Can. J. Math. Vol. **45** (4), 1993 pp. 847–862

THE ANALYTIC RANK OF A FAMILY OF ELLIPTIC CURVES

LIEM MAI

ABSTRACT We study the family of elliptic curves E_m $X^3 + Y^3 = m$ where m is a cubefree integer

The elliptic curves E_m with even analytic rank and those with odd analytic rank are proved to be equally distributed It is proved that the number of cubefree integers $m \leq X$ such that the analytic rank of E_m is even and ≥ 2 is at least $CX^{2/3-\varepsilon}$, where ε is arbitrarily small and C is a positive constant, for X large enough Therefore, if we assume the Birch and Swinnerton-Dyer conjecture, the number of all cubefree integers $m \leq X$ such that the equation $X^3 + Y^3 = m$ have at least two independent rational solutions is at least $CX^{2/3-\varepsilon}$

1. **Introduction.** For an elliptic curve E over $\mathbb{Q}$, the set of all rational points $E(\mathbb{Q})$ is known to be a finitely generated abelian group by a theorem of Mordell-Weil. We will call its rank the *(algebraic) rank* of the elliptic curve. It is positive if and only if E has infinitely many rational points. One important problem in the study of elliptic curves is to determine their ranks.

Attached to an elliptic curve E of conductor N, we have an L-series $L_E(s) = \sum_{n=1}^{\infty} a_n n^{-s}$ (see Silverman [12]). If we define

$$\zeta_E(s) = N^{s/2}(2\pi)^{-s}\Gamma(s)L_E(s),$$

then for modular elliptic curves it is known that $\zeta_E(s)$ has analytic continuation and satisfies

$$\zeta_E(s) = W\zeta_E(2-s)$$

with $W = \pm 1$. Here, W is called the *root number*. The so-called Taniyama-Weil conjecture says that all elliptic curves over $\mathbb{Q}$ are modular (see Taniyama [13]). Weil's converse theorem allows us to reduce the conjecture to a problem in analytic continuation and functional equation of a family of Dirichlet series (see Weil [14]).

In connection with the rank of an elliptic curve E, the weak form of Birch and Swinnerton-Dyer conjecture states that the rank of E is equal to the order of vanishing at the central point $s = 1$ of $L_E(s)$ and its parity is determined by the root number (see Silverman [12]).

DEFINITION. The analytic rank of an elliptic curve E is the order of vanishing at the central point $s = 1$ of $L_E(s)$.

Received by the editors November 12, 1991
AMS subject classification 11G05, 14H52

Now, if χ is a Dirichlet character, we can form the twisted L series $L(s) = \sum_{n=1}^{\infty} a_n \chi(n) n^{-s}$. If χ is quadratic, this is an L-series of another elliptic curve E_χ over $\mathbb{Q}$. Fixing an elliptic curve E over $\mathbb{Q}$, we can consider the family E_χ of such twisted curves of E. What can we say about the number of such twisted curves which have algebraic rank $\geq r$, for a fixed positive integer r? What can we say about analytic rank?

In the case of such quadratic twists, Gouvea and Mazur in [4] gave a partial answer variation of the algebraic rank. More specifically let E have the Weierstrass equation $Y^2 = X^3 + AX + B$. For any squarefree integer D, denote E_D the quadratic twist of E by D (*i.e.* by the Legendre symbol $(\frac{D}{\cdot})$). Then E_D is an elliptic curve and has the equation $DY^2 = X^3 + AX + B$. Assuming the Birch and Swinnerton-Dyer conjecture, Gouvea and Mazur have proved that for X large enough, the number of squarefree integers $D < X$ such that E_D has even algebraic rank ≥ 2 (*i.e.* $W_{E_D} = 1$ and E_D has infinitely many rational points) is at least $CX^{1/2-\varepsilon}$ for C a positive constant and ε arbitrarily small. In general, no information is obtained for higher-order twisted curves. (See Silverman [12] for the definition of the twist of E.) In this paper, we consider certain cubic twists, namely

$$X^3 + Y^3 = m.$$

The problem of determining whether an integer can be expressed as the sum of two rational cubes has a long history. As mentioned in [15], Dickson listed 50 papers on the subject before 1918 in his History of the Theory of Numbers. Equivalently, we want to study the family of elliptic curves $E_m: X^3 + Y^3 = m$. It is known that they are twisted curves of the fixed elliptic curves $E_1: X^3 + Y^3 = 1$ by cubic characters. In [15], Zagier and Kramarz gave numerical data suggesting that about 23.3% of the curves E_m which have even algebraic rank (*i.e.* with root number 1, assuming the Birch and Swinnerton-Dyer conjecture) have algebraic rank ≥ 2.

In this paper, we obtain a similar result to Gouvea and Mazur's for this family of cubic twisted curves.

MAIN THEOREM. *For X large enough, the set of all cubefree integers $m < X$ such that the analytic rank of E_m is even and greater or equal to 2 is at least $CX^{2/3-\varepsilon}$ for a positive constant C and arbitrarily small ε.*

Therefore, assuming the Birch and Swinnerton-Dyer conjecture, the set of all cubefree integers $m < X$ such that E_m has even rank ≥ 2 is at least $CX^{2/3-\varepsilon}$.

We recall some facts about the family E_m.

For m cubefree, the curve $E_m: X^3+Y^3 = m$ has the Weierstrass form $Y^2 = X^3 - 2^4 3^3 m^2$. This can be seen through the map:

$$\begin{aligned} E_m: X^3 + Y^3 = m &\longrightarrow E'_m: Y^2 = X^3 - 2^4 3^3 m^2 \\ (X, Y) &\longmapsto \big(2^2 3(X^2 - XY + Y^2), 2^2 3^2 (X - Y)(X^2 - XY + Y^2)\big). \end{aligned}$$

About the torsion subgroup of $E_m(\mathbb{Q})$, Nagell (see [11]) showed that for $m \neq 1, 2$, $E_m(\mathbb{Q})$ is torsionfree and $|E_1(\mathbb{Q})| = 3$, $|E_2(\mathbb{Q})| = 2$.

https://doi.org/10.4153/CJM-1993-048-9 Published online by Cambridge University Press

The root number W_m is also known explicitly. Indeed Birch and Stephens in [1] prove that

$$W_m = \prod_p W_m(p) \tag{1}$$

where for $p \neq 3$,

$$W_m(p) = \begin{cases} -1 & \text{if } p|m, \quad p \equiv 2 \pmod 3 \\ 1 & \text{elsewhere} \end{cases}$$

and for $p = 3$,

$$W_m(3) = \begin{cases} 1 & \text{if } m \equiv \pm 1, \pm 3 \pmod 9 \\ -1 & \text{if } m \equiv 0, \pm 2, \pm 4 \pmod 9). \end{cases}$$

In §2, we will prove that for X large enough, the number of cubefree integers $m < X$ such that E_m has nonzero algebraic rank is at least $CX^{2/3-\varepsilon}$ for C a positive constant and ε arbitrarily small.

In §3, it is proved that the curves E_m with root number 1 have density $\frac{1}{2}$ among the set $\{m \text{ cubefree}\}$. Therefore, assuming the Birch and Swinnerton-Dyer conjecture, half of the E_m's will have even rank and half with odd rank, asymptotically.

