Congruent Number Elliptic Curves with Rank at Least Two

Lorenz Halbeisen
Department of Mathematics, ETH Zentrum, Rämistrasse 101, 8092 Zürich, Switzerland
lorenz.halbeisen@math.ethz.ch

Norbert Hungerbühler
Department of Mathematics, ETH Zentrum, Rämistrasse 101, 8092 Zürich, Switzerland
norbert.hungerbuehler@math.ethz.ch

key-words: congruent number elliptic curves, integral Pythagorean triples

2010 Mathematics Subject Classification: 11G05 11D09

Abstract

We give an infinite family of congruent number elliptic curves, each with rank at least two, which are related to integral solutions of $m^2 = n^2 + nl + l^2$.

1 Introduction

Elliptic curves and their geometric and algebraic structure have been a flourishing field of research in the past. They find prominent applications in cryptography and played a key role in the proof of Fermat’s Last Theorem. A salient feature of the algebraic structure of an elliptic curve is its rank. Among general elliptic curves, congruent number curves of high rank are of particular interest (see, e.g., [3]). More difficult than finding an individual congruent number curve of high rank is to find infinite families of such curves. Johnstone and Spearman [8] constructed such a family with rank at least three which is related to rational points on the biquadratic curve $w^2 = t^4 + 14t^2 + 4$. In the present paper, we show an elementary construction for an infinite family of congruent number curves of rank at least two which are related to the quadratic diophantine equation $m^2 = n^2 + nl + l^2$, and which have three integral points with positive $y$-coordinate on a straight line. Incidentally, some members of the family exhibit surprisingly high individual rank. We start by fixing the notions and notations used throughout the text.

A positive integer $A$ is called a congruent number if $A$ is the area of a right-angled triangle with three rational sides. So, $A$ is congruent if and only if there exists a rational Pythagorean triple $(a, b, c)$ (i.e., $a, b, c \in \mathbb{Q}$, $a^2 + b^2 = c^2$, and $ab \neq 0$), such that $\frac{ab}{2} = A$. The sequence of integer congruent numbers starts with

$$5, 6, 7, 13, 14, 15, 20, 21, 22, 23, 24, 28, 29, 30, 31, 34, 37, \ldots$$

(see, e.g., the On-Line Encyclopedia of Integer Sequences [11]). For example, $A = 7$ is a congruent number, witnessed by the rational Pythagorean triple

$$\left(\frac{24}{5}, \frac{35}{12}, \frac{337}{60}\right).$$
It is well-known that $A$ is a congruent number if and only if the cubic curve
\[ C_A : y^2 = x^3 - A^2x \]
has a rational point $(x_0, y_0)$ with $y_0 \neq 0$. The cubic curve $C_A$ is called a **congruent number elliptic curve** or just **congruent number curve**. This correspondence between rational points on congruent number curves and rational Pythagorean triples can be made explicit as follows: Let
\[ C(Q) := \{(x, y, A) \in \mathbb{Q} \times \mathbb{Q}^* \times \mathbb{Z}^* : y^2 = x^3 - A^2x\}, \]
where $\mathbb{Q}^* := \mathbb{Q} \setminus \{0\}$, $\mathbb{Z}^* := \mathbb{Z} \setminus \{0\}$, and
\[ P(Q) := \{(a, b, c, A) \in \mathbb{Q}^3 \times \mathbb{Z}^* : a^2 + b^2 = c^2 \text{ and } ab = 2A\}. \]
Then, it is easy to check that
\[ \psi : \quad P(Q) \to C(Q) \]
\[ (a, b, c, A) \mapsto \left( \frac{b(b + c)}{2}, \frac{b^2(b + c)}{2}, A \right) \quad (1) \]
is bijective and
\[ \psi^{-1} : \quad C(Q) \to P(Q) \]
\[ (x, y, A) \mapsto \left( \frac{2xAy}{y}, \frac{x^2 - A^2}{y}, \frac{x^2 + A^2}{y}, A \right). \quad (2) \]
For positive integers $A$, a triple $(a, b, c)$ of non-zero rational numbers is called a **rational Pythagorean $A$-triple** if $a^2 + b^2 = c^2$ and $A = \left\lfloor \frac{ab}{2} \right\rfloor$. Notice that if $(a, b, c)$ is a rational Pythagorean $A$-triple, then $A$ is a congruent number and $|a|, |b|, |c|$ are the lengths of the sides of a right-angled triangle with area $A$. Notice also that we allow $a, b, c$ to be negative.

