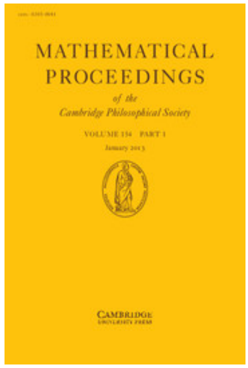

Average Frobenius distribution for the degree two primes of a number field

KEVIN JAMES and ETHAN SMITH

Mathematical Proceedings of the Cambridge Philosophical Society / *FirstView* Article / January 2013, pp 1 - 27
DOI: 10.1017/S0305004112000631, Published online: 16 January 2013

Math. Proc. Camb. Phil. Soc.: page 1 of 27
doi:10.1017/S0305004112000631

Average Frobenius distribution for the degree two primes of a number field

BY KEVIN JAMES

Department of Mathematical Sciences, Clemson University, Box 340975 *Clemson, SC* 29634-0975*, U.S.A.*
e-mail: kevja@clemson.edu
URL: www.math.clemson.edu/~kevja

AND ETHAN SMITH

Centre de recherches mathématiques, Université de Montréal, P.O. Box 6128*, Centre-ville Station, Montréal, Québec, H*3*C* 3*J*7*, Canada;*
and
Department of Mathematical Sciences, Michigan Technological University, 1400 *Townsend Drive, Houghton, Michigan,* 49931-1295*, U.S.A.*
e-mail: ethans@mtu.edu
URL: www.math.mtu.edu/~ethans

(*Received* 1 *November* 2011; *revised* 30 *October* 2012)

Abstract

Let K be a number field and r an integer. Given an elliptic curve E, defined over K, we consider the problem of counting the number of degree two prime ideals of K with trace of Frobenius equal to r. Under certain restrictions on K, we show that "on average" the number of such prime ideals with norm less than or equal to x satisfies an asymptotic identity that is in accordance with standard heuristics. This work is related to the classical Lang–Trotter conjecture and extends the work of several authors.

1. *Introduction*

Let E be an elliptic curve defined over a number field K. For a prime ideal $\mathfrak{P}$ of the ring of integers $\mathcal{O}_K$ where E has good reduction, we let $a_{\mathfrak{P}}(E)$ denote the trace of the Frobenius morphism at $\mathfrak{P}$. It follows that the number of points on the reduction of E modulo $\mathfrak{P}$ satisfies the identity

$$\#E_{\mathfrak{P}}(\mathcal{O}_K/\mathfrak{P}) = \mathbf{N}\mathfrak{P} + 1 - a_{\mathfrak{P}}(E),$$

where $\mathbf{N}\mathfrak{P} := \#(\mathcal{O}_K/\mathfrak{P})$ denotes the norm of $\mathfrak{P}$. It is a classical result of Hasse that

$$|a_{\mathfrak{P}}(E)| \leqslant 2\sqrt{\mathbf{N}\mathfrak{P}}.$$

See [**18**, p. 131] for example.

It is well known that if p is the unique rational prime lying below $\mathfrak{P}$ (i.e., $p\mathbb{Z} = \mathbb{Z} \cap \mathfrak{P}$), then $\mathcal{O}_K/\mathfrak{P}$ is isomorphic to the finite field $\mathbb{F}_{p^f}$ for some positive integer f. We refer to this integer f as the (absolute) *degree* of $\mathfrak{P}$ and write $\deg \mathfrak{P} = f$. Given a fixed elliptic curve E and fixed integers r and f, the classical heuristics of Lang and Trotter [**14**] may be generalized to consider the prime counting function

$$\pi_E^{r,f}(x) := \#\{\mathbf{N}\mathfrak{P} \leqslant x : a_{\mathfrak{P}}(E) = r \text{ and } \deg \mathfrak{P} = f\}.$$

Conjecture 1 (Lang–Trotter for number fields). *Let E be a fixed elliptic curve defined over K, and let r be a fixed integer. In the case that E has complex multiplication, also assume that $r \neq 0$. Let f be a positive integer. There exists a constant $\mathfrak{C}_{E,r,f}$ such that*

$$\pi_E^{r,f}(x) \sim \mathfrak{C}_{E,r,f} \begin{cases} \frac{\sqrt{x}}{\log x} & \text{if } f = 1, \\ \log\log x & \text{if } f = 2, \\ 1 & \text{if } f \geqslant 3, \end{cases} \tag{1}$$

as $x \to \infty$.

Remark 2. It is possible that the constant $\mathfrak{C}_{E,r,f}$ may be zero. In this event, we interpret the conjecture to mean that there are only finitely many such primes. In the case that $f \geqslant 3$, we always interpret the conjecture to mean that there are only finitely many such primes.

Remark 3. The first appearance of Conjecture 1 in the literature seems to be in the work of David and Pappalardi [**6**]. It is not clear to the authors what the constant $\mathfrak{C}_{E,r,f}$ should be for the cases when $f \geqslant 2$. Indeed, it does not appear that an explicit constant has ever been conjectured for these cases. We hope that one of the benefits of our work is that it will shed some light on what the constant should look like for the case $f = 2$.

Given a family $\mathcal{C}$ of elliptic curves defined over K, by the *average Lang–Trotter problem* for $\mathcal{C}$, we mean the problem of computing an asymptotic formula for

$$\frac{1}{\#\mathcal{C}} \sum_{E \in \mathcal{C}} \pi_E^{r,f}(x).$$

We refer to this expression as the *average order* of $\pi_E^{r,f}(x)$ over $\mathcal{C}$. In order to provide support for Conjecture 1, several authors have proven results about the average order of $\pi_E^{r,f}(x)$ over various families of elliptic curves. See [**1**, **2**, **4**, **5**, **6**, **9**, **11**, **12**]. In each case, the results have been found to be in accordance with Conjecture 1. Unfortunately, at present, it is necessary to take $\mathcal{C}$ to be a family of curves that must "grow" at some specified rate with respect to the variable x. The authors of the works [**1**, **9**, **12**] put a great deal of effort into keeping the average as "short" as possible. This seems like a difficult task for the cases of the average Lang–Trotter problem that we will consider here.

In [**4**], it was shown how to solve the average Lang–Trotter problem when $K/\mathbb{Q}$ is an Abelian extension and $\mathcal{C}$ is essentially the family of elliptic curves defined by (7) below. It turns out that their methods were actually sufficient to handle some non-Abelian Galois extensions as well in the case when $f = 2$. In [**12**], the results of [**4**] were extended to the setting of any Galois extension $K/\mathbb{Q}$ except in the case that $f = 2$. In this paper, we consider the case when $f = 2$ and $K/\mathbb{Q}$ is an arbitrary Galois extension. We show how the problem of computing an asymptotic formula for

$$\frac{1}{\#\mathcal{C}} \sum_{E \in \mathcal{C}} \pi_E^{r,2}(x)$$

may be reduced to a certain average error problem for the Chebotarëv Density Theorem that may be viewed as a variation on a classical problem solved by Barban, Davenport and Halberstam. We then show how to solve this problem in certain cases.

2. *An average error problem for the Chebotarëv Density Theorem*

For the remainder of the article it will be assumed that $K/\mathbb{Q}$ is a finite degree Galois extension with group G. Our technique for computing an asymptotic formula for the average order of $\pi_E^{r,2}(x)$ involves estimating sums of the form

$$\theta(x; C, q, a) := \sum_{\substack{p \leqslant x \\ \left(\frac{K/\mathbb{Q}}{p}\right) \subseteq C \\ p \equiv a \pmod q}} \log p,$$

where the sum is over the primes p which do not ramify in K, $((K/\mathbb{Q})/p)$ denotes the Frobenius class of p in G, and C is a union of conjugacy classes of G consisting entirely of elements of order two. Since the last two conditions on p under the sum may be in conflict for certain choices of q and a, we will need to take some care when attempting to estimate such sums via the Chebotarëv Density Theorem.

For each positive integer q, we fix a primitive q-th root of unity and denote it by ζ_q. It is well known that there is an isomorphism

$$(\mathbb{Z}/q\mathbb{Z})^\times \xrightarrow{\sim} \mathrm{Gal}(\mathbb{Q}(\zeta_q)/\mathbb{Q}) \tag{2}$$

given by $a \mapsto \sigma_{q,a}$ where $\sigma_{q,a}$ denotes the unique automorphism in $\mathrm{Gal}(\mathbb{Q}(\zeta_q)/\mathbb{Q})$ such that $\sigma_{q,a}(\zeta_q) = \zeta_q^a$. By definition of the Frobenius automorphism, it turns out that if p is a rational prime, then $((\mathbb{Q}(\zeta_q)/\mathbb{Q})/p) = \sigma_{q,a}$ if and only if $p \equiv a \pmod q$. See [**20**, pp. 11–14] for example. More generally, for any number field the extension $K(\zeta_q)/K$ is Galois, and under restriction of automorphisms of $K(\zeta_q)$ down to $\mathbb{Q}(\zeta_q)$ we have mappings

$$\mathrm{Gal}(K(\zeta_q)/K) \xrightarrow{\sim} \mathrm{Gal}(\mathbb{Q}(\zeta_q)/K \cap \mathbb{Q}(\zeta_q)) \hookrightarrow \mathrm{Gal}(\mathbb{Q}(\zeta_q)/\mathbb{Q}).$$

Therefore, via (2), we obtain a natural injection

$$\mathrm{Gal}(K(\zeta_q)/K) \hookrightarrow (\mathbb{Z}/q\mathbb{Z})^\times. \tag{3}$$

We let $G_{K,q}$ denote the image of the map (3) in $(\mathbb{Z}/q\mathbb{Z})^\times$ and $\varphi_K(q) := \# G_{K,q}$. Note that $\varphi_\mathbb{Q}$ is the usual Euler φ-function. For $a \in G_{K,q}$ and a prime ideal $\mathfrak{p}$ of K, it follows that $((K(\zeta_q)/K)/\mathfrak{p}) = \sigma_{q,a}$ if and only if $\mathbf{N}\mathfrak{p} \equiv a \pmod q$.

Now let G' denote the commutator subgroup of G, and let K' denote the fixed field of G'. We will use the notation throughout the article. It follows that K' is the maximal Abelian subextension of K. By the Kronecker–Weber Theorem [**13**, p. 210], there is a smallest integer m_K so that $K' \subseteq \mathbb{Q}(\zeta_{m_K})$. For every $q \geqslant 1$, it follows that $K \cap \mathbb{Q}(\zeta_{qm_K}) = K'$. Furthermore, the extension $K(\zeta_{qm_K})/\mathbb{Q}$ is Galois with group isomorphic to the fibered product

$$\{(\sigma_1, \sigma_2) \in \mathrm{Gal}(\mathbb{Q}(\zeta_{qm_K})/\mathbb{Q}) \times G : \sigma_1|_{K'} = \sigma_2|_{K'}\}.$$

See [**8**, pp. 592–593] for example. It follows that

$$[K(\zeta_{qm_K}) : \mathbb{Q}] = \frac{\varphi(qm_K)n_K}{n_{K'}} = \varphi_K(qm_K)n_K, \tag{4}$$

where here and throughout we use the notation $n_F := [F : \mathbb{Q}]$ to denote the degree of a number field F.

For each $\tau \in \mathrm{Gal}(K'/\mathbb{Q})$, it follows from the above facts that there is a finite list $\mathcal{S}_\tau$ of congruence conditions modulo m_K (really a coset of G_{K,m_K} in $(\mathbb{Z}/m_K\mathbb{Z})^\times$) such that for any rational prime not ramifying in K', $((K'/\mathbb{Q})/p) = \tau$ if and only if $p \equiv a \pmod{m_K}$ for some $a \in \mathcal{S}_\tau$. Now, suppose that τ has order one or two in $\mathrm{Gal}(K'/\mathbb{Q})$, and let $\mathcal{C}_\tau$ be the subset of order two elements of G that restrict to τ on K', i.e.,

$$\mathcal{C}_\tau := \{\sigma \in G : \sigma|_{K'} = \tau \text{and } |\sigma| = 2\}.$$

Since $K'/\mathbb{Q}$ is Abelian, it follows that $\mathcal{C}_\tau$ is a union of conjugacy classes in G. Then for each $a \in (\mathbb{Z}/qm_K\mathbb{Z})^\times$, the Chebotarëv Density Theorem gives the asymptotic formula

$$\theta(x; \mathcal{C}_\tau, qm_K, a) \sim \frac{\#\mathcal{C}_\tau}{\varphi_K(qm_K)n_K} x, \tag{5}$$

provided that $a \equiv b \pmod{m_K}$ for some $b \in \mathcal{S}_\tau$. Otherwise, the sum on the left is empty. For $Q \geqslant 1$, we define the *Barban–Davenport–Halberstam average square error* for this problem by

$$\mathcal{E}_K(x; Q, \mathcal{C}_\tau) := \sum_{q \leqslant Q} \sum_{a=1}^{qm_K}{}' \left(\theta(x; C, qm_K, a) - \frac{\#\mathcal{C}_\tau}{\varphi_K(qm_K)n_K} x\right)^2, \tag{6}$$

where the prime on the sum over a means that the sum is to be restricted to those a such that $a \equiv b \pmod{m_K}$ for some $b \in \mathcal{S}_\tau$.

