Hindawi Publishing Corporation
Journal of Numbers
Volume 2014, Article ID 825634, 5 pages
http://dx.doi.org/10.1155/2014/825634

Hindawi

Research Article

On the Equation $y^2 = x^3 - pqx$

Iftikhar A. Burhanuddin[1] and Ming-Deh A. Huang[2]

[1] *Adobe Research India Lab, Bangalore, Karnataka, India*
[2] *Department of Computer Science, University of Southern California, Los Angeles, CA 90089-0781, USA*

Correspondence should be addressed to Iftikhar A. Burhanuddin; iftikhar.burhanuddin@gmail.com

Received 4 May 2014; Accepted 1 July 2014; Published 16 July 2014

Academic Editor: Cheon S. Ryoo

We consider certain quartic twists of an elliptic curve. We establish the rank of these curves under the Birch and Swinnerton-Dyer conjecture and obtain bounds on the size of Shafarevich-Tate group of these curves. We also establish a reduction between the problem of factoring integers of a certain form and the problem of computing rational points on these twists.

1. Introduction

In this paper, we investigate certain quartic twists of the elliptic curve $y^2 = x^3 - x$ and present some of their interesting properties. Specifically, we consider the family of elliptic curves $E_D : y^2 = x^3 - Dx$, where $D = pq$ with p and q distinct prime numbers, $p \equiv q \equiv 3 \bmod 16$. These elliptic curves have complex multiplication by $\mathbb{Q}(i)$. The 2-torsion point $(0, 0)$ generates the torsion subgroup of the Mordell-Weil group $E_D(\mathbb{Q})$. Our first result concerns the rank of $E_D(\mathbb{Q})$ and an interesting valuational property of points in $E_D(\mathbb{Q})$. More specifically we obtain the following.

Theorem 1. *Let $E_D : y^2 = x^3 - Dx$, where $D = pq$ with p and q distinct prime numbers and $p \equiv q \equiv 3 \bmod 16$. Then the rank of the Mordell-Weil group $E_D(\mathbb{Q})$ is less than or equal to 1. If the rank is one, then for every point R of $E_D(\mathbb{Q})$ which is not in $\langle (0,0) \rangle + 2E_D(\mathbb{Q})$, the p-adic and q-adic valuations of $x(R)$ must have opposite parity. Moreover, under the Birch and Swinnerton-Dyer conjecture, the rank of $E_D(\mathbb{Q})$ is one.*

The situation where p and q do not satisfy the congruence condition in Theorem 1 is less clear. Recently Li and Zeng [1] showed, under the Birch and Swinnerton-Dyer conjecture, that, for $D = pq$ where p and q are distinct odd primes, there exists an elliptic curve $E_{2rD} : y^2 = x^3 - 2rDx$, where r depends on the classes of p and q modulo 8, such that the elliptic curve has rank 1 and the valuations at p and q of x-coordinate $x([k]Q)$ are not equal for odd k, where Q is a generator of the Mordell-Weil group $E_{2rD}(\mathbb{Q})$.

By assuming conjectures, in addition to the Birch and Swinnerton-Dyer conjecture, we also obtain the following.

Theorem 2. *Let $E_D : y^2 = x^3 - Dx$, where $D = pq$ with p and q distinct prime numbers and $p \equiv q \equiv 3 \bmod 16$. Then the following holds under the Birch and Swinnerton-Dyer conjecture, the elliptic curve analog of the Brauer-Siegel theorem, and the Hardy-Littlewood's F conjecture. For every $\epsilon > 0$ there are infinitely many E_D with $D = pq$ and p and q prime with $p \equiv q \equiv 3 \bmod 16$, such that $\#Ш(E_D) \gg |\Delta(E_D)|^{1/12-\epsilon}$, where $Ш(E_D)$ is the Shafarevich-Tate group of E_D and $\Delta(E_D)$ is the minimal discriminant of E_D.*

Let E be an elliptic curve over $\mathbb{Q}$. The naïve height of the elliptic curve is defined to be

$$h^*(E) = \frac{1}{12} \log \max \left\{ \left| c_4(E) \right|^3, \left| c_6(E) \right|^2 \right\}, \tag{1}$$

where $c_4(E)$ and $c_6(E)$ are the c-invariants associated to a minimal model of E.

