# An Asymptotic for the Number of Solutions to Linear Equations in Prime Numbers from Specified Chebotarev Classes

Daniel M. Kane

September 8, 2010

## 1 Introduction and Statement of Results

The bulk of this paper will consist of proving the following Theorem on solving linear equations in prime numbers:

**Theorem 1.** *Let $k \geq 3$ be an integer. Let $K_i/\mathbb{Q}$ be a finite Galois extensions $(1 \leq i \leq k)$ with $G_i = Gal(K_i/\mathbb{Q})$. Let $a_1, \ldots, a_k$ be non-zero integers with no common divisor. Let $C_i$ be a conjugacy class of $G_i$ for each $i$. Let $K_i^a$ be the maximal abelian extension of $\mathbb{Q}$ contained in $K_i$, and let $D_i$ be its discriminant. Let $D$ be the least common multiple of the $D_i$. Let $H_i^0$ be the subgroup of $(\mathbb{Z}/D\mathbb{Z})^*$ corresponding to $K_i^a$ via global class field theory. Let $H_i$ be the coset of $H_i^0$ corresponding to the projection of an element of $C_i$ to $Gal(K_i^a/\mathbb{Q})$. Additionally let $n$ by an integer and let $A$ and $X$ be positive integers, then*

$$\sum_{\substack{p_i \leq X \\ [K_i/\mathbb{Q}, p_i] = C_i \\ \sum_i a_i p_i = n}} \prod_{i=1}^{k} \log(p_i) = \left( \prod_{i=1}^{k} \frac{|C_i|}{|G_i|} \right) C_\infty C_D \left( \prod_{p \nmid D} C_p \right) + O\left( X^{k-1} \log^{-A}(X) \right). \tag{1}$$

*Where the sum of the right hand side is over sets of prime numbers $p_1, \ldots, p_n \leq X$ so that $\sum_{i=1}^k a_i p_i = n$, and the Artin symbol $[K_i/\mathbb{Q}, p_i]$ lands in the conjugacy class $C_i$ of $G_i$. On the left hand side,*

$$C_\infty = \int_{\substack{x_i \in [0,X] \\ \sum_i a_i x_i = n}} \left( \sum_{i=1}^{k} a_i \frac{\partial}{\partial x_i} \right) dx_1 \wedge dx_2 \wedge \ldots \wedge dx_k,$$

$$C_D = D \left( \frac{\#\{\{x_i\} \in ((\mathbb{Z}/D\mathbb{Z})^*)^k : x_i \in H_i, \sum_{i=1}^k a_i x_i \equiv n \pmod{D}\}}{\prod_{i=1}^k |H_i|} \right),$$

*and the second product is over primes $p$ not dividing $D$ of*

$$C_p = p \left( \frac{\#\{\{x_i\} \in ((\mathbb{Z}/p\mathbb{Z})^*)^k : \sum_{i=1}^k a_i x_i \equiv n \pmod{D}\}}{(p-1)^k} \right).$$

*Additionally the implied constant in the $O$ term may depend on $k, K_i, C_i, a_i$, and $A$, but not on $X$ or $n$. Additionally, if $k = 2$ and $K_i, C_i, a_i, A, X$ are fixed, then Equation (1) holds for all but $O(X \log^{-A}(X))$ values of $n$.*

This Theorem should be thought of as a generalization of standard results on the number of solutions in prime numbers to a single linear equation (see for example Theorem 19.2 and Proposition 19.5 of [1]). Our principle innovation is that in Theorem 1 instead of letting the $p_i$ be any primes, we require that they have specified Artin symbols with respect to the extensions $K_i$. This necessitates some changes to the right hand side of Equation 1 from the standard results due to (1) the Chebotarev Density Theorem, and (2) congruence relations forced on the $p_i$ by Global Class-Field Theory.

We begin by describing the motivation behind Theorem 1, and in particular explain the various terms on the right hand side of Equation 1. To begin with, the Prime Number Theorem says that the distribution that assigns $\log(p)$ to the prime $p$, is approximated by the distribution assigning 1 to each positive integer. The integral in $C_\infty$ provides an approximation to the number of solutions based on this heuristic. The other terms on the right hand side can be thought of as corrections to this heuristic.

The first of these to consider is $\left(\prod_{i=1}^{k} \frac{|C_i|}{|G_i|}\right)$. This term comes from the Chebotarev Density Theorem, and expresses the fact that only a $\frac{|C_i|}{|G_i|}$ fractions of primes $p$ have Artin symbol $[K_i/\mathbb{Q}, p] = C_i$.

The terms $C_D$ and $C_p$ can be thought of as local contributions coming from congruential information about the primes $p_i$. The term $C_D$ encodes the idea that rather than having a uniform distribution modulo $D$, primes $p_i$ in the appropriate Chebotarev class instead have reductions that are uniformly distributed over $H_i$. The correction term $C_p$ finally encodes the fact that modulo $p$ primes are uniformly distributed over the non-zero residue classes, rather than uniformly distributed over all residue classes.

Finally it should be noted that the error term is $o(X^{k-1}\log(X)^{-1})$, whereas if $n$ is bounded away from both the largest and smallest possible values that can be taken by $\sum_i a_i x_i$ for $x_i \in [0, X]$ then $C_\infty$ will be on the order of $X^{k-1}$. For $K_i, C_i$ fixed, the first term is a constant. $C_D$ is either 0 or is bounded away from both 0 and $\infty$. Lastly, for $p \nmid Dn\prod_i a_i$ inclusion-exclusion tells us that $C_p = 1 + O(p^{-2})$, and for $p|n$, $p \nmid D\prod_i a_i$, $C_p = 1 + O(p^{-1})$. This means that unless $C_p = 0$ for some $p$, $\prod_p C_p$ is within a bounded multiple of $\prod_{p|n}(1 + O(p^{-1})) = \exp(O(\log\log\log n))$. Therefore, unless $C_D = 0$, $C_p = 0$ for some $p$, or $n$ is near the boundary of the available range, the main term on the right hand side of Equation 1 dominates the error.

Our proof will closely mimic the proof of Theorem 19.2 in [1], although we will have to redo much of the work in order to generalize to our larger setting. The basic idea of the proof is fairly simple. We will be interested in studying the generating function $G$ for the prime numbers in a particular Chebotarev class. We first show that $G$ can be approximated in the $L^\infty$ norm by a function $G^\sharp$, which essentially replaces the Von Mangoldt function by a product of local

factors. This is done using separate techniques for evaluation at numbers with or without good rational approximations. We consider the natural integral involving the $G$'s to compute the left hand side of Equation 1 and show that we can afford to replace the $G$'s by corresponding $G^\sharp$'s. From there the integral is computed in a relatively straightforward manner.

Our treatment will proceed as follows. In Section 2 we will give a number of definitions including those of $G$ and $G^\sharp$ and prove some basic facts about them. We will also introduce a pair of functions $F$, and $F^\sharp$ closely related to $G$ and $G^\sharp$, but somewhat easier to work with. In Section 3 we show that $F^\sharp$ is a good approximation of $F$ in the $L^\infty$ norm. In Section 4 we use this to show that $G^\sharp$ is a good approximation of $G$. In Section 5 we use these results to prove Theorem 1. Finally in Section 6 we provide an application of Theorem 1 by using it to construct elliptic curves whose discriminants are divisible only by primes that split completely in some given extension of $\mathbb{Q}$.

# 2 Preliminaries

In this section we introduce some of the basic terminology and results that will be used throughout the rest of the paper. In Section 2.1 we define the functions $F$ and $G$ along with some of the basic facts relating them. In Section 2.2 we define $F^\sharp$ and $G^\sharp$ along with some related terminology and again prove some basic facts. Finally in Section 2.3 we prove a result on the distribution of smooth numbers that will prove useful to us later.

## 2.1 $G$ and $F$

We begin with a standard definition:

**Definition.** *Let $e(x)$ denote the function $e(x) = e^{2\pi i x}$.*

We now define $G$ as the generating function for primes $\leq X$ with $[K/\mathbb{Q}, p] = C$.

**Definition.** *Suppose that $K/\mathbb{Q}$ is a finite Galois extension with $G = Gal(K/\mathbb{Q})$, $C$ a conjugacy class of $G$, and $X$ a positive real number. We then define the generating function*

$$G_{K,C,X}(\alpha) = \sum_{\substack{p \leq X \\ [K/\mathbb{Q},p]=C}} \log(p) e(\alpha p).$$

*Where the sum is over primes $p \leq X$ with $[K/\mathbb{Q}, p] = C$.*

$G$ is a little awkward to deal with and we would rather work with a related function defined in terms of characters. We first need one auxiliary definition:

**Definition.** *Let $L/\mathbb{Q}$ be a number field. Let $\Lambda_L$ be the Von Mangoldt function on ideals of $L$, defined by*

$$\Lambda_L(\mathfrak{a}) = \begin{cases} \log(N(\mathfrak{p})) & \text{if } \mathfrak{a} = \mathfrak{p}^n \\ 0 & \text{otherwise} \end{cases}$$

*which assigns $\log(N(\mathfrak{p}))$ to a power of a prime ideal $\mathfrak{p}$, and 0 to ideals that are not powers of primes.*

We now define

**Definition.** *If $L/\mathbb{Q}$ is a number field, $\xi$ is a Grossencharacter of $L$, and $X$ a positive number, define the function*

$$F_{L,\xi,X}(\alpha) = \sum_{N(\mathfrak{a}) \leq X} \Lambda_L(\mathfrak{a})\xi(\mathfrak{a})e(\alpha N(\mathfrak{a})).$$

*Where the sum above is over ideals $\mathfrak{a}$ of norm at most $X$. Notice that if $\xi = 1$ this generating function is dominated by the primes in $L$ with splitting degree 1 over $\mathbb{Q}$.*

Note that for both $F$ and $G$, we will often suppress the $X$ when it is clear what the cutoff is. We now demonstrate the relationship between $F$ and $G$.

