On the Selmer Groups of Elliptic Curves in Quadratic Twist Families

by

SIMAN YAT-FAI WONG

B. Sc., University of British Columbia, 1990

Submitted to the Department of Mathematics
in partial fulfillment of the requirements
for the degree of

Doctor of Philosophy in Mathematics

at the
Massachusetts Institute of Technology
May 1995

Signature of Author ______________________________
Department of Mathematics
May 12, 1995

Certified by ______________________________
Barry Mazur, Professor of Mathematics

Certified by ______________________________
Michael Artin, Professor of Mathematics

Accepted by ______________________________
David Vogan
Chairman, Graduate Committee

On the Selmer Groups of Elliptic Curves in Quadratic Twist Families

BY

SIMAN YAT-FAI WONG

Submitted to the Department of Mathematics on May 12, 1995
in partial fulfillment of the requirements for the
degree of Doctor of Philosophy in Mathematics

Abstract

Let K be a number field with odd class number in which the ideal (2) splits completely. Let $E : y^2 = x(x - A)(x - B)$ be an elliptic curve over K. For any quadratic extension L/K, let $\mathrm{Sel}_2'(E_L)$ denotes the set of homogeneous spaces of the quadratic twist of E by L that are trivial in every $\mathfrak{p}$-adic completion of K, for all finite odd primes $\mathfrak{p}$ of K. Assuming the Burgess estimate for character sums over number fields and mild divisibility conditions on A, B and $A - B$, we derive an asymptotic formula for the size of Sel_2' for the quadratic twist family of E over K. The main term of the asymptotic formula grows linearly with respect to the number of extensions L/K, and therefore the asymptotic constant can be interpreted to be the average Sel_2'-rank of the twist family of E. Examining the structure of the asymptotic constant, we see that this average rank grows exponentially with respect to the degree of K; moreover, it decreases (not to zero) as the number of prime divisors of $AB(A - B)$ increases.

Thesis Supervisor: Dr. Barry Mazur
Title: Professor of Mathematics

Acknowledgements

Having arrived at MIT ignorant and inexperienced, I would never have been able to finish my studies without the help and support from everybody around here. A full citation being impossible, I should at least mention

Professor Barry Mazur, who has gone beyond his duty to supervise my thesis. He patiently answers my questions, tells me to have fun, shows me how to prove Sylow's theorems, and explains to me what congruence ideals have to do with congruences. I am forever indebted to him for his guidance, tolerance and encouragement;

Professor Michael Artin, for his useful comments on my writing and for his answers to my sporadic questions; Professor Haynes Miller, for his candid advice and for administering my oral exam; Professor Glenn Stevens and the BU algebra seminar group, for the many interesting talks and dinners;

the Nature Sciences and Engineering Research Council of Canada, for its crucial finanical support;

my family, for their unconditional support and constant reminders that I have been at school for too long;

Professor Lawrence G. Roberts, for his help and support and for putting up with me for over a decade; and Chris Elliots, for all the free postage and for telling me 'to work with Mazur or else become a hell of a good lawyer';

Farshid Hajir, for teaching me the fine art of root discriminant and for explaining to me why the Enterprise does not have seatbelts, among other things; Paul Gunnells, for all the lattices, icosahedrons and Mafia stories;

C. Kenneth Fan, for all the stimulating conversations, on mathematics and other topics; Timothy Chow, for his quick and precise answers, always non-TEXnical, to my questions before I ask them; and Bruce Fischer, for all of his advice, always useful and never corny;

the MIT Anime Club, for renewing my old love and for making MIT more bearable; and the Friday-night-Anime-gang: Betty Pun, Dan Klain and Glenn Tesler, for keeping me company and for making sure that I finished my meals on time.

Kyosuke: *97, 98, 99, 100.*
Madoka: *You miscounted it again.*
Kyosuke: *It's a 99 that's infinitely close to 100!*
...

'Summer'. No matter how many years go by, we probably won't forget this 'season'.
April. Under the sunlight that would make one doze off, we first met. June. In the brilliant light and wind. August. Over the hot seashore, we ran across.
That wasn't just a passing 'season', it was the 'everlasting summer' that we went through.
The 80's that went like a dream, I won't forget this happiness.

Matsumoto Isumi,
Kimagura Orange Road.

I ... I finally can do a decent job as a nursery staff. There were lots of hardships, but ever since I was a student, in sad occasions and happy occasions, all of you, who gathered here, supported me by scolding me, or by cheering me up. I'm still an unreliable man and may cause trouble for all of you, but, from now on, I'll do my best ...

Takahashi Rumiko,
Maison Ikkoku.

1. Introduction

The notion of the rank of an elliptic curve is already implicit in the work of Poincaré (1901) and is rigorously established by Mordell (1921). However, despite decades of active research, many basic questions remain open. First of all, there is still no deterministic algorithm for computing the rank of a general elliptic curve; the classical descent process rests on the finiteness of the Tate-Shafarevich group (or rather pieces of it), and until the last few years not a single example of this latter group has been computed. Next, curves over a fixed field with large rank are difficult to construct, the current record over $\mathbb{Q}$ being 21 [10]. Last but not least, almost nothing is known about the qualitative aspect of the rank function; for example, are there curves with arbitrarily large rank, and how does the rank function of a given curve behave as we enlarge the number field?

Number theorists often try to 'smooth out' a function by studying its average behavior in a family. For elliptic curves a natural family arises when we take quadratic twists. The first result in this direction is due to Goldfeld:

Theorem A (Goldfeld [6]) *Let E be a modular elliptic curve over $\mathbb{Q}$. Let $\mathcal{D}(T)$ be the set of integers $|D| \leq T$ which are discriminants of quadratic extensions of $\mathbb{Q}$, and denote by E_D the quadratic twist of E by $\mathbb{Q}(\sqrt{D})$. Assume that the Riemann hypothesis holds for the L-function of all E_D. Then for any $\epsilon > 0$ there exists a number $T(E, \epsilon)$ such that, for $T > T(E, \epsilon)$, the average analytic rank satisfies the bound*

$$\frac{1}{\#\mathcal{D}(T)} \sum_{D \in \mathcal{D}(T)} rank_{an}(E_D) \leq 3.25 + \epsilon.$$

Brumer [1] has recently studied the average rank over *all* elliptic curves over $\mathbb{Q}$. First, note that any elliptic curve over $\mathbb{Q}$ has a unique model of the form $E_{r,s} : y^2 = x^3 + rx + s$ with $r, s \in \mathbb{Z}$, such that for any prime p, if p^4 divides r then p^6 does not divide s. Let $\mathcal{C}(T)$ be the set of elliptic curves $E_{r,s}$ with $|r| \leq T^{1/3}$ and $|s| \leq T^{1/2}$. Then

Theorem B (Brumer [1]) *Assume that all elliptic curves over $\mathbb{Q}$ are modular, and that their L-functions satisfy the Riemann hypothesis. Then as T goes to infinity, the average analytic rank satisfies the bound*

$$\frac{1}{\#\mathcal{C}(T)} \sum_{E \in \mathcal{C}(T)} rank_{an}(E) \leq 2.3 + o_E(1).$$

These results give asymptotic upper bounds for the average rank. With regard to average lower bound, we have the following result:

Theorem C (Gouvêa-Mazur [7]) *Let E be a modular elliptic curve over $\mathbb{Q}$. Then for any $\epsilon > 0$ there exists a constant $C(E, \epsilon) > 0$ so that as D runs through all* *square-free integers which are prime to twice the conductor of* $E/\mathbb{Q}$.

$$\#\{D \in \mathbb{Z} : |D| < X,\ \mathit{rank}_{an}(E_D) \geq 2 \text{ and is even }\} > C(E,\epsilon)X^{1/2-\epsilon}.$$

Stewart-Top [13] have given a different proof of this result, for the actual Mordell-Weil rank of instead of the analytic rank, but a smaller exponent 1/6. Using the connection between quadratic twists of modular elliptic curves and half-integral weight modular forms, Frey-Happle [5] have conducted computer search for twists of six modular curves with even rank at least two; their data is not incompatible with the possibility that the exponent in the Gouvêa-Mazur theorem could be as large as $1-\epsilon$ for any $\epsilon > 0$.

Descent theory shows that the 'weak Mordell-Weil group' $E(K)/2E(K)$ injects into the 2-Selmer group of $E(K)$. Thus the 2-Selmer rank, which can be explicitly determined via local calculation, furnishes an effective upper bound of the Mordell-Weil rank. For the twist family $y^2 = x^3 - Dx$ related to the congruent number problem , Heath-Brown has recently obtained an asymptotic formula for the average of the moments of 2-Selmer rank:

Theorem D (Heath-Brown [3], [4]) *Let E_D be the elliptic curve over $\mathbb{Q}$ defined by $y^2 = x^3 - Dx$, and let $s(D)$ by its 2-Selmer rank modulo 2-torsion. Then for any integer $k > 0$,*

$$\sum_{\substack{0<D<X \\ D \text{ odd, sq-free}}} 2^{ks(D)} = \frac{X}{2\zeta(2)} \prod_{j=1}^{k}(1+2^j) + o_k(1).$$

The number of terms of the sum is $3X/8\zeta(2) + \mathcal{O}(\sqrt{X})$ and each summand is at least one, so the sum is bounded from below by $3X/8\zeta(2)$. But the right hand side is also on the order of X, so the asymptotic formula suggests that most of the twists of E have small rank; in fact we have the following

Corollary (Heath-Brown[4])

$$\frac{\#\{0 < D < X : D \text{ odd, square-free}; s(D) > r\}}{\#\{0 < D < X : D \text{ odd, square-free}\}} \leq 1.7313 \times 2^{(r-r^2)/2} + o_r(1).$$

In this paper we study Heath-Brown's asymptotic formula for the first moment of the 2-Selmer rank for a class of elliptic curves over number fields. Let K be a number field. For any ideal $\mathcal{I}$ of the ring of integers $\mathcal{O}_K$ of K, denote by $\omega_0(\mathcal{I})$ the number of prime ideals of $\mathcal{O}_K$ with odd residue characteristic ('the odd primes') which divide $\mathcal{I}$. Let U_K be the unit group of $\mathcal{O}_K$, and let u be the order of U_K/U_K^2. Then we have the following

Theorem. *Let A, B be nonzero integers in $\mathcal{O}_K$ with $A \neq B$. Denote by E the elliptic curve $y^2 = x(x-A)(x-B)$. For any quadratic extension L/K, denote by E_L the quadratic twist of E by L/K. Suppose*

(1) *K has odd class number, and the Dedekind zeta function of K has no Siegel zeros;*
(2) *the ideal (2) splits completely in K, and K contains a unit of every signature;*
(3) *A is not divisible by any odd primes, and B is odd;*
(4) *the ideal $(A-B)$ is not a square;*
(5) *A, B (resp. $-A, -B$) are not both square in $\mathcal{O}_K$;*
(6) *the Burgess estimate is true for K (cf. the discussion below).*

Denote by $Sel_2'(E_D)$ the subgroup of $H^1(G_K, E_D[2])$ whose elements when restricted to $H^1(G_{K_\mathfrak{p}}, E_D[2])$ are trivial for all odd prime $\mathfrak{p}$ of K. As we run through quadratic extensions L/K whose discriminant $D_{L/K}$ are prime to $2AB(A-B)$, we have the asymptotic formula

$$\sum_{\substack{L/K \\ \mathbb{N}(D_{L/K}) \leq X}} \#Sel_2'(E_L) = B_{E,K} C_{E,K} X + O\left(\frac{X(\log\log X)^8}{(\log X)^{1/4}}\right),$$

where

$$\begin{aligned} C_{E,K} &= \frac{u}{\zeta_K(2)} \prod_{\mathfrak{p} | 2AB(A-B)} \left(1 - \frac{1}{\mathbb{N}(\mathfrak{p})^2}\right), \\ B_{E,K} &= \frac{u^2 2^{[K:\mathbb{Q}]}}{4} + \frac{1}{2^{\omega_0(A-B)+\omega(B)+2}} \left(1 + \sum_{\epsilon_2,\epsilon_3}{}' \langle \epsilon_2, \epsilon_3 \rangle \sum_{\beta} \left(\frac{AB}{\underline{\beta}}\right) \frac{\mathbb{P}_\beta}{2^{[K:\mathbb{Q}]}} \right. \\ &\quad \left. + \Psi(A) \sum_{\epsilon_1,\epsilon_2,\epsilon_3}{}'' \langle \epsilon_1, \epsilon_2 \rangle \langle \epsilon_1, \epsilon_3 \rangle \langle \epsilon_2, \epsilon_3 \rangle \sum_{\beta,\beta_5} \frac{\mathbb{R}_{\beta,\beta_5}}{2^{[K:\mathbb{Q}]}} \langle \beta, \beta_5 \rangle \left(\frac{A}{\underline{\beta\beta_5}}\right) \left(\frac{-1}{\underline{\beta_5}}\right)\right), \end{aligned}$$

and $\Psi(A)$ is 1 if $A \in \mathcal{O}_K$ is a unit, and is zero otherwise ($\underline{\beta}$ and $\underline{\beta}_5$ run through all odd ideals dividing $A-B$ and B, respectively (cf. §3); cf. §7 for the definition of $\mathbb{P}_\beta$, $\mathbb{R}_{\beta,\beta_5}$, $\sum'$ and $\sum''$).

The number of terms of the sum is of the order of $C_{E,K}X$, so this asymptotic formula shows that $B_{E,K}$ is the average size of Sel_2' of the quadratic twist family of E over K. Moreover, as we enlarge K so that the hypotheses of the theorem are satisfied, we get a bound on the growth of the average rank of the twist family. Lastly, notice that as the number of odd prime divisors of $(A-B)$ and (B) increase, the average rank $B_{E,K}$ actually *decreases.* This is rather surprising, since the more divisors $(A-B)$ and (B) have the more descent equations are available (cf. §3), and hence allows the rank to possibly get bigger. One could argue based on the structure of $B_{E,K}$ that the descent equations are all independent, each with probability 1/2 of being solvable. It would be of great interest to find a more satisfactory explanation.

