ACTA ARITHMETICA
LXXVIII.2 (1996)

Euler's concordant forms

by

Ken Ono (Princeton, N.J., and University Park, Penn.)

1. Introduction. In [6] Euler asks for a classification of those pairs of distinct non-zero integers M and N for which there are integer solutions (x, y, t, z) with $xy \neq 0$ to

$$x^2 + My^2 = t^2 \quad \text{and} \quad x^2 + Ny^2 = z^2. \tag{1}$$

This is known as *Euler's concordant forms problem*, and when $M = -N$ Euler's problem is the *congruent number problem.* Tunnell gave a conditional solution to the congruent number problem using elliptic curves and modular forms. Using these ideas, we consider Euler's problem which reduces to a study of the elliptic curve over $\mathbb{Q}$:

$$E_{\mathbb{Q}}(M, N): \quad y^2 = x^3 + (M + N)x^2 + MNx.$$

If $E_{\mathbb{Q}}(M, N)$ has positive rank, then there are infinitely many primitive integer solutions to (1); but if $E_{\mathbb{Q}}(M, N)$ has rank 0, then there may be a non-trivial solution. Such a solution exists if and only if the torsion group is $\mathbb{Z}2 \times \mathbb{Z}8$ or $\mathbb{Z}2 \times \mathbb{Z}6$. We classify all such cases, thereby reducing Euler's problem to a question of ranks. In some cases, the ranks of quadratic twists of $E_{\mathbb{Q}}(M, N)$ are described by the representations of integers by ternary quadratic forms. Consequently, we obtain results regarding Euler's problem, and the existence of solutions to a pair of Pell's equations. Moreover, we give a new and elementary method, using the theory of lacunary modular forms, which establishes that there are infinitely many rank 0 quadratic twists of $E_{\mathbb{Q}}(M, N)$ by discriminants in arithmetic progressions.

2. Results. A solution to (1) is *primitive* if x, y, t, and z are positive integers and $\gcd(x, y) = 1$. In [1] E. T. Bell parametrized the solutions of (1) in terms of polynomials in 41 variables, a solution that is difficult to absorb.

1991 *Mathematics Subject Classification*: Primary 05A17; Secondary 11P83.
Key words and phrases: Euler's concordant forms problem.
The author is supported by NSF grants DMS-9304580 and DMS-9508976.

In [17] T. Ono mentions various cases of (1) where it is known that there are infinitely many solutions. For example, if $M = 1$ and $N = 2n^2 - 1$ with $n \neq 0, 1$, and 2, then there are infinitely many primitive solutions.

By multiplying the two equations in (1) together, and then multiplying by x^2/y^6, we get

$$\frac{x^2t^2z^2}{y^6} = \frac{x^6}{y^6} + (M+N)\left(\frac{x^4}{y^4}\right) + MN\left(\frac{x^2}{y^2}\right). \tag{2}$$

If we then replace x^2/y^2 by x and also xtz/y^3 by y we find that

$$y^2 = x^3 + (M+N)x^2 + MNx. \tag{3}$$

In studying the points of $E_{\mathbb{Q}}(M, N)$, we note that one may make the further assumption that the $\gcd(M, N)$ be a square-free integer. To see this we note that if d is a non-zero integer, then $E_{\mathbb{Q}}(d^2M, d^2N)$ is isomorphic to $E_{\mathbb{Q}}(M, N)$ by replacing y by y/d^3 and x by x/d^2. Also note that $E_{\mathbb{Q}}(M, N) \cong E_{\mathbb{Q}}(N, M)$, hence we may freely interchange the order of M and N in what follows. Furthermore, we also note that $E_{\mathbb{Q}}(M, N) \cong E_{\mathbb{Q}}(-M, N - M) \cong E_{\mathbb{Q}}(-N, M - N)$ by replacing x by $x - M$ and $x - N$. Therefore we could without loss of generality assume that M and N are both positive integers. Using the standard definitions, one can easily verify that the discriminant of $E_{\mathbb{Q}}(M, N)$ is $\Delta = 16M^2N^2(M - N)^2$ and its j-invariant is

$$j = \frac{256(M^2 - MN + N^2)^3}{M^2N^2(M - N)^2}.$$

By Mordell's theorem, $E_{\mathbb{Q}}(M, N)$ forms a finitely generated abelian group, and so satisfies

$$E_{\mathbb{Q}}(M, N) \cong E_{\text{tor}} \times \mathbb{Z}^r$$

where E_{tor}, the *torsion subgroup* of $E_{\mathbb{Q}}(M, N)$, is a finite abelian group and the rank r is a non-negative integer. However, by Mazur's theorem E_{tor} satisfies

$$E_{\text{tor}} \in \begin{cases} \mathbb{Z}m, & \text{where } 1 \leq m \leq 10, \text{ or } m = 12, \\ \mathbb{Z}2 \times \mathbb{Z}2m, & \text{where } 1 \leq m \leq 4. \end{cases}$$

Computing the rank r of an elliptic curve E has been the focus of significant interest, and of central importance is the Hasse–Weil L-function $L(E, s)$. For every prime p let $N(p)$ denote the number of points (including the point at infinity) on E_p, the reduction of E modulo p. Define $a(p) := p + 1 - N(p)$. Then $L(E, s)$ is defined by

$$L(E, s) := \sum_{n=1}^{\infty} \frac{a(n)}{n^s} = \prod_{p|\Delta} \frac{1}{1 - a(p)p^{-s}} \prod_{p\nmid\Delta} \frac{1}{1 - a(p)p^{-s} + p^{1-2s}}.$$

The conjectures of Birch and Swinnerton-Dyer (B-SD) connect the analytic properties of the Hasse–Weil L-function $L(E,s)$ for an elliptic curve E over $\mathbb{Q}$ with its rank. A weak version is:

CONJECTURE (B-SD). *Let E be an elliptic curve over $\mathbb{Q}$, and let $L(E,s) = \sum_{n=1}^{\infty} a(n)/n^s$ be its Hasse–Weil L-function. Then $L(E,s)$ has an analytic continuation to the entire complex plane and the rank of E is positive if and only if $L(E,1) = 0$.*

In [4] Coates and Wiles proved that if E is a positive rank elliptic curve over $\mathbb{Q}$ with complex multiplication, then $L(E,1) = 0$, and as we shall see in Section 4, by the work of Kolyvagin, M. R. Murty, V. K. Murty, Bump, Friedberg, and Hoffstein much more is now known concerning this conjecture for *modular* elliptic curves.

Returning to Euler's problem, if (1) has a non-trivial integer solution $(\alpha,\beta,\gamma,\delta)$, then by (2) we see that $E_{\mathbb{Q}}(M,N)$ contains the $\mathbb{Q}$-rational point $(\alpha^2/\beta^2, \alpha\gamma\delta/\beta^3)$. By factoring (2) and letting $y = 0$, we find the three trivial order 2 points $(0,0)$, $(-M,0)$, and $(-N,0)$, and so $\mathbb{Z}2 \times \mathbb{Z}2$ is always a subgroup of the torsion subgroup of $E_{\mathbb{Q}}(M,N)$. Since these points have $y = 0$, it is not possible for them to correspond to a non-trivial solution of (1); hence a solution of (1), if there are any, must correspond to points of infinite order or torsion points with order different from 2.

If $M = -N$, the congruent number case, or if $M = 2N$, or if $M = \frac{1}{2}N$, then the elliptic curve $E_{\mathbb{Q}}(M,N)$ has $j = 1728$ and hence has complex multiplication by $\mathbb{Q}(i)$. If $M = 2N$, then by replacing x by $x - N$ in $E(2N,N)$ we obtain the more familiar model

$$y^2 = x^3 - N^2 x.$$

Since the torsion subgroups of all of these curves is $\mathbb{Z}2 \times \mathbb{Z}2$ and these torsion points do not afford any solutions, a non-trivial solution to Euler's problem exists if and only if the rank of $E_{\mathbb{Q}}(2N,N)$ is positive, which is precisely the condition for determining whether or not N is a congruent number. Consequently, by Tunnell's theorem we obtain:

COROLLARY 1. *Let n be a square-free integer, d any non-zero integer, and let $M = 2d^2n$ and $N = d^2n$.*

- *If n is odd and there is a non-trivial solution to* (1)*, then the number of integer representations of n by $2x^2 + y^2 + 32z^2$ equals the number of its integer representations $2x^2 + y^2 + 8z^2$. Furthermore, assuming B-SD, if the representation numbers of n by these two ternary quadratic forms are equal, then there are infinitely many primitive solutions to* (1)*.*
- *If n is even and there is a non-trivial solution to* (1)*, then the number of integer representations of $n/2$ by $4x^2 + y^2 + 32z^2$ equals the number of its integer representations by $4x^2 + y^2 + 8z^2$. Furthermore, assuming B-SD, if*

the representation numbers of $n/2$ by these two ternary quadratic forms are equal, then there exist infinitely many primitive solutions to (1).

