Submitted to Rocky Mountain Journal of Mathematics - NOT THE PUBLISHED VERSION

ROCKY MOUNTAIN JOURNAL OF MATHEMATICS
Vol. , No. , YEAR
https://doi.org/rmj.YEAR..PAGE

CRITERIA FOR DETERMINING NON-θ-CONGRUENT NUMBERS

VICTOR MANUEL ARICHETA, JERICO BACANI, AND RENZ JIMWEL MINA

ABSTRACT. This paper deals with the θ-congruent number problem and θ-congruent number elliptic curves, generalizations of the classical congruent number problem and congruent number elliptic curves. In particular, we identify sufficient conditions for a non-special angle θ and a prime p so that the corresponding θ-congruent number elliptic curve $E_{p,\theta}$ has rank zero. Consequently, we show that for infinitely many angles θ, there are infinitely many primes which are not θ-congruent.

1. Introduction

The congruent number problem is considered as one of the oldest problems in number theory. It asks which positive integers represent the area of a right triangle with rational sides. This problem remains open. Some notable progress towards its resolution include the works of Tunnell [8], Heegner [3], and Monsky [6]. A generalization of this problem was proposed by Fujiwara [1] and is called the *θ-congruent number problem*. For $\theta \in (0,\pi)$ such that $\cos\theta = \frac{s}{r}$, where $s,r \in \mathbb{Z}$, $r > |s|$ and $\gcd(s,r) = 1$, the θ-congruent number problem asks which positive integers n satisfy the condition that $n\sqrt{r^2-s^2}$ is the area of a triangle having an angle θ and rational sides. Positive integers satisfying this condition are called *θ-congruent*. A positive integer that is not θ-congruent is called *non-θ-congruent*. The case when $\theta = \pi/2$ is the classical congruent number problem.

Similar to the case of the classical congruent number problem, determining whether a positive integer is θ-congruent or not can be achieved by computing the (Mordell-Weil) rank of a certain elliptic curve. The *θ-congruent number elliptic curve*, or simply *θ-CN elliptic curve*, is the elliptic curve

$$E_{n,\theta} : y^2 = x^3 + 2snx^2 - (r^2 - s^2)n^2x.$$

Fujiwara [1] showed that a positive integer $n \neq 1,2,3,6$ is θ-congruent if and only if $E_{n,\theta}$ has positive rank. Thus, $n \neq 1,2,3,6$ is non-θ-congruent if and only if $E_{n,\theta}$ has rank zero.

Most of the results on the θ-congruent number problem involve the special angles $\theta = \pi/3$ and $2\pi/3$. These include the works of Fujiwara [1], Kan [5], Hibino and Kan [4], Yoshida [9, 10], and Goto [2]. The goal of this paper is to explore the case when θ is not a special angle, that is, when θ is not a rational multiple of π, with the added condition that $\cos\theta$ is also rational. This implies $(s,r) \neq (\pm 1,2)$. In particular, we prove the following theorems, which give sufficient conditions for a

...
...
...

2020 *Mathematics Subject Classification.* 11G05, 14H52.
Key words and phrases. elliptic curves, Selmer groups, θ-congruent number problem.

1 Aug 2024 06:25:26 PDT
230916-Mina Version 2 - Submitted to Rocky Mountain J. Math.

Submitted to Rocky Mountain Journal of Mathematics - NOT THE PUBLISHED VERSION

non-special angle θ and a prime p so that p is not θ-congruent. The Legendre symbol is denoted by $\left(\frac{\cdot}{\cdot}\right)$.

Theorem 1.1. *Let $\theta \in (0,\pi)$ be such that $\cos\theta = \frac{2k-1}{2k}$, where k is an odd number and $4k-1 = q^t$ for some prime q and positive integer t. Let $p \nmid 2kq$ be prime. If any one of the following holds,*

i. *$p \equiv 3 \pmod 4$, $\left(\frac{p}{q}\right) = 1$, and $\left(\frac{p}{k'}\right) = -1$ for all prime factors k' of k,*

ii. *$t = 1$, $k \equiv 3 \pmod 4$, and p satisfies both*
   a. *$p \equiv 3, 5, or\ 7 \pmod 8$, and $\left(\frac{p}{q}\right) = -1$,*
   b. *$\left(\frac{p}{k'}\right) = -1$ for all prime factors k' of k except for exactly one $k' \equiv 3 \pmod 4$,*

iii. *$t = 1$, $k \equiv 1 \pmod 4$, k has a prime factor $k' \equiv 3 \pmod 4$, and p satisfies both*
   a. *$p \equiv 1, 3, or\ 7 \pmod 8$, and $\left(\frac{p}{q}\right) = -1$,*
   b. *$\left(\frac{p}{k'}\right) = -1$ for all prime factors k' of k except for exactly one $k' \equiv 3 \pmod 4$,*

then $E_{p,\theta}$ has rank zero and p is not θ-congruent.

Theorem 1.2. *Let $\theta \in (0,\pi)$ be such that $\cos\theta = \frac{r-1}{r}$, where r is an odd number and $2r-1 = q^t$ for some prime q and positive integer t. Let $p \nmid 2rq$ be prime. If any one of the following holds,*

i. *t is odd, $r \equiv 1 \pmod 4$, and p satisfies the following,*
   a. *$p \equiv 3 \pmod 8$ and $\left(\frac{q}{p}\right) = -1$,*
   b. *$\left(\frac{p}{r'}\right) = -1$ for all prime factors r' of r,*

ii. *t is even, $q \equiv 3 \pmod 4$, and p satisfies the following,*
   a. *$p \equiv 3 \pmod 8$ and $\left(\frac{q}{p}\right) = -1$,*
   b. *$\left(\frac{p}{r'}\right) = -1$ for all prime factors r' of r,*

iii. *$t = 1$, $r \equiv 3 \pmod 4$, and p satisfies the following,*
   a. *$p \equiv 5\ or\ 7 \pmod 8$ and $\left(\frac{-q}{p}\right) = -1$,*
   b. *$\left(\frac{p}{r'}\right) = -1$ for all prime factors r' of r except for exactly one $r' \equiv 3 \pmod 4$,*

then $E_{p,\theta}$ has rank zero and p is not θ-congruent.

To prove Theorems 1.1 and 1.2, we use the method of descent via 2-isogeny. (See Section 2 for more details.) In particular, we show that the conditions given in Theorems 1.1 and 1.2 guarantee that the θ-CN elliptic curve $E_{p,\theta}$ has Selmer rank zero. The Selmer rank — which can be determined from an analysis of the solvability of certain homogenous spaces — gives an upper bound for the rank of an elliptic curve, so the rank of the θ-CN elliptic curve $E_{p,\theta}$ is also zero. By Fujiwara's result, the prime p is not θ-congruent.

Example 1.3. As an illustration, suppose $\cos\theta = \frac{5}{6}$, corresponding to the non-special angle $\theta \approx 33.557°$. Then $k = 3$, and $4k-1 = 11$ is prime. By Theorem 1.1 parts (i) and (ii), a prime $p \neq 2, 3, 11$ is not θ-congruent if one of the following holds:

a. $p \equiv 3 \pmod 4$, $\left(\frac{p}{11}\right) = 1$, and $\left(\frac{p}{3}\right) = -1$,
b. $p \equiv 3, 5, \text{or } 7 \pmod 8$, $\left(\frac{p}{11}\right) = -1$, and $\left(\frac{p}{3}\right) = 1$.

These conditions are equivalent to the following conditions, respectively:

a. $p \equiv 11 \pmod{12}$ and $p \equiv 1, 3, 4, 5, \text{or } 9 \pmod{11}$,
b. $p \equiv 7, 13, \text{or } 19 \pmod{24}$ and $p \equiv 2, 6, 7, 8, \text{or } 10 \pmod{11}$.

1 Aug 2024 06:25:26 PDT
230916-Mina Version 2 - Submitted to Rocky Mountain J. Math.

Submitted to Rocky Mountain Journal of Mathematics - NOT THE PUBLISHED VERSION

Note that these are sufficient conditions for a prime p to be non-θ-congruent, but they are not necessary. For example, the prime 17 is not θ-congruent since the rank of the corresponding θ-CN elliptic curve is zero.

Remark 1.4. To apply the method of descent via 2-isogeny, we need a list of the prime divisors of the discriminant $4^3r^2n^6(r^2-s^2)$ of $E_{n,\theta}$. We will assume in this paper that n is a prime number and $r^2-s^2=(r+s)(r-s)$ is an odd prime power to simplify this step. If $s>0$, then $r-s=1$, and if $s<0$, then $r+s=1$. In both cases, we get that $r^2-s^2=2r-1=q^t$ for some prime q and positive integer t. Additionally, we assume that r is an odd number or twice an odd number but not having n and q as its primes factors.

Let $q=8m+3$ be a prime number. Note that there are infinitely many such primes. For each such prime, consider the odd number $k=(q+1)/4=2m+1$ and the corresponding non-special angle $\theta=\cos^{-1}\frac{2k-1}{2k}$. Then any prime p that satisfies the conditions in Theorem 1.1 part (i) — for which there are infinitely many — is not θ-congruent. This yields the following corollary.

Corollary 1.5. *For infinitely many $\theta\in(0,\pi)$, there are infinitely many primes that are not θ-congruent.*

2. Preliminaries

We discuss briefly the method of descent via 2-isogeny. We refer the reader to Chapter X of [7] for more details about this method.

