The Cohen-Lenstra Heuristics Follow from Bhargava's Mass Formula

Kevin H. Wilson

December 31, 2016

1 Introduction

There has been quite a bit of work in the arithmetic statistics community over the past decade on two conjectures: the Cohen-Lenstra Heuristics [4] and Bhargava's conjecture[1] on the density of discriminants of S_n fields [2] (and specifically Kedlaya's extensions [6]). The purpose of this note is to show that these conjectures are *consistent*, and in fact, a particular subset of Bhargava's conjecture for dihedral extensions would prove the Cohen-Lenstra Heuristics.

Let $n > 1$ be an integer, $G \leq S_n$ be a transitive permutation group of degree n, and k a global field. Let $\mathcal{F} = \mathcal{F}(n, G, k)$ be the set of degree n field extensions K of k which have Galois closure L with $\mathrm{Gal}(L/k) \cong G$. Further, let $c : \mathcal{F} \to \mathbb{R}_{\geq 0}$ be some *counting function* and write

$$\mathcal{F}_c(X) = \{K \in \mathcal{F} : c(K) < X\}.$$

Supposing that $\#\mathcal{F}_c(X) < \infty$ for all X, we can ask for its asymptotics.

Question 1.1. Let $N_c(n, G, k; X) = N_c(X) = \#\mathcal{F}_c(X)$. Does there exist some "nice" function $f_c(X)$ (e.g., a polynomial in X and $\log X$) such that

$$N_c(X) \sim f_c(X)?$$

This question has been answered in the affirmative for quite a few combinations of n, G, k, and c. In particular, much work has been done when $c = \mathrm{Disc}$ is the absolute value of the discriminant of the number field. In that case, with $k = \mathbb{Q}$, the count was derived for G abelian by Mäki [9] and Wright [12], $n = 3$ and $G = S_3$ by Davenport and Heilbronn [5], and $n = 4, 5$ and $G = S_n$ by Bhargava [1, 3]. This was recently extended by Bhargava, Shankar, and Wang [**?**] to k an arbitrary global field.

More general counting functions have also appeared in the literature. Specifically, Wood extended Mäki's and Wright's work [11] to greatly expand the type of counting function's by which abelian extensions of arbitrary base fields can be counted.

Bhargava noted in [2] that all the known asymptotics tended to appear as nice Euler products times some power of X and some power of $\log X$. Bhargava gave one description of these products in the case $G = S_n$, but Kedlaya gave a more general interpretation for all G when c arises as the conductor of a Galois representation [6]. Specifically, fix a finite group G and a faithful

[1] This conjecture grew out of the work of many people, notably starting with a conjecture of Linnick [**?**] the that the number of S_n fields with absolute discriminant bounded by X should be $\asymp X$. Bhargava's contribution was to interpret the constant of proportionality, which is the most critical component for this note.

representation $\eta : G \to \mathrm{GL}_m(\mathbb{C})$. Then η defines a counting function $c = c_\eta$ on $\mathcal{F}(n, G, k)$ which is the global Artin conductor of η.

For each prime $\mathfrak{p}$ of the base field k, write $S_G(p)$ for the set of Galois representations $\rho : \mathrm{Gal}(k^{\mathrm{sep}}/k) \to G$ and define the *expected number* $E(N)$ of extensions with global Artin conductor $N = \prod_p p^{e_p}$ to be

$$E(N) = \prod_p \frac{1}{|G|} \sum_{\substack{\rho \in S_G(p) \\ \mathrm{cond}(\rho) = e_p}} 1$$

where $\mathrm{cond}(\rho)$ is the *local* Artin conductor of ρ. The key assumption here is the independence of the various primes. We then take the heuristic that

$$\sum_{N \geq 1} E(N) \sim N_c(X).$$

We will be interested in studying dihedral extensions of $\mathbb{Q}$, which are closely related to the class groups of quadratic fields (see Section 2). Studying the characters attached to these extensions (Section 3) and examining the Dirichlet series attached to $E(N)$ (Section 4 for finite primes, Section 5 for the archimedean primes, and Section 6 for putting them together), we prove the following theorem in Section 7.

