ELEMENTS OF CLASS GROUPS AND SHAFAREVICH-TATE GROUPS OF ELLIPTIC CURVES

Antal Balog and Ken Ono

Abstract. The problem of estimating the number of imaginary quadratic fields whose ideal class group has an element of order $\ell \geq 2$ is classical in number theory. Analogous questions for quadratic twists of elliptic curves have been the focus of recent interest. Whereas works of Stewart and Top [St-T], and of Gouvêa and Mazur [G-M] address the nontriviality of Mordell-Weil groups, less is known about the nontriviality of Shafarevich-Tate groups. Here we obtain a new type of result for the nontriviality of class groups of imaginary quadratic fields using the "circle method", and then we combine it with works of Frey, Kolyvagin and the second author to obtain results on the nontriviality of Shafarevich-Tate groups of certain elliptic curves. For $E = X_0(11)$, these results imply that

$$\#\left\{-X < D < 0 \ : \ D \text{ fundamental and } \text{Ш}(E(D), \mathbb{Q})[5] \neq \{0\}\right\} \gg \frac{X^{3/5}}{\log^2 X}.$$

1. Introduction and Statement of Results.

Throughout, suppose that D is the fundamental discriminant of the quadratic field $\mathbb{Q}(\sqrt{D})$, and that $h(D)$ is the associated ideal class number. If p is an odd prime, then Cohen and Lenstra [C-L] have conjectured that the "probability" that $p \nmid h(D)$ for negative D is

$$\prod_{i=1}^{\infty}(1-p^{-i}) = 1 - \frac{1}{p} - \frac{1}{p^2} + \frac{1}{p^5} + \cdots .$$

Although there is extensive numerical evidence supporting this prediction, little is known. In terms of densities, Davenport and Heilbronn [D-H] proved that at least half of the negative discriminants D have the property that $3 \nmid h(D)$. Much less is known for primes $p \geq 5$. For

1991 *Mathematics Subject Classification.* Primary 11G05, 11G40.

Key words and phrases. Shafarevich-Tate groups, quadratic twists of elliptic curves, the circle method.

The first author is supported by the Hungarian Science Foundation grant T25617. The second author is supported by NSF grant DMS-9874947, an Alfred P. Sloan Foundation Research Fellowship, a David and Lucile Packard Research Fellowship, and an H. I. Romnes Fellowship.

such primes, if $\epsilon > 0$ and $X > 0$ is sufficiently large, then Kohnen and the second author have shown [Ko-O] that

$$\#\{-X < D < 0 \ : \ h(D) \not\equiv 0 \pmod{p}\} \geq \left(\frac{2(p-2)}{\sqrt{3}(p-1)} - \epsilon\right)\frac{\sqrt{X}}{\log X}. \tag{1.1}$$

It is natural to consider the complementary problem of estimating, for any given integer $\ell \geq 2$, the number of $-X < D < 0$ for which $\mathrm{CL}(D)[\ell]$ is nontrivial. Here $\mathrm{CL}(D)[\ell]$ denotes the ℓ-torsion subgroup of the ideal class group of $\mathbb{Q}(\sqrt{D})$ (note: in Theorem 1 and Lemma 6.2 we abuse notation and let $\mathrm{CL}(d)$ denote the ideal class group of $\mathbb{Q}(\sqrt{d})$ whether or not d is a fundamental discriminant). Recent works by Murty [M] and Soundararajan [So] address these problems. For example, using sieve methods Soundararajan proved [So] that if ℓ is a multiple of 4, then

$$\#\{-X < D < 0 \ : \ \mathrm{CL}(D)[\ell] \neq \{0\}\} \gg_\epsilon X^{\frac{1}{2}+\frac{2}{\ell}-\epsilon}. \tag{1.2}$$

We obtain further results estimating the number of $-X < D < 0$ with $\mathrm{CL}(D)[\ell] \neq \{0\}$. Suppose that $K/\mathbb{Q}$ is a finite Galois extension, with discriminant Δ_K, and suppose that c is a conjugacy class in $\mathrm{Gal}(K/\mathbb{Q})$. Wong [Wo] noticed the utility of establishing the existence of infinitely many $D < 0$ for which $\mathrm{CL}(D)[\ell] \neq \{0\}$, where each odd prime factor p of D is unramified in K and has $\mathrm{Frob}(p) \in c$. Although he claimed [Th. 2, Wo] that there are always indeed infinitely many such D, a gap has been found in his proof. Here we remedy the situation by obtaining a general quantitative result which approaches the quality of Murty's [M] and Soundararajan's estimates [So] (for example, as in (1.2)). Using the "circle method", we obtain the following result.

Theorem 1. *Let $\ell \geq 2$ be an integer, $K/\mathbb{Q}$ a finite Galois extension and c a conjugacy class in $\mathrm{Gal}(K/\mathbb{Q})$. Suppose that $M \equiv 1 \pmod{24}$ is a positive square-free integer for which $\left(\frac{2}{q}\right) = 1$ for any prime $q \mid (M, \ell\Delta_K)$. Let $S(K, c, M)$ be the set of positive odd square-free integers coprime to M whose prime factors p are all unramified in $K/\mathbb{Q}$ with $\mathrm{Frob}(p) \in c$. Then we have*

$$\#\{d < X \ : \ d \in S(K, c, M), \ \mu(d) = 1, \text{ and } \mathrm{CL}(-dM)[\ell] \neq \{0\}\} \gg \frac{X^{\frac{1}{2}+\frac{1}{2\ell}}}{\log^2 X}.$$

In Theorem 1, $\mu(n)$ denotes the usual Möbius function, and the implied constant depends on ℓ, M, K and c.

Remark 1. We stress that Theorem 1 is proved using the circle method, rather than the more customary approach involving sieve methods (for example, see [M, So, St-T, G-M]). We would be very interested in a sieve theoretic argument which proves or improves upon Theorem 1.

Theorem 1 has implications for the arithmetic of elliptic curves. We begin by fixing notation. Suppose that $E/\mathbb{Q}$ is an elliptic curve

$$E: \quad y^2 = x^3 + ax + b. \tag{1.3}$$

Let $\Delta(E)$ denote its discriminant, and let $N(E)$ denote its conductor. For integers d which are not perfect squares, let $E(d)$ denote the d-quadratic twist of E

$$E(d): \quad dy^2 = x^3 + ax + b. \tag{1.4}$$

Moreover, if E is an elliptic curve defined over a number field K, then let $\mathrm{rk}(E, K)$ denote the rank of the Mordell-Weil group $E(K)$. Similarly, let $Ш(E, K)$ denote the Shafarevich-Tate group of E/K, and if p is a prime, then let $\mathrm{rk}_p(Ш(E, K))$ denote its p-rank.

It is natural to investigate the indivisibility of orders of Shafarevich-Tate groups. By the works of Kohnen, James and the second author [Ko-O, J-O], if $E/\mathbb{Q}$ is an elliptic curve, then for all but finitely many primes ℓ we have

$$\#\{-X < D < 0 \ : \ \mathrm{rk}(E(D), \mathbb{Q}) = 0 \ \text{ and } \ Ш(E(D), \mathbb{Q})[\ell] = \{0\}\} \gg_{E,\ell} \frac{\sqrt{X}}{\log X}. \tag{1.5}$$

This is analogous to estimate (1.1) for class numbers. For the complementary question, works by Beaver, Bölling, Cassels, Kramer, and Rohrlich [B, Bö, Ca, Kr, R] produce families of elliptic curves whose Shafarevich-Tate groups contain elements of order ℓ for primes $\ell \leq 5$.

Wong suggested [Wo] a method which promised to produce infinitely many quadratic twists of $X_0(11)$ whose Shafarevich-Tate groups have elements of order 5. This observation was a combination of a theorem of Frey [F], a result of the second author [O1], and [Th. 2, Wo]. Recently, the second author generalized the results in [O1], and these new theorems make it possible to extend Wong's observations to a wider class of elliptic curves. Unaware of the gap in the proof of [Th. 2, Wo], the second author mistakenly used the result to claim [Th. 5, Cor. 6, O2]. Armed with Theorem 1, we are pleased to resolve this problem. We obtain the following stronger result for curves $E/\mathbb{Q}$ whose torsion subgroup is $\mathbb{Z}/3\mathbb{Z}, \mathbb{Z}/5\mathbb{Z}$ or $\mathbb{Z}/7\mathbb{Z}$.

Theorem 2. *Let $E/\mathbb{Q}$ be an elliptic curve whose torsion subgroup over $\mathbb{Q}$ is $\mathbb{Z}/\ell\mathbb{Z}$ with $\ell \in \{3, 5, 7\}$. If E is good at ℓ (see §4 for the definition of "good"), then*

$$\#\{-X < D < 0 \ : \ L(E(D), 1) \neq 0, \ \mathrm{rk}(E(D), \mathbb{Q}) = 0 \ \text{ and } \ \ell \mid \#Ш(E(D), \mathbb{Q})\} \gg_E \frac{X^{\frac{1}{2}+\frac{1}{2\ell}}}{\log^2 X}.$$

Remark 2. Although we do not have a proof, it is plausible that every $E/\mathbb{Q}$ that has good reduction at ℓ is good at ℓ. In particular, if E has good reduction at ℓ and there is a prime $5 \leq p \equiv -1 \pmod{\ell}$ for which $\mathrm{ord}_p(N(E)) = 1$ and $\ell \nmid \mathrm{ord}_p(\Delta(E))$, then E is good at ℓ. These conditions are very inclusive and include almost every elliptic curve (in the sense of arithmetic density). For example, they already apply to the first curve, ordered by conductor, containing a torsion point of order 7. This is the conductor 26 elliptic curve

$$E: \quad y^2 + xy + y = x^3 - x^2 - 3x + 3,$$

and so Theorem 2 implies that

$$\#\{-X < D < 0 \ : \ \mathrm{rk}(E(D), \mathbb{Q}) = 0 \quad \text{and} \quad Ш(E(D), \mathbb{Q})[7] \neq \{0\}\} \gg \frac{X^{4/7}}{\log^2 X}.$$

Nevertheless, it is simple to use Theorem 2 in general. For example, we will show that

$$\#\{-X < D < 0 \ : \ \mathrm{rk}(X_0(11)(D)) = 0 \ \text{ and } \ Ш(X_0(11)(D), \mathbb{Q})[5] \neq \{0\}\} \gg \frac{X^{3/5}}{\log^2 X}.$$