The hypotheses (2) to (5) in the statement of the theorem are made to simplify the calculation of the asymptotic constant; they can be removed using with more tedious computation. The odd class number hypothesis is more essential; more precisely, denote by r the 2-rank of the class group of K: then, for general number fields K, we would have $r+1$ pairs of integral descent equations (cf. section 2). The Burgess estimate we need is as follows: let χ be an ideal character of K with conductor $\mathcal{N}$: then as $\mathcal{I}$ ranges over all ideals which are prime to $\mathcal{N}$, we want

$$\sum_{X<\mathbb{N}(\mathcal{I})\leq 2X} \chi(\mathcal{I}) \ll_{K,\epsilon} \mathbb{N}(\mathcal{N})^{1/2} X^{\frac{3}{16}+\epsilon}.$$

For $K = \mathbb{Q}$ this was first proved by Burgess [2], using Weil's estimate of character sums over finite fields (so do all subsequent proofs). A recent refinement of the proof (over $\mathbb{Q}$) by Montgomery [8] might lead to a proof for general number fields.

The organization of this paper is as follows. After we set up the notations in section 2, we rewrite in section 3 the standard complete 2-descent equations so that $\mathfrak{p}$-adic solutions at a finite, odd prime $\mathfrak{p}$, if exist, can be made $\mathfrak{p}$-adically integral. This allows us to express the $\mathfrak{p}$-adic solvability of these integral descent equations in terms of the quadratic residue of the coefficients of the equations. The sum of the size of Sel_2' over the quadratic twist family then becomes a sum of product of quadratic symbols (section 4). Following Heath-Brown, we apply in section 5 and 6 various analytic techniques (notably the Burgess estimate of character sums) to show that most of the summands contributes to the error term. To finish the proof of the theorem, we evaluate the remaining terms in section 7 to obtain the asymptotic constant.

2. Preliminary & Notations

Let K be a number field. Denote by $\mathcal{O}_K$ be ring of integers of K, and by U_K the unit group of $\mathcal{O}_K$. A finite place of K is said to be **odd** (resp. **even**) if its norm (to $\mathbb{Q}$) is odd (resp. even); the same term applies to elements of $\mathcal{O}_K$. Denote by $\mathbb{N}(\mathcal{I})$ the norm of the ideal $\mathcal{I}$.

For any finite place $\mathfrak{p}$ of K, denote by $K_\mathfrak{p}$ the completion of K at p, and by $\mathcal{O}_\mathfrak{p}$ the ring of integers in $K_\mathfrak{p}$.

Let S be a finite set of places of K, including all the infinite ones. Fix a real number $X > 0$. For any ideal $\mathcal{L}$ of $\mathcal{O}_K$, there exists an element $\lambda \in \mathcal{O}_K$ such that

$$\begin{aligned} \mathrm{ord}_v(\lambda) &= \mathrm{ord}_v(\mathcal{L}) && v \in S \text{ and finite} \\ &= 0 && v \notin S \text{ and } \mathbb{N}(v) < X. \end{aligned}$$

Such a (non-unique) element λ is called a (X,S)**-generator** of $\mathcal{L}$.

Since the class number of K is finite and since the unit group of $\mathcal{O}_K$ is finitely generated,

$$K(S) := \{x \in K^*/K^{*2} : \mathrm{ord}_v(x) \text{ is even for all } v \notin S\}$$

is a *finite* Abelian group of exponent 2. For any element $\beta \in K(S)$, denote by the $\underline{b}$ the ideal generated by the square-free part of the principal ideal (b); in particular, $\underline{b}$ is supported on S.

Now, assume that the class number of K is odd. Then for any two elements b_1, b_2 in $K(S)$ there exists a (X,S)-generator of $\gcd(b_1,b_2)$. Moreover, the choice of β in $K(S)$ is unique up to a multiple of units. If b_1, b_2 are coprime, we stipulate that $\beta = 1$. We call β an (X,S)**-integer representative** of $\gcd(b_1,b_2)$.

The following elementary fact will be used subsequently without further comment.

Lemma 1. *Let $\mathcal{A} \subset \mathcal{O}_K$ be a proper ideal, and let $\chi : (\mathcal{O}_K/\mathcal{A})^* \to \mathbb{C}$ be a quadratic character. Suppose the class number of K is odd. If $\chi|_{U_K}$ is trivial, then χ induces an ideal class character modulo $\mathcal{A}$.* □

3. Integral descent

Let $A, B \in \mathcal{O}_K$ be nonzero so that A, B and $A - B$ are pairwise coprime, B is odd, and A is not divisible by any odd primes. Denote by E the elliptic curve

$$E : y^2 = x(x - A)(x - B).$$

For any nonzero $D \in \mathcal{O}_K$ which is prime to $AB(A - B)$, denote by E_D the quadratic twist of E by $K(\sqrt{D})$:

$$E_D : y^2 = x(x - AD)(x - BD).$$

Let S_D be the set consisting of all the infinite places of K together with the finite places which divide $2AB(A - B)$ or the square-free part of the ideal (D).

Since the class number of K need not be 1, we cannot parameterize the quadratic twists of E by varying D over all the square-free integers. Instead we vary over all the square-free *ideals* of $\mathcal{O}_K$, each of which corresponds to $\#(U_K/U_K^2)$ quadratic extensions of K.

Standard complete two-descent [12] asserts that the elements of the 2-Selmer group of $E_D(K)$ are in bijective correspondence with pairs $(b_1, b_2) \in K(S_D) \times K(S_D)$ for which the following equations are locally solvable at all places of $\mathcal{O}_K$:

$$b_1 z_1^2 - b_2 z_2^2 = AD \qquad (1)$$

$$b_1 z_1^2 - b_1 b_2 z_3^2 = BD. \qquad (2)$$

We would like to express the solvability in $K_\mathfrak{p}$ of these equations via the quadratic residue of the b_i modulo $\mathfrak{p}$. To do that, we need to transform the descent equations so that if there is a non-trivial solution in $K_\mathfrak{p}$, there would be one in $\mathcal{O}_\mathfrak{p}$. As a first step, we need to bound the $\mathfrak{p}$-adic valuation of the 'denominators' of a local solution.

Lemma 2. *Let $\mathfrak{p} \in S_D$ be a finite place. Suppose $(z_1, z_2, z_3) \in K_\mathfrak{p}^* \times K_\mathfrak{p}^* \times K_\mathfrak{p}$ is a non-trivial solution to the descent equations. Then*

$$\mathrm{ord}_\mathfrak{p}(z_2), \mathrm{ord}_\mathfrak{p}(z_3) \geq \min(\mathrm{ord}_\mathfrak{p}(z_1), 0).$$

Proof. From (1) we see that

$$\mathrm{ord}_\mathfrak{p}(b_1) + 2\mathrm{ord}_\mathfrak{p}(z_2) \geq \min(\mathrm{ord}(b_1) + 2\mathrm{ord}_\mathfrak{p}(z_1), \mathrm{ord}_\mathfrak{p}(AD)).$$

Since $1 \geq \mathrm{ord}_\mathfrak{p}(b_1), \mathrm{ord}_\mathfrak{p}(b_2) \geq 0$ and $\mathrm{ord}_\mathfrak{p}(AD) \geq 0$, it follows that

$$\mathrm{ord}_\mathfrak{p}(z_2) \geq \min(\mathrm{ord}_\mathfrak{p}(z_1), 0). \qquad (3)$$

If $\mathrm{ord}_{\mathfrak{p}}(b_1 b_2) \leq 1$, then apply the same argument to (2) will give the other half of the lemma. Now, suppose $\mathrm{ord}_{\mathfrak{p}}(b_1) = \mathrm{ord}_{\mathfrak{p}}(b_2) = 1$. From (2) we get

$$(4) \qquad 2 + 2\mathrm{ord}_{\mathfrak{p}}(z_3) \geq \min(\mathrm{ord}_{\mathfrak{p}}(z_1), \mathrm{ord}_{\mathfrak{p}}(BD)).$$

The left side is even, whence $\mathrm{ord}_{\mathfrak{p}}(z_1) \geq 0$, and hence from (3), we get $\mathrm{ord}_{\mathfrak{p}}(z_2) \geq 0$.

Subtract (2) from (1), we get

$$0 \leq \mathrm{ord}_{\mathfrak{p}}(A - B) + \mathrm{ord}_{\mathfrak{p}}(D) = 1 + \mathrm{ord}_{\mathfrak{p}}(b_1 z_3^2 - z_2^2).$$

If $\mathrm{ord}_{\mathfrak{p}}(z_3) < 0$, then the right side is zero, whence $\mathrm{ord}_{\mathfrak{p}}(A - B) = \mathrm{ord}_{\mathfrak{p}}(D) = 0$ and $\mathrm{ord}_{\mathfrak{p}}(z_3) = -1$. Since $B, A-B, D$ are pairwise coprime, this implies that $\mathrm{ord}_{\mathfrak{p}}(B) > 0$, whence by (4), we get $2 + 2(-1) \geq \min(1, 1)$, a contradiction. Thus $\mathrm{ord}_{\mathfrak{p}}(z_3) \geq 0$, as desired. □

Corollary 1. *The descent equations (1), (2) have a non-trivial solution in $K_{\mathfrak{p}}$ for a finite place $\mathfrak{p}$ if and only if the following equations have a non-trivial solution in $\mathcal{O}_{\mathfrak{p}}$:*

$$(5) \qquad b_1 R^2 - ADS^2 = b_2 W^2$$

$$(6) \qquad b_1 R^2 - BDS^2 = b_1 b_2 Z^2. \quad \square$$

Lemma 3. *If B is odd, then we can choose $b_1 \in K(S_D)$ to be odd as well.*

Proof. Let τ be an even prime. Suppose $\mathrm{ord}_{\tau}(b_1) = \mathrm{ord}_{\tau}(b_2) = 1$. Since BD is odd, (6) implies that $\mathrm{ord}_{\tau}(S) > 0$, whence $\mathrm{ord}_{\tau}(R) > 0$. (5) then implies that $\mathrm{ord}_{\tau}(W) > 0$, and henceord$_{\tau}(S) > 1$. (6) then implies that $\mathrm{ord}_{\tau}(Z) > 0$. Then all four variables R, S, W, Z are divisible by τ, a contradiction, and so $\mathrm{ord}_{\tau}(b_1)$ and $\mathrm{ord}_{\tau}(b_2)$ cannot be both 1.

Now, suppose $\mathrm{ord}_{\tau}(b_1) = 1$. Since BD is odd, (6) implies that τ divides S. Since $\mathrm{ord}_{\tau}(b_2) = 0$ now, (5) implies that $\mathrm{ord}_{\tau}(W) > 0$, whence $\mathrm{ord}_{\tau}(R) > 0$; (6) then implies that $\mathrm{ord}_{\tau}(Z) > 0$, a contradiction. Thus $\mathrm{ord}_{\tau}(b_1) = 0$. □

Remarks. In fact, we've counted each Selmer element (mod 2-torsion) *four times.*

Now that we are reduced to looking for $\mathcal{O}_{\mathfrak{p}}$-solutions, for an odd place $\mathfrak{p}$ it is natural to try to work modulo $\mathfrak{p}$ and then apply Hensel's lemma. However, the right side of (6) involves both b_1 and b_2, and hence when $\mathfrak{p}$ divides $\gcd(b_1, b_2)$ we might need to work with higher power of $\mathfrak{p}$. We now study the divisibility property of the b_i and the $\mathcal{O}_{\mathfrak{p}}$-solutions so that, at the end, the coefficients of our descent equations are all square-free for any $\mathfrak{p} \in S_D$.

Lemma 4. *(1) Let $R, S, W, Z \in \mathcal{O}_{\mathfrak{p}}$ be a non-trivial solution to (5), (6). Suppose $\mathrm{ord}_{\mathfrak{p}}(b_1 b_2) \leq 1$. If $\mathrm{ord}_{\mathfrak{p}}(D) > 0$, then $\mathrm{ord}_{\mathfrak{p}}(R) > 0$ if $\mathrm{ord}_{\mathfrak{p}}(b_2) = 1$, and $\mathrm{ord}_{\mathfrak{p}}(W) > 0$ if $\mathrm{ord}_{\mathfrak{p}}(b_1) = 1$.*

(2) Let $\mathfrak{p} \in S_D$ be a finite place; then

$$\begin{aligned} \mathrm{ord}_{\mathfrak{p}}(b_1) = 1, \mathrm{ord}_{\mathfrak{p}}(b_2) = 1 &\Rightarrow \mathrm{ord}_{\mathfrak{p}}(D) = 1; \\ \mathrm{ord}_{\mathfrak{p}}(b_1) = 1, \mathrm{ord}_{\mathfrak{p}}(b_2) = 0 &\Rightarrow \mathrm{ord}_{\mathfrak{p}}(BD) = 1; \\ \mathrm{ord}_{\mathfrak{p}}(b_1) = 0, \mathrm{ord}_{\mathfrak{p}}(b_2) = 1 &\Rightarrow \mathrm{ord}_{\mathfrak{p}}(D(A-B)) = 1. \end{aligned}$$

Proof. Part (1) is clear, and part (2) follows from the following statements:

(i) If $\mathrm{ord}_{\mathfrak{p}}(B) > 0$, then $\mathrm{ord}_{\mathfrak{p}}(b_2) = 0$.

(ii) If $\mathrm{ord}_{\mathfrak{p}}(b_1) > 0$, then $\mathrm{ord}_{\mathfrak{p}}(A-B) = 0$.

(i) First, suppose $\mathrm{ord}_{\mathfrak{p}}(b_1) > 0$. (5) gives $\mathrm{ord}_{\mathfrak{p}}(S) > 0$, whence by (6), $\mathrm{ord}_{\mathfrak{p}}(R) > 0$. Then both $\mathrm{ord}_{\mathfrak{p}}(Z), \mathrm{ord}_{\mathfrak{p}}(W) > 0$, by (6) and (5), respectively. This is impossible. Next, suppose $\mathrm{ord}_{\mathfrak{p}}(b_1) = 0$. (6) gives $\mathrm{ord}_{\mathfrak{p}}(R) > 0$, whence by (5), $\mathrm{ord}_{\mathfrak{p}}(S) > 0$; then again both $\mathrm{ord}_{\mathfrak{p}}(Z), \mathrm{ord}_{\mathfrak{p}}(W) > 0$, a contradiction.

