Abstract. In this paper, we consider the average order of the 2-Selmer groups of elliptic curves over $\mathbb{Q}$ given by the equation $E : y^2 = x(x + a)(x + b)$, where $a$ and $b$ are integers. We show that, with $a$ being fixed, the average order of the 2-Selmer groups of such curves closely depends on $a$. More exactly, we show that the average order is bounded if $|a|$ is not a square and unbounded if $|a|$ is the square of an integer.

1. Introduction

For a given elliptic curve $E$ defined over $\mathbb{Q}$ possessing a 2-torsion point, we denote by $\text{Sel}_2(E/\mathbb{Q})$ the 2-Selmer group of $E$ over $\mathbb{Q}$. While it is known that the order of $\text{Sel}_2(E/\mathbb{Q})$ can be arbitrarily large (cf., [1], [11]), the study of its average value has attracted the attention of some authors. For instance, with purely analytic tools, Heath-Brown ([7], [8]) studied the congruent number curves and his results provide very good understanding on the distribution of the orders of 2-Selmer groups of the congruent number curves. In particular, the main results of [7], [8] imply the existence of a high ratio of rank 0 congruent number curves. In [14], we investigated the average order of the 2-Selmer groups of the elliptic curves over $\mathbb{Q}$ given by the equation

$$E(a, b) : y^2 = x(x + a)(x + b),$$

namely the curves over $\mathbb{Q}$ with 2-torsion $\mathbb{Z}_2 \times \mathbb{Z}_2$ (the so called generalized Frey-Hellegouarch curves). Motivated by a question posed by A. Brumer, we considered the sum

$$S(X) := \sum_{1 \leq |a|, |b| \leq X \atop a \neq b} \#\text{Sel}_2(E(a, b)).$$

Influenced by Heath-Brown’s approach to the problem in [7], by estimating character sums, we showed that there exists an absolute constant $c > 0$ such that

$$S(X) \leq cX^2.$$  

1991 Mathematics Subject Classification. 11G05, 14H52.

Key words and phrases. Elliptic Curves, 2-descent Procedure, Character Sums.
In other words, we proved that the average order of the 2-Selmer groups of curves given by (1.1) is bounded. This also implies that the average rank of the Mordell-Weil groups of these curves is bounded.

A natural question is to ask about the average order of \( \text{Sel}_2(E(a, b)) \) with one variable, say \( b \), varying over a certain interval. If one could show that the average order of the 2-Selmer groups of \( E(a, b) \) with \( b \) running over every interval of size between \( |a|^{1-\epsilon} \) and \( |a|^{1+\epsilon} \) was uniformly bounded as \( |a| \to \infty \), then (1.2) would be obviously true. Unfortunately, the average order of \( \text{Sel}_2(E(a, b)) \) in this sense depends on \( a \) quite complicatedly, and it is not possible to get a uniform estimate for \( b \) running over a that small interval. Moreover, even ignoring the uniformity, the expected boundedness may not hold always. For example, if contrasting two families of curves, the Legendre curves \( E(1, u) \) and curves \( E(2, u) \) with \( 1 < |u| \leq X \), one would be able to find out that, while the average order of \( \text{Sel}_2(E(2, u)) \) is absolutely bounded, the average order of \( \text{Sel}_2(E(1, u)) \) is unbounded with an order of magnitude \( \sqrt{\log X} \).

This seems mysterious, the secret, however, does not lie deep. The key difference between these two families of curves is that 1 is a square and 2 is not. For a given curve \( E(a, b) \), the order of \( \text{Sel}_2(E(a, b)) \) depends on the number of some special factorizations of \( a, b \) and \( a - b \). Roughly speaking, the closer \( |a|, |b| \) and \( |a - b| \) are to squares, or the fewer prime divisors \( ab(a - b) \) has, a higher ratio the admissible factorizations occupy in the factorizations. This heuristic explains why the average size of \( \text{Sel}_2(E(1, u)) \) differs from that of \( \text{Sel}_2(E(2, u)) \) significantly.

In this paper, we shall show that this phenomenon persists for any fixed \( a \), in accordance with whether \( |a| \) is a square or not. For a non-zero integer \( a \), and a positive number \( X \), let

\[
S(a; X) := \sum_{\substack{1 \leq |b| \leq X \\ b \neq a}} \#\text{Sel}_2(E(a, b)). \tag{1.3}
\]

In the case that \( |a| \) is not a square, we prove that the average order of \( \text{Sel}_2(E(a, b)) \) is bounded by a constant depending on \( a \).

**Theorem 1.1.** Suppose \( a \) is a fixed nonzero integer, \( |a| \) is not a square. Then there exist some positive constants \( c_1 \) and \( c_2 \), depending only on \( a \), such that for every \( X \geq 2 \) we have

\[
c_1 X < S(a; X) \leq c_2 X. \tag{1.4}
\]

The following corollary is an obvious consequence of Theorem 1.1.

**Corollary 1.2.** Suppose \( a \) is a fixed nonzero integer, \( |a| \) is not a square. Then the average Mordell-Weil rank of elliptic curves \( E(a, b) \) is bounded by a constant depending on \( a \).

When \( a = \pm d^2 \) for some integer \( d \), we expect a lower bound \( \sqrt{\log X} \) for the average order of the 2-Selmer groups of the curves \( E(\pm d^2, u) \) as \( |u| \) varies up to \( X \). One should note that, while the sum of \( S(\pm d^2; X) \) has a lower bound with order of magnitude \( X \sqrt{\log X} \), an explicit lower bound depends on \( d \). Not seeking for the best possible explicit constant, we shall prove
Theorem 1.3. Let $d$ denote an integer. Suppose $A > 0$ and $0 < \epsilon < 1$ are any fixed numbers. Then there exist constants $c_3 > 0$ and $X_0 > 0$, depending only on $A$ and $\epsilon$, such that, for every $X > X_0$, we have

$$S(\pm d^2; X) \geq c_3 \left( \frac{\phi(d)}{d} \right) \frac{3}{4} \cdot X^{\sqrt{\log X}}$$

if $|d| \leq (\log X)^A$, and

$$S(\pm d^2; X) \geq c_3 \left( \frac{\phi(d)}{d} \right) \frac{1}{2} \cdot X^{\sqrt{\log X}}$$

if $|d| \leq X^{1-\epsilon}$. Here and throughout, by $\phi(d)$ and $\omega(d)$ we denote respectively Euler’s totient function and the number of distinct prime divisors of $d$.

One may ask whether $X^{\sqrt{\log X}}$ gives the correct order of magnitude of $S(\pm d^2; X)$ for fixed $d$. In the same manner as we prove Theorem 1.1, we can prove an upper bound for $S(d^2; X)$, uniformly for $d$ relatively small with respect to $X$.

Theorem 1.4. Suppose $X > 3$ and $A > 0$ is any fixed real number. If $d \leq (\log X)^A$, then there exists a constant $c_4 > 0$, depending on $A$, such that

$$S(\pm d^2; X) \leq c_4 \left( \frac{d}{\phi(d)} \right)^5 \cdot X^{\sqrt{\log X}}.$$
s(n): the squarefree kernel of n, i.e., the largest squarefree integer dividing n.

$m \pmod {n}$ or $(\overline{m})_n$: (for $(m, n) = 1$) the inverse of $m$ modulo $n$, i.e., $m\overline{m} \equiv 1 \pmod {n}$.

$a \pmod {n}$: (in display) $a$ running over a complete residue system modulo $n$, i.e., $\mathbb{Z}/n\mathbb{Z}$.

$a \pmod {n^\times}$: (in display) $a$ running over the elements of $(\mathbb{Z}/n\mathbb{Z})^\times$.

Moreover, when used for the range of a variable involved in a sum, eg., $M < m \leq 2M$, a capital letter always stands for a power of 2.

**Remark:** In the proofs of the theorems, it often happens that, at a certain stage, we have to treat several similar cases (or estimate some similar sums). If the cases or sums can be treated in the same manner, we always only treat one of them to avoid unnecessary duplications. Besides, in complicated formulas, to shorten the display, we take it as a convention to leave out error terms that have smaller order of magnitude than the term(s) displayed.

## 2. Some Lemmas

In this section we state several lemmas which will be needed in the next sections.

**Lemma 2.1.** For integers $a, b$ satisfying $ab(a - b) \neq 0$, $(a, b) = 1$, and a squarefree integer $\Delta > 0$, the order of $\text{Sel}_2(E(a\Delta, b\Delta))$ is equal to the number of homogeneous spaces described by the quadratic equation systems

\[
\begin{align*}
& a'\delta_1 V^2 + \frac{b}{b'} \cdot \delta_4 W^2 = \delta_2 \nu X^2 \\
& b'\delta_1 V^2 + \frac{a}{a'} \cdot \delta_4 W^2 = \delta_3 \nu Y^2 \\
\end{align*}
\]

(2.1)

which possess a solution with $W \neq 0$ in every local field including $\mathbb{R}$, where $|a'|$, $|b'|$ and $\nu$ are respectively divisors of $|a|$, $|b|$ and $|a - b|$, $\Delta = \delta_1 \delta_2 \delta_3 \delta_4$, and both $|a'|\delta_1 \delta_2 \nu$ and $|b'|\delta_1 \delta_3 \nu$ are squarefree. Moreover, the number of such homogeneous spaces with $a'$ (or $b'$) having fixed sign is equal to $\frac{1}{2}\#\text{Sel}_2(E(a\Delta, b\Delta))$.

**Proof.** This is a consequence of the complete 2-descent (c.f., [12], pages 281 – 282). One can also refer to §2 of [14] for the detailed discussion or easily verify this by following the 2-descent carried out in [7]. For the last part, one can just proceed the 2-descent on $E(a\Delta, b\Delta)(\mathbb{Q})/\{O, T_2\}$ for a certain appropriate 2-torsion point $T_2$. □

**Lemma 2.2.** Suppose $\epsilon > 0$ is any fixed number, $X$, $M$ and $N$ are sufficiently large real numbers, and $\{a_m\}$ and $\{b_n\}$ are two complex sequences, supported on odd integers, satisfying $|a_m|$, $|b_n| \leq 1$. Fix positive integers $h$, $q$ satisfying $(h, q) = 1$ and $q \leq \{\min(M, N)\}^{\epsilon/3}$. Let

\[ S := \sum_{m, n} a_m b_n \left( \frac{m}{n} \right), \]

where the summation is subject to

\[ M < m \leq 2M, \quad N < n \leq 2N, \quad mn \leq X \quad \text{and} \quad mn \equiv h \pmod {q}. \]
Then we have
\[ S \ll MN^{\frac{15}{16} + \epsilon} + M^{\frac{15}{16} + \epsilon} N, \]
where the constant involved in the \( \ll \)-symbol depends on \( \epsilon \) only.