In §4, we introduce the additional condition $W_m = 1$ and prove the main theorem.

2. **Distribution of the set of E_m's with nonzero rank.** In [4], it is shown that for every squarefree integer D of the form $V(U^3 + AUV^2 + BV^3)$, $(U, V) \in \mathbb{Z}^2$ the quadratic twisted curve:

$$E_D \colon DY^2 = X^3 + AX + B$$

contains a rational point which is either of infinite order or of order > 2.

Since all E_D except for a finite number have no rational torsion points of order > 2, they need only count the squarefree $D \leq X$ of the form $V(U^3 + AUV^2 + BV^3)$.

Recall that the twisted curves $E_m \colon X^3 + Y^3 = m$ has the Weierstrass form:

$$E'_m \colon Y^2 = X^3 - 2^4 3^3 m^2.$$

We will prove that, for certain m, then E'_m contains integral, hence rational points.

As mentioned in §1, all E'_m except for $m = 1$ and 2 have no rational torsion, and we will count the cubefree integers m of that form.

LEMMA 2.1. *E'_m has integral points $\Longleftrightarrow$ m has one of the six forms:* $\pm\frac{b(a^2-b^2)}{4}$, $\pm\frac{1}{24}(3a^2b - 3b^3) \pm \frac{1}{24}(a^3 - 9ab^2)$ *for some* $a, b \in \mathbb{Z}$.

PROOF. Suppose E'_m has an integral point (X, Y), then

$$\begin{aligned} X^3 &= Y^2 + 3(12m)^2 \\ &= (Y + 12m\sqrt{-3})(Y - 12m\sqrt{-3}). \end{aligned}$$

https://doi.org/10.4153/CJM-1993-048-9 Published online by Cambridge University Press

Since the ring of integers O_K of $K = \mathbb{Q}(\sqrt{-3})$ is a Dedekind domain, we have the factorization

$$(Y + 12m\sqrt{-3}) = \prod (P_\iota)^{m_\iota}$$
$$(Y - 12m\sqrt{-3}) = \prod (\bar{P}_\iota)^{m_\iota}$$

which shows that $X^3 = \prod (P_\iota \bar{P}_\iota)^{m_\iota} = \prod (p_\iota)^{a_\iota m_\iota}$ where $a_\iota = 1$ or 2.

Since $X \in \mathbb{Z}$, $3|a_\iota m_\iota$ for all i, hence $3|m_\iota$.

Therefore, since O_K is a principal ideal domain,

$$(Y + 12m\sqrt{-3}) = \left(\prod P_\iota^{m_\iota/3}\right)^3$$
$$= (a + b\sqrt{-3})^3 \text{ for } a, b, \in \mathbb{Z}.$$

This implies

$$Y + 12m\sqrt{-3} = \alpha(a + b\sqrt{-3})^3$$
$$= \alpha\big((a^3 - 9ab^2) + \sqrt{-3}(3a^2b - 3b^3)\big)$$

where α is a unit of the ring of integers $\mathbb{Z}[\frac{1+\sqrt{-3}}{2}]$.

If $\alpha = \pm 1$, then $m = \pm\frac{1}{12}(3a^2b - 3b^3) = \pm\frac{b(a^2-b^2)}{4}$.

If $\alpha = \pm\frac{1}{2} \pm \frac{\sqrt{-3}}{2}$, $m = \pm\frac{1}{24}(3a^2b - 3b^3) \pm \frac{1}{24}(a^3 - 9ab^2)$.

Conversely, if m is one of the above forms, then E'_m has at least one integral point, namely:

$$(X, Y) = \big(a^2 + 3b^2, \pm(a^3 - 9ab^2)\big) \quad \text{or}$$
$$(X, Y) = \left(a^2 + 3b^2, \pm\frac{1}{2}(a^3 - 9ab^2) \pm \frac{(-3)}{2}(3a^2b - 3b^3)\right) \qquad \blacksquare$$

LEMMA 2.2. *Suppose $(X, Y) \in E'_m(\mathbb{Q})$. Then there is $e \in \mathbb{Z}$ such that $X = X_0/e^2$, $Y = Y_0/e^3$ and $X_0, Y_0 \in \mathbb{Z}$.*

PROOF. For any prime p such that $\nu_p(X) =$ (order of X at p) < 0, we have

$$0 > \nu_p(X^3) = 3\nu_p(X) = \nu_p\big(Y^2 + 3(12m^2)\big)$$
$$= \nu_p(Y^2) = 2\nu_p(Y).$$

In particular $2|\nu_p(X)$.

Let $e = \prod_{\substack{p \text{ prime} \\ \nu_p(X)<0}} p^{-\nu_p(X)/2}$ and $X_0 = Xe^2$, $Y_0 = Ye^3$ then $X_0, Y_0 \in \mathbb{Z}$. $\blacksquare$

Lemma 2.2 implies that if E'_m has a rational point then E'_{me^3} has an integral point for some $e \in \mathbb{Z}$, and vice versa. We want to count

$$\#\{m \text{ cubefree} \le X : E'_m \text{ has rational points}\}$$
$$= \#\{m \text{ cubefree} \le X : E'_{me^3} \text{ has integral points for some } e \in \mathbb{Z}\}$$
$$= \#\Big\{m \text{ cubefree } \le X : m = \frac{b(a^2 - b^2)}{4e^3} \text{ or}$$
$$m = \pm\frac{1}{24e^3}(3a^2b - 3b^3) \pm \frac{1}{24e^3}(a^3 - 9ab^2) \text{ for some } a, b, e \in \mathbb{Z}\Big\}.$$

https://doi.org/10.4153/CJM-1993-048-9 Published online by Cambridge University Press

Now fix $e = 1$ and consider the case $m = \frac{b(a^2-b^2)}{4}$. Let Φ be the following injection:

$$S = \Big\{(a,b) : (a,b) = 1,\ m = b\big(a^2 - (4b)^2\big) \le X \text{ and } m \text{ is cubefree}\Big\}$$
$$\longrightarrow T = \left\{(a',b') : m' = \frac{b'(a'^2 - b'^2)}{4} \le X \text{ and } m' \text{ is cubefree}\right\}$$
$$(a,b) \longmapsto (a, 4b).$$

Our aim is to prove $|T| \gg X^{2/3}$. For each m, we can find at most $d(m) = O(X^{\varepsilon})$ values for b and for each b, at most 2 values of a such that $m = \frac{b(a^2-b^2)}{4}$. Therefore, $|T| \gg X^{2/3}$ will imply that:

$$\#\{m \le X, m \text{ is cubefree and } E'_m \text{ has an integral point}\} \gg X^{2/3-\varepsilon}.$$

To do this, we will prove that $|S| \gg X^{2/3}$.

