Congruent Numbers and The Rank of Elliptic Curves

Yuanbo Liu [1, a]

[1]Qingdao University, Shandong Province ,China

liuyuanbo15@126.com

Keywords: Non-congruent number; Congruent number; Elliptic Curves

Abstract. Let p and q be prime with $p \equiv 3(\bmod 8)$ and $q \equiv 5(\bmod 8)$,and let $(\frac{p}{q}) = -1$. If $n = pq$, then n is a congruent if and only if the equation $2qw^2 = 1 + p^2 z^4$ has rational solutions. And The Birch Swinnerton-Dyer conjecture predicts that the rank of $E_n(Q)$ is one.

Introduction

If $n = \frac{1}{2}ab$ with rational numbers a, b being two right sides of a rational right triangle, the n is a congruent number. Otherwise n is a non-congruent number. The elliptic curve has an equation $E_n : y^2 = x^3 - n^2 x$, then n is a congruent if and only if $E_n(Q)$ has a non-zero rank. The problem of congruent number is very old and Arab scholars discussed it in the tenth century [1].

The Birch Swinnerton-Dyer conjecture predicts that if $n \equiv 5, 6 or 7(\bmod 8)$ it is a congruent [2]. The conjecture also made by Alter, Curtz and Kubota [3].

In this paper we discuss $n = pq$ with $p \equiv 3(\bmod 8)$ and $q \equiv 5(\bmod 8)$.

1. 2-isogeny

Let E/Q and E'/Q be Elliptic curves given respectively by the equations

$$E_n : y^2 = x^3 - n^2 x \text{ and } E'_n : y^2 = x^3 + 4n^2 x$$

and let

$$\phi : E \to E', \phi(x, y) = (y^2/x^2, y(x^2 + n^2)/x^2)$$

be the isogeny of degree 2 with kernel $E[\phi] = \{o, (0,0)\}$.

Then there is an exact sequence

$$0 \to E'(Q)/\phi(E(Q)) \to Q(S,2) \to WC(E/Q) \qquad (*)$$

$$(X, Y) \mapsto X \quad , \quad d \mapsto \{C_d/Q\}$$

$$o \mapsto 1$$

$$(0,0) \mapsto -1$$

where $S = \{\infty\} \cup \{p | 2n\}$ and $Q(S,2) = \{b \in Q^{*2}/Q^* : ord_p(b) \equiv 0(\bmod 2), \forall p \notin S\}$.

Furthermore, for each $d \in Q(S,2)$, let C_d/Q be the homogeneous space for E/Q by the equation $C_d : dw^2 = d^2 + 4n^2 z^4$. Then the ϕ-Selmer group is

$$S^{(\phi)}(E/Q) \cong \{d \in Q(S,2) : C_d(Q_p) \neq \varnothing, \forall p \in S\}.$$

Finally, we have the map

$$\varphi : C_d \to E', \varphi(z,w) = (\frac{d}{z^2}, -\frac{dw}{z^3}). (***)$$

Let $\hat{\phi} : E' \to E$ be the dual of ϕ so that $\phi\hat{\phi} = [2]$ and $\hat{\phi}\phi = [2]$. Let C'_d/Q be the homogeneous space for E'/Q by the equation $C'_d : dw^2 = d^2 - n^2 z^4$.Then the $\hat{\phi}$-Selmer group is

$$S^{(\hat{\phi})}(E'/Q) \cong \{d \in Q(S,2) : C'_d(Q_p) \neq \varnothing, \forall p \in S\}.$$

Moreover, we have the following exact sequences:

$$0 \to \frac{E'(Q)[\hat{\phi}]}{\phi(E(Q)[2])} \to \frac{E'(Q)}{\phi(E(Q))} \to \frac{E(Q)}{2E(Q)} \to \frac{E(Q)}{\hat{\phi}(E'(Q))} \to 0. \ (**)$$

2. n=pq

Lemma 1. Let $n = pq$ with $p \equiv 3 (\mathrm{mod}\, 8)$ and $q \equiv 5 (\mathrm{mod}\, 8)$,and let $(\frac{p}{q}) = -1$. Then the $\hat{\phi}$-Selmer group $S^{(\hat{\phi})}(E'/Q) = \{\pm 1, \pm n\}$, and $\frac{E(Q)}{\hat{\phi}(E'(Q))} = \{o, (0,0), (\pm n, 0)\}$.

