Congruent Number Elliptic Curves Related to Integral Solutions of $m^2 = n^2 + nl + l^2$

Lorenz Halbeisen and Norbert Hungerbühler
Department of Mathematics
ETH Zentrum
8092 Zürich
Switzerland
lorenz.halbeisen@math.ethz.ch
norbert.hungerbuehler@math.ethz.ch

Abstract
We construct 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, for example, [2]). More difficult than finding an individual congruent number curve of high rank is to find infinite families of such curves. Johnstone and Spearman [7] 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 that 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, namely rank five (whereas...
the members of the family given by Johnstone and Spearman [7] all have rank three. We
start by recalling some basic results on congruent numbers.

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, for example, the On-Line Encyclopedia of Integer Sequences [10, A003273]).

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. With respect to some congruent number $A$,
the correspondence between rational points $(x, y)$ with $y \neq 0$ on the congruent number curve
$C_A$ on the one hand, and rational Pythagorean triples $(a, b, c)$ with $ab = 2A$ on the other
hand, is given by

$$(a, b, c) \mapsto \left( \frac{b(b+c)}{2}, \frac{b^2(b+c)}{2} \right), \quad (1)$$

and

$$(x, y) \mapsto \left( \frac{2xA}{y}, \frac{x^2 - A^2}{y}, \frac{x^2 + A^2}{y} \right). \quad (2)$$

For a positive integer $A$, a triple $(a, b, c)$ of non-zero rational (integral) numbers such that
$a^2 + b^2 = c^2$ and $A = \frac{|ab|}{2}$ is called a rational (integral) Pythagorean $A$-triple. 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. In particular, 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 an integral Pythagorean $A$-triple. In this case, we obtain $A = mn(m^2 - n^2)$ and by (1)

$$(a, b, c) \mapsto \left( \frac{m^2(m^2 - n^2)}{x}, \frac{m^2(m^2 - n^2)}{y} \right). \quad (3)$$

Notice that in this case, the point $(x, y)$ on $C_A$ that corresponds to the integral Pythagorean
$A$-triple $(a, b, c)$ is an integral point.

Concerning the equations

$$m = n^2 + nl + l^2$$

**eq(m)**
and
\[ m^2 = n^2 + nl + l^2 \]  \hspace{1cm} \text{eq}(m^2) \]
we first prove the following result (for a geometric representation of integral solutions of \( x^2 + xy + y^2 = m^2 \), see Halbeisen and Hungerbühler [5]):

**Proposition 1.** Let \( p_1 < p_2 < \cdots < p_j \) be primes, such that \( p_i \equiv 1 \pmod{6} \) for \( 1 \leq i \leq j \), and let
\[ m = \prod_{i=1}^{j} p_i. \]

(a) The number of positive, integral solutions \((n, l)\) of eq\((m)\) with \( l < n \) is \( 2^j \).

(b) For each integral solution of eq\((m)\), \( n \) and \( l \) are relatively prime and neither \( n \) nor \( l \) is a multiple of \( p_i \) (for \( 1 \leq i \leq j \)).

(c) The number of positive, integral solutions \((n, l)\) of eq\((m^2)\) with \( l < n \) is \( \frac{3^j - 1}{2} \).

(d) Among the \( \frac{3^j - 1}{2} \) integral solutions solutions \((n, l)\) of eq\((m^2)\) with \( l < n \) we find \( 2^{j-1} \) solutions \((n, l)\) such that \( n \) and \( l \) are relatively prime. In particular, if \( j = 1 \) and \( p \equiv 1 \pmod{6} \), then the solution in positive integers \( l < n \) of
\[ p^2 = n^2 + nl + l^2, \]
such that \( n \) and \( l \) are relatively prime, is unique.

