ACTA ARITHMETICA
117.1 (2005)

Average size of 2-Selmer groups of elliptic curves, II

by

Gang Yu (Ann Arbor, MI)

1. Introduction. For a given elliptic curve E defined over $\mathbb{Q}$ possessing a 2-torsion point, we denote by $\mathrm{Sel}_2(E/\mathbb{Q})$ the 2-Selmer group of E over $\mathbb{Q}$. While it is known that the order of $\mathrm{Sel}_2(E/\mathbb{Q})$ 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 of the distribution of the orders of 2-Selmer groups of such curves. In particular, the main results of [7], [8] imply the existence of a positive proportion 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

$$E(a,b):\ y^2 = x(x+a)(x+b), \tag{1.1}$$

that is, 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

$$S(X) := \sum_{\substack{1\le|a|,|b|\le X\\ a\ne b}} \#\,\mathrm{Sel}_2(E(a,b)).$$

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

$$S(X) \le cX^2. \tag{1.2}$$

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.

2000 *Mathematics Subject Classification*: 11L40, 14H52.
Key words and phrases: elliptic curves, 2-descent procedure, character sums.

A natural question to ask is about the average order of $\mathrm{Sel}_2(E(a,b))$ 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 $|a|^{1-\varepsilon}$ and $|a|^{1+\varepsilon}$ was uniformly bounded as $|a| \to \infty$, then (1.2) would be obviously true. Unfortunately, the average order of $\mathrm{Sel}_2(E(a,b))$ in this sense depends on a quite complicatedly, and it is not possible to get a uniform estimate for b running over that small interval. Moreover, even ignoring the uniformity, the expected boundedness may not always hold. For example, considering the Legendre curves $E(1,u)$ and curves $E(2,u)$ with $1 < |u| \le X$, one finds out that, while the average order of $\mathrm{Sel}_2(E(2,u))$ is absolutely bounded, the average order of $\mathrm{Sel}_2(E(1,u))$ 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 $\mathrm{Sel}_2(E(a,b))$ 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 all the factorizations. This heuristic explains why the average size of $\mathrm{Sel}_2(E(1,u))$ differs from that of $\mathrm{Sel}_2(E(2,u))$ 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

$$S(a;X) := \sum_{\substack{1\le|b|\le X\\ b\ne a}} \#\,\mathrm{Sel}_2(E(a,b)). \tag{1.3}$$

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

THEOREM 1.1. *Suppose a is a fixed non-zero integer and $|a|$ is not a square. Then there exist positive constants c_1 and c_2, depending only on a, such that for every $X \ge 2$ we have*

$$c_1 X < S(a;X) \le c_2 X. \tag{1.4}$$

The following corollary is an obvious consequence of Theorem 1.1.

COROLLARY 1.2. *Suppose a is a fixed non-zero integer and $|a|$ 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 $0 < \varepsilon < 1$ are any fixed numbers. Then there exist constants $c_3 > 0$ and $X_0 > 0$, depending only on A and ε, such that, for every $X > X_0$, we have*

$$S(\pm d^2; X) \geq c_3 \left(\frac{\phi(d)}{d}\right)^{3/2} \left(\frac{3}{4}\right)^{\omega(d)} \cdot X\sqrt{\log X} \tag{1.5}$$

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

$$S(\pm d^2; X) \geq c_3 \left(\frac{\phi(d)}{d}\right)^{3/2} \left(\frac{1}{2}\right)^{\omega(d)} \cdot X\sqrt{\log X} \tag{1.6}$$

if $|d| \leq X^{1-\varepsilon}$. 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*

$$S(\pm d^2; X) \leq c_4 \left(\frac{d}{\phi(d)}\right)^5 \cdot X\sqrt{\log X}. \tag{1.7}$$

In our proof of Theorem 1.3 (see Sections 3 and 4), while it seems necessary to consider $S(d^2; X)$ and $S(-d^2; X)$ separately as the related systems of quadratic equations (see Lemma 2.1) are formally different, the proofs for the bounds of $S(d^2; X)$ and $S(-d^2; X)$ are similar. To avoid unnecessary repetition, we shall prove the lower bounds for $S(d^2; X)$ only. We also remark that, with extra effort, we can eliminate the factor $(d/\phi(d))^5$ in Theorem 1.4, though we shall not do so in this paper.

The rest part of the paper is devoted to proving Theorems 1.1 and 1.3. The proof for Theorem 1.4 can be carried out by imitating the proof for Theorem 1.1; therefore, it is omitted.

Throughout the paper, we have fixed meanings for the following notation:

- $\mu(n)$: the Möbius function which takes value 0 if n has any square divisor other than 1 and otherwise takes value $(-1)^{\omega(n)}$.
- $\square$: by writing $m \equiv \square \pmod d$, we mean that m is prime to d and is a quadratic residue modulo d.
- $\tau_k(n)$: the usual k-fold divisor function.
- $P(n)$: the largest prime divisor of n.
- $p(n)$: the smallest prime divisor of n.

- $s(n)$: the radical of n, i.e., the largest squarefree integer dividing n.
- $\overline{m} \pmod n$ 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, e.g., $M < m \le 2M$, 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. Moreover, in complicated formulas, we 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 $\mathrm{Sel}_2(E(a\Delta, b\Delta))$ is equal to the number of homogeneous spaces described by the quadratic equation systems*

$$\begin{cases} a'\delta_1 V^2 + \dfrac{b}{b'} \cdot \delta_4 W^2 = \delta_2 \nu X^2, \\ b'\delta_1 V^2 + \dfrac{a}{a'} \cdot \delta_4 W^2 = \delta_3 \nu Y^2, \end{cases} \tag{2.1}$$

which have a solution with $W \neq 0$ in every local field including $\mathbb{R}$, where $|a'|$, $|b'|$ and ν 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 spaces with a' (or b') having fixed sign is equal to $\frac{1}{2}\#\mathrm{Sel}_2(E(a\Delta, b\Delta))$.

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

Lemma 2.2. *Suppose $\varepsilon > 0$ 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 $|a_m|, |b_n| \le 1$. Fix positive integers h, q satisfying $(h,q)=1$ and $q \le \{\min(M,N)\}^{\varepsilon/3}$. Let*

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

where the summation is subject to

$$M < m \le 2M, \quad N < n \le 2N, \quad mn \le X, \quad mn \equiv h \pmod q.$$

Then

$$S \ll MN^{15/16+\varepsilon} + M^{15/16+\varepsilon}N, \tag{2.2}$$

where the constant involved in the $\ll$-symbol depends on ε only.

Proof. This is essentially Lemma 4 of [7], proved basing on the work of Burgess [3]. One can also refer to Lemma 4.1 of [13]. ∎

LEMMA 2.3 ([13, Lemma 4.2]). *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*

$$\sum_{n\le x,\,(n,r)=1} \mu^2(n)s^{-\omega(n)}\chi(n) \ll x\tau(r)\exp(-\eta\sqrt{\log x}) \tag{2.3}$$

with a positive constant $\eta = \eta_{s,N}$, uniformly for $q \le \log^N x$. ∎

LEMMA 2.4. *Let s and C be two positive integers, and $A > 0$ be any fixed number. For $X > 1$, let $T \le \exp(\sqrt{\log X})$ and $M, N \ge T$ 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 χ_1, $\chi_2 \pmod q$, where $q \ll (\log X)^A$, we have*

$$\sum_{m,n} \mu^2(m)\mu^2(n)s^{-\omega(m)-\omega(n)}\chi_1(m)\chi_2(n) \ll \tau(r)X\exp(-\eta\sqrt{\log T})\log X \tag{2.4}$$

where the sum is over coprime variables satisfying the conditions

$$M < m \le 2M, \quad N < n \le 2N, \quad mn \le X,$$
$$mn \equiv h \pmod C, \quad (mn, r) = 1,$$

and the constant involved in the $\ll$-symbol depends on s and C only.

Proof. This is just a little 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

$$\frac{1}{\phi(C)} \sum_{\chi \pmod C} \chi(m)\chi(n)\overline{\chi}(h)$$

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. ∎

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 with the property that there exists a positive constant* c *such that, for every prime* p,

$$|\alpha(p)-1|<cp^{-1} \quad \text{and} \quad |\alpha(p^k)|<c+1 \quad \text{for } k\geq 2. \tag{2.5}$$

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* $\chi\,(mod\ q)$, *we have*

$$\sum_{n\leq x,\,(n,r)=1}\mu^2(n)s^{-\omega(n)}\alpha(n)\chi(n)\ll x\tau(r)\exp(-\eta\sqrt{\log x}), \tag{2.6}$$

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

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

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

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

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

where $G_1(z,\chi)$ is analytic and absolutely convergent for $\mathrm{Re}(z)>3/4$. Then an application of Perron's formula (cf. [10, Chapter 5, Theorem 1]) and estimates of Dirichlet L-functions yields (2.6). ∎

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 the conditions of Lemma* 2.4, *we have*

$$\sum_{m,n}\frac{\mu^2(m)\alpha_1(m)\chi_1(m)}{s^{\omega(m)}}\cdot\frac{\mu^2(n)\alpha_2(n)\chi_2(n)}{s^{\omega(n)}} \ll \tau(r)X\exp(-\eta\sqrt{\log T})\log X, \tag{2.7}$$

where 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, and M and N are sufficiently large real numbers satisfying*

$$N^{1/100} < M \le \exp((\log N)^2). \tag{2.8}$$

Suppose $\alpha_1(n)$ and $\alpha_2(n)$ are multiplicative functions satisfying (2.5) *for some constant $c > 0$. Let*

$$S(M,N) := \sum_{\substack{M<m\le 2M\\ N<n\le 2N\\ (mn,2ab)=1\\ am\equiv\square \,(\mathrm{mod}\, n)\\ b\equiv\square\,(\mathrm{mod}\, m)}} \mu^2(mn)\alpha_1(m)\alpha_2(n). \tag{2.9}$$

Then

$$S(M,N) \ll \frac{MN}{\sqrt{\log M \log N}}, \tag{2.10}$$

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, $s \equiv \square \,(\mathrm{mod}\, t)$ if and only if

$$2^{-\omega(t)} \prod_{p\mid t} \left(1 + \left(\frac{s}{p}\right)\right) = 1,$$

which, when t is squarefree, is equivalent to

$$2^{-\omega(t)} \sum_{d\mid t} \left(\frac{s}{d}\right) = 1.$$

Thus we have

$$S(M,N) = \sum_{\substack{M<m_1m_2\le 2M\\ N<n_1n_2\le 2N\\ (m_1m_2n_1n_2,2ab)=1}} \frac{\mu^2(m_1m_2n_1n_2)\alpha_1(m_1m_2)\alpha_2(n_1n_2)}{2^{\omega(m_1m_2n_1n_2)}} \left(\frac{am_1m_2}{n_1}\right)\left(\frac{b}{m_1}\right). \tag{2.11}$$

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

$$\sum_{n_2\le N/T} \frac{MN(\log\log M)^c}{n_2}\left(M^{-1/16+10^{-3}} + \left(\frac{N}{n_2}\right)^{-1/16+10^{-3}}\right) \ll \frac{MN}{(\log N)^2} \ll \frac{MN}{\sqrt{\log M \log N}}, \tag{2.12}$$

which is admissible for (2.10).