Unlike the congruent number problem, it is the case that there are torsion points which afford non-trivial solutions. For example, if we let $M = 5$ and $N = 32$, then the elliptic curve $E_{\mathbb{Q}}(5, 32)$ has rank zero yet $(2, 1, 3, 6)$ is a non-trivial solution to (1). It turns out that this solution is the unique primitive solution and it corresponds to certain torsion points of order 3 on the elliptic curve $E_{\mathbb{Q}}(5, 32)$. A thorough investigation of the torsion subgroups of $E_{\mathbb{Q}}(M, N)$ shows that certain torsion points of order 3 and certain torsion points of order 4 correspond to non-trivial solutions of (1). In all other cases, there are non-trivial solutions to (1) if and only if the rank of $E_{\mathbb{Q}}(M, N)$ is positive. In Section 3 we will prove the following classification theorem.

Main Theorem 1. *The torsion subgroups of $E_{\mathbb{Q}}(M, N)$ are uniquely determined by the following conditions*:

• *The torsion subgroup of $E_{\mathbb{Q}}(M, N)$ contains $\mathbb{Z}2 \times \mathbb{Z}4$ if M and N are both squares, or $-M$ and $N - M$ are both squares, or if $-N$ and $M - N$ are both squares.*

• *The torsion subgroup of $E_{\mathbb{Q}}(M, N)$ is $\mathbb{Z}2 \times \mathbb{Z}8$ if there exists a non-zero integer d such that $M = d^2u^4$ and $N = d^2v^4$, or $M = -d^2v^4$ and $N = d^2(u^4 - v^4)$, or $M = d^2(u^4 - v^4)$ and $N = -d^2v^4$, where (u, v, w) forms a Pythagorean triple (i.e. $u^2 + v^2 = w^2$).*

• *The torsion subgroup of $E_{\mathbb{Q}}(M, N)$ is $\mathbb{Z}2 \times \mathbb{Z}6$ if there exists integers a and b such that $a/b \notin \{-2, -1, -1/2, 0, 1\}$ and $M = a^4 + 2a^3b$ and $N = 2ab^3 + b^4$.*

• *In all other cases, the torsion subgroup of $E_{\mathbb{Q}}(M, N)$ is $\mathbb{Z}2 \times \mathbb{Z}2$.*

As a corollary we obtain the following complete classification of the primitive solutions to (1) which correspond to torsion points in $E_{\mathbb{Q}}(M, N)$.

Main Corollary 1. *The primitive solutions to* (1) *afforded by the torsion points of $E_{\mathbb{Q}}(M, N)$ are as follows*:

• *If there exists a non-zero integer d such that $M = d^2u^4$ and $N = d^2v^4$ and (u, v, w) is a Pythagorean triple, then the unique primitive solution to* (1) *arising from the torsion subgroup of $E_{\mathbb{Q}}(M, N)$ is $(|duv|, 1, |duw|, |dvw|)$.*

• *If there exists a non-zero integer d such that $M = -d^2v^4$ and $N = d^2(u^4 - v^4)$ (resp. $M = d^2(u^4 - v^4)$ and $N = -d^2v^4$) where (u, v, w) is a Pythagorean triple, then the unique primitive solution to* (1) *arising from the torsion subgroup of $E_{\mathbb{Q}}(M, N)$ is $(|dvw|, 1, |duv|, |duw|)$ (resp. $(|dvw|, 1, |duw|, |duv|)$).*

• *If there exists integers a and b such that $a/b \notin \{-2, -1, -1/2, 0, 1\}$ and $M = a^4 + 2a^3b$ and $N = 2ab^3 + b^4$, then the unique primitive solution to* (1)

arising from the torsion subgroup of $E_{\mathbb{Q}}(M,N)$ *is* $(|ab|, 1, |a(a+b)|, |b(a+b)|)$.

• *In all other cases, there are no non-trivial solutions to* (1) *afforded by the torsion points of* $E_{\mathbb{Q}}(M,N)$.

So when the torsion subgroup of $E_{\mathbb{Q}}(M,N)$ is $\mathbb{Z}2 \times \mathbb{Z}2$ or $\mathbb{Z}2 \times \mathbb{Z}4$, then there are non-trivial solutions (infinitely many) to (1) if and only if the rank of $E_{\mathbb{Q}}(M,N)$ is positive.

In the general case, assuming the Shimura–Taniyama–Weil conjecture (STW) and B-SD, we establish how explicit knowledge of the Fourier expansions of weight 3/2 modular forms can lead to a theoretical solution of suitable cases of Euler's problem. In several cases we explicitly carry out the details in connection with representation numbers by ternary quadratic forms. For convenience, if Q is a quadratic form, then let $r(n,Q)$ be the number of integer representations of n by Q. We obtain:

Main Theorem 2. *Let* n_1 *be a positive square free integer.*

(a) *Suppose that* $L(E_{\mathbb{Q}}(6n_1,-18n_1),1) \neq 0$ *and* $r(n_1,x^2+2y^2+12z^2) \neq r(n_1,2x^2+3y^2+4z^2)$. *Let* $n_2 \equiv n_1 \bmod 24$ *be a positive square-free integer and suppose that*

$$(M,N) \in \left\{ \begin{matrix} (24d^2n_2, 18d^2n_2),\ (6d^2n_2, -18d^2n_2),\ (-6d^2n_2, -24d^2n_2), \\ (6d^2n_2, 54d^2n_2), \quad (48d^2n_2, -6d^2n_2),\ (-48d^2n_2, -54d^2n_2) \end{matrix} \right\}$$

for some non-zero integer d. *If* $r(n_2,x^2+2y^2+12z^2) \neq r(n_2,2x^2+3y^2+4z^2)$, *then the rank of* $E_{\mathbb{Q}}(M,N)$ *is unconditionally* 0. *If these representation numbers are equal, then assuming B-SD the rank of* $E_{\mathbb{Q}}(M,N)$ *is positive.*

(b) *Suppose that* $L(E_{\mathbb{Q}}(40n_1,-10n_1),1) \neq 0$ *and* $r(n_1,x^2+2y^2+20z^2) \neq r(n_1,2x^2+4y^2+5z^2)$. *Let* $n_2 \equiv n_1, 9n_1 \bmod 40$, *be a positive square-free integer and suppose that*

$$(M,N) \in \{(50d^2n_2, 10d^2n_2),\ (40d^2n_2, -10d^2n_2),\ (-40d^2n_2, -50d^2n_2)\}$$

for some non-zero integer d. *If* $r(n_2,x^2+2y^2+20z^2) \neq r(n_2,2x^2+3y^2+4z^2)$, *then the rank of* $E_{\mathbb{Q}}(M,N)$ *is unconditionally* 0. *If these representation numbers are equal, then assuming B-SD the rank of* $E_{\mathbb{Q}}(M,N)$ *is positive.*

(c) *Suppose that* $L(E_{\mathbb{Q}}(9n_1,-3n_1),1) \neq 0$ *and* $r(n_1,x^2+7y^2+7z^2-2yz) \neq r(n_1,3x^2+4y^2+5z^2-4yz)$. *Let* $n_2 \equiv n_1 \bmod 24$ *be a positive square-free integer and suppose that*

$$(M,N) \in \left\{ \begin{matrix} (12d^2n_2, 3d^2n_2), \quad (9d^2n_2, -3d^2n_2), \quad (-9d^2n_2, -12d^2n_2), \\ (27d^2n_2, 24d^2n_2),\ (3d^2n_2, -24d^2n_2),\ (-3d^2n_2, -27d^2n_2) \end{matrix} \right\}$$

for some non-zero integer d. *If* $r(n_2,x^2+7y^2+7z^2-2yz) \neq r(n_2,3x^2+4y^2+5z^2-4yz)$, *then the rank of* $E_{\mathbb{Q}}(M,N)$ *is unconditionally* 0. *If these representation numbers are equal, then assuming B-SD the rank of* $E_{\mathbb{Q}}(M,N)$ *is positive.*

Consequently, we obtain:

Main Corollary 2. *Assume that d is any non-zero integer, and that (M, N) is a pair of integers belonging to one of the families given in* (a), (b) *or* (c) *of Main Theorem* 2. *Then in each case we obtain*:

(a) *Let n_2 be an odd positive square-free integer. If $r(n_2, x^2 + 2y^2 + 12z^2) \neq r(n_2, 2x^2 + 3y^2 + 4z^2)$, then there are unconditionally no primitive solutions to* (1). *If these representation numbers are equal, then assuming B-SD there are infinitely many primitive solutions to* (1).

(b) *Let n_2 be an odd positive square-free integer. If $r(n_2, x^2 + 2y^2 + 20z^2) \neq r(n_2, 2x^2 + 4y^2 + 5z^2)$, then there are unconditionally no primitive solutions to* (1). *If these representation numbers are equal, then assuming B-SD there are infinitely many primitive solutions to* (1).

(c) *Let $n_2 \not\equiv 7 \bmod 8$ be an odd positive square-free integer. If $r(n_2, x^2 + 7y^2 + 7z^2 - 2yz) \neq r(n_2, 3x^2 + 4y^2 + 5z^2 - 4yz)$, then there are unconditionally no primitive solutions to* (1). *If these representation numbers are equal, then assuming B-SD there are infinitely many primitive solutions to* (1).

With the theory of *lacunary* modular forms, we show that there are infinitely many quadratic twists in each of the families mentioned in Main Corollary 2 with rank 0.