(ii) Suppose $\mathrm{ord}_{\mathfrak{p}}(A-B) \neq 0$ (and hence 1); then $\mathrm{ord}_{\mathfrak{p}}(B) = \mathrm{ord}_{\mathfrak{p}}(D) = 0$, whence (6) implies that $\mathrm{ord}_{\mathfrak{p}}(S) > 0$, which in turns implies $\mathrm{ord}_{\mathfrak{p}}(R) > 0$. (5) then implies $\mathrm{ord}_{\mathfrak{p}}(W) > 0$. This forces $\mathrm{ord}_{\mathfrak{p}}(Z) = 0$. Subtract (5) from (6), we get

$$\begin{aligned} 3 &\leq \mathrm{ord}_{\mathfrak{p}}((A-B)DS^2) \\ &= \mathrm{ord}_{\mathfrak{p}}(b_2) + \mathrm{ord}_{\mathfrak{p}}(b_1 Z^2 - W^2) \leq 2, \end{aligned}$$

a contradiction. □

Fix a real number $X > 0$. In view of part (2) of the lemma, we can express b_1, b_2 as elements of $K(S_D)$ as follow:

$$b_1 = \beta_1\beta_4\beta_5, \;\; b_2 = \tau\beta\beta_2\beta_4,$$

where τ is an (X, S_D)-integer generator of a square-free product of even primes, and the β's are (X, S_D)-integer generators of the following ideals:

$$\begin{aligned} \beta_4 &= \gcd(b_1, b_2), & \beta_2 &= \gcd(D, b_2/\beta_4), \\ \beta_1 &= \gcd(D, b_1/\beta_4), & \beta_3 &= (D/\beta_4); \\ \beta_5 &= \gcd(B, b_1/\beta_4), & \beta &= \gcd(A-B, b_2/\beta_4), \end{aligned}$$

and the β's satisfy the following relations (in $K(S_D)$)

$$\begin{aligned} &D = \beta_1\beta_2\beta_3\beta_4, \\ &\beta | A - B; \;\; \beta \text{ odd}; \\ &\beta_5 | B; \;\; \beta_5 \text{ odd}. \end{aligned}$$

In view of part (1) of the lemma, our $\mathcal{O}_{\mathfrak{p}}$-descent equations now take the final form

$$\beta_2\beta_5 R^2 - \beta_3 A S^2 = \tau\beta\beta_1 W^2 \tag{7}$$

$$\beta_2\beta_5 R^2 - \beta_3 B S^2 = \tau\beta\beta_4\beta_5 Z^2. \tag{8}$$

4. Local Solvability

We now devise criteria for the local solvability of the system obtained at the end of the previous section. By general theory, the system is solvable at all places p which do not divide $2AB(A-B)\underline{D}$ (recall that for an element $D \in K(S_D)$, $\underline{D}$ denotes square-free part of the ideal (D) supported at S_D). By our choice of A, B and D, we see that $\mathfrak{p}|2AB(A-B)\underline{D}$ precisely when $\mathfrak{p}|2$ or if $\mathfrak{p}$ divides exactly one of A, B, $\underline{D}$ or $A-B$. From now on $\mathfrak{p}$ denotes an finite odd place which divides $AB(A-B)\underline{D}$.

The following sufficient and necessary solvability criteria for (7), (8) are clear:

$$\begin{aligned}
\left(\frac{\tau\beta\beta_1\beta_2\beta_5}{\mathfrak{p}}\right) &= \left(\frac{\tau\beta\beta_2\beta_4}{\mathfrak{p}}\right) = 1 && \text{if } \mathfrak{p}|\underline{\beta}_3, \\
\left(-\frac{\tau\beta\beta_1\beta_3A}{\mathfrak{p}}\right) &= \left(-\frac{\tau\beta\beta_3\beta_4\beta_5B}{\mathfrak{p}}\right) = 1 && \text{if } \mathfrak{p}|\underline{\beta}_2, \\
\left(\frac{\beta_2\beta_3\beta_5A}{\mathfrak{p}}\right) &= \left(\frac{\beta_2\beta_3\beta_5B}{\mathfrak{p}}\right) = 1 && \text{if } \mathfrak{p}|\underline{\beta}.
\end{aligned}$$

(note that $A-B=\beta m$ in $K(S_D)$, so the two conditions for $\mathfrak{p}|\underline{\beta}$ are equivalent). If $\mathfrak{p}|\underline{\beta}_1$, then first we need

$$\left(\frac{\beta_2\beta_3\beta_5A}{\mathfrak{p}}\right) = 1.$$

This implies that $\tau\beta\beta_4\beta_5Z^2 = \beta_2\beta_5R^2 - \beta_3BS^2 \equiv \beta_3S^2(A-B) \pmod{\mathfrak{p}}$, thus we need

$$\left(\frac{\beta_2\beta_3\beta_5A}{\mathfrak{p}}\right) = \left(\frac{\tau\beta\beta_3\beta_4\beta_5(A-B)}{\mathfrak{p}}\right) = 1.$$

If $\mathfrak{p}|\underline{\beta}_4$, then similarly we have

$$\left(\frac{\beta_2\beta_3\beta_5B}{\mathfrak{p}}\right) = \left(-\frac{\tau\beta\beta_1\beta_3(A-B)}{\mathfrak{p}}\right) = 1.$$

Finally, suppose $\mathfrak{p}|\underline{\beta}_5$. Rewrite (8) as

$$R^2 = \frac{\beta_3B}{\beta_2\beta_5}S^2 + \frac{\beta\beta_4}{\beta_2}Z^2, \tag{9}$$

we see that its solvability in $K_{\mathfrak{p}}$ is expressed by the Hilbert symbol

$$\left(\frac{\frac{\beta_3B}{\beta_2\beta_5}, \frac{\beta\beta_4}{\beta_2}}{\mathfrak{p}}\right).$$

Since $\mathfrak{p}|\beta_5$ and $\underline{\beta}_5 = \gcd(B, b_1/\beta_4)$, the coefficients of (9) are all in $\mathcal{O}_{\mathfrak{p}}^*$, whence the Hilbert symbol is trivial. Thus the only requirement for $\mathfrak{p}|\underline{\beta}_5$ is

$$\left(-\frac{\tau\beta\beta_1\beta_3A}{\mathfrak{p}}\right) = 1.$$

Following Heath-Brown, we set

$$\begin{aligned}
\Pi_3 &= \prod_{\mathfrak{p}|\underline{\beta_3}} \left(1+\left(\frac{\tau\beta\beta_1\beta_2\beta_5}{\mathfrak{p}}\right)+\left(\frac{\tau\beta\beta_2\beta_4}{\mathfrak{p}}\right)+\left(\frac{\beta_1\beta_4\beta_5}{\mathfrak{p}}\right)\right)\\
\Pi_2 &= \prod_{\mathfrak{p}|\underline{\beta_2}} \left(1+\left(-\frac{\tau\beta\beta_1\beta_3 A}{\mathfrak{p}}\right)+\left(-\frac{\tau\beta\beta_3\beta_4\beta_5 B}{\mathfrak{p}}\right)+\left(\frac{\beta_1\beta_4\beta_5 AB}{\mathfrak{p}}\right)\right)\\
\Pi_1 &= \prod_{\mathfrak{p}|\underline{\beta_1}} \left(1+\left(\frac{\tau\beta\beta_3\beta_4\beta_5(A-B)}{\mathfrak{p}}\right)+\left(\frac{\tau\beta\beta_2\beta_4(A-B)A}{\mathfrak{p}}\right)+\left(\frac{\beta_2\beta_3\beta_5 A}{\mathfrak{p}}\right)\right)\\
\Pi_4 &= \prod_{\mathfrak{p}|\underline{\beta_4}} \left(1+\left(-\frac{\tau\beta\beta_1\beta_3(A-B)}{\mathfrak{p}}\right)+\left(-\frac{\tau\beta\beta_1\beta_2\beta_5(A-B)B}{\mathfrak{p}}\right)+\left(\frac{\beta_2\beta_3\beta_5 B}{\mathfrak{p}}\right)\right)\\
\Pi_0 &= \prod_{\mathfrak{p}|\underline{\beta}} \left(1+\left(\frac{\beta_2\beta_3\beta_5 A}{\mathfrak{p}}\right)\right)\\
\Pi_5 &= \prod_{\mathfrak{p}|\underline{\beta_5}} \left(1+\left(-\frac{\tau\beta\beta_1\beta_3 A}{\mathfrak{p}}\right)\right)
\end{aligned}$$

For $\alpha \in \mathcal{O}_K$, let $\omega(\alpha)$ be the number of distinct $\mathcal{O}_K$-prime ideals that divide $\underline{\alpha}$. Then

$$4^{-\omega(D)}2^{-\omega_0(A-B)}2^{-\omega_0(B)}\Pi_0\Pi_1\Pi_2\Pi_3\Pi_4\Pi_5 = \begin{cases} 1 & \text{if (7), (8) are locally solvable at all finite, odd places} \\ 0 & \text{otherwise.}\end{cases}$$

Expand $\prod_3$ into a sum, we get

$$\Pi_3 = \sum \left(\frac{\tau\beta\beta_1\beta_2\beta_5}{\mathfrak{d}_{34}}\right)\left(\frac{\tau\beta\beta_2\beta_4}{\mathfrak{d}_{31}}\right)\left(\frac{\beta_1\beta_4\beta_5}{\mathfrak{d}_{32}}\right),$$

where the sum is taken over *ideal* factorizations

$$\underline{\beta_3} = \mathfrak{d}_{30}\mathfrak{d}_{31}\mathfrak{d}_{32}\mathfrak{d}_{34}.$$

Similarly, we have

$$\begin{aligned}
\Pi_2 &= \sum \left(-\frac{\tau\beta\beta_1\beta_3 A}{\mathfrak{d}_{24}}\right)\left(-\frac{\tau\beta\beta_3\beta_4\beta_5 B}{\mathfrak{d}_{21}}\right)\left(\frac{\beta_1\beta_4\beta_5 AB}{\mathfrak{d}_{23}}\right), && \underline{\beta_2} = \prod_{j\neq 2}\mathfrak{d}_{2j}.\\
\Pi_1 &= \sum \left(\frac{\tau\beta\beta_3\beta_4\beta_5(A-B)}{\mathfrak{d}_{12}}\right)\left(\frac{\tau\beta\beta_2\beta_4 A(A-B)}{\mathfrak{d}_{13}}\right)\left(\frac{\beta_2\beta_3\beta_5 A}{\mathfrak{d}_{14}}\right), && \underline{\beta_1} = \prod_{j\neq 1}\mathfrak{d}_{1j}.\\
\Pi_4 &= \sum \left(-\frac{\tau\beta\beta_1\beta_3(A-B)}{\mathfrak{d}_{42}}\right)\left(-\frac{\tau\beta\beta_1\beta_2\beta_5 B(A-B)}{\mathfrak{d}_{43}}\right)\left(\frac{\beta_2\beta_3\beta_5 B}{\mathfrak{d}_{41}}\right), && \underline{\beta_4} = \prod_{j\neq 4}\mathfrak{d}_{4j}.\\
\Pi_0 &= \sum \left(\frac{\beta_2\beta_3\beta_5 A}{\mathfrak{d}}\right), && \mathfrak{d}|\underline{\beta}.\\
\Pi_5 &= \sum \left(-\frac{\tau\beta\beta_1\beta_3 A}{\mathfrak{d}_5}\right), && \mathfrak{d}_5|\underline{\beta_5}.
\end{aligned}$$

Fix a real number $X > 0$. For each index ij, choose an (X, S_D)-generator β_{ij} of $\mathfrak{d}_{ij}$ so that

(10) $$\beta_i = \prod_{j \neq i} \beta_{ij}. \quad (\text{in } K(S_D))$$

Thus every pair of descent equations gives rise to an 19-tuple $(\beta_{ij}; \beta; \beta_5)$. We end this section with an expression for the average 2-Selmer rank in terms of a sum over these 19-tuples. It is this new expression that we shall estimate in subsequent sections.

In the argument above we need to choose an (X, S_D)-generator for various ideals. Such choices are unique up to multiplication by units, subject to the condition that the product of these generators represents a specific element in $K(S_D)$. But we need to avoid duplication: for example, if both β_1 and β_4 vary over the units in U_K/U_K^2 then $\beta_1\beta_2 \in K(S_D)$ would be repeated $u := \#(U_K/U_K^2)$ times. To facilitate subsequent discussion we introduce the following definitions:

Definition. *A **free variable** is one which takes on values in $\mathcal{O}_K/(U_K)^2$.*
*A **restricted variable** is one which takes on values in $\mathcal{O}_K/U_K$.*

The previous section establishes a 1-to-4 correspondence between $(2,\infty)$-Selmer elements (mod 2-torsion) and pairs $(b_1, b_2) \in K(S_D)$; moreover, those pairs corresponding to $(2,\infty)$-Selmer elements (mod 2-torsions) are shown to arise from factorizations (in $K(S_D)$) $D = \beta_1\beta_2\beta_3\beta_4$, $A - B = \beta m$ as follows:

(11) $$b_1 = \beta_1\beta_4\beta_5, \;\; b_2 = \tau\beta\beta_2\beta_4. \quad (\text{in } K(S_D))$$

We now reverse this process by reconstructing the 2-Selmer elements from the 19-tuples $(\beta_{ij}; \beta; \beta_5; \tau)$ for which the corresponding descent equations are locally solvable at all finite, odd places. First, fix a real number $X > 0$. Fix a set of square-free, (X, S_D)-elements

$$\{\beta \in \mathcal{O}_K/U_K : \underline{\beta}|\text{odd}(A-B)\}, \;\; \{\beta_5 \in \mathcal{O}_K/U_K : \underline{\beta_5}|\text{odd}(B)\}, \;\; \{\tau \in \mathcal{O}_K/U_K : \underline{\tau} \text{ very odd}\}.$$

Choose such elements τ, β and β_5. For each ideal factorization $\underline{D} = \prod \mathfrak{d}_{ij}$, fix an (X, S_D)-generator β_{ij} for each $\mathfrak{d}_{ij}$. Pick some i, j, k, let three variables $\beta_{1i}, \beta_{2j}, \beta_{3k}$ free, and let the remaining ones be restricted. Apply (11) and we will run through exactly once all the $(2,\infty)$-Selmer elements for E_D, where the odd part of $\text{Disc}(K(\sqrt{D})/K)$ has a fixed norm.