3. *Notation and statement of results*

We are now ready to state our main results on the average Lang–Trotter problem. Recall that the ring of integers $\mathcal{O}_K$ is a free $\mathbb{Z}$-module of rank n_K, and let $\mathcal{B} = \{\gamma_j\}_{j=1}^{n_K}$ be a fixed integral basis for $\mathcal{O}_K$. We denote the coordinate map for the basis $\mathcal{B}$ by

$$[\cdot]_{\mathcal{B}} : \mathcal{O}_K \xrightarrow{\sim} \bigoplus_{j=1}^{n_K} \mathbb{Z} = \mathbb{Z}^{n_K}.$$

If $\mathbf{A}, \mathbf{B} \in \mathbb{Z}^{n_K}$, then we write $\mathbf{A} \leqslant \mathbf{B}$ if each entry of $\mathbf{A}$ is less than or equal to the corresponding entry of $\mathbf{B}$. For two algebraic integers $\alpha, \beta \in \mathcal{O}_K$, we write $E_{\alpha,\beta}$ for the elliptic curve given by the model

$$E_{\alpha,\beta} : Y^2 = X^3 + \alpha X + \beta.$$

From now on, we assume that the entries of $\mathbf{A}, \mathbf{B}$ are all non-negative, and we take as our family of elliptic curves the set

$$\mathcal{C} := \mathcal{C}(\mathbf{A}; \mathbf{B}) = \{E_{\alpha,\beta} : -\mathbf{A} \leqslant [\alpha]_{\mathcal{B}} \leqslant \mathbf{A}, -\mathbf{B} \leqslant [\beta]_{\mathcal{B}} \leqslant \mathbf{B}, -16(4\alpha^3 + 27\beta^2) \neq 0\}. \tag{7}$$

To be more precise, this box should be thought of as a box of equations or models since the same elliptic curve may appear multiple times in $\mathcal{C}$. For $1 \leqslant i \leqslant n_K$, we let a_i denote the i-th entry of $\mathbf{A}$ and b_i denote the i-th entry of $\mathbf{B}$. Associated to box $\mathcal{C}$, we define the quantities

$$\mathrm{V}_1(\mathcal{C}) := 2^{n_K} \prod_{i=1}^{n_K} a_i, \qquad \mathrm{V}_2(\mathcal{C}) := 2^{n_K} \prod_{i=1}^{n_K} b_i,$$

$$\min_1(\mathcal{C}) := \min_{1 \leqslant i \leqslant n_K} \{a_i\}, \qquad \min_2(\mathcal{C}) := \min_{1 \leqslant i \leqslant n_K} \{b_i\},$$

$$\mathrm{V}(\mathcal{C}) := \mathrm{V}_1(\mathcal{C})\mathrm{V}_2(\mathcal{C}), \qquad \min(\mathcal{C}) := \min\{\min_1(\mathcal{C}), \min_2(\mathcal{C})\},$$

which give a description of the size of the box $\mathcal{C}$. In particular,

$$\#\mathcal{C} = \mathrm{V}(\mathcal{C}) + O\left(\frac{\mathrm{V}(\mathcal{C})}{\min(\mathcal{C})}\right).$$

Our first main result is that the average order problem for $\pi_E^{r,2}(x)$ may be reduced to the Barban–Davenport–Halberstam type average error problem described in the previous section.

THEOREM 4. *Let r be a fixed odd integer, and recall the definition of $\mathcal{E}_K(x;\,Q,\mathcal{C}_\tau)$ as given by (6). If*

$$\mathcal{E}_K(x;\,x/(\log x)^{12},\mathcal{C}_\tau) \ll \frac{x^2}{(\log x)^{11}}$$

for every τ of order dividing two in $\mathrm{Gal}(K'/\mathbb{Q})$ and if $\min(\mathcal{C}) \geqslant \sqrt{x}$, then there exists an explicit constant $\mathfrak{C}_{K,r,2}$ such that

$$\frac{1}{\#\mathcal{C}}\sum_{E\in\mathcal{C}}\pi_E^{r,2}(x) = \mathfrak{C}_{K,r,2}\log\log x + O(1),$$

where the implied constants depend at most on K and r. Furthermore, the constant $\mathfrak{C}_{K,r,2}$ is given by

$$\mathfrak{C}_{K,r,2} = \frac{2}{3n_K}\prod_{\ell\mid r}\left(\frac{\ell}{\ell-\left(\frac{-1}{\ell}\right)}\right)\sum_{\substack{\tau\in\mathrm{Gal}(K'/\mathbb{Q})\\|\tau|=1,2}}\#\mathcal{C}_\tau\sum_{g\in\mathcal{S}_\tau}\mathfrak{c}_r^{(g)},$$

where the product is taken over the rational primes ℓ dividing r,

$$\mathfrak{c}_r^{(g)} := \sum_{\substack{k=1\\(k,2r)=1}}^{\infty}\frac{1}{k}\sum_{\substack{n=1\\(n,2r)=1}}^{\infty}\frac{1}{n\varphi_K(m_Knk^2)}\sum_{a\in(\mathbb{Z}/n\mathbb{Z})^\times}\left(\frac{a}{n}\right)\#C_g(r,a,n,k) \tag{8}$$

and

$$C_g(r,a,n,k) := \left\{b\in(\mathbb{Z}/m_Knk^2\mathbb{Z})^\times : 4b^2\equiv r^2-ak^2 \pmod{nk^2},\, b\equiv g \pmod{m_K}\right\}.$$

Alternatively, the constant $\mathfrak{C}_{K,r,2}$ may be written as

$$\mathfrak{C}_{K,r,2} = \frac{n_{K'}}{3\pi\varphi(m_K)}\prod_{\ell\mid r}\left(\frac{\ell}{\ell-\left(\frac{-1}{\ell}\right)}\right)\prod_{\ell\nmid 2rm_K}\left(\frac{\ell\left(\ell-1-\left(\frac{-1}{\ell}\right)\right)}{(\ell-1)\left(\ell-\left(\frac{-1}{\ell}\right)\right)}\right)\sum_{\substack{\tau\in\mathrm{Gal}(K'/\mathbb{Q})\\|\tau|=1,2}}\#\mathcal{C}_\tau\sum_{g\in\mathcal{S}_\tau}\prod_{\substack{\ell\mid m_K\\\ell\nmid 2r}}\mathfrak{K}_r^{(g)}, \tag{9}$$

where the products are taken over the rational primes ℓ satisfying the stated conditions and $\mathfrak{K}_r^{(g)}$ is defined by

$$\mathfrak{K}_r^{(g)} := \begin{cases} \dfrac{\ell^{\frac{\nu_\ell(4g^2-r^2)+1}{2}}-1}{\ell^{\frac{\nu_\ell(4g^2-r^2)-1}{2}}(\ell-1)} & \text{if } \nu_\ell(4g^2-r^2)<\nu_\ell(m_K) \text{ and } 2\nmid\nu_\ell(4g^2-r^2),\\[2ex] \dfrac{\ell^{\frac{\nu_\ell(4g^2-r^2)}{2}+1}-1}{\ell^{\frac{\nu_\ell(4g^2-r^2)}{2}}(\ell-1)}+\dfrac{\left(\frac{(r^2-4g^2)/\ell^{\nu_\ell(r^2-4g^2)}}{\ell}\right)}{\ell^{\frac{\nu_\ell(4g^2-r^2)}{2}}\left(\ell-\left(\frac{(r^2-4g^2)/\ell^{\nu_\ell(r^2-4g^2)}}{\ell}\right)\right)} & \text{if } \nu_\ell(4g^2-r^2)<\nu_\ell(m_K) \text{ and } 2\mid\nu_\ell(4g^2-r^2),\\[2ex] \dfrac{\ell^{2\left\lceil\frac{\nu_\ell(m_K)}{2}\right\rceil+1}(\ell+1)\left(\ell^{\left\lceil\frac{\nu_\ell(m_K)}{2}\right\rceil}-1\right)+\ell^{\nu_\ell(m_K)+2}}{\ell^{3\left\lceil\frac{\nu_\ell(m_K)}{2}\right\rceil}(\ell^2-1)} & \text{if } \nu_\ell(4g^2-r^2)\geqslant\nu_\ell(m_K). \end{cases}$$

Remark 5. The notation $\nu_\ell(4g^2-r^2)$ in the definition of $\mathfrak{K}_r^{(g)}$ is a bit strange as g is defined to be an element of $(\mathbb{Z}/m_K\mathbb{Z})^\times$. This can be remedied by choosing any integer representative of g, and noting that any choice with $4g^2 \equiv r^2 \pmod{\ell^{\nu_\ell(m_K)}}$ corresponds to the case that $\nu_\ell(4g^2 - r^2) \geqslant \nu_\ell(m_K)$.

Remark 6. We have chosen to restrict ourselves to the case when r is odd since it simplifies some of the technical difficulties involved in computing the constant $\mathfrak{C}_{K,r,2}$. A result of the same nature should hold for non-zero even r as well. For the case $r = 0$, see Theorem 10 below.

The proof of Theorem 4 proceeds by a series of reductions. We make no restriction on the number field K except that it be a finite degree Galois extension of $\mathbb{Q}$. In Section 5, we reduce the proof of Theorem 4 to the computation of a certain average of class numbers. In Section 6, we reduce that computation to a certain average of special values of Dirichlet L-functions. In Section 7, the problem is reduced to the problem of bounding $\mathcal{E}_K(x; Q, \mathcal{C}_\tau)$. Finally, in Section 8, we compute the constant $\mathfrak{C}_{K,r,2}$.

Under certain conditions on the Galois group $G = \mathrm{Gal}(K/\mathbb{Q})$, we are able to completely solve our problem by bounding $\mathcal{E}_K(x; Q, \mathcal{C}_\tau)$. One easy case is when the Galois group G is equal to its own commutator subgroup, i.e., when G is a perfect group. In this case, we say that the number field K is *totally non-Abelian*. The authors of [**4**] were able to prove a version of Theorem 4 whenever G is Abelian. That is, when the commutator subgroup is trivial, or equivalently, when $K = K'$. It turns out that their methods are actually sufficient to handle some non-Abelian number fields as well. In particular, their technique is sufficient whenever there is a finite list of congruence conditions that determine exactly which rational primes decompose as a product of degree two primes in K. Such a number field need not be Abelian over $\mathbb{Q}$. For example, the splitting field of the polynomial $x^3 - 2$ possesses this property. If K is a finite degree Galois extension of $\mathbb{Q}$ possessing this property, we say that K is 2-*pretentious*. The name is meant to call to mind the notion that such number fields "pretend" to be Abelian over $\mathbb{Q}$, at least as far as their degree two primes are concerned.[1]

In Section 9, we give more precise descriptions of 2-pretentious and totally non-Abelian number fields and prove some basic facts which serve to characterize such fields. Then, in Section 10, we show how to give a complete solution to the average order problem for $\pi_E^{r,2}(x)$ whenever K may be decomposed $K = K_1K_2$, where K_1 is a 2-pretentious Galois extension of $\mathbb{Q}$, K_2 is totally non-Abelian, and $K_1 \cap K_2 = \mathbb{Q}$.

THEOREM 7. *Let r be a fixed odd integer, and assume that K may be decomposed as above. If* $\min(\mathcal{C}) \geqslant \sqrt{x}$, *then*

$$\frac{1}{\#\mathcal{C}} \sum_{E \in \mathcal{C}} \pi_E^{r,2}(x) = \mathfrak{C}_{K,r,2} \log\log x + O(1),$$

where the implied constant depends at most upon K and r, and the constant $\mathfrak{C}_{K,r,2}$ is as in Theorem 4.

By a slight alteration in the method we employ to prove Theorem 4, we can also provide a complete solution to our problem for another class of number fields.

[1] We borrow the term pretentious from Granville and Soundararajan who use the term to describe the way in which one multiplicative function "pretends" to be another in a certain technical sense.

THEOREM 8. *Let r be a fixed odd integer, and suppose that K' is ramified only at primes which divide $2r$. If* $\min(\mathcal{C}) \geqslant \sqrt{x}$, *then*

$$\frac{1}{\#\mathcal{C}} \sum_{E \in \mathcal{C}} \pi_E^{r,2}(x) = \mathfrak{C}_{K,r,2} \log\log x + O(1),$$

where the implied constant depends at most upon K and r. Furthermore, the constant $\mathfrak{C}_{K,r,2}$ may be simplified to

$$\mathfrak{C}_{K,r,2} = \frac{\#C}{3\pi} \prod_{\ell > 2} \frac{\ell\left(\ell - 1 - \left(\frac{-r^2}{\ell}\right)\right)}{(\ell - 1)\left(\ell - \left(\frac{-1}{\ell}\right)\right)},$$

where the product is taken over the rational primes $\ell > 2$ and $C = \{\sigma \in \mathrm{Gal}(K/\mathbb{Q}) : |\sigma| = 2\}$.

Remark 9. We note that the required growth rate $\min(\mathcal{C}) \geqslant \sqrt{x}$ for Theorems 4, 7, 8 can be relaxed to $\min(\mathcal{C}) \geqslant \sqrt{x}/\log x$. The key piece of information necessary for making the improvement is to observe that (14) can be improved to $\mathcal{H}(T) \ll T^2/\log T$, where $\mathcal{H}(T)$ is the sum defined by (12). Indeed, the techniques used to prove Propositions 16 and 17 below can be used to show that $\mathcal{H}(T)$ is asymptotic to some constant multiple of $T^2/\log T$.

Following [**6**], we also obtain an easy result concerning the average *supersingular* distribution of degree two primes. To this end, we define the prime counting function

$$\pi_E^{\mathrm{ss},2}(x) := \#\{\mathbf{N}\mathfrak{P} \leqslant x : E \text{ is supersingular at } \mathfrak{P},\ \deg \mathfrak{P} = 2\}.$$

Recall that if $\mathfrak{P}$ is a degree two prime of K lying above the rational prime p, then E is supersingular at $\mathfrak{P}$ if and only if $a_{\mathfrak{P}}(E) = 0, \pm p, \pm 2p$. By a straightforward adaption of [**6**, pp. 199–200], we obtain the following.

THEOREM 10. *Let K be any Galois number field. Then provided that* $\min(\mathcal{C}) \geqslant \log\log x$,

$$\frac{1}{\#\mathcal{C}} \sum_{E \in \mathcal{C}} \pi_E^{0,2}(x) \ll 1,$$

where the implied constant depends at most upon K and r. Furthermore, if $\min(\mathcal{C}) \geqslant \sqrt{x}/\log x$, *then*

$$\frac{1}{\#\mathcal{C}} \sum_{E \in \mathcal{C}} \pi_E^{\mathrm{ss},2}(x) \sim \frac{\#C}{12 n_K} \log\log x,$$

where $C = \{\sigma \in \mathrm{Gal}(K/\mathbb{Q}) : |\sigma| = 2\}$.

Since the proof of this result merely requires a straightforward adaptation of [**6**, pp. 199–200], we choose to omit it.

Remark 11. In all of our computations, the number field K and the integer r are assumed to be fixed. We have not kept track of the way in which our implied constants depend on these two parameters. Thus, all implied constants in this article may depend on K and r even though we do not make this explicit in what follows.

4. *Counting isomorphic reductions*

In this section, we count the number of models $E \in \mathcal{C}$ that reduce modulo $\mathfrak{P}$ to a given isomorphism class.