More generally, we will prove that:

THEOREM 1. *Given integers M and a_0, b_0, such that $b_0, a_0 - 4b_0$, $a_0 + 4b_0$ are relatively prime to $2M$ and positive integers m_1, m_2, m_3 such that $m_i \ge 2$, $m_2 + m_3 \ge 5$. Let*

$$S_1 = \Big\{(a,b) : m = b\big(a^2 - (4b)^2\big) < X,\ (a,b) = 1,\ b, a - 4b,\ a + 4b \text{ are } m_1,\ m_2,\ m_3 \text{ powerfree respectively},\ a \equiv a_0 \pmod{2M},\ b \equiv b_0 \pmod{2M}\Big\}$$

then

$$|S_1| \ge CX^{2/3} + O(X^{1/3+1/3m_2+1/3m_3+\varepsilon}) + O(X^{1/2+\varepsilon})$$

where $C > 0$, ε is arbitrarily small and X is large enough.

PROOF OF THE THEOREM. At first, note that the above conditions on (a,b) imply that b, $a - 4b$, $a + 4b$ are pairwise coprime.

If we choose (a,b) such that $b \le (X/16)^{1/3}$ then $(4b)^2 \le X/b$. In this case, if $a^2 \le 2(4b)^2$, then $a^2 \le X/b + (4b)^2$, *i.e.* $m = b\big(a^2 - (4b)^2\big) \le X$ and $a-4b, a+4b$ are $\ll X^{1/3}$. We have

$$|S_1| = \sum_{(a,b)\in S_1} \Big(\sum_{d^{m_1}|b} \mu(d)\Big)\Big(\sum_{e^{m_2}|a-4b} \mu(e)\Big)\Big(\sum_{f^{m_3}|a+4b} \mu(f)\Big)$$
$$\ge \sum_{\substack{(a,b)=1 \\ 0<b\le(X/16)^{1/3} \\ 4b\le a\le 4\sqrt{2}b \\ a\equiv a_0 \pmod{2M}, b\equiv b_0 \pmod{2M}}} \Bigg(\sum_{\substack{d^{m_1}|b \\ d\ll X^{1/3m_1}}} \sum_{\substack{e^{m_2}|a-4b \\ e\ll X^{1/3m_2}}} \sum_{\substack{f^{m_3}|a+4b \\ f\ll X^{1/3m_3}}} \mu(d)\mu(e)\mu(f)\Bigg)$$
$$\sum_{\substack{d\ll X^{1/3m_1} \\ e\ll X^{1/3m_2} \\ f\ll X^{1/3m_3} \\ (d,2M)=(e,2M)=(f,2M)=1}} \mu(d)\mu(e)\mu(f) \sum_{\substack{0<b\le(X/16)^{1/3} \\ b\equiv 0 \pmod{d^{m_1}} \\ b\equiv b_0 \pmod{2M}}} \sum_{\substack{4b\le a\le 4\sqrt{2}b \\ a\equiv 4b \pmod{e^{m_2}} \\ a\equiv -4b \pmod{f^{m_3}} \\ a\equiv a_0 \pmod{2M} \\ (a,b)=1}} 1$$

Note that e^{m_2}, f^{m_3} and $2M$ are pairwise coprime.

Now

$$\sum_{\substack{A\le a\le B\\ a\equiv * \pmod{e^{m_2}f^{m_3}2M}\\ (a,b)=1}} 1 = \sum_{\substack{A\le a\le B\\ a\equiv * \pmod{e^{m_2}f^{m_3}2M}}} \sum_{\substack{n|a\\ n|b}} \mu(n)$$

$$= \sum_{n|b} \mu(n)\Big(\sum_{\substack{A/n\le a'\le B/n\\ a=na'\equiv * \pmod{e^{m_2}f^{m_3}2M}}} 1\Big)$$

(n and $e^{m_2}f^{m_3}2M$ are coprime since $\Big(b, \big(a^2-(4b)^2 2M\big)\Big)=1$)

$$= \sum_{n|b}\mu(n)\Big\{\frac{B-A}{ne^{m_2}f^{m_3}2M}+O(1)\Big\}$$

$$= \frac{B-A}{e^{m_2}f^{m_3}2M}\sum_{n|b}\frac{\mu(n)}{n}+O\Big(\sum_{n|b}|\mu(n)|\Big)$$

$$= \frac{B-A}{e^{m_2}f^{m_3}2M}\frac{\phi(b)}{b}+O(X^{\varepsilon}).$$

Then

$$|S_1| \ge \sum_{\substack{d\ll X^{1/3m_1}\\ e\ll X^{1/3m_2}\\ f\ll X^{1/3m_3}\\ (d,2M)=(e,2M)=(f,2M)=1}} \mu(d)\mu(e)\mu(f) \sum_{\substack{0<b\le (X/16)^{1/3}\\ b\equiv 0 \pmod{d^{m_1}}\\ b\equiv b_0 \pmod{2M}}} \Big(\frac{4\sqrt{2}-4}{e^{m_2}f^{m_3}2M}\phi(b)+O(X^{\varepsilon})\Big)$$

$$= \frac{4\sqrt{2}-4}{2M} \sum_{\substack{d\ll X^{1/3m_1}\\ e\ll X^{1/3m_2}\\ f\ll X^{1/3m_3}\\ (d,2M)=(e,2M)=(f,2M)=1}} \mu(d)\mu(e)\mu(f)$$

$$\Big\{\frac{1}{e^{m_2}f^{m_3}} \sum_{\substack{0<b\le (X/16)^{1/3}\\ b\equiv 0 \pmod{d^{m_1}}\\ b\equiv b_0 \pmod{2M}}} \phi(b)+O\Big(\frac{X^{1/3+\varepsilon}}{d^{m_1}}\Big)\Big\}$$

$$= \frac{4\sqrt{2}-4}{2M} \sum_{\substack{d\ll X^{1/3m_1}\\ e\ll X^{1/3m_2}\\ f\ll X^{1/3m_3}\\ (d,2M)=(e,2M)=(f,2M)=1}} \frac{\mu(d)\mu(e)\mu(f)}{e^{m_2}f^{m_3}} \sum_{\substack{0<b\le (X/16)^{1/3}\\ b\equiv 0 \pmod{d^{m_1}}\\ b\equiv b_0 \pmod{2M}}} \phi(b)$$

$$+ O(X^{1/3+1/3m_2+1/3m_3+\varepsilon})$$

since the series $\sum_d \frac{1}{d^{m_1}}$ converges.

