Canad. Math. Bull. Vol. **53** (4), 2010 pp. 661–666
doi:10.4153/CMB-2010-071-3

# Congruent Number Elliptic Curves with Rank at Least Three

Jennifer A. Johnstone and Blair K. Spearman

*Abstract.* We give an infinite family of congruent number elliptic curves each with rank at least three.

## 1 Introduction

A positive integer $n$ is a congruent number if it is equal to the area of a right triangle with rational sides. Equivalently, the congruent number elliptic curve $E_n : y^2 = x(x^2 - n^2)$ has positive rank. Congruent numbers have been intensively studied. For recent references see Chahal [1] and Coates [2]. The purpose of this paper is to give an infinite family of congruent number elliptic curves with rank at least 3. We prove the following.

**Theorem 1.1** *The curve $w^2 = t^4 + 14t^2 + 4$ has infinitely many points. Let $(t, w)$ with $t \neq 0$ be one of them. Set $t = u/v$, where $u$ and $v$ are integers with* $\gcd(u, v) = 1$. *Define the positive integer $n$ by*

$$n = 6(u^4 + 2u^2v^2 + 4v^4)(u^4 + 8u^2v^2 + 4v^4). \tag{1.1}$$

*Then the congruent number elliptic curve $y^2 = x(x^2 - n^2)$ has rank at least three.*

In Section 2, we give a series of lemmas. In Section 3, we prove the theorem and justify that the resulting congruent numbers are distinct modulo squares.

## 2 Some Useful Lemmas

**Lemma 2.1** *If $u$ and $v$ are integers with $(u, v) = 1$, then the quantities*

(i) $\pm 6(u^4 + 2u^2v^2 + 4v^4)(u^4 + 8u^2v^2 + 4v^4)$
(ii) $\pm 6(u^4 + 2u^2v^2 + 4v^4)$
(iii) $\pm 2(u^4 + 2u^2v^2 + 4v^4)(u^4 + 8u^2v^2 + 4v^4)$
(iv) $\pm 2(u^4 + 2u^2v^2 + 4v^4)$

*are not equal to squares in $\mathbb{Q}$.*

**Proof** For (i), if $u$ is odd, then

$$2 \parallel 6(u^4 + 2u^2v^2 + 4v^4)(u^4 + 8u^2v^2 + 4v^4).$$

Received by the editors December 17, 2007; revised October 16, 2008.
Published electronically July 26, 2010.
Research supported by the Natural Sciences and Engineering Research Council of Canada.
AMS subject classification: **11G05**.
Keywords: congruent number, elliptic curve, rank.

If $u$ is even, so that $v$ is odd, then

$$2^5 \parallel 6(u^4 + 2u^2v^2 + 4v^4)(u^4 + 8u^2v^2 + 4v^4).$$

These calculations show that in either case the given quantities cannot be equal to a square in $\mathbb{Q}$. The proofs in the other cases are similar and are therefore omitted. ■

***Lemma 2.2*** *If $u$ and $v$ are nonzero integers with $(u, v) = 1$, then the quantities*

(i) $\pm(u^4 + 2u^2v^2 + 4v^4)$
(ii) $\pm(u^4 + 8u^2v^2 + 4v^4)$

*are not equal to squares in $\mathbb{Q}$.*

**Proof** In order for any of these quantities to be equal to a square in $\mathbb{Q}$, we must clearly choose the plus sign. In that case, a pair $(u, v)$ satisfying the conditions in the lemma and yielding a square, say $z^2$, would give rise to a rational point $(x, y) = (u^2/v^2, zu/v^3)$ on one of the following elliptic curves:

$$y^2 = x(x^2 + 2x + 4),$$

$$y^2 = x(x^2 + 8x + 4).$$

These curves have conductors 192 and 96 respectively. Each has rank 0 and their only finite rational points are $(0, 0)$ and $(0, 0)$, $(-2, \pm 4)$ respectively, none of which is consistent with $x = u^2/v^2$ and $u \neq 0$. ■

***Lemma 2.3*** *For integers $u, v$ such that $(u, v) = 1$, we have*

(i) $3 \nmid (u^4 + 8u^2v^2 + 4v^4)$,
(ii) $3 \nmid (u^4 + 2u^2v^2 + 4v^4)$.