As $\mathbb{D}$ runs through 19-tuples $(\beta_{ij}; \beta; \beta_5; \tau)$ with the same $\mathbb{N}(\underline{D})$ ($\underline{D}$ odd), we have

$$\sum_{\mathbb{D}} \Pi_0 \cdots \Pi_5 = 4^{\omega(D)} 2^{\omega_0(A-B)} 2^{\omega_0(B)} \cdot 4 \sum_{\mathbb{N}(\underline{D}) \text{ fixed}} 2^{s(D)},$$

where $\omega_0(A-B)$ denotes the number of *odd* primes dividing $A - B$, $s(D)$ is the rank of 2-Selmer (mod 2-torsion), and the extra factor of 4 is due to the fact that each non-torsion 2-Selmer element corresponds to *four* pairs $(b_1, b_2) \in K(S_D)$. Finally, we arrive at the sought-after expression for the average 2-Selmer rank:

(12) $$\sum_{\mathbb{N}(\underline{D}) \leq X} \;\; = \;\; \sum_{\mathbb{D}} g(\mathbb{D}),$$

where the sum on the right is taken over the 21-tuples $(\beta_{ij}; \beta, \mathfrak{b}; \beta_5, \mathfrak{b}_5; \tau)$ as $\mathfrak{b}$ (resp. $\mathfrak{b}_5$) runs through all ideals that divide $\underline{\beta}$ (resp. $\underline{\beta}_5$), and with $\mathfrak{d}_{ij} := \underline{\beta}_{ij}$,

$$\begin{aligned} g(\mathbb{D}) \;=\; & \left(\frac{\beta}{\mathfrak{d}_{34}\mathfrak{d}_{31}\mathfrak{d}_{24}\mathfrak{d}_{21}\mathfrak{d}_{12}\mathfrak{d}_{13}\mathfrak{d}_{42}\mathfrak{d}_{43}}\right)\left(\frac{A}{\mathfrak{d}_{24}\mathfrak{d}_{23}\mathfrak{d}_{14}\mathfrak{d}_{13}}\right)\left(\frac{B}{\mathfrak{d}_{21}\mathfrak{d}_{23}\mathfrak{d}_{41}\mathfrak{d}_{43}}\right) \times \\ & \left(\frac{A-B}{\mathfrak{d}_{12}\mathfrak{d}_{13}\mathfrak{d}_{42}\mathfrak{d}_{43}}\right)\left(\frac{-1}{\mathfrak{d}_{24}\mathfrak{d}_{21}\mathfrak{d}_{42}\mathfrak{d}_{43}}\right)\left(\frac{\beta_2\beta_3\beta_5 A}{\mathfrak{b}}\right) \times \\ & \left(\frac{\beta_5}{\mathfrak{d}_{12}\mathfrak{d}_{14}\mathfrak{d}_{21}\mathfrak{d}_{23}\mathfrak{d}_{32}\mathfrak{d}_{34}\mathfrak{d}_{41}\mathfrak{d}_{43}}\right)\left(-\frac{\beta\beta_1\beta_3 A}{\mathfrak{b}_5}\right) \times \\ & \left(\frac{\tau}{\mathfrak{d}_{24}\mathfrak{d}_{21}\mathfrak{d}_{12}\mathfrak{d}_{13}\mathfrak{d}_{31}\mathfrak{d}_{34}\mathfrak{d}_{42}\mathfrak{d}_{43}\mathfrak{b}_5}\right) \times \\ & \frac{1}{2^{\omega_0(A-B)-\omega_0(B)-2}} \prod_i 4^{-\omega(\mathfrak{d}_{i0})} \prod_{j\neq 0} 4^{-\omega(\mathfrak{d}_{ij})} \prod_{k\neq i,j} \prod_l \left(\frac{\beta_{kl}}{\mathfrak{d}_{ij}}\right). \end{aligned}$$

For future references, note that we can let as many presently restricted variables to be free, each additional one being compensated by a factor of $1/u$ on the right side of (12).

5. Heath-Brown's estimate, I

We now begin our estimate of the sum

$$\sum_{\mathbb{D}} g(\mathbb{D}),$$

where $\mathbb{D}$ runs through 21-tuples corresponding to twists E_D by quadratic extensions of K whose discriminants have norm at most X. Recall our convention $\mathfrak{d}_{ij} := \underline{\beta}_{ij}$.

Divide the range of each β_{ij} into intervals $A_{ij} < |\mathbb{N}(\mathfrak{d}_{ij})| \leq 2A_{ij}$, where A_{ij} is a power of 2. This gives us $O(\log^{16} X)$ nonempty subsums, which we denote by $S(A)$, where A is the 18-tuple $(A_{ij}; \beta; \beta_5)$. We may assume that

$$1 \ll \prod_{ij} A_{ij} \ll X, \tag{13}$$

since $\prod_{ij} A_{ij} \leq \mathbb{N}(\prod_{ij} \mathfrak{d}_{ij}) \leq X$.

Call the indices ij, kl **linked** if $i \neq k$, and precisely one of the conditions $l \neq 0, i$ or $j \neq 0, k$ holds. This means that exactly one of

$$\left(\frac{\beta_{ij}}{\mathfrak{d}_{kl}}\right), \left(\frac{\beta_{kl}}{\mathfrak{d}_{ij}}\right)$$

occurs in the expression for $g(\mathbb{D})$. The main result of this section is the following

Lemma 5. *There exists a constant $\kappa > 0$ depending on A, B and K such that*

$$\sum_A |S(A)| \ll \frac{X}{\log^{1/4} X} (\log\log X)^8,$$

where A runs through those 18-tuples corresponding to twists of norm at most X, for which either there are at most 3 elements $A_{ij} > G := e^{\kappa(\ln\ln X)^2}$, or there are linked indices ij, kl with $A_{ij} > G$ and $\mathbb{N}(\mathfrak{d}_{kl}) > 1$.

The proof is broken down into several cases, depending on the size of the linked variables. Suppose ij and kl are linked, and that $\left(\frac{\beta_{ij}}{\mathfrak{d}_{kl}}\right)$ occurs in $g(\mathbb{D})$. This quadratic symbol is the only factor in $g(\mathbb{D})$ in which both indices ij and kl occur. Collecting together the factors of $g(\mathbb{D})$ that involve only ij or kl, respectively, we can write

$$g(\mathbb{D}) = \left(\frac{\beta_{ij}}{\mathfrak{d}_{kl}}\right) a(ij)b(kl),$$

where both $a(ij), b(kl)$ have absolute value at most one. Let ij be a free index, and introduce two or three more free indices so that at least one of the free indices has first coordinate 1, 2 and 3, respectively (cf. §4). Then

$$|S(A)| \leq 2^{\omega_0(A-B)} 2^{\omega_0(B)} \sum_{\beta_{uv}} \left| \sum_{\beta_{ij},\beta_{kl}} \left(\frac{\beta_{ij}}{\underline{\beta}_{kl}}\right) a(ij)b(kl) \right|,$$

where the factor $2^{\omega_0(A-B)}$ comes from the trivial estimate for $\sum_{\mathfrak{b}_5|\beta_5}(-\beta\beta_1\beta_3 A/\mathfrak{b}_5)$, and similarly for $2^{\omega_0(B)}$; and the range of summation is as follows:

- for any index st, we have $A_{st} < \mathbb{N}(\underline{\beta}_{st}) \leq 2A_{st}$;
- $|\mathbb{N}(\underline{\beta}_{ij}\underline{\beta}_{kl})| \leq X/\prod_{uv\neq ij,kl} A_{uv}$ (by (13)).

We now invoke

Lemma 6. *Let η and $\mathfrak{m}$ be free and restricted variables, respectively. Let a_η and $b_{\mathfrak{m}}$ be complex numbers of absolute value at most one. Given $M, N, X > 1$, we have the estimate*

$$\left|\sum_{\eta,\mathfrak{m}} \left(\frac{\eta}{\mathfrak{m}}\right) a_\eta b_{\mathfrak{m}}\right| \ll \frac{MN}{min(M,N)^{1/32}}$$

uniformly in X, where η (resp. $\mathfrak{m}$) runs through square free ideals of norm between N and $2N$ (resp. M and $2M$) supported outside of S_D, and $\mathbb{N}(\underline{\eta}\mathfrak{m}) \leq X$.

Proof. cf. [3], §6. □

This immediately implies that

$$S(A) \ll \left(\prod_{u,v} A_{uv}\right) \frac{A_{ij}A_{kl}}{\min(A_{ij}, A_{kl})^{1/32}} \ll \frac{X}{\min(A_{ij}, A_{kl})^{1/32}}.$$

Thus we get

Lemma 7. $S(A) \ll X/\log^{17} X$ *whenever there exits linked indices ij, kl with A_{ij}, A_{kl}* $\geq \log^{544} X$. □

Now, consider the case in which $A_{ij} \geq \log^{544} X$, but every index kl linked to ij has $A_{kl} < \log^{544} X$. Let β' be the product of these β_{kl}, and let $\mathfrak{d}' := \underline{b}'$. We can write $g(\mathbb{D})$ as

$$4^{-\omega(\beta_{ij})} \left(\frac{\beta_{ij}}{\mathfrak{d}'}\right) \chi'(\beta_{ij}) c,$$

where c is independent of β_{ij} and satisfies $|c| \leq 1$, and χ' comes from the reciprocity law for Hilbert symbols:

$$\chi'(*) = \underbrace{\prod_{\mathfrak{p}|2} \left(\frac{*, \beta''}{\mathfrak{p}}\right)}_{\chi} \cdot \underbrace{\prod_{\mathfrak{p}|\infty} \left(\frac{*, \beta''}{\mathfrak{p}}\right)}_{\chi_\infty},$$

where β'' is the product of those β_{kl} such that $\left(\frac{\beta_{kl}}{\mathfrak{d}_{ij}}\right)$ occurs (and hence need to be flipped). Choose a set of free indices that includes ij. Denote by uv those indices other than ij and are not linked to ij. Then

$$|S(A)| \leq \sum_{\beta_{uv}} \left| \sum_{\beta_{ij}} 4^{-\omega(\beta_{ij})} \left(\frac{\beta_{ij}}{\mathfrak{d}'}\right) \chi'(\beta_{ij}) \right|,$$

where β_{ij} is coprime at S_D to all other β_{uv}, and satisfies

$$A_{ij} < \mathbb{N}(\beta_{ij}) \leq \min\left(2A_{ij}, \frac{X}{\prod_{uv} A_{uv}}\right). \tag{14}$$

Let G be the kernel of the restriction of χ_∞ to U/U^2, and let $\{\epsilon_l\}$ be a set of coset representatives of $(U/U^2)/G$. Then

$$|S(A)| \leq u^{15} \sum_{\beta_{uv}} \left| \sum_{\epsilon_l} \chi_\infty(\epsilon_l) \left[\sum_{\beta_{ij}}{}' 4^{-\omega(\beta_{ij})} \left(\frac{\beta_{ij}}{\mathfrak{d}'}\right) \chi(\beta_{ij}) \left(\sum_{\epsilon \in G} \left(\frac{\epsilon}{\mathfrak{d}'}\right) \chi(\epsilon) \right) \right] \right|.$$

where β_{ij} is now a *restricted* variable over the same range (14). Now, the inner-most sum over $\epsilon \in G$ is either 0 or $\#G$. In the first case $S(A)$ must then be zero. The second case occurs precisely when the restriction of $\left(\frac{\cdot}{\mathfrak{d}'}\right) \chi(\cdot)$ to G is trivial, which by lemma 1 induces an ideal character of $\mathcal{O}_K$. We now invoke

Lemma 8. *Let χ be a non-principal, narrow ideal character mod $\mathfrak{q}$. For any ideal $\mathcal{R}$ and any integer $N > 0$, we have*

$$\sum_{\substack{\mathbb{N}(\mathcal{A}) \leq X \\ (\mathcal{A}, \mathcal{R}) = 1}} \mu^2(\mathcal{A}) 4^{-\omega(\mathcal{A})} \chi(\mathcal{A}) \ll \frac{X d(\mathcal{R})}{e^{c\sqrt{\log X}}}$$

with a positive $c = c_N$, uniformly for $\mathfrak{q} \leq \log^N X$ ($d(\mathcal{R})$ = the number of distinct ideals dividing $\mathcal{R}$; μ = Mobius function).

Proof. cf. [3], §6. □

To apply this, take $\mathfrak{q}$ = (conductor of χ) $\cdot\, \mathfrak{d}'$ and $\mathcal{R} = \prod_{uv} \mathfrak{d}_{uv}$. Then $\mathbb{N}(\mathfrak{q}) \ll (\log^{544} X)^{15}$, and we conclude that

$$S(A) \ll \frac{A_{ij}}{e^{c\sqrt{\log A_{ij}}}} \sum_{\beta_{uv}} d(\mathcal{R})$$

provided that $\mathfrak{d}' \neq (1)$ (in order that $(\cdot/\mathfrak{d}')\chi(\cdot)$ be non-trivial). Since the ideals $\mathfrak{d}_{uv}$ are coprime in pairs, $d(\mathcal{R}) = \prod_{uv} d(\mathfrak{d}_{uv})$. Write the zeta function of K as $\zeta_K(s) = \sum_n a_n n^{-s}$; then for any ideal $\mathcal{J}$ of norm n, $d(\mathcal{J}) \leq \sum_{st=n} a_s a_t$, whence the Tauberian theorem gives

$$\sum_{\mathbb{N}(\mathfrak{d}_{kl}) \leq A_{kl}} d(\mathfrak{d}_{kl}) \leq \sum_{st \leq A_{kl}} a_s a_t \ll A_{kl} \log A_{kl}.$$

Consequently, we have $S(A) \ll X \log^{15} X e^{-c\sqrt{\log A_{ij}}}$ provided that $\mathfrak{d}' \neq \mathcal{O}_K$. Thus we have

Lemma 9. *There exists an absolute constant $\kappa > 0$ such that whenever there are linked indices ij, kl for which $A_{ij} \geq e^{\kappa(\log\log X)^2}$ and $\mathbb{N}(\mathfrak{d}_{kl}) > 1$, we have*

$$S(A) \ll \frac{X}{\log^{17} X}. \quad \square$$

To finish the proof of lemma 5, we now handle the case where at most three of the indices ij lie in ranges satisfying

$$A_{ij} \geq G := e^{\kappa(\log\log X)^2},$$

where G is assumed to be a power of 2. With $\sum'$ denoting the condition of at most three $A_{ij} \geq G$, we have

$$\sum_{A_{ij}}{}' |S(A)| \ll \sum_{\mathbb{N}(\underline{n}_1 \cdots \underline{n}_{16}) \leq X} 4^{-\omega(\underline{n}_1) - \ldots - \omega(\underline{n}_{16})},$$

where the $\underline{n}_i$ are square-free and coprime in pairs, and at most three of them have norm greater than $2G$. Write

$$m = \prod_{n_i \leq 2G} n_i, \;\; n = \prod_{n_i > 2G} n_i.$$

Then $\mathbb{N}(\underline{m}) \leq (2G)^{16}$, and $\mathbb{N}(\underline{n}) \leq X/\mathbb{N}(\underline{m})$. Moreover, each $\underline{m}$ can arise at most