If $a, b, c$ are positive integers such that $a^2 + b^2 = c^2$ and $A = \frac{ab}{2}$ is integral, then the triple $(a, b, c)$ is a called a **Pythagorean $A$-triple**. For any positive integers $m$ and $n$ with $m > n$, the triple
\[ \left( \frac{2mn}{a}, \frac{m^2 - n^2}{b}, \frac{m^2 + n^2}{c} \right) \]
is a Pythagorean $A$-triple. In this case, we obtain $A = mn(m^2 - n^2)$ and
\[ \psi(a, b, c, A) = \left( \frac{m^2(m^2 - n^2)}{x}, \frac{m^2(m^2 - n^2)^2}{y}, A \right). \quad (3) \]
In particular, the point $(x, y)$ on $C_A$ which corresponds to the Pythagorean $A$-triple $(a, b, c)$ is an integral point.

Concerning the equation
\[ m^2 = n^2 + nl + l^2, \]
we would like to mention the following fact (see Dickson [2, Exercises XXII.2, p. 80] or Cox [1, Chapter 1]):
FACT 1. Let \( p_1 < p_2 < \ldots < p_j \) be primes, such that \( p_i \equiv 1 \mod 6 \) for \( 1 \leq i \leq j \), and let

\[ m = \prod_{i=1}^{j} p_i. \]

Then the number of positive, integral solutions \( l < n \) of

\[ m = n^2 + nl + l^2 \]

is \( 2^{j-1} \). By definition of \( m \), for each integral solution of \( m = n^2 + nl + l^2 \), \( n \) and \( l \) are relatively prime, denoted \( (n, l) = 1 \).

Moreover, the number of positive, integral solutions \( l < n \) of

\[ m^2 = n^2 + nl + l^2 \]

is \( 2^{j-1} \). Among the \( \frac{3^j-1}{2} \) integral solutions \( l < n \) of \( m^2 = n^2 + nl + l^2 \) we find \( 2^{j+1} \) solutions with \( (n, l) = 1 \). In particular, if \( j = 1 \) and \( p \equiv 1 \mod 6 \), then the solution in positive integers \( n < l \) of

\[ p^2 = n^2 + nl + l^2 \]

is unique and \( (n, l) = 1 \).

For a geometric representation of integral solutions of \( x^2 + xy + y^2 = m^2 \), see Halbeisen and Hungerbühler [5].

If \( m, n, l \) are positive integers such that \( m^2 = n^2 + nl + l^2 \), then, for \( k := n + l \), each of the following three triples

\[ \left( \frac{2mn}{a_1}, \frac{m^2 - n^2}{b_1}, \frac{m^2 + n^2}{c_1} \right), \]
\[ \left( \frac{2ml}{a_2}, \frac{m^2 - l^2}{b_2}, \frac{m^2 + l^2}{c_2} \right), \]
\[ \left( \frac{2mk}{a_3}, \frac{k^2 - m^2}{b_3}, \frac{k^2 + m^2}{c_3} \right), \]

is a Pythagorean \( A \)-triple for \( A = mn(m^2 - n^2) = ml(m^2 - l^2) = km(k^2 - m^2) \) (see Hungerbühler [7]). In particular, with \( m, n, l \) and (3) we obtain three distinct integral points on \( C_A \).