**Proposition 2.** *Let $K$ and $C$ be as above. Pick a $c \in C$. Let $L \subseteq K$ be the fixed field of $c$. Then we have that*

$$G_{K,C,X}(\alpha) = \frac{|C|}{|G|}\left(\sum_{\chi} \overline{\chi}(c) F_{L,\chi,X}(\alpha)\right) + O(\sqrt{X}). \tag{2}$$

*Where the sum is over characters $\chi$ of the subgroup $\langle c \rangle \subset G$, which by global class field theory can be thought of as characters of $L$.*

*Proof.* We begin by considering the sum on the right hand side of Equation (2). It is equal to

$$\begin{aligned} \sum_{\chi} \overline{\chi}(c) F_{L,\chi,X}(\alpha) &= \sum_{\chi} \sum_{N(\mathfrak{a}) \leq X} \Lambda_L(\mathfrak{a})\overline{\chi}(c)\chi(\mathfrak{a})e(\alpha N(\mathfrak{a})) \\ &= \sum_{N(\mathfrak{a}) \leq X} \Lambda_L(\mathfrak{a})e(\alpha N(\mathfrak{a})) \sum_{\chi} \overline{\chi}(c)\chi([K/L, \mathfrak{a}]) \\ &= \operatorname{ord}(c) \sum_{\substack{N(\mathfrak{a}) \leq X \\ [K/L,\mathfrak{a}] = c}} \Lambda_L(\mathfrak{a})e(\alpha N(\mathfrak{a})). \end{aligned}$$

Up to an error of $O(\sqrt{X})$, we can ignore the contributions from elements whose norms are powers of primes, because there are $O(\sqrt{X}/\log(X))$ higher powers of primes that are at most $X$. Therefore the above equals

$$\operatorname{ord}(c) \sum_{\substack{N(\mathfrak{p}) \leq X \\ [K/L,\mathfrak{p}] = c \\ N(\mathfrak{p}) \text{ is prime}}} \log(N(\mathfrak{p}))e(\alpha N(\mathfrak{a})) + O(\sqrt{X}).$$

We must now ask the question of which primes $p \in \mathbb{Z}$ can be written as the norm of a prime $\mathfrak{p} \subset L$ with $[K/L, \mathfrak{p}] = c$, and for such $p$, how many different primes $\mathfrak{p}$ have this property. If we have such a $\mathfrak{p}$, it must have splitting degree 1 over $\mathbb{Q}$. Therefore if $\mathfrak{q}$ is a prime of $K$ sitting over $\mathfrak{p}$, then (unless $\mathfrak{q}$ is ramified over $\mathbb{Q}$, which can be ignored since only finitely many primes ramify), the Frobenius element of $\mathfrak{q}$ in $\mathrm{Gal}(K/\mathbb{Q})$ must be $c$. In fact, since $\mathfrak{q}$ is the only prime of $K$ over $\mathfrak{p}$, such ideals $\mathfrak{p}$ correspond exactly to ideals $\mathfrak{q}$ of $K$ with $[K/\mathbb{Q}, \mathfrak{q}] = c$. Therefore a prime $p \in \mathbb{Z}$ appears as the norm of such a $\mathfrak{p}$ if and only if $[K/\mathbb{Q}, p] = C$. Next we need to know if $p$ is such a prime how many such ideals $\mathfrak{q}$ there are. Since all ideals over $p$ are conjugate in $G$, and since $\sigma p$ has Frobenius element $\sigma c \sigma^{-1}$, the number of such $\mathfrak{q}$ is $|N_c/D_{\mathfrak{q}}|$ (the normalizer of $c$ mod the decomposition group of $\mathfrak{q}$). We have that $|N_c| = \frac{|G|}{|C|}$, and $D_{\mathfrak{q}} = \langle c \rangle$, which is of size $\mathrm{ord}(c)$. Therefore the sum on the right hand side of Equation (2) is

$$\frac{|G|}{|C|} \sum_{\substack{p \leq X \\ [K/\mathbb{Q}, p] = C}} \log(p) e(\alpha p) + O(\sqrt{X}).$$

Multiplying by $\frac{|C|}{|G|}$ completes the proof of the Proposition. □

## 2.2 Local Approximations

Here we define some simpler functions meant to approximate $F$ and $G$. In order to do so we will need a number of auxiliary definitions:

**Definition.** *For $p$ a prime let*

$$\Lambda_p(n) = \begin{cases} 0 & \text{if } p|n \\ \frac{1}{1-p^{-1}} & \text{else} \end{cases}.$$

$\Lambda_p$ can be thought of as a local approximation to the Von Mangoldt function, based only on the residue of $n$ modulo $p$. Putting these functions together we get

**Definition.** *Let $z$ be a positive real. Define a function $\Lambda_z$ by*

$$\Lambda_z(n) = \prod_{p \leq z} \Lambda_p(n) = \begin{cases} 0 & \text{if } p|n \text{ for some prime } p < z \\ \prod_{p<z} \frac{1}{1-p^{-1}} & \text{otherwise} \end{cases}.$$

There are also some related definitions which will prove useful later.

**Definition.** *Let*

$$C(z) = \prod_{p \leq z} \frac{1}{1-p^{-1}}.$$

**Definition.** *Let*

$$P(z) = \prod_{p \leq z} p.$$

$$P(z,q) = \prod_{p \leq z, p \nmid q} p.$$

We note that

$$\Lambda_z(n) = C(z) \sum_{d|(n,P(z))} \mu(d).$$

Also, note that

$$\Lambda_z(n) = C(z) \sum_{d|(n,P(z,q))} \mu(d) \cdot \left( \begin{cases} 1 & \text{if } (n,q) = 1 \\ 0 & \text{otherwise} \end{cases} \right).$$

and that

$$C(z) = \Theta(\log(z)).$$

We will need some other local contributions to the Von Mangoldt function to take into account splitting information. In particular we define:

**Definition.** *Let $K/\mathbb{Q}$ be a Galois extension and $C \subset G = Gal(K/\mathbb{Q})$ a conjugacy class of the Galois group. If $C$ projects down to an element of $G^{ab}$, which by global class field theory corresponds to some coset $H$ of a subgroup of $(\mathbb{Z}/D\mathbb{Z})^*$ for some integer $D$, we define $\Lambda_{K,C}$ to be the arithmetic function:*

$$\Lambda_{K,C}(n) = \begin{cases} \frac{\phi(D)}{|H|} & \text{if } n \in H \\ 0 & \text{otherwise} \end{cases}.$$

This accounts for the conjugacy conditions implied by $n$ being a prime with Artin symbol $C$.

**Definition.** *Let $L$ be a number field. Consider $K/L$, its Galois closure. Consider the image of $Gal(K/L)$ in $Gal(K/\mathbb{Q})^{ab}$. By global class field theory, this corresponds to a subgroup $H_L$ of $(\mathbb{Z}/D_L\mathbb{Z})^*$ for some positive integer $D_L$. Let*

$$\Lambda_{L/\mathbb{Q}}(n) = \begin{cases} \frac{\phi(D_L)}{|H_L|} & \text{if } n \in H_L \\ 0 & \text{otherwise} \end{cases}.$$

$\Lambda_{L/\mathbb{Q}}$ is supposed to account for the congruence conditions that are implied by being a norm from $L$ down to $\mathbb{Q}$.

We are now prepared to define our approximations $F^\sharp$ and $G^\sharp$ to $F$ and $G$.

**Definition.** *For $K/\mathbb{Q}$ Galois, $C$ a conjugacy class in $Gal(K/\mathbb{Q})$, and $z$ and $X$ positive integers, we define the generating function*

$$G^\sharp_{K,C,X,z}(\alpha) = \frac{|C|}{|G|} \sum_{n \leq X} \Lambda_{K,C}(n) \Lambda_z(n) e(\alpha n).$$

*We also let*

$$G^\flat_{K,C,X,z}(\alpha) = G_{K,C,X}(\alpha) - G^\sharp_{K,C,X,z}(\alpha).$$

**Definition.** *For $L/\mathbb{Q}$ a number field, $\xi$ a Grossencharacter of $L$, and $X$ and $z$ a positive numbers, we define the function*

$$F^{\sharp}_{L,\xi,X,z}(\alpha) = \begin{cases} \sum_{n\leq X} \Lambda_{L/\mathbb{Q}}(n)\Lambda_z(n)\chi(n)e(\alpha n) & \text{if } \xi = \chi \circ N_{L/\mathbb{Q}} \text{ for some character } \chi \\ 0 & \text{otherwise} \end{cases}.$$

*Note that the $\Lambda_{L/\mathbb{Q}}$ term means that this function is independent of the choice of $\chi$ if there are multiple $\chi$ to choose from. We also define*

$$F^{\flat}_{L,\xi,X,z}(\alpha) = F_{L,\xi,X}(\alpha) - F^{\sharp}_{L,\xi,X,z}(\alpha).$$

Again for these functions we will often suppress the $X$.

We claim that $F^{\sharp}$ and $G^{\sharp}$ are good approximations of $F$ and $G$, and in particular we will prove that:

**Theorem 3.** *Let $K/\mathbb{Q}$ be a finite Galois extension, and let $C$ be a conjugacy class of $Gal(K/\mathbb{Q})$. Let $A$ be a positive integer and $B$ a suitably large multiple of $A$. Then if $X$ is a positive number, $z = \log^B(X)$, and $\alpha$ any real number, then*

$$\left|G^{\flat}_{K,C,X,z}(\alpha)\right| = O\left(X\log^{-A}(X)\right), \tag{3}$$

*where the implied constant depends on $K, C, A, B$, but not on $X$ or $\alpha$.*

**Theorem 4.** *Given $L/\mathbb{Q}$ a number field, and $\xi$ a Grossencharacter of $L$. Let $A$ be a positive integer and $B$ a suitably large multiple of $A$. Then if $X$ is a positive number, $z = \log^B(X)$, and $\alpha$ any real number, then*

$$\left|F^{\flat}_{L,\xi,X,z}(\alpha)\right| = O\left(X\log^{-A}(X)\right), \tag{4}$$

*where the implied constant depends on $L, \xi, A, B$, but not on $X$ or $\alpha$.*

The proofs of these Theorems will be the bulk of Sections 3 and 4

## 2.3 Smooth Numbers

We also need some results on the distribution of smooth numbers. We begin with a definition:

**Definition.** *Let $S(z, Y)$ be the number of $n \leq Y$ so that $n|P(z)$. In other words the number of $n \leq Y$ so that $n$ is squarefree and has no prime factors bigger than $z$.*

We make use of the following bound on $S(z, Y)$:

**Lemma 5.** *If $z = \log^B(X)$ and $Y \leq X$, then*

$$S(z, Y) \leq Y^{1-1/(2B)} \exp\left(O(\sqrt{\log(X)})\right)$$

*Proof.* Notice that

$$\int_{y=0}^{Y} S(z,y)dy = \frac{1}{2\pi}\int_{1-i\infty}^{1+i\infty}(s(s+1))^{-1}\prod_{p\leq z}(1+p^{-s})Y^{s+1}ds.$$

Note that,

$$\left|\prod_{p\leq z}(1+p^{-s})\right| = \left|\exp\left(\sum_{p\leq z}p^{-s}+O(1)\right)\right| \leq \exp\left(\frac{z^{1-\Re(s)}}{1-\Re(s)}\right).$$

Changing the line of integration to $1-\Re(s)=\frac{1}{2B}$, we get that the integrand is at most $s^{-2}Y^{2-1/(2B)}\exp\left(O(\sqrt{\log(X)})\right)$. Integrating and evaluating at $2Y$, we get that

$$Y^{2-1/(2B)}\exp\left(O(\sqrt{\log(X)})\right) \geq \int_{y=0}^{2Y} S(z,y)dy \geq YS(z,Y),$$

proving our result. □

# 3 Approximation of $F$

In this section we will prove Theorem 4, restated here:

**Theorem 4.** *Given $L/\mathbb{Q}$ a number field, and $\xi$ a Grossencharacter of $L$. Let $A$ be a positive integer and $B$ a suitably large multiple of $A$. Then if $X$ is a positive number, $z=\log^B(X)$, and $\alpha$ any real number, then*

$$\left|F^{\flat}_{L,\xi,X,z}(\alpha)\right| = O\left(X\log^{-A}(X)\right),$$

*where the implied constant depends on $L,\xi,A,B$, but not on $X$ or $\alpha$.*

In order to prove Theorem 4 we will split into cases based upon whether $\alpha$ is well approximated by a rational number of small denominator. If it is (the smooth case) we proceed to use the theory of $L$-functions to approximate $F$. If $\alpha$ is not well approximated (the rough case), we generalize results on exponential sums over primes to show that $|F|$ is small. In either case, the approximation of $F^{\sharp}$ is not difficult to approximate.