**Proof.**
(a) By Dickson [1, Exercises XXII.2, p.80], the number of integral solutions of eq\((m)\) is \( 6E(m) \), where \( E(m) \) is the excess of the number of divisors \( 3h + 1 \) of \( m \) over the number of divisors of the form \( 3h + 2 \). By definition of \( m \), \( E(m) = 2^j \). Now, with each positive, integral solution \((n, l)\) of eq\((m)\) with \( 0 < l < n \) we obtain the following 12 pairwise different integral solutions:
\[
(n, l), \ (l, n), \ (-n, -l), \ (-l, -n), \ \\
(-n, n + l), \ (n + l, -n), \ (n, -n - l), \ (-n - l, n), \ \\
(-l, n + l), \ (n + l, -l), \ (l, -n - l), \ (-n - l, l).
\]

So, if \( e(m) \) denotes the number of positive, integral solutions \((n, l)\) of eq\((m)\) with \( l < n \), then \( 6E(m) \geq 12e(m) \). On the other hand, every integral solution of \( m = n^2 + nl + l^2 \) corresponds to a unique positive, integral solution \((n, l)\) with \( l < n \), which implies that \( 6E(m) = 12e(m) \) and consequently we obtain \( e(m) = 2^{j-1} \).

(b) This follows immediately from the definition of \( m \).
Again by Dickson [1, Exercises XXII.2, p. 80], the number of integral solutions of eq\((m^2)\) is \(6E(m^2)\), where \(E(m^2) = 3^j\). Let \(e(m^2)\) denote the number of positive, integral solutions \((n, l)\) of \(m^2 = n^2 + nl + l^2\) with \(l < n\). In addition to the \(12e(m^2)\) integral solutions of eq\((m^2)\), we have the 6 solutions
\[(m, 0), (0, m), (-m, 0), (0, -m), (-m, m), (m, -m).\]
So, \(6E(m^2) = 12e(m^2) + 6\) and consequently we obtain \(e(m^2) = \frac{3^j - 1}{2}\).

For the sake of simplicity, let us call a positive, integral solution \((n, l)\) of eq\((m^2)\) with \(l < n\) a normal solution. Among the normal solutions \((n, l)\) of eq\((m^2)\), we distinguish between the ones with \(n\) and \(l\) relatively prime, which we call primitive solutions, and the other ones, which we call composite. For a given \(m\), there is a one-to-one correspondence between composite solutions of eq\((m^2)\) with \((n, l) = d > 1\) and primitive solutions of eq\(((m/d)^2)\) via the correspondence
\[m^2 = n^2 + nl + l^2 \iff (m/d)^2 = (n/d)^2 + (n/d)(l/d) + (l/d)^2.\]

The proof is now by induction on \(j\). For \(j = 1\), the statement follows from the definition of \(m\). Suppose the statement holds when \(m\) has \(j - 1\) or less prime factors. Then, let \(m\) have \(j\) prime factors. We observe by the above correspondence that the number of composite solutions to eq\((m^2)\) is
\[\sum_{\substack{r|\ m \\
0 < r < m}} P(r^2),\]
where \(P(r^2)\) is the number of primitive solutions to \(r^2 = n^2 + nl + l^2\). By the inductive step, if \(r\) is comprised of \(i\) prime factors of \(m\) then \(P(r^2) = 2^{i-1}\). Furthermore, the number of distinct factors \(r\) of \(m\) with \(i\) prime factors is \((\frac{j}{i})\), and therefore, by the binomial theorem, the number of composite solutions to eq\((m^2)\) is
\[\sum_{\substack{r|\ m \\
0 < r < m}} P(r^2) = \sum_{i=1}^{j-1} \binom{j}{i} 2^{i-1} = \frac{1}{2} ((1 + 2)^j - 2^j - 1) = \frac{3^j - 1}{2} - 2^{j-1}.\]

Since the total number of solutions to eq\((m^2)\) is \(\frac{3^j - 1}{2}\), by subtracting the number of composite solutions we finally obtain \(P(m^2) = 2^{j-1}\), which completes the proof.

Let us now consider the relationship between positive, integral solutions of \(m^2 = n^2 + nl + l^2\) and integral Pythagorean triples.

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
\[
\left(\frac{2mn}{a_1}, \frac{m^2 - n^2}{b_1}, \frac{m^2 + n^2}{c_1}\right),
\]
is an integral Pythagorean $A$-triple for

$$A = mn(m^2 - n^2) = ml(m^2 - l^2) = km(k^2 - m^2) = klmn$$

(see Hungerbühler [6]). In particular, with $m, n, l$ and (3) we obtain three distinct integral points on $C_A$.

