Compositio Mathematica **106:** 349–360, 1997.

Twists of elliptic curves

K. ONO*
School of Mathematics, Institute for Advanced Study, Princeton, New Jersey 08540, USA
e-mail:onomath.ias.edu
Department of Mathematics, Penn State University, University Park, Pennsylvania 16802, USA
e-mail:onomath.psu.edu

Received: 14 November 1995; accepted in final form 16 March 1996

Abstract. If E is an elliptic curve over $\mathbb{Q}$, then let $E(D)$ denote the $D-$quadratic twist of E. It is conjectured that there are infinitely many primes p for which $E(p)$ has rank 0, and that there are infinitely many primes ℓ for which $E(\ell)$ has positive rank. For some special curves E we show that there is a set S of primes p with density $\frac{1}{3}$ for which if $D = \Pi p_j$ is a squarefree integer where $p_j \in S$, then $E(D)$ has rank 0. In particular $E(p)$ has rank 0 for every $p \in S$. As an example let E_1 denote the curve

$$E_1 : y^2 = x^3 + 44x^2 - 19360x + 1682384.$$

Then its associated set of primes S_1 consists of the prime 11 and the primes p for which the order of the reduction of $X_0(11)$ modulo p is odd. To obtain the general result we show for primes $p \in S$ that the rational factor of $L(E(p), 1)$ is nonzero which implies that $E(p)$ has rank 0. These special values are related to surjective $\mathbb{Z}/2\mathbb{Z}$ Galois representations that are attached to modular forms. Another example of this result is given, and we conclude with some remarks regarding the existence of positive rank prime twists via polynomial identities.

Mathematics Subject Classifications (1991): Primary 14H52; Secondary 11G05.

Key words: Elliptic curves, modular forms.

1. Introduction

Let E be an elliptic curve over $\mathbb{Q}$ with the given Weierstrass equation

$$E\colon\ y^2 = x^3 + ax^2 + bx + c, \tag{1}$$

where a, b and c are integers. In this paper all curves and their points are assumed to be $\mathbb{Q}-$rational. If D is a squarefree integer, then let $E(D)$ denote the $D-$quadratic twist of E that is given by

$$E(D)\colon\ y^2 = x^3 + aDx^2 + bD^2x + cD^3. \tag{2}$$

Recently there have been a number of investigations regarding the distribution of ranks of elliptic curves in various families. For instance one may consult the works

* The author is supported by NSF grants DMS-9508976 and DMS-9304580.

of Brumer–McGuiness, Goldfeld, Gouvêa–Mazur, Lieman, Mestre, Mai–Murty, Ono, and Stewart–Top [2, 3, 8, 9, 14, 15, 16, 17, 19, 25].

In this paper we examine the following conjecture that was brought to the author's attention by J. Silverman.

CONJECTURE 1. If E is an elliptic curve, then there are infinitely many primes p for which $E(p)$ has rank 0, and there are infinitely many primes ℓ for which $E(\ell)$ has positive rank.

In this direction there are a number of results deduced from an analysis of 2-descents (see [22]) that confirm part of this conjecture for the *congruent number* curve

$$E'\colon\ y^2 = x^3 - x.$$

For instance it is known that if $p \equiv 3 \pmod 8$ is prime, then $E'(p)$ has rank 0. As another example if $p \equiv 5 \pmod 8$ is prime, then $E'(2p)$ has rank 0.

2. New examples

Using a completely different method we prove part of this conjecture for certain special elliptic curves. For these curves we show that there are infinitely many primes p for which $E(p)$ has rank 0, and we also obtain a surprising multiplicative property. We show the existence of a set S of primes p with density $\frac{1}{3}$ with the special property that if $D = \Pi_j p_j$ is a squarefree integer where $p_j \in S$, then $E(D)$ has rank 0.

