ON THE QUADRATIC TWISTS OF A FAMILY OF ELLIPTIC CURVES

GANG YU

Abstract. In this paper is considered the average size of the 2-Selmer groups of a class of quadratic twists of each elliptic curve over $\mathbb{Q}$ with $\mathbb{Q}$-torsion group $\mathbb{Z}_2 \times \mathbb{Z}_2$. The existence is shown of a positive proportion of quadratic twists of such a curve, each of which has rank 0 Mordell-Weil group.

§1. *Introduction.* For an elliptic curve E over $\mathbb{Q}$, we denote by $E(\mathbb{Q})$ its Mordell-Weil group. While Mazur [**9**, **10**] has shown that the torsion part can be one of only finitely many possibilities, little is known about the rank. Nevertheless, it is generally believed that curves with large ranks comprise a small "proportion" of all elliptic curves. In particular, it is conjectured that "almost all" elliptic curves have rank 0 or 1. Moreover, Goldfeld [**2**] conjectured that the average rank of the quadratic twists of any given elliptic curve over $\mathbb{Q}$ is $1/2$. A quick consequence of this is that, for any elliptic curve over $\mathbb{Q}$, asymptotically, there are at least half of the quadratic twists of this curve which have rank 0. Thus there is a comparatively weaker conjecture stating that, for any elliptic curve over $\mathbb{Q}$, the rank 0 quadratic twists comprise a positive proportion of all quadratic twists of the given curve. In the general case, this conjecture, though much weaker than the other famous ones related to elliptic curves, is still open.

There have been numerous papers treating this problem for modular curves. Because of the work of Kolyvagin [**8**], most of them are focusing on the non-vanishing of the L-functions (see [**6**, **7**, **11**, **12**, **13**, **14**]). In light of the work of Shimura [**15**] and Waldspurger [**17**], people have been able to get some partial results. With the knowledge about the Fourier coefficients of some new forms, James [**7**] proved that the quadratic twists for some given curve over $\mathbb{Q}$ have rank 0 for a positive proportion of square-free numbers. In [**19**], Wong proved that there is an infinite family of non-isomorphic elliptic curves such that, for each curve, a positive proportion of the quadratic twists have rank 0.

In a series of two papers [**4**, **5**], Heath-Brown studies the average order of the 2-Selmer groups of the congruent number curves $E_n : y^2 = x^3 - n^2x$. As a byproduct of his main theorems, it is shown that a positive proportion of such curves have rank 0. In other words, a positive proportion of the quadratic twists of $E : y^2 = x^3 - x$ have rank 0. In this paper, we shall generalize this to all curves over $\mathbb{Q}$ with 2-torsion part $\mathbb{Z}_2 \times \mathbb{Z}_2$. Namely, we shall consider the curves $E = E(a, b)$ defined by the equation

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

[MATHEMATIKA, **52** (2005), 139–154]

with $a, b \in \mathbb{Z}$ and $ab(a-b) \neq 0$. We shall prove

THEOREM 1. *For the curve E given by* (1.1), *a positive proportion of its quadratic twists have rank* 0. *Moreover, assuming the parity conjecture of Mordell-Weil ranks, a positive proportion of its quadratic twists have rank* 1.

One notes that, if not to pursue a quantitative version of Theorem 1 but just to prove the underlying proportional result qualitatively, one just needs to consider those E with $(a, b) = 1$. Moreover, by a simple linear transformation, we can make a even and b odd and $ab > 0$. Note that $E(-a, -b)$ gives a quadratic twist of $E(a, b)$; thus, for our purpose, it suffices to consider the curves

$$E(2a, b) : y^2 = x(x + 2a)(x + b) \tag{1.2}$$

with $(2a, b) = 1$ and $a, b > 0$.

We shall derive the theorem (for the curve $E(2a, b)$ given by (1.2)) by bounding the average size of the 2-Selmer groups of the quadratic twists E_D with D running over a subset of $\mathbb{N}$ of positive proportion. For convenience, throughout we shall assume that $b > 2a > 0$ and $2 \nmid a$. From the forthcoming proof, one should be able to see that the first assumption does not lose generality and the second asssumption, which makes the problem a little special, can be eliminated by considering the other case in exactly the same way. We shall not repeat the work for the case that $2|a$.

Thus, we suppose henceforth that the curve $E = E(2a, b)$ satisfies $0 < 2a < b$ and $(2a, b) = (2, a) = 1$. For its quadratic twists

$$E_D : y^2 = x(x + 2aD)(x + bD),$$

we shall let D run over some special subset of $\mathbb{N}$.

Let C be the conductor of E, so that C is the product of the square-free kernel of $ab(b-2a)$ and one of the numbers 8, 16 or 32. We shall consider those $D \in S(X; h)$, where

$$S(X; h) := \{1 \leqslant D \leqslant X : \mu^2(D) = 1, D \equiv h \bmod C\},$$

and h is a fixed integer coprime to C. Here and throughout, $\mu(\cdot)$ denotes the Möbius function (and thus $\mu^2(\cdot)$ is the character function of square-free numbers).

Let $c = b - 2a$. We describe several conditions, say Ca, Cb and Cc, as follows (where p denotes a prime):

(Ca): if $p|a$, and $\mathrm{ord}_p(a)$ is even, then $(\frac{bh}{p}) = -1$,

(Cb): if $p|b$, and $\mathrm{ord}_p(b)$ is even, then $(\frac{2ah}{p}) = -1$,

(Cc): if $p|c$, and $\mathrm{ord}_p(c)$ is even, then $(\frac{-bh}{p}) = -1$.

Briefly, we denote by $r(D)$ and $s(D)$ the Mordell-Weil rank and 2-Selmer rank of E_D, respectively. With a method similar to that Heath-Brown [**4**] used

for the congruent number curve, we are able to prove the following

THEOREM 2. *If h is an integer coprime to C and satisfying the conditions* (Ca), (Cb) *and* (Cc), *then, for the curve given by* (1.2),

$$\sum_{D\in S(X;h)} 2^{s(D)} = (3+o(1))\#S(X;h).$$

Combining Theorem 2 with the parity of $s(D)$ proved by Monsky [**11**], we actually can prove a quantitative result for rank 0 quadratic twists of the curve given by (1.2).

