Quartic and $\mathbb{D}_\ell$ Fields of Degree $\ell$ with given Resolvent

Henri Cohen, Frank Thorne

Institut de Mathématiques de Bordeaux

January 14, 2013, Bordeaux
Number fields will always be considered up to isomorphism. Dirichlet series associated to number fields of given degree $n$:

$$
\Phi_n(s) = \sum_{[K:\mathbb{Q}] = n} |\text{disc}(K)|^{-s}.
$$

Knowing $\Phi_n$ explicitly is equivalent to knowing how many $K$ for each discriminant. One usually imposes additional conditions: for instance $\Phi_n(G; s)$: Galois group of the Galois closure isomorphic to $G$, or $\Phi_n(k; s)$: here $k$ quadratic resolvent field of degree $\ell$ field of Galois group $D_\ell$, more generally degree $d$ resolvent field of semi-direct product of a subgroup of $(\mathbb{Z}/\ell\mathbb{Z})^*$ of order $d$ by $C_\ell$, for instance quadratic resolvent of cubic, also cubic resolvent of quartic.
Theorem (Mäki et al)

*If $G$ is an abelian group then $\Phi_n(G; s)$ is an explicitly determinable finite linear combination of (infinite) Euler products.*

Examples:

$$\Phi_2(C_2; s) = -1 + \left(1 + \frac{1}{2^{2s}} + \frac{2}{2^{3s}}\right) \prod_{p \neq 2} \left(1 + \frac{1}{p^s}\right),$$

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

If $G$ is not abelian, conjecturally not possible.
Theorem (Mäki et al)

If $G$ is an abelian group then $\Phi_n(G; s)$ is an explicitly determinable finite linear combination of (infinite) Euler products.

**Examples :**

\[
\Phi_2(C_2; s) = -1 + \left( 1 + \frac{1}{2^{2s}} + \frac{2}{2^{3s}} \right) \prod_{p \neq 2} \left( 1 + \frac{1}{p^s} \right),
\]

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

If $G$ is not abelian, conjecturally not possible.
Instead of fixing the Galois group, we can fix the *resolvent* field. Examples:

- If $K$ is a noncyclic cubic field, or more generally a field of degree $\ell$ with Galois closure $D_\ell$, its Galois closure contains a unique quadratic field $k = \mathbb{Q}(\sqrt{D})$, the *quadratic resolvent*. We may want to consider $\Phi_\ell(k; s)$, where $k$ (or $D$) is fixed.

- More generally, same with $D_\ell$ replaced by semidirect product of $C_\ell$ with subgroup of $(\mathbb{Z}/\ell\mathbb{Z})^*$.

- If $K$ is a quartic field with $A_4$ or $S_4$ Galois group of Galois closure, the latter contains a cubic field $k$, unique and cyclic in the $A_4$ case, and unique up to conjugation and noncyclic in the $S_4$ case, the *cubic resolvent*. We may want to consider $\Phi_4(k; s)$, where $k$ is fixed.
Introduction IV

Theorem

- (Morra, C., 2008.) $\Phi_3(k; s)$ is a finite linear combination of explicit Euler products.
- (Diaz y Diaz, Olivier, C., 2000.) $\Phi_4(k; s)$ is a finite linear combination of explicit Euler products.
- (C., 2012.) $\Phi_\ell(k; s)$ is a finite linear combination of explicit Euler products.

$M_n(k; X) :$ Number of fields $K$ of degree $n$ with resolvent $k$ and $f(K) \leq X.$

Corollary

There exist strictly positive constants $C_n(k)$ such that $M_n(k; X) = C_n(k) \cdot X + O(X^{1-1/\ell})$ (much better remainder terms can be obtained) with the following exception : in the $D_\ell$ case, if $k = \mathbb{Q}(\sqrt{\ell^*})$ with $\ell^* = (-1)^{(\ell-1)/2} \ell$ and $\ell \equiv 3 \pmod{4}$ then $M_n(k; X) = C_n(k) \cdot (X \log(X) + C'_n(k)X) + O(X^{1-1/\ell}).$
Theorem

- (Morra, C., 2008.) $\Phi_3(k; s)$ is a finite linear combination of explicit Euler products.
- (Diaz y Diaz, Olivier, C., 2000.) $\Phi_4(k; s)$ is a finite linear combination of explicit Euler products.
- (C., 2012.) $\Phi_\ell(k; s)$ is a finite linear combination of explicit Euler products.

$M_n(k; X)$: Number of fields $K$ of degree $n$ with resolvent $k$ and $f(K) \leq X$.

Corollary

There exist strictly positive constants $C_n(k)$ such that

$$M_n(k; X) = C_n(k) \cdot X + O(X^{1-1/\ell}) \text{ (much better remainder terms can be obtained) with the following exception: in the } D_\ell \text{ case, if}$$

$k = \mathbb{Q}(\sqrt{\ell^*})$ with $\ell^* = (-1)^{(\ell-1)/2} \ell$ and $\ell \equiv 3 \pmod{4}$ then

$$M_n(k; X) = C_n(k) \cdot (X \log(X) + C'_n(k)X) + O(X^{1-1/\ell}).$$
Unfortunately, in all of these results, “explicit” is not very nice: all involve sums over characters of certain subgroups or twisted ray class groups, not easy to determine in general, (easy in each specific case).

In fact, case in point: knowledge of the size of say 3-part of class groups is very poor: smaller than the whole, but gaining a small exponent is hard (Ellenberg–Venkatesh). For instance, conjecturally the number of cubic fields of given discriminant $d$ should be $d^\varepsilon$ for any $\varepsilon > 0$, but the best known result due to EV is $d^{1/3+\varepsilon}$.

We do not improve on this, but give instead nice explicit formulas for $\Phi_\ell(k; s)$ (in particular $\Phi_3(k; s)$) and $\Phi_4(k; s)$ Note that for $\Phi_\ell$ we have $\text{disc}(K) = \text{disc}(k)^{(\ell-1)/2} f(K)^{\ell-1}$ and for $\Phi_4$ we have $\text{disc}(K) = \text{disc}(k) f(K)^2$ for some $f(K) \in \mathbb{Z}_{\geq 1}$. We set

$$\Phi_n(k; s) = 1/c(n) + \sum_K f(K)^{-s},$$

where $c(n) = 1/(\ell - 1)$ for $\Phi_\ell$ and $c(n) = 1/\text{Aut}(k)$ for $\Phi_4$. 
Unfortunately, in all of these results, "explicit" is not very nice: all involve sums over characters of certain subgroups or twisted ray class groups, not easy to determine in general, (easy in each specific case).

In fact, case in point: knowledge of the size of say 3-part of class groups is very poor: smaller than the whole, but gaining a small exponent is hard (Ellenberg–Venkatesh). For instance, conjecturally the number of cubic fields of given discriminant \( d \) should be \( d^{\varepsilon} \) for any \( \varepsilon > 0 \), but the best known result due to EV is \( d^{1/3+\varepsilon} \).

We do not improve on this, but give instead nice explicit formulas for \( \Phi_\ell(k; s) \) (in particular \( \Phi_3(k; s) \)) and \( \Phi_4(k; s) \). Note that for \( \Phi_\ell \) we have \( \text{disc}(K) = \text{disc}(k)^{(\ell-1)/2} f(K)^{\ell-1} \) and for \( \Phi_4 \) we have \( \text{disc}(K) = \text{disc}(k) f(K)^2 \) for some \( f(K) \in \mathbb{Z}_{\geq 1} \). We set

\[
\Phi_n(k; s) = 1/c(n) + \sum_K f(K)^{-s},
\]

where \( c(n) = 1/(\ell - 1) \) for \( \Phi_\ell \) and \( c(n) = 1/\text{Aut}(k) \) for \( \Phi_4 \).
Unfortunately, in all of these results, “explicit” is not very nice: all involve sums over characters of certain subgroups or twisted ray class groups, not easy to determine in general, (easy in each specific case).

In fact, case in point: knowledge of the size of say 3-part of class groups is very poor: smaller than the whole, but gaining a small exponent is hard (Ellenberg–Venkatesh). For instance, conjecturally the number of cubic fields of given discriminant \(d\) should be \(d^\varepsilon\) for any \(\varepsilon > 0\), but the best known result due to EV is \(d^{1/3+\varepsilon}\).

We do not improve on this, but give instead nice explicit formulas for \(\Phi_\ell(k; s)\) (in particular \(\Phi_3(k; s)\)) and \(\Phi_4(k; s)\). Note that for \(\Phi_\ell\) we have \(\text{disc}(K) = \text{disc}(k)^{(\ell - 1)/2} f(K)^{\ell - 1}\) and for \(\Phi_4\) we have \(\text{disc}(K) = \text{disc}(k) f(K)^2\) for some \(f(K) \in \mathbb{Z}_{\geq 1}\). We set

\[
\Phi_n(k; s) = 1/c(n) + \sum_K f(K)^{-s},
\]

where \(c(n) = 1/(\ell - 1)\) for \(\Phi_\ell\) and \(c(n) = 1/\text{Aut}(k)\) for \(\Phi_4\).
In a preceding talk, gave statements and details of the proofs of the theorems. Here, we give the theorems but focus on algorithmic aspects.

Note: $D$ always a fundamental discriminant, resolvent quadratic field $k = \mathbb{Q}(\sqrt{D})$. We set $L = \mathbb{Q}(\sqrt{D}, \sqrt{-3})$, biquadratic field, $\tau_1, \tau_2$ generators of $G = \text{Gal}(L/\mathbb{Q})$, $T = \{\tau_1 + 1, \tau_2 + 1\}$ in the group ring $\mathbb{F}_3[G]$, and $B = \{(1), (\sqrt{-3}), (3), (3\sqrt{-3})\}$ as ideals of $L$.

The ray class groups which occur here are

$$G_b = (\text{Cl}_b(L)/\text{Cl}_b(L)^3)[T] \quad \text{with} \quad b \in B.$$
In a preceding talk, gave statements and details of the proofs of the theorems. Here, we give the theorems but focus on algorithmic aspects.

Note: $D$ always a fundamental discriminant, resolvent quadratic field $k = \mathbb{Q}(\sqrt{D})$. We set $L = \mathbb{Q}(\sqrt{D}, \sqrt{-3})$, biquadratic field, $\tau_1, \tau_2$ generators of $G = \text{Gal}(L/\mathbb{Q})$, $T = \{\tau_1 + 1, \tau_2 + 1\}$ in the group ring $\mathbb{F}_3[G]$, and $\mathcal{B} = \{(1), (\sqrt{-3}), (3), (3\sqrt{-3})\}$ as ideals of $L$.

The ray class groups which occur here are

$$G_b = (\text{Cl}_b(L)/\text{Cl}_b(L)^3)[T], \quad \text{with} \quad b \in \mathcal{B}.$$
In a preceding talk, gave statements and details of the proofs of the theorems. Here, we give the theorems but focus on algorithmic aspects.

Note: $D$ always a fundamental discriminant, resolvent quadratic field $k = \mathbb{Q}(\sqrt{D})$. We set $L = \mathbb{Q}(\sqrt{D}, \sqrt{-3})$, biquadratic field, $\tau_1, \tau_2$ generators of $G = \text{Gal}(L/\mathbb{Q})$, $T = \{\tau_1 + 1, \tau_2 + 1\}$ in the group ring $\mathbb{F}_3[G]$, and $B = \{(1), (\sqrt{-3}), (3), (3\sqrt{-3})\}$ as ideals of $L$. The ray class groups which occur here are

$$G_b = (\text{Cl}_b(L)/\text{Cl}_b(L)^3)[T], \quad \text{with} \quad b \in B.$$
The main theorem of C.-Morra and of the first part of Morra’s thesis is that

\[ \Phi_3(D; s) = \sum_{b \in B} A_b(s) \sum_{\chi \in \hat{G}_b} \omega \chi(3) F(b, \chi, s), \]

where \( A_b(s) \) are constant multiples of a single Euler factor at 3, \( \omega \chi \) depends on the character \( \chi \) but takes only the values 0, \( \pm 1 \), and \( 2 \), and

\[ F(b, \chi, s) = \prod_{(\frac{-3D}{p}) = 1} \left( 1 + \frac{\omega \chi(p)}{p^s} \right). \]
This proves the claim that we have an “explicit” finite linear combination of Euler products. However not very easy to use in practice. It does lead however to the estimate given above:

\[ M_3(D; X) = C_3(D) \cdot X + O(X^{2/3}) , \]

except in the special case \( D = -3 \) (enumeration of pure cubic fields) where the result is

\[ M_3(D; X) = C_3(D) \cdot X(\log(X) + C'_3(D)) + O(X^{2/3}) . \]
In joint work with F. Thorne, we have transformed the above theorem into a much more usable formula. Need to define:

- **$D^*$** discriminant of mirror field of $k = \mathbb{Q}(\sqrt{D})$, i.e., $D^* = -3D$ if $3 \nmid D$, $D^* = -D/3$ if $3 \mid D$.

- **$\mathcal{L}_N$** : cubic fields of discriminant $N$ (only used for $N = D^*$ and $N = -27D$).

- **$\mathcal{L}(D) = \mathcal{L}_{D^*} \cup \mathcal{L}_{-27D}$**.

- If $E$ is a cubic field and $p$ a prime number,

$$
\omega_E(p) = \begin{cases} 
-1 & \text{if } p \text{ is inert in } E, \\
2 & \text{if } p \text{ is totally split in } E, \\
0 & \text{otherwise.}
\end{cases}
$$
In joint work with F. Thorne, we have transformed the above theorem into a much more usable formula. Need to define:

- \( D^* \) discriminant of mirror field of \( k = \mathbb{Q}(\sqrt{D}) \), i.e., \( D^* = -3D \) if \( 3 \nmid D \), \( D^* = -D/3 \) if \( 3 \mid D \).