An *isogeny* from one elliptic curve to another is a homomorphism that is given by rational functions. If such a mapping exists, then we say that the two elliptic curves are *isogenous*. Note that there is an isogeny of degree two attached to the elliptic curve $E_{n,\theta}$ and it is given by $\phi: E_{n,\theta}\to E'_{n,\theta}$, $(x,y)\mapsto(y^2/x^2,-y((r^2-s^2)n^2+x^2)/x^2)$, where $E'_{n,\theta}: y^2=x^3-4snx^2+4r^2n^2x$. Also, there exists a map $\widehat{\phi}: E'_{n,\theta}\to E_{n,\theta}$ called the *dual isogeny to ϕ* given by $(x,y)\mapsto(y^2/4x^2, y(4r^2n^2-x^2)/8x^2)$. Let

$$S:=\{\text{primes } p \text{ such that } p\mid\Delta_{E_{n,\theta}}=4^3r^2n^6(r^2-s^2)\}\cup\{\infty\}$$

and

$$\mathbb{Q}(S,2):=\{d\in\mathbb{Q}^*/(\mathbb{Q}^*)^2:\operatorname{ord}_p(d)\equiv 0 \pmod 2 \text{ for all primes } p\notin S\},$$

where ord_p is the p-adic valuation on $\mathbb{Q}$. For each $d\in\mathbb{Q}(S,2)$, define the *homogeneous spaces*

$$C_d/\mathbb{Q}: dw^2=d^2-4sndz^2+4r^2n^2z^4$$

and

$$C'_d/\mathbb{Q}: dw^2=d^2+8sndz^2-16(r^2-s^2)n^2z^4.$$

For simplicity, we may replace z by $z/2$ in the second homogeneous space to obtain

$$C'_d/\mathbb{Q}: dw^2=d^2+2sndz^2-(r^2-s^2)n^2z^4.$$

The *ϕ-Selmer group* and *$\widehat{\phi}$-Selmer group* are defined as

$$S^{(\phi)}(E_{n,\theta}/\mathbb{Q}):=\{d\in\mathbb{Q}(S,2):C_d(\mathbb{Q}_p)\neq\emptyset\ \forall\ p\in S\},$$

$$S^{(\widehat{\phi})}(E'_{n,\theta}/\mathbb{Q}):=\{d\in\mathbb{Q}(S,2):C'_d(\mathbb{Q}_p)\neq\emptyset\ \forall\ p\in S\},$$

1 Aug 2024 06:25:26 PDT
230916-Mina Version 2 - Submitted to Rocky Mountain J. Math.

Submitted to Rocky Mountain Journal of Mathematics - NOT THE PUBLISHED VERSION

respectively. Define the map $\delta : E'(\mathbb{Q}) \longrightarrow \mathbb{Q}^*/(\mathbb{Q}^*)^2$ by

$$\begin{aligned} \delta(\mathscr{O}) &= 1 \pmod{(\mathbb{Q}^*)^2}, \\ \delta(0,0) &= 4r^2n^2 \equiv 1 \pmod{(\mathbb{Q}^*)^2}, \\ \delta(x,y) &= x \pmod{(\mathbb{Q}^*)^2}, \ (x,y) \neq (0,0), \mathscr{O}, \end{aligned}$$

where $\mathscr{O}$ is the point at infinity. Similarly, define $\delta' : E(\mathbb{Q}) \longrightarrow \mathbb{Q}^*/(\mathbb{Q}^*)^2$ by

$$\begin{aligned} \delta'(\mathscr{O}) &= 1 \pmod{(\mathbb{Q}^*)^2}, \\ \delta'(0,0) &= -(r^2 - s^2) \pmod{(\mathbb{Q}^*)^2}, \\ \delta'(x,y) &= x \pmod{(\mathbb{Q}^*)^2}, \ (x,y) \neq (0,0), \mathscr{O}. \end{aligned}$$

The images of the maps δ and δ' are values $d \in \mathbb{Q}(S,2)$ that are elements of the corresponding Selmer groups. An upper bound for the rank of $E_{n,\theta}$ is given by

$$\operatorname{rank}(E_{n,\theta}(\mathbb{Q})) \leq \dim_{\mathbb{F}_2} S^{(\phi)}(E_{n,\theta}/\mathbb{Q}) + \dim_{\mathbb{F}_2} S^{(\widehat{\phi})}(E'_{n,\theta}/\mathbb{Q}) - 2.$$

This bound is also called the *Selmer rank*. Thus, we only need to determine when the Selmer rank becomes zero.

3. Proof of main results

We have the following proofs of the two theorems.

Proof of Theorem 1.1. First, consider part (i). The θ-CN elliptic curve is given by

$$E_{p,\theta} : y^2 = x^3 + 2(2k-1)px^2 - (4k-1)p^2x.$$

Write $k = k_1^{m_1} k_2^{m_2} \cdots k_n^{m_n}$, where k_i's are distinct odd primes and m_i's are positive integers. We obtain the sets $S = \{\infty, 2, k_1, k_2, \ldots, k_n, q, p\}$ and

$$\mathbb{Q}(S,2) = \left\{ \begin{array}{l} \pm 1, \pm 2, \pm p, \pm q, \pm 2p, \pm 2q, \pm pq, \pm 2pq, \pm k_{i_1} \cdots k_{i_j}, \\ \pm 2k_{i_1} \cdots k_{i_j}, \pm pk_{i_1} \cdots k_{i_j}, \pm qk_{i_1} \cdots k_{i_j}, \pm 2pk_{i_1} \cdots k_{i_j}, \\ \pm 2qk_{i_1} \cdots k_{i_j}, \pm pqk_{i_1} \cdots k_{i_j}, \pm 2pqk_{i_1} \cdots k_{i_j}, \\ \text{where } i_j, j \in \{1,2,\ldots,n\} \text{ and } i_j \neq i_{j'} \text{ for } j \neq j' \end{array} \right\}.$$

Note that $\mathbb{Q}(S,2)$ contains 2^{n+4} distinct elements. The curve is 2-isogenous to $E'_{p,\theta}$ given by

$$E'_{p,\theta} : y^2 = x^3 - 4(2k-1)px^2 + 16k^2p^2x,$$

and for $d \in \mathbb{Q}(S,2)$, the corresponding homogeneous spaces are given by

$$C_d : dw^2 = d^2 - 4(2k-1)pdz^2 + 16k^2p^2z^4 \tag{1}$$

and

$$C'_d : dw^2 = d^2 + 2(2k-1)pdz^2 - (4k-1)p^2z^4. \tag{2}$$

Note that the image of $(0,0)$ and $\mathscr{O}$ under δ is $1 \in S^{(\phi)}(E_{p,\theta}/\mathbb{Q})$. The other values of $d \in \mathbb{Q}(S,2)$ are considered below. For the following cases, we denote by $f(w)$ and $g(z)$ the left-hand side and right-hand side of Equation (1), respectively.

Submitted to Rocky Mountain Journal of Mathematics - NOT THE PUBLISHED VERSION

1.1 $d < 0$. Note that $C_d(\mathbb{R}) = \emptyset$ since $f(w) \leq 0$, while $g(z) > 0$.

1.2 $d = 2d'$ for some d'. Let $(z,w) \in C_d(\mathbb{Q}_2)$. Note that $\mathrm{ord}_2(f(w))$ is odd. On the other hand, let $\mathrm{ord}_2(z) = v$. Then $\mathrm{ord}_2(d^2) = 2$, $\mathrm{ord}_2(-4(2k-1)pdz^2) = 3+2v$, and $\mathrm{ord}_2(16k^2p^2z^4) = 4+4v$, all of which are distinct. Hence, $\mathrm{ord}_2(g(z)) = \min\{2, 3+2v, 4+4v\} = 2$ or $4+4v$, which in any case is even, so a contradiction. Thus, $C_d(\mathbb{Q}_2) = \emptyset$.

1.3 $d = qd'$ for some d'. Let $(z,w) \in C_d(\mathbb{Q}_q)$. Note that $\mathrm{ord}_q(f(w))$ is odd. On the other hand, let $\mathrm{ord}_q(z) = v$. Then $\mathrm{ord}_q(g(z)) = 2$ or $4v$, which in any case is even, so a contradiction. Thus, $C_d(\mathbb{Q}_q) = \emptyset$.

1.4 $d = k_i d'$ for some d'. Let $(z,w) \in C_d(\mathbb{Q}_{k_i})$.

1.4.1 Suppose $\mathrm{ord}_{k_i}(z) > 0$. Note that $\mathrm{ord}_{k_i}(f(w))$ is odd. On the other hand, $\mathrm{ord}_{k_i}(g(z)) = 2$, which is even, so a contradiction. Thus, $C_d(\mathbb{Q}_{k_i}) = \emptyset$.

1.4.2 Suppose $\mathrm{ord}_{k_i}(z) = 0$. Note that $\mathrm{ord}_{k_i}(g(z)) \geq 1$. This implies that $\mathrm{ord}_{k_i}(f(w)) \geq 1$, so $\mathrm{ord}_{k_i}(w) \geq 0$. Hence, $z, w \in \mathbb{Z}_{k_i}$. Dividing both sides of Equation (1) by k_i and reducing modulo k_i, we get $d'w^2 \equiv 4pd'z^2 \pmod{k_i}$. This implies that $\left(\frac{p}{k_i}\right) = 1$.

1.4.3 Suppose $\mathrm{ord}_{k_i}(z) =: -v < 0$. Let $z = Z/k_i^v$, so that $\mathrm{ord}_{k_i}(Z) = 0$. By simplifying, we get

$$k_i^{4v+1}d'w^2 = k_i^{4v+2}d'^2 - 4(2k-1)pk_i^{2v+1}d'Z^2 + 16k^2p^2Z^4. \tag{3}$$

We abuse notation and denote by $f(w)$ and $g(Z)$ the left-hand side and right-hand side of Equation (3), respectively.

1.4.3.1 Suppose $2v+1 > 2m_i$. Note that $\mathrm{ord}_{k_i}(f(w))$ is odd. On the other hand, $\mathrm{ord}_{k_i}(g(Z)) = 2m_i$, which is even, so a contradiction. Thus, $C_d(\mathbb{Q}_{k_i}) = \emptyset$.

1.4.3.2 Suppose $2v+1 < 2m_i$. Note that $\mathrm{ord}_{k_i}(g(Z)) = 2v+1$. This implies that $\mathrm{ord}_{k_i}(f(w)) = 2v+1$, so $\mathrm{ord}_{k_i}(w) = -v$. Let $w = W/k_i^v$, so that $\mathrm{ord}_{k_i}(W) = 0$. Then $Z, W \in \mathbb{Z}_{k_i}$. Dividing both sides of Equation (3) by k_i^{2v+1} and reducing modulo k_i, we get $d'W^2 \equiv 4pd'Z^2 \pmod{k_i}$. This implies that $\left(\frac{p}{k_i}\right) = 1$.

Thus, if $\left(\frac{p}{k_i}\right) = -1$ then $C_d(\mathbb{Q}_{k_i}) = \emptyset$.