LEMMA 12. *Let $\mathfrak{P}$ be a prime ideal of K and let E' be an elliptic curve defined over $\mathcal{O}_K/\mathfrak{P}$. Suppose that* $\deg \mathfrak{P} = 2$ *and* $\mathfrak{P} \nmid 6$. *Then the number of $E \in \mathcal{C}$ for which E is isomorphic to E' over $\mathcal{O}_K/\mathfrak{P}$ is*

$$\#\{E \in \mathcal{C} : E_{\mathfrak{P}} \cong E'\} = \frac{\mathrm{V}(\mathcal{C})}{\mathbf{N}\mathfrak{P}\#\mathrm{Aut}(E')} + O\left(\frac{\mathrm{V}(\mathcal{C})}{\mathbf{N}\mathfrak{P}^2} + \frac{\mathrm{V}(\mathcal{C})}{\min(\mathcal{C})\sqrt{\mathbf{N}\mathfrak{P}}} + \frac{\mathrm{V}(\mathcal{C})}{\min_1(\mathcal{C})\min_2(\mathcal{C})}\right).$$

Proof. Since $\deg \mathfrak{p} = 2$, the residue ring $\mathcal{O}_K/\mathfrak{P}$ is isomorphic to the finite field $\mathbb{F}_{p^2}$, where p is the unique rational prime lying below $\mathfrak{P}$. Since $\mathfrak{P} \nmid 6$, the characteristic p is greater than 3. Hence, E' may be modeled by an equation of the form

$$E_{a,b} : Y^2 = X^3 + aX + b$$

for some $a, b \in \mathcal{O}_K/\mathfrak{P}$. The number of equations of this form that are isomorphic to E' is exactly

$$\frac{p^2-1}{\#\mathrm{Aut}(E')} = \frac{\mathbf{N}\mathfrak{P}-1}{\#\mathrm{Aut}(E')}.$$

Therefore,

$$\#\{E \in \mathcal{C} : E_{\mathfrak{P}} \cong E'\} = \frac{\mathbf{N}\mathfrak{P}-1}{\#\mathrm{Aut}(E')}\#\{E \in \mathcal{C} : E_{\mathfrak{P}} = E_{a,b}\}.$$

Suppose that $E \in \mathcal{C}$ such that $E_{\mathfrak{P}} = E_{a,b}$, say $E : Y^2 = X^2 + \alpha X + \beta$. Then either $\alpha \equiv a \pmod{\mathfrak{P}}$ and $\beta \equiv b \pmod{\mathfrak{P}}$ or $E_{\alpha,\beta}$ is not minimal at $\mathfrak{P}$. If E is not minimal at $\mathfrak{P}$, then $\mathfrak{P}^4 \mid \alpha$ and $\mathfrak{P}^6 \mid \beta$. For $a, b \in \mathcal{O}_K/\mathfrak{P}$, we adapt the argument of [**6**, p. 192] in the obvious manner to obtain the estimates

$$\#\{\alpha \in \mathcal{O}_K : -\mathbf{A} \leqslant [\alpha]_{\mathcal{B}} \leqslant \mathbf{A}, \alpha \equiv a \pmod{\mathfrak{P}}\} = \frac{\mathrm{V}_1(\mathcal{C})}{\mathbf{N}\mathfrak{P}} + O\left(\frac{\mathrm{V}_1(\mathcal{C})}{\min_1(\mathcal{C})\sqrt{\mathbf{N}\mathfrak{P}}}\right),$$
$$\#\{\beta \in \mathcal{O}_K : -\mathbf{B} \leqslant [\beta]_{\mathcal{B}} \leqslant \mathbf{B}, \alpha \equiv b \pmod{\mathfrak{P}}\} = \frac{\mathrm{V}_2(\mathcal{C})}{\mathbf{N}\mathfrak{P}} + O\left(\frac{\mathrm{V}_2(\mathcal{C})}{\min_2(\mathcal{C})\sqrt{\mathbf{N}\mathfrak{P}}}\right).$$

It follows that

$$\#\{E \in \mathcal{C} : E_{\mathfrak{P}} = E_{a,b}\} = \frac{\mathrm{V}(\mathcal{C})}{\mathbf{N}\mathfrak{P}^2} + O\left(\frac{\mathrm{V}(\mathcal{C})}{\min(\mathcal{C})\mathbf{N}\mathfrak{P}^{3/2}} + \frac{\mathrm{V}(\mathcal{C})}{\min_1(\mathcal{C})\min_2(\mathcal{C})\mathbf{N}\mathfrak{P}} + \frac{\mathrm{V}(\mathcal{C})}{\mathbf{N}\mathfrak{P}^{10}}\right),$$

where the last term in the error accounts for the curves which are not minimal at $\mathfrak{P}$.

5. *Reduction of the average order to an average of class numbers*

In this section, we reduce our average order computation to the computation of an average of class numbers. Given a (not necessarily fundamental) discriminant $D < 0$, if $D \equiv 0, 1 \pmod 4$, we define the *Hurwitz–Kronecker class number* of discriminant D by

$$H(D) := \sum_{\substack{k^2 \mid D \\ \frac{D}{k^2} \equiv 0,1 \pmod 4}} \frac{h(D/k^2)}{w(D/k^2)}, \tag{10}$$

where $h(d)$ denotes the class number of the unique imaginary quadratic order of discriminant d and $w(d)$ denotes the order of its unit group.

A simple adaption of the proof of [**17**, theorem 4·6] to count isomorphism classes with weights (as in [**15**, p. 654]) yields the following result, which is attributed to Deuring [**7**].

THEOREM 13 (Deuring). *Let p be a prime greater than 3, and let r be an integer such that $p \nmid r$ and $r^2 - 4p^2 < 0$. Then*

$$\sum_{\substack{\tilde{E}/\mathbb{F}_{p^2} \\ \#\tilde{E}(\mathbb{F}_{p^2}) = p^2+1-r}} \frac{1}{\#\mathrm{Aut}(\tilde{E})} = H(r^2 - 4p^2),$$

where the sum on the left is over the $\mathbb{F}_{p^2}$-isomorphism classes of elliptic curves possessing exactly $p^2 + 1 - r$ points and $\mathrm{Aut}(\tilde{E})$ denotes the $\mathbb{F}_{p^2}$-automorphism group of any representative of $\tilde{E}$.

PROPOSITION 14. *Let r be any integer. If $\min(\mathcal{C}) \geqslant \sqrt{x}$, then*

$$\frac{1}{\#\mathcal{C}} \sum_{E \in \mathcal{C}} \pi_E^{r,2}(x) = \frac{n_K}{2} \sum_{\substack{3|r| < p \leqslant \sqrt{x} \\ f_K(p) = 2}} \frac{H(r^2 - 4p^2)}{p^2} + O(1),$$

where the sum on the right is over the rational primes p which do not ramify and which split into degree two primes in K.

Remark 15. We do not place any restriction on r in the above, nor do we place any restriction on K except that the extension $K/\mathbb{Q}$ be Galois.

Proof. For each $E \in \mathcal{C}$, we write $\pi_E^{r,2}(x)$ as a sum over the degree two primes of K and switch the order of summation, which yields

$$\frac{1}{\#\mathcal{C}} \sum_{E \in \mathcal{C}} \pi_E^{r,2}(x) = \frac{1}{\#\mathcal{C}} \sum_{\substack{\mathbf{N}\mathfrak{P} \leqslant x \\ \deg \mathfrak{P} = 2}} \sum_{\substack{E \in \mathcal{C} \\ a_{\mathfrak{P}}(E) = r}} 1 = \sum_{\substack{\mathbf{N}\mathfrak{P} \leqslant x \\ \deg \mathfrak{P} = 2}} \left[\frac{1}{\#\mathcal{C}} \sum_{\substack{\tilde{E}/(\mathcal{O}_K/\mathfrak{P}) \\ a_{\mathfrak{P}}(\tilde{E}) = r}} \#\{E \in \mathcal{C} : E_{\mathfrak{P}} \cong \tilde{E}\} \right],$$

where the sum in brackets is over the isomorphism classes $\tilde{E}$ of elliptic curves defined over $\mathcal{O}_K/\mathfrak{P}$ having exactly $\mathbf{N}\mathfrak{P} + 1 - r$ points.

Removing the primes with $\mathbf{N}\mathfrak{P} \leqslant (3r)^2$ introduces at most a bounded error depending on r. For the primes with $\mathbf{N}\mathfrak{P} > (3r)^2$, we apply Theorem 13 and Lemma 12 to estimate the expression in brackets above. The result is equal to

$$\frac{H(r^2 - 4\mathbf{N}\mathfrak{P})}{\mathbf{N}\mathfrak{P}} + O\left(H(r^2 - 4\mathbf{N}\mathfrak{P}) \left[\frac{1}{\mathbf{N}\mathfrak{P}^2} + \frac{1}{\min(\mathcal{C})\sqrt{\mathbf{N}\mathfrak{P}}} + \frac{1}{\min_1(\mathcal{C}) \min_2(\mathcal{C})} \right] \right). \quad (11)$$

Summing the main term of (11) over the appropriate $\mathfrak{P}$ gives

$$\sum_{\substack{(3r)^2 < \mathbf{N}\mathfrak{P} \leqslant x \\ \deg \mathfrak{P} = 2}} \frac{H(r^2 - 4\mathbf{N}\mathfrak{P})}{\mathbf{N}\mathfrak{P}} = \frac{n_K}{2} \sum_{\substack{3|r| < p \leqslant \sqrt{x} \\ f_K(p) = 2}} \frac{H(r^2 - 4p^2)}{p^2},$$

where the sum on the right is over the rational primes p which split into degree two primes in K.

To estimate the error terms, we proceed as follows. For $T > 0$, let

$$\mathcal{H}(T) := \sum_{3|r|<p\leqslant T} H(r^2-4p^2). \tag{12}$$

Given a discriminant $d < 0$, we let χ_d denote the Kronecker symbol $\left(\frac{d}{\cdot}\right)$. The class number formula states that

$$\frac{h(d)}{w(d)} = \frac{|d|^{1/2}}{2\pi} L(1,\chi_d), \tag{13}$$

where $L(1,\chi_d) = \sum_{n=1}^{\infty} \chi_d(n)/n$. Thus, the class number formula together with the definition of the Hurwitz–Kronecker class number implies that

$$\begin{aligned}\mathcal{H}(T) &\ll \sum_{k\leqslant 2T} \frac{1}{k} \sum_{\substack{3|r|<p\leqslant T\\ k^2|r^2-4p^2}} p\log p \leqslant T\log T \sum_{k\leqslant 2T}\frac{1}{k} \sum_{\substack{3|r|<p\leqslant 4T\\ k|r^2-4p^2}} 1\\ &\ll T\log T \sum_{k\leqslant 2T}\frac{1}{k} \sum_{\substack{a\in(\mathbb{Z}/k\mathbb{Z})^\times\\ 4a^2\equiv r^2 \pmod k}} \sum_{\substack{p\leqslant 4T\\ p\equiv a \pmod k}} 1.\end{aligned}$$

We apply the Brun–Titchmarsh inequality [**10**, p. 167] to bound the sum over p and the Chinese Remainder Theorem to deduce that

$$\#\{a\in(\mathbb{Z}/k\mathbb{Z})^\times : 4a^2\equiv r^2 \pmod k\} \leqslant 2^{\omega(k)},$$

where $\omega(k)$ denotes the number of distinct prime factors of k. The result is that

$$\mathcal{H}(T) \ll T^2\log T \sum_{k\leqslant 2T} \frac{2^{\omega(k)}}{k\varphi(k)\log(4T/k)} \ll T^2\log T\sum_{k\leqslant 2T}\frac{2^{\omega(k)}\log k}{k\varphi(k)\log(4T)} \ll T^2. \tag{14}$$

From this, we deduce the bounds

$$\sum_{\substack{(3r)^2<\mathbf{N}\mathfrak{P}\leqslant x\\ \deg\mathfrak{P}=2}} H(r^2-4\mathbf{N}\mathfrak{P}) \ll \sum_{3|r|<p\leqslant\sqrt{x}} H(r^2-4p^2) = \mathcal{H}(\sqrt{x}) \ll x,$$

$$\sum_{\substack{(3r)^2<\mathbf{N}\mathfrak{P}\leqslant x\\ \deg\mathfrak{P}=2}} \frac{H(r^2-4\mathbf{N}\mathfrak{P})}{\sqrt{\mathbf{N}\mathfrak{P}}} \ll \sum_{3|r|<p\leqslant\sqrt{x}} \frac{H(r^2-4p^2)}{p} = \int_{3|r|}^{\sqrt{x}} \frac{\mathrm{d}\mathcal{H}(T)}{T} \ll \sqrt{x},$$

and

$$\sum_{\substack{(3r)^2<\mathbf{N}\mathfrak{P}\leqslant x\\ \deg\mathfrak{P}=2}} \frac{H(r^2-4\mathbf{N}\mathfrak{P})}{\mathbf{N}\mathfrak{P}^2} \ll \sum_{3|r|<p\leqslant\sqrt{x}} \frac{H(r^2-4p^2)}{p^4} = \int_{3|r|}^{\sqrt{x}} \frac{\mathrm{d}\mathcal{H}(T)}{T^4} \ll 1.$$

Using these estimates, it is easy to see that summing the error terms of (11) over $\mathfrak{P}$ yields a bounded error whenever $\min(\mathcal{C}) \geqslant \sqrt{x}$.

6. *Reduction to an average of special values of Dirichlet L-functions*

In the previous section, we reduced the problem of computing the average order of $\pi_E^{r,2}(x)$ to that of computing a certain average of Hurwitz–Kronecker class numbers. In this section, we reduce the computation of that average of Hurwitz–Kronecker class numbers to the computation of a certain average of special values of Dirichlet L-functions. Recall that if χ is a

Dirichlet character, then the Dirichlet L-function attached to χ is given by

$$L(s,\chi) := \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s}$$

for $s > 1$. If χ is not trivial, then the above definition is valid at $s = 1$ as well. As in the previous section, given an integer d, we write χ_d for the Kronecker symbol $\left(\frac{d}{\cdot}\right)$. We now define

$$A_{K,2}(T;r) := \sum_{\substack{k\leqslant 2T\\(k,2r)=1}} \frac{1}{k} \sum_{\substack{3|r|<p\leqslant T\\ f_K(p)=2\\ k^2|r^2-4p^2}} L\left(1, \chi_{d_k(p^2)}\right)\log p, \tag{15}$$

where the condition $f_K(p) = 2$ means that p factors in K as a product of degree two prime ideals of $\mathcal{O}_K$, and we put $d_k(p^2) := (r^2-4p^2)/k^2$ whenever $k^2 \mid r^2 - 4p^2$.

PROPOSITION 16. *Let r be any odd integer. If there exists a constant $\mathfrak{C}'_{K,r,2}$ such that*

$$A_{K,2}(T;r) = \mathfrak{C}'_{K,r,2}T + O\left(\frac{T}{\log T}\right),$$

then

$$\frac{n_K}{2} \sum_{\substack{3|r|<p\leqslant\sqrt{x}\\ f_K(p)=2}} \frac{H(r^2-4p^2)}{p^2} = \mathfrak{C}_{K,r,2}\log\log x + O(1),$$

where $\mathfrak{C}_{K,r,2} = (n_K/2\pi)\mathfrak{C}'_{K,r,2}$.