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

$$\begin{aligned}(2.13)\qquad &\ll \sum_{N/T<n_2\leq N} \frac{\mu^2(n_2)|\alpha_2(n_2)|}{2^{\omega(n_2)}} \cdot \frac{N}{n_2} \cdot \tau(n_2) M \exp(-\eta\sqrt{\log M}) \\ &\ll \frac{MN(\log\log N)^{c+1}}{\exp(\eta\sqrt{\log M})},\end{aligned}$$

which is more than enough.

The subsum subject to condition (3) is actually

$$(2.14)\qquad \sum_{\substack{M<m\leq 2M\\(m,2a\overline{b})=1\\ b\equiv\square \,(\mathrm{mod}\, m)}} \mu^2(m)\alpha_1(m) \sum_{\substack{N<n\leq 2N\\(n,2abm)=1}} \frac{\mu^2(n)\alpha_2(n)}{2^{\omega(n)}}.$$

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

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

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

$$\begin{aligned}\sum_{\substack{N<n\leq 2N\\(n,2abm)=1}} \frac{\mu^2(n)\alpha_2(n)}{2^{\omega(n)}} &\ll \prod_{p|2abm}\left(1 + \frac{1}{2p} + \frac{c}{2p^2}\right)\frac{N}{\sqrt{\log N}} \\ &\ll \left(\frac{m}{\phi(m)}\right)^{1/2} \frac{N}{\sqrt{\log N}}.\end{aligned}$$

(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

$$(2.15)\qquad \sum_{\substack{m\leq M\\(m,2a\overline{b})=1\\ b\equiv\square \,(\mathrm{mod}\, m)}} \mu^2(m)\alpha(m) \ll \frac{M}{\sqrt{\log M}}.$$

Let $f(s)$ be the generating function of the sum in (2.15). Then for $\mathrm{Re}(s) > 1$, we have

$$f(s) = \prod_{\substack{p\nmid 2a \\ (\frac{b}{p})=1}} \left(1 + \frac{\alpha(p)}{p^s}\right) = k(s) \prod_{\substack{p\geq 3 \\ (\frac{b}{p})=1}} \left(1 + \frac{1}{p^s}\right), \tag{2.16}$$

where $k(s)$, depending on a and b, is analytic and absolutely convergent on the half-plane $\mathrm{Re}(s) > \delta$ for any fixed $\delta > 0$. Thus, for any squarefree m satisfying $(m, 2ab) = 1$ and $b \equiv \square \pmod m$, we have

$$\alpha(m) = \sum_{d|m} \gamma(d)\varrho(m/d), \tag{2.17}$$

where

$$\gamma(d) = 1 \quad \text{if } b \equiv \square \pmod d, \qquad \gamma(d) = 0 \quad \text{otherwise},$$

and the arithmetic function $\varrho(d)$ satisfies, for any fixed $\delta > 0$ and $X \geq 1$,

$$\sum_{d\leq X} |\varrho(d)| \ll X^{\delta}. \tag{2.18}$$

From the classical result that

$$\sum_{n\leq X} \gamma(n) \ll_b \frac{X}{\sqrt{\log X}},$$

combined with (2.17) and (2.18), we have

$$\begin{aligned}\sum_{\substack{m\leq M \\ (m,2ab)=1 \\ b\equiv\square \,(\mathrm{mod}\, m)}} \mu^2(m)\alpha(m) &\ll \sum_{m\leq M} \gamma(m)\sqrt{\frac{M}{m}} = \sqrt{M} \int_2^M \frac{1}{\sqrt{t}}\, d\sum_{m\leq t} \gamma(m) \\ &\ll \frac{M}{\sqrt{\log M}} + \sqrt{M} \int_2^M \frac{\sum_{m\leq t}\gamma(m)}{t^{3/2}}\, dt \\ &\ll \frac{M}{\sqrt{\log M}},\end{aligned}$$

as required. ∎

Finally, 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 with $(a, q) = 1$, we write

$$\psi(x; q, a) := \sum_{\substack{n\leq x \\ n\equiv a \,(\mathrm{mod}\, q)}} \Lambda(n), \qquad E(x; q, a) := \psi(x; q, a) - \frac{x}{\phi(q)}.$$

LEMMA 2.8 (The Bombieri–Vinogradov Theorem). *Suppose $x > 3$, $\varepsilon > 0$ is any fixed small real number, and $Q = x^{1/2-\varepsilon}$. Then for any $A > 0$, we*

have

$$\sum_{q\le Q}\max_{(a,q)=1}\max_{y\le x}|E(y;q,a)|\ll x(\log x)^{-A}, \tag{2.19}$$

the constant implied by the $\ll$-symbol depending only on ε and A.

Proof. This is actually a weaker form of Theorem 4 of Bombieri [2] (see also [4, Theorem, Chapter 28]). ∎

3. Proof of the first part of Theorem 1.3. We shall prove the theorem for $S(d^2;X)$. Formally, there is some minor difference between the treatment for d odd and even, but they are essentially the same. In this section, we shall only consider the case of d odd. The other case can be done in the same way. For d odd, 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 $1\le u\le X/2$ is prime to $2d$, with $|2u-d^2|$ squarefree.

By Lemma 2.1, $\#\mathrm{Sel}_2(E(d^2,2u))$ is equal to the number of quadratic equation systems

$$\begin{cases} u_0V^2+\dfrac{d^2}{f}W^2=vZ^2,\\ fV^2+\dfrac{2u}{u_0}W^2=vY^2, \end{cases} \tag{3.1}$$

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 $u_0\equiv 1 \pmod 8$ positive, which can be written as

$$\begin{cases} u_0V^2+d^2W^2=Z^2,\\ V^2+2u_1W^2=Y^2, \end{cases} \tag{3.2}$$

where $u_1=u/u_0$. One equivalent form of (3.2) is

$$\begin{cases} (2u_0u_1-d^2)W^2+Z^2=u_0Y^2,\\ d^2W^2-Z^2=-u_0V^2. \end{cases} \tag{3.3}$$

Note that 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 $\#\mathrm{Sel}_2(E(d^2,2u))$ over u then we 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 system (3.2) to be solvable in every $\mathbb{Q}_p$, it suffices to be solvable in $\mathbb{Q}_p$ with $p\,|\,2du_0u_1(2u_0u_1-d^2)$.

We first note that (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 in 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 $4(2u_0u_1 - d^2)VW$, $-4u_0VY$, $4VZ$, $-4d^2WY$, $8u_1WZ$ and $4YZ$. If for $p \,|\, u_0u_1d(2u_0u_1 - d^2)$, $(V, W, Y, Z) \in \mathbb{F}_p^4$ 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 $p \,|\, u_0u_1d(2u_0u_1 - d^2)$, 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 variables non-zero in $\mathbb{F}_p$.

We note that for any $p \,|\, u_0u_1$, the system (3.2) is always non-trivially solvable in $\mathbb{F}_p$. For example, for $p \,|\, u_0$, $V^2 + 2u_1W^2 = Y^2$ has p^2 solutions $(V, W, Y) \in \mathbb{F}_p^3$, $2p-1$ of which have $W = 0$, 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 $p \,|\, u_1$.

For $p \,|\, 2u_0u_1 - d^2$, (3.3) is non-trivially 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 $V_0Y_0Z_0 \neq 0$.

Things are a little more complicated for $p \,|\, d$. We consider 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 γ is a square root of u_0 in $\mathbb{F}_p$.

(II): $\left(\frac{u_0}{p}\right) = -1$. In this case, (3.2) cannot be non-trivially solvable in $\mathbb{F}_p$. However, if we suppose $\mathrm{ord}_p(d) = k$ and let $d = p^k d_0$, then the system

$$\begin{cases} u_0V^2 + d_0^2W^2 = Z^2, \\ p^{2k}V^2 + 2u_1W^2 = Y^2, \end{cases}$$

is non-trivially solvable in $\mathbb{F}_p$ if $\left(\frac{2u_1}{p}\right) = 1$. Thus, it is then 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,

$$\left(\frac{u_0}{p}\right) = 1 \quad \text{or} \quad \left(\frac{2u - d^2}{p}\right) = -1 \quad \text{for each prime } p \,|\, d. \tag{3.4}$$

Therefore, (3.2) is non-trivially solvable in $\mathbb{Q}_p$ for $p \,|\, d$ if and only if (3.4) holds.