$16^{\omega(\underline{m})}$ times; and $\underline{n}$, at most $\binom{16}{3}3^{\omega(\underline{n})}$ times. Thus

$$\sum_{A_{ij}}{}'|S(A)| \ll \sum_{\substack{\underline{m},\underline{n} \\ \gcd(\underline{m},\underline{n})=\mathcal{O}_K \\ \mathbb{N}(\underline{mn})\leq X}} 16^{\omega(\underline{m})}\binom{16}{3}3^{\omega(\underline{n})}4^{-\omega(\underline{m})}4^{-\omega(\underline{n})}$$

$$\ll \sum_{\substack{\mathbb{N}(\underline{m}) \\ \leq (2G)^{16}}} 4^{\omega(\underline{m})} \sum_{\substack{\mathbb{N}(\underline{n})\leq \\ X/\mathbb{N}(\underline{m})}} \left(\frac{3}{4}\right)^{\omega(n)}.$$

It follows from the Tauberian theorem that, for any fixed $\gamma > 0$, we have

$$(15) \qquad \sum_{\mathbb{N}(\underline{n})\leq N} \gamma^{\omega(\underline{n})} \ll N(\log N)^{\gamma-1}.$$

Since $X/\mathbb{N}(\underline{m}) \gg X/G^{16} \gg \sqrt{X}$, we have $\log(X/\mathbb{N}(\underline{m})) \gg \log X$, whence

$$\sum_{A_{ij}}{}'|S(A)| \ll \frac{X}{\log^{1/4} X} \sum_{\substack{\mathbb{N}(\underline{m}) \\ \leq (2G)^{16}}} 4^{\omega(\underline{m})}\mathbb{N}(\underline{m})^{-1}.$$

A second application of (15) plus partial summation shows that the sum on the right is $O(\log^4 G)$, whence

$$\sum_{A_{ij}}{}'|S(A)| \ll \frac{X}{\log^{1/4} X}\log^4 G \ll \frac{X}{\log^{1/4} X}(\log\log X)^8.$$

Combine this with lemma 7 and 9 then gives lemma 5.

6. Heath-Brown's estimate, II

Heath-Brown's elegant combinatorial argument in ([3], lemma 9) applies without a hitch to our set-up, and yields

Lemma 10. *A sum $S(A)$* not *considered by lemma 8 must have exactly four elements $A_{ij} \geq G$, and the remaining values $\mathbb{N}(\underline{\beta}_{kl})$ must take the value 1 (such β_{kl} will be called the* ***trivial variables****). The possible set of non-trivial indices are*

$$\begin{array}{llll@{\qquad}llll} 10, & 20, & 30, & 40 & i0, & ji, & ki, & li \\ i0, & j0, & ij, & ji & ij, & ik, & lj, & lk \\ i0, & ij, & ik, & il & ij, & ji, & kl, & lk. \end{array} \qquad \square$$

It remains to handle these 24 types of sums. Describe the indices (or the corresponding variables) ij and kl as being **joined** if both quadratic symbols

$$\left(\frac{\beta_{ij}}{\mathfrak{d}_{kl}}\right), \left(\frac{\beta_{kl}}{\mathfrak{d}_{ij}}\right)$$

occur in the expression for $g(\mathbb{D})$. This happens precisely when

$$i \neq k \text{ and } j, l \neq i, k, 0.$$

If two indices are not joined then we say that they are **independent**. For each type of sum in lemma 10 there exists at least one pair of independent variables. Relabel the four variables which occur non-trivially as $n_1, \dots, n_4$, and write $N_1, \dots, N_4$ for the corresponding A_{ij}, we can then assume that n_3, n_4 are independent. Our next step is to estimate $S(A)$ for the sums in lemma 10 as

$$\sum_{n_1,n_2}\left|\sum_{n_3,n_4}\chi_3(\underline{n}_3)\chi_4(\underline{n}_4)4^{-\omega(\underline{n}_1\cdots\underline{n}_4)}\right| \tag{16}$$

for some ideal characters χ_3, χ_4. The second half of this section is devoted to show that, for all but four of the 24 types of sums in lemma 10, we can arrange χ_3, χ_4 to be distinct ideal characters: lemma 11 below will then apply and show that these 20 types of sums contribute to the error term of the asymptotic formula. The remaining four sums will be analyzed in the next section.

To estimate $S(A)$ by (16), recall that we express the average 2-Selmer rank in terms of a sum of $g(\mathbb{D})$, where

$$\begin{aligned} g(\mathbb{D}) &= \frac{1}{2^{\omega_0(A-B)+\omega(B)+2}}\left(\frac{A}{\mathfrak{b}\mathfrak{b}_5}\right)\left(\frac{-\beta}{\mathfrak{b}_5}\right)\left(\frac{\beta_5}{\mathfrak{b}}\right)\left(\frac{\tau}{\mathfrak{b}_5}\right) \\ &\quad \times\prod_{i\neq j}\chi_{ij}\prod_{i}4^{-\omega(\mathfrak{d}_{i0})}\prod_{j\neq 0}4^{-\omega(\mathfrak{d}_{ij})}\prod_{k\neq i,j}\prod_{l}\left(\frac{\beta_{kl}}{\mathfrak{d}_{ij}}\right), \end{aligned} \tag{17}$$

and where χ_{ij} are characters on the *odd* elements of $\mathcal{O}_K$, given by the following table:

i,j	1	2	3	4
1	X	$\left(\frac{\tau\beta\beta_5(A-B)}{\mathfrak{d}_{12}}\right)\left(\frac{\beta_{12}}{\mathfrak{b}_5}\right)$	$\left(\frac{\tau\beta\beta_5A(A-B)}{\mathfrak{d}_{13}}\right)\left(\frac{\beta_{13}}{\mathfrak{b}_5}\right)$	$\left(\frac{\beta_5A}{\mathfrak{d}_{14}}\right)\left(\frac{\beta_{14}}{\mathfrak{b}_5}\right)$
2	$\left(\frac{-\tau\beta\beta_5B}{\mathfrak{d}_{21}}\right)\left(\frac{\beta_{21}}{\mathfrak{b}}\right)$	X	$\left(\frac{\beta_5AB}{\mathfrak{d}_{23}}\right)\left(\frac{\beta_{23}}{\mathfrak{b}}\right)$	$\left(\frac{-\tau\beta A}{\mathfrak{d}_{24}}\right)\left(\frac{\beta_{24}}{\mathfrak{b}}\right)$
3	$\left(\frac{\tau\beta}{\mathfrak{d}_{31}}\right)\left(\frac{\beta_{31}}{\mathfrak{b}\mathfrak{b}_5}\right)$	$\left(\frac{\beta_{32}}{\mathfrak{b}}\right)\left(\frac{\beta_5}{\mathfrak{d}_{32}}\right)\left(\frac{\beta_{32}}{\mathfrak{b}_5}\right)$	X	$\left(\frac{\tau\beta\beta_5}{\mathfrak{d}_{34}}\right)\left(\frac{\beta_{34}}{\mathfrak{b}\mathfrak{b}_5}\right)$
4	$\left(\frac{\beta_5B}{\mathfrak{d}_{41}}\right)$	$\left(\frac{-\tau\beta(A-B)}{\mathfrak{d}_{42}}\right)$	$\left(\frac{-\tau\beta\beta_5B(A-B)}{\mathfrak{d}_{43}}\right)$	X

The χ_{ij} play no role in our previous estimates of $S(A)$, but they will be important for us now.

Independent variables that occur in lemma 10 never appear in the same quadratic symbol, so $g(\mathbb{D})$ can be written as

$$\frac{PQ}{2^{\omega_0(A-B)+\omega_0(B)+1}}\prod_{i=1}^{4}\chi_i(n_i)\phi_i(n_i), \tag{18}$$

where

- $n_1, \dots, n_4$ are the non-trivial variables in lemma 10; they are coprime in pairs, square-free and satisfies $N_i < \mathbb{N}(\underline{n}_i) \leq 2N_i$;
- χ_i is the character in the table above corresponding to n_i;

- P is the result of applying the reciprocity law for Hilbert symbols for each pair of joined variables n_i, n_j to produce

$$\langle n_1, n_2\rangle := \prod_{\mathfrak{p}|2\infty} \left(\frac{n_i, n_j}{\mathfrak{p}}\right) = \left(\frac{n_i}{n_j}\right)\left(\frac{n_j}{n_i}\right)$$

- ϕ_i is the product of the quadratic characters $(\beta_{uv}/\underline{n}_i)$ that occur in (17), with β_{uv} being one of the trivial variables;
- $Q = 4^{-\omega(\underline{n}_1\cdots\underline{n}_4)}$;

To express $S(A)$ with $g(\mathbb{D})$ in the form (18), we must now designate a set of free variables among the sixteen β_{ij}. Declare the independent variables n_3, n_4 to be free. Adjoin to the list $\{n_3, n_4\}$ the smallest subset of $\{\beta_{10}, \beta_{20}, \beta_{30}\}$ so that the resulting set contains at least one variable with first coordinate 1, 2 and 3, respectively. Set all remaining variables to 1. These free variables, together with n_1, n_2 (if not already free), then constitute a complete set of variables for each type of sum in lemma 10. Any non-trivial ϕ_i is then the product of $(\beta_{j0}/\underline{n}_i)$ for some $j = 1, 2, 3$. Hence $S(A)$ can now be estimated by the expression

$$u^3 \sum_{n_1,n_2} \Big| \sum_{n_3,n_4} \chi_3(\underline{n}_3)\chi_4(\underline{n}_4)4^{-\omega(\underline{n}_1\cdots\underline{n}_4)}P\Big|, \tag{19}$$

with n_3, n_4 free and independent (the factor u^3 is due to the possibility that three of the free variables are trivial variables). Observe that P is now the product of the characters $\psi_3(n_3), \psi_4(n_4)$, depending on n_1, n_2, together with a factor depending on n_1, n_2 along.

Claim *Except for the indices* $10, 20, 30, 40; 30, 31, 32, 34; i0, ji, ki, li$, *we can label the non-trivial variables so that* $\psi_3 = \psi_4$ *and* $\chi_3 \neq \chi_4$ *as ideal characters.*

We shall label the variables such that

$$\begin{cases} n_1, n_3 \text{ are joined if and only if } n_1, n_4 \text{ are,} \\ \text{and similarly for } n_2, n_3 \text{ and } n_2, n_4. \end{cases} \tag{20}$$

This will imply that $\psi_3 = \psi_4$, and hence we are reduced to show that $\chi_3 \neq \chi_4$.

For the argument to work, we now make the following extra hypotheses:

Hypothesis

1) the ideal $(A - B)$ *is not a square;*

2) not both A, B *are square in* $\mathcal{O}_K$*;*

3) not both $-A$, $-B$ *are square in* $\mathcal{O}_K$.

Consider sums with indices $i0, j0, ij, ji$. Then at least one of ij, ji corresponds to a non-trivial ideal character: hypothesis (1) takes care of the pairs $12, 21$; $13, 31$; $24, 42$; $34, 43$, regardless of the values of $\beta, \mathfrak{b}$, β_5, $\mathfrak{b}_5$ and A; A is non-square, and hence $14, 41; 23, 32$ hold. Say χ_{ij} is non-trivial; then the labeling

$$n_1 = \beta_{i0}, \quad n_2 = \beta_{ji}, \quad n_3 = \beta_{j0}, \quad n_4 = \beta_{ij}$$

satisfies (20), with $\psi_3 = \psi_4 = \text{id}$. and $\chi_3 \neq \chi_4$ as ideal characters.

Next, consider sums with indices $i0, ij, ik, il$. Hypothesis (1) (resp. (2)) guarantees that the first and the fourth rows (resp. the second row) of the table contain a non-trivial ideal character. The same is true for the third row if $\underline{\beta} \neq \mathcal{O}_K$ or $\underline{\beta}_5 \neq \mathcal{O}_K$. In these cases, the labeling

$$n_1 = \beta_{ik}, \quad n_2 = \beta_{il}, \quad n_3 = \beta_{i0}, \quad n_4 = \beta_{ij},$$

again satisfies (20), with with $\psi_3 = \psi_4 = \text{id}$ and $\chi_3 \neq \chi_4$.

Next, consider sums with indices ij, ji, kl, lk. Then ij, ji necessarily correspond to different ideal characters: hypothesis (1) takes care of the pairs 12, 21; 13, 31; 24, 42; 34, 43. Since A, B are coprime and not both square, the indices 14, 41; 23, 32 are taken care of. Then under the labeling

$$n_1 = \beta_{kl}, \quad n_2 = \beta_{lk}, \quad n_3 = \beta_{il}, \quad n_4 = \beta_{ji},$$

we have $\chi_3 \neq \chi_4$, and ψ_3, ψ_4 are both given by $\langle *, n_1 n_2 \rangle$. We can arrange that $i \neq 4$, whence ij is a free variable. As n_3 runs through all unit representatives (which does not affect χ_3), ψ_3 becomes

$$\langle n_3, n_1 n_2 \rangle \sum_{\epsilon \in U_K/U_K^2} \langle \epsilon, n_1 n_2 \rangle$$

The ϵ-sum is either zero or u, so for fixed n_1 and n_2, we can treat ψ_3 as an ideal character. The same goes for ψ_4, and the two ideal characters so obtained are the same. Thus the claim is verified for the indices ij, ji, kl, lk.

Finally, consider the sums with indices ij, il, lj, lk. We claim that, by the hypothesis, we can assume that ij, ik to correspond to different ideal character. Hypothesis (1) and (2) gives the case $i = 1$ and, by interchanging i and l, the case $l = 1$. Next, take $j = 1$. For $i = 4$, hypothesis (1) implies that each of 41, 42 and 41, 43 corresponds to characters with different conductor. For the reminding sum with indices 21, 24, 31, 34, hypothesis (3) plus the fact that A, B are coprime imply that 21 and 24 correspond to different ideal character. With say ij, ik correspond to different characters, the labeling

$$n_1 = \beta_{lj}, \quad n_2 = \beta_{lk}, \quad n_3 = \beta_{ij}, \quad n_4 = \beta_{ik}$$

then satisfies the original claim, with ψ_3 equals to ψ_4 as ideal characters.