- \( \mathcal{L}_N \) : cubic fields of discriminant \( N \) (only used for \( N = D^* \) and \( N = -27D \)).

- \( \mathcal{L}(D) = \mathcal{L}_{D^*} \cup \mathcal{L}_{-27D} \).

- If \( E \) is a cubic field and \( p \) a prime number,

\[
\omega_E(p) = \begin{cases} 
-1 & \text{if } p \text{ is inert in } E, \\
2 & \text{if } p \text{ is totally split in } E, \\
0 & \text{otherwise.}
\end{cases}
\]
Theorem (Thorne, C.)

We have

\[ c_D \Phi_3(D; s) = \frac{1}{2} M_1(s) \prod_{\left( \frac{-3D}{p} \right) = 1} \left( 1 + \frac{2}{p^s} \right) + \sum_{E \in \mathcal{L}(D)} M_{2,E}(s) \prod_{\left( \frac{-3D}{p} \right) = 1} \left( 1 + \frac{\omega_E(p)}{p^s} \right) \]

where \( c_D = 1 \) if \( D = 1 \) or \( D < -3 \), \( c_D = 3 \) if \( D = -3 \) or \( D > 1 \), and the 3-Euler factors \( M_1(s) \) and \( M_{2,E}(s) \) are given in the following table.

<table>
<thead>
<tr>
<th>Condition on ( D )</th>
<th>( M_1(s) )</th>
<th>( M_{2,E}(s), E \in \mathcal{L}_D^* )</th>
<th>( M_{2,E}(s), E \in \mathcal{L}_{-27D} )</th>
</tr>
</thead>
<tbody>
<tr>
<td>( 3 \nmid D )</td>
<td>( 1 + 2/3^{2s} )</td>
<td>( 1 + 2/3^{2s} )</td>
<td>( 1 - 1/3^{2s} )</td>
</tr>
<tr>
<td>( D \equiv 3 \pmod{9} )</td>
<td>( 1 + 2/3^{s} )</td>
<td>( 1 + 2/3^{s} )</td>
<td>( 1 - 1/3^{s} )</td>
</tr>
<tr>
<td>( D \equiv 6 \pmod{9} )</td>
<td>( 1 + 2/3^{s} + 6/3^{2s} )</td>
<td>( 1 + 2/3^{s} + 3\omega_E(3)/3^{2s} )</td>
<td>( 1 - 1/3^{s} )</td>
</tr>
</tbody>
</table>
The Cubic Case: Examples

Examples:

\[ \Phi_3(-4; s) = \frac{1}{2} \left(1 + \frac{2}{3^{2s}}\right) \prod_{\left(\frac{12}{p}\right) = 1} \left(1 + \frac{2}{p^s}\right). \]

Here \( \mathcal{L}(D) = \emptyset \).

\[ \Phi_3(-255; s) = \frac{1}{2} \left(1 + \frac{2}{3^s} + \frac{6}{3^{2s}}\right) \prod_{\left(\frac{6885}{p}\right) = 1} \left(1 + \frac{2}{p^s}\right) \]

\[ + \left(1 - \frac{1}{3^s}\right) \prod_{p} \left(1 + \frac{\omega_E(p)}{p^s}\right), \]

where \( E \) is the cubic field determined by \( x^3 - 12x - 1 = 0 \).

In words, the splitting of primes in the single cubic field \( E \) determines all cubic fields with quadratic resolvent \( \mathbb{Q}(\sqrt{-255}) \) (“One field to rule them all”).
The Cubic Case : Examples

Examples :

\[ \Phi_3(-4; s) = \frac{1}{2} \left( 1 + \frac{2}{3^{2s}} \right) \prod_{\left( \frac{12}{p} \right) = 1} \left( 1 + \frac{2}{p^s} \right). \]

Here \( \mathcal{L}(D) = \emptyset \).

\[ \Phi_3(-255; s) = \frac{1}{2} \left( 1 + \frac{2}{3^s} + \frac{6}{3^{2s}} \right) \prod_{\left( \frac{6885}{p} \right) = 1} \left( 1 + \frac{2}{p^s} \right) \]

\[ + \left( 1 - \frac{1}{3^s} \right) \prod_p \left( 1 + \frac{\omega_E(p)}{p^s} \right), \]

where \( E \) is the cubic field determined by \( x^3 - 12x - 1 = 0 \).

In words, the splitting of primes in the single cubic field \( E \) determines all cubic fields with quadratic resolvent \( \mathbb{Q}(\sqrt{-255}) \) (“One field to rule them all”).
The Cubic Case: Examples

Examples:

\[ \Phi_3(-4; s) = \frac{1}{2} \left( 1 + \frac{2}{3^{2s}} \right) \prod_{(\frac{12}{p}) = 1} \left( 1 + \frac{2}{p^s} \right). \]

Here \( \mathcal{L}(D) = \emptyset \).

\[ \Phi_3(-255; s) = \frac{1}{2} \left( 1 + \frac{2}{3^s} + \frac{6}{3^{2s}} \right) \prod_{(\frac{6885}{p}) = 1} \left( 1 + \frac{2}{p^s} \right) \]

\[ + \left( 1 - \frac{1}{3^s} \right) \prod_p \left( 1 + \frac{\omega_E(p)}{p^s} \right), \]

where \( E \) is the cubic field determined by \( x^3 - 12x - 1 = 0 \).

In words, the splitting of primes in the single cubic field \( E \) determines all cubic fields with quadratic resolvent \( \mathbb{Q}(\sqrt{-255}) \) (“One field to rule them all”).
Several ideas enter in the proof of Thorne’s theorem. An easy one is to show that there exists a bijection between pairs of conjugate characters $\chi$ of $G_b$ and fields $E \in \mathcal{L}(D)$.

A more difficult one is the use of a relatively recent theorem of Nakagawa–Ono giving exact identities between class numbers of certain cubic forms.
Several ideas enter in the proof of Thorne’s theorem. An easy one is to show that there exists a bijection between pairs of conjugate characters $\chi$ of $G_b$ and fields $E \in \mathcal{L}(D)$.

A more difficult one is the use of a relatively recent theorem of Nakagawa–Ono giving exact identities between class numbers of certain cubic forms.
To estimate the number of cubic fields of given discriminant $Dn^2$, it is in particular necessary to estimate the number of auxiliary fields $E$ which occur, i.e., the cardinality of $L(D)$. This is given as follows:

**Theorem (Nakagawa, Ono, Thorne)**

Denote by $r_{k3}(D)$ the $3$-rank of the class group of $k = \mathbb{Q}(\sqrt{D})$. We have

$$|L(D)| = \begin{cases} 
(3^{r_{k3}(D)} - 1)/2 & \text{if } D < 0, \\
(3^{r_{k3}(D)+1} - 1)/2 & \text{if } D > 0. 
\end{cases}$$

As mentioned, the problem is that we have only very weak upper bounds for $3^{r_{k3}(D)}$ (in $O(|D|^{1/3+\varepsilon})$), although should be $O(|D|^\varepsilon)$.

A special case of the above, already in C.-Morra, is a consequence of a precise form of Scholtz’s mirror theorem: if $D < 0$ and $3 \nmid h(D)$ then $L(D) = \emptyset$, so the formula is as simple as possible.
To estimate the number of cubic fields of given discriminant $Dn^2$, it is in particular necessary to estimate the number of auxiliary fields $E$ which occur, i.e., the cardinality of $\mathcal{L}(D)$. This is given as follows:

**Theorem (Nakagawa, Ono, Thorne)**

Denote by $rk_3(D)$ the 3-rank of the class group of $k = \mathbb{Q}(\sqrt{D})$. We have

$$|\mathcal{L}(D)| = \begin{cases} (3^{rk_3(D)} - 1)/2 & \text{if } D < 0, \\ (3^{rk_3(D)+1} - 1)/2 & \text{if } D > 0. \end{cases}$$

As mentioned, the problem is that we have only very weak upper bounds for $3^{rk_3(D)}$ (in $O(|D|^{1/3+\varepsilon})$), although should be $O(|D|^{\varepsilon})$.

A special case of the above, already in C.-Morra, is a consequence of a precise form of Scholtz’s mirror theorem: if $D < 0$ and $3 \nmid h(D)$ then $\mathcal{L}(D) = \emptyset$, so the formula is as simple as possible.
Computing the number $N_3(k; X)$ of cubic fields having a given quadratic resolvent $k = \mathbb{Q}(\sqrt{D})$ and absolute discriminant up to $X$ can be done very fast using the theorem and standard techniques of analytic number theory ($X = 10^{20}$ is feasible), see below. We can also sum on $D$ and compute the total number $N_3(X)$ of cubic fields, although this is less efficient than the method of K. Belabas.

It is tempting to try to prove the known result that $N_3(X) \sim c \cdot X$ for a known constant $c$ (essentially $c = 1/\zeta(3)$). It is probably possible to do this, or at least to obtain $N_3(X) = O(X^{1+\varepsilon})$, but since this has been proved (rather easily in fact) by other methods, it seems to be unnecessary work.
Computing the number $N_3(k; X)$ of cubic fields having a given quadratic resolvent $k = \mathbb{Q}(\sqrt{D})$ and absolute discriminant up to $X$ can be done very fast using the theorem and standard techniques of analytic number theory ($X = 10^{20}$ is feasible), see below. We can also sum on $D$ and compute the total number $N_3(X)$ of cubic fields, although this is less efficient than the method of K. Belabas.

It is tempting to try to prove the known result that $N_3(X) \sim c \cdot X$ for a known constant $c$ (essentially $c = 1/\zeta(3)$). It is probably possible to do this, or at least to obtain $N_3(X) = O(X^{1+\varepsilon})$, but since this has been proved (rather easily in fact) by other methods, it seems to be unnecessary work.
Using the above formula, it is natural to want to do two things:

- Compute the constants $C_3(D)$ such that $M_3(D; X) = C_3(D) \cdot X + O(X^{2/3})$ (and similar if $D = -3$).
- Compute exactly $M_3(D; X)$ for reasonable $D$ and large values of $X$.

The constant $C_3(D)$ (for $D \neq -3$) is given by the following formula, where we recall that $D^* = -3D$ if $3 \nmid D$ and $D^* = -D/3$ otherwise:

$$C_3(D) = c_1(D) \text{Res}_{s=1} \prod_{(D^*/p)=1} \left( 1 + \frac{2}{p^s} \right),$$

where $c_1(D) = 11/9, 5/3, 7/5$ for $3 \nmid D$, $D \equiv 3 \pmod{9}$, and $D \equiv 6 \pmod{9}$ respectively, and $\text{Res}_{s=1}$ denotes the residue at 1.
The Cubic Case: Algorithmic Aspects

Using the above formula, it is natural to want to do two things:

• Compute the constants $C_3(D)$ such that $M_3(D; X) = C_3(D) \cdot X + O(X^{2/3})$ (and similar if $D = -3$).

• Compute exactly $M_3(D; X)$ for reasonable $D$ and large values of $X$.

The constant $C_3(D)$ (for $D \neq -3$) is given by the following formula, where we recall that $D^* = -3D$ if $3 \nmid D$ and $D^* = -D/3$ otherwise:

$$C_3(D) = c_1(D) \cdot \text{Res}_{s=1} \prod_{\left(\frac{D^*}{p}\right)=1} \left(1 + \frac{2}{p^s}\right),$$

where $c_1(D) = 11/9, 5/3, 7/5$ for $3 \nmid D$, $D \equiv 3 \pmod{9}$, and $D \equiv 6 \pmod{9}$ respectively, and $\text{Res}_{s=1}$ denotes the residue at 1.
To compute this residue we use a well-known “folklore trick” : let $k' = \mathbb{Q}(\sqrt{D^*})$ be the mirror field of $k = \mathbb{Q}(\sqrt{D})$, and $\zeta_k'(s)$ its Dedekind zeta function. We can write $\zeta_k'(s)/\zeta(2s) = P_1(s)P_0(s)$ with

$$P_1(s) = \prod_{(\frac{D^*}{p})=1} \frac{1 + 1/p^s}{1 - 1/p^s}$$
and
$$P_0(s) = \prod_{p|D^*} (1 + 1/p^s),$$
in other words

$$L(s) := \frac{\zeta_k'(s)}{\zeta(2s)P_0(s)} = \prod_{(\frac{D^*}{p})=1} \frac{1 + 1/p^s}{1 - 1/p^s}. $$

First note that computing numerical values of $L(s)$ (in fact for integer $s \geq 2$ as well as its residue at $s = 1$) is easy : $P_0(s)$ is a finite product, $\zeta(2s)$ is easy (in fact explicit), and $\zeta_k'(s) = \zeta(s)L(\chi_{D^*}, s)$ can also be easily computed, either by elementary means ($\chi$-Euler Mac-Laurin, recall that $D^*$ is not very large), or using the functional equation.
To compute this residue we use a well-known “folklore trick” : let $k' = \mathbb{Q}(\sqrt{D^*})$ be the mirror field of $k = \mathbb{Q}(\sqrt{D})$, and $\zeta_{k'}(s)$ its Dedekind zeta function. We can write $\frac{\zeta_{k'}(s)}{\zeta(2s)} = P_1(s)P_0(s)$ with

$$P_1(s) = \prod_{(D^*/p)=1} \frac{1 + 1/p^s}{1 - 1/p^s} \quad \text{and} \quad P_0(s) = \prod_{p|D^*} (1 + 1/p^s),$$

in other words

$$L(s) := \frac{\zeta_{k'}(s)}{\zeta(2s)P_0(s)} = \prod_{(D^*/p)=1} \frac{1 + 1/p^s}{1 - 1/p^s}. $$