Theorem 1.2. *Bhargava's heuristics (as reinterpreted by Kedlaya) imply that*

$$\frac{\sum_K \left|\mathrm{Cl}(K)^2[p]\right|}{\sum_K 1} \to 1 + p^{-1}$$

for K real and

$$\frac{\sum_K \left|\mathrm{Cl}(K)^2[p]\right|}{\sum_K 1} \to 2.$$

for K imaginary.

2 Dihedral Fields and Class Groups

In this section we recall the relationship between dihedral extesions of $\mathbb{Q}$ and the class groups of quadratic fields. Recall that if $K = \mathbb{Q}(\sqrt{D})$ is a quadratic extension of $\mathbb{Q}$ and $H(K)$ is the Hilbert class field of K then $H(K)/\mathbb{Q}$ is already Galois. So in particular, if M/K is an unramified cyclic extension of K of degree n, then $M/\mathbb{Q}$ is Galois and $\mathrm{Gal}(M/\mathbb{Q}) \cong C_n \rtimes C_2 \cong D_n$. Then writing $C_n = \langle \sigma \rangle$ and $C_2 = \langle \tau \rangle$, we see that K is the fixed field of σ and so, since M/K is unramifed, the inertia group I_p at every prime p of $\mathbb{Q}$ must have $I_p \cap \langle \sigma \rangle$ trivial.

However, D_n contains the rotations σ^i and the order 2 reflections $\sigma^i \tau$. The product of any two reflections is a rotation, which is nontrivial whenever the two multiplied reflections are distinct. This implies that at all ramified primes p, I_p must be an order 2 group which contains a reflection and the identity.

On the other hand, if $M/\mathbb{Q}$ is a Galois extension of degree $2n$ with Galois group $\mathrm{Gal}(M/\mathbb{Q}) \cong D_n$, then M is cyclic of degree n over the fixed field K of σ. This extension is unramified if and only if the inertia groups $I_p \leq \mathrm{Gal}(M/\mathbb{Q})$ at every prime p have $I_p \cap \langle \sigma \rangle = \{e\}$. This proves the following theorem.

Proposition 2.1. *There is a one-to-one correspondence between on the one hand dihedral extensions $M/\mathbb{Q}$ with $\mathrm{Gal}(M/\mathbb{Q}) \cong D_n$ with $I_p \cap \langle \sigma \rangle = \{e\}$ for all finite primes p and on the other hand pairs (K, M) where K is a quadratic extension of $\mathbb{Q}$ and M/K is an unramified cyclic extension.*

Next we would like to relate the number of unramified cyclic extensions M/K of degree n to the number of elements in $\mathrm{Cl}(K)[n]$. Recall that every unramified extension of K is a subextension of $H(K)$. Moreover, $\mathrm{Gal}(H(K)/K) \cong \mathrm{Cl}(K)$. Thus, every unramified cyclic extension of degree n corresponds to a cyclic quotient of $\mathrm{Cl}(K)$ of order n. Since $\mathrm{Cl}(K)$ is a finite abelian group, duality assures us that cyclic quotients of order n are in one-to-one correspondence with cyclic subgroups of order n. But the number of cyclic subgroups of G of order n is well-known. So we arrive at the following.

Proposition 2.2. *If K is a quadratic field and $n = p_1^{e_1} \cdots p_r^{e_r}$, then the number of unramified cyclic extensions of degree n of K is equal to*

$$\prod_{i=1}^{r} \frac{|\mathrm{Cl}(K)[p_i^{e_i}]| - \left|\mathrm{Cl}(K)[p_i^{e_i-1}]\right|}{p^{e_r}(p-1)}. \tag{1}$$