Let F vary over a family of number fields of a fixed extension degree over $\mathbb{Q}$. Let Δ_F, h_F, and R_F denote, respectively, the discriminant, the class number, and the regulator of F. The Brauer-Siegel theorem [2] states that if $|\Delta_F|$ tends to infinity then $\log h_F R_F \sim \log |\Delta_F|^{1/2}$. The elliptic curve analog of the Brauer-Siegel Theorem [3] asserts that, for a family

of elliptic curves defined over a fixed number field K such that the height $h^*(E)$ tends to infinity, $\log(\#Ш(E)\mathrm{Reg}(E)) \sim h^*(E)$.

The Hardy and Littlewood conjecture F [4] concerns polynomials of the form ax^2+bx+c, where a, b, c are integers and a is positive. It asserts that if the greatest common divisor of the coefficients is 1 and b^2-4ac is not a square, and either $a+b$ or c is odd, then asymptotically, the number $P(n)$ of primes less than n of the form ax^2+bx+c is given by $\lambda(\sqrt{n}/\sqrt{a}\log n)$, where λ is a constant depending only on a, b, c.

The curve E_D has $y^2=x^3-Dx$ as a minimal model, with discriminant $\Delta = 64D^3$ and naïve height $h^* = (1/4)\log 48D = (1/12)\log|\Delta| + (1/4)\log 12$. The elliptic analog of Brauer-Siegel implies that $\#Ш \ll |\Delta|^{1/12+\epsilon}$, and Theorem 2 implies that the bound is essentially tight.

We remark that a result of de Weger [5] demonstrates that for every $\epsilon > 0$ there exist infinitely many elliptic curves of rank 0 with

$$\#Ш(E) \gg |\Delta(E)|^{1/12-\epsilon}, \tag{2}$$

assuming the BSD conjecture in the rank 0 case and a conjecture of Shintani and Shimura that the Riemann hypothesis holds for the Ranking-Selberg zeta function associated to the weight 3/2 modular form associated to an elliptic curve by the Shintani-Shimura lift.

The result was improved in [6] where it was shown that, for every $\epsilon > 0$, there are infinitely many elliptic curves E of rank 0 such that

$$\#Ш(E) \gg |\Delta(E)|^{(1/2)-\epsilon} \tag{3}$$

assuming the BSD conjecture in the rank 0 case and the conjecture of Shintani and Shimura.

The proof of Theorem 1 is given in Section 2. The proof of Theorem 2 is given in Section 3. By Theorem 1, any point R of the Mordell-Weil group $E_D(\mathbb{Q})$ which is not in $\langle(0,0)\rangle + 2E_D(\mathbb{Q})$ must behave differently with respect to p-adic and q-adic valuations. This sets the stage for reductions between the problem of factoring integers of the form D and the problem of computing nontorsion rational points on E_D. This is discussed in Section 4. In one direction, it is shown that how given a rational nontorsion point P, the factors p and q of D can be found in time polynomial in the height of P. We note that the cases where E_D have rational points of small height are those that give rise to large Shafarevich-Tate groups (see Section 3).

2. Proof of Theorem 1

This section is devoted to the proof of Theorem 1. Part of the analysis closely follows Sections X.6 and X.4.9 from Silverman's book [7]. First we recall some facts that follow as the exposition in Example X.4.8 and Proposition X.4.9 applies to our situation. We also adopt the notation there.

Let E_D over $\mathbb{Q}$ be the elliptic curve

$$E_D : y^2 = x^3 - Dx, \tag{4}$$

where $D \in \mathbb{Z}$ (the subscript D will be dropped when it is clear from the context). Then E_D is isogenous to the elliptic curve

$$E'_D : Y^2 = X^3 + 4DX \tag{5}$$

via the isogeny $\phi : E_D \to E'_D, (x,y) \mapsto (y^2/x^2, -y(D+x^2)/x^2)$. The kernel $E[\phi]$ of ϕ consists of $(0,0)$ and O, the identity of E_D. Let $\widehat{\phi} : E'_D \to E_D$ be the dual isogeny of ϕ.