Main Theorem 3. *Let d be a non-zero integer.*

• *Let $1 \leq r \leq 23$ be an odd integer. Then there are infinitely many positive square-free integers $n \equiv r \bmod 24$ such that for*

$$(M, N) \in \left\{ \begin{matrix} (24d^2n, 18d^2n),\ (6d^2n, -18d^2n),\ (-6d^2n, -24d^2n), \\ (6d^2n, 54d^2n),\quad (48d^2n, -6d^2n),\ (-48d^2n, -54d^2n) \end{matrix} \right\}$$

the rank of $E_{\mathbb{Q}}(M, N)$ is 0. *In each of these cases, there are no primitive solutions to* (1).

• *If $1 \leq r \leq 40$ is an odd integer, then there are infinitely many positive square-free integers $n \equiv r$ or $9r \bmod 40$ such that for*

$$(M, N) \in \{(50d^2n, 10d^2n),\ (40d^2n, -10d^2n),\ (-40d^2n, -50d^2n)\}$$

the rank of $E_{\mathbb{Q}}(M, N)$ is 0. *In each of these cases, there are no primitive solutions to* (1).

• *Let r be one of* 1, 3, 5, 9, 11, 13, 17, 19 *or* 21. *Then there are infinitely many positive square-free integers $n \equiv r \bmod 24$ such that for*

$$(M, N) \in \left\{ \begin{matrix} (12d^2n, 3d^2n),\quad (9d^2n, -3d^2n),\quad (-9d^2n, -12d^2n), \\ (27d^2n, 24d^2n),\ (3d^2n, -24d^2n),\ (-3d^2n, -27d^2n) \end{matrix} \right\}$$

the rank of $E_{\mathbb{Q}}(M, N)$ is 0. *In such cases there are no primitive solutions to* (1).

3. The torsion subgroup of $E_{\mathbb{Q}}(M,N)$. To obtain Main Theorem 1, we use the following 2-descent proposition [7, 4.1, p. 37]:

PROPOSITION 1. *Let $P=(x',y')$ be a $\mathbb{Q}$-rational point on E, an elliptic curve over $\mathbb{Q}$ given by*

$$y^2=(x-\alpha)(x-\beta)(x-\gamma)$$

where α, β, and $\gamma\in\mathbb{Q}$. Then there exists a $\mathbb{Q}$-rational point $Q=(x,y)$ on E such that $2Q=P$ if and only if $x'-\alpha, x'-\beta$, and $x'-\gamma$ are all $\mathbb{Q}$-rational squares.

As an immediate corollary we obtain

COROLLARY 2. *If M and N are distinct non-zero integers, then there exists a non-trivial solution to (1) if and only if there exist non-trivial points $P=(x',y')$ and $Q=(x,y)$ on $E_{\mathbb{Q}}(M,N)$ such that $2Q=P\notin\{(0,0),(-M,0),(-N,0)\}$.*

Proof. First note that (3) has the factorization $y^2=x(x+M)(x+N)$. Suppose that $(x,y,t,z)=(a,b,c,d)$ is a non-trivial solution to (1). Then $P=(a^2/b^2,acd/b^3)$ is a point on $E_{\mathbb{Q}}(M,N)$ and $a^2+Mb^2=c^2$ and $a^2+Nb^2=d^2$. Hence we find that $a^2/b^2, a^2/b^2+M=c^2/b^2$, and $a^2/b^2+N=d^2/b^2$ are all rational squares. Then by the proposition above there exists a point Q such that $P=2Q$.

Suppose that there exists a $\mathbb{Q}$-rational point $Q=(x,y)$ such that $P=(x',y')=2Q$. We may assume that $x'=a^2/b^2$ since by the duplication formula (see [27, 28]) it is known that the x-coordinate of $2Q$ (denoted by $X(2Q)$) is

$$X(2Q)=\left(\frac{x^2-MN}{2y}\right)^2=x'.$$

Hence by the above proposition we know that a^2/b^2+M and a^2/b^2+N are both non-zero squares; hence by multiplying through by b^2 we obtain the primitive solution $(|a|,|b|,\sqrt{a^2+Mb^2},\sqrt{a^2+Nb^2})$ to (1). ∎

Proof of Main Theorem 1. We prove this theorem by investigating the cases where the torsion subgroup contains points of order $4, 8$, and 3.

• In the first case, we first observe that $\mathbb{Z}2\times\mathbb{Z}4$ is in the torsion subgroup of $E_{\mathbb{Q}}(M,N)$ if and only if there exists a point of order 4. $E_{\mathbb{Q}}(M,N)$ has a point Q of order 4 if and only if $2Q=(x',y')$, an order 2 point, is one of $(0,0),(-M,0)$, or $(-N,0)$. But by the above proposition, it is known that $(0,0)$ (resp. $(-M,0)$, and $(-N,0)$) is twice another point if and only if M and N are both squares (resp. $-M$ and $N-M$ are both squares and $-N$ and $M-N$ are both squares).

We now explicitly list the four points of order 4. If $M = m^2$ and $N = n^2$ (we assume that $m, n > 0$), then

$$X(2Q) = \left(\frac{x^2 - m^2n^2}{2y}\right)^2 = 0.$$

Hence it is clear that $x = \pm mn$. By solving for y in (3) we find that the four order 4 points are

$$(mn, \pm mn(m+n)) \quad \text{and} \quad (-mn, \pm mn(m-n)). \tag{4}$$

Now if $-M = m^2$ and $N - M = k^2$, then

$$X(2Q) = \left(\frac{x^2 + m^2(k^2 - m^2)}{2y}\right)^2 = m^2.$$

Then by letting $y = \pm(x^2 + m^2(k^2 - m^2))/(2m)$ and solving for x in (3), we obtain the four order 4 points:

$$(m^2 - mk, \pm k(m^2 - mk)) \quad \text{and} \quad (m^2 + mk, \pm k(m^2 + mk)). \tag{5}$$

If $-N$ and $M - N$ are both squares, then the four order 4 points are found as in this last case.

• In this case we determine when the torsion subgroup is $\mathbb{Z}2 \times \mathbb{Z}8$. Since $\mathbb{Z}2 \times \mathbb{Z}4$ is a subgroup of $\mathbb{Z}2 \times \mathbb{Z}8$, we consider each of the cases which arose when determining whether or not $\mathbb{Z}2 \times \mathbb{Z}4$ is contained in the torsion group.

First we consider the case where $M = m^2$ and $N = n^2$. So if $Q = (x, y)$ is a point of order 8, then $2Q$ must be one of the four order 4 points given above. In particular, it is easy to see that $X(2Q) = mn$. By the proposition, such a point Q exists if and only if $mn, mn+m^2$, and $mn+n^2$ are all squares. Since we may assume that $\gcd(M, N)$ is square free, we may assume that $\gcd(m, n) = 1$. Hence it is clear that both m and n are squares, say $m = u^2$ and $n = v^2$. We now know that $u^2v^2, u^2v^2+u^4$, and $u^2v^2+v^4$ are all squares. This occurs if and only if $u^2+v^2 = w^2$ (i.e. (u, v, w) is a Pythagorean triple). So we find that if M and N are both squares and the torsion group is $\mathbb{Z}2\times\mathbb{Z}8$, then $M = d^2u^4$ and $N = d^2v^4$ where (u, v, w) is a Pythagorean triple and d is some non-zero integer.

Now we consider the case where $-M = m^2$ and $N - M = k^2$ (the case where $M - N = k^2$ and $-N = n^2$ is handled similarly). If $Q = (x, y)$ is a point of order 8, then by the discussion above we find that $X(2Q) = m^2+mk$ (by choosing the signs of m and k if necessary). Hence by the proposition we find that m^2+mk, mk, and $mk+k^2$ are all squares if and only if there is such a point Q. Since we may assume that the $\gcd(M, N)$ is square-free, we may also assume that the $\gcd(m, k) = 1$. Since mk is a square, we may assume that both are positive and also that m and k are both squares, say $m = v^2$ and $k = u^2$. Therefore $v^4 + u^2v^2$, u^2v^2, and $u^2v^2 + u^4$ are all squares, which

then implies that $u^2 + v^2 = w^2$. Hence we find that the torsion subgroup is $\mathbb{Z}2 \times \mathbb{Z}8$ when $M = -d^2v^4$ and $N = d^2(u^4 - v^4)$.

• In this case we determine those $E_{\mathbb{Q}}(M, N)$ for which the torsion subgroup is $\mathbb{Z}2 \times \mathbb{Z}6$. To do this use the triplication formula (see [28]) which determines whether or not a point $Q = (x, y)$ has order 3. In the case of $E_{\mathbb{Q}}(M, N)$, it turns out that Q has order 3 if and only if

$$3x^4 + 4(M + N)x^3 + 6MNx^2 - M^2N^2 = 0.$$

As a degree 4 homogeneous polynomial in the variables M, N, and x, it has a rational parametrization (due to Nigel Boston)

$$\frac{M}{x} = (1 + t)^2 - 1, \qquad \frac{N}{x} = \left(1 + \frac{1}{t}\right)^2 - 1.$$

So replacing t by a/b (where $\gcd(a, b) = 1$) we find that

$$\frac{M}{x} = \frac{2ab + a^2}{b^2} \quad \text{and} \quad \frac{N}{x} = \frac{2ab + b^2}{a^2}.$$

By the Nagell–Lutz theorem, we know that x is an integer and from the last two equalities we find that $x = a^2b^2$. Hence $M = 2a^3b+a^4$ and $N = 2ab^3+b^4$. Note that if $a/b \in \{-2, -1, -1/2, 0, 1\}$ then we do not obtain an elliptic curve.