THEOREM 1a. *For any integer d, let $\omega'(d)$ denote the number of primes p dividing d with $\mathrm{ord}_p(d)$ even. Then, for the elliptic curve E given by equation* (1.2), *among all positive square-free numbers, the proportion of those D with E_D having rank* 0 *is at least*

$$2^{-\omega'(abc)-2}\,\frac{\varphi(C)}{3C},$$

where $\varphi(\cdot)$ is the Euler function.

Essentially the same proof gives a similar result about rank 1 quadratic twists. But in this case the corresponding result is conditional.

THEOREM 1b. *Let E satisfy the same conditions as in Theorem* 1. *Then, under the parity conjecture about the ranks of its quadratic twists, the proportion of square-free quadratic twists that have rank* 1 *is at least*

$$2^{-\omega'(abc)-3}\,\frac{5\varphi(C)}{3C}.$$

One notes that Theorems 1a and 1b obviously imply Theorem 1. Based on the result of Theorem 2, one can prove Theorems 1a and 1b in a similar way. Thus, for brevity, we shall only prove Theorems 1a and 2.

§2. *Proof of Theorem* 1a. Recall that $c = b - 2a$. From our conditions on a, b, we have a, b, c pairwise coprime and odd. Suppose that

$$a = p_1^{\alpha_1}\cdots p_i^{\alpha_i}, \qquad b = q_1^{\beta_1}\cdots q_j^{\beta_j}, \qquad c = l_1^{\gamma_1}\cdots l_k^{\gamma_k}$$

are the prime factorizations of a, b and c, respectively. Then the conductor of E is given by

$$C = 2^{\mu} p_1 \cdots p_i q_1 \cdots q_j l_1 \cdots l_k \tag{2.1}$$

for some integer $3 \leqslant \mu \leqslant 5$. According to Monsky [**11**], the parity of the 2-Selmer rank of E_D satisfies

$$(-1)^{s(D)} = \omega_E,$$

where ω_E is the root number in the functional equation of $L_E(s)$, if and only if $(\frac{-C}{D}) = 1$. Thus, if we choose D so that

$$\left(\frac{-C}{D}\right) = \omega_E, \tag{2.2}$$

then $s(D)$ will be even. So, we will choose D in a residue class $h \pmod C$ so that

$$\omega_E = \left(\frac{-C}{D}\right) = \left(\frac{-C}{h}\right) = \left(\frac{-2^\mu p_1 \cdots l_k}{h}\right)$$

which, with the law of quadratic reciprocity, is equivalent to

$$(-1)^{(h-1)/2+(h-1)(p_1\cdots l_k-1)/4}\left(\frac{2^\mu}{h}\right)\prod_{i'=1}^{i}\left(\frac{h}{p_{i'}}\right)\prod_{j'=1}^{j}\left(\frac{h}{q_{j'}}\right)\prod_{k'=1}^{k}\left(\frac{h}{l_{k'}}\right) = \omega_E. \tag{2.3}$$

From the fact that $b - 2a = c$, and that a, b, c are all odd, we know that a, b and c cannot all be squares. Thus, on the left side of (2.3), there is at least one Jacobi symbol whose value is not determined by the conditions (Ca), (Cb) and (Cc). This implies that, no matter what values $\omega_E(=\pm 1)$ and $p_1 \cdots l_k \pmod 4$ take, there must be some $h \pmod C$ satisfying the conditions (Ca), (Cb) and (Cc) and the parity condition (2.3). Furthermore, it is not hard to see that we have exactly $2^{-\omega'(abc)-2}\varphi(C)$ odd congruence classes modulo C satisfying conditions (Ca), (Cb), (Cc) and (2.3). (The conditions (Ca), (Cb), (Cc) account for the factor $2^{-\omega'(abc)}$, the fact that h is odd accounts for a factor 2^{-1}, and the fact that h satisfies (2.3) accounts for the last factor 2^{-1}.)

Now, for a fixed h satisfying (Ca), (Cb), (Cc) and condition (2.2), from the facts that

$$\sum_{D\in S(X;h)} 2^{s(D)} = (3 + o(1))\#S(X;h), \tag{2.4}$$

and that $s(D)$ is even, we conclude that, asymptotically, at least $1/3$ of the elements D of $S(X;h)$ satisfy $s(D) = 0$. Note that $r(D) \leqslant S(D)$; we thus conclude that, asymptotically, at least $1/3$ of the E_D with $D \in S(X;h)$ have rank 0. Since for different h_1, h_2 coprime to C we have $\#S(X;h_1) \sim \#S(X;h_2)$ as $X \to \infty$, we have completed the proof. □

§3. *Order of the* 2*-Selmer group.* We apply a discussion similar to that Heath-Brown uses in [**4**]. For each square-free D, the four 2-torsion points

$$\vartheta, \qquad (0,0), \qquad (-2aD, 0), \qquad (-bD, 0)$$

comprise a subgroup $\mathbb{Z}_2 \times \mathbb{Z}_2$ of the torsion part of $E_D(\mathbb{Q})$; call it $E_D(\mathbb{Q})_{2\text{–tors}}$.

For any non-torsion point $P := (x, y) \in E_D(\mathbb{Q})$, the coset in $P + E_D(\mathbb{Q})_{2\text{–tors}}$ consists of

$$(x, y), \qquad \left(\frac{2abD^2}{x}, *\right), \qquad \left(\frac{-2aD(x+bD)}{x+2aD}, *\right), \qquad \left(\frac{-bD(x+2aD)}{x+bD}, *\right)$$

which contains exactly one (x', y') with $x' > 0$ and $|x'|_2 < 1$. Choosing this one as the representative of $P + E_D(\mathbb{Q})_{2\text{-tors}}$, we have a canonical map

$$\theta : \frac{E_D(\mathbb{Q})}{E_D(\mathbb{Q})_{\text{tors}}} \longrightarrow G \times G \times G, \quad \text{where } G := \frac{\mathbb{Q}^\times}{\mathbb{Q}^{\times 2}},$$

$$(x', y') \longmapsto (x', x' + 2aD, x' + bD) \pmod{\mathbb{Q}^{\times 2}}.$$

Further, the image of θ has size $2^{r(D)}$.