First note that computing numerical values of $L(s)$ (in fact for integer $s \geq 2$ as well as its residue at $s = 1$) is easy : $P_0(s)$ is a finite product, $\zeta(2s)$ is easy (in fact explicit), and $\zeta_{k'}(s) = \zeta(s)L(\chi_{D^*}, s)$ can also be easily computed, either by elementary means ($\chi$-Euler Mac-Laurin, recall that $D^*$ is not very large), or using the functional equation.
Second, note that

\[ L(s) = \prod_{\left(\frac{D^*}{p}\right) = 1} \frac{1 + 1/p^s}{1 - 1/p^s} = \prod_{\left(\frac{D^*}{p}\right) = 1} \left(1 + \frac{2}{p^s} + \cdots\right), \]

so is close to the quantity of which we want to compute the residue. In fact, easy result (this is the first part of the “folklore trick”): we have

\[ \prod_{\left(\frac{D^*}{p}\right) = 1} \left(1 + \frac{2}{p^s}\right) = \prod_{n \geq 1} L(ns)^{a(n)}, \text{ with } a(n) = \frac{1}{n} \sum_{d \mid n, 2 \nmid n/d} \mu(n/d)(-2)^{d-1}. \]

Thus, since \( a(1) = 1 \), the desired residue at \( s = 1 \) is equal to \( \text{Res}_{s=1} L(s) \prod_{n \geq 2} L(n)^{a(n)}. \)

In practice, not used exactly as above, but first compute partial Euler product (say \( p \leq 50 \) or \( p \leq 100 \)), and rest of partial \( L \), so that the convergence of \( \prod_{n \geq 2} L(n)^{a(n)} \) be very fast (this is the second part of the “trick”).
Second, note that

\[
L(s) = \prod_{\left(\frac{D^*}{p}\right) = 1} \frac{1 + 1/p^s}{1 - 1/p^s} = \prod_{\left(\frac{D^*}{p}\right) = 1} \left(1 + \frac{2}{p^s} + \cdots\right),
\]

so is close to the quantity of which we want to compute the residue. In fact, easy result (this is the first part of the “folklore trick”): we have

\[
\prod_{\left(\frac{D^*}{p}\right) = 1} \left(1 + \frac{2}{p^s}\right) = \prod_{n \geq 1} L(ns)^a(n), \text{ with } a(n) = \frac{1}{n} \sum_{d \mid n \atop 2 \nmid n/d} \mu(n/d)(-2)^{d-1}.
\]

Thus, since \(a(1) = 1\), the desired residue at \(s = 1\) is equal to \(\text{Res}_{s=1} L(s) \prod_{n \geq 2} L(n)^{a(n)}\).

In practice, not used exactly as above, but first compute partial Euler product (say \(p \leq 50\) or \(p \leq 100\)), and rest of partial \(L\), so that the convergence of \(\prod_{n \geq 2} L(n)^{a(n)}\) be very fast (this is the second part of the “trick”).
Second, note that

\[ L(s) = \prod_{(D^*_p) = 1} \frac{1 + 1/p^s}{1 - 1/p^s} = \prod_{(D^*_p) = 1} \left( 1 + \frac{2}{p^s} + \cdots \right), \]

so is close to the quantity of which we want to compute the residue. In fact, easy result (this is the first part of the “folklore trick”): we have

\[ \prod_{(D^*_p) = 1} \left( 1 + \frac{2}{p^s} \right) = \prod_{n \geq 1} L(ns)^{a(n)}, \text{ with } a(n) = \frac{1}{n} \sum_{d \mid n, 2 \nmid n/d} \mu(n/d)(-2)^{d-1}. \]

Thus, since \( a(1) = 1 \), the desired residue at \( s = 1 \) is equal to

\[ \text{Res}_{s=1} L(s) \prod_{n \geq 2} L(n)^{a(n)}. \]

In practice, not used exactly as above, but first compute partial Euler product (say \( p \leq 50 \) or \( p \leq 100 \), and rest of partial \( L \), so that the convergence of \( \prod_{n \geq 2} L(n)^{a(n)} \) be very fast (this is the second part of the “trick”).
In seconds, can compute large tables of $C_3(D)$ to hundreds of decimal places if desired. Examples:

\[
\begin{align*}
C_3(-4) &= 0.13621906762412128414498673543420136815 \\
C_3(-15) &= 0.17637191872547206599912366625284592827 \\
C_3(-39) &= 0.21450798544832170587469131992778267288 \\
C_3(5) &= 0.08188400744596363582320375022985579559 \\
C_3(12) &= 0.08038289770565540456224053202127264959 \\
C_3(24) &= 0.08468504275517336717406122046594741323
\end{align*}
\]
We now consider the problem of computing the exact number $M_3(D; X)$ of cubic fields having given quadratic resolvent field of discriminant $D$. This is more subtle.

First assume that we are in the case where the set $\mathcal{L}(D)$ of auxiliary fields in the C.-Thorne theorem is empty, so that we get a formula with no additional term (in fact a consequence of Scholtz, already observed in C.-Morra). This happens exactly when $D < 0$ and $3 \nmid h(D)$, and we then have

$$\Phi_3(D; s) = \frac{1}{2} L_3(s) \prod_{(\frac{-3D}{p})=1} \left(1 + \frac{2}{p^s}\right),$$

where $L_3(s) = 1 + 2/3^{2s}, 1 + 2/3^s, 1 + 2/3^s + 6/3^{2s}$ for $3 \nmid D, D \equiv 3 \pmod{9}, D \equiv 6 \pmod{9}$ respectively, and we recall that $M_3(D; X) + 1/2$ is the summatory function of the Dirichlet series coefficients of $\Phi_3$. 
We now consider the problem of computing the exact number $M_3(D; X)$ of cubic fields having given quadratic resolvent field of discriminant $D$. This is more subtle.

First assume that we are in the case where the set $\mathcal{L}(D)$ of auxiliary fields in the C.-Thorne theorem is empty, so that we get a formula with no additional term (in fact a consequence of Scholtz, already observed in C.-Morra). This happens exactly when $D < 0$ and $3 \nmid h(D)$, and we then have

$$
\Phi_3(D; s) = \frac{1}{2} L_3(s) \prod_{p, \left(\frac{-3D}{p}\right) = 1} \left(1 + \frac{2}{p^s}\right),
$$

where $L_3(s) = 1 + 2/3^{2s}$, $1 + 2/3^s$, $1 + 2/3^s + 6/3^{2s}$ for $3 \nmid D$, $D \equiv 3 \pmod{9}$, $D \equiv 6 \pmod{9}$ respectively, and we recall that $M_3(D; X) + 1/2$ is the summatory function of the Dirichlet series coefficients of $\Phi_3$. 
It is immediate to take care of $L_3(s)$, so must deal with Euler product. Once again, use $\zeta_k'(s)$. Here the folklore trick is of no use to us, but note that

$$
\prod_{\left(\frac{D^*}{p}\right)=1} \left(1 + 2/p^s\right) / \zeta_k'(s) = P_1(s)P_0(s)P_{-1}(s) \quad \text{with}
$$

$$
P_1(s) = \prod_{\left(\frac{D^*}{p}\right)=1} (1 + 2/p^s)(1 - 1/p^s)^{-2},
$$

$$
P_0(s) = \prod_{p|D^*} (1 - 1/p^s),
$$

$$
P_{-1}(s) = \prod_{\left(\frac{D^*}{p}\right)=1} (1 - 1/p^{2s}).
$$
Main point: $P_0(s)$ is a finite Euler product, and $P_1(s)$ and $P_{-1}(s)$ are Euler products of the form $\prod_p (1 + O(1/p^{2s}))$. Thus, can obtain a counting algorithm in $O(X^{1/2})$, details omitted.

Remark: we could include other zeta or $L$ functions so that the Euler products be $\prod_p (1 + O(1/p^{3s}))$, but the extra computation needed for these zeta or $L$ function brings the time again to $O(X^{1/2})$. 
Main point: \( P_0(s) \) is a finite Euler product, and \( P_1(s) \) and \( P_{-1}(s) \) are Euler products of the form \( \prod p (1 + O(1/p^{2s})) \). Thus, can obtain a counting algorithm in \( O(X^{1/2}) \), details omitted.

Remark: we could include other zeta or \( L \) functions so that the Euler products be \( \prod p (1 + O(1/p^{3s})) \), but the extra computation needed for these zeta or \( L \) function brings the time again to \( O(X^{1/2}) \).
The Cubic Case: Computing $M_3(D; X)$ IV

Can compute in minutes $M_3(D; 10^{12})$, and in a few days $M_3(D; 10^{20})$. Examples:

\[
M_3(-4; 10^{19}) = 1362190676241140759 \\
M_3(-15; 10^{19}) = 1763719187254777573 \\
M_3(-39; 10^{19}) = 2145079854482525318 .
\]

Know that $M_3(D; X) = C_3(D) \cdot X + O(X^{2/3})$, $C_3(D)$ computed above. In view of the tables, it seems that the error is closer to $O(X^{1/4+\varepsilon})$ for all $\varepsilon > 0$. 
Can compute in minutes $M_3(D; 10^{12})$, and in a few days $M_3(D; 10^{20})$.

Examples:

\[
M_3(-4; 10^{19}) = 1362190676241140759 \\
M_3(-15; 10^{19}) = 1763719187254777573 \\
M_3(-39; 10^{19}) = 2145079854482525318 .
\]

Know that $M_3(D; X) = C_3(D) \cdot X + O(X^{2/3})$, $C_3(D)$ computed above. In view of the tables, it seems that the error is closer to $O(X^{1/4+\varepsilon})$ for all $\varepsilon > 0$. 
The Cubic Case: Computing $M_3(D; X)$

For the above computation we have assumed that the set $\mathcal{L}(D)$ of auxiliary fields is empty. When this set is nonempty the problem becomes much more difficult. The main term is treated in the same way, but as far as I can see the auxiliary terms cannot. Consider for example the noncyclic cubic field $E$ of smallest absolute discriminant $-23$ defined by $x^3 - x - 1 = 0$ (which in fact does not occur as an auxiliary field, but no matter), and define for any prime $p$, $\omega_E(p) = -1$ if $p$ is inert in $E$, $\omega_E(p) = 2$ if $p$ is totally split, and $\omega_E(p) = 0$ otherwise, and let

$$
\phi_E(s) = \prod_{\left(\frac{-23}{p}\right) = 1} \left(1 + \frac{\omega_E(p)}{p^s}\right) =: \sum_{n \geq 1} \frac{a_E(n)}{n^s}
$$

and $M(E; X) = \sum_{n \leq X} a_E(n)$.

I do not know how to compute $M(E; X)$ faster than $O(X)$. Help?
The Cubic Case: Computing $M_3(D; X)$

For the above computation we have assumed that the set $\mathcal{L}(D)$ of auxiliary fields is empty. When this set is nonempty the problem becomes much more difficult. The main term is treated in the same way, but as far as I can see the auxiliary terms cannot. Consider for example the noncyclic cubic field $E$ of smallest absolute discriminant $-23$ defined by $x^3 - x - 1 = 0$ (which in fact does not occur as an auxiliary field, but no matter), and define for any prime $p$, $\omega_E(p) = -1$ if $p$ is inert in $E$, $\omega_E(p) = 2$ if $p$ is totally split, and $\omega_E(p) = 0$ otherwise, and let

$$\phi_E(s) = \prod_{\left(\frac{-23}{p}\right)=1} \left(1 + \frac{\omega_E(p)}{p^s}\right) =: \sum_{n \geq 1} \frac{a_E(n)}{n^s}$$

and $M(E; X) = \sum_{n \leq X} a_E(n)$.

I do not know how to compute $M(E; X)$ faster than $O(X)$. Help?
The theorem used to prove the emptiness of $\mathcal{L}(D)$ when $D < 0$ and $3 \nmid D$ (C.-Morra) is Scholtz’s reflection theorem (Spiegelungssatz) on the precise link between the 3-ranks of the class groups of $\mathbb{Q}(\sqrt{D})$ and $\mathbb{Q}(\sqrt{-3D})$ (not only an inequality but the condition for equality).

More generally, the main theorem used in Thorne’s theorem given above is the theorem of Nakagawa–Ono on exact identities between class numbers of certain cubic forms, leading to a beautiful functional equation for Shintani’s zeta functions associated to such forms.

The main obstruction to finding a complete analogue of the C.-Thorne theorem for the case of $D_\ell$ fields is the partial lack of such results in that case (see discussion below).
The Cubic Case: Comments

• The theorem used to prove the emptiness of \( \mathcal{L}(D) \) when \( D < 0 \) and \( 3 \nmid D \) (C.-Morra) is Scholtz’s reflection theorem (Spiegelungssatz) on the precise link between the 3-ranks of the class groups of \( \mathbb{Q}(\sqrt{D}) \) and \( \mathbb{Q}(\sqrt{-3D}) \) (not only an inequality but the condition for equality).

• More generally, the main theorem used in Thorne’s theorem given above is the theorem of Nakagawa–Ono on exact identities between class numbers of certain cubic forms, leading to a beautiful functional equation for Shintani’s zeta functions associated to such forms.

• The main obstruction to finding a complete analogue of the C.-Thorne theorem for the case of \( D_\ell \) fields is the partial lack of such results in that case (see discussion below).
Generalizing the cubic case, we now consider degree \( \ell \) extensions with Galois group \( D_\ell \) and given quadratic resolvent \( k \).

The work done in A. Morra’s thesis and in C.-Morra can be generalized to that case, although with some difficulty. We obtain a similar expression now involving sums over characters of \( \mathbb{G}_b = (\text{Cl}_b(L)/\text{Cl}_b(L^\ell))[T] \), where \( L = \mathbb{Q}(\sqrt{D}, \zeta_\ell) \), \( G = \text{Gal}(L/\mathbb{Q}) \cong C_2 \times C_\ell \) or \( G \cong C_\ell \), and \( T \) a similar set of one or two elements in the group ring \( \mathbb{F}_\ell[G] \). In fact, if \( \ell \geq 5 \) (more generally if \( \ell \) is greater than or equal to twice the degree of the base field plus 3) a number of formulas simplify because the ideals which occur in the computations are now coprime to \( \ell \).