In particular we note that by Dirichlet's approximation Theorem, we can always find a pair $(a,q)$ with $a$ and $q$ relatively prime and $q<M=\Theta(X\log^{-B}(X))$ with $\left|\alpha-\frac{a}{q}\right|\leq\frac{1}{qM}$. We consider the smooth case to be the one where $q\leq z$.

## 3.1 $\alpha$ Smooth

In this Section we will prove the following Proposition:

**Proposition 6.** *Let $L$ be a number field, and $\xi$ a Grossencharacter. If $z = \log^B(X)$, $Y \leq X$ and $\alpha = \frac{a}{q}$ with $a$ and $q$ relatively prime and $q \leq z$, then for some constant $c > 0$ (depending only on $L$, $\xi$ and $B$),*

$$|F^\flat_{L,\xi,Y,z}(\alpha)| = O\left(X \exp\left(-c\sqrt{\log(X)}\right)\right).$$

We note that this result can easily be extended to all smooth $\alpha$. In particular we have:

**Corollary 7.** *Let $L$ and $\xi$ be as above. Let $A$ be a constant, and $B$ a sufficiently large multiple of $A$. Let $z = \log(X)^B$. Suppose that $\alpha = \frac{a}{q} + \theta$ with $a$ and $q$ relatively prime, $q \leq z$ and $|\theta| \leq \frac{1}{qM}$. Then*

$$|F^\flat_{L,\xi,X,z}(\alpha)| = O(X \log^{-A}(X)).$$

*Given Proposition 6.* Noting that if $F^\flat_{L,\xi,X}(\alpha) = \sum_{n \leq X} a_n e(\alpha n)$, then by Able summation and Proposition 6,

$$\begin{aligned}
F^\flat_{L,\xi,X}(\alpha) &= \sum_{n \leq X} a_n e\left(\frac{na}{q}\right) e\left(n\theta\right) \\
&= (1 - e(\theta)) \left( \sum_{Y \leq X} F^\flat_{L,\xi,Y}\left(\frac{a}{q}\right) e(Y\theta) \right) + F^\flat_{L,\xi,X}\left(\frac{a}{q}\right) e((X+1)\theta) \\
&= O\left(X^{-1} \log^B(X)\right) \left( \sum_{Y \leq X} O\left(X \log^{-A-B}(X)\right) \right) + O\left(X \log^{-A-B}(X)\right) \\
&= O\left(X \log^{-A}(X)\right).
\end{aligned}$$

□

In order to prove Proposition 6 we will need to separately approximate $F$ and $F^\sharp$. For the former we will also need to review some basic facts about Hecke $L$-functions.

### 3.1.1 Results on $L$-functions

We consider $L$-functions of the form $L(\xi\chi, s)$ where $\chi$ is a Dirichlet character thought of as a Grossencharacter via $\chi(\mathfrak{a}) = \chi(N_{L/\mathbb{Q}}(\mathfrak{a}))$. We let $d$ be the degree of $L$ over $\mathbb{Q}$, and let $D_L$ be the discriminant. We let $\mathfrak{m}$ be the modulus of the character $\xi$, and $q$ the modulus of $\chi$. We note that $\xi\chi$ has modulus at most $q\mathfrak{m}$. Therefore by [1], in the paragraph above Theorem 5.35, $L(\xi\chi)$ has conductor $\mathfrak{q} \leq 4^d |d_K| N(\mathfrak{m}) q^d$, and by Theorem 5.35 of [1], for some constant $c$ depending only on $L$, $L(\xi\chi, s)$ has no zero in the region

$$\sigma > 1 - \frac{c}{d \log(|d_K| N(\mathfrak{m}) q^d (|t| + 3))}$$

except for possibly one Siegel zero. Note also that $L(\xi\chi, s)$ has a simple pole at $s = 1$ if $\xi = \bar{\chi}$, and otherwise is holomorphic. Noting that

$$\frac{-L'(\xi\chi, s)}{L(\xi\chi, s)} = \sum_{\mathfrak{a}} \Lambda_L(\mathfrak{a})\xi\chi(\mathfrak{a})N(\mathfrak{a})^{-s},$$

and that the $n^{-s}$ coefficient of the above is at most $d\log(n)$, we may apply Theorem 5.13 of [1] and obtain for a suitable constant $c > 0$,

$$\sum_{N(\mathfrak{a})\leq Y} \Lambda_L(\mathfrak{a})\xi(\mathfrak{a})\chi(\mathfrak{a}) = \tag{5}$$
$$rY - \frac{Y^\beta}{\beta} + O\left(Y\exp\left(\frac{-c\log Y}{\sqrt{\log Y} + 3\log(q^d) + O(1)}\right)(\log(Yq^d) + O(1))^4\right),$$

where the term $\frac{Y^\beta}{\beta}$ should be taken with $\beta$ the Siegel zero if it exists; $r = 0$ unless $\xi\chi = 1$, in which case, $r = 1$; and the implied constants may depend and $L, \xi$ but not on $\chi$ or $Y$.

In order to make use of Equation 5 we will need to prove bounds on the size of Siegel zeroes. In particular we show that:

**Lemma 8.** *Fixing $\xi$ a Grossencharacter, if $\beta$ is a Siegel zero of $L(\xi\chi, s)$ with $q$ the modulus of $\chi$, we have that for any $\epsilon > 0$,*

$$\beta > 1 - \frac{c(\epsilon)}{q^\epsilon}.$$

*Proof.* We follow the proof of Theorem 5.28 part 2 from [1], and note the places where we are different. We note that Theorem 5.35 states that we only need by concerned when $\xi\chi$ is totally real. We then consider two such $\chi$ having Siegel zeros. We use instead, $L(s) = \zeta_L(s)L(\xi\chi_1, s)L(\xi\chi_2, s)L(\xi^2\chi_1\chi_2)$, which has conductor $O(q_1q_2)^{2d}$ instead of the one listed in the book. This gives us a convexity bound on the integral term of $O((q_1q_2)^d x^{1-\beta})$, instead of the one listed. Again assuming that $\beta > 3/4$, we take $x > c(q_1q_2)^{4d}$. We notice that we still have (5.64) for $\sigma > 1 - 1/d$ sufficiently large by noting that $|\sum_{N(\mathfrak{a})\leq x} \xi\chi(\mathfrak{a})| = O(x^{1-1/d} + \max(x, q))$. Therefore, Equation (5.75) of [1] becomes

$$L(\xi\chi_2, 1) \gg (1 - \beta_1)(q_1q_2)^{-4d(1-\beta_1)}(\log(q_1q_2))^{-2}.$$

The rest of the argument from [1] follows more or less directly. □

### 3.1.2 Approximation of $F$

We prove

**Proposition 9.** *With $L, \xi, \chi, Y, r$ as above*

$$F_{L,\xi\chi,Y}(0) = rY + O\left(X\exp(-c\sqrt{X})\right). \tag{6}$$

*Proof.* Applying Lemma 8 with $\epsilon = 1 - 1/(2B)$ to Equation 5, we get that

$$\sum_{N(\mathfrak{a})\leq Y} \Lambda_L(\mathfrak{a})\xi(\mathfrak{a})\chi(\mathfrak{a}) = rY - \frac{Y^\beta}{\beta} + O\left(X\exp(-c\sqrt{\log(X)})\right)$$
$$= rY + O\left(Y\exp(-c(\epsilon)\sqrt{\log(Y)}\right) + O\left(X\exp(-c\sqrt{\log(X)})\right).$$

Noting that it holds trivially for $Y \leq \sqrt{X}$, we have that

$$F_{L,\xi\chi,Y}(0) = \sum_{N(\mathfrak{a})\leq Y} \Lambda_L(\mathfrak{a})\xi(\mathfrak{a})\chi(\mathfrak{a}) = rY + O\left(X\exp(-c\sqrt{\log(X)})\right).$$

□

### 3.1.3 Approximation of $F^\sharp$

**Proposition 10.** *With $L, \xi, \chi, Y, r$ as above, $z = \log^B(X)$,*

$$F^\sharp_{L,\xi\chi,Y}(0) = rY + O\left(X\exp(-c\sqrt{X})\right).$$

*Proof.* If $\xi\chi$ is not of the form $\chi'\circ N_{L/\mathbb{Q}}$, then $F^\sharp = 0$ and we are done. Otherwise let $\xi\chi$ be as above with $\chi'$ a character of modulus $q'$. We have that

$$\begin{aligned}
F^\sharp_{L,\chi',Y}(0) &= \sum_{n\leq Y} \Lambda_{L/\mathbb{Q}}(n)\Lambda_z(n)\chi'(n) \\
&= C(z)\sum_{n\leq Y}\sum_{d|(P(z,q'D_L),n)} \mu(d)\Lambda_{L/\mathbb{Q}}(n)\chi'(n) \\
&= C(z)\sum_{d|P(z,q'D_L)}\sum_{n=dm\leq Y} \mu(d)\Lambda_{L/\mathbb{Q}}(n)\chi'(n) \\
&= C(z)\sum_{d|P(z,q'D_L)} \mu(d)\chi'(d)\sum_{m\leq Y/d} \Lambda_{L/\mathbb{Q}}(dm)\chi'(m).
\end{aligned}$$

Consider for a moment the inner sum over $m$. It is periodic with period dividing $q'D_L$. Note that the sum over a period is 0 unless $\chi'$ is trivial on $H_L$, in which case the average value is $\overline{\chi'}(d)\frac{\phi(q'D_L)}{q'D_L}$. Since $r = 1$ if $\chi'$ vanishes on $H_L$ and $r = 0$ otherwise, we have that:

$$F^\sharp_{L,\chi,X}(0) = C(z)\left(\frac{\phi(q'D_L)}{q'D_L}\right)\sum_{\substack{d|P(z,qD_L)\\ d\leq Y}}\left(\frac{r\mu(d)X}{d} + O(qD_L)\right).$$

The sum of error term here is at most $O\left(C(z)q^2S(z,Y)\right)$ which by Lemma 5 is $O\left(Y^{1-1/(2B)}\log^2(z)q^2\exp(O(\sqrt{\log(X)}))\right)$. The remaining term is

$$rYC(z)\frac{\phi(q'D_L)}{q'D_L}\sum_{\substack{d|P(z,q'D_L)\\ d\leq Y}}\frac{\mu(d)}{d}.$$