Now, suppose that $(2rt^{-2}, st^{-3})$ is the representative of P satisfying $(rs, t) = 1$, $r > 0$, $2 \nmid t$. Then

$$s^2 = 2r(2r + 2aDt^2)(2r + bDt^2).$$

Suppose that $(r, D) = D_0$ and write $r = r'D_0$. Then

$$s^2 = 4{D_0}^3 r' \left(r' + \frac{aD}{D_0}t^2\right)\left(2r' + \frac{bD}{D_0}t^2\right),$$

so that

$$D_0 \left(\frac{s}{2{D_0}^2}\right)^2 = r' \left(r' + \frac{aD}{D_0}t^2\right)\left(2r' + \frac{bD}{D_0}t^2\right)$$

by noticing that ${D_0}^2 | s$ since D_0 is square-free.

Suppose that

$$\left(r', r' + \frac{aD}{D_0}t^2\right) = (r', a) =: u, \quad \text{say},$$

$$\left(r', 2r' + \frac{bD}{D_0}t^2\right) = (r', b) =: v, \quad \text{say},$$

and

$$\left(r' + \frac{aD}{D_0}t^2, 2r' + \frac{bD}{D_0}t^2\right) = \left(b - 2a, r' + \frac{aD}{D_0}t^2\right) =: w, \quad \text{say}.$$

Obviously u, v, w are coprime in pairs, $2 \nmid uvw$ and, since we are considering things $\bmod \mathbb{Q}^{\times 2}$, we may assume that uvw is square-free. Then we have

$$r' = uvD_1V^2,$$

$$r' + \frac{aD}{D_0}t^2 = uwD_2Y^2,$$

$$2r' + \frac{bD}{D_0}t^2 = vwD_3Z^2,$$

where $D_1D_2D_3 = D_0$. Writing $D/D_0 = D_4$, $a = a'u$, $b = b'v$ and $c = b - 2a = c'w$, we have the following system of quadratic equations:

$$\begin{cases} vD_1V^2 + a'D_4W^2 = wD_2Y^2, \\ 2uD_1V^2 + b'D_4W^2 = wD_3Z^2. \end{cases} \tag{3.1}$$

As with u, v, w, we can absorb square divisors of a', b', c' into the variables V, W, Y, Z, so we assume now that a', b', c' are square-free. From the definition

of the Selmer group for an elliptic curve, the number of systems (3.1) which are everywhere locally solvable equals $2^{s(D)}$, the order of the 2-Selmer group modulo the 2-torsion group. Note that, if a prime p does not divide any of the coefficients of the system, then the system is solvable in $\mathbb{Q}_p - \{0\}$. So it suffices just to consider the primes $p|abcD$.

We start the prime division discussion as follows:

P1. if $p|D_1$, then we need $(\frac{a'wD_2D_4}{p}) = (\frac{b'wD_3D_4}{p}) = 1$,

P2. if $p|D_2$, then we need $(\frac{-a'vD_1D_4}{p}) = (\frac{c'vD_3D_4}{p}) = 1$,

P3. if $p|D_3$, then we need $(\frac{-2b'uD_1D_4}{p}) = (\frac{-2c'uD_2D_4}{p}) = 1$,

P4. if $p|D_4$, then we need $(\frac{vwD_1D_2}{p}) = (\frac{2uwD_1D_3}{p}) = 1$.

Before we present the prime division discussion about a', b', c' and u, v, w, we explain why we have restricted h to satisfying conditions (Ca), (Cb), (Cc). The purpose of choosing h in this way is to ensure that, if the system (3.1) is $\mathbb{Q}_p$-solvable for all p, then $(a', u) = (b', v) = (c', w) = 1$. For example, if there were some prime p dividing (a', u) for a $\mathbb{Q}_p$-solvable system (3.1), then we know that $\mathrm{ord}_p(a)$ must be even and thus (Ca) holds in this case, and from (3.1) we have

$$\left(\frac{vwD_1D_2}{p}\right) = \left(\frac{b'wD_3D_4}{p}\right) = 1,$$

which implies that

$$\left(\frac{bD_1D_2D_3D_4}{p}\right) = \left(\frac{bD}{p}\right) = \left(\frac{bh}{p}\right) = 1,$$

contrary to restriction (Ca). Thus, we may assume that $a'b'c'uvw$ is square-free. So, now for any $\mathbb{Q}_p$-solvable system (3.1), we have

P5. if $p|a'$, then $(\frac{vwD_1D_2}{p}) = 1$,

P6. if $p|b'$, then $(\frac{2uwD_1D_3}{p}) = 1$,

P7. if $p|c'$, then $(\frac{2uvD_2D_3}{p}) = 1$,

P8. if $p|u$, then $(\frac{b'wD_3D_4}{p}) = 1$,

P9. if $p|v$, then $(\frac{a'wD_2D_4}{p}) = 1$,

P10. if $p|w$, then $(\frac{-a'vD_1D_4}{p}) = 1$.

In view of the prime division discussions, if, for example, $p \mid D_1$, then we need

$$\frac{1}{4}\left\{1 + \left(\frac{a'wD_2D_4}{p}\right)\right\}\left\{1 + \left(\frac{b'wD_3D_4}{p}\right)\right\} = 1,$$

namely,

$$\frac{1}{4}\left\{1 + \left(\frac{a'wD_2D_4}{p}\right) + \left(\frac{b'wD_3D_4}{p}\right) + \left(\frac{a'b'D_2D_3}{p}\right)\right\} = 1. \tag{3.2}$$

By taking the product of (3.2) over all the prime factors p of D_1, with the same notation as Heath-Brown's, we denote

$$\Pi(D_1) := \prod_{p|D_1} \frac{1}{4}\left\{1+\left(\frac{a'wD_2D_4}{p}\right)+\left(\frac{b'wD_3D_4}{p}\right)+\left(\frac{a'b'D_2D_3}{p}\right)\right\}$$
$$= 4^{-\omega(D_1)} \sum_{D_1=D_{10}D_{12}D_{13}D_{14}} \left(\frac{a'wD_2D_4}{D_{13}}\right)\left(\frac{b'wD_3D_4}{D_{12}}\right)\left(\frac{a'b'D_2D_3}{D_{14}}\right), \tag{3.3}$$

and we can similarly denote $\Pi(D_2)$, $\Pi(D_3)$ and $\Pi(D_4)$ according to conditions P2, P3 and P4. We also denote

$$\Pi(u) := 2^{-\omega(u)} \sum_{u_s|u} \left(\frac{b'wD_3D_4}{u_s}\right), \tag{3.4}$$

where $\omega(u)$ is the number of different prime factors of u, and similarly define $\Pi(v)$, $\Pi(w)$, $\Pi(a')$, $\Pi(b')$ and $\Pi(c')$ in accordance with the conditions P5–P10.

