ROCKY MOUNTAIN
JOURNAL OF MATHEMATICS
Volume 41, Number 6, 2011

ARITHMETIC PROGRESSIONS ON CONGRUENT NUMBER ELLIPTIC CURVES

BLAIR K. SPEARMAN

ABSTRACT. We give an infinite family of congruent number elliptic curves each possessing a nontrivial rational arithmetic progression. These elliptic curves yield a new infinite family of congruent number curves having rank at least three.

1. Introduction. The congruent number elliptic curves are defined by

$$E_n : y^2 = x(x^2 - n^2),$$

where n is a positive integer. If P_i, $i = 1, 2, 3$, are rational points on E_n, then they form an arithmetic progression if their $x-$coordinates $x_i = x(P_i)$ form an arithmetic progression. Such an arithmetic progression is called trivial if at least one of the points P_i is a torsion point, that is, $P_i \in \{(0, 0), (n, 0), (-n, 0)\}$ for some $i = 1, 2, 3$. Otherwise the arithmetic progression is nontrivial. In [**2**], Bremner, Silverman and Tzanakis showed that the curves E_n do not possess a nontrivial arithmetic progression of integral points if the rank of E_n is equal to 1. They do give one congruent number curve with a nontrivial arithmetic progression of integral points, namely,

$$y^2 = x(x^2 - 1254^2),$$

with integral points

$$(-528, 26136), \qquad (-363, 22869), \qquad (-198, 17424).$$

In [**1**] Bremner noted that rational points in arithmetic progression tend to be independent in the group of rational points. This suggests a possible rank of at least 3 for E_{1254}. In fact the rank of E_{1254} is

2010 AMS *Mathematics subject classification.* Primary 11G05.
Keywords and phrases. Arithmetic progression, congruent number, elliptic curve, rank.
Research supported by the Natural Sciences and Engineering Research Council of Canada.
Received by the editors on April 20, 2009, and in revised form on May 5, 2009.
DOI:10.1216/RMJ-2011-41-6-2033

equal to 3. The purpose of this paper is to give infinitely many curves E_n containing a nontrivial arithmetic progression of rational points of length three. In addition we confirm that these points are independent in the group of rational points of E_n and show that the rank of E_n is at least three. None of these arithmetic progressions extend to length four. In Section 2 we give a series of lemmas which will be used in proving that the rank is at least 3. In Section 3 we prove our main theorem. Finally we prove that infinitely many of the resulting congruent numbers n given in Theorem 1, are distinct modulo squares. We now state our main theorem.

Theorem 1. *The curve*

$$w^2 = 9t^4 + 4t^2 + 36 \tag{1}$$

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*

$$n = 6(3u^4 - 4u^2v^2 + 12v^4)(3u^4 + 4u^2v^2 + 12v^4), \tag{2}$$

and three points $P_i = (x_i, y_i)$, $i = 1, 2, 3$ *by*

$$\begin{aligned}(x_1, y_1) = (&-18(u^2 - 2v^2)^2(3u^4 - 4u^2v^2 + 12v^4),\\ &144(-u^2 + 2v^2)(3u^4 - 4u^2v^2 + 12v^4)^2uv),\end{aligned}$$

(3)

$$\begin{aligned}(x_2, y_2) &= (-3(3u^4 - 4u^2v^2 + 12v^4)^2, 9(3u^4 - 4u^2v^2 + 12v^4)^2 \\ &\qquad \times (u^2 + 2v^2)wv^2),\\ (x_3, y_3) &= (-48u^2v^2(3u^4 - 4u^2v^2 + 12v^4), 72uv(3u^4 - 4u^2v^2 + 12v^4)^2 \\ &\qquad \times (u^2 + 2v^2)).\end{aligned}$$

Then the points (x_i, y_i) *on the congruent number elliptic curve* $y^2 = x(x^2 - n^2)$ *have their* x *coordinates in arithmetic progression and the rank of* E_n *is at least* 3.

