

Factoring integers and computing elliptic curve rational points

Iftikhar A. Burhanuddin and Ming-Deh A. Huang

Department of Computer Science,
University of Southern California, Los Angeles, CA 90089-0781.
{burhanud|huang}@usc.edu

Abstract. We conjecturally relate via a polynomial-time reduction, a subproblem of integer factoring to the problem of computing the Mordell-Weil group of an elliptic curve from a special family. This raises an interesting question about the growth of the height of the generators of the above group with respect to the discriminant of the elliptic curve. We gather numerical evidence to shed light on this behavior.

1 Introduction

In this paper we relate a subproblem of integer factoring to the problem of computing the Mordell-Weil group of an elliptic curve from a special family. Specifically, we consider the family of elliptic curves $E = E_D : y^2 = x^3 - Dx$, where $D = pq$ with p and q distinct prime numbers, $p \equiv q \equiv 3 \pmod{16}$. Employing the method of two-descent, we show that under the Birch Swinnerton-Dyer conjecture, the Mordell-Weil rank of E is one. Moreover, let $E' = E'_D : y^2 = x^3 + 4Dx$ be the isogenous curve of E . We prove that, assuming BSD (and $(\frac{p}{q}) = 1$), the homogeneous spaces C'_p and C'_{-q} of E' have rational points, where C'_d denotes the curve $dW^2 = d^2 - DZ^4$. We then argue that a generator of the Mordell-Weil group must behave differently with respect to the p -adic and q -adic valuations. This together with the descent analysis sets the stage for reductions between the problem of factoring integers D and the problem of computing rational points on E_D .

Let Δ denote the discriminant of E . In one direction, we prove that, if the naive height of the (non-torsion) generator of $E(\mathbb{Q})$ grows polynomially in $\log \Delta$, then factoring D is polynomial time reducible to computing the generator of the group. Extensive computation suggests that for all elliptic curves this growth is that of polynomial of degree at most 3 (conjecture 4).

In the other direction, we show that if either of the homogeneous spaces C'_p and C'_{-q} of E' have rational points of naive height polynomially bounded in $\log \log \Delta$, then computing a non-torsion rational point of

E is polynomial time reducible to factoring D . Heuristic arguments and numerical evidence suggest that the set of elliptic curves E_D , with associated homogeneous spaces having rational points of naive height bounded by $\log \log \Delta$, is infinite.

The theoretical results and the computations motivated by these results raise the following questions:

1. Are the problem of factoring integers D of the form $D = pq$ with p and q prime numbers, $p \equiv q \equiv 3 \pmod{16}$, and the problem of computing a non-torsion rational point of $E_D : y^2 = x^3 - Dx$ polynomial time equivalent?
2. How is the minimal (canonical) height of a rational non-torsion point of E_D upper-bounded by Δ , the discriminant of the elliptic curve? (Computations hint at a $\text{poly}(\log \Delta)$ bound.)
3. What is the upper bound of the minimal height of a rational point of the homogeneous spaces of $E'_D : y^2 = x^3 + 4Dx$ in terms of the discriminant of E_D ?

We remark that the data, which we gathered (§7), seems to be of independent interest as it raises questions about the computational nature of two-descent, the Mordell-Weil groups of a special family of elliptic curves and similar issues about elliptic curves in general.

We thank S. Kamienny, W. Raskind and W. Stein for stimulating conversations. The authors are grateful to the latter for providing us with access to computing resources without which the computational aspects of this paper would not have seen the light of day. All computations were performed using SAGE [8]. We were supported in part by the following NSF grant CCR-0306393.

2 The descent procedure

A theorem of Mordell states that $E(\mathbb{Q})$, the group of rational points of an elliptic curve, is finitely generated. Questions about existence and enumeration of the generators of this abelian group, in particular its rank, lead to interesting and challenging problems.

Let $\phi : E \rightarrow E'$ be an isogeny between elliptic curves E, E' defined over \mathbb{Q} and $\hat{\phi} : E' \rightarrow E$ be the dual isogeny of ϕ . The following exact sequence arises from the Galois cohomology associated to E :

$$0 \rightarrow E'(\mathbb{Q})/\phi(E(\mathbb{Q})) \rightarrow S^{(\phi)}(E) \rightarrow \text{III}(E)[\phi] \rightarrow 0 \quad (1)$$

where $S^{(\phi)}(E)$ is the ϕ -Selmer group of E over \mathbb{Q} and $\text{III}(E)$ is the (conjecturally finite) Shafarevich-Tate group of E over \mathbb{Q} . The definitions of the aforementioned groups can be found in [7, Chapter X]. We will proceed to give only a flavor of these objects.