In the cubic case, one of the main objects was the “mirror field” \( \mathbb{Q}(\sqrt{-3D}) \). In the \( D_\ell \) case, the mirror field is now cyclic of degree \( \ell - 1 \), equal to \( k' = \mathbb{Q}(\sqrt{D}(\zeta_\ell - \zeta_\ell^{-1})) \).
Generalizing the cubic case, we now consider degree \( \ell \) extensions with Galois group \( D_\ell \) and given quadratic resolvent \( k \).
The work done in A. Morra’s thesis and in C.-Morra can be generalized to that case, although with some difficulty. We obtain a similar expression now involving sums over characters of \( G_b = (Cl_b(L)/Cl_b(L)^\ell)[T] \), where \( L = \mathbb{Q}((\sqrt{D}, \zeta_\ell)) \), \( G = \text{Gal}(L/\mathbb{Q}) \simeq C_2 \times C_\ell \) or \( G \simeq C_\ell \), and \( T \) a similar set of one or two elements in the group ring \( \mathbb{F}_\ell[G] \). In fact, if \( \ell \geq 5 \) (more generally if \( \ell \) is greater than or equal to twice the degree of the base field plus 3) a number of formulas simplify because the ideals which occur in the computations are now coprime to \( \ell \).

In the cubic case, one of the main objects was the “mirror field” \( \mathbb{Q}(\sqrt{-3D}) \). In the \( D_\ell \) case, the mirror field is now cyclic of degree \( \ell - 1 \), equal to \( k' = \mathbb{Q}(\sqrt{D}(\zeta_\ell - \zeta_\ell^{-1})) \).
Thus once again we have an “explicit” formula for $\Phi_\ell(D; s)$ involving characters of ray class groups, and we can at least deduce, as in the cubic case, that the counting function $M_\ell(D; X)$ satisfies

$$M_\ell(D; X) = C_\ell(D) \cdot X + O(X^{1-1/\ell})$$

with the exception of $\ell \equiv 3 \pmod{4}$ and $D = -\ell$, where

$$M_\ell(D; X) = C_\ell(D)(X \log(X) + C_\ell'(D)) + O(X^{1-1/\ell}) .$$

It is now possible to generalize part of one of Thorne’s theorem: the bijection will now be between a Galois orbit of characters of order $\ell$ $(\chi, \ldots, \chi^{\ell-1})$ and a field of degree $\ell$ whose Galois closure is the semi-direct product of $(\mathbb{Z}/\ell\mathbb{Z})^*$ with $C_\ell$. 
Thus once again we have an “explicit” formula for $\Phi_\ell(D; s)$ involving characters of ray class groups, and we can at least deduce, as in the cubic case, that the counting function $M_\ell(D; X)$ satisfies

$$M_\ell(D; X) = C_\ell(D) \cdot X + O(X^{1-1/\ell}),$$

with the exception of $\ell \equiv 3 \pmod{4}$ and $D = -\ell$, where

$$M_\ell(D; X) = C_\ell(D)(X \log(X) + C'_\ell(D)) + O(X^{1-1/\ell}).$$

It is now possible to generalize part of one of Thorne’s theorem: the bijection will now be between a Galois orbit of characters of order $\ell$ ($\chi, \ldots, \chi^{\ell-1}$) and a field of degree $\ell$ whose Galois closure is the semi-direct product of $(\mathbb{Z}/\ell\mathbb{Z})^*$ with $C_\ell$. 
What is now lacking are two related things:

- A generalization of Scholtz’s mirror theorem to the mirror field $k'$ of degree $\ell - 1$ given above. Even though such exist in the literature (work of G. Gras in JTNB), they are not sufficiently precise to be useful. For $\ell = 5$, a result of Y. Kishi (2005) gives such a precise result, so should be able to solve completely that case.

- A generalization of Nakagawa-Ono’s theorem. This seems both much more important and more difficult, but considering the perfect analogy with the cubic case, it should exist. Would have consequences on the $\ell$-rank of Selmer groups of elliptic curves.
What is now lacking are two related things:

- A generalization of Scholtz’s mirror theorem to the mirror field $k'$ of degree $\ell - 1$ given above. Even though such exist in the literature (work of G. Gras in JTNB), they are not sufficiently precise to be useful. For $\ell = 5$, a result of Y. Kishi (2005) gives such a precise result, so should be able to solve completely that case.

- A generalization of Nakagawa-Ono’s theorem. This seems both much more important and more difficult, but considering the perfect analogy with the cubic case, it should exist. Would have consequences on the $\ell$-rank of Selmer groups of elliptic curves.
The quadratic resolvent $k$ of a degree $\ell$ number field with Galois group $D_\ell$ is sometimes a subfield of $\mathbb{Q}(\zeta_\ell)$, i.e., equal to $k = \mathbb{Q}(\sqrt{\ell^*})$ with $\ell^* = (-1)^{(\ell-1)/2} \ell$. For $\ell = 3$ these are pure cubic fields. What are these fields for higher $\ell$, for instance $\ell = 5$? Are they defined by simple polynomial equations?

Here we find a marked difference between $\ell \equiv 1 \pmod{4}$ ($k$ real) and $\ell \equiv 3 \pmod{4}$ ($k$ complex). In particular as mentioned:

- For $\ell \equiv 1 \pmod{4}$, formula more complicated, and the number $M_\ell(k; X)$ of such fields with $f(K) \leq X$ satisfies
  $$M_\ell(k; X) = C_\ell \cdot X + O(X^{1-1/\ell}).$$

- For $\ell \equiv 3 \pmod{4}$, conjecturally simplest possible formula (need Scholtz), proved by computer for $\ell \leq 43$, and as mentioned above
  $$M_\ell(k; X) = C_\ell \cdot (X \log(X) + C'_\ell \cdot X) + O(X^{1-1/\ell}).$$
The quadratic resolvent $k$ of a degree $\ell$ number field with Galois group $D_\ell$ is sometimes a subfield of $\Bbb Q(\zeta_\ell)$, i.e., equal to $k = \Bbb Q(\sqrt{\ell^*})$ with $\ell^* = (-1)^{(\ell-1)/2}\ell$. For $\ell = 3$ these are pure cubic fields. What are these fields for higher $\ell$, for instance $\ell = 5$? Are they defined by simple polynomial equations?

Here we find a marked difference between $\ell \equiv 1 \pmod{4}$ ($k$ real) and $\ell \equiv 3 \pmod{4}$ ($k$ complex). In particular as mentioned:

- For $\ell \equiv 1 \pmod{4}$, formula more complicated, and the number $M_\ell(k; X)$ of such fields with $f(K) \leq X$ satisfies
  $$M_\ell(k; X) = C_\ell \cdot X + O(X^{1-1/\ell}).$$

- For $\ell \equiv 3 \pmod{4}$, conjecturally simplest possible formula (need Scholtz), proved by computer for $\ell \leq 43$, and as mentioned above
  $$M_\ell(k; X) = C_\ell \cdot (X \log(X) + C'_\ell \cdot X) + O(X^{1-1/\ell}).$$
The $D_\ell$ Case IV

The quadratic resolvent $k$ of a degree $\ell$ number field with Galois group $D_\ell$ is sometimes a subfield of $\mathbb{Q}(\zeta_\ell)$, i.e., equal to $k = \mathbb{Q}(\sqrt{\ell^*})$ with $\ell^* = (-1)^{(\ell-1)/2}$. For $\ell = 3$ these are pure cubic fields. What are these fields for higher $\ell$, for instance $\ell = 5$? Are they defined by simple polynomial equations?

Here we find a marked difference between $\ell \equiv 1 \pmod{4}$ ($k$ real) and $\ell \equiv 3 \pmod{4}$ ($k$ complex). In particular as mentioned:

- For $\ell \equiv 1 \pmod{4}$, formula more complicated, and the number $M_\ell(k; X)$ of such fields with $f(K) \leq X$ satisfies $M_\ell(k; X) = C_\ell \cdot X + O(X^{1-1/\ell})$.

- For $\ell \equiv 3 \pmod{4}$, conjecturally simplest possible formula (need Scholtz), proved by computer for $\ell \leq 43$, and as mentioned above $M_\ell(k; X) = C_\ell \cdot (X \log(X) + C'_\ell \cdot X) + O(X^{1-1/\ell})$. 
Once again, we want to compute both the constants $C_\ell(D)$, and the exact value of $M_\ell(k; X)$.

The computation of $C_\ell(D)$ is done using methods similar to, but more complicated than the case $\ell = 3$. In particular, we must replace the function $\zeta_{k'}(s)/\zeta(2s)$ used in that case, by $\prod_{d|\ell-1} \zeta_{k'_d}(ds)\mu(d)$, where $k'_d$ is the unique subfield of $k'$ such that $[k' : k'_d] = d$. Again in seconds we obtain large tables to hundreds of decimals, most of the time being spent in writing a bug-free program!
Once again, we want to compute both the constants \( C_\ell(D) \), and the exact value of \( M_\ell(k; X) \).

The computation of \( C_\ell(D) \) is done using methods similar to, but more complicated than the case \( \ell = 3 \). In particular, we must replace the function \( \zeta_{k'}(s)/\zeta(2s) \) used in that case, by \( \prod_{d | (\ell - 1)} \zeta_{k'_d}(ds)^{\mu(d)} \), where \( k'_d \) is the unique subfield of \( k' \) such that \( [k' : k'_d] = d \). Again in seconds we obtain large tables to hundreds of decimals, most of the time being spent in writing a bug-free program!
The computation of $M_{\ell}(k; X)$ is once again more difficult. We first have a conjecture, which is a generalization to $D_{\ell}$ of the theorem of C.-Morra:

**Conjecture**: If $D < 0$ and $\ell \nmid h(D)$, the groups $G_b$ are all trivial. Should be true in particular for $D = -\ell$ when $\ell \equiv 3 \pmod{4}$.

Since for $\ell = 3$ this is a consequence of Scholtz, need a precise generalization. Of course, for any individual $D$, can be proved on a computer, so not conjectural. Tested for thousands of $(\ell, D)$, and for $D = -\ell$, $\ell \equiv 3 \pmod{4}$, $\ell < 60$. 
When this is satisfied, again simple formula for \( \Phi_\ell(D; s) \):

\[
\Phi_\ell(D; s) = \frac{1}{\ell - 1} L_\ell(s) \prod_{p \equiv D \equiv \pm 1 (\text{mod } \ell)} \left( 1 + \frac{\ell - 1}{p^s} \right),
\]

with \( L_\ell(s) = 1 + (\ell - 1)/\ell^{2s} \) if \( \ell \nmid D \) and \( L_\ell(s) = 1 + (\ell - 1)/\ell^s \) if \( \ell \mid D \) (for \( \ell \geq 5 \)).

Use same tricks as before to reduce to the computation of the summatory function of \( \zeta_{k'}(s) \). Note \( k' \) cyclic of degree \( \ell - 1 \).

Special and simpler case: \( k' = \mathbb{Q}(\zeta_\ell) \). We have

\[
\zeta_{k'}(s) = \prod_{0 \leq j < \ell - 1} L(\omega^j, s) := \sum_{n \geq 1} a(n)/n^s,
\]

where \( \omega \) generator of group of Dirichlet characters modulo \( \ell \). If \( M(X) = \sum_{n \leq X} a(n) \), how to compute \( M(X) \) ?

Using recursively the method of the hyperbola, can compute in \( O(X^{1-1/(\ell-1)}) \) (e.g., \( O(X^{1/2}) \) for \( \ell = 3 \), \( O(X^{3/4}) \) for \( \ell = 5 \)). Help?
When this is satisfied, again simple formula for \( \Phi_\ell(D; s) \):

\[
\Phi_\ell(D; s) = \frac{1}{\ell - 1} L_\ell(s) \prod_{p \equiv (D/p) \equiv \pm 1 \pmod{\ell}} \left(1 + \frac{\ell - 1}{p^s}\right),
\]

with \( L_\ell(s) = 1 + (\ell - 1)/\ell^{2s} \) if \( \ell \nmid D \) and \( L_\ell(s) = 1 + (\ell - 1)/\ell^s \) if \( \ell \mid D \) (for \( \ell \geq 5 \)).

Use same tricks as before to reduce to the computation of the summatory function of \( \zeta_{k'}(s) \). Note \( k' \) cyclic of degree \( \ell - 1 \).

Special and simpler case : \( k' = \mathbb{Q}(\zeta_\ell) \). We have

\[
\zeta_{k'}(s) = \prod_{0 \leq j < \ell - 1} L(\omega^j, s) := \sum_{n \geq 1} a(n)/n^s,
\]

where \( \omega \) generator of group of Dirichlet characters modulo \( \ell \). If \( M(X) = \sum_{n \leq X} a(n) \), how to compute \( M(X) \)?

Using recursively the method of the hyperbola, can compute in \( O(X^{1-1/(\ell-1)}) \) (e.g., \( O(X^{1/2}) \) for \( \ell = 3 \), \( O(X^{3/4}) \) for \( \ell = 5 \)). Help?
When this is satisfied, again simple formula for $\Phi_\ell(D; s)$:

$$\Phi_\ell(D; s) = \frac{1}{\ell - 1} L_\ell(s) \prod_{\substack{p \equiv (D/p) \equiv \pm 1 \pmod{\ell} }} \left( 1 + \frac{\ell - 1}{p^s} \right),$$

with $L_\ell(s) = 1 + (\ell - 1)/\ell^{2s}$ if $\ell \nmid D$ and $L_\ell(s) = 1 + (\ell - 1)/\ell^s$ if $\ell \mid D$ (for $\ell \geq 5$).

Use same tricks as before to reduce to the computation of the summatory function of $\zeta_{k'}(s)$. Note $k'$ cyclic of degree $\ell - 1$.

Special and simpler case: $k' = \mathbb{Q}(\zeta_\ell)$. We have

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

where $\omega$ generator of group of Dirichlet characters modulo $\ell$. If $M(X) = \sum_{n \leq X} a(n)$, how to compute $M(X)$?