Remark 3. It is interesting to compare the estimate in Theorem 2 with current lower bounds for the number of quadratic twists of a fixed elliptic curve with rank ≥ 2. Stewart and Top [St-T], improving on earlier conditional work of Gouvêa and Mazur [G-M], have shown that the Parity Conjecture implies that

$$\#\{-X < D < 0 \ : \ \mathrm{rk}(E(D), \mathbb{Q}) \geq 2\} \gg X^{1/2},$$

and have obtained the unconditional result

$$\#\{-X < D < 0 \ : \ \mathrm{rk}(E(D), \mathbb{Q}) \geq 2\} \gg \frac{X^{1/7}}{\log^2 X}.$$

Using Theorem 2, we show, for certain elliptic curves $E/\mathbb{Q}$, that there are infinitely many number fields K for which both

$$\mathrm{rk}(E, K) \gg \log([K : \mathbb{Q}]), \tag{1.6}$$

$$\mathrm{rk}_\ell(Ш(E, K)) \gg \log([K : \mathbb{Q}]). \tag{1.7}$$

Theorem 3. *Suppose that $E/\mathbb{Q}$ is an elliptic curve whose torsion subgroup over $\mathbb{Q}$ is $\mathbb{Z}/\ell\mathbb{Z}$ with $\ell \in \{3, 5, 7\}$. If E is good at ℓ (see §4 for the definition of "good"), then for every pair of non-negative integers r_m and r_s there are $r_m + r_s$ square-free integers $d_1, d_2, \dots, d_{r_m+r_s}$ for which both*

$$\mathrm{rk}(E, \mathbb{Q}(\sqrt{d_1}, \sqrt{d_2}, \dots, \sqrt{d_{r_m+r_s}})) \geq 2r_m,$$
$$\mathrm{rk}_\ell(Ш(E, \mathbb{Q}(\sqrt{d_1}, \sqrt{d_2}, \dots, \sqrt{d_{r_m+r_s}}))[\ell]) \geq 2r_s.$$

In §2 we give preliminaries on elliptic curves and describe some applications of a theorem of Frey. In §3 we consider the nonvanishing of Hasse-Weil L-functions of elliptic curves at $s = 1$. In §4 we combine the results from §2 and §3 to prove Theorems 2 and 3 assuming the truth of Theorem 1. In §5 we prove a technical result in additive number theory via the circle method, and in §6 we use this result to prove Theorem 1.

Acknowledgements.

S. Donnelly, D. R. Heath-Brown, M. Papanikolas, D. Rohrlich and T. Wooley.

2. Implications of a theorem of Frey.

In this section we recall an important theorem of Frey, and indicate how it is used to obtain Theorem 2. We begin by fixing notation. Suppose that $E/\mathbb{Q}$ is an elliptic curve over $\mathbb{Q}$, and that $j(E)$ is its j-invariant. If p is prime and $S(E,\mathbb{Q})$ denotes its Selmer group, then we have

$$1 \to E(\mathbb{Q})/pE(\mathbb{Q}) \to S(E,\mathbb{Q})[p] \to Ш(E,\mathbb{Q})[p] \to 1. \tag{2.1}$$

The next theorem follows from work of Frey [Fr] on quadratic twists of elliptic curves with rational points of odd prime order ℓ (note: a theorem of Mazur implies that $\ell \in \{3,5,7\}$).

Theorem 2.1. *Suppose that $E/\mathbb{Q}$ is an elliptic curve with a $\mathbb{Q}$-rational torsion point of odd prime order ℓ, and suppose that $\ell \nmid N(E)$. Let $S(E,\ell)$ be the set of primes*

$$S(E,\ell) := \{p \mid N(E) \ : \ 2 < p \equiv -1 \pmod{\ell},\ \ell \nmid \mathrm{ord}_p(\Delta(E)),\ \text{and } \mathrm{ord}_p(j(E)) < 0\}.$$

We have

$$\mathrm{CL}(4d)[\ell] \neq \{0\} \implies S(E(d),\mathbb{Q})[\ell] \neq \{0\},$$

whenever $d \equiv 3 \pmod 4$ is a negative square-free integer coprime to $\ell N(E)$ satisfying:

1. *If $\mathrm{ord}_\ell(j(E)) < 0$, then $\left(\frac{d}{\ell}\right) = -1$.*
2. *If $p \mid N(E)$ is an odd prime with $p \notin S(E,\ell)$, then*

$$\left(\frac{d}{p}\right) = \begin{cases} -1 & \text{if } \mathrm{ord}_p(j(E)) \geq 0, \\ -1 & \text{if } \mathrm{ord}_p(j(E)) < 0 \text{ and } E/\mathbb{Q}_p \text{ is a Tate curve}, \\ 1 & \text{otherwise.} \end{cases}$$

This result provides explicit examples of quadratic twists of certain elliptic curves whose ℓ-Selmer groups are nontrivial. To prove Theorem 2, we set out to construct negative discriminants D satisfying the conditions of Theorem 2.1 for which $\mathrm{CL}(D)[\ell] \neq \{0\}$ and $\mathrm{rk}(E(D),\mathbb{Q}) = 0$. The following elementary observation plays a crucial role in the proof of Theorem 2; it essentially reduces the proof to the construction of a suitable set of primes.

Corollary 2.2. *Suppose that $E/\mathbb{Q}$ is an elliptic curve with a $\mathbb{Q}$-rational torsion point of odd prime order ℓ, and suppose that $\ell \nmid N(E)$. Let $M \equiv 1 \pmod 4$ be any positive square-free integer coprime to $\ell N(E)$ with the property that $-M$ satisfies conditions (1) and (2) for d in Theorem 2.1. Let S be any infinite set of odd primes satisfying the following conditions:*

1. *For all $q \in S$ we have $(q, \ell N(E)M) = 1$.*
2. *We have $q_a \equiv q_b \pmod 4$ for all $q_a, q_b \in S$.*
3. *If $p \mid \ell N(E)$ is an odd prime for which $p \notin S(E,\ell)$, then $\left(\frac{q_a}{p}\right)\left(\frac{q_b}{p}\right) = 1$ for all $q_a, q_b \in S$.*

If j is a positive integer and $q_1, q_2, \ldots, q_{2j} \in S$ are distinct primes, then apart from at most finitely many exceptions we have

$$\mathrm{rk}(E(-Mq_1q_2\cdots q_{2j}),\mathbb{Q}) = 0 \ \text{ and } \ \mathrm{CL}(-4Mq_1q_2\cdots q_{2j})[\ell] \neq \{0\}$$

$$\implies \quad Ш(E(-Mq_1q_2\cdots q_{2j}),\mathbb{Q})[\ell] \neq \{0\}.$$

Proof. By hypothesis, $-M$ satisfies the conditions for d in Theorem 2.1. Moreover, by the hypotheses on the set of primes in S, it follows that $-Mq_1q_2\cdots q_{2j}$ also satisfies the conditions for d in the statement of Theorem 2.1 since $2j$ is even. Consequently, Theorem 2.1 implies that

$$\mathrm{CL}(-4Mq_1q_2\cdots q_{2j})[\ell]\neq\{0\} \implies S(E(-Mq_1q_2\cdots q_{2j}),\mathbb{Q})[\ell]\neq\{0\}.$$

In view of (2.1), the claim now follows from the fact that every elliptic curve $E/\mathbb{Q}$ has at most finitely many quadratic twists possessing a $\mathbb{Q}$-rational torsion point of odd prime order ℓ (for example, see [Prop. 1, G-M]).

□

To prove Theorem 3, we require some standard facts regarding relations between the p-ranks of Shafarevich-Tate and Mordell-Weil groups of elliptic curves upon a quadratic extension. We require the following fact (for a proof see [Lemma 3.1, O-P]).

Lemma 2.3. *Let E be an elliptic curve defined over a number field K. Let p be an odd prime, and let d be a non-square in K. Let $r(E,K)$ denote either* $\mathrm{rk}(E,K)$, $\mathrm{rk}_p(S(E,K)[p])$, *or* $\mathrm{rk}_p(Ш(E,K)[p])$. *Then*

$$r\left(E,K\left(\sqrt{d}\right)\right)=r(E,K)+r(E(d),K).$$

We conclude this section with the criterion which is used to obtain Theorem 3.

Lemma 2.4. *Suppose that $E/\mathbb{Q}$ is an elliptic curve, and that $d_1,d_2,\dots,d_{r_s}$ are r_s distinct square-free numbers such that for all $1\le j\le r_s$ we have*

$$Ш(E(d_j),\mathbb{Q})[p]\neq\{0\} \quad\text{and}\quad L(E(d_j),1)\neq 0.$$

If r_m is non-negative, then there are r_m distinct square-free integers, say $D_1,D_2,\dots,D_{r_m}$, for which

$$\begin{aligned}&\mathrm{rk}(E,\mathbb{Q}(\sqrt{D_1},\sqrt{D_2},\dots,\sqrt{D_{r_m}},\sqrt{d_1},\dots,\sqrt{d_{r_s}}))\ge 2r_m,\\ &\mathrm{rk}_p(Ш(E,\mathbb{Q}(\sqrt{D_1},\sqrt{D_2},\dots,\sqrt{D_{r_m}},\sqrt{d_1},\dots,\sqrt{d_{r_s}})[p])\ge 2r_s.\end{aligned}$$

Proof. By the work of Stewart and Top [St-T] on ranks of twists of elliptic curves, it follows that for every positive integer r_m there are distinct square-free integers $D_1,D_2,\dots,D_{r_m}$ for which

$$\mathrm{rk}(E(D_i),\mathbb{Q})\ge 2.$$

Therefore, Lemma 2.3 implies that

$$\mathrm{rk}(E,\mathbb{Q}(\sqrt{D_1},\sqrt{D_2},\dots,\sqrt{D_{r_m}}))\ge\sum_{j=1}^{r_m}\mathrm{rk}(E(D_j),\mathbb{Q})\ge 2r_m. \tag{2.2}$$

Kolyvagin's theorem [Kol] on the Birch and Swinnerton-Dyer Conjecture (note: finiteness of $Ш(E,\mathbb{Q})$ and the existence of the Cassels-Tate pairing implies that $\mathrm{rk}_p(Ш(E,\mathbb{Q}))[p]$ is even) implies, for each d_i, that

$$\mathrm{rk}_p(Ш(E(d_i),\mathbb{Q})[p]) \geq 2.$$

Therefore, by Lemma 2.3 again we have

$$\mathrm{rk}_p(Ш(E,\mathbb{Q}(\sqrt{d_1},\sqrt{d_2},\ldots,\sqrt{d_{r_s}}))[p]) \geq \sum_{j=1}^{r_s} \mathrm{rk}_p(Ш(E(d_i),\mathbb{Q})) \geq 2r_s. \tag{2.3}$$

Consequently, (2.2), (2.3) and Lemma 2.3 imply that

$$\mathrm{rk}(E,\mathbb{Q}(\sqrt{D_1},\sqrt{D_2},\ldots,\sqrt{D_{r_m}},\sqrt{d_1},\sqrt{d_2},\ldots,\sqrt{d_{r_s}}) \geq 2r_m,$$
$$\mathrm{rk}_p(E,\mathbb{Q}(\sqrt{D_1},\sqrt{D_2},\ldots,\sqrt{D_{r_m}},\sqrt{d_1},\sqrt{d_2},\ldots,\sqrt{d_{r_s}}) \geq 2r_s.$$

This completes the proof.