By solving for y in (3) where $x = a^2b^2$, we find that the two order 3 points are

$$(a^2b^2, \pm a^2b^2(a + b)^2). \tag{6}$$

• Since $\mathbb{Z}2\times\mathbb{Z}2$ is always contained in the torsion subgroup of $E_{\mathbb{Q}}(M, N)$, the torsion subgroup (by Mazur's theorem) must be one of $\mathbb{Z}2 \times \mathbb{Z}2, \mathbb{Z}2 \times \mathbb{Z}4, \mathbb{Z}2\times\mathbb{Z}6$, or $\mathbb{Z}2\times\mathbb{Z}8$. Therefore if M and N are distinct non-zero integers which do not occur in the list above, then by process of elimination, the torsion subgroup of $E_{\mathbb{Q}}(M, N)$ must be $\mathbb{Z}2 \times \mathbb{Z}2$. ∎

As an immediate corollary we obtain Main Corollary 1.

Proof of Main Corollary 1. As a consequence of Corollary 2, we see that non-trivial solutions afforded by the torsion subgroup of $E_{\mathbb{Q}}(M, N)$ exist if and only if the torsion subgroup is either $\mathbb{Z}2 \times \mathbb{Z}8$ or $\mathbb{Z}2 \times \mathbb{Z}6$. Moreover, from its proof, we find that in these cases the non-trivial solutions must correspond to the order 4 or 3 torsion points. In each of these cases one may simply plug in the values of M and N into (4), (5), and (6) to obtain the x-coordinates of these points. There is only one positive x-coordinate belonging to order 4 and 3 points, hence there is a unique primitive solution as a consequence of the proof of Corollary 2. ∎

4. Modular forms and quadratic twists of $E_{\mathbb{Q}}(M,N)$. As a consequence of the results in the last section, we see that when the torsion subgroup of $E_{\mathbb{Q}}(M,N)$ is $\mathbb{Z}2\times\mathbb{Z}2$ or $\mathbb{Z}2\times\mathbb{Z}4$, then there are primitive solutions to (1) if and only if the rank of $E_{\mathbb{Q}}(M,N)$ is positive. Moreover, there are infinitely many such primitive solutions for any (M,N) if and only if the rank of $E_{\mathbb{Q}}(M,N)$ is positive.

The *Shimura–Taniyama–Weil Conjecture* (STW) asserts that certain weight 2 newforms correspond to the L-functions of elliptic curves over $\mathbb{Q}$. More precisely, a weak version of the conjecture is:

Conjecture (STW). *If E is an elliptic curve over $\mathbb{Q}$ with conductor N and L-function $L(E,s)=\sum_{n=1}^{\infty}a(n)/n^s$, then the Mellin transform of $L(E,s)$, $f(z)=\sum_{n=1}^{\infty}a(n)q^n$ is a weight 2 newform in $S_2(N,\chi_0)$ where χ_0 is the trivial Dirichlet character* mod N.

If E is a curve for which the STW conjecture holds, then E is known as a *modular elliptic curve*. By the works of Carayol, Eichler, and Shimura it is known that if $f(z)=\sum_{n=1}^{\infty}a(n)q^n$ is a weight 2 newform with integer coefficients with trivial character χ_0, then there exists an elliptic curve E over $\mathbb{Q}$ with $L(E,s)=\sum_{n=1}^{\infty}a(n)/n^s$. Recently Wiles [31] has proven the conjecture for semistable elliptic curves, and Diamond and Kramer [5] have proved the conjecture for curves with full 2-torsion. In particular, if $M\neq N$ are non-zero integers, then $E_{\mathbb{Q}}(M,N)$ is a modular elliptic curve.

By combining B-SD and STW, it turns out that the rank of an elliptic curve over $\mathbb{Q}$ is positive if and only if the special value of a certain modular L-function at $s=1$ is 0. Recently from the works of Kolyvagin, M. R. Murty, V. K. Murty, Bump, Friedberg, and Hoffstein (see [3, 10, 14]) we have:

Theorem 1. *If E is a modular elliptic curve where $L(E,1)\neq 0$, then the rank of E is* 0.

Let ψ be a Dirichlet character mod M and let $f(z)\in S_k(N,\chi)$ with Fourier expansion $f(z)=\sum_{n=1}^{\infty}a(n)q^n$. Then the function $f_\psi(z)$, the *ψ-twist* of $f(z)$, defined by

$$f_\psi(z)=\sum_{n=1}^{\infty}\psi(n)a(n)q^n \tag{7}$$

is also a modular form and is contained in $S_k(NM^2,\chi\psi^2)$. Now we relate these twists when ψ is a quadratic character to the twists of an elliptic curve.

If E is an elliptic curve over $\mathbb{Q}$ given by the equation $y^2=x^3+Ax^2+Bx+C$ and D is a square-free integer, then the equation of its *D-quadratic twist* is

$$Dy^2=x^3+Ax^2+Bx+C.$$

This curve is denoted by E_D. If D is a square-free integer, then the D-quadratic twist of $E_{\mathbb{Q}}(M,N)$ is given by $Dy^2 = x^3 + (M+N)x^2 + MNx$. By multiplying both sides of this model by D^3 and then replacing D^2y by y and Dx by x we find that the D-quadratic twist of $E_{\mathbb{Q}}(M,N)$ is

$$y^2 = x^3 + (DM+DN)x^2 + D^2MNx, \tag{8}$$

the curve $E_{\mathbb{Q}}(DM,DN)$. If $L(E_{\mathbb{Q}}(M,N),s) = \sum_{n=1}^{\infty} a(n)/n^s$ is the L-function for $E_{\mathbb{Q}}(M,N)$, then the L-function for its quadratic twist

$$L(E_{\mathbb{Q}}(DM,DN),s) = \sum_{n=1}^{\infty} a_D(n)q^n$$

is

$$\sum_{n=1}^{\infty} \frac{\chi_D(n)a(n)}{n^s}$$

where $\chi_D(n)$ is the quadratic character for $\mathbb{Q}(\sqrt{D})/\mathbb{Q}$. Specifically this means that for almost all primes p, $a_D(p) = \left(\frac{D}{p}\right)a(p)$ where $\left(\frac{D}{p}\right)$ is the usual Kronecker–Legendre symbol.

Now we briefly describe the theory of half-integral weight modular forms as developed by Shimura. Let N be a positive integer that is divisible by 4. Now define $\left(\frac{c}{d}\right)$ and ε_d by

$$\left(\frac{c}{d}\right) := \begin{cases} -\left(\frac{c}{|d|}\right) & \text{if } c,d<0, \\ \left(\frac{c}{|d|}\right) & \text{otherwise.} \end{cases}$$

$$\varepsilon_d := \begin{cases} 1, & d \equiv 1 \bmod 4, \\ i, & d \equiv 3 \bmod 4. \end{cases}$$

Also let $(cz+d)^{1/2}$ be the principal square root of $(cz+d)$ (i.e. with positive imaginary part). Let χ be a Dirichlet character mod$N$. Then a meromorphic function $f(z)$ on $\mathfrak{H}$ is called a *half-integer weight modular form* if

$$f\left(\frac{az+b}{cz+d}\right) = \chi(d)\left(\frac{c}{d}\right)^{2\lambda+1} \varepsilon_d^{-1-2\lambda}(cz+d)^{\lambda+1/2} f(z)$$

for all $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Gamma_0(N)$. Such a form is called a form with weight $\lambda + 1/2$ and character χ. The set of all such forms that are holomorphic on $\mathfrak{H}$ as well as at the cusps is denoted by $M_{\lambda+1/2}(N,\chi)$ and is a finite-dimensional $\mathbb{C}$-vector space. The set of those $f(z)$ in $M_{\lambda+1/2}(N,\chi)$ that also vanish at the cusps, the cusp forms, is denoted by $S_{\lambda+1/2}(N,\chi)$.

As in the case of integer weight forms, there are Hecke operators that preserve $M_{\lambda+1/2}(N,\chi)$ and $S_{\lambda+1/2}(N,\chi)$. However, for these forms the Hecke operators act on Fourier expansions in square towers; specifically, if p is a

prime, then the Hecke operator T_{p^2} acts on $f(z) \in M_{\lambda+1/2}(N, \chi)$ by

$$f(z)|T_{p^2} := \sum_{n=0}^{\infty} \left(a(p^2 n) + \chi(p) \left(\frac{(-1)^\lambda n}{p} \right) p^{\lambda-1} a(n) + \chi(p^2) p^{2\lambda-1} a(n/p^2) \right) q^n. \tag{9}$$

As in the integer weight case, a form $f(z)$ is called an *eigenform* if for every prime p there exists a complex number λ_p such that

$$f(z)|T_{p^2} = \lambda_p f(z).$$

The canonical example of weight $1/2$ modular forms is

$$\theta(z) := \sum_{n \in \mathbb{Z}} q^{n^2} = 1 + 2q + 2q^4 + 2q^9 + \dots$$

However, this is an example of a more general phenomenon from which many examples of forms are obtained. For example, if $Q(x_1, \dots, x_k)$ is a positive definite quadratic form in k variables then let $r(n, Q)$ denote the number of representations of n by Q. The generating function for $r(n, Q)$ defined by

$$\theta_Q(z) := \sum_{x_1, \dots, x_k \in \mathbb{Z}^k} q^{Q(x_1, \dots, x_k)} \tag{10}$$

is a weight $k/2$ modular form on some congruence group. Here we illustrate how to construct cusp forms using quadratic forms. Two positive definite quadratic forms Q_1 and Q_2 are in the same genus if they are equivalent over $\mathbb{R}$ and over $\mathbb{Z}_p$ for every prime p. Then let $\theta_{Q_1}(z)$ and $\theta_{Q_2}(z)$ be defined as in (10). In [26] Siegel showed that if Q_1 and Q_2 are in the same genus then the function $F(z) := \theta_{Q_1}(z) - \theta_{Q_2}(z)$ is a cusp form.