$S^{(\phi)}(E)$ is a finite group, whose elements can be viewed as curves called *homogeneous spaces* with the property that they have a point over \mathbb{R} and \mathbb{Q}_p for every prime p . This group is computable and its size upper bounds the size of $E'(\mathbb{Q})/\phi(E(\mathbb{Q}))$, the so-called *weak* Mordell-Weil group. It follows from the theory of height functions on elliptic curves that once we have computed the latter group, $E(\mathbb{Q})$, the Mordell-Weil group can be recovered.

The above *descent by ϕ isogeny* procedure reduces the computation of weak Mordell-Weil group to the question of (non-)existence of a rational point on a finite number of homogeneous spaces. The inability to decide whether a homogeneous space is a non-trivial element of $\text{III}(E)[\phi]$ is what makes rank computation using this procedure difficult.

In this context, the BSD conjecture comes to the rescue as it gives us information about the rank of the elliptic curve, via the order of zeros of the L -function of the curve. We give an overview of this conjecture in the next section.

3 Birch and Swinnerton-Dyer Conjecture

Let $L_E(s)$ be the L -function associated to E , an elliptic curve over \mathbb{Q} of conductor N and

$$\Lambda_E(s) = (2\pi)^{-s} \Gamma(s) N(E)^{s/2} L_E(s). \quad (2)$$

Then by the Modularity theorem [2], Λ_E has an analytic continuation to the entire complex plane, and it satisfies a functional equation relating the values at s and at $2 - s$: $\Lambda_E(s) = w(E) \Lambda_E(2 - s)$, where $w(E) = \pm 1$ is called the global root number of E .

Let r_E^{an} and r_E denote the analytic and arithmetic rank of E which are the order of vanishing of $L_E(s)$ at $s = 1$ and the abelian group rank of $E(\mathbb{Q})$ respectively. The fascinating BSD conjecture and its associated formula are as follows:

Conjecture 1. (Birch and Swinnerton-Dyer)

$$r_E^{an} = r_E \quad (3)$$

Moreover,

$$\frac{L_E^{(r_E)}(1)}{r_E!} = \frac{\#\text{III}(E) \cdot R(E) \cdot \Omega \cdot \prod_p c_p}{(\#E(\mathbb{Q})_{tors})^2} \quad (4)$$

The left hand side of Eq. 4 denotes the leading coefficient of the Taylor expansion of $L_E(s)$ at $s = 1$. The terms on the right hand side of the formula are as follows: Ω is defined to be $\int_{E(\mathbb{R})} |\omega|$, where $\omega := dx/(2y+a_1x+a_3)$ is the invariant differential on a global minimal Weierstrass equation for E over \mathbb{Q} ; $R(E)$ stands for the elliptic regulator of $E(\mathbb{Q})/E(\mathbb{Q})_{tors}$, computed using the canonical height pairing; and $c_p := \#E(\mathbb{Q}_p)/E_0(\mathbb{Q}_p)$ refers to the Tamagawa number at p , where $E_0(\mathbb{Q}_p)$ is the subgroup of the group of \mathbb{Q}_p -points of E that reduce to a non-singular point on the reduced curve at p .

4 Analysis of E_D

In this section we will study a particular class of elliptic curves parameterized by primes p and q and obtain the structure of the associated Selmer groups subject to congruence conditions. The reader eager to learn about the reduction mentioned in the Introduction can skip this section.

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

$$E_D : y^2 = x^3 - Dx.$$

where $D \in \mathbb{Z}$ (we will drop D as a subscript when it is clear from the context). E_D is isogenous to the elliptic curve

$$E'_D : Y^2 = X^3 + 4DX$$

via the isogeny $\phi : E_D \rightarrow E'_D, (x, y) \mapsto (y^2/x^2, -y(D+x^2)/x^2)$ and let $\hat{\phi} : E'_D \rightarrow E_D$ be the dual isogeny of ϕ .

We will consider the curve $E_{pq} : y^2 = x^3 - pqx$, where p and q are odd and distinct primes and perform descent via ϕ , which is an isogeny of degree 2 [7, Proposition X.4.9].

