TRANSACTIONS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 358, Number 4, Pages 1563–1584
S 0002-9947(05)03806-7
Article electronically published on October 31, 2005

# AVERAGE SIZE OF 2-SELMER GROUPS OF ELLIPTIC CURVES, I

GANG YU

ABSTRACT. In this paper, we study a class of elliptic curves over $\mathbb{Q}$ with $\mathbb{Q}$-torsion group $\mathbb{Z}_2 \times \mathbb{Z}_2$, and prove that the average order of the 2-Selmer groups is bounded.

## 1. INTRODUCTION

For a given elliptic curve $E$ defined over $\mathbb{Q}$, we denote by $\mathrm{Sel}_2(E/\mathbb{Q})$ the 2-Selmer group of $E$ over $\mathbb{Q}$.[1] It is known that the order of $\mathrm{Sel}_2(E/\mathbb{Q})$ can be arbitrarily large (cf. [1], [8]). For a more explicit example, one can refer to the construction of Heath-Brown [5] of congruent number curves with large 2-Selmer groups.

In [5], Heath-Brown also considered the average order of the 2-Selmer groups of the congruent number curves

$$E_D: \quad y^2 = x^3 - D^2 x,$$

with $D$ being squarefree. He showed that the average order of $\mathrm{Sel}_2(E_D/\mathbb{Q})$, as $D \to \infty$, is 12.

Our special interest in this paper will be about the average size of $\mathrm{Sel}_2(E(a,b)/\mathbb{Q})$, where $E(a,b)$ is given by

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

with $a$ and $b$ being integers satisfying $ab(a-b) \neq 0$.

Based on his numerical investigations, A. Brumer asked: Is the average order of the 2-Selmer groups of the curves $E(a,b)$ unbounded? Here the meaning of "average" is with $|a|$, $|b| < X$ for any sufficiently large parameter $X$.

For elliptic curve $E(a,b)$, one can carry out the complete 2-descent procedure over $\mathbb{Q}$ (cf. [10, Chapter 10, Proposition 1.4]). Following the reductions people generally do in this case (cf. [5], for example), we shall give the explicit form of the related homogeneous spaces in (2.5) and thereafter be able to describe the order of $\mathrm{Sel}_2(E(a,b)/\mathbb{Q})$ in a way related to quadratic residues. By estimating character sums and appealing to a simple upper bound sieve, we are able to answer Brumer's question as follows.

Received by the editors September 16, 2000 and, in revised form, May 2, 2004.
2000 *Mathematics Subject Classification.* Primary 11G05, 14H52.
*Key words and phrases.* Elliptic curves, 2-descent procedure, character sums.

[1] For the readers who are not familiar with elliptic curves, the definition of Selmer group can be found in [10, pages 296–297]. For each curve $E(a,b)$ that is considered in this paper, via complete 2-descent over $\mathbb{Q}$, $\mathrm{Sel}_2(E/\mathbb{Q})$ is essentially the 2-group consist of the homogeneous spaces (2.5) that possess a nontrivial point in $\mathbb{Q}_p^4$ for every $p$ (including $\mathbb{Q}_\infty = \mathbb{R}$). The group operation of homogeneous spaces can also be found in [10, page 288].

**Theorem 1.** *Suppose $X$ is sufficiently large. Let*

$$S(X) := \sum_{\substack{1<|a|,|b|\le X \\ a\neq b}} \#Sel_2(E(a,b)/\mathbb{Q}). \tag{1.1}$$

*Then there exist some positive constants $c_1$ and $c_2$, both being absolute, such that*

$$c_1X^2 < S(X) \le c_2X^2. \tag{1.2}$$

For any elliptic curve $E(a,b)$, we denote its Mordell-Weil rank $r(E(a,b))$. Then Theorem 1 yields

**Corollary.** *Suppose $X$ is sufficiently large. Then there exists an absolute constant $c_3 > 0$ such that*

$$\sum_{\substack{1<|a|,|b|\le X \\ a\neq b}} 2^{r(E(a,b))} \le c_3X^2. \tag{1.3}$$

It is possible, following our proof for Theorem 1, to get an explicit constant $c_3$ in the Corollary. Such kinds of results are of great interest to many number theorists (eg. [2]). In this paper, however, we shall not do so because the curves in our question comprise a very small subset of the curves over $\mathbb{Q}$.

Throughout the paper, for odd integer $m$, by $\left(\frac{\cdot}{m}\right)$ we denote the Jacobi symbol modulo $m$; for positive integer $n$, we denote by $\tau_k(n)$ the number of ways to represent $n$ as the product of $k$ positive integers; and $\tau_2(n) := \tau(n)$ is thus the ordinary divisor function; by $s(n)$ we denote the "squarefull part" of $n$, namely the greatest squarefull divisor of $n$; by $P(n)$ and $p(n)$ we denote respectively the largest and the smallest prime divisors of $n$; by $\omega(n)$ we denote the number of distinct prime divisors of $n$; by $\mu(n)$ we denote the Möbius function, namely $\mu(n) = (-1)^{\omega(n)}$ if $n$ is squarefree and $\mu(n) = 0$ otherwise; for integers $m$ and $n$, where $n > 0$ and $(m,n) = 1$, the congruence

$$m \equiv \square \pmod{n}$$

means $m \in (\mathbb{Z}/n\mathbb{Z})^{\times 2}$. Throughout and henceforth, $\epsilon$ will be defined as a sufficiently small positive constant, not necessarily the same at each appearance; any capital letter, if involved in expressing the range of a variable, always takes a power of 2.

## 2. Transformation

Note the lower bound is trivial; we shall only show the upper bound. Let $S^+(X)$ be the subsum of $S(X)$ with both $a$ and $b$ being positive. Then we see that $S(X) \ll S^+(2X)$. Thus, to prove an upper bound, we just need to consider the curves $E(a,b)$ with both $a$ and $b$ being positive. Hence, we shall prove the claimed upper bound for the sum of the orders of 2-Selmer groups of the curves

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

with $1 \le a, b \le X$ and $a \neq b$.

We shall define by $\Delta$ the greatest common divisor of $a$ and $b$, and the curves in consideration are thus

$$E(a\Delta, b\Delta) : \quad y^2 = x(x+a\Delta)(x+b\Delta), \tag{2.1}$$

with $\Delta \le X$, $1 \le a, b \le X/\Delta$, $a \neq b$ and $(a,b) = 1$. We may and shall only consider the curves satisfying $b < a$.

Note the curve $E(a\Delta, b\Delta)$ has 2-torsion $\mathbb{Z}_2 \times \mathbb{Z}_2$. The image of the canonical "2-descent" map (cf. [10, Chapter 10, Proposition 1.4])

$$\theta: \quad \frac{E(a\Delta, b\Delta)(\mathbb{Q})}{2E(a\Delta, b\Delta)(\mathbb{Q})} \quad \longrightarrow \quad G \quad \times \quad G, \qquad \text{where} \qquad G := \frac{\mathbb{Q}^\times}{\mathbb{Q}^{\times 2}},$$

has size $2^{r(E(a\Delta,b\Delta))+2}$, where for $P := (x, y) \in E(a\Delta, b\Delta)(\mathbb{Q})$,

$$\theta(P) = \begin{cases} (x + a\Delta, x + b\Delta) & (\text{mod } \mathbb{Q}^\times)^2, \text{ if } x \neq 0, -a, \\ (a, b) & (\text{mod } \mathbb{Q}^\times)^2, \text{ if } x = 0, \\ (a(a-b), b-a) & (\text{mod } \mathbb{Q}^\times)^2, \text{ if } x = -a, \\ (1, 1) & (\text{mod } \mathbb{Q}^\times)^2, \text{ if } x = \infty. \end{cases}$$

Now suppose we have a curve $E(a\Delta, b\Delta)$ given by (2.1). Similar to [5], we start the complete 2-descent procedure letting $\left(\frac{r}{t^2}, \frac{s}{t^3}\right)$ be a representative of any non-torsion point $P \in E(a\Delta, b\Delta)(\mathbb{Q})$ in the coset $P + \text{Tors}(E(a\Delta, b\Delta)(\mathbb{Q}))$, satisfying $r, s > 0$ and $(rs, t) = 1$. (Note that there are precisely two such representatives in $P + \text{Tors}(E(a\Delta, b\Delta)(\mathbb{Q}))$. We do not specify which one it is, and this does not matter much because we are only trying to prove an upper bound.) Taking the coordinates into the equation, we have

$$s^2 = r(r + a\Delta t^2)(r + b\Delta t^2). \tag{2.2}$$

Suppose $(r, r + b\Delta t^2) := b_0\delta$, where $\delta \mid \Delta$, $b_0 \mid b$ such that $\left(b_0, \frac{\Delta}{\delta}\right) = 1$. Then, by writing $r = b_0\delta r'$ and noting that $\delta$ is squarefree, we have $\left(r', \frac{b\Delta}{b_0\delta}\right) = 1$, and equation (2.2) becomes

$$\delta\left(\frac{s}{\delta^2 b_0}\right)^2 = r'\left(b_0 r' + a \cdot \frac{\Delta}{\delta} t^2\right)\left(r' + \frac{b}{b_0} \cdot \frac{\Delta}{\delta} t^2\right). \tag{2.3}$$

We suppose $\left(r', b_0 r' + a \cdot \frac{\Delta}{\delta} t^2\right) := a_0$; then it is easy to see that $a_0 \mid a$ and $\left(a_0, \frac{\Delta}{\delta}\right) = 1$. If writing $r' = a_0 r''$, then we further have $\left(r'', \frac{a}{a_0} \cdot \frac{\Delta}{\delta} t^2\right) = 1$. Now the equation (2.3) becomes

$$\delta\left(\frac{s}{\delta^2 a_0 b_0}\right)^2 = r''\left(b_0 r'' + \frac{a}{a_0} \cdot \frac{\Delta}{\delta} \cdot t^2\right)\left(a_0 r'' + \frac{b}{b_0} \cdot \frac{\Delta}{\delta} \cdot t^2\right). \tag{2.4}$$

Finally, we suppose the greatest common divisor of the last two factors of the right-hand side of (2.4) is $\beta$. Then we see that $\beta \mid (a - b)$ and $\left(\beta, abr''t \cdot \frac{\Delta}{\delta}\right) = 1$. Therefore, we get homogeneous spaces described by the quadratic equation systems

$$\begin{cases} \delta_1 b_0 V^2 + \frac{a}{a_0} \cdot \frac{\Delta}{\delta} T^2 = \delta_2 \beta Y^2, \\ \delta_1 a_0 V^2 + \frac{b}{b_0} \cdot \frac{\Delta}{\delta} T^2 = \delta_3 \beta Z^2, \end{cases} \tag{2.5}$$

where $\delta = \delta_1\delta_2\delta_3$ is a factorization of $\delta$ such that all the coefficients in a single equation are pairwise coprime. We note that, modulo $\mathbb{Q}^{\times 2}$, two systems with the same values of $\delta_j$, $j = 1, 2, 3$, are equivalent if every one of $a_0$, $b_0$ and $\beta$ of one system differs from that corresponding to the other system by a square factor. Therefore, in counting admissible systems, $a_0$, $b_0$ and $\beta$ are always supposed to be squarefree.