Using recursively the method of the hyperbola, can compute in $O(X^{\frac{1-1}{\ell-1}})$ (e.g., $O(X^{1/2})$ for $\ell = 3$, $O(X^{3/4})$ for $\ell = 5$). Help?
When this is satisfied, again simple formula for $\Phi_\ell(D; s)$:

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

with $L_\ell(s) = 1 + (\ell - 1)/\ell^{2s}$ if $\ell \nmid D$ and $L_\ell(s) = 1 + (\ell - 1)/\ell^s$ if $\ell \mid D$ (for $\ell \geq 5$).

Use same tricks as before to reduce to the computation of the sumatory function of $\zeta_{k'}(s)$. Note $k'$ cyclic of degree $\ell - 1$.

Special and simpler case : $k' = \mathbb{Q}(\zeta_\ell)$. We have

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

where $\omega$ generator of group of Dirichlet characters modulo $\ell$. If $M(X) = \sum_{n \leq X} a(n)$, how to compute $M(X)$?

Using recursively the method of the hyperbola, can compute in $O(X^{1-1/(\ell-1)})$ (e.g., $O(X^{1/2})$ for $\ell = 3$, $O(X^{3/4})$ for $\ell = 5$). Help?
Can compute in a few days $M_5(D; 10^{13})$ or $M_7(D; 10^{11})$. Examples:

$$M_5(-3; 10^{12}) = 50785334021 \quad M_5(-15; 10^{12}) = 78804743357$$

$$M_7(-3; 10^{10}) = 296332445 \quad M_7(-35; 10^{10}) = 530024447$$

Although the proven error is $O(X^{1-1/\ell})$, in view of the tables, a rather bold guess would give $O(X^{(\ell-2)/(2(\ell-1))} + \varepsilon)$. 
Can compute in a few days $M_5(D; 10^{13})$ or $M_7(D; 10^{11})$. Examples:

$$M_5(-3; 10^{12}) = 50785334021 \quad M_5(-15; 10^{12}) = 78804743357$$

$$M_7(-3; 10^{10}) = 296332445 \quad M_7(-35; 10^{10}) = 530024447$$

Although the proven error is $O(\lambda^{1-1/\ell})$, in view of the tables, a rather bold guess would give $O(\lambda^{(\ell-2)/(2(\ell-1)) + \varepsilon})$. 
The “special case” is when $D = \ell^* = (-1)^{(\ell-1)/2} \ell$, which must be treated a little differently. When $\ell \equiv 3 \pmod{4}$, conjecturally simplest formula (true for $\ell < 60$) for instance

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

Recall that $M_7(-7; X)$ is now asymptotic to $C_7(-7) \cdot X \log(X)$ (with $C_7(-7) = 0.01210526342145122980185788033$). Leads for instance to

$$
M_7(-7; 10^{10}) = 3342900105
$$
The “special case” is when $D = \ell^* = (-1)^{(\ell-1)/2} \ell$, which must be treated a little differently. When $\ell \equiv 3 \pmod{4}$, conjecturally simplest formula (true for $\ell < 60$) for instance

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

Recall that $M_7(-7; X)$ is now asymptotic to $C_7(-7) \cdot X \log(X)$ (with $C_7(-7) = 0.01210526342145122980185788033$). Leads for instance to

$$M_7(-7; 10^{10}) = 3342900105$$
When $\ell \equiv 1 \pmod{4}$, additional terms. For instance:

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

where $E$ is the quintic field of discriminant $5^7$ with Galois group $C_4 \rtimes C_5$ defined by $x^5 + 5x^3 + 5x - 1 = 0$, and $\omega_E(p) = -1$ if $p = 5$ or $p$ is inert in $E$, $\omega_E(p) = 4$ if $p$ is totally split in $E$, and $\omega_E(p) = 0$ otherwise.

Interestingly, the condition that $p$ is totally split is equivalent to $\varepsilon = (-1 + \sqrt{5})/2$ being a fifth power modulo $p$ ($\varepsilon^{(p-1)/5} \equiv 1 \pmod{p}$), which is faster to test.

Still does not seem to be reducible to an Abelian computation, so time $O(X)$ instead of $O(X^{3/4})$. Help? Example:

$$M_5(5; 10^{10}) = 203782163$$
When \( \ell \equiv 1 \pmod{4} \), additional terms. For instance:

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

where \( E \) is the quintic field of discriminant \( 5^7 \) with Galois group \( C_4 \times C_5 \) defined by \( x^5 + 5x^3 + 5x - 1 = 0 \), and \( \omega_E(p) = -1 \) if \( p = 5 \) or \( p \) is inert in \( E \), \( \omega_E(p) = 4 \) if \( p \) is totally split in \( E \), and \( \omega_E(p) = 0 \) otherwise.

Interestingly, the condition that \( p \) is totally split is equivalent to \( \varepsilon = (-1 + \sqrt{5})/2 \) being a fifth power modulo \( p \) \( (\varepsilon(p-1)/5 \equiv 1 \pmod{p}) \), which is faster to test.

Still does not seem to be reducible to an Abelian computation, so time \( O(X) \) instead of \( O(X^{3/4}) \). Help? Example:

\[
M_5(5; 10^{10}) = 203782163
\]
When \( \ell \equiv 1 \pmod{4} \), additional terms. For instance:

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

where \( E \) is the quintic field of discriminant 57 with Galois group \( C_4 \rtimes C_5 \) defined by \( x^5 + 5x^3 + 5x - 1 = 0 \), and \( \omega_E(p) = -1 \) if \( p = 5 \) or \( p \) is inert in \( E \), \( \omega_E(p) = 4 \) if \( p \) is totally split in \( E \), and \( \omega_E(p) = 0 \) otherwise.

Interestingly, the condition that \( p \) is totally split is equivalent to \( \varepsilon = (-1 + \sqrt{5})/2 \) being a fifth power modulo \( p \) \( (\varepsilon^{(p-1)/5} \equiv 1 \pmod{p}) \), which is faster to test.

Still does not seem to be reducible to an Abelian computation, so time \( O(X) \) instead of \( O(X^{3/4}) \). Help? Example:

\[
M_5(5; 10^{10}) = 203782163
\]
The Quartic $A_4$ and $S_4$-Case: Introduction

Let $K$ be a quartic field, $\tilde{K}$ its Galois closure, assume $\text{Gal}(\tilde{K}/\mathbb{Q}) \cong A_4$ or $S_4$. There exists a cubic subfield $k$ of $\tilde{K}$, unique up to conjugation, the resolvent cubic. In the same way, we want to compute explicitly $\Phi_4(k; s)$ (if $\text{Gal}(\tilde{K}/\mathbb{Q})$ not $A_4$ or $S_4$, different and simpler). Here Kummer theory much simpler since no roots of unity to adjoin.

But $S_4$ more complicated group: we will need to distinguish between a great number of possible splittings of the prime $2$ (more than 20). We first give the result, and then an indication of the (much more complicated) proof. Very similar to the cubic case: Need to define $\omega_E(p)$, and a set $\mathcal{L}(k)$ of quartic fields, but also $s_k(p)$ for a cubic field $k$. 
Let $K$ be a quartic field, $\tilde{K}$ its Galois closure, assume $\text{Gal}(\tilde{K}/\mathbb{Q}) \cong A_4$ or $S_4$. There exists a cubic subfield $k$ of $\tilde{K}$, unique up to conjugation, the resolvent cubic. In the same way, we want to compute explicitly $\Phi_4(k; s)$ (if $\text{Gal}(\tilde{K}/\mathbb{Q})$ not $A_4$ or $S_4$, different and simpler). Here Kummer theory much simpler since no roots of unity to adjoin.

But $S_4$ more complicated group : we will need to distinguish between a great number of possible splittings of the prime 2 (more than 20). We first give the result, and then an indication of the (much more complicated) proof. Very similar to the cubic case : Need to define $\omega_E(p)$, and a set $\mathcal{L}(k)$ of quartic fields, but also $s_k(p)$ for a cubic field $k$. 
Let $p$ be a prime number.

- If $k$ is a cubic field, we set

$$s_k(p) = \begin{cases} 
1 & \text{if } p \text{ is } (21) \text{ or } (1^21) \text{ in } k, \\
3 & \text{if } p \text{ is } (111) \text{ in } k, \\
0 & \text{otherwise.}
\end{cases}$$

- If $E$ is a quartic field, we set

$$\omega_E(p) = \begin{cases} 
-1 & \text{if } p \text{ is } (4), (22), (21^2) \text{ in } E \\
1 & \text{if } p \text{ is } (211), (1^211) \text{ in } E \\
3 & \text{if } p \text{ is } (1111) \text{ in } E \\
0 & \text{otherwise.}
\end{cases}$$

(Splitting notation self-explanatory.)
Let $k$ be a cubic field.

- $\mathcal{L}_{k,n^2}$: quartic fields with cubic resolvent $k$ and discriminant $n^2 \text{disc}(k)$, in addition totally real if $k$ is totally real.

- $\mathcal{L}(k) = \mathcal{L}_{k,1} \cup \mathcal{L}_{k,4} \cup \mathcal{L}_{k,16} \cup \mathcal{L}_{k,64,\text{tr}}$, where the index $\text{tr}$ means that 2 must be totally ramified.

Theorem (Thorne, C.)

Let $k$ be a cubic field, $r_2(k)$ number of complex places, $a(k) = |\text{Aut}(k)|$ (3 for $k$ cyclic, 1 otherwise). We have

$$2^{r_2(k)} \Phi_4(k; s) = \frac{1}{a(k)} M_1(s) \prod_{p \neq 2} \left( 1 + \frac{s_k(p)}{p^s} \right)$$

$$+ \sum_{E \in \mathcal{L}(k)} M_{2,E}(s) \prod_{p \neq 2} \left( 1 + \frac{\omega_E(p)}{p^s} \right),$$
Let \( k \) be a cubic field.

- \( \mathcal{L}_{k,n^2} \): quartic fields with cubic resolvent \( k \) and discriminant \( n^2 \text{disc}(k) \), in addition totally real if \( k \) is totally real.

- \( \mathcal{L}(k) = \mathcal{L}_{k,1} \cup \mathcal{L}_{k,4} \cup \mathcal{L}_{k,16} \cup \mathcal{L}_{k,64,\text{tr}} \), where the index \( \text{tr} \) means that 2 must be totally ramified.

**Theorem (Thorne, C.)**

*Let \( k \) be a cubic field, \( r_2(k) \) number of complex places, \( a(k) = |\text{Aut}(k)| \) (3 for \( k \) cyclic, 1 otherwise). We have*

\[
2^{r_2(k)} \Phi_4(k; s) = \frac{1}{a(k)} M_1(s) \prod_{p \neq 2} \left( 1 + \frac{s_k(p)}{p^s} \right) + \sum_{E \in \mathcal{L}(k)} M_{2,E}(s) \prod_{p \neq 2} \left( 1 + \frac{\omega_E(p)}{p^s} \right),
\]
The Quartic $A_4$ and $S_4$-Case: The Theorem II

where $M_1(s)$ and $M_{2,E}(s)$ are Euler factors at 2 which are polynomials of degree less than or equal to 4 in $1/2^s$; 6 splitting types for $M_1(s)$, and 23 types for $M_{2,E}(s)$:

<table>
<thead>
<tr>
<th>$k$-split</th>
<th>$M_1(s)$</th>
<th>$8M_1(1)$</th>
</tr>
</thead>
<tbody>
<tr>
<td>(3)</td>
<td>$1 + 3/2^{3s}$</td>
<td>11</td>
</tr>
<tr>
<td>(21)</td>
<td>$1 + 1/2^{2s} + 4/2^{3s} + 2/2^{4s}$</td>
<td>15</td>
</tr>
<tr>
<td>(111)</td>
<td>$1 + 3/2^{2s} + 6/2^{3s} + 6/2^{4s}$</td>
<td>23</td>
</tr>
<tr>
<td>$(1^21)_0$</td>
<td>$1 + 1/2^{s} + 2/2^{3s} + 4/2^{4s}$</td>
<td>16</td>
</tr>
<tr>
<td>$(1^21)_4$</td>
<td>$1 + 1/2^{s} + 2/2^{2s} + 4/2^{4s}$</td>
<td>18</td>
</tr>
<tr>
<td>$(1^3)$</td>
<td>$1 + 1/2^{s} + 2/2^{3s}$</td>
<td>14</td>
</tr>
</tbody>
</table>

(Index 0 or 4 indicates discriminant modulo 8).
### The Quartic $A_4$ and $S_4$-Case: The Theorem III