□

3. Nonvanishing of central values of twisted Hasse-Weil L-functions.

Suppose that $F_E(z) = \sum_{n=1}^{\infty} a_E(n)q^n \in S_2(\Gamma_0(N(E)))$ ($q := e^{2\pi iz}$ throughout) is the weight 2 newform on $\Gamma_0(N(E))$ associated to $E/\mathbb{Q}$ by the modularity of elliptic curves over $\mathbb{Q}$. Moreover, let $L(E,s)$ denote its Hasse-Weil L-function which is defined by analytically continuing

$$L(E,s) = L(F_E,s) = \sum_{n=1}^{\infty} \frac{a_E(n)}{n^s}.$$

As usual, let $\chi_D = \left(\frac{D}{\bullet}\right)$ denote the usual Kronecker character for the quadratic field $\mathbb{Q}(\sqrt{D})$ (note: recall that D always denotes a fundamental discriminant in this paper). Let $F_E \otimes \chi_D$ denote the newform that is the D-quadratic twist of F_E, and let $L(F_E \otimes \chi_D, s)$ denote the associated L-function. In particular, if $(D, N(E)) = 1$, then

$$L(E(D),s) = L\left(F_E \otimes \chi_D, s\right) = \sum_{n=1}^{\infty} \frac{\chi_D(n)a_E(n)}{n^s}. \tag{3.1}$$

Moreover, if δ_E (resp. $\delta_{E(D)}$) denotes the sign of the functional equation of $L(E,s)$ (resp. $L(E(D),s)$), then we have the fundamental relation

$$\delta_{E(D)} = \delta_E \cdot \mathrm{sign}(D) \cdot \left(\frac{D}{N(E)}\right). \tag{3.2}$$

Such relations will be very important in the sequel.

Celebrated works of Kohnen [Ko] and Waldspurger [W] on the Shimura correspondence [Sh] provide formulas for many of the central critical values $L(E(D),1) = L(F_E \otimes \chi_D, 1)$ in terms of the Fourier coefficients of certain half-integral weight cusp forms. Here we briefly recall some of the main results (see [Th. 1, W], [§2, O-Sk]).

For every fundamental discriminant D, define D_0 by

$$D_0 := \begin{cases} |D| & \text{if } D \text{ is odd,} \\ |D|/4 & \text{if } D \text{ if even.} \end{cases} \tag{3.3}$$

There is a positive integer $\mathfrak{N}(E)$ with $N(E) \mid \mathfrak{N}(E)$, a Dirichlet character χ modulo $4\mathfrak{N}(E)$, a non-zero complex number Ω_{F_E}, a non-zero half-integral weight Hecke eigenform

$$g_E(z) = \sum_{n=1}^{\infty} b_E(n) q^n \in S_{\frac{3}{2}}(\Gamma_0(4\mathfrak{N}(E)), \chi), \tag{3.4}$$

and arithmetic progressions of D coprime to $4\mathfrak{N}(E)$ with the property that if $\delta_E D > 0$, then

$$b_E(D_0)^2 = \epsilon_D \cdot \frac{L(F_E \otimes \chi_D, 1) D_0^{\frac{1}{2}}}{\Omega_{F_E}}, \tag{3.5}$$

where ϵ_D is algebraic. Moreover, the coefficients $a_E(n), b_E(n)$ and the values of χ are in O_L, the ring of integers of some fixed number field L (for example, see [Ste]). In addition, if $p \nmid 4\mathfrak{N}(E)$ is prime, then

$$\lambda(p) = \chi(p) a_E(p), \tag{3.6}$$

where $\lambda(p)$ is the eigenvalue of $g_E(z)$ for the half-integer weight Hecke operator $T^{\chi}(p^2)$ on $S_{\frac{3}{2}}(\Gamma_0(4\mathfrak{N}(E)), \chi)$.

The next result, which follows from [Lemma 3.3, O2], is useful for producing many non-zero L-values.

Lemma 3.1. *Assume the notation above, and suppose that $E/\mathbb{Q}$ is an elliptic curve without a $\mathbb{Q}$-rational torsion point of order 2. Suppose that $a \in (\mathbb{Z}/24\mathbb{Z})^{\times}$, $q_1, q_2, \dots, q_s$ are distinct odd primes, and that $\epsilon_1, \epsilon_2, \dots, \epsilon_s \in \{\pm 1\}$. Furthermore, suppose there is a square-free integer $n_0 \equiv a \pmod{24}$ for which $\left(\frac{n_0}{q_i}\right) = \epsilon_i$, for each $1 \le i \le s$, with*

$$L(E(\delta_E n_0), 1) \neq 0 \quad \text{and} \quad (n_0, \mathfrak{N}(E)) = 1.$$

Then there is a positive odd square-free integer $m_2 \equiv a \pmod{24}$ for which $\left(\frac{m_2}{q_i}\right) = \epsilon_i$, for all $1 \le i \le s$, and a set of odd primes S_E with positive Frobenius density such that for every positive integer j we have

$$L(E(\delta_E m_2 p_1 p_2 \cdots p_{2j}), 1) \neq 0,$$

whenever $p_1, p_2, \dots, p_{2j} \in S_E$ are distinct primes not dividing m_2. Moreover, if $p_a, p_b \in S_E$, then $p_a \equiv p_b \pmod{24}$, and for all $1 \le i \le s$ we have $\left(\frac{p_a}{q_i}\right)\left(\frac{p_b}{q_i}\right) = 1$.

Proof. By taking a simple linear combination of twists, and twists of twists of $g_E(z)$, define the cusp form

$$g_E^*(z) = \sum_{n \in A} b_E(n) q^n, \tag{3.7}$$

where A consists of those positive integers n for which $n \equiv a \pmod{24}$, and where $\left(\frac{n}{q_i}\right) = \epsilon_i$ for each $1 \leq i \leq s$. By the existence of n_0, (3.5) implies that $g_E^*(z)$ is nonzero. Moreover, $g_E^*(z)$ is an eigenform, for all but finitely many Hecke operators $T^\chi(p^2)$, whose eigenvalues satisfy (3.6). Since $E/\mathbb{Q}$ has no $\mathbb{Q}$-rational torsion point of order 2, it follows, by the Chebotarev Density Theorem, that a positive proportion of the primes p have the property that $a_E(p)$ is odd. Therefore, [Lemma 3.3, O2] readily applies to $g_E^*(z)$.

Let v be a place of O_L above 2, and suppose that $m_2 \in A$ is an integer for which $\mathrm{ord}_v(b_E(m_2))$ is minimal. Since $g_E^*(z)$ is nonzero, it follows that $b_E(m_2) \neq 0$. Moreover, since $g_E^*(z)$ is an eigenform, it follows that m_2 can be taken to be square-free. The conclusion of [Lemma 3.3, O2] implies that there is a set of primes S_E with positive Frobenius density such that for each positive integer j we have

$$b_E(m_2 p_1 p_2 \cdots p_{2j}) \neq 0,$$

whenever $p_1, p_2, \ldots, p_{2j} \in S_E$ are distinct primes not dividing m_2. By (3.5), it follows that

$$L(E(\delta_E m_2 p_1 p_2 \cdots p_{2j}), 1) \neq 0.$$

Lastly, since $m_2 p_1 p_2 \cdots p_{2j} \in A$, it follows that if $p_a, p_b \in S_E$, then $p_a \equiv p_b \pmod{24}$, and $\left(\frac{p_a}{q_i}\right)\left(\frac{p_b}{q_i}\right) = 1$ for each $1 \leq i \leq s$. This completes the proof.

□

Remark 4. By the proof of [Lemma 3.3, O2], which is based on Galois representations, it is evident that the set S_E in Lemma 3.1 always contains, as a subset, a set of primes p which are unramified in some fixed finite Galois extension $K/\mathbb{Q}$ whose $\mathrm{Frob}(p)$ is in some fixed conjugacy class of $\mathrm{Gal}(K/\mathbb{Q})$. Moreover, if p is an odd prime which does not divide the level of $g_E^*(z)$, then p is unramified in $K/\mathbb{Q}$; this implies, by (3.5), that every prime dividing m_2 in Lemma 3.1 is unramified in K.

4. Deduction of Theorems 2 and 3 from Theorem 1.

Here we deduce Theorems 2 and 3 from Theorem 1. The results from §2 and §3 are required for these deductions. We begin with the definition of "good".

Definition 4.1. *An elliptic curve $E/\mathbb{Q}$ is "good at ℓ" if the following are all true:*

1. *We have that $\ell \nmid N(E)$.*
2. *There is a prime $p \geq 5$ for which $\mathrm{ord}_p(N(E)) = 1$.*
3. *There is a positive square-free integer $Q \equiv 1 \pmod{24}$ coprime to $\ell N(E)$ for which $-Q$ satisfies the conditions (1) and (2) for d in Theorem 2.1, and which has*

$$\delta_{E(-4Q)} = +1.$$

Deduction of Theorem 2 from Theorem 1. Let Q be a positive square-free integer which justifies that E is good at ℓ. By (3.2) applied to $E(-4)$, every positive square-free integer $d' \equiv Qx^2 \pmod{24\ell N(E)}$ has the property that

$$\delta_{E(-4d')} = +1, \tag{4.1}$$

where $(x, 6\ell N(E)) = 1$. Moreover, each such $-d'$ satisfies the conditions (1) and (2) for d in Theorem 2.1.

