Elliptic Curve and Integer Factorization

Zhizhong Pan, Xiao Li

Speaker: Zhizhong Pan

2021/8/12

Contents:

- 1.From congruent number to elliptic curve
- 2.Previous works
- 3.Our works
- 4.Remaining Problem

From congruent number to elliptic curve

- Congruent number: We say a positive square-free integer n is congruent number, if there is a right triangle whose area is n.

- n is congruent number $\Leftrightarrow E_n: y^2 = x^3 - n^2x$ has non-torsion point.

- Proposition: $E_n: y^2 = x^3 - n^2x$ has non-torsion point $\mathrm{P} = (\mathrm{x}, \mathrm{y}), \mathrm{y} \neq 0 \Leftrightarrow \exists \mathrm{r}, \mathrm{s}, \Delta \in \mathbb{N},\ \mathrm{s.t.}\ \mathrm{n}\Delta^2 = (r+s)(r-s)rs$. We can see that $r+s,\ r-s,\ r,\ s$ may include factors of n.
- Proof: $y^2 = x^3 - n^2x \Leftrightarrow ny^2 = nx(x-n)(x+n) \Leftrightarrow n(m^2y)^2 = (nm)(mx)(mx+mn)(mx-mn)$. Then let $\mathrm{r} = \mathrm{mx}, \mathrm{s} = \mathrm{mn}$.

From congruent number to elliptic curve

- It is natural to related a subproblem of integer factoring to the problem of computing the Mordell-Weil group of elliptic curve E_n. But there are two problems remaining.

- 1.If n is not a congruent number, how do we combine the Integer Factorization with the elliptic curve?
- 2. Is there an efficient way to find the point?

- Solution1: Relate a greater family of elliptic curve.
- Solution2: The current approach is decent method and Heegner point method.

Previous works

- In 2003, Burhanuddin and Huang considered the family of elliptic curves $E_D: y^2 = x^3 - Dx$ where $D = pq$ with p and q distinct prime integers, $p \equiv q \equiv 3 \; mod \; 16$, and $\left(\frac{p}{q}\right) = 1$. Furthermore they speculated that the problem of integer factorization and the problem of computing the rational points of the elliptic curve can be polynomial-time equivalent.

- For the 2-Selmer group. They compute that $S(\phi) = \{1, pq\}$, $S'^{(\phi)} = \{1, p, -q, -pq\}$. At that time $\mathrm{Ran}k(E_D) = 1$, and the non-torsion points on E_D can factor D.

Previous works

- In 2014 Li and Zeng studied a family of elliptic curve $E_{2Dr}: y^2 = x^3 - 2Drx$ where $D = pq$ with p and q distinct prime integers, $2Dr$ is square-free. They proved that there are infinitely many $r > 1$ such that E_{2Dr} has conjectural rank one and $v_p(x(kP)) \neq v_q(x(kP))$ for any odd integer k, where P is the generator of E_{2Dr}. Furthermore, assuming the Generalized Riemann hypothesis holds, the minimal value of r is in$O(log^4(D))$.

- For the 2-Selmer group. They compute that $S(\phi) = \{1,2Dr\}$, $S'^{(\phi)} = \{1, A, -2Dr/A, -2Dr\}$, in which A is divisible by only one of p or q. At that time Ran$k(E_D) = 1$, and the non-torsion points on E_D can factor D.

Our works

- Firstly, we focus on a larger family of elliptic curve $E_{Dr}: y^2 = x^3 - Drx$ where $D = pq$ is the integer we want to factor and r is an arbitrary integer. Employing the method of two-descent, we reduce the problem of factoring integer to computing the Mordell-Weil group of $E_{Dr}: y^2 = x^3 - Drx$.

- The second work of this article is to improve their method of calculating 2-Selmer group. We give a way to compute the 2-Selmer group of a family of elliptic curve $E_{Dr}: y^2 = x^3 - Drx$, where $D = pq$ is a product of two distinct odd primes and r is an arbitrary integer.