2. Some lemmas.

Lemma 1. *If u and v are integers with $(u, v) = 1$, then none of the given quantities is equal to a square in* $\mathbf{Q}$.

(i) $\pm 6(3u^4 - 4u^2v^2 + 12v^4)(3u^4 + 4u^2v^2 + 12v^4)$,

(ii) $\pm 2(3u^4 - 4u^2v^2 + 12v^4)$.

Proof. For case (i) with the plus sign, if u is odd then

$$2 \parallel 6(3u^4 - 4u^2v^2 + 12v^4)(3u^4 + 4u^2v^2 + 12v^4).$$

If u is even so that v is odd, then

$$2^5 \parallel 6(3u^4 - 4u^2v^2 + 12v^4)(3u^4 + 4u^2v^2 + 12v^4).$$

These calculations show that the given quantity cannot be equal to a square in $\mathbf{Q}$. The rest of the proof is similar. □

Lemma 2. *If u and v are nonzero integers with $(u, v) = 1$ then none of the given quantities is equal to a square in* $\mathbf{Q}$.

(i) $\pm 3(3u^4 + 4u^2v^2 + 12v^4)$,

(ii) $\pm (3u^4 + 4u^2v^2 + 12v^4)$,

(iii) $\pm (3u^4 - 4u^2v^2 + 12v^4)(3u^4 + 4u^2v^2 + 12v^4)$,

(iv) $\pm 3(3u^4 - 4u^2v^2 + 12v^4)$.

Proof. In order for any of these quantities to be equal to a square in $\mathbf{Q}$ we must choose the plus sign since $(3u^4 \pm 4u^2v^2 + 12v^4) > 0$. In that case, a pair (u, v) satisfying the conditions in Lemma 2 and yielding a square, say z^2, would in the first two cases, give rise to a rational point $(x, y) = (u^2/v^2,\ zu/v^3)$ on one of the following elliptic curves,

$$y^2 = 3x(3x^2 + 4x + 12),$$
$$y^2 = x(3x^2 + 4x + 12).$$

These curves have conductors 576 and 192, respectively. Each has rank 0 and their only finite rational points are $(0, 0)$ and $(0, 0)$, $(2, \pm 8)$, respectively, none of which is consistent with $x = u^2/v^2$ and $u \neq 0$. In the third case we would be led in a similar manner to the quartic curve

$$y^2 = (3x^2 - 4x + 12)(3x^2 + 4x + 12), \tag{4}$$

which is birationally equivalent to

$$y^2 = x^3 - 1971x - 32130.$$

This elliptic curve has conductor 24, and rank 0, allowing us to conclude that the quartic curve in (4) has as its only finite rational points $(0, \pm 12)$, neither of which is consistent with $x = u^2/v^2$ and $u \neq 0$. In the fourth case we are led to the quartic curve

$$y^2 = 3(3x^4 - 4x^2 + 12), \tag{5}$$

which is birationally equivalent to

$$y^2 = x^3 - 84x + 160.$$

This elliptic curve has conductor 576, and rank 0, allowing us to conclude that the quartic curve in (5) has as its only finite rational points $(0, \pm 6)$, neither of which is consistent with $x = u^2/v^2$ and $u \neq 0$. This proves the lemma. □

Lemma 3. *For integers u, v such that $(u, v) = 1$, none of the given quantities is equal to a square in* $\mathbf{Q}$.

(i) $\pm(3u^4 - 4u^2v^2 + 12v^4)$,

(ii) $\pm 3(3u^4 - 4u^2v^2 + 12v^4)(3u^4 + 4u^2v^2 + 12v^4)$.