The error introduced by extending the sum to all $d|P(z,q'D_L)$ is at most

$$O\left(YC(z)\int_Y^\infty S(z,y)y^{-2}dy\right)$$

. By Lemma 5 this is

$$O\left(Y^{1-1/(2B)}\log(z)\exp(O(\sqrt{\log(X)}))\right).$$

Once we have extended the sum we are left with

$$\begin{aligned} rYC(z)\frac{\phi(q'D_L)}{q'D_L}\sum_{d|P(z,q'D_L)}\frac{\mu(d)}{d} &= rYC(z)\left(\frac{\phi(q'D_L)}{q'D_L}\right)\left(\frac{\phi(P(z,q'D_L))}{P(z,q'D_L)}\right) \\ &= rYC(z)\left(\frac{\phi(P(z))}{P(z)}\right) \\ &= rY. \end{aligned}$$

Hence

$$F^\sharp_{L,\xi_\chi,Y,z}(0) = rY + O\left(Y^{1-1/(2B)}\log^2(z)q^2\exp(O(\sqrt{\log(X)}))\right).$$

After splitting into cases based upon whether or not $Y$ is less than $\sqrt{X}$ it follows that

$$F^\sharp_{L,\xi_\chi,Y,z}(0) = rY + O\left(X\exp(-c\sqrt{X})\right).$$

□

### 3.1.4 Proof of Proposition 6

*Proof.* Combining Propositions and we obtain that

$$F^\flat_{L,\xi_\chi,Y,z}(0) = O\left(X\exp(-c\sqrt{X})\right).$$

Our Proposition follows immediately after noting that

$$F^\flat_{L,\xi,X,z}\left(\frac{a}{q}\right) = \sum_\chi e_\chi F^\flat_{L,\xi_\chi,X,z}(0).$$

Where $e_\chi$ is the appropriate Gauss sum. □

## 3.2 $\alpha$ Rough

In this section we will show that $|F^\flat(\alpha)|$ is small for $\alpha$ not well approximated by a rational of small denominator. We will do this by showing that both $|F(\alpha)|$ and $|F^\sharp(\alpha)|$ are small. The proof of the latter will resemble the proof of Proposition 3.1.4. The proof of the former will require some machinery including some Lemmas about rational approximations and exponential sums of polynomials.

### 3.2.1 Bounds on $F^\sharp$

**Proposition 11.** *Fix $L$ a number field, and $\xi$ a Grossencharacter. Fix $B$ and let $z = \log^B(X)$. Let $\alpha$ be a real number. If there exist relatively prime integers $a$ and $q$ so that*

$$\left|\alpha - \frac{a}{q}\right| < \frac{1}{q^2},$$

*then,*

$$|F^\sharp_{L,\xi,z}(\alpha)| = O\left(X\log(X)\log(z)q^{-1} + q\log(q)\log(z) + X^{1-1/(4B)}\exp(O(\sqrt{\log(X)}))\right).$$

*Proof.* We note that the result is trivial unless $\xi = N_{L/\mathbb{Q}}(\chi)$ for some Dirichlet character $\chi$ of modulus $Q$. Hence we may assume that

$$F^\sharp_{L,\xi,z}(\alpha) = \sum_{n\leq X} \Lambda_{L/\mathbb{Q}}(n)\Lambda_z(n)\chi(n)e(\alpha n).$$

Let $D_L$ be the discriminant of $L$. We note that

$$\begin{aligned}
F^\sharp_{L,\xi,z}(\alpha) &= \sum_{n\leq X} \Lambda_{L/\mathbb{Q}}(n)\Lambda_z(n)\chi(n)e(\alpha n) \\
&= C(z)\sum_{n\leq X}\sum_{d|(n,P(z,QD_L))} \mu(d)\Lambda_{L/\mathbb{Q}}(n)\chi(n)e(\alpha n) \\
&= C(z)\sum_{d|P(z,QD_L)} \mu(d)\chi(d)\sum_{md=n\leq X} \Lambda_{L/\mathbb{Q}}(dm)\chi(m)e(\alpha dm) \\
&\leq C(z)\sum_{d|P(z,QD_L)} \left|\sum_{m\leq X/d} \Lambda_{L/\mathbb{Q}}(dm)\chi(m)e(\alpha dm)\right|.
\end{aligned}$$

In order to analyze the last sum, we split it based on the conjugacy class of $m$ modulo $QD_L$. These each gives geometric series with ratio of terms $e(\alpha QD_L d)$. Hence we can bound this sum as $\min\left(\frac{X}{d}, \frac{QD_L}{2||dQD_L\alpha||}\right)$, where $||x||$ is the distance from $x$ to the nearest integer. Therefore we have that

$$|F^\sharp_{\chi,z}(\alpha)| = O\left(C(z)\sum_{d\leq X^{1-1/(4B)}} \min\left(\frac{X}{d}, \frac{QD_L}{2||dQD_L\alpha||}\right) + C(z)X^{1/4B}S(z,X)\right).$$

We bound the sum in the first term by looking at what happens as $d$ ranges over an interval of length $\frac{q}{3QD_L}$. We get that $dQD_L\alpha = x_0 + kQ\alpha$ for $x_0$ the value at the beginning of the interval and $k$ an integer at most $\frac{q}{3QD_L}$. Notice that $kQD_L\alpha$ is within $\frac{1}{3q}$ of $\frac{kQD_L a}{q}$, which must be distinct for different values of $k$. Hence none of the fractional parts of $dQD_L\alpha$ can be within $\frac{1}{3q}$ of each other. Hence the sum over this range of $d$ is at most $\frac{X}{d} + \frac{2QD_L}{2/(3q)} + \frac{2QD_L}{2(2/2q)} + \ldots =$

$O\left(\frac{X}{d} + 3qQD_L \log(q)\right)$. Since we have $3QD_L X^{1-1/(4B)}/q + 1$ of these intervals the first term is at most

$$O\left(X + \frac{X}{(q/(3QD_L))} + \frac{X}{2(q/(3QD_L))} + \ldots + 9Q^2 D_L^2 \log(q) X^{1-1/(4B)} + 3qQD_L \log(q)\right)$$
$$= O\left(X \log(X) q^{-1} + \log(q) X^{1-1/(4B)} + q \log(q)\right).$$

The other term is bounded by Lemma 5 as

$$O\left(\log(z) X^{1-1/(4B)} \exp\left(O(\sqrt{\log(X)})\right)\right).$$

Putting it together we get that

$$|F^{\sharp}_{L,\xi,z}(\alpha)| = O\left(X \log(X) \log(z) q^{-1} + q \log(q) \log(z) + X^{1-1/(4B)} \exp(O(\sqrt{\log(X)})\right).$$

□

### 3.2.2 Lemmas on Rational Approximation

In the coming Sections we will need some results on rational approximation of numbers. In particular we will need to know how often multiples of a given $\alpha$ have a good rational approximation. In order to discuss these issues we first make the following definition:

**Definition.** *We say that a real number $\alpha$ has a* rational approximation with denominator $q$ *if there exists relatively prime integers $a$ and $q$ so that*

$$\left|\alpha - \frac{a}{q}\right| < \frac{1}{q^2}.$$

We now prove a couple of Lemmas about it.

**Lemma 12.** *Let $X, Y, A$ be positive integers. Let $\alpha$ be a real number with rational approximation of denominator $q$. Suppose that for some $B$, that $XYB^{-1} > q > B$. Then for all but $O\left(Y\left(A^{1/2}B^{-1/2} + A^2B^{-1} + \log(AY)A^3X^{-1}\right)\right)$ of the integers $n$ with $1 \le n \le Y$, $n\alpha$ has a rational approximation with denominator $q'$ for some $XA^{-1} > q' > A$.*

*Proof.* By Dirichlet's approximation theorem, $n\alpha$ always has a rational approximation $\frac{a}{q'}$ with $q' < XA^{-1}$ and

$$\left|n\alpha - \frac{a}{q'}\right| < \frac{1}{q' XA^{-1}}.$$

Therefore, $n\alpha$ lacks an appropriate rational approximation only when the above has a solution for some $q' \le A$. If such is the case then dividing by $n$ we find that $\alpha$ is within $(q')^{-1}n^{-1}X^{-1}A$ of some rational number of denominator $d$ so that $d|nq'$. Note that this error is at most $d^{-1}X^{-1}A$.

Given such a rational approximation to $\alpha$ with denominator $d$, we claim that it contributes to at most $YA^2d^{-1}$ bad $n$'s. This is because there are at most $A$ values of $q'$. Furthermore, for each value of $q'$, we still need that $n$ is a multiple of $\frac{d}{(d,q')} \geq dA^{-1}$. Hence for each $q'$, there are at most $YAd^{-1}$ bad $n$.

Next we pick an integer $n_0$. We will now consider only $Y \geq n \geq n_0$ so that $\alpha n$ has no suitable rational approximation. We do this by analyzing the denominators $d$ for which some rational number of denominator $d$ approximates $\alpha$ to within $X^{-1}A(\max(d, n_0))^{-1}$. Suppose that we have some $d \neq q$ which does this. $\alpha$ is within $q^{-2}$ of a number with denominator $q$, and within $X^{-1}n_0^{-1}A$ of one with denominator $d$. These two rational numbers differ by at least $(dq)^{-1}$ and therefore

$$(dq)^{-1} \leq q^{-2} + X^{-1}An_0^{-1}.$$

Hence either $dq^{-1}$ or $X^{-1}An_0^{-1}dq$ is at least $\frac{1}{2}$. Hence either $d \geq \frac{q}{2}$, or

$$d \geq \frac{Xn_0}{2Aq} \geq \frac{n_0B}{2AY}.$$

Therefore the smallest such $d$ is at least the minimum of $\frac{q}{2}$ and $\frac{n_0B}{2AY}$.

Next suppose that we have two different such denominators, say $d$ and $d'$. The fractions they represent are separated by at least $(dd')^{-1}$ and yet are both close to $\alpha$. Therefore

$$(dd')^{-1} \leq X^{-1}A(d^{-1} + d'^{-1}).$$

Therefore we have that $\max(d, d') \geq \frac{X}{2A}$. Hence there is at most one denominator less than $\frac{X}{2A}$.

Next we wish to bound the number of such denominators $d$ in a dyadic interval $[K, 2K]$. We note that the corresponding fractions are all within $X^{-1}AK^{-1}$ of $\alpha$, and that any two are separated by at least $(2K)^{-2}$. Therefore the number of such $d$ is at most $1 + 8KX^{-1}A$.

To summarize we potentially have the following $d$ each giving at most $YA^2d^{-1}$ bad $n$'s.