Specifically, we have the following theorem due to Schoeneberg [22] which explicitly computes the level and character of such cusp forms when there are an even number of variables in the quadratic form.

THEOREM (Schoeneberg). *Let Q be a positive definite quadratic form in $2k$ variables with determinant D and let $\Delta := (-1)^k D$ be its discriminant. If A is the $2k \times 2k$ matrix which represents Q, then let N be the smallest positive integer such that NA^{-1} is an integral matrix with even diagonal entries. Then $\theta_Q(z)$, as defined in* (10), *is in $M_k(2N, \chi)$ where $\chi(n) := \left(\frac{\Delta}{n}\right)$.*

Now equipped with results of Schoeneberg and Siegel we construct three weight $3/2$ eigenforms which are critical to the sequel. We simply searched through a list of reduced ternary quadratic forms and we found the following convenient weight $3/2$ forms, which by the methods of this paper, correspond to elliptic curves with full 2-torsion. The referee has informed us of a paper by Lehman [11] where a systematic version of this method is described. Moreover, there is an explicit table containing all the weight $3/2$ theta series arising from positive definite ternary quadratic forms with level

≤ 100. Consequently, with some routine computation, more cases of Euler's problem may be handled with the results in [11].

PROPOSITION 2. *Let* $Q_1 = x^2 + 2y^2 + 12z^2$, $Q_2 = 2x^2 + 3y^2 + 4z^2$, $Q_3 = x^2 + 2y^2 + 20z^2$, $Q_4 = 2x^2 + 4y^2 + 5z^2$, $Q_5 = x^2 + 7y^2 + 7z^2 - 2yz$, *and* $Q_6 = 3x^2 + 4y^2 + 5z^2 - 4yz$ *and define*

$$f_1(z) := \frac{1}{2}(\theta_{Q_1}(z) - \theta_{Q_2}(z)),$$
$$f_2(z) := \frac{1}{2}(\theta_{Q_3}(z) - \theta_{Q_4}(z)),$$
$$f_3(z) := \frac{1}{2}(\theta_{Q_5}(z) - \theta_{Q_6}(z)).$$

Then as weight $3/2$ *cusp forms we find that* $f_1(z) \in S_{3/2}\big(48, \big(\frac{6}{n}\big)\big)$, $f_2(z) \in S_{3/2}\big(80, \big(\frac{10}{n}\big)\big)$, *and* $f_3(z) \in S_{3/2}\big(192, \big(\frac{3}{n}\big)\big)$.

P r o o f. We prove the proposition for $f_3(z)$, leaving $f_1(z)$ and $f_2(z)$ to the reader. First we note that Q_5 and Q_6 are two ternary quadratic forms which are in the same genus. Hence by Siegel's theorem $f_3(z)$ is a weight $3/2$ cusp form on some congruence subgroup.

Let $\widetilde{Q}_5 = 7y^2+7z^2-2yz$ and $\widetilde{Q}_6 = 4y^2+5z^2-4yz$. Then by Schoeneberg's theorem we find that $\theta_{\tilde{Q}_5}(z) \in M_1\big(192, \big(\frac{-3}{n}\big)\big)$ and $\theta_{\tilde{Q}_6}(z) \in M_1\big(64, \big(\frac{-1}{n}\big)\big)$. It is easy to see that $\theta_{Q_5}(z) = \theta(z)\theta_{\tilde{Q}_5}(z)$ and that $\theta_{Q_6}(z) = \theta(3z)\theta_{\tilde{Q}_6}(z)$. Since $\theta(z) \in M_{1/2}(4, \chi_0)$ and $\theta(3z) \in M_{1/2}\big(12, \big(\frac{3}{n}\big)\big)$, we see that

$$\theta_{Q_5}\left(\frac{az+b}{cz+d}\right) = \left(\frac{c}{d}\right)\varepsilon_d^{-1}\left(\frac{-3}{d}\right)(cz+d)^{3/2}\theta_{Q_5}(z)$$

and

$$\theta_{Q_6}\left(\frac{az+b}{cz+d}\right) = \left(\frac{3}{d}\right)\left(\frac{c}{d}\right)\varepsilon_d^{-1}\left(\frac{-1}{d}\right)(cz+d)^{3/2}\theta_{Q_6}(z)$$

for all $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Gamma_0(192)$. But since $\varepsilon_d^{-2} = \big(\frac{-1}{d}\big)$ we find that $\theta_{Q_5}(z)$ and $\theta_{Q_6}(z)$ are contained in $M_{3/2}\big(192, \big(\frac{3}{n}\big)\big)$, and so $f_3(z) := \frac{1}{2}(\theta_{Q_5}(z) - \theta_{Q_6}(z)) \in S_{3/2}\big(192, \big(\frac{3}{n}\big)\big)$ since Q_5 and Q_6 are in the same genus. ∎

The critical link between the theory of half integer weight modular forms and the integer weight modular forms is the *Shimura lift*. The Shimura lifts are a family of maps which take the L-function of a half-integer weight cusp form and return the L-function of an integer weight modular form. More precisely, let $f(z) = \sum_{n=1}^{\infty} a(n)q^n \in S_{\lambda+1/2}(N, \chi)$ where $\lambda \geq 1$. Define the Dirichlet character ψ by $\psi(d) = \chi(d)\big(\frac{-1}{d}\big)^{\lambda}$. Now define $A(n)$ by the formal product of L-functions

$$\sum_{n=1}^{\infty} \frac{A(n)}{n^s} := L(s - \lambda + 1, \psi) \sum_{n=1}^{\infty} \frac{a(n^2)}{n^s}.$$

Then Shimura proved that the Mellin transform of this product, which we denote by $S(f(z)) = \sum_{n=1}^{\infty} A(n)q^n$, is a weight 2λ modular form. In fact, it is known that $S(f(z)) \in M_{2\lambda}(N/2, \chi^2)$. Furthermore, if $\lambda \geq 2$, then $S(f(z)) \in S_{2\lambda}(N/2, \chi^2)$.

Shimura conjectured that there are formulae involving special values of modular L-functions relating the Fourier coefficients of $f(z)$ with those of $S(f(z))$. First we fix some necessary notation. If $F(z) = \sum_{n=1}^{\infty} A(n)q^n$ is a modular form, then its L-function $L(F, s)$ is defined by

$$L(F, s) = \sum_{n=1}^{\infty} \frac{A(n)}{n^s}.$$

Now if ψ is a Dirichlet character and if $F_\psi(z) = \sum_{n=1}^{\infty} \psi(n)A(n)q^n$ is the ψ-twist of $F(z)$, then we let $L(F, \psi, s)$ denote the modular L-function for $F_\psi(z)$.

In [30] Waldspurger proved this conjecture explicitly. For our purposes we use:

THEOREM (Waldspurger). *Let $f(z) \in S_{\lambda+1/2}(N, \chi)$ be an eigenform of the Hecke operators T_{p^2} such that $S(f(z)) = F(z) \in S_{2\lambda}^{\text{new}}(M, \chi^2)$ for an appropriate positive integer M. Denote their respective Fourier expansions by $f(z) = \sum_{n=1}^{\infty} a(n)q^n$ and $F(z) = \sum_{n=1}^{\infty} A(n)q^n$. Let n_1 and n_2 be two positive square-free integers such that $n_1/n_2 \in \mathbb{Q}_p^{\times 2}$ for all $p \,|\, N$. Then*

$$a^2(n_1)L\left(F, \left(\frac{-1}{n}\right)^{\lambda} \chi^{-1}\chi_{n_2}, \lambda\right)\chi(n_2/n_1)n_2^{\lambda-1/2} = a^2(n_2)L\left(F, \left(\frac{-1}{n}\right)^{\lambda} \chi^{-1}\chi_{n_1}, \lambda\right)n_1^{\lambda-1/2}. \tag{11}$$

By combining Waldspurger's theorem with B-SD we find that we can determine whether or not the ranks of certain twists of an elliptic curve over $\mathbb{Q}$ are positive.