For clarity, we note a few special cases when Propositions 2.1 and 2.2 are combined. First, note that if $M/K/\mathbb{Q}$ is as in Proposition 2.1, then $\mathrm{Disc}(M/\mathbb{Q}) = \mathrm{Disc}(M/K)\,\mathrm{Disc}(K)^n = \mathrm{Disc}(K)^n$ since M/K is unramified. Let $\sqrt[n]{\mathrm{Disc}} : \mathcal{F}(2n, D_n) \to \mathbb{R}_{\geq 0}$ denote the function $M \mapsto \sqrt[n]{\mathrm{Disc}(M)}$. Then we write $\mathcal{F}^{\mathrm{refl}}(2n, D_n, \sqrt[n]{\mathrm{Disc}}; X)$ denote the set of dihedral extensions $M/\mathbb{Q}$ with $\mathrm{Gal}(M/\mathbb{Q}) \cong D_n$ having $\sqrt[n]{\mathrm{Disc}(M)} < X$ and whose inertia groups I_p at all finite primes contain no nontrivial rotations. Then the two previous propositions immediately yield the following corollary.

Corollary 2.3. *If $n = p$ is prime, then*

$$\#\mathcal{F}^{\mathrm{refl}}(2n, D_n, \sqrt[n]{\mathrm{Disc}}; X) = \frac{1}{p-1} \sum_{K \in \mathcal{F}(2, C_2, \mathrm{Disc}; X)} \left[|\mathrm{Cl}(K)[p]| - 1 \right].$$

3 The character table of dihedral groups

Recall from the introduction that one of the most interesting sources of counting functions $c : \mathcal{F} \to \mathbb{R}_{\geq 0}$ are those that arise as the Artin conductor of $\mathrm{Gal}(L/\mathbb{Q}) \cong G \to \mathrm{GL}_m(\mathbb{C})$ where $G \to \mathrm{GL}_m(\mathbb{C})$ is a fixed Galois representation. As we are interested in dihedral extensions in this paper, we recall some basic facts about dihedral groups.

As in Section 2, let $n \geq 2$ and let D_n be the dihedral group of symmetries of the regular n-gon generated by a rotation σ of order n and a reflection τ. We may choose σ and τ such that $\sigma\tau = \tau\sigma^{-1}$. Note that $D_2 \cong V_4$.

Proposition 3.1. *The subgroups of the dihedral group D_n are the cyclic groups $C_m \leq \langle \sigma \rangle$ with $m \mid n$, the dihedral groups D_m with $m \mid n$, and the subgroups $\langle \sigma^i \tau \rangle$ of order 2 which contain a single reflection. Of these, the rotation subgroups are always normal, and if $n = 2$, then all subgroups are normal. Further, if $n > 2$ is even, then the two $D_{n/2}$ are normal as well.*

Next we recall that $\tau\sigma\tau = \sigma^{-1}$, and $\sigma\tau\sigma^{-1} = \sigma^2\tau$ implies the following.

Proposition 3.2. *When n is even, the dihedral group D_n has $n/2 + 3$ conjugacy classes consisting of the pairs of rotations $\{\sigma^i, \sigma^{-i}\}$ (with $i = 0$ and $i = n/2$ yielding singletons), and the two sets of reflections $\{\sigma^{2i}\tau \mid 0 \leq i \leq n/2\}$ and $\{\sigma^{2i+1}\tau \mid 0 \leq i \leq n/2\}$.*

When n is odd, D_n has $2 + (n-1)/2$ conjugacy classes, consisting of the pairs of rotations $\{\sigma^i, \sigma^{-i}\}$ (with $i = 0$ yielding a singleton), and the collection of all reflections $\{\sigma^i\tau \mid 0 \leq i \leq n-1\}$.

Finally, we recall the character table of D_n.

Proposition 3.3. *When n is even, the dihedral group D_n has the trivial representation, three nontrivial one-dimensional representations (arising from the three C_2 quotients of D_n), and $n/2-1$ two-dimensional representations.*

When n is odd, the dihedral group D_n has the trivial representation, one nontrivial one-dimensional representation, and $(n-1)/2$ two-dimensional representations.

In both cases, in the two-dimensional representations, σ^i maps to either the identity or a nontrivial rotation of $\mathbb{C}^2$, and $\sigma^j\tau$ maps to a reflection of $\mathbb{C}^2$.