We note that, with our choice of representatives of non-torsion point $P \in E(a\Delta, b\Delta)(\mathbb{Q})$ in the coset $P + \text{Tors}(E(a\Delta, b\Delta)(\mathbb{Q}))$, the number of systems (2.5) possessing a non-trivial solution in $\mathbb{Z}^4$ is precisely equal to $2^{r(E(a,b))+1}$ and the number of those which are non-trivially solvable in every local field $\mathbb{Q}_p$ is equal to $\frac{1}{2}\#\text{Sel}_2(E(a, b)/\mathbb{Q})$. This also implies that the order of $\text{Sel}_2(E(a\Delta, b\Delta)/\mathbb{Q})$ is

trivially bounded by $\tau(ab(a-b))\tau_4(\Delta)$. Note that, for integers $m$, $n$, we have $\tau(mn)\leq\tau(m)\tau(n)$, thus the sum of orders of the 2-Selmer groups of the curves $E(a\Delta,b\Delta)$ with $\Delta>(\log X)^5$ is bounded by

$$\begin{aligned}
&\sum_{\Delta>(\log X)^5}\tau_4(\Delta)\sum_{\substack{a\leq X/\Delta\\ b\leq X/\Delta}}\tau(ab(a-b))\\
&\ll\sum_{\Delta>(\log X)^5}\tau_4(\Delta)\Big(\sum_{\substack{a\leq X/\Delta\\ b\leq X/\Delta}}\tau^2(a)\tau(a-b)\sum_{\substack{a\leq X/\Delta\\ b\leq X/\Delta}}\tau^2(b)\tau(a-b)\Big)^{\frac{1}{2}} \qquad (2.6)\\
&\ll\sum_{\Delta>(\log X)^5}\tau_4(\Delta)\cdot\frac{X^2}{\Delta^2}(\log X)^4\\
&\ll X^2(\log X)^{-\frac{1}{2}}.
\end{aligned}$$

Here in (2.6) we have used the estimate (cf. [7, formula (5.24)])

$$\sum_{n\leq N}\tau^2(n)\ll N(\log N)^3.$$

Therefore, we shall merely consider the curves $E(a\Delta,b\Delta)$ with $\Delta\leq(\log X)^5$. It is also clear that we may only consider those curves with $\Delta$ being squarefree. Moreover, based on similar reasoning as in (2.6), we may only consider those $a$ and $b$ such that $s(a\Delta),s(b\Delta),s((a-b)\Delta)\leq(\log X)^5$.

We would like to write

$$\begin{cases} a_0:=a(1)a_1, & \frac{a}{a_0}:=a(2)a_2,\\ b_0:=b(1)b_1, & \frac{b}{b_0}:=b(2)b_2,\\ \beta:=c(1)c_1, & \frac{a-b}{\beta}:=c(2)c_2, \end{cases} \qquad (2.7)$$

such that all the prime divisors of $a(j)$, $b(j)$ and $c(j)$, $j=1,2$, respectively divide $2s(a\Delta)$, $2s(b\Delta)$ and $2s((a-b)\Delta)$, and the six variables $a_1,a_2,b_1,b_2,c_1$ and $c_2$ are odd, squarefree, pairwise coprime and prime to $a(1)$, $a(2)$, $b(1)$, $b(2)$, $c(1)$ and $c(2)$ in correspondent pairs. With this change, the system (2.6) becomes

$$\begin{cases} \delta_1 b(1)b_1V^2+a(2)a_2\cdot\frac{\Delta}{\delta}T^2=\delta_2c(1)c_1Y^2,\\ \delta_1 a(1)a_1V^2+b(2)b_2\cdot\frac{\Delta}{\delta}T^2=\delta_3c(1)c_1Z^2. \end{cases} \qquad (2.8)$$

From the definition of a 2-Selmer group, we see that $\#\mathrm{Sel}_2(E(a,b)/\mathbb{Q})$ is now equal to twice the number of inequivalent systems (2.8) that are non-trivially solvable in every $\mathbb{Q}_p$. We shall only consider those local fields $\mathbb{Q}_p$ for $p$ an odd prime divisor of $a_1a_2b_1b_2c_1c_2$, and thus we see that, to be everywhere locally solvable, (2.8) must satisfy the following conditions:

$$\begin{cases} \delta_1\delta_2b(1)c(1)b_1c_1 & \equiv\square \pmod{a_2},\\ \frac{\Delta}{\delta_1\delta_2}b(2)c(1)b_2c_1 & \equiv\square \pmod{a_1},\\ \delta_1\delta_3a(1)c(1)a_1c_1 & \equiv\square \pmod{b_2},\\ \frac{\Delta}{\delta_1\delta_3}a(2)c(1)a_2c_1 & \equiv\square \pmod{b_1},\\ -\frac{\Delta}{\delta_2\delta_3}a(2)b(1)a_2b_1 & \equiv\square \pmod{c_1},\\ \delta_2\delta_3a(1)b(1)a_1b_1 & \equiv\square \pmod{c_2}. \end{cases} \qquad (2.9)$$

Therefore, apart from some subsums with negligible contributions, the sum of the problem is about the variables $\Delta$, $\delta_\nu$, $\nu = 1, 2, 3$, $a(j), b(j), c(j), j = 1, 2$, and $a_j$, $b_j$, $c_j$, $j = 1, 2$, subject to (2.8) and that $\Delta \le (\log X)^5$, $\delta_1\delta_2\delta_3 \mid \Delta$, that $a(1)a(2), b(1)b(2), c(1)c(2) \le (\log X)^5$, $1 \le b(1)b(2)b_1b_2 < a(1)a(2)a_1a_2 \le X/\Delta$ and that $a(1)a(2)a_1a_2 - b(1)b(2)b_1b_2 = c(1)c(2)c_1c_2$. Moreover, $a(1)a(2)a_1a_2$, $b(1)b(2)b_1b_2$ and $c(1)c(2)c_1c_2$ are pairwise coprime, and $a_1$, $a_2$, $b_1$, $b_2$, $c_1$ and $c_2$ are odd, squarefree and pairwise coprime.

In what follows we shall only consider a sum about the six variables $a_1$, $a_2$, $b_1$, $b_2$, $c_1$ and $c_2$, with all the other variables regarded as fixed. For brevity, we denote this partial sum by $\tilde{S}(X)$. One should note that this sum depends on the variables other than the six in consideration. Let

$$D := a(1)a(2)b(1)b(2)c(1)c(2).$$

Note that $D\Delta^2$ runs over squarefull numbers and twice over squarefull numbers up to some power of $\log X$, and the factorizations of $D\Delta^2$ contribute $O((D\Delta^2)^\epsilon)$ for a fixed sufficiently small $\epsilon > 0$. To show that the whole sum is bounded by $X^2$, namely, to prove Theorem 1, it suffices to show the following

**Theorem 2.** *Suppose $X$ is sufficiently large. Then, under all the above conditions, for the fixed variables other than $a_j, b_j, c_j, j = 1, 2$,*

$$\tilde{S}(X) \ll \frac{X^2}{(D\Delta^2)^{\frac{1}{2}+2\epsilon}}, \tag{2.10}$$

*where the implied constant depends only on $\epsilon$.*

In case all the unimportant variables are fixed, to formally simplify the formulas with the congruence restrictions involved, we rewrite (2.9) as

$$\begin{cases} A(2)b_1c_1 \equiv \ \square \pmod{a_2}, \\ A(1)b_2c_1 \equiv \ \square \pmod{a_1}, \\ B(2)a_1c_1 \equiv \ \square \pmod{b_2}, \\ B(1)a_2c_1 \equiv \ \square \pmod{b_1}, \\ C(1)a_2b_1 \equiv \ \square \pmod{c_1}, \\ C(2)a_1b_1 \equiv \ \square \pmod{c_2}, \end{cases} \tag{2.11}$$

with all the new letters $A(j)$, $B(j)$ and $C(j)$, $j = 1, 2$, replacing the corresponding terms in (2.9).

These congruences will be referred to very often in estimating various sums. By abuse of notation, we shall use $\Sigma_{A(2)}$, for example, to indicate that the summation is subject to the first congruence in (2.11).

By $\tilde{S}_1(X)$ we denote the subsum of $\tilde{S}(X)$ subject to $b_1 \le \sqrt{X/\Delta b(1)b(2)}$ and $c_1 \le \sqrt{X/\Delta c(1)c(2)}$, and $a_1 \ge a_2$. We shall only estimate this subsum. From the proof for the upper bound of $\tilde{S}_1(X)$, it will be quite clear that the others can be handled in the same manner. Let

$$F := \exp\big((\log X)^{\frac{1}{6}}\big).$$

We divide the sum $\tilde{S}_1(X)$ into two parts: $\tilde{S}_{11}(X)$ subject to $\sqrt{X}/F < b_1, c_1 \le \sqrt{X}$ and $\tilde{S}_{12}(X)$ subject to $b_1$ or $c_1 \le \sqrt{X}/F$. We shall respectively estimate $\tilde{S}_{11}(X)$ and $\tilde{S}_{12}(X)$ in sections 4 and 5, showing that they are bounded by the upper bound of (2.10) to finish the proof of Theorem 2.