Now let $M_1 \equiv 1 \pmod 4$ be any prime not dividing $\ell N(E)Q$ for which $\left(\frac{2}{M_1}\right) = 1$ and $\delta_{E(M_1)} = -1$. That such an M_1 can be chosen follows, by the Law of Quadratic Reciprocity, from (3.2) and Definition 4.1 (2). Now apply Lemma 3.1 to $E(M_1)$, where $a \equiv M_1 \pmod{24}$, and where the q_i's and ϵ_i's are chosen to sieve out those exponents n in the Fourier expansion, coprime to M_1, for which $M_1 n \equiv Q \pmod{24\ell N(E)}$. The remaining coefficients are supported on those n for which $M_1 n \equiv Qx^2 \pmod{24\ell N(E)}$, where $(x, 6\ell N(E))) = 1$. By (4.1), if n is such a positive square-free integer, then $\delta_{E(-4M_1 n)} = +1$ and $-M_1 n$ satisfies conditions (1) and (2) for d in Theorem 2.1. By a famous result of Friedberg and Hoffstein [Th. B (i), F-H], there are infinitely many such square-free n for which

$$L(E(-M_1 n), 1) \neq 0. \tag{4.2}$$

Therefore, Lemma 3.1 applies to $E(M_1)$, since it is also a curve without a $\mathbb{Q}$-rational point of order 2. Lemma 3.1 and (4.2) allow us to conclude that there is a positive square-free integer $M_2 \equiv M_1 \pmod{24\ell N(E)}$, coprime to M_1, and a set of primes $S_{E(M_1)}$ with positive Frobenius density such that for every positive integer j we have

$$L(E(-M_1 M_2 p_1 p_2 \cdots p_{2j}), 1) \neq 0, \tag{4.3}$$

whenever $p_1, p_2, \ldots, p_{2j} \in S_{E(M_1)}$ are distinct odd primes not dividing $M_1 M_2$. By Remark 4, one can construct a finite Galois extension, say $K/\mathbb{Q}$, for which there is a conjugacy class $c \in \mathrm{Gal}(K/\mathbb{Q})$ with the property that every prime p unramified in K with $\mathrm{Frob}(p) \in c$ is in $S_{E(M_1)}$. Furthermore, Lemma 3.1 implies that this set satisfies the hypotheses on S in Corollary 2.2.

By Kolyvagin's theorem on the Birch and Swinnerton-Dyer Conjecture [Kol], (4.3) implies, for every positive integer j and every collection of distinct primes $p_1, p_2, \ldots, p_{2j} \in S_{E(M_1)}$ coprime to $M_1 M_2$, that

$$\mathrm{rk}(E(-M_1 M_2 p_1 p_2 \cdots p_{2j}), \mathbb{Q}) = 0 \quad \text{and} \quad \#Ш(E(-M_1 M_2 p_1 p_2 \cdots p_{2j}), \mathbb{Q}) < +\infty.$$

Therefore, Corollary 2.2 and Theorem 1 applies with $M = M_1 M_2 \equiv 1 \pmod{24}$. Theorem 2 now follows easily since $(M, \Delta_K) \mid M_1$, a fact which follows from Remark 4.

□

Example 1. Suppose that $E/\mathbb{Q}$ is an elliptic curve with torsion subgroup $\mathbb{Z}/\ell\mathbb{Z}$ where $\ell \in \{3, 5, 7\}$. If E has good reduction at ℓ and there is a prime $5 \leq p_0 \equiv -1 \pmod{\ell}$ for

which $\ell \nmid \mathrm{ord}_{p_0}(\Delta(E))$ and $\mathrm{ord}_{p_0}(N(E)) = 1$, then E is good at ℓ. This follows from the fact that Definition 4.1 (3) is satisfied using (3.2). To see this, observe that the negative square-free integers d in Theorem 2.1 are not required to satisfy a quadratic residue condition modulo p_0, and the fact that $\mathrm{ord}_{p_0}(N(E)) = 1$ implies that $\mathrm{ord}_{p_0}(j(E)) < 0$ (see [p. 359, S]). These conditions apply to the conductor 26 elliptic curve

$$E: \quad y^2 + xy + y = x^3 - x^2 - 3x + 3.$$

Its torsion subgroup over $\mathbb{Q}$ is $\mathbb{Z}/7\mathbb{Z}$ and $\Delta(E) = -2^7 \cdot 13$. By letting $p_0 = 13$, we find that E is good at 7. Consequently, Theorem 2 implies that

$$\#\{-X < D < 0 \ : \ \mathrm{rk}(E(D), \mathbb{Q}) = 0 \ \text{ and } \ Ш(E(D), \mathbb{Q})[7] \neq \{0\}\} \gg \frac{X^{4/7}}{\log^2 X}.$$

Example 2. Let E be the conductor 11 elliptic curve

$$E: \quad y^2 + y = x^3 - x^2 - 10x - 20.$$

This is the modular curve $X_0(11)$, and its torsion subgroup over $\mathbb{Q}$ is $\mathbb{Z}/5\mathbb{Z}$. Furthermore, we have that

$$j(E) = -\frac{2^{12} \cdot 31^3}{11^5}.$$

Definition 4.1 (1) and (2) are both clearly satisfied. Condition (1) in Theorem 2.1 is vacuous since $\mathrm{ord}_5(j(E)) = 0$. Since $S(E, 5)$ is empty, the only condition in Definition 4.1 (3) is confirmed by finding any positive square-free $Q \equiv 1 \pmod{24}$ coprime to 55 for which $\left(\frac{-Q}{11}\right) = -1$ and $\delta_{X_0(11)(-4Q)} = +1$. It turns out that $Q = 1$ enjoys these two properties, and so Theorem 2 implies that

$$\#\{-X < D < 0 \ : \ \mathrm{rk}(E(D), \mathbb{Q}) = 0 \ \text{ and } \ Ш(E(D), \mathbb{Q})[5] \neq \{0\}\} \gg \frac{X^{3/5}}{\log^2 X}.$$

Deduction of Theorem 3 from Theorem 1. Theorem 1 implies Theorem 2. Theorem 2 and Lemma 2.4 implies Theorem 3.

□

5. Proof of a technical result in additive number theory.

If $\mathcal{P}$ is an infinite set of primes and q and b are coprime integers, then let $\mathcal{P}(x, q, b)$ be the number of primes $p \in \mathcal{P}$ with $p \leq x$ and $p \equiv b \pmod{q}$. We say that $\mathcal{P}$ satisfies a "Siegel-Walfisz condition for an integer Δ" if for every fixed integer $C > 0$ we have

$$\mathcal{P}(x, q, b) = \frac{\gamma}{\phi(q)}\pi(x) + O\left(\frac{x}{\log^C x}\right), \tag{5.1}$$

uniformly for all $(q, \Delta) = 1$ and all $(q, b) = 1$. Here $\pi(x) \sim \frac{x}{\log x}$ is the usual prime counting function, and $0 < \gamma \leq 1$ is the density of the primes in $\mathcal{P}$. The proof of the following result in additive number theory is the main objective of this section.

Theorem 5.1. *Suppose that A, B, Δ, ℓ and c_0 are positive integers for which*

$$(A, B) = (c_0, \Delta) = 1, \quad A + B \equiv 2 \pmod{\Delta}, \qquad \text{and} \quad 4\ell^2 \mid \Delta.$$

Let $\mathcal{P}$ be an infinite set of primes satisfying a Siegel-Walfisz condition for Δ that is a subset of those primes p for which $p \equiv c_0 \pmod{\Delta}$. If $R(X)$ denotes the number of positive integers $d \le X$ of the form

$$d = ABp_1 \dots p_{2\ell} = m^{2\ell} - n^2,$$

where the $p_j \in \mathcal{P}$ are distinct, then

$$R(X) \gg \frac{X^{\frac{1}{2}+\frac{1}{2\ell}}}{\log^2 X}.$$

Remark 5. The implied constant in Theorem 5.1 depends on $\mathcal{P}$, ℓ, A, B, Δ and c_0. If we denote the number of those representations with $(m, 2n) = 1$, $p_j \nmid AB$, and $p_1 \dots p_{2\ell} \ge m^\ell$ by $R_0(X)$, then we actually prove that the lower bound holds for $R_0(X)$.

We stress that the formulation of Theorem 5.1 is dictated by the application we have in mind (i.e. the proof of Theorem 1). Nevertheless, this theorem is closely connected to work of Perelli [P] and work of Brüdern, Kawada and Wooley [B-K-W] on the solvability of $F(m) = p + q$, where $F(m)$ is an integer valued polynomial and p, q are primes. However, Theorem 5.1 pertains to sets of primes which are also subsets of a single arithmetic progression modulo Δ. For the sake of a general result which imposes no conditions on c_0, we guarantee the local solvability modulo Δ (i.e. the obvious ℓ-th power residue condition) by requiring that there be 2ℓ many primes rather than just two primes (note: two primes is already sufficient for the proof of Theorem 1).

To prove Theorem 5.1 we shall obtain a lower bound for $R_1(x)$, the number of solutions of the following ternary additive problem

$$2m^\ell = Ap_1 \dots p_\ell + Bp_{\ell+1} \dots p_{2\ell}, \tag{5.2}$$

where the primes $p_j \in \mathcal{P}$ (and similarly $p_{\ell+j} \in \mathcal{P}$), for $1 \le j \le \ell$, satisfy the conditions

$$x^{1/2\ell} < p_j \le x^{1/\ell} \text{ for } j = 1, \dots, \ell - 1, \quad \text{and} \quad x^{1-\frac{1}{2\ell}} < p_1 \dots p_\ell \le x. \tag{5.3}$$

Notice, that writing $n = m^\ell - \min(Ap_1 \dots p_\ell, Bp_{\ell+1} \dots p_{2\ell}) > 0$ we have that

$$m^{2\ell} - n^2 = (m^\ell - n)(m^\ell + n) = ABp_1 \dots p_{2\ell}.$$

If $d = ABp_1 \dots p_{2\ell}$ is represented in this way, then the number of representations is at most $\binom{2\ell}{\ell}$. Next, if not all primes p_j are distinct in (5.2), then either $2m^\ell = ap + bp$ or $2m^\ell = a + bp^2$ with some prime $p > x^{1/2\ell}$ and integers a and b. Obviously we have $m \ll x^{1/\ell}$. In the first

case $p|m$ and $b \ll x/p$. In the second case we have $b \ll x/p^2$, and the fact that p, m, and b determine a. Therefore, the contribution of these solutions to $R_1(x)$ is bounded by

$$\ll \sum_p \sum_m \sum_b 1 \ll \sum_p \frac{x^{1+1/\ell}}{p^2} \ll x^{1+1/2\ell}.$$

In the remaining representations $p_j \nmid AB$, $p_1 \dots p_{2\ell} > x^{2-2/\ell} \geq m^\ell$ if x is sufficiently large, and $(m, n) \mid (Ap_1 \dots p_\ell, Bp_{\ell+1} \dots p_{2\ell}) = 1$. Finally, we observe that $2m^\ell \equiv 2c_0^\ell \pmod{\Delta}$ implies $(m, 2) = 1$, and so we have

$$R(X) \geq R_0(X) \gg R_1(x) + O\left(x^{1+\frac{1}{2\ell}}\right), \tag{5.4}$$

where $X = ABx^2$. For the remainder of this section, X is assumed to be a fixed sufficiently large real number.