From the above discussion, it is then easy to verify the following lemma, though the formula (3.8) looks very complicated.

LEMMA 2. *With the previous notation,*

$$2^{s(D)} = \sum_{\vec{D}} \sum_{\vec{a}} \sum_{\vec{b}} \sum_{\vec{c}} \Pi(D_1)\cdots\Pi(D_4)\Pi(u)\cdots\Pi(c') \tag{3.5}$$

where the sum is taken over all the factorizations

$$D = D_1D_2D_3D_4, \qquad \gamma(a) = a'u, \qquad \gamma(b) = a'v \qquad \text{and} \qquad \gamma(c) = c'w,$$

and $\gamma(m)$ is m divided by its largest square divisor.

This may further be written as

$$2^{s(D)} = \sum_{\vec{D}} g(\vec{D}), \tag{3.6}$$

where the sum is taken over all the factorizations of

$$D = \prod_{1\leqslant i\leqslant 4,\ 0\leqslant j\neq i\leqslant 4} D_{ij}$$

and where, with $\star$ briefly representing the letters a', b', c', u, v, w and the $a'_s, b'_s, c'_s, u_s, v_s, w_s$

$$g(\vec{D}) = \sum_{\gamma(a)=a'u} \sum_{\gamma(b)=b'v} \sum_{\gamma(c)=c'w} \sum_{u_s|u} \sum_{v_s|v} \sum_{w_s|w} \sum_{a'_s|a'} \sum_{b'_s|b'} \sum_{c'_s|c'} g_\star(\vec{D}) \tag{3.7}$$

with

$$g_\star(\vec{D}) = 2^{-\omega(abc)}\left(\frac{-1}{\alpha}\right)\left(\frac{2}{\beta}\right)\prod_{i=1}^{4} 4^{-\omega(D_{i0})} \prod_{j\neq 0,i} 4^{-\omega(D_{ij})} \prod_{k\neq i,j} \prod_{0\leqslant l\neq k\leqslant 4} \left(\frac{D_{kl}}{D_{ij}}\right)$$
$$\times \left(\frac{a'}{D_{13}D_{14}D_{23}D_{24}v_sw_s}\right)\left(\frac{b'}{D_{12}D_{14}D_{32}D_{34}u_s}\right)\left(\frac{c'}{D_{21}D_{24}D_{31}D_{34}}\right)$$
$$\times \left(\frac{u}{D_{31}D_{32}D_{41}D_{42}b'_sc'_s}\right)\left(\frac{v}{D_{21}D_{23}D_{41}D_{43}w_sa'_sc'_s}\right)$$

$$\times\left(\frac{w}{D_{12}D_{13}D_{42}D_{43}u_s v_s a'_s b'_s}\right)\prod_{j\neq 1}\left(\frac{D_{1j}}{a'_s b'_s w_s}\right)\prod_{j\neq 2}\left(\frac{D_{2j}}{a'_s c'_s v_s}\right)$$

$$\times\prod_{j\neq 3}\left(\frac{D_{3j}}{b'_s c'_s u_s}\right)\prod_{j\neq 4}\left(\frac{D_{4j}}{u_s v_s w_s}\right), \tag{3.8}$$

where

$$\alpha = D_{23}D_{24}D_{31}D_{32}w_s \quad \text{and} \quad \beta = D_{31}D_{32}D_{41}D_{42}\,b'_s c'_s.$$

§4. *Some error cases.* With the expression in Lemma 1, the sum $\sum 2^{s(D)}$ is translated into a multiple character sum with 28 new variables, 12 of which are divisors of a, b and c of some special types and the other 16 variables D_{ij} are subject to the conditions that each D_{ij} is square-free, that they are pairwise coprime and that their product D satisfies

$$D \leqslant X, \qquad D \equiv h \bmod C.$$

The main contribution to the asymptotic formula of $\sum 2^{s(D)}$ arises from the terms with D and abc having several special types of factorizations that will be specified in the last section. We divide the range of each D_{ij} into intervals $(A_{ij}, 2A_{ij}]$ with A_{ij} running over powers of 2 and

$$1 \ll \prod A_{ij} \ll X.$$

This gives us $O(\log^{16} X)$ non-empty subsums, each written as $S(\vec{A})$, with $\vec{A}$ referring to the 16-tuple of numbers A_{ij}. Further, we shall with a brief notation $S_\star(\vec{A})$ define the sum of $g_\star(\vec{D})$ with the D_{ij}'s running over the A_{ij}.

With Heath-Brown's terminology, two variables ♣ and ♠ are called "linked" if exactly one of the Jacobi symbols

$$\left(\frac{\spadesuit}{\clubsuit}\right) \quad \text{or} \quad \left(\frac{\clubsuit}{\spadesuit}\right)$$

occurs in $g(\vec{D})$. In the case that we have ♠ $= D_{ij}$ and ♣ $= D_{kl}$ for some variables $D_{ij} \neq D_{kl}$, it is clear that they are linked if and only if $i \neq k$ and precisely one of the conditions $l \neq 0$, j or $j \neq 0, k$ holds.

Two unlinked variables D_{ij} and D_{kl} are called "joined" if both Jacobi symbols

$$\left(\frac{D_{ij}}{D_{kl}}\right) \quad \text{and} \quad \left(\frac{D_{kl}}{D_{ij}}\right)$$

occur in the expression of $g(\vec{D})$; otherwise they are called "independent".

Before giving estimates to some error cases, we state two lemmas concerning estimating character sums here. The first one is Lemma 6 of [**4**] and the second is Lemma 4.1 of [**20**].