**Proof** Each of the quantities $(u^4 + 8u^2v^2 + 4v^4)$ and $(u^4 + 2u^2v^2 + 4v^4)$ is congruent to $(u^2 + v^2)^2$ modulo 3. Then we observe that $3 \nmid (u^2 + v^2)$, since $-1$ is not a quadratic residue modulo 3. The result follows. ■

***Lemma 2.4*** *For integers $u, v$ such that $(u, v) = 1$, neither of the following quantities is equal to a square in $\mathbb{Q}$.*

$$\pm(u^4 + 2u^2v^2 + 4v^4)(u^4 + 8u^2v^2 + 4v^4).$$

**Proof** Clearly we must choose the plus sign in order for one of the given quantities to equal a square in $\mathbb{Q}$. If $(u^4+2u^2v^2+4v^4)(u^4+8u^2v^2+4v^4)$ were equal to a square in $\mathbb{Q}$, then an easy calculation shows that each of $u^4+2u^2v^2+4v^4$ and $u^4+8u^2v^2+4v^4$ is equal to a square. However, by Lemma 2.2 this is impossible. This proves Lemma 2.4. ■

***Lemma 2.5*** *There exist infinitely many pairs of rational numbers $(t, w)$ such that*

$$w^2 = t^4 + 14t^2 + 4.$$

**Proof** The given quartic curve is birationally equivalent to the elliptic curve

$$Y^2 = X^3 - 6588X + 39312.$$

It has rank one, conductor 960 and Mordell–Weil group $E(\mathbb{Q}) \simeq \mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. Hence the given quartic has infinitely many rational points. ■

https://doi.org/10.4153/CMB-2010-071-3 Published online by Cambridge University Press

## 3 Proof of Theorem 1.1

**Proof** Lemma 2.5 shows that there are infinitely many points $(t, w)$ on the curve

$$w^2 = t^4 + 14t^2 + 4,$$

and we can choose $t \neq 0$. Clearly $n$ is positive. Rank estimation uses the following method, which is described in Silverman and Tate [3]. Let $\Gamma$ denote the group of rational points of an elliptic curve $E$ in the form $y^2 = x(x^2 + ax + b)$. Let $\mathbb{Q}^*$ be the multiplicative group of non-zero rational numbers and let $\mathbb{Q}^{*2}$ denote the subgroup of squares of elements of $\mathbb{Q}^*$. Define the group homomorphism $\alpha$ from $\Gamma$ to $\mathbb{Q}^*/\mathbb{Q}^{*2}$ as follows.

$$\alpha(P) = \begin{cases} 1(\operatorname{mod} \mathbb{Q}^{*2}) & \text{for } P = O, \text{ the point at infinity,} \\ b(\operatorname{mod} \mathbb{Q}^{*2}) & \text{for } P = (0, 0), \\ x(\operatorname{mod} \mathbb{Q}^{*2}) & \text{for } P = (x, y) \text{ with } x \neq 0. \end{cases}$$

Simultaneously, we study a second curve $y^2 = x(x^2 - 2ax + a^2 - 4b)$ and its group of rational points $\bar{\Gamma}$. In an analogous manner, we introduce a second group homomorphism $\bar{\alpha}$ from $\bar{\Gamma}$ to $\mathbb{Q}^*/\mathbb{Q}^{*2}$ defined by

$$\bar{\alpha}(P) = \begin{cases} 1(\operatorname{mod} \mathbb{Q}^{*2}) & \text{for } P = O, \text{ the point at infinity,} \\ a^2 - 4b(\operatorname{mod} \mathbb{Q}^{*2}) & \text{for } P = (0, 0), \\ x(\operatorname{mod} \mathbb{Q}^{*2}) & \text{for } P = (x, y) \text{ with } x \neq 0. \end{cases}$$

The rank $r$ of the given curve $E$ satisfies

$$2^r = \frac{|\alpha(\Gamma)||\bar{\alpha}(\bar{\Gamma})|}{4}.$$

It suffices to show that $|\alpha(\Gamma)| \geq 32$.