Let us now turn back to the curve \( C_A \). It is convenient to consider the curve \( C_A \) in the projective plane \( \mathbb{P}^2 \), where the curve is given by

\[ C_A : y^2z = x^3 - A^2xz^2. \]

On the points of \( C_A \), one can define a commutative, binary, associative operation \( + \), where \( O \), the neutral element of the operation, is the projective point \( (0,1,0) \) at infinity. More formally, if \( P \) and \( Q \) are two points on \( C_A \), then let \( P \# Q \) be the third intersection
point of the line through \( P \) and \( Q \) with the curve \( C_A \). If \( P = Q \), the line through \( P \) and \( Q \) is replaced with the tangent in \( P \). Then \( P + Q \) is defined by stipulating

\[
P + Q := \mathcal{O}(P \# Q),
\]

where for a point \( R \) on \( C_A \), \( \mathcal{O}(R) \) is the point reflected across the \( x \)-axis. The following figure shows the congruent number curve \( C_A \) for \( A = 5 \), together with two points \( P \) and \( Q \) and their sum \( P + Q \).

More explicitly, for two points \( P = (x_0, y_0) \) and \( Q = (x_1, y_1) \) on a congruent number curve \( C_A \), the point \( P + Q = (x_2, y_2) \) is given by the following formulas:

- If \( x_0 \neq x_1 \), then
  \[
x_2 = \lambda^2 - x_0 - x_1, \quad y_2 = \lambda(2x_0 - x_2) - y_0,
\]
  where
  \[
  \lambda := \frac{y_1 - y_0}{x_1 - x_0}.
\]

- If \( P = Q \), i.e., \( x_0 = x_1 \) and \( y_0 = y_1 \), then
  \[
x_2 = \lambda^2 - 2x_0, \quad y_2 = 3x_0\lambda - \lambda^3 - y_0,
\]
  where
  \[
  \lambda := \frac{3x_0^2 - A^2}{2y_0}.
\]

Below we shall write \( 2 \ast P \) instead of \( P + P \).

- If \( x_0 = x_1 \) and \( y_0 = -y_1 \), then \( P + Q := \mathcal{O} \). In particular, \( (0,0) + (0,0) = (A,0) + (A,0) = (-A,0) + (-A,0) = \mathcal{O} \).

- Finally, we define \( \mathcal{O} + P := P \) and \( P + \mathcal{O} := P \) for any point \( P \), in particular, \( \mathcal{O} + \mathcal{O} = \mathcal{O} \).
With the operation “+”, \((C_A, +)\) is an abelian group with neutral element \(O\). Let \(C_A(Q)\) be the set of rational points on \(C_A\) together with \(O\). It is easy to see that \((C_A(Q), +)\) is a subgroup of \((C_A, +)\). Moreover, it is well known that the group \((C_A(Q), +)\) is finitely generated. One can readily check that the three points \((0, 0)\) and \((\pm A, 0)\) are the only points on \(C_A\) of order 2, and one easily finds other points of finite order on \(C_A\). However, it is well known that if \(A\) is a congruent number and \((x_0, y_0)\) is a rational point on \(C_A\) with \(y_0 \neq 0\), then the order of \((x_0, y_0)\) is infinite. In particular, if there exists one rational Pythagorean \(A\)-triple, then there exist infinitely many such triples (for an elementary proof of this result, which is based on a theorem of Fermat’s, see Halbeisen and Hungerbühler [6]). Furthermore, Mordell’s Theorem states that the group of rational points on \(C_A\) is finitely generated, and by the Fundamental Theorem of Finitely Generated Abelian Groups, the group of rational points on an elliptic curve is isomorphic to some group of the form

\[
\mathbb{Z}/n_1\mathbb{Z} \times \ldots \times \mathbb{Z}/n_k\mathbb{Z} \times \mathbb{Z}^r,
\]

where \(n_1, \ldots, n_k\) and \(r\) are positive integers. The group \(\mathbb{Z}/\mathbb{Z}_{n_1} \times \ldots \times \mathbb{Z}/\mathbb{Z}_{n_k}\), which is generated by rational points of finite order, is the so-called torsion group, and \(r\) is called the rank of the curve. Now, since \(C_A\) does not have rational points of finite order besides the points \((0, 0)\) and \((\pm A, 0)\), the torsion group of \(C_A\) is isomorphic to \(\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}\).