So from the discussion above we have

$$\#\operatorname{Sel}_2(E(d^2, 2u)) \geq \sum_{\substack{u_0 \,|\, u \\ u_0 \equiv 1 \,(\mathrm{mod}\, 8) \\ u_0 \equiv \square \,(\mathrm{mod}\, 2u - d^2)}}^{*} \mu^2(u_0), \tag{3.5}$$

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

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

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

$$S(d^2; X) \geq \sum_{\substack{X^{\theta_2} < u_0 \leq X^{\theta_1} \\ u_0 \equiv 1 \,(\mathrm{mod}\, 8) \\ (u_0, d) = 1}} \mu^2(u_0) \sum_{\substack{n \leq X - d^2 \\ n \equiv -d^2 \,(\mathrm{mod}\, 2u_0) \\ u_0 \equiv \square \,(\mathrm{mod}\, n) \\ (n, d) = 1}} \mu^2(n) \alpha(d, u_0, n). \tag{3.6}$$

To split the condition $u_0 \equiv \square \,(\mathrm{mod}\, n)$ so that the inner sum of (3.6) is easier to estimate, 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

$$\begin{aligned} &S(d^2; X) \\ &\geq \sum_{\substack{X^{\theta_2} < u_0 \leq X^{\theta_1} \\ u_0 \equiv 1 \,(\mathrm{mod}\, 8) \\ (u_0, d) = 1}} \mu^2(u_0) \sum_{\substack{m \leq X^{\theta_3} \\ (m, 2u_0 d) = 1 \\ u_0 \equiv \square \,(\mathrm{mod}\, m)}} \mu^2(m) \sum_{\substack{X/2m < p \leq (X - d^2)/m \\ p \equiv -d^2 \overline{m} \,(\mathrm{mod}\, 2u_0) \\ (\frac{u_0}{p}) = 1}} \alpha(d, u_0, mp). \end{aligned} \tag{3.7}$$

Since $u_0 \equiv 1 \,(\mathrm{mod}\, 8)$, we have

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

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

$$\alpha(d, u_0, n) = 4^{-\omega(d)} \sum_{s(d)=d_1d_2d_3d_4} 3^{\omega(d_1)}(-1)^{\omega(d_3)} \left(\frac{u_0}{d_2d_4}\right)\left(\frac{n}{d_3d_4}\right).$$

Thus, in the case $d \le (\log X)^A$, letting $\theta_1 = 1/3$, $\theta_2 = 2/9$ and $\theta_3 = 1/24$ (or any other appropriate choice for the values of θ_j, $j = 1, 2, 3$), we get

$$\begin{aligned}(3.8)\quad & S(d^2; X)\\ &\ge \frac{1}{\log X} \sum_{\substack{X^{2/9} < u_0 \le X^{1/3}\\ u_0 \equiv 1 \pmod 8\\ (u_0, d)=1}} \mu^2(u_0) \sum_{\substack{m \le X^{1/24}\\ (m, 2u_0d)=1\\ u_0 \equiv \square \pmod m}} \mu^2(m)\\ &\quad \times \sum_{\substack{X/2m < k \le X/m\\ k \equiv -d^2\overline{m} \pmod{2u_0}}} \alpha(d, u_0, mk)\Lambda(k) + O\Bigg(\sum_{u_0 \le X^{1/3}} \sum_{m \le X^{1/24}} \sqrt{\frac{X}{m}}\Bigg)\\ &= \frac{1}{4^{\omega(d)} \log X} \sum_{s(d)=d_1d_2d_3d_4} 3^{\omega(d_1)}(-1)^{\omega(d_3)} \sum_{\substack{X^{2/9} < u_0 \le X^{1/3}\\ u_0 \equiv 1 \pmod 8\\ (u_0, d)=1}} \mu^2(u_0)\left(\frac{u_0}{d_2d_4}\right)\\ &\quad \times \sum_{\substack{m \le X^{1/24}\\ (m, 2u_0d)=1\\ u_0 \equiv \square \pmod m}} \mu^2(m)\left(\frac{m}{d_3d_4}\right) \sum_{\substack{X/2m < k \le X/m\\ k \equiv -d^2\overline{m} \pmod{2u_0}}} \left(\frac{k}{d_3d_4}\right)\Lambda(k) + O(X^{41/48}).\end{aligned}$$

As we shall see, the main term has order of magnitude $\gg X(\log X)^{1/2-\varepsilon}$ for any $\varepsilon > 0$. 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

$$\begin{aligned}(3.9)\quad & \sum_{\substack{X/2m < k \le X/m\\ k \equiv -d^2\overline{m} \pmod{2u_0}}} \left(\frac{k}{d_3d_4}\right)\Lambda(k)\\ &= \sum_{a \pmod{d_3d_4}^\times} \left(\frac{a}{d_3d_4}\right) \sum_{\substack{X/2m < k \le X/m\\ k \equiv -d^2\overline{m} \pmod{2u_0}\\ k \equiv a \pmod{d_3d_4}}} \Lambda(k)\\ &= \sum_{a \pmod{d_3d_4}^\times} \left(\frac{a}{d_3d_4}\right) \sum_{\substack{X/2m < k \le X/m\\ k \equiv -d^2(\overline{m})_{2u_0} + 2au_0(\overline{2u_0})_{d_3d_4} \pmod{2u_0d_3d_4}}} \Lambda(k),\end{aligned}$$

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

$$\begin{aligned}(3.10)\quad &\frac{1}{\phi(2u_0d_3d_4)}\left(\frac{X}{m}-\frac{X}{2m}\right)\\ &\quad+E\left(\frac{X}{m};2u_0d_3d_4,-d^2(\overline{m})_{2u_0}+2au_0(\overline{2u_0})_{d_3d_4}\right)\\ &\quad-E\left(\frac{X}{2m};2u_0d_3d_4,-d^2(\overline{m})_{2u_0}+2au_0(\overline{2u_0})_{d_3d_4}\right)\\ &=\alpha_1(\vec{d},a,m,u_0;X)+\alpha_2(\vec{d},a,m,u_0;X)+\alpha_3(\vec{d},a,m,u_0;X),\quad \text{say,}\end{aligned}$$

where we write $\vec{d}$ 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 α_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, from Lemma 2.8, we have

$$\begin{aligned}(3.11)\quad &S_3(d^2;X)\\ &\ll\frac{d}{\log X}\sum_{w\le 2X^{1/3}(\log X)^A}\sum_{m\le X^{1/24}}\max_{a\,(\mathrm{mod}\,w)^\times}\left|\psi\left(\frac{X}{2m};w,a\right)-\frac{X/2m}{\phi(w)}\right|\\ &\ll(\log X)^{A-1}\sum_{m\le X^{1/24}}\frac{X}{m}\left(\log\frac{X}{m}\right)^{-A-3}\ll\frac{X}{(\log X)^3}.\end{aligned}$$

With exactly the same estimate, we get

$$(3.12)\qquad S_2(d^2;X)\ll\frac{X}{(\log X)^3}.$$

Since for odd integers $q>1$,

$$\sum_{a\,(\mathrm{mod}\,q)^\times}\left(\frac{a}{q}\right)=0,$$

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

$$
\begin{aligned}
(3.13)\quad & S_1(d^2;X) \\
&= \frac{1}{4^{\omega(d)}\log X}\sum_{s(d)=d_1d_2} 3^{\omega(d_1)} \sum_{\substack{X^{2/9}<u_0\le X^{1/3}\\ u_0\equiv 1 \,(\mathrm{mod}\, 8)\\ (u_0,d_1)=1}} \frac{\mu^2(u_0)}{\phi(2u_0)}\left(\frac{u_0}{d_2}\right) \\
&\quad\times \sum_{\substack{m\le X^{1/24}\\ (m,2u_0d_1d_2)=1\\ u_0\equiv\square \,(\mathrm{mod}\, m)}} \mu^2(m)\left(\frac{X}{m}-\frac{X}{2m}\right) \\
&\sim \frac{X}{2^{2\omega(d)+3}\log X}\sum_{s(d)=d_1d_2} 3^{\omega(d_1)} \sum_{\substack{m\le X^{1/24}\\ (m,2d_1d_2)=1}} \frac{\mu^2(m)}{m2^{\omega(m)}} \\
&\quad\times \sum_{\substack{\chi_1 \,(\mathrm{mod}\, m)\\ \chi_1^2=\chi_0}} \sum_{\chi_2 \,(\mathrm{mod}\, 8)} \sum_{\substack{X^{2/9}<u_0\le X^{1/3}\\ (u_0,md_1)=1}} \frac{\mu^2(u_0)\chi_1\chi_2(u_0)}{\phi(u_0)}\left(\frac{u_0}{d_2}\right),
\end{aligned}
$$

where, in the last step, an error of $O(X/(\log X)^B)$ for a large $B>0$ has been discarded.

For notational convenience, we denote by $\chi := \chi_1\chi_2\big(\frac{\cdot}{d_2}\big)$ a character modulo $8md_1d_2$. Then from the simple fact that

$$
(3.14)\qquad \frac{1}{\phi(u_0)} = \frac{1}{u_0}\sum_{s\mid u_0}\frac{\mu^2(s)}{\phi(s)},
$$

the innermost sum of (3.13) is equal to

$$
\begin{aligned}
(3.15)\quad & \sum_{s\le(\log X)^2}\frac{\mu^2(s)\chi(s)}{s\phi(s)} \sum_{\substack{X^{2/9}/s<t\le X^{1/3}/s\\ (s,t)=1}}\frac{\mu^2(t)\chi(t)}{t} + O((\log X)^{-1}) \\
&= \sum_{s\le(\log X)^2}\frac{\mu^2(s)\chi(s)}{s\phi(s)} \sum_{a \,(\mathrm{mod}\, 8msd_1d_2)^\times}\chi(a) \sum_{\substack{X^{2/9}/s<t\le X^{1/3}/s\\ t\equiv a \,(\mathrm{mod}\, 8msd_1d_2)}}\frac{\mu^2(t)}{t} \\
&\quad + O((\log X)^{-1}).
\end{aligned}
$$

Note that

$$
(3.16)\qquad \sum_{\substack{X^{2/9}/s<t\le X^{1/3}/s\\ t\equiv a \,(\mathrm{mod}\, 8msd_1d_2)}}\frac{\mu^2(t)}{t} = \sum_{\substack{h\le\sqrt{X^{1/3}/s}\\ (h,2msd_1d_2)=1}}\frac{\mu(h)}{h^2} \sum_{\substack{X^{2/9}/sh^2<r\le X^{1/3}/sh^2\\ r\equiv a\overline{h}^2 \,(\mathrm{mod}\, 8msd_1d_2)}}\frac{1}{r}
$$

$$= \sum_{\substack{h\le X^{1/12}\\(h,2msd_1d_2)=1}} \frac{\mu(h)}{h^2} \sum_{\substack{X^{2/9}/sh^2<r\le X^{1/3}/sh^2\\ r\equiv a\overline{h}^2 \,(\mathrm{mod}\, 8msd_1d_2)}} \frac{1}{r} + O(X^{-1/12}\log X)$$

$$= \sum_{\substack{h\le X^{1/12}\\(h,2msd_1d_2)=1}} \frac{\mu(h)}{h^2}\cdot\left(\frac{\log X}{72msd_1d_2} + O\left(\frac{sh^2}{X^{2/9}}\right)\right) + O(X^{-1/12}\log X)$$

$$= \frac{\log X}{72\zeta(2)msd_1d_2}\prod_{p\mid 2msd_1d_2}\left(1-\frac{1}{p^2}\right)^{-1} + O(X^{-1/12}\log X).$$