In the case of the congruent number curve E', there are similar results for integers with few prime factors. For instance, again using a careful analysis of 2-descents [22], it is known that E'_{pqr} has rank 0 if p, q, and r are primes satisfying

$$p \equiv 1 \pmod 8, \qquad q \equiv 3 \pmod 8, \qquad r \equiv 3 \pmod 8, \quad \text{and}$$

$$\left(\frac{p}{q}\right) = -\left(\frac{p}{r}\right).$$

We recall some essential facts. Throughout this note we let q denote the uniformizing variable $q := e^{2\pi i z}$ where $\mathrm{Im}(z) > 0$, and all integer weight newforms will be normalized eigenforms of all the Hecke operators. For every integer weight newform $f(z) = \Sigma_{n=1}^{\infty} a(n) q^n \in S_k(N, \chi)$ with rational integer coefficients, there exists a Galois representation ρ_f (see [6,7])

$$\rho_f\colon\ \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\mathbb{Z}/2\mathbb{Z})$$

with the property that if $p \nmid 2N$ is prime, then

$$\mathrm{tr}(\rho_f(\mathrm{Frob}_p)) \equiv a(p) \pmod 2.$$

https://doi.org/10.1023/A:1000191408511 Published online by Cambridge University Press

We shall make use of such representations.

We also make use of Shimura's theory of half-integral weight modular forms, a theory that we now briefly describe (see [23]). Let N be a positive integer that is divisible by 4 and define $(\frac{c}{d})$ and ϵ_d by

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

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

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 modulo N. Then a meromorphic function $g(z)$ on $\mathfrak{H} = \{\mathrm{Im}(z) > 0\}$ is called a *half integer weight modular form* with *Nebentypus* χ and weight $\lambda + \frac{1}{2}$ if

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

for all

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0(N).$$

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 forms a finite dimensional $\mathbb{C}-$vector space. The subspace of those $g(z)$ 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 $M_{\lambda+\frac{1}{2}}(N,\chi)$ and $S_{\lambda+\frac{1}{2}}(N,\chi)$. However for these forms the Hecke operators act on Fourier expansions in square towers; specifically if $p \nmid N$ is a prime, then the Hecke operator T_{p^2} acts on $g(z) = \Sigma_{n=1}^{\infty} b(n)q^n \in M_{\lambda+\frac{1}{2}}(N,\chi)$ by

$$g(z) \mid T_{p^2}$$

$$:= \sum_{n=0}^{\infty} (b(p^2 n) + \chi(p)\left(\frac{(-1)^{\lambda} n}{p}\right) p^{\lambda-1} b(n) + \chi(p^2) p^{2\lambda-1} b(n/p^2))q^n.$$

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

$$g(z) \mid T_{p^2} = \lambda_p g(z).$$

https://doi.org/10.1023/A:1000191408511 Published online by Cambridge University Press

The connection between half integer weight forms and the integer weight modular forms are the *Shimura lifts,* a family of maps which takes the L-function of a half integer weight cusp form and returns the L-function of an integer weight modular form. More precisely let $g(z) = \Sigma_{n=1}^{\infty} b(n)q^n \in S_{\lambda+(1/2)}(N, \chi)$ where $\lambda \geq 1$. Let t be a positive square-free integer and define the Dirichlet character ψ_t by $\psi_t(n) = \chi(n)(\frac{(-1)^{\lambda}}{n})(\frac{t}{n})$. Now define $A_t(n)$ by the formal product of L-functions

$$\sum_{n=1}^{\infty} \frac{A_t(n)}{n^s} := L(s - \lambda + 1, \psi_t) \sum_{n=1}^{\infty} \frac{b(tn^2)}{n^s}.$$

Then Shimura proved that the Mellin transform of this product, which we denote by $\mathrm{SH}_t(g(z)) = \Sigma_{n=1}^{\infty} A_t(n)q^n$ is a weight 2λ modular form in $M_{2\lambda}(N/2, \chi^2)$. Furthermore if $\lambda \geq 2$, then $\mathrm{SH}_t(g(z))$ happens to be a cusp form.