Proof. We will use the exact sequence (*) to compute $\frac{E(Q)}{\hat{\phi}(E'(Q))}$. Now $S = \{2, p, q, \infty\}$ and

$$Q(S,2) = \{\pm 1, \pm 2, \pm p, \pm q, \pm 2p, \pm 2q, \pm pq, \pm 2pq\}.$$

For $d \in Q(S,2)$, C'_d has the equation

$$C'_d : dw^2 = d^2 - p^2 q^2 z^4 .$$

Claim: For each $d \in Q(S,2), d \neq \pm 1, \pm n$, there exist $p \in S$ such that $C'_d(Q_p) = \varnothing$.

1) $d = \pm p$, $C'_{\pm p} : \pm p w^2 = p^2 - p^2 q^2 z^4$. Let $(\frac{z'}{t}, \frac{w'}{t^2}) = (pz, pw)$ with $(z', w', t) \in Z$, then $C'_d : p w'^2 = t^4 - q^2 z'^4$. Since $q|t$ if and only if $q|w'$, Then suppose $(z', w', t) \in C'_{\pm p}(Q_q)$ with $0 \neq (z', w', t) \in Z_p$ and $ord_q w' = 0$. We have $(\frac{\pm p}{q}) = 1$, then $(\frac{p}{q}) = 1$ which contradicts $(\frac{p}{q}) = -1$. Therefore $C'_{\pm p}(Q_q) = \varnothing$.

2) $d = 2d'$, $d' \in Q(S,2)$ and $ord_2 d = 0$, $C'_d : 2d' w'^2 = 4d'^2 t^4 - p^2 q^2 z'^4$. Then $ord_2 2pw'^2 = 1 + 2k_1$, $ord_2 4d' t^4 = 2 + 4k_2$ and $ord_2(p^2 q^2 z'^4) = 4k_3$. Therefore $C'_{2d}(Q_2) = \varnothing$.

3) $d = \pm q$, $C'_{\pm q} : \pm q w^2 = q^2 - p^2 q^2 z^4$. Let $(\frac{z'}{t}, \frac{w'}{t^2}) = (qz, qw)$ with $(z', w', t) \in Z$, then $C'_d : q w'^2 = t^4 - p^2 z'^4$. Since $q|t$ if and only if $q|z'$. Then suppose $(z', w', t) \in C'_{\pm p}(Q_q)$ with $0 \neq (z', w', t) \in Z_p$ and $ord_q z' t = 0$. We have $(\frac{p^2}{q})_4 = 1$, then $(\frac{\pm p}{q}) = 1$ which contradicts $(\frac{p}{q}) = -1$. Therefore $C'_{\pm q}(Q_q) = \varnothing$.

This completes the proof of claim so we have $S^{(\hat{\phi})}(E'/Q) = \{\pm 1, \pm n\}$. Then $\frac{E(Q)}{\hat{\phi}(E'(Q))} = \{o, (0,0), (\pm n, 0)\}$,since $\{o, (0,0), (\pm n, 0)\} \in \frac{E(Q)}{\hat{\phi}(E'(Q))}$.

Lemma 2. Let $n = pq$ with $p \equiv 3 (\bmod 8)$ and $q \equiv 5 (\bmod 8)$,and let $(\frac{p}{q}) = -1$. Then the ϕ-Selmer group $S^{(\phi)}(E/Q) \in \{1, 2q\}$, and $\left|\frac{E'(Q)}{\phi(E(Q))}\right| \le 2$.