1.5 $d = p$. Let $(z,w) \in C_d(\mathbb{Q}_2)$.

1.5.1 Suppose $\mathrm{ord}_2(z) \geq 0$. Note that $\mathrm{ord}_2(g(z)) = 0$. This implies that $\mathrm{ord}_2(f(w)) = 0$, so $\mathrm{ord}_2(w) = 0$. Hence, $z, w \in \mathbb{Z}_2$. Reducing Equation (1) modulo 4, we get $pw^2 \equiv 1 \pmod 4$. Thus, $p \equiv 1 \pmod 4$.

1.5.2 Suppose $\mathrm{ord}_2(z) =: -v < 0$. Let $z = Z/2^v$, so that $\mathrm{ord}_2(Z) = 0$. By simplifying, we get

$$2^{4v-4}w^2 = 2^{4v-4}p - 2^{2v-2}(2k-1)pZ^2 + k^2pZ^4. \tag{4}$$

We abuse notation and denote by $f(w)$ and $g(Z)$ the left-hand side and right-hand side of Equation (4), respectively.

1.5.2.1 Suppose $v = 1$. Note that $\mathrm{ord}_2(g(Z)) \geq 0$. Then $\mathrm{ord}_2(f(w)) \geq 0$, so $\mathrm{ord}_2(w) \geq 0$. Hence, $Z, w \in \mathbb{Z}_2$. Reducing Equation (4) modulo 4, we get $w^2 \equiv p \pmod 4$. Thus, $p \equiv 1 \pmod 4$.

1.5.2.2 Suppose $v > 1$. Note that $\mathrm{ord}_2(g(Z)) = 0$. This implies $\mathrm{ord}_2(f(w)) = 0$, so $\mathrm{ord}_2(w) = -(2v-2)$. Let $w = W/2^{2v-2}$, so that $\mathrm{ord}_2(W) = 0$. Then $Z, W \in \mathbb{Z}_2$. Reducing Equation (4) modulo 4, we get $W^2 \equiv p \pmod 4$. Thus, $p \equiv 1 \pmod 4$.

Thus, if $p \equiv 3 \pmod 4$ then $C_d(\mathbb{Q}_2) = \emptyset$.

1 Aug 2024 06:25:26 PDT
230916-Mina Version 2 - Submitted to Rocky Mountain J. Math.

Submitted to Rocky Mountain Journal of Mathematics - NOT THE PUBLISHED VERSION

We have shown that if $\left(\frac{p}{k_i}\right) = -1$ for all $i = 1, \ldots, n$, and $p \equiv 3 \pmod 4$, then $S^{(\phi)}(E_{p,\theta}/\mathbb{Q}) = \{1\}$.

The group $S^{(\widehat{\phi})}(E'_{p,\theta}/\mathbb{Q})$ is considered next. Note that $2r-1 = 4k-1 = q^t$ implies $q \equiv 3 \pmod 4$ and t is odd. Thus, $-(4k-1) = -q^t \equiv -q \pmod{(\mathbb{Q}^*)^2}$. Note that the images of $\mathscr{O}$ and $(0,0)$ under δ' are $1, -q \in S^{(\widehat{\phi})}(E'_{p,\theta}/\mathbb{Q})$, respectively. The other values of $d \in \mathbb{Q}(S,2)$ are considered below. For the following cases, we denote by $f(w)$ and $g(z)$ the left-hand side and right-hand side of Equation (2), respectively.

2.1 $d = p, -qp$. The homogeneous space (2) has a global solution $(z,w) = (1,0)$. Thus, $p \in S^{(\widehat{\phi})}(E'_{p,\theta}/\mathbb{Q})$. By closure property, since $-q, p \in S^{(\widehat{\phi})}(E'_{p,\theta}/\mathbb{Q})$, we have $-qp \in S^{(\widehat{\phi})}(E'_{p,\theta}/\mathbb{Q})$.

2.2 $d = k_i d'$ for some d'. Let $(z,w) \in C'_d(\mathbb{Q}_{k_i})$. Note that $\operatorname{ord}_{k_i}(f(w))$ is odd. On the other hand, let $\operatorname{ord}_{k_i}(z) = v$. Then $\operatorname{ord}_{k_i}(g(z)) = 2$ or $4v$, which in any case is even, so a contradiction. Thus, $C'_d(\mathbb{Q}_{k_i}) = \emptyset$.

2.3 $d = 2d'$ for some d'. Let $(z,w) \in C'_d(\mathbb{Q}_2)$. Note that $\operatorname{ord}_2(f(w))$ is odd. On the other hand, let $\operatorname{ord}_2(z) = v$.

2.3.1 Suppose $v \neq 0, 1$. Then $\operatorname{ord}_2(g(z)) = 2$ or $4v$, which in any case is even, so a contradiction.

2.3.2 Suppose $v = 0$. Then $\operatorname{ord}_2(g(z)) = 0$, which is even, so a contradiction.

2.3.3 Suppose $v = 1$. Then $\operatorname{ord}_2(g(z)) = 2$, which is even, so a contradiction.

Therefore, $C'_d(\mathbb{Q}_2) = \emptyset$.

2.4 $d = q$. Let $(z,w) \in C'_d(\mathbb{Q}_p)$. Note that $\operatorname{ord}_p(2k-1) \geq 0$.

2.4.1 Suppose $\operatorname{ord}_p(z) \geq 0$. Note that $\operatorname{ord}_p(g(z)) \geq 0$. This implies that $\operatorname{ord}_p(f(w)) \geq 0$, so $\operatorname{ord}_p(w) \geq 0$. Hence, $z, w \in \mathbb{Z}_p$. Reducing Equation (2) modulo p, we get $w^2 \equiv q \pmod p$. Thus, $\left(\frac{q}{p}\right) = 1$.

2.4.2 Suppose $\operatorname{ord}_p(z) =: -v < 0$. Note that $\operatorname{ord}_p(g(z)) = 2-4v$. This implies that $\operatorname{ord}_p(f(w)) = 2-4v$, so $\operatorname{ord}_p(w) = -(2v-1)$. Letting $(z,w) = (Z/p^v, W/p^{2v-1})$ and by simplifying, we get

$$W^2 = p^{4v-2}q + 2(2k-1)p^{2v-1}Z^2 - q^{t-1}Z^4, \tag{5}$$

and $\operatorname{ord}_p(Z) = \operatorname{ord}_p(W) = 0$. Then $Z, W \in \mathbb{Z}_p$. Reducing Equation (5) modulo p, we get $W^2 \equiv -q^{t-1}Z^4 \pmod p$. Thus, $\left(\frac{-1}{p}\right) = 1$, i.e., $p \equiv 1 \pmod 4$.

Thus, if $\left(\frac{q}{p}\right) = -1$ and $p \equiv 3 \pmod 4$ then $C'_d(\mathbb{Q}_p) = \emptyset$.

2.5 $d = -1, qp, -p$. By closure property, if $\left(\frac{q}{p}\right) = -1$ and $p \equiv 3 \pmod 4$ then $q \notin S^{(\widehat{\phi})}(E'_{p,\theta}/\mathbb{Q})$, and $-q, p, -qp \in S^{(\widehat{\phi})}(E'_{p,\theta}/\mathbb{Q})$ implies that $-1, qp, -p \notin S^{(\widehat{\phi})}(E'_{p,\theta}/\mathbb{Q})$.

By reciprocity law, we have shown that if $p \equiv 3 \pmod 4$ and $\left(\frac{p}{q}\right) = 1$, then we obtain $S^{(\widehat{\phi})}(E'_{p,\theta}/\mathbb{Q}) = \{1, -q, p, -qp\}$. Therefore, if part (i) holds then

$$S^{(\phi)}(E_{p,\theta}/\mathbb{Q}) = \{1\} \quad \text{and} \quad S^{(\widehat{\phi})}(E'_{p,\theta}/\mathbb{Q}) = \{1, -q, p, -qp\} \cong (\mathbb{Z}/2\mathbb{Z})^2.$$

Thus, $\operatorname{rank}(E_{p,\theta}(\mathbb{Q})) \leq 0 + 2 - 2 = 0$.

Next, we prove part (ii). We use the same set-up as above. For the group $S^{(\phi)}(E_{p,\theta}/\mathbb{Q})$, cases 1.1, 1.2 and 1.3 of part (i) still hold, and $1 \in S^{(\phi)}(E_{p,\theta}/\mathbb{Q})$. We consider the remaining cases.

1.4 $d = pd'$ for some d'. Let $(z,w) \in C_d(\mathbb{Q}_p)$.

Submitted to Rocky Mountain Journal of Mathematics - NOT THE PUBLISHED VERSION

1.4.1 Suppose $\mathrm{ord}_p(z) > 0$. Note that $\mathrm{ord}_p(f(w))$ is odd. On the other hand, $\mathrm{ord}_p(g(z)) = 2$, which is even, so a contradiction. Thus, $C_d(\mathbb{Q}_p) = \emptyset$.

1.4.2 Suppose $\mathrm{ord}_p(z) = 0$. Note that $\mathrm{ord}_p(g(z)) \geq 2$. This implies that $\mathrm{ord}_p(f(w)) \geq 2$, so $\mathrm{ord}_p(w) \geq 1$. Letting $w = pW$, we get $pd'W^2 = d'^2 - 4(2k-1)d'z^2 + 16k^2z^4$ and $\mathrm{ord}_p(W) \geq 0$. Hence, $z, W \in \mathbb{Z}_p$. Reducing this equation modulo p, we get $d'^2 - 4(2k-1)d'z^2 + 16k^2z^4 \equiv 0 \pmod{p}$. Multiplying both sides by $4k^2$ and adding both sides by $-d'^2(4k-1)$, we get $(8k^2z^2 - (2k-1)d')^2 \equiv -d'^2(4k-1) \pmod{p}$. This implies that $\left(\frac{-(4k-1)}{p}\right) = \left(\frac{-q}{p}\right) = 1$.

1.4.3 Suppose $\mathrm{ord}_p(z) =: -v < 0$. Note that $\mathrm{ord}_p(f(w))$ is odd. On the other hand, $\mathrm{ord}_p(g(z)) = 2 - 4v$, which is even, so a contradiction. Thus, $C_d(\mathbb{Q}_p) = \emptyset$.