Now

$$\sum_{\substack{0<b\le (X/16)^{1/3}\\ b\equiv 0 \pmod{d^{m_1}}\\ b\equiv b_0 \pmod{2M}}} \phi(b) = \sum_{\substack{0<b\le (X/16)^{1/3}\\ b\equiv 0 \pmod{d^{m_1}}\\ b\equiv b_0 \pmod{2M}}} b\sum_{t|b}\frac{\mu(t)}{t}$$
$$= \sum_{t\le (X/16)^{1/3}} \mu(t) \sum_{\substack{0<b'\le (X/16)^{1/3}/t\\ tb'\equiv 0 \pmod{d^{m_1}}\\ tb'\equiv b_0 \pmod{2M}}} b'$$
$$= \sum_{r|d^{m_1}2M}\ \sum_{\substack{t\le (X/16)^{1/3}\\ (t,d^{m_1}.2M)=r}} \mu(t) \sum_{\substack{0<b'\le (X/16)^{1/3}/t\\ tb'\equiv 0 \pmod{d^{m_1}}\\ tb'\equiv b_0 \pmod{2M}}} b'$$
$$= \sum_{r|d^{m_1}}\ \sum_{\substack{t\le (X/16)^{1/3}\\ (t,d^{m_1}.2M)=r}} \mu(t) \sum_{\substack{0<b'\le (X/16)^{1/3}/t\\ tb'\equiv 0 \pmod{d^{m_1}}\\ tb'\equiv b_0 \pmod{2M}}} b'.$$

The last step follows noting that if $(r,2M)\neq 1$, then $(t,2M)\neq 1$ and this contradicts the condition $tb'\equiv b_0 \pmod{2M}$, and $(b_0,2M)=1$. Moreover, the two congruence conditions on b' can be combined into one, as $(t,2M)=1$, and $(t,d^{m_1})=r$. Therefore, we have

$$\sum_{\substack{0<b\le (X/16)^{1/3}\\ b\equiv 0 \pmod{d^{m_1}}\\ b\equiv b_0 \pmod{2M}}} \phi(b) = \sum_{r|d^{m_1}}\ \sum_{\substack{0\le t\le (X/16)^{1/3}\\ (t,d^{m_1}.2M)=r}} \mu(t) \sum_{\substack{0<b'\le (X/16)^{1/3}/t\\ b'\equiv b_0' \pmod{(d^{m_1}/r).2M}}} b'$$

where b_0' is an integer such that $tb_0'\equiv b_0 \pmod{2M}$.

We need a lemma:

LEMMA 2.3.
$$\sum_{\substack{0<x\le Z\\ x\equiv x_0(n)}} x = \frac{1}{2n}Z^2 + O(Z).$$

PROOF. Note that we can always choose $0\le x_0\le n$. Moreover, if $n\ge Z$ the conclusion is clear. Therefore, we need only consider the case $n\le Z$. In that case, we have

$$\sum_{\substack{0<x\le Z\\ x\equiv x_0 \pmod{n}}} x = \sum_{-x_0/n<y\le (Z-x_0)/n} (x_0+ny)$$
$$= \sum_y x_0 + n\sum_y y$$
$$= x_0\Big(\frac{Z}{n}+O(1)\Big) + n\Big(\frac{1}{2}\Big(\frac{Z}{n}\Big)^2 + O\Big(\frac{Z}{n}\Big)\Big)$$
$$= \frac{1}{2n}Z^2 + O(Z). \qquad \blacksquare$$

Applying the lemma, we have:

$$\sum_{\substack{0<b\leq(X/16)^{1/3}\\ b\equiv 0 \pmod{d^{m_1}}\\ b\equiv b_0 \pmod{2M}}} \phi(b) = \sum_{r|d^{m_1}} \sum_{\substack{t\leq(X/16)^{1/3}\\ (t,d^{m_1}2M)=r}} \mu(t)\left\{\frac{1}{(d^{m_1}/r)4M}\frac{(X/16)^{2/3}}{t^2}+O\left(\frac{X^{1/3}}{t}\right)\right\}$$

$$= \sum_{r|d^{m_1}} \sum_{\substack{t\leq(X/16)^{1/3}\\ (t,d^{m_1}2M)=r}} \frac{\mu(t)}{t^2}\left\{\frac{r}{d^{m_1}}\frac{1}{4M}(X/16)^{2/3}\right\} + O(X^{1/3}\log X)$$

$$= (X/16)^{2/3}\frac{1}{4M}\frac{1}{d^{m_1}}\sum_{r|d^{m_1}} r \sum_{\substack{t\leq X^{1/3}\\ (t,d^{m_1}2M)=r}} \frac{\mu(t)}{t^2} + O(X^{1/3}\log X).$$

Writing $t=rs$, we may suppose that $(r,s)=1$, else $\mu(t)=0$. Moreover $(rs,d^{m_1}2M)=r$, then $(s,d^{m_1}2M)=1$. Hence:

$$\sum_{\substack{0<b\leq(X/16)^{1/3}\\ b\equiv 0 \pmod{d^{m_1}}\\ b\equiv b_0 \pmod{2M}}} \phi(b) = (X/16)^{2/3}\frac{1}{4M}\frac{1}{d^{m_1}}\sum_{r|d^{m_1}}\frac{\mu(r)}{r} \sum_{\substack{s\leq X^{1/3}/r\\ (s,d^{m_1}2M)=1}} \frac{\mu(s)}{s^2} + O(X^{1/3}\log X)$$

$$= (X/16)^{2/3}\frac{1}{4M}\frac{1}{d^{m_1}}\sum_{r|d^{m_1}}\frac{\mu(r)}{r}$$

$$\left\{\frac{1}{\zeta(2)}\prod_{p|d^{m_1}2M}\left(1-\frac{1}{p^2}\right)^{-1}+O\left(\frac{r}{X^{1/3}}\right)\right\} + O(X^{1/3}\log X)$$

$$= \frac{(X/16)^{2/3}}{\zeta(2)}\frac{1}{4M}\frac{1}{d^{m_1}}\left(\sum_{r|d^{m_1}}\frac{\mu(r)}{r}\right)\left(\prod_{p|d^{m_1}2M}\left(1-\frac{1}{p^2}\right)^{-1}\right)$$

$$+ O(X^{1/3}\log X)$$

$$= \frac{(X/16)^{2/3}}{\zeta(2)}\frac{1}{4M}\frac{1}{d^{m_1}}\prod_{p|2M}\left(1-\frac{1}{p^2}\right)^{-1}\prod_{p|d}\left(1+\frac{1}{p}\right)^{-1} + O(X^{1/3}\log X).$$

Therefore, we get

$$|S_1| \geq \left(\sum_{\substack{e\ll X^{1/3m_2}\\ (e,2M)=1}}\frac{\mu(e)}{e^{m_2}}\right)\left(\sum_{\substack{f\ll X^{1/3m_3}\\ (f,2M)=1}}\frac{\mu(f)}{f^{m_3}}\right)\left(\sum_{\substack{d\ll X^{1/3m_1}\\ (d,2M)=1}}\frac{\mu(d)}{d^{m_1}}\prod_{p|d}\left(1+\frac{1}{p}\right)^{-1}\right)C_0.X^{2/3}$$

$$+ O(X^{1/3+1/3m_2+1/3m_3+\varepsilon}) + O\left(X^{1/3}\log X\sum_{d\ll X^{1/3m_1}} 1\right)$$

where $C_0 = \frac{4\sqrt{2}-4}{(16)^{2/3}}\frac{1}{(2M)^2}\frac{1}{2\zeta(2)}\prod_{p|2M}\left(1-\frac{1}{p^2}\right)^{-1}$.