4 Computing $\mu_p(s)$ at finite primes

For any (finite) prime p, let $S^{\text{refl}}_{D_n}(p) = S^{\text{refl}}_{D_n}$ the the set of continuous homomorphisms $\rho : \text{Gal}(\bar{\mathbb{Q}}_p/\bar{\mathbb{Q}}) \to D_n$ where the image of inertia under ρ does not contain a rotation. Then define

$$\mu_p(s) = \frac{1}{|D_n|} \sum_{\rho \in S^{\text{refl}}_{D_n}} p^{-\operatorname{cond}(\rho)s}$$

where $\operatorname{cond}(\rho)$ is the conductor of ρ when composed with faithful two-dimensional representation $D_n \to \text{GL}_2(\mathbb{C})$. Note that this is well-defined since the value of the character of every two-dimensional representation on reflections is 0.

Proposition 4.1. *When p is odd and n is even, $\mu_p(s) = 1 + 2p^{-s}$. When p is odd and n is even, $\mu_p(s) = 1 + p^{-s}$.*

Proof. We begin with the easiest case, when $(p, 2n) = 1$ and so ρ is actually *tame*. Then ρ factors through the tame Galois group $\text{Gal}(\bar{\mathbb{Q}}_p/\mathbb{Q}_p)^{\text{tame}}$ which is (topologically) generated by g and h with $hgh^{-1} = g^p$, and the inertia group is (topologically) generated by g. Thus continuous homomorphisms $\rho : \text{Gal}(\bar{\mathbb{Q}}_p/\mathbb{Q}_p) \to D_n$ are in one-to-one correspondence with pairs of elements $g, h \in D_n$ with $hgh^{-1} = g^p$, and for any such pair, the value of $\operatorname{cond}(\rho)$ depends only on the image of g. On the other hand, g must map to either e or a reflection under our assumptions. In either case, since p is odd, $g^p = g$, and so we are looking for elements $h \in Z_g(D_n)$ where $Z_g(D_n)$ is the centralizer of g in D_n. Then, abusing notation a bit and using the fact that $Z_e(D_n) = D_n$, we wish to compute

$$\mu_p(s) = \frac{1}{|D_n|} \left[|D_n| p^{-\operatorname{cond}(e)s} + \sum_{\sigma^i\tau} |Z_{\sigma^i\tau}(D_n)| p^{-\operatorname{cond}(\sigma^i\tau)s} \right].$$

Now for any $g \in D_n$, we see that $\operatorname{cond}(g)$ is the number of eigenvalues of $\rho(g)$ which are not equal to 1. Thus, for $g = e$, we have $\operatorname{cond}(e) = 0$ for g a reflection we have $\operatorname{cond}(g) = 1$. This reduces our sum to

$$\mu_p(s) = 1 + \frac{p^{-s}}{|D_n|} \sum_{\sigma^i\tau} |Z_{\sigma^i\tau}(D_n)|.$$

When n is odd, all reflections are conjugate, and so the orbit-stabilizer theorem tells us that $|Z_{\sigma^i\tau}(D_n)| = 2$ since half of all the elements of D_n are reflections. On the other hand, if n is even, then there are two conjugacy classes of reflections, so $|Z_{\sigma^i\tau}(D_n)| = 4$. And so the proposition is proved.

Next we consider the case when p is odd and $p \mid n$. Then it is no longer guaranteed *a priori* that the higher ramification groups at p are trivial. However, we know that the quotients of the higher ramification groups I_i/I_{i+1} for $i \geq 1$ are products of cyclic groups of order p. But if I_1 has a quotient which contains an element of order $p \neq 2$, then I_1 must contain a rotation. We are assuming that this is *not* the case in our definition of μ_p. This means that all the $\rho \in S_{D_n}^{\text{refl}}$ are *tame* and so we can repeat the above computation for all such p. □

Finally, we come to the case when $p = 2$. Things are a bit more complicated, but it turns out that the value of $\mu_2(1)$ has the same form as the value of $\mu_p(1)$ for all odd p. Specifically, we have the following.