Thus, if $\left(\frac{-q}{p}\right) = -1$ then $C_d(\mathbb{Q}_p) = \emptyset$.

1.5 $d = k_i d'$ for some d'. Here, k_i could be any prime factor of k but we exclude exactly one k_i that is congruent to 3 modulo 4 and we treat this case in item 1.6. The existence of such prime factor is valid since $k \equiv 3 \pmod{4}$ by assumption. In this case, if $\left(\frac{p}{k_i}\right) = -1$ then $C_d(\mathbb{Q}_{k_i}) = \emptyset$. The proof is identical to case 1.4 of part (i).

1.6 $d = k_i$ where $k_i \equiv 3 \pmod{4}$ is the prime factor of k excluded in case 1.5. Replacing z by $z/2$, we get

$$k_i w^2 = k_i^2 - (2k-1)pk_i z^2 + k^2p^2z^4. \tag{6}$$

Denote by $g(z)$ the right-hand side of Equation (6). Let $(z, w) \in C_d(\mathbb{Q}_2)$.

1.6.1 Suppose $\mathrm{ord}_2(z) \geq 0$. Note that $\mathrm{ord}_2(g(z)) \geq 0$. This implies that $\mathrm{ord}_2(f(w)) \geq 0$, so $\mathrm{ord}_2(w) \geq 0$. Hence, $z, w \in \mathbb{Z}_2$. Reducing Equation (6) modulo 8, we get $k_i w^2 \equiv 1 - (2k-1)pk_i z^2 + z^4 \pmod{8}$. By assumption, $k_i \equiv 3 \pmod{4}$ and $k \equiv 3 \pmod{4}$.

1.6.1.1 Suppose $\mathrm{ord}_2(z) = 0$. Then $k_i w^2 \equiv 1 + 3pk_i + 1 \equiv 2 + 3pk_i \pmod{8}$. This implies that $w^2 \equiv 2k_i + 3p \equiv 6 + 3p \pmod{8}$, so $p \equiv 1 \pmod{8}$.

1.6.1.2 Suppose $\mathrm{ord}_2(z) = 1$. Then $k_i w^2 \equiv 1 + 3pk_i(4) + 0 \equiv 5 \pmod{8}$, a contradiction.

1.6.1.3 Suppose $\mathrm{ord}_2(z) > 1$. Then $k_i w^2 \equiv 1 \pmod{8}$, a contradiction.

1.6.2 Suppose $\mathrm{ord}_2(z) =: -v < 0$. Note that $\mathrm{ord}_2(g(z)) = -4v$. This implies that $\mathrm{ord}_2(f(w)) = -4v$, so $\mathrm{ord}_2(w) = -2v$. Letting $(z, w) = (Z/2^v, W/2^{2v})$ and by simplifying, we get

$$k_i W^2 = 2^{4v}k_i^2 - 2^{2v}(2k-1)pk_i Z^2 + k^2p^2Z^4, \tag{7}$$

and $\mathrm{ord}_2(Z) = \mathrm{ord}_2(W) = 0$. Then $Z, W \in \mathbb{Z}_2$. Reducing Equation (7) modulo 4, we get $k_i W^2 \equiv 1 \pmod{4}$, a contradiction since $k_i \equiv 3 \pmod{4}$. Thus, $C_d(\mathbb{Q}_2) = \emptyset$.

Thus, if $p \equiv 3, 5, \text{or } 7 \pmod{8}$ then $C_d(\mathbb{Q}_2) = \emptyset$.

By reciprocity law, we have shown that if $\left(\frac{p}{q}\right) = -1$, $\left(\frac{p}{k_i}\right) = -1$ for all k_i except one $k_i \equiv 3 \pmod{4}$, and $p \equiv 3, 5, \text{ or } 7 \pmod{8}$, then $S^{(\phi)}(E_{p,\theta}/\mathbb{Q}) = \{1\}$.

Next, we consider $S^{(\widehat{\phi})}(E'_{p,\theta}/\mathbb{Q})$. Note that cases 2.1, 2.2, and 2.3 of part (i) still hold and $1, -q \in S^{(\widehat{\phi})}(E'_{p,\theta}/\mathbb{Q})$. We consider the remaining cases.

2.4 $d = q$. Let $(z, w) \in C'_d(\mathbb{Q}_{k_i})$, where $k_i \equiv 3 \pmod{4}$ is the prime factor of k excluded in case 1.5.

Submitted to Rocky Mountain Journal of Mathematics - NOT THE PUBLISHED VERSION

2.4.1 Suppose $\operatorname{ord}_{k_i}(z) \geq 0$. Note that $\operatorname{ord}_{k_i}(g(z)) \geq 0$. This implies that $\operatorname{ord}_{k_i}(f(w)) \geq 0$, so $\operatorname{ord}_{k_i}(w) \geq 0$. Hence, $z, w \in \mathbb{Z}_{k_i}$. Note that $t = 1$ by assumption, so $4k - 1 = q$. Dividing both sides of Equation (2) by q and reducing modulo k_i, we get $w^2 \equiv -1 - 2pz^2 - p^2z^4 \pmod{k_i}$, that is, $w^2 \equiv -(pz^2+1)^2 \pmod{k_i}$. If $\operatorname{ord}_{k_i}(pz^2+1) = 0$, then $\left(\frac{-1}{k_i}\right) = 1$, a contradiction since $k_i \equiv 3 \pmod 4$. Thus, $pz^2 + 1 \equiv 0 \pmod{k_i}$, that is, $\left(\frac{-p}{k_i}\right) = 1$. Since $\left(\frac{-1}{k_i}\right) = -1$, we obtain $\left(\frac{p}{k_i}\right) = -1$.

2.4.2 Suppose $\operatorname{ord}_{k_i}(z) =: -v < 0$. Note that $\operatorname{ord}_{k_i}(g(z)) = -4v$. This implies that $\operatorname{ord}_{k_i}(f(w)) = -4v$, so $\operatorname{ord}_{k_i}(w) = -2v$. Letting $(z,w) = (Z/k_i^v, W/k_i^{2v})$ and by simplifying, we get

$$W^2 = k_i^{4v}q + 2(2k-1)pk_i^{2v}Z^2 - p^2Z^4, \tag{8}$$

and $\operatorname{ord}_{k_i}(Z) = \operatorname{ord}_{k_i}(W) = 0$. Then $Z, W \in \mathbb{Z}_{k_i}$. Reducing Equation (8) modulo k_i, we get $W^2 \equiv -p^2Z^4 \pmod{k_i}$, that is, $\left(\frac{-1}{k_i}\right) = 1$, a contradiction since $k_i \equiv 3 \pmod 4$. Thus, $C'_d(\mathbb{Q}_{k_i}) = \emptyset$.

Thus, if $\left(\frac{p}{k_i}\right) = 1$ then $C'_d(\mathbb{Q}_{k_i}) = \emptyset$.

2.5 $d = -1, qp, -p$. By closure property, if $\left(\frac{p}{k_i}\right) = 1$ then $q \notin S^{(\widehat{\phi})}(E'_{p,\theta}/\mathbb{Q})$, and $-q, p, -qp \in S^{(\widehat{\phi})}(E'_{p,\theta}/\mathbb{Q})$ implies that $-1, qp, -p \notin S^{(\widehat{\phi})}(E'_{p,\theta}/\mathbb{Q})$.

We have shown that if $\left(\frac{p}{k_i}\right) = 1$ for exactly one $k_i \equiv 3 \pmod 4$, then $S^{(\widehat{\phi})}(E'_{p,\theta}/\mathbb{Q}) = \{1, -q, p, -qp\}$. Therefore, if part (ii) holds then

$$S^{(\phi)}(E_{p,\theta}/\mathbb{Q}) = \{1\} \quad \text{and} \quad S^{(\widehat{\phi})}(E'_{p,\theta}/\mathbb{Q}) = \{1, -q, p, -qp\} \cong (\mathbb{Z}/2\mathbb{Z})^2.$$

Thus, $\operatorname{rank}(E_{p,\theta}(\mathbb{Q})) \leq 0 + 2 - 2 = 0$.

Lastly, we prove part (iii). For $S^{(\phi)}(E_{p,\theta}/\mathbb{Q})$, all of the cases of part (ii) hold except case 1.6.

1.6 $d = k_i$, where $k_i \equiv 3 \pmod 4$ is the prime factor of k excluded in case 1.5 of part (ii). Replacing z by $z/2$, we get

$$k_iw^2 = k_i^2 - (2k-1)pk_iz^2 + k^2p^2z^4. \tag{9}$$

Denote by $g(z)$ the right-hand side of Equation (9). Let $(z,w) \in C_d(\mathbb{Q}_2)$.

1.6.1 Suppose $\operatorname{ord}_2(z) \geq 0$. Note that $\operatorname{ord}_2(g(z)) \geq 0$. This implies that $\operatorname{ord}_2(f(w)) \geq 0$, so $\operatorname{ord}_2(w) \geq 0$. Hence, $z, w \in \mathbb{Z}_2$. Reducing Equation (9) modulo 8, we get $k_iw^2 \equiv 1 - (2k-1)pk_iz^2 + z^4 \pmod 8$. By assumption, $k_i \equiv 3 \pmod 4$ and $k \equiv 1 \pmod 4$.

1.6.1.1 Suppose $\operatorname{ord}_2(z) = 0$. Then $k_iw^2 \equiv 1 - pk_i + 1 \equiv 2 - pk_i \pmod 8$. This implies that $w^2 \equiv 2k_i - p \equiv 6 - p \pmod 8$, so $p \equiv 5 \pmod 8$.