The error term is

$$O(X^{1/3+1/3m_2+1/3m_3+\varepsilon}) + O(X^{1/2+\varepsilon}).$$

The main term is

$$\frac{1}{L(m_2,\chi_0)}\frac{1}{L(m_3,\chi_0)}C_0PX^{2/3} + O(X^{1/2+\varepsilon})$$

where χ_0 is the prinicpal character mod $2M$ and

$$\begin{aligned} P &= \sum_{\substack{d \ll X^{1/3m_1} \\ (d,2M)=1}} \frac{\mu(d)}{d^{m_1}} \prod_{p|d}\Big(1+\frac{1}{p}\Big)^{-1} \\ &= \sum_{\substack{d=1 \\ (d,2M)=1}}^{\infty} \frac{\mu(d)}{d^{m_1}} \prod_{p|d}\Big(1+\frac{1}{p}\Big)^{-1} + O(X^{(-m_1+1)/3m_1}) \\ &= \prod_{(p,2M)=1}\Big(1-\frac{1}{p^{m_1-1}(p+1)}\Big) + O(X^{-1/6}). \end{aligned}$$

Since the Euler product

$$\prod_{(p,2M)=1}\Big(1-\frac{1}{p^{s-m_1}}\frac{1}{p^{m_1-1}(p+1)}\Big)$$

converges absolutely for $\mathrm{Re}(s) \geq m_1$ and each Euler factor is nonzero at $s = m_1$, P is also nonzero.

This concludes the proof of Theorem 1. ∎

3. **Distribution of the set of E_m's with nonzero rank.** In this section, we will prove that the set of $\{m \text{ cubefree} : W_m = 1\}$ has density $\frac{1}{2}$ in the set of cubefree integers m.

LEMMA 3.1. *For any Dirichlet character τ of conductor q, we have*

$$\sum_{m \text{ cubefree} \leq X} (-1)^{\tau_2(m)}\tau(m) = O\big(\sqrt{X}(\log X)\sqrt{q}\log q\big)$$

where $\tau_2(m)$ is the number of distinct primes $p \equiv 2 \pmod 3$ such that $p|m$.

PROOF. Every cubefree integer can be written uniquely in the form r^2s, where r, s are squarefree integers and $(r,s) = 1$. We have

$$\begin{aligned} \tau_2(r^2s) &= \tau_2(r^2) + \tau_2(s) \\ &= \tau_2(r) + \tau_2(s). \end{aligned}$$

Then

$$\begin{aligned} \sum_{\substack{m \text{ cubefree} \leq X \\ 3 \nmid m}} (-1)^{\tau_2(m)}\tau(m) &= \sum_{\substack{r^2s \leq X \\ (r,3)=(s,3)=(r,s)=1}} (-1)^{\tau_2(r)}\tau(r^2)(-1)^{\tau_2(s)}\tau(s) \\ &= \sum_{r,s} \chi(r)\tau(r^2)\chi(s)\tau(s) \end{aligned}$$

where the sum only includes squarefree values of r, and s and $\chi(\cdot) = (\frac{\cdot}{3})$, the nonprincipal character module 3. (As $3 \nmid r$ and r is squarefree, $(-1)^{\tau_2(r)} = \chi(r)$). Then

$$\sum_{\substack{m \text{ cubefree} \leq X \\ 3 \nmid m}} (-1)^{\tau_2(m)}\tau(m) = \sum_{\substack{r \leq \sqrt{X} \\ r \text{ squarefree}}} \chi(r)\tau(r^2) \sum_{\substack{s \leq X/r^2 \\ s \text{ squarefree}}} \chi_r(s)\chi(s)\tau(s)$$

https://doi.org/10.4153/CJM-1993-048-9 Published online by Cambridge University Press

in which χ_r is the principal character modulo r, *i.e.* $\chi_r(s) = 1$ if $(r,s) = 1$ and 0 otherwise. Now

$$\begin{aligned}\sum_{\substack{m \text{ cubefree} \leq X \\ 3 \nmid m}} (-1)^{\tau_2(m)}\tau(m) &= \sum_{\substack{r \leq \sqrt{X} \\ r \text{ squarefree}}} \chi(r)\tau(r^2) \sum_{s \leq X/r^2} \chi_r(s)\chi(s)\tau(s)\Big(\sum_{t^2 | s} \mu(t)\Big) \\ &= \sum_{\substack{r \leq \sqrt{X} \\ r \text{ squarefree}}} \chi(r)\tau(r^2) \sum_{t \leq \sqrt{X}/r} \mu(t)\chi_r(t^2)\chi(t^2)\tau(t^2) \\ &\quad \times \sum_{s_0 \leq X/r^2t^2} \chi_r(s_0)\chi(s_0)\tau(s_0).\end{aligned}$$

The innermost sum is $O(\sqrt{q}\log q)$ by the Polya-Vinogradov inequality, then we have

$$\sum_{\substack{m \text{ cubefree} \leq X \\ 3 \nmid m}} (-1)^{\tau_2(m)}\tau(m) = \sum_{\substack{r \leq \sqrt{X} \\ r \text{ squarefree}}} O\Big(\frac{\sqrt{X}}{r}\sqrt{q}\log q\Big) = O\big(\sqrt{X}(\log X)\sqrt{q}\log q\big).$$

Finally we have:

$$\begin{aligned}\sum_{m \text{ cubefree} \leq X} (-1)^{\tau_2(m)}\tau(m) &= \sum_{\substack{m \text{ cubefree} \leq X \\ 3 \nmid m}} + \sum_{\substack{m \text{ cubefree} \leq X \\ 3 \| m}} + \sum_{\substack{m \text{ cubefree} \leq X \\ 3^2 \| m}} \\ &= \sum_{\substack{m \text{ cubefree} \leq X \\ 3 \nmid m}} + \sum_{\substack{m_1 \text{ cubefree} \leq X/3 \\ 3 \nmid m_1}} + \sum_{\substack{m_2 \text{ cubefree} \leq X/9 \\ 3 \nmid m_2}} \\ &= O(\sqrt{X}\log X\sqrt{q}\log q).\end{aligned}$$

Here, $p^k \| m$ means that $p^k | m$ but $p^s \nmid m$ for $s > k$. ∎

LEMMA 3.2. *The set $\{m$ cubefree, $\tau_2(m)$ is even$\}$ has density $\frac{1}{2}$ in the set $\{m$ cubefree$\}$.*

PROOF. We have

$$\begin{aligned}\sum_{\substack{m \text{ cubefree} \leq X \\ \tau_2(m) \text{ is even}}} 1 &= \sum_{m \text{ cubefree} \leq X} \frac{1}{2}\big(1 + (-1)^{\tau_2(m)}\big) \\ &= \frac{1}{2} \sum_{m \text{ cubefree} \leq X} 1 + O(\sqrt{X}\log X)\end{aligned}$$ ∎

We also use the following well-known fact:

LEMMA 3.3. *The set $\{m$ cubefree$\}$ has density $\frac{1}{\zeta(3)}$ in the set of positive integers.*

Now we want to prove

THEOREM 2. *The set $\{m$ cubefree, $W_m = 1\}$ has density $\frac{1}{2}$ in the set $\{m$ cubefree$\}$.*

PROOF. By (1) in §1, we have

$$\sum_{\substack{m \text{ cubefree} \leq X \\ W_m = 1}} 1 = \sum_{\substack{m \text{ cubefree} \leq X \\ \tau_2(m) \text{ is even} \\ m \equiv \pm 1, \pm 3 \pmod 9}} 1 + \sum_{\substack{m \text{ cubefree} \leq X \\ \tau_2(m) \text{ is odd} \\ m \equiv 0, \pm 2, \pm 4 \pmod 9}} 1.$$