Now we define the notation that is used in Theorem 1. Let E be a modular elliptic curve with conductor N whose Hasse-Weil L-function is given by

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

In particular this implies that there is a weight 2 newform $F(z) = \Sigma_{n=1}^{\infty} A(n)q^n \in S_2(N, \chi_1)$ where χ_1 is the trivial Dirichlet character modulo N.

Now suppose that for some positive integer M there exists a cusp form $g(z) = \Sigma_{n=1}^{\infty} b(n)q^n \in S_{3/2}(M, (\frac{d}{\cdot}))$ that is an eigenform of the Hecke operators T_{p^2} for which the image of $g(z)$ under the Shimura lift is $F(z)$. Now let S denote the set of primes p for which $b(p)$ is odd. With this notation we prove the following theorem.

THEOREM 1. *Using the notation above, suppose there exists an integer weight newform $f(z) = \Sigma_{n=1}^{\infty} a(n)q^n$ with rational integer coefficients whose residual $\mathbb{Z}/2\mathbb{Z}$-Galois representation ρ_f is surjective and whose Fourier expansion satisfies*

$$f(z) \equiv g(z) \pmod 2.$$

Furthermore suppose that for every squarefree integer n_2 for which $b(n_2)$ is odd there exists a squarefree integer n_1, where $(n_1/n_2) \in \mathbb{Q}_p^{\times 2}$ for every prime $p \mid M$, with the property that

$$L(E(-dn_1), 1) \cdot b(n_1) \neq 0.$$

If $D = \Pi_j p_j$ is a squarefree integer with $p_j \in S$, then $E(-dD)$ has rank 0. *Moreover S has density $\frac{1}{3}$.*

Proof. From the works of Bump–Friedberg–Hoffstein, Coates–Wiles, Kolyvagin, and Murty–Murty, Waldspurger's theorem [26] implies the following theorem.

https://doi.org/10.1023/A:1000191408511 Published online by Cambridge University Press

THEOREM. *Let E' be a modular elliptic curve over $\mathbb{Q}$ with $L(E', s) = \Sigma_{n=1}^{\infty} A(n)/n^s$. Let $g(z) = \Sigma_{n=1}^{\infty} b(n)q^n \in S_{3/2}(M, (\frac{d}{\cdot}))$ be an eigenform of the Hecke operators T_{p^2} such that $SH_1(g(z)) = F(z) = \sum_{n=1}^{\infty} A(n)q^n$. Now let Let n_1 be a positive squarefree integer such that $b(n_1) \neq 0$ and such that $L(E'_{-dn_1}, 1) \neq 0$. Suppose that n_2 is a positive squarefree integer such that $n_1/n_2 \in \mathbb{Q}_p^{\times 2}$ for every prime $p \mid M$. If $b(n_2) \neq 0$, then the rank of E'_{-dn_2} is unconditionally 0.*

With this theorem, if $p \in S$, then since $b(p) \equiv a(p) \pmod 2$ is odd (hence is nonzero), it follows that $E(-dp)$ has rank 0. Moreover by multiplicativity of the Fourier coefficients of newforms, it follows that

$$a(m)a(n) = a(mn)$$

if $\gcd(m, n) = 1$. Therefore we find that if $D = \Pi_i p_i$ is a squarefree integer where $p_i \in S$, then $a(D) \equiv b(D) \equiv 1 \pmod 2$ and hence $E(-dD)$ has rank 0.

To complete the proof we need to establish that S has density $\frac{1}{3}$. Since $a(n) \equiv b(n) \pmod 2$ for all n, we simply need to examine the coefficients $a(p)$ when p is prime. The Galois representation ρ_f

$$\rho_f : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\mathbb{Z}/2\mathbb{Z})$$

has the property that

$$\mathrm{tr}(\rho_f(\mathrm{Frob}_p)) \equiv a(p) \pmod 2$$

for all but finitely many primes. However $\mathrm{GL}_2(\mathbb{Z}/2\mathbb{Z}) = \mathrm{PGL}_2(\mathbb{Z}/2\mathbb{Z})$ is isomorphic to S_3, and since ρ_f is surjective, we find by Chebotarev's density theorem that the set of primes p for which $\mathrm{tr}(\rho_f(\mathrm{Frob}_p)) \equiv 1 \pmod 2$, those primes where the image has order 3, has density $\frac{1}{3}$. □