## 3. Some lemmas

In this section, we state some lemmas that we need in the estimation of $\tilde{S}_{11}(X)$ and $\tilde{S}_{12}(X)$.

**Lemma 3.1.** *Suppose $M$ and $N$ are sufficiently large real numbers, and $\{a_m\}$ and $\{b_n\}$ are two complex sequences satisfying $|a_m|$, $|b_n| \ll 1$. Then*

$$\sum_{m\le M} a_m \sum_{n\le N} b_n \left(\frac{m}{n}\right) \ll_\epsilon MN^{\frac{15}{16}+\epsilon} + M^{\frac{15}{16}+\epsilon}N. \tag{3.1}$$

*Proof.* This is essentially Lemma 4 of [5], proved based on the work of Burgess [3]. One can also refer to [11, Lemma 4.1]. □

**Lemma 3.2.** *Suppose $s$ is a fixed positive integer, and $\alpha(n)$ is a multiplicative function satisfying that there exists a positive constant $c$ such that, for every prime $p$,*

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

*Then for arbitrary positive integers $N$ and $r$, and any $\epsilon > 0$, there exists a positive constant $\kappa = \kappa_{c,s,\epsilon,N}$ such that for every $q \le \log^N x$ and any non-principal character $\chi(\mathrm{mod} q)$, we have*

$$\sum_{n\le x,(n,r)=1} \mu^2(n)s^{-\omega(n)}\alpha(n)\chi(n) \ll x\exp(-\kappa\sqrt{\log x}) + x^\epsilon \tau_x(r), \tag{3.2}$$

*where $\tau_x(r) = \sum_{d|r,d\le x} 1$ and the constant involved in the $\ll$-symbol depends on $c$, $s$ and $N$ only. In particular, if $r \ll x^A$ for some fixed constant $A$, we have*

$$\sum_{n\le x,(n,r)=1} \mu^2(n)s^{-\omega(n)}\alpha(n)\chi(n) \ll x\exp(-\kappa\sqrt{\log x}). \tag{3.3}$$

*Proof.* As a more general version of the Lemma 4.2 of [11], Lemma 2.5 in [12] gives

$$\sum_{n\le x,(n,r)=1} \mu^2(n)s^{-\omega(n)}\alpha(n)\chi(n) \ll x\tau(r)\exp(-\kappa_0\sqrt{\log x}), \tag{3.4}$$

for a constant $\kappa_0 = \kappa_0(c,s,N)$ and with the constant in the $\ll$-symbol depending on $c$, $s$ and $N$ only. To show (3.2), we first have

$$\begin{aligned}&\sum_{n\le x,(n,r)=1} \mu^2(n)s^{-\omega(n)}\alpha(n)\chi(n)\\ &\quad= \sum_{d|r} \mu(d)s^{-\omega(d)}\alpha(d)\chi(d) \sum_{\substack{m\le x/d\\(m,d)=1}} \mu^2(m)s^{-\omega(m)}\alpha(m)\chi(m).\end{aligned}$$

Note that $\alpha(k) \ll \left(\frac{k}{\phi(k)}\right)^c \ll (\log\log x)^c$ for $k$ satisfying $\log k \ll \log x$, and that $\tau(r) \ll x^{\epsilon/3}$ for any $\epsilon > 0$. Let $\epsilon > 0$ be a fixed small constant; the terms with $d > x^{1-\epsilon/2}$ contribute at most

$$\ll \sum_{\substack{d|r\\ x^{1-\epsilon/2}<d\le x}} |\alpha(d)| \cdot \frac{x(\log\log x)^c}{d} \ll x^\epsilon \tau_x(r).$$

For the other part, from (3.4), we have

$$\begin{aligned}
&\sum_{\substack{d|r\\ d\le x^{1-\epsilon/2}}} \mu(d)s^{-\omega(d)}\alpha(d)\chi(d)\sum_{\substack{m\le x/d\\ (m,d)=1}}\mu^2(m)s^{-\omega(m)}\alpha(m)\chi(m)\\
\ll&\sum_{\substack{d|r\\ d\le x^{1-\epsilon/2}}}\mu^2(d)|\alpha(d)|\cdot\frac{x}{d}\cdot\tau(d)\exp(-\kappa_0\sqrt{\log(x/d)})\\
\ll& x\exp(-\kappa_0\sqrt{\frac{\epsilon}{3}\log x})\sum_{d\le x^{1-\epsilon/2}}\frac{\tau(d)}{d}\\
\ll& x\exp(-\kappa_0\sqrt{\frac{\epsilon}{4}\log x}).
\end{aligned}$$

Letting $\kappa=\sqrt{\frac{\epsilon}{4}}\kappa_0$, we have proved (3.2). □

In the proof of Theorem 2, we shall also appeal to a simple upper bound sieve result.

**Lemma 3.3.** *Let $g$ be a natural number, and let $a_i, b_i$ $(i=1,2,\cdots,g)$ be pairs of integers satisfying*

$$(a_i,b_i)=1,\quad i=1,2,\cdots,g,$$

*and*

$$E:=\prod_{i=1}^{g}a_i\prod_{1\le i<j\le g}(a_ib_j-a_jb_i)\neq 0.$$

*For prime $p$, let $\rho(p)$ be the number of solutions of*

$$\prod_{i=1}^{g}(a_in+b_i)\equiv 0\pmod p.$$

*Then for any constant $\delta>0$ and $D\le x^{\delta}$, we have*

$$\#\{n\le x : p\mid\prod_{i=1}^{g}(a_in+b_i)\Rightarrow p>D\}\ll\prod_{p\mid E}\left(1-\frac{1}{p}\right)^{\rho(p)-g}\frac{x}{\log^g D},$$

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

*Proof.* This is a straightforward corollary of Theorem 2.2 in [4]. □

**Lemma 3.4.** *For $N\ge 3$, we have*

$$\sum_{n\le N}\frac{1}{\phi(n)2^{\omega(n)}}\ll\sqrt{\log N}\tag{3.5}$$

*and*

$$\sum_{N<n\le 2N}\frac{1}{\phi(n)2^{\omega(n)}}\ll\frac{1}{\sqrt{\log N}}.\tag{3.6}$$

*Proof.* We first recall the well-known result

$$\sum_{n\le N}2^{-\omega(n)}=(c+o(1))N(\log N)^{-\frac{1}{2}},\tag{3.7}$$

where $c > 0$ is a fixed constant (cf. [9], for example). By partial summation, this yields

$$\sum_{n\le N}\frac{1}{n2^{\omega(n)}} = (2c+o(1))(\log N)^{\frac{1}{2}}.$$

Thus, we have

$$\begin{aligned}\sum_{n\le N}\frac{1}{\phi(n)2^{\omega(n)}} &= \sum_{n\le N}\frac{1}{n2^{\omega(n)}}\prod_{d|n}\frac{\mu^2(d)}{\phi(d)}\\ &= \sum_{d\le N}\frac{\mu^2(d)}{d\phi(d)}\sum_{k\le N/d}\frac{1}{k2^{\omega(dk)}}\\ &\le \sum_{d\le N}\frac{1}{d\phi(d)}\sum_{k\le N/d}\frac{1}{k2^{\omega(d)}}\\ &\ll \sum_{d\le N}\frac{\sqrt{\log(2N/d)}}{d\phi(d)} \ll \sqrt{\log N},\end{aligned}$$

which gives (3.5). Similarly, we can prove (3.6). □

The following two lemmas will be frequently referred to in the estimation of $\tilde{S}_{11}(X)$ and $\tilde{S}_{12}(X)$. The proofs of these two lemmas are a little complicated and will be given in section 6.

**Lemma 3.5.** *Suppose $M$ and $N$ are sufficiently large real numbers, and $a$ and $b$ are fixed integers satisfying*

$$(\log N)^{100} < M \le N \quad \text{and} \quad |ab| \le (\log N)^{1000}. \tag{3.8}$$

*Let*

$$S(M,N) := \sum \frac{\mu^2(mn)}{\phi(mn)}, \tag{3.9}$$

*where the summation is subject to $M < m \le 2M$, $N < n \le 2N$, $(mn, ab) = 1$, $am \equiv \square \pmod n$ and $bn \equiv \square \pmod m$. Then we have*

$$S(M,N) \ll (\log M \log N)^{-\frac{1}{2}}, \tag{3.10}$$

*where the constant involved in the symbol $\ll$ is absolute.*

**Lemma 3.6.** *Suppose $A$, $B$ and $C$ are sufficiently large real numbers satisfying*

$$A \le B \le C \quad \text{and} \quad A \ge (\log C)^{1000}. \tag{3.11}$$

*Suppose $\alpha$, $\beta$ and $\gamma$ are fixed non-zero integers satisfying*

$$\alpha,\ \ \beta,\ \ \gamma \le (\log C)^{100}. \tag{3.12}$$

*Define*

$$S(A,B,C) := \sum_{A<a\le 2A}\frac{\mu^2(a)}{\phi(a)}\sum_{B<b\le 2B}\frac{\mu^2(b)}{\phi(b)}\sum_{C<c\le 2C}\frac{\mu^2(c)}{\phi(c)}, \tag{3.13}$$

*where the sum is also subject to the fact that*

$$2\nmid abc,\ \ a,b,c \text{ and } \alpha\beta\gamma \text{ are pairwise coprime}, \tag{3.14}$$

*and*

$$\begin{cases} \alpha bc \equiv \square \pmod{a}, \\ \beta ac \equiv \square \pmod{b}, \\ \gamma ab \equiv \square \pmod{c}. \end{cases} \tag{3.15}$$