For $m \equiv 0 \pmod 9$, we get

$$\sum_{\substack{m \text{ cubefree } \le X \\ \tau_2(m) \text{ is odd} \\ m\equiv 0 \pmod 9}} 1 = \sum_{\substack{m \text{ cubefree } \le X/9 \\ \tau_2(m) \text{ is odd} \\ 3 \nmid m}} 1 \quad \text{(by Lemma 3.1)}$$
$$= \frac{1}{2} \sum_{\substack{m \text{ cubefree } \le X/9 \\ 3 \nmid m}} 1 + O(\sqrt{X} \log X)$$
$$= \sum_{\substack{m \text{ cubefree } \le X \\ \tau_2(m) \text{ is even} \\ m\equiv 0 \pmod 9}} 1 + O(\sqrt{X} \log X).$$

For $m \equiv \pm 3 \pmod 9$, similarly we get

$$\sum_{\substack{m \text{ cubefree } \le X \\ \tau_2(m) \text{ is even} \\ m\equiv \pm 3 \pmod 9}} 1 = \frac{1}{2} \sum_{\substack{m \text{ cubefree } \le X \\ m\equiv \pm 3 \pmod 9}} 1 + O(\sqrt{X} \log X).$$

For $(\imath, 3) = 1$, we get

$$\sum_{\substack{m \text{ cubefree } \le X \\ \tau_2(m) \text{ is even} \\ m\equiv \imath \pmod 9}} 1 = \sum_{\substack{m \text{ cubefree } \le X \\ \tau_2(m) \text{ is even}}} \frac{1}{\phi(9)} \sum_{\chi \pmod 9} \chi(m)\bar{\chi}(\imath)$$
$$= \sum_{\chi \pmod 9} \bar{\chi}(\imath) \frac{1}{\phi(9)} \sum_{\substack{m \text{ cubefree } \le X \\ \tau_2(m) \text{ is even}}} \chi(m)$$
$$= \frac{1}{6} \sum_{\chi} \bar{\chi}(\imath) \sum_{m \text{ cubefree } \le X} \chi(m) \Big(\frac{1}{2} \big(1 + (-1)^{\tau_2(m)} \big) \Big)$$
$$= \frac{1}{12} \sum_{\chi} \bar{\chi}(\imath) \sum_{m \text{ cubefree } \le X} \chi(m) + O(\sqrt{X} \log X) \quad \text{(by Lemma 3.1)}$$
$$= \frac{1}{12} \sum_{m \text{ cubefree } \le X} \sum_{\chi} \bar{\chi}(\imath)\chi(m) + O(\sqrt{X} \log X)$$
$$= \frac{1}{2} \sum_{\substack{m \text{ cubefree } \le X \\ m\equiv \imath \pmod 9}} 1 + O(\sqrt{X} \log X).$$

Therefore, we get

$$\sum_{\substack{m \text{ cubefree } \le X \\ W_m = 1}} 1 = \frac{1}{2} \sum_{\substack{m \text{ cubefree } \le X \\ m\equiv \pm 1, \pm 3 \pmod 9}} 1 + \frac{1}{2} \sum_{\substack{m \text{ cubefree } \le X \\ m\equiv 0, \pm 2, \pm 4 \pmod 9}} 1 + O(\sqrt{X} \log X)$$
$$= \frac{1}{2} \sum_{m \text{ cubefree } \le X} 1 + O(\sqrt{X} \log X). \qquad \blacksquare$$

https://doi.org/10.4153/CJM-1993-048-9 Published online by Cambridge University Press

4. **Distribution of E_m's with nontrivial even analytic rank.** We restate the main theorem.

MAIN THEOREM. *For X large enough, we have:*

$$\{m \text{ cubefree} < X : \text{Analytic rank of } E_m \text{ is even and} \geq 2\} \gg X^{2/3-\varepsilon}.$$

PROOF. If we choose m of the form $m = b\big(a^2 - (4b)^2\big)$ then $\text{rank}(E_m) \geq 1$. Since E_m is a CM elliptic curve, the analytic rank of E_m is ≥ 1 by Coates and Wiles' theorem [3]. Moreover, if we choose m such that the root number $W_m = 1$, then the analytic rank of E_m is even and hence ≥ 2.

In Theorem 1, we choose

$$m_1 = m_2 = 2, \quad m_3 = 3$$

and

$$M = 9.$$

For a given congruence class (a_0, b_0) mod 18, W_m is determined completely by the parity of $\tau_2(m)$. For example, if we choose $(a_0, b_0) \equiv (3, 1) \pmod{18}$ then $m \equiv 2 \pmod 9$, *i.e.* $W_m = 1$ iff $\tau_2(m)$ is odd. Choose (a_0, b_0) so that $W_m = 1$ if and only if $\tau_2(m)$ is odd. Then

$$\#\{m \text{ cubefree} \leq X : \text{Analytic rank of } E_m \text{ is even and} \geq 2\} \geq |S_2|$$

where

$$S_2 = \Big\{m \leq X : m = b\big(a^2 - (4b)^2\big) \text{ for some } a, b \in \mathbb{N},\ (a,b) = 1,\ 0 < b \leq (X/16)^{1/3},\ 4b \leq a \leq 4\sqrt{2}b,\ b, a-4b \text{ are squarefree, and } a+4b \text{ is cubefree},\ a \equiv a_0 \pmod{18},\ b \equiv b_0 \pmod{18} \text{ and } \tau_2(m) \text{ is odd}\Big\}.$$

Letting $(*)$ be the conditions on (a, b) such that $m = b\big(a^2 - (4b)^2\big) \in S_2$, except for the last condition on $\tau_2(m)$, we see that the theorem follows if we can show

$$\sum_{\substack{(a,b) \text{ satisfies } (*) \\ \tau_2(m) \text{ is odd}}} 1 = CX^{2/3} + O(X^{13/21+\varepsilon}).$$

We have

$$\begin{aligned} \sum_{\substack{(a,b) \text{ satisfies } (*) \\ \tau_2(m) \text{ is odd}}} 1 &= \sum_{(a,b) \text{ satisfies } (*)} \frac{1}{2}\Big(1 - (-1)^{\tau_2(m)}\Big) \\ &= \frac{1}{2} \sum_{(a,b) \text{ satisfies } (*)} 1 - \frac{1}{2} \sum_{(a,b) \text{ satisfies } (*)} (-1)^{\tau_2(m)}. \end{aligned}$$

https://doi.org/10.4153/CJM-1993-048-9 Published online by Cambridge University Press

By Theorem 2 (and our choice of m_1, m_2, m_3), the first sum is $CX^{2/3} + O(X^{11/18+\varepsilon})$ where $C > 0$ and ε is arbitrarily small. Now, for $m \in S_2$, we have:

$$\begin{aligned}(-1)^{\tau_2(m)} &= (-1)^{\tau_2(b)}(-1)^{\tau_2(a-4b)}(-1)^{\tau_2(a+4b)}\\ &= \Big(\frac{b_0}{3}\Big)\Big(\frac{a_0-4b_0}{3}\Big)(-1)^{\tau_2(a+4b)}\end{aligned}$$

since b and $a-4b$ are squarefree. For example, if $(a_0, b_0) \equiv (3,1) \pmod{18}$ then $(\frac{b_0}{3})(\frac{a_0-4b_0}{3}) = -1$.