Before we give some immediate corollaries, we should mention that it is not apparent how often the above theorem applies. Although it is true that this theorem is easy to apply in practice, it is not clear how often the hypotheses of the theorem are satisfied. The author is inclined to believe that this phenomenon is very common, but he does not see how to quantify this assertion.

Before we mention corollaries, we define some relevant partition functions that are similar to those that have occurred in other settings [1]. Let $e_1(n)$ (resp. $e_2(n)$) denote the number of two colored partitions of n into an even number of parts where the parts of the first color are distinct even integers (resp. multiples of 6) and the parts of the second color are distinct multiples of 22 (resp. 18). Similarly let $o_1(n)$ (resp. $o_2(n)$) denote the number of two colored partitions of n into an odd number of parts where the parts of the first color are distinct even integers (resp. multiples of 6) and the parts of the second color are distinct multiples of 22 (resp. 18). Define the two partition functions $a_1(n)$ and $a_2(n)$ by

$$a_1(n) := e_1(n-1) - o_1(n-1),$$
$$a_2(n) := e_2(n-1) - o_2(n-1).$$

https://doi.org/10.1023/A:1000191408511 Published online by Cambridge University Press

The generating functions for $a_1(n)$ are $a_2(n)$ are

$$\begin{aligned}\sum_{n=1}^{\infty} a_1(n)q^n &= q\prod_{n=1}^{\infty}(1-q^{2n})(1-q^{22n})\\ \sum_{n=1}^{\infty} a_2(n)q^n &= q\prod_{n=1}^{\infty}(1-q^{6n})(1-q^{18n}).\end{aligned} \tag{3}$$

Recalling that Dedekind's eta function $\eta(z)$ is a weight $\frac{1}{2}$ cusp form given by the infinite product

$$\eta(z) := q^{1/24}\prod_{n=1}^{\infty}(1-q^n),$$

we find that

$$\eta(2z)\eta(22z) = \sum_{n=1}^{\infty} a_1(n)q^n$$

$$\eta(6z)\eta(18z) = \sum_{n=1}^{\infty} a_2(n)q^n.$$

COROLLARY 1. *Let E_1 denote the elliptic curve given by*

$$E_1\colon\ y^2 = x^3 + 44x^2 - 19360x + 168234.$$

If D is a squarefree integer for which $a_1(D)$ is odd, then $E_1(D)$ has rank 0. *Moreover the set S_1 of primes p for which $a_1(p)$ is odd has density $\frac{1}{3}$.*

Proof. It turns out that the modular form $f(z) = \eta(2z)\eta(22z) \in S_1(44, (-11/\cdot))$ is a newform. Therefore it follows from the theory of Hecke operators that if m and n are relatively prime positive integers, then

$$a_1(m)a_1(n) = a_1(mn). \tag{4}$$

By Euler's Pentagonal number theorem we find that

$$\begin{aligned}\eta(2z)\eta(22z) &= \sum_{n=1}^{\infty} a_1(n)q^n\\ &= q\left(\sum_{k\in\mathbb{Z}}(-1)^k q^{3k^2+k}\right)\cdot\left(\sum_{j\in\mathbb{Z}}(-1)^j q^{33j^2+11j}\right).\end{aligned}$$

https://doi.org/10.1023/A:1000191408511 Published online by Cambridge University Press

As a consequence we find that $a_1(n) = 0$ if $n \equiv 2, 6, 7, 8, 10 \pmod{11}$. Therefore the Galois representation ρ_f attached to $\eta(2z)\eta(22z)$ satisfies

$$\mathrm{tr}(\rho_f(\mathrm{Frob}_p)) \equiv a_1(p) \equiv 0 \pmod{2}.$$

for at least half the primes. Therefore since the image of ρ_f is a subgroup of S_3, by the Chebotarev density theorem the representation ρ_f is surjective if there exists a single odd prime $p \neq 11$ for which $a_1(p)$ is odd. Since $a_1(5)$ is odd, it follows that ρ_2 is surjective and the set of primes p for which $a_1(p)$ is odd has density $\frac{1}{3}$.