LEMMA 3. *Let N be sufficiently large. Then, for arbitrary positive integers q, r and any non-principal character $\chi \pmod q$,*

$$\sum_{n\leqslant x,(n,r)=1} \mu^2(n)4^{-\omega(n)}\chi(n) \ll xd(r)\exp(-\eta\sqrt{\log x}) \tag{4.1}$$

with a positive constant $\eta = \eta_N$, *uniformly for* $q \leqslant \log^N x$. *Here and throughout* $d(r)$ *denotes the usual divisor function.*

LEMMA 4. *Suppose that* $\varepsilon > 0$ *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* $|a_m|, |b_n| \leqslant 1$. *Fix positive integers* h, q *satisfying* $(h, q) = 1$ *and* $q \leqslant \{\min(M, N)\}^{\varepsilon/3}$. *Let*

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

where the summation is subject to

$$M < m \leqslant 2M, \qquad N < n \leqslant 2N, \qquad mn \leqslant X \qquad \text{and} \qquad mn \equiv h \pmod{q}.$$

Then

$$S \ll MN^{15/16+\varepsilon} + M^{15/16+\varepsilon} N, \tag{4.2}$$

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

Henceforth, we set

$$T := \exp((\log X)^{1/20}) \quad \text{and} \quad K := (\log X)^{340}. \tag{4.3}$$

Now we consider some subsums of $\sum 2^{s(D)}$ in the following several cases.

- Case 1: $A_{ij}, A_{kl} > K$, where D_{ij} and D_{kl} are linked.

First we note that, from Lemma 1, $g_\star(\vec{D})$ can be written in the form

$$g_\star(\vec{D}) = \left(\frac{D_{ij}}{D_{kl}}\right) \lambda(D_{ij}) \xi(D_{kl}) \zeta, \tag{4.4}$$

where the function $\lambda(D_{ij})$ is the product of $4^{-\omega(D_{ij})}$ and the Jacobi symbols appearing in (3.8) that contain D_{ij} (other than $(\frac{D_{ij}}{D_{kl}})$), and similarly for $\xi(D_{kl})$, and ζ is the product of $2^{-\omega(abc)}$, $4^{-\omega(D/D_{ij}D_{kl})}$ and the other Jacobi symbols left. It is clear that $|\lambda(D_{ij})|, |\xi(D_{kl})|, |\zeta| \leqslant 1$.

Let $S(\vec{A})$ be with $A_{ij}, A_{kl} > K$. From (4.4), we have

$$S(\vec{A}) \ll \max_{\lambda, \xi} \sum_{\substack{A_{rs} < D_{rs} \leqslant 2A_{rs} \\ (r,s) \neq (i,j), (k,l)}} \left| \sum_{D_{ij}, D_{kl}} \left(\frac{D_{ij}}{D_{kl}}\right) \lambda(D_{ij}) \xi(D_{kl}) \right|, \tag{4.5}$$

where the maximum is actually taken with respect to the factorizations of abc which affect the values of $\lambda(D_{ij})$ and $\xi(D_{kl})$. We can take ε arbitrarily small in Lemma 3 when X is sufficiently large. In particular, we have

$$S(\vec{A}) \ll \sum_{\substack{A_{rs} < D_{rs} \leqslant 2A_{rs} \\ (r,s) \neq (i,j), (k,l)}} A_{ij} A_{kl} K^{-1/20} \ll \Big(\prod A_{ij}\Big) K^{-1/20} \ll X(\log X)^{-17}. \tag{4.6}$$

In view of this, we conclude that the subsum of $\sum 2^{s(D)}$ with two linked variables $D_{ij}, D_{kl} > K$ is bounded by

$$\sum_{\vec{A}}{}' X(\log X)^{-17} \ll (\log X)^{16} \cdot X(\log X)^{-17} \ll X(\log X)^{-1}. \tag{4.7}$$

Here and throughout the superscript "′" indicates that the sum is subject to the prescribed restrictions.

- Case 2: $A_{ij} > T$, and $A_{kl} \leqslant K$ for all D_{kl} linked with D_{ij} and the product of the D_{kl} is not 1.

We write D' as the product of all the D_{kl} linked with D_{ij}; then trivially $D' \ll (\log X)^{4800}$. Applying the law of quadratic reciprocity to the "joined" pairs of Jacobi symbols involving D_{ij}, we can write $g_\star(\vec{D})$ in the form

$$g_\star(\vec{D}) = 4^{-\omega(D_{ij})} \left(\frac{D_{ij}}{D'}\right) \chi(D_{ij})\zeta, \tag{4.8}$$

where χ is a character modulo C arising from the product of the Jacobi symbols involving D_{ij}, the factors of abc and a modulo 4 character from the application of quadratic reciprocity, and ζ is the product of $2^{-\omega(abc)}$, $4^{-\omega(D/D_{ij})}$ and the other Jacobi symbols left. It is obvious that $|\zeta| \leqslant 1$ and that ζ does not depend on D_{ij}. Thus we have

$$S(\vec{A}) \leqslant \sum_{\vec{a},\vec{b},\vec{c}} |S_\star(\vec{A})| \leqslant \sum_{\vec{a},\vec{b},\vec{c}} \sum_{\substack{D_{rs} \\ (r,s)\neq(i,j)}} \left| \sum_{D_{ij}} \mu^2(D_{ij}) 4^{-\omega(D_{ij})} \left(\frac{D_{ij}}{D'}\right) \chi(D_{ij}) \right|, \tag{4.9}$$

where the notation $\vec{a}$, $\vec{b}$ and $\vec{c}$ indicate that the summation is over factorizations of abc as shown in (3.7), where the inner sum is also subject to that D_{ij} is coprime to all the other variables D_{rs} and

$$D_{ij} \equiv h\bar{k} \pmod{C},$$

where $\bar{n}$ defines the multiplicative inverse of n with respect to the given modulo, and k is the product of all other D_{rs} modulo C. This last restriction can be removed by introducing the characters modulo C into play. Noticing that χ in (4.9) is also of modulo C, we have

$$S(\vec{A}) \ll \sum_{\chi(\bmod C)} \sum_{\substack{D_{rs} \\ (r,s)\neq(i,j)}} \left| \sum_{D_{ij}} \mu^2(D_{ij}) 4^{-\omega(D_{ij})} \left(\frac{D_{ij}}{D'}\right) \chi(D_{ij}) \right|,$$

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

In the case that $D' \neq 1$, Lemma 2 implies that

$$S(\vec{A}) \ll A_{ij} \exp(-\eta\sqrt{A_{ij}}) \prod_{(r,s)\neq(i,j)} \left(\sum_{D_{rs}} d(D_{rs}) \right) \ll X \exp(-\eta\sqrt{A_{ij}})(\log X)^{15}.$$

This implies that, in this case,

$$\sum_{\vec{A}}{}' |S(\vec{A})| \ll X(\log X)^{-1}. \tag{4.10}$$

- Case 3: $A_{ij} > T$ for at most three variables D_{ij}.