*Then we have*

$$S(A,B,C) \ll (\log A \log B \log C)^{-\frac{1}{2}}, \tag{3.16}$$

*where the constant involved in the symbol "$\ll$" is absolute.*

## 4. Estimate of $\tilde{S}_{11}(X)$

This sum is very easily estimated. Since the ranges of $b_1$ and $c_1$ are short enough, we simply discard three congruence restrictions in (2.11), and get

$$\tilde{S}_{11}(X) \ll \sum_{\substack{a_1,a_2 \\ a_1a_2 \le \frac{X}{\Delta a(1)a(2)}}} \mu^2(a_1a_2) \sum_{\substack{\sqrt{X}/F < b_1 \le \sqrt{X/\Delta b(1)b(2)} \\ \sqrt{X}/F < c_1 \le \sqrt{X/\Delta c(1)c(2)} \\ A(2),B(1),C(1)}} \mu^2(b_1c_1) \sum_{b_2,c_2} 1, \tag{4.1}$$

where, subject to $b(1)b(2)b_1b_2 + c(1)c(2)c_1c_2 = a(1)a(2)a_1a_2$, the innermost sum is trivially bounded by $1 + a(1)a(2)X(b_1c_1\Delta D)^{-1}$. Thus we have

$$\begin{aligned} \tilde{S}_{11}(X) \ll & \frac{Xa(1)a(2)}{\Delta D} \sum_{\substack{a_1,a_2 \\ a_1a_2 \le \frac{X}{\Delta a(1)a(2)}}} \mu^2(a_1a_2) \sum_{\substack{\sqrt{X}/F < b_1,c_1 \le \sqrt{X} \\ A(2),B(1),C(1)}} \frac{\mu^2(b_1c_1)}{b_1c_1} \\ & + \sum_{\substack{a_1,a_2 \\ a_1a_2 \le \frac{X}{\Delta a(1)a(2)}}} \mu^2(a_1a_2) \sum_{\substack{\sqrt{X}/F < b_1 \le \sqrt{X}/\Delta b(1)b(2) \\ \sqrt{X}/F < c_1 \le \sqrt{X}/\Delta c(1)c(2) \\ A(2),B(1),C(1)}} \mu^2(b_1c_1) \\ = & \tilde{S}_{111}(X) + \tilde{S}_{112}(X), \quad \text{say.} \end{aligned} \tag{4.2}$$

Summing over $a_1$, we get

$$\tilde{S}_{111}(X) \ll \frac{X^2}{\Delta^2 D} \sum_{a_2 \le X} \frac{\mu^2(a_2)}{a_2} \sum_{\substack{\sqrt{X}/F < b_1,c_1 \le \sqrt{X} \\ A(2),B(1),C(1)}} \frac{\mu^2(b_1c_1)}{b_1c_1}. \tag{4.3}$$

We divide the ranges of $a_2$, $b_1$ and $c_1$ into diadic intervals $(A_2, 2A_2]$, $(B_1, 2B_1]$ and $(C_1, 2C_1]$, respectively. (So $A_2$, $B_1$ and $C_1$ take powers of 2.) From Lemma 3.6, we see that the subsum of (4.3) subject to $a_2 > (\log X)^{1000}$ is simply bounded by

$$\frac{X^2}{\Delta^2 D} \sum_{\substack{(\log X)^{1000} < A_2 \le X \\ \sqrt{X}/F < B_1,C_1 \le \sqrt{X}}} \frac{1}{\sqrt{\log A_2 \log B_1 \log C_1}} \ll \frac{X^2 (\log F)^2}{\Delta^2 D \sqrt{\log X}}. \tag{4.4}$$

The subsum of (4.3) subject to $a_2 \le (\log X)^{1000}$, from Lemma 3.5, is bounded by

$$\begin{aligned}
&\frac{X^2}{\Delta^2 D} \sum_{a_2 \le (\log X)^{1000}} \frac{\mu^2(a_2)}{a_2} \sum_{\substack{\sqrt{X}/F < b_1, c_1 \le \sqrt{X} \\ B(1), C(1)}} \frac{\mu^2(b_1 c_1)}{b_1 c_1} \\
&\ll \frac{X^2}{\Delta^2 D} \sum_{a_2 \le (\log X)^{1000}} \frac{1}{a_2} \sum_{\sqrt{X}/F < B_1, C_1 \le \sqrt{X}} \frac{1}{\sqrt{\log B_1 \log C_1}} \\
&\ll \frac{X^2 (\log F)^2 \log\log X}{\Delta^2 D \log X}.
\end{aligned} \tag{4.5}$$

Hence, from (4.3) – (4.5), we have an estimate for $\tilde{S}_{111}(X)$ which is admissible for (2.10), by noting $\log F = (\log X)^{\frac{1}{6}}$.

In exactly the same manner, namely, by appealing to Lemmas 3.5 and 3.6, one can easily show that

$$\tilde{S}_{112}(X) \ll \frac{X^2}{\Delta^2 \sqrt{D \log X}} + \frac{X^2 \log\log X}{\Delta^2 \sqrt{D} \log X}, \tag{4.6}$$

which is also admissible for (2.10) since $D\Delta^2 \le (\log X)^{25}$.

## 5. Estimate of $\tilde{S}_{12}(X)$

First we note that

$$\tilde{S}_{12}(X) \ll \sum_{\substack{B, C \le \sqrt{X} \\ BC \le X/F}} \tilde{S}_{12}(B, C, X), \tag{5.1}$$

where $B$ and $C$ run over powers of 2 and

$$\tilde{S}_{12}(B, C, X) = \sum_{a_1, a_2} \mu^2(a_1 a_2) \sum_{\substack{B < b_1 \le 2B, C < c_1 \le 2C \\ A(2), B(1), C(1)}} \mu^2(b_1 c_1) \sum_{\substack{b_2, c_2 \\ A(1), B(2), C(2)}} \mu^2(b_2 c_2), \tag{5.2}$$

where, in the innermost sum, the $b_2$ and $c_2$ are also subject to $b(1)b(2)b_1 b_2 + c(1)c(2)c_1 c_2 = a(1)a(2)a_1 a_2$.

For notational convenience, here and henceforth, we shall leave aside, without additional warning, any errors which obviously contribute $O(X^2/\Delta^2 D)$ to $\tilde{S}(X)$. With this convention, in the sum $\tilde{S}_{12}(B, C, X)$, we suppose that $b_2, c_2 > \sqrt{X}/(\log X)^5$.

We write $b_2$ and $c_2$ in the sum in terms of

$$b_2 := mpM \quad \text{and} \quad c_2 := nqN,$$

such that, for a fixed positive number $\eta < 10^{-10}$,

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

and

$$\left(\frac{X}{BC}\right)^{\eta} < mp \le p\left(\frac{X}{BC}\right)^{\eta} \quad \text{and} \quad \left(\frac{X}{BC}\right)^{\eta} < nq \le q\left(\frac{X}{BC}\right)^{\eta}.$$

With this decomposition, $\tilde{S}_{12}(B,C,X)$ is then equal to

(5.3)
$$\sum_{a_1,a_2,b_1,c_1}\mu^2(a_1a_2b_1c_1)\sum_{p,q}\sum_{\substack{m,n\\ B(2)a_1c_1\equiv\square \pmod m\\ C(2)a_1b_1\equiv\square \pmod n}}\mu^2(mn)\sum_{\substack{M,N\\ A(1)mpMc_1\equiv\square \pmod{a_1}}}\mu^2(MN).$$

Without loss of generality, we shall just consider the subsum of (5.3) with $p<q$. We now split this subsum into two parts: $\tilde{S}_{121}(B,C,X)$ subject to $p\le\left(\frac{X}{BC}\right)^{\eta^2}$, and $\tilde{S}_{122}(B,C,X)$ subject to $p>\left(\frac{X}{BC}\right)^{\eta^2}$.

**Estimate of $\tilde{S}_{122}(B,C,X)$.** In (5.3), we let $p$ and $q$ be absorbed by $M$ and $N$, respectively. Then we see that

(5.4)
$$\tilde{S}_{122}(B,C,X)=\sum_{a_1,a_2,b_1,c_1}\sum_{\substack{m,n\le\left(\frac{X}{BC}\right)^{\eta}\\ B(2)a_1c_1\equiv\square \pmod m\\ C(2)a_1b_1\equiv\square \pmod n}}\mu^2(mn)\sum_{\substack{M,N\\ A(1)mMc_1\equiv\square \pmod{a_1}}}\mu^2(MN),$$

where in the innermost sum, $M$ and $N$ also satisfy

$$b(1)b(2)b_1mM+c(1)c(2)c_1nN=a(1)a(2)a_1a_2 \tag{5.5}$$

and

$$p(MN)>\left(\frac{X}{BC}\right)^{\eta^2}. \tag{5.6}$$

The solutions of (5.5) for $M$ and $N$ are in the form

$$M=l_1(k)=c(1)c(2)c_1nk+M_0,\quad N=l_2(k)=-b(1)b(2)b_1mk+N_0,$$

where $(M_0,N_0)\in\mathbb{Z}_+^2$ is the solution of (5.5) with $M_0$ being minimal, and $k$ runs up to at most $\frac{a(1)a(2)X}{D\Delta b_1c_1mn}$. To estimate the innermost sum, we still need some technical treatment for the congruence. We split $a_1$ into form

$$a_1:=rlR\quad\text{ with }\quad P(r)<l<p(R) \tag{5.7}$$

and

$$\left(\frac{X}{BC}\right)^{\eta}<rl\le l\left(\frac{X}{BC}\right)^{\eta}, \tag{5.8}$$

and then we replace the congruence involved in the innermost sum by

$$A(1)mMc_1\equiv\square \pmod r.$$

With this change, from (5.4) we have

$$\tilde{S}_{122}(B,C,X)\ll\sum_{\substack{r,l,R\\ a_2,b_1,c_1}}\sum_{\substack{m,n\le\left(\frac{X}{BC}\right)^{\eta}\\ B(2)rlRc_1\equiv\square \pmod m\\ C(2)rlRb_1\equiv\square \pmod n}}\mu^2(mn)\sum_{\substack{k\le\frac{a(1)a(2)X}{D\Delta b_1c_1mn}\\ p(l_1(k)l_2(k))>\left(\frac{X}{BC}\right)^{\eta^2}\\ A(1)mc_1l_1(k)\equiv\square \pmod r}}1. \tag{5.9}$$

Since the coefficient of $k$ in $A(1)mc_1l_1(k)$ is prime to $r$, the congruence involved in the innermost sum gives precisely $\frac{\phi(r)}{2^{\omega(r)}}$ residue classes of $k$ modulo $r$. For each