Here the error gives a negligible contribution to the entire sum, and the main term of (3.15) vanishes when χ is non-principal. Thus the terms that give a 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 (3.13)–(3.16),

$$\begin{aligned}(3.17)\quad & S_1(d^2;X)\\ &\ge \frac{X\left(\frac{3}{4}\right)^{\omega(d)}}{8\log X}\sum_{\substack{m\le X^{1/24}\\(m,2d)=1}}\frac{\mu^2(m)}{2^{\omega(m)}m}\sum_{\substack{s\le(\log X)^2\\(s,2md)=1}}\frac{\mu^2(s)}{s\phi(s)}\cdot\frac{\phi(8ms\cdot s(d))\log X}{72\zeta(2)ms\cdot s(d)}\\ &= \frac{X\phi(d)\left(\frac{3}{4}\right)^{\omega(d)}}{144\zeta(2)d}\sum_{\substack{m\le X^{1/24}\\(m,2d)=1}}\frac{\mu^2(m)\phi(m)}{m^2 2^{\omega(m)}}\sum_{\substack{s\le(\log X)^2\\(s,2md)=1}}\frac{\mu^2(s)}{s^2}\\ &\ge \frac{X\phi(d)\left(\frac{3}{4}\right)^{\omega(d)}}{144\zeta(2)d}\sum_{\substack{m\le X^{1/24}\\(m,2d)=1}}\frac{\mu^2(m)\phi(m)}{m^2 2^{\omega(m)}}.\end{aligned}$$

By Perron's formula, it is easy to see that

$$(3.18)\qquad \sum_{\substack{m\le X^{1/24}\\(m,2d)=1}}\frac{\mu^2(m)\phi(m)}{m^2 2^{\omega(m)}} \ge c\left(\frac{\phi(d)}{d}\right)^{1/2}\sqrt{\log X}$$

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

$$(3.19)\qquad S(d^2;X)\ge c'\left(\frac{\phi(d)}{d}\right)^{3/2}\left(\frac{3}{4}\right)^{\omega(d)}\cdot X\sqrt{\log X}$$

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 $d\le X^{1-\varepsilon}$ for any fixed $0<\varepsilon<10^{-2}$. For the second part of Theorem 1.3, in considering the solvability of (3.2) in $\mathbb{Q}_p$ with $p\,|\,d$, we require $\left(\frac{u_0}{p}\right)=1$

instead of (3.4). This change results in replacing the factor $(3/4)^{\omega(d)}$ in the coefficient by $(1/2)^{\omega(d)}$. 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

$$S(d^2;X) \geq \frac{1}{\log X} \sum_{\substack{X^{\theta_2}<u_0\leq X^{\theta_1}\\ u_0\equiv 1 \,(\mathrm{mod}\, 8)\\ (u_0,d)=1\\ u_0\equiv \square \,(\mathrm{mod}\, d)}} \mu^2(u_0) \sum_{\substack{m\leq X^{\theta_3}\\ (m,2u_0d)=1\\ u_0\equiv\square \,(\mathrm{mod}\, m)}} \mu^2(m) \sum_{\substack{X/2m<k\leq X/m\\ k\equiv -d^2\overline{m} \,(\mathrm{mod}\, 2u_0)}} \Lambda(k). \tag{4.1}$$

Throughout this section, let

$$\theta_1 = \frac{1}{2}(1-\varepsilon^2)-\varepsilon^3, \quad \theta_2 = \frac{1}{2}(1-\varepsilon^2)-2\varepsilon^3, \quad \theta_3 = \varepsilon^2.$$

Note that $2u_0 \leq 2X^{\theta_1} \leq (X/m)^{1/2-\varepsilon^3}$. Estimating the error term by the Bombieri–Vinogradov Theorem as we did for the first case, apart from an error $O(X(\log X)^{-A})$, where $A>1$ is a certain fixed number, we have

$$S(d^2;X) \geq \frac{1}{\log X} \sum_{\substack{X^{\theta_2}<u_0\leq X^{\theta_1}\\ u_0\equiv 1 \,(\mathrm{mod}\, 8)\\ (u_0,d)=1\\ u_0\equiv \square \,(\mathrm{mod}\, d)}} \frac{\mu^2(u_0)}{\phi(u_0)} \sum_{\substack{m\leq X^{\theta_3}\\ (m,2u_0d)=1\\ u_0\equiv\square \,(\mathrm{mod}\, m)}} \mu^2(m)\left(\frac{X}{m}-\frac{X}{2m}\right). \tag{4.2}$$

Thus

$$\begin{aligned} S(d^2;X) &\geq \frac{X}{2\log X} \sum_{\substack{m\leq X^{\theta_3}\\ (m,2d)=1}} \frac{\mu^2(m)}{m} \sum_{\substack{X^{\theta_2}<u_0\leq X^{\theta_1}\\ u_0\equiv 1 \,(\mathrm{mod}\, 8)\\ (u_0,md)=1\\ u_0\equiv \square \,(\mathrm{mod}\, md)}} \frac{\mu^2(u_0)}{\phi(u_0)} \qquad (4.3)\\ &\gg \frac{X}{\log X} \sum_{\substack{m\leq X^{\theta_3}\\ (m,2d)=1}} \frac{\mu^2(m)}{m} \sum_{X^{\theta_2}<U=2^j\leq X^{\theta_1}/2} \frac{1}{U} \sum_{\substack{U<u_0\leq 2U\\ u_0\equiv 1 \,(\mathrm{mod}\, 8)\\ (u_0,md)=1\\ u_0\equiv \square \,(\mathrm{mod}\, md)}} \frac{\mu^2(u_0)u_0}{\phi(u_0)}\\ &\gg \sum_U \frac{X2^{-\omega(d)}}{U\log X} \sum_{\substack{m\leq X^{\theta_3}\\ (m,2d)=1}} \frac{\mu^2(m)}{m2^{\omega(m)}}\\ &\quad \times \sum_{\substack{\chi \,(\mathrm{mod}\, md)\\ \chi^2=\chi_0}} \sum_{\chi' \,(\mathrm{mod}\, 8)} \sum_{U<u_0\leq 2U} \frac{\mu^2(u_0)u_0\chi\chi'(u_0)}{\phi(u_0)}, \end{aligned}$$

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

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

$$\sum_{s\leq(\log X)^{10}} \frac{\mu^2(s)\chi\chi'(s)}{\phi(s)} \sum_{\substack{U/s<t\leq 2U/s\\(t,s)=1}} \mu^2(t)\chi\chi'(t) + O(U(\log X)^{-10}),$$

which, from the Pólya–Vinogradov Theorem, is bounded by

$$\sum_{s\leq(\log X)^{10}} \frac{(mds)^{(1+\varepsilon^3)/2}}{\phi(s)} + U(\log X)^{-10} \ll (md)^{1/2+\varepsilon^3} + U(\log X)^{-10}.$$

And this contributes to $S(d^2;X)$ at most

$$X(\log X)^{-9} + \sum_U \frac{Xd^{1/2+\varepsilon^3}}{U\log X} \sum_{m\leq X^{\theta_3}} \frac{m^{1/2+\varepsilon^3}\mu^2(m)}{m}$$
$$\ll X^{1+(1/2+\varepsilon^3)(1-\varepsilon+\theta_3)-\theta_2} + X(\log X)^{-9} \ll X(\log X)^{-9}.$$

Thus, apart from these admissible errors, we have

$$\begin{aligned}(4.4)\quad & S(d^2;X)\\ &\gg \sum_{X^{\theta_2}<U=2^j\leq X^{\theta_1}/2} \frac{X2^{-\omega(d)}}{U\log X} \sum_{\substack{m\leq X^{\theta_3}\\(m,2d)=1}} \frac{\mu^2(m)}{m2^{\omega(m)}} \sum_{\substack{U<u_0\leq 2U\\(u_0,2md)=1}} \frac{\mu^2(u_0)u_0}{\phi(u_0)}\\ &\gg \sum_U \frac{X\phi(d)2^{-\omega(d)}}{d\log X} \sum_{\substack{m\leq X^{\theta_3}\\(m,2d)=1}} \frac{\mu^2(m)\phi(m)}{m^2 2^{\omega(m)}}\\ &\gg_\varepsilon 2^{-\omega(d)}\left(\frac{\phi(d)}{d}\right)^{3/2}\cdot X\sqrt{\log X}.\end{aligned}$$

And this finishes the proof of the second part of Theorem 1.3.

5. The sum $S(a;X)$. For Theorem 1.1, 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 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 will be the same as well.

Every curve under consideration will therefore be of the form $E(a,u\Delta)$, where every prime divisor of Δ 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 Δ a fixed squarefree divisor of a, u prime to a. From Lemma 2.1, we thus need to count the number of quadratic equation systems

$$\begin{cases} \delta_1 u_0 V^2 + \dfrac{a}{\delta\alpha}\, T^2 = \delta_2\beta Y^2, \\ \delta_1\alpha V^2 + \dfrac{u\Delta}{\delta u_0}\, T^2 = \delta_3\beta Z^2, \end{cases} \tag{5.1}$$

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

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

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

$$\frac{u-a/\Delta}{\beta} := h^2\xi, \qquad \frac{u}{u_0} := j^2\varrho,$$

where ξ and ϱ are squarefree. Then the following conditions are necessary for the system (5.1) to be everywhere locally solvable:

$$\begin{cases} -\alpha a\delta_2\delta_3 u_0 \equiv \square \ (\mathrm{mod}\,\beta), \\ \alpha\beta a\delta_1\delta_3 \equiv \square \ (\mathrm{mod}\,u_0), \\ \alpha\beta\delta_1\delta_3 \equiv \square \ (\mathrm{mod}\,\varrho), \\ \alpha\delta_2\delta_3 u_0 \equiv \square \ (\mathrm{mod}\,\xi). \end{cases} \tag{5.2}$$

Since Δ divides a, there are $O_a(1)$ choices for δ_1, δ_2 and δ_3. Hence it suffices to show that for each fixed choice of δ_1, δ_2, δ_3 and Δ, the number of systems (5.2) which are everywhere locally solvable is $O(X)$. Thus, in the following we shall let Δ and δ_i, $i=1,2,3$, be fixed.

