leq n \leq E} B(X/n) + \sum_{1 \leq n \leq X/E} \left(\tfrac{D^*}{n}\right) \lfloor X/n \rfloor - \lfloor E \rfloor B(X/E)\ .$$

The optimal value of E in this formula is close to $E = X^{1/2}$, so as claimed above $A_3(X)$ is computed in $O(X^{1/2+\varepsilon})$ time, hence $M_3(D;X)$ also.

Thanks to these formulas, we can compute the following tables, where the given quantities are as follows: $M_3(D;X)$ is as above, $P_3(D;X)$ is the nearest integer to $C_3(D) \cdot X$, where $C_3(D)$ is given above, and $E_3(D;X)$ is an approximation to $(M_3(D;X) - P_3(D;X))/X^{1/4}$; indeed, even though we have only proved that the error is at most $O(X^{2/3})$, it seems to be much closer to $O(X^{1/4+\varepsilon})$. In this table, as in all that follow, the values for $X = 10^n$ for small n are much easier to compute and are available on the author's website.

TABLE 1. Number of cubic fields L with $K = \mathbb{Q}(\sqrt{-4})$ and $f(L) \leq X$

X	$M_3(-4; X)$	$P_3(-4; X)$	$E_3(-4; X)$
10^{10}	1362190594	1362190676	-0.26
10^{11}	13621906974	13621906762	0.38
10^{12}	136219069065	136219067624	1.44
10^{13}	1362190679530	1362190676241	1.85
10^{14}	13621906760943	13621906762412	-0.46
10^{15}	136219067626288	136219067624121	0.39
10^{16}	1362190676222935	1362190676241213	-1.83
10^{17}	13621906762416611	13621906762412128	0.25
10^{18}	136219067623987308	136219067624121284	-4.23
10^{19}	1362190676241140759	1362190676241212841	-1.28

TABLE 2. Number of cubic fields L with $K = \mathbb{Q}(\sqrt{-15})$ and $f(L) \leq X$

X	$M_3(-15; X)$	$P_3(-15; X)$	$E_3(-15; X)$
10^{10}	1763718442	1763719187	-2.36
10^{11}	17637191093	17637191873	-1.39
10^{12}	176371916883	176371918725	-1.84
10^{13}	1763719181402	1763719187255	-3.29
10^{14}	17637191878041	17637191872547	1.74
10^{15}	176371918703468	176371918725472	-3.91
10^{16}	1763719187210265	1763719187254721	-4.45
10^{17}	17637191872586499	17637191872547207	2.21
10^{18}	176371918725343565	176371918725472066	-4.06
10^{19}	1763719187254777573	1763719187254720660	1.01

TABLE 3. Number of cubic fields L with $K = \mathbb{Q}(\sqrt{-39})$ and $f(L) \leq X$

X	$M_3(-39; X)$	$P_3(-39; X)$	$E_3(-39; X)$
10^{10}	2145079645	2145079854	-0.66
10^{11}	21450797505	21450798545	-1.85
10^{12}	214507985582	214507985448	0.13
10^{13}	2145079851212	2145079854483	-1.84
10^{14}	21450798558854	21450798544832	4.43
10^{15}	214507985447211	214507985448322	-0.20
10^{16}	2145079854454820	2145079854483217	-2.84
10^{17}	21450798544855633	21450798544832171	1.32
10^{18}	214507985448208429	214507985448321706	-3.58
10^{19}	2145079854482525318	2145079854483217059	-12.30

5.4. **The special case for $\ell = 3$.** The special case $D = -3$ for $\ell = 3$ corresponds to the enumeration of *pure cubic fields* $\mathbb{Q}(\sqrt[3]{m})$. There are a few additional difficulties compared to the general case which are easily taken care of, so we will simply give the algorithm and the corresponding table, leaving the details of the proofs to the reader. The formula for the Dirichlet series, proved in [8], is as follows:

Proposition 5.4. *We have*

$$\Phi_{3,\mathbb{Q}(\sqrt{-3})}(s) = \frac{1}{6}\left(1+\frac{2}{3^s}+\frac{6}{3^{2s}}\right)\prod_{p\neq 3}\left(1+\frac{2}{p^s}\right)$$
$$+\frac{1}{3}\left(1-\frac{1}{3^s}\right)\prod_{p\equiv\pm1 \pmod 9}\left(1+\frac{2}{p^s}\right)\prod_{p\equiv\pm2,\ \pm4 \pmod 9}\left(1-\frac{1}{p^s}\right).$$