- One $d$ at least $\frac{q}{2}$.
- One $d$ at least $\frac{n_0B}{2AY}$
- For each diadic interval $[K, 2K]$ with $K \geq \frac{X}{2A}$ at most $10KX^{-1}A$ such $d$'s

Notice that there are $\log(2AY)$ such diadic intervals, and that each contributes at most $10YA^3X^{-1}$ bad $n$'s. We also potentially have $n_0$ bad $n$'s from the numbers less than $n_0$. Hence the number of $n$ for which there is no suitable rational approximation of $n\alpha$ is at most

$$O\left(n_0 + YA^2B^{-1} + Y^2AB^{-1}n_0^{-1} + \log(AY)YA^3X^{-1}\right).$$

Substituting $n_0 = YA^{1/2}B^{-1/2}$ yields our result. □

We will also need the following related Lemma:

**Lemma 13.** *Let $X, A, C$ be positive integers. Let $\alpha$ be a real number with rational approximation of denominator $q$. Suppose that for some $B > 2A$, that $XB^{-1} > q > B$. Then there exists a set $S$ of natural numbers so that*

- *elements of $S$ are of size at least $\Omega(BA^{-1})$.*
- *The sum of the reciprocals of the elements of $S$ is $O(A^3B^{-1} + X^{-1}A^4C)$.*
- *for all positive integers $n \leq C$, either $n$ is a multiple of some element of $S$ or $n\alpha$ has a rational approximation with some denominator $q'$ with $XA^{-1}n^{-1} > q' > A$.*

*Proof.* We use the same basic techniques as the proof of Lemma 12. We note that $n\alpha$ always has a rational approximation $\frac{a}{q'}$ accurate to within $\frac{1}{q'XA^{-1}n^{-1}}$ with $q' < XA^{-1}n^{-1}$. This means that we have an appropriate rational approximation of $n\alpha$ unless this $q'$ is less than $A$. In that case it holds that

$$\left|\alpha - \frac{a}{nq'}\right| \leq \frac{1}{q'XA^{-1}}.$$

Hence to each such $n$ we can assign a rational approximation $\frac{a}{nq'}$ of $\alpha$. The $m$ that are assigned to a rational approximation $\frac{a}{d}$ are those so that

$$m\left|\alpha - \frac{a}{d}\right| \leq \frac{1}{XA^{-1}m^{-1}D}$$

where $D$ is the denominator of $\frac{ma}{d}$. $D = \frac{d}{(m,d)}$. It must also be the case that $D$ is at most $A$. Hence it suffices to let $S$ be the union of all $\frac{d}{D}$ where $A \geq D$, $D|d$ and

$$\left|\alpha - \frac{a}{d}\right| \leq \frac{1}{XA^{-1}D} \leq \frac{1}{XA^{-1}}.$$

We have to show that the elements of $S$ are big enough and that the sum of their reciprocals satisfies the appropriate bound. Note that for each such $d$, it contributes at most $O\left(\frac{A^2}{d}\right)$ to the sum of reciprocals.

First off we should note that if we have any such denominator $d$ other than $q$, $\alpha$ is within $q^{-2}$ of a rational number of denominator $q$ and within $X^{-1}A$ of one of denominator $d$. Hence we have that

$$(dq)^{-1} \leq q^{-2} + X^{-1}A.$$

Hence

$$d \geq \min\left(\frac{q}{2}, \frac{X}{2A}\right).$$

Note that in any case $\frac{d}{A} = \omega(BA^{-1})$, and hence contributes at most $O(A^3B^{-1})$ to the sum of reciprocals.

Next note that if we have two of these approximations with denominators $d$ and $d'$ that

$$(dd')^{-1} \leq 2XA^{-1}.$$

Therefore the second largest such $d$ is at least $\sqrt{2XA^{-1}}$.

Next we consider the contribution from all such approximations with $d$ lying in a diadic interval $[K, 2K]$ all of these approximations are within $X^{-1}A$ of $\alpha$ and are separated from each other by at least $\frac{1}{4K^2}$. Therefore, there are at most $1 + 8X^{-1}AK^2$. If we ensure that $K$ is at least $\sqrt{2XA^{-1}}$, this is $O(X^{-1}AK^2)$. Hence all of these $d$'s contribute at most $O(X^{-1}A^3K)$ to the sum of reciprocals. Furthermore we can ignore terms with $K > AC$. Taking the sum over intervals we get at most $O(X^{-1}A^4C)$.

□

We will be using Lemma 13 to bound the number of ideals of $L$ so that $N(\mathfrak{a})\alpha$ has a good rational approximation. In order to do this we will also need the following:

**Lemma 14.** *Fix $L$ be a number field. Let $n$ be a positive integer, and let $X$ and $\epsilon$ be positive real numbers. Then we have that:*

$$\sum_{\substack{n|N(\mathfrak{a}) \\ N(\mathfrak{a})<X}} \frac{1}{N(\mathfrak{a})} = O\left(\frac{X\log(X)n^{\epsilon}}{n}\right),$$

$$\sum_{\substack{n|N(\mathfrak{ab}) \\ N(\mathfrak{ab})<X}} \frac{1}{N(\mathfrak{ab})} = O\left(\frac{X\log^2(X)n^{\epsilon}}{n}\right).$$

*(The first sum is over ideals $\mathfrak{a}$ with norm a multiple of $n$ and $\leq X$, the second over pairs of ideals $\mathfrak{a}$ and $\mathfrak{b}$, the norm of whose product satisfies the same condition).*

*Proof.* We will prove the first of the two equations and note that the second follows from a similar argument. Let $d = [L : \mathbb{Q}]$. Let $p_1, \ldots, p_k$ be the distinct primes dividing $n$. We claim that for such an ideal $\mathfrak{a}$ must be a multiple of some ideal $\mathfrak{a}_0$ with $N(\mathfrak{a}_0) = nm$ with $m = \prod_{i=1}^{k} p_i^{a_i}$ for some $0 \leq a_i < d$. We obtain this by starting with the ideal (1) and repeatedly multiplying by primes of $\mathfrak{a}$ whose norm is a power of one of the $p_i$ (noting that this exponent is at most $d$). We note that the number of possible values of $m$ is $k^d$. Since $k = O(\log(n))$ this is $O(n^{\epsilon})$. For each value of $m$ there are $O(n^{\epsilon})$ ideals of norm exactly $nm$, and hence there are $O(n^{\epsilon})$ possible ideals $\mathfrak{a}_0$.

We now need to bound the sum over ideals $\mathfrak{b}$ so that the norm of $\mathfrak{a}_0\mathfrak{b}$ is at most $X$ of $\frac{1}{N(\mathfrak{a}_0\mathfrak{b})}$. This is at most $\frac{1}{n}$ times the sum over ideals $\mathfrak{b}$ of norm at most $X$ of $\frac{1}{N(\mathfrak{b})}$. This latter sum is $O(\log(X))$. This completes the proof. □

### 3.2.3 Lemmas on Exponential Sums

We will need a Lemma on the size of exponential sums of polynomials along the lines of Lemma 20.3 of [1]. Unfortunately, the $X^\epsilon$ term that shows up there will be unacceptable for our application. So instead we prove:

**Lemma 15.** *Pick a positive integer $X$. Let $[X] = \{1, 2, \ldots, X\}$. Let $P$ be a polynomial with leading term $cx^k$ for some integer $c \neq 0$. Let $\alpha$ be a real number with a rational approximation of denominator $q$. Then*

$$\left| \sum_{x \in [X]} e(\alpha P(x)) \right| \ll |c| X \left( \frac{1}{q} + \frac{1}{X} + \frac{q}{X^k} \right)^{10^{-k}},$$

*where the implied constant depends on $k$, but not on the other coefficients of $P$.*

*Proof.* We proceed by induction on $k$. We take as a base case $k = 1$. Then we have that $P$ is a linear function with linear term $c$. $\alpha$ is within $q^{-2}$ of a rational number of denominator $q$. Therefore $c\alpha$ is within $cq^{-2}$ of a number of denominator between $qc^{-1}$ and $q$. If $c \geq q/2$, there is nothing to prove. Otherwise, $c\alpha$ cannot be within $q^{-1} - cq^{-2} = O(q^{-1})$ of an integer. Therefore the sum is at most $O(\min(X, q))$, which clearly satisfies the desired inequality.

Squaring we find that

$$\left| \sum_{x \in [X]} e(\alpha P(x)) \right| = \left( \sum_{a,b \in [X]} e(\alpha(P(a) - P(b))) \right)^{1/2}.$$

Breaking the inner sum up based on the value of $n = a - b$, we note that $P(n + b) - P(b)$ is a polynomial of degree $k - 1$ with leading term $nckx^{k-1}$. Letting $[X_n]$ be the interval of length $X - |n|$ that $b$ could be in given that $b \in [X]$ and $b + n \in [X]$, we are left with at most

$$\left( \sum_{n \in [-X, X]} \left| \sum_{b \in [X_n]} e(\alpha(P(b + n) - P(b))) \right| \right)^{1/2}.$$

Let $B = \min(q, X^k/q)$. We consider separately the terms in the above sum where $n\alpha$ has no rational approximation with denominator between $B^{1/5}$ and $X^{k-1}B^{-1/5}$. We note by Lemma 12 that the number of such $n$ is at most $O(X(B^{-2/5} + \log(X)B^{3/5}X^{1-k}))$. Each of those terms contributes $O(X)$ to the sum and hence together they contribute at most

$$O(X(B^{-1/5} + \log(X)B^{3/10}X^{(1-k)/2})).$$

Which is within the required bounds.

For the other terms, the inductive hypothesis tells us that the sum for fixed $n$ is at most

$$O\left( |c| X \left( B^{-1/5} + \frac{1}{X - |n|} + \frac{X^{k-1}B^{-1/5}}{(X - |n|)^{k-1}} \right)^{-5^{k-1}} \right).$$

Summing over $n$ and taking a square root gives an appropriate bound. $\square$

We apply this Lemma to get a bound on exponential sums of norms of ideals of a number field. In particular we show that:

**Lemma 16.** *Fix $L$ a number field of degree $d$, and $\xi$ a Grossencharacter of modulus $\mathfrak{m}$. Then given a positive number $X$ and a real number $\alpha$ which has a rational approximation of denominator $q$, we have that*

$$\left| \sum_{N(\mathfrak{a}) \leq X} \xi(\mathfrak{a}) e(\alpha N(\mathfrak{a})) \right| = O\left( X \left( \frac{1}{q} + \frac{1}{X^{1/d}} + \frac{q}{X} \right)^{10^{-d}/2} \right).$$

*Proof.* First we split the sum up into ideal classes modulo $\mathfrak{m}$. In order to represent an element of such a class we note that for $\mathfrak{a}_0$ a fixed element of such a class then other elements $\mathfrak{a}$ in the same class correspond to points $\frac{\mathfrak{a}}{\mathfrak{a}_0}$ in some quadrant of a lattice in $L \otimes \mathbb{R}$. Note that points in this lattice over count these ideals since if two differ by an element of $O_L^*$, they correspond to the same ideal. On the other hand if we take some fundamental domain of the elements of unit norm in $L \otimes \mathbb{R}$ modulo $O_L^*$ and consider its positive multiples, we get a smoothly bounded region, $R$ whose lattice points correspond exactly to the ideals in this region. Notice that the norm is a polynomial form of degree $d$ on $R$. By taking $R$ intersected with the points of norm at most $X$ we get a region $R_X$ whose lattice points correspond exactly to the ideals in this class of norm at most $X$. Let $Y = (qX)^{1/2d}$. We attempt to partition these lattice points into segments of length $Y$ with a particular orientation. The number that we fail to include is proportional to $Y$ times the surface area of $R_X$ which is $O(YX^{1-1/d})$. On each interval, we attempt to approximate $\xi$ by a constant. We note that on this region $\xi$ is a smoothly varying function of $x/(N(x))^{1/d}$. Therefore the error introduced at each point, $x$, is $O(YN(x)^{-1/d})$. The summed value over these points of $N(x)^{-1/d}$ is by Able Summation $O(\int_{x=0}^{X} x^{-1/d} dx) = O(X^{1-1/d})$, thus producing another error of size at most $O(YX^{1-1/d})$. We are left with $O(XY^{-1})$ intervals of length $Y$ of the exponential sum of $e(\alpha N(x))$. Recalling that $N(x)$ is a polynomial of degree $d$ with rational leading coefficient with bounded numerator and denominator, we may (perhaps after looking at only every $k^{th}$ point to make the leading coefficient integral) apply Lemma 15 and get that the sum over each segment is

$$O\left( Y \left( \frac{1}{q} + \frac{1}{Y} + \frac{q}{Y^d} \right)^{10^{-d}} \right).$$

Noting that each of the error terms we introduced is less than the bound given, we are done. $\square$

Able summation yields the following Corollary.