**Proof.** This is essentially Lemma 4 of [7], proved based on the work of Burgess [3]. One can also refer to Lemma 4.1 of [13]. \( \square \)

**Lemma 2.3.** Suppose \( s \) is a fixed positive integer. Let \( N \) be sufficiently large. Then for arbitrary positive integers \( q, r \) and any non-principal character \( \chi \pmod{q} \), we have
\[ \sum_{n \leq x, (n, r) = 1} \mu^2(n)s^{-\omega(n)}\chi(n)\ll x\tau(r)\exp(-\eta\sqrt{\log x}) \]  \hspace{1cm} (2.3)
with a positive constant \( \eta = \eta_{s,N} \), uniformly for \( q \leq \log^N x \).

**Proof.** This is Lemma 4.2 of [13]. \( \square \)

**Lemma 2.4.** Let \( s \) and \( C \) be two positive integers, \( A > 0 \) be any fixed number. For \( X > 1 \), let \( T \leq \exp(\sqrt{\log X}) \) and \( M, N \geq T \) be given. There exists some constant \( \eta > 0 \) such that, for any positive integer \( r \), any integer \( h \) prime to \( C \), and any distinct characters \( \chi_1, \chi_2 \pmod{q} \), where \( q \ll (\log X)^A \), we have
\[ \sum_{m,n} \mu^2(m)\mu^2(n)s^{-\omega(m)}-\omega(n)\chi_1(m)\chi_2(n) \ll \tau(r)X\exp(-\eta\sqrt{\log T})\log X \]  \hspace{1cm} (2.4)
where the sum is over coprime variables satisfying the conditions
\[ M < m \leq 2M, \quad N < n \leq 2N, \quad mn \leq X, \quad mn \equiv h \pmod{C}, \quad (mn, r) = 1, \]
and the constant involved in the \( \ll \)-symbol depends on \( s \) and \( C \) only.

**Proof.** This is just a little bit different from Lemma 10 of [7], where \( mn \) runs over an arithmetic progression modulo 8. Replacing the condition \( mn \equiv h \pmod{C} \) by introducing the summation
\[ \frac{1}{\phi(C)} \sum_{\chi \pmod{C}} \chi(m)\chi(n)\bar{\chi}(h) \]
as a factor to the sum, we see that, for every fixed \( \chi \pmod{C} \), at least one of \( \chi\chi_1 \) and \( \chi\chi_2 \) is non-principal. Then a direct application of (2.3) yields the Lemma. \( \square \)

In our applications, sometimes we require a more general version of Lemmas 2.3 and 2.4. More precisely, we need estimates similar to (2.3) and (2.4) with the summands involving some extra multiplicative factors.
Lemma 2.5. Assume all the conditions in Lemma 2.3. Suppose \( \alpha(n) \) is a multiplicative function satisfying that there exists a positive constant \( c \) such that, for every prime \( p \),

\[
|\alpha(p) - 1| < cp^{-1} \quad \text{and} \quad |\alpha(p^k)| < c + 1 \quad \text{for} \quad k \geq 2.
\]  

(2.5)

Then for arbitrary positive integers \( N \) and \( r \) there exists a positive constant \( \eta = \eta_{s,N} \) such that for every \( q \leq \log^N x \) and any non-principal character \( \chi \pmod{q} \), we have

\[
\sum_{n \leq x, (n,r)=1} \mu^2(n) s^{-\omega(n)} \alpha(n) \chi(n) \ll x \tau(r) \exp(-\eta \sqrt{\log x}),
\]  

(2.6)

with the constant involved in the \( \ll \)-symbol depending on \( c \) and \( s \) only.

Proof A proof of this lemma can be carried out by exactly the same method as used in the proof of Lemma 4.2 in [13]. For the generating function

\[
g(z) := \sum_{n=1, (n,r)=1}^{\infty} \frac{\mu^2(n) s^{-\omega(n)} \alpha(n) \chi(n)}{n^z},
\]

in a zero-free region of the L-function, we have the decomposition

\[
g(z) = \prod_{p|r} \left(1 + \frac{\chi(p)}{sp^z}\right)^{-1} G_1(z, \chi)L(z, \chi)^{\frac{1}{2}},
\]

where \( G_1(z, \chi) \) is analytic and absolutely convergent on \( \text{Re}(z) > \frac{3}{4} \). Then an application of Perron’s formula and estimates of Dirichlet L-functions yields (2.6). \( \square \)

Similarly, we have a generalization of Lemma 2.5.

Lemma 2.6. Suppose \( \alpha_1(m) \) and \( \alpha_2(n) \) are two multiplicative functions satisfying (2.5) for some fixed \( c \). Then, under all the conditions of Lemma 2.4, we have

\[
\sum_{m,n} \frac{\mu^2(m) \alpha_1(m) \chi_1(m)}{s^{\omega(m)}} \cdot \frac{\mu^2(n) \alpha_2(n) \chi_2(n)}{s^{\omega(n)}} \ll \tau(r)X \exp(-\eta \sqrt{\log T}) \log X,
\]  

(2.7)

where in the sum \( m \) and \( n \) are subject to the conditions given in Lemma 2.4, the constant involved in the \( \ll \)-symbol depending on \( c \), \( s \) and \( C \) only.

The next lemma deals with a special kind of sum. The estimate given here is required in the proof of Theorem 1.1.
Lemma 2.7. Suppose $a$ and $b$ are fixed non-zero integers and $b$ is not a square, $M$ and $N$ are sufficiently large real numbers satisfying
\[ N^{1/100} < M \leq \exp((\log N)^2). \tag{2.8} \]

Suppose $\alpha_1(n)$ and $\alpha_2(n)$ are multiplicative functions satisfying (2.5) for some constant $c > 0$. Let
\[ S(M, N) := \sum_{\substack{M < m \leq 2M \\ N < n \leq 2N \\ (mn, 2ab) = 1}} \mu^2(mn)\alpha_1(m)\alpha_2(n). \tag{2.9} \]

Then we have
\[ S(M, N) \ll \frac{MN}{\sqrt{\log M \log N}}, \tag{2.10} \]
where the constant involved in the $\ll$-symbol depends on $a$, $b$ and $c$.

Proof. We start from the fact that, for coprime integers $s$ and $t$, where $t$ is positive and odd, $s \equiv \square (\text{mod } t)$ if and only if
\[ 2^{-\omega(t)} \prod_{p | t} \left(1 + \left(\frac{s}{p}\right)\right) = 1, \]
which, when $t$ is squarefree, is equivalent to
\[ 2^{-\omega(t)} \sum_{d | t} \left(\frac{s}{d}\right) = 1. \]

Thus we have
\[ S(M, N) = \sum_{\substack{M < m \leq 2M \\ N < n \leq 2N \\ (m_1m_2n_1n_2, 2ab) = 1}} \mu^2(m_1m_2n_1n_2)\alpha_1(m_1m_2)\alpha_2(n_1n_2) \left(\frac{am_1m_2}{n_1}\right) \left(\frac{b}{m_1}\right). \tag{2.11} \]

Let $T := (\log N)^{49}$. We shall split the sum (2.9) into three parts according to the range of $n_2$: 1. $n_2 \leq \frac{N}{T}$; 2. $\frac{N}{T} < n_2 \leq N$; 3. $N < n_2 \leq 2N$.

We note that $\alpha_1(n)$ and $\alpha_2(n)$ are bounded by both $2^{\omega(n)}$ and $(\log \log n)^c$. From Lemma 2.2, the subsum subject to condition 1 is bounded by
\[ \sum_{n_2 \leq \frac{N}{T}} \frac{MN(\log \log M)^c}{n_2} \left( M^{-\frac{1}{10} + 10^{-3}} + \left(\frac{N}{n_2}\right)^{-\frac{1}{10} + 10^{-3}} \right) \ll \frac{MN}{(\log N)^2} \ll \frac{MN}{\sqrt{\log M \log N}}, \tag{2.12} \]
which is admissible for (2.10).

Noticing that, if \( n_1 \neq 1 \), \( \left( \frac{b}{n_1} \right) \) and \( \left( \frac{b}{n_1} \right) \) are both non-principal characters of conductor \( O(T) \), and that either the range of \( m_1 \) or the range of \( m_2 \) is \( \gg \exp(T^\epsilon) \), we conclude from Lemma 2.5 that the subsum subject to condition 2 is

\[
\ll \sum_{n_2 \leq N} \frac{\mu^2(n_2)|\alpha_2(n_2)|}{2^{\omega(n_2)}} \cdot \frac{N}{n_2} \cdot \tau(n_2)M \exp(-\eta \sqrt{\log M}) \ll \frac{MN(\log \log N)^{c+1}}{\exp(\eta \sqrt{\log M})}, \tag{2.13}
\]

which is more than enough.

For the subsum subject to condition 3, we note that the sum is actually

\[
\sum_{m \leq M} \mu^2(m)\alpha_1(m) \sum_{n \leq N} \frac{\mu^2(n)\alpha_2(n)}{2^{\omega(n)}}. \tag{2.14}
\]

From (2.5), we see that, in a zero-free region of \( \zeta(s) \), the generating function of the inner sum is of the form

\[
g(s) = \sqrt{\zeta(s)}h(s) \prod_{p \mid 2abm} \left( 1 + \frac{\alpha_2(p)}{2p^s} \right)^{-1},
\]

where \( h(s) \) is analytic and absolutely convergent in the half plane \( \Re(s) > \delta \) for any fixed \( \delta > 0 \). A standard application of Perron’s formula (see, for example, proof of Theorem 14.9 in [9]) yields

\[
\sum_{N < n \leq 2N} \frac{\mu^2(n)\alpha_2(n)}{2^{\omega(n)}} \ll \prod_{p \mid 2abm} \left( 1 + \frac{1}{2p} + \frac{c}{2p^2} \right) \frac{N}{\sqrt{\phi(m)}} \ll \left( \frac{m}{\phi(m)} \right)^{\frac{1}{2}} \frac{N}{\sqrt{\log N}}.
\]

(One should note that a condition on the comparison of the sizes of \( M \) and \( N \) (such as (2.8)) is necessary in estimating errors on the boundary of the contour integral.)