We also note that, in some sense, β and ξ, u_0 and ϱ are symmetric in pairs, so we will just consider the subsum of $S(a;X)$ with $\beta \le \sqrt{X/\Delta h^2}$ and $u_0 \le \sqrt{X/\Delta j^2}$ and the resulting upper bound for this subsum serves as an upper bound of the whole sum. (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

$$\kappa := -\alpha a\delta_2\delta_3, \qquad \mu := \alpha a\delta_1\delta_3, \qquad \varrho := \alpha\delta_1\delta_3, \qquad \nu := \alpha\delta_2\delta_3.$$

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

$$S(a;X) \ll \sum_{h,j} \sum_{u_0 \le \sqrt{X}/j} \mu^2(u_0) \sum_{\substack{\beta \le \sqrt{X}/h \\ \kappa u_0 \equiv \square \pmod{\beta} \\ \mu\beta \equiv \square \pmod{u_0} \\ (\beta,u_0)=1}} \mu^2(\beta) \sum_{\substack{\xi,\varrho \\ \varrho\beta \equiv \square \pmod{\varrho} \\ \nu u_0 \equiv \square \pmod{\xi}}} \mu^2(\xi)\mu^2(\varrho). \tag{5.3}$$

We note that, when $2 \,|\, \beta\xi$ or $2 \,|\, u_0\varrho$, 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 β, u_0, ϱ and ξ 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 $m = j^2 u_0 \varrho$ with $u_0\varrho$ squarefree. Thus the subsum of (5.3) subject to $h > (\log X)^2$ is bounded by

$$\sum_{h > (\log X)^2} \sum_{\beta \le \sqrt{X/\Delta h^2}} \sum_{\substack{m \le X/\Delta \\ m \equiv a/\Delta \pmod{h^2\beta}}} \tau(m). \tag{5.4}$$

The partial sum of (5.4) with $h > X^{1/7}$ is simply bounded by

$$\ll \sum_{h > X^{1/7}} \sum_{\beta \le \sqrt{X/\Delta h^2}} X^{\varepsilon} \left(1 + \frac{X}{h^2\beta}\right) \ll X^{6/7+2\varepsilon}.$$

When $h \le X^{1/7}$, we have $h^2\beta \le (X/\Delta)^{2/3-\varepsilon}$. From the well known result on the distribution of the divisor function over arithmetic progressions (see, for example, the introductory part of [5]), the partial sum of (5.4) with $(\log X)^2 < h \le X^{1/7}$ is bounded by

$$\sum_{(\log X)^2 < h \le X^{1/7}} \sum_{\beta \le \sqrt{X/\Delta h^2}} \frac{1}{\phi(h^2\beta)} \cdot \frac{X}{\Delta} \log X \ll X.$$

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 $u_0 \ne 1$ and $\beta \ne 1$, 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 non-trivial for ξ (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/Δ is a square and $u_0 = u/j^2$, both giving an admissible contribution). 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 non-trivial. The treatment for the subsum with $\alpha\delta_1\delta_3$ not a square is similar to that for the subsum with $a\alpha\delta_1\delta_3$ 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 fourth congruences as the restrictions on the variables. (This is actually the more difficult case.) Therefore, we have

$$\begin{aligned}(6.1)\qquad S_1(a;X) &\ll \sum_{u_0\le\sqrt{X}}\mu^2(u_0)\sum_{h,j}\sum_{\substack{\xi,\varrho\\ \varrho\equiv\square\,(\mathrm{mod}\,\varrho)\\ \nu u_0\equiv\square\,(\mathrm{mod}\,\xi)}}\mu^2(\xi)\mu^2(\varrho)+X\\ &\ll \sum_{h,j\le(\log X)^2}\sum_{u_0\le\sqrt{X}}\mu^2(u_0)\sum_{\substack{\varrho\le X/u_0j^2\\ \varrho\equiv\square\,(\mathrm{mod}\,\varrho)\\ \varrho\equiv(a\nu/\Delta)\cdot\square\,(\mathrm{mod}\,\xi)}}\mu^2(\varrho)+X,\end{aligned}$$

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

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 $|d| \le (\log X)^4$, and any N satisfying $X/(\log X)^4 \ll N \ll X$,

$$(6.2)\qquad \widehat{S}_I(N) := \sum_{\substack{\sqrt{N}/(\log N)^2<\varrho\le N\\ (\varrho,bc)=1\\ b\equiv\square\,(\mathrm{mod}\,\varrho)}}\mu^2(\varrho)\sum_{\substack{\xi\le N\\ (\xi,a)=1\\ \xi\equiv c\overline{d}\,(\mathrm{mod}\,\varrho)\\ \varrho\equiv a\square\,(\mathrm{mod}\,\xi)}}\mu^2(\xi)\ll N.$$

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 $u_0 \asymp h^2\xi/j^2\varrho \le \sqrt{X}$, the contribution of the terms with $\varrho \le \sqrt{N}/(\log N)^4$ is small. Hence, in the following we shall focus on proving (6.2).

Let

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

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

$$(6.3)\qquad \widehat{S}_I(N) = \sum_{\substack{\sqrt{N}/(\log N)^2<\varrho\le N/\widehat{E}\\ (\varrho,bc)=1\\ b\equiv\square\,(\mathrm{mod}\,\varrho)}}\mu^2(\varrho)\sum_{\substack{\xi\le N\\ (\xi,a)=1\\ \xi\equiv c\overline{d}\,(\mathrm{mod}\,\varrho)\\ \varrho\equiv a\square\,(\mathrm{mod}\,\xi)}}\mu^2(\xi)+O(N).$$

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

$$\widehat{S}_I(N,R) := \sum_{\substack{R<\varrho\le 2R\\(\varrho,bc)=1\\ b\equiv\square \,(\mathrm{mod}\,\varrho)}} \mu^2(\varrho) \sum_{\substack{\xi\le N\\(\xi,a)=1\\ \xi\equiv c\overline{d}\,(\mathrm{mod}\,\varrho)\\ \varrho\equiv a\square\,(\mathrm{mod}\,\xi)}} \mu^2(\xi) \ll \frac{N}{\sqrt{\log N\log(N/R)}}, \tag{6.4}$$

because then we have

$$\begin{aligned}\widehat{S}_I(N) &\ll \sum_R \frac{N}{\sqrt{\log N\log(N/R)}} + N\\ &\ll \frac{N}{\sqrt{\log N}} \sum_{\frac12\log N<i\le \frac{\log N-\sqrt{\log N}}{\log 2}} \frac{1}{\sqrt{\log N - i\log 2}} + N \ll N.\end{aligned} \tag{6.5}$$

Next, we write

$$\xi = kpK,$$

so that for a fixed positive constant $\varepsilon < 1/100$,

$$P(k) < p < p(K), \quad (N/R)^{\varepsilon} < pk \le p(N/R)^{\varepsilon}. \tag{6.6}$$

Then we have

$$\widehat{S}_I(N,R) \ll \sum_{\substack{R<\varrho\le 2R\\(\varrho,bc)=1\\ b\equiv\square\,(\mathrm{mod}\,\varrho)}} \mu^2(\varrho) \sum_{\substack{p,k\\ \varrho\equiv a\square\,(\mathrm{mod}\,k)}} \mu^2(k) \sum_{\substack{K\le N/pk\\ p(K)>p\\ K\equiv c\overline{dpk}\,(\mathrm{mod}\,\varrho)}} 1. \tag{6.7}$$

We split the sum (6.7) into two parts: $\widehat{\Sigma}_I^1(N,R)$ with $p > (N/R)^{\varepsilon^2}$ and $\widehat{\Sigma}_I^2(N,R)$ the rest. The methods we shall use to estimate the two sums are essentially the same, but there will be some minor technical differences. We estimate $\widehat{\Sigma}_I^1(N,R)$ first.

• *Estimate of* $\widehat{\Sigma}_I^1(N,R)$. 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 find

$$\begin{aligned}\widehat{\Sigma}_I^1(N,R) &\ll \sum_{\substack{R<\varrho\le 2R\\(\varrho,bc)=1\\ b\equiv\square\,(\mathrm{mod}\,\varrho)}} \sum_{\substack{k\le (N/R)^{\varepsilon}\\ \varrho\equiv a\square\,(\mathrm{mod}\,k)}} \sum_{\substack{K\le N/k\\ p(K)\ge (N/R)^{\varepsilon^2}\\ K\equiv c\overline{dk}\,(\mathrm{mod}\,\varrho)}} 1\\ &\ll \sum_{\substack{R<\varrho\le 2R\\(\varrho,bc)=1\\ b\equiv\square\,(\mathrm{mod}\,\varrho)}} \sum_{\substack{k\le (N/R)^{\varepsilon}\\ \varrho\equiv a\square\,(\mathrm{mod}\,k)}} \sum_{\substack{m\le N/Rk\\ p(m\varrho+c\overline{dk})>(N/R)^{\varepsilon^2}}} 1.\end{aligned} \tag{6.8}$$

Since

$$\frac{N}{kR} \gg \left(\frac{N}{R}\right)^{1-\varepsilon},$$

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

$$\begin{aligned}(6.9)\qquad \widehat{\Sigma}_I^1(N,R) &\ll \sum_{\substack{R<\varrho\le 2R\\(\varrho,bc)=1\\ b\equiv\square \,(\mathrm{mod}\,\varrho)}} \sum_{\substack{k\le (N/R)^{\varepsilon}\\ \varrho\equiv a\square\,(\mathrm{mod}\,k)}} \frac{N\varrho}{Rk\phi(\varrho)\log(N/R)}\\ &\ll \frac{N}{R\log(N/R)} \sum_{\substack{R<\varrho\le 2R\\(\varrho,bc)=1\\ b\equiv\square \,(\mathrm{mod}\,\varrho)}} \frac{\varrho}{\phi(\varrho)} \sum_{\substack{k\le (N/R)^{\varepsilon}\\ \varrho\equiv a\square\,(\mathrm{mod}\,k)}} \frac{1}{k}.\end{aligned}$$