**Corollary 17.** *Fix $L$ a number field of degree $d$, and $\xi$ a Grossencharacter of modulus $\mathfrak{m}$. Then given a positive number $X$ and a real number $\alpha$ which has a rational approximation of denominator $q$, we have that*

$$\left|\sum_{N(\mathfrak{a})\leq X}\log(N(\mathfrak{a}))\xi(\mathfrak{a})e(\alpha N(\mathfrak{a}))\right| = O\left(X\log(X)\left(\frac{1}{q}+\frac{1}{X^{1/d}}+\frac{q}{X}\right)^{10^{-d}/2}\right).$$

### 3.2.4 Bounds on $F$

We are finally ready to prove our bound on $F$.

**Proposition 18.** *Fix a number field $L$ of degree $d$ and a Grossencharacter $\xi$. Let $X \geq 0$ be a real number. Let $\alpha$ be a real number with a rational approximation of denominator $q$ where $XB^{-1} > q > B$ for some $B > 0$. Then $F_{L,\xi,X}(\alpha)$ is*

$$O\left(X\left(\log^2(X)B^{-10^{-d}/12}+\log^2(X)X^{-10^{-d}/60}+\log^2(X)X^{-10^{-d}/10d}+\log^{2+d^2/2}(X)B^{-1/6}\right)\right).$$

*Where the asymptotic constant may depend on $L$ and $\xi$, but not on $X, q, B$ or $\alpha$.*

*Proof.* Our proof is along the same lines as Theorem 13.6 of [1]. We first note that the suitable generalization of Equation (13.39) of [1] still applies. Letting $y = z = X^{2/5}$, we find that $F_{L,\xi,X}(\alpha)$ equals

$$\begin{aligned}
&\sum_{\substack{N(\mathfrak{ab})\leq X\\ N(\mathfrak{a})<X^{2/5}}}\mu(\mathfrak{a})\xi(\mathfrak{a})\log(N(\mathfrak{b}))\xi(b)e(\alpha N(\mathfrak{a})N(\mathfrak{b}))\\
&-\sum_{\substack{N(\mathfrak{abc})\leq X\\ N(\mathfrak{b}),N(\mathfrak{c})\leq X^{2/5}}}\mu(\mathfrak{b})\Lambda_L(\mathfrak{c})\xi(\mathfrak{bc})\xi(\mathfrak{a})e(\alpha N(\mathfrak{bc})N(\mathfrak{a}))\\
&+\sum_{\substack{N(\mathfrak{abc})\leq X\\ N(\mathfrak{b}),N(\mathfrak{c})\geq X^{2/5}}}\mu(\mathfrak{b})\xi(\mathfrak{b})\Lambda_L(\mathfrak{c})\xi(\mathfrak{ac})e(\alpha N(\mathfrak{b})N(\mathfrak{ac}))+O(X^{2/5}).
\end{aligned}$$

The first term we bound by using Corollary 17 on the sum over $\mathfrak{b}$. Letting $A = B^{1/4} \leq X^{1/8}$, then by Lemmas 13 and 14 we can bound the sum over terms where $\alpha N(\mathfrak{a})$ has no rational approximation with denominator between $A$ and $\frac{X}{AN(\mathfrak{a})}$ by

$$O\left(X\left(\log^2(X)\left(A^3B^{-1}+X^{-3/5}A^4\right)\left(\frac{B}{A}\right)^{\epsilon}\right)\right) = O\left(X\log^2(X)B^{-1/4+\epsilon}\right).$$

For other values of $\mathfrak{b}$, Corollary 17 bounds the sum as

$$O\left(X\log^2(X)\left(B^{-1/4}+X^{-3/5d}\right)^{10^{-d}/2}\right).$$

The second term is bounded using similar considerations. We let $A = \min(B^{1/4}, X^{1/41})$, and use Lemmas 13 and 14 to bound the sum over terms with $\mathfrak{b}$ and $\mathfrak{c}$ such that $N(\mathfrak{bc})\alpha$ has no rational approximation with norm between $A$ and $\frac{X}{AN(\mathfrak{bc})}$ by

$$O\left(X\log^3(X)\left(\frac{B}{A}\right)^{\epsilon}\left(B^{-1/4}+X^{-1}A^4X^{4/5}\right)\right)$$
$$= O\left(X\log^3(X)\left(B^{-1/4+\epsilon}+X^{-1/10}\right)\right).$$

Using Lemma 16, we bound the sum over other values of $\mathfrak{b}$ and $\mathfrak{c}$ as

$$O\left(X\log^2(X)\left(A^{-1}+X^{-1/5d}\right)^{10^{-d}/2}\right).$$

The last sum, we first change to a sum over $\mathfrak{b}$ and $\mathfrak{d} = \mathfrak{a}\cdot\mathfrak{c}$. We have coefficients

$$x(\mathfrak{b}) = \mu(\mathfrak{b})\xi(\mathfrak{b}),$$

and

$$y(\mathfrak{d}) = \sum_{\substack{\mathfrak{a}\cdot\mathfrak{c}=\mathfrak{d}\\ N(\mathfrak{c})\geq X^{2/5}}} \Lambda_L(\mathfrak{c})\xi(\mathfrak{ac}).$$

We note that $|y(\mathfrak{d})| \leq \log(N(\mathfrak{d})) \leq \log(X)$. Our third term then becomes

$$\sum_{\substack{N(\mathfrak{bd})\leq X\\ N(\mathfrak{b}),N(\mathfrak{d})\geq X^{2/5}}} x(\mathfrak{b})y(\mathfrak{d})e(\alpha N(\mathfrak{b})N(\mathfrak{d})).$$

To this we apply the bilinear forms trick. First we split the sum over $\mathfrak{b}$ into parts based on which diadic interval (of the form $[K, 2K]$), the norm of $\mathfrak{b}$ lies in. Next for each of these summands we apply Cauchy-Schwartz to bound it by

$$\left(\left(\sum_{N(\mathfrak{b})\in[K,2K]}|x(\mathfrak{b})|^2\right)\left(\sum_{N(\mathfrak{b})\in[K,2K]}\left(\sum_{\substack{N(\mathfrak{d})\leq X/N(\mathfrak{b})\\ N(mfd)\geq X^{2/5}}} y(\mathfrak{d})e(\alpha N(\mathfrak{bd}))\right)^2\right)\right)^{1/2}$$
$$= O(K^{1/2})\left(\sum_{\substack{N(\mathfrak{b})\in[K,2K]\\ N(\mathfrak{d}),N(\mathfrak{d}')\leq X/N(\mathfrak{b})\\ N(\mathfrak{d}),N(\mathfrak{d}')\geq X^{2/5}}} x(\mathfrak{d})\overline{x(\mathfrak{d}')}e(\alpha N(\mathfrak{b})(N(\mathfrak{d})-N(\mathfrak{d}')))\right)^{1/2}$$
$$\leq O(K^{1/2}\log(X))\left(\sum_{\substack{X^{2/5}\leq N(\mathfrak{d}),N(\mathfrak{d}')\\ N(\mathfrak{d}),N(\mathfrak{d}')\leq X/(2K)}}\left|\sum_{\substack{N(\mathfrak{b})\in[K,2K]\\ N(\mathfrak{b})\leq X/N(\mathfrak{d})\\ N(\mathfrak{b})\leq X/N(\mathfrak{d}')}} e(\alpha(N(\mathfrak{d})-N(\mathfrak{d}'))N(\mathfrak{b}))\right|\right)^{1/2}.$$

Now we let $A = \min(B^{1/3}, X^{1/16})$. We bound terms separately based on whether or not $\alpha(N(\mathfrak{d}) - N(\mathfrak{d}'))$ has a rational approximation with denominator between $A$ and $KA^{-1}$. Applying Lemma 12 with $X = K$, $Y = XK^{-1}$ and $A$ and $B$ what they are, we get that the number of values of $N(\mathfrak{d}) - N(\mathfrak{d}')$ that cause this to happen is

$$O\left(XK^{-1}\left(B^{-1/3} + \log(X)A^4K^{-1}\right)\right) = O(XK^{-1}B^{-1/3}).$$

Let $B(\alpha)$ be the sum over such $n$ of $e(\alpha n)$. Let $H(\alpha) = \sum_{X^{2/5} \leq N(\mathfrak{a}) \leq X/K} e(\alpha N(\mathfrak{a}))$. Then the number of pairs of $\mathfrak{d}$ and $\mathfrak{d}'$ such that there is no rational approximation with appropriate denominator is

$$\int_0^1 B(\alpha)|H(\alpha)|^2 d\alpha.$$

This is at most $XK^{-1}B^{-1/3}$ times the $L^2$ norm of $H$ squared. This latter term is $\sum_{X^{2/5} \leq n \leq X/K} W(n)^2$, where $W(n)$ is the number of ways of writing $n$ as the norm of an ideal in $L$. Notice that $W^2(n)$ is at most $\tau_d^2(n)$, where $\tau_d(n)$ is the number of ways of writing $n$ as a product of $d$ integers. We know this because $W$ is multiplicative and if we write a power of a prime $p$ as the norm of an ideal, $\mathfrak{a}$, factoring $\mathfrak{a}$ into its primary parts gives a representation of $n$ as a product of $d$ integers. We therefore have that $W^2(n) \leq \tau_{d^2}(n)$ and hence the above sum is $O(XK^{-1}\log^{d^2}(X))$. Hence the total contribution from terms with such $\mathfrak{d}$ and $\mathfrak{d}'$ is at most

$$O\left(\left(K^{1/2}\log(X)\right)\left(K\left(XK^{-1}B^{-1/3}\right)\left(XK^{-1}\log^{d^2}(X)\right)\right)^{1/2}\right)$$
$$= O\left(X\log^{1+d^2/2}(X)B^{-1/6}\right).$$

And the sum over $K$ of these terms is at most

$$O\left(X\log^{2+d^2/2}(X)B^{-1/6}\right).$$

On the other hand, the sum over $\mathfrak{d}$ and $\mathfrak{d}'$ so that $\alpha(N(\mathfrak{d}) - N(\mathfrak{d}'))$ has a rational approximation with appropriate denominator is bounded by Lemma 16 by

$$O\left(\left(K^{1/2}\log(X)\right)\left(\left(XK^{-1}\right)^2 K\left(A^{-1} + K^{-1/d}\right)^{10^{-d}/2}\right)^{1/2}\right)$$
$$= O\left(X\log(X)\left(A^{-1} + K^{-1/d}\right)^{10^{-d}/4}\right).$$

Summing over all of the intervals we get

$$O\left(X\log^2(X)\left(A^{-1} + X^{-2/5d}\right)^{10^{-d}/4}\right).$$

Putting this all together, we get the desired bound for $F$. □

### 3.3 Putting it Together

We are finally prepared to prove Theorem 4.