As usual, let $e(\alpha) = e^{2\pi i\alpha}$, and let $P = AB\Delta$. We introduce the generating functions

$$f(\alpha) = \sum_{p_1,\dots,p_\ell} e(p_1 \dots p_\ell\, \alpha) = \sum_{n \leq x} c_n e(n\alpha), \tag{5.5}$$

$$g(\alpha) = \sum_m \ell m^{\ell-1} e(m^\ell \alpha) = \sum_{m \leq M} w_m e(m^\ell \alpha), \tag{5.6}$$

where the p_j satisfy (5.3), and m satisfies

$$m \leq M = \left(\frac{(A+B)x}{2}\right)^{1/\ell}, \quad (m, P) = 1. \tag{5.7}$$

It is trivial that $0 \leq c_n \leq \ell! \ll 1$, and a straightforward calculation using (5.1) (with $q = 1$) shows that

$$f(0) = \sum_{n \leq x} c_n = \sum_{p_1,\dots,p_\ell} 1 \asymp \frac{x}{\log x}. \tag{5.8}$$

The coefficients w_m in the definition of $g(\alpha)$ serve to simplify the analysis. However, we note that in our computation each solution of (5.2) is then weighted by $0 < w_m = \ell m^{\ell-1} \leq \ell M^{\ell-1} \ll x^{1-\frac{1}{\ell}}$. By the orthogonality of the trigonometric functions, we have

$$x^{1-\frac{1}{\ell}} R_1(x) \gg R_2(x) := \int_0^1 f(A\alpha) f(B\alpha) g(-2\alpha)\, d\alpha. \tag{5.9}$$

This section is devoted to the proof of the following estimate.

$$R_2(x) = 2\ell(2, \ell) \prod_{p|\Delta} (\ell, p-1) f^2(0) + O\left(\frac{x^2}{\log^3 x}\right), \tag{5.10}$$

which together with (5.4), (5.8) and (5.9) implies Theorem 5.1.

We begin by examining the function $g(\alpha)$. Without the condition that $(m, P) = 1$ and the presence of the weight $w_m = \ell m^{\ell-1}$, the results we would require are described in detail in [V]. Nevertheless, it is not too difficult to modify them for our purposes. First we introduce some more notation. The symbol $\sum_{u\,(q)}$ will denote a sum over the complete residue system modulo q, while $\sum_{(u,q)=1}$ denotes a sum over those classes modulo q that are coprime to q. For integers $q \geq 1$ and a, we require the Gaussian sum

$$G(q, a) = \sum_{\substack{u\,(q)\\(u,q,P)=1}} e\left(\frac{au^\ell}{q}\right),$$

and the auxiliary function

$$V(\eta) = \sum_{n \leq \frac{(A+B)x}{2}} e(n\eta).$$

Lemma 5.2. *If a and $q \geq 1$ are integers, and η is a real number, then*

$$g\left(\frac{a}{q} + \eta\right) = \frac{(q, P)\phi(P)}{q\phi(q, P)P} \cdot G(q, a)V(\eta) + O\left(qM^{\ell-1}(1 + |\eta|M^\ell)\right).$$

Here and in the sequel $\phi(q, P) = \phi((q, P))$, the Euler function evaluated at the greatest common divisor of q and P.

Proof. The corresponding result is [Lemma 2.7, V]. By gathering the terms in residue classes modulo q we get

$$g\left(\frac{a}{q} + \eta\right) = \sum_{\substack{u\,(q)\\(u,q,P)=1}} e\left(\frac{au^\ell}{q}\right) \sum_{\substack{m \leq M\\(m,P)=1\\m \equiv u\,(q)}} \ell m^{\ell-1} e(m^\ell \eta),$$

and the result follows, by partial summation, from the estimate

$$\sum_{\substack{m \leq y\\(m,P)=1\\m \equiv u\,(q)}} 1 = \sum_{d|P} \mu(d) \sum_{\substack{md \leq y\\md \equiv u\,(q)}} 1 = \sum_{\substack{d|P\\(d,q)=1}} \mu(d)\left(\frac{y}{qd} + O(1)\right).$$

□

Lemma 5.3. *If $M^{1/2} < q \le N := M^{\ell-1/2}$, $(a,q)=1$ and $|\alpha - \frac{a}{q}| \le \frac{1}{qN}$, then we have*

$$g(2\alpha) \ll M^{\ell - 2^{-(\ell+1)}}.$$

Proof. This is essentially Weyl's inequality. Our statement actually follows from [Lemma 2.4, V] which states that if $(a,q)=1$ and $|\alpha - \frac{a}{q}| < q^{-2}$ then for any $\epsilon > 0$ one has

$$\sum_{m \le y} e(\alpha m^\ell) \ll y^{1+\epsilon} \left(\frac{1}{q} + \frac{1}{y} + \frac{q}{y^\ell} \right)^{2^{1-\ell}}. \tag{5.11}$$

Let $y \le M$ and write

$$\sum_{\substack{m \le y \\ (m,P)=1}} e(2\alpha m^\ell) = \sum_{d|P} \mu(d) \sum_{m \le y/d} e(2\alpha d^\ell m^\ell).$$

By Dirichlet's Approximation Theorem, for any fixed d there are coprime integers a' and q' for which $1 \le q' \le 2N$ and $|2\alpha d^\ell - \frac{a'}{q'}| \le \frac{1}{q'2N} \le (q')^{-2}$. We use (5.11) with this approximation where $\epsilon = 2^{-(\ell+1)}$. If $\frac{2ad^\ell}{q} = \frac{a'}{q'}$, then $\frac{1}{2} M^{1/2} d^{-\ell} < q' \le 2N$, otherwise

$$\frac{1}{qq'} \le \left| \frac{2ad^\ell}{q} - \frac{a'}{q'} \right| \le \left| 2\alpha d^\ell - \frac{2ad^\ell}{q} \right| + \left| 2\alpha d^\ell - \frac{a'}{q'} \right| \le \frac{2d^\ell}{qN} + \frac{1}{q'2N}$$

implies that $\frac{N}{4d^\ell} \le q' \le 2N$. In either case, we have

$$\sum_{m \le y/d} e(2\alpha d^\ell m^\ell) \ll M^{1 - 2^{-(\ell+1)}}.$$

Since we have $\sum_{d|P} 1 \ll 1$, and since the weights w_m are monotonic, the result follows.

□

Lemma 5.4. *If $(q_1, q_2) = 1$, then $G(q_1, a_1) G(q_2, a_2) = G(q_1 q_2, a_1 q_2 + a_2 q_1)$.*

Proof. This is basically [Lemma 2.10, V], and follows easily from the Chinese Remainder Theorem.

□

Lemma 5.5. *If p is prime and a is an integer coprime to p, then $|G(p,a)| \le (\ell, p-1) p^{1/2}$.*

Proof. This follows easily from [Lemma 4.3, V].

□

Lemma 5.6. *Suppose $p|P$ is prime, and let $s = \mathrm{ord}_p(2\ell)$. If $p \nmid a$ and $k \geq \max(2, 2s+1)$, then $G(p^k, a) = G(p^k, 2a) = 0$.*

Proof. We prove the case of $G(p^k, 2a) = 0$; the other proof is identical. It is easy to see that the following is true

$$\sum_{\substack{u \,(p^k)\\ p\nmid u}} e\left(\frac{2au^\ell}{p^k}\right) = \sum_{\substack{u\,(p^{k-s-1})\\ p\nmid u}} \sum_{v\,(p^{s+1})} e\left(\frac{2a(u+vp^{k-s-1})^\ell}{p^k}\right) =$$

$$= \sum_{\substack{u\,(p^{k-s-1})\\ p\nmid u}} e\left(\frac{2au^\ell}{p^k}\right) \sum_{v\,(p^{s+1})} e\left(\frac{2\ell a u^{\ell-1}v}{p^{s+1}}\right) = 0.$$

The last equality follows from the summation over v. In the next to last step we used the Binomial Theorem and the hypotheses on k.

□

Lemma 5.7. *If $(q, a) = 1$, then*

$$G(q, 2a) \ll q^{1-\frac{1}{\ell}}.$$

Proof. This is essentially [Th. 4.2, V], and follows immediately from Lemma 5.4, Lemma 5.5, and Lemma 5.6.

□

Finally, we will need the large sieve (although with extra work we can avoid using it) [Lemma 5.3, V].

Lemma 5.8. (The Large Sieve) *For any complex coefficients c_n we have*

$$\sum_{q\leq Q} \sum_{(a,q)=1} \left| \sum_{n\leq x} c_n e\left(\frac{an}{q}\right)\right|^2 \leq (x+Q^2) \sum_{n\leq x} |c_n|^2.$$

The next statement is the main formula from which Theorem 5.1 will follow. It is proved using the circle method.

Theorem 5.9. *For any $1 \leq Q \leq M^{\min\left(\frac{1}{6}, \frac{\ell}{2(\ell+1)}\right)}$ we have*

$$R_2(x) = \sum_{q\leq Q} \sum_{(a,q)=1} \frac{(q,P)\phi(P)}{q\phi(q,P)P} \cdot G(q,-2a) f\left(\frac{aA}{q}\right) f\left(\frac{aB}{q}\right) + O\left(\frac{x^2}{Q^{1/\ell}}\right).$$

Remark 6. Theorem 5.9 is a result which is far more general than as stated here. In fact, one can derive a useful formula for the number of solutions to

$$2m^\ell = AU + BV,$$

with virtually any conditions on U and V. Our statement remains valid for arbitrary complex coefficients c_n, not just those defined in (5.5). In general the x^2 in the error term should be replaced by $x\sum_{n\le x}|c_n|^2$.