Proof. Consider the first given quantity where the plus sign would have to be chosen in order to obtain a square in $\mathbf{Q}$. In this case the given quantity is congruent to $2u^2v^2$ modulo 3. Since 2 is not a quadratic residue modulo 3, we require $3 \mid u$ or $3 \mid v$. Combining these with the condition $\gcd(u, v) = 1$ yields

$$3 \parallel (3u^4 - 4u^2v^2 + 12v^4).$$

so that $3u^4 - 4u^2v^2 + 12v^4$ cannot be equal to a square in $\mathbf{Q}$. The proof of the second part of the statement is similar. □

Lemma 4. *There exist infinitely many pairs of rational numbers (t, w) such that*

$$w^2 = 9t^4 + 4t^2 + 36.$$

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

$$E(\mathbf{Q}) \simeq Z \times Z/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}.$$

Hence the given quartic has infinitely many rational points. □

3. Proof of theorem.

Proof. Lemma 4 shows that there are infinitely many points (t, w) on the curve

$$w^2 = 9t^4 + 4t^2 + 36,$$

so we can choose $t \neq 0$. Examining the factors on the right hand side of equation (2), we observe that n is positive. Easy calculations show that the points (x_i, y_i), $i = 1, 2, 3$, lie on the curve $y^2 = x(x^2 - n^2)$ and that

$$x_2 - x_1 = x_3 - x_2 = 3(u^2 - 6v^2)(3u^2 - 2v^2)(3u^4 - 4u^2v^2 + 12v^4).$$

Hence the points (x_i, y_i) are in arithmetic progression although their order depends on the relative sizes of u and v. Next we estimate the rank of $y^2 = x(x^2 - n^2)$. Rank estimation uses the following method which is described in Silverman and Tate [**4**]. Let Γ denote the group of rational points of an elliptic curve E in the form $y^2 = x(x^2 + ax + b)$. Let $\mathbf{Q}^*$ be the multiplicative group of non-zero rational numbers and let $\mathbf{Q}^{*2}$ denote the subgroup of squares of elements of $\mathbf{Q}^*$. Define the group homomorphism α from Γ to $\mathbf{Q}^*/\mathbf{Q}^{*2}$ as follows:

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

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

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

The rank r of the given curve E satisfies

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

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

From the definition of α we have

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

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

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

It follows from Lemma 1 (i) that these images are distinct modulo $\mathbf{Q}^{*2}$. We just list generators of the subgroup of $\alpha(\Gamma)$ which we are constructing. Therefore we have

$$\alpha(\Gamma) \supseteq \langle -1, n \rangle .$$

We have three non-torsion points $P_i = (x_i, y_i)$ on $y^2 = x(x^2 - n^2)$ given in (3), whose images under the mapping α we examine next. From (3) we obtain

$$\alpha(P_1) \equiv -2(3u^4 - 4u^2v^2 + 12v^4)(\operatorname{mod} \mathbf{Q}^{*2}),$$

so that

$$\alpha(\Gamma) \supseteq S_1 \cup \{-2(3u^4 - 4u^2v^2 + 12v^4)\}.$$

We check that $\alpha(P_1)$ is not congruent modulo $\mathbf{Q}^{*2}$ to any element of S_1. From Lemma 1 (ii) we see that the quantities $\pm 2(3u^4 - 4u^2v^2 + 12v^4)$

are not equal to squares in $\mathbf{Q}$. If $\pm\alpha(P_1)n$ were congruent to a square modulo $\mathbf{Q}^{*2}$ we would have after minor simplification that

$$\pm 3(3u^4 + 4u^2v^2 + 12v^4) \equiv 1(\operatorname{mod} \mathbf{Q}^{*2})$$

which contradicts Lemma 2 (i). Therefore

$$\alpha(\Gamma) \supseteq S_2 \doteqdot \left\langle -1, n, -2(3u^4 - 4u^2v^2 + 12v^4)\right\rangle.$$