From this we deduce the following:

$$6M_3(-3;X) = A_1(X)+2A_1(X/3)+6A_1(X/9)+2U_1(X)/3-3\ ,$$
$$A_1(X) = \sum_{\substack{y\le X^{1/3}\\ |\mu(3y)|=1\\ p\mid y \implies \left(\frac{D}{p}\right)=1}} 2^{\omega^+(y)} \sum_{\substack{x\le (X/y^3)^{1/2}\\ |\mu(3x)|=1\\ (x,y)=1}} \mu(x)3^{\omega^+(x)}A_2(X/(x^2y^3))\ ,$$
$$A_2(X) = A_3(X)-2A_3(X/3)+A_3(X/9)\ ,$$
$$A_3(X) = 2\sum_{1\le n\le X^{1/2}} \lfloor X/n\rfloor - \lfloor X^{1/2}\rfloor^2\ ,$$
$$U_1(X) = U_2(X)-U_2(X/3)\ ,$$
$$U_2(X) = \sum_{\substack{y\le X^{1/3}\\ |\mu(3y)|=1}} \mu(y)(-2)^{\omega_9(y)} \sum_{\substack{x\le (X/y^3)^{1/2}\\ |\mu(3x)|=1\\ (x,y)=1\\ p\mid x \implies p\equiv\pm1 \pmod 9}} (-3)^{\omega_9(x)}U_3(X/(x^2y^3))\ .$$

Finally, let $\rho = (-1+\sqrt{-3})/2$ be a primitive cube root of unity, set $\chi_9(n) = 0,1,\rho,0,\rho^2$ for $n\equiv 0,\pm1,\pm2,\pm3,\pm4$ modulo 9 respectively, and let $\psi_9(n)$ be its summatory function, equal to $0,1,-\rho^2,-\rho^2,0,\rho^2,\rho^2,-1,0$ for $n\equiv 0,1,2,3,4,5,6,7,8$ modulo 9. We have

$$U_3(X) = 2\mathrm{Re}\left(\sum_{1\le n\le X^{1/2}} \chi_9(n)\overline{\psi_9}(X/n)\right) - |\psi_9(X^{1/2})|^2\ ,$$

from which we deduce Table 4

5.5. **The case $\ell = 5$.** Again we summarize the reductions made above in this case:

$$4M_5(D;X)+1 = \begin{cases} A_1(X)+4A_1(X/25) & \text{if } 5\nmid D\ ,\\ A_1(X)+4A_1(X/5) & \text{if } 5\mid D\ .\end{cases}$$

Here

$$P_R(s)^{-1} = \prod_{p\mid D\ell}(1-1/p^{f(p)s})^{(\ell-1)/(e(p)f(p))}\ .$$

It is immediate to check that $p=\ell=5$ is always totally ramified in K', while if $p\mid D$ but $p\neq 5$, we always have $e(p)=2$, and $f(p)=1$ if $p\equiv\pm1 \pmod 5$, $f(p)=2$

TABLE 4. Number of pure cubic fields L with $f(L) \le X$

X	$M_3(-3;X)$	$P_3(-3;X)$	$E_3(-3;X)$
10^{10}	17045461815	17045463465	-5.22
10^{11}	185860709664	185860709585	0.14
10^{12}	2012667847513	2012667845156	2.36
10^{13}	21667285929697	21667285944613	-8.39
10^{14}	232078934410572	232078934376706	10.71
10^{15}	2474850093045781	2474850093072833	-4.81
10^{16}	26289108423790515	26289108423786084	0.44
10^{17}	278297159168325245	278297159168438350	-6.36
10^{18}	2937032340990444425	2937032340990158620	9.04

if $p \equiv \pm 2 \pmod 5$, so the corresponding Euler factors of $P_R(s)^{-1}$ are $(1-1/p^s)^2$ and $(1-1/p^{2s})$, hence

$$P_R(s)^{-1} = \prod_{p \mid 5D} \left((1-1/p^s) \left(1 - \left(\frac{p}{5} \right) / p^s \right) \right) .$$

If as above we write $P_R(s)^{-1} = \sum_{n \ge 1} r(n)/n^s$, then if $r(n) \neq 0$ we must have $n = xy^2$ with x and y coprime, squarefree and dividing $5D$, and in that case

$$r(n) = \left(\frac{y}{5} \right) \prod_{p \mid x} \left(- \left(1 + \left(\frac{p}{5} \right) \right) \right) .$$

Thus

$$A_1(X) = \sum_{\substack{x,\ y \mid 5D \\ \text{squarefree, coprime}}} \left(\frac{y}{5} \right) \prod_{p \mid x} \left(- \left(1 + \left(\frac{p}{5} \right) \right) \right) A_2(X/(xy^2)) .$$

To treat the other two factors $Q_1(s)$ and $P_F(s)^{-1}$ it is preferable to separate them.