Let $M_{\mathbb{Q}}$ be the set of primes of \mathbb{Z} and ∞ (that is, a complete set of inequivalent absolute values on \mathbb{Q}). Let $S = \{\infty, 2, p, q\} \subset M_{\mathbb{Q}}$ and \mathbb{Q}_{ν} denote the completion of \mathbb{Q} with respect to the absolute value associated to $\nu \in S$. In particular, \mathbb{Q}_{∞} denotes \mathbb{R} and for $\nu \in S \setminus \{\infty\}$, \mathbb{Q}_{ν} denotes the ν -adic numbers. Let

$$\mathbb{Q}(S, 2) := \{b \in \mathbb{Q}^*/\mathbb{Q}^{*2} \mid \nu(b) \equiv 0 \pmod{2} \text{ for all } \nu \notin S\}.$$

We take the following representatives for the cosets in $\mathbb{Q}(S, 2)$:

$$\{\pm 1, \pm 2, \pm p, \pm 2p, \pm q, \pm 2q, \pm pq, \pm 2pq\}.$$

Let $WC(E)$ denote the Weil-Chat let group for 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 $C_d \in WC(E)$ and $C'_d \in WC(E')$, also referred to as quartics, are given by the equations

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

The ϕ -Selmer group is a subset of $\mathbb{Q}(S, 2)$

$$S^{(\phi)} \cong \{d \in \mathbb{Q}(S, 2) : C_d(\mathbb{Q}_\nu) \neq \emptyset \text{ for all } \nu \in S\}.$$

The $\hat{\phi}$ -Selmer group has an analogous isomorphism where C_d is replaced by C'_d .

Remark 1. Our proof techniques will make frequent use of a bivariate version of Hensel lemma [7, Exercise 10.12] to lift approximate solutions on the above quartics.

From [7, Proposition X.4.9], the images of $(0, 0)$, the 2-torsion point of $E'(\mathbb{Q})$ and $E(\mathbb{Q})$ in the Selmer groups are given by

$$pq \in S^{(\phi)}(E) \text{ and } -pq \in S^{(\hat{\phi})}(E') \quad (5)$$

respectively. We will restrict our analysis to the case where p and q are distinct primes such that $p \equiv q \equiv 3 \pmod{16}$.

4.1 The structure of $S^{(\phi)}(E)$

If $-d < 0$, then $-dw^2$ is negative and $d^2 + 4pqz^4$ is not and this implies that

$$-d \notin S^{(\phi)}(E). \quad (6)$$

Remark 2. Suppose $\gamma = \alpha + \beta$, where $\alpha, \beta \in \mathbb{Q}_t$ for some prime t . Let $v = v_t$ be the normalized valuation associated to prime t , that is, $v_t(t) = 1$. If $v(\alpha) \neq v(\beta)$ then $v(\gamma) = \min(v(\alpha), v(\beta))$ and if $v(\alpha) = v(\beta)$ then $v(\gamma) \geq v(\alpha)$. We will repeatedly use this property of valuations in this section.

Let t denote p or q . Suppose $(z, w) \in C_2(\mathbb{Q}_t) : w^2 = 2 + 2pqz^4$ then $2v(w) = \min(0, 1 + 4v(z))$. The scenario $v(z) < 0$ is not possible. Let us suppose $v(z) \geq 0$ then $v(w) = 0$. The congruence $w^2 \equiv 2 \pmod{t}$ has a solution iff $(\frac{2}{t}) = 1$ and this solution lifts to a point on C_2 . Hence for $t = p, q$, $C_2(\mathbb{Q}_t) \neq \emptyset \Leftrightarrow t \equiv \pm 1 \pmod{8}$ but this contradicts our choice of p and q . Therefore

$$2 \notin S^{(\phi)}(E). \quad (7)$$

If $(z, w) \in C_p(\mathbb{Q}_q) : w^2 = p + 4qz^4$ then $2v(w) = \min(0, 1 + 4v(z))$. Assuming $v(z) < 0$ leads us to a contradiction. If $v(z) \geq 0$ then $v(w) = 0$ and hence $w^2 \equiv p \pmod{q}$. Therefore $C_p(\mathbb{Q}_q) \neq \emptyset \Leftrightarrow (\frac{p}{q}) = 1$.

Suppose $(z, w) \in C_p(\mathbb{Q}_p)$, then $2v(w) = \min(1, 4v(z))$. It follows that necessarily $v(z) = -i \leq 0$ which in turn implies $v(w) = 2v(z)$. Substituting w and z by w'/p^{2i} and z'/p^i respectively, we have $C_p'' : w'^2 = p^{1+4i} + 4qz'^4$ with w' and z' units. Taking $z' = 1$ and w' equal to a solution to the congruence $w'^2 \equiv 4q \pmod{p}$, we realize that (z', w') lifts to a point in $C_p''(\mathbb{Q}_p) \Leftrightarrow (\frac{4q}{p}) = 1$. This proves that $C_p(\mathbb{Q}_p) \neq \emptyset \Leftrightarrow (\frac{q}{p}) = 1$.