$t \equiv \square \pmod r$, let the solution of $A(1)mc_1l_1(k) \equiv t \pmod r$ be $k \equiv \beta \pmod r$ with $0 < \beta = \beta(t,r) < r$. Replace $k$ by $rs + \beta$. Then we have

$$l_1(k) = L_1(s) = (c(1)c(2)c_1nr)s + (M_0 + c(1)c(2)c_1n\beta)$$

and

$$l_2(k) = L_2(s) = (-b(1)b(2)b_1mr)s + (N_0 - b(1)b(2)b_1m\beta),$$

where $s$ runs up to at most $\frac{a(1)a(2)X}{D\Delta b_1c_1mnr}$. The innermost of sum in (5.9) is thus bounded by

$$\sum_{t \equiv \square \pmod r} \sum_{\substack{s \le \frac{a(1)a(2)X}{D\Delta b_1c_1mnr} \\ p(L_1(s)L_2(s)) > \left(\frac{X}{BC}\right)^{\eta^2}}} 1. \tag{5.10}$$

We apply Lemma 3.3 to the inner sum of (5.10). Note that

$$E = a(1)a(2)b(1)b(2)c(1)c(2)a_1a_2b_1c_1mnr^3 = DlRa_2b_1c_1mnr^4$$

and the coefficients of $s$ in $L_1(s)$ and $L_2(s)$ have greatest common divisor $r$, thus $\rho(p) = 0$ if $p \mid r$ and $\rho(p) = 1$ if $p \mid E$, but $p \nmid r$. We also note that

$$\frac{a(1)a(2)X}{D\Delta b_1c_1mnr} > \left(\frac{X}{BC}\right)^{100\eta^2},$$

by Lemma 3.3 (with $g = 2$). The innermost sum of (5.9) is then bounded by

$$\begin{aligned} &\ll \frac{a(1)a(2)X}{rD\Delta b_1c_1mn} \cdot \frac{DlRa_2b_1c_1mn}{\phi(DlRa_2b_1c_1mn)} \cdot \frac{r^2}{\phi^2(r)} \cdot \frac{\phi(r)}{2^{\omega(r)}} \cdot \frac{1}{(\log(X/BC))^2} \\ &\ll \frac{a(1)a(2)X}{\Delta\phi(D)(\log(X/BC))^2} \cdot \frac{r}{\phi(r)2^{\omega(r)}} \cdot \frac{Ra_2}{\phi(Ra_2b_1c_1mn)}. \end{aligned} \tag{5.11}$$

Taking (5.11) back into (5.9), we get

$$\tilde{S}_{122}(B,C,X) \ll G \sum_{\substack{r,l,R \\ a_2,b_1,c_1}} \frac{\mu^2(rlRa_2b_1c_1)Rra_2}{2^{\omega(r)}\phi(Rra_2b_1c_1)} \sum_{\substack{m,n \le \left(\frac{X}{BC}\right)^{\eta} \\ B(2)rlRc_1 \equiv \square \pmod m \\ C(2)rlRb_1 \equiv \square \pmod n}} \frac{\mu^2(mn)}{\phi(mn)}, \tag{5.12}$$

where

$$G := \frac{a(1)a(2)X}{\Delta\phi(D)(\log(X/BC))^2}.$$

Now for the sum on the right-hand side of (5.12), we would like to sum over $R$ first. We split the sum into two parts, subject to $l > \left(\frac{X}{BC}\right)^{\eta^2}$ and $l \le \left(\frac{X}{BC}\right)^{\eta^2}$, respectively. For the first part, we let $l$ be absorbed by $R$. Note that in this case,

$$\frac{R}{\phi(R)} = \prod_{p \mid R}\left(1 - \frac{1}{p}\right)^{-1} \ll \left(1 - \left(\frac{BC}{X}\right)^{\eta^2}\right)^{-\frac{\log X}{\eta^2 \log(X/BC)}} \ll_\eta 1,$$

thus the part subject to $l > \big(\frac{X}{BC}\big)^{\eta^2}$ is bounded by

$$G \sum_{\substack{a_2\le\sqrt{X}\\(a_2,2a(1)a(2))=1}} \frac{\mu^2(a_2)a_2}{\phi(a_2)} \sum_{\substack{B<b_1\le 2B, C<c_1\le 2C\\A(2),B(1),C(1)}} \frac{\mu^2(b_1c_1)}{\phi(b_1c_1)} \sum_{r\le\big(\frac{X}{BC}\big)^{\eta}} \frac{r\mu^2(r)}{\phi(r)2^{\omega(r)}}$$

$$\sum_{m,n\le\big(\frac{X}{BC}\big)^{\eta}} \frac{\mu^2(mn)}{\phi(mn)} \sum_{\substack{R\le\frac{X}{\Delta a(1)a(2)a_2 r}\\B(2)rRc_1\equiv\square \pmod m\\C(2)rRb_1\equiv\square \pmod n\\p(R)>\big(\frac{X}{BC}\big)^{\eta^2}}} 1. \tag{5.13}$$

The inner sum in (5.13) about $r$, $m$, $n$ and $R$ , by Lemmas 3.3 (with $g = 1$) and 3.4, is bounded by

(5.14)

$$\sum_{r\le\big(\frac{X}{BC}\big)^{\eta}} \frac{r\mu^2(r)}{\phi(r)2^{\omega(r)}} \sum_{m,n\le\big(\frac{X}{BC}\big)^{\eta}} \frac{\mu^2(mn)}{\phi(mn)} \cdot \frac{X}{\Delta a(1)a(2)a_2 r} \cdot 2^{-\omega(mn)} \cdot \frac{1}{\log(X/BC)}$$

$$\ll \frac{X\big(\log(X/BC)\big)^{\frac12}}{\Delta a(1)a(2)}.$$

Thus the entire sum of (5.13) is bounded by

$$\frac{GX\big(\log(X/BC)\big)^{\frac12}}{\Delta a(1)a(2)} \sum_{\substack{a_2\le\sqrt{X}\\(a_2,2a(1)a(2))=1}} \frac{\mu^2(a_2)}{\phi(a_2)} \sum_{\substack{B<b_1\le 2B, C<c_1\le 2C\\A(2),B(1),C(1)}} \frac{\mu^2(b_1c_1)}{\phi(b_1c_1)}. \tag{5.15}$$

One can split the sum in (5.15) into two parts, apply Lemma 3.5 to the part with $a_2 \le (\log X)^{100}$ (with the congruence $A(2)$ discarded), divide the range of $a_2$ in the other part, $(\log X)^{100} < a_2 \le \sqrt{X}$, into diadic intervals and appeal to Lemma 3.6. Then one gets an upper bound

(5.16)

$$\frac{GX\big(\log(X/BC)\big)^{\frac12}}{\Delta a(1)a(2)} \cdot \frac{\sqrt{\log X}}{\sqrt{\log B\log C}} = \frac{X^2\sqrt{\log X}}{\Delta^2\phi(D)\big(\log B\log C\big)^{\frac12}\big(\log(X/BC)\big)^{\frac32}}.$$

Now we estimate the part of the sum in (5.12) with $l \le \big(\frac{X}{BC}\big)^{\eta^2}$. Since $R$ is squarefree, we have

$$\frac{R}{\phi(R)} = \sum_{d|R} \frac{\mu^2(d)}{\phi(d)} = \sum_{\substack{d|R\\d\le X^{2\eta}}} \frac{1}{\phi(d)} + O(X^{-\eta}). \tag{5.17}$$

The error term $O(X^{-\eta})$ is obviously negligible. (Replacing $\frac{R}{\phi(R)}$ in (5.12) by $O(X^{-\eta})$, noting that $l \le \big(\frac{X}{BC}\big)^{\eta^2}$, it is easy to see that the error term in (5.17) gives a contribution $O(X^{2-\eta+\epsilon})$ to $\tilde{S}_{122}(B,C,X)$.) Thus, essentially, the subsum

of the sum in (5.12) with respect to $l \le \left(\frac{X}{BC}\right)^{\eta^2}$ is bounded by

(5.18)
$$G \sum_{\substack{a_2 \le \sqrt{X} \\ (a_2, 2a(1)a(2))=1}} \frac{\mu^2(a_2)a_2}{\phi(a_2)} \sum_{\substack{B < b_1 \le 2B, C < c_1 \le 2C \\ A(2), B(1), C(1)}} \frac{\mu^2(b_1c_1)}{\phi(b_1c_1)} \sum_{m,n \le \left(\frac{X}{BC}\right)^{\eta}} \frac{\mu^2(mn)}{\phi(mn)}$$
$$\sum_{l \le \left(\frac{X}{BC}\right)^{\eta^2}} \left(\frac{X}{BC}\right)^{\eta} \sum_{\substack{/l < r \le \left(\frac{X}{BC}\right)^{\eta} \\ P(r) < l}} \frac{r\mu^2(r)}{\phi(r)2^{\omega(r)}} \sum_{d \le X^{2\eta}} \frac{1}{\phi(d)} \sum_{\substack{R' \le \frac{X}{\Delta a(1)a(2)a_2 rld} \\ B(2)rldR'c_1 \equiv \square \pmod m \\ C(2)rldR'b_1 \equiv \square \pmod n \\ p(R') > l}} 1.$$

By Lemma 3.3, the innermost sum of (5.18) is bounded by

$$O\left(\frac{1}{2^{\omega(mn)} \log l} \cdot \frac{X}{\Delta a(1)a(2)a_2 rld}\right), \tag{5.19}$$

and then we note that

$$\sum_{d \le X^{2\eta}} \frac{1}{d\phi(d)} \ll 1.$$

Moreover, by applying the argument following (5.15), the summation over $a_2$, $b_1$ and $c_1$ (along with the factor $\frac{1}{a_2}$ from (5.19)) gives a factor bounded by $\frac{\sqrt{\log X}}{\sqrt{\log B \log C}}$. Thus the sum in (5.18) is bounded by

$$\frac{GX\sqrt{\log X}}{\Delta a(1)a(2)\sqrt{\log B \log C}} \sum_{m,n \le \left(\frac{X}{BC}\right)^{\eta}} \frac{\mu^2(mn)}{\phi(mn)2^{\omega(mn)}}$$
$$\sum_{l \le \left(\frac{X}{BC}\right)^{\eta^2}} \frac{1}{l \log l} \sum_{\substack{/l < r \le \left(\frac{X}{BC}\right)^{\eta} \\ P(r) < l}} \frac{\mu^2(r)}{\phi(r)2^{\omega(r)}},$$

which, from Lemma 3.4, is bounded by

$$\frac{GX\sqrt{\log X} \log\left(X/BC\right)}{\Delta a(1)a(2)\sqrt{\log B \log C}} \sum_{l \le \left(\frac{X}{BC}\right)^{\eta^2}} \frac{1}{l \log l} \sum_{\substack{/l < r \le \left(\frac{X}{BC}\right)^{\eta} \\ P(r) < l}} \frac{\mu^2(r)}{\phi(r)2^{\omega(r)}}. \tag{5.20}$$