To recapitulate, for the sums not excluded in lemma 10, (19) can be written as

$$u^3 \sum_{n_1, n_2} \Big| \sum_{n_3, n_4} \chi_3(n_3)\psi_3(n_3)\chi_4(n_4)\psi_4(n_4) 4^{-\omega(n_1 \cdots n_4)} \Big|$$

with $\chi_3\psi_3 \neq \chi_4\psi_4$ as ideal characters.

We now consider sums with indices 20, 12, 32, 42. For such sums the terms $g(\mathbb{D})$

takes the form

$$\frac{1}{2^{\omega_0(A-B)+\omega_0(B)+1}}\left(\frac{A}{\mathfrak{b}\mathfrak{b}_5}\right)\left(\frac{\beta_{32}}{\mathfrak{b}}\right)\left(\frac{-\beta}{\mathfrak{b}_5}\right)\left(\frac{\beta_5}{\mathfrak{b}}\right)4^{-\omega(\underline{\beta}_{20}\underline{\beta}_{12}\underline{\beta}_{32}\underline{\beta}_{42})}$$
$$\times\left(\frac{A-B}{\mathfrak{d}_{12}}\right)\left(\frac{A-B}{\mathfrak{d}_{42}}\right)\left(\frac{-\beta}{\mathfrak{d}_{42}}\right)\left(\frac{\beta}{\mathfrak{d}_{12}}\right)\left(\frac{\tau}{\mathfrak{d}_{12}\mathfrak{d}_{42}}\right)$$
$$\times\left(\frac{\beta_{32}}{\mathfrak{b}_5}\right)\left(\frac{\beta_5}{\mathfrak{d}_{32}}\right)\left(\frac{\beta_{12}}{\mathfrak{b}_5}\right)\left(\frac{\beta_5}{\mathfrak{d}_{12}}\right)\langle\beta_{12},\beta_{32}\rangle\langle\beta_{12},\beta_{42}\rangle\langle\beta_{32},\beta_{42}\rangle,$$

with $\beta_{12},\beta_{32},\beta_{42}$ as free variables and β_{20} as a restricted one. With the labeling

$$n_1=\beta_{32},\ n_2=\beta_{42},\ n_3=\beta_{20},\ n_4=\beta_{12},$$

we have

$$\chi_3=\text{ id},\qquad \chi_4=\left(\frac{\beta(A-B)}{*}\right)\left(\frac{\beta_5}{*}\right)\left(\frac{*}{\mathfrak{b}_5}\right)\left(\frac{\tau}{*}\right)$$
$$\psi_3=\text{ id},\qquad \psi_4=\langle *,n_1n_2\rangle.$$

As before for fixed n_1,n_2 we let n_4 runs freely and turn ψ_4 into either zero or an ideal character. We claim that if $\psi_4\neq 0$ then $\chi_4\psi_4\neq$ id.

If $\mathfrak{b}_5\neq\underline{\beta}_5$, then the odd part of the conductor of $\chi_4\psi_4$ is non-trivial. Thus we can assume $\mathfrak{b}_5=\underline{\beta}_5$. If $\underline{\beta}=(A-B)$, choose $\epsilon\in U_K$ such that $\epsilon\beta$ is not equal to n_1n_2 times a square in $\mathcal{O}_K$. Then

$$\chi_4\psi_4=\langle *,\beta_5n_1n_2\rangle$$

is non-trivial. If the square-free part of $\underline{\beta(A-B)}$ contains an odd prime, then

$$\left(\frac{\text{odd}[\beta(A-B)]}{\underline{\lambda}}\right)=\left(\frac{\lambda}{\text{odd}[\underline{\beta(A-B)}]}\right)\langle\text{odd}[\beta(A-B)],\lambda\rangle$$

is non-trivial. Finally, if the square-free part of the ideal $\underline{\beta(A-B)}$ consists of even primes only, then we need

Lemma 11. *Let $\mathfrak{p}_2$ be an even prime, and let $\tau\in\mathcal{O}_K$ be a uniformizer of $\mathfrak{p}_2$ such that τ is prime to all other even primes. Let $\alpha\in\mathcal{O}_K$ be an odd integer so that $\langle\epsilon,\alpha\rangle=1$ for all units $\epsilon\in U_K$ (and hence $\langle *,\alpha\rangle$ defines an ideal character). Suppose K has a unit of every signature. Then the* ideal *characters*

$$\left(\frac{\tau}{*}\right),\ \langle *,\alpha\rangle$$

are distinct.

Proof. For any odd prime $\mathcal{P}$, choose an integer π such that $(\pi)=\mathcal{P}^{2n+1}$. Then

$$\left(\frac{\tau}{\mathcal{P}}\right)=\left(\frac{\tau,\pi}{\mathcal{P}}\right)=\prod_{\mathfrak{p}\nmid 2\infty}\left(\frac{\tau,\pi}{\mathfrak{p}}\right)=\langle\tau,\pi\rangle,$$

by the product formula of Hilbert symbols. By the Chinese reminder theorem, there exists an odd integer $\pi \in \mathcal{O}_K$ such that π has quadratic defect (4) with respect to $\mathfrak{p}_2$ (cf. [11], 63:4), and is congruent to 1 modulo every other even prime. Then

$$\left(\frac{\tau,\pi}{\mathfrak{p}_2}\right) = -1, \quad \left(\frac{\alpha,\pi}{\mathfrak{p}_2}\right) = 1, \quad \text{and} \quad \left(\frac{\tau,\pi}{\mathfrak{p}}\right) = \left(\frac{\alpha,\pi}{\mathfrak{p}}\right) = 1$$

for all other even primes $\mathfrak{p}$. It follows that

$$\prod_{\mathfrak{p}|2}\left(\frac{\pi,\tau}{\mathfrak{p}}\right) \neq \prod_{\mathfrak{p}|2}\left(\frac{\pi,\alpha}{\mathfrak{p}}\right). \tag{21}$$

If K has a unit of every signature, then we can adjust π by a multiple of a unit so that

$$\prod_{\mathfrak{p}|\infty}\left(\frac{\pi,\tau}{\mathfrak{p}}\right) = \prod_{\mathfrak{p}|\infty}\left(\frac{\pi,\alpha}{\mathfrak{p}}\right),$$

and this modification of π does not affect (21), by the hypothesis on α. The lemma then follows. □

This takes care of the indices 20, 12, 32, 42; the indices 30, 13, 23, 43 can be taken care of similarly. We now invoke

Lemma 12. *Let χ_1, χ_2 be distinct ideal characters of modulus $\mathcal{A}_1, \mathcal{A}_2$, respectively. Let $\mathcal{R}$ be any non-trivial ideal. Then there exists an absolute constant $c > 0$ such that, for any $X > 0$ and any integers $M, N \geq G > 0$, as $\mathfrak{m}$ and $\mathfrak{n}$ runs through coprime ideals of norm between M and $2M$ (resp. N and $2N$) whose product is prime to $\mathcal{R}$ and of norm at most X, we have the estimate*

$$\sum_{\mathfrak{m},\mathfrak{n}} \mu^2(\mathfrak{m})\mu^2(\mathfrak{n})4^{-\omega(\mathfrak{m})-\omega(\mathfrak{n})}\chi_1(\mathfrak{m})\chi_2(\mathfrak{n}) \ll d(\mathcal{R})\frac{X\log X}{e^{c\sqrt{\log G}}}.$$

Proof. cf. [3], §6. □

It follows that the sums $S(A)$ in questions are all $O(X(\log X)^{-17})$, since the constant κ in lemma 7 can be taken to be sufficiently large. The total contribution of these sums is therefore $O(X/\log X)$. We summarize as follows.

Lemma 13. *We have*

$$\sum_{A} S(A) \ll \frac{X(\log\log X)^8}{(\log X)^{1/4}},$$

where the sum A is for all sets other than those corresponding to indices

$$\begin{array}{ll} 10, 20, 30, 40; & \\ 30, 31, 32, 34; & \textit{(necessarily with } \underline{\beta} = \underline{\beta}_5 = \mathcal{O}_K\textit{)} \\ 10, 21, 31, 41; & \\ 40, 14, 24, 34. & \end{array}$$

7. Leading terms

In this section we analyze the four types of sums not considered by lemma 13 and show that they contribute to the main term of the asymptotic formula. This completes the proof of our theorem.

Case 1: Sums with indices 10, 20, 30, 40.

As β_{10}, β_{20} and β_{30} are free and all trivial variables take the value 1, $g(\mathbb{D})$ is reduced to

$$\frac{1}{2^{\omega_0(A-B)+\omega_0(B)+2}} \left(\frac{\beta_{20}\beta_{30}\beta_5 A}{\mathfrak{b}}\right) \left(\frac{-\beta\beta_{10}\beta_{30}A}{\mathfrak{b}_5}\right) \left(\frac{\tau}{\mathfrak{b}_5}\right) 4^{-\omega(\underline{\beta}_{10}\cdots\underline{\beta}_{40})},$$

Thus the contribution of all sums with indices 10, 20, 30, 40 and $A_{ij} \geq G$ is

$$\begin{aligned} &\frac{1}{2^{\omega_0(A-B)+\omega_0(B)+1}} \sum_{\tau} \sum_{\beta} \sum_{\beta_5} \sum_{\mathfrak{b}|\beta} \sum_{\mathfrak{b}_5|\beta_5} \\ &\quad \left(\frac{-A\beta\tau}{\mathfrak{b}_5}\right) \left(\frac{A\beta_5}{\mathfrak{b}}\right) \sum_{\beta_{i0}} \left(\frac{\beta_{20}}{\mathfrak{b}}\right) \left(\frac{\beta_{30}}{\mathfrak{b}}\right) \left(\frac{\beta_{10}}{\mathfrak{b}_5}\right) \left(\frac{\beta_{30}}{\mathfrak{b}_5}\right) 4^{-\omega(\underline{\beta}_{10}\cdots\underline{\beta}_{40})}, \end{aligned} \tag{22}$$

where the inner-most sum is subject to the conditions

$$\mathbb{N}(\underline{\beta}_{i0}) > G \quad \text{and} \quad \mathbb{N}(\underline{\beta}_{10}\cdots\underline{\beta}_{40}) \leq X.$$

Exactly as in Heath-Brown ([3], §5), we can remove the condition $\mathbb{N}(\beta_{i0}) > G$ with an error term $\ll X(\log\log X)^2/(\log X)^{1/4}$.

Denote by $\sum_{\mathfrak{m}}$ the sum over all square-free ideals $\mathfrak{m}$ of norm at most X which are prime to $2AB(A-B)$; then the inner-most sum in (22) can be written as

$$\sum_{\mathfrak{m}} 4^{-\omega(\mathfrak{m})} \sum_{\substack{\underline{v}|\mathfrak{m} \\ \underline{\beta}_{30}:=\mathfrak{m}/\underline{v}}} \left(\frac{\beta_{30}}{\mathfrak{b}\mathfrak{b}_5}\right) \sum_{\substack{\underline{\lambda}|\underline{v} \\ \underline{\beta}_{20}:=\underline{v}/\underline{\lambda}}} \left(\frac{\beta_{20}}{\mathfrak{b}}\right) \sum_{\underline{\beta}_{10}|\underline{\lambda}} \left(\frac{\beta_{10}}{\mathfrak{b}_5}\right) \tag{23}$$

β_{10} is free, so the β_{10}-sum is zero unless $(*/\mathfrak{b}_5)$ is trivial on units. Let $u := \#(U_K/U_K^2)$; then the β_{10}-sum becomes

$$u \sum_{\mathfrak{d}_{10}|\underline{\lambda}} \left(\frac{\mathfrak{d}_1}{\mathfrak{b}_5}\right). \tag{24}$$

This sum (without the u factor) is a multiplicative function with respect to $\underline{\lambda}$, so for a square-free ideal λ, (24) is zero unless $(\mathfrak{d}/\mathfrak{b}_5) = 1$ for all $\mathfrak{d}|\underline{\lambda}$, in which case it becomes $u2^{\omega(\underline{\lambda})}$. Thus (23) becomes

$$\sum_{\mathfrak{m}} u4^{-\omega(\underline{m})} \sum_{\substack{\underline{v}|\mathfrak{m} \\ \underline{\beta}_{30}:=\mathfrak{m}/\underline{v}}} \left(\frac{\beta_{30}}{\mathfrak{b}\mathfrak{b}_5}\right) \sum_{\substack{\underline{\lambda}|\underline{v} \\ \underline{\beta}_{20}:=\underline{v}/\underline{\lambda}}} \begin{cases} 2^{\omega(\underline{\lambda})}\left(\frac{\beta_{20}}{\mathfrak{b}}\right) & \text{if } \left(\frac{\mathfrak{d}}{\mathfrak{b}_5}\right)=1 \text{ for all } \mathfrak{d}|\underline{\lambda}; \\ 0 & \text{otherwise.} \end{cases}$$

For a square-free ideal $\underline{v}$, denote by $\underline{v}_1$ the product of all prime divisors $\mathfrak{p}$ of $\underline{v}_1$ such that $(\mathfrak{p}/\mathfrak{b}_5) = 1$, and write $\underline{v} = \underline{v}_1\underline{v}_2$. Then the summand of the λ-sum above is zero unless $\underline{\lambda}|\underline{v}_1$, whence the λ-sum above becomes

$$\begin{aligned} 2^{\omega(v)} \sum_{\underline{z}|\underline{v}_1} 2^{-\omega(zv_2)}\left(\frac{zv_2}{\mathfrak{b}}\right) &= 2^{\omega(v_1)}\left(\frac{v_2}{\mathfrak{b}}\right)\sum_{\underline{z}|\underline{v}_1} 2^{-\omega(z)}\left(\frac{z}{\mathfrak{b}}\right) \\ &= 2^{\omega(v_1)}\left(\frac{v_1}{\mathfrak{b}}\right) 2^{-\omega(v_1)} \prod_{\substack{\mathfrak{p}|\underline{v_1} \\ (\mathfrak{p}/\underline{v_1})=1}} 3 \\ &= \left(\frac{v_2}{\mathfrak{b}}\right) 3^{\#\{\mathfrak{p}|\underline{v}\,:\,(\mathfrak{p}/\mathfrak{b})=(\mathfrak{p}/\mathfrak{b}_5)=1\}}. \end{aligned}$$