Thus, to show that the contribution from the subsum subject to the condition 3 is also admissible, it suffices to show that, for an arithmetic function \( \alpha(m) \) satisfying (2.5), and a sufficiently large \( M \), we have

\[
\sum_{m \leq M} \mu^2(m)\alpha_1(m) \ll \frac{M}{\sqrt{\log M}}. \tag{2.15}
\]

Let \( f(s) \) be the generating function of the sum in (2.15), then when \( \Re(s) > 1 \), we have

\[
f(s) = \prod_{p \mid 2a} \left( 1 + \frac{\alpha(p)}{p^s} \right) = \kappa(s) \prod_{p \mid 2} \left( 1 + \frac{1}{p^s} \right), \tag{2.16}
\]
where $k(s)$, depending on $a$ and $b$, is analytic and absolutely convergent on the half-plane $Re(s) > \delta$ for any fixed $\delta > 0$. Thus, for any squarefree $m$ satisfying $(m, 2ab) = 1$ and $b \equiv \square \pmod{m}$, we have
\[
\alpha(m) = \sum_{d|m} \gamma(d) \rho(m/d),
\]
where
\[
\gamma(d) = 1 \text{ if } b \equiv \square \pmod{d} \text{ and } \gamma(d) = 0 \text{ otherwise},
\]
and the arithmetic function $\rho(d)$ satisfies that, for any fixed $\delta > 0$ and $X \geq 1$
\[
\sum_{d \leq X} |\rho(d)| \ll X^\delta.
\]
(2.18)
From the classic result that
\[
\sum_{n \leq X} \gamma(n) \ll \frac{X}{\sqrt{\log X}},
\]
combining with (2.17) and (2.18), we have
\[
\sum_{m \leq M} \mu^2(m) \alpha(m) \ll \sum_{m \leq M} \gamma(m) \sqrt{\frac{M}{m}} = \sqrt{M} \int_2^M \frac{1}{\sqrt{t}} d \sum_{m \leq t} \gamma(m)
\]
\[
\ll \frac{M}{\sqrt{\log M}} + \sqrt{M} \int_2^M \frac{\sum_{m \leq t} \gamma(m)}{t^2} dt \ll \frac{M}{\sqrt{\log M}},
\]
as required. □

At last, we state the Bombieri-Vinogradov Theorem which we shall appeal to several times in the proof of Theorem 1.3. As usual, for fixed positive integers $a$ and $q$, $(a, q) = 1$, we write
\[
\psi(x; q, a) := \sum_{n \equiv a \pmod{q}} \Lambda(n) \quad \text{and} \quad E(x; q, a) := \psi(x; q, a) - \frac{x}{\phi(q)},
\]
Lemma 2.8. (The Bombieri-Vinogradov Theorem) Suppose $x > 3$, $\epsilon > 0$ is any fixed small real number, $Q = x^{1/2-\epsilon}$. Then for any $A > 0$, we have
\[
\sum_{q \leq Q} \max_{(a, q) = 1} \max_{y \leq x} |E(y; q, a)| \ll x(\log x)^{-A}
\]
(2.19)
the constant implied by the $\ll$-symbol depending only on $\epsilon$ and $A$.

Proof. This is actually a weaker form of Theorem 4 of Bombieri [2]. □
3. Proof of the first part of Theorems 1.3

We shall prove the Theorem for $S(d^2; X)$. Formally, there is some minor difference between the treatment for $d$ being odd and that for $d$ being even, but they are essentially the same. In the section, we shall only consider the case that $d$ is odd. The case with $d$ being even can be done in the same way. For an odd $d$, to get a lower bound, we shall only consider the curves given by the equation

$$E(d^2, 2u) : y^2 = x(x + d^2)(x + 2u),$$

where $1 \leq u \leq X/2$ is prime to $2d$, with $|2u - d^2|$ being squarefree.

From Lemma 2.1, we see that $\#\text{Sel}_2(E(d^2, 2u))$ is equal to the number of the quadratic equation systems

$$\left\{ \begin{array}{l}
u_0 V^2 + \frac{d^2}{f} W^2 = vZ^2 \\fV^2 + \frac{2u}{u_0} W^2 = vY^2 \end{array} \right. \quad (3.1)$$

that are everywhere locally solvable, where $|u_0|$ is a squarefree divisor of $2u$, $v$ is a positive divisor of $2u - d^2$ and $|f|$ is a squarefree divisor of $d$.

We shall only count the systems with $v = 1$, $f = 1$ and $u_0 \equiv 1 \pmod{8}$ being positive, which can be written as

$$\left\{ \begin{array}{l}
u_0 V^2 + d^2 W^2 = Z^2 \\V^2 + 2u_1 W^2 = Y^2, \end{array} \right. \quad (3.2)$$

where $u_1 = \frac{u}{u_0}$. One equivalent form of (3.2) is

$$\left\{ \begin{array}{l}(2u_0 u_1 - d^2) W^2 + Z^2 = u_0 Y^2 \\d^2 W^2 - Z^2 = -u_0 V^2. \end{array} \right. \quad (3.3)$$

Note for each curve $E(d^2, 2u)$, if only counting the systems (3.2) that are everywhere locally solvable, we sum up this part of $\#\text{Sel}_2(E(d^2, 2u))$ over $u$ then get a lower bound for $S(d^2; X)$. Heuristically, such a simplification is not harmful to the bound we are seeking, and the resulting lower bound will have the expected order of magnitude. For the systems (3.2), to be solvable in every $\mathbb{Q}_p$, it suffices to be solvable in $\mathbb{Q}_p$, with $p \mid 2du_0 u_1 (2u_0 u_1 - d^2)$.

We first note that the system (3.2) is always solvable in $\mathbb{Q}_2$ under the assumption $u_0 \equiv 1 \pmod{8}$. In fact, one can take $V = 1, W = 4$ and get the corresponding 2-adic unit solutions of $Y$ and $Z$.

If we write the two equations in (3.2) as $f(x, y) = 0$ and $g(x, y) = 0$ where $\{x, y\} \subset \{V, W, Y, Z\}$, then the Jacobian of the quadratic system $f(x, y) = g(x, y) = 0$, with respect to the possible choices of $(x, y)$, is respectively given by $4(2u_0 u_1 - d^2) VW, -4u_0 VY, 4VZ, -4d^2 WY, 8u_1 WZ$ and $4YZ$. If for $p \mid u_0 u_1 d(2u_0 u_1 - d^2), (V, W, Y, Z) \in \mathbb{F}_p$ is a solution of (3.2) in $\mathbb{F}_p$ with at most one of $\{V, W, Y, Z\}$ equal to 0, it is easy to see that at least one of the six possible Jacobians is not 0 in $\mathbb{F}_p$. Thus, from (a very special case of) Hensel’s Lemma, this solution of (3.2) in $\mathbb{F}_p$ can be lifted to a solution, say $(V_0, W_0, Y_0, Z_0) \in \mathbb{Z}_p^4$ with at most one of $V_0, W_0, Y_0$ and $Z_0$ being 0. Moreover, it is fairly easy to check that any
solution \( (V_0, W_0, Y_0, Z_0) \in \mathbb{Z}_p^4 \) of (3.2) in \( \mathbb{Z}_p \) with precisely one variable equal to 0 yields a solution \( (V_1, W_1, Y_1, Z_1) \in (\mathbb{Z}_p^\times)^4 \) of (3.2). (This can be achieved by replacing the 0 variable by \( p^k \) for a sufficiently large integer \( k \).)

Thus, for \( p \mid u_0 u_1 d(2u_0 u_1 - d^2) \), to determine whether a system (3.2) is “non-trivially” solvable in \( \mathbb{Q}_p \), it suffices to check whether this system (or a reduced equivalent one) has a “non-trivial” solution in \( \mathbb{F}_p \): a solution with at least three of the variables being non-zero in \( \mathbb{F}_p \).

We note that for any \( p \mid u_0 u_1 \), system (3.2) is always non-trivially solvable in \( \mathbb{F}_p \). For example, for \( p \mid u_0 \), note that \( V^2 + 2u_1 W^2 = Y^2 \) has \( p^2 \) solutions \( (V, W, Y) \in \mathbb{F}_p^3 \), \( 2p - 1 \) of which satisfy that \( W = 0 \), thus we always have a solution \( (V_0, W_0, Y_0) \in \mathbb{F}_p^3 \) for the equation with \( W_0 \neq 0 \). We must then have either \( V_0 \neq 0 \) or \( Y_0 \neq 0 \) (or both). Let \( Z_0 = dW_0 \), then we have a non-trivial solution \( (V_0, W_0, Y_0, Z_0) \in \mathbb{F}_p^4 \) of the system (3.2). Similarly, one can show that every system (3.2) is non-trivially solvable in \( \mathbb{F}_p \), if \( p \mid u_1 \).

For \( p \mid 2u_0 u_1 - d^2 \), we see that (3.3) is nontrivially solvable in \( \mathbb{F}_p \) if and only if \( \left( \frac{u_0}{p} \right) = 1 \) and, if this condition is satisfied, one can find a non-trivial solution \( (V_0, W_0, Y_0, Z_0) \in \mathbb{F}_p^4 \) of (3.3) with \( W_0 = 0 \) and \( V_0 Y_0 Z_0 \neq 0 \).

It is a little more complicated for \( p \mid d \). We consider this in two cases.

(I). \( \left( \frac{u_0}{p} \right) = 1 \)

In this case, it is easy to find a non-trivial solution of (3.2) in \( \mathbb{F}_p \) : \( W = 0, V = Y \neq 0 \) and \( Z = \gamma V \) where \( \gamma \) is a square root of \( u_0 \) in \( \mathbb{F}_p \).

(II). \( \left( \frac{u_0}{p} \right) = -1 \)

In this case, (3.2) can not be non-trivially solvable in \( \mathbb{F}_p \). However, if we suppose \( \text{ord}_p(d) = k \) and let \( d = p^k d_0 \), then the system

\[
\begin{aligned}
&u_0 V^2 + d_0^2 W^2 = Z^2 \\
p^{2k} V^2 + 2u_1 W^2 = Y^2
\end{aligned}
\]

is non-trivially solvable in \( \mathbb{F}_p \) if \( \left( \frac{2u_1}{p} \right) = 1 \). Thus, under this condition, this system is non-trivially solvable in \( \mathbb{Q}_p \). Moreover, a solution, say \( (V_0, W_0, Y_0, Z_0) \in (\mathbb{Z}_p^\times)^4 \) of this system gives a non-trivial solution \( (p^k V_0, W_0, Y_0, p^k Z_0) \) of (3.2) in \( \mathbb{Q}_p \).