Proof. Combining the class number formula (13) with the definition of the Hurwitz–Kronecker class number, we obtain the identity

$$\frac{n_K}{2} \sum_{\substack{3|r|<p\leqslant\sqrt{x}\\ f_K(p)=2}} \frac{H(r^2-4p^2)}{p^2} = \frac{n_K}{4\pi} \sum_{\substack{3|r|<p\leqslant\sqrt{x}\\ f_K(p)=2}} \sum_{\substack{k^2|r^2-4p^2\\ d_k(p^2)\equiv 0,1 \pmod 4}} \frac{\sqrt{4p^2-r^2}}{kp^2} L\left(1, \chi_{d_k(p^2)}\right). \tag{16}$$

By assumption r is odd, and hence $r^2 - 4p^2 \equiv 1 \pmod 4$. Thus, if $k^2 \mid r^2 - 4p^2$, it follows that k must be odd and $k^2 \equiv 1 \pmod 4$. Whence, the sum over k above may be restricted to odd integers whose squares divide $r^2 - 4p^2$, and the congruence conditions on $d_k(p^2) = (r^2-4p^2)/k^2$ may be omitted. Furthermore, if ℓ is a prime dividing (k,r) and $k^2 \mid r^2 - 4p^2$, then

$$0 \equiv r^2 - 4p^2 \equiv -(2p)^2 \pmod{\ell^2},$$

and it follows that $\ell = p$. This is not possible for $p > 3|r|$ since the fact that ℓ divides r implies that $\ell \leqslant r$. Hence, the sum on k above may be further restricted to integers which are coprime to r. Therefore, switching the order of summation in (16) and employing the approximation $\sqrt{4p^2-r^2} = 2p + O(1/p)$ gives

$$\frac{n_K}{2} \sum_{\substack{3|r|<p\leqslant\sqrt{x}\\ f_K(p)=2}} \frac{H(r^2-4p^2)}{p^2} = \frac{n_K}{2\pi} \sum_{\substack{k\leqslant 2\sqrt{x}\\(k,2r)=1}} \frac{1}{k} \sum_{\substack{3|r|<p\leqslant\sqrt{x}\\ f_K(p)=2\\ k^2|r^2-4p^2}} \frac{L\left(1,\chi_{d_k(p^2)}\right)}{p} + O(1).$$

With $A_{K,2}(T;r)$ as defined by (15), the main term on the right-hand side is

$$\frac{n_K}{2\pi}\sum_{\substack{k\leqslant 2\sqrt{x}\\(k,2r)=1}}\frac{1}{k}\sum_{\substack{3|r|<p\leqslant\sqrt{x}\\ f_K(p)=2\\ k^2|r^2-4p^2}}\frac{L\left(1,\chi_{d_k(p^2)}\right)}{p}=\frac{n_K}{2\pi}\int_{3|r|}^{\sqrt{x}}\frac{\mathrm{d}A_{K,2}(T;r)}{T\log T}.$$

By assumption, $A_{K,2}(T;r)=\mathfrak{C}'_{K,r,2}T+O(T/\log T)$. Hence, integrating by parts gives

$$\frac{n_K}{2\pi}\int_{3|r|}^{\sqrt{x}}\frac{\mathrm{d}A_{K,2}(T;r)}{T\log T}=\frac{n_K}{2\pi}\mathfrak{C}'_{K,r,2}\log\log x+O(1).$$

7. *Reduction to a problem of Barban–Davenport–Halberstam Type*

Propositions 14 and 16 reduce the problem of computing an asymptotic formula for

$$\frac{1}{\#\mathcal{C}}\sum_{E\in\mathcal{C}}\pi_E^{r,2}(x)$$

to the problem of showing that there exists a constant $\mathfrak{C}'_{K,r,2}$ such that

$$A_{K,2}(T;r)=\sum_{\substack{k\leqslant 2T\\(k,2r)=1}}\frac{1}{k}\sum_{\substack{3|r|<p\leqslant T\\ f_K(p)=2\\ k^2|r^2-4p^2}}L\left(1,\chi_{d_k(p^2)}\right)\log p=\mathfrak{C}'_{K,r,2}T+O(T/\log T). \tag{17}$$

In this section, we reduce this to a problem of "Barban–Davenport–Halberstam type."

Since every rational prime p that does not ramify and splits into degree two primes in K must either split completely in K' or split into degree two primes in K', we may write

$$A_{K,2}(T;r)=\sum_{\substack{\tau\in\mathrm{Gal}(K'/\mathbb{Q})\\|\tau|=1,2}}A_{K,\tau}(T;r),$$

where the sum runs over the elements $\tau\in\mathrm{Gal}(K'/\mathbb{Q})$ of order dividing two, $A_{K,\tau}(T;r)$ is defined by

$$A_{K,\tau}(T;r):=\sum_{\substack{k\leqslant 2T\\(k,2r)=1}}\frac{1}{k}\sum_{\substack{3|r|<p\leqslant T\\ \left(\frac{K/\mathbb{Q}}{p}\right)\subseteq\mathcal{C}_\tau\\ k^2|r^2-4p^2}}L\left(1,\chi_{d_k(p^2)}\right)\log p, \tag{18}$$

and $\mathcal{C}_\tau$ is the subset of all order two elements of $\mathrm{Gal}(K/\mathbb{Q})$ whose restriction to K' is equal to τ. Thus, it follows that (17) holds if there exists a constant $\mathfrak{C}_r^{(\tau)}$ such that

$$A_{K,\tau}(T,r)=\mathfrak{C}_r^{(\tau)}T+O(T/\log T)$$

for every element $\tau\in\mathrm{Gal}(K'/\mathbb{Q})$ of order dividing two.

PROPOSITION 17. *Let r be a fixed odd integer, let τ be an element of* $\mathrm{Gal}(K'/\mathbb{Q})$ *of order dividing two, and recall the definition of $\mathcal{E}_K(x;Q,\mathcal{C}_\tau)$ as given by (6). If*

$$\mathcal{E}_K(T;T/(\log T)^{12},\mathcal{C}_\tau)\ll\frac{T^2}{(\log T)^{11}}, \tag{19}$$

then

$$A_{K,\tau}(T;r)=\mathfrak{C}_r^{(\tau)}T+O\left(\frac{T}{\log T}\right), \tag{20}$$

where

$$\mathfrak{C}_r^{(\tau)} = \frac{2\#\mathcal{C}_\tau}{3n_K}\prod_{\ell\mid r}\left(\frac{\ell}{\ell-\left(\frac{-1}{\ell}\right)}\right)\sum_{g\in\mathcal{S}_\tau}\sum_{\substack{k=1\\(k,2r)=1}}^{\infty}\frac{1}{k}\sum_{\substack{n=1\\(n,2r)=1}}^{\infty}\frac{1}{n\varphi_K(m_Knk^2)}\sum_{a\in(\mathbb{Z}/n\mathbb{Z})^\times}\left(\frac{a}{n}\right)\#C_g(r,a,n,k) \tag{21}$$

and

$$C_g(r,a,n,k) = \{b\in(\mathbb{Z}/m_Knk^2\mathbb{Z})^\times : 4b^2\equiv r^2-ak^2 \pmod{nk^2},\, b\equiv g \pmod{m_K}\}.$$

Proof. Suppose that d is a discriminant, and let

$$S_d(y) := \sum_{\substack{n\leqslant y\\(n,2r)=1}}\chi_d(n).$$

Burgess' bound for character sums [**3**, theorem 2] implies that

$$\sum_{n\leqslant y}\chi_d(n) \ll y^{1/2}|d|^{7/32}.$$

Since r is a fixed integer, we have that

$$|S_d(y)| = \left|\sum_{m\mid 2r}\mu(m)\sum_{\substack{n\leqslant y\\m\mid n}}\chi_d(n)\right| \ll y^{1/2}|d|^{7/32},$$

where the implied constant depends on r alone. Therefore, for any $U>0$, we have that

$$\sum_{\substack{n>U\\(n,2r)=1}}\frac{\chi_d(n)}{n} = \int_U^\infty\frac{\mathrm{d}S_d(y)}{y} \ll \frac{|d|^{7/32}}{\sqrt{U}}. \tag{22}$$

Now, we consider the case when $d=d_k(p^2)=(r^2-4p^2)/k^2$ with $(k,2r)=1$ and $p>3|r|$. Since r is odd, it is easily checked that $\chi_{d_k(p^2)}(2)=(5/2)=-1$, and $\chi_{d_k(p^2)}(\ell)=(-1/\ell)$ for any prime ℓ dividing r. Therefore, we may write

$$L(1,\chi_{d_k(p^2)}) = \frac{2}{3}\prod_{\ell\mid r}\left(1-\frac{\left(\frac{-1}{\ell}\right)}{\ell}\right)^{-1}\sum_{\substack{n=1\\(n,2r)=1}}^{\infty}\left(\frac{d_k(p^2)}{n}\right)\frac{1}{n},$$

the product being over the primes ℓ dividing r. Since we also have the bound $|d_k(p^2)|\leqslant(2p/k)^2$, the inequality (22) implies that

$$A_{K,\tau}(T;r) = \frac{2}{3}\prod_{\ell\mid r}\left(1-\frac{\left(\frac{-1}{\ell}\right)}{\ell}\right)^{-1}\sum_{\substack{k\leqslant 2T\\(k,2r)=1}}\frac{1}{k}\sum_{\substack{n\leqslant U\\(n,2r)=1}}\frac{1}{n}\sum_{\substack{3|r|<p\leqslant T\\\left(\frac{K/\mathbb{Q}}{p}\right)\subseteq\mathcal{C}_\tau\\k^2\mid r^2-4p^2}}\left(\frac{d_k(p^2)}{n}\right)\log p+O\left(\frac{T^{23/16}}{\sqrt{U}}\right).$$

For any $V>0$, we also have that

$$\sum_{\substack{V<k\leqslant 2T\\(k,2r)=1}}\frac{1}{k}\sum_{\substack{n\leqslant U\\(n,2r)=1}}\frac{1}{n}\sum_{\substack{3|r|<p\leqslant T\\\left(\frac{K/\mathbb{Q}}{p}\right)\subseteq\mathcal{C}_\tau\\k^2\mid r^2-4p^2}}\left(\frac{d_k(p^2)}{n}\right)\log p \ll \log T\log U\sum_{\substack{V<k\leqslant 2T\\(k,2r)=1}}\frac{1}{k}\sum_{\substack{m\leqslant T\\k^2\mid r^2-4m^2}}1,$$

where the last sum on the right runs over all integers $m \leqslant T$ such that $k^2 \mid r^2 - 4m^2$. To bound the double sum on the right, we employ the Chinese Remainder Theorem to see that

$$\sum_{\substack{V<k\leqslant 2T\\(k,2r)=1}} \frac{1}{k} \sum_{\substack{m\leqslant T\\k^2|r^2-4m^2}} 1 < \sum_{\substack{V<k\leqslant 2T\\(k,2r)=1}} \frac{1}{k} \sum_{\substack{m\leqslant 2T\\k|r^2-4m^2}} 1 \leqslant \sum_{\substack{V<k\leqslant 2T\\(k,2r)=1}} \frac{\#\{z\in\mathbb{Z}/k\mathbb{Z} : 4z^2 \equiv r^2 \pmod{k}\}}{k}\frac{T}{k}$$
$$\leqslant T \sum_{V<k\leqslant 2T} \frac{2^{\omega(k)}}{k^2} < T\int_V^\infty \frac{\mathrm{d}N(y)}{y^2} \leqslant \frac{T\log V}{V},$$

where $\omega(k)$ is the number of distinct prime divisors of k and $N(y) = \sum_{k\leqslant y} 2^{\omega(k)} \leqslant y\log y$. See [**16**, p. 68] for example. Therefore, since including the primes $p \leqslant 3|r|$ introduces an error that is $O(\log U \log V)$, we have

$$A_{K,\tau}(T;r) = \frac{2}{3}\prod_{\ell|r}\left(\frac{\ell}{\ell-\left(\frac{-1}{\ell}\right)}\right) \sum_{\substack{k\leqslant V\\(k,2r)=1}} \frac{1}{k} \sum_{\substack{n\leqslant U\\(n,2r)=1}} \frac{1}{n} \sum_{\substack{p\leqslant T\\ \left(\frac{K/\mathbb{Q}}{p}\right)\subseteq C_\tau\\ k^2|r^2-4p^2}} \left(\frac{d_k(p^2)}{n}\right)\log p$$
$$+O\left(\frac{T^{23/16}}{\sqrt{U}} + \frac{T\log T\log U\log V}{V} + \log U\log V\right).$$

If n is odd, the value of $(d_k(p^2)/n)$ depends only on the residue of $d_k(p^2)$ modulo n. Thus, we may regroup the terms of the innermost sum on p to obtain

$$A_{K,\tau}(T;r) = \frac{2}{3}\prod_{\ell|r}\left(\frac{\ell}{\ell-\left(\frac{-1}{\ell}\right)}\right) \sum_{\substack{k\leqslant V\\(k,2r)=1}} \frac{1}{k} \sum_{\substack{n\leqslant U\\(n,2r)=1}} \frac{1}{n} \sum_{a\in(\mathbb{Z}/n\mathbb{Z})^\times} \left(\frac{a}{n}\right) \sum_{\substack{p\leqslant T\\ \left(\frac{K/\mathbb{Q}}{p}\right)\subseteq C_\tau\\ 4p^2\equiv r^2-ak^2 \pmod{nk^2}}} \log p$$
$$+O\left(\frac{T^{23/16}}{\sqrt{U}} + \frac{T\log T\log U\log V}{V} + \log U\log V\right).$$

Suppose that there is a prime $p \mid nk^2$ and satisfying the congruence $4p^2 \equiv r^2 - ak^2 \pmod{nk^2}$. Since $(k,r) = 1$, it follows that p must divide n. Therefore, there can be at most $O(\log n)$ such primes for any given values of a, k and n. Thus,

$$\begin{aligned} A_{K,\tau}(T;r) = \frac{2}{3}&\prod_{\ell|r}\left(\frac{\ell}{\ell-\left(\frac{-1}{\ell}\right)}\right)\\ &\times \sum_{\substack{k\leqslant V\\(k,2r)=1}} \frac{1}{k} \sum_{\substack{n\leqslant U\\(n,2r)=1}} \frac{1}{n} \sum_{a\in(\mathbb{Z}/n\mathbb{Z})^\times} \left(\frac{a}{n}\right) \sum_{\substack{b\in(\mathbb{Z}/nk^2\mathbb{Z})^\times\\ 4b^2\equiv r^2-ak^2 \pmod{nk^2}}} \sum_{\substack{p\leqslant T\\ \left(\frac{K/\mathbb{Q}}{p}\right)\subseteq C_\tau\\ p\equiv b \pmod{nk^2}}} \log p\\ &+O\left(\frac{T^{23/16}}{\sqrt{U}} + \frac{T\log T\log U\log V}{V} + U\log U\log V\right). \end{aligned} \tag{23}$$

We now make the choice

$$U := \frac{T}{(\log T)^{20}}, \tag{24}$$
$$V := (\log T)^4. \tag{25}$$

Note that with this choice the error above is easily $O(T/\log T)$.