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

$$\frac{N}{R\sqrt{\log(N/R)}} \sum_{\substack{R<\varrho\le 2R\\(\varrho,bc)=1\\ b\equiv\square \,(\mathrm{mod}\,\varrho)}} \frac{\varrho}{\phi(\varrho)} \ll \frac{N}{\sqrt{\log N\log(N/R)}},$$

and from Lemma 2.7, the remainder is bounded by

$$\begin{aligned}(6.10)\qquad &\frac{N}{R\log(N/R)} \sum_{\exp(\sqrt{\log(N/R)})<2^i\le (N/R)^{\varepsilon}} 2^{-i}\\ &\qquad\times \sum_{\substack{R<\varrho\le 2R\\(\varrho,bc)=1\\ b\equiv\square \,(\mathrm{mod}\,\varrho)}} \frac{\varrho}{\phi(\varrho)} \sum_{\substack{2^i<k\le 2^{i+1}\\ \varrho\equiv a\square\,(\mathrm{mod}\,k)}} \frac{k}{\phi(k)}\\ &\ll \frac{N}{R\log(N/R)} \sum_i \frac{1}{\sqrt{\log(2^i)}}\cdot\frac{R}{\sqrt{\log R}} \ll \frac{N}{\sqrt{\log N\log(N/R)}}.\end{aligned}$$

Therefore, we have shown that

$$(6.11)\qquad \widehat{\Sigma}_I^1(N,R) \ll \frac{N}{\sqrt{\log N\log(N/R)}},$$

as desired.

- *Estimate of* $\widehat{\Sigma}_I^2(N,R)$. By a simple upper bound sieve, we have

$$\begin{aligned}(6.12)\qquad &\widehat{\Sigma}_I^2(N,R)\\ &\ll \sum_{\substack{R<\varrho\le 2R\\(\varrho,bc)=1\\ b\equiv\square \,(\mathrm{mod}\,\varrho)}} \mu^2(\varrho) \sum_{p\le (N/R)^{\varepsilon^2}} \sum_{\substack{(N/R)^{\varepsilon}/p<k\le (N/R)^{\varepsilon}\\ P(k)<p\\ \varrho\equiv a\square\,(\mathrm{mod}\,k)}} \mu^2(k) \sum_{\substack{K\le N/kp\\ p(K)>p\\ K\equiv c\overline{k}\overline{p}\,(\mathrm{mod}\,\varrho)}} 1\end{aligned}$$

$$\ll N \sum_{\substack{R<\varrho\le 2R\\(\varrho,bc)=1\\ b\equiv\square\,(\mathrm{mod}\,\varrho)}} \frac{\mu^2(\varrho)}{\phi(\varrho)} \sum_{p\le (N/R)^{\varepsilon^2}} \frac{1}{p\log p} \sum_{\substack{(N/R)^{\varepsilon}/p<k\le (N/R)^{\varepsilon}\\ P(k)<p\\ \varrho\equiv a\square\,(\mathrm{mod}\,k)}} \frac{\mu^2(k)}{k}.$$

For the innermost sum in (6.12), we have

$$\sum_{\substack{(N/R)^{\varepsilon}/p<k\le (N/R)^{\varepsilon}\\ P(k)<p\\ \varrho\equiv a\square\,(\mathrm{mod}\,k)}} \frac{\mu^2(k)}{k} \tag{6.13}$$

$$\ll \left(\log\frac{N}{R}\right)^{-2} \sum_{q'<p} \frac{\log q'}{q'} \sum_{q''<p} \frac{\log q''}{q''} \sum_{\substack{(N/R)^{\varepsilon}/pq'q''<k\le (N/R)^{\varepsilon}/q'q''\\ P(k)<p\\ \varrho\equiv a\square\,(\mathrm{mod}\,k)}} \frac{\mu^2(k)}{k}$$

$$\ll \left(\frac{\log p}{\log(N/R)}\right)^{2} \sum_{\substack{(N/R)^{\varepsilon/2}<k\le (N/R)^{\varepsilon}\\ \varrho\equiv a\square\,(\mathrm{mod}\,k)}} \frac{\mu^2(k)}{k}.$$

Hence, similar to the estimate of (6.10), an application of Lemma 2.7 yields

$$\widehat{\Sigma}_I^2(N,R) \tag{6.14}$$

$$\ll \frac{N}{(\log(N/R))^2} \sum_{p\le (N/R)^{\varepsilon^2}} \frac{\log p}{p} \sum_{\substack{R<\varrho\le 2R\\(\varrho,bc)=1\\ b\equiv\square\,(\mathrm{mod}\,\varrho)}} \frac{\mu^2(\varrho)}{\phi(\varrho)} \sum_{\substack{(N/R)^{\varepsilon/2}<k\le (N/R)^{\varepsilon}\\ \varrho\equiv a\square\,(\mathrm{mod}\,k)}} \frac{\mu^2(k)}{k}$$

$$\ll \frac{N}{\log(N/R)} \sum_{H} \sum_{\substack{R<\varrho\le 2R\\(\varrho,bc)=1\\ b\equiv\square\,(\mathrm{mod}\,\varrho)}} \frac{\mu^2(\varrho)}{\phi(\varrho)} \sum_{\substack{H<k\le 2H\\ \varrho\equiv a\square\,(\mathrm{mod}\,k)}} \frac{\mu^2(k)}{k}$$

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

In view of (6.4) and (6.5), the estimates (6.11) and (6.14) together yield

$$\widehat{S}_I(N) \ll N,$$

which, along with our discussion at the very beginning of this section, implies that

$$S_1(a;X) \ll X. \tag{6.15}$$

7. Estimate of $S_2(a;X)$. We set

$$\widehat{F} := \exp((\log X)^{1/6}). \tag{7.1}$$

Let $S_{21}(a;X)$ be the subsum of (5.3) subject to $u_0, \beta > \widehat{F}$ and $u_0\beta \le X/\widehat{F}$, and $S_{22}(a;X)$ the rest, both also with the conditions $u_0 > 1$ and $\beta > 1$.

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

$$\widehat{\Sigma}_{21} := \sum_{U<u_0\le 2U} \mu^2(u_0) \times \sum_{\substack{B<\beta\le 2B\\ \kappa u_0\equiv\square \,(\mathrm{mod}\,\beta)\\ \mu\beta\equiv\square\,(\mathrm{mod}\,u_0)\\ (\beta,u_0)=1}} \mu^2(\beta) \sum_{\substack{\xi,\varrho\\ \varrho\beta\equiv\square\,(\mathrm{mod}\,\varrho)\\ \nu u_0\equiv\square\,(\mathrm{mod}\,\xi)}} \mu^2(\xi)\mu^2(\varrho), \tag{7.2}$$

where, in the inner sum, ξ and ϱ also satisfy $\varrho \le X/u_0j^2$ and $j^2u_0\varrho - h^2\beta\xi = a/\Delta$.

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

$$\widehat{\Sigma}_{21} \ll_a \frac{X}{(hj)^{1+\delta}\sqrt{\log B \log U}\log(X/UB)} \tag{7.3}$$

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

$$\varrho = npN, \quad \xi = mqM, \tag{7.4}$$

where p and q are prime,

$$P(n) < p < p(N), \quad P(m) < q < p(M), \tag{7.5}$$

and

$$\left(\frac{X}{UB}\right)^{\varepsilon} < np \le p\left(\frac{X}{UB}\right)^{\varepsilon}, \quad \left(\frac{X}{UB}\right)^{\varepsilon} < mq \le q\left(\frac{X}{UB}\right)^{\varepsilon}. \tag{7.6}$$

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

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

$$\widehat{\Sigma}_{211} \ll \sum_{U<u_0\le 2U} \mu^2(u_0) \times \sum_{\substack{B<\beta\le 2B\\ \kappa u_0\equiv\square \,(\mathrm{mod}\,\beta)\\ \mu\beta\equiv\square\,(\mathrm{mod}\,u_0)\\ (\beta,u_0)=1}} \mu^2(\beta) \sum_{\substack{m,n\le (X/UB)^{\varepsilon}\\ \varrho\beta\equiv\square\,(\mathrm{mod}\,n)\\ \nu u_0\equiv\square\,(\mathrm{mod}\,m)}} \mu^2(mn) \sum_{M,N} 1, \tag{7.7}$$

where, in the innermost sum, M and N are subject to

$$j^2u_0nN - h^2\beta mM = a/\Delta, \tag{7.8}$$

and

$$p(MN) > \left(\frac{X}{UB}\right)^{\varepsilon^2}. \tag{7.9}$$

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 have leading coefficients j^2u_0n and $h^2\beta m$ respectively, and thus the variable k is running up to at most $X/\Delta(hj)^2u_0\beta mn$. Applying a 2-dimensional upper bound sieve (e.g., [6, Theorem 2.2]), we find that the innermost sum of (7.7) is bounded by

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

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

$$\begin{aligned}\frac{X(\log(X/UB))^{-2}}{\Delta\phi((hj)^2)} &\sum_{U<u_0\le 2U}\frac{\mu^2(u_0)}{\phi(u_0)}\\ &\times\sum_{\substack{B<\beta\le 2B\\ \kappa u_0\equiv\square\,(\mathrm{mod}\,\beta)\\ \mu\beta\equiv\square\,(\mathrm{mod}\,u_0)}}\frac{\mu^2(\beta)}{\phi(\beta)}\sum_{\substack{m,n\le(X/UB)^{\varepsilon}\\ \varrho\beta\equiv\square\,(\mathrm{mod}\,n)\\ \nu u_0\equiv\square\,(\mathrm{mod}\,m)}}\frac{\mu^2(mn)}{\phi(mn)}.\end{aligned} \tag{7.10}$$