<table>
<thead>
<tr>
<th>$k$-split</th>
<th>$E$-split</th>
<th>$n^2$</th>
<th>$M_{2,E}(s)$, $E \in \mathcal{L}_{k,n^2}$</th>
<th>$k$-split</th>
<th>$E$-split</th>
<th>$n^2$</th>
<th>$M_{2,E}(s)$, $E \in \mathcal{L}_{k,n^2}$</th>
</tr>
</thead>
<tbody>
<tr>
<td>(3)</td>
<td>(31)</td>
<td>1</td>
<td>$1 + 3/2^{3s}$</td>
<td>(1^2 1)_0</td>
<td>(21)</td>
<td>1</td>
<td>$1 + 1/2^s + 2/2^{3s} - 4/2^{4s}$</td>
</tr>
<tr>
<td>(3)</td>
<td>(1^4)</td>
<td>64</td>
<td>$1 - 1/2^{3s}$</td>
<td>(1^2 1)_0</td>
<td>(1^2 11)</td>
<td>1</td>
<td>$1 + 1/2^s + 2/2^{3s} + 4/2^{4s}$</td>
</tr>
<tr>
<td>(21)</td>
<td>(4)</td>
<td>1</td>
<td>$1 + 1/2^{2s} - 2/2^{4s}$</td>
<td>(1^2 1)_0</td>
<td>(1^2 1^2)</td>
<td>4</td>
<td>$1 + 1/2^s - 2/2^{3s}$</td>
</tr>
<tr>
<td>(21)</td>
<td>(211)</td>
<td>1</td>
<td>$1 + 1/2^{2s} + 4/2^{3s} + 2/2^{4s}$</td>
<td>(1^2 1)_0</td>
<td>(1^2 1^1)</td>
<td>1</td>
<td>$1 + 1/2^s + 2/2^{3s} - 4/2^{4s}$</td>
</tr>
<tr>
<td>(21)</td>
<td>(2^2)</td>
<td>16</td>
<td>$1 + 1/2^{2s} - 4/2^{3s} + 2/2^{4s}$</td>
<td>(1^2 1^4)</td>
<td>(2^1)</td>
<td>4</td>
<td>$1 + 1/2^s - 2/2^{2s}$</td>
</tr>
<tr>
<td>(21)</td>
<td>(1^2 1^2)</td>
<td>16</td>
<td>$1 + 1/2^{2s} - 2/2^{4s}$</td>
<td>(1^2 1^4)</td>
<td>(1^2 11)</td>
<td>4</td>
<td>$1 + 1/2^s + 2/2^{3s} + 4/2^{4s}$</td>
</tr>
<tr>
<td>(21)</td>
<td>(4)</td>
<td>64</td>
<td>$1 - 1/2^{2s}$</td>
<td>(1^2 1^4)</td>
<td>(2^1)</td>
<td>16</td>
<td>$1 + 1/2^s - 2/2^{2s}$</td>
</tr>
<tr>
<td>(1^1 1)</td>
<td>(2^2)</td>
<td>16</td>
<td>$1 - 1/2^{2s} - 2/2^{3s} + 2/2^{4s}$</td>
<td>(1^2 1^4)</td>
<td>(1^2 1^2)</td>
<td>16</td>
<td>$1 + 1/2^s - 2/2^{3s}$</td>
</tr>
<tr>
<td>(1^1 1)</td>
<td>(1^2 1^2)</td>
<td>16</td>
<td>$1 + 3/2^{2s} + 6/2^{3s} + 6/2^{4s}$</td>
<td>(1^3)</td>
<td>(1^3 1)</td>
<td>1</td>
<td>$1 + 1/2^s + 2/2^{3s}$</td>
</tr>
<tr>
<td>(1^1 1)</td>
<td>(1^2 1^2)</td>
<td>16</td>
<td>$1 - 1/2^{2s} + 2/2^{3s} - 2/2^{4s}$</td>
<td>(1^3)</td>
<td>(1^4)</td>
<td>4</td>
<td>$1 + 1/2^s - 2/2^{3s}$</td>
</tr>
</tbody>
</table>
The Quartic $A_4$ Case : Example

We give three examples: one in the much simpler $A_4$ case, two in the $S_4$ case.

Let $k$ be the cyclic cubic field of discriminant 49 defined by $x^3 - x^2 - 2x + 1 = 0$. We have

$$\Phi_4(k; s) = \frac{1}{3} \left( 1 + \frac{3}{2^3 s} \right) \prod_{p \equiv \pm 1 \pmod{14}} \left( 1 + \frac{3}{p^s} \right)$$

Note that since we are in an abelian situation, the splitting of $p$ is equivalent to congruences.

Thus

$$\Phi_4(k; s) = \frac{1}{3} + \frac{1}{8^s} + \frac{1}{13^s} + \frac{1}{29^s} + \frac{1}{41^s} + \frac{1}{43^s} + \frac{1}{71^s} + \frac{1}{83^s} + \frac{1}{97^s} + \frac{3}{104^s} + \cdots,$$

where $a/f^s$ means that there are $a$ quartic $A_4$-fields of discriminant $49 \cdot f^2$. 
We give three examples: one in the much simpler $A_4$ case, two in the $S_4$ case. Let $k$ be the cyclic cubic field of discriminant 49 defined by $x^3 - x^2 - 2x + 1 = 0$. We have

$$
\Phi_4(k; s) = \frac{1}{3} \left( 1 + \frac{3}{2^{3s}} \right) \prod_{p\equiv\pm1 \pmod{14}} \left( 1 + \frac{3}{p^s} \right)
$$

Note that since we are in an abelian situation, the splitting of $p$ is equivalent to congruences. Thus

$$
\Phi_4(k; s) = \frac{1}{3} + \frac{1}{8^s} + \frac{1}{13^s} + \frac{1}{29^s} + \frac{1}{41^s} + \frac{1}{43^s} + \frac{1}{71^s} + \frac{1}{83^s} + \frac{1}{97^s} + \frac{3}{104^s} + \cdots,
$$

where $a/f^s$ means that there are $a$ quartic $A_4$-fields of discriminant $49 \cdot f^2$. 
Let $k$ be the noncyclic totally real cubic of discriminant 148 defined by $x^3 - x^2 - 3x + 1 = 0$. Then

$$
\Phi_4(k; s) = \left(1 + \frac{1}{2^s} + \frac{2}{2^{3s}}\right) \prod_{p \neq 2} \left(1 + \frac{s_k(p)}{p^s}\right).
$$

Let $k$ be the noncyclic totally real cubic of discriminant 229 defined by $x^3 - 4x - 1 = 0$. Then

$$
\Phi_4(k; s) = \left(1 + \frac{1}{2^{2s}} + \frac{4}{2^{3s}} + \frac{2}{2^{4s}}\right) \prod_{p \neq 2} \left(1 + \frac{s_k(p)}{p^s}\right)
+ \left(1 - \frac{1}{2^{2s}}\right) \prod_p \left(1 + \frac{\omega_E(p)}{p^s}\right),
$$

where $E$ is the $S_4$-quartic field of discriminant 64 · 229 defined by $x^4 - 2x^3 - 4x^2 + 4x + 2 = 0$. 
Comments essentially identical to the cubic case: the number of necessary auxiliary quartic fields $|\mathcal{L}(k)|$ is equal to

$$2^{rk_2(Cl_4(k))} - 1,$$

where $rk_2$ is the 2-rank and $Cl_4(k)$ the ray class group of conductor 4. We do not know how to control this well.

In fact, it is widely conjectured that $N_4(A_4; X) \sim c \cdot X^{1/2} \log X$, but the above does not allow to obtain any nontrivial result (best known, using in fact elementary methods, is $O(X^{3/4+\varepsilon})$).

On the other hand computing the number $N_4(k; X)$ of quartic fields having a given cubic resolvent $k$ and absolute discriminant up to $X$ can again be done very fast using the theorem and standard techniques of analytic number theory.
The Quartic $A_4$ and $S_4$ Cases: Comments

Comments essentially identical to the cubic case: the number of necessary auxiliary quartic fields $|\mathcal{L}(k)|$ is equal to

$$2^{\text{rk}_2(\text{Cl}_4(k))} - 1,$$

where $\text{rk}_2$ is the 2-rank and $\text{Cl}_4(k)$ the ray class group of conductor 4. We do not know how to control this well.

In fact, it is widely conjectured that $N_4(A_4; X) \sim c \cdot X^{1/2} \log X$, but the above does not allow to obtain any nontrivial result (best known, using in fact elementary methods, is $O(X^{3/4+\varepsilon})$).

On the other hand computing the number $N_4(k; X)$ of quartic fields having a given cubic resolvent $k$ and absolute discriminant up to $X$ can again be done very fast using the theorem and standard techniques of analytic number theory.
Comments essentially identical to the cubic case: the number of necessary auxiliary quartic fields $|\mathcal{L}(k)|$ is equal to

$$2^{rk_2(\text{Cl}_4(k))} - 1,$$

where $rk_2$ is the 2-rank and $\text{Cl}_4(k)$ the ray class group of conductor 4. We do not know how to control this well.

In fact, it is widely conjectured that $N_4(A_4; X) \sim c \cdot X^{1/2} \log X$, but the above does not allow to obtain any nontrivial result (best known, using in fact elementary methods, is $O(X^{3/4+\varepsilon})$).

On the other hand computing the number $N_4(k; X)$ of quartic fields having a given cubic resolvent $k$ and absolute discriminant up to $X$ can again be done very fast using the theorem and standard techniques of analytic number theory.
Completely analogous to the cubic or $D_ℓ$ case: need to compute constants $C(k)$ entering in the asymptotics $M(k; X) \sim C(k) \cdot X$, and to compute $M(k; X)$ exactly. For the computation of $C(k)$ we use the same “folklore trick”: in particular we need to compute numerical values of the Dedekind zeta function $ζ_k(s)$ at positive integers as well as its residue at 1.

This is very easy if $k$ is cyclic (the $A_4$ case), and not too difficult (using the approximate functional equation) if not since $k$ is a cubic field. This has been done and published 10 years ago.
Completely analogous to the cubic or $D_ℓ$ case: need to compute constants $C(k)$ entering in the asymptotics $M(k; X) \sim C(k) \cdot X$, and to compute $M(k; X)$ exactly. For the computation of $C(k)$ we use the same “folklore trick”: in particular we need to compute numerical values of the Dedekind zeta function $ζ_k(s)$ at positive integers as well as its residue at 1.

This is very easy if $k$ is cyclic (the $A_4$ case), and not too difficult (using the approximate functional equation) if not since $k$ is a cubic field. This has been done and published 10 years ago.
Computing $M(k; X)$ is relatively easy only in the $A_4$ case when $\mathcal{L}(k) = \emptyset$: using the same methods we are reduced to the computation of the summatory function of the coefficients of $\zeta_k(s)$, which is easy to do using the method of the hyperbola since in the cyclic case $\zeta_k(s) = \zeta(s)L(\chi, s)L(\overline{\chi}, s)$, leading to a $O(X^{2/3})$ method.

For instance if $k$ is cyclic cubic of discriminant 49 we have seen that

$$\Phi_4(k; s) = \frac{1}{3} \left(1 + \frac{3}{2^3s}\right) \prod_{p \equiv \pm 1 \pmod{14}} \left(1 + \frac{3}{p^s}\right).$$

We should be able to compute $M(k; 10^{14})$ in a week, and we have $M(k; 10^{10}) = 934968027$ (2 minutes, will go much further of course).
Computing $M(k; X)$ is relatively easy only in the $A_4$ case when $\mathcal{L}(k) = \emptyset$: using the same methods we are reduced to the computation of the summatory function of the coefficients of $\zeta_k(s)$, which is easy to do using the method of the hyperbola since in the cyclic case $\zeta_k(s) = \zeta(s)\mathcal{L}(\chi, s)\mathcal{L}(\overline{\chi}, s)$, leading to a $O(X^{2/3})$ method.

For instance if $k$ is cyclic cubic of discriminant 49 we have seen that

$$\Phi_4(k; s) = \frac{1}{3} \left(1 + \frac{3}{2^{3s}}\right) \prod_{p \equiv \pm 1 \pmod{14}} \left(1 + \frac{3}{p^s}\right).$$

We should be able to compute $M(k; 10^{14})$ in a week, and we have $M(k; 10^{10}) = 934968027$ (2 minutes, will go much further of course).
On the other hand if we are either in the $A_4$ case but with $\mathcal{L}(k)$ nonempty, or in the $S_4$ case, even though the formulas are completely explicit I do not know how to obtain an algorithm which runs faster than $O(X)$:

- In the $A_4$ case, because the additional terms need to check whether a prime is totally split or not in a certain quartic $A_4$ field.
- In the $S_4$ case, because the main term needs to check whether a prime is totally split or not in a noncyclic cubic field.
On the other hand if we are either in the $A_4$ case but with $\mathcal{L}(k)$ nonempty, or in the $S_4$ case, even though the formulas are completely explicit I do not know how to obtain an algorithm which runs faster than $O(X)$:

- In the $A_4$ case, because the additional terms need to check whether a prime is totally split or not in a certain quartic $A_4$ field.
- In the $S_4$ case, because the main term needs to check whether a prime is totally split or not in a noncyclic cubic field.
The techniques are similar to the cubic case (without the complication of adjoining cube roots of unity), but we need to work much more for essentially two reasons.

- First, we must make a precise list of all possible splittings in an $S_4$-quartic extension: apparently not in the literature. Done partly in the 1970’s by J. Martinet and A. Jehanne, but incomplete (they could have completed it but did not really need it).

- Second, we need to compute precisely some subtle arithmetic quantities, and this is done using techniques of global, but mainly local class field theory. This was done around 2000 by F. Diaz y Diaz, M. Olivier, and C.

- We must then study in detail the set of quartic fields $\mathcal{L}(k)$ (this was not necessary in the cubic case), and relate some twisted ray class groups to more common objects.
The main theorem of [CDO] is as follows:

**Theorem (Diaz y Diaz, Olivier, C.)**

Let $k$ be a cubic field. We have

$$\Phi_4(k; s) = \frac{2^{2-r_2(k)}}{a(k)2^{3s}} \sum_{c \mid 2\mathbb{Z}_k} z_k(c)(Nc)^{s-1} \prod_{p \mid c} \left(1 - \frac{1}{Np^s}\right) \sum_{\chi \in \hat{G}_c^2} F_k(\chi, s),$$

$$F_k(\chi, s) = \prod_p \left(1 + \frac{s_\chi(p)}{p^s}\right), \quad s_\chi(p) = \sum_{a \mid p\mathbb{Z}_k \text{ squarefree}} \chi(a),$$

$z_k(c) = 1$ or $2$ depending on $c$ and the splitting of $2$ in $k$, and $G_{c^2}$ is essentially (but not exactly) $Cl_{c^2}(k)/Cl_{c^2}(k)^2$ (recall that $a(k) = |\text{Aut}(k)|$).
For exposition, we treat $S_4$. Classical result (Hasse ?):

**Theorem**

There is a bijection between $S_4$-quartic fields $K$ with cubic resolvent $k$ and quadratic extensions $K_6/k$ of trivial norm, i.e., $K_6 = k(\sqrt[3]{\alpha})$ with $N_{k/Q}(\alpha)$ a square, so in particular $N(\sigma(K_6/k))$ is a square.