Parity conjecture

- Corollary: Let elliptic curve $E_D: y^2 = x^3 - Dx$, with $4 \nmid D$, and D quartic-free . We denote the rank of E_D by r_E, then

$$(-1)^{r_E} = w_E = w_\infty \cdot w_2 \cdot \prod_{p^2 \| D} w_p$$

In which

$$w_\infty = \mathrm{sgn}(-D)$$

$$w_2 = \begin{cases} -1 & D \equiv 1,3,11,13 \ mod\ 16 \\ 1 & \text{otherwise} \end{cases}$$

$$w_p = \left(\frac{-1}{p}\right) = \begin{cases} -1 & p \equiv 3 \ mod\ 4 \\ 1 & p \equiv 1 \ mod\ 4 \end{cases}$$

Two-descent method for E_{Dr}

- Considering the elliptic curve $E_{Dr}: y^2 = x^3 - Drx$, denote it by E. And denote its dual curve $E_{-4Dr}: y^2 = x^3 + 4Drx$ by $\hat{E}$.

- Define the two-descent map:

$$\alpha: E(\mathbb{Q}) \to \mathbb{Q}^\times / \mathbb{Q}^{\times 2}$$
$$(x, y) \longmapsto \bar{x}$$
$$\infty \longmapsto 1$$
$$T \longmapsto -\overline{Dr}$$
$$\hat{\alpha}: \hat{E}(\mathbb{Q}) \to \mathbb{Q}^\times / \mathbb{Q}^{\times 2}$$
$$(\hat{x}, \hat{y}) \longmapsto \bar{\hat{x}}$$
$$\hat{\infty} \longmapsto 1$$
$$\hat{T} \longmapsto \overline{Dr}$$

Theorem: we have the following properties:

- (1)α, $\hat{\alpha}$ are group homomorphisms
- (2)$\mathrm{Im}\alpha \subseteq < -1,2, b_i > \triangleq \mathrm{S}, b_i | Dr$,

  $\mathrm{Im}\hat{\alpha} \subseteq < -1,2, b_i > \triangleq \hat{\mathrm{S}}, b_i | 4Dr$.
- (3)If $b \in \mathrm{Im}\alpha$, then $\frac{-\overline{Dr}}{b} \in \mathrm{Im}\alpha$,

  If$b \in \mathrm{Im}\hat{\alpha}$, then $\frac{\overline{Dr}}{b} \in \mathrm{Im}\hat{\alpha}$.
- (4) $\{1, -\overline{Dr}\} \subseteq \mathrm{Im}\alpha, \{1, \overline{Dr}\} \subseteq \mathrm{Im}\hat{\alpha}$
- (5) $|\mathrm{Im}\alpha| \cdot |\mathrm{Im}\hat{\alpha}| = 2^{r_E+2}$

- Theorem : For $\forall b \in S, b \in \mathrm{Im}\alpha \Leftrightarrow C_b' : w^2 = b - \frac{2rD}{b} z^4$ has solutions in $\mathbb{Q}$.

  For$\forall b \in \hat{S}, b \in \mathrm{Im}\widehat{\alpha} \Leftrightarrow C_b : w^2 = b + \frac{8rD}{b} z^4$ has solutions in $\mathbb{Q}$.

- But deciding whether C_b' and C_b have solutions in $\mathbb{Q}$ is a difficult problem, so instead we consider whether they have solutions on local $\mathbb{Q}_p$ $(p|2Dr\infty)$.

- Definition: Define $S'(\phi) \triangleq \{b \in S | C_b'(\mathbb{Q}_p) \neq \Phi, \forall p|2Dr\infty\}$, called the 2-Shafarevich group of E.

  Define $S(\phi) \triangleq \{b \in \hat{S} | C_b(\mathbb{Q}_p) \neq \Phi, \forall p|2Dr\infty\}$, called the 2-Shafarevich group of $\hat{E}$.

Theorem: Suppose $r_E \geq 1, |S'(\phi)| = 4, |S(\phi)| = 2$ or $|S(\phi)| = 4, |S'(\phi)| = 2 \Leftrightarrow$ $Ш'(\phi) = Ш(\phi) = \{1\}$ and $r_E = 1$.