It is also easy to check that (3.2) is solvable in \( \mathbb{Q}_p \) only if

\[
\left( \frac{u_0}{p} \right) = 1 \quad \text{or} \quad \left( \frac{2u_1}{p} \right) = 1,
\]

or, equivalently,

\[
\left( \frac{u_0}{p} \right) = 1 \quad \text{or} \quad \left( \frac{2u - d^2}{p} \right) = -1 \text{ for each prime } p \mid d.
\]

Therefore, (3.2) is non-trivially solvable in \( \mathbb{Q}_p \) for \( p \mid d \) if and only if (3.4) holds.
So from the discussion above we have

\[ \#\text{Sel}_2(E(d^2, 2u)) \geq \sum_{u_0 \mid u} * \mu^2(u_0), \tag{3.5} \]

where the asterisk indicates that (3.4) holds. By writing \( n := 2u - d^2 \), and introducing a function \( \alpha(d, u_0, n) \) defined by

\[ \alpha(d, u_0, n) := \prod_{p \mid d} \left( 1 - \frac{1}{4} \left( 1 - \left( \frac{u_0}{p} \right) \right) \left( 1 + \left( \frac{n}{p} \right) \right) \right), \]

we have, for sufficiently large \( X \), and any fixed \( 0 < \theta_2 < \theta_1 \leq 1 \)

\[ S(d^2; X) \geq \sum_{X^2 u_0 \leq X^3} \mu^2(u_0) \sum_{n \equiv d^2 \pmod{2u_0}} \mu^2(n) \alpha(d, u_0, n). \tag{3.6} \]

To split the condition \( u_0 \equiv \square \pmod{n} \) so that the inner sum of (3.6) is easier to be estimated, we count only those integers \( n \) with a large prime divisor, we shall write \( n = mp \) with \( p \) a large prime factor of \( n \). For any fixed \( 0 < \theta_3 < 1 \), from (3.6), we get

\[ S(d^2; X) \geq \sum_{X^2 u_0 \leq X^3} \mu^2(u_0) \sum_{m \leq X - d^2} \mu^2(m) \sum_{X/2m < p \leq X - d^2} \alpha(d, u_0, mp). \tag{3.7} \]

Note \( u_0 \equiv 1 \pmod{8} \), so we have

\[ \left( \frac{u_0}{p} \right) = \left( \frac{p}{u_0} \right) = \left( \frac{-d^2 m}{u_0} \right) = \left( \frac{m}{u_0} \right) = \left( \frac{u_0}{m} \right) = 1, \]

from the restriction that \( u_0 \equiv \square \pmod{m} \). So the condition \( \left( \frac{u_0}{p} \right) = 1 \) attached to the inner sum is automatically satisfied. We also note that

\[ \alpha(d, u_0, n) = 4^{-\omega(d)} \sum_{s(d) = d_1 d_2 d_3 d_4} 3^{\omega(d_1)}(-1)^{\omega(d_3)} \left( \frac{u_0}{d_2 d_4} \right) \left( \frac{n}{d_3 d_4} \right), \]
Thus, in the case \( d \leq (\log X)^{A} \), letting \( \theta_{1} = \frac{1}{3}, \theta_{2} = \frac{2}{5} \) and \( \theta_{3} = \frac{1}{24} \) (or any other appropriate choice for the values of \( \theta_{j}, j = 1, 2, 3 \)), we get

\[
S(d^{2} ; X) \geq \frac{1}{\log X} \sum_{X^{2/9} < u_{0} \leq X^{1/3}} \mu^{2}(u_{0}) \sum_{m \leq X^{1/24}} \mu^{2}(m) \sum_{(u_{0} , d) = 1 \atop (m, 2u_{0}d) = 1} \alpha(d, u_{0}, mk) \Lambda(k) + O \left( \sum_{u_{0} \leq X^{1/3}} \sum_{m \leq X^{1/24}} \sqrt{\frac{X}{m}} \right)
\]

\[
= \frac{1}{4^{\omega(d)}} \log X \sum_{s(d) = d_{1} d_{2} d_{3} d_{4}} 3^{\omega(d_{1})} (-1)^{\omega(d_{3})} \sum_{X^{2/9} < u_{0} \leq X^{1/3}} \mu^{2}(u_{0}) \left( \frac{u_{0}}{d_{2} d_{4}} \right) \sum_{X/2m < k \leq X/m} \frac{m}{d_{3} d_{4}} \Lambda(k) + O(X^{41/48}). \tag{3.8}
\]

As we shall see, the main term has order of magnitude \( \gg X(\log X)^{1/2-\epsilon} \) for any \( \epsilon > 0 \). Just for notational convenience, henceforth we will leave out all the error terms that are \( O(X) \).

For the inner sum of (3.8), we note that

\[
\sum_{X/2m < k \leq X/m} \left( \frac{k}{d_{3} d_{4}} \right) \Lambda(k) = \sum_{a \pmod{d_{3} d_{4}} \times} \left( \frac{a}{d_{3} d_{4}} \right) \sum_{X/2m < k \leq X/m} \Lambda(k) \tag{3.9}
\]

where for integer \( t \) prime to \( m \), \((m)_{t}\) indicates the inverse of \( m \) in \((\mathbb{Z}/t\mathbb{Z})^{\times}\). Now we write the inner sum of (3.8) as

\[
\frac{1}{\phi(2u_{0}d_{3} d_{4})} \left( \frac{X}{m} - \frac{X}{2m} \right) + E \left( \frac{X}{m} ; 2u_{0} d_{3} d_{4} , -d^{2} (m)_{2u_{0}} + 2au_{0} (2u_{0})_{d_{3} d_{4}} \right) - E \left( \frac{X}{2m} ; 2u_{0} d_{3} d_{4} , -d^{2} (m)_{2u_{0}} + 2au_{0} (2u_{0})_{d_{3} d_{4}} \right) \tag{3.10}
\]

\[
= \alpha_{1}(\vec{d}, a, m, u_{0}; X) + \alpha_{2}(\vec{d}, a, m, u_{0}; X) + \alpha_{3}(\vec{d}, a, m, u_{0}; X), \text{ say,}
\]

where we use a notation \( \vec{d} \) rather than \( d \) to indicate that the terms depend on the factorization of \( d \) described before.
By \( S_1(d^2; X) \), \( S_2(d^2; X) \) and \( S_3(d^2; X) \), we denote respectively the subsums of the last multiple sum in (3.7) corresponding to the three parts of the inner sum of (3.8), as described in (3.9). For the entire sum, we expect that the summand \( \alpha_1 \) contributes the main term while the others give error terms. We thus want to show that \( S_2(d^2; X) \) and \( S_3(d^2; X) \) are well bounded, but \( S_1(d^2; X) \) gives the major contribution. We shall use the Bombieri-Vinogradov Theorem (actually, a weaker form suffices) to bound the sums \( S_2(d^2; X) \) and \( S_3(d^2; X) \), and use a direct computation to deal with the sum \( S_1(d^2; X) \).

First for \( S_3(d^2; X) \), from Lemma 2.8, we have

\[
S_3(d^2; X) \ll \frac{d}{\log X} \sum_{m \leq X^{1/3}\log X} \sum_{a \equiv (\mod m)} \max \left| \psi\left( \frac{X}{2m}; w, a \right) - \frac{X/2m}{\phi(w)} \right|.
\]

With exactly the same estimate, we get

\[
S_2(d^2; X) \ll \frac{X}{(\log X)^3}.
\]

Note for odd integer \( q > 1 \),

\[
\sum_{a \equiv (\mod q)} \left( \frac{a}{q} \right) = 0,
\]

thus the terms of \( S_1(d^2; X) \) subject to \( d_3d_4 \neq 1 \) vanish. Hence

\[
S_1(d^2; X) = \frac{1}{4\omega(d) \log X} \sum_{s(d) = d_1d_2} 3^\omega(d_1) \sum_{X^{2/9} < u_0 \leq X^{1/3}} \mu^2(u_0) \left( \frac{u_0}{d^2} \right)
\]

\[
\sum_{m \leq X^{1/24}} \mu^2(m) \left( \frac{X}{m} - \frac{X}{2m} \right)
\]

\[
= \frac{X}{2\omega(d)^3 + 3 \log X} \sum_{s(d) = d_1d_2} 3^\omega(d_1) \sum_{m \leq X^{1/24}} \mu^2(m) \frac{m}{m^{2\omega(m)}}
\]

\[
\sum_{\chi_1 \equiv (\mod m)} \sum_{\chi_2 \equiv (\mod m)} \chi_1^2 = \chi_0 \chi_2 \equiv (\mod 8) \sum_{X^{2/9} < u_0 \leq X^{1/3}} \mu^2(u_0) \chi_1 \chi_2(u_0) \left( \frac{u_0}{d_2} \right),
\]

where, in the last step, an error of \( O\left( \frac{X}{\log X} \right) \) for a large \( B > 0 \) has been discarded.
For notational convenience, we denote \( \chi := \chi_1 \chi_2 (\frac{a}{4}) \) as a character modulo \( 8md_1d_2 \). Then from the simple fact that
\[
\frac{1}{\phi(u_0)} = \frac{1}{u_0} \sum_{s \mid u_0} \frac{\mu^2(s)}{\phi(s)},
\]
the innermost sum of (3.13) is equal to
\[
\sum_{s \leq (\log X)^2} \frac{\mu^2(s) \chi(s)}{s \phi(s)} \sum_{X^{2/9} / s < t \leq X^{1/3} / s} \frac{\mu^2(t) \chi(t)}{t} + O((\log X)^{-1})
\]
\[
= \sum_{s \leq (\log X)^2} \frac{\mu^2(s) \chi(s)}{s \phi(s)} \sum_{a \pmod{8msd_1d_2}} \chi(a) \sum_{X^{2/9} / s \leq t \leq X^{1/3} / s} \frac{\mu^2(t)}{t} + O((\log X)^{-1}).
\]
Note
\[
\sum_{X^{2/9} / s < t \leq X^{1/3} / s} \frac{\mu^2(t)}{t} = \sum_{h \leq X^{1/12}} \frac{\mu(h)}{h^2} \sum_{X^{2/9} / sh^2 < r \leq X^{1/3} / sh^2} \frac{1}{r} + O(\log X)
\]
\[
= \sum_{h \leq X^{1/12}} \frac{\mu(h)}{h^2} \cdot \left( \frac{\log X}{72msd_1d_2} + O\left( \frac{X^{2/9}}{X^{2/7}} \right) \right) + O(\log X)
\]
\[
= \frac{\log X}{72 \zeta(2) msd_1d_2} \prod_{p \mid 2msd_1d_2} \left( 1 - \frac{1}{p^2} \right)^{-1} + O(\log X).
\]
Here the error gives negligible contribution to the entire sum, and the main term of (3.15) vanishes when \( \chi \) is non-principal. Thus the terms that give major contribution are those subject to \( \chi_1 = \chi_0 \), \( \chi_2 = \chi_0 \) and \( d_2 = 1 \). Therefore, with our convention, we have, from
By Perron’s formula, it is easy to see that

\[
S_1(d^2; X) \geq \frac{X \phi(d)(\frac{3}{4})^{\omega(d)}}{144 \zeta(2)d} \sum_{m \leq X^{1/4} \atop (m,2d)=1} \frac{\mu^2(m)}{m^{2 \omega(m)}} \sum_{s \leq (\log X)^2 \atop (s,2md)=1} \frac{\mu^2(s)}{s^2} \cdot \frac{\phi(8sm \cdot s(d)) \log X}{72 \zeta(2)ms \cdot s(d)}
\]

(3.17)

for some absolute constant \(c > 0\). Therefore, (3.17) and (3.18), along with (3.11) and (3.12), yield that

\[
S(d^2; X) \geq c' \left( \frac{\phi(d)}{d} \right)^{\frac{1}{2}} \left( \frac{3}{4} \right)^{\omega(d)} \cdot X \sqrt{\log X},
\]

(3.19)

for some absolute constant \(c' > 0\). This proves the first part of Theorem 1.3.