Now define the weight $\frac{3}{2}$ cusp form $g(z)$ by

$$g(z) := \sum_{n=1}^{\infty} b_1(n)q^n = f(z)\Theta(z)$$

$$= \left(\sum_{n=1}^{\infty} a_1(n)q^n\right) \cdot \left(1 + 2q + 2q^4 + 2q^9 + \cdots\right).$$

By (5) we find that $a_1(n) \equiv b_1(n) \pmod{2}$ for all n. Moreover $g(z)$ is an eigenform of the Hecke operators T_{p^2} and its image of under the Shimura correspondence is $F(z) = \Sigma_{n=1}^{\infty} A(n)q^n = \eta^2(z)\eta^2(11z)$ which is a newform in $S_2(11, \chi_1)$ where χ_1 is the trivial character. Therefore it follows that the Hasse-Weil $L-$function of $X_0(11)$ is given by

$$L(X_0(11), s) = \sum_{n=1}^{\infty} \frac{A(n)}{n^s}.$$

One can easily verify that E_1 is the -11-quadratic twist of the elliptic curve $X_0(11)$ given by

$$y^2 + y = x^3 - x^2 - 10x - 20.$$

By the multiplicativity of $a_1(n)$, it follows that if m and n are relatively prime positive integers for which $b_1(m)$ and $b_1(n)$ are odd, then $b_1(mn)$ is also odd. Therefore with a little computation this completes the proof of the corollary. □

COROLLARY 2. *Let E_2 denote the elliptic curve given by*

$$E_2 \colon\ y^2 = x^3 - 432.$$

If $D > 1$ is a squarefree integer for which $a_2(D)$ is odd, then $E_2(D)$ has no nontrivial rational points. Moreover the set S_2 of primes p for which $a_2(p)$ is odd has density $\frac{1}{3}$.

https://doi.org/10.1023/A:1000191408511 Published online by Cambridge University Press

Proof. This proof is similar to the proof of Corollary 1. It turns out that $f(z) = \eta(6z)\eta(18z) = \Sigma_{n=1}^{\infty} a_2(n)q^n \in S_1(108, (-3/\cdot))$ is a newform. The representation ρ_f is also surjective following a similar argument to the one given in Corollary 1.

The weight $\frac{3}{2}$ cusp form $g(z) \in S_{3/2}(108, (3/\cdot)$ defined by

$$g(z) := \sum_{n=1}^{\infty} b_2(n)q^n = \eta(6z)\eta(18z)\Theta(z)$$

$$= \left(\sum_{n=1}^{\infty} a_2(n)q^n\right) \cdot \left(1 + 2q + 2q^4 + \ldots\right)$$

is almost an eigenform of the Hecke operators. If $g_0(z) := g(z) \,|T_{25} = 6q^2 + 6q^5 - 6q^8 - \ldots$, then $G(z) := g(z) - \frac{1}{3}g_0(z)$ is an eigenform of all the Hecke operators and its image under the Shimura lift is $\eta^2(3z)\eta^2(9z)$, a weight 2 newform in $S_2(27, \chi_1)$. Fortunately it turns out that $g_0(z) \equiv 0 \pmod 6$, and so $G(z) \equiv g(z) \pmod 2$. As in the proof of Corollary 1, we find that $a_2(n) \equiv b_2(n) \pmod 2$ for all n. However if $\eta^2(3z)\eta^2(9z) = \sum_{n=1}^{\infty} A(n)q^n$, then