In fact $K_6$ is the unique extension of $k$ in $\tilde{K}$ such that $\text{Gal}(\tilde{K}/K_6) \cong C_4$.

In addition $\zeta_K(s) = \zeta(s)\zeta_{K_6}(s)/\zeta_k(s)$ and $\text{disc}(K) = \text{disc}(k)N(\sigma(K_6/k))$.

Finally, if $K_6 = k(\sqrt[3]{\alpha})$ of trivial norm and $x^3 + a_2x^2 + a_1x + a_0$ is the characteristic polynomial of $\alpha$, a defining polynomial for $K$ is $x^4 + 2a_2x^2 - 8\sqrt{-a_0}x + a_2^2 - 4a_1$. 
Proposition

There is a one-to-one correspondence between on the one hand quadratic extensions of $k$ of trivial norm, together with the trivial extension $k/k$, and on the other hand pairs $(\alpha, \overline{u})$, where $\alpha$ is an integral, squarefree ideal of $k$ of square norm whose class modulo principal ideals is a square in the class group of $k$, and $\overline{u} \in S[N]$, where

$$S(N) = \{ \overline{u}, \ u \mathbb{Z}_k = q^2, \ N(u) \text{ square} \}.$$  

Using the same theorem of Hecke as in the cubic case, introducing suitable twisted ray class groups and ray Selmer groups, and doing some combinatorial work, we obtain essentially the CDO theorem, where $z_k(c)$ is given as the index of a twisted ray class group in another.
Proposition

There is a one-to-one correspondence between on the one hand quadratic extensions of $k$ of trivial norm, together with the trivial extension $k/k$, and on the other hand pairs $(\alpha, \overline{u})$, where $\alpha$ is an integral, squarefree ideal of $k$ of square norm whose class modulo principal ideals is a square in the class group of $k$, and $\overline{u} \in S[N]$, where

$$ S(N) = \{ \overline{u}, \ u\mathbb{Z}_k = q^2, \mathcal{N}(u) \text{ square} \} . $$

Using the same theorem of Hecke as in the cubic case, introducing suitable twisted ray class groups and ray Selmer groups, and doing some combinatorial work, we obtain essentially the CDO theorem, where $z_k(c)$ is given as the index of a twisted ray class group in another.
Using a number of exact sequences, we can then show that $z_k(c)$ is the index of $(\mathbb{Z}_k/c^2)^*[N]$ in $(\mathbb{Z}_k/c^2)^*$, where $[N]$ means the subgroup of elements having a lift of square norm.

This is “elementary”: no more class groups, unit groups, or Selmer groups. However difficult to compute; we have done it only when $k$ is a cubic field. It uses local class field theory and some rather surprising algebraic arguments.

Challenge: prove without using CFT the following

**Proposition**

Let $k$ be a cubic field and $p$ an unramified prime ideal dividing 2. Then if $c = 2\mathbb{Z}_k/p$ we have $z_k(c) = 1$, in other words any element of $(\mathbb{Z}_k/c^2)^*$ has a lift of square norm.

We would be interested to know such a proof. Putting everything together proves the CDO theorem.
Using a number of exact sequences, we can then show that $z_k(c)$ is the index of $(\mathbb{Z}_k/c^2)^*[N]$ in $(\mathbb{Z}_k/c^2)^*$, where $[N]$ means the subgroup of elements having a lift of square norm. This is “elementary” : no more class groups, unit groups, or Selmer groups. However difficult to compute ; we have done it only when $k$ is a cubic field. It uses local class field theory and some rather surprising algebraic arguments.

Challenge : prove without using CFT the following

Proposition

Let $k$ be a cubic field and $\mathfrak{p}$ an unramified prime ideal dividing 2. Then if $c = 2\mathbb{Z}_k/\mathfrak{p}$ we have $z_k(c) = 1$, in other words any element of $(\mathbb{Z}_k/c^2)^*$ has a lift of square norm.

We would be interested to know such a proof. Putting everything together proves the CDO theorem.
Using a number of exact sequences, we can then show that $z_k(c)$ is the index of $(\mathbb{Z}_k/c^2)^*[N]$ in $(\mathbb{Z}_k/c^2)^*$, where $[N]$ means the subgroup of elements having a lift of square norm. This is “elementary” : no more class groups, unit groups, or Selmer groups. However difficult to compute ; we have done it only when $k$ is a cubic field. It uses local class field theory and some rather surprising algebraic arguments.

Challenge : prove without using CFT the following

**Proposition**

Let $k$ be a cubic field and $p$ an unramified prime ideal dividing 2. Then if $c = 2\mathbb{Z}_k/p$ we have $z_k(c) = 1$, in other words any element of $(\mathbb{Z}_k/c^2)^*$ has a lift of square norm.

We would be interested to know such a proof. Putting everything together proves the CDO theorem.
We are now in the same situation as in the cubic case after A. Morra’s thesis: the Dirichlet series $\Phi_4(k; s)$ is an explicit finite linear combination of Euler products. However these involve characters over rather complicated class groups, so not sufficiently explicit to allow algorithmic computation. We will do the same as for the cubic case, make it completely explicit and algorithmic.

We essentially need to do four things:

• Compute and/or interpret the twisted class groups $G_{c^2}$ in terms of more standard types of class groups.
• Determine all possible splitting types of primes in the fields $(k, K_6, K)$.
• Study the fields in $\mathcal{L}(k)$.
• Interpret the sums over characters of $G_{c^2}$ as sums over quartic fields $E \in \mathcal{L}(k)$. 
We are now in the same situation as in the cubic case after A. Morra’s thesis: the Dirichlet series $\Phi_4(k; s)$ is an explicit finite linear combination of Euler products. However, these involve characters over rather complicated class groups, so not sufficiently explicit to allow algorithmic computation. We will do the same as for the cubic case, make it completely explicit and algorithmic. We essentially need to do four things:

- Compute and/or interpret the twisted class groups $G_{c, 2}$ in terms of more standard types of class groups.
- Determine all possible splitting types of primes in the fields $(k, K_6, K)$.
- Study the fields in $\mathcal{L}(k)$.
- Interpret the sums over characters of $G_{c, 2}$ as sums over quartic fields $E \in \mathcal{L}(k)$. 
The Quartic $A_4$ and $S_4$ Case: Indication of Proof VII

- Twisted class groups $G_{c2}$: needs to be studied in detail (1 page), uses global CFT but not difficult. This study has a surprising corollary:

**Proposition**

Let $k$ be a cubic field. There exists $u \in k^*$ coprime to 2 such that $u\mathcal{O}_k = q^2$, $N(u)$ is a square, and $u \not\equiv 1 \pmod{4\mathcal{O}_k}$.

I do not know how to prove this without CFT.

- Splitting of primes in $(k, K_6, K)$. As mentioned, this was partly done by Martinet and Jehanne, but need to do it completely. Two steps: first prove that certain splittings are impossible, second for the remaining ones find examples. For fun, here is the table of impossibilities:
• Twisted class groups $G_{c2}$: needs to be studied in detail (1 page), uses global CFT but not difficult. This study has a surprising corollary:

**Proposition**

Let $k$ be a cubic field. There exists $u \in k^*$ coprime to 2 such that $u\mathbb{Z}_k = q^2$, $N(u)$ is a square, and $u \not\equiv 1 \pmod{4\mathbb{Z}_k}$.

I do not know how to prove this without CFT.

• Splitting of primes in $(k, K_6, K)$. As mentioned, this was partly done by Martinet and Jehanne, but need to do it completely. Two steps: first prove that certain splittings are impossible, second for the remaining ones find examples. For fun, here is the table of impossibilities:
## The Quartic $A_4$ and $S_4$ Case: Prime Splits I

<table>
<thead>
<tr>
<th>$k$-split</th>
<th>$K_6$-split</th>
<th>$K$-split</th>
<th>Possible for $p \neq 2$?</th>
<th>Possible for $p = 2$?</th>
</tr>
</thead>
<tbody>
<tr>
<td>(3)</td>
<td>(6)</td>
<td>—</td>
<td>ZETA</td>
<td>ZETA</td>
</tr>
<tr>
<td>(3)</td>
<td>(33)</td>
<td>(31)</td>
<td>OK</td>
<td>OK</td>
</tr>
<tr>
<td>(3)</td>
<td>(3²)</td>
<td>(1⁴)</td>
<td>SQN</td>
<td>OK</td>
</tr>
<tr>
<td>(21)</td>
<td>(42)</td>
<td>(4)</td>
<td>OK</td>
<td>OK</td>
</tr>
<tr>
<td>(21)</td>
<td>(411)</td>
<td>—</td>
<td>ZETA</td>
<td>ZETA</td>
</tr>
<tr>
<td>(21)</td>
<td>(41²)</td>
<td>—</td>
<td>ZETA</td>
<td>ZETA</td>
</tr>
<tr>
<td>(21)</td>
<td>(222)</td>
<td>(22)</td>
<td>STICK</td>
<td>STICK</td>
</tr>
<tr>
<td>(21)</td>
<td>(2211)</td>
<td>(211)</td>
<td>OK</td>
<td>OK</td>
</tr>
<tr>
<td>(21)</td>
<td>(221²)</td>
<td>(21²)</td>
<td>SQN</td>
<td>GRP(1)</td>
</tr>
<tr>
<td>(21)</td>
<td>(2²2)</td>
<td>(2²)</td>
<td>OK</td>
<td>OK</td>
</tr>
<tr>
<td>(21)</td>
<td>(2²11)</td>
<td>(1³1)</td>
<td>RAM</td>
<td>RAM</td>
</tr>
<tr>
<td>(21)</td>
<td>(2²11)</td>
<td>(1²1²)</td>
<td>OK</td>
<td>OK</td>
</tr>
<tr>
<td>(21)</td>
<td>(2²1²)</td>
<td>(1⁴)</td>
<td>SQN</td>
<td>OK</td>
</tr>
</tbody>
</table>
### The Quartic $A_4$ and $S_4$ Case: Prime Splits II

<table>
<thead>
<tr>
<th>$k$-split</th>
<th>$K_6$-split</th>
<th>$K$-split</th>
<th>Possible for $p \neq 2$?</th>
<th>Possible for $p = 2$?</th>
</tr>
</thead>
<tbody>
<tr>
<td>(111)</td>
<td>(222)</td>
<td>—</td>
<td>ZETA</td>
<td>ZETA</td>
</tr>
<tr>
<td>(111)</td>
<td>(2211)</td>
<td>(22)</td>
<td>OK</td>
<td>OK</td>
</tr>
<tr>
<td>(111)</td>
<td>(221^2)</td>
<td>—</td>
<td>ZETA</td>
<td>ZETA</td>
</tr>
<tr>
<td>(111)</td>
<td>(21111)</td>
<td>(211)</td>
<td>STICK</td>
<td>STICK</td>
</tr>
<tr>
<td>(111)</td>
<td>(2111^2)</td>
<td>(21^2)</td>
<td>SQN</td>
<td>GRP(2)</td>
</tr>
<tr>
<td>(111)</td>
<td>(21^{2}1^2)</td>
<td>(2^2)</td>
<td>OK</td>
<td>OK</td>
</tr>
<tr>
<td>(111)</td>
<td>(111111)</td>
<td>(1111)</td>
<td>OK</td>
<td>OK</td>
</tr>
<tr>
<td>(111)</td>
<td>(1^21111)</td>
<td>(1^211)</td>
<td>SQN</td>
<td>GRP(3)</td>
</tr>
<tr>
<td>(111)</td>
<td>(1^21211)</td>
<td>(1^21^2)</td>
<td>OK</td>
<td>OK</td>
</tr>
<tr>
<td>(111)</td>
<td>(1^21^211)</td>
<td>(1^31)</td>
<td>RAM</td>
<td>RAM</td>
</tr>
<tr>
<td>(111)</td>
<td>(1^21^21^2)</td>
<td>(1^4)</td>
<td>SQN</td>
<td>OK</td>
</tr>
<tr>
<td>$k$-split</td>
<td>$K_6$-split</td>
<td>$K$-split</td>
<td>Possible for $p \neq 2$?</td>
<td>Possible for $p = 2$?</td>
</tr>
<tr>
<td>-----------</td>
<td>-------------</td>
<td>-----------</td>
<td>--------------------------</td>
<td>--------------------------</td>
</tr>
<tr>
<td>$(1^2 1)$</td>
<td>$(2^2 2)$</td>
<td>—</td>
<td>ZETA</td>
<td>ZETA</td>
</tr>
<tr>
<td>$(1^2 1)$</td>
<td>$(2^2 11)$</td>
<td>$(21^2)$</td>
<td>OK</td>
<td>OK</td>
</tr>
<tr>
<td>$(1^2 1)$</td>
<td>$(2^2 1^2)$</td>
<td>$(2^2)$</td>
<td>SQN</td>
<td>GRP(4)</td>
</tr>
<tr>
<td>$(1^2 1)$</td>
<td>$(1^2 1 2^2)$</td>
<td>$(21^2)$</td>
<td>GRP(5)</td>
<td>GRP(5)</td>
</tr>
<tr>
<td>$(1^2 1)$</td>
<td>$(1^2 1 2 11)$</td>
<td>$(1^2 11)$</td>
<td>OK</td>
<td>OK</td>
</tr>
<tr>
<td>$(1^2 1)$</td>
<td>$(1^2 1 2 1 2)$</td>
<td>$(1^2 12)$</td>
<td>SQN</td>
<td>GRP(6)</td>
</tr>
<tr>
<td>$(1^2 1)_0$</td>
<td>$(1^4 2)$</td>
<td>$(2^2)$</td>
<td>SQN</td>
<td>PARITY</td>
</tr>
<tr>
<td>$(1^2 1)_4$</td>
<td>$(1^4 2)$</td>
<td>$(2^2)$</td>
<td>SQN</td>
<td>OK</td>
</tr>
<tr>
<td>$(1^2 1)$</td>
<td>$(1^4 1 1)$</td>
<td>$(1^2 1^2)$</td>
<td>SQN</td>
<td>OK</td>
</tr>
<tr>
<td>$(1^2 1)$</td>
<td>$(1^4 1^2)$</td>
<td>$(1^4)$</td>
<td>OK</td>
<td>OK</td>
</tr>
<tr>
<td>$(1^3)$</td>
<td>$(2^3)$</td>
<td>$(2^2)$</td>
<td>GRP(7)</td>
<td>GRP(7)</td>
</tr>
<tr>
<td>$(1^3)$</td>
<td>$(1^3 1^3)$</td>
<td>$(1^2 1^2)$</td>
<td>GRP(8)</td>
<td>GRP(8)</td>
</tr>
<tr>
<td>$(1^3)$</td>
<td>$(1^3 1^3)$</td>
<td>$(1^3 1)$</td>
<td>OK</td>
<td>OK</td>
</tr>
<tr>
<td>$(1^3)$</td>
<td>$(1^6)$</td>
<td>$(1^4)$</td>
<td>SQN</td>
<td>OK</td>
</tr>
</tbody>
</table>
In these tables, anything other than OK means the splitting is impossible, for quite a number of reasons: ZETA because of the zeta relation, SQN because of the square norm condition, STICK because of Stickelberger’s theorem, RAM because of ramification indices, and more generally GRP(i) because of case-by-case reasoning on decomposition and inertia groups. The whole study with proof requires 6 tedious pages.