Let $M_{\mathbb{Q}}$ be the set of primes of $\mathbb{Z}$ and ∞. Let $S \subset M_{\mathbb{Q}}$ that consists of ∞ and all primes dividing 2 or D. Let $\mathbb{Q}_\nu$ denote the completion of $\mathbb{Q}$ with respect to the absolute value associated to $\nu \in S$. In particular, $\mathbb{Q}_\infty$ denotes $\mathbb{R}$ and for $\nu \in S \setminus \{\infty\}$, $\mathbb{Q}_\nu$ denotes the ν-adic numbers. Let $\mathbb{Q}(S,2)$ be the subgroup of $\mathbb{Q}^*/\mathbb{Q}^{*2}$ defined as follows:

$$\mathbb{Q}(S,2) := \left\{ b \in \frac{\mathbb{Q}^*}{\mathbb{Q}^{*2}} \mid \nu(b) \equiv 0 \bmod 2,\ \forall \nu \notin S \right\}. \tag{6}$$

Now let $D = pq$, where p and q are odd and distinct primes, and the group $\mathbb{Q}(S,2)$ is generated by -1, 2, p and q.

Let $\mathrm{WC}(E)$ denote the Weil-Châtelet group of E, the group of equivalence classes of homogeneous spaces for E over $\mathbb{Q}$. For each $d \in \mathbb{Q}(S,2)$, the corresponding homogeneous spaces $C_d \in \mathrm{WC}(E)$ and $C'_d \in \mathrm{WC}(E')$, also referred to as quartics, are given by the equations

$$\begin{aligned} C_d &: dw^2 = d^2 + 4pqz^4, \\ C'_d &: dW^2 = d^2 - pqZ^4. \end{aligned} \tag{7}$$

Identifying $E[\phi]$ with μ_2, we have $H^1(G_{\mathbb{Q}}, E[\phi]) \cong \mathbb{Q}^*/\mathbb{Q}^{*2}$, under which the ϕ-Selmer group can be viewed as a subset of $\mathbb{Q}(S,2)$ as follows:

$$S^{(\phi)}(E) \cong \left\{ d \in \mathbb{Q}(S,2) : C_d(\mathbb{Q}_\nu) \neq \emptyset,\ \forall \nu \in S \right\}. \tag{8}$$

The $\widehat{\phi}$-Selmer group $S^{(\widehat{\phi})}(E')$ has an analogous isomorphism where C_d is replaced by C'_d.

There is the well-known exact sequence:

$$0 \longrightarrow \frac{E'(\mathbb{Q})}{\phi(E(\mathbb{Q}))} \longrightarrow S^{(\phi)}(E) \longrightarrow Ш\left(\frac{E}{\mathbb{Q}}\right)[\phi] \longrightarrow 0, \tag{9}$$

where the map $E'(\mathbb{Q})/\phi(E(\mathbb{Q})) \to S^{(\phi)}(E)$ is defined through the connecting homomorphism $\delta : E'(\mathbb{Q}) \to H^1(G_{\mathbb{Q}}, E[\phi])$ with $\delta(E'(\mathbb{Q})) \subset S^{(\phi)}(E)$. Under the isomorphism $H^1(G_{\mathbb{Q}}, E[\phi]) \cong \mathbb{Q}^*/\mathbb{Q}^{*2}$ we have $\delta(0,0) = 4D$ and $\delta(x,y) = x$ if $x \neq 0, \infty$.

Similarly there is an injection $f : E(\mathbb{Q})/\widehat{\phi}(E'(\mathbb{Q})) \to S^{(\widehat{\phi})}(E')$ sending $(0,0)$ to $-16D$ and (x,y) to x if $x \neq 0, \infty$.

Thus, the images of $(0,0)$, the 2-torsion point of $E'(\mathbb{Q})$, and $E(\mathbb{Q})$ in the Selmer groups are given by

$$pq \in S^{(\phi)}(E), \qquad -pq \in S^{(\widehat{\phi})}\left(E'\right), \tag{10}$$

respectively.

We now restrict our attention to

$$E = E_D : y^2 = x^3 - Dx, \tag{11}$$

where $D = pq$ and p and q are distinct primes such that $p \equiv q \equiv 3 \bmod 16$. Also swapping p and q if necessary we have $(p/q) = (-q/p) = 1$.

Below is a descent analysis on the 2-isogenous elliptic curves E and E'. We would like to thank an anonymous referee for valuable suggestions, which we adopt here. Our original analysis can be found in [8, Appendix B].