4. Proof of the Second Part of Theorem 1.3

In this section, we let \(d \leq X^{1-\epsilon}\) for any fixed \(0 < \epsilon < 10^{-2}\). For the second part of Theorem 1.3, in considering the solvability of (3.2) in \(\mathbb{Q}_p\) with \(p \mid d\), we request \(\left( \frac{u_0}{p} \right) = 1\) instead of (3.4). This change results in a change of the factor \((\frac{3}{4})^{\omega(d)}\) in the coefficient by \((\frac{1}{2})^{\omega(d)}\). However, with this modification, we are able to treat the lower bound for larger values of \(d\). Following the discussion in the last section up to (3.7), we have

\[
S(d^2; X) \geq \frac{1}{\log X} \sum_{X^{\theta_2} < u_0 \leq X^{\theta_3} \atop \theta_1 < \frac{u_0}{8} \equiv 1 \pmod{8} \atop \theta_1 < \frac{u_0}{2d} \equiv 1 \pmod{d}} \mu^2(u_0) \sum_{m \leq X^{\theta_3} \atop (m,2ud)=1 \atop u_0 \equiv \Box \pmod{m}} \mu^2(m) \sum_{X/2m < k \leq X/m \atop k \equiv -d^2 \overline{m} \pmod{2u_0}} \Lambda(k).
\]

(4.1)

Throughout this section, let

\[
\theta_1 = \frac{1}{2}(1 - \epsilon^2) - \epsilon^3, \quad \theta_2 = \frac{1}{2}(1 - \epsilon^2) - 2\epsilon^3 \quad \text{and} \quad \theta_3 = \epsilon^2.
\]
Note then $2u_0 \leq 2X^{\theta_1} \leq (X/m)^{\frac{1}{2} - \epsilon_3}$. Estimate the error term by the Bombieri-Vinogradov Theorem as we did for the first case, then, apart from an error $O(X(\log X)^{-A})$, where $A > 1$ is a certain fixed number, we have

$$S(d^2; X) \geq \frac{1}{2\log X} \sum_{m \leq X^\theta_3} \frac{\mu^2(m)}{m} \sum_{u_0 \equiv 1 (\mod 8)} \sum_{u_0 \equiv \square (\mod d)} \frac{\mu^2(u_0)}{\phi(u_0)} \left( \frac{X - X}{2m} \right). \quad (4.2)$$

Thus we have

$$S(d^2; X) \geq \frac{X}{\log X} \sum_{m \leq X^\theta_3} \frac{\mu^2(m)}{m} \sum_{u_0 \equiv 1 (\mod 8)} \sum_{u_0 \equiv \square (\mod d)} \frac{\mu^2(u_0)}{\phi(u_0)} \left( \frac{X - X}{2m} \right) \quad (4.3)$$

$$\gg \sum_{U} \frac{X^{2-\omega(d)}}{\log X} \sum_{m \leq X^\theta_3} \frac{\mu^2(m)}{m^{2\omega(m)}} \sum_{\chi \bmod md} \sum_{\chi' \bmod 8} \frac{\mu^2(u_0)\chi\chi'(u_0)}{\phi(u_0)} \left( \frac{X - X}{2m} \right)^{u_0 \leq 2U}$$

where the constants involved in the $\ll$-symbols are absolute.

From (3.14), we see that, when $\chi' \neq \chi_0$, the innermost sum of (4.3) is equal to

$$\sum_{s \leq (\log X)^{10}} \frac{\mu^2(s)\chi'\chi'(s)}{\phi(s)} \sum_{U/s < t \leq 2U/s} \frac{\mu^2(t)\chi\chi'(t)}{\phi(t)} + O(U(\log X)^{-10}),$$

which, from the Polya-Vinogradov Theorem, is bounded by

$$\sum_{s \leq (\log X)^{10}} \frac{(mds)^{\frac{1}{2} + \epsilon_3}}{\phi(s)} + U(\log X)^{-10} \ll (md)^{\frac{1}{2} + \epsilon_3} + U(\log X)^{-10}.$$
Thus, apart from these admissible errors, we have

\[
S(d^2; X) \gg \sum_{X^{e_2} < U \leq U \leq X^{e_1}} \frac{X^2 - \omega(d)}{U \log X} \sum_{m \leq X^{e_3}} \frac{\mu^2(m)}{m^{2\omega(m)}} \sum_{U < u_0 \leq 2U} \frac{\mu^2(u_0)u_0}{\phi(u_0)} \sum_{(m, 2d) = 1} \frac{\mu^2(m)\phi(m)}{m^{2\omega(m)}}
\]

\[\gg 2^{-\omega(d)} \left( \frac{\phi(d)}{d} \right)^3 \cdot X \sqrt{\log X}.\]

And this finishes the proof of the second part of Theorem 1.

5. The Sum \(S(a; X)\)

For Theorem 1, since the lower bound is trivial, all we need to show is the upper bound. By a simple change of variables if necessary, we may assume \(a\) is positive. Moreover, for notational convenience, we shall only consider the curves \(E(a, b)\) with \(b\) being positive. The other part, namely, the sum over the curves \(E(a, b)\) with \(-X \leq b \leq -1\) can be treated in exactly the same manner, and the upper bound would be the same as well.

Every curve in consideration thus will be in the form of \(E(a, u\Delta)\), where every prime divisor of \(\Delta\) is a divisor of \(a\) and \(u\) is prime to \(a\). We note that, for \(a, b, c \in \mathbb{Z}, c \neq 0, E(a, b)\) and \(E(ac^2, bc^2)\) are \(\mathbb{Q}\)-isomorphic and have isomorphic 2-Selmer groups over \(\mathbb{Q}\). Thus, if one can show that the partial sum of \(S(a; X)\) with \((a, b) = \Delta\) for every squarefree integer \(\Delta \mid a\) is \(O_a(X)\), then one simply has the same upper bound for \(S(a; X)\). Therefore, we can consider only the curves \(E(a, u\Delta)\), with \(\Delta\) a fixed squarefree divisor of \(a\), \(u\) prime to \(a\).

From Lemma 2.1, we thus need to count the number of the quadratic equation systems

\[
\begin{align*}
\delta_1 u_0 V^2 + \frac{\alpha}{\delta_0} T^2 &= \delta_2 Y^2, \\
\delta_1 \alpha V^2 + \frac{u\Delta}{\delta_0 u_0} T^2 &= \delta_3 Z^2,
\end{align*}
\]

which are everywhere locally solvable, where \(\delta \mid \Delta, \delta = \delta_1 \delta_2 \delta_3, |\alpha| \mid a/\Delta, u_0\) and \(\beta\) are respectively positive squarefree divisors of \(u\) and \(u - a/\Delta\). Note the system (5.1) corresponds to the element \((a_1, b_1)\) of \(\text{Sel}_2(E(a, u\Delta))\) given by

\((a_1, b_1) = (u_0 \delta_1 \delta_2 \beta, \alpha \delta_1 \delta_3 \beta) \pmod{\mathbb{Q}^\times 2},\)

we thus suppose both \(u_0 \delta_1 \delta_2 \beta\) and \(|\alpha| \delta_1 \delta_3 \beta\) are squarefree. Let

\[
\frac{u - a/\Delta}{\beta} := h^2 \xi, \quad \frac{u}{u_0} := j^2 \rho,
\]

where \(\xi\) and \(\rho\) are squarefree. Then, it is necessary for an everywhere locally solvable system (5.1) to satisfy the following conditions.
AVERAGE SIZE OF 2-SELMER GROUPS

\[
\begin{cases}
-\alpha a\delta_2\delta_3 u_0 \equiv \square \pmod{\beta} \\
\alpha \beta a\delta_1 \delta_3 \equiv \square \pmod{u_0} \\
\alpha \beta \delta_1 \delta_3 \equiv \square \pmod{\rho} \\
\alpha \delta_2 \delta_3 u_0 \equiv \square \pmod{\xi}.
\end{cases}
\]

(5.2)

Since \(\Delta\) divides \(a\), there are \(O_a(1)\) choices for \(\delta_1, \delta_2\) and \(\delta_3\). Hence it suffices to show that for each fixed choice of \(\delta_1, \delta_2, \delta_3\) and \(\Delta\), the number of systems (5.2) which are everywhere locally solvable is \(O(X)\). Thus, in the next we shall let \(\Delta\) and \(\delta_i, i = 1, 2, 3\), be fixed.

We also note that, in some sense, \(\beta\) and \(\xi\), \(u_0\) and \(\rho\) are symmetric in pairs, so we will just consider the subsum of \(S(a; X)\) with \(\beta \leq \sqrt{X/\Delta h^2}\) and \(u_0 \leq \sqrt{X/\Delta j^2}\) and the resulting upper bound for this subsum serves as an upper bound of the whole sum. (If following our treatment for this partial sum, one can easily see that the same upper bound holds for the subsums left out.)

For simplicity, we write \(\kappa := -\alpha a\delta_2\delta_3; \mu := \alpha a\delta_1 \delta_3; \rho := \alpha \delta_1 \delta_3; \nu := \alpha \delta_2 \delta_3\).

Then, from (5.2) and with our convention, we have

\[
S(a; X) \ll \sum_{h,j} \sum_{u_0 \leq \sqrt{X/j}} \mu^2(u_0) \sum_{\beta \leq \sqrt{X/h}} \mu^2(\beta) \sum_{\substack{\kappa u_0 \equiv \square \pmod{h} \\ \mu \beta \equiv \square \pmod{u_0} \atop (\beta, u_0) = 1}} \mu^2(\xi)\mu^2(\rho).
\]

(5.3)

We note that, when \(2 | \beta\xi\) or \(2 | u_0\rho\), we can replace \(h^2\) and \(j^2\) by \(2h^2\) and \(2j^2\), and this does not affect our upper bound at all. Thus, without loss of generality, in the following all the variables \(\beta, u_0, \rho\) and \(\xi\) will be supposed to be odd integers and we will not specify this in computations.