Proposition: When $S'(\phi) = \left\{1, A, \frac{-2Dr'}{A}, -2Dr'\right\}$, $S(\phi) = \{1, 2Dr'\}, r_E = 1$. At that time, the map α, $\hat{\alpha}$ can be written as

$$\alpha: E(\mathbb{Q}) \to \mathbb{Q}^{\times}/\mathbb{Q}^{\times 2}$$

$$\infty \longmapsto 1$$

$$T \longmapsto -\overline{Dr}$$

$$(2k+1)P \longmapsto A \text{ or } \frac{-\overline{Dr}}{A}$$

$$(2k+1)P + T \longmapsto \frac{-\overline{Dr}}{A} \text{ or } A$$

$$2kP \longmapsto 1$$

$$2kP + T \longmapsto -2\overline{Dr}$$

$$\hat{\alpha}: \hat{E}(\mathbb{Q}) \to \mathbb{Q}^{\times}/\mathbb{Q}^{\times 2}$$

$$\hat{\infty} \longmapsto 1$$

$$\hat{T} \longmapsto \overline{Dr}$$

$$k\hat{P} \longmapsto 1$$

$$k\hat{P} + \hat{T} \longmapsto \overline{Dr}$$

Theorem 1: Assuming $D = pq$ is a product of two distinct odd primes, suppose the parity conjecture is true, then

- (1) There exists infinity many integer r, such that the rank of E_{Dr} is greater or equal to one.

- (2) When the rank of E_{Dr} is greater or equal to one, and $S(\phi) = \{1, \overline{Dr}\}$, $S'^{(\phi)} = \{1, A, -\overline{Dr}/A, -\overline{Dr}\}$, where $\overline{Dr}$ means Dr with the square factors removed, A is divisible by only one of p or q, then E_{Dr} has conjectural rank one. At that time, $v_p(x(kP)) \neq v_q(x(kP))$ for any odd integer k, in which P is the generator of E_{2Dr}. Then we can factor D.

- Theorem 2: Let $C_d: w^2 = d + \frac{D}{d} z^4,\ D = (-1)^m 2^n \prod_{i=1}^{n_1} p_i \prod_{j=1}^{n_2} q_j^2 \prod_{k=1}^{n_3} r_k^3$, $d|D$ and d is square-free. We have:

(1) *When* $m = 0$, $C_d(\mathbb{Q}_\infty) \neq \Phi \Leftrightarrow d > 0$.
When $m = 1$, $C_d(\mathbb{Q}_\infty) \neq \Phi$ *holds for any* d.

(2) 1) *When* $2 \nmid d$
- *i)* *If* $n = 0$, $C_d(\mathbb{Q}_2) \neq \Phi \Leftrightarrow d \equiv 1 \bmod 8$ *or* $d + \frac{D}{d} \equiv 0 \bmod 16$ *or* $d + \frac{D}{d} \equiv 4 \bmod 32$ *or* $\frac{D}{d} \equiv 1 \bmod 8$.
- *ii)* *If* $n = 1$, $C_d(\mathbb{Q}_2) \neq \Phi \Leftrightarrow d \equiv 1 \bmod 8$ *or* $d + \frac{D}{d} \equiv 1 \bmod 8$.
- *iii)* *If* $n = 2$, $C_d(\mathbb{Q}_2) \neq \Phi \Leftrightarrow d \equiv 1 \bmod 8$ *or* $d + \frac{D}{d} \equiv 1 \bmod 8$ *or* $\frac{D}{4d} \equiv 1 \bmod 4$.
- *iv)* *If* $n = 3$, $C_d(\mathbb{Q}_2) \neq \Phi \Leftrightarrow d \equiv 1 \bmod 8$.

2) *When* $2 \mid d$
- *i)* *If* $n = 1$, $C_d(\mathbb{Q}_2) \neq \Phi \Leftrightarrow d + \frac{D}{d} \equiv 1 \bmod 8$ *or* $\frac{D}{d} \equiv 1 \bmod 8$.
- *ii)* *If* $n = 2$, $C_d(\mathbb{Q}_2) \neq \Phi \Leftrightarrow \frac{d}{2} + \frac{D}{2d} \equiv 0 \bmod 32$ *or* $\frac{d}{2} + \frac{D}{2d} \equiv 2 \bmod 16$ *or* $\frac{d}{2} + \frac{D}{2d} \equiv 8 \bmod 32$.
- *iii)* *If* $n = 3$, $C_d(\mathbb{Q}_2) \neq \Phi \Leftrightarrow \frac{D}{4d} \equiv 1 \bmod 4$.