Thus, in view of (7.3), it suffices to show that

$$\begin{aligned}\sum_{U<u_0\le 2U}\frac{\mu^2(u_0)}{\phi(u_0)}\sum_{\substack{B<\beta\le 2B\\ \kappa u_0\equiv\square\,(\mathrm{mod}\,\beta)\\ \mu\beta\equiv\square\,(\mathrm{mod}\,u_0)}}\frac{\mu^2(\beta)}{\phi(\beta)}\sum_{\substack{m,n\le(X/UB)^{\varepsilon}\\ \varrho\beta\equiv\square\,(\mathrm{mod}\,n)\\ \nu u_0\equiv\square\,(\mathrm{mod}\,m)}}\frac{\mu^2(mn)}{\phi(mn)}\\ \ll\frac{\log(X/UB)}{\sqrt{\log U\log B}}.\end{aligned} \tag{7.11}$$

We see that, by reformulating the congruence restrictions, it suffices to show that $\log(X/UB)/\sqrt{\log U\log B}$ is an upper bound for

$$\begin{aligned}\sum_{\substack{U<u_1u_2\le 2U\\ B<b_1b_2\le 2B}}&\frac{\left(\frac{\kappa u_1u_2}{b_1}\right)\left(\frac{\mu b_1b_2}{u_1}\right)}{\phi(u_1u_2b_1b_2)2^{\omega(u_1u_2b_1b_2)}}\\ &\times\sum_{\substack{m_1m_2\le(X/UB)^{\varepsilon}\\ n_1n_2\le(X/UB)^{\varepsilon}}}\frac{\left(\frac{\nu u_1u_2}{m_1}\right)\left(\frac{\varrho b_1b_2}{n_1}\right)}{\phi(m_1m_2n_1n_2)2^{\omega(m_1m_2n_1n_2)}},\end{aligned} \tag{7.12}$$

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 $\widehat{\Sigma}_{211}$, it suffices to show that $\log(X/UB)/\sqrt{\log U \log B}$ is an upper bound for the two sums $\widehat{\Sigma}^{\alpha}_{211}$ and $\widehat{\Sigma}^{\beta}_{211}$, respectively given by

$$\sum_{\substack{u_1,b_1\le T\\ U/u_1<u_2\le 2U/u_1\\ B/b_1<b_2\le 2B/b_1}} \frac{\left(\frac{\kappa u_1u_2}{b_1}\right)\left(\frac{\mu b_1b_2}{u_1}\right)}{\phi(u_1u_2b_1b_2)2^{\omega(u_1u_2b_1b_2)}}\,S$$

and

$$\sum_{\substack{u_2,b_2\le T\\ U/u_2<u_1\le 2U/u_2\\ B/b_2<b_1\le 2B/b_2}} \frac{\left(\frac{\kappa u_1u_2}{b_1}\right)\left(\frac{\mu b_1b_2}{u_1}\right)}{\phi(u_1u_2b_1b_2)2^{\omega(u_1u_2b_1b_2)}}\,S$$

with

$$S = \sum_{\substack{m_1,n_1\le T\\ m_2\le (X/UB)^{\varepsilon}m_1^{-1}\\ n_2\le (X/UB)^{\varepsilon}n_1^{-1}}} \frac{\left(\frac{\nu u_1u_2}{m_1}\right)\left(\frac{\varrho b_1b_2}{n_1}\right)}{\phi(m_1m_2n_1n_2)2^{\omega(m_1m_2n_1n_2)}},$$

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

To estimate $\widehat{\Sigma}^{\alpha}_{211}$, we sum over u_2 first. When $m_1b_1 \neq 1$, Lemma 2.5 implies that the inner sum over u_2 is

$$\sum_{\substack{U/u_1<u_2\le 2U/u_1\\ (u_2,2b_2m_2n_1n_2u_1)=1}} \frac{\mu^2(u_2)\left(\frac{u_2}{m_1b_1}\right)}{\phi(u_2)2^{\omega(u_2)}} \ll \tau(b_2m_2n_1n_2u_1)(\log X)^{-4}, \tag{7.13}$$

which implies that the terms with $m_1b_1 \neq 1$ contribute to $\widehat{\Sigma}^{\alpha}_{211}$ at most

$$\begin{aligned} &\ll (\log X)^{-4} \sum_{u_1,b_1,b_2,m_1,m_2,n_1,n_2} \frac{1}{\phi(u_1b_1b_2m_1m_2n_1n_2)} \\ &\ll (\log X)^{-4}(\log X)^2(\log T)^4 \ll (\log X)^{-1}, \end{aligned} \tag{7.14}$$

which is admissible. Similarly, by summing over b_2 first, those terms with

$n_1u_1 \neq 1$ contribute negligible errors to $\widehat{\Sigma}^{\alpha}_{211}$ too. Therefore, we essentially have

$$\begin{aligned}\widehat{\Sigma}^{\alpha}_{211} &\ll \sum_{\substack{U<u_2\leq 2U\\ B<b_2\leq 2B}} \frac{1}{\phi(u_2b_2)2^{\omega(u_2b_2)}}\Bigg(\sum_{m\leq (X/UB)^{\varepsilon}} \frac{1}{\phi(m)2^{\omega(m)}}\Bigg)^2 \\ &\ll \frac{\log(X/UB)}{\sqrt{\log U\log B}},\end{aligned} \tag{7.15}$$

as required.

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

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

$$\widehat{\Sigma}_{211} \ll \frac{X}{\Delta\phi((hj)^2)\sqrt{\log B\log U\log(X/UB)}}, \tag{7.16}$$

which agrees with (7.3).

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

$$\begin{aligned}&\frac{X}{\Delta\phi((hj)^2)} \sum_{\substack{U<u_0\leq 2U\\ B<\beta\leq 2B\\ \kappa u_0\equiv\square\,(\mathrm{mod}\,\beta)\\ \mu\beta\equiv\square\,(\mathrm{mod}\,u_0)}} \frac{\mu^2(u_0\beta)}{\phi(u_0\beta)} \\ &\qquad\times \sum_{p\leq (X/UB)^{\varepsilon^2}} \frac{1}{p(\log p)^2} \sum_{\substack{m\leq (X/UB)^{\varepsilon}\\ (X/UB)^{\varepsilon}p^{-1}<n\leq (X/UB)^{\varepsilon}\\ P(n)<p\\ \varrho\beta\equiv\square\,(\mathrm{mod}\,n)\\ \nu u_0\equiv\square\,(\mathrm{mod}\,m)}} \frac{\mu^2(mn)}{\phi(mn)}.\end{aligned} \tag{7.17}$$

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

$$\begin{aligned}&\frac{X}{\Delta\phi((hj)^2)} \sum_{\substack{U<u_2\leq 2U\\ B<b_2\leq 2B}} \frac{1}{\phi(u_2b_2)2^{\omega(u_2b_2)}} \sum_{m\leq (X/UB)^{\varepsilon}} \frac{1}{\phi(m)2^{\omega(m)}} \\ &\qquad\times \sum_{p\leq (X/UB)^{\varepsilon^2}} \frac{1}{p(\log p)^2} \sum_{\substack{(X/UB)^{\varepsilon}p^{-1}<n\leq (X/UB)^{\varepsilon}\\ P(n)<p}} \frac{1}{\phi(n)2^{\omega(n)}}\end{aligned} \tag{7.18}$$

$$\begin{aligned}
&\ll \frac{X\sqrt{\log(X/UB)}}{\Delta\phi((hj)^2)}\cdot\frac{1}{\sqrt{\log B\log U}}\\
&\quad\times\sum_{p\le(X/UB)^{\varepsilon^2}}\frac{1}{p(\log p)^2}\biggl(\frac{\log p}{\log(X/UB)}\biggr)^3\sum_{n'\le(X/UB)^{\varepsilon}}\frac{2^{-\omega(n')}}{\phi(n')}\\
&\ll \frac{X\sqrt{\log(X/UB)}}{\Delta\phi((hj)^2)}\cdot\frac{1}{\sqrt{\log B\log U}}\cdot\frac{1}{(\log(X/UB))^{3/2}}\\
&\ll \frac{X}{\Delta\phi((hj)^2)\sqrt{\log B\log U}\log(X/UB)},
\end{aligned}$$

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 $u_0,\beta>\sqrt{X}/\widehat{F}$ and $S_{222}(a;X)$ subject to u_0 or $\beta\le\widehat{F}$.

For $S_{221}(a;X)$, we simply discard three congruences in (5.3) and, by comparison with (7.2), we get

$$\begin{aligned}
S_{221}(a;X)&\ll\sum_{h,j}\sum_{\substack{\sqrt{X}/\widehat{F}<u_0\le\sqrt{X}/j\\ \sqrt{X}/\widehat{F}<\beta\le\sqrt{X}/h\\ \kappa u_0\equiv\square\,(\mathrm{mod}\,\beta)}}\mu^2(2u_0\beta)\sum_{\xi,\varrho}1\\
&\ll\sum_{h,j}\sum_{\substack{\sqrt{X}/\widehat{F}<u_0\le\sqrt{X}/j\\ \sqrt{X}/\widehat{F}<\beta\le\sqrt{X}/h\\ \kappa u_0\equiv\square\,(\mathrm{mod}\,\beta)}}\mu^2(2u_0\beta)\biggl(1+\frac{X}{\Delta(hj)^2u_0\beta}\biggr)\\
&=:\Sigma'_{221}+\Sigma''_{221},\quad\text{say,}
\end{aligned}\tag{7.19}$$

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

$$\Sigma'_{221}\ll\sum_{h,j}\sum_{\substack{\sqrt{X}/\widehat{F}<u_0\le\sqrt{X}/j\\ \sqrt{X}/\widehat{F}<\beta\le\sqrt{X}/h}}\frac{\mu^2(2u_0\beta)}{2^{\omega(\beta)}}\sum_{\beta_1\mid\beta}\biggl(\frac{\kappa u_0}{\beta_1}\biggr).\tag{7.20}$$

We consider the sum in dependence on the size of β_1.