Note that the double sum in (5.20) is bounded by

$$\begin{aligned}
&\sum_{l\le\left(\frac{X}{BC}\right)^{\eta^2}}\frac{1}{l\log l}\sum_{\left(\frac{X}{BC}\right)^{\eta}/l<r\le\left(\frac{X}{BC}\right)^{\eta}\atop P(r)<l}\frac{\mu^2(r)}{r2^{\omega(r)}}\\
\ll&\frac{1}{\log(X/BC)}\sum_{l\le\left(\frac{X}{BC}\right)^{\eta^2}}\frac{1}{l\log l}\sum_{\left(\frac{X}{BC}\right)^{\eta}/l<r\le\left(\frac{X}{BC}\right)^{\eta}\atop P(r)<l}\frac{\mu^2(r)}{r2^{\omega(r)}}\sum_{p|r}\log p\\
\ll&\frac{1}{\log(X/BC)}\sum_{l\le\left(\frac{X}{BC}\right)^{\eta^2}}\frac{1}{l\log l}\sum_{p<l}\frac{\log p}{p}\sum_{\left(\frac{X}{BC}\right)^{\eta}/lp<r'\le\left(\frac{X}{BC}\right)^{\eta}/p}\frac{1}{r'2^{\omega(r')}}\qquad(5.21)\\
\ll&\frac{1}{\log(X/BC)}\sum_{l\le\left(\frac{X}{BC}\right)^{\eta^2}}\frac{1}{l\log l}\sum_{p<l}\frac{\log p}{p}\cdot\frac{\log l}{\sqrt{\log X/BC}}\\
\ll&\frac{1}{\sqrt{\log(X/BC)}}.
\end{aligned}$$

Take (5.21) back into (5.20); then for this part we have the same bound as (5.16). Hence, we have shown that

$$\tilde{S}_{122}(B,C,X)\ll\frac{X^2\sqrt{\log X}}{\Delta^2\phi(D)\big(\log B\log C\big)^{\frac{1}{2}}\big(\log(X/BC)\big)^{\frac{3}{2}}}.\qquad(5.22)$$

Summing up the bound (5.22) over $B$ and $C$, we have

$$\begin{aligned}
&\frac{X^2\sqrt{\log X}}{\Delta^2\phi(D)}\sum_{B,C}\frac{1}{\big(\log B\log C\big)^{\frac{1}{2}}\big(\log(X/BC)\big)^{\frac{3}{2}}}\\
\ll&\frac{X^2}{\Delta^2\phi(D)}\int_0^{\frac{1}{2}}\int_0^{\frac{1}{2}}\frac{1}{\sqrt{st}(1-s-t)^{\frac{3}{2}}}\,dsdt\qquad(5.23)\\
\ll&\frac{X^2}{\Delta^2\phi(D)},
\end{aligned}$$

thus we have proved that

$$\sum_{B,C}\tilde{S}_{122}(B,C,X)\ll\frac{X^2}{\Delta^2\phi(D)}.\qquad(5.24)$$

**Estimate of $\tilde{S}_{121}(B,C,X)$.** It is very similar to the estimate of $\tilde{S}_{122}(B,C,X)$. First of all, we still have $q$ being absorbed by $N$. Then we have

$$\begin{aligned}
\tilde{S}_{121}(B,C,X)\ll&\sum_{a_1,a_2,b_1,c_1}\sum_{p\le\left(\frac{X}{BC}\right)^{\eta^2}}\sum_{\left(\frac{X}{BC}\right)^{\eta}/p<m\le\left(\frac{X}{BC}\right)^{\eta}\atop P(m)<p\atop B(2)a_1c_1\equiv\square\pmod m}\mu^2(m)\\
&\sum_{n\le\left(\frac{X}{BC}\right)^{\eta}\atop C(2)a_1b_1\equiv\square\pmod n}\mu^2(n)\sum_{M,N\atop A(1)mpMc_1\equiv\square\pmod{a_1}}\mu^2(MN),\qquad(5.25)
\end{aligned}$$

where in the innermost sum, $M$ and $N$, also satisfy

$$b(1)b(2)b_1mpM + c(1)c(2)c_1nN = a(1)a(2)a_1a_2 \quad \text{and} \quad p(MN) > p. \tag{5.26}$$

As we have done for $\tilde{S}_{122}(B,C,X)$, from (5.25), we write $M$ and $N$ as two linear forms $l_1$ and $l_2$ in terms of a single variable $k$, with leading coefficients $c(1)c(2)c_1n$ and $-b(1)b(2)b_1mp$, respectively, $k$ running up to at most $\frac{a(1)a(2)X}{D\Delta b_1c_1mnp}$.

As before, to estimate the innermost sum, we split $a_1$ into the form of $rlR$ such that (5.7) and (5.8) are satisfied. We also replace the congruence involved in the innermost sum by

$$A(1)mpMc_1 \equiv \square \pmod r.$$

With this change, from (5.25) we have

$$\begin{aligned}\tilde{S}_{121}(B,C,X) \ll \sum_{\substack{r,l,R\\ a_2,b_1,c_1}} \sum_{p\le\left(\frac{X}{BC}\right)^{\eta^2}} \sum_{\substack{\left(\frac{X}{BC}\right)^{\eta}/p<m\le\left(\frac{X}{BC}\right)^{\eta}\\ P(m)<p\\ B(2)rlRc_1\equiv\square \pmod m}} \mu^2(m) \\ \sum_{\substack{n\le\left(\frac{X}{BC}\right)^{\eta}\\ C(2)rlRb_1\equiv\square \pmod n}} \mu^2(n) \sum_{\substack{k\le\frac{a(1)a(2)X}{D\Delta b_1c_1mnp}\\ p(l_1(k)l_2(k))>p\\ A(1)mpc_1l_1(k)\equiv\square \pmod r}} 1.\end{aligned} \tag{5.27}$$

Applying the same argument as that from (5.9) through (5.12), we have

$$\begin{aligned}\tilde{S}_{121}(B,C,X) \ll & G' \sum_{\substack{r,l,R\\ a_2,b_1,c_1}} \frac{\mu^2(rlRa_2b_1c_1)a_2R}{2^{\omega(r)}\phi(a_2b_1c_1R)} \sum_{p\le\left(\frac{X}{BC}\right)^{\eta^2}} \frac{1}{p(\log p)^2} \\ & \sum_{\substack{\left(\frac{X}{BC}\right)^{\eta}/p<m\le\left(\frac{X}{BC}\right)^{\eta}\\ P(m)<p\\ B(2)rlRc_1\equiv\square \pmod m}} \frac{\mu^2(m)}{\phi(m)} \sum_{\substack{n\le\left(\frac{X}{BC}\right)^{\eta}\\ C(2)rlRb_1\equiv\square \pmod n}} \frac{\mu^2(n)}{\phi(n)},\end{aligned} \tag{5.28}$$

where

$$G' := \frac{X\phi(a(1)a(2))}{\Delta\phi(D)}.$$

Applying Lemma 3.3, and with exactly the same method involved in (5.14), (5.19)–(5.21), one can easily check that the summation over $r$, $l$ and $R$ gives a factor bounded by

$$2^{-\omega(mn)} \cdot \frac{X}{a(1)a(2)a_2\sqrt{\log(X/BC)}}.$$

Thus, by appealing to Lemma 3.4 and the method used in (5.21) again, we have

$$\begin{aligned}\tilde{S}_{121}(B,C,X) \ll & \frac{G'X}{a(1)a(2)\sqrt{\log(X/BC)}} \sum_{\substack{a_2\le\sqrt{X}\\(a_2,2a(1)a(2))=1}} \frac{\mu^2(a_2)}{\phi(a_2)} \\ & \sum_{\substack{B<b_1\le 2B, C<c_1\le 2C\\ A(2),B(1),C(1)}} \frac{\mu^2(b_1c_1)}{\phi(b_1c_1)} \sum_{p\le\left(\frac{X}{BC}\right)^{\eta^2}} \frac{1}{p(\log p)^2} \\ & \sum_{\substack{\left(\frac{X}{BC}\right)^{\eta}/p<m\le\left(\frac{X}{BC}\right)^{\eta}\\ P(m)<p}} \frac{\mu^2(m)}{2^{\omega(m)}\phi(m)} \sum_{n\le\left(\frac{X}{BC}\right)^{\eta}} \frac{\mu^2(n)}{2^{\omega(n)}\phi(n)}.\end{aligned} \tag{5.29}$$

From Lemma 3.4, the summation over $n$ gives a factor $O(\sqrt{\log(X/BC)})$. Applying the idea involved in (5.21) twice, we see that the summation over $p$ and $m$ contributes a factor $O\big((\log(X/BC))^{-3/2}\big)$. Again, by applying the argument following (5.15), the summation over $a_2$, $b_1$ and $c_1$ contributes a factor

$$O\big((\log X)^{\frac{1}{2}}(\log B\log C)^{-\frac{1}{2}}\big).$$

From these and (5.29), we have an upper bound for $\tilde{S}_{121}(B,C,X)$, the same as in (5.22). Hence, by (5.23), we also have

$$\sum_{B,C}\tilde{S}_{121}(B,C,X) \ll \frac{X^2}{\Delta^2\phi(D)}. \tag{5.30}$$

Therefore, on assuming Lemmas 3.5 and 3.6, the upper bound (2.10) has been proved.