1.6.1.2 Suppose $\operatorname{ord}_2(z) = 1$. Then $k_iw^2 \equiv 1 - 4pk_i + 0 \equiv 5 \pmod 8$, so a contradiction.

1.6.1.3 Suppose $\operatorname{ord}_2(z) > 1$. Then $k_iw^2 \equiv 1 \pmod 8$, so a contradiction.

1.6.2 Suppose $\operatorname{ord}_2(z) =: -v < 0$. Note that $\operatorname{ord}_2(g(z)) = -4v$. This implies that $\operatorname{ord}_2(f(w)) = -4v$, so $\operatorname{ord}_2(w) = -2v$. Letting $(z,w) = (Z/2^v, W/2^{2v})$ and by simplifying, we get

$$k_iW^2 = 2^{4v}k_i^2 - 2^{2v}(2k-1)pk_iZ^2 + k^2p^2Z^4, \tag{10}$$

and $\operatorname{ord}_2(Z) = \operatorname{ord}_2(W) = 0$. Then $Z, W \in \mathbb{Z}_2$. Reducing Equation (10) modulo 4, we get $k_iW^2 \equiv 1 \pmod 4$, a contradiction since $k_i \equiv 3 \pmod 4$. Thus, $C_d(\mathbb{Q}_2) = \emptyset$.

Thus, if $p \equiv 1, 3, \text{or } 7 \pmod 8$ then $C_d(\mathbb{Q}_2) = \emptyset$.

1 Aug 2024 06:25:26 PDT
230916-Mina Version 2 - Submitted to Rocky Mountain J. Math.

Submitted to Rocky Mountain Journal of Mathematics - NOT THE PUBLISHED VERSION

We have shown that if $\left(\frac{p}{q}\right) = -1$, $\left(\frac{p}{k_i}\right) = -1$ for all k_i except one $k_i \equiv 3 \pmod 4$, and $p \equiv 1, 3,$ or $7 \pmod 8$, then $S^{(\phi)}(E_{p,\theta}/\mathbb{Q}) = \{1\}$.

For $S^{(\widehat{\phi})}(E'_{p,\theta}/\mathbb{Q})$, all of the cases in part (ii) hold. Thus, if $\left(\frac{p}{k_i}\right) = 1$ for exactly one $k_i \equiv 3 \pmod 4$, then $S^{(\widehat{\phi})}(E'_{p,\theta}/\mathbb{Q}) = \{1, -q, p, -qp\}$. Therefore, if part (iii) holds then

$$S^{(\phi)}(E_{p,\theta}/\mathbb{Q}) = \{1\} \quad \text{and} \quad S^{(\widehat{\phi})}(E'_{p,\theta}/\mathbb{Q}) = \{1, -q, p, -qp\} \cong (\mathbb{Z}/2\mathbb{Z})^2.$$

Thus, $\operatorname{rank}(E_{p,\theta}(\mathbb{Q})) \leq 0 + 2 - 2 = 0$. $\square$

We prove the second theorem.

Proof of Theorem 1.2. First, consider part (i). The θ-CN elliptic curve is given by

$$E_{p,\theta} : y^2 = x^3 + 2(r-1)px^2 - (2r-1)p^2x.$$

Write $r = r_1^{m_1} r_2^{m_2} \cdots r_n^{m_n}$, where r_i's are distinct odd primes and m_i's are positive integers. We obtain the sets $S = \{\infty, 2, r_1, r_2, \ldots, r_n, q, p\}$ and

$$\mathbb{Q}(S,2) = \left\{ \begin{array}{l} \pm 1, \pm 2, \pm p, \pm q, \pm 2p, \pm 2q, \pm pq, \pm 2pq, \pm r_{i_1} \cdots r_{i_j}, \\ \pm 2r_{i_1} \cdots r_{i_j}, \pm pr_{i_1} \cdots r_{i_j}, \pm qr_{i_1} \cdots r_{i_j}, \pm 2pr_{i_1} \cdots r_{i_j}, \\ \pm 2qr_{i_1} \cdots r_{i_j}, \pm pqr_{i_1} \cdots r_{i_j}, \pm 2pqr_{i_1} \cdots r_{i_j}, \\ \text{where } i_j, j \in \{1, 2, \ldots, n\} \text{ and } i_j \neq i_{j'} \text{ for } j \neq j'. \end{array} \right\}.$$

Note that $\mathbb{Q}(S,2)$ contains 2^{n+4} distinct elements. The curve is 2-isogenous to $E'_{p,\theta}$ given by

$$E'_{p,\theta} : y^2 = x^3 - 4(r-1)px^2 + 4r^2p^2x,$$

and for $d \in \mathbb{Q}(S,2)$, the corresponding homogeneous spaces are given by

$$C_d : dw^2 = d^2 - 4(r-1)pdz^2 + 4r^2p^2z^4 \tag{11}$$

and

$$C'_d : dw^2 = d^2 + 2(r-1)pdz^2 - (2r-1)p^2z^4. \tag{12}$$

Note that the image of $\mathscr{O}$ and $(0,0)$ under δ is $1 \in S^{(\phi)}(E_{p,\theta}/\mathbb{Q})$. The other values of $d \in \mathbb{Q}(S,2)$ are considered below. For the following cases, denote by $f(w)$ and $g(z)$ the left-hand side and right-hand side of Equation (11), respectively.

1.1 $d < 0$. Note that $C_d(\mathbb{R}) = \emptyset$ since $f(w) \leq 0$, while $g(z) > 0$.

1.2 $d = qd'$ for some d'. Note that $\operatorname{ord}_q(f(w))$ is odd. On the other hand, let $\operatorname{ord}_q(z) = v$. Then $\operatorname{ord}_q(g(z)) = 2$ or $4v$, which in any case is even, so a contradiction. Thus, $C_d(\mathbb{Q}_q) = \emptyset$.

1.3 $d = r_i d'$ for some d'. Let $(z,w) \in C_d(\mathbb{Q}_{r_i})$.

1.3.1 Suppose $\operatorname{ord}_{r_i}(z) > 0$. Note that $\operatorname{ord}_{r_i}(f(w))$ is odd. On the other hand, $\operatorname{ord}_{r_i}(g(z)) = 2$, which is even, so a contradiction. Thus, $C_d(\mathbb{Q}_{r_i}) = \emptyset$.

1.3.2 Suppose $\operatorname{ord}_{r_i}(z) = 0$. Note that $\operatorname{ord}_{r_i}(g(z)) \geq 1$. This implies that $\operatorname{ord}_{r_i}(f(w)) \geq 1$, so $\operatorname{ord}_{r_i}(w) \geq 0$. Hence, $z, w \in \mathbb{Z}_{r_i}$. Dividing both sides of Equation (11) by r_i and reducing modulo r_i, we get $d'w^2 \equiv 4pd'z^2 \pmod{r_i}$. This implies that $\left(\frac{p}{r_i}\right) = 1$.

1.3.3 Suppose $\mathrm{ord}_{r_i}(z) =: -v < 0$. Let $z = Z/r_i^v$, so that $\mathrm{ord}_{r_i}(Z) = 0$. By simplifying, we get

$$r_i^{4v+1} d' w^2 = r_i^{4v+2} d'^2 - 4(r-1) p r_i^{2v+1} d' Z^2 + 4r^2 p^2 Z^4. \tag{13}$$

We abuse notation and denote by $f(w)$ and $g(Z)$ the left-hand side and right-hand side of Equation (13), respectively.

1.3.3.1 Suppose $2v+1 > 2m_i$. Note that $\mathrm{ord}_{r_i}(f(w))$ is odd. On the other hand, $\mathrm{ord}_{r_i}(g(Z)) = 2m_i$, which is even, so a contradiction. Thus, $C_d(\mathbb{Q}_{r_i}) = \emptyset$.

1.3.3.2 Suppose $2v+1 < 2m_i$. Note that $\mathrm{ord}_{r_i}(g(Z)) = 2v+1$. This implies that $\mathrm{ord}_{r_i}(f(w)) = 2v+1$, so $\mathrm{ord}_{r_i}(w) = -v$. Let $w = W/r_i^v$, so that $\mathrm{ord}_{r_i}(W) = 0$. Then $Z, W \in \mathbb{Z}_{r_i}$. Dividing both sides of Equation (13) by r_i^{2v+1} and reducing modulo r_i, we get $d'W^2 \equiv 4pd'Z^2 \pmod{r_i}$. This implies that $\left(\frac{p}{r_i}\right) = 1$.

Thus, if $\left(\frac{p}{r_i}\right) = -1$, then $C_d(\mathbb{Q}_{r_i}) = \emptyset$.

1.4 $d = 2$. Let $(z, w) \in C_d(\mathbb{Q}_p)$. Note that $\mathrm{ord}_p(r-1) \geq 0$.

1.4.1 Suppose $\mathrm{ord}_p(z) \geq 0$. Note that $\mathrm{ord}_p(g(z)) \geq 0$. This implies that $\mathrm{ord}_p(f(w)) \geq 0$, so $\mathrm{ord}_p(w) \geq 0$. Hence, $z, w \in \mathbb{Z}_p$. Reducing Equation (11) modulo p, we get $w^2 \equiv 2 \pmod{p}$, i.e., $\left(\frac{2}{p}\right) = 1$. Thus, $p \equiv 1$ or $7 \pmod{8}$.

1.4.2 Suppose $\mathrm{ord}_p(z) =: -v < 0$. Note that $\mathrm{ord}_p(g(z)) = 2 - 4v$. This implies that $\mathrm{ord}_p(f(w)) = 2 - 4v$, so $\mathrm{ord}_p(w) = -(2v-1)$. Letting $(z, w) = (Z/p^v, W/p^{2v-1})$ and by simplifying, we get

$$W^2 = 2p^{4v-2} - 4(r-1)p^{2v-1}Z^2 + 2r^2 Z^4, \tag{14}$$

and $\mathrm{ord}_p(Z) = \mathrm{ord}_p(W) = 0$. Then $Z, W \in \mathbb{Z}_p$. Reducing Equation (14) modulo p, we get $W^2 \equiv 2r^2 Z^4 \pmod{p}$, i.e., $\left(\frac{2}{p}\right) = 1$. Thus, $p \equiv 1$ or $7 \pmod{8}$.

Thus, if $p \equiv 3$ or $5 \pmod{8}$ then $C_d(\mathbb{Q}_p) = \emptyset$.

1.5 $d = p$. Let $(z, w) \in C_d(\mathbb{Q}_2)$. Note that $\mathrm{ord}_2(r-1) \geq 2$ since $r \equiv 1 \pmod{4}$ by assumption.