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

where E can be taken to be the CM elliptic curve with conductor 27 given by

$$E\colon\ y^2 = x^3 + 16.$$

It is easy to verify that E_2 is the -3-quadratic twist of E. As in Corollary 1, one may check that the hypotheses in Theorem 1 are satisfied; therefore if D is a squarefree integer for which $a_2(D)$ is odd, then $b_2(D)$ is odd and $E(-3D) = E_2(D)$ has rank 0. Since it is well known that for all such $D > 1$, the torsion group is trivial, the result now follows. □

We now mention the following interesting corollary that gives an elliptic curve description of the sets S_1 and S_2. If E is an elliptic curve and p is a prime, then let $|E(\mathbb{Z}/p\mathbb{Z})|$ denote the number of rational points of the reduction of E modulo p.

COROLLARY 3. *The sets of primes S_1 and S_2 satisfy*

$$S_1 = \{11\} \cup \{\text{primes } p \text{ where } |X_0(11)(\mathbb{Z}/p\mathbb{Z})| \text{ is odd}\}$$

$$S_2 = \{\text{primes } p \text{ where } |E(\mathbb{Z}/p\mathbb{Z})| \text{ is odd}\}$$

where E is the elliptic curve given by

$$E:\ \ y^2 = x^3 + 16.$$

https://doi.org/10.1023/A:1000191408511 Published online by Cambridge University Press

Proof. By the fact that $(1 - X^n)^2 \equiv (1 - X^{2n}) \pmod 2$, we find that

$$\eta(2z)\eta(22z) = \sum_{n=1}^{\infty} a_1(n)q^n \equiv \eta^2(z)\eta^2(11z) \pmod 2,$$

$$\eta(6z)\eta(18z) = \sum_{n=1}^{\infty} a_2(n)q^n \equiv \eta^2(3z)\eta^2(9z) \pmod 2.$$

Recall from the proofs of Corollaries 1 and 2 that $\eta^2(z)\eta^2(11z)$ and $\eta^2(3z)\eta^2(9z)$ are the Mellin transforms of $L(X_0(11), s)$ and $L(E, s)$ respectively.

If p is a prime for which $X_0(11)$ has good reduction, then

$$a_1(p) \equiv p + 1 - |X_0(11)(\mathbb{Z}/p\mathbb{Z})| \pmod 2.$$

Hence if p is a prime for which $X_0(11)$ has good reduction, then $p \in S_1$, if and only if $|X_0(11)(\mathbb{Z}/p\mathbb{Z})|$ is odd. Since $X_0(11)$ only has bad reduction at $p = 11$, a brief computation shows that 11 is also in S_1. Exactly the same argument holds for S_2. □

Remark 1. By the theory of lacunary modular forms, it follows that the set of positive integers for which $a_i(n) = 0$ has arithmetic density 1.

Remark 2. If $D = \Sigma_j p_j$ is a square-free integer where $p_j \in S_i$, then assuming the conjecture of Birch and Swinnerton Dyer it can be shown that the order of the Tate–Shafarevich group of $E_i(D)$ is, up to small scalar factors, (coming from the local Tamagawa numbers) $b_i^2(D)$. Since the $b_i(D)$ are themselves values of special partition functions, is there a combinatorial realization of elements of the Tate-Shafarevich groups of these twists analogous to the combinatorial realizations of certain ideal class groups in [20]?

Remark 3. The methods used here also will give nonvanishing quadratic twists of more generic modular $L-$functions at the central critical value.

3. Further remarks

In this section we make some remarks concerning prime twists of elliptic curves. First we recall the following conjecture of Bouniakowsky [21].