From the definition of $\alpha$ we have

$$\alpha(\Gamma) \supseteq \{1, -1\}.$$

Since $\alpha((\pm n, 0)) \equiv \pm n(\operatorname{mod} \mathbb{Q}^{*2})$, we obtain

$$\alpha(\Gamma) \supseteq S_1 \doteqdot \{1, -1, n, -n\}.$$

It follows from Lemma 2.1(i) that these images are distinct modulo $\mathbb{Q}^{*2}$. For brevity we just list generators of the subgroup of $\alpha(\Gamma)$ that we are constructing. Therefore we have $\alpha(\Gamma) \supseteq \langle -1, n\rangle$. Consider the following three non-torsion points $P_1, P_2, P_3$ on $y^2 = x(x^2 - n^2)$:

$$P_1 = (-36u^2v^2(u^4 + 8u^2v^2 + 4v^4), 36uv(u^2 - 2v^2)(u^4 + 8u^2v^2 + 4v^4)^2),$$

$$P_2 = (12(u^4 + 2u^2v^2 + 4v^4)^2, 36(u^4 - 4v^4)(u^4 + 2u^2v^2 + 4v^4)^2),$$

$$P_3 = (-36u^2v^2(u^4 + 2u^2v^2 + 4v^4), 36uv^3(u^4 + 2u^2v^2 + 4v^4)^2w).$$

https://doi.org/10.4153/CMB-2010-071-3 Published online by Cambridge University Press

We will show that these points are independent in $\Gamma$. As

$$\alpha(P_1) \equiv -(u^4 + 8u^2v^2 + 4v^4)(\bmod \mathbb{Q}^{*2}),$$

we see that $\alpha(\Gamma) \supseteq S_1 \cup \{(u^4 + 8u^2v^2 + 4v^4)\}$. We check that $\alpha(P_1)$ is not congruent modulo $\mathbb{Q}^{*2}$ to any element of $S_1$. From Lemma 2.2(ii), we see that $\pm(u^4+8u^2v^2+4v^4)$ are not equal to squares in $\mathbb{Q}$. If $\pm\alpha(P_1)n$ were congruent to a square modulo $\mathbb{Q}^{*2}$ we would have a contradiction to Lemma 2.1(ii). Therefore,

$$\alpha(\Gamma) \supseteq S_2 \doteqdot \langle -1, n, (u^4 + 8u^2v^2 + 4v^4)\rangle.$$

Next we turn to $\alpha(P_2)$. We must show that $\alpha(P_2) \not\equiv s(\bmod \mathbb{Q}^{*^2})$ for all $s \in S_2$. If this congruence were to hold for some $s \in S_2$, then there would exist integers $c_1, c_2$ with $c_1, c_2 \in \{0, 1\}$ such that

$$\alpha(P_2) \equiv \pm n^{c_1}(u^4 + 8u^2v^2 + 4v^4)^{c_2}(\bmod \mathbb{Q}^{*2})$$

or

$$3 \equiv \pm n^{c_1}(u^4 + 8u^2v^2 + 4v^4)^{c_2}(\bmod \mathbb{Q}^{*2}).$$

Comparing powers of 3 on both sides of this congruence, we deduce from (1.1) and Lemma 2.3(i), (ii) that $c_1 = 1$, from which it follows that at least one of the quantities $\pm 3n$ or $\pm 2(u^4 + 2u^2v^2 + 4v^4)$ must be equal to a square in $\mathbb{Q}$. However, this would contradict Lemma 2.1(iii), (iv). Therefore,

$$\alpha(\Gamma) \supseteq S_3 \doteqdot \langle -1, n, (u^4 + 8u^2v^2 + 4v^4), 3\rangle$$

and $|S_3| = 16$. To finish, we show that show that $\alpha(P_3) \not\equiv s(\bmod \mathbb{Q}^{*^2})$ for all $s \in S_3$. If this congruence were to hold, then there would exist integers $e_i$, $i = 1, 2, 3$, and $e_i \in \{0, 1\}$ such that

$$\alpha(P_3) \equiv \pm 3^{e_1} n^{e_2}(u^4 + 8u^2v^2 + 4v^4)^{e_3}(\bmod \mathbb{Q}^{*2}),$$

that is,

$$(u^4 + 2u^2v^2 + 4v^4) \equiv \pm 3^{e_1} n^{e_2}(u^4 + 8u^2v^2 + 4v^4)^{e_3}(\bmod \mathbb{Q}^{*2}). \tag{3.1}$$

Comparing powers of 2 on both sides of (3.1), we deduce as in the proof outlined in Lemma 2.1 that

$$2^{2m} \parallel \pm 3^{e_1} n^{e_2}(u^4 + 8u^2v^2 + 4v^4)^{e_3}$$

for some nonnegative integer $m$. Again, as from the proof of Lemma 2.1, the exact power of 2 dividing $n$ is odd and therefore $e_2 = 0$. Now (3.1) reduces to

$$(u^4 + 2u^2v^2 + 4v^4) \equiv \pm 3^{e_1}(u^4 + 8u^2v^2 + 4v^4)^{e_3}(\bmod \mathbb{Q}^{*2}). \tag{3.2}$$

https://doi.org/10.4153/CMB-2010-071-3 Published online by Cambridge University Press