1.5.1 Suppose $\mathrm{ord}_2(z) \geq 0$. Note that $\mathrm{ord}_2(g(z)) \geq 0$. This implies that $\mathrm{ord}_2(f(w)) \geq 0$, so $\mathrm{ord}_2(w) \geq 0$. Hence, $z, w \in \mathbb{Z}_2$. Reducing Equation (11) modulo 4, we get $pw^2 \equiv 1 \pmod{4}$. Thus, $p \equiv 1 \pmod{4}$.

1.5.2 Suppose $\mathrm{ord}_2(z) =: -v < 0$. Note that $\mathrm{ord}_2(g(z)) = 2 - 4v$. This implies that $\mathrm{ord}_2(f(w)) = 2 - 4v$, so $\mathrm{ord}_2(w) = -(2v-1)$. Letting $(z, w) = (Z/2^v, W/2^{2v-1})$ and by simplifying, we get

$$W^2 = 2^{4v-2}p - 2^{2v}(r-1)pZ^2 + r^2 p Z^4, \tag{15}$$

and $\mathrm{ord}_2(Z) = \mathrm{ord}_2(W) = 0$. Then $Z, W \in \mathbb{Z}_2$. Reducing Equation (15) modulo 4, we get $W^2 \equiv r^2 p Z^4 \pmod{4}$. Thus, $p \equiv 1 \pmod{4}$.

Thus, if $p \equiv 3 \pmod{4}$ then $C_d(\mathbb{Q}_2) = \emptyset$.

1.6 $d = 2p$. Let $(z, w) \in C_d(\mathbb{Q}_2)$.

1.6.1 Suppose $\mathrm{ord}_2(z) > 0$. Note that $\mathrm{ord}_2(f(w))$ is odd. On the other hand, $\mathrm{ord}_2(g(z)) = 2$, which is even, so a contradiction. Thus, $C_d(\mathbb{Q}_2) = \emptyset$.

1.6.2 Suppose $\mathrm{ord}_2(z) = 0$. Note that $\mathrm{ord}_2(g(z)) \geq 2$. This implies that $\mathrm{ord}_2(f(w)) \geq 2$, so $\mathrm{ord}_2(w) \geq 1$. Letting $w = 2W$ and dividing both sides of Equation (11) by 4, we get $2W^2 = p - 2(r-1)pz^2 + r^2 p z^4$ and $\mathrm{ord}_2(W) \geq 0$. Hence, $z, W \in \mathbb{Z}_2$. Reducing this

Submitted to Rocky Mountain Journal of Mathematics - NOT THE PUBLISHED VERSION

equation modulo 8, we get $2W^2 \equiv 2p \pmod 8$. If $\mathrm{ord}_2(W) > 0$, then $p \equiv 0 \pmod 4$, a contradiction. If $\mathrm{ord}_2(W) = 0$, then $p \equiv 1 \pmod 4$.

1.6.3 Suppose $\mathrm{ord}_2(z) =: -v < 0$. Note that $\mathrm{ord}_2(f(w))$ is odd. On the other hand, $\mathrm{ord}_2(g(z)) = 2-4v$, which is even, so a contradiction. Thus, $C_d(\mathbb{Q}_2) = \emptyset$.

Thus, if $p \equiv 3 \pmod 4$ then $C_d(\mathbb{Q}_2) = \emptyset$.

We have shown that if $p \equiv 3 \pmod 8$ and $\left(\frac{p}{r_i}\right) = -1$ for all $i = 1, \ldots, n$, then $S^{(\phi)}(E_{p,\theta}/\mathbb{Q}) = \{1\}$.

The group $S^{(\widehat{\phi})}(E'_{p,\theta}/\mathbb{Q})$ is considered next. Note that t is odd by assumption, so $-(2r-1) = -q^t \equiv -q \pmod{(\mathbb{Q}^*)^2}$. Thus, the images of $\mathscr{O}$ and $(0,0)$ under δ' are $1, -q \in S^{(\widehat{\phi})}(E'_{p,\theta}/\mathbb{Q})$, respectively. The other values of $d \in \mathbb{Q}(S,2)$ are considered below. For the following cases, we denote by $f(w)$ and $g(z)$ the left-hand side and right-hand side of Equation (12), respectively.

2.1 $d = p, -qp$. The homogeneous space (12) has a global solution $(z,w) = (1,0)$. Thus, $p \in S^{(\widehat{\phi})}(E'_{p,\theta}/\mathbb{Q})$. By closure property, since $-q, p \in S^{(\widehat{\phi})}(E'_{p,\theta}/\mathbb{Q})$, we have $-qp \in S^{(\widehat{\phi})}(E'_{p,\theta}/\mathbb{Q})$.

2.2 $d = r_i d'$ for some d'. Let $(z,w) \in C'_d(\mathbb{Q}_{r_i})$. Note that $\mathrm{ord}_{r_i}(f(w))$ is odd. On the other hand, let $\mathrm{ord}_{r_i}(z) = v$. Then $\mathrm{ord}_{r_i}(g(z)) = 2$ or $4v$, which in any case is even, so a contradiction. Thus, $C'_d(\mathbb{Q}_{r_i}) = \emptyset$.

2.3 $d = 2d'$ for some d'. Let $(z,w) \in C'_d(\mathbb{Q}_2)$. Note that $\mathrm{ord}_2(f(w))$ is odd. On the other hand, let $\mathrm{ord}_2(z) = v$. Then $\mathrm{ord}_2(g(z)) = 2$ or $4v$, which in any case is even, so a contradiction. Thus, $C'_d(\mathbb{Q}_2) = \emptyset$.

2.4 $d = q$. Let $(z,w) \in C'_d(\mathbb{Q}_p)$. Note that $\mathrm{ord}_p(r-1) \geq 0$.

2.4.1 Suppose $\mathrm{ord}_p(z) \geq 0$. Note that $\mathrm{ord}_p(g(z)) \geq 0$. This implies that $\mathrm{ord}_p(f(w)) \geq 0$, so $\mathrm{ord}_p(w) \geq 0$. Hence, $z, w \in \mathbb{Z}_p$. Reducing Equation (12) modulo p, we get $w^2 \equiv q \pmod p$. Thus, $\left(\frac{q}{p}\right) = 1$.

2.4.2 Suppose $\mathrm{ord}_p(z) =: -v < 0$. Note that $\mathrm{ord}_p(g(z)) = 2-4v$. This implies that $\mathrm{ord}_p(f(w)) = 2-4v$, so $\mathrm{ord}_p(w) = -(2v-1)$. Letting $(z,w) = (Z/p^v, W/p^{2v-1})$ and by simplifying, we get

$$W^2 = qp^{4v-2} + 2(r-1)p^{2v-1}Z^2 - q^{t-1}Z^4, \tag{16}$$

and $\mathrm{ord}_p(Z) = \mathrm{ord}_p(W) = 0$. Then $Z, W \in \mathbb{Z}_p$. Reducing Equation (16) modulo p, we get $W^2 \equiv -q^{t-1}Z^4 \pmod p$, i.e., $\left(\frac{-1}{p}\right) = 1$ since t is odd. Thus, $p \equiv 1 \pmod 4$.

Thus, if $p \equiv 3 \pmod 4$ and $\left(\frac{q}{p}\right) = -1$ then $C'_d(\mathbb{Q}_p) = \emptyset$.

2.5 $d = -1, qp, -p$. By closure property, if $p \equiv 3 \pmod 4$ and $\left(\frac{q}{p}\right) = -1$ then $q \notin S^{(\widehat{\phi})}(E'_{p,\theta}/\mathbb{Q})$, and $-q, p, -qp \in S^{(\widehat{\phi})}(E'_{p,\theta}/\mathbb{Q})$ implies that $-1, qp, -p \notin S^{(\widehat{\phi})}(E'_{p,\theta}/\mathbb{Q})$.

We have shown that if $p \equiv 3 \pmod 4$ and $\left(\frac{q}{p}\right) = -1$, then we obtain $S^{(\widehat{\phi})}(E'_{p,\theta}/\mathbb{Q}) = \{1, -q, p, -qp\}$. Therefore, if part (i) holds, then

$$S^{(\phi)}(E_{p,\theta}/\mathbb{Q}) = \{1\} \quad \text{and} \quad S^{(\widehat{\phi})}(E'_{p,\theta}/\mathbb{Q}) = \{1, -q, p, -qp\} \cong (\mathbb{Z}/2\mathbb{Z})^2.$$

Thus, $\mathrm{rank}(E_{p,\theta}/\mathbb{Q}) \leq 0 + 2 - 2 = 0$.

1 Aug 2024 06:25:26 PDT
230916-Mina Version 2 - Submitted to Rocky Mountain J. Math.

Submitted to Rocky Mountain Journal of Mathematics - NOT THE PUBLISHED VERSION

Next, we prove part (ii). We use the same set-up as above. Since t is assumed to be even and $q \equiv 3 \pmod 4$, we get $r \equiv 1 \pmod 4$. For $S^{(\phi)}(E_{p,\theta}/\mathbb{Q})$, all of the cases of part (i) hold. Thus, if $p \equiv 3 \pmod 8$ and $\left(\frac{p}{r_i}\right) = -1$ for all $i = 1, \ldots, n$, then $S^{(\phi)}(E_{p,\theta}/\mathbb{Q}) = \{1\}$.

The group $S^{(\widehat{\phi})}(E'_{p,\theta}/\mathbb{Q})$ is considered next. Since t is even, we have $-(2r-1) = -q^t \equiv -1 \pmod{(\mathbb{Q}^*)^2}$. Thus, the images of $\mathscr{O}$ and $(0,0)$ under δ' are $1, -1 \in S^{(\widehat{\phi})}(E'_{p,\theta}/\mathbb{Q})$, respectively. Note also that cases 2.2 and 2.3 of part (i) still hold. The other values of $d \in \mathbb{Q}(S,2)$ are considered below.

2.1 $d = p, -p$. The homogeneous space (12) has a global solution $(z,w) = (1,0)$. Thus, $p \in S^{(\widehat{\phi})}(E'_{p,\theta}/\mathbb{Q})$. By closure property, since $-1, p \in S^{(\widehat{\phi})}(E'_{p,\theta}/\mathbb{Q})$, we have $-p \in S^{(\widehat{\phi})}(E'_{p,\theta}/\mathbb{Q})$.

2.4 $d = q, -q$. Let $(z,w) \in C'_q(\mathbb{Q}_q)$.