Proposition 4.2. *When n is odd we have*

$$\mu_2(s) = 1 + \frac{1}{2^{-2s}} + \frac{2}{2^{-3s}}$$

and when n is even we have

$$\mu_2(s) = 1 + \frac{2}{2^{-2s}} + \frac{4}{2^{-3s}}$$

In particular, $\mu_2(1) = 3/2 = 1 + 1/2$ when n is odd and $\mu_2(1) = 2 = 1 + 2/2$ when n is even.

Proof. First we consider the tame case. Then again we're looking for pairs $g, h \in D_n$ with $hgh^{-1} = g^2$ and g a reflection or the identity. But if g is a reflection, then $g^2 = e \neq g$, and so it must be that $g = e$. That is, if ρ is at most tamely ramified at 2, then it is actually *unramified.* So the contribution from tamely ramified extensions to $\mu_2(1)$ is simply 1.

In the wild case, since the inertia group I_0 has order 2, the ramification group $I_1 = I_0$. Then we can use Proposition 3.1, to see that the image of ρ must be either exactly I_1 or a dihedral group D_m with $m \mid n$. In the case where the image of ρ is exactly I_1, we may simply look up the wildly ramified, C_2 extensions of $\mathbb{Q}_2$ (e.g., with [7]). Letting t denote the number of nontrivial ramification groups (i.e., I_t is the first trivial ramification group of ρ), we see that there are two fields with $t = 2$ and four fields with $t = 3$. In either case, the conductor is equal to t. So the total contribution to $\mu_2(s)$ is

$$\frac{1}{|D_n|} \sum_{\substack{\rho \in S_{D_n}^{\text{refl}} \\ \text{im}\,\rho \text{ reflection}}} 2^{-t(\rho)s} = \frac{1}{|D_n|} \sum_{\text{reflections in } D_n} \left[2 \cdot 2^{-2s} + 4 \cdot 2^{-3s}\right] = \frac{1}{2}\left[\frac{2}{2^{-2s}} + \frac{4}{2^{-3s}}\right] = \frac{1}{2^{-2s}} + \frac{2}{2^{-3s}}.$$

What remains to compute is the contribution to $\mu_2(s)$ coming from ρ whose image is a full dihedral group D_m. However, the image of wild ramification is a *normal* nontrivial 2-group in D_m. When m is odd, there are no such subgroups, and so if n is odd, then our computation is finished.

On the other hand, when n is even, then *only* value of $m \mid n$ for which the reflection subgroups are normal is $m = 2$. Note that there are $n/2$ subgroups of D_n isomorphic to $D_2 \cong V_4$, namely, $\langle \sigma^{n/2}, \sigma^i \tau \rangle$ with $0 \le i < n/2$.

We can then look at the enumeration of all Galois quartic extensions of $\mathbb{Q}_2$ with Galois group V_4 and note that only three of them have an inertia group isomorphic to C_2. Two of these have conductor 3 and one has conductor 2. Now V_4 has six automorphisms, and so for any of these three kernels, there are six distinct maps $\text{Gal}(\bar{\mathbb{Q}}_2/\mathbb{Q}_2) \to V_4$ with that kernel. Of these, only four have the image of inertia as a reflection. So in total the contribution to $\mu_2(s)$ is

$$\frac{1}{|D_n|} \cdot \#\{D_2 \le D_n\} \cdot 4 \cdot \left[\frac{1}{2^{-2s}} + \frac{2}{2^{-3s}}\right] = \frac{1}{2n} \cdot \frac{n}{2} \cdot 4 \cdot \left[\frac{1}{2^{-2s}} + \frac{2}{2^{-3s}}\right] = \left[\frac{1}{2^{-2s}} + \frac{2}{2^{-3s}}\right].$$

This completes the proof of the proposition. □

5 Computing $\mu_p(s)$ at infinite primes

Infinite primes behave slightly differently than finite primes. In particular, instead of weighting each Galois representation $G_{\mathbb{R}} = \mathrm{Gal}(\mathbb{C}/\mathbb{R}) \to D_n$ by some prime number, we weight them simply by 1. That is, if S is a collection of continuous homomorphisms $G_{\mathbb{R}} \to D_n$, then the weight $\mu_{\mathbb{R}}^S$ is simply $|S|$.