THEOREM 2. *Let E be a modular elliptic curve over $\mathbb{Q}$ with $L(E, s) = \sum_{n=1}^{\infty} A(n)/n^s$. Let $f(z) = \sum_{n=1}^{\infty} a(n)q^n \in S_{3/2}\left(N, \left(\frac{d}{n}\right)\right)$ be an eigenform of the Hecke operators T_{p^2} such that $S(f(z)) = F(z) = \sum_{n=1}^{\infty} A(n)q^n$. Now let n_1 be a positive square-free integer such that $a(n_1) \neq 0$ and such that $L(E_{-dn_1}, 1) \neq 0$. Suppose that n_2 is a positive square-free integer such that $n_1/n_2 \in \mathbb{Q}_p^{\times 2}$ for every prime $p \,|\, N$. If $a(n_2) \neq 0$, then the rank of E_{-dn_2} is unconditionally 0. If $a(n_2) = 0$, then assuming B-SD the rank of E_{-dn_2} is positive.*

P r o o f. In (11) we now substitute 1 for λ and replace χ by $\left(\frac{d}{n}\right)$. Then by solving for $L\left(F, \left(\frac{-dn_2}{n}\right), 1\right)$ we obtain

$$L\left(F, \left(\frac{-dn_2}{n}\right), 1\right) = \frac{a^2(n_2)L\left(F, \left(\frac{-dn_1}{n}\right), 1\right)\sqrt{n_1}}{\sqrt{n_2}a^2(n_1)}.$$

Since E is a modular elliptic curve corresponding to the weight 2 newform $F(z)$, we find that

$$L(E_{-dn_2}, 1) = \frac{a^2(n_2)L(E_{-dn_1}, 1)\sqrt{n_1}}{\sqrt{n_2}a^2(n_1)}.$$

So by hypothesis we find that $L(E_{-dn_2}, 1) = 0$ if and only if $a(n_2) = 0$. If $a(n_2) \neq 0$, then by Theorem 1 we find that the rank of E_{-dn_2} is unconditionally 0. If $a(n_2) = 0$, then by B-SD the rank of E_{-dn_2} is positive. ∎

We now prove Main Theorem 2.

P r o o f o f M a i n T h e o r e m 2. We now prove Main Theorem 2 which contains explicit examples of the above theorem. Using the cusp forms $f_1(z)$, $f_2(z)$ and $f_3(z)$ from Proposition 2, let $S(f_i(z)) = \sum_{n=1}^{\infty} A_i(n)q^n$ for $1 \leq i \leq 3$. For example, we found that

$$\begin{aligned} S(f_1(z)) &= q - q^3 - 2q^5 + q^9 + 4q^{11} - 2q^{13} + 2q^{15} + 2q^{17} + \dots \\ &= \eta(2z)\eta(4z)\eta(6z)\eta(12z) \end{aligned}$$

and

$$\begin{aligned} S(f_3(z)) &= q + q^3 - 2q^5 + q^9 - 4q^{11} - 2q^{13} - 2q^{15} + 2q^{17} + \dots \\ &= \frac{\eta^4(4z)\eta^4(12z)}{\eta(2z)\eta(6z)\eta(8z)\eta(24z)}. \end{aligned}$$

In fact, it should be noted that $S(f_3(z))$ is $S(f_1(z))$ twisted by the quadratic character $\left(\frac{-1}{n}\right)$, which implies that the corresponding curves are twists of each other by $D = -1$.

Since the Hecke operators T_{p^2} and T_p commute with the Shimura lift and the images $S(f_i(z))$ are all weight 2 newforms, it follows that all three weight 3/2 forms are eigenforms.

We find that $S(f_1(z)) \in S_2^{\text{new}}(24, \chi_0), S(f_2(z)) \in S_2^{\text{new}}(40, \chi_0)$, and $S(f_3(z)) \in S_2^{\text{new}}(48, \chi_0)$. In these cases the weight 2 newforms correspond to certain $E_{\mathbb{Q}}(M, N)$. Since elliptic curves with conductor 24, 40, and 48 are all modular, it is easy to verify that the $L(E_{\mathbb{Q}}(M, N), s)$ are the Mellin transforms of the $S(F_i(z))$.

The pairs (M, N) for which $L(E_{\mathbb{Q}}(M, N), s)$ corresponds to $S(f_1(z))$ are $(-4, -3)$, $(-1, 3)$, $(1, 4)$, $(-1, -9)$, $(-8, 1)$, and $(8, 9)$. Those corresponding to $S(f_2(z))$ are $(-5, -1)$, $(-4, 1)$, and $(4, 5)$, and those corresponding to

$S(f_3(z))$ are $(-4,-1)$, $(-3,1)$, $(3,4)$, $(-9,-8)$, $(-1,8)$, and $(1,9)$. By Theorems 1 and 2 and since the coefficient of q^n in $f_i(z)$ is $\frac{1}{2}(r(n,Q_{2i-1}) - r(n,Q_{2i}))$ by Proposition 2 we obtain the main result. ∎

We immediately obtain Main Corollary 2 by the following computations.

Proof of Main Corollary 2. Since the torsion subgroups (by Main Theorem 1) are not $\mathbb{Z}2 \times \mathbb{Z}8$ nor $\mathbb{Z}2 \times \mathbb{Z}6$, we only need to determine the ranks of the relevant curves. By the last theorem, we only need to look for square-free positive integers n_1 in each arithmetic progression which satisfy the hypotheses of the last theorem. We check these case by case.

• In the first case one can check that the conditions of Main Theorem 2 are satisfied by $n_1 = 1, 3, 5, 7, 57, 35, 13, 39, 17, 67, 93$, and 23, and they are the representatives for the odd arithmetic progressions $\bmod 24$ in increasing order by residue class.

• In the second case the hypotheses of Main Theorem 2 are satisfied by $n_1 = 1, 3, 5, 7, 11, 13, 55, 17, 61, 145, 31$, and 195. The arithmetic progressions come in pairs and hence we only need one representative for each pair.

• In the third case the conditions of the theorem are satisfied by $n_1 = 1, 3, 5, 57, 11, 37, 17, 19$, and 21. These are representatives for the odd arithmetic progressions $\bmod 24$ (except those that are $7 \bmod 8$) in increasing order by residue class. We note that for every non-negative integer n

$$r(8n+7, x^2+7y^2+7z^2-2yz) = r(8n+7, 3x^2+4y^2+5z^2-4yz)$$

hence the conditions of the theorem are not satisfied for the arithmetic progression $7 \bmod 8$. ∎

We now show how one may use results like Main Theorem 2 to establish the existence of infinitely many quadratic twists of certain curves with rank 0. Using impressive analytic estimates on certain special values of modular L-functions, L. Mai and M. R. Murty [12] proved that a modular elliptic curve E has infinitely many quadratic twists by $D \equiv 1 \bmod 4N$, where N is the conductor of E, with rank 0. Here we show that this is indeed the case in the families of quadratic twists in Main Corollary 2. To do this we will use the theory of modular forms with complex multiplication as developed by Hecke and Serre. The author developed two other elementary methods of guaranteeing the existence of rank 0 quadratic twists in [15, 16]. In fact, in [16] it is shown that for some elliptic curves E there exists a set S of primes with density $1/3$ for which the D-twist of E has rank 0 provided that all the prime factors of D are in S.

First we give essential preliminaries and definitions regarding modular forms with complex multiplication. Let $K = \mathbb{Q}(\sqrt{-d})$ be an imaginary quadratic field with integer ring O_K with discriminant $-D$. A Hecke Grössencharakter ϕ of weight $k \geq 2$ with conductor Λ, an ideal in O_K, is a

group homomorphism from $I(\Lambda)$, the group of fractional ideals prime to Λ, to $\mathbb{C}^\times$ satisfying

$$\phi(\alpha O_K) = \alpha^{k-1} \quad \text{when } \alpha \equiv 1 \bmod \Lambda.$$

Given such a ϕ, define a formal power series $\Psi(z)$ in $q = e^{2\pi i z}$ by

$$\Psi(z) := \sum_{\mathfrak{a}} \phi(\mathfrak{a}) q^{N(\mathfrak{a})},$$

where the sum is taken over all integral ideals $\mathfrak{a}$ prime to Λ and $N(\mathfrak{a})$ is the ideal norm of $\mathfrak{a}$ in O_K. The function $\Psi(z)$ is a newform in $S_k^{\text{new}}\big(DN(\Lambda), \big(\frac{-d}{n}\big)\frac{\phi(nO_K)}{n^{k-1}}\big)$. Such forms are known as modular forms with *complex multiplication.* Using these definitions we find that if

$$\Psi(z) = \sum_{n=1}^{\infty} a(n) q^n,$$

then for every prime p where $\big(\frac{-d}{p}\big) = -1$ we have $a(p) = 0$ (then there are no ideals of norm p). These are the *inert* primes of K.

Now introduce the notion of a lacunary modular form. Suppose that $f(z) = \sum_{n=1}^{\infty} a(n)q^n \in M_k(N, \chi)$ for some positive integers k and N and some suitable Dirichlet character χ. The form $f(z)$ is called *lacunary* if almost all of the Fourier coefficients $a(n)$ are zero. In this setting we take "almost all" to mean that $a(n) = 0$ on a subset of the positive integers with density one. In [23], Serre proved that such a form $f(z)$ is lacunary if and only if $f(z)$ is expressible as a finite linear combination of modular forms with complex multiplication.

We now use these ideas to prove Main Theorem 3.

Proof of Main Theorem 3. First we recall the following fact concerning the restriction of the Fourier expansion of an integer weight modular form to an arithmetic progression.