CONJECTURE [Bouniakowsky's] *Let $F(x)$ be an irreducible polynomial over $\mathbb{Q}$ with integer coefficients for which the only positive integer n dividing all $F(k)$ for every integer k is $n = 1$. Then there exist infinitely many positive integers m for which $F(m)$ is prime.*

As a consequence of this conjecture we obtain:

https://doi.org/10.1023/A:1000191408511 Published online by Cambridge University Press

THEOREM 2. *Let E be an elliptic curve given by the Weierstrass equation*

$$E\colon\ y^2 = x^3 + ax^2 + bx + c,$$

where a, b, and c are integers that do not satisfy both

$$a + b \equiv 1 \pmod 2,$$

$$a \equiv c \equiv 0 \pmod 3 \quad \text{and} \quad b \equiv 2 \pmod 3.$$

Assuming Bouniakowsky's conjecture, if E is an elliptic curve with no rational points of order 2, then there exists infinitely many primes p for which $E(p)$ has positive rank.

Proof. If we define polynomials $X(u), Y(u)$, and $D(u)$ by

$$\begin{aligned} X(u) &:= u^4 - 2bu^2 - 8cu + (b^2 - 4ac), \\ Y(u) &:= u^6 + 2au^5 + 5bu^4 + 20cu^3 - 5(b^2 - 4ac)u^2 \\ &\quad + (8a^2c - 2ab^2 - 4bc)u - (b^3 - 4abc + 8c^2), \\ D(u) &:= 4(u^3 + au^2 + bu + c), \end{aligned}$$

then we find that

$$Y^2(u) = X^3(u) + aD(u)X^2 + bD^2(u)X + cD^3(u).$$

This identity is a special case of Legendre's identity that is the topic in [10]. Therefore for every integer u the point $(X(u), Y(u))$ lies on $E(D(u))$. By Bouniakowsky's conjecture there exists infinitely many positive integers u for which $D(u)/4$ is prime. Since $E(D(u))$ is isomorphic to $E(D(u)/4)$ over $\mathbb{Q}$, it suffices to show that for all but finitely many integers u that the point $(X(u), Y(u))$ has infinite order. However by Mazur's theorem, if $(X(u), Y(u))$ has finite order, then its order must be $2, 3, 4, \ldots, 9, 10$ or 12. However by the doubling formulas if this point has finite order, then the polynomials $X(u)$ and $Y(u)$ must satisfy a finite number of polynomial equations. Therefore there are at most finitely many integers u for which $(X(u), Y(u))$ has finite order. □

Assuming a reformulation of Bouniakowsky's conjecture, one can deduce that there are infinitely many primes p for which $E(p)$ has positive rank. However since his conjecture seems well beyond current techniques it does not seem reasonable to do so.

It is interesting to note that the strongest results in the direction of Bouniakowshy's conjecture imply the existence of infinitely many positive rank cubic twists of certain elliptic curves where the twisting factor is at most a product of two primes. Assuming the conjectures of Birch and Swinnerton Dyer, it is known that there are

infinitely many primes p for which $p-$cubic twists of certain elliptic curves have positive rank. If c is a nonzero integer, then let E'_c denote the elliptic curve with complex multiplication by $\mathbb{Q}(\sqrt{-3})$ defined by

$$E'_c\colon\ y^2 = x^3 + c. \tag{5}$$

If D is a cube free integer, then the *cubic twist* of E'_c is E'_{D^2c} and is given by

$$y^2 = x^3 + cD^2.$$

THEOREM 3. *If c is an odd integer that is not a perfect square, then there exist infinitely many integers D that are at most the product of two primes for which E'_{cD^2} has positive rank.*

Proof. If $D(u) := u^2 - c$, then it turns out that the point $(D(u), uD(u))$ is a point on the elliptic curve $E'_{cD^2(u)}$, the $D(u)$-cubic twist of the elliptic curve E'_c.

By Iwaniec's theorem [11] since $D(u)$ is irreducible over $\mathbb{Q}$ and c is odd, there are infinitely many integers u for which $D(u)$ is at most the product of two primes. By the same argument that appeared in the proof of Theorem 2, there are at most finitely many integers u for which the point $(D(u), uD(u))$ has finite order. □

Acknowledgements

I thank E. Bombieri, H. Darmon, A. Granville, D. Lieman, V.K. Murty, C. Pomerance, and J. Silverman for their helpful comments during the preparation of this paper.