Infinite primes also behave slightly differently than finite primes in the allowance for ramification. In particular, we do *not* place restrictions on the ramification of K at infinity in our setting. That is, the image of inertia (i.e., all of $G_{\mathbb{R}}$) is allowed to contain a rotation. Thus, the weight $\mu_{\mathbb{R}}$ is simply $|D_n[2]|/|D_n|$, which is $(n+1)/2n$ when n is odd and $(n+2)/2n$ when n is even.

On the other hand, we note that if we want to average over imaginary or real quadratic fields K, then we note that if the image of inertia is a rotation or trivial, then K is a real quadratic field, else it is an imaginary quadratic field. Thus, defining $\mu_{\mathbb{R}}^+$ (resp. $\mu_{\mathbb{R}}^-$) to be the weight at infinity for real (resp. imaginary) quadratic fields, we have the following proposition.

Proposition 5.1. *With $\mu_{\mathbb{R}}^{\pm}$ as above, we have $\mu_{\mathbb{R}}^+ = 1/2n$ when n is odd and $1/n$ when n is even, and we have $\mu_{\mathbb{R}}^- = 1/2$ in either case.*

6 The expected number of dihedral fields

At this point, the philosophy that Bhargava articulates [2] would have us compute the "expected number" $E(N)$ of Galois D_n extensions $M/\mathbb{Q}$ with $\mathrm{Cond}(M) < X$ and whose inertia groups at all finite primes do not contain a nontrivial rotation. Specifically, for $N = \prod_p p^{e_p}$, we set

$$E(N) = \prod_p \frac{1}{|D_n|} \sum_{\substack{\rho \in S_{D_n}^{\mathrm{refl}}(p) \\ \mathrm{cond}(\rho) = e_p}} 1. \tag{2}$$

The key assumption here is that the primes behave independently. Then we can set

$$\Phi(s) = \sum_{N \geq 1} \frac{E(N)}{N^s} = \prod_p \mu_p(s). \tag{3}$$

As usual, the analytic properties of $\Phi(s)$ should tell us about the growth of $\sum_{N \geq 1} E(N)$.

6.1 n odd

Theorem 6.1. *When n is odd, $\Phi(s)$ admits a meromorphic continuation to all $s \in \mathbb{C}$ and has a simple pole at $s = 1$. The residue $\mathrm{Res}_{s=1}\,\Phi(s) = \zeta(2)^{-1}$. Thus, by standard Tauberian theorems,*

$$\sum_{N \geq 1} E(N) \sim \zeta(2)^{-1} X.$$

Proof. From the computations of $\mu_p(s)$ in Section 4, we see that the $\Phi(s)$ defined in (3) converges absolutely for $\Re(s) \geq 1$. Multiplying and dividing by $1 - p^{-s}$ at all p we find that for $\Re(s) \geq 1$

$$\Phi(s) = \frac{1 - 2^{-s}}{1 - 2^{-s}} \cdot \mu_2(s) \cdot \prod_{p \text{ odd}} \frac{1 - p^{-2s}}{1 - p^{-s}}.$$

Then if we also multiply and divide by $1 + 2^{-s}$ we arrive at

$$\Phi(s) = \frac{\mu_2(s)}{1+2^{-s}} \frac{\zeta(s)}{\zeta(2s)}.$$

This function, of course, has a meromorphic continuation to all $s \in \mathbb{C}$ with its only zero or pole with $\Re(s) \geq 1$ being a simple pole at $s = 1$. From our computation of $\mu_2(1)$ in Proposition 4.2, we find that

$$\operatorname{Res}_{s=1} \Phi(s) = \zeta(2)^{-1},$$

and so we arrive at the theorem. □

6.2 n even

In the case of n even, the same computation as in the proof of Theorem 6.2 will yield a double pole coming from $\zeta(s)^2$ at $s = 1$ and so we would expect a growth rate of $X \log X$. But recall from ???? that for our purposes we are less interested in the expected number of D_n fields with conductor N, but the expected number of D_n fields divided by the size of the two torsion in the class group of the quadratic subfield.