Recall the definitions of $\mathcal{C}_\tau$ and $\mathcal{S}_\tau$ from Section 2. Then every prime p counted by the innermost sum of (23) satisfies the condition that $((K'/\mathbb{Q})/p) = \tau$, and hence it follows that $p \equiv g \pmod{m_K}$ for some $g \in \mathcal{S}_\tau$. Therefore, we may rewrite the main term of (23) as

$$\frac{2}{3}\prod_{\ell \mid r}\left(\frac{\ell}{\ell-\left(\frac{-1}{\ell}\right)}\right)\sum_{g\in\mathcal{S}_\tau}\sum_{\substack{k\leqslant V\\(k,2r)=1}}\frac{1}{k}\sum_{\substack{n\leqslant U\\(n,2r)=1}}\frac{1}{n}\sum_{a\in(\mathbb{Z}/n\mathbb{Z})^\times}\left(\frac{a}{n}\right)\sum_{\substack{b\in(\mathbb{Z}/m_Knk^2\mathbb{Z})^\times\\4b^2\equiv r^2-ak^2 \pmod{nk^2}\\b\equiv g \pmod{m_K}}}\theta(T;\mathcal{C}_\tau,m_Knk^2,b). \tag{26}$$

In accordance with our observation in Section 2, the condition that $b \equiv g \pmod{m_K}$ ensures that the two Chebotarëv conditions $((K/\mathbb{Q})/p) \subseteq \mathcal{C}_\tau$ and $p \equiv b \pmod{m_Knk^2}$ are compatible. Therefore, we choose to approximate (26) by

$$T\frac{2\#\mathcal{C}_\tau}{3n_K}\prod_{\ell \mid r}\left(\frac{\ell}{\ell-\left(\frac{-1}{\ell}\right)}\right)\sum_{g\in\mathcal{S}_\tau}\sum_{\substack{k\leqslant V\\(k,2r)=1}}\frac{1}{k}\sum_{\substack{n\leqslant U\\(n,2r)=1}}\frac{1}{n\varphi_K(m_Knk^2)}\sum_{a\in(\mathbb{Z}/n\mathbb{Z})^\times}\left(\frac{a}{n}\right)\#C_g(r,a,n,k), \tag{27}$$

where $C_g(r,a,n,k)$ is as defined in the statement of the proposition.

For the moment, we ignore the error in this approximation and concentrate on the supposed main term. The following lemma, whose proof we delay until Section 11, implies that the expression in (27) is equal to $\mathfrak{C}_r^{(\tau)}T + O(T/\log T)$ for U and V satisfying (24) and (25).

LEMMA 18.
With $\mathfrak{C}_r^{(\tau)}$ as defined in (21), we have

$$\mathfrak{C}_r^{(\tau)} = \frac{2\#\mathcal{C}_\tau}{3n_K}\prod_{\ell \mid r}\left(\frac{\ell}{\ell-\left(\frac{-1}{\ell}\right)}\right)\sum_{g\in\mathcal{S}_\tau}\sum_{\substack{k\leqslant V\\(k,2r)=1}}\frac{1}{k}\sum_{\substack{n\leqslant U\\(n,2r)=1}}\frac{1}{n\varphi_K(m_Knk^2)}\sum_{a\in(\mathbb{Z}/n\mathbb{Z})^\times}\left(\frac{a}{n}\right)\#C_g(r,a,n,k)$$
$$+O\left(\frac{1}{\sqrt{U}}+\frac{\log V}{V^2}\right).$$

We now consider the error in approximating (26) by (27). The error in the approximation is equal to a constant (depending only on K and r) times

$$\sum_{g\in\mathcal{S}_\tau}\sum_{\substack{k\leqslant V\\(k,2r)=1,\\n\leqslant U\\(n,2r)=1}}\frac{1}{kn}\sum_{a\in(\mathbb{Z}/n\mathbb{Z})^\times}\left(\frac{a}{n}\right)\sum_{b\in C_g(r,a,n,k)}\left(\theta(T;\mathcal{C}_\tau,m_Knk^2,b)-\frac{\#\mathcal{C}_\tau}{n_K\varphi_K(m_Knk^2)}T\right).$$

We note that for each $b \in (\mathbb{Z}/m_Knk^2\mathbb{Z})^\times$, there is at most one $a \in (\mathbb{Z}/n\mathbb{Z})^\times$ such that $ak^2 \equiv 4b^2 - r^2 \pmod{nk^2}$. Therefore, interchanging the sum on a with the sum on b and applying the Cauchy–Schwarz inequality, the above error is bounded by

$$\sum_{k\leqslant V}\frac{1}{k}\left[\sum_{n\leqslant U}\frac{\varphi(m_Knk^2)}{n^2}\right]^{1/2}\left[\sum_{n\leqslant U}\sum_{\substack{g\in\mathcal{S}_\tau,\\b\in(\mathbb{Z}/m_Knk^2\mathbb{Z})^\times\\b\equiv g \pmod{m_K}}}\left(\theta(T;\mathcal{C}_\tau,m_Knk^2,b)-\frac{\#\mathcal{C}_\tau}{n_K\varphi_K(m_Knk^2)}T\right)^2\right]^{1/2}.$$

We bound this last expression by a constant times

$$V\sqrt{\log U}\sqrt{\mathcal{E}_K(T;UV^2,\mathcal{C}_\tau)},$$

where $\mathcal{E}_K(T; UV^2, \mathcal{C}_\tau)$ is defined by (6). Given our assumption (19) and our choices (24) and (25) for U and V, the proposition now follows.

8. *Computing the average order constant for a general Galois extension*

In this section, we finish the proof of Theorem 4 by computing the product formula (9) for the constant $\mathfrak{C}_{K,r,2}$. It follows from Propositions 14, 16 and 17 that

$$\mathfrak{C}_{K,r,2} = \frac{n_K}{2\pi}\mathfrak{C}'_{K,r,2},$$

where

$$\mathfrak{C}'_{K,r,2} = \sum_{\substack{\tau\in\mathrm{Gal}(K'/\mathbb{Q})\\ |\tau|=1,2}} \mathfrak{C}_r^{(\tau)}$$

and $\mathfrak{C}_r^{(\tau)}$ is defined by

$$\mathfrak{C}_r^{(\tau)} = \frac{2\#\mathcal{C}_\tau}{3n_K}\prod_{\ell\mid r}\left(\frac{\ell}{\ell-\left(\frac{-1}{\ell}\right)}\right)\sum_{g\in\mathcal{S}_\tau}\sum_{\substack{k=1\\(k,2r)=1}}^{\infty}\frac{1}{k}\sum_{\substack{n=1\\(n,2r)=1}}^{\infty}\frac{1}{n\varphi_K(m_Knk^2)}\sum_{a\in(\mathbb{Z}/n\mathbb{Z})^\times}\left(\frac{a}{n}\right)\#C_g(r,a,n,k).$$

We now recall the definition

$$\mathfrak{c}_r^{(g)} = \sum_{\substack{k=1\\(k,2r)=1}}^{\infty}\frac{1}{k}\sum_{\substack{n=1\\(n,2r)=1}}^{\infty}\frac{1}{n\varphi_K(m_Knk^2)}\sum_{a\in(\mathbb{Z}/n\mathbb{Z})^\times}\left(\frac{a}{n}\right)\#C_g(r,a,n,k)$$

and note that

$$\mathfrak{C}_r^{(\tau)} = \frac{2\#\mathcal{C}_\tau}{3n_K}\prod_{\ell\mid r}\left(\frac{\ell}{\ell-\left(\frac{-1}{\ell}\right)}\right)\sum_{g\in\mathcal{S}_\tau}\mathfrak{c}_r^{(g)}.$$

It remains then to show that

$$\mathfrak{c}_r^{(g)} = \frac{n_{K'}}{\varphi(m_K)}\prod_{\ell\nmid 2rm_K}\left(\frac{\ell\left(\ell-1-\left(\frac{-1}{\ell}\right)\right)}{(\ell-1)\left(\ell-\left(\frac{-1}{\ell}\right)\right)}\right)\prod_{\substack{\ell\mid m_K\\ \ell\nmid 2r}}\mathfrak{K}_r^{(g)}, \tag{28}$$

where the products are taken over the rational primes ℓ satisfying the stated conditions, recalling that $\mathfrak{K}_r^{(g)}$ was defined by

$$\mathfrak{K}_r^{(g)} = \begin{cases} \dfrac{\ell^{\frac{\nu_\ell(4g^2-r^2)+1}{2}}-1}{\ell^{\frac{\nu_\ell(4g^2-r^2)-1}{2}}(\ell-1)} & \text{if } \nu_\ell(4g^2-r^2)<\nu_\ell(m_K) \text{ and } 2\nmid\nu_\ell(4g^2-r^2),\\[2ex] \dfrac{\ell^{\frac{\nu_\ell(4g^2-r^2)}{2}+1}-1}{\ell^{\frac{\nu_\ell(4g^2-r^2)}{2}}(\ell-1)} + \dfrac{\left(\frac{(r^2-4g^2)/\ell^{\nu_\ell(r^2-4g^2)}}{\ell}\right)}{\ell^{\frac{\nu_\ell(4g^2-r^2)}{2}}\left(\ell-\left(\frac{(r^2-4g^2)/\ell^{\nu_\ell(r^2-4g^2)}}{\ell}\right)\right)} & \text{if } \nu_\ell(4g^2-r^2)<\nu_\ell(m_K) \text{ and } 2\mid\nu_\ell(4g^2-r^2),\\[2ex] \dfrac{\ell^{2\left\lceil\frac{\nu_\ell(m_K)}{2}\right\rceil+1}(\ell+1)\left(\ell^{\left\lceil\frac{\nu_\ell(m_K)}{2}\right\rceil}-1\right)+\ell^{\nu_\ell(m_K)+2}}{\ell^{3\left\lceil\frac{\nu_\ell(m_K)}{2}\right\rceil}(\ell^2-1)} & \text{if } \nu_\ell(4g^2-r^2)\geqslant\nu_\ell(m_K). \end{cases}$$

By the Chinese Remainder Theorem and equation (4),

$$\begin{aligned}\mathfrak{c}_r^{(g)} &= \sum_{\substack{k=1\\(k,2r)=1}}^{\infty} \frac{1}{k} \sum_{\substack{n=1\\(n,2r)=1}}^{\infty} \frac{1}{n\varphi_K(m_K nk^2)} \sum_{a\in(\mathbb{Z}/n\mathbb{Z})^\times} \left(\frac{a}{n}\right) \#C_g(r,a,n,k)\\ &= n_{K'} \sum_{\substack{k=1\\(k,2r)=1}}^{\infty} \frac{1}{k} \sum_{\substack{n=1\\(n,2r)=1}}^{\infty} \frac{1}{n\varphi(m_K nk^2)} \sum_{a\in(\mathbb{Z}/n\mathbb{Z})^\times} \left(\frac{a}{n}\right) \prod_{\ell\mid m_K nk^2} \#C_g^{(\ell)}(r,a,n,k),\end{aligned}$$

where the product is taken over the distinct primes ℓ dividing $m_K nk^2$,

$$C_g^{(\ell)}(r,a,n,k) := \{b \in (\mathbb{Z}/\ell^{\nu_\ell(m_K nk^2)}\mathbb{Z})^\times : 4b^2 \equiv r^2 - ak^2 \pmod{\ell^{\nu_\ell(nk^2)}},\, b \equiv g \pmod{\ell^{\nu_\ell(m_K)}}\},$$

and ν_ℓ is the usual ℓ-adic valuation. With somewhat different notation, the following evaluation of $\#C_g^{(\ell)}(r,a,n,k)$ can be found in [**4**].