Proof . We also use the exact sequence (*) to compute $\frac{E'(Q)}{\phi(E(Q))}$. Now $S = \{2, p, q, \infty\}$ and

$$Q(S,2) = \{\pm 1, \pm 2, \pm p, \pm q, \pm 2p, \pm 2q, \pm pq, \pm 2pq\}.$$

For $d \in Q(S,2)$, C_d has the equation

$$C_d : dw^2 = d^2 + 4p^2q^2z^4.$$

Claim: For each $d \in Q(S,2)$, $d \ne 1, 2p$, there exist $p \in S$ such that $C_d(Q_p) = \varnothing$.

1) $C_d(Q_\infty) = \varnothing \Leftrightarrow d < 0$. Then $d > 0$.

2) $d = q, p$, $C_d : dw^2 = d^2 + 4p^2q^2z^4$. Let $(\frac{z'}{t}, \frac{w'}{t^2}) = (dz, dw)$ with $(z', w', t) \in Z$, then $C_d : dw'^2 = t^4 + 4\frac{n^2}{d^2}z'^4$. Since $\frac{n}{d}\big| t$ if and only if $\frac{n}{d}\big| w'$, then suppose $(z', w', t) \in C_d(Q_{\frac{n}{d}})$ with $0 \ne (z', w', t) \in Z_{\frac{n}{d}}$ and $ord_q w' = 0$. We have $(\frac{d}{n/d}) = 1$, which contradicts $(\frac{p}{q}) = -1$. Therefore $C_d(Q_{\frac{n}{d}}) = \varnothing$.

3) $p\big| d$, $C_d : dw'^2 = t^4 + 4\frac{n^2}{d^2}z'^4$ with $(z', w', t) \in Z$. Since $p\big| t$ if and only if $p\big| z'$,then suppose $(z', w', t) \in C_d(Q_p)$ with $0 \ne (z', w', t) \in Z_p$ and $ord_q tz' = 0$. Then $(\frac{-1}{p}) = 1$, which contradicts $p \equiv 3 (\bmod 8)$.

This completes the proof of claim so we have ϕ-Selmer group $S^{(\phi)}(E/Q) \in \{1, 2q\}$. Then $\left|\frac{E'(Q)}{\phi(E(Q))}\right| \le \left|S^{(\phi)}(E/Q)\right| \le 2$. This completes the proof of Lemma 2.

Theorem . Let p and q be prime satisfy $p \equiv 3 (\bmod 8)$ and $q \equiv 5 (\bmod 8)$,and let $(\frac{p}{q}) = -1$. If $n = pq$, then the rank of $E_n(Q)$ is one if and only if $C_{2q}(Q) \ne \varnothing$.

Proof. Since the exact sequence (**) ,Lemma1 and Lemma2, $E_n(Q)$ is one if and only if $\left|\frac{E'(Q)}{\phi(E(Q))}\right| > 1$. And $\left|\frac{E'(Q)}{\phi(E(Q))}\right| > 1$if and only if $C_{2q}(Q) \ne \varnothing$, since the map (***). This completes the proof of Theorem.

As we all know $C_{2q}(Q) \ne \varnothing$ if and only if $2qw^2 = 1 + p^2z^4$ has rational solutions. And this theorem proofs $r(E_n(Q)) \le 1$. The Birch Swinnerton-Dyer conjecture predicts that the rank of $E_n(Q)$ is non-zero with $n \equiv 5 (\bmod 8)$. Then the rank of $E_n(Q)$ is one and the equation $2qw^2 = 1 + q^2z^4$ have rational solutions.

References

[1] Feng K., Non-Congruent Numbers, Odd Graphs and the Birch-Swinnerton-Dyer Conjecture , Invent Math, (1987),89:527-560.

[2] Koblit W., Introduction to Elliptic Curves and Modular Forms, Springer-Verlag.(1973)

[3] R. Alter, T. B. Curtz and K. K. Kubota, Remarks and results on congruent numbers, in: Proc.3rd South Eastern Conf. Combin., Graph Theory and Compute., 1972, Florida Atlantic Univ., Boca Raton, Fla., (1972),27-35.

[4] Silverman J.H., The Arithmetic of Elliptic Curves, Springer-Verlag,.(1986)