References

1. G. Andrews, *The Theory of Partitions*, Addison-Wesley, 1976.
2. A. Brumer, *The average rank of elliptic curves* I, *Inventiones Math.* 109 (1992), 445–472.
3. A. Brumer and O. McGuinness, *The behaviour of the Mordell–Weil group of elliptic curves*, Bull. Amer. Math. Soc. 23 (1990) 375–382.
4. D. Bump, S. Friedberg and J. Hoffstein *Nonvanishing theorems for L-functions of modular forms and their derivatives*, Inventiones Math. 102 (1990), 543–618.
5. J. Coates and A. Wiles, *On the conjecture of Birch and Swinnerton–Dyer*, Inventiones Math. 39 (1977), 223–251.
6. P. Deligne, *Formes modulaires et représentations ℓ-adiques*, Sem. Bourbaki, exposé 355, Springer Lect. Notes. Math. 179, Springer-Verlag, Berlin (1969), 139–172.
7. P. Deligne and J.-P. Serre, *Formes modulaires de poids 1*, Ann. Scient. École Normale Sup. 4^e série t.7 (1974), 507–530.
8. D. Goldfeld, *Conjectures on elliptic curves over quadratic fields*, Number Theory (Proc. Conf. in Carbondale), Ed. M. Nathanson, Springer Lect. Notes. Math. 751 (1979), 108–118.
9. F. Gouvêa and B. Mazur, *The square-free sieve and the rank of elliptic curves*, J. Amer. Math. Soc. 4 (1991), 1–23.
10. L. Guo and K. Ono, *Legendre and elliptic curves*, preprint.
11. H. Iwaniec, *Almost primes represented by quadratic polynomials*, Inventiones Math. 47 (1978), 171–188.
12. N. Koblitz, *Introduction to elliptic curves and modular forms*, Springer-Verlag, 1984.

13. V. A. Kolyvagin, *Finiteness of $E(\mathbb{Q})$ and the Tate–Shafarevich group of $E(\mathbb{Q})$ for a subclass of Weil curves (Russian)*, Izv. Akad. Nauk, USSR, ser. Matem. 52 (1988).
14. D. Lieman, *Nonvanishing of L-series associated to cubic twists of elliptic curves*, Annals of Math. 140 (1994) 81–108.
15. L. Mai, *The analytic rank of a family of elliptic curves*, Can. J. Math. 45 (1993), 847–862.
16. L. Mai and R. Murty, *A note on quadratic twists of an elliptic curve*, Elliptic curves and related topics, CRM Proc. Lect. Notes, Ed. H. Kisilevsky and M. R. Murty 4 (1994), 121–124.
17. J.-F. Mestre, *Rang de courbes elliptiques d'invariant donné*, C.R. Acad. Sci. Paris Sér. I Math. 314, no. 12 (1992) 919–922.
18. M. R. Murty and V. K. Murty, *Mean values of derivatives of modular $L-$series*, Annals of Math. 133 (1991), 447–475.
19. K. Ono, Rank zero quadratic twists of modular elliptic curves, *Compositio Math*. 104 (1996), 293–304.
20. K. Ono and L. Sze, *$4-$cores, characters of finite general linear groups, and class numbers*, Acta Arith., to appear.
21. P. Ribenboim, *The little book of big primes*, Springer–Verlag, New York, 1991.
22. P. Serf, *Congruent numbers and elliptic curves*, Computational Number Theory, Proc. Colloq., Debrecen, Walter de Gruyter, Berlin (1991), 227–238.
23. G. Shimura, *On modular forms of half-integral weight*, Ann. Math. 97 (1973), 440–481.
24. J. Silverman, *The arithmetic of elliptic curves*, Springer-Verlag, New York, 1986.
25. 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.
26. J. L. Waldspurger, *Sur les coefficients de Fourier des formes modulaires de poids demi-entier*, J. Math. Pures et Appl. 60 (1981), 375–484.