Lemma 1. *Let $f(z) = \sum_{n=0}^{\infty} a(n)q^n$ be a modular form in $M_k(N, \chi)$ and let $d := \gcd(r, t)$. If $0 \le r < t$, then*

$$f_{r,t}(z) = \sum_{n \equiv r \bmod t} a(n) q^n$$

is the Fourier expansion of a modular form in $M_k(Nt^2/d)$.

Define

$$F_1(z) := f_1(z)\theta(24z) = \sum_{n=1}^{\infty} A_1(n) q^n, \quad F_2(z) := f_2(z)\theta(40z) = \sum_{n=1}^{\infty} A_2(n) q^n,$$

and

$$F_3(z) := f_3(z)\theta(24z) = \sum_{n=1}^{\infty} A_3(n)q^n.$$

It is easily verified that $F_1(z) \in S_2(192, \chi_0), F_2(z) \in S_2(160, \chi_0)$, and $F_3(z) \in S_2(192, \chi_0)$. Let $a_i(n)$ $(1 \le i \le 3)$ denote the Fourier coefficients of $f_i(z)$.

By (9), it is clear that the Hecke operators T_{p^2} act on $a_i(n)$, in square towers. In other words, if n is a positive square-free integer, then $a_i(nm^2)$ is uniquely determined by $a_i(n)$ and the eigenvalues for T_{p^2} for primes $p \,|\, m$. In fact, it is easy to verify that if $a_i(n) = 0$, then $a_i(nm^2) = 0$ for every non-zero integer m.

Let $F_{1,r}(z)$ be the weight 2 cusp form defined by

$$F_{1,r}(z) := \sum_{n \equiv r \bmod 24} A_1(n)q^n.$$

By Lemma 1, it is clear that $F_{1,r}(z)$ is a weight 2 modular form (in fact, a cuspidal one) with respect to the congruence subgroup $\Gamma_0(24^2 \cdot 96)$. It is easy to verify that if n is a square-free integer such that $nm^2 \equiv r \bmod 24$ and m is prime to 6, then $n \equiv r \bmod 24$.

Let $1 \le r \le 24$ be a positive odd integer. Suppose that there are only finitely many square-free positive integers $n \equiv r \bmod 24$ such that $a_1(n) \neq 0$, say $n_1, \dots, n_{t_r}$. So by the definition of $F_1(z)$, we find that

$$F_{1,r}(z) = \Big(\sum_{i=1}^{t_r} \sum_{\gcd(m,24)=1} a_1(n_i m^2) q^{n_i m^2} \Big) \Big(\sum_{n \in \mathbb{Z}} q^{24n^2} \Big).$$

Since the set of positive integers that are represented by any binary quadratic form has density zero in the set of non-negative integers, we find that $F_{1,r}(z)$ is a lacunary modular form. Hence by Serre's theorem it must be the case that $F_{1,r}(z)$ is a finite linear combination of complex multiplication modular forms of weight 2. Since $F_{1,r}(z)$ has level $24^2 \cdot 96 = 2^{11}3^3$ and the discriminants of the CM fields divide the level, the only imaginary quadratic fields whose Hecke Grössencharakters can occur in this linear combination are $\mathbb{Q}(i), \mathbb{Q}(\sqrt{-2}), \mathbb{Q}(\sqrt{-3})$, and $\mathbb{Q}(\sqrt{-6})$.

Now if there exists a prime p which is inert in each of these fields such that the coefficient $A_1(pm) \neq 0$ where $pm \equiv r \bmod 24$ and $\gcd(p, m) = 1$, then $F_{1,r}(z)$ cannot be a linear combination of such CM forms. This follows from the fact that the coefficients in every newform are multiplicative and there are no ideals with norm p in any of these fields. It is impossible for any of the CM forms in the linear combination to have a non-zero coefficient associated with the exponent pm. The smallest prime which is inert in each of these fields is $p = 23$. For $r = 1$ it turns out that $A_1(23 \cdot 71) = -16 \neq 0$. Hence $F_{1,1}(z)$ is not a linear combination of CM forms, hence it is not

lacunary. This contradicts the assumption that there are only finitely many square-free positive integers $n \equiv 1 \bmod 24$ such that $a_1(n) \neq 0$. Hence there are infinitely many n such that $a_1(n) \neq 0$, and by Main Corollary 2 this implies that the given pairs (M, N) of integers are rank 0 quadratic twists. For $r = 3, 5, 7, 9, 11, 13, 15, 17, 19, 21$, and 23 we find that $A_1(987) = -16$, $A_1(437) = 16$, $A_1(391) = 8$, $A_1(345) = -8$, $A_1(299) = -8$, $A_1(253) = -16$, $A_1(207) = 4$, $A_1(713) = -32$, $A_1(115) = -8$, $A_1(69) = 4$, and $A_1(23) = 4$ respectively. All of these indices contain either 23, 47, or 71 as a simple prime factor and all three primes are inert in all four quadratic imaginary fields. All of these coefficients are non-zero, which shows that none of the $F_{1,r}(z)$ are lacunary, thereby contradicting the assumption that there are only finitely many square-free positive integers $n \equiv r \bmod 24$ where $a_1(n) \neq 0$.

In the second case, suppose that there are only finitely many square-free positive integers $n \equiv r$ or $9r \bmod 40$ such that $a_2(n) \neq 0$, say $n_1, \ldots, n_{t_r}$. It is easy to verify that if $nm^2 \equiv r$ or $9r \bmod 40$ where n is square-free, then $n \equiv r$ or $9r \bmod 40$. Hence if we define $F_{r,9r}(z)$ by

$$F_{r,9r}(z) = \sum_{n \equiv r, 9r \bmod 40} A_2(n) q^n,$$

then $F_{r,9r}(z)$ is a weight 2 cusp form with respect to the group $\Gamma_0(40^2 \cdot 160)$ and by hypothesis satisfies

$$F_{r,9r}(z) = \Big(\sum_{i=1}^{t_r} \sum_{\gcd(m,40)=1} a_2(n_i m^2) q^{n_i m^2} \Big) \Big(\sum_{n \in \mathbb{Z}} q^{40n^2} \Big).$$

Again as in the first case we find that $F_{r,9r}(z)$ is a lacunary modular form and hence it is a finite linear combination of CM forms with respect to $\mathbb{Q}(i)$, $\mathbb{Q}(\sqrt{-2})$, $\mathbb{Q}(\sqrt{-5})$, and $\mathbb{Q}(\sqrt{-10})$. However, we find that $A_2(1209) = 32$, $A_2(923) = 8$, $A_2(1085) = 8$, $A_2(527) = -8$, $A_2(651) = -24$, $A_2(213) = 24$, $A_2(775) = 4$, $A_2(217) = -8$, $A_2(341) = -8$, $A_2(1065) = -24$, $A_2(31) = 4$, and $A_2(355) = -4$. All of these coefficients are non-zero and they cover all pairs of residue classes r, $9r \bmod 40$ with r odd. Since all the exponents above contain either 31 or 71 as simple factors and they are inert in all four quadratic imaginary fields, it is not the case that any of the $F_{r,9r}(z)$ are finite linear combinations of CM forms. Hence by Serre's theorem none of them are lacunary; therefore if $1 \leq r \leq 40$ is odd, then there are infinitely many square-free integers $n \equiv r$ or $9r \bmod 40$ for which the relevant $E_{\mathbb{Q}}(M, N)$ twisted by n has rank 0.

In the third case for $1 \leq r \leq 24$ odd, we define

$$F_{3,r}(z) = \sum_{n \equiv r \bmod 24} A_3(n) q^n.$$

If there are only finitely many square-free positive integers $n \equiv r \bmod 24$ such that $a_3(n) \neq 0$, say $n_1, \dots, n_{t_r}$, then $F_{3,r}(z)$ has the following factorization:

$$F_{3,r}(z) = \Big(\sum_{i=1}^{t_r} \sum_{\gcd(m,24)=1} a_3(n_i m^2) q^{n_i m^2} \Big) \Big(\sum_{n \in \mathbb{Z}} q^{24n^2} \Big).$$

So $F_{3,r}(z)$ is a lacunary weight 2 cusp form with respect to the group $\Gamma_0(24^2 \cdot 96)$. Hence by Serre's theorem, $F_{3,r}(z)$ is a finite linear combination of CM forms with respect to $\mathbb{Q}(i)$, $\mathbb{Q}(\sqrt{-2})$, $\mathbb{Q}(\sqrt{-3})$, and $\mathbb{Q}(\sqrt{-6})$. For $r = 1, 3, 5, 9, 11, 13, 17, 19$, and 21 we find that $A_3(1081) = 16$, $A_3(483) = 16$, $A_3(437) = -16$, $A_3(345) = -8$, $A_3(851) = 32$, $A_3(805) = 48$, $A_3(161) = -8$, $A_3(115) = -16$, and $A_3(69) = -4$ respectively. All of these coefficients are non-zero and these indices all contain at least one of 23 or 47, primes that are inert in each of these four quadratic imaginary fields, as simple prime factors. As in the previous two cases, if $r = 1, 3, 5, 9, 11, 13, 17, 19$, or 21, then there are infinitely many square-free positive integers $n \equiv r \bmod 24$ such that the quadratic twist of $E_{\mathbb{Q}}(M, N)$ by n has rank 0. ∎

5. Simultaneous Pellian equations. Let M and N be distinct positive integers. In this section we investigate the existence of simultaneous non-trivial integer solutions (a, b, c) to the pair of Pellian equations

$$a^2 - Mb^2 = 1 \quad \text{and} \quad c^2 - Nb^2 = 1. \tag{12}$$

Such a solution (a, b, c) is called *non-trivial* if $b \neq 0$. Using the methods developed by Schmidt [20, 21], Schlickewei [19] proved that the number of simultaneous integer solutions (a, b, c) to (12) is $\ll 4 \cdot 8^{2^{78}}$. In recent work by Masser and Rickert [13], this bound has been lowered to 132, and M. Bennett has informed me that he [2] has lowered this bound to 28.