LEMMA 19. *Let k and n be positive integers satisfying the condition $(nk, 2r) = 1$. Suppose that ℓ is any prime dividing $m_K nk^2$. If $\ell \nmid m_K$, then*

$$\#C_g^{(\ell)}(r,a,n,k) = \begin{cases} 1 + \left(\frac{r^2-ak^2}{\ell}\right) & \text{if } \ell \nmid r^2 - ak^2,\\ 0 & \text{otherwise;}\end{cases}$$

if $\ell \mid m_K$, then

$$\#C_g^{(\ell)}(r,a,n,k) = \begin{cases} \ell^{\min\{\nu_\ell(nk^2),\nu_\ell(m_K)\}} & \text{if } 4g^2 \equiv r^2 - ak^2 \pmod{\ell^{\min\{\nu_\ell(nk^2),\nu_\ell(m_K)\}}},\\ 0 & \text{otherwise.}\end{cases}$$

In particular,

$$\#C_g^{(\ell)}(r,1,1,k) = \begin{cases} 2 & \text{if } \ell \mid k \text{and } \ell \nmid m_K,\\ \ell^{\min\{2\nu_\ell(k),\nu_\ell(m_K)\}} & \text{if } \ell \mid m_K \text{and } 4g^2 \equiv r^2 \pmod{\ell^{\min\{2\nu_\ell(k),\nu_\ell(m_K)\}}},\\ 0 & \text{otherwise.}\end{cases}$$

By Lemma 19 we note that if ℓ is a prime dividing m_K and ℓ does not divide nk, then $\#C_g^{(\ell)}(r,a,n,k) = 1$. We also see that $\#C_g^{(\ell)}(r,a,n,k) = 0$ if $(r^2 - ak^2, n) > 1$. Finally, if $\ell \mid k$ and $\ell \nmid n$, then

$$\#C_g^{(\ell)}(r,a,n,k) = \#C_g^{(\ell)}(r,1,1,k)$$

as $\nu_\ell(nk^2) = 2\nu_\ell(k)$ in this case. Therefore, using the formula $\varphi(mn) = \varphi(m)\varphi(n)(m,n)/$

$\varphi((m,n))$, we have

$$\begin{aligned}
\mathfrak{c}_r^{(g)} &= n_{K'} \sum_{\substack{k=1\\(k,2r)=1}}^{\infty} \frac{1}{k^2\varphi(m_K k)} \sum_{\substack{n=1\\(n,2r)=1}}^{\infty} \frac{\varphi\left((n, m_K k)\right)}{n\varphi(n)(n, m_K k)} \sum_{\substack{a\in(\mathbb{Z}/n\mathbb{Z})^\times\\(r^2-ak^2,n)=1}} \left(\frac{a}{n}\right) \prod_{\ell|nk} \#C_g^{(\ell)}(r,a,n,k)\\
&= n_{K'} \sum_{\substack{k=1\\(k,2r)=1}}^{\infty} \frac{1}{k^2\varphi(m_K k)} \sum_{\substack{n=1\\(n,2r)=1}}^{\infty} \frac{\varphi\left((n, m_K k)\right) \prod_{\substack{\ell|k\\ \ell\nmid n}} \#C_g^{(\ell)}(r,1,1,k)}{n\varphi(n)(n, m_K k)} c_k(n)\\
&= \frac{n_{K'}}{\varphi(m_K)} \sum_{\substack{k=1\\(k,2r)=1}}^{\infty} \frac{\varphi((m_K,k))}{(m_K,k)k^2\varphi(k)} \sum_{\substack{n=1\\(n,2r)=1}}^{\infty} \frac{\varphi\left((n, m_K k)\right) \prod_{\substack{\ell|k\\ \ell\nmid n}} \#C_g^{(\ell)}(r,1,1,k)}{n\varphi(n)(n, m_K k)} c_k(n)\\
&= \frac{n_{K'}}{\varphi(m_K)} \sideset{}{'}\sum_{k=1}^{\infty} \frac{\varphi((m_K,k)) \prod_{\ell|k} \#C_g^{(\ell)}(r,1,1,k)}{(m_K,k)k^2\varphi(k)}\\
&\quad\times \sum_{\substack{n=1\\(n,2r)=1}}^{\infty} \frac{\varphi\left((n, m_K k)\right) c_k(n)}{n\varphi(n)(n, m_K k) \prod_{\ell|(k,n)} \#C_g^{(\ell)}(r,1,1,k)}.
\end{aligned} \tag{29}$$

Here $c_k(n)$ is defined by

$$c_k(n) := \sum_{\substack{a\in(\mathbb{Z}/n\mathbb{Z})^\times\\(r^2-ak^2,n)=1}} \left(\frac{a}{n}\right) \prod_{\ell|n} \#C_g^{(\ell)}(r,a,n,k), \tag{30}$$

for $(n,2r)=1$, and the prime on the sum over k is meant to indicate that the sum is to be restricted to those k which are coprime to $2r$ and not divisible by any prime ℓ for which $\#C_g^{(\ell)}(r,1,1,k)=0$.

LEMMA 20. *Assume that k is an integer coprime to $2r$. The function $c_k(n)$ defined by equation (30) is multiplicative in n. Suppose that ℓ is a prime not dividing $2r$. If $\ell \nmid km_K$, then*

$$\frac{c_k(\ell^e)}{\ell^{e-1}} = \begin{cases} \ell-3 & \text{if } 2 \mid e,\\ -\left(1+\left(\frac{-1}{\ell}\right)\right) & \text{if } 2 \nmid e.\end{cases}$$

If $\ell \mid km_K$, then

$$\frac{c_k(\ell^e)}{\ell^{e-1}} = \#C_g^{(\ell)}(r,1,1,k) \begin{cases} \ell-1 & \text{if } 2 \mid e,\\ 0 & \text{if } 2 \nmid e\end{cases}$$

in the case that $\nu_\ell(m_K) \leqslant 2\nu_\ell(k)$; and

$$\frac{c_k(\ell^e)}{\ell^{e-1}} = \#C_g^{(\ell)}(r,1,1,k) \left(\frac{(r^2-4g^2)/\ell^{2\nu_\ell(k)}}{\ell}\right)^e \ell$$

in the case that $2\nu_\ell(k) < \nu_\ell(m_K)$. Furthermore, for $(n,2r)=1$, we have

$$c_k(n) \ll \frac{n\prod_{\ell|(n,k)} \#C_g^{(g)}(r,1,1,k)}{\kappa_{m_K}(n)},$$

where for any integer N, $\kappa_N(n)$ is the multiplicative function defined on prime powers by

$$\kappa_N(\ell^e) := \begin{cases} \ell & \text{if } \ell \nmid N \text{and } 2 \nmid e,\\ 1 & \text{otherwise.}\end{cases} \tag{31}$$

Remark 21. Lemma 20 is essentially proved in [**4**], but we give the proof in Section 11 for completeness.

Using the lemma and recalling the restrictions on k, we factor the sum over n in (29) as

$$\begin{aligned}
&\sum_{\substack{n=1\\(n,2r)=1}}^{\infty} \frac{\varphi\left((n, m_K k)\right) c_k(n)}{n\varphi(n)(n, m_K k)\prod_{\ell\mid(k,n)} \#C_g^{(\ell)}(r,1,1,k)}\\
&\quad = \prod_{\ell\nmid 2rm_K k}\left[\sum_{e\geqslant 0}\frac{c_k(\ell^e)}{\ell^e\varphi(\ell^e)}\right]\prod_{\substack{\ell\mid m_K k\\(\ell\nmid 2r)}}\left[1+\sum_{e\geqslant 1}\frac{\left(1-\frac{1}{\ell}\right)c_k(\ell^e)}{\ell^e\varphi(\ell^e)\#C_g^{(\ell)}(r,1,1,k)}\right]\\
&\quad = \prod_{\ell\nmid 2rm_K k} F_0(\ell)\prod_{\substack{\ell\mid m_K k\\(\ell\nmid 2r)}} F_1^{(g)}(\ell,k)\\
&\quad = \prod_{\ell\nmid 2rm_K} F_0(\ell)\prod_{\substack{\ell\mid m_K\\ \ell\nmid 2r}} F_1^{(g)}(\ell,1)\prod_{\substack{\ell\mid k\\ \ell\nmid m_K\\(\ell\nmid 2r)}}\frac{F_1^{(g)}(\ell,k)}{F_0(\ell)}\prod_{\substack{\ell\mid(m_K,k)\\(\ell\nmid 2r)}}\frac{F_1^{(g)}(\ell,k)}{F_1^{(g)}(\ell,1)}
\end{aligned}$$

where for any odd prime ℓ, we make the definitions

$$\begin{aligned}
F_0(\ell) &:= 1-\frac{\left(\frac{-1}{\ell}\right)\ell+3}{(\ell-1)^2(\ell+1)},\\
F_1^{(g)}(\ell,k) &:= \begin{cases} 1+\dfrac{\left(\frac{(r^2-4g^2)/\ell^{2\nu_\ell(k)}}{\ell}\right)}{\ell-\left(\frac{(r^2-4g^2)/\ell^{2\nu_\ell(k)}}{\ell}\right)} & \text{if } 2\nu_\ell(k)<\nu_\ell(m_K) \text{and } 4g^2\equiv r^2 \pmod{\ell^{2\nu_\ell(k)}},\\ 1+\frac{1}{\ell(\ell+1)} & \text{if } 2\nu_\ell(k)\geqslant\nu_\ell(m_K) \text{and } 4g^2\equiv r^2 \pmod{\ell^{\nu_\ell(m_K)}}.\end{cases}
\end{aligned}$$

Substituting this back into (29) and factoring the sum over k, we have

$$\begin{aligned}
\mathfrak{c}_r^{(g)} &= \frac{n_{K'}}{\varphi(m_K)}\prod_{\ell\nmid 2rm_K} F_0(\ell)\prod_{\substack{\ell\mid m_K\\ \ell\nmid 2r}} F_1^{(g)}(\ell,1)\\
&\quad\times\prod_{\ell\nmid 2rm_K}\left(1+\sum_{e\geqslant 1}\frac{F_1(\ell,\ell^e)2^{\omega(\ell^e)}}{F_0(\ell)\ell^{2e}\varphi(\ell^e)}\right)\prod_{\substack{\ell\nmid 2r\\ \ell\mid m_K}}\left(1+\sum_{e\geqslant 1}\frac{\left(1-\frac{1}{\ell}\right)\#C_g^{(\ell)}(r,1,1,\ell^e)F_1^{(g)}(\ell,\ell^e)}{\ell^{2e}\varphi(\ell^e)F_1^{(g)}(\ell,1)}\right).
\end{aligned}$$

Using Lemma 19 and the definitions of $F_0(\ell)$ and $F_1^{(g)}(\ell,k)$ to simplify, we have proved (28).

9. *Pretentious and totally non-Abelian number fields*

In this section, we give the definitions and basic properties of pretentious and totally non-Abelian number fields.

DEFINITION 22. *We say that a number field F is totally non-Abelian if $F/\mathbb{Q}$ is Galois and* $\mathrm{Gal}(F/\mathbb{Q})$ *is a perfect group, i.e.,* $\mathrm{Gal}(F/\mathbb{Q})$ *is equal to its own commutator subgroup.*

Recall that a group is Abelian if and only if its commutator subgroup is trivial. Thus, in this sense, perfect groups are as far away from being Abelian as possible. However, we adopt the convention that the trivial group is perfect, and so the trivial extension ($F=\mathbb{Q}$) is both Abelian and totally non-Abelian. The following proposition follows easily from basic group theory and the Kronecker–Weber Theorem [**13**, p. 210].

PROPOSITION 23. *Let F be a number field. Then F is totally non-Abelian if and only if F is linearly disjoint from every cyclotomic field, i.e., $F \cap \mathbb{Q}(\zeta_q) = \mathbb{Q}$ for every $q \geqslant 1$.*

DEFINITION 24. *Let f be a positive integer. We say that a number field F is f-pretentious if there exists a finite list of congruence conditions $\mathcal{L}$ such that, apart from a density zero subset of exceptions, every rational prime p splits into degree f primes in F if and only if p satisfies a congruence on the list $\mathcal{L}$.*

If F is a Galois extension and $f \nmid n_F$, then no rational prime may split into degree f primes in F. In this case, we say that F is "vacuously" f-pretentious. In this sense, we say the trivial extension ($F = \mathbb{Q}$) is f-pretentious for every $f \geqslant 1$. The term pretentious is meant to call to mind the notion that such number fields "pretend" to be Abelian over $\mathbb{Q}$, at least in so far as their degree f primes are concerned. Indeed, one can prove that the 1-pretentious number fields are precisely the Abelian extensions of $\mathbb{Q}$, and every Abelian extension is f-pretentious for every $f \geqslant 1$ (being vacuously f-pretentious for every f not dividing the degree of the extension). The smallest non-Abelian group to be the Galois group of a 2-pretentious extension of $\mathbb{Q}$ is the symmetric group $S_3 := \langle r, s : |r| = 3, s^2 = 1, rs = sr^{-1}\rangle$. The smallest groups that cannot be the Galois group of a 2-pretentious extension of $\mathbb{Q}$ are the dihedral group $D_4 = \langle r, s : |r| = 4, s^2 = 1, rs = sr^{-1}\rangle$ and the quaternion group $Q_8 := \langle -1, i, j, k : (-1)^2 = 1, i^2 = j^2 = k^2 = ijk = -1\rangle$.

PROPOSITION 25. *Suppose that F is a 2-pretentious Galois extension of $\mathbb{Q}$, and let F' denote the fixed field of the commutator subgroup of $\mathrm{Gal}(F/\mathbb{Q})$. Let τ be an order two element of $\mathrm{Gal}(F'/\mathbb{Q})$, and let $\mathcal{C}_\tau$ be the subset of order two elements of $G = \mathrm{Gal}(F/\mathbb{Q})$ whose restriction to F' is equal to τ. Then for any rational prime p that does not ramify in F, we have that $((F'/\mathbb{Q})/p) = \tau$ if and only if $p \equiv g \pmod{m_F}$ for some $g \in \mathcal{S}_\tau$ if and only if $((F/\mathbb{Q})/p) \subseteq \mathcal{C}_\tau$.*

Proof. In Section 2, we saw that the first equivalence holds. Indeed, this is the definition of $\mathcal{S}_\tau$. Furthermore, if $((F/\mathbb{Q})/p) \subseteq \mathcal{C}_\tau$, then $((F'/\mathbb{Q})/p) = ((F/\mathbb{Q})/p)|_{F'} = \tau$, and so $p \equiv g \pmod{m_F}$ for some $g \in \mathcal{S}_\tau$. Thus, it remains to show that if $p \equiv g \pmod{m_F}$ for some $g \in \mathcal{S}_\tau$, then $((F/\mathbb{Q})/p) \subseteq \mathcal{C}_\tau$.

Since F is 2-pretentious, there exists a a finite list of congruences $\mathcal{L}$ that determine, apart from a density zero subset of exceptions, which rational primes split into degree two primes in F. Lifting congruences, if necessary, we may assume that all of the congruences on the list $\mathcal{L}$ have the same modulus, say m. Lifting congruences again, if necessary, we may assume that $m_F \mid m$. Since $m_F \mid m$, it follows that $\mathbb{Q}(\zeta_m) \cap F = F'$ by definition of F'. As noted in Section 2, the extension $F(\zeta_m)/\mathbb{Q}$ is Galois with group

$$\mathrm{Gal}\left(F(\zeta_m)/\mathbb{Q}\right) \cong \{(\sigma_1, \sigma_2) \in \mathrm{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q}) \times G : \sigma_1|_{F'} = \sigma_2|_{F'}\}. \tag{1}$$

Let $\varpi : \mathrm{Gal}(F/\mathbb{Q}) \to \mathrm{Gal}(F'/\mathbb{Q})$ be the natural projection given by restriction of automorphisms. We first show that $[F : F'] = \#\ker\varpi$ is odd, which allows us to deduce that $\mathcal{C}_\tau$ is not empty. For each $\sigma \in G = \mathrm{Gal}(F/\mathbb{Q})$, we let C_σ denote the conjugacy class of σ in G. We note that (1) and the Chebotarëv Density Theorem together imply that for each $\sigma \in \ker\varpi$ the density of primes p such that $p \equiv 1 \pmod{m}$ and $((F/\mathbb{Q})/p) = C_\sigma$ is equal to $(\#C_\sigma/\varphi_F(m)n_F) = n_{F'}\#C_\sigma/\varphi(m)n_F > 0$. In particular, the trivial automorphism $1_F \in \ker\varpi$, and so it follows by definition of 2-pretentious that at most a density zero subset of the $p \equiv 1 \pmod{m}$ may split into degree two primes in F. However, if $[F : F'] = \#\ker\varpi$ is even, then $\ker\varpi$ would contain an element of order 2 and the same argument with σ replacing 1_F would imply that there is a positive density of $p \equiv 1 \pmod{m}$ that split into degree two primes in F. Therefore, we conclude that $[F : F']$ is odd. Now letting σ be any element of G such that $\varpi(\sigma) = \sigma|_{F'} = \tau$, we find that $\sigma^{[F:F']} \in \mathcal{C}_\tau$, and so $\mathcal{C}_\tau$ is not empty.