Based on integral solutions of \(m^2 = n^2 + nl + l^2\), we will show that there are infinitely many congruent number curves \(C_A\) with rank at least two (for congruent number curves with rank at least three see Johnstone and Spearman [8]).

### 2 Rank at Least Two

In order to “compute” the rank of a curve of the form

\[
\Gamma : y^2 = x^3 + Bx,
\]

according to Silverman and Tate [10, Chapter III.6.], we first have to write down several equations of the form

\[
b_1M^4 + b_2e^2 = N^4 \tag{4}
\]

\[
\bar{b}_1\bar{M}^4 + \bar{b}_2\bar{e}^2 = \bar{N}^4, \tag{5}
\]

namely one for each factorisation \(B = b_1b_2\) and \(-4B = \bar{b}_1\bar{b}_2\), respectively, where \(b_1\) and \(\bar{b}_1\) are square-free. Then we have to decide, how many of these equations have integral solutions: Let \(\#\alpha(\Gamma)\) be the number of equations of the form (4) for which we find integral solutions \(M, e, N\) with \(e \neq 0\), and let \(\#\alpha(\bar{\Gamma})\) be the corresponding number with respect to equations of the form (5). Then, if \(r > 0\),

\[
2^r = \frac{\#\alpha(\Gamma) \cdot \#\alpha(\bar{\Gamma})}{4}.
\]
Moreover, one can show that if \((x, y)\) is a rational point on \(\Gamma\), where \(y \neq 0\), then one can write that point in the form

\[
x = \frac{b_1 M^2}{e^2}, \quad y = \frac{b_1 MN}{e^3},
\]

where \(M, e, N\) is an integral solution of an equation of the form (4), and vice versa. The analogous statement holds for rational points on the curve \(\tilde{\Gamma}: y^2 = x^3 - 4Bx\) with respect to equations of the form (5).

Now we are ready to prove

**Theorem 2.** Let \(m, n, l\) be pairwise relatively prime positive integers, where \(m = \prod_{i=1}^{j} p_i\) is a product of pairwise distinct primes \(p_i \equiv 1 \mod 6\) and \(m^2 = n^2 + nl + l^2\). Furthermore, let \(k := n + l\) and let \(A := klmn\). Then the rank of the curve

\[
C_A : y^2 = x^3 - A^2 x
\]

is at least two.

**Proof.** Since we have at least one rational point \((x, y)\) on \(C_A\) with \(y \neq 0\), we know that the rank \(r\) of \(C_A\) is positive. So, to show that the rank of the curve \(C_A\) is at least two, it is enough to show that \(\#\alpha(C_A) \geq 9\). For this, we have to show that there are integral solutions for (4) for at least 9 distinct square-free integers \(b_1\) dividing \(-A^2\), or equivalently, we have to find at least 9 rational points on \(C_A\), such that the 9 corresponding integers \(b_1\) are pairwise distinct, which we will do now.

Notice that because of (6), to compute \(b_1\) from a rational point \(P = (x, y)\) on \(C_A\) with \(x \neq 0\), it is enough to know the \(x\)-coordinate of \(P\) and then compute \(x \mod Q^2\) (i.e., we compute \(x\) modulo squares of rationals). The \(x\)-coordinates of the three integral points we get by (1) from the three Pythagorean \(A\)-triples \((a_1, b_1, c_1), (a_2, b_2, c_2), (a_3, b_3, c_3)\) generated by \(m, n, l, k\), are

\[
x_1 = m^2(m^2 - n^2) = m^2 k l, \quad x_2 = m^2(m^2 - l^2) = m^2 k n, \quad k^2(k^2 - m^2) = k^2 n l,
\]

and modulo squares, this gives us three values for \(b_1\), namely

\[
b_{1,1} = kl, \quad b_{1,2} = kn, \quad b_{1,3} = nl.
\]