We also note that there are at most \(O(\tau(m))\) ways to factor an integer \(m\) as \(m = j^2 u_0 \rho\) with \(u_0 \rho\) being squarefree. Thus the subsum of (5.3) subject to \(h > (\log X)^2\) is bounded by

\[
\sum_{h>(\log X)^2} \sum_{\beta \leq \sqrt{X/h}} \sum_{m \leq X/\Delta \atop m \equiv \frac{\xi}{\rho} \pmod{h^2\beta}} \tau(m).
\]

(5.4)

The partial sum of (5.4) with \(h > X^{\frac{1}{4}}\) is simply bounded by

\[
\ll \sum_{h > X^{\frac{1}{4}}} \sum_{\beta \leq \sqrt{\frac{X}{h^2 \beta}}} X^\epsilon \left(1 + \frac{X}{h^2 \beta}\right) \ll X^{\frac{\epsilon}{2} + 2\epsilon}.
\]

When \(h \leq X^{\frac{1}{4}}\), we have \(h^2 \beta \leq \left(\frac{X}{h}\right)^{3-\epsilon}\). From the well known result on the distribution of the divisor function over arithmetic progressions (see, for example, the introduction part of
the partial sum of (5.4) with \((\log X)^2 < h \leq X^{\frac{1}{4}}\) is bounded by

\[
\sum_{(\log X)^2 < h \leq X^{\frac{1}{4}}} \sum_{\beta \leq \sqrt{\frac{X}{h}}} \frac{1}{\Delta} \cdot \frac{X}{\log X} \ll X.
\]

Thus the subsum of (5.3) subject to \(h > (\log X)^2\) is \(O(X)\). Similarly, we can show that the subsum of (5.3) with \(j > (\log X)^2\) gives a contribution at most \(O(X)\) as well. Thus apart from this error (which is admissible for our estimate), it suffices to sum with respect to \(h\) and \(j\) up to \((\log X)^2\). We will split the sum on the right hand side of (5.3) into subsums \(S_1(a; X)\), say, with \(\beta = 1\) or \(u_0 = 1\) and \(S_2(a; X)\), say, with \(u_0 \neq 1\) and \(\beta \neq 1\), respectively, and give estimates separately. In the next two sections, we shall show that \(S_1(a; X)\) and \(S_2(a; X)\) are both bounded by \(O(X)\), and Theorem 1.1 will thus follow.

6. Estimate of \(S_1(a; X)\)

The treatments for the subsums respectively subject to \(\beta = 1\) and \(u_0 = 1\) are the same, and the same upper bound holds for the two sums. Thus, without loss of generality, we shall only consider the subsum with \(\beta = 1\). In the case \(\beta = 1\), the first congruence condition of (5.2) vanishes, and the last one is nontrivial for \(\xi\) (except possibly the case that \(\alpha \delta_2 \delta_3 u_0\) is a square which happens when either \(\alpha \delta_2 \delta_3\) is a square and \(u_0 = 1\) or \(a / \Delta\) is a square and \(u_0 = u / j^2\), both giving an admissible contribution). Note the assumption that \(a\) is not a perfect square guarantees that at least one of \(\alpha \delta_1 \delta_3\) and \(a \alpha \delta_1 \delta_3\) is not a square, thus at least one of the congruences is nontrivial. The treatment for the subsum under the assumption that \(\alpha \delta_1 \delta_3\) is not a square is similar to that for the subsum subject to \(a \alpha \delta_1 \delta_3\) being not a square. Hence, without loss of generality, we shall assume that \(\alpha \delta_1 \delta_3\) is not a square and shall use the third and the fourth congruences as the restrictions over the variables. (This is actually the more difficult case). Therefore, we have

\[
S_1(a; X) \ll \sum_{u_0 \leq \sqrt{X}} \mu^2(u_0) \sum_{h,j} \sum_{\substack{\xi, \rho \equiv 0 \pmod{\Delta} \\nu u_0 \equiv \Box \pmod{\rho}} \mu^2(\xi) \mu^2(\rho) + X
\]

\[
\ll \sum_{h,j \leq (\log X)^2} \sum_{u_0 \leq \sqrt{X}} \mu^2(u_0) \sum_{\substack{\rho \leq X/\sqrt{u_0 j^2} \\nu \equiv \Box \pmod{\rho} \\rho \equiv a \Box \pmod{\xi} \rho \equiv a \Box \pmod{\xi}}} \mu^2(\rho) + X,
\]

where the innermost sum is also subject to \(j^2 u_0 \rho - h^2 \xi = a / \Delta\).

To show \(S_1(a; X) \ll X\), we shall prove that, for some fixed non-zero integers \(a\), \(b\) and \(c\) where \(b\) is not a perfect square, and any integer \(d\) satisfying \(|d| \leq (\log X)^2\), and any \(N\) satisfying \(X / (\log X)^4 \ll N \ll X\),

\[
\tilde{S}_1(N) := \sum_{\substack{\sqrt{N}/(\log N)^2 < \rho \leq \sqrt{N} \\\rho \equiv \Box \pmod{\rho} \\rho \equiv \Box \pmod{\xi}}} \mu^2(\rho) \sum_{\substack{\xi \leq N \\xi \equiv d \pmod{\rho} \\xi \equiv \Box \pmod{\xi}}} \mu^2(\xi) \ll N.
\]

(6.2)
To see that (6.2) implies $S_1(a; X) \ll X$, we note that the summation over $h$ and $j$ is negligible and, under the assumption that $u_0 \asymp h^2\xi/j^2\rho \leq \sqrt{X}$, the contribution of the terms with $\rho \leq \sqrt{N}/(\log N)^4$ is small. Hence, in the following we shall devote to proving (6.2).

Let

$$\hat{E} := \exp(\sqrt{\log N}).$$

Then it is obvious that the subsum of $\hat{S}_I(N)$ subject to $N/\hat{E} < \rho \leq N$ gives upper bound $O(N)$. (We can use a simple bound $O(N\rho^{-1})$ for the inner sum of $\hat{S}_I(N)$ from (6.2), then by Perron’s formula to estimate the sum over $\rho$.) Thus,

$$\hat{S}_I(N) = \sum_{\rho \leq N/\hat{E}} \mu^2(\rho) \sum_{\xi \leq N} \mu^2(\xi) + O(N).$$  \hspace{1cm} (6.3)

By dividing the range of $\rho$ into dyadic intervals, we see that, to prove (6.2), it suffices to show that, for any $\sqrt{N}/(\log N)^2 \ll R \ll N/\hat{E}$,

$$\hat{S}_I(N, R) \ll \sum_{R < \rho \leq 2R} \mu^2(\rho) \sum_{\xi \leq N} \mu^2(\xi) \ll \frac{N}{\log N \log(N/R)},$$  \hspace{1cm} (6.4)

because then we have

$$\hat{S}_I(N) \ll \sum_R \frac{N}{\sqrt{\log N \log(N/R)}} + N \ll \frac{N}{\sqrt{\log N}} \sum_{\frac{1}{2} \log N < i \leq \frac{\log N - \sqrt{\log N}}{\log 2}} \frac{1}{\sqrt{\log N - i \log 2}} + N \ll N.$$  \hspace{1cm} (6.5)

Next, we write

$$\xi = kpK,$$

such that for a fixed positive constant $\epsilon < \frac{1}{100}$,

$$P(k) < p < p(K), \quad \text{and} \quad (N/R)^\epsilon < pk \leq p(N/R)^\epsilon.$$  \hspace{1cm} (6.6)

Then we have

$$\hat{S}_I(N, R) \ll \sum_{R < \rho \leq 2R} \mu^2(\rho) \sum_{\rho \equiv \square (\mod \rho)} \mu^2(k) \sum_{K \leq N/pk} 1.$$  \hspace{1cm} (6.7)
We split sum (6.7) into two parts: \( \hat{\sum}_1(N, R) \) for the subsum with \( p > (N/R)^2 \) and \( \hat{\sum}_2(N, R) \) for the other. The methods we shall use to estimate the two sums are essentially the same, but there will be some minor technical differences. We estimate \( \hat{\sum}_1(N, R) \) first.

- **Estimate of \( \hat{\sum}_1(N, R) \)**. For this special sum, let \( p \) be absorbed by \( K \), and we take away the Möbius functions and the \( p \)-smoothness restriction on \( k \). Then we see

\[
\hat{\sum}_1(N, R) \ll \sum_{R < \rho \leq 2R \atop (\rho, bc) = 1} \sum_{\substack{k \leq (N/R)^* \\ \rho \equiv a \square (mod k)}} \sum_{\substack{K \leq N/k \\ p(K) > (N/R)^2 \atop K \equiv cdk (mod \rho)}} 1
\]

Note that

\[
\frac{N}{kR} \gg \left( \frac{N}{R} \right)^{1-\epsilon},
\]

from a simple upper bound sieve (eg., [6, Theorem 2.2]), we have

\[
\hat{\sum}_1(N, R) \ll \sum_{R < \rho \leq 2R \atop (\rho, bc) = 1} \sum_{\substack{k \leq (N/R)^* \\ \rho \equiv a \square (mod k)}} \frac{N\rho}{Rk\phi(\rho) \log (N/R)}
\]

\[
\ll \frac{N}{R \log (N/R)} \sum_{R < \rho \leq 2R \atop (\rho, bc) = 1} \frac{\rho}{\phi(\rho)} \sum_{\substack{k \leq (N/R)^* \\ \rho \equiv a \square (mod k)}} \frac{1}{k}.
\]  

(6.9)

Note the subsum of the last formula in (6.9) subject to \( k \leq \exp(\sqrt{\log (N/R)}) \) is bounded by

\[
\frac{N}{R \sqrt{\log (N/R)}} \sum_{R < \rho \leq 2R \atop (\rho, bc) = 1} \frac{\rho}{\phi(\rho)} \ll \frac{N}{\sqrt{\log N \log (N/R)}},
\]

and from Lemma 2.7, the other is bounded by

\[
\frac{N}{R \log (N/R)} \sum_{\exp(\sqrt{\log (N/R)}) < 2^i \leq (N/R)^*} 2^{-i} \sum_{R < \rho \leq 2R \atop (\rho, bc) = 1} \frac{\rho}{\phi(\rho)} \sum_{\substack{2^i < k \leq 2^i+1 \\ \rho \equiv a \square (mod k)}} \frac{k}{\phi(k)}
\]

\[
\ll \frac{N}{R \log (N/R)} \sum_i \frac{1}{\sqrt{\log (2^i)}} \cdot \frac{R}{\sqrt{\log R}}
\]

\[
\ll \frac{N}{\sqrt{\log N \log (N/R)}}.
\]  

(6.10)
Therefore, we have shown that
\[
\hat{\Sigma}_I^1(N, R) \ll \frac{N}{\sqrt{\log N \log(N/R)}},
\]  
(6.11)
as desired.