Write m as the product of the D_{ij} with $A_{ij} \leqslant T$ and n as the product of the D_{ij} with $A_{ij} > T$. Trivially, each m can arise at most $16^{\omega(m)}$ times and each n

can arise at most $\binom{16}{3}3^{\omega(n)}$ times. For any fixed $\gamma > 0$, it is well known that

$$\sum_{n\leqslant N}\gamma^{\omega(n)} \ll N(\log N)^{\gamma-1}$$

holds for every $N \geqslant 3$. Thus,

$$\begin{aligned}\sum_{A_{ij}}{}'|S(\vec{A})| &\ll \sum_{m\leqslant T^{16}} 4^{\omega(m)} \sum_{n\leqslant X/m}\left(\frac{3}{4}\right)^{\omega(n)} \ll \sum_{m\leqslant T^{16}} 4^{\omega(m)}\frac{X}{m}\left(\log\frac{X}{m}\right)^{-1/4}\\ &\ll \frac{X}{(\log X)^{1/4}}\sum_{m\leqslant T^{16}}\frac{4^{\omega(m)}}{m} \ll \frac{X}{(\log X)^{1/4}}\cdot(\log T)^4 \ll X(\log X)^{-1/20}.\end{aligned} \tag{4.11}$$

In addition to the subsums considered above, some $S_\star(\vec{A})$ obviously give negligible contribution. If $A_{ij} > T$ and D_{ij} is linked with some non-trivial divisor of abc, then, with the argument given in the second case, we have

$$\sum_{\vec{A}}{}'|S_\star(\vec{A})| \ll X(\log X)^{-1}. \tag{4.12}$$

Collecting the estimates (4.7), (4.10), (4.11) and (4.12) together, we have the following lemma.

LEMMA 5. *With the previous notation,*

$$\sum_{\vec{A}}{}'|S(\vec{A})| \ll X(\log X)^{-1/20}, \tag{4.13}$$

where the sum over $\vec{A}$ is for all sets in which either there are at most three $A_{ij} \geqslant T$, or there are linked variables D_{ij} and D_{kl} with $A_{ij} \geqslant T$ and $D_{kl} > 1$.

Furthermore,

$$\sum_{\vec{A}}{}'|S_\star(\vec{A})| \ll X(\log X)^{-1}, \tag{4.14}$$

where the sum over $\vec{A}$ is for those $A_{ij} \geqslant T$ with D_{ij} linked with a non-trivial factor of abc.

§5. *More error cases.* From Lemma 4, we see that the main terms arise from the cases that at least four of the D_{ij} are with $A_{ij} \geqslant T$, and no two of them are linked, and every variable D_{kl} linked to any one of these D_{ij} must be 1. Before distinguishing some of these cases which still give negligible contributions from the others which the main term arises from, first we want to identify the cases that are not included in the estimate (4.13).

To take an example, let us say that $A_{12}, A_{21} > T$. Then we have

$$D_{30} = D_{31} = D_{32} = D_{40} = D_{41} = D_{42} = D_{23} = D_{24} = D_{13} = D_{14} = 1,$$

since these variables are either linked with D_{12} or D_{21}, or both. Thus, among A_{10}, A_{20}, A_{34} and A_{43}, two or more must be greater than T. If we assume that $A_{10} > T$, then we must have $D_{34} = D_{43} = 1$ since they are linked with D_{10}; similarly, if $A_{34} > T$, then we have $D_{10} = D_{20} = 1$ since these variables are

linked with D_{34}. This yields that, if $A_{12}, A_{21} > T$, then we have either

$$A_{12}, A_{21}, A_{10}, A_{20} > T \quad \text{and all other variables } D_{ij} = 1,$$

or

$$A_{12}, A_{21}, A_{34}, A_{43} > T \quad \text{and all other variables } D_{ij} = 1.$$

We note that the cases excluded by Lemma 4 are the same as those excluded by Lemma 8 in [**4**]. With a case by case discussion, Heath-Brown [**4**] actually shows that each of the left cases not included in Lemma 4 is with exactly 4 non-trivial D_{ij}. Moreover, the indices of the four variables with a range greater than T are given by

$$\begin{array}{lll} 10, 20, 30, 40, & i0, j0, ij, ji, & i0, ij, ik, il, \\ i0, ji, ki, li, & ij, ik, lj, lk, & ij, ji, kl, lk, \end{array} \tag{5.1}$$

where i, j, k and l are distinct non-zero indices, and in each case all the other variables D_{ij} are 1. As a reminder, in every case listed, no two variables are linked.

For each one of these cases, by re-labelling the variables, we may write $S(\vec{A})$ in the form

$$\sum_{\gamma(a)=a'u} \sum_{\gamma(b)=b'v} \sum_{\gamma(c)=c'w} \sum_{u_s|u} \sum_{v_s|v} \sum_{w_s|w} \sum_{a'_s|a'} \sum_{b'_s|b'} \sum_{c'_s|c'} \times \sum_{n_1,n_2,n_3,n_4} \chi_1(n_1)\chi_2(n_2)\chi_3(n_3)\chi_4(n_4)PQ, \tag{5.2}$$

where $Q = 4^{-\omega(n_1n_2n_3n_4)}$ and P comes from the product of $2^{-\omega(abc)}$ and some terms ± 1 from applying the law of quadratic reciprocity, and χ_i are the characters modulo 8, arising from $(\frac{-1}{\alpha})$ and $(\frac{2}{\beta})$ in the expression of $g(\vec{D})$.