Due to our choice of p and q , $(\frac{p}{q}) = -(\frac{q}{p})$ and hence

$$p \notin S^{(\phi)}(E). \quad (8)$$

Similar analysis illustrates that

$$q \notin S^{(\phi)}(E). \quad (9)$$

By Eqs. 5-9, $S^{(\phi)}(E) = \langle pq \rangle$ and Eq. 1 enables us to demonstrate that $\text{III}(E/\mathbb{Q})[\phi] = 0$.

4.2 The structure of $S^{(\hat{\phi})}(E')$

We will proceed to compute the structure of the $S^{(\hat{\phi})}(E')$ group, working with the quartics $C'_d : dW^2 = d^2 - pqZ^4$.

Employing reasoning similar to the previous section, we obtain $C'_p(\mathbb{Q}_q)$ is non-empty $\Leftrightarrow (\frac{p}{q}) = 1$ and moreover if $(Z, W) \in C'_p(\mathbb{Q}_q)$ then $v_q(Z) \geq 0$. By analogy, $C'_p(\mathbb{Q}_p) \neq \emptyset$ is equivalent to $(\frac{-q}{p}) = 1$ and $(Z, W) \in C'_p(\mathbb{Q}_p)$ implies that $v_p(Z) \leq 0$.

Let $(Z, W) \in C'_p(\mathbb{Q}_2) : W^2 = p - qZ^4$. Suppose $v(Z) = 0$ and $v(W) = i > 0$. Substituting W and Z by $2^i W'$ and Z' respectively, we have $2^{2i} W'^2 = p - qZ'^4$ with W' and Z' units. If the conditions $p - q \equiv 16, p - 17q \equiv 16, p - q \equiv 0, p - 17q \equiv 0 \pmod{32}$ hold, then the

congruence $2^{2i}W'^2 \equiv p - qZ'^4 \pmod{32}$ has solutions (i, Z', W') : $(2, 1, 1)$, $(2, 3, 1)$, $(3, 1, 1)$, $(3, 3, 1)$ respectively such that (Z', W') lifts to a \mathbb{Q}_2 -point.

This leads to

$$\left(\frac{p}{q}\right) = \left(\frac{-q}{p}\right) = 1 \text{ and } p \equiv q \pmod{16} \Rightarrow p \in S^{(\hat{\phi})}(E') \quad (10)$$

By symmetry, $q \in S^{(\hat{\phi})}(E')$ under conditions identical to above statement with the roles of p and q being reversed.

Also for $t = p, q$, $C'_{-1}(\mathbb{Q}_t) \neq \emptyset \Leftrightarrow t \equiv 1 \pmod{4}$, which contradicts our selection of p and q . Therefore

$$-1 \notin S^{(\hat{\phi})}(E'). \quad (11)$$

Next if $(Z, W) \in C'_{-2}(\mathbb{Q}_2) : -2W^2 = 4 - pqZ^4$ then $1 + 2v(W) = \min(2, 4v(Z))$, which is a contradiction and we have illustrated that

$$-2 \notin S^{(\hat{\phi})}(E'). \quad (12)$$

Similarly,

$$2 \notin S^{(\hat{\phi})}(E'). \quad (13)$$

It is a fact that $\left(\frac{p}{q}\right) = -\left(\frac{q}{p}\right)$, since $p \equiv q \equiv 3 \pmod{4}$. Let us assume *without loss of generality* that $\left(\frac{p}{q}\right) = 1$. This implies $\left(\frac{-q}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{q}{p}\right) = 1$, since $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$.

By Eq. 10, $p \in S^{(\hat{\phi})}(E')$ and as $-pq \in S^{(\hat{\phi})}(E')$ (Eq. 5), $-q \in S^{(\hat{\phi})}(E')$ and we have proved that $S^{(\hat{\phi})}(E') = \langle p, -q \rangle$.

4.3 An elliptic curve of conjectural rank 1

The purpose of this subsection is to prove that the elliptic curve of interest has rank 1 under certain assumptions. Utilizing techniques inspired by the ones used in proving Proposition X.6.2(c) [7], we obtain

$$\begin{aligned} r_E + \dim_2 \text{III}(E'/\mathbb{Q})[\hat{\phi}] &= \dim_2 S^{(\phi)}(E) + \dim_2 S^{(\hat{\phi})}(E') - 2 \\ &= 1. \end{aligned}$$

where \dim_2 is the dimension as a $\mathbb{Z}/2\mathbb{Z}$ -vector space. In particular,

$$r_E \leq 1. \quad (14)$$

Next, we will investigate the zeros of the L -function of E at $s = 1$. The global root number $w(E)$ can be computed from the local root numbers: $w(E) = \prod_{p \leq \infty} w_p(E)$, where $w_p(E) = \pm 1$ and equal to 1 for the primes of good reduction, -1 for $p = \infty$. Hence $w(E) = -\prod_{p|\Delta} w_p(E)$.