- **Estimate of \( \hat{\Sigma}_I^2(N, R) \).** By a simple upper bound sieve, we have
\[
\hat{\Sigma}_I^2(N, R) \ll \sum_{\frac{R}{\rho} \leq 2R} \mu^2(\rho) \sum_{p \leq (N/R)^2} \sum_{\frac{(N/R)^s}{p} < k \leq (N/R)^s} \frac{\mu^2(k)}{\phi(p)} \sum_{\frac{P(k)}{\rho} < p} \sum_{\frac{P}{\rho} \equiv a \bar{a} \pmod{k}} \frac{1}{k}.
\]  
(6.12)

For the innermost sum in (6.12), we have
\[
\sum_{\frac{(N/R)^s}{p} < k \leq (N/R)^s} \frac{\mu^2(k)}{k} \ll \left( \frac{\log p}{\log N/R} \right)^2 \sum_{\frac{(N/R)^s}{p} < k \leq (N/R)^s} \frac{\mu^2(k)}{k}.
\]  
(6.13)

Hence, similar to the estimate of (6.10), an application of Lemma 2.7 yields
\[
\hat{\Sigma}_I^2(N, R) \ll \frac{N}{\log(N/R)^2} \sum_{p \leq (N/R)^2} \frac{\log p}{\log N/R} \sum_{\frac{R}{\rho} \leq 2R} \mu^2(\rho) \sum_{\frac{P}{\rho} \equiv a \bar{a} \pmod{k}} \mu^2(k) \sum_{\frac{P(k)}{\rho} < p} \sum_{\frac{P}{\rho} \equiv a \bar{a} \pmod{k}} \frac{1}{k}.
\]  
(6.14)

In view of (6.4) and (6.5), (6.11) and (6.14) together yield
\[
\hat{S}_I(N) \ll N,
\]  
(6.15)

which, along with our discussion in the very beginning of this section, implies that
\[
S_1(a; X) \ll X.
\]  
(6.15)
7. Estimate of $S_2(a; X)$

We set

$$\hat{F} := \exp((\log X)^\frac{1}{6}).$$  \hspace{1cm} (7.1)

Let $S_2(a; X)$ be the subsum of (5.3) subject to $u_0, \beta > \hat{F}$ and $u_0\beta \leq X/\hat{F}$, and $S_{22}(a; X)$ for the other, both also with conditions that $u_0 > 1$ and $\beta > 1$.

- **Estimate of $S_{21}(a; X)$**. We divide the ranges of $u_0$ and $\beta$ into dyadic intervals. Note that $h$ and $j$ play a negligible role in the summation, we will just estimate, for fixed $h, j \leq (\log X)^2$, and $\hat{F} < U, B \leq \sqrt{X}/\hat{F}$,

$$\hat{\Sigma}_{21} := \sum_{U < u_0 \leq 2U} \mu^2(u_0) \sum_{B < \beta \leq 2B} \mu^2(\beta) \sum_{\kappa u_0 \equiv \square \pmod{\beta}, \mu \beta \equiv \square \pmod{u_0}, \nu u_0 \equiv \square \pmod{\beta}} \mu^2(\xi)\mu^2(\rho),$$

where, in the inner sum, $\xi$ and $\rho$ also satisfy $\rho \leq X/u_0 j^2$ and $j^2u_0\rho - h^2\beta\xi = a/\Delta$.

We note that, to show that $S_{21}(a; X) \ll X$, it suffices to show that

$$\hat{\Sigma}_{21} \ll a X (hj)^{1+\delta} \sqrt{\log B \log U \log(X/UB)}$$

for some $\delta > 0$. Now for a fixed $0 < \epsilon < 10^{-10}$, we write

$$\rho = npN \quad \text{and} \quad \xi = mqM,$$

where $p$ and $q$ are prime,

$$P(n) < p < p(N), \quad P(m) < q < p(M),$$

and

$$\left( \frac{X}{UB} \right)^\epsilon < np \leq p \left( \frac{X}{UB} \right)^\epsilon, \quad \left( \frac{X}{UB} \right)^\epsilon < mq \leq q \left( \frac{X}{UB} \right)^\epsilon. \hspace{1cm} (7.6)$$

Without loss of generality, we may only estimate the subsum subject to $p < q$, which will be further divided into two parts: $\hat{\Sigma}_{211}$ subject to $p > \left( \frac{X}{UB} \right)^\epsilon^2$, and $\hat{\Sigma}_{212}$ subject to $p \leq \left( \frac{X}{UB} \right)^\epsilon^2$.

**Estimate of $\hat{\Sigma}_{211}$**. In (7.4), let $p$ and $q$ be absorbed by $N$ and $M$, respectively, then we have

$$\hat{\Sigma}_{211} \ll \sum_{U < u_0 \leq 2U} \mu^2(u_0) \sum_{B < \beta \leq 2B} \mu^2(\beta) \sum_{m,n \leq \left( \frac{X}{UB} \right)^\epsilon} \mu^2(mn) \sum_{M,N} 1,$$

(7.7)
where, in the innermost sum, $M$ and $N$ are subject to

$$j^2u_0nN - h^2\beta m M = a/\Delta,$$  \hspace{1cm} (7.8)

and

$$p(MN) > \left(\frac{X}{UB}\right)^{\epsilon^2}.$$  \hspace{1cm} (7.9)

Note from (7.8), we can write $M$ and $N$ as two linear forms $l_1$ and $l_2$ of a single variable, say $k$. The two linear forms respectively have leading coefficients $j^2u_0n$ and $h^2\beta m$, and thus the variable $k$ is running up to at most $\frac{X}{\Delta(hj)^2u_0\beta mn}$. Applying a 2-dimensional upper bound sieve (e.g., [6, Theorem 2.2]), the innermost sum of (7.7) is bounded by

$$\frac{X}{\Delta \phi((hj)^2u_0\beta mn)(\log(X/UB))^2},$$

and so $\hat{\Sigma}_{211}$ is bounded by

$$\frac{X(\log(X/UB))^{-2}}{\Delta \phi((hj)^2)} \sum_{U < u_0 \leq 2U} \frac{\mu^2(u_0)}{\phi(u_0)} \sum_{B < \beta \leq 2B} \frac{\mu^2(\beta)}{\phi(\beta)} \sum_{m,n \leq \left(\frac{X}{\sqrt{\log U}}\right)^*} \frac{\mu^2(mn)}{\phi(mn)}. \hspace{1cm} (7.10)$$

Thus, to be admissible for (7.3), it suffices to show that

$$\sum_{U < u_0 \leq 2U} \frac{\mu^2(u_0)}{\phi(u_0)} \sum_{B < \beta \leq 2B} \frac{\mu^2(\beta)}{\phi(\beta)} \sum_{m,n \leq \left(\frac{X}{\sqrt{\log U}}\right)^*} \frac{\mu^2(mn)}{\phi(mn)} \ll \frac{\log(X/UB)}{\sqrt{\log U \log B}}. \hspace{1cm} (7.11)$$

We see that, by reforming the congruence restrictions, it suffices to show that $\frac{\log(X/UB)}{\sqrt{\log U \log B}}$ is an upper of the following sum

$$\sum_{U < u_1u_2 \leq 2U} \sum_{B < b_1b_2 \leq 2B} \phi(u_1u_2b_1b_2)2^{\omega(u_1u_2b_1b_2)} \sum_{m_1m_2 \leq \left(\frac{X}{\sqrt{\log U}}\right)^*} \frac{(nu_1u_2m_1)(ob_1b_2n_1)}{\phi(m_1m_2n_1m_2)2^{\omega(m_1m_2n_1m_2)}}, \hspace{1cm} (7.12)$$

where all the variables are odd, squarefree and coprime in pairs.

Let $T := (\log X)^{1000}$.

Then, from Lemma 2.2, it can be seen that any subsum subject to one of the following conditions gives a negligible contribution.
(1). range of \( m_1 \) longer than \( T \);
(2). range of \( n_1 \) longer than \( T \);
(3). both \( b_1 \) and \( u_2 \) have ranges longer than \( T \);
(4). both \( b_2 \) and \( u_1 \) have ranges longer than \( T \).

Therefore, to finish estimating \( \hat{\Sigma}_{211} \), it suffices to show that \( \log(X/UB) / \sqrt{\log U \log B} \) is an upper of two sums \( \hat{\Sigma}_{211}^\alpha \) and \( \hat{\Sigma}_{211}^\beta \), respectively given by

\[
\sum_{u_1, b_1 \leq T} \sum_{b \leq \frac{2U}{b_1}} \frac{(\kappa u_1 u_2)(\mu b_2)}{\phi(u_1 u_2 b_1 b_2) 2^\omega(u_1 u_2 b_1 b_2)} \sum_{m_1, n_1 \leq \nu} \frac{(\nu u_1 u_2)}{\phi(m_1 m_2 n_1 n_2) 2^\omega(m_1 m_2 n_1 n_2)},
\]

and

\[
\sum_{u_2, b_2 \leq T} \sum_{b \leq \frac{2U}{b_2}} \frac{(\kappa u_1 u_2)(\mu b_2)}{\phi(u_1 u_2 b_1 b_2) 2^\omega(u_1 u_2 b_1 b_2)} \sum_{m_1, n_1 \leq \nu} \frac{(\nu u_1 u_2)}{\phi(m_1 m_2 n_1 n_2) 2^\omega(m_1 m_2 n_1 n_2)},
\]

where in both sums, all the variables are odd, squarefree and coprime in pairs.

To estimate \( \hat{\Sigma}_{211}^\alpha \), we sum over \( u_2 \) first. When \( m_1 b_1 \neq 1 \), Lemma 2.5 implies that the inner sum over \( u_2 \) is

\[
\sum_{u_2, b_2 \leq T} \sum_{b \leq \frac{2U}{b_2}} \frac{\mu^2(u_2)(\frac{u_2}{m_1 b_1})}{\phi(u_2) 2^\omega(u_2)} \ll \tau(b_2 m_2 n_1 n_2 u_1)(\log X)^{-4},
\]

which yields that the terms with \( m_1 b_1 \neq 1 \) contribute to \( \hat{\Sigma}_{211}^\alpha \) at most

\[
\ll (\log X)^{-4} \sum_{u_1, b_1, b_2, m_1, m_2, n_1, n_2} \frac{1}{\phi(u_1 b_1 b_2 m_1 m_2 n_1 n_2)} \ll (\log X)^{-4}(\log X)^2(\log T)^4 \ll (\log X)^{-1},
\]

which is admissible. Similarly, by summing over \( b_2 \) first, those terms with \( n_1 u_1 \neq 1 \) contribute negligible errors to \( \hat{\Sigma}_{211}^\alpha \) too. Therefore, we essentially have

\[
\hat{\Sigma}_{211}^\alpha \ll \sum_{U \leq u_2 \leq 2U} \sum_{B \leq b_2 \leq 2B} \frac{1}{\phi(u_2 b_2) 2^\omega(u_2 b_2)} \left( \sum_{m \leq \frac{X}{T^2}} \frac{1}{\phi(m) 2^\omega(m)} \right)^2 \ll \frac{\log(X/UB)}{\sqrt{\log U \log B}},
\]

as required.
The estimate of $\hat{\Sigma}_{211}$ is similar. Instead of using Lemma 2.5, we use Lemma 2.6 and get the same upper bound as for $\hat{\Sigma}_{211}$.