Therefore, the theorem follows from

LEMMA 4.1.

$$\sum_{\substack{(a,b)\text{ satisfies }(*)\\ \text{for some } m}} (-1)^{\tau_2(a+4b)} = O(X^{13/21+\varepsilon}).$$

PROOF. Denote the sum on the left hand side as S_2', we have

$$S_2' = \sum_{\substack{0<b\le (X/16)^{1/3}\\ b\equiv b_0 \pmod{2M}\\ b \text{ squarefree}}} \sum_{\substack{4b\le a\le 4\sqrt{2}b\\ a\equiv a_0 \pmod{2M}\\ a-4b \text{ squarefree}\\ a+4b \text{ cubefree}\\ (a,b)=1}} (-1)^{\tau_2(a+4b)}.$$

To simplify the notations, let $a' = a-4b$, $a_0' = a_0 - 4b_0$ and $C = 4\sqrt{2}-4$. Also note that the condition $(a,b)=1$ is equivalent to $(a',b)=1$ for our set. We have:

$$\begin{aligned}S_2' &= \sum_{\substack{0<b\le (X/16)^{1/3}\\ b\equiv b_0 \pmod{2M}}} \sum_{\substack{a'\le Cb\\ a'\equiv a_0' \pmod{2M}\\ (a',b)=1\\ a'+8b \text{ is cubefree}}} (-1)^{\tau_2(a'+8b)} \sum_{d^2|b} \mu(d) \sum_{e^2|a'} \mu(e)\\ &= \sum_{\substack{d\ll X^{1/6}\\ e\ll X^{1/6}\\ (d,2M)=(e,2M)=1}} \mu(d)\mu(e) \sum_{\substack{0<b\le (X/16)^{1/3}\\ b\equiv 0 \pmod{d^2}\\ b\equiv b_0 \pmod{2M}}} \sum_{\substack{a'\le Cb\\ a'\equiv a_0' \pmod{2M}\\ a'\equiv 0 \pmod{e^2}\\ a'+8b \text{ is cubefree}\\ (a',b)\equiv 1}} (-1)^{\tau_2(a'+8b)}.\end{aligned}$$

The contribution of terms with $Y < e \ll X^{1/6}$ where Y is a parameter to be chosen later, is

$$\begin{aligned}&\ll \sum_{\substack{d\ll X^{1/6}\\ Y<e\ll X^{1/6}\\ (d,2M)=(e,2M)=1}} |\mu(d)\mu(e)| \sum_{\substack{0<b\le (X/16)^{1/3}\\ b\equiv b_0 \pmod{2M}\\ b\equiv 0 \pmod{d^2}}} \Big(O\Big(\frac{b}{e^2}\Big)\Big)\\ &= \sum_{\substack{d\ll X^{1/6}\\ Y<e\ll X^{1/6}}} |\mu(d)\mu(e)|\, O\Big(\frac{X^{2/3}}{e^2d^2}\Big)\\ &= O\Big(\frac{X^{2/3}}{Y}\Big).\end{aligned}$$

https://doi.org/10.4153/CJM-1993-048-9 Published online by Cambridge University Press

Now, the contribution of terms with $0 < e \le Y$ is

$$\sum_{\substack{d \ll X^{1/6} \\ 0<e\le Y \\ (d,2M)=(e,2M)=1}} \mu(d)\mu(e) \sum_{\substack{0<b\le (X/16)^{1/3} \\ b\equiv 0 \pmod{d^2} \\ b\equiv b_0 \pmod{2M}}} \sum_{\substack{n|b \\ n\le Cb}} \mu(n) \sum_{\substack{a''\le Cb/n \\ na''\equiv a_0' \pmod{2M} \\ na''\equiv 0 \pmod{e^2} \\ na''+8b \text{ is cubefree}}} (-1)^{\tau_2(na''+8b)}.$$

Let us write $na'' + 8b = r^2 s$ where r, s are squarefree and $(r,s) = 1$. Also denote χ_r the principal character modulo r, we see that the above is

$$\sum_{\substack{d \ll X^{1/6} \\ 0<e\le Y \\ (d,2M)=(e,2M)=1}} \mu(d)\mu(e) \sum_{\substack{0<b\le (X/16)^{1/3} \\ b\equiv 0 \pmod{d^2} \\ b\equiv b_0 \pmod{2M}}} \sum_{\substack{n|b \\ n\le Cb}} \mu(n) \sum_{\substack{0\le r\le \sqrt{(C+8)b} \\ r \text{ squarefree}}} \left(\frac{r}{3}\right)$$
$$\times \sum_{\substack{8b/r^2\le s\le (C+8)b/r^2 \\ r^2 s\equiv a_0'+8b \pmod{2M} \\ r^2 s\equiv 8b \pmod{e^2} \\ r^2 s\equiv 8b \pmod{n} \\ s \text{ is squarefree}}} \left(\frac{s}{3}\right)\chi_r(s)$$
$$= \sum_{\substack{d \ll X^{1/6} \\ 0<e\le Y \\ (d,2M)=(e,2M)=1}} \mu(d)\mu(d) \sum_{\substack{0<b\le (X/16)^{1/3} \\ b\equiv 0 \pmod{d^2} \\ b\equiv b_0 \pmod{2M}}} \sum_{\substack{n|b \\ n\le Cb}} \mu(n) \sum_{\substack{0\le r\le \sqrt{(C+8)b} \\ r \text{ squarefree}}} \left(\frac{r}{3}\right)$$
$$\times \sum_{0\le s_1\le \sqrt{(C+8)b}/r} \chi_r(s_1)\mu(s_1) \sum_{\substack{8b/r^2 s_1^2\le s_2\le (C+8)b/r^2 s_1^2 \\ r^2 s_1^2 s_2\equiv a_0'+8b \pmod{2M} \\ r^2 s_1^2 s_2\equiv 8b \pmod{e^2} \\ r^2 s_1^2 s_2\equiv 8b \pmod{n}}} \left(\frac{s_2}{3}\right)\chi_r(s_2).$$

Consider the terms with $n \ge Z$, where Z is another parameter to be chosen later. The contribution of such terms is, on noting $n|b$,

$$\ll \sum_{d,e}\sum_{b}\sum_{Z\le n}\sum_{r}\sum_{s_1}\left(O\left(\frac{b}{r^2 s_1^2 e^2 n}\right) + O(1)\right)$$
$$= \sum_{d,e}\sum_{b}\sum_{Z\le n}\sum_{r}\left(O\left(\frac{b}{r^2 e^2 n}\right) + O\left(\frac{\sqrt{b}}{r}\right)\right)$$
$$= \sum_{d,e}\sum_{b}\sum_{Z\le n}\left(O\left(\frac{b}{e^2 n}\right) + O(b^{1/2}\log b)\right)$$
$$= \sum_{d,e}\sum_{b}\left(O\left(\frac{b^{1+\varepsilon}}{Ze^2}\right) + O(b^{1/2+\varepsilon})\right)$$
$$= \sum_{d,e}\left(O\left(\frac{X^{2/3+\varepsilon}}{Zd^2e^2}\right) + O\left(\frac{X^{1/2+\varepsilon}}{d^2}\right)\right)$$
$$= O\left(\frac{X^{2/3+\varepsilon}}{Z}\right) + O(X^{1/2+\varepsilon}Y).$$