Finally, let $g \in \mathcal{S}_\tau$ be arbitrarily chosen, and let a by any integer such that $a \equiv g \pmod{m_F}$. Again using (1) and the Chebotarëv Density Theorem, we see that the density of rational primes p satisfying the two conditions $p \equiv a \pmod{m}$ and $((F/\mathbb{Q})/p) \subseteq \mathcal{C}_\tau$ is equal to $\#\mathcal{C}_\tau/\varphi_F(m)n_F > 0$. Since every such prime must split into degree two primes in F and since a was an arbitrary integer satisfying the condition $a \equiv g \pmod{m_F}$, it follows from the definition of 2-pretentious that, apart from a density zero subset of exceptions, every rational prime $p \equiv g \pmod{m_F}$ must split into degree two primes in F. Therefore, if p is any rational prime not ramifying in F and satisfying the congruence condition $p \equiv g \pmod{m_F}$, then $((F'/\mathbb{Q})/p) = \tau$ and $((F/\mathbb{Q})/p) = C'$ for some conjugacy class C' of order two elements in F. Hence, it follows that $((F/\mathbb{Q})/p) = C' \subseteq \mathcal{C}_\tau$.

10. *Proofs of Theorems* 7 *and* 8

In this section, we give the proof of Theorem 7 and sketch the alteration in strategy that gives the proof of Theorem 8. The main tool in this section is a certain variant of the classical Barban–Davenport–Halberstam Theorem. The setup is as follows. Let F/F_0 be a Galois extension of number fields, let C be any subset of $\mathrm{Gal}(F/F_0)$ that is closed under conjugation, and for any pair of integers q and a, define

$$\theta_{F/F_0}(x; C, q, a) := \sum_{\substack{\mathbf{N}\mathfrak{p} \leqslant x \\ \deg \mathfrak{p} = 1 \\ \left(\frac{F/F_0}{\mathfrak{p}}\right) \subseteq C \\ \mathbf{N}\mathfrak{p} \equiv a \pmod{q}}} \log \mathbf{N}\mathfrak{p},$$

where the sum is taken over the degree one prime ideals $\mathfrak{p}$ of F_0. If $F_0(\zeta_q) \cap F = F_0$, it follows from the ideas discussed in Section 2 that

$$\theta_{F/F_0}(x; C, q, a) \sim \frac{n_{F_0}\#C}{n_F \varphi_{F_0}(q)} x$$

whenever $a \in G_{F_0,q}$. The following is a restatement of the main result of [**19**].

THEOREM 26. *Let $M > 0$. If $x(\log x)^{-M} \leqslant Q \leqslant x$, then*

$$\sideset{}{'}\sum_{q \leqslant Q} \sum_{a \in G_{k,q}} \left(\theta_{F/F_0}(x; C, q, a) - \frac{n_{F_0}\#C}{n_F \varphi_{F_0}(q)} x \right)^2 \ll x Q \log x, \tag{33}$$

where the prime on the outer summation indicates that the sum is to be restricted to those $q \leqslant Q$ satisfying $F \cap F_0(\zeta_q) = F_0$. The constant implied by the symbol $\ll$ depends on F and M.

Proof of Theorem 7. In light of Theorem 4, it suffices to show that

$$\mathcal{E}_K(x; x/(\log x)^{12}, \mathcal{C}_\tau) \ll \frac{x^2}{(\log x)^{11}}$$

for every element τ of order dividing two in $\mathrm{Gal}(K'/\mathbb{Q})$.

By assumption, we may decompose the field K as a disjoint compositum, writing $K = K_1 K_2$, where $K_1 \cap K_2 = \mathbb{Q}$, K_1 is a 2-pretentious Galois extension of $\mathbb{Q}$, and K_2 is totally non-Abelian. Let G_1, G_2 denote the Galois groups of $K_1/\mathbb{Q}$ and $K_2/\mathbb{Q}$, respectively. We identify the Galois group $G = \mathrm{Gal}(K/\mathbb{Q})$ with $G_1 \times G_2$. Since K_2 is totally non-Abelian, it follows that $G' = G_1' \times G_2$, and hence $K' = K_1'$ and $m_K = m_{K_1}$. Let $C_{2,2}$ denote the subset of all order two elements in G_2 and let $C_{1,\tau}$ denote the subset of elements in G_1 whose restriction to K' is equal to τ. Recalling that every element of $\mathcal{C}_\tau$ must have order two in G, we find that under the identification $G = G_1 \times G_2$, we have

$$\mathcal{C}_\tau = \{1\} \times C_{2,2}$$

if $|\tau| = 1$ and

$$\mathcal{C}_\tau = C_{1,\tau} \times \left(C_{2,2} \cup \{1\}\right)$$

if $|\tau| = 2$. Here we have used Proposition 25 with $F = K_1$ and the fact that $K' = K_1'$. We now break into cases depending on whether $\tau \in \mathrm{Gal}(K'/\mathbb{Q})$ is trivial or not. First, suppose that τ is trivial. Then for each $a \in (\mathbb{Z}/qm_K\mathbb{Z})^\times$ such that $a \equiv b \pmod{m_K}$ for some $b \in \mathcal{S}_\tau$, we have

$$\begin{aligned}
\theta(x; \mathcal{C}_\tau, qm_K, a) - \frac{\#\mathcal{C}_\tau}{n_K \varphi_K(qm_K)} x &= \sum_{\substack{p \leqslant x \\ p \equiv a \pmod{qm_K} \\ \left(\frac{K/\mathbb{Q}}{p}\right) \subseteq \mathcal{C}_\tau}} \log p - \frac{\#\mathcal{C}_\tau}{n_K \varphi_K(qm_K)} x \\
&= \frac{1}{n_{K_1}} \sum_{\substack{\mathbf{N}\mathfrak{p} \leqslant x \\ \deg \mathfrak{p} = 1 \\ \mathbf{N}\mathfrak{p} \equiv a \pmod{qm_K} \\ \left(\frac{K/K_1}{\mathfrak{p}}\right) \subseteq C_{2,2}}} \log \mathbf{N}\mathfrak{p} - \frac{\#C_{2,2}}{n_K \varphi_{K_1}(qm_{K_1})} x \\
&= \frac{1}{n_{K_1}} \left(\theta_{K/K_1}(x; C_{2,2}, qm_{K_1}, a) - \frac{n_{K_1} \#C_{2,2}}{n_K \varphi_{K_1}(qm_{K_1})} x \right).
\end{aligned}$$

Thus, we have that

$$\mathcal{E}_K(x; x/(\log x)^{12}, \mathcal{C}_\tau) = \frac{1}{n_{K_1}^2} \sum_{q \leqslant \frac{x}{(\log x)^{12}}} \sum_{a \in G_{K_1, qm_K}} \left(\theta_{K/K_1}(x; C_{2,2}, qm_{K_1}, a) - \frac{n_{K_1} \#C_{2,2}}{n_K \varphi_{K_1}(qm_{K_1})} x \right)^2.$$

We note that $K_1(\zeta_{qm_K}) \cap K = K_1$ for all $q \geqslant 1$ since K_2 is totally non-Abelian. Hence, the result follows for this case by applying Theorem 26 with $F_0 = K_1$ and $F = K$.

Now, suppose that $|\tau| = 2$. Then the condition $((K/\mathbb{Q})/p) \subseteq \mathcal{C}_\tau$ is equivalent to the two conditions $((K_1/\mathbb{Q})/p) \subseteq C_{1,\tau}$ and $((K_2/\mathbb{Q})/p) \subseteq C_{2,2} \cup \{1\}$. Using Proposition 25 and the fact that $K_1' = K'$, this is equivalent to the two conditions $p \equiv b \pmod{m_K}$ for some $b \in \mathcal{S}_\tau$ and $((K_2/\mathbb{Q})/p) \subseteq C_{2,2} \cup \{1\}$. Hence, for each $a \in (\mathbb{Z}/qm_K\mathbb{Z})^\times$ such that $a \equiv b \pmod{m_K}$ for some $b \in \mathcal{S}_\tau$, we have

$$\theta(x; \mathcal{C}_\tau, qm_K, a) - \frac{\#\mathcal{C}_\tau}{n_K \varphi_K(qm_K)} x = \theta_{K_2/\mathbb{Q}}(x; C_{2,2} \cup \{1\}, qm_K, a) - \frac{1 + \#C_{2,2}}{n_{K_2} \varphi(qm_K)} x$$

as

$$\frac{\#C_{1,\tau}}{n_{K_1} \varphi_{K_1}(qm_K)} = \frac{n_{K_1}/n_{K_1'}}{n_{K_1} \varphi_{K_1}(qm_K)} = \frac{1}{\varphi(qm_K)}.$$

Thus, we have that

$$\mathcal{E}_K(x; x/(\log x)^{12}, \mathcal{C}_\tau) = \sum_{q \leqslant \frac{x}{(\log x)^{12}}} \sum_{a \in (\mathbb{Z}/qm_K\mathbb{Z})^\times} \left(\theta_{K_2/\mathbb{Q}}(x; C_{2,2} \cup \{1\}, qm_K, a) - \frac{1 + \#C_{2,2}}{n_{K_2} \varphi(qm_K)} x \right)^2.$$

Here, as well, we have that $\mathbb{Q}(\zeta_{qm_K}) \cap K_2 = \mathbb{Q}$ for all $q \geqslant 1$ because K_2 is totally non-Abelian. Hence, the result follows for this case by applying Theorem 26 with $F_0 = \mathbb{Q}$ and $F = K_2$.

Proof sketch of Theorem 8 In order to obtain this result, we change our strategy from the proof of Theorem 4 slightly. In particular, if K' is ramified only at primes which divide $2r$, then it follows that $\mathbb{Q}(\zeta_q) \cap K = \mathbb{Q}$ whenever $(q, 2r) = 1$. Therefore, we go back to equation (23) in the proof of Proposition 17 and apply the Chebotarëv Density Theorem immediately. Then we use Cauchy–Schwarz and Theorem 26 to bound the error in this approximation.

11. *Proofs of Lemmas*

Proof of Lemma 18. It suffices to show that

$$\mathfrak{c}_r^{(g)} = \sum_{\substack{k\leqslant V\\(k,2r)=1}} \frac{1}{k} \sum_{\substack{n\leqslant U\\(n,2r)=1}} \frac{1}{n\varphi_K(m_K nk^2)} \sum_{a\in(\mathbb{Z}/n\mathbb{Z})^\times} \left(\frac{a}{n}\right) \#C_g(r,a,n,k) + O\left(\frac{1}{\sqrt{U}} + \frac{\log V}{V^2}\right)$$

for each $g \in \mathcal{S}_\tau$, where $\mathfrak{c}_r^{(g)}$ is defined by (8). We note that since K is a fixed number field, it follows that m_K is fixed. Thus, using Lemma 19, Lemma 20 and equation (4), we have that

$$\begin{aligned}
&\mathfrak{c}_r^{(g)} - \sum_{\substack{k\leqslant V\\(k,2r)=1}} \frac{1}{k} \sum_{\substack{n\leqslant U\\(n,2r)=1}} \frac{1}{n\varphi_K(m_K nk^2)} \sum_{a\in(\mathbb{Z}/n\mathbb{Z})^\times} \left(\frac{a}{n}\right) \#C_g(r,a,n,k)\\
&\ll \sum_{\substack{k\leqslant V\\(k,2r)=1}} \frac{\prod_{\ell|k} \#C_g^{(\ell)}(r,1,1,k)}{k^2\varphi(k)} \sum_{\substack{n>U\\(n,2r)=1}} \frac{c_k(n)}{n\varphi(n)\prod_{\ell|(n,k)} \#C_g^{(\ell)}(r,1,1,k)}\\
&\quad + \sum_{\substack{k>V\\(k,2r)=1}} \frac{\prod_{\ell|k} \#C_g^{(\ell)}(r,1,1,k)}{k^2\varphi(k)} \sum_{\substack{n=1\\(n,2r)=1}}^{\infty} \frac{c_k(n)}{n\varphi(n)\prod_{\ell|(n,k)} \#C_g^{(\ell)}(r,1,1,k)} \qquad (34)\\
&\ll \sum_{\substack{k\leqslant V\\(k,2r)=1}} \frac{\prod_{\ell|k} \#C_g^{(\ell)}(r,1,1,k)}{k^2\varphi(k)} \sum_{\substack{n>U\\(n,2r)=1}} \frac{1}{\kappa_{m_K}(n)\varphi(n)}\\
&\quad + \sum_{\substack{k>V\\(k,2r)=1}} \frac{\prod_{\ell|k} \#C_g^{(\ell)}(r,1,1,k)}{k^2\varphi(k)} \sum_{\substack{n=1\\(n,2r)=1}}^{\infty} \frac{1}{\kappa_{m_K}(n)\varphi(n)}.
\end{aligned}$$

where for any integer N, $\kappa_N(n)$ is the multiplicative function defined by (31). In [**5**, p. 175], we find the bound

$$\sum_{n>U} \frac{1}{\kappa_1(n)\varphi(n)} \ll \frac{1}{\sqrt{U}}.$$

Therefore,

$$\begin{aligned}
\sum_{n>U} \frac{1}{\kappa_{m_K}(n)\varphi(n)} &= \sum_{\substack{mn>U\\(n,m_K)=1\\ \ell|m\Rightarrow\ell|m_K}} \frac{1}{\kappa_1(n)\varphi(n)\varphi(m)} \leqslant \sum_{\substack{m\geqslant 1\\ \ell|m\Rightarrow\ell|m_K}} \frac{1}{\varphi(m)} \sum_{n>U/m} \frac{1}{\kappa_1(n)\varphi(n)}\\
&\ll \frac{1}{\sqrt{U}} \sum_{\substack{m\geqslant 1\\ \ell|m\Rightarrow\ell|m_K}} \frac{\sqrt{m}}{\varphi(m)} = \frac{1}{\sqrt{U}} \prod_{\ell|m_K} \left(1 + \frac{\ell}{(\ell-1)(\sqrt{\ell}-1)}\right)\\
&\ll \frac{1}{\sqrt{U}}.
\end{aligned}$$

Similarly, using Lemma 19, we have that

$$\begin{aligned}
\sum_{\substack{k>V\\(k,2r)=1}} \frac{\prod_{\ell|k} \#C_g^{(\ell)}(r,1,1,k)}{k^2\varphi(k)} &\leqslant \sum_{\substack{m\geqslant 1\\ \ell|m\Rightarrow \ell|m_K}} \frac{m_K}{m^2\varphi(m)} \sum_{\substack{k>V/m\\(k,2rm_K)=1}} \frac{2^{\omega(k)}}{k^2\varphi(k)}\\
&\ll \sum_{\substack{m\geqslant 1\\ \ell|m\Rightarrow \ell|m_K}} \frac{\log(V/m)}{m^2\varphi(m)(V/m)^2}\\
&\leqslant \frac{\log V}{V^2} \sum_{\substack{m\geqslant 1\\ \ell|m\Rightarrow \ell|m_K}} \frac{1}{\varphi(m)}\\
&= \frac{\log V}{V^2} \prod_{\ell|m_K} \left(1+\frac{\ell}{(\ell-1)^2}\right)\\
&\ll \frac{\log V}{V^2}
\end{aligned}$$

as

$$\sum_{k>V} \frac{2^{\omega(k)}}{k^2\varphi(k)} = \int_V^\infty \frac{\mathrm{d}N_0(t)}{t^3} \ll \frac{\log V}{V^2},$$

where

$$N_0(t) := \sum_{k\leqslant t} \frac{k^3 2^{\omega(k)}}{k^2\varphi(k)} \ll \frac{t}{\log t} \sum_{k\leqslant t} \frac{k^3 2^{\omega(k)}/k^2\varphi(k)}{k} \ll \frac{t}{\log t} \exp\left\{\sum_{\ell\leqslant t} \frac{2}{\ell-1}\right\} \ll t\log t.$$

Substituting these bounds into (34) finishes the proof of the lemma.