We will use the formulae presented in [6] to compute the local root numbers of the elliptic curve.

Lemma 1. *Let $E : y^2 = x^3 - pqx$ be an elliptic curve over \mathbb{Q} with p, q distinct primes such that $p \equiv q \equiv 3 \pmod{16}$. Then $w(E) = -1$.*

Proof. We begin by listing some properties and invariants of E , which will play a role in the root number computation. The discriminant of E , $\Delta(E) = 2^6 p^3 q^3$, $c_4 = 48pq$, $c_6 = 0$, additive type III reduction at 2; $p; q$. E has potential good reduction everywhere as $j(E) = 1728$.

Let t be either p or q . Suppose $t > 3$ then $e_t = \frac{12}{\gcd(v_t(\Delta), 12)} = 4$ and from the formulae [6, Fact 3], $w_t(E) = \left(\frac{-2}{t}\right) = \left(\frac{-1}{t}\right)\left(\frac{2}{t}\right) = -1 \cdot -1 = 1$. If $t = 3$, then [6, Table II] states that $w_3(E) = 1$.

To calculate $w_2(E)$ we need the following data: $c'_4 = 3pq$, $c'_4 \equiv 3 \pmod{4}$, $c'_4 \equiv 11 \pmod{16}$ and $c_{6,7} = 0$. Referring to [6, Table III], since $c'_4 - 4c_{6,7} \equiv 11 \pmod{16}$, we have demonstrated that $w_2(E) = 1$.

Therefore $w(E) = -1 \cdot w_2(E) \cdot w_p(E) \cdot w_q(E) = -1$.

Lemma 2. *Let E be the same as in lemma 1. Assuming $r_E^{an} = 1$ (or alternatively the BSD conjecture), $r_E = 1$.*

Proof. Plugging in the value of the root number into Eq. 2, the functional equation of $\Lambda_E(s)$ and taking $s = 1$ we have $\Lambda_E(1) = -\Lambda_E(1)$ and hence $\Lambda_E(1) = 0$. This implies that $L_E(1) = 0$. In other words,

$$r_E^{an} > 0. \quad (15)$$

Recall that $r_E \leq 1$ (Eq. 14). Now assuming $r_E^{an} = 1$ [4], (or assuming the BSD conjecture) we can conclude that

$$r_E = 1. \quad (16)$$

4.4 Generator of $E_D(\mathbb{Q})$

We have shown that $S^{\hat{\phi}}(E') = \{1, p, -q, -pq\}$ (assuming $\left(\frac{p}{q}\right) = 1$), that is, for each $d \in S^{\hat{\phi}}(E')$ the homogeneous space C'_d has a point in every completion of \mathbb{Q} . Also there is a map from C'_d to E , given by $(Z, W) \mapsto \left(\frac{d}{Z^2}, \frac{dW}{Z^3}\right)$. As $r_E = 1$, we have $\dim_2 \text{III}(E'/\mathbb{Q})[\hat{\phi}] = 0$, that is, these

quartics have \mathbb{Q} -points. In particular, on E we have the rational points $R_1 := (\frac{p}{Z_1^2}, \frac{pW_1}{Z_1^3})$, where $v_p(Z_1) \leq 0, v_q(Z_1) \geq 0$ and $R_2 := (\frac{-q}{Z_2^2}, \frac{-qW_2}{Z_2^3})$, where $v_p(Z_2) \geq 0, v_q(Z_2) \leq 0$. The other elements of the Selmer group give rise to O and $(0, 0)$ respectively.

Let $E(\mathbb{Q}) = \langle T \rangle + \mathbb{Z}P$, where $T = (0, 0)$. Though it is not clear whether P is in the image of the map $C'_d \rightarrow E$, we will proceed to show that the integers $v_p(x(P)), v_q(x(P))$ are not the same and this will help us to factor pq .

We remark that if R is a rational point on $E, R \neq O, T$ then using the group law formulae we arrive at the identity $x(R) \cdot x(R+T) = -pq$. This observation will be useful as we know that for $i = 1, 2, R_i = k_iP + l_iT$, for some $k_i \in \mathbb{Z}$, where $l_i = 0$ or 1 .