(1) $\beta_1>(\log X)^{100}$; both of the ranges of u_0 and β_1 are long 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) $1<\beta_1\le(\log X)^{100}$; 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

$$\ll \sum_{h,j} \sum_{u_0} \sum_{\beta} 2^{-\omega(\beta)} \ll \sum_{h,j} \frac{X(\log X)^{-1/2}}{hj} \ll X(\log X)^{-1/3}. \tag{7.21}$$

From the above discussion, we thus have

$$\Sigma'_{221} \ll X(\log X)^{-1/3}. \tag{7.22}$$

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

$$\Sigma''_{221} \ll X(\log X)^{-1/6}. \tag{7.23}$$

Therefore, we have shown that

$$S_{221}(a; X) \ll X(\log X)^{-1/6}. \tag{7.24}$$

For $S_{222}(a; X)$, we let

$$\Omega := \exp\left(\frac{\log X}{(\log\log X)^{3/2}}\right), \quad \Phi := \Phi(\Omega) = \Omega^{100\log\log X}. \tag{7.25}$$

First we note that

$$S_{222}(a; X) \ll \sum_{\substack{u_0,\beta \\ \kappa u_0 \equiv \square \,(\mathrm{mod}\,\beta) \\ \mu\beta \equiv \square \,(\mathrm{mod}\,u_0)}} \mu^2(2u_0\beta) \sum_{\substack{\xi,\varrho \\ \varrho\beta \equiv \square \,(\mathrm{mod}\,\varrho) \\ \nu u_0 \equiv \square \,(\mathrm{mod}\,\xi)}} \mu^2(\xi)\mu^2(\varrho), \tag{7.26}$$

where in the inner sum ξ, ϱ also satisfy $\varrho \le X/u_0 j^2$ and $j^2 u_0 \varrho - h^2\beta\xi = a/\Delta$. Now we write

$$\varrho := nN, \quad \xi := mM, \tag{7.27}$$

with mn being Ω-smooth and $p(MN) > \Omega$. Then, apart from some very small error terms,

$$S_{222}(a; X) \ll \sum_{h,j} \sum_{\substack{u_0,\beta \\ \kappa u_0 \equiv \square \,(\mathrm{mod}\,\beta) \\ \mu\beta \equiv \square \,(\mathrm{mod}\,u_0)}} \mu^2(2u_0\beta) \sum_{\substack{m,n \le \Phi \\ \varrho\beta \equiv \square \,(\mathrm{mod}\,n) \\ \nu u_0 \equiv \square \,(\mathrm{mod}\,m)}} \mu^2(mn) \sum_{M,N} 1, \tag{7.28}$$

where in the inner sum M and N satisfy $nN \le X/u_0 j^2$, $j^2 u_0 nN - h^2\beta mM = a/\Delta$ 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),

$$S_{222}(a;X) \ll \frac{X}{(\log\Omega)^2} \sum_{\substack{1<u_0,\beta\le\sqrt{X}\\ u_0 \text{ or } \beta\le\widehat{F}\\ \kappa u_0\equiv\square \pmod\beta\\ \mu\beta\equiv\square\pmod{u_0}}} \frac{\mu^2(2u_0\beta)}{\phi(u_0\beta)} \sum_{\substack{m,n\le\Phi\\ \varrho\beta\equiv\square\pmod n\\ \nu u_0\equiv\square\pmod m}} \frac{\mu^2(mn)}{\phi(mn)} \tag{7.29}$$

$$\ll \frac{X(\log\log X)^7}{(\log X)^2} \sum_{\substack{1<u_0,\beta\le\sqrt{X}\\ u_0 \text{ or } \beta\le\widehat{F}\\ \kappa u_0\equiv\square \pmod\beta\\ \mu\beta\equiv\square\pmod{u_0}}} \frac{\mu^2(2u_0\beta)}{u_0\beta} \sum_{\substack{m,n\le\Phi\\ \varrho\beta\equiv\square\pmod n\\ \nu u_0\equiv\square\pmod m}} \frac{\mu^2(mn)}{mn}.$$

The fixed variables κ,μ,ϱ,ν have no specific effects here, u_0 and β are essentially symmetric. So we shall just consider the subsum with $1<u_0\le\widehat{F}$, which is bounded by

$$\frac{X(\log\log X)^7}{(\log X)^2} \sum_{\substack{1<\beta\le(\log X)^{100}\\ 1<u_0\le\widehat{F}}} \frac{\mu^2(2u_0\beta)}{u_0\beta} \sum_{\substack{m,n\le\Phi\\ \varrho\beta\equiv\square\pmod n}} \frac{\mu^2(mn)}{mn} \tag{7.30}$$

$$+ \frac{X(\log\log X)^7}{(\log X)^2} \sum_{\substack{(\log X)^{100}<\beta\le\sqrt{X}\\ 1<u_0\le\widehat{F}\\ \kappa u_0\equiv\square\pmod\beta}} \frac{\mu^2(2u_0\beta)}{u_0\beta} \sum_{\substack{m,n\le\Phi\\ \varrho\beta\equiv\square\pmod n\\ \nu u_0\equiv\square\pmod m}} \frac{\mu^2(mn)}{mn}.$$

The first sum in (7.30), by applying Perron's formula and the zero-free region of L-functions, is simply bounded by

$$\frac{X(\log\log X)^7}{(\log X)^2} \sum_{\substack{1<\beta\le(\log X)^{100}\\ 1<u_0\le\widehat{F}}} \frac{\mu^2(2u_0\beta)}{u_0\beta}\cdot(\log\Phi)^{3/2} \tag{7.31}$$

$$\ll \frac{X(\log\log X)^7}{(\log X)^2}\cdot\log\widehat{F}\cdot\log\log X\cdot(\log\Phi)^{3/2} \ll \frac{X(\log\log X)^9}{(\log X)^{1/3}},$$

which is admissible for our requirement.

By reformulating the congruences attached to the innermost sum, the second sum in (7.30) can be rewritten as

$$\frac{X(\log\log X)^7}{(\log X)^2} \sum_{\substack{(\log X)^{100}<\beta\le\sqrt{X}\\ 1<u_0\le\widehat{F}\\ \kappa u_0\equiv\square\pmod\beta}} \frac{\mu^2(2u_0\beta)}{u_0\beta} \times \sum_{m,n\le\Phi} \frac{\mu^2(mn)}{mn2^{\omega(mn)}} \sum_{\substack{m_1\mid m\\ n_1\mid n}} \left(\frac{\nu u_0}{m_1}\right)\left(\frac{\varrho\beta}{n_1}\right). \tag{7.32}$$

Then from Lemma 2.2 and Perron's formula, combined with the zero-free region of L-functions, this is

$$\begin{aligned}(7.33)\quad &\ll \frac{X\sqrt{\log \Phi}(\log\log X)^7}{(\log X)^2} \sum_{\substack{(\log X)^{100}<\beta\le\sqrt{X}\\ 1<u_0\le \widehat{F}\\ \kappa u_0\equiv \square \,(\mathrm{mod}\,\beta)}} \frac{\mu^2(2u_0\beta)}{u_0\beta}\\ &\quad\times \sum_{\substack{m_1m_2\le\Phi\\ m_1\le(\log X)^{100}}} \frac{1}{m_1m_2 2^{\omega(m_1m_2)}}\\ &\ll \frac{X(\log\log X)^7}{\log X} \sum_{1<u_0\le(\log X)^{100}} \frac{1}{u_0}\cdot\sqrt{\log X}\\ &\quad+\frac{X(\log\log X)^7}{\log X} \sum_{(\log X)^{100}<u_0\le\widehat{F}} \frac{1}{u_0} \sum_{\substack{\beta_1\beta_2\le\sqrt{X}\\ \beta_1\le(\log X)^{100}}} \frac{1}{\beta_1\beta_2 2^{\omega(\beta_1\beta_2)}}\\ &\ll \frac{X(\log\log X)^8}{(\log X)^{1/3}}.\end{aligned}$$

Hence, from (7.29)–(7.33), we have shown that

$$(7.34)\qquad S_{222}(a;X)\ll X(\log X)^{-1/6}.$$

Together with (7.24), this implies that

$$(7.35)\qquad S_{22}(a;X)\ll X(\log X)^{-1/6}.$$

Therefore, we have proved that

$$(7.36)\qquad S_2(a;X)\ll X.$$

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

References

[1] R. Bölling, *Die Ordnung der Schafarewitsch–Tate Gruppe kann beliebig gross werden*, Math. Nachr. 67 (1975), 157–179.
[2] E. Bombieri, *On the large sieve*, Mathematika 12 (1965), 201–225.
[3] D. A. Burgess, *On character sums and L-series, II*, Proc. London Math. Soc. (3) 13 (1963), 524–536.
[4] H. Davenport, *Multiplicative Number Theory*, 2nd ed., Grad. Texts in Math. 74, Springer, 1980.
[5] E. Fouvry and H. Iwaniec, *The divisor function over arithmetic progressions*, Acta Arith. 61 (1992), 271–287.
[6] H. Halberstam and H. E. Richert, *Sieve Methods*, London Math. Soc. Monogr., Academic Press, 1974.

[7] D. R. Heath-Brown, *The size of Selmer groups for the congruent number problem I*, Invent. Math. 111 (1993), 171–195.
[8] —, *The size of Selmer groups for the congruent number problem II*, ibid. 118 (1994), 331–370.
[9] A. Ivić, *The Riemann Zeta-Function*, Wiley, 1985.
[10] A. A. Karatsuba, *Basic Analytic Number Theory*, translated from the Russian by M. B. Nathanson, Springer, 1993.
[11] K. Kramer, *A family of semistable elliptic curves with large Tate–Shafarevich groups*, Proc. Amer. Math. Soc. 89 (1983), 379–386.
[12] J. Silverman, *The Arithmetic of Elliptic Curves*, Grad. Texts in Math. 106, Springer, 1986.
[13] G. Yu, *Rank* 0 *quadratic twists of a family of elliptic curves*, Compositio Math. 135 (2003), 331–356.
[14] —, *Average size of* 2*-Selmer groups of a family of elliptic curves*, Trans. Amer. Math. Soc., to appear.

Department of Mathematics
The University of Michigan
525 E. University Avenue
Ann Arbor, MI 48109-1109, U.S.A.
E-mail:

Current address:
Department of Mathematics
The University of South Carolina
1523 Greene Street
Columbia, SC 29208, U.S.A.
E-mail: yu@math.sc.edu

Received on 26.6.2003
and in revised form on 17.7.2004 (4567)