However, genus theory teaches us that if K has discriminant N, then $\left|\mathrm{Cl}^+(K)[2]\right| = 2^{\omega(N)}$ where $\omega(N)$ is the number of prime divisors of N and $\mathrm{Cl}^+(K)$ is the *narrow class group* of K. Thus, we can define

$$E'(N) = \frac{1}{\left|\mathrm{Cl}^+(K)[2]\right|} \prod_p \frac{1}{|D_n|} \sum_{\substack{\rho \in S_{D_n}^{\mathrm{refl}}(p) \\ \mathrm{cond}(\rho) = e_p}} 1. \tag{4}$$

Forming the directly series

$$\Phi'(s) = \sum_{N \geq 1} \frac{E'(N)}{N^s} = \prod_p \mu'_p(s).$$

Here we recall that for odd p, $\mu_p(s) = 1 + 2p^{-s}$ and so $\mu'_p(s) = 1 + p^{-s}$. For $p = 2$, we have that $\mu_2(s) = 1 + 2/2^{2s} + 4/2^{3s}$ and so $\mu'_2(s) = 1 + 1/2^{2s} + 2/2^{3s}$. Of course, these are *equal* to values of $\mu_p(s)$ when n is odd, and so the same proof of Theorem 6.1 applies to the following theorem.

Theorem 6.2. *When n is even, $\Phi'(s)$ admits a meromorphic continuation to all $s \in \mathbb{C}$ and has a simple pole at $s = 1$. The residue $\operatorname{Res}_{s=1} \Phi(s) = \zeta(2)^{-1}$. Thus, by standard Tauberian theorems,*

$$\sum_{N \geq 1} E'(N) \sim \zeta(2)^{-1} X.$$

6.3 An aside on the narrow class group

In (5) we defined $E'(N)$ in terms of the *narrow* class group. We would like to show that we could equally well define $E'(N)$ in terms of the class group, and Theorem 6.2 would remain unchanged. More specifically, let

$$E''(N) = \frac{1}{|\mathrm{Cl}(K)[2]|} \prod_p \frac{1}{|D_n|} \sum_{\substack{\rho \in S_{D_n}^{\mathrm{refl}}(p) \\ \mathrm{cond}(\rho) = e_p}} 1. \tag{5}$$

Corollary 6.3. *We have that*

$$\sum_{N \geq 1} E''(N) \sim \frac{1}{2} \sum_{N \geq 1} E'(N).$$

Recall the exact sequence

$$1 \to F_\infty(K) \to \mathrm{Cl}^+(K) \to \mathrm{Cl}(K) \to 1, \tag{6}$$

where $F_\infty(K) \leq C_2$. This tells us that

$$\frac{1}{2}E'(N) \leq E''(N) \leq E'(N).$$

But we also know that $F_\infty(K)$ is nontrivial if and only if K is real and the fundamental unit ε of K has norm 1. But if there is some prime $p \equiv 3 \pmod 4$ with $p \mid \mathrm{Disc}(K)$, there can be no such unit (or else $x^2 \equiv -1$ would have a solution modulo p), and so $\mathrm{Cl}^+(K) \neq \mathrm{Cl}(K)$ for all such K. In fact, we have the following.

Lemma 6.4. *Let K be a real quadratic field and suppose $F_\infty = C_2$. Then (6) splits if and only if there is a prime $p \equiv 3 \pmod 4$ with $p \mid \mathrm{Disc}(K)$.*

Proof. See, for instance, [8, Théorème 8]. □

So if all prime divisors $p \mid N$ satisfy $p \equiv 1 \pmod 4$ then $E''(N) = E'(N)$. On the other hand, if N has a divisor which is congruent to $3 \pmod 4$, then $E''(N) = \frac{1}{2}E'(N)$.