## 6. Proof of Lemmas 3.5 and 3.6

First we prove Lemma 3.5. Without loss of generality, we assume $m$ and $n$ are running over odd integers in the specified intervals. (Thus throughout the proof, all the important variables, $m_1$, $m_2$, $n_1$ and $n_2$ are odd integers.) We start from the fact that, for coprime integers $\alpha$ and $\beta$, where $\beta$ is positive and odd, $\alpha\equiv\square \pmod{\beta}$ if and only if

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

which, in case $\beta$ is squarefree, is equivalent to

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

Thus we have

$$S(M,N) \ll \sum_{\substack{M<m_1m_2\le 2M\\ N<n_1n_2\le 2N\\ (m_1m_2n_1n_2,ab)=1}} \frac{\mu^2(m_1m_2n_1n_2)}{\phi(m_1m_2n_1n_2)}\cdot 2^{-\omega(m_1m_2n_1n_2)}\left(\frac{am_1m_2}{n_1}\right)\left(\frac{bn_1n_2}{m_1}\right). \tag{6.1}$$

Let

$$T := (\log N)^{49}.$$

We shall split the sum (6.1) into several parts according to ranges of the variables:

1. $m_2, n_1 > T$ or $m_1, n_2 > T$;
2. $m_1, n_1 \le T$;
3. $m_2, n_2 \le T$.

We note that

$$2^{\omega(k)}\phi(k) = k\prod_{p|k} 2\cdot\left(1-\frac{1}{p}\right)\ge k.$$

From this and Lemma 3.1, the subsum subject to condition 1 is trivially bounded by

$$\sum_{\substack{m\le M/T\\ n\le N/T}} \frac{1}{mn}\left(\left(\frac{M}{m}\right)^{-\frac{1}{16}+\epsilon}+\left(\frac{N}{n}\right)^{-\frac{1}{16}+\epsilon}\right)\ll \log M\log N\cdot T^{-\frac{1}{16}+\epsilon}\ll\frac{1}{\log N}, \tag{6.2}$$

which is admissible for (3.10).

For the subsum subject to the condition 2, we sum over $n_2$ first. Note that $abm_1m_2n_1\ll\left(\frac{N}{n_1}\right)^2$, from (3.3) and partial summation, and the terms with $m_1\ne 1$ contribute at most

$$\ll \sum_{\substack{1<m_1\le T\\ n_1\le T\\ \frac{M}{m_1}<m_2\le\frac{2M}{m_1}}} \frac{1}{m_1m_2n_1}\cdot\exp(-\kappa\sqrt{\log(N/n_1)})\ll\frac{1}{(\log N)^2}, \tag{6.3}$$

which is more than enough. Thus, apart from this small error, the subsum subject to condition 2 is dominated by the terms with $m_1=1$. For this "main term", we split the range of $n_1$ into three parts: $n_1=1$, $1<n_1\le(\log M)^{49}$ and $(\log M)^{49}<n_1\le T$. For the second part, we first note that it can be written as

$$\sum_{\substack{1<n_1\le(\log M)^{49}\\ \frac{N}{n_1}<n_2\le\frac{2N}{n_1}\\ (n_1n_2,ab)=1}} \frac{\mu^2(n_1n_2)}{\phi(n_1n_2)2^{\omega(n_1n_2)}}\left(\frac{a}{n_1}\right)\sum_{\substack{M<m_2\le 2M\\ (m_2,abn_1n_2)=1}}\frac{\mu^2(m_2)}{\phi(m_2)2^{\omega(m_2)}}\left(\frac{m_2}{n_1}\right). \tag{6.4}$$

By Lemma 3.2 and partial summation, the inner sum of (6.4) is bounded by

$$\exp(-\kappa\sqrt{\log M})+M^{-\frac{2}{3}}\tau_{2M}(abn_1n_2)\ll\exp(-\kappa\sqrt{\log M})+M^{-\frac{1}{2}}\tau_{2M}(n_2). \tag{6.5}$$

While the first term on the right side of (6.5), from Lemma 3.4, contributes to (6.4)

$$\ll\sum_{\substack{1<n_1\le(\log M)^{49}\\ \frac{N}{n_1}<n_2\le\frac{2N}{n_1}}}\frac{\mu^2(n_1n_2)}{\phi(n_1n_2)2^{\omega(n_1n_2)}}\cdot\exp(-\kappa\sqrt{\log M})\ll\exp(-\frac{\kappa}{2}\sqrt{\log M})(\log N)^{-\frac{1}{2}},$$

the second term, which appears only when $N \gg M^2$, again from Lemma 3.4, contributes to (6.4)

$$\begin{aligned}
&\ll M^{-\frac{1}{2}} \sum_{n_1 \le (\log M)^{49}} \frac{1}{n_1} \sum_{\frac{N}{n_1} < n_2 \le \frac{2N}{n_1}} \frac{\mu^2(n_2)\tau_{2M}(n_2)}{\phi(n_2)2^{\omega(n_2)}} \\
&\ll M^{-\frac{1}{2}} \sum_{n_1 \le (\log M)^{49}} \frac{1}{n_1} \sum_{n_2' \le 2M} \frac{1}{\phi(n_2')2^{\omega(n_2')}} \sum_{\frac{N}{n_1 n_2'} < n_2'' \le \frac{2N}{n_1 n_2'}} \frac{1}{\phi(n_2'')2^{\omega(n_2'')}} \\
&\ll M^{-\frac{1}{2}} \sum_{n_1 \le (\log M)^{49}} \frac{1}{n_1} \sum_{n_2' \le 2M} \frac{1}{n_2'} \cdot \frac{1}{\sqrt{\log(N/n_1 n_2')}} \\
&\ll M^{-\frac{1}{3}} (\log N)^{-\frac{1}{2}},
\end{aligned}$$

both being admissible for (3.10).

For the third part, by Lemmas 3.1 and 3.4, we have an upper bound

$$\sum_{N/T < n_2 \le N/(\log M)^{49}} \frac{1}{2^{\omega(n_2)}\phi(n_2)} \cdot (\log M)^{-3} \ll \frac{\log T}{(\log M)^3 \sqrt{\log N}} \ll \frac{1}{(\log M)^2 \sqrt{\log N}},$$

which is negligible to the bound (3.10).

Hence, the subsum of $S(M, N)$ subject to condition 2 is essentially bounded by

$$\sum_{\substack{M < m_2 \le 2M \\ N < n_2 \le 2N \\ (m_2 n_2, ab) = 1}} \frac{\mu^2(m_2 n_2)}{\phi(m_2 n_2) 2^{\omega(m_2 n_2)}} \ll (\log M \log N)^{-\frac{1}{2}}, \tag{6.6}$$

by Lemma 3.4, which is exactly (3.10).

Now for the subsum subject to the condition 3: $m_2, n_2 \le T$. We first note

$$\left(\frac{m_1}{n_1}\right)\left(\frac{n_1}{m_1}\right) = \frac{1}{2}\left(1 - (-1)^{\frac{m_1-1}{2} + \frac{n_1-1}{2}} + (-1)^{\frac{m_1-1}{2}} + (-1)^{\frac{n_1-1}{2}}\right). \tag{6.7}$$

Thus this subsum is divided into four sums corresponding to the decomposition (6.7). Each one is of form

$$\sum_{\substack{m_2, n_2 \le T \\ M < m_1 m_2 \le 2M \\ N < n_1 n_2 \le 2N \\ (m_1 m_2 n_1 n_2, ab) = 1}} \frac{\mu^2(m_1 m_2 n_1 n_2)}{\phi(m_1 m_2 n_1 n_2)} \cdot 2^{-\omega(m_1 m_2 n_1 n_2)} \left(\frac{\pm a m_2}{n_1}\right)\left(\frac{\pm b n_2}{m_1}\right). \tag{6.8}$$

By exactly the same treatment as that for the subsum subject to condition 2, we have the upper bound (3.10).

The proof for Lemma 3.6 is similar. First we note that for $k \ll X$, similar to (5.17), we have

$$\frac{1}{\phi(k)} = \frac{1}{k} \sum_{d \mid k} \frac{\mu^2(d)}{\phi(d)} = \frac{1}{k} \sum_{\substack{d \mid k \\ d \le (\log X)^5}} \frac{\mu^2(d)}{\phi(d)} + O\left(\frac{\tau(k)}{k(\log X)^4}\right), \tag{6.9}$$

and clearly,

$$\sum_{k \le X} \frac{\tau(k)}{k(\log X)^4} = \frac{1}{(\log X)^4} \sum_{st \le X} \frac{1}{st} \ll \frac{1}{(\log X)^2}. \tag{6.10}$$

Thus, by splitting $a$, $b$ and $c$ in $S(A,B,C)$ respectively into the products of two variables $a_1$ and $a_2$, $b_1$ and $b_2$, $c_1$ and $c_2$, with $a_1$, $b_1$, $c_1$ being the ones $\le (\log C)^5$, and replacing the moduli $a$, $b$ and $c$ respectively by $a_2$, $b_2$ and $c_2$, we see that, to prove the lemma, it suffices to show that

$$S'(A,B,C) := \sum_{\substack{A<a\le 2A\\ B<b\le 2B\\ C<c\le 2C}} \mu^2(abc) \ll \frac{ABC}{\sqrt{\log A\log B\log C}}, \tag{6.11}$$

where the extra conditions involved in the summation are precisely those for $S(A,B,C)$ except that the constant 1000 in (3.11) changes to 995, and the constant 100 in (3.12) changes to 110. Now we translate the condition (3.15) into the equivalent formula

$$2^{-\omega(abc)}\sum_{\substack{a'|a\\ b'|b\\ c'|c}}\left(\frac{\alpha bc}{a'}\right)\left(\frac{\beta ac}{b'}\right)\left(\frac{\gamma ab}{c'}\right)= 1. \tag{6.12}$$