Comparing powers of 3 on both sides of (3.2) and using Lemma 2.3, we deduce that $e_1 = 0$. Thus we treat the cases with $(e_1, e_2, e_3) = (0, 0, 0)$ or $(0, 0, 1)$ and deduce from (3.2) with $e_1 = 0$ that

$$(u^4 + 2u^2v^2 + 4v^4) \equiv \begin{cases} \pm 1 (\operatorname{mod} \mathbb{Q}^{*2}) & \text{if } (e_1, e_2, e_3) = (0, 0, 0), \\ \pm(u^4 + 8u^2v^2 + 4v^4)(\operatorname{mod} \mathbb{Q}^{*2}) & \text{if } (e_1, e_2, e_3) = (0, 0, 1). \end{cases}$$

Hence at least one of the quantities

$$\pm\,(u^4 + 2u^2v^2 + 4v^4)$$
$$\pm\,(u^4 + 2u^2v^2 + 4v^4)(u^4 + 8u^2v^2 + 4v^4)$$

is equal to a square in $\mathbb{Q}$. This contradicts Lemmas 2.2(i) and 2.4. Thus $\alpha(\Gamma)$ contains the seventeen elements in $S_3 \cup \{(u^4 + 2u^2v^2 + 4v^4\}$, and, as $|\alpha(\Gamma)|$ is a power of 2, we see that $|\alpha(\Gamma)| \geq 32$. This proves that the rank of $\Gamma$ is at least 3. ■

***Remark 3.1*** Our theorem allows us to deduce the existence of infinitely many integral congruent numbers, distinct modulo squares, whose associated elliptic curves have rank at least three. If this were not the case, then there would exist a finite set of nonzero rational numbers $\{d_i, = 1, \dots, m\}$ that are inequivalent modulo $\mathbb{Q}^*$, such that for each congruent number $n$ in our theorem we have

$$n = 6(u^4 + 2u^2v^2 + 4v^4)(u^4 + 8u^2v^2 + 4v^4) \equiv d_i (\operatorname{mod}\ \mathbb{Q}^{*^2}),$$

for exactly one $d_i$. Equivalently, setting $t = u/v$, we obtain

$$6(t^4 + 2t^2 + 4)(t^4 + 8t^2 + 4) = d_i y^2$$

for some rational number $y$ depending on $n$. Our infinitely many distinct values of $n$ would give rise to an infinite set of distinct points on the family of algebraic curves

$$d_i Y^2 = 6(X^4 + 2X^2 + 4)(X^4 + 8X^2 + 4).$$

However, this is impossible since we have finitely many curves of genus three, each of which has only finitely many points.

***Remark 3.2*** The point $(t, w) = (1/2, 11/4)$ lies on the curve $w^2 = t^4 + 14t^2 + 4$. Thus we can apply our theorem with $(u, v) = (1, 2)$ yielding the congruent number $n = 42486$. Our theorem implies that the associated congruent number elliptic curve $y^2 = x(x^2 - n^2)$ has rank at least 3. Magma confirms that the rank is exactly 3. We attempted to find a further specialization of the values $(u, v)$ in our theorem that would give an infinite family of congruent number curves with rank at least 4 but were unsuccessful. A straightforward calculation shows that the squarefree parts of the congruent numbers in our theorem are congruent to 6 modulo 8, so that if rank 4 could be attained for some of these curves, then we would expect from the conjecture of Birch and Swinnerton-Dyer that, in fact, the rank would be at least 5.

## References

[1] J. S. Chahal, *Congruent numbers and elliptic curves.* Amer. Math. Monthly **113**(2006), no. 4, 308–317.

[2] J. H. Coates, *Congruent number problem.* Q. J. Pure Appl. Math. **1**(2005), no. 1, 14–27.

[3] J .H. Silverman and J. Tate, *Rational points on elliptic curves.* Ungraduate Texts in Mathematics, Springer-Verlag, New York, 1992.

*Mathematics and Statistics, University of British Columbia Okanagan, Kelowna, BC*
*e-mail*: johnstone33@hotmail.com
Blair.Spearman@ubc.ca

https://doi.org/10.4153/CMB-2010-071-3 Published online by Cambridge University Press