The aim of this section is to show that there are several infinite families of such systems where one may deduce the non-existence of non-trivial solutions to (12) by simply computing the number of representations of certain integers by pairs of ternary quadratic forms.

We first prove the following elementary proposition.

LEMMA 2. *If M and N are distinct positive integers and (a, b, c) is a non-trivial solution to* (12), *then $(x, y) = (1/b^2, ac/b^3)$ is a point of infinite order on the elliptic curve $E_{\mathbb{Q}}(M, N)$. In particular, if $E_{\mathbb{Q}}(M, N)$ has rank* 0, *then there are no non-trivial solutions to* (12).

Proof. Suppose that (a, b, c) is a non-trivial solution to (12). It is easy to see that $1 + Mb^2 = a^2$ and $1 + Nb^2 = c^2$. Therefore $(x, y, t, z) = (1, b, a, c)$ is a non-trivial solution to (1). It is easy to see that this implies that

$$a^2 c^2 = 1 + (M + N)b^2 + MNb^4,$$

which after multiplying through by $1/b^6$ becomes

$$\frac{a^2c^2}{b^6} = \frac{1}{b^6} + \frac{M+N}{b^4} + \frac{MN}{b^2}.$$

Hence $(x, y) = (1/b^2, ac/b^3)$ is a rational point on $E_{\mathbb{Q}}(M, N)$. Moreover, by the Lutz–Nagell theorem [7, Theorem 5.1], since the coordinates of torsion points are integers, we may assume that $b = \pm 1$.

By Main Corollary 1, the primitive solutions (x, y, t, z) to (12) afforded by the torsion points of $E(M, N)$ are completely classified. It is a straightforward exercise to deduce that $(1/b^2, ac/b^3)$ is not any of the torsion points found in the proof of Main Theorem 1. ∎

We immediately obtain the following as a consequence of Lemma 2, Corollary 1, and Main Corollary 2.

Main Corollary 3. *Let d be any non-zero integer.*

(i) *Let n be an odd positive square-free integer and suppose that $(M, N) = (2d^2n, d^2n)$. If $2r(n, 2x^2 + y^2 + 32z^2) \neq r(n, 2x^2 + y^2 + 8z^2)$, then there are no non-trivial solutions to* (12).

(ii) *Let n be an even positive square-free integer and suppose that $(M, N) = (2d^2n, d^2n)$. If $2r(n/2, 4x^2 + y^2 + 32z^2) \neq r(n/2, 4x^2 + y^2 + 8z^2)$, then there are no non-trivial solutions to* (12).

(iii) *Let n be an odd positive square-free integer and suppose that $(M, N) = (24d^2n, 18d^2n)$ or $(6d^2n, 54d^2n)$. If $r(n, x^2 + 2y^2 + 12z^2) \neq r(n, 2x^2 + 3y^2 + 4z^2)$, then there are no non-trivial solutions to* (12).

(iv) *Let n be an odd positive square-free integer and suppose that $(M, N) = (50d^2n, 10d^2n)$. If $r(n, x^2 + 2y^2 + 20z^2) \neq r(n, 2x^2 + 4y^2 + 5z^2)$, then there are no non-trivial solutions to* (12).

(v) *Let $n \not\equiv 7 \bmod 8$ be an odd positive square-free integer for which $(M, N) = (12d^2n, 3d^2n)$ or $(27d^2n, 24d^2n)$. If $r(n, x^2 + 7y^2 + 7z^2 - 2yz) \neq r(n, 3x^2 + 4y^2 + 5z^2 - 4yz)$, then there are no non-trivial primitive solutions to* (12).

Remark. In [18] Rickert proves that there are no non-trivial solutions to (12) where $M = 2$ and $N = 3$. By the above proposition, it is easy to obtain this result because $E(2, 3)$ is a rank 0 elliptic curve.

Acknowledgements. The author thanks Michael Bennett, Nigel Boston, David Bradley, Darrin Doud, and Kevin James for their help during the preparation of this manuscript. He especially thanks Kevin for correcting some errors which appeared in earlier versions of this manuscript. The author is also indebted to the referee for doing an exceptional job.

References

[1] E. T. Bell, *The problems of congruent numbers and concordant forms*, Proc. Amer. Acad. Sci. 33 (1947), 326–328.

[2] M. Bennett, private communication.

[3] D. Bump, S. Friedberg and J. Hoffstein, *Nonvanishing theorems for L-functions of modular forms and their derivatives*, Invent. Math. 102 (1990), 543–618.

[4] J. Coates and A. Wiles, *On the conjecture of Birch and Swinnerton-Dyer*, ibid. 39 (1977), 223–251.

[5] F. Diamond and K. Kramer, *Modularity of a family of elliptic curves*, Math. Res. Lett. 2 (3) (1995), 299–304.

[6] L. Euler, *De binis formulis speciei* $xx + myy$ *et* $xx + nyy$ *inter se concordibus et disconcordibus*, Opera Omnia Series 1 vol. 5 (1780), 48–60, Leipzig–Berlin–Zürich, 1944.

[7] D. Husemöller, *Elliptic Curves*, Springer, New York, 1987.

[8] A. Knapp, *Elliptic Curves*, Princeton Univ. Press, 1992.

[9] N. Koblitz, *Introduction to Elliptic Curves and Modular Forms*, Springer, 1984.

[10] V. A. Kolyvagin, *Finiteness of* $E(\mathbb{Q})$ *and the Tate–Shafarevich group of* $E(\mathbb{Q})$ *for a subclass of Weil curves*, Izv. Akad. Nauk SSSR Ser. Mat. 52 (1988), 522–540 (in Russian).

[11] J. Lehman, *Levels of positive definite ternary quadratic forms*, Math. Comp. 58, 197 (1992), 399–417.

[12] L. Mai and M. R. Murty, *A note on quadratric twists of an elliptic curve*, in: Elliptic Curves and Related Topics, CRM Proc. Lecture Notes, Amer. Math. Soc., 1994, 121–124.

[13] D. Masser and J. Rickert, *Simultaneous Pell equations*, J. Number Theory, to appear.

[14] M. R. Murty and V. K. Murty, *Mean values of derivatives of modular L-series*, Ann. of Math. 133 (1991), 447–475.

[15] K. Ono, *Rank zero quadratic twists of modular elliptic curves*, Compositio Math., to appear.

[16] —, *Twists of elliptic curves*, Compositio Math., to appear.

[17] T. Ono, *Variations on a Theme of Euler*, Plenum, New York, 1994.

[18] J. Rickert, *Simultaneous rational approximations and related Diophantine equations*, Math. Proc. Cambridge Philos. Soc. 113 (1993), 461–472.

[19] H. P. Schlickewei, *The number of subspaces occurring in the p-adic subspace theorem in Diophantine approximation*, J. Reine Angew. Math. 406 (1990), 44–108.

[20] W. M. Schmidt, *Norm form equations*, Ann. of Math. 96 (1972), 526–551.

[21] —, *Diophantine Approximations*, Lecture Notes in Math. 785, Springer, 1980.

[22] B. Schoeneberg, *Das Verhalten von mehrfachen Thetareihen bei Modulsubstitutionen*, Math. Ann. 116 (1939), 511–523.

[23] J.-P. Serre, *Divisibilité de certaines fonctions arithmétiques*, Enseign. Math. 22 (1976), 227–260.

[24] G. Shimura, *Introduction to the Arithmetic Theory of Automorphic Functions*, Princeton Univ. Press, 1971.

[25] —, *On modular forms of half-integral weight*, Ann. of Math. 97 (1973), 440–481.

[26] C. Siegel, *Über die analytische Theorie der quadratischen formen*, in: Gesammelte Abhandlungen, Bd. 3, Springer, 1966, 326–405.

[27] J. Silverman, *The Arithmetic of Elliptic Curves*, Springer, New York, 1986.

[28] J. Silverman and J. Tate, *Rational Points on Elliptic Curves*, Springer, New York, 1992.

[29] J. Tunnell, *A classical Diophantine problem and modular forms of weight* $\frac{3}{2}$, Invent. Math. 72 (1983), 323–334.

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

[31] A. Wiles, *Modular elliptic curves and Fermat's Last Theorem*, Ann. of Math. 141 (1995), 443–551.

School of Mathematics
Institute for Advanced Study
Princeton, New Jersey 08540
U.S.A.
E-mail: ono@math.ias.edu

Department of Mathematics
Penn State University
University Park, Pennsylvania 16802
U.S.A.
E-mail: ono@math.psu.edu

Received on 16.10.1995
and in revised form on 11.3.1996 (2878)