Now, exchanging in each of the three Pythagorean \(A\)-triples the two catheti \(a_i\) and \(b_i\) (for \(i = 1, 2, 3\)), we obtain again three distinct integral points on \(C_A\), whose \(x\)-coordinates modulo squares give us

\[
b_{1,4} = mn, \quad b_{1,5} = ml, \quad b_{1,6} = mk.
\]

Finally, if we replace each hypothenuse \(c_j\) of these six Pythagorean \(A\)-triples with \(-c_j\), we obtain again six distinct integral points on \(C_A\), whose \(x\)-coordinates modulo squares give us

\[
b_{1,7} = -kl, \quad b_{1,8} = -kn, \quad b_{1,9} = -nl
\]

\[
b_{1,10} = -mn, \quad b_{1,11} = -ml, \quad b_{1,12} = -mk.
\]
In addition to these 12 integral points on $C_A$ (and the corresponding $b_1$'s), we have the two integral points $(\pm A, 0)$ on $C_A$, which give us

$$b_{1,13} = klmn \quad \text{and} \quad b_{1,14} = -klmn.$$  

Recall that, by assumption, $m$ is square-free and $k, l, n$ are pairwise relatively prime. Therefore, if for some $i, j$ with $1 \leq i < j \leq 14$, $b_{1,i} \equiv b_{1,j}$ modulo squares, at least two of the integers $k, l, n$ are squares, say $n = u^2$, and $l = v^2$ or $k = v^2$. Then

$$m^2 = u^4 + u^2v^2 + v^4 \quad \text{(in the case when } l = v^2),$$

or

$$m^2 = u^4 - u^2v^2 + v^4 \quad \text{(in the case when } k = v^2).$$

If $l = v^2$, this implies that $u^2 = 1$ and $v = 0$, or $u = 0$ and $v^2 = 1$, and if $k = v^2$, this implies that $u^2 = 1$ and $v = 0$, $u = 0$ and $v^2 = 1$, or $u^2 = v^2 = 1$ (see, for example, Mordell [9, p.19f] or Euler [4, p.16]).

So, at most one of the integers $k, l, n$ is a square, which implies that $\#\alpha(C_A) \geq 14$ and this completes the proof.

As an immediate consequence we get the following

**Corollary 3.** Let $m, n, l$ be as in Theorem 2 and let $q$ be a non-zero integer. Then the rank of the curve $C_{Aq^4}$ is at least two.

**Proof.** Notice that if $m, n, l$ are such that $m^2 = n^2 + nl + l^2$, then, for $mq, nq, lq$, we have $(mq)^2 = (nq)^2 + nq \cdot lq + (lq)^2$, which implies that for $\tilde{A} = kq \cdot lq \cdot mq \cdot nq = Aq^4$, the rank of the curve $C_{\tilde{A}}$ is at least two.

q.e.d.

## 3 Odds and Ends

As a matter of fact we would like to mention that the three integral points on $C_A$ which correspond to an integral solution of $m^2 = n^2 + nl + l^2$ lie on a straight line.

**Fact 4.** Let $m, n, l$ be positive integers such that $m^2 = n^2 + nl + l^2$, let $k = n + l$, and let $A = klmn$. Then the three integral points

$$\left(\frac{m^2(n^2 - m^2)}{x_1}, \frac{m^2(n^2 - m^2)^2}{y_1}\right),$$

$$\left(\frac{m^2(m^2 - n^2)}{x_2}, \frac{m^2(m^2 - n^2)^2}{y_2}\right),$$

$$\left(\frac{k^2(k^2 - m^2)}{x_3}, \frac{k^2(k^2 - m^2)^2}{y_3}\right),$$

on the curve $C_A$ lie on a straight line.
Proof. For $i = 2, 3$ let 

$$
\lambda_{1,i} := \frac{y_i - y_1}{x_i - x_1}.
$$

It is enough to show that $\lambda_{1,2} = \lambda_{1,3}$, or equivalently, that $\lambda_{1,3} - \lambda_{1,2} = 0$. Now, an easy calculation shows that $\lambda_{1,2} = k^2$ and that $\lambda_{1,3} - k^2 = \frac{0}{k(k-n)} = 0$. q.e.d.