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

Let us now turn back to the curve $C_A$, where $A$ is a congruent number. One can readily check that the three points $(0, 0)$ and $(\pm A, 0)$ are the only points on $C_A$ of order 2 with respect to the group law of elliptic curves. Moreover, one can show that these three points, together with the point at infinity, are the only points of finite order (for an elementary proof of this result, which is based on a theorem of Fermat; see Halbeisen and Hungerbühler [4]). This implies 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. So, Mordell’s theorem (which states that the group of rational points on $C_A$ is finitely generated) and the fundamental theorem of finitely generated abelian groups imply that the group of rational points on a congruent number curve $C_A$ is isomorphic to

$$\frac{\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}^r}{\text{torsion group}},$$

where $r > 0$ is the aforementioned rank of $C_A$.

## 2 Rank at least two

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 — where many of the curves $C_A$ have rank three or four and several curves have even rank five (see Section 3).

The following result, which can be found in Silverman and Tate [9, Chapter III.6.1], allows us to compute the rank — or at least a lower bound of the rank — of certain elliptic curves. For simplicity, we state the result just for congruent number curves.

**Proposition 2.** Let $b$ be a non-zero integer and let $\bar{b} := -4b$. Furthermore, let

$$B := \{ b_1 \in \mathbb{Z} : b_1 | b, \text{ and } b_1 \text{ is square-free} \}$$

and

$$\bar{B} := \{ \bar{b}_1 \in \mathbb{Z} : \bar{b}_1 | \bar{b}, \text{ and } \bar{b}_1 \text{ is square-free} \}.$$
Finally, let $\beta_b$ and $\beta_{\bar{b}}$ be the number of integers $b_1 \in B$ and $\bar{b}_1 \in \bar{B}$, respectively, such that the corresponding equation
\begin{align}
b_1 M^4 + \frac{b_1}{e} e^4 &= N^2 \tag{4} \\
\bar{b}_1 \bar{M}^4 + \frac{\bar{b}_1}{\bar{e}} \bar{e}^4 &= \bar{N}^2 \tag{5}
\end{align}
has integral solutions, where $e \neq 0$, $\bar{e} \neq 0$, and $(M, e) = (\bar{M}, \bar{e}) = 1$.

Then the rank $r$ of the curve $y^2 = x^3 + bx$ satisfies the equation

$$2^r = \beta_b \cdot \beta_{\bar{b}}.$$

Moreover, if $(x, y)$ is a rational point on the curve $y^2 = x^3 + bx$ with $y \neq 0$, then one can write that point in the form
\begin{align}
x &= \frac{b_1 M^2}{e^2}, \\
y &= \frac{b_1 M N}{e^3}, \tag{6}
\end{align}
where $M, e, N$ is an integral solution of (4) with $N > 0$ and $(M, e) = 1$, and vice versa. The analogous statement holds for rational points on the curve $y^2 = x^3 + \bar{b}x$ with respect to equations of the form (5).

Now we are ready to prove

**Theorem 3.** 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 $p_i \equiv 1 \pmod{6}$ and $m^2 = n^2 + nl + l^2$. Furthermore, let $k := n + l$ and let $A := klmn$. Then the rank of the congruent number 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 would be enough to show that $\beta_{-A^2} \geq 9$. 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. Even though it would be enough to find integral solutions for (4) for at least 9 distinct square-free integers $b_1$, we shall give 16 solutions, such that a single additional solution for (4) would give us a rank of at least three (see Proposition 5).

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 integral 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

$$x_1 = m^2(m^2 - n^2) = m^2 kl, \quad x_2 = m^2(m^2 - l^2) = m^2 kn, \quad x_3 = k^2(k^2 - m^2) = k^2 nl,$$

and modulo squares, this gives us three values for $b_1$ modulo squares, namely

$$b_{1,1} \equiv kl, \quad b_{1,2} \equiv kn, \quad b_{1,3} \equiv nl.$$

Now, exchanging in each of the three integral 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 gives us again three values for $b_1$ modulo squares, namely

$$b_{1,4} \equiv mn, \quad b_{1,5} \equiv ml, \quad b_{1,6} \equiv mk.$$

Finally, if we replace each hypotenuse $c_j$ of these six integral Pythagorean $A$-triples with $-c_j$, we obtain again six distinct integral points on $C_A$, whose $x$-coordinates give us six values for $b_1$ modulo squares, namely

$$b_{1,7} \equiv -kl, \quad b_{1,8} \equiv -kn, \quad b_{1,9} \equiv -nl$$

$$b_{1,10} \equiv -mn, \quad b_{1,11} \equiv -ml, \quad b_{1,12} \equiv -mk.$$

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 two more values for $b_1$ modulo squares, namely