Lemma 6.5. *Let $\mathcal{D}(X)$ be the set of all positive fundamental discriminants less than X which have no prime divisor $\equiv 3 \pmod 4$. Then*

$$\sum_{N \in \mathcal{D}(X)} E'(N) = o(X).$$

Proof. Forming the Diriclet series

$$\sum_{N \in \mathcal{D}} \frac{E'(N)}{N^s} = \prod_{p \not\equiv 3 \pmod 4} \mu'_p(s). \tag{7}$$

As in the previous subsections, we may, upto a bounded constant, replace $\mu'_2(s)$ with $1 + 2^{-s}$. Then, multiplying and dividing by $\prod_{p \not\equiv 3 \pmod 4} 1 - p^{-s}$ we find that (7) is equal to the product of a holomorphic function and the function

$$\prod_{p \not\equiv 3 \pmod 4} \left(1 - p^{-s}\right)^{-1}.$$

However, this function has been well-studied, e.g. in [10, Satz 3]. In particular, this implies that the sum in question is $O(X/\sqrt{\log X})$. □

This lemma allows us to replace $E''(N)$ by $\frac{1}{2}E'(N)$ for all N, and this completes the proof of Corollary 6.3.

7 Proof of Theorem 1.2

Bacon ipsum dolor amet chuck rump bacon, strip steak spare ribs porchetta pork belly swine filet mignon. Beef ground round pork belly pork loin. Alcatra cupim biltong tongue prosciutto bresaola pork brisket. Shank venison ground round bacon kielbasa cow chicken tongue.

Bresaola turducken jerky pork belly brisket cupim pancetta. Strip steak spare ribs chuck corned beef cow sausage shankle bacon biltong alcatra filet mignon ground round flank. Pork chop venison salami tenderloin brisket cow. Pancetta hamburger cupim, andouille porchetta corned beef tenderloin shoulder. Frankfurter bacon pancetta sirloin.

Short loin drumstick alcatra shoulder sirloin. Pork chop leberkas turkey picanha turducken, ham hock kielbasa porchetta drumstick frankfurter filet mignon. Filet mignon turducken meatball bresaola shank. Tail rump kielbasa jowl, t-bone doner shoulder pork chop sirloin ham hock beef ribs short ribs ball tip flank. Andouille kielbasa hamburger ham hock beef ribs meatloaf. T-bone swine cow frankfurter flank pork loin chuck shank capicola rump spare ribs short loin bacon.

References

[1] M. Bhargava. The density of discriminants of quartic rings and fields. *Annals of Mathematics*, 162(2):1031–1063, 2005.

[2] M. Bhargava. Mass formulae for extensions of local fields, and conjectures on the density of number field discriminants. *International Mathematics Research Notices*, (17), 2007.

[3] M. Bhargava. The density of discriminants of quintic rings and fields. *Annals of Mathematics*, 172(3):1559–1591, 2010.

[4] H. Cohen and H. W. Lenstra, Jr. Heuristics on class groups of number fields. In *Number theory, Noordwijkerhout 1983 (Noordwijkerhout, 1983)*, volume 1068 of *Lecture Notes in Math.*, pages 33–62. Springer, Berlin, 1984.

[5] H. Davenport and H. Heilbronn. On the density of discriminants of cubic fields ii. *Proceedings of the Royal Society of London Series A*, 322(1551):405–420, 1971.

[6] K. Kedlaya. Mass formulas for local Galois representations. *International Mathematics Research Notices*, (17), 2007. With an appendix by Daniel Gulotta.

[7] The LMFDB Collaboration. The l-functions and modular forms database. `http://www.lmfdb.org`, 2013. [Online; accessed 1 November 2016].

[8] S. Louboutin. Groupes des classes d'idéaux triviaux. *Acta Arithmetica*, 54:61–74, 1989.

[9] S. Mäki. The conductor density of abelian number fields. *Journal of the London Mathematical Society (2)*, 47(1):18–30, 1993.

[10] G.J. Rieger. über die Anzahl der als Summe von zwei Quadraten darstellbaren und in einer primen Restklasse gelegenen Zahlen unterhalb einer positiven Schranke. ii. *J. Reine Angew. Math.*, 217:200–216, 1965.

[11] M. M. Wood. Mass formulas for local Galois representations to wreath products and cross products. *Algebra Number Theory*, 2(4):391–405, 2008.

[12] D.J. Wright. Distribution of discriminants of abelian extensions. *Proc. London Math. Soc. (3)*, 58:17–50, 1989.