1. Let $v_p(x(P)), v_q(x(P)) \leq 0$, that is, P reduces to a non-singular point on the reduced curve modulo p and q . Then for all $k \in \mathbb{Z}, v_p(x(kP)), v_q(x(kP)) \leq 0$, which is not possible, since R_1, R_2 are not of the form kP or $kP + T$.
2. Let $v_p(x(P)) = m, v_q(x(P)) = n, m, n \geq 1$. Recall that the component group at p and q is $\mathbb{Z}/2\mathbb{Z}$. First, let us suppose that $k \in \mathbb{Z}$ is even. Then kP reduces to a non-singular point modulo p and q and we head towards a contradiction due to reasons similar to the previous case. If k is odd, kP reduces to the singular point $(0, 0)$ on the reduced curve modulo p and q . This implies $kP \neq R_1$ or R_2 . If $m = n$, then $x(kP + T) \neq x(R_1), x(R_2)$. And hence the case we are left with is $m \neq n$.
3. In the last scenario, $v_p(x(P)) \geq 1, v_q(x(P)) \leq 0$ and these numbers are different.

The above discussion proves that the x-coordinate of a generator of E behaves differently with respect to v_p and v_q .

5 The reduction

Definition 1. Let E be an elliptic curve over $\mathbb{Q}, P \in E(\mathbb{Q})$ and $x(P) = \frac{a}{b}$, we define the naive height of P to be $h_x(P) = \log \max\{|a|, |b|\}$.

Definition 2. Let E be an elliptic curve over \mathbb{Q} of positive rank and T_{max} denote the point of greatest naive height among a set of generators of $E(\mathbb{Q})/E(\mathbb{Q})_{tors}$.

Definition 3. Let $f \in \mathbb{Z}[X]$.

$$I_f := \{E/\mathbb{Q} \text{ with } r_E > 0 \mid [h_x(T_{max})] \leq f(\log |\Delta|)\}.$$

In other words, the number of bits to represent the point T_{max} (or any other generator of $E(\mathbb{Q})$) is a polynomial in the logarithm of the discriminant of the elliptic curve.

Let $D = pq$ where p, q are odd, distinct primes and denote the problem of integer factoring D by IF-D. The elliptic curve $E_D : y^2 = x^3 - Dx$ over \mathbb{Q} has $\mathbb{Z}/2\mathbb{Z} = \langle(0,0)\rangle$ torsion group and $\Delta = 2^6 \cdot D^3$. The problem of computing Mordell-Weil group generators for E_D will be denoted by CMWG- E_D .

Suppose $D = pq$, where p, q are the same primes as in lemma 1. Let us recapitulate the results of the previous section: E_D has conjectural rank 1 (lemma 2) and the x-coordinate of the generator of $E(\mathbb{Q})$ has different valuations with respect to p and q (§4.4). For the rest of this section E_D will denote the aforementioned elliptic curve.

Definition 4. Let $f \in \mathbb{Z}[X]$.

$$I_f^* := \{E_D/\mathbb{Q} \mid E_D \in I_f\}.$$

The fact that I_f, I_f^* are non-empty, follows from computational evidence which we present towards the end of this paper.

Let the problems of factoring integers D such that the associated elliptic curve E_D is in I_f^* and computing generators for the elliptic curves in I_f^* be denoted by IF-D-f and CMWG- E_D -f respectively. The main result of this paper is the following:

Theorem 1. Fixing $f \in \mathbb{Z}[X]$, IF-D-f \leq_P CMWG- E_D -f.

Proof. Suppose given a particular D , we can compute P , a (non-torsion) generator of $E_D(\mathbb{Q})$. We can factor D , since $v_p(x(P)) \neq v_q(x(P))$. Moreover as $h_x(P)$ is a polynomial in $\log \Delta$, we have proved that this is a polynomial time reduction.

We remark that one of the procedures to compute a generator 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 $(\frac{p}{q}) = 1$) and this gives us a rational point of E_D via the map $\psi : C'_d \rightarrow E$, $\psi(Z, W) = (d/Z^2, dW/Z^3)$. But to write down the equation of the homogeneous space requires knowledge of a factor of D .

This observation prompts us to ask whether it is *enough* to factor, to compute a non-torsion rational point on E_D . In order for this reduction to be polynomial time we require that the heights of rational points on associated homogeneous spaces be appropriately bounded.

Definition 5. Let S_{E_D} denote a point (Z, W) on C'_p or C'_{-q} with the smallest naive Z -height.

Definition 6. Let $g \in \mathbb{Z}[X]$.

$$J_g^* := \{E_D/\mathbb{Q} \mid \lceil h_Z(S_{E_D}) \rceil \leq g(\log \log \Delta)\}.$$

Let the problem of computing a non-torsion rational point for the elliptic curves in J_g^* be denoted by CNRP- E_D - g .

Theorem 2. Fixing $g \in \mathbb{Z}[X]$, CNRP- E_D - $g \leq_P$ IF- D .