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

Now, it remains to show that the square-free parts of the $b_{1,j}$'s are pairwise distinct. By assumption, $m$ is square-free and $k, l, n$ are pairwise relatively prime. Therefore, if for some $i, j$ with $1 \leq i < j \leq 14$, $b_{1,i} \equiv b_{1,j} \pmod{Q^2}$, 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 [8, p. 19f] or Euler [3, p. 16]). So, at most one of the integers $k, l, n$ is a square, which shows that at least 14 equations of the form (4) — for different square-free integers $b_1$ dividing $A^2$— have integral solutions. Notice that so far, because the corresponding points on $C_A$ are integral, we always had $|\epsilon| = 1$. 

7
Now, we show that there are also solutions for (4) with $b_{1,15} = 1$ and $b_{1,16} = -1$. Assume first that there is a solution for (4) with $b_{1,15} = 1$ and $e = 1$, i.e., there are positive integers $M$ and $N$ such that

$$M^4 - A^2 = N^2.$$  

Then we also have

$$A^2M^4 - A^4 = (AN)^2,$$

which shows that $\tilde{M} := A, \tilde{e} := M$, and $\tilde{N} := AN$, satisfy

$$-\tilde{M}^4 + A^2\tilde{e}^4 = \tilde{N}^2,$$

and hence, there is a solution for (4) with $b_{1,16} = -1$. Notice that since $|\tilde{e}| \neq 1$, the corresponding point on $C_A$ is not an integral point.

It remains to find a solution for (4) with $b_{1,15} = 1$ and $e = 1$. Since $m, n, l, k$ are pairwise relatively prime positive integers and $k = n + l$, exactly one of $n, l, k$ is even, i.e., at least one of $n$ and $l$ is odd. Without loss of generality, assume that $n$ is odd. Furthermore, by definition of $m$, $m$ is odd. Let $p := \frac{m+n}{2}$ and $q := \frac{m-n}{2}$. Then $p$ and $q$ are positive integers. Now, $m = p + q, n = p - q$, and $m^2 - n^2 = 4pq$, and since $m^2 - n^2 = kl$, we have

$$A = klmn = 4pq(p + q)(p - q).$$

Notice that since $pq(p+q)$ is even, we have $A \equiv 0 \pmod{8}$. An easy calculation shows that $M := p^2 + q^2$ and $N := (p^2 - q^2)^2 - (2pq)^2$ satisfy

$$M^4 - A^2 = N^2.$$

So, there is a solution for (4) with $b_{1,15} = 1$ and $e = 1$, which gives us again an integral point on $C_A$

This shows that $\beta_{-A^2} \geq 16$ and completes the proof. \qed

As an immediate consequence we get the following

**Corollary 4.** Let $m, n, l$ be as in Theorem 3 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. \qed

### 3 Rank at least three

**Proposition 5.** For $A = 341880$, the rank of the curve $C_A$ is at least three.
Proof. For \( k = 40, l = 7, m = 37, n = 33 \), we have \( A = klmn, m^2 = n^2 + nl + l^2 \), and \( k = n + l \). Thus, by Theorem 3, the rank of the curve \( C_A \) is at least two. Now, for \( b_{1,17} = -30 \), which is distinct from the square-free values of \( b_{1,1}, \ldots, b_{1,16} \), we get that \( M = 98, e = 1 \), \( N = 33600 \) is an integral solution of (4), which implies that the rank of \( C_A \) is at least three. In fact, with the help of {\texttt{sage}}, one can show that the rank of \( C_A \) is equal to three. \hfill \Box

As a final remark concerning the rank of congruent number curves, we would like to mention that with the help of \( \texttt{sage} \) we found that many 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 plenty of curves of rank 3 or 4, as well as the following curves of rank 5:

\[
\begin{array}{cccccc}
A = klmn & m = \prod p_i & l & n & k = n + l \\
237,195,512,400 & 7 \cdot 127 & 464 & 561 & 1025 \\
8,813,542,297,560 & 7 \cdot 13 \cdot 37 & 232 & 3,245 & 3,477 \\
10,280,171,942,040 & 37 \cdot 67 & 741 & 2,024 & 2,765 \\
81,096,660,783,600 & 37 \cdot 103 & 2,139 & 2,261 & 4,400