Remark 7. If in the definition of $g(\alpha)$ and of $G(q,a)$ we replace P by $P\prod_{p<Q}p$, then the upper bound in Lemma 5.7 improves to $q^{1/2+\epsilon}$ for $q\le Q$, and the exponent of Q in the error term of Theorem 5.9 improves from $1/\ell$ to $1/2-\epsilon$. This change makes it possible to make use of a Siegel-Walfisz type condition with $C=2+\epsilon$. However, such an approach makes the proofs of Lemma 5.2 and Lemma 5.3 considerably more difficult since $\sum_{d|P}1\ll 1$ is no longer true.

Proof of Theorem 5.9. We are going to use the parameters introduced earlier; for convenience we repeat their definitions

$$M=\left(\frac{(A+B)x}{2}\right)^{1/\ell},\quad N=M^{\ell-1/2}\asymp\frac{x}{M^{1/2}},\quad Q\le M^{\min\left(\frac{1}{6},\frac{\ell}{2^{(\ell+1)}}\right)}. \tag{5.12}$$

By Dirichlet's Approximation Theorem, for every real number $\frac{1}{N}\le\alpha<1+\frac{1}{N}$ there is a rational approximation

$$\left|\alpha-\frac{a}{q}\right|<\frac{1}{qN}\quad\text{ with }1\le a\le q\le N\ \text{ and }\ (a,q)=1.$$

This interval, a piece of the "major arcs", is denoted by $\mathfrak{M}(a/q)$, that is

$$\mathfrak{M}(a/q)=\left\{\frac{a}{q}-\frac{1}{qN}<\alpha<\frac{a}{q}+\frac{1}{qN}\right\},$$

and they are disjoint for $q\le M^{1/2}$. The rest, the "minor arcs", is denoted by $\mathfrak{m}$, that is

$$\mathfrak{m}=\left\{\frac{1}{N}\le\alpha<1+\frac{1}{N}\right\}\setminus\bigcup_{q\le M^{1/2}}\bigcup_{(a,q)=1}\mathfrak{M}(a/q).$$

Note that the functions, $f(\alpha)$ and $g(\alpha)$ have period 1; thus we can freely choose any interval of length 1, rather than the unit interval in (5.9). We use this fact later again. Our starting point is the decomposition

$$\begin{aligned}R_2(x)&=\int_{\frac{1}{N}}^{1+\frac{1}{N}}f(A\alpha)f(B\alpha)g(-2\alpha)\,d\alpha=\\&=\sum_{q\le M^{1/2}}\sum_{(a,q)=1}\int_{\mathfrak{M}(a/q)}f(A\alpha)f(B\alpha)g(-2\alpha)\,d\alpha+\int_{\mathfrak{m}}f(A\alpha)f(B\alpha)g(-2\alpha)\,d\alpha.\end{aligned} \tag{5.13}$$

The integral over $\mathfrak{m}$ is small because $g(-2\alpha)$ itself is small on the minor arcs by Lemma 5.3. Indeed, by the Cauchy–Schwarz Inequality, Parseval's Identity, and (5.8), we have

$$\int_{\mathfrak{m}}f(A\alpha)f(B\alpha)g(-2\alpha)\,d\alpha\ll M^{\ell-2^{-(\ell+1)}}\int_0^1|f(A\alpha)f(B\alpha)|\,d\alpha\ll M^{\ell-2^{-(\ell+1)}}x. \tag{5.14}$$

On a major arc $\mathfrak{M}(a/q)$ we use the more precise bound of Lemma 5.2. Note that for $q \le M^{1/2}$ and $\frac{a}{q}+\eta \in \mathfrak{M}(a/q)$ (i.e. $|\eta| < \frac{1}{qN}$) the error term in Lemma 5.2 is bounded by $qM^{\ell-1}(1+|\eta|x) \ll M^{\ell-\frac12}$. We have, by the Cauchy–Schwarz Inequality and Parseval's Identity again, that

$$\sum_{q\le M^{1/2}}\sum_{(a,q)=1}\int_{\mathfrak{M}(a/q)}\left|f\left(A(\frac{a}{q}+\eta)\right)f\left(B(\frac{a}{q}+\eta)\right)\right|M^{\ell-1}q(1+|\eta|x)\,d\eta \ll \tag{5.15}$$

$$\ll M^{\ell-\frac12}\int_0^1 |f(A\alpha)f(B\alpha)|\,d\alpha \ll M^{\ell-\frac12}x.$$

Obviously both (5.14) and (5.15) are smaller than the stated error term by (5.12). Applying Lemma 5.2 to $g(-2\alpha)$ in (5.13), we find that

$$R_2(x) =$$

$$= \sum_{q\le M^{1/2}}\sum_{(a,q)=1}\frac{(q,P)\phi(P)}{q\phi(q,P)P}\cdot G(q,-2a)\int_{-\frac{1}{qN}}^{\frac{1}{qN}} f\left(A(\frac{a}{q}+\eta)\right)f\left(B(\frac{a}{q}+\eta)\right)V(-2\eta)\,d\eta +$$

$$+ O(M^{\ell-2^{-(\ell+1)}}x).$$

Next we estimate the contribution of $Q < q \le M^{1/2}$ by using Lemma 5.7 and the Large Sieve (Lemma 5.8). We can be rather crude. Note also that $V(-2\eta) \ll \min(x, |\eta|^{-1})$. By the Cauchy–Schwarz Inequality, we obtain

$$\sum_{Q<q\le M^{1/2}}\sum_{(a,q)=1}\frac{(q,P)\phi(P)}{q\phi(q,P)P}G(q,-2a)\int_{-\frac{1}{qN}}^{\frac{1}{qN}} f\left(A(\frac{a}{q}+\eta)\right)f\left(B(\frac{a}{q}+\eta)\right)V(-2\eta)\,d\eta \ll$$

$$\ll Q^{-1/\ell}\int_{-1/2}^{1/2}\min(x,|\eta|^{-1})\sum_{Q<q\le M^{1/2}}\sum_{(a,q)=1}\left|f\left(A(\frac{a}{q}+\eta)\right)f\left(B(\frac{a}{q}+\eta)\right)\right|d\eta \ll$$

$$\ll Q^{-1/\ell}\int_{-1/2}^{1/2}\min(x,|\eta|^{-1})(x+M)\sum_{n\le x}|c_n e(n\eta)|^2 \ll x^2Q^{-1/\ell}.$$

For the remaining range of q, we extend each integral to the interval $\{-\frac12 < \eta < \frac12\}$. Trivially, $V(-2\eta) \ll |\eta|^{-1} \le qN$ on the extension. By Parseval's Identity for the last time, the error introduced by this extension is bounded by

$$2\sum_{q\le Q}\sum_{(a,q)=1}\frac{(q,P)\phi(P)}{q\phi(q,P)P}|G(q,-2a)|\int_{\frac{1}{qN}}^{\frac12}\left|f\left(A(\frac{a}{q}+\eta)\right)f\left(B(\frac{a}{q}+\eta)\right)V(-2\eta)\right|d\eta \ll$$

$$\ll N\sum_{q\le Q}\sum_{(a,q)=1}q^{1-1/\ell}\int_0^1\left|f\left(A(\frac{a}{q}+\eta)\right)f\left(B(\frac{a}{q}+\eta)\right)\right|d\eta \ll M^{\ell-\frac12}xQ^{3-1/\ell}.$$

Collecting all these bounds we arrive at

$$R_2(x) = \\ = \sum_{q\le Q}\sum_{(a,q)=1}\frac{(q,P)\phi(P)}{q\phi(q,P)P}G(q,-2a)\int_0^1 f\left(A(\frac{a}{q}+\eta)\right)f\left(B(\frac{a}{q}+\eta)\right)V(-2\eta)\,d\eta + \\ + O\left(\frac{x^2}{Q^{1/\ell}}\right).$$

Notice that the integral counts

$$e\left(\frac{aAp_1\dots p_\ell}{q}\right)e\left(\frac{aBp_{\ell+1}\dots p_{2\ell}}{q}\right)$$

whenever $Ap_1\dots p_\ell + Bp_{\ell+1}\dots p_{2\ell} = 2n \le (A+B)x$, and this equals $f\left(\frac{aA}{q}\right)f\left(\frac{aB}{q}\right)$.

□

To complete the proof of Theorem 5.1 we now compute $f\left(\frac{aA}{q}\right)$. First note that every $q \le Q$ can be uniquely factored into $q = dq'$, where d is composed only from primes dividing Δ and $(q',\Delta) = 1$. Next, by Lemma 5.4 and Lemma 5.6 we have that $G(q,2a) = 0$ unless $d|\Delta$. Here we require the technical condition that $4\ell^2|\Delta$. If $d|\Delta$, then we have

$$f\left(\frac{aA}{q}\right) = \sum_{n\le x} c_n e\left(\frac{aAn}{q}\right) = \sum_{(b,q)=1} e\left(\frac{aAb}{q}\right)\sum_{\substack{n\le x\\ n\equiv b\,(q)}} c_n = \sum_{\substack{(b,q)=1\\ b\equiv c_0^\ell\,(d)}} e\left(\frac{aAb}{q}\right)\sum_{\substack{n\le x\\ n\equiv b\,(q')}} c_n,$$

since $c_n = 0$ unless $n \equiv c_0^\ell\,(\Delta)$. We now compute the inner sum above. By the Siegel-Walfisz condition (note: the p_j in the sums below satisfy the conditions in (5.3)), we find that

$$\sum_{\substack{n\le x\\ n\equiv b\,(q')}} c_n = \sum_{p_1}\cdots\sum_{p_{\ell-1}}\sum_{p_\ell\equiv\frac{b}{p_1\cdots p_{\ell-1}}\,(q')} 1 = \frac{1}{\phi(q')}\sum_{p_1}\cdots\sum_{p_{\ell-1}}\sum_{p_\ell} 1 + O\left(\frac{x}{\log^C x}\right) = \\ = \frac{1}{\phi(q')}\sum_{n\le x} c_n + O\left(\frac{x}{\log^C x}\right) = \frac{1}{\phi(q')}f(0) + O\left(\frac{x}{\log^C x}\right).$$

This estimate is uniform in b, and the main term is independent of b, thus we have

$$f\left(\frac{aA}{q}\right) = \frac{1}{\phi(q')}f(0)\sum_{\substack{(b,q)=1\\ b\equiv c_0^\ell\,(d)}} e\left(\frac{aAb}{q}\right) + O\left(\frac{q'x}{\log^C x}\right).$$