Proof. We use a IF-D blackbox to factor D and write down the equations of the homogeneous spaces. Since the rational point (Z, W) on the homogeneous space we are in pursuit of, has height which is a polynomial in $\log \log \Delta$, we can afford to search naively and in parallel on the above quartics. It follows that the reduction takes time polynomial in $\log \Delta$.

Remark 3. Let us reconsider the quartic $C'_p : W^2 = p - qZ^4$. Suppose $Z = 1$, $p = 3 + 16k'$ and $q = 3 + 16k''$ for some $k', k'' \in \mathbb{Z}$ then $W^2 = 2^4(k' - k'')$. We observe that if there are infinitely many pairs of primes p, q of the type appearing in lemma 1 such that $(\frac{p}{q}) = 1$ and $k' - k''$ is a square, then there are infinitely many elliptic curves in the sets I_f^* and J_g^* , for every f and g , non-zero polynomial of degree at least 1 and non-zero polynomial respectively. An analogous statement can be made about the quartic $C'_{-q} : -W^2 = q - pZ^4$.

In the simplest case taking $q = 3$ and $Z = 1$ ($(\frac{p}{19}) = 1$, since $p \equiv 3 \pmod{16}$), the question bowls down to *are there infinitely many primes p of the form $3 + 16n^2$?* The answer is affirmative under Hardy-Littlewood's F conjecture [3].

6 Heights of generators of $E(\mathbb{Q})$

The purpose of these sections is to elaborate on the paucity of the above reductions. The height of a rational point on an elliptic curve measures the *size* of the point. We turn to the literature to obtain bounds on the heights of generators of $E(\mathbb{Q})$ and it will be evident that this phenomenon is not understood well enough.

Conjecture 2. [5] Let Δ_{min} denote the minimal discriminant of an elliptic curve. For all elliptic curves of the form $y^2 = x^3 + ax + b$, with $a, b \in \mathbb{Z}$, one has the lower bound for the canonical height:

$$\hat{h}(P) \gg \log |\Delta_{min}|$$

for any rational point P which is not a torsion point.

Due to a result of J. Silverman, which applies to elliptic curves with integral j -invariant such as E_D , the above conjecture is a theorem.

Conjecture 3. [5] Let $H(E) = \max(|a|^3, |b|^2)$. For all elliptic curves $y^2 = x^3 + ax + b$ with $a, b \in \mathbb{Z}$, we have

$$\#\text{III}(E) \cdot R(E) \ll H(E)^{1/12} N^{\epsilon(N)} c^{r_E} (\log N)^{r_E}$$

with N is the conductor of the curve, c is some universal constant, and $\epsilon(N) \rightarrow 0$ as $N \rightarrow \infty$. In fact, $\epsilon(N)$ may have the explicit form

$$\epsilon(N) = c' (\log N \log \log N)^{-1/2}.$$

Theorem 2.1 in [5] states that the difference between the canonical height of a point and its naive height is bounded, in other words the growth of the naive height and canonical height with respect to the discriminant of the elliptic curve differ by a constant.

Since we are interested in elliptic curves of rank 1, in which case $R(E)$ equals the canonical height of the generator of the elliptic curve, we observe that the lower and upper bounds in terms of the naive height are linear and exponential in $\log \Delta(E)$ respectively. Due to the enormous gap between the bounds, we turn to computation to get a glimpse of what happens in reality.

7 Computation

Remark 4. In the tables which follow “k: #E” denotes #E number of curves with the quantity of interest in the interval $[k - 1, k)$.

We present results of $R(E) \cdot \#\text{III}(E)$ computation (via L -series calculations assuming the validity of the BSD conjectural formula) for the class of elliptic curves E_D appearing in lemma 1. We chose to obtain a bound on the canonical height of the generator of the elliptic curve in this fashion instead of computing the generator because in the worst case the latter might take an unreasonable amount of time.

We computed $\hat{h}(E) \cdot \#\text{III}(E)$ for elliptic curves of interest with $3 < p < q$ and $N_E = 2^5 p^2 q^2 < 10^{14}$ and tabulate $c_E := \frac{\hat{h}(E) \cdot \#\text{III}(E)}{\log \Delta(E)}$ computations.

k	1	2	3	4	5	6	7	8	9	10	11	12	13	14
$\#E$	1755	689	297	153	81	45	24	10	10	3	3	3	1	1

For the 3075 elliptic curves in above table $\frac{\hat{h}(E) \cdot \#\text{III}(E)}{\log^2 \Delta(E)} < 1$.

The elliptic curve with the smallest discriminant we consider has $\Delta = 2^6 \cdot 19^3 \cdot 67^3 > 10^{11}$ and hence $L^{(1)}(1)$ computations are expensive due to iterative calculations of the transcendental functions involved.