Next we turn to $\alpha(P_2)$. We must show that $\alpha(P_2) \not\equiv s(\operatorname{mod} \mathbf{Q}^{*^2})$ 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

$$\alpha(P_2) \equiv \pm n^{c_1}(-2\left(3u^4 - 4u^2v^2 + 12v^4)\right)^{c_2} (\operatorname{mod} \mathbf{Q}^{*2}),$$

or

$$-3 \equiv \pm n^{c_1}\left(-2(3u^4 - 4u^2v^2 + 12v^4)\right)^{c_2} (\operatorname{mod} \mathbf{Q}^{*2}).$$

Comparing powers of 2 on both sides of this congruence we deduce from (2) and consideration of the power of 2 in $3u^4 \pm 4u^2v^2 + 12v^4$ that $c_1 = c_2$. For the congruence to hold we clearly cannot have $c_1 = c_2 = 0$ so that $c_1 = c_2 = 1$. Therefore one of

$$\pm(3u^4 + 4u^2v^2 + 12v^4)$$

must be equal to a square in $\mathbf{Q}$. This contradicts Lemma 2 (ii). Therefore

$$\alpha(\Gamma) \supseteq S_3 \doteqdot \left\langle -1, n, -2(3u^4 - 4u^2v^2 + 12v^4), 3\right\rangle,$$

and $|S_3| = 16$. To finish we show that show that $\alpha(P_3) \not\equiv s(\operatorname{mod} \mathbf{Q}^{*^2})$ 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

$$\alpha(P_3) \equiv \pm 3^{e_1} n^{e_2}(-2(3u^4 - 4u^2v^2 + 12v^4))^{e_3}(\operatorname{mod} \mathbf{Q}^{*2}),$$

that is,

$$(6) \quad -3(3u^4 - 4u^2v^2 + 12v^4) \equiv \pm 3^{e_1} n^{e_2}(-2(3u^4 - 4u^2v^2 + 12v^4))^{e_3}(\operatorname{mod} \mathbf{Q}^{*2}).$$

Examining the power of 2 dividing the left hand side of (6) we deduce as in the proof of Lemma 1 that

$$2^{2m} \parallel -3(3u^4 - 4u^2v^2 + 12v^4)$$

for some nonnegative integer m so that for some nonnegative integer t we have

$$2^{2t} \parallel \pm 3^{e_1} n^{e_2} (-2(3u^4 - 4u^2v^2 + 12v^4))^{e_3}.$$

Combining the method of proof of Lemma 1 (i) with a consideration of the power of 2 dividing $(3u^4 \pm 4u^2v^2 + 12v^4)$, we deduce that $e_2 = e_3$. Thus (6) reduces to

$$(7) \quad -3(3u^4 - 4u^2v^2 + 12v^4) \equiv \pm 3^{e_1} 3^{e_2} (3u^4 + 4u^2v^2 + 12v^4)^{e_2} (\operatorname{mod} \mathbf{Q}^{*2}).$$

Treating the cases $(e_1, e_2) = (0,0), (1,0), (0,1), (1,1)$ in order we deduce from (7) that one of the following quantities must be equal to a square in $\mathbf{Q}$.

$$\pm 3(3u^4 - 4u^2v^2 + 12v^4),$$
$$\pm (3u^4 - 4u^2v^2 + 12v^4),$$
$$\pm (3u^4 - 4u^2v^2 + 12v^4)(3u^4 + 4u^2v^2 + 12v^4).$$
$$\pm 3(3u^4 - 4u^2v^2 + 12v^4)(3u^4 + 4u^2v^2 + 12v^4).$$

This contradicts Lemma 2 (iv), Lemma 3 (i), Lemma 2 (iii) and Lemma 3 (ii). Thus $\alpha(\Gamma)$ contains the 17 elements in $S_3 \cup \{-2(3u^4 - 4u^2v^2 + 12v^4)\}$ and as $|\alpha(\Gamma)|$ is a power of 2, we see that $|\alpha(\Gamma)| \geq 32$. This proves that the rank of Γ is at least 3. □

4. Infinitely many rational arithmetic progressions.

Corollary 1. *There exist infinitely many congruent numbers distinct modulo squares whose associated elliptic curves E_n have rank at least 3 and which contain a nontrivial arithmetic progression.*