(3) $\forall t \mid d$, t *is prime*
1) *When* $t = p_i$, $C_d(\mathbb{Q}_t) \neq \Phi \Leftrightarrow (\frac{D/d}{t}) = 1$.
2) *When* $t = q_j$, $C_d(\mathbb{Q}_t) \neq \Phi \Leftrightarrow (\frac{-d^2/D}{t})_4 = 1$.
3) *When* $t = r_k$, $C_d(\mathbb{Q}_t) \neq \Phi \Leftrightarrow (\frac{D/dt^2}{t}) = 1$.

(4) $\forall t \nmid d$, t *is prime*
1) *When* $t = p_i$, $C_d(\mathbb{Q}_t) \neq \Phi \Leftrightarrow (\frac{d}{t}) = 1$.
2) *When* $t = q_j$, $C_d(\mathbb{Q}_t) \neq \Phi \Leftrightarrow (\frac{d}{t}) = 1$ *or* $(\frac{D/dt^2}{t}) = 1$.
3) *When* $t = r_k$, $C_d(\mathbb{Q}_t) \neq \Phi \Leftrightarrow (\frac{d}{t}) = 1$.

The proof of Burhanuddin and Huang

Proof. Accroding to Corollary 1, we can get $(-1)^{r_E} = w_\infty \cdot w_2 \cdot w_p = -1 \cdot 1 \cdot 1 = -1$, so $r_E \geq 1$.

(1) For $E_D : y^2 = x^3 - Dx$, $S = \{\infty\} \bigcup \{p, q\}$, $Q(S, 2) =< -1, p, q > \bigcup \{\infty\}$. $\forall d \in Q(S, 2)$, apply theorem (2) to investigate the local solution of $C'_d : w^2 = d - \frac{D}{d} z^4$.
Because of $(\frac{q}{p}) = (-1)^{\frac{p-1}{2}} (-1)^{\frac{q-1}{2}} (\frac{p}{q}) = -1 \Rightarrow C_{pq}(\mathbb{Q}_p) = \Phi$, so $-1, pq \notin S'(\phi)$.
Because of $(\frac{q}{p}) = (-1)^{\frac{p-1}{2}} (-1)^{\frac{q-1}{2}} (\frac{p}{q}) = -1 \Rightarrow C_{-p}(\mathbb{Q}_p) = \Phi$, so $-p, q \notin S'(\phi)$.
Because of $p - \frac{D}{p} \equiv 0 \ mod\ 16 \Rightarrow C_p(\mathbb{Q}_2) \neq \Phi$; $(\frac{-q}{p}) = (-1)^{\frac{p-1}{2}} (\frac{p}{q}) = 1 \Rightarrow C_p(\mathbb{Q}_p) \neq \Phi$; $(\frac{p}{q}) = 1 \Rightarrow C_p(\mathbb{Q}_q) \neq \Phi$, so $p, -q \in S'(\phi)$.
Thus $S'(\phi) = \{1, p, -q, -pq\}$.

(2) For $E_{-4D} : y^2 = x^3 + 4Dx$, $\widehat{S} = \{\infty\} \bigcup \{2, p, q\}$, $\widehat{Q}(\widehat{S}, 2) =< -1, 2, p, q > \bigcup \{\infty\}$. $\forall d \in \widehat{Q}(\widehat{S}, 2)$, apply theorem (2) to investigate the local solution of $C_d : w^2 = d + \frac{4D}{d} z^4$.
Because of $4D > 0$, so $-1, -2, -p, -q, -2p, -2q, -2pq \notin S(\phi)$.
Because of $(\frac{2}{p}) = (-1)^{\frac{p-1}{2}} = -1 \Rightarrow C_2(\mathbb{Q}_p) = \Phi$, so $2, 2pq \notin S(\phi)$.
Because of $p \equiv 3 \ mod\ 4$, $\frac{4D}{4p} \equiv q \equiv 3 \ mod\ 4 \Rightarrow C_p(\mathbb{Q}_2) = \Phi$, so $p,\ q \notin S(\phi)$.
Because of $2p + \frac{D}{2p} \equiv 2p + 2q \equiv 12 \ mod\ 16 \Rightarrow C_{2p}(\mathbb{Q}_2) = \Phi$, so $2p, 2q \notin S(\phi)$.
Thus $S(\phi) = \{1, pq\}$.