When $K = \mathbb{Q}$ or $\mathbb{Q}_\nu$, we have an injection

$$f : \frac{E(K)}{\widehat{\phi}(E'(K))} \longrightarrow \frac{K^*}{K^{*2}} \tag{12}$$

induced from the connecting homomorphism $\delta : E'(K) \to H^1(G_K, E[\phi]) \cong K^*/K^{*2}$ sending $(0,0)$ to $-16D$ and (x, y) to x if $x \neq 0, \infty$. When $K = \mathbb{Q}_\nu$, we write $S^{(\widehat{\phi})}(K)$ for the actual image of f. By virtue of the exact sequence

$$0 \longrightarrow \frac{E'(K)}{\phi(E(K))} \longrightarrow H^1\left(G_K, E[\phi]\right) \longrightarrow \mathrm{WC}(E)[\phi] \longrightarrow 0 \tag{13}$$

it follows that $S^{(\widehat{\phi})}(E')$ consists of $a \in \mathbb{Q}(S, 2)$ with localizations in $S^{(\widehat{\phi})}(\mathbb{Q}_\nu)$ for all ν.

Suppose $P \in E(\mathbb{Q}_\nu)$, ν being equal to 2, or a place of good reduction then $2 \mid \nu(x(P))$ and we find that $f(P) \in \mathbb{Z}_\nu^*$.

For $\nu = p$ or $\nu = q$, E has bad, type III reduction. The group $E(\mathbb{Q}_\nu)$ is generated by $E_0(\mathbb{Q}_\nu)$ and the point $T = (0,0)$ [7, Table 15.1]. Since both $E_1(\mathbb{Q}_\nu) \cong \mathbb{Z}_\nu$ and $E_0(\mathbb{Q}_\nu)/E_1(\mathbb{Q}_\nu) \cong \overline{E}_{ns}(\mathbb{F}_\nu) \cong \mathbb{F}_\nu$ (the last isomorphism due to the type of reduction being additive) are divisible by 2, so is the group $E_0(\mathbb{Q}_\nu)$. It follows that $S^{(\widehat{\phi})}(\mathbb{Q}_\nu) = \langle -pq \rangle$. We recall that it is assumed that $p \equiv q \equiv 3 \bmod 16$, labeled so that $(p/q) = (-q/p) = 1$. Since p and $-q$ are squares modulo q and modulo p, respectively, we have illustrated that $S^{(\widehat{\phi})}(\mathbb{Q}_p) = \langle p \rangle$ and $S^{(\widehat{\phi})}(\mathbb{Q}_q) = \langle -q \rangle$.

For $d \in \mathbb{Q}(S, 2)$ to be an element of $S^{(\widehat{\phi})}(E')$, it is necessary and sufficient that when localized it maps to a unit in $S^{(\widehat{\phi})}(\mathbb{Q}_\nu)$ when ν is 2 and when ν is a place of good reduction and to an element of $S^{(\widehat{\phi})}(\mathbb{Q}_\nu)$ when ν is p and q. It follows that the Selmer group $S^{(\widehat{\phi})}(E')$ is $\langle p, -q \rangle$.

Next, we consider the group $S^{(\phi)}(E)$. If $P \in E'(\mathbb{R})$ then $x(P) \geq 0$. This fact coupled with reasoning similar to the preceding paragraphs shows that $S^{(\phi)}(E) = \langle pq \rangle$.

From the exact sequences

$$0 \longrightarrow \frac{E'(\mathbb{Q})}{\phi(E(\mathbb{Q}))} \longrightarrow S^{(\phi)}(E) \longrightarrow \mathrm{III}\left(\frac{E}{\mathbb{Q}}\right)[\phi] \longrightarrow 0$$

$$0 \longrightarrow \frac{E(\mathbb{Q})}{\widehat{\phi}(E'(\mathbb{Q}))} \longrightarrow S^{(\widehat{\phi})}\left(E'\right) \longrightarrow \mathrm{III}\left(\frac{E'}{\mathbb{Q}}\right)\left[\widehat{\phi}\right] \longrightarrow 0,$$