- Study of $\mathcal{L}(k)$: recall that

$$\mathcal{L}(k) = \mathcal{L}_{k,1} \cup \mathcal{L}_{k,4} \cup \mathcal{L}_{k,16} \cup \mathcal{L}_{k,64,\text{tr}}.$$  

The reason for the importance of this set is:

**Proposition**

$E \in \mathcal{L}(k)$ if and only if the corresponding $K_6$ of trivial norm is of the form $K_6 = k(\sqrt{\alpha})$ with $\alpha$ coprime to 2, totally positive, and $\alpha \mathbb{Z}_k = q^2$ (i.e., $\alpha$ virtual unit).
In these tables, anything other than OK means the splitting is impossible, for quite a number of reasons: ZETA because of the zeta relation, SQN because of the square norm condition, STICK because of Stickelberger’s theorem, RAM because of ramification indices, and more generally GRP(i) because of case-by-case reasoning on decomposition and inertia groups. The whole study with proof requires 6 tedious pages.

- Study of $\mathcal{L}(k)$: recall that

$$\mathcal{L}(k) = \mathcal{L}_{k,1} \cup \mathcal{L}_{k,4} \cup \mathcal{L}_{k,16} \cup \mathcal{L}_{k,64,\text{tr}}.$$ 

The reason for the importance of this set is:

**Proposition**

$E \in \mathcal{L}(k)$ if and only if the corresponding $K_6$ of trivial norm is of the form $K_6 = k(\sqrt{\alpha})$ with $\alpha$ coprime to 2, totally positive, and $\alpha \mathbb{Z}_k = q^2$ (i.e., $\alpha$ virtual unit).
The Quartic $A_4$ and $S_4$ Case: $\mathcal{L}(k)$ II

Proposition

- $|\mathcal{L}(k)| = 2^{r_k}(Cl_4(k)) - 1$.
- $|\mathcal{L}_{k,1}| = (2^{r_k}(Cl(k)) - 1)/a(k)$.
- $\mathcal{L}_{k,4} = \mathcal{L}_{k,16} = \mathcal{L}_{k,64,\text{tr}} = \emptyset$ (equivalently $\mathcal{L}(k) = \mathcal{L}_{k,1}$) if and only if $k$ is totally real and all totally positive units are squares.
- If one of $\mathcal{L}_{k,4}$, $\mathcal{L}_{k,16}$, $\mathcal{L}_{k,64,\text{tr}}$ is nonempty the other two are empty.

It is then possible to give in terms of the splitting of 2 in $k$ and the existence or nonexistence of certain virtual units, necessary and sufficient conditions for $\mathcal{L}_{k,4}$, $\mathcal{L}_{k,16}$, or $\mathcal{L}_{k,64,\text{tr}}$ to be nonempty. The complete study of these sets require in all an additional 6 pages.
Proposition

• \(|\mathcal{L}(k)| = 2^{\text{rk}_2(\text{Cl}_4(k))} - 1\).
• \(|\mathcal{L}_{k,1}| = (2^{\text{rk}_2(\text{Cl}(k))} - 1)/a(k)\).
• \(\mathcal{L}_{k,4} = \mathcal{L}_{k,16} = \mathcal{L}_{k,64,\text{tr}} = \emptyset\) (equivalently \(\mathcal{L}(k) = \mathcal{L}_{k,1}\)) if and only if \(k\) is totally real and all totally positive units are squares.
• If one of \(\mathcal{L}_{k,4}, \mathcal{L}_{k,16}, \mathcal{L}_{k,64,\text{tr}}\) is nonempty the other two are empty.

It is then possible to give in terms of the splitting of 2 in \(k\) and the existence or nonexistence of certain virtual units, necessary and sufficient conditions for \(\mathcal{L}_{k,4}, \mathcal{L}_{k,16}, \text{ or } \mathcal{L}_{k,64,\text{tr}}\) to be nonempty. The complete study of these sets require in all an additional 6 pages.
The final thing that we need to do is to show that the sums over characters of $G_{c^2}$ as which occur in the CDO theorem correspond to sums over quartic fields $E \in \mathcal{L}(k)$. Even though this is analogous to the cubic case, it is much more subtle, and again involves some local and global class field theory and 4 additional pages. Once this is done, the usual combinatorics done in the cubic case lead to our main theorem.
The final thing that we need to do is to show that the sums over characters of $G_{c^2}$ as which occur in the CDO theorem correspond to sums over quartic fields $E \in \mathcal{L}(k)$. Even though this is analogous to the cubic case, it is much more subtle, and again involves some local and global class field theory and 4 additional pages. Once this is done, the usual combinatorics done in the cubic case lead to our main theorem.
We may require that our fields $K$, in addition to having $k$ as cubic resolvent, satisfies a finite number of local conditions (for instance splittings of certain primes, etc...). One of the most natural generalizations of our work, already mentioned in [CDO] is to add signature conditions: if $k$ is a cubic field of signature $(1, 1)$ then $K$ has necessarily signature $(2, 1)$. But if $k$ is totally real then $K$ is either totally real or totally complex, and we may want to compute explicitly the corresponding Dirichlet series $\Phi_4^+(k; s)$, where we restrict the sum to totally real $K$.

The CDO theorem is valid almost verbatim:
We may require that our fields $K$, in addition to having $k$ as cubic resolvent, satisfies a finite number of local conditions (for instance splittings of certain primes, etc...). One of the most natural generalizations of our work, already mentioned in [CDO] is to add signature conditions: if $k$ is a cubic field of signature $(1, 1)$ then $K$ has necessarily signature $(2, 1)$. But if $k$ is totally real then $K$ is either totally real or totally complex, and we may want to compute explicitly the corresponding Dirichlet series $\Phi_4^+(k; s)$, where we restrict the sum to totally real $K$.

The CDO theorem is valid almost verbatim:
Theorem

\[ \Phi_4^+(k; s) = \frac{1}{a(k)2^{3s}} \sum_{c \mid 2\mathbb{Z}_k} z_k(c)(\mathcal{N}c)^{s-1} \prod_{p \mid c} \left(1 - \frac{1}{\mathcal{N}p^s}\right) \sum_{\chi \in \hat{G}^+_{c^2}} F_k(\chi, s), \]

with the same definition of \( z_k(c) \) and \( F_k(\chi, s) \), and \( G^+_{c^2} \) is a “narrow” twisted ray class group.

Thus the only difference with the CDO theorem is the replacement of \( G_{c^2} \) by \( G^+_{c^2} \), and the coefficient in front equal to 1 instead of \( 2^{2-r_2(k)} = 4 \) since \( k \) is totally real.

As a consequence (already noted in CDO) it is a theorem that asymptotically the proportion of totally real \( K \) with given cubic resolvent \( k \) among all of them is \( 1/4 \) : in fact we can prove that the convergence is quite fast (at least \( O(X^{-1/2}) \), but in practice \( O(X^{-3/4+\epsilon}) \)).
Signatures II

Theorem

$$\Phi_4^+(k; s) = \frac{1}{a(k)2^{3s}} \sum_{c \mid 2\mathbb{Z}_k} z_k(c)(\mathcal{N}c)^{s-1} \prod_{p \mid c} \left(1 - \frac{1}{\mathcal{N}p^s}\right) \sum_{\chi \in \hat{G}_{c_2}^+} F_k(\chi, s),$$

with the same definition of \(z_k(c)\) and \(F_k(\chi, s)\), and \(G_{c_2}^+\) is a “narrow” twisted ray class group.

Thus the only difference with the CDO theorem is the replacement of \(G_{c_2}\) by \(G_{c_2}^+\), and the coefficient in front equal to 1 instead of \(2^{2-r_2(k)} = 4\) since \(k\) is totally real.

As a consequence (already noted in CDO) it is a theorem that asymptotically the proportion of totally real \(K\) with given cubic resolvent \(k\) among all of them is \(1/4\) : in fact we can prove that the convergence is quite fast (at least \(O(X^{-1/2})\), but in practice \(O(X^{-3/4+\varepsilon})\)).
Theorem

\[ \Phi_4^+(k; s) = \frac{1}{a(k)2^{3s}} \sum_{c \mid 2\mathbb{Z}_k} z_k(c)(\mathcal{N}c)^{s-1} \prod_{p \mid c} \left(1 - \frac{1}{\mathcal{N}p^s}\right) \sum_{\chi \in \mathcal{G}_{c_2}^+} F_k(\chi, s), \]

with the same definition of \( z_k(c) \) and \( F_k(\chi, s) \), and \( \mathcal{G}_{c_2}^+ \) is a “narrow” twisted ray class group.

Thus the only difference with the CDO theorem is the replacement of \( \mathcal{G}_{c_2} \) by \( \mathcal{G}_{c_2}^+ \), and the coefficient in front equal to 1 instead of \( 2^{2-r_2(k)} = 4 \) since \( k \) is totally real.

As a consequence (already noted in CDO) it is a theorem that asymptotically the proportion of totally real \( K \) with given cubic resolvent \( k \) among all of them is \( 1/4 \) : in fact we can prove that the convergence is quite fast (at least \( O(X^{-1/2}) \), but in practice \( O(X^{-3/4 + \varepsilon}) \)).
We then transform the CDO+ theorem into a theorem of the same nature as the main theorem without signatures: the only changes are: first, an additional factor of $1/4$, and second and more importantly, the set $\mathcal{L}(k)$ is changed into a new set $\mathcal{L}^*(k)$, where we simply remove the condition that $E$ be totally real when $k$ is totally real. We give one example in the $A_4$ case and one in the $S_4$ case.

**Example for $A_4$:** Let again $k$ be the cyclic cubic field of discriminant $49$. Then

$$
\Phi^+_4(k; s) = \frac{1}{4} \left( \Phi_4(k; s) + \left( 1 - \frac{1}{2^{3s}} \right) \prod_{p \mathbb{Z}_k = p_1p_2p_3} \left( 1 + \frac{\omega_E(p)}{p^s} \right) \right),
$$

where $E$ is the totally complex $A_4$-quartic field of discriminant $64 \cdot 49$ with cubic resolvent $k$ defined by $x^4 - 2x^3 + 2x^2 + 2 = 0$. 
We then transform the CDO+ theorem into a theorem of the same nature as the main theorem without signatures: the only changes are: first, an additional factor of $1/4$, and second and more importantly, the set $\mathcal{L}(k)$ is changed into a new set $\mathcal{L}^*(k)$, where we simply remove the condition that $E$ be totally real when $k$ is totally real. We give one example in the $A_4$ case and one in the $S_4$ case.

**Example for $A_4$:** Let again $k$ be the cyclic cubic field of discriminant $49$. Then

$$
\Phi_4^+(k; s) = \frac{1}{4} \left( \Phi_4(k; s) + \left( 1 - \frac{1}{2^3 s} \right) \prod_{p \mathbb{Z}_k = p_1 p_2 p_3} \left( 1 + \frac{\omega_E(p)}{p^s} \right) \right),
$$

where $E$ is the totally complex $A_4$-quartic field of discriminant $64 \cdot 49$ with cubic resolvent $k$ defined by $x^4 - 2x^3 + 2x^2 + 2 = 0$. 
**Signatures IV**

**Example for $S_4$**: Let $k$ be the noncyclic totally real cubic field of discriminant 229 defined by $x^3 - 4x - 1 = 0$. Then

\[
\Phi_4^+(k; s) = \frac{1}{4} \left( \Phi_4(k; s) + \left( 1 + \frac{1}{2^{2s}} - \frac{2}{2^{4s}} \right) \prod_{p \neq 2} \left( 1 + \frac{\omega_{E_1}(p)}{p^s} \right) \right)
\]

\[
+ \left( 1 - \frac{1}{2^{2s}} \right) \prod_{p \neq 2} \left( 1 + \frac{\omega_{E_{64}}(p)}{p^s} \right)
\]

where $E_1$ is the unique totally complex quartic field of discriminant 229 and cubic resolvent $k$ defined by $x^4 - x + 1 = 0$ and $E_{64}$ is the unique totally complex quartic field of discriminant $64 \cdot 229$ and cubic resolvent $k$ in which 2 is totally ramified, defined by $x^4 - 2x^3 + 4x^2 - 2x + 5$. 