When $p \nmid 5D$ we have $e(p) = 1$, and when $f(p) > 1$ we have $f(p) = 2$ if $p \equiv -\left(\frac{D}{p} \right) \pmod 5$, and $f(p) = 4$ when $p \equiv \pm 2 \pmod 5$. Thus,

$$P_F(s)^{-1} = \prod_{\substack{p \equiv -\left(\frac{D}{p} \right) \pmod 5 \\ p \nmid 5D}} (1-1/p^{2s})^2 \prod_{\substack{p \equiv \pm 2 \pmod 5 \\ p \nmid 5D}} (1 - 1/p^{4s}) = \sum_{n \ge 1} f(n)/n^s ,$$

where $f(n) \neq 0$ implies that $n = x^2 y^4$ with x and y coprime, squarefree, and coprime to $5D$, $p \mid x$ implies $p \equiv -\left(\frac{D}{p} \right) \pmod 5$, $p \mid y$ implies $p \not\equiv \left(\frac{D}{p} \right) \pmod 5$, and $f(n) = (-2)^{\omega(x)} (-1)^{\omega_{\pm 2}(y)}$, where $\omega_{\pm 2}(y)$ is the number of prime divisors of y congruent to ± 2 modulo 5. Hence

$$A_2(X) = \sum_{\substack{y \le X^{1/4} \\ \text{cond}}} (-1)^{\omega_{\pm 2}(y)} \sum_{\substack{x \le (X/y^4)^{1/2} \\ \text{cond}}} (-2)^{\omega(x)} A_3'(X/(x^2 y^4))$$

for some intermediate counting function $A_3'(X)$, where "cond" are the conditions given above. Furthermore,

$$Q_1(s) = \prod_{p\equiv\left(\frac{D}{p}\right)\equiv\pm1 \pmod 5}(1-10/p^{2s}+20/p^{3s}-15/p^{4s}+4/p^{5s}) = \sum_{n\geq1}g(n)/n^s\ ,$$

where $g(n)\neq0$ if and only if n is of the form $n=x_2^2x_3^3x_4^4x_5^5$ with the x_i squarefree, pairwise coprime, and divisible only by primes p such that $p\equiv\left(\frac{D}{p}\right)\equiv\pm1 \pmod 5$, in which case

$$g(n) = (-10)^{\omega(x_2)}(20)^{\omega(x_3)}(-15)^{\omega(x_4)}(4)^{\omega(x_5)}\ ,$$

so that

$$A_3'(X) = \sum_{\substack{x_5\leq X^{1/5}\\ \text{cond}}}4^{\omega(x_5)}\sum_{\substack{x_4\leq(X/x_5^5)^{1/4}\\ \text{cond}}}(-15)^{\omega(x_4)}\sum_{\substack{x_3\leq(X/(x_4^4x_5^5))^{1/3}\\ \text{cond}}}20^{\omega(x_3)}\ \cdot$$
$$\cdot\sum_{\substack{x_2\leq(X/(x_3^3x_4^4x_5^5))^{1/2}\\ \text{cond}}}(-10)^{\omega(x_2)}A_3(X/(x_2^2x_3^3x_4^4x_5^5))\ ,$$

where as above $A_3(X)$ is the summatory function of the Dirichlet coefficients of the Dedekind zeta function $\zeta_{K'}(s)$.

Remark 5.5. The above formulas may look incredibly messy, but first they are immediate to program, and second as explained above, the running time will be dominated by the time needed to compute $A_3(X)$, and *not* by the multiple summations, which will only multiply the time by a *small* constant factor.

As mentioned above, to compute $A_3(X)$ we use the method of the hyperbola (Proposition 5.2) three times.

In our case $\ell=5$, since $\omega^2=\chi_5$, we have

$$\zeta_{K'}(s) = \zeta(s)L(\chi_5,s)L(\omega\chi_D,s)L(\overline{\omega}\chi_D,s)\ .$$

Thus, we write

$$\zeta(s)L(\chi_5,s) = \sum_{n\geq1}a_{3,1}(n)/n^s\ ,\quad L(\omega\chi_D,s)L(\overline{\omega}\chi_D,s) = \sum_{n\geq1}a_{3,2}(n)/n^s\ ,$$

and the corresponding summatory functions $A_{3,1}(X)$ and $A_{3,2}(X)$ are computed thanks to Proposition 5.2 (as usual the functions χ_5, $\omega\chi_D$, and $\overline{\omega}\chi_D$ as well as their summatory functions are periodic with small period, so they are tabulated), and using Proposition 5.2 once more, we obtain the desired summatory function $A_3(X)$ since $a_3(n)$ is the arithmetic convolution of $a_{3,1}(n)$ and $a_{3,2}(n)$, for a total running time in $O(X^{3/4+\varepsilon})$. Here it seems that the error in the asymptotic estimate proved to be $O(X^{4/5+\varepsilon})$ is closer to $O(X^{3/8})$, so we set $E_5(D;X) = (M_5(D;X) - P_5(D;X))/X^{3/8}$. (See Tables 5 and 6.)