$$0 \longrightarrow \frac{E'(\mathbb{Q})\left[\widehat{\phi}\right]}{\phi(E(\mathbb{Q})[2])} \longrightarrow \frac{E'(\mathbb{Q})}{\phi(E(\mathbb{Q}))} \longrightarrow \frac{E(\mathbb{Q})}{2E(\mathbb{Q})} \longrightarrow \frac{E(\mathbb{Q})}{\widehat{\phi}(E'(\mathbb{Q}))} \longrightarrow 0 \tag{14}$$

following an analysis similar to that used in proving Proposition X.6.2(c) [7], we obtain

$$r_E + \dim_2 \mathrm{III}\left(\frac{E}{\mathbb{Q}}\right)[2] = \dim_2 S^{(\phi)}(E) + \dim_2 S^{(\widehat{\phi})}\left(E'\right) - 2 = 1, \tag{15}$$

where r_E denotes the rank of $E(\mathbb{Q})$ and $\dim_2$ is the dimension as a $\mathbb{Z}/2\mathbb{Z}$-vector space. In particular, $r_E \leq 1$.

When $r_E = 1$, then $\dim_2 \mathrm{III}(E\mathbb{Q})[2] = 0$. Since

$$\dim_2 \mathrm{III}\left(\frac{E}{\mathbb{Q}}\right)[2] = \dim_2 \mathrm{III}\left(\frac{E'}{\mathbb{Q}}\right)\left[\widehat{\phi}\right] + \dim_2 \mathrm{III}\left(\frac{E}{\mathbb{Q}}\right)[\phi] \tag{16}$$

it follows that $\mathrm{III}(E'/\mathbb{Q})[\widehat{\phi}]$ is trivial, so f gives an isomorphism $E(\mathbb{Q})/\widehat{\phi}(E'(\mathbb{Q})) \to S^{(\widehat{\phi})}(E')$. So the points on $E(\mathbb{Q})$ map onto $S^{(\widehat{\phi})}(E') = \langle p, -q \rangle$. Since the image of $(0,0)$ is $-pq$, we find that, for any point R in $E(\mathbb{Q})$ but not in $\langle (0,0) \rangle + 2E(\mathbb{Q})$, $\nu_p(x(R))$ and $\nu_q(x(R))$ have opposite parity.

To finish the proof of Theorem 1, we need to argue, on BSD, that the elliptic curves E_D have Mordell-Weil rank 1. To this end we investigate the zeros of the L-series of E at $s = 1$. For the curves of interest the global root number $w(E)$ can be computed from the formulae in [9] and it equals -1. Evaluating the functional equation $\Lambda_E(s)$ at $s = 1$, we have $\Lambda_E(1) = -\Lambda_E(1)$ and hence $\Lambda_E(1) = 0$. This implies that $L_E(1) = 0$; in other words, the analytic rank $r_E^{an} > 0$.

If $r_E^{an} = 1$; that is, $L_E^{(1)}(1) \neq 0$, then $r_E = 1$, by a result of Kolyvagin [10]. Alternatively, since $r_E \leq 1$ and $r_E^{an} > 0$, it follows from the BSD conjecture that $r_E = r_E^{an} = 1$.

This completes the proof of Theorem 1.

3. Proof of Theorem 2

The curve E_D has $y^2 = x^3 - Dx$ as a minimal model, with discriminant $\Delta = 64D^3$ and height $(1/4)\log 48D$. The 2-torsion point $(0,0)$ generates the torsion subgroup of the Mordell-Weil group $E_D(\mathbb{Q})$.

Let E_D' denote $y^2 = x^3 + 4Dx$ the isogenous curve of E_D, and let C_d' represent the homogeneous spaces $dW^2 = d^2 - DZ^4$ of E_D'.

One way to compute a rational point of E_D is to search for a rational point on the homogeneous spaces: $C'_p : W^2 = p - qZ^4$, $C'_{-q} : -W^2 = q - pZ^4$ (assuming $(p/q) = 1$) and this gives us a rational point of E_D via the map $\psi : C'_d \to E$, $\psi(Z, W) = (d/Z^2, dW/Z^3)$. For example if $C'_p : W^2 = p - qZ^4$ has a rational point (z, w), where the numerator and denominator of z are polynomially bounded in D, then a rational point on E_D can be found of canonical height $O(\log D)$.