Set $n(v) := \#\{\mathfrak{p}|\underline{v} : (\mathfrak{p}/\mathfrak{b}) = (\mathfrak{p}/\mathfrak{b}_5) = 1\}$. Then (23) becomes

$$\begin{aligned} \sum_{\mathfrak{m}} 4^{-\omega(\mathfrak{m})} \sum_{\substack{\underline{v}|\mathfrak{m} \\ \underline{\beta}_{30}:=\mathfrak{m}/\underline{v}}} \left(\frac{\beta_{30}}{\mathfrak{b}\mathfrak{b}_5}\right)\left(\frac{v_2}{\mathfrak{b}}\right) 3^{n(v)} &= \sum_{\mathfrak{m}} 4^{-\omega(\mathfrak{m})}\left(\frac{m}{\mathfrak{b}\mathfrak{b}_5}\right)\sum_{\underline{v}|\mathfrak{m}}\left(\frac{v}{\mathfrak{b}\mathfrak{b}_5}\right)\left(\frac{v_2}{\mathfrak{b}}\right) 3^{n(v)} \\ &\ll \sum_{\mathfrak{m}} 4^{-\omega(\mathfrak{m})} \sum_{\underline{v}|\mathfrak{m}} 3^{n(v)}. \\ &= \sum_{\mathfrak{m}} 4^{-\omega(\mathfrak{m})} \prod_{\substack{\mathfrak{p}|\mathfrak{m} \\ (\mathfrak{p}/\mathfrak{b})=(\mathfrak{p}/\mathfrak{b}_5)=1}} 4 \\ &= \sum_{\mathfrak{m}} \left(\frac{1}{4}\right)^{\#\{\mathfrak{p}|\mathfrak{m}\,:\,(\mathfrak{p}/\mathfrak{b})=-1 \text{ or } (\mathfrak{p}/\mathfrak{b}_5)=-1\}}. \end{aligned} \tag{25}$$

Write this series as $\sum_{m\leq X} a_m$; then a_m are the coefficients of the Dirichlet series defined by

$$\begin{aligned} &\prod_{\substack{\mathfrak{p} \\ (\mathfrak{p}/\mathfrak{b})=-1}}\left(1+\frac{1}{4\mathbb{N}(\mathfrak{p})^s}\right) \prod_{\substack{\mathfrak{p} \\ (\mathfrak{p}/\mathfrak{b}_5)=-1}}\left(1+\frac{1}{4\mathbb{N}(\mathfrak{p})^s}\right) \\ &\times \prod_{\substack{\mathfrak{p} \\ (\mathfrak{p}/\mathfrak{b})=(\mathfrak{p}/\mathfrak{b}_5)=1}}\left(1+\frac{1}{\mathbb{N}(\mathfrak{p})^s}\right) \prod_{\substack{\mathfrak{p} \\ (\mathfrak{p}/\mathfrak{b})=(\mathfrak{p}/\mathfrak{b}_5)=-1}}\left(1+\frac{1}{4\mathbb{N}(\mathfrak{p})^s}\right)^{-1}. \end{aligned}$$

If one of $\underline{\beta}, \underline{\beta}_5 \neq \mathcal{O}_K$, then for $s \sim 1$ this product is asymptotically bounded by $1/\sqrt{s-1}$, whence the Tauberian theorem implies that (25) is bounded by $X/\sqrt{\log X}$. Consequently, the sum (22) is bounded by $O(X/\sqrt{\log X})$ unless $\mathfrak{b} = \mathfrak{b}_5 = \mathcal{O}_K$. Thus

(22) becomes

$$\begin{aligned}
&\frac{1}{2^{\omega_0(A-B)+\omega_0(B)+2}}\sum_{\tau}\sum_{\beta}\sum_{\beta_5}\sum_{\beta_{i0}} 4^{-\omega(\underline{\beta}_{10}\cdots\underline{\beta}_{40})}+O\left(X\frac{(\log\log X)^2}{(\log X)^{1/4}}\right)\\
=\;& 2^{\#\tau}\frac{u^3}{4}\sum_{\mathfrak{m}} 1+O\left(X\frac{(\log\log X)^2}{(\log X)^{1/4}}\right).
\end{aligned}$$

Case 2: Sums with indices $30, 31, 32, 34$.

For such sums, β_{32}, β_{34} are restricted non-trivial variables, β_{10}, β_{20} are free and trivial, β_{30} is free and non-trivial, and all other variables take the value 1. Recall that the sum in question is non-trivial only if $\underline{\beta}=\underline{\beta}_5=\mathcal{O}_K$, in which case we can simply take $\beta=\beta_5=1$. Set (say) β_{10}, β_{20} to be (trivial) free variables and set all other trivial variables to 1. Turn the remaining free variable with first coordinate 3 into a restricted one, compensated by multiplying the sum by u. Then the sum becomes

$$(26)\quad \frac{u}{2^{\omega_0(A-B)+\omega_0(B)+2}}\sum_{\tau}\sum_{\substack{\mathfrak{d}_{3j};\\ \beta_{10},\beta_{20}}} 4^{-\omega(\mathfrak{d}_{30}\cdots\mathfrak{d}_{34})}\left(\frac{\beta_{10}}{\mathfrak{d}_{32}}\right)\left(\frac{\beta_{20}}{\mathfrak{d}_{31}}\right)\left(\frac{\beta_{10}\beta_{20}}{\mathfrak{d}_{34}}\right)\left(\frac{\tau}{\mathfrak{d}_{31}\mathfrak{d}_{34}}\right).$$

Since β_{10} and β_{20} are free, the sums $\sum_{\beta_{10}}(\beta_{10}/\mathfrak{d}_{32}\mathfrak{d}_{34})$ and $\sum_{\beta_{20}}(\beta_{20}/\mathfrak{d}_{31}\mathfrak{d}_{34})$ are zero unless the characters $(\cdot/\mathfrak{d}_{3j}\mathfrak{d}_{34})$ are trivial on $U := U_K/U_K^2$; in that case, both sums take the value u. Simplify the notation by writing $\mathfrak{d}_j = \mathfrak{d}_{3j}$; then (26) becomes

$$\begin{aligned}
&\frac{u^3}{2^{\omega_0(A-B)+\omega_0(B)+2}}\sum_{\tau}\sum_{\mathfrak{m}}\frac{1}{4^{\omega(\mathfrak{m})}}\sum_{\underline{v}|\mathfrak{m}}\sum_{\substack{\underline{\lambda}|\underline{v}\\ (U/\mathfrak{m}\underline{\lambda})=1}}\sum_{\substack{\mathfrak{d}|\underline{\lambda}\\ (U/\underline{v}\mathfrak{d})=1}}\left(\frac{\tau}{\underline{v}\mathfrak{d}}\right)\\
=\;&\frac{u^3}{2^{\omega_0(A-B)+\omega_0(B)+2}}\sum_{\tau}\sum_{\mathfrak{m}}\frac{1}{4^{\omega(\mathfrak{m})}}\sum_{\underline{v}|\mathfrak{m}}\sum_{\substack{\underline{\lambda}|\underline{v}\\ (U/\mathfrak{m}\underline{\lambda})=1}}\frac{1}{u}\sum_{\epsilon\in U}\sum_{\mathfrak{d}|\underline{\lambda}}\left(\frac{\epsilon\tau}{\underline{v}\mathfrak{d}}\right)\\
=\;&\frac{u^2}{2^{\omega_0(A-B)+\omega_0(B)+2}}\sum_{\tau}\sum_{\epsilon\in U}\sum_{\mathfrak{m}}\frac{1}{4^{\omega(\mathfrak{m})}}\sum_{\underline{v}|\mathfrak{m}}\left(\frac{\tau\epsilon}{\underline{v}}\right)\sum_{\substack{\underline{\lambda}|\underline{v}\\ (U/\mathfrak{m}\underline{\lambda})=1}}\begin{cases}2^{\omega(\lambda)} & \text{if } \left(\frac{\epsilon\tau}{\mathfrak{p}}\right)=1\ \forall\,\mathfrak{p}|\underline{\lambda};\\ 0 & \text{otherwise.}\end{cases}\\
=\;&\frac{u}{2^{\omega_0(A-B)+\omega_0(B)+2}}\sum_{\tau}\sum_{\epsilon,\epsilon'\in U}\sum_{\mathfrak{m}}\frac{1}{4^{\omega(\mathfrak{m})}}\sum_{\underline{v}|\mathfrak{m}}\left(\frac{\tau\epsilon}{\underline{v}}\right)\sum_{\underline{\lambda}|\underline{v}}\begin{cases}2^{\omega(\lambda)}\left(\frac{\epsilon'}{\mathfrak{m}\underline{\lambda}}\right) & \text{if } \left(\frac{\epsilon\tau}{\mathfrak{p}}\right)=1\ \forall\,\mathfrak{p}|\underline{\lambda};\\ 0 & \text{otherwise.}\end{cases}\\
=\;&\frac{u}{2^{\omega_0(A-B)+\omega_0(B)+2}}\sum_{\tau}\sum_{\epsilon,\epsilon'\in U}\sum_{\mathfrak{m}}\frac{1}{4^{\omega(\mathfrak{m})}}\left(\frac{\epsilon'}{\mathfrak{m}}\right)\sum_{\underline{v}|\mathfrak{m}}\left(\frac{\tau\epsilon}{\underline{v}}\right)\prod_{\substack{\mathfrak{p}|\underline{v}\\ \left(\frac{\epsilon\tau}{\mathfrak{p}}\right)=1}}\left(1+2\left(\frac{\epsilon'}{\mathfrak{p}}\right)\right)\\
\ll\;&\frac{u}{2^{\omega_0(A-B)+\omega_0(B)+2}}\sum_{\tau}\sum_{\epsilon,\epsilon'\in U}\sum_{\mathfrak{m}}\frac{1}{4^{\omega(\mathfrak{m})}}\left(\frac{\epsilon'}{\mathfrak{m}}\right)\sum_{\underline{v}|\mathfrak{m}}\left(\frac{\tau\epsilon}{\underline{v}}\right)3^{\#\{\mathfrak{p}|\underline{v}\,:\,\left(\frac{\epsilon\tau}{\mathfrak{p}}\right)=\left(\frac{\epsilon'}{\mathfrak{p}}\right)=1\}}
\end{aligned}$$

$$= \frac{u}{2^{\omega_0(A-B)+\omega_0(B)+2}} \sum_{\tau} \sum_{\epsilon,\epsilon' \in U} \sum_{\mathfrak{m}} \frac{1}{4^{\omega(\mathfrak{m})}} \left(\frac{\epsilon'}{\mathfrak{m}}\right) \times$$

$$\prod_{\substack{\mathfrak{p}|\mathfrak{m} \\ \left(\frac{\epsilon\tau}{\mathfrak{p}}\right)=\left(\frac{\epsilon'}{\mathfrak{p}}\right)=1}} \left(1+3\left(\frac{\tau\epsilon}{\mathfrak{p}}\right)\right) \prod_{\substack{\mathfrak{p}|\mathfrak{m} \\ \left(\frac{\epsilon\tau}{\mathfrak{p}}\right)=-1 \text{ or } \left(\frac{\epsilon'}{\mathfrak{p}}\right)=-1}} \left(1+\left(\frac{\tau\epsilon}{\mathfrak{p}}\right)\right)$$

$$= \frac{u}{2^{\omega_0(A-B)+\omega_0(B)+2}} \sum_{\tau} \sum_{\epsilon,\epsilon' \in U} \sum_{\mathfrak{m}} \frac{(\epsilon'/\mathfrak{m})}{4^{\omega(\mathfrak{m})}} 4^{\#\{\mathfrak{p}|\mathfrak{m} : \left(\frac{\epsilon\tau}{\mathfrak{p}}\right)=\left(\frac{\epsilon'}{\mathfrak{p}}\right)=1\}} 2^{\#\{\mathfrak{p}|\mathfrak{m} : \left(\frac{\epsilon\tau}{\mathfrak{p}}\right)=1, \left(\frac{\epsilon'}{\mathfrak{p}}\right)=-1\}}$$

$$= \frac{u}{2^{\omega_0(A-B)+\omega_0(B)+2}} \sum_{\tau} \sum_{\epsilon,\epsilon' \in U} \sum_{\mathfrak{m}} \left(\frac{\epsilon'}{\mathfrak{m}}\right) 4^{-\#\{\mathfrak{p}|\mathfrak{m} : \left(\frac{\epsilon\tau}{\mathfrak{p}}\right)=-1\}} 2^{-\#\{\left(\frac{\epsilon\tau}{\mathfrak{p}}\right)=1, \left(\frac{\epsilon'}{\mathfrak{p}}\right)=-1\}}$$

The Tauberian argument for (25) applies in here as well and shows that the contribution to the main term of the asymptotic formula comes from the summands with $\epsilon = \epsilon' = \tau = 1$. Thus the contribution of (26) is

$$\frac{u}{2^{\omega_0(A-B)+\omega_0(B)+2}} \sum_{\mathfrak{m}} 1 + O\left(\frac{X(\log\log X)^8}{(\log X)^{1/4}}\right).$$

Case 3: Sums with indices 10, 21, 31, 41.