2.4.1 Suppose $\mathrm{ord}_q(z) > 0$. Note that $\mathrm{ord}_q(f(w))$ is odd. On the other hand, $\mathrm{ord}_q(g(z)) = 2$, which is even, so a contradiction. Thus, $C'_q(\mathbb{Q}_q) = \emptyset$.

2.4.2 Suppose $\mathrm{ord}_q(z) = 0$. Note that $\mathrm{ord}_q(g(z)) \geq 1$. This implies that $\mathrm{ord}_q(f(w)) \geq 1$, so $\mathrm{ord}_q(w) \geq 0$. Hence, $z, w \in \mathbb{Z}_q$. Dividing both sides of Equation (12) by q and reducing modulo q, we get $w^2 \equiv -pz^2 \pmod q$. Thus, $\left(\frac{-p}{q}\right) = 1$.

2.4.3 Suppose $\mathrm{ord}_q(z) =: -v < 0$. Let $z = Z/q^v$, so that $\mathrm{ord}_q(Z) = 0$. By simplifying, we get

$$q^{4v}w^2 = q^{4v+1} + 2(r-1)pq^{2v}Z^2 - q^{t-1}p^2Z^4. \tag{17}$$

We abuse notation and denote by $f(w)$ and $g(Z)$ the left-hand side and right-hand side of Equation (17), respectively.

2.4.3.1 Suppose $2v > t-1$. Note that $\mathrm{ord}_q(g(Z)) = t-1$. This implies that $\mathrm{ord}_q(f(w)) = t-1$, so $\mathrm{ord}_q(w) = (t-1-4v)/2$. Let $w = W/q^{(t-1-4v)/2}$, so that $\mathrm{ord}_q(W) = 0$. Then $Z, W \in \mathbb{Z}_q$. Dividing both sides of Equation (17) by q^{t-1} and reducing modulo q, we get $W^2 \equiv -p^2Z^2 \pmod q$, i.e., $\left(\frac{-1}{q}\right) = 1$. Thus, $q \equiv 1 \pmod 4$.

2.4.3.2 Suppose $2v < t-1$. Note that $\mathrm{ord}_q(g(Z)) = 2v$. This implies that $\mathrm{ord}_q(f(w)) = 2v$, so $\mathrm{ord}_q(w) = -v$. Let $w = W/q^v$, so that $\mathrm{ord}_q(W) = 0$. Then $Z, W \in \mathbb{Z}_q$. Dividing both sides of Equation (17) by q^{2v} and reducing modulo q, we get $W^2 \equiv -pZ^2 \pmod q$. Thus, $\left(\frac{-p}{q}\right) = 1$.

Thus, if $\left(\frac{-p}{q}\right) = -1$ and $q \equiv 3 \pmod 4$ then $C'_q(\mathbb{Q}_q) = \emptyset$. By closure property, $-q \notin S^{(\widehat{\phi})}(E'_{p,\theta}/\mathbb{Q})$ whenever $\left(\frac{-p}{q}\right) = -1$ and $q \equiv 3 \pmod 4$.

2.5 $d = qp, -qp$. By closure property, since $p, -p \in S^{(\widehat{\phi})}(E'_{p,\theta}/\mathbb{Q})$ and $q, -q \notin S^{(\widehat{\phi})}(E'_{p,\theta}/\mathbb{Q})$ whenever $\left(\frac{-p}{q}\right) = -1$ and $p \equiv 3 \pmod 4$ then $pq, -pq \notin S^{(\widehat{\phi})}(E'_{p,\theta}/\mathbb{Q})$ whenever $\left(\frac{-p}{q}\right) = -1$ and $p \equiv 3 \pmod 4$.

We have shown that if $\left(\frac{-p}{q}\right) = -1$ and $q \equiv 3 \pmod 4$ then $S^{(\widehat{\phi})}(E'_{p,\theta}/\mathbb{Q}) = \{1, -1, p, -p\}$. Therefore, if part (ii) holds then

$$S^{(\phi)}(E_{p,\theta}/\mathbb{Q}) = \{1\} \quad \text{and} \quad S^{(\widehat{\phi})}(E'_{p,\theta}/\mathbb{Q}) = \{1, -1, p, -p\} \cong (\mathbb{Z}/2\mathbb{Z})^2.$$

Thus, $\mathrm{rank}(E_{p,\theta}(\mathbb{Q})) \leq 0 + 2 - 2 = 0$.

Lastly, we prove part (iii). We use the same set-up as above. For the group $S^{(\phi)}(E_{p,\theta}/\mathbb{Q})$, cases 1.1 and 1.2 of part (i) still hold, and $1 \in S^{(\phi)}(E_{p,\theta}/\mathbb{Q})$. We investigate the remaining cases.

1 Aug 2024 06:25:26 PDT
230916-Mina Version 2 - Submitted to Rocky Mountain J. Math.

Submitted to Rocky Mountain Journal of Mathematics - NOT THE PUBLISHED VERSION

1.3 $d = pd'$ for some d'. Let $(z,w) \in C_d(\mathbb{Q}_p)$. Note that $\mathrm{ord}_p(r-1) \geq 0$.

1.3.1 Suppose $\mathrm{ord}_p(z) > 0$. Note that $\mathrm{ord}_p(f(w))$ is odd. On the other hand, $\mathrm{ord}_p(g(z)) = 2$, which is even, so a contradiction. Thus, $C_d(\mathbb{Q}_p) = \emptyset$.

1.3.2 Suppose $\mathrm{ord}_p(z) = 0$. Note that $\mathrm{ord}_p(g(z)) \geq 2$. This implies that $\mathrm{ord}_p(f(w)) \geq 2$, so $\mathrm{ord}_p(w) \geq 1$. Letting $w = pW$, we get $pd'W^2 = d'^2 - 4(r-1)d'z^2 + 4r^2z^4$ and $\mathrm{ord}_p(W) \geq 0$. Then $z, W \in \mathbb{Z}_p$. Reducing this equation modulo p, we get $d'^2 - 4(r-1)d'z^2 + 4r^2z^4 \equiv 0 \pmod p$. Multiplying both sides by r^2 and adding both sides by $-d'^2(2r-1)$, we get $(2r^2z^2 - (r-1)d')^2 \equiv -d'^2(2r-1) \pmod p$. This implies that $\left(\frac{-(2r-1)}{p}\right) = \left(\frac{-q}{p}\right) = 1$.

1.3.3 Suppose $\mathrm{ord}_p(z) =: -v < 0$. Note that $\mathrm{ord}_p(f(w))$ is odd. On the other hand, $\mathrm{ord}_p(g(z)) = 2 - 4v$, which is even, so a contradiction. Thus, $C_d(\mathbb{Q}_p) = \emptyset$.

Thus, if $\left(\frac{-q}{p}\right) = -1$ then $C_d(\mathbb{Q}_p) = \emptyset$.

1.4 $d = r_i d'$ for some d'. Here, r_i could be any prime factor of r but we exclude exactly one r_i that is congruent to 3 modulo 4 and we treat this case in item 1.5. The existence of such prime factor is valid since $r \equiv 3 \pmod 4$ by assumption. In this case, if $\left(\frac{p}{r_i}\right) = -1$, then $C_d(\mathbb{Q}_{r_i}) = \emptyset$. The proof is identical to case 1.3 of part (i).

1.5 $d = r_i$ where $r_i \equiv 3 \pmod 4$ is the prime factor of r excluded in case 1.4. Let $(z,w) \in C_d(\mathbb{Q}_2)$. Note that $\mathrm{ord}_2(r-1) = 1$ since $r \equiv 3 \pmod 4$ by assumption.

1.5.1 Suppose $\mathrm{ord}_2(z) \geq 0$. Note that $\mathrm{ord}_2(g(z)) = 0$. This implies that $\mathrm{ord}_2(f(w)) = 0$, so $\mathrm{ord}_2(w) = 0$. Hence, $z, w \in \mathbb{Z}_2$. Reducing Equation (11) modulo 4, we get $r_i w^2 \equiv 1 \pmod 4$, a contradiction since $r_i \equiv 3 \pmod 4$. Thus, $C_d(\mathbb{Q}_2) = \emptyset$.

1.5.2 Suppose $\mathrm{ord}_2(z) =: -v < 0$. Note that $\mathrm{ord}_2(g(z)) = 2 - 4v$. This implies that $\mathrm{ord}_2(f(w)) = 2 - 4v$, so $\mathrm{ord}_2(w) = -(2v-1)$. Letting $(z,w) = (Z/2^v, W/2^{2v-1})$ and simplifying, we get

$$r_i W^2 = 2^{4v-2} r_i^2 - 2^{2v}(r-1)pr_i Z^2 + r^2p^2Z^4, \tag{18}$$

and $\mathrm{ord}_2(Z) = \mathrm{ord}_2(W) = 0$. Then $Z, W \in \mathbb{Z}_2$. Reducing Equation (18) modulo 4, we get $r_i W^2 \equiv 1 \pmod 4$, a contradiction since $r_i \equiv 3 \pmod 4$. Thus, $C_d(\mathbb{Q}_2) = \emptyset$.

In any case, $C_d(\mathbb{Q}_2) = \emptyset$.

1.6 $d = 2$. Let $(z,w) \in C_d(\mathbb{Q}_2)$. Note that $\mathrm{ord}_2(r-1) = 1$.

1.6.1 Suppose $\mathrm{ord}_2(z) > 0$. Note that $\mathrm{ord}_2(f(w))$ is odd. On the other hand, $\mathrm{ord}_2(g(z)) = 2$, which is even, so a contradiction. Thus, $C_d(\mathbb{Q}_2) = \emptyset$.

1.6.2 Suppose $\mathrm{ord}_2(z) = 0$. Note that $\mathrm{ord}_2(g(z)) \geq 2$. This implies that $\mathrm{ord}_2(f(w)) \geq 2$, so $\mathrm{ord}_2(w) \geq 1$. Letting $w = 2W$ and simplifying, we get $2W^2 = 1 - 2(r-1)pz^2 + r^2p^2z^4$ and $\mathrm{ord}_2(W) \geq 0$. Hence, $z, W \in \mathbb{Z}_2$. Assuming $r \equiv 3 \pmod 4$ and reducing this equation modulo 8, we get $2W^2 \equiv 6 \pmod 8$, so a contradiction. Thus, $C_d(\mathbb{Q}_2) = \emptyset$.