We note that in the special case where $p-q$ is a square the curve E_D does have a small rational point $(-q, q\sqrt{p-q})$. Thus if there are infinitely many such pairs of primes p and q, then there are infinitely many E_D with $D = pq$ with a rational point of height bounded by $O(\log D)$. In the simplest case taking $q = 3$, the question boils down to whether there are infinitely many primes p of the form $3 + 16n^2$. The answer is affirmative under Hardy-Littlewood's F conjecture [4].

Thus assuming Hardy-Littlewood's F conjecture and BSD, there is a subfamily of infinitely many E_D such that $D = pq$ with p and q prime and $p \equiv q \equiv 3 \bmod 16$ such that, for any ϵ, $0 < \epsilon < 1$, $\mathrm{Reg}(E_D) < D^\epsilon$ for sufficiently large D. Theorem 2 now follows from the elliptic analog of the Brauer-Siegel theorem and the fact that E_D has minimal discriminant $\Delta = 64D^3$ and height $(1/4)\log 48D$.

4. Implications on Computational Complexity

In Theorem 1 we argue that any point R of the Mordell-Weil group $E_D(\mathbb{Q})$ which is not in $\langle(0,0)\rangle + 2E_D(\mathbb{Q})$ must behave differently with respect to p-adic and q-adic valuations. This sets the stage for reductions between the problem of factoring integers of the form D and the problem of computing nontorsion rational points on E_D.

We discuss below that how given a rational nontorsion point P, the factors p and q of D can be found in time polynomial in the height of P.

Let $\mathrm{den}(r)$ and $\mathrm{num}(r)$ be the numerator and denominator of $r \in \mathbb{Q}$, respectively. Let $h(r) = \log_2 \max(|\mathrm{num}(r)|, |\mathrm{den}(r)|)$, the naïve logarithmic height of $r \in \mathbb{Q} \setminus \{0\}$. And let $h(S)$ be the naïve logarithmic height of $S \in \{E_D(\mathbb{Q}) \setminus \langle(0,0)\rangle\}$ which is $\log_2 \max(h(x(S)), h(y(S)))$.

Suppose we are given P, a nontorsion rational point on E_D. A point $R \in E_D(\mathbb{Q}) \setminus (E_D[\phi] + 2E_D(\mathbb{Q}))$ can be constructed by "halving" P using the duplication formula [7, Algorithm 2.3 (d)]. We note that the canonical height of R is not greater than that of P. From the reasoning above we have $v_p(x(R)) \neq v_q(x(R))$. Below we describe how p and q can be recovered from R.

Clearing the denominators of point R, we consider $u \cdot x(R)$, where $u = \mathrm{den}(x(R)) \cdot \mathrm{den}(y(R))$. (Taking u to be $\mathrm{lcm}(\mathrm{den}(x(R)), \mathrm{den}(y(R)))$ will also suffice for our argument but might lead to trickier analysis). We note that the integer $u \cdot x(R)$ can be viewed as the x-coordinate of a point on the projective curve $y^2 \cdot z = x^3 - D \cdot x \cdot z^2$.

Since $v_p(u \cdot x(R)) \neq v_q(u \cdot x(R))$, it follows that computing $\gcd(u \cdot x(R)/D^k, D)$ gives us either p or q but neither 1 nor D, where $k \in \mathbb{Z}_{\geq 0}$ such that $D^k \mid u \cdot x(R)$ but D^{k+1} does not. Moreover, $h(u \cdot x(R)) \leq 3 \cdot h(R)$. Suppose $u \cdot x(R) = c \cdot D^k$, for $c \in \mathbb{Z}$; then $h(u \cdot x(R)) = h(c) + k \cdot h(D) \leq 3 \cdot h(R)$. The fact that $h(c) > 0$ implies $k \cdot h(D) \leq 3 \cdot h(R) - h(c) < 3 \cdot h(R)$ and hence $k < 3 \cdot h(R)/h(D)$. The integer k can be found using the usual doubling trick in $O(\log_2 k)$ bits operations. And the running time of the reduction is

$$O\left(\log_2 k\right) \cdot M\left(3 \cdot h\left(R\right)\right), \tag{17}$$

where $M(b)$ is the bit operations to multiply two b-bits numbers. Therefore the overall time complexity of the reduction is softly linear in the height of the point R for fixed D.

Further, suppose that height of the point P is a polynomial in the height of the elliptic curve E_D; then the time complexity of the reduction is polynomial in $\log_2 D$.