Now we consider the terms with $n \leq Z$. Using the Polya-Vinogradov inequality and noting that s_2 is determined by congruences mod $e^2 n$, such terms contribute

$$\begin{aligned}
&\ll \sum_{d,e}\sum_{b}\sum_{n\leq Z}\sum_{r}\sum_{s_1} O(e^{1+\varepsilon}n^{1/2+\varepsilon}) \\
&= \sum_{d,e}\sum_{b}\sum_{n\leq Z}\sum_{r} O\Big(\frac{\sqrt{b}}{r}e^{1+\varepsilon}n^{1/2+\varepsilon}\Big) \\
&= \sum_{d,e}\sum_{b}\sum_{n\leq Z} O(b^{1/2+\varepsilon}e^{1+\varepsilon}n^{1/2+\varepsilon}) \\
&= \sum_{d,e}\sum_{b} O(b^{1/2+\varepsilon}e^{1+\varepsilon}Z^{1/2+\varepsilon}) \\
&= \sum_{d,e} O\Big(\frac{X^{1/2+\varepsilon}}{d^2}e^{1+\varepsilon}Z^{1/2+\varepsilon}\Big) \\
&= O(X^{1/2+\varepsilon}Y^{2+\varepsilon}Z^{1/2+\varepsilon}).
\end{aligned}$$

In summary, we get

$$S_2' = O\Big(\frac{X^{2/3}}{Y}\Big) + O\Big(\frac{X^{2/3+\varepsilon}}{Z}\Big) + O(X^{1/2+\varepsilon}Y^{2+\varepsilon}Z^{1/2+\varepsilon}).$$

Choosing $Y = X^{1/21}$ and $Z = X^{1/21}$, we have

$$S_2' = O(X^{13/21+\varepsilon}).$$

This concludes the proof of Lemma 4.1 and also the Main Theorem. ∎

REMARK. In the case that $m = 3pq$, where p, q are primes $\equiv 2 \pmod 3$, $W_m = 1$. Satgé [8] computed the Selmer groups S_λ and $S_{\lambda'}$ (λ is a 3-isogeny and λ' its dual—more concretely, λ is the projection:

$$\lambda\colon E_m(\mathbb{C}) \longrightarrow \frac{E_m(\mathbb{C})}{\langle(0, \pm 12\sqrt{-3}m)\rangle} \cong E_m'(\mathbb{C})).$$

Indeed, $S_\lambda \cong (\mathbb{Z}/3\mathbb{Z})^3$ and $S_\lambda' \cong (0)$.

By the exact sequences of descent:

$$0 \longrightarrow \frac{E_m'(\mathbb{Q})}{\lambda E_m(\mathbb{Q})} \longrightarrow S_\lambda \longrightarrow Ш[\lambda] \longrightarrow 0$$
$$0 \longrightarrow \frac{E_m(\mathbb{Q})}{\lambda' E_m'(\mathbb{Q})} \longrightarrow S_\lambda' \longrightarrow Ш'[\lambda'] \longrightarrow 0$$

and the fact that:

$$\mathrm{rank}\big(E_m(\mathbb{Q})\big) = \dim_{\mathbb{F}_3}\Big(\frac{E_m(\mathbb{Q})}{\lambda'\big(E_m'(\mathbb{Q})\big)}\Big) + \dim_{\mathbb{F}_3}\Big(\frac{E_m'(\mathbb{Q})}{\lambda'\big(E_m(\mathbb{Q})\big)}\Big) - 1$$

we see that if $m = 3pq = b\big(a^2-(4b)^2\big)$ then $1 \leq \mathrm{rank}(E_m) \leq 2$. Since $W_m = 1$, assuming the Birch and Swinnerton-Dyer conjecture, we get $\mathrm{rank}(E_m) = 2$ and also $Ш[\lambda] = 0$ by the above exact sequences. This happens when, say $b = 3$, $a - 4b = q$, $a + 4b = p$.

In other words, we have

https://doi.org/10.4153/CJM-1993-048-9 Published online by Cambridge University Press

COROLLARY. *Assuming the Birch and Swinnerton-Dyer conjecture, if p, q are two primes such that $p - q = 24$, then* $\operatorname{rank}(E_m) = 2$, *for $m = 3pq$ and* $Ш[\lambda] = 0$.

Note that the number of such pairs of primes (p, q) satisfying $3pq \leq X$ is conjectured to be

$$\gg \frac{X^{1/2}}{\log^2 X}.$$

ACKNOWLEDGEMENT. The author wishes to thank Profs. Ram Murty and Kumar Murty for their suggestions and discussions during this work. He also thanks the referees for various helpful comments.

REFERENCES

1. B J Birch and N M Stephens, *The parity of the rank of the Mordell-Weil group*, Topology **5**(1966), 295–299

2. J S Cassels, *The rational solutions of the Diophantine equation $Y^2 = X^3 - D$*, Acta Math **82**(1950), 243–273

3. J Coates and A Wiles, *On the conjecture of Birch and Swinnerton-Dyer*, Invent Math **39**(1977), 223–251

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

5. K Ireland and I M Rosen, *A classical introduction to modern number theory*, Springer-Verlag, New York, 1982

6. L Mai, *The average analytic rank of a family of elliptic curves*, J Number Theory, to appear

7. K Rubin, *The work of Kolyvagin on the arithmetics of elliptic curves*, Lecture Notes in Mathematics **1399**, New York, Springer-Verlag, 1989

8. P Satgé, *Groupes de Selmer and corps cubiques*, J Number Theory **23**(1986), 294–317

9. ———, *Quelques resultats sur les entiers qui sont sommes des cubes de deux rationels*, Soc Math France, Asterisque **147-148**(1987), 335–341

10. ———, *Un analogue du calcul de Heegner*, Invent Math **87**(1987), 425–439

11. E S Selmer, *The Diophantine equation $AX^3 + BY^3 + CZ^3 = 0$*, Acta Math **85**(1951), 203–362

12. J Silverman, *The arithmetics of elliptic curves*, Springer-Verlag, New York, 1986

13. Y Taniyama, *L-functions of number fields and zeta functions of abelian varieties*, J Math Soc Japan **9**(1957), 330–336

14. A Weil, *Uber die Bestimmung Dirichletscher Reihen durch Funktionalgleichungen*, Math Annalen **168** (1967), 149–156

15. D Zagier and G Kramarz, *Numerical investigations related to the L-series of certain elliptic curves*, J Ind Math Soc **52**(1987), 51–69

Centre de Recherches Mathematiques
Université de Montréal
CP 6128-A
Montreal, Quebec
H3C 3J7