Finally, each b in the sum above can be written as $b = c_0^\ell q' \bar{q'} + b'd$, where $(b', q') = 1$ and $q'\bar{q'} \equiv 1\,(d)$. We recall the well–known formula for the Ramanujan sum [Th. 272, H-W] for an arbitrary modulus q

$$\sum_{(b,q)=1} e\left(\frac{ab}{q}\right) = \phi(q)\frac{\mu\left(\frac{q}{(a,q)}\right)}{\phi\left(\frac{q}{(a,q)}\right)}.$$

For convenience, if we let $q_A = q'/(A, q')$ and $q_B = q'/(B, q')$, then this implies that

$$\sum_{\substack{(b,q)=1\\ b\equiv c_0^\ell\,(d)}} e\left(\frac{aAb}{q}\right) = \sum_{(b',q')=1} e\left(\frac{aA(c_0^\ell q'\bar{q'} + b'd)}{q}\right) =$$

$$= e\left(\frac{aAc_0^\ell \bar{q'}}{d}\right) \sum_{(b',q')=1} e\left(\frac{aAb'd}{q'}\right) = \phi(q')\frac{\mu(q_A)}{\phi(q_A)} e\left(\frac{aAc_0^\ell \bar{q'}}{d}\right).$$

If $Q \le \log^{C/2} x$, then these results together with (5.8) and the fact that $A + B \equiv 2 \pmod{\Delta}$ implies that

$$f\left(\frac{aA}{q}\right) f\left(\frac{aB}{q}\right) = \frac{\mu(q_A)\mu(q_B)}{\phi(q_A)\phi(q_B)} e\left(\frac{2ac_0^\ell \bar{q'}}{d}\right) f^2(0) + O\left(\frac{x^2}{\log^C x}\right).$$

By Theorem 5.9, we then get

$$R_2(x) = \tag{5.16}$$

$$= f^2(0)\frac{\phi(P)}{P} \sum_{d|\Delta} \sum_{\substack{q' \le \frac{Q}{d}\\ (q',\Delta)=1}} \frac{\mu(q_A)\mu(q_B)(q', P)}{q'\phi(q_A)\phi(q_B)\phi(d)\phi(q', P)} \sum_{(a,dq')=1} G(dq', -2a) e\left(\frac{2ac_0^\ell \bar{q'}}{d}\right) +$$

$$+ O\left(\frac{x^2}{Q^{1/\ell}}\right) + O\left(\frac{x^2 Q^{2-\frac{1}{\ell}}}{\log^C x}\right).$$

To complete the proof, we now aim to produce (5.10). By letting $Q = \log^{3\ell} x$ and $C = 6\ell$, we find that the error terms in (5.16) are $O(x^2/\log^3 x)$ as claimed in (5.10). Therefore, the remainder of the proof is devoted to the computation of the triple sum in (5.16). Let us write

$$\kappa(q) = \sum_{(a,q)=1} G(q, -2a) e\left(\frac{2ac_0^\ell \bar{q'}}{d}\right),$$

where $q = dq'$ and $d \mid \Delta$ and $(q', \Delta) = 1$. By the Chinese Remainder Theorem, we find that this function is multiplicative. In particular, we have $\kappa(q'd) = \kappa(q')\kappa(d)$. Next, note that from $(A, B) = 1$ we have $\mu(q_A)\mu(q_B) = \mu^2(q')\mu(q', AB)$. We have to compute $\kappa(p)$ for any prime $p \nmid \Delta$ and also $\kappa(p^k)$ for any prime power $p^k \mid \Delta$.

If $p \nmid \Delta$ is prime, then

$$\kappa(p) = \sum_{\substack{u \,(p) \\ (u,p,AB)=1}} \sum_{(a,p)=1} e\left(\frac{-2au^\ell}{p}\right) = \begin{cases} 1-p & \text{if } p \mid AB,\ p \nmid \Delta, \\ 0 & \text{if } p \nmid AB\Delta. \end{cases} \tag{5.17}$$

By an obvious change of variables, if $d \mid \Delta$ and $(c_0, \Delta) = 1$, then

$$\kappa(d) = \sum_{(a,d)=1} \sum_{(u,d)=1} e\left(\frac{2a(u^\ell - 1)}{d}\right).$$

Let us also introduce the notation

$$\rho(p^k) = \#\{u \,(p^k) : \, u^\ell \equiv 1 \pmod{p^k}\},$$

and recall that

$$\rho(p^k) = (\ell, p-1)(\ell, p^{k-1}) \qquad \text{if } p \neq 2,$$
$$\rho(2^k) = \begin{cases} 1 & \text{if } 2 \nmid \ell, \\ (2\ell, 2^{k-1}) & \text{if } 2 \mid \ell. \end{cases}$$

If $p \mid \Delta$ is an odd prime, then

$$\kappa(p) = \sum_{(u,p)=1} \sum_{(a,p)=1} e\left(\frac{2a(u^\ell - 1)}{p}\right) = \rho(p)(p-1) + (p - 1 - \rho(p))\,(-1) = p(\ell, p-1) - (p-1), \tag{5.18}$$

while $\kappa(p^k) = 0$ for any $k \geq 2$ and $p \nmid 2\ell$ by Lemma 5.6. Let s be the integer $s = \mathrm{ord}_p(2\ell)$. In the remaining cases we have $s \geq 1$. Suppose now that $p \mid \ell$ but $p \neq 2$ and $k \geq 2$. We have

$$\kappa(p^k) = \sum_{(u,p^k)=1} \sum_{(a,p^k)=1} e\left(\frac{2a(u^\ell - 1)}{p^k}\right) =$$
$$= \rho(p^k)\phi(p^k) + \sum_{n=0}^{k-1} \sum_{\substack{(u,p^k)=1 \\ p^n \mid u^\ell - 1 \\ p^{n+1} \nmid u^\ell - 1}} \sum_{(a,p^k)=1} e\left(\frac{2a(u^\ell - 1)}{p^k}\right).$$

Obviously $2(u^\ell - 1) = Up^n$ with some integer $p \nmid U$, and the inner sum becomes p^n copies of the Ramanujan sum attached to p^{k-n} (i.e. $p^n \mu(p^{k-n})$). Therefore, we find that

$$\kappa(p^k) = \rho(p^k)\phi(p^k) - p^{k-1} \sum_{\substack{(u,p^k)=1 \\ p^{k-1} \mid u^\ell - 1 \\ p^k \nmid u^\ell - 1}} 1 = \rho(p^k)\phi(p^k) - p^{k-1}\left(p\rho(p^{k-1}) - \rho(p^k)\right) = \tag{5.19}$$
$$= p^k\left(\rho(p^k) - \rho(p^{k-1})\right) = \begin{cases} (\ell, p-1)(p^{2k-1} - p^{2k-2}) & \text{if } 2 \leq k \leq s+1, \\ 0 & \text{if } k \geq s+2. \end{cases}$$

The computation of $\kappa(2^k)$ is similar, and it turns out that

$$\kappa(2^k) = \begin{cases} 1 & \text{if } k = 1, \\ 4 & \text{if } k = 2, \\ 2^{2k-2} & \text{if } 3 \le k \le s+2, \text{ and } 2 \mid \ell, \\ 0 & \text{otherwise.} \end{cases} \tag{5.20}$$

Note that the "otherwise" above implies that either $2 \nmid \ell$ and $k \ge 3$, or $2 \mid \ell$ and $k \ge s+3$. If we replace q' by q in (5.16), the second line of (5.17) implies immediately that the summand with respect to q in (5.16) is zero unless $q \mid AB$. If X is sufficiently large, then clearly we have $Q \ge AB\Delta$, and so the sum over $q \le Q/d$ and $(q, \Delta) = 1$ becomes a sum over $q \mid AB$ with $(q, \Delta) = 1$. Using our formulas for $\kappa(qd)$ (i.e. (5.17-20)), (5.16) reduces to

$$R_2(x) = f^2(0)\frac{\phi(P)}{P} \sum_{d \mid \Delta} \sum_{\substack{q \mid AB \\ (q,\Delta)=1}} \frac{\mu(q)\kappa(d)\kappa(q)}{\phi(d)\phi^2(q)} + O\left(\frac{x^2}{\log^3 x}\right) =$$

$$= f^2(0)\frac{\phi(P)}{P} \prod_{p \mid 2\ell} \left(1 + \frac{\kappa(p)}{\phi(p)} + \frac{\kappa(p^2)}{\phi(p^2)} + \dots\right) \prod_{\substack{p \mid \Delta \\ p \nmid 2\ell}} \left(1 + \frac{\kappa(p)}{\phi(p)}\right) \prod_{\substack{p \mid AB \\ p \nmid \Delta}} \left(1 - \frac{\kappa(p)}{\phi^2(p)}\right) +$$

$$+ O\left(\frac{x^2}{\log^3 x}\right) = 2\ell(2, \ell) \prod_{p \mid \Delta} (\ell, p-1) f^2(0) + O\left(\frac{x^2}{\log^3 x}\right).$$

This is (5.10), and so the proof of Theorem 5.1 is complete.

6. Proof of theorem 1.

To reduce Theorem 1 to Theorem 5.1 we need two more elementary facts. We state them as Lemmas 6.1 and 6.2.

Lemma 6.1. *If the integers M and Δ satisfy*

$$M \equiv 1 \pmod{(24, \Delta)}, \quad \left(\frac{2}{p}\right) = 1 \text{ for every prime } p \mid (M, \Delta),$$

then there are positive integers a and b such that

$$Ma^2 + b^2 \equiv 2 \pmod{\Delta}, \quad (Ma, b) = 1, \quad (ab, M\Delta) = 1.$$

Proof. First we prove that there are integers u and v, coprime to Δ, such that $M \equiv 2u^2 - v^2 \pmod{\Delta}$. By Chinese Remainder Theorem, it suffices to check, for any $p^k \mid \Delta$, that there are u and v coprime to p such that $M \equiv 2u^2 - v^2 \pmod{p^k}$. For $p = 2$ and $k \le 3$ the choice $u = v = 1$ is a good one since $M \equiv 1 \pmod{(8, \Delta)}$. Suppose that $k \ge 3$ and that $v_0^2 \equiv 2 - M$

(mod 2^k) (i.e. $u = 1$, $v = v_0$ is a solution mod 2^k, $2 \nmid v_0$). Then $u = 1$ and one of $v_1 = v_0$ or $v_2 = v_0 + 2^{k-1}$ is a solution mod 2^{k+1} since $v_2^2 \equiv v_0^2 + 2^k \pmod{2^{k+1}}$. This settles the case of $p = 2$.