D	r	p,q,r
$D \equiv 1 \bmod 8$	$r \equiv 1 \bmod 8$	$p \equiv 5,7 \bmod 8$ and $\left(\frac{D}{r}\right) = -1$
	$r \equiv 3 \bmod 8$	$p \equiv 3,7 \bmod 8$ and $\left(\frac{D}{r}\right) = -1$
	$r \equiv 7 \bmod 8$	$p \equiv 3,5 \bmod 8$ and $\left(\frac{D}{r}\right) = -1$
$D \equiv 3 \bmod 8$	$r \equiv 1 \bmod 8$	$p \equiv 5,7 \bmod 8$ and $\left(\frac{D}{r}\right) = -1$
	$r \equiv 3 \bmod 8$	$p \equiv 5,7 \bmod 8$
	$r \equiv 5 \bmod 8$	$p \equiv 1 \bmod 8$ and $\left(\frac{r}{p}\right) = -1$
		$p \equiv 3 \bmod 8$ and $\left(\frac{r}{q}\right) = -1$
		$p \equiv 5 \bmod 8$ and $\left(\frac{r}{q}\right) = 1$
		$p \equiv 7 \bmod 8$ and $\left(\frac{r}{p}\right) = 1$
	$r \equiv 7 \bmod 8$	$p \equiv 1,5 \bmod 8$ and $\left(\frac{r}{p}\right) = -1$
		$p \equiv 3,7 \bmod 8$ and $\left(\frac{r}{q}\right) = -1$
$D \equiv 5 \bmod 8$	$r \equiv 1 \bmod 8$	$p \equiv 3,7 \bmod 8$ and $\left(\frac{D}{r}\right) = -1$
	$r \equiv 3 \bmod 8$	$p \equiv 1,7 \bmod 8$ and $\left(\frac{r}{p}\right) = -1$
		$p \equiv 3,5 \bmod 8$ and $\left(\frac{r}{q}\right) = -1$
	$r \equiv 5 \bmod 8$	$p \equiv 3,7 \bmod 8$
	$r \equiv 7 \bmod 8$	$p \equiv 1 \bmod 8$ and $\left(\frac{r}{p}\right) = -1$
		$p \equiv 3 \bmod 8$ and $\left(\frac{r}{p}\right) = 1$
		$p \equiv 5 \bmod 8$ and $\left(\frac{r}{q}\right) = -1$
		$p \equiv 7 \bmod 8$ and $\left(\frac{r}{q}\right) = 1$
$D \equiv 7 \bmod 8$	$r \equiv 1 \bmod 8$	$p \equiv 3,5 \bmod 8$ and $\left(\frac{D}{r}\right) = -1$
	$r \equiv 3 \bmod 8$	$p \equiv 1 \bmod 8$ and $\left(\frac{r}{p}\right) = -1$
		$p \equiv 3 \bmod 8$ and $\left(\frac{r}{q}\right) = 1$
		$p \equiv 5 \bmod 8$ and $\left(\frac{r}{p}\right) = 1$
		$p \equiv 7 \bmod 8$ and $\left(\frac{r}{q}\right) = -1$
	$r \equiv 5 \bmod 8$	$p \equiv 1 \bmod 8$ and $\left(\frac{r}{p}\right) = -1$
		$p \equiv 3 \bmod 8$ and $\left(\frac{r}{p}\right) = 1$
		$p \equiv 5 \bmod 8$ and $\left(\frac{r}{q}\right) = 1$
		$p \equiv 7 \bmod 8$ and $\left(\frac{r}{q}\right) = -1$

Remaining Problem

- 1. While D varies in $\mathbb{Z}$, probability that the points on E_{Dr} can factor D.
- 2. More efficient way to find the point on E_{Dr}.
- 3.There is a way to find point on surface $y^2 = x^3 - Drz$?

Thanks!