In this case, the summands $g(\mathbb{D})$ take the form

$$\frac{4^{-\omega(\mathfrak{d}_{10}\mathfrak{d}_{21}\mathfrak{d}_{31}\mathfrak{d}_{41})}}{2^{\omega_0(A-B)+\omega_0(B)+2}} \left(\frac{A}{\mathfrak{b}}\right) \left(\frac{-A}{\mathfrak{b}_5}\right) \left(\frac{\beta_5}{\mathfrak{b}}\right) \left(\frac{\beta}{\mathfrak{b}_5}\right) \left(\frac{\tau}{\mathfrak{b}_5}\right) \langle\beta_{21},\beta_{31}\rangle\langle\beta_{21},\beta_{41}\rangle\langle\beta_{31},\beta_{41}\rangle$$

$$(27) \qquad \times \left(\frac{-1}{\mathfrak{d}_{21}}\right) \left(\frac{\beta}{\mathfrak{d}_{31}}\right) \left(\frac{\beta_{31}}{\mathfrak{b}}\right) \left(\frac{\tau}{\mathfrak{d}_{21}\mathfrak{d}_{31}}\right) \left(\frac{\beta}{\mathfrak{d}_{21}}\right) \left(\frac{\beta_{21}}{\mathfrak{b}}\right) \left(\frac{\beta_5 B}{\mathfrak{d}_{21}\mathfrak{d}_{41}}\right) \left(\frac{\beta_{31}}{\mathfrak{b}_5}\right).$$

$\mathfrak{b}_5$ and the square-free part of the ideals $\underline{\beta_5}\underline{B}$ are disjoint, thus if $\mathfrak{b}_5 \neq \mathcal{O}_K$, the last two characters of the second line of (27) furnishes a pair of distinct ideal characters; lemma 10 then applies and shows that the sum contributes to the error term. Similarly, we can take $\underline{\beta_5} = \underline{B}$ and $\underline{\beta} = \mathfrak{b}$. Set $\beta_5 = B$; then (27) is reduced to

$$\frac{4^{-\omega(\mathfrak{d}_{10}\mathfrak{d}_{21}\mathfrak{d}_{31}\mathfrak{d}_{41})}}{2^{\omega_0(A-B)+\omega_0(B)+2}} \left(\frac{AB}{\mathfrak{b}}\right) \left(\frac{-1}{\mathfrak{d}_{21}}\right) \left(\frac{\tau}{\mathfrak{d}_{21}\mathfrak{d}_{31}}\right) \langle\beta,\beta_{21}\beta_{31}\rangle\langle\beta_{21},\beta_{31}\rangle\langle\beta_{21},\beta_{41}\rangle\langle\beta_{31},\beta_{41}\rangle.$$

Simplify the notation by writing $\beta_j = \beta_{j1}$. Then with β_2 and β_3 as free variables, the sum becomes

$$\frac{u}{2^{\omega_0(A-B)+\omega_0(B)+2}} \sum_{\beta} \sum_{\epsilon_2,\epsilon_3 \in U} \langle\epsilon_2,\epsilon_3\rangle \left(\frac{AB}{\underline{\beta}}\right) \sum_{\tau} \sum_{\mathfrak{d}_i} 4^{-\omega(\mathfrak{d}_{10}\mathfrak{d}_{21}\mathfrak{d}_{31}\mathfrak{d}_{41})}$$

$$\times \langle -1,\beta_2\rangle\langle\beta,\beta_2\beta_3\rangle\langle\beta_2,\beta_3\rangle\langle\beta_2,\beta_4\rangle\langle\beta_3,\beta_4\rangle$$

$$(28) \qquad \times \left(\frac{\tau}{\mathfrak{d}_{21}\mathfrak{d}_{31}}\right) \langle\epsilon_2,\beta\beta_3\beta_4\rangle\langle\epsilon_3,\beta\beta_2\beta_4\rangle$$

To evaluate this sum, introduce the hypothesis that the ideal (2) splits completely in K. For any even prime $\mathfrak{p}$ of K and for any odd integer $\lambda \in \mathcal{O}_K$, define

$$\chi_{\mathfrak{p}}(\lambda) := \begin{cases} 1 & \text{if } \lambda \equiv 1 \pmod{\mathfrak{p}^2}; \\ -1 & \text{if } \lambda \equiv -1 \pmod{\mathfrak{p}^2}. \end{cases}$$

Then we have the following equality:

$$\left(\frac{\beta_2,\beta_3}{\mathfrak{p}}\right)\left(\frac{\beta_2,\beta_4}{\mathfrak{p}}\right)\left(\frac{\beta_3,\beta_4}{\mathfrak{p}}\right)$$
$$(29) \qquad = \frac{\chi_{\mathfrak{p}}(\beta_2)}{2}\left[1+\chi_{\mathfrak{p}}(\beta_2\beta_3)+\chi_{\mathfrak{p}}(\beta_2\beta_4)-\chi_{\mathfrak{p}}(\beta_3\beta_4)\right].$$

Assume that K has a unit of every signature. Then we can take $\beta,\beta_2,\beta_3,\beta_4$ in (28) to be totally real, whence $\langle\beta_i,\beta_j\rangle$ depends only on the even primes. In view of (29), we have

$$\langle\beta_2,\beta_3\rangle\langle\beta_2,\beta_4\rangle\langle\beta_3,\beta_4\rangle$$
$$(30) \qquad = \frac{1}{2^{[K:\mathbb{Q}]}}\prod_{\mathfrak{p}|2}\left(\chi_{\mathfrak{p}}(\beta_2)\cdot[1+\text{ sum of product of } \chi_{\mathfrak{p}_i}(\beta_j\beta_k)]\right).$$

We now seek conditions under which the product of (30) with the rest of the characters in (28) is a non-trivial character, and hence ensures that the $\mathfrak{d}_j$-sum in (28) contributes to the error term.

Lemma 14. *Suppose that the ideal* (2) *splits completely in* K*. Given* $\epsilon\in U_K$*, if there exists an even prime* $\mathfrak{p}$ *such that* $\epsilon\not\equiv 1 \pmod{\mathfrak{p}^3}$*, then* $\langle\epsilon,*\rangle$*, as a character on the totally positive elements in* $\mathcal{O}_K$*, has conductor divisible by* $\mathfrak{p}^3$*.*

Proof. Since $\mathfrak{p}$ has norm 2, the hypothesis on ϵ implies that $\epsilon\equiv\pm3$ or $-1 \pmod{\mathfrak{p}^3}$. Now, classical computation of the Hilbert symbol over $\mathbb{Z}_2$ gives

$$\left(\frac{-1,\pm1}{2}\right)=1, \qquad \left(\frac{-1,\pm3}{2}\right)=-1.$$

Thus $\left(\frac{\epsilon,*}{\mathfrak{p}}\right)$ is a character modulo $\mathfrak{p}^3$. The lemma then follows. □

Expanding the product on the right side, we get a sum where each of its terms is a product of characters modulo $\mathfrak{p}^2$ for various even primes $\mathfrak{p}$. Now, if one of ϵ_2,ϵ_3 satisfies the condition of the lemma, then the $\mathfrak{d}_j$-sum in (28) contains a non-trivial character and hence contributes to the error term. The same holds if $\underline{\tau}\neq\mathcal{O}_K$, by lemma 11. Denote by $\sum'_\epsilon$ the sum over units ϵ in U_K/U_K^2 which do *not* satisfies the condition of lemma 14. Then, modulo the error term, the sum (28) becomes

$$\frac{u}{2^{\omega_0(A-B)+\omega_0(B)+2}}\sum_{\epsilon_2,\epsilon_3}{}'\langle\epsilon_2,\epsilon_3\rangle\sum_{\beta}\left(\frac{AB}{\underline{\beta}}\right)\sum_{\mathfrak{d}_i}4^{-\omega(\mathfrak{d}_{10}\mathfrak{d}_{21}\mathfrak{d}_{31}\mathfrak{d}_{41})}$$
$$(31) \qquad \times\ \langle-1,\beta_2\rangle\langle\beta,\beta_2\beta_3\rangle\langle\beta_2,\beta_3\rangle\langle\beta_2,\beta_4\rangle\langle\beta_3,\beta_4\rangle$$

In view of (30), the product of characters in (31) is non-trivial unless for some even prime $\mathfrak{p}$, we have

$$(32) \qquad \begin{cases} \langle -1, \beta_2 \rangle = \prod_{\mathfrak{q}|2} \chi_{\mathfrak{q}}(\beta_2), \quad \text{and} \\ \prod_{\mathfrak{q}|2} \left(\frac{\beta, \beta_2\beta_3}{\mathfrak{q}} \right) = \chi_{\mathfrak{p}}(\beta_2\beta_3). \end{cases}$$

For each β, let $\mathbb{P}_\beta$ be the number of even primes $\mathfrak{p}$ for which (32) holds; then, modulo the error term, the sum (28) becomes

$$\begin{aligned} & \frac{u}{2^{\omega_0(A-B)+\omega_0(B)+2}} \sum_{\epsilon_2,\epsilon_3}{}' \langle \epsilon_2, \epsilon_3 \rangle \sum_{\beta} \left(\frac{AB}{\underline{\beta}} \right) \mathbb{P}_\beta \sum_{\mathfrak{d}_j} \frac{4^{-\omega(\mathfrak{d}_{10}\mathfrak{d}_{21}\mathfrak{d}_{31}\mathfrak{d}_{41})}}{2^{[K:\mathbb{Q}]}} \\ = & \frac{u}{2^{\omega_0(A-B)+\omega_0(B)+2+[K:\mathbb{Q}]}} \left(\sum_{\mathfrak{m}} 1 \right) \sum_{\epsilon_2,\epsilon_3}{}' \langle \epsilon_2, \epsilon_3 \rangle \sum_{\beta} \left(\frac{AB}{\underline{\beta}} \right) \mathbb{P}_\beta. \end{aligned}$$

Case 4: Sums with indices 40, 14, 24, 34.

The argument (27) applies to the present case as well and shows that, modulo the error term, the sum in question becomes (with $\beta_j := \beta_{j4}$)

$$(33) \qquad \begin{aligned} & \frac{1}{2^{\omega_o(A-B)+\omega_0(B)+2}} \sum_{\beta,\beta_5} \langle \beta, \beta_5 \rangle \left(\frac{A}{\mathfrak{b}\mathfrak{b}_5} \right) \left(\frac{-1}{\mathfrak{b}_5} \right) \\ & \times \sum_{\mathfrak{d}_i} \left(\frac{-1}{\mathfrak{d}_2} \right) \left(\frac{A}{\mathfrak{d}_1\mathfrak{d}_2} \right) \langle \beta, \beta_2\beta_3 \rangle \langle \beta_5, \beta_1\beta_3 \rangle \langle \beta_1, \beta_2 \rangle \langle \beta_1, \beta_3 \rangle \langle \beta_2, \beta_3 \rangle. \end{aligned}$$

If A is divisible by an even prime, then by lemma 11 the $\mathfrak{d}_i$-sum above contains a non-trivial character and hence contributes to the error term. Now, suppose A is a unit. Recall that $\beta_1, \beta_2, \beta_3$ are all free variables. Repeat the same argument for case 3, we see that the sum (33) becomes

$$\begin{aligned} & \frac{1}{2^{\omega_o(A-B)+\omega_0(B)+2}} \sum_{\beta,\beta_5} \langle \beta, \beta_5 \rangle \left(\frac{A}{\mathfrak{b}\mathfrak{b}_5} \right) \left(\frac{-1}{\mathfrak{b}_5} \right) \sum_{\epsilon_1,\epsilon_2,\epsilon_3}{}'' \langle \epsilon_1, \epsilon_2 \rangle \langle \epsilon_1, \epsilon_3 \rangle \langle \epsilon_2, \epsilon_3 \rangle \\ & \times \sum_{\mathfrak{d}_i} \left(\frac{-1}{\mathfrak{d}_2} \right) \left(\frac{A}{\mathfrak{d}_1\mathfrak{d}_2} \right) \langle \beta, \beta_2\beta_3 \rangle \langle \beta_5, \beta_1\beta_3 \rangle \langle \beta_1, \beta_2 \rangle \langle \beta_1, \beta_3 \rangle \langle \beta_2, \beta_3 \rangle, \end{aligned}$$

where all the β's can be chosen to be totally positive, and $\sum''$ denotes the sum over triples of units $(\epsilon_1, \epsilon_2, \epsilon_3)$ in U_K/U_K^2 so that at least one of $\epsilon_1\epsilon_2, \epsilon_1\epsilon_3$ or $\epsilon_2\epsilon_3$ do *not* satisfy the condition of lemma 14.

Given a pair (β, β_5), denote by $\mathbb{R}_{\beta,\beta_5}$ the number of even prime $\mathfrak{p}$ for which the following conditions are satisfied:

$$\begin{aligned} \langle -1, \beta_2 \rangle &= \prod_{\mathfrak{q}|2} \chi_{\mathfrak{q}}(\beta_2), \\ \chi_{\mathfrak{p}}(\beta_2\beta_3) &= \prod_{\mathfrak{q}|2} \left(\frac{\beta, \beta_2\beta_3}{\mathfrak{q}} \right) \prod_{\mathfrak{q}|2} \left(\frac{\beta_5, \beta_1\beta_3}{\mathfrak{q}} \right) \end{aligned}$$

Then, modulo the error terms, the sum (33) gives, *when A a unit*,

$$\frac{1}{2^{\omega_o(A-B)+\omega_0(B)+2+[K:\mathbb{Q}]}}\left(\sum_{\mathfrak{m}}1\right)\sum_{\epsilon_1,\epsilon_2,\epsilon_3}{}''\langle\epsilon_1,\epsilon_2\rangle\langle\epsilon_1,\epsilon_3\rangle\langle\epsilon_2,\epsilon_3\rangle\sum_{\beta,\beta_5}\mathbb{R}_{\beta,\beta_5}\langle\beta,\beta_5\rangle\left(\frac{A}{\mathfrak{b}\mathfrak{b}_5}\right)\left(\frac{-1}{\mathfrak{b}_5}\right)$$

This completes the calculation for case 4, and hence the proof of our theorem. □

References

1. A. Brumer. The average rank of elliptic curves. I. Invent. Math.. **108** pp. 445-472, 1992.
2. D. A. Burgess. *On character sums and L-series. II.* Proc. Lond. Math. Soc., III. Ser. 13. 1963.
3. D. R. Heath-Brown. *The size of Selmer groups for the congruent number problem.* Invent. Math. **111**. 1993.
4. D. R. Heath-Brown. *The size of Selmer groups for the congruent number problem. II.* Invent. Math. **118**. 1994.
5. G. Frey. W. Happle. Analytic rank of elliptic curves. Computer data. 1992.
6. D. Goldfeld. *Conjectures on elliptic curves over quadratic fields.* LNM 751 pp. 108-118. 1979.
7. F. Gouvea. B. Mazur. *The square-free sieve and the rank of elliptic curves.* J. AMS **4** (1991).
8. H. Montgomery. private communication.
9. W. Narkiewicz. *Elementary and Analytic Theory of Algebraic Numbers*, 2nd. Springer-Verlag, 1990.
10. K. Nagao. T. Kouya. *An example of elliptic curves over* $\mathbb{Q}$ *with rank* ≥ 21. Proc. Japan Acad. 70 (1994), 104-105.
11. O. T. O'Meara, *Introduction to quadratic forms.* Springer-Verlag, 1973.
12. J. H. Silverman, *The Arithmetic of Elliptic Curves.* Springer-Verlag, 1985.
13. C. L. Stewart, J. Top, *On ranks of twists of elliptic curves and power-free values of binary forms.* Preprint 1993.