We note that in the special case where $p - q$ is a square the curve E_D does have a small rational point $(-q, q\sqrt{p-q})$, and finding such a point is easily reduced to factoring D. Therefore in this case finding a rational point on E_D and factoring D are polynomial time equivalent.

More generally we remark that one of the procedures to compute a rational point of E_D is to search for a rational point on the homogeneous spaces: $C'_p : W^2 = p - qZ^4$, $C'_{-q} : -W^2 = q - pZ^4$ (assuming $(p/q) = 1$) and this gives us a rational point of E_D via the map $\psi : C'_d \to E, \psi(Z, W) = (d/Z^2, dW/Z^3)$. The knowledge of the two factors p and q allows us to write down the equation of the homogeneous spaces. Moreover suppose either one of the two homogeneous spaces has a small rational point, say $C'_p : W^2 = p - qZ^4$ has a rational point (w, z) where the numerator and denominator of z are polynomially bounded in $\log D$. Then a rational point (w, z) can be found by exhaustive search (since z is so small), and a rational point of E_D can be obtained from such (w, z). Consequently in such cases finding a rational point on E_D and factoring D are polynomial time equivalent. Note that these are also cases that give rise to large Ш groups in Theorem 2.

In general it is an interesting open question to determine to what extent finding a rational point on E_D and factoring D are polynomial time equivalent.

In light of the question of finding a rational point on E_D, it may be interesting to investigate the efficiency of Heegner point computation when restricted to these elliptic curves E_D. Assuming BSD we observe the dependence of the Heegner index on $\#Ш(E_D)$, which may be big (for instance under the Brauer-Siegel Analogue for elliptic curves). It follows that factoring numbers of the form D by computing a point in $E_D(\mathbb{Q})$ via the Heegner point method would be computationally expensive. We refer to [8] for a detailed discussion.

Conflict of Interests

The authors declare that there is no conflict of interests regarding the publication of this paper.

Acknowledgments

The authors would like to thank the anonymous referees of an earlier version of the paper for valuable suggestions. The authors would also like to thank William Stein for providing access to Sage software system [11] via http://modular.math.washington.edu/ (funded by National Science Foundation Grant no. DMS-0821725). The second author was supported in part by NSF Grants CCR-0306393 and CNS-0627458.

References

[1] X. Li and J. Zeng, "On the elliptic curve $y^2 = x^3 - 2rDx$ and factoring integers," *Science China Mathematics*, vol. 57, no. 4, pp. 719–728, 2014.

[2] R. Brauer, "On the zeta-functions of algebraic number fields," *American Journal of Mathematics*, vol. 69, pp. 243–250, 1947.

[3] M. Hindry, "Why is it difficult to compute the Mordell-Weil group?" in *Diophantine Geometry Proceedings*, U. Zannier, Ed., vol. 4 of *Scuola Normale Superiore*, pp. 197–219, 2007.

[4] G. H. Hardy and J. E. Littlewood, "Some problems of "Partitio numerorum"; III: on the expression of a number as a sum of primes," *Acta Mathematica*, vol. 44, no. 1, pp. 1–70, 1923.

[5] B. M. M. de Weger, "$A + B = C$ and big III 's," *Quarterly Journal of Mathematics*, vol. 49, no. 193, pp. 105–128, 1998.

[6] I. A. Burhanuddin and M.-D. A. Huang, "Elliptic curves with large Shafarevich-Tate group," *Journal of Number Theory*, vol. 133, no. 2, pp. 369–374, 2013.

[7] J. H. Silverman, *The Arithmetic of Elliptic Curves*, Springer, New York, NY, USA, 1992.

[8] I. A. Burhanuddin, *Some computational problems motivated by the Birch and Swinnerton-Dyer conjecture [Ph.D. dissertation]*, University of Southern California, 2007.

[9] B. J. Birch and N. M. Stephens, "The parity of the rank of the Mordell-Weil group," *Topology*, vol. 5, pp. 295–299, 1966.

[10] V. A. Kolyvagin, "Euler systems," in *The Grothendieck Festschrift, Volume II*, Progress in Mathematics, 87, pp. 435–483, Birkhäuser, Boston, Mass, USA, 1990.

[11] W. A. Stein, "Sage Mathematics Software (Version 5.0)," The Sage Development Team, 2012, http://www.sagemath.org/.