*Proof.* We note that $\alpha$ can always be approximated by $\frac{a}{q}$ for some relatively prime integers $a, q$ with $q \leq X \log^{-B}(X)$ so that

$$\left|\alpha - \frac{a}{q}\right| \leq \frac{1}{qX \log^{-B}(X)}.$$

We split into cases based upon weather $q \leq z$.

If $q \leq z$ our result follows from Corollary 7.

If $q \geq z$, our result follows from Propositions 11 and 18. □

## 4 Approximation of $G$

Here we prove Theorem 3. We restate it here:

**Theorem 3.** *Let $K/\mathbb{Q}$ be a finite Galois extension, and let $C$ be a conjugacy class of $Gal(K/\mathbb{Q})$. Let $A$ be a positive integer and $B$ a suitably large multiple of $A$. Then if $X$ is a positive number, $z = \log^B(X)$, and $\alpha$ any real number, then*

$$\left|G^{\flat}_{K,C,X,z}(\alpha)\right| = O\left(X \log^{-A}(X)\right),$$

*where the implied constant depends on $K, C, A, B$, but not on $X$ or $\alpha$.*

*Proof.* Recall Proposition 2 which states that

$$G_{K,C,X}(\alpha) = \frac{|C|}{|G|}\left(\sum_{\chi} \overline{\chi}(c) F_{L,\chi,X}(\alpha)\right) + O(\sqrt{X}).$$

Therefore we know that $G_{K,C,X}(\alpha)$ is within $O(\sqrt{X})$ of

$$\frac{|C|}{|G|}\left(\sum_{\chi} \overline{\chi}(c) F_{L,\chi,X}(\alpha)\right).$$

Applying Theorem 4, this is within $O\left(X \log^{-A}(X)\right)$ of

$$\begin{aligned}\frac{|C|}{|G|}\left(\sum_{\chi} \overline{\chi}(c) F^{\sharp}_{L,\chi,X,z}(\alpha)\right) &= \frac{|C|}{|G|}\left(\sum_{\chi}\sum_{n\leq X} \overline{\chi}(c)\Lambda_{L/\mathbb{Q}}(n)\Lambda_z(n)\chi(n)e(\alpha n)\right) \\ &= \frac{|C|}{|G|}\left(\sum_{n\leq X} \Lambda_z(n)e(\alpha n)\left(\Lambda_{L/\mathbb{Q}}(n)\sum_{\chi}\overline{\chi}(c)\chi(n)\right)\right).\end{aligned}$$

Note that in the above, $\chi$ is summed over characters of $\mathrm{Gal}(K/L)$ and that $\chi(n)$ is taken to be 0 unless $\chi$ can be extended to a character of $\mathrm{Gal}(K/\mathbb{Q})^{ab}$, in which

case $\chi(n)$ is well defined for $n \in H_L$. Notice also that $\chi(n)$ being undefined for $n \notin H_L$ does not matter since $\Lambda_L(n)$ is 0 in those cases. We wish the evaluate the inner sum over $\chi$ in the case where $n \in H_L$.

Let the kernel of the map $\langle c \rangle \to \mathrm{Gal}(K/\mathbb{Q})^{ab}$ be generated by $c^k$ for some $k|\mathrm{ord}(c)$. Then $\chi(n)$ is 0 unless $\chi(c^k) = 1$. Therefore we can consider the sum as being over characters $\chi$ of $\langle c \rangle / c^k$. Taking $K^a$ to be the maximal abelian subextension of $K$ over $\mathbb{Q}$, this sum is then $k$ if $[K^a/\mathbb{Q}, n] = c$ and 0 otherwise. Hence this sum is non-zero if and only if $n \in H_C$. The index of $H_C$ in $H_L$ is $[H_L : H_K]$, which is in turn the size of the image of $\langle c \rangle$ in $\mathrm{Gal}(K/\mathbb{Q})^{ab}$, or $|\langle c \rangle / \langle c^k \rangle| = k$. Hence $\Lambda_L(n) \sum_\chi \overline{\chi}(c)\chi(n) = \Lambda_{K,C}(n)$. Therefore $G_{K,C,X}(\alpha)$ is within $O\left(X \log^{-A}(X)\right)$ of

$$\frac{|C|}{|G|} \sum_{n \leq X} \Lambda_{K,C}(n)\Lambda_z(n)e(\alpha n) = G^\sharp_{K,C,X,z}(\alpha).$$

□

# 5 Proof of Theorem 1

We now have all the tools necessary to prove Theorem 1. Our basic strategy will be as follows. We first define a generating function $H$ for the number of ways to write $n$ as $\sum_i a_i p_i$ for $p_i$ primes satisfying the appropriate conditions. It is easy to write $H$ in terms of the function $G$. First we will show that if $H$ is replaced by $H^\sharp$ by replacing these $G$'s by $G^\sharp$'s, this will introduce only a small change (in an appropriate norm). Dealing with $H^\sharp$ will prove noticeably simpler than dealing with $H$ directly. We will essentially be able to approximate the coefficients of $H^\sharp$ using sieving techniques. Finally we combine these results to prove the Theorem.

## 5.1 Generating Functions

We begin with some basic definitions.

**Definition.** *Let $K_i, C_i, a_i, X$ be as in the statement of Theorem 1. Then we define*

$$S_{K_i,C_i,a_i,X}(n) := \sum_{\substack{p_i \leq X \\ [K_i/\mathbb{Q},p_i]=C_i \\ \sum_i a_i p_i = n}} \prod_{i=1}^{k} \log(p_i).$$

*(i.e. the left hand side of Equation 1). We define the generating function*

$$H_{K_i,C_i,a_i,X}(\alpha) := \sum_n S_{K_i,C_i,a_i,X}(n)e(n\alpha).$$

*Notice that this is everywhere convergent since there are only finitely many non-zero terms.*

We know from basic facts about generating functions that

$$H_{K_i,C_i,a_i,X}(\alpha) = \prod_{i=1}^{k} G_{K_i,C_i,X}(a_i\alpha). \tag{7}$$

We would like to approximate the $G$'s by corresponding $G^\sharp$'s. Hence we define

**Definition.**

$$H^\sharp_{K_i,C_i,a_i,z,X}(\alpha) := \prod_{i=1}^{k} G^\sharp_{K_i,C_i,z,X}(a_i\alpha).$$

$$H^\flat_{K_i,C_i,a_i,z,X}(\alpha) := H_{K_i,C_i,a_i,X}(\alpha) - H^\sharp_{K_i,C_i,a_i,z,X}(\alpha).$$

We now prove that this is a reasonable approximation.

**Lemma 19.** *Let $A$ be a constant, and $z = \log^B(X)$ for $B$ a sufficiently large multiple of $A$. If $k \geq 3$,*

$$\left|H^\flat_{K_i,C_i,a_i,z,X}\right|_1 = O(X^{k-1}\log^{-A}(X)).$$

*If $k = 2$,*

$$\left|H^\flat_{K_i,C_i,a_i,z,X}\right|_2 = O(X^{3/2}\log^{-A}(X)).$$

*Where in the above we are taking the $L^1$ or $L^2$ norm respectively of $H^\flat_{K_1,C_i,a_i,X}$ as a function on $[0,1]$.*

*Proof.* Our basic technique is to write each of the $G$'s in Equation 7 as $G^\sharp + G^\flat$ and to expand out the resulting product. We are left with a copy of $H^\sharp$ and a number of terms which are each a product of $k$ $G^\sharp$ or $G^\flat$'s, where each such term has at least one $G^\flat$. We need several facts about various norms of the $G^\sharp$ and $G^\flat$'s. We recall that the squared $L^2$ norm of a generating function is the sum of the squares of it's coefficients.

- By Theorem 3, the $L^\infty$-norm of $G^\flat$ is $O\left(X\log^{-2A-k}(X)\right)$.
- The $L^\infty$ norm of $G^\sharp$ is clearly $O\left(X\log\log(X)\right)$.
- $|G^\sharp|_2^2 = O(X\log\log^2(X))$.
- $|G|_2^2 = O(X\log(X))$.
- Combining the last two statements, we find that $|G^\flat|_2^2 = O(X\log(X))$.

For $k \geq 3$, we note that by Cauchy-Schwartz the $L^1$ norm of a product of $k$ functions is at most the products of the $L^2$ norms of two of them times the products of the $L^\infty$ norms of the rest. Using this and ensuring that at least one of the terms we take the $L^\infty$ norm of is a $G^\flat$, we obtain our bound on $|H^\flat|_1$.

For $k = 2$, we note that the $L^2$ norm of a product of two functions is at most the $L^2$ norm of one times the $L^\infty$ norm of the other. Applying this to our product, ensuring that we take the $L^\infty$ norm of a $G^\flat$ we get the desired bound on $|H^\flat|_2$. □

## 5.2 Dealing with $H^\sharp$

Now that we have shown that $H^\sharp$ approximates $H$, it will be enough to compute the coefficients of $H^\sharp$.

**Proposition 20.** *Let $A$ be a constant, and $z = \log^B(X)$ for $B$ a sufficiently large multiple of $A$. The $e(n\alpha)$ coefficient of $H^\sharp_{K_i,C_i,a_i,z,X}(\alpha)$ is given by the right hand side of Equation 1, or*

$$\left(\prod_{i=1}^{k} \frac{|C_i|}{|G_i|}\right) C_\infty C_D \left(\prod_{p \nmid D} C_p\right) + O\left(X^{k-1} \log^{-A}(X)\right).$$

*Proof.* We note that the quantity of interest is equal to

$$\left(\prod_{i=1}^{k} \frac{|C_i|}{|G_i|}\right) \sum_{\substack{n_1,\ldots,n_k \leq X \\ \sum_{i=1}^k a_i n_i = n}} \left(\prod_{i=1}^{k} \Lambda_{K_i,C_i}(n_i)\right) \left(\prod_{i=1}^{k} \Lambda_z(n_i)\right). \tag{8}$$

First we consider the number of tuples of $n_i$ that we are summing over. Making a linear change of variables with determinant 1 so that one of the coordinates is $x = \sum_i a_i n_1$, we notice that we are summing over the lattice points of some covolume 1 lattice in a convex region with volume $C_\infty$ and surface area $O\left(X^{k-2}\right)$. Therefore if some affine sublattice $L$ of the set of tuples of integers $(n_i)$ so that $\sum_i a_i n_i = n$ of index $I$ is picked, the number of tuples $(n_i)$ in our sum in this class is $C_\infty/I + O(X^{k-2})$. We can write $\Lambda_{K_i,C_i}(n)$ as a sum of indicator functions for congruences classes of $n$ modulo $d$. We can also write $\Lambda_z(n) = C(z) \sum_{d|(n,P(z))} \mu(d)$ another sum over sublattices. Hence we can write the expression in Equation 8 as a constant (which is $O(C(z))^k$) times the sum over certain affine sublattices of $L$ of $\pm 1$ times the number of points of the intersection of this sublattice with our region. These sublattices are of the following form:

$$\{n_i : \sum_i a_i n_i = n, n_i \equiv x_i \pmod{D}, d_i | n_i\},$$

where $d_i$ are chosen elements of $H_i \subseteq (\mathbb{Z}/D\mathbb{Z})^*$, and $d_i | P(z)$ are integers.