Let E be any elliptic curve over \mathbb{Q} and $e_P := \frac{h(P)}{\log |\Delta(E)|}$ where P is the point among a set of generators for $E(\mathbb{Q})$ with greatest naive height $h(P)$. Lang in [5] made the observation that with the data in the literature that existed at that point in time, e_P is at most 4. Inspired by Lang's comment we turn to existing databases of elliptic curves to gather data.

7.1 Cremona database

We computed e_P values for elliptic curves in Cremona's *allgens* database [1], which lists generators of positive rank curves of conductor at most 120,000. The following table lists statistics for e_P , which was defined above, where P is selected from the generators for $E(\mathbb{Q})$ listed in Cremona's tables.

k	1	2	3	4	5	6	7	8	9	10	[11, 21]	22
$\#E$	459494	5101	881	293	123	69	31	28	18	9	30	2

Two of the above curves have $\frac{h_P}{\log^2 |\Delta(E)|}$ values in the $[1, 2)$ interval while the remaining 466,077 have their values in $[0, 1)$.

7.2 Stein-Watkins database

The Stein-Watkins database [9] lists 136,924,520 elliptic curves of conductor at most 10^8 along with the leading coefficient of the Taylor expansion of $L_E(s)$ at $s = 1$. The i th row of the table below lists $c_E := \lceil \frac{\text{Reg}(E) \cdot \#\text{III}(E)}{\log^i |\Delta(E)|} \rceil$ computed using the BSD conjectural formula (Eq. 4) for 90,948,447 positive analytic rank curves in the database.

i	k	1	2	3	4	5	6	[7, 587]	698	846
1	$\#E$	82715006	5534744	1400359	544699	264103	146319	343215	1	1
i	k	1	2	3	4	5	6	[7, 24]	32	39
2	$\#E$	90932640	12169	2164	724	294	148	306	1	1

7.3 Conclusion

Based on the above tables we make the following conjecture:

Conjecture 4. In theorem 1, taking the polynomial f to be a polynomial of degree at most 3, suffices to make the reduction be polynomial time for all elliptic curves E_D .

Remark 5. We would like to also make an analogous conjecture for the polynomial g in theorem 2, but unfortunately not much seems to be known about heights of rational points on quartics and with the limited amount of data we have collected, we are unable to make any observations.

An experimental study of the heights of rational points on homogeneous spaces of elliptic curves of interest follows: we selected the first 500 primes greater than 3 that were congruent to 3 mod 16 and computed a generator for these 124,750 elliptic curves E_{pq} using two-descent feature of the mwrank program with a logarithmic height bound of 10. Increasing the height bound makes computation prohibitive and since we work with a fixed bound, as the sizes of primes increase, the ratio of the number of curves which yield a generator to the total number of curves tested decreases.

30,180 of these curves yielded generators, all of which arose from a rational point $R = (Z, W)$ on a homogeneous space. We present results of $c_E := \frac{h_Z(R)}{\log \log \Delta(E)}$ calculations in the table below.

k	1	2	3	4	5	6	7
$\#E$	7482	5252	4800	4308	4264	3611	463

Computation suggests that the set $J_{\log \log \Delta}^*$ is infinite.

References

1. Cremona, J.E. <http://www.maths.nott.ac.uk/personal/jec/ftp/data/>.
2. Edixhoven B. *Rational elliptic curves are modular (after Breuil, Conrad, Diamond and Taylor)*, Séminaire Bourbaki, 871 (2000). In: Astérisque 276 (2002), 161–188.
3. Jacobson, Jr., M.J.; Williams, H.C. *New quadratic polynomials with high densities of prime values*. Math. Comp., 72, 499-519 (2003).
4. Kolyvagin, V. A. *Euler Systems*, In The Grothendieck Festschrift, Vol. 2 (Ed. P. Cartier et al.). Boston, MA: Birkhuser, pp. 435-483, 1990.
5. Lang, S. *Conjectured Diophantine estimates on elliptic curves*. Arithmetic and geometry, Vol. I, Progr. Math., vol. 35 (1983), 155–171.
6. Rizzo O. G. *Average root numbers for a nonconstant family of elliptic curves*. Compositio Mathematica 136 (2003), 1–23.
7. Silverman, J. H. *The arithmetic of elliptic curves*. Graduate Texts in Mathematics, 106. Springer-Verlag, New York, 1986.
8. Stein, W.A.; Joyner, D. *SAGE: System for Algebra and Geometry Experimentation*. Comm. Computer Algebra 39 (2005).
9. Stein, W.A.; Watkins, M. <http://modular.ucsd.edu/papers/stein-watkins/>.