Thus, from the discussions after (7.10), we have shown that

$$\hat{\Sigma}_{211} \ll \frac{X}{\Delta \phi((hj)^2) \sqrt{\log B \log U \log(X/UB)}},$$

which agrees to (7.3).

**Estimate of $\hat{\Sigma}_{212}$**. We may closely follow the estimate of $\hat{\Sigma}_{211}$. First we have $q$ absorbed by $M$ in (7.4). Then following the argument from (7.7) -- (7.10), we see that $\hat{\Sigma}_{212}$ is bounded by

$$X \Delta \phi((hj)^2) \sum_{U < u_0 \leq 2U} \frac{\mu^2(u_0 \beta)}{\phi(u_0 \beta)} \sum_{\substack{p \leq (\frac{X}{\sqrt{U}})^2 \phi(n) 2^{\omega(n)}}} \sum_{m \leq (\frac{X}{\sqrt{U}})^\epsilon} \frac{\mu^2(mn)}{\phi(mn)}.\tag{7.17}$$

Now, by exactly the same methods as used from (7.12) through (7.15) and the idea used in (6.13), apart from some small errors, we see that $\hat{\Sigma}_{212}$ is bounded by

$$X \Delta \phi((hj)^2) \sum_{U < u_2 \leq 2U} \frac{1}{\phi(u_2 b_2) 2^{\omega(u_2 b_2)}} \sum_{m \leq (\frac{X}{\sqrt{U}})^\epsilon} \frac{1}{\phi(m) 2^{\omega(m)}} \sum_{\substack{p \leq (\frac{X}{\sqrt{U}})^2 \phi(n) 2^{\omega(n)}}} \frac{1}{p(\log p)^2} \sum_{\substack{P(n) < p \phi(n) \equiv \Box \pmod{m} \nu u_0 \equiv \Box \pmod{m}}} \left(\frac{\chi}{\sqrt{U}}\right)^- n \leq \left(\frac{\chi}{\sqrt{U}}\right)^\epsilon \left(\frac{\log p}{\log(X/UB)}\right) \sum_{n' \leq (\frac{X}{\sqrt{U}})^\epsilon} 2^{-\omega(n')} \frac{1}{\phi(n')},\tag{7.18}$$

which is what we wanted. Together with the estimate (7.16), this yields

$$S_{21}(a; X) \ll X.$$

**Estimate of $S_{22}(a; X)$**. We split $S_{22}(a; X)$ into two parts: $S_{221}(a; X)$ subject to $u_0, \beta > \sqrt{X/\hat{F}}$ and $S_{222}(a; X)$ subject to $u_0$ or $\beta \leq \hat{F}$. 
For $S_{221}(a; X)$, we simply discard three congruences in (5.3) and, compared with (7.2), we get

$$S_{221}(a; X) \ll \sum_{h,j} \sum_{\sqrt{X}/F < u_0 \leq \sqrt{X}/j} \mu^2(2u_0\beta) \sum_{\xi,\rho} 1 \ll \sum_{h,j} \sum_{\sqrt{X}/F < u_0 \leq \sqrt{X}/j} \mu^2(2u_0\beta) \left(1 + \frac{X}{\Delta(hj)^2u_0\beta}\right)$$

(7.19)

where the two sums $\Sigma'_{221}$ and $\Sigma''_{221}$ are respectively subject to the summands $1$ and $\frac{X}{\Delta(hj)^2u_0\beta}$. The estimates of these two sums are quite easy. First we note

$$\Sigma'_{221} \ll \sum_{h,j} \sum_{\sqrt{X}/F < u_0 \leq \sqrt{X}/j} \mu^2(2u_0\beta) \Omega^2(u_0\beta) \left(\sum_{\kappa u_0 \equiv \Box \pmod{\beta}} \right)$$

(7.20)

We consider the sum in accordance with the size of $\beta_1$.

(1). $\beta_1 > (\log X)^{100}$; both of the ranges of $u_0$ and $\beta_1$ are longer enough to imply a factor $(\log X)^{-5}$ by appealing to Lemma 2.2. Thus the contribution of this part is at most $O(X(\log X)^{-4})$.

(2). $1 < \beta_1 \leq (\log X)^{100}$; summing over $u_0$ first, we see the contribution is $O(X(\log X)^{-c})$ for any fixed $c > 0$.

(3). $\beta_1 = 1$; this gives the largest contribution, which is

$$\ll \sum_{h,j} \sum_{\sqrt{X}/F < u_0 \leq \sqrt{X}/j} 2^{-\omega(\beta)} \ll \sum_{h,j} \frac{X(\log X)^{-\frac{1}{2}}}{hj} \ll X(\log X)^{-\frac{1}{2}}.$$ 

(7.21)

From the above discussions, we thus have

$$\Sigma'_{221} \ll X(\log X)^{-\frac{1}{4}}.$$ 

(7.22)

For $\Sigma''_{221}$, by dividing the ranges into dyadic intervals and applying same argument as that for $\Sigma'_{221}$, we can easily see

$$\Sigma''_{221} \ll X(\log X)^{-\frac{3}{4}}.$$ 

(7.23)

Therefore, we have shown that the

$$S_{221}(X) \ll X(\log X)^{-\frac{1}{2}}.$$ 

(7.24)
For $S_{222}(a; X)$, we let
\[
\Omega := \exp\left(\frac{\log X}{(\log \log X)^{\frac{1}{2}}}\right), \quad \text{and} \quad \Phi := \Phi(\Omega) = \Omega^{100(\log \log X)}.
\]
(7.25)

First we note
\[
S_{222}(a; X) \ll \sum_{u_0, \beta} \mu^2(2u_0\beta) \sum_{\xi,\rho} \mu^2(\xi)\mu^2(\rho),
\]
(7.26)
where in the inner sum $\xi, \rho$ also satisfy $\rho \leq X/u_0j^2$ and $j^2u_0\rho - h^2\beta\xi = a/\Delta$. Now we write
\[
\rho := nN \quad \text{and} \quad \xi := mM,
\]
(7.27)
with $mn$ being $\Omega$-smooth and $p(MN) > \Omega$. Then, apart from some very small error terms
\[
S_{222}(a; X) \ll \sum_{h,j} \sum_{\kappa_0,\beta} \mu^2(2u_0\beta) \sum_{\mu,\nu} \mu^2(mn) \sum_{M, N} 1,
\]
(7.28)
where in the inner sum $M$ and $N$ satisfy $nN \leq X/u_0j^2$, $j^2u_0nN - h^2\beta mM = a/\Delta$ and $p(MN) > \Omega$. By writing $M$ and $N$ in the form of two linear forms and appealing to a 2-dimensional upper bound sieve, we get, from (7.28),
\[
S_{222}(a; X) \ll \frac{X}{(\log \Omega)^{\frac{1}{2}}} \sum_{1 < u_0, \beta \leq \sqrt{X}} \frac{\mu^2(2u_0\beta)}{\phi(u_0\beta)} \sum_{1 < u_0, \beta \leq \sqrt{X}} \frac{\mu^2(mn)}{\phi(mn)}
\]
\[
\ll \frac{X(\log \log X)^7}{(\log X)^2} \sum_{\kappa_0,\beta} \frac{\mu^2(2u_0\beta)}{u_0\beta} \sum_{\mu,\nu} \frac{\mu^2(mn)}{mn}.
\]
(7.29)

Note all the fixed variables $\kappa, \mu, \varrho, \nu$ have no specific effects here, $u_0$ and $\beta$ are essentially symmetric. So we shall just consider the subsum with $1 < u_0 \leq \hat{F}$, which is bounded by
\[
\frac{X(\log \log X)^7}{(\log X)^2} \sum_{1 < \beta \leq (\log X)^{100}} \frac{\mu^2(2u_0\beta)}{u_0\beta} \sum_{\mu,\nu} \frac{\mu^2(mn)}{mn}
\]
\[
+ \frac{X(\log \log X)^7}{(\log X)^2} \sum_{\kappa_0,\beta} \frac{\mu^2(2u_0\beta)}{u_0\beta} \sum_{\mu,\nu} \frac{\mu^2(mn)}{mn}.
\]
(7.30)
The first sum in (7.30), from applying Perron’s formula and zero-free region of $L$-functions, is simply bounded by
\[
\frac{X(\log \log X)^7}{(\log X)^2} \sum_{1 < \beta \leq (\log X)^{100}} \frac{\mu^2(2u_0\beta)}{u_0\beta} \cdot (\log \Phi)^{\frac{3}{2}} \leq \frac{X(\log \log X)^7}{(\log X)^2} \cdot \log \hat{F} \cdot \log \log X \cdot (\log \Phi)^{\frac{3}{2}} \ll \frac{X(\log \log X)^9}{(\log X)^{\frac{3}{2}}},
\] (7.31)
which is admissible for our requirement.

By reforming the congruences attached to the innermost sum, the second sum in (7.30) can be rewritten as
\[
\frac{X(\log \log X)^7}{(\log X)^2} \sum_{1 < u_0 \leq \hat{F}} \frac{\mu^2(2u_0\beta)}{u_0\beta} \sum_{m,n \leq \Phi} \frac{\mu^2(mn)}{mn2^\omega(mn)} \sum_{\kappa \equiv 0 \mod u_0} \left( \frac{\nu u_0}{m_1} \right) \left( \frac{\rho \beta}{n_1} \right). \quad (7.32)
\]
Then from Lemma 2.2 and Perron’s formula, combining with the zero-free region of $L$-functions, this is
\[
\ll \frac{X(\log \log X)^7}{(\log X)^2} \sum_{1 < u_0 \leq \hat{F}} \frac{\mu^2(2u_0\beta)}{u_0\beta} \sum_{m,n \leq \Phi} \frac{\mu^2(mn)}{mn2^\omega(mn)} \sum_{\kappa \equiv 0 \mod u_0} \left( \frac{\nu u_0}{m_1} \right) \left( \frac{\rho \beta}{n_1} \right) \ll \frac{X(\log \log X)^8}{(\log X)^{\frac{3}{2}}}. \quad (7.33)
\]
Hence, from (7.29) – (7.33), we have shown that
\[
S_{222}(a; X) \ll X(\log X)^{-\frac{1}{6}}, \quad (7.34)
\]
along with (7.24), which implies that
\[
S_{22}(a; X) \ll X(\log X)^{-\frac{1}{2}}. \quad (7.35)
\]
Therefore, we have proved that
\[
S_2(a; X) \ll X. \quad (7.36)
\]
Acknowledgements

The author is grateful to the anonymous referee for many helpful comments and suggestions.

REFERENCES

14. ______, Average size of 2-Selmer groups of a family of elliptic curves, to appear in the Transactions of AMS.