1.6.3 Suppose $\mathrm{ord}_2(z) =: -v < 0$. Note that $\mathrm{ord}_2(f(w))$ is odd. On the other hand, $\mathrm{ord}_2(g(z)) = 2 - 4v$, which is even, so a contradiction. Thus, $C_d(\mathbb{Q}_2) = \emptyset$.

In any case, $C_d(\mathbb{Q}_2) = \emptyset$.

1.7 $d = 2r_i$ where $r_i \equiv 3 \pmod 4$ is the prime factor of r excluded in case 1.4. Let $(z,w) \in C_d(\mathbb{Q}_p)$. Note that $\mathrm{ord}_p(r-1) \geq 0$.

1 Aug 2024 06:25:26 PDT
230916-Mina Version 2 - Submitted to Rocky Mountain J. Math.

Submitted to Rocky Mountain Journal of Mathematics - NOT THE PUBLISHED VERSION

1.7.1 Suppose $\operatorname{ord}_p(z) \geq 0$. Note that $\operatorname{ord}_p(g(z)) \geq 0$. This implies that $\operatorname{ord}_p(f(w)) \geq 0$, so $\operatorname{ord}_p(w) \geq 0$. Hence, $z, w \in \mathbb{Z}_p$. Reducing Equation (11) modulo p, we get $2r_i w^2 \equiv 1 \pmod{p}$. Thus, $\left(\frac{2r_i}{p}\right) = 1$.

1.7.2 Suppose $\operatorname{ord}_p(z) =: -v < 0$. Note that $\operatorname{ord}_p(g(z)) = 2-4v$. This implies that $\operatorname{ord}_p(f(w)) = 2-4v$, so $\operatorname{ord}_p(w) = -(2v-1)$. Letting $(z,w) = (Z/p^v, W/p^{2v-1})$ and simplifying, we get

$$2r_i W^2 = p^{4v-2} r_i^2 - 2(r-1)p^{2v-1} r_i z^2 + r^2 z^4, \tag{19}$$

and $\operatorname{ord}_p(Z) = \operatorname{ord}_p(W) = 0$. Then $Z, W \in \mathbb{Z}_p$. Reducing Equation (19) modulo p, we get $2r_i W^2 \equiv r^2 Z^4 \pmod{p}$. Thus, $\left(\frac{2r_i}{p}\right) = 1$.

Thus, if $\left(\frac{2r_i}{p}\right) = -1$ then $C_d(\mathbb{Q}_p) = \emptyset$.

We have shown that if $\left(\frac{p}{r_i}\right) = -1$ for all r_i except one with $r_i \equiv 3 \pmod{4}$, $\left(\frac{-q}{p}\right) = -1$ and $\left(\frac{2r_i}{p}\right) = -1$, where r_i is the one excluded above, then $S^{(\phi)}(E_{p,\theta}/\mathbb{Q}) = \{1\}$. The condition that $\left(\frac{2r_i}{p}\right) = -1$ is equivalent to $p \equiv 1$ or $7 \pmod{8}$ and $\left(\frac{r_i}{p}\right) = -1$, or $p \equiv 3$ or $5 \pmod{8}$ and $\left(\frac{r_i}{p}\right) = 1$.

Next, we consider $S^{(\widehat{\phi})}(E'_{p,\theta}/\mathbb{Q})$. Note that the cases 2.1, 2.2 and 2.3 of part (i) still hold and $1, -q \in S^{(\widehat{\phi})}(E'_{p,\theta}/\mathbb{Q})$. We consider the remaining cases.

2.4 $d = q$. Let $(z,w) \in C'_d(\mathbb{Q}_{r_i})$ where $r_i \equiv 3 \pmod{4}$ is the prime factor of r excluded in case 1.4.

2.4.1 Suppose $\operatorname{ord}_{r_i}(z) \geq 0$. Note that $\operatorname{ord}_{r_i}(g(z)) \geq 0$. This implies that $\operatorname{ord}_{r_i}(f(w)) \geq 0$, so $\operatorname{ord}_{r_i}(w) \geq 0$. Hence, $z, w \in \mathbb{Z}_{r_i}$. Note that $t = 1$ by assumption, so $2r - 1 = q$. Dividing both sides of Equation (12) by q and reducing modulo r_i, we get $w^2 \equiv -1 - 2pz^2 - p^2 z^4 \pmod{r_i}$, that is, $w^2 \equiv -(pz^2+1)^2 \pmod{r_i}$. If $\operatorname{ord}_{r_i}(pz^2+1) = 0$, then $\left(\frac{-1}{r_i}\right) = 1$, a contradiction since $r_i \equiv 3 \pmod{4}$. Thus, $pz^2 + 1 \equiv 0 \pmod{r_i}$, that is, $\left(\frac{-p}{r_i}\right) = 1$. Since $\left(\frac{-1}{r_i}\right) = -1$, we obtain $\left(\frac{p}{r_i}\right) = -1$.

2.4.2 Suppose $\operatorname{ord}_{r_i}(z) =: -v < 0$. Note that $\operatorname{ord}_{r_i}(g(z)) = -4v$. This implies that $\operatorname{ord}_{r_i}(f(w)) = -4v$, so $\operatorname{ord}_{r_i}(w) = -2v$. Letting $(z,w) = (Z/r_i^v, W/r_i^{2v})$ and simplifying, we get

$$W^2 = r_i^{4v} q + 2(r-1)p r_i^{2v} Z^2 - p^2 Z^4, \tag{20}$$

and $\operatorname{ord}_{r_i}(Z) = \operatorname{ord}_{r_i}(W) = 0$. Then $Z, W \in \mathbb{Z}_{r_i}$. Reducing Equation (20) modulo r_i, we get $W^2 \equiv -p^2 Z^4 \pmod{r_i}$, that is, $\left(\frac{-1}{r_i}\right) = 1$, a contradiction since $r_i \equiv 3 \pmod{4}$. Thus, $C'_d(\mathbb{Q}_{r_i}) = \emptyset$.

Thus, if $\left(\frac{p}{r_i}\right) = 1$ then $C'_d(\mathbb{Q}_{r_i}) = \emptyset$.

2.5 $d = -1, qp, -p$. By closure property, if $\left(\frac{p}{r_i}\right) = 1$ then $q \notin S^{(\widehat{\phi})}(E'_{p,\theta}/\mathbb{Q})$, and $-q, p, -qp \in S^{(\widehat{\phi})}(E'_{p,\theta}/\mathbb{Q})$ implies that $-1, qp, -p \notin S^{(\widehat{\phi})}(E'_{p,\theta}/\mathbb{Q})$.

We have shown that if $\left(\frac{p}{r_i}\right) = 1$, for exactly one $r_i \equiv 3 \pmod{4}$, then $S^{(\widehat{\phi})}(E'_{p,\theta}/\mathbb{Q}) = \{1, -q, p, -qp\}$. Therefore, if part (iii) holds then

$$S^{(\phi)}(E_{p,\theta}/\mathbb{Q}) = \{1\} \quad \text{and} \quad S^{(\widehat{\phi})}(E'_{p,\theta}/\mathbb{Q}) = \{1, -q, p, -qp\} \cong (\mathbb{Z}/2\mathbb{Z})^2.$$

Thus, $\operatorname{rank}(E_{p,\theta}(\mathbb{Q})) \leq 0 + 2 - 2 = 0$. $\square$

1 Aug 2024 06:25:26 PDT
230916-Mina Version 2 - Submitted to Rocky Mountain J. Math.

Submitted to Rocky Mountain Journal of Mathematics - NOT THE PUBLISHED VERSION

Acknowledgements. The authors would like to thank the following for the support given in the conduct of the study: the University of the Philippines Baguio; the Office of the Chancellor of the University of the Philippines Diliman, through the Office of the Vice Chancellor for Research and Development; and the Department of Science and Technology-Accelerated Science and Technology Human Resource Development Program.

References

[1] M. Fujiwara, *θ-congruent numbers*, in: Number Theory (Eger, 1996), edited by K. Gyory et al., de Gruyter, Berlin, (1998), 235–241.

[2] T. Goto, *A study on the Selmer groups of the elliptic curves with a rational* 2*-torsion*, PhD thesis, Kyushu Univ., 2002.

[3] K. Heegner, *Diophantische analysis und modulfunktionen*, Math. Z., 56 (1952), 227–253.

[4] T. Hibino and M. Kan, *θ-congruent numbers and Heegner points*, Arch. Math., 77 (2001), 303–308.

[5] M. Kan, *θ-congruent numbers and elliptic curves*, Acta Arith., 94 no. 2, (2000), 153–160.

[6] P. Monsky, *Mock Heegner points and congruent numbers*, Math. Z., 204 no. 1, (1990), 45–67.

[7] J. H. Silverman, *The Arithmetic of Elliptic Curves*, vol. 106, Springer, 2009.

[8] J. B. Tunnell, *A classical Diophantine problem and modular forms of weight* $3/2$, Invent. Math., 72 (1983), 323–334.

[9] S. Yoshida, *Some variants of the congruent number problem I*, Kyushu J. Math., 55 (2001), 387–404.

[10] S. Yoshida, *Some variants of the congruent number problem II*, Kyushu J. Math., 56 (2002), 147–165.

INSTITUTE OF MATHEMATICS, UNIVERSITY OF THE PHILIPPINES DILIMAN, 1101 QUEZON CITY, PHILIPPINES
Email address: vmaricheta@math.upd.edu.ph

DEPARTMENT OF MATHEMATICS AND COMPUTER SCIENCE, UNIVERSITY OF THE PHILIPPINES BAGUIO, 2600 BAGUIO CITY, PHILIPPINES
Email address: jbbacani@up.edu.ph

DEPARTMENT OF MATHEMATICS AND COMPUTER SCIENCE, UNIVERSITY OF THE PHILIPPINES BAGUIO, 2600 BAGUIO CITY, PHILIPPINES
Email address: rsmina1@up.edu.ph

1 Aug 2024 06:25:26 PDT
230916-Mina Version 2 - Submitted to Rocky Mountain J. Math.