Proof of Lemma 20. The multiplicativity of $c_k(n)$ follows easily by the Chinese Remainder Theorem. We now compute $c_k(n)$ when $n=\ell^e$ is a prime power and $\ell \nmid 2r$.

If $\ell \nmid m_K$, then by Lemma 19,

$$\begin{aligned}
c_k(\ell^e) &= \sum_{\substack{a\in(\mathbb{Z}/\ell^e\mathbb{Z})^\times\\(r^2-ak^2,\ell^e)=1}} \left(\frac{a}{\ell}\right)^e \#C_g^{(\ell)}(r,a,\ell^e,k)\\
&= \ell^{e-1} \sum_{a\in(\mathbb{Z}/\ell\mathbb{Z})^\times} \left(\frac{a}{\ell}\right)^e \left(\frac{r^2-ak^2}{\ell}\right)^2 \left[1+\left(\frac{r^2-ak^2}{\ell}\right)\right] \qquad (35)\\
&= \ell^{e-1} \sum_{a\in\mathbb{Z}/\ell\mathbb{Z}} \left(\frac{a}{\ell}\right)^e \left[\left(\frac{r^2-ak^2}{\ell}\right)^2 + \left(\frac{r^2-ak^2}{\ell}\right)\right].
\end{aligned}$$

If $\ell \mid k$, then this last expression gives

$$\frac{c_k(\ell^e)}{\ell^{e-1}} = 2\sum_{a\in\mathbb{Z}/\ell\mathbb{Z}} \left(\frac{a}{\ell}\right)^e = \#C_g^{(\ell)}(r,1,1,k) \begin{cases} \ell-1 & \text{if } 2\mid e,\\ 0 & \text{if } 2\nmid e\end{cases}$$

as $(k,r)=1$. If $\ell\nmid k$, then (35) gives

$$\begin{aligned}\frac{c_k(\ell^e)}{\ell^{e-1}}&=\sum_{a\in\mathbb{Z}/\ell\mathbb{Z}}\left(\frac{a}{\ell}\right)^e\left[\left(\frac{r^2-a}{\ell}\right)^2+\left(\frac{r^2-a}{\ell}\right)\right]\\&=\sum_{b\in\mathbb{Z}/\ell\mathbb{Z}}\left(\frac{r^2-b}{\ell}\right)^e\left[\left(\frac{b}{\ell}\right)^2+\left(\frac{b}{\ell}\right)\right]\\&=\begin{cases}\ell-3 & \text{if } 2\mid e,\\ -\left(1+\left(\frac{-1}{\ell}\right)\right) & \text{if } 2\nmid e.\end{cases}\end{aligned}$$

Now, we consider the cases when $\ell\mid m_K$. First, suppose that $1\leqslant\nu_\ell(m_K)\leqslant 2\nu_\ell(k)$. Then as $\nu_\ell(m_K)\leqslant 2\nu_\ell(k)<e+2\nu_\ell(k)=\nu_\ell(nk^2)$, we have that $4g^2\equiv r^2-ak^2 \pmod{\ell^{\nu_\ell(m_K)}}$ if and only if $4g^2\equiv r^2 \pmod{\ell^{\nu_\ell(m_K)}}$. Therefore,

$$\begin{aligned}\#C_g^{(\ell)}(r,a,\ell^e,k)&=\begin{cases}\ell^{\nu_\ell(m_K)} & \text{if } 4g^2\equiv r^2 \pmod{\ell^{\nu_\ell(m_K)}},\\ 0 & \text{otherwise,}\end{cases}\\&=\#C_g^{(\ell)}(r,1,1,k)\end{aligned}$$

for all $a\in(\mathbb{Z}/\ell^e\mathbb{Z})^\times$. Since $\ell\mid k$ and $(k,r)=1$, it follows that $\ell\nmid r^2-ak^2$ for all $a\in\mathbb{Z}/\ell^e\mathbb{Z}$. Whence, in this case,

$$\begin{aligned}\frac{c_k(\ell^e)}{\ell^{e-1}}&=\frac{1}{\ell^{e-1}}\sum_{\substack{a\in\mathbb{Z}/\ell^e\mathbb{Z}\\(r^2-ak^2,\ell)=1}}\left(\frac{a}{\ell}\right)^e\#C_g^{(\ell)}(r,a,\ell^e,k)\\&=\#C_g^{(\ell)}(r,1,1,k)\sum_{a\in\mathbb{Z}/\ell\mathbb{Z}}\left(\frac{a}{\ell}\right)^e\\&=\#C_g^{(\ell)}(r,1,1,k)\begin{cases}\ell-1 & \text{if } 2\mid e,\\ 0 & \text{if } 2\nmid e.\end{cases}\end{aligned}$$

Now, suppose that $2\nu_\ell(k)<\nu_\ell(m_K)$. We write $k=\ell^{\nu_\ell(k)}k_\ell$ with $(\ell,k_\ell)=1$, and let $t=\min\{\nu_\ell(m_K),e+2\nu_\ell(k)\}$. Then $t>2\nu_\ell(k)$ and $4g^2\equiv r^2-ak^2 \pmod{\ell^t}$ if and only if $ak_\ell^2\equiv r^2-4g^2/\ell^{2\nu_\ell(k)} \pmod{\ell^{t-2\nu_\ell(k)}}$. Combining this information with Lemma 19, we have that

$$\#C_g^{(\ell)}(r,a,\ell^e,k)=\begin{cases}\ell^t & \text{if } \ell^{2\nu_\ell(k)}\mid r^2-4g^2 \text{and } ak_\ell^2\equiv\frac{r^2-4g^2}{\ell^{2\nu_\ell(k)}} \pmod{\ell^{t-\nu_\ell(k)}},\\ 0 & \text{otherwise.}\end{cases}$$

In particular, we see that $c_k(\ell^e)=0$ if $r^2\not\equiv 4g^2 \pmod{\ell^{2\nu_\ell(k)}}$. Suppose that $r^2\equiv 4g^2$

(mod $\ell^{2\nu_\ell(k)}$). Since $(g, m_K) = 1$ and $\ell \mid m_K$, we have that

$$\begin{aligned}
c_k(\ell^e) &= \sum_{\substack{a\in\mathbb{Z}/\ell^e\mathbb{Z}\\(r^2-ak^2,\ell)=1}} \left(\frac{a}{\ell}\right)^e \#C_g^{(\ell)}(r, a, \ell^e, k)\\
&= \sum_{\substack{a\in\mathbb{Z}/\ell^e\mathbb{Z}\\ ak^2\not\equiv r^2 \pmod{\ell}\\ ak^2\equiv r^2-4g^2 \pmod{\ell^t}}} \left(\frac{a}{\ell}\right)^e \ell^t\\
&= \sum_{\substack{a\in\mathbb{Z}/\ell^e\mathbb{Z}\\ ak^2\equiv r^2-4g^2 \pmod{\ell^t}}} \left(\frac{a}{\ell}\right)^e \ell^t\\
&= \sum_{\substack{a\in\mathbb{Z}/\ell^e\mathbb{Z}\\ ak_\ell^2\equiv \frac{r^2-4g^2}{\ell^{2\nu_\ell(k)}} \pmod{\ell^{t-2\nu_\ell(k)}}}} \left(\frac{ak_\ell^2}{\ell}\right)^e \ell^t\\
&= \ell^t \sum_{\substack{a\in\mathbb{Z}/\ell^e\mathbb{Z}\\ a\equiv \frac{r^2-4g^2}{\ell^{2\nu_\ell(k)}} \pmod{\ell^{t-2\nu_\ell(k)}}}} \left(\frac{a}{\ell}\right)^e\\
&= \ell^t \ell^{e-t+2\nu_\ell(k)} \left(\frac{(r^2-4g^2)/\ell^{2\nu_\ell(k)}}{\ell}\right)^e.
\end{aligned}$$

Therefore, in the case that $\ell \mid m_K$ and $2\nu_\ell(k) < \nu_\ell(m_K)$, we have

$$\frac{c_k(\ell^e)}{\ell^{e-1}} = \#C_g^{(\ell)}(r, 1, 1, k)\left(\frac{(r^2-4g^2)/\ell^{2\nu_\ell(k)}}{\ell}\right)^e \ell$$

since

$$\#C_g^{(\ell)}(r, 1, 1, k) = \begin{cases} \ell^{2\nu_\ell(k)} & \text{if } r^2 \equiv 4g^2 \pmod{\ell^{2\nu_\ell(k)}},\\ 0 & \text{otherwise.}\end{cases}$$

Acknowledgement. We would like to thank the anonymous referee for many helpful suggestions and a very careful reading of the manuscript. The second author would also like to thank David Grant, Hershy Kisilevsky, and Dimitris Koukoulopoulos for helpful discussions during the preparation of this paper.

REFERENCES

[**1**] S. BAIER. The Lang–Trotter conjecture on average. *J. Ramanujan Math. Soc.* **22**(4) (2007), 299–314.

[**2**] J. BATTISTA, J. BAYLESS, D. IVANOV and K. JAMES. Average Frobenius distributions for elliptic curves with nontrivial rational torsion. *Acta Arith.* **119**(1) (2005), 81–91.

[**3**] D. A. BURGESS. On character sums and L-series. II. *Proc. London Math. Soc.* (3) **13** (1963), 524–536.

[**4**] N. CALKIN, B. FAULKNER, K. JAMES, M. KING and D. PENNISTON. Average Frobenius distributions for elliptic curves over abelian extensions. *Acta Arith.* **149**(3) (2011), 215–244.

[**5**] C. DAVID and F. PAPPALARDI. Average Frobenius distributions of elliptic curves. *Internat. Math. Res. Notices* **1999**(4) (1999), 165–183.

[**6**] C. DAVID and F. PAPPALARDI. Average Frobenius distribution for inerts in $\mathbb{Q}(i)$. *J. Ramanujan Math. Soc.* **19**(3) (2004), 181–201.

[**7**] M. DEURING. Die Typen der Multiplikatorenringe elliptischer Funktionenkörper. *Abh. Math. Sem. Hansischen Univ.* **14** (1941), 197–272.

[**8**] D. S. DUMMIT and R. M. FOOTE. *Abstract Algebra* (John Wiley & Sons Inc., Hoboken, NJ, third edition, 2004).

[**9**] E. FOUVRY and M. R. MURTY. On the distribution of supersingular primes. *Canad. J. Math.* **48**(1) (1996), 81–104.

[**10**] H. IWANIEC and E. KOWALSKI. *Analytic Number Theory* American Mathematical Society Colloquium Publications, vol. 53. (American Mathematical Society, Providence, RI, 2004).

[**11**] K. JAMES. Average Frobenius distributions for elliptic curves with 3-torsion. *J. Number Theory* **109**(2) (2004), 278–298.

[**12**] K. JAMES and E. SMITH. Average Frobenius distribution for elliptic curves defined over finite Galois extensions of the rationals. *Math. Proc. Camb. Phil. Soc.* **150**(3) (2011), 439–458.

[**13**] S. LANG. *Algebraic Number Theory*. Graduate Texts in Mathematics, vol. 110. (Springer-Verlag, New York, 1994), second edition.

[**14**] S. LANG and H. TROTTER. *Frobenius Distributions in* GL_2*-extensions*. Lecture Notes in Mathematics, vol. 504. (Springer-Verlag, Berlin, 1976). Distribution of Frobenius automorphisms in GL_2-extensions of the rational numbers.

[**15**] H.W. LENSTRA, JR. Factoring integers with elliptic curves. *Ann. of Math. (2)* **126**(3) (1987), 649–673.

[**16**] M. RAM MURTY. *Problems in Analytic Number Theory*. Graduate Texts in Mathematics, vol. 206. (Springer-Verlag, New York, 2001). Readings in Mathematics.

[**17**] R. SCHOOF. Nonsingular plane cubic curves over finite fields. *J. Combin. Theory Ser. A* **46**(2) (1987), 183–211.

[**18**] J. H. SILVERMAN. *The Arithmetic of Elliptic Curves.* Graduate Texts in Mathematics, vol. 106. (Springer-Verlag, New York, 1992), Corrected reprint of the 1986 original.

[**19**] E. SMITH. A variant of the Barban–Davenport–Halberstam theorem. *Int. J. Number Theory* **7**(8) (2011), 2203–2218.

[**20**] L. C. WASHINGTON. *Introduction to Cyclotomic Fields*. Graduate Texts in Mathematics, vol. 83. (Springer-Verlag, New York, 1997), second edition.