We first claim that the contribution from terms with any $d_i$ bigger than $X^{1/(2k)}$ is negligible. In fact, these terms cannot account for more than

$$O(C(z)^k)k \sum_{\substack{d|P(z) \\ d \geq X^{1/(2k^2)}}} \frac{X^{k-1}}{d} = O(\log\log(X)^k) \int_{X^{1/(2k)}}^{\infty} X^{k-1} S(z,y) y^{-2} dy$$

$$= O\left(X^{k-1-1/((2B)(2k))} \exp\left(O\left(\sqrt{\log(X)}\right)\right)\right).$$

(Using Lemma 5 to bound the integral above). Throwing out these terms, we would like to approximate the number of tuples in our sum in each of these sublattices by $C_\infty$ over the index. The error introduced is $O\left(\log\log^k(X) X^{k-2}\right)$

per term times $O\left(X^{1/2}\right)$ terms. Hence we can throw this error away. So we have a sum over sets of $d_i|P(z), d_i \leq X^{1/(2k)}$ and $x_i$ of an appropriate constant times $C_\infty/I$. We would like to remove the limitation that $d_i \leq X^{1/(2k)}$ in this sum. We note that once we get rid of the parts of the $d_i$ that share common factors with $D\prod_i a_i$ (for which there are finitely many possible values), the value of $I$ is at least $\frac{\prod_i d_i}{\gcd(d_i)}$. This is because we can compute the index separately for each prime $p$. If $p$ divides some set of $d_i$ other than all of them, we are forcing the corresponding $x_i$ to have specified values modulo $p$, when otherwise these values could have been completely arbitrary. If we let $d = \gcd(d_i)$, then we can bound the sum of the reciprocals of the values of $I$ that we are missing as

$$k\sum_d d^{-k+1}\left(\int_0^\infty S(z,y)y^{-2}dy\right)^{k-1}\left(\int_{X^{1/(2k)}/d}^\infty S(z,y)y^{-2}dy\right).$$

This is small by Lemma 5 and a basic computation.

We now wish to evaluate the sum over all $x_i$ and $d_i$ the sum of the appropriate constant times $\frac{1}{I}$. We note that if we were instead trying to evaluate

$$\sum_{\substack{n_i \pmod N \\ \sum_i a_i n_i \equiv n \pmod N}} \left(\prod_{i=1}^k \Lambda_{K_i,C_i}(n_i)\right)\left(\prod_{i=1}^k \Lambda_z(n_i)\right),$$

for $N$ a sufficiently divisible integer, we would get exactly this sum of $\frac{1}{I}$ times the total number of $n_i \bmod N$ so that $\sum_i a_i n_i \equiv n \pmod N$. This is because the number of points in each sublattice would be exactly $\frac{1}{I}$ of the total points. Hence our final answer up to acceptable errors is

$$C_\infty\left(\prod_{i=1}^k \frac{|C_i|}{|K_i|}\right)\left(\frac{\displaystyle\sum_{\substack{n_i \pmod N \\ \sum_i a_i n_i \equiv n \pmod N}} \left(\prod_{i=1}^k \Lambda_{K_i,C_i}(n_i)\right)\left(\prod_{i=1}^k \Lambda_z(n_i)\right)}{\#\{(n_i) \pmod N : \sum_i a_i n_i \equiv n \pmod N\}}\right).$$

Note that $\Lambda_z(n) = \prod_{p\leq z}\Lambda_p(n)$ is a product of terms over the congruence class of $n$ modulo $p$. Similarly $\Lambda_{K_i,C_i}(n)$ only depends on $n$ modulo $D$. Therefore we may use the Chinese Remainder Theorem to write the fraction above as a produce of $p$-primary parts and a $D$-primary part.

For $p \nmid D, p \nmid P(z)$ the local factor is clearly 1.

For $p \nmid D, p|P(z)$, the $p$-primary factor is

$$\frac{\displaystyle\sum_{\substack{n_i \pmod{p^n} \\ \sum_i a_i n_i \equiv n \pmod{p^n}}} \left(\prod_{i=1}^k \Lambda_p(n_i)\right)}{\#\{(n_i) \pmod{p^n} : \sum_i a_i n_i \equiv n \pmod{p^n}\}}$$

for some appropriately large $n$. In fact we can pick $n = 1$ since $\Lambda_p(n_i)$ only cares about $n_i$ modulo $p$, and since $p$ does not divide all the $a_i$ any solution to $\sum_i a_i n_i \equiv n \pmod p$ lifts to a solution modulo $p^n$ in exactly $p^{(n-1)(k-1)}$ different ways. Hence the local factor is

$$\begin{aligned}
&\frac{\sum_{\substack{n_i \pmod p \\ \sum_i a_i n_i \equiv n \pmod p}} \left(\prod_{i=1}^{k} \Lambda_p(n_i)\right)}{\#\{(n_i) \pmod p : \sum_i a_i n_i \equiv n \pmod p\}} \\
=&\frac{\left(\frac{p}{p-1}\right)^k \#\{(n_i) \pmod p : n_i \not\equiv 0 \pmod p, \sum_i a_i n_i \equiv n \pmod p\}}{p^{k-1}} \\
=&C_p.
\end{aligned}$$

Where above we used that since some $a_i \not\equiv 0 \pmod p$ that there were exactly $p^{k-1}$ solutions modulo $p$.

Next we will compute the $D$-primary factor. Note that by reasoning similar to the above we can compute the factor modulo $D$ rather than some power of $D$. Next we will consider the function $\Lambda_{K_i,C_i}(n) \prod_{p|D} \Lambda_p(n)$. This is 0 unless $n$ is in $H_i$. Otherwise it is $\left(\frac{\phi(D)}{|H_i|}\right)\left(\prod_{p|D} \frac{p}{p-1}\right) = \frac{D}{|H_i|}$. Hence this factor is

$$\left(\prod_{i=1}^{k} \frac{D}{|H_i|}\right)\left(\frac{\#\{(n_i) \pmod D : n_i \in H_i, \sum_i a_i n_i \equiv n \pmod D\}}{\#\{(n_i) \pmod D : \sum_i a_i n_i \equiv n \pmod D\}}\right) = C_D.$$

Putting these factors together we obtain our result. □

## 5.3 Putting it Together

We are finally able to prove Theorem 1

*Proof.* Let $B$ be a sufficiently large multiple of $A$, and $z = \log^B(X)$.

For $k \geq 3$ we have that

$$S_{K_i,C_i,a_i,X}(n) = \int_0^1 H_{K_i,C_i,a_i,X}(\alpha) e(-n\alpha).$$

By Lemma 19 this is

$$\int_0^1 H^{\sharp}_{K_i,C_i,a_i,z,X}(\alpha) e(-n\alpha)$$

up to acceptable errors. This is the $e(n\alpha)$ coefficient of $H^{\sharp}_{K_i,C_i,a_i,z,X}(\alpha)$, which by Proposition 20 is as desired.

For $k = 2$, we let $T_{K_i,C_i,a_i,X}(n)$ be the corresponding right hand side of Equation 1. It will suffice to show that

$$\sum_{|n| \leq \sum_i |a_i| X} (S_{K_i,C_i,a_i,X}(n) - T_{K_i,C_i,a_i,X}(n))^2 = O(X^3 \log^{-2A}(X)).$$

If we define the generating function

$$J_{K_i,C_i,a_i,X}(\alpha) = \sum_{|n| \leq \sum_i |a_i| X} T_{K_i,C_i,a_i,X}(n) e(n\alpha)$$

we note that the above is equivalent to showing that

$$|H_{K_i,C_i,a_i,X} - J_{K_i,C_i,a_i,X}|_2 = O(X^{3/2} \log^{-A}(X)).$$

But Lemma 19 that

$$|H_{K_i,C_i,a_i,X} - H^{\sharp}_{K_i,C_i,a_i,z,X}|_2 = O(X^{3/2} \log^{-A}(X))$$

and by Proposition 20 that

$$|H^{\sharp}_{K_i,C_i,a_i,z,X} - J_{K_i,C_i,a_i,X}|_2 = O(X^{3/2} \log^{-A}(X)).$$

This completes the proof. □

# 6 Application

Finally we present an application of Theorem 1 to constructing elliptic curves whose discriminants are divisible only by primes with certain splitting properties.

**Theorem 21.** *Let $K$ be a number field. Then there exists and elliptic curve defined over $\mathbb{Q}$ so that all primes dividing its discriminant split completely in $K$.*

*Proof.* We begin by assuming that $K$ is a normal extension of $\mathbb{Q}$. We will choose an elliptic curve of the form:

$$y^2 = X^3 + AX + B.$$

Here we will let $A = pq/4$, $B = npq^2$ where $n$ is a small integer and $p, q$ are primes that split over $K$. The discriminant is then

$$\begin{aligned} -16(4A^3 + 27B^3) &= -64p^3q^3/64 - 432n^2p^2q^4 \\ &= -p^2q^3(p + 432n^2q). \end{aligned}$$

Hence we need to find primes $p, q, r$ that split completely over $K$ with $p + 432n^2q - r = 0$. We do this by applying Theorem **??** with $k = 3$, $K_i = K$, $C_i = \{e\}$, and $X$ large. As long as $C_D > 0$ and $C_p > 0$ for all $p$, the main term will dominate the error and we will be guaranteed solutions. If $n = D$, this suffices to grantee solutions. This is because for $C_D$ to be non-zero we need to have solutions $n_1 + 0n_2 - n_3 \equiv 0 \pmod{D}$ with $n_i$ all in some particular subgroup of $(\mathbb{Z}/D\mathbb{Z})^*$. This can clearly be satisfied by $n_1 = n_3$. For $p = 2$, $C_p$ is non-zero since there is a solution to $n_1 + 0n_2 - n_3 \equiv 0 \pmod{2}$ with none of the $n_i$ divisible by 2 (take $(1, 1, 1)$). For $p > 2$, we need to show that there are solutions to $n_1 + 432D^2n_2 - n_3 \equiv 0 \pmod{p}$ with none of the $n_i$ 0 modulo $p$. This can be done because after picking $n_2$, any number modulo $p$ can be written as a difference of things that are not multiples of $p$. □

# 7 Acknowledgements

This work was done with the support of an NDSEG graduate fellowship.

# References

[1] Henryk Iwaniec, Emmanuel Kowalski, *Analytic Number Theory*, American Mathematical Society, 2004.