As a last remark we would like to mention that with the help of SAGE we found that some of the curves which correspond to an integral solution of $m^2 = n^2 + nl + l^2$ have rank 3 or higher. In fact, we found several curves of rank 3 or 4, as well as the following curves of rank 5:

| $A = klmn$ | $m = \prod p_i$ | $l$ | $n$ | $k = n + l$ |
|------------|-----------------|-----|-----|------------|
| 237 195 512 400 | 7 · 127 | 464 | 561 | 1 025 |
| 8 813 542 297 560 | 7 · 13 · 37 | 232 | 3 245 | 3 477 |
| 10 280 171 942 040 | 37 · 67 | 741 | 2 024 | 2 765 |
| 81 096 660 783 600 | 37 · 103 | 2 139 | 2 261 | 4 400 |
| 225 722 120 463 840 | 13 · 19 · 31 | 505 | 7 392 | 7 897 |
| 457 485 316 904 280 | 7 · 31 · 37 | 895 | 7 544 | 8 439 |
| 5 117 352 889 729 080 | 67 · 223 | 1 551 | 14 105 | 15 656 |
| 281 692 457 452 791 000 | 79 · 409 | 9 064 | 26 811 | 35 875 |
| 24 666 188 870 481 576 600 | 13 · 31 · 223 | 46 169 | 57 400 | 103 569 |

It is possible that these curves might be candidates for high rank congruent number elliptic curves (for another approach see Dujella, Janfada, Salami [3]).

References

[1] David A. Cox, *Primes of the form $x^2 + ny^2$. Fermat, class field theory, and complex multiplication*, 2nd ed., John Wiley & Sons, Hoboken (NJ), 2013.

[2] Leonard Eugene Dickson, *Introduction to the theory of numbers*, 7th ed., The University of Chicago Press, Chicago (IL), 1951.

[3] Andrej Dujella, Ali S. Janfada, and Sajad Salami, *A search for high rank congruent number elliptic curves*, *Journal of Integer Sequences*, vol. 12 (2009), no. 5, Article 09.5.8, 11.

[4] Leonhard Euler, *De binis formulis speciei $xx + myy$ et $xx + nyy$ inter se concordibus et discordibus* (Conventui exhibuit die 5. Junii 1780), *Mémoires de l’Académie impériale des sciences de St. Pétersbourg*, 5e série, Tome VIII (1817–18), 3–45.

[5] Lorenz Halbeisen and Norbert Hungerbühler, *A geometric representation of integral solutions of $x^2 + xy + y^2 = m^2$, (submitted)*.

[6] ______, *A theorem of Fermat on congruent number curves*, *Hardy-Ramanujan Journal* (to appear), arXiv:1803.09604v1 [math.NT].

8
[7] Norbert Hungerbühler, *A proof of a conjecture of Lewis Carroll*, Mathematics Magazine, vol. 69 (1996), 182–184.

[8] Jennifer A. Johnstone and Blair K. Spearman, *Congruent number elliptic curves with rank at least three*, Canadian Mathematical Bulletin. Bulletin Canadien de Mathématiques, vol. 53 (2010), 661–666.

[9] Louis Joel Mordell, *Diophantine Equations*, Academic Press, London·New York, 1969.

[10] Joseph H. Silverman and John Tate, *Rational Points on Elliptic Curves*, 2nd ed., Springer-Verlag, New York, 2015.

[11] Neil James Alexander Sloane, *The On-Line Encyclopedia of Integer Sequences*, A003273, Oct 2013.