TABLE 5. Number of D_5 quintic fields L with $K = \mathbb{Q}(\sqrt{-3})$ and $f(L) \le X$

X	$M_5(-3;X)$	$P_5(-3;X)$	$E_5(-3;X)$
10^6	50817	50785	0.18
10^7	508038	507853	0.44
10^8	5078754	5078532	0.22
10^9	50784256	50785324	−0.45
10^{10}	507849182	507853244	−0.72
10^{11}	5078531182	5078532445	−0.09
10^{12}	50785334021	50785324450	0.30

TABLE 6. Number of D_5 quintic fields L with $K = \mathbb{Q}(\sqrt{-15})$ and $f(L) \le X$

X	$M_5(-15;X)$	$P_5(-15;X)$	$E_5(-15;X)$
10^6	78897	78805	0.52
10^7	787986	788048	−0.15
10^8	7879958	7880481	−0.52
10^9	78805084	78804814	0.11
10^{10}	788050642	788048138	0.45
10^{11}	7880487110	7880481380	0.43
10^{12}	78804743357	78804813801	−2.23

5.6. **The special case for $\ell = 5$.** Once again, we only give the algorithm and the corresponding table. We first give a preliminary result and then the formula for the Dirichlet series, all proved in [10].

Proposition 5.6. *Let E be the quintic field defined by $x^5 + 5x^3 + 5x - 1 = 0$, with discriminant 5^7 and Galois group $C_5 \rtimes C_4$, and let p be a prime such that $p \equiv 1 \pmod 5$. The following are equivalent:*

(1) *p is totally split in E.*
(2) *$\varepsilon = (-1 + \sqrt{5})/2$ is a fifth power modulo p, in other words $\varepsilon^{(p-1)/5} \equiv 1 \pmod p$.*

In practice, testing the second condition is faster.

Theorem 5.7. *Keep the above notation, and set*

$$\omega_E(p) = \begin{cases} -1 & \text{if } p \text{ is inert or totally ramified in } E\ , \\ 4 & \text{if } p \text{ is totally split in } E\ , \\ 0 & \text{otherwise.} \end{cases}$$

We have

$$\Phi_{5,\mathbb{Q}(\sqrt{5})}(s) = \frac{1}{20}\left(1 + \frac{4}{5^s}\right) \prod_{p \equiv 1 \pmod 5} \left(1 + \frac{4}{p^s}\right) + \frac{1}{5} \prod_p \left(1 + \frac{\omega_E(p)}{p^s}\right) .$$

It is immediate to see that $\omega_E(p) = 0$ when $p \not\equiv 1 \pmod 5$, that the only totally ramified (or ramified) prime is $p = 5$, so the only computation that must be done is to test whether $p \equiv 1 \pmod 5$ satisfies the second condition of the above proposition. Unfortunately, this is a nonabelian condition, so I do not see any way to compute $M(D;X)$ with an algorithm faster than $O(X)$. Thus, using rather naive methods we obtain Table 7:

TABLE 7. Number of D_5 quintic fields L in the special case $K = \mathbb{Q}(\sqrt{5})$ and $f(L) \le X$

X	$M_5(5;X)$	$P_5(5;X)$	$E_5(5;X)$
10^6	20426	20378	0.27
10^7	203938	203782	0.37
10^8	2037874	2037819	0.06
10^9	20378156	20378187	-0.01
10^{10}	203782163	203781871	0.05

Note that because of the nonabelian second term, with a similar amount of computation than the general case, we reach a much smaller value of X. This does *not* happen when $\ell \equiv 3 \pmod 4$ (see e.g., $\ell = 7$ below) since there is no nonabelian term.

5.7. **The case $\ell = 7$.** The case $\ell = 7$ (and the case of larger ℓ) is similar but slightly more complicated than the case $\ell = 5$, and the tedious details are left to the reader. We give the tables below for $D = -3$ and $D = -35$, where here we set $E_7(D;X) = (M_7(D;X) - P_7(D;X)/X^{5/12}$ (it would seem that the error is $O(X^{(\ell-2)/(2(\ell-1))+\varepsilon})$).