For odd primes $p \mid \Delta$, Hensel's Lemma implies that it is enough to prove that there are integers u and v, coprime to p, for which $M \equiv 2u^2 - v^2 \pmod{p}$. If $3 \mid \Delta$, then $M \equiv 1 \pmod 3$ and $u = v = 1$ is an obvious choice. If $p \mid M$, let $u = 1$ and choose v so that $v^2 \equiv 2 \pmod{p}$. Finally, if $p \nmid 6M$, then the set of residue classes $\{M - 2u^2 : 0 \le u \le \frac{p-1}{2}\}$ cannot be disjoint to the set of residue classes $\{v^2 : 0 \le v \le \frac{p-1}{2}\}$ by the Pigeon Hole Principle. This provides a pair of integers u and v which completes the proof if both are coprime to p. If they are not both coprime to p, then either $M \equiv -v_0^2 \pmod{p}$ and then $u = 2v_0$ and $v = 3v_0$ is a good choice for u and v. Otherwise we have $M \equiv 2u_0^2 \pmod{p}$, in which case $u = 3u_0$, $v = 4u_0$ is a good choice.

To obtain the claimed statement, let $u\bar{u} \equiv 1 \pmod{\Delta}$ and choose a to be any positive integer $a \equiv \bar{u} \pmod{\Delta}$ for which $(a, M) = 1$, and then choose b to be any positive integer $b \equiv \bar{u}v \pmod{\Delta}$ for which $(b, aM) = 1$. (note: by Dirichlet's Theorem, a and b can be chosen to be big primes).

□

The next lemma [Prop. 1, So] provides the essential criterion for producing elements in class groups.

Lemma 6.2. *Let $\ell \ge 2$ be an integer and let $d \ge 63$ be a square–free integer for which*

$$dt^2 = m^{2\ell} - n^2,$$

where m and n are integers with $(m, 2n) = 1$ and $m^\ell \le d$. Then $\mathrm{CL}(-d)$ contains an element of order 2ℓ.

Proof of Theorem 1. Let $K/\mathbb{Q}$ be a finite Galois extension, c a conjugacy class in $\mathrm{Gal}(K/\mathbb{Q})$, and $M \equiv 1 \pmod{24}$ a positive square-free integer with the property that $\left(\frac{2}{q}\right) = 1$ for every prime $q \mid (M, \ell\Delta_K)$. Let $\Delta := \mathrm{lcm}\,(4\ell^2, \Delta_K)$ and choose an arbitrary prime $p_0 \in S(K, c, M)$. Then there is a cyclotomic extension K'/K and a conjugacy class c' in $\mathrm{Gal}(K'/\mathbb{Q})$ such that every prime p which is unramified in $K'/\mathbb{Q}$ with $\mathrm{Frob}(p) \in c'$ has the property that $p \equiv p_0 \pmod{\Delta}$. Furthermore, we have $S(K', c', M) \subset S(K, c, M)$. Let $\mathcal{P}$ denote the set of these primes.

Observe that the prime factors of the discriminant of K' are the same as those of Δ. Therefore, if q is coprime to Δ, the conjugacy class c' splits into $\phi(q)$ classes of equal size in the qth cyclotomic extension of K'. In particular, the constant in the Chebotarev Density Theorem is $\frac{1}{\phi(q)} \cdot \frac{\#c'}{\#\mathrm{Gal}(K'/\mathbb{Q})}$. The Chebotarev Density Theorem applied to cyclotomic extensions of K' implies that $\mathcal{P}$ satisfies the Siegel-Walfisz condition for Δ. This is the number field generalization of the Siegel-Walfisz Theorem describing the uniform distribution of primes in residue classes. The proof follows as in the classical case (for example, see [D], [Go], [Mi]) after one notices that the only Artin L-functions for irreducible representations that might have exceptional real zeros are those associated with real 1-dimensional representations (i.e.

quadratic Dirichlet characters). Then the required estimates for the zero-free regions for Artin L-functions (for example, see [Go] or [Mi]) are exactly the same as those in the classical case.

By Lemma 6.1, there are positive integers a and b for which Theorem 5.1 applies with $A = Ma^2$ and $B = b^2$, and where ℓ, Δ, $c_0 = p_0$ and $\mathcal{P}$ are given. Consequently, there are at least $\gg X^{\frac{1}{2}+\frac{1}{2\ell}} \log^{-2} X$ integers of the form

$$M(ab)^2 p_1 \dots p_{2\ell} = m^{2\ell} - n^2 \leq X,$$

where the $p_j \in \mathcal{P}$ are distinct, $p_j \nmid Mab\Delta$, $(m, 2n) = 1$ and $p_1 \dots p_{2\ell} \geq m^\ell$. By Lemma 6.2, we have that $\mathrm{CL}(-d)$ contains an element of order ℓ for all of the above $d = Mp_1 \dots p_{2\ell}$.

□

References

[B] C. D. Beaver, *5-torsion in the Shafarevich-Tate group of a family of elliptic curves*, J. Number Th. **82** (2000), 25-46.

[Bö] R. Bölling, *Die Ordung der Schafarewitsch-Tate Gruppe kann beliebeg gross werden*, Math. Nachr. **67** (1975), 157-179.

[B-K-W] J. Brüdern, K. Kawada and T. Wooley, *Additive representation in thin sequences, II: the binary Goldbach problem*, to appear, Mathematika.

[Ca] J. W. S. Cassels, *Arithmetic on curves of genus 1 (VI). The Tate-Shafarevich group can be arbitrarily large*, J. reine. angew. math. **214/215** (1964), 65-70.

[C-L] H. Cohen and H. Lenstra, *Heuristics on class groups of number fields*, Number Theory (Noordwijkerhout, 1983), Springer Lect. Notes in Math. **1068** (1984), 33-62.

[D] H. Davenport, *Multiplicative number theory*, Springer Verlag, New York, 1980.

[D-H] H. Davenport and H. Heilbronn, *On the density of discriminants of cubic fields II*, Proc. Royal Soc., A **322** (1971), 405-420.

[F-H] S. Friedberg and J. Hoffstein, *Nonvanishing theorems for automophic L-functions on GL*(2), Ann. Math. **142** (1995), 385-423.

[Fr] G. Frey, *On the Selmer group of twists of elliptic curves with $\mathbb{Q}$-rational torsion points*, Canad. J. Math. **XL** (1988), 649-665.

[Go] L. J. Goldstein, *A generalization of the Siegel-Walfisz theorem*, Trans. A. M. S. **149** (1970), 417-429.

[G-M] F. Gouvêa and B. Mazur, *The square-free sieve and the rank of elliptic curves*, J. Amer. Math. Soc. **4** (1991), 1-23.

[H-W] G. H. Hardy and E. M. Wright, *An introduction to the theory of numbers*, Oxford Univ. Press, Oxford, 1979.

[J-O] K. James and K. Ono, *Selmer groups of quadratic twists of elliptic curves*, Math. Ann. **314** (1999), 1-17.

[Ko] W. Kohnen, *Fourier coefficients of modular forms of half-integral weight*, Math. Ann. **271** (1985), 237-268.

[Ko-O] W. Kohnen and K. Ono, *Indivisibility of class numbers of imaginary quadratic fields and orders of Tate-Shafarevich groups of elliptic curves with complex multiplication*, Invent. Math. **135** (1999), 387-398.

[Kol] V. Kolyvagin, *Finiteness of $E(\mathbb{Q})$ and $Ш_{E/\mathbb{Q}}$ for a subclass of Weil curves (Russian)*, Izv. Akad. Nauk., USSR, ser. Matem. **52** (1988), 522-540.

[Kr] K. Kramer, *A family of semistable elliptic curves with large Tate-Shafarevich groups*, Proc. Amer. Math. Soc. **89** (1983), 379-386.

[Mi] T. Mitsui, *Generalized Prime Number Theorem*, Japan J. Math. **26** (1956), 1-42.

[M] M. R. Murty, *Exponents of class groups of quadratic fields*, Topics in Number Theory (Ed. S. Ahlgren et. al.), Kluwer Acad. Press **467** (1999), 229-239.

[O1] K. Ono, *Twists of elliptic curves*, Compositio Math. **106** (1997), 349-360.

[O2] K. Ono, *Nonvanishing of quadratic twists of modular L-functions and applications to elliptic curves*, J. reine angew. math **533** (2001), 81-97.

[O-P] K. Ono and M. A. Papanikolas, *Quadratic twists of modular forms and elliptic curves*, accepted for publication, Millenial Conference Proc. (Urbana, Illinois 2000), A. K. Peters.

[O-Sk] K. Ono and C. Skinner, *Non-vanishing of quadratic twists of modular L-functions*, Invent. Math. **134** (1998), 651-660.

[P] A. Perelli, *Goldbach numbers represented by polynomials*, Rev. Mat. Iberoamericana **12** (1996), 477-490.

[R] D. Rohrlich, *Unboundedness of the Tate-Shafarevich group in families of quadratic twists, Appendix to J. Hoffstein and W. Luo, Nonvanishing of L-series and the combinatorial sieve*, Math. Res. Lett. **4** (1997), 435-444.

[Sh] G. Shimura, *On modular forms of half-integral weight*, Annals of Math. **97** (1973), 440-481.

[S] J. H. Silverman, *The Arithmetic of Elliptic Curves*, Springer-Verlag, New York, 1986.

[So] K. Soundararajan, *Divisibility of class numbers of imaginary quadratic fields*, J. London Math. Soc. **61** (2000), 681-690.

[Ste] G. Stevens, Λ-*adic modular forms of half-integral weight and a* Λ-*adic Shintani lifting*, Arith. Geometry (Tempe, Az. 1993) Contemp. Math., Amer. Math. Soc. **174** (1994), 129-151.

[St-T] C. Stewart and J. Top, *On ranks of twists of elliptic curves and power-free values of binary forms*, J. Amer. Math. Soc, **8 no. 4** (1995), 947-974.

[V] R. C. Vaughan, *The Hardy–Littlewood Method*, Cambridge University Press, 1981.

[W] J.-L.Waldspurger, *Sur les coefficients de Fourier des formes modulaires de poids demi-entier*, J. Math. Pures et Appl. **60** (1981), 375-484.

[Wo] S. Wong, *Elliptic curves and class number divisibility*, Int. Math. Res. Not. **12** (1999), 661-672.

Alfréd Rényi Mathematical Institute P.O. Box 127, Budapest 1364, Hungary
E-mail address: balog@renyi.hu

Dept. Math., University of Wisconsin, Madison, Wisconsin, 53706, USA.
E-mail address: ono@math.wisc.edu