Then we have

$$\begin{aligned} S'(A,B,C) = &\sum_{\substack{a'\le 2A\\ (a',2\alpha\beta\gamma)=1}} \frac{\mu^2(a')}{2^{\omega(a')}} \sum_{\substack{A/a'<a''\le 2A/a'\\ (a'',2\alpha\beta\gamma a')=1}} \frac{\mu^2(a'')}{2^{\omega(a'')}} \sum_{\substack{b'\le 2B\\ (b',2\alpha\beta\gamma)=1}} \frac{\mu^2(b')}{2^{\omega(b')}}\\ &\sum_{\substack{B/b'<b''\le 2B/b'\\ (b'',2\alpha\beta\gamma a''b')=1}} \frac{\mu^2(b'')}{2^{\omega(b'')}} \sum_{\substack{c'\le 2C\\ (c',2\alpha\beta\gamma)=1}} \frac{\mu^2(c')}{2^{\omega(c')}}\\ &\sum_{\substack{C/c'<c''\le 2C/c'\\ (c'',2\alpha\beta\gamma a''b''c')=1}} \frac{\mu^2(c'')}{2^{\omega(c'')}}\left(\frac{\alpha b'b''c'c''}{a'}\right)\left(\frac{\beta a'a''c'c''}{b'}\right)\left(\frac{\gamma a'a''b'b''}{c'}\right). \end{aligned} \tag{6.13}$$

Let

$$T := (\log C)^{100}.$$

Then from Lemma 3.1, the subsums satisfying one of the conditions

$$(1).\ a', b''c'' > T, \quad (2).\ b', a''c'' > T, \quad (3).\ c', a''b'' > T, \tag{6.14}$$

give at most a contribution

$$T^{-\frac{1}{16}+\epsilon}\sum_{a',a'',b',b'',c',c''} 1 \ll \frac{ABC}{(\log C)^3},$$

which is negligible. Thus, excluding the subsums subject to (6.14), the subsums left to be considered satisfy

$$a', b', c' \le T \tag{6.15}$$

or

$$a'', b'', c'' \le T. \tag{6.16}$$

Now, for the subsum subject to (6.15), if summing over $c''$ first, then by Lemma 3.2 we see that, apart from an error $O(ABC\exp(-\kappa\sqrt{\log C}))$ which arises from the

terms with $a'b' \neq 1$, this subsum is actually equal to

$$\begin{aligned}(6.17)\qquad &\sum_{\substack{A<a''\leq 2A\\ B<b''\leq 2B\\ (a''b'',2\alpha\beta\gamma)=1}} \frac{\mu^2(a''b'')}{2^{\omega(a''b'')}} \sum_{\substack{c'\leq T\\ (c',2\alpha\beta\gamma a''b'')=1}} \frac{\mu^2(c')}{2^{\omega(c')}}\left(\frac{\gamma a''b''}{c'}\right) \sum_{\substack{C/c'<c''\leq 2C/c'\\ (c'',2\alpha\beta\gamma a''b''c')=1}} \frac{\mu^2(c'')}{2^{\omega(c'')}}\\ =\ &\sum_{\substack{c'\leq T\\ \frac{C}{c'}<c''\leq\frac{2C}{c'}\\ (c'c'',2\alpha\beta\gamma)=1}} \frac{\mu^2(c'c'')}{2^{\omega(c'c'')}} \sum_{\substack{A<a\leq 2A\\ (a,2\alpha\beta\gamma c'c'')=1}} \frac{\mu^2(a)}{2^{\omega(a)}}\left(\frac{\gamma a}{c'}\right) \sum_{\substack{B<b\leq 2B\\ (b,2\alpha\beta\gamma ac'c'')=1}} \frac{\mu^2(b)}{2^{\omega(b)}}\left(\frac{b}{c'}\right).\end{aligned}$$

Following the same treatment as for (6.4), it is easy to see that the contribution from the terms with $c' \neq 1$ is at most $O\big(ABC(\log C)^{-\frac{1}{2}}(\exp(-\kappa\sqrt{\log B}) + B^{-\frac{1}{3}})\big)$, which is negligible. Then, apart from this error term, the sum (6.17) is equal to

$$(6.18)\qquad \sum_{\substack{C<c\leq 2C\\ (c,2\alpha\beta\gamma)=1}} \frac{\mu^2(c)}{2^{\omega(c)}} \sum_{\substack{A<a\leq 2A\\ (a,2\alpha\beta\gamma c)=1}} \frac{\mu^2(a)}{2^{\omega(a)}} \sum_{\substack{B<b\leq 2B\\ (b,2\alpha\beta\gamma ac)=1}} \frac{\mu^2(b)}{2^{\omega(b)}},$$

which, by (3.7), is simply bounded by

$$(6.19)\qquad \sum_{c\leq 2C)=1} \frac{1}{2^{\omega(c)}} \sum_{a\leq 2A} \frac{1}{2^{\omega(a)}} \sum_{b\leq 2B} \frac{1}{2^{\omega(b)}} \ll \frac{ABC}{\sqrt{\log A \log B \log C}},$$

as desired.

Hence, to finish the proof, we only need to show that the subsum subject to (6.16) is admissible for (3.16). From the identity

$$(6.20)\qquad \left(\frac{-b'c'}{a'}\right)\left(\frac{a'b'}{c'}\right)\left(\frac{a'c'}{b'}\right) = \frac{1}{2}\left(1+\left(\frac{-1}{a'b'}\right)+\left(\frac{-1}{a'c'}\right)-\left(\frac{-1}{b'c'}\right)\right),$$

this subsum is divided into four subsums corresponding to (6.20), each of which is typically of form

$$\begin{aligned}(6.21)\qquad &\sum_{\substack{a''\leq T\\ (a'',2\alpha\beta\gamma)=1}} \frac{\mu^2(a'')}{2^{\omega(a'')}} \sum_{\substack{A/a''<a'\leq 2A/a''\\ (a',2\alpha\beta\gamma a'')=1}} \frac{\mu^2(a')\chi_1(a')}{2^{\omega(a')}} \sum_{\substack{b''\leq T\\ (b'',2\alpha\beta\gamma)=1}} \frac{\mu^2(b'')}{2^{\omega(b'')}}\\ &\sum_{\substack{B/b''<b'\leq 2B/b''\\ (b',2\alpha\beta\gamma a'b'')=1}} \frac{\mu^2(b')\chi_2(b')}{2^{\omega(b')}} \sum_{\substack{c''\leq T\\ (c'',2\alpha\beta\gamma a''b'')=1}} \frac{\mu^2(c'')}{2^{\omega(c'')}}\\ &\sum_{\substack{C/c''<c'\leq 2C/c''\\ (c',2\alpha\beta\gamma a'b'c'')=1}} \frac{\mu^2(c'')\chi_3(c')}{2^{\omega(c')}}\left(\frac{-\alpha b''c''}{a'}\right)\left(\frac{\beta a''c''}{b'}\right)\left(\frac{\gamma a''b''}{c'}\right),\end{aligned}$$

where $\chi_i$, $i = 1, 2, 3$, are certain characters modulo 4.

Again, from Lemma 3.2, the contribution of the terms in (6.21) with $a''b'' \neq 1$ or $\chi_3\big(\frac{\gamma}{\cdot}\big) \neq \chi_0$ is at most $O(ABC\exp(-\kappa\sqrt{\log C}))$, which is negligible. Thus, apart

from this error, (6.21) is essentially equal to

(6.22)
$$\sum_{\substack{A<a'\le 2A\\(a',2\alpha\beta\gamma)=1}}\frac{\mu^2(a')\chi_1(a')}{2^{\omega(a')}}\sum_{\substack{B<b'\le 2B\\(b',2\alpha\beta\gamma a')=1}}\frac{\mu^2(b')\chi_2(b')}{2^{\omega(b')}}\sum_{\substack{c''\le T\\(c'',2\alpha\beta\gamma)=1}}\frac{\mu^2(c'')}{2^{\omega(c'')}}\left(\frac{-\alpha c''}{a'}\right)\left(\frac{\beta c''}{b'}\right)$$
$$\sum_{\substack{C/c''<c'\le 2C/c''\\(c',2\alpha\beta\gamma a'b'c'')=1}}\frac{\mu^2(c')}{2^{\omega(c')}}.$$

It is now clear that, by exactly the same treatment as used from (6.17) through (6.19), (6.22) is bounded by
$$\frac{ABC}{\sqrt{\log A\log B\log C}},$$
as required. Therefore, we have proved Lemma 3.6.

## Acknowledgement

The author is grateful to professors Andrew Granville and Carl Pomerance for their constant encouragement, and to Professor Carl Pomerance for his helpful comments. The author also greatly thanks the referee for his/her 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. MR0384812 (52:5684)
2. A. Brumer, *The average rank of elliptic curves, I*, Invent. Math **109** (1992), 445–472. MR1176198 (93g:11057)
3. D.A.Burgess, *On character sums and L-series, II*, Proc. Lond. Math. Soc., III. Ser.13, (1963), 524–536. MR0148626 (26:6133)
4. H. Halberstam and H. E. Richert, *Sieve Methods*, Academic Press, 1974. MR0424730 (54:12689)
5. D. R. Heath-Brown, *The size of Selmer groups for the congruent number problem I*, Invent. Math. **111** (1) (1993), 171–195. MR1193603 (93j:11038)
6. ———, *The size of Selmer groups for the congruent number problem II*, Invent. Math. **118** (2) (1994), 331–370. MR1292115 (95h:11064)
7. A. Ivic, *The Riemann zeta-function*, John Wiley & Sons, 1985. MR0792089 (87d:11062)
8. K. Kramer, *A family of semistable elliptic curves with large Tate-Shafarevitch groups*, Proc. Amer. Math Soc. **89** (1983), 379–386. MR0715850 (85d:14059)
9. A. Selberg, *Note on a paper by L. G. Sathe*, J. Indian Math. Soc. **18** (1954), 83–87. MR0067143 (16:676a)
10. J. Silverman, *The arithmetic of elliptic curves*, GTM 106, Springer, 1986. MR0817210 (87g:11070)
11. G. Yu, *Rank* 0 *quadratic twists of a family of elliptic curves*, Compositio Math **135** (3) (2003), 331–356. MR1956817 (2004b:11082)
12. ———, *Average size of* 2*-Selmer groups of elliptic curves, II*, to appear in Acta Arith.

Department of Mathematics, LeConte College, 1523 Greene Street, University of South Carolina, Columbia, South Carolina 29208

*E-mail address*: yu@math.sc.edu