It is very nice that, in each case, at least two variables are independent, and so we can reduce (5.2) to

$$\sum \cdots \sum \sum_{n_1,n_2} \left| \sum_{n_3} \sum_{n_4} \chi_3(n_3)\chi_4(n_4)PQ \right|, \tag{5.3}$$

where n_3 and n_4 are assumed to be independent and P can be written as the product of $2^{-\omega(abc)}$ and characters $\psi_3(n_3)$, $\psi_4(n_4)$ modulo 4, depending on the other variables alone. So we need to estimate sums of the form

$$\sum_{n_3} \sum_{n_4} (\psi_3\chi_3)(n_3)(\psi_4\chi_4)(n_4)\mu^2(n_3)\mu^2(n_4)4^{-\omega(n_3)}4^{-\omega(n_4)}, \tag{5.4}$$

where n_3 and n_4 are respectively running over some large intervals, satisfying $(n_3, n_4) = 1$ and n_3n_4 congruent to some fixed number modulo C.

To give a non-trivial estimate for (5.4) when either $\psi_3\chi_3$ or $\psi_4\chi_4$ is non-principal, we appeal to the following result.

LEMMA 6. *Let $X > 0$ and $M, N \geqslant T > 0$ be given. Then for any positive integer r, any odd integer h, and any distinct characters $\chi_1, \chi_2 \pmod 8$,*

$$\sum_{m,n} \mu^2(m)\mu^2(n)4^{-\omega(m)-\omega(n)}\chi_1(m)\chi_2(n) \ll d(r)X \exp(-\eta\sqrt{\log T}) \log X \tag{5.5}$$

for some positive absolute constant η, *where the sum is over coprime variables satisfying the conditions*

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

Proof. This is just a little bit different from Lemma 10 of [**3**], where mn is running over an arithmetic progression modulo 8. We can easily get estimate (5.5) from Lemma 2 by noticing that in this case at least one of the characters χ_1, χ_2 is non-principal. □

We write A_{ij} as A_3 if n_3 comes from n_{ij}, similarly for A_4. In the case $A_3, A_4 \geqslant T$, if some character attached to n_3 or n_4, say $\psi_3\chi_3$, is non-trivial, then by using Lemma 3, one gets an upper bound for the above sum, which leads to an upper bound for $S(\vec{A})$ acceptable in the error term of Theorem 2.

We claim that, except for the four cases with the following indices

$$10, 20, 30, 40; \qquad 10, 12, 13, 14; \qquad 30, 13, 23, 43; \qquad 40, 14, 24, 34, \quad (5.6)$$

we can choose the labelling properly so that at least one of $\psi_3\chi_3$ and $\psi_4\chi_4$ is non-trivial. Sometimes we may achieve this by finding $\psi_3 = \psi_4$ while $\chi_3 \neq \chi_4$, or, under the assumptions made at the beginning of this section, we can show that some cases other than those in (5.6) do not happen.

I. $i0, j0, ij, ji$. In four of the six cases, it is not difficult to find the n_3 and n_4 that we need. Except for $(i, j) = (1, 2)$ or $(3, 4)$, at least one of D_{ij} and D_{ji} corresponds to a non-trivial character. Since any pair of variables is independent, if $\chi_{ij} \neq \chi_0$, then by taking

$$n_3 = D_{i0}, \qquad n_4 = D_{ij},$$

we have $\psi_3 = \psi_4$ and $\chi_3 = \chi_0 \neq \chi_4$. When $(i, j) = (1, 2)$ or $(3, 4)$, things become interesting. For example, if $i = 1$, $j = 2$, then in this case, except for $\Pi(D_1)$, $\Pi(D_2)$ and $\Pi(u)$, all the factors in (3.5) are trivially 1. Since a'_s, b'_s, c'_s, v_s and w_s have to be 1 because of (4.14), and $b'w, c'v$ are respectively linked with D_{12}, D_{21}, again from (4.14), we just need to consider the case $b'w = c'v = 1$, which implies that $b = c = 1$. (Recall that this actually means $b \equiv c \equiv 1 \pmod{\mathbb{Q}^\times)^2}$, *i.e.*, both b and c are squares.) But this is absurd because

$$b - c = 2a \equiv 2 \mod 4.$$

The same contradiction arises in the case $(i, j) = (3, 4)$.

II. ij, ji, kl, lk. In the case $(i, j) \neq (1, 2)$ and $(3, 4)$, we may take $n_3 = D_{ij}$ and $n_4 = D_{ji}$, and it turns out that the characters attached to n_3 and n_4 are different. The interesting case is $(i, j) = (1, 2)$ or $(3, 4)$. Assume that $i = 1$, $j = 2$. Because of Lemma 2, it suffices to consider the case $b'_s = b'$, $w_s = w$, $c'_s = c'$ and $v_s = v$. We take $n_3 = D_{12}, n_4 = D_{21}$; then $\psi_3 = \psi_4$ because both n_3 and n_4 are joined with D_{34} and D_{43}. If we had $\chi_3 = \chi_4$, then we must have

$$b'w \equiv c'v \pmod 4$$

because of the law of quadratic reciprocity, which implies that

$$2a = b - c \equiv 0 \pmod 4,$$

contrary to the fact that $2 \nmid a$.

III. ij, ik, lj, lk. Among all of these, except for cases (13, 14, 23, 24) and (31, 32, 41, 42), it can be seen that, if taking $n_3 = D_{ij}, n_4 = D_{ik}$ with $i \neq 1$, then the characters attached to n_3, n_4 are different. In the case (31, 32, 41, 42), because of (4.14), we just need consider the cases where $b' = c' = 1, u_s = u$ and $v = w = 1$, which again implies that $b = c = 1$, leading to a contradiction. In the case (13, 14, 23, 24), we have the same conclusion.

IV. $i0, ij, ik, il$. If $i \neq 1$, then things are almost trivial, since one can choose $n_3 = D_{i0}$, and easily take n_4 to be some other variable so that the characters attached to n_3 and n_4 are different.

V. $i0$, ji, ki, li. These two cases are not in the same category as the above, but the criterion is the same. When $i = 1$ or 2, there is at least one variable, ji, say, with associated character $(\frac{2}{*})$. We may then take

$$n_3 = D_{i0}, \qquad n_4 = D_{ij}.$$

(Note that n_3 and n_4 are independent).

§6. *Conclusion of Theorem* 2*: the leading terms.* From the above discussion, we know all cases except for the four non-trivial variables with indices

$$10, 20, 30, 40; \quad \text{or} \quad 10, 12, 13, 14; \quad \text{or} \quad 30, 13, 23, 43; \quad \text{or} \quad 40, 14, 24, 34.$$

The contributions from all the other cases are acceptable by the error term in Theorem 2.