TABLE 8. Number of D_7 septic fields L with $K = \mathbb{Q}(\sqrt{-3})$ and $f(L) \le X$

X	$M_7(-3;X)$	$P_7(-3;X)$	$E_7(-3;X)$
10^6	29689	29633	0.18
10^7	296453	296332	0.15
10^8	2962722	2963322	-0.28
10^9	29634095	29633216	0.16
10^{10}	296332445	296332163	0.02

TABLE 9. Number of D_7 septic fields L with $K = \mathbb{Q}(\sqrt{-35})$ and $f(L) \le X$

X	$M_7(-35;X)$	$P_7(-35;X)$	$E_7(-35;X)$
10^6	52918	53000	-0.26
10^7	529927	530000	-0.09
10^8	5300615	5300003	0.28
10^9	53000137	53000025	0.02
10^{10}	530024447	530000255	1.65

5.8. **The special case for $\ell = 7$.** The special case for $\ell = 7$ is *simpler* than that for $\ell = 5$ since (as for all $\ell \equiv 3 \pmod 4$, $\ell > 3$), there is only the main term, in other words by Theorem 1.1, we have

$$\Phi_{7,\mathbb{Q}(\sqrt{-7})}(s) = \frac{1}{6}\left(1 + \frac{6}{7^s}\right) \prod_{p \equiv \pm 1 \pmod 7} \left(1 + \frac{6}{p^s}\right) .$$

Note that the condition $p \equiv \pm 1 \pmod 7$ can simply be tested by characters, and so using similar methods to the above, we obtain the following table:

TABLE 10. Number of D_7 septic fields L in the special case $K = \mathbb{Q}(\sqrt{-7})$ and $f(L) \leq X$

X	$M_7(-7;X)$	$P_7(-7;X)$	$E_7(-7;X)$
10^6	222984	222793	0.60
10^7	2506500	2506662	-0.20
10^8	27858604	27853959	2.16
10^9	306400832	306412989	-2.16
10^{10}	3342900105	3342863878	2.47

References

[1] Henri Cohen, *Advanced Topics in Computational Number Theory*, Graduate Texts in Mathematics, vol. 193, Springer-Verlag, New York, 2000. MR1728313 (2000k:11144)

[2] Henri Cohen, *Comptage exact de discriminants d'extensions abéliennes* (French, with English and French summaries), J. Théor. Nombres Bordeaux **12** (2000), no. 2, 379–397. Colloque International de Théorie des Nombres (Talence, 1999). MR1823191 (2002b:11158)

[3] H. Cohen, *High precision computation of Hardy–Littlewood constants*, preprint available on the author's web page.

[4] Henri Cohen, *Number Theory. Vol. II. Analytic and Modern Tools*, Graduate Texts in Mathematics, vol. 240, Springer, New York, 2007. MR2312338 (2008e:11002)

[5] Henri Cohen, Francisco Diaz y Diaz, and Michel Olivier, *On the density of discriminants of cyclic extensions of prime degree*, J. Reine Angew. Math. **550** (2002), 169–209, DOI 10.1515/crll.2002.071. MR1925912 (2004a:11115)

[6] Henri Cohen, Francisco Diaz y Diaz, and Michel Olivier, *Cyclotomic extensions of number fields*, Indag. Math. (N.S.) **14** (2003), no. 2, 183–196, DOI 10.1016/S0019-3577(03)90003-6. MR2026813 (2004i:11131)

[7] Henri Cohen, Francisco Diaz y Diaz, and Michel Olivier, *Counting discriminants of number fields* (English, with English and French summaries), J. Théor. Nombres Bordeaux **18** (2006), no. 3, 573–593. MR2330428 (2008d:11127)

[8] Henri Cohen and Anna Morra, *Counting cubic extensions with given quadratic resolvent*, J. Algebra **325** (2011), 461–478, DOI 10.1016/j.jalgebra.2010.08.027. MR2745550 (2012b:11168)

[9] H. Cohen and F. Thorne, *Dirichlet series associated to cubic fields with given quadratic resolvent*, Michigan Math. Journal, to appear.

[10] H. Cohen and F. Thorne, *On D_ℓ-Extensions of odd prime degree ℓ*, preprint.

UNIVERSITÉ DE BORDEAUX, INSTITUT DE MATHÉMATIQUES, U.M.R. 5251 DU C.N.R.S., 351 COURS DE LA LIBÉRATION, 33405 TALENCE CEDEX, FRANCE

E-mail address: `Henri.Cohen@math.u-bordeaux1.fr`