Proof. We need only verify that an infinite subset of the congruent numbers given in Theorem 1 are distinct modulo squares. If this were not the case then there would exist a finite set of nonzero rational numbers $\{d_i, = 1, \dots, m\}$ which are inequivalent modulo $\mathbf{Q}^{*2}$, such that for each congruent number n in our Theorem we have

$$n = 6(3u^4 - 4u^2v^2 + 12v^4)(3u^4 + 4u^2v^2 + 12v^4)$$
$$\equiv d_i (\operatorname{mod} \mathbf{Q}^{*^2}), \text{ for exactly one } d_i.$$

Equivalently, setting $t = u/v$, we obtain

$$6(3t^4 - 4t^2 + 12)(3t^4 + 4t^2 + 12) = d_i y^2,$$

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

$$d_i Y^2 = 6(3X^4 - 4X^2 + 12)(3X^4 + 4X^2 + 12).$$

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

Example 1. If we choose $(t, w) = (1, 7)$ satisfying (1) so that $(u, v) = (1, 1)$, then (2) and (3) give the example referred to in the introduction.

$$n = 1254,$$
$$(x_1, y_1) = (-198, 17424),$$
$$(x_2, y_2) = (-363, 22869),$$
$$(x_3, y_3) = (-528, 26136).$$

If we choose $(t, w) = (9/14, 1227/14)$ satisfying (1) so that $(u, v) = (9, 14)$, then (2) and (3) give the following congruent number and associated arithmetic progression in the x-coordinates.

$$n = 1362094185654 = 2 \cdot 3^3 \cdot 19 \cdot 241 \cdot 577 \cdot 9547,$$
$$(x_1, y_1) = (-726285533238, 982022971974022944),$$
$$(x_2, y_2) = (-522094929723, 909026269374801699),$$
$$(x_3, y_3) = (-317904326208, 746779526919152496).$$

Remark 1. Another infinite family of congruent number curves with rank at least three is given in [**3**]. These congruent numbers have the form

$$N = 6(U^4 + 2U^2V^2 + 4V^4)(U^4 + 8U^2V^2 + 4V^4), \tag{8}$$

for integers U, V with $\gcd(U,V) = 1$ and $T = U/V$ satisfying

$$T^4 + 14T^2 + 4 = W^2, \quad T \neq 0,$$

for some rational number W. Despite the somewhat similar appearance of these two families and the fact that the squarefree parts of both sets of congruent numbers are congruent to 6 modulo 8, these families are not identical. Although it is unknown if these families have any overlap, we can easily give an infinite subset of the congruent numbers n in this paper which cannot be equivalent modulo squares to any of the congruent numbers N given in (8). Therefore these n comprise a new family of congruent number curves with rank at least 3. For this purpose we require pairs of rational numbers (w, t) satisfying (1) such that if $t = u/v$ with $\gcd(u,v) = 1$ then $3 \nmid uv$. Suppose that we can do this. Let n be the congruent number given by (2). If there exists a congruent number N given by (8) with the property that nN is equal to the square of an integer then referring to (2) and (8) it would follow that $nN/36 = d^2$ for some integer d. As a congruence modulo 3 we would have

$$d^2 \equiv 2(U^2 + V^2)^4 u^4 v^4 \pmod 3.$$

This congruence is impossible since 2 is a quadratic nonresidue modulo 3 and $3 \nmid 2(U^2 + V^2)^4 u^4 v^4$. It remains therefore to find the pairs (w, t) satisfying (1) such that if $t = u/v$, $\gcd(u,v) = 1$ then $3 \nmid uv$. We consider the elliptic curve