Now, if we have indices 10, 20, 30, 40, note that, in all the cases with respect to the factors of a, b, c, we just need to consider the term in the case

$$u_s = v_s = w_s = a'_s = b'_s = c'_s = 1,$$

for the contribution of any other case is negligible because of (4.14). Thus

$$g(\vec{D}) = 4^{-\omega(D)} \sum_{D = D_{10} D_{20} D_{30} D_{40}, D_{j0} \geqslant T} 1,$$

which is easily seen to lead to the contribution

$$(1 + o(1))\#S(X; h). \tag{6.1}$$

In the case we have indices 10, 12, 13, 14, the same discussion results in the contribution

$$(1 + o(1))\#S(X; h). \tag{6.2}$$

Now, for case 30, 13, 23, 43, by (4.14), we have $u_s = b'_s = c'_s = 1$, $v_s = v$, $w_s = w$ and $a'_s = a'$; thus, if writing $D_{ij} = D_i$, we have

$$g(\vec{D}) = 2^{-\omega(abc)}4^{-\omega(D)} \sum_{\substack{\gamma(a)=a'u \\ \gamma(b)=b'v \\ \gamma(c)=c'w}} \sum_{\substack{D=D_1D_2D_3D_4 \\ D_i \geqslant T}} \left(\frac{vwD_1D_2}{a'D_4}\right) \times \left(\frac{a'wD_2D_4}{vD_1}\right)\left(\frac{-a'vD_1D_4}{wD_2}\right), \tag{6.3}$$

the summand of which, from the elementary identity

$$1 + \left(\frac{-1}{AB}\right) + \left(\frac{-1}{AC}\right) - \left(\frac{-1}{BC}\right) = 2\left(\frac{-BC}{A}\right)\left(\frac{AB}{C}\right)\left(\frac{AC}{B}\right),$$

is exactly

$$\frac{1}{2}\left\{1 + \left(\frac{-1}{vwD_1D_2}\right) + \left(\frac{-1}{a'wD_2D_4}\right) - \left(\frac{-1}{-a'vD_1D_4}\right)\right\}. \tag{6.4}$$

The terms involving $(\frac{-1}{*})$ can be dealt with by the estimate of character sums. For example, for the term involving $(\frac{-1}{vwD_1D_2})$, we may take

$$n_3 = D_1, \qquad n_4 = D_4,$$

and, using Lemma 5, assign its contribution into the error term. Thus, the total contribution in this case is

$$\left(\frac{1}{2} + o(1)\right)\#S(X;h) \tag{6.5}$$

Similarly, we have the same contribution from the last case. Putting this together with contributions (6.1), (6.2) and (6.5), we have proved Theorem 2.

Acknowledgements. The author is grateful to Professors Andrew Granville and Carl Pomerance for their helpful comments and encouragement, and to Kevin James for showing the author his PhD thesis.

References

1. D. A. Burgess. On character sums and *L*-series, II. *Proc. Lond. Math. Soc.*, (3), (1963), 524–536.

2. D. Goldfeld. Conjectures on elliptic curves over quadratic fields. *Number Theory, Carbondale* 1979 (*Proc. Southern Illinois Conf., Southern Illinois Univ., Carbondale, Ill.*, 1979), *Lecture Notes in Math.*, 751, Springer (Berlin, 1979), 108–118.

3. F. Gouvea and B. Mazur. The square-free sieve and the rank of elliptic curves. *J. Amer. Math. Soc.*, 4 (1991), 1–23.

4. D. R. Heath-Brown. The size of Selmer groups for the congruent number problem, I. *Invent. Math.*, 111 (1993), 171–195.

5. D. R. Heath-Brown. The size of Selmer groups for the congruent number problem, II. *Invent. Math.*, 118 (1994), 331–370.

6. K. James. An example of an elliptic curve with a positive density of prime quadratic twists which have rank zero. *Topics in Number Theory* (*University Park, PA* 1997) (1999), 223–227.

7. K. James. *L*-series with non-zero central critical value. *J. Amer. Math. Soc.*, 11 (1998), 635–641.

8. V. A. Kolyvagin. Finiteness of $E(\mathbb{I})$ and the Tate-Shafarevich group of $E(\mathbb{Q})$ for a subclass of Weil curves. *Izv. Akad. Nauk SSSR Ser. Mat.*, 52 (1988), 522–540, 670–671.
9. B. Mazur. Modular curves and the Eisenstein ideal. *IHES Publ. Math.*, 47 (1977), 33–186.
10. B. Mazur. Rational isogenies of prime degree. *Invent. Math.*, 44 (1978), 129–162.
11. P. Monsky. Generalizing the Birch-Stephens theorem. I: modular curves. *Math. Z.*, 221 (1996), 415–420.
12. K. Ono. Rank zero quadratic twists of modular elliptic curves. *Compositio Math.*, 104 (1996), 293–304.
13. K. Ono. Twists of elliptic curves. *Compositio Math.*, 106 (1997), 349–360.
14. K. Ono and C. Skinner. Fourier coefficients of half-integral weight modular forms modulol. *Ann. Math.*, (2), 147 (1998), 453–476.
15. K. Ono and C. Skinner. Non-vanishing of quadratic twists of modular *L*-functions. *Invent. Math.*, 134 (1998), 651–660.
16. G. Shimura. On modular forms of half integral wieght. *Ann. Math.*, (2), 97 (1973), 440–481.
17. J. Silverman. The arithmetic of elliptic curves. *GTM* 106, Springer (1986).
18. J. L. Waldspurger. Sur les coefficients de Fourier des formes modulaires de poids demi-entier. *J. Math. Pures Appl.*, 60 (1981), 375–484.
19. S. Wong. Elliptic curves and class number divisibility. *Internat. Math. Res. Notices* (1999), 661–672.
20. G. Yu. Rank 0 quadratic twists of a family of elliptic curves. *Compositio Math.*, 135 (2003), 331–356.

Professor Gang Yu,
Department of Mathematics,
University of Michigan,
525 E. University Ave.,
Ann Arbor, MI 48109-1109,
USA.
E-mail: gangyu@math.lsa.umich.edu.

MSC (2000): *Primary* 14H52*; Secondary* 11G05.

Received on the 10*th of May*, 2003.