$$y^2 = x(x^2 + 4/9x + 4). \tag{9}$$

A point of infinite order on this curve is $P = (2/3, 16/9)$. Induction shows that if $Q \in \{2P, 6P, 10P, \dots\}$, then $v_3(x(Q)) = 0$, where v_3 denotes the usual $3-adic$ valuation [**5**]. Further we note that, since Q is the double of a point on (9), $x(Q)$ must be equal to the square of a rational number say $x(Q) = t^2$, $t \in \mathbf{Q}$. If we write $t = u/v$ for integers u, v with $\gcd(u,v) = 1$ then $3 \nmid uv$ as required and the rational number t has the property that

$$9t^4 + 4t^2 + 36 = w^2$$

for some rational number w. A further infinite subset of the congruent numbers we just finished constructing would be distinct modulo squares using the same proof as in Corollary 1. This establishes the claim made in this remark.

Example 2. There may exist other families of congruent number curves containing nontrivial rational arithmetic progressions. For example it might be possible to develop the properties of the following family as was done for the family given in this paper. The curve

$$w^2 = 4t^4 - 4t^3 + 10t^2 - 12t + 6,$$

has infinitely many points. Choose $t \neq \pm 1, 1/2$, and set $t = u/v$ where u and v are integers with $\gcd(u, v) = 1$. Define the positive integer n by

$$n = 2(3u^2 - 4uv + 2v^2)(u^2 + 2v^2)(u^4 + 2u^2v^2 - 4uv^3 + 2v^4), \tag{10}$$

and three points (x_i, y_i), $i = 1, 2, 3$ by

(11)
$$\begin{aligned}
x_1 &= -2(u^2 + 2uv - 2v^2)^2(u^4 + 2u^2v^2 - 4uv^3 + 2v^4),\\
y_1 &= 8u(u - 2v)(u^2 + 2uv - 2v^2)(u^4 + 2u^2v^2 - 4uv^3 + 2v^4)^2,\\
x_2 &= -2(u^4 + 2u^2v^2 - 4uv^3 + 2v^4)^2,\\
y_2 &= 4(u^4 + 2u^2v^2 - 4uv^3 + 2v^4)^2(u^2 - uv + v^2)v^2w,\\
x_3 &= -2u^2(u - 2v)^2(u^4 + 2u^2v^2 - 4uv^3 + 2v^4),\\
y_3 &= 8u(u - 2v)(u^4 + 2u^2v^2 - 4uv^3 + 2v^4)^2(u^2 - uv + v^2).
\end{aligned}$$

Then the points (x_i, y_i) on the congruent number elliptic curve $y^2 = x(x^2 - n^2)$ have their x coordinates in arithmetic progression. If we choose $(t, w) = (-1/7, 138/49)$ so that $(u, v) = (-1, 7)$ then the formulas in (10) and (11) give (after scaling by 3^4) the following congruent number and three points in arithmetic progression on the associated elliptic curve.

$$\begin{aligned}
n &= 1978086 = 2 \cdot 3 \cdot 11 \cdot 17 \cdot 41 \cdot 43,\\
(x_1, y_1) &= (-1908386, 718997320)\,,\\
(x_2, y_2) &= (-971618, 1698388264)\,,\\
(x_3, y_3) &= (-34850, 369214840)\,.
\end{aligned}$$

REFERENCES

1. A. Bremner, *On arithmetic progressions on elliptic curves*, Experiment. Math. **8** (1999), 409–413.

2. A. Bremner, J.H. Silverman and N. Tzanakis, *Integral points in arithmetic progression on* $y^2 = x(x^2 - n^2)$, J. Number Theory **80** (2000), 187–208.

3. J.A. Johnstone and B.K. Spearman, *Congruent number elliptic curves with rank at least three*, Canad. Math. Bull., to appear.

4. J.H. Silverman and J. Tate, *Rational points on elliptic curves*, Springer, New York, 1985.

5. L.C. Washington, *Elliptic curves, number theory and cryptography*, Chapman and Hall, Boca Raton, FL, 2003.

Mathematics and Statistics, University of British Columbia, Okanagan, Kelowna, BC, Canada, V1V 1V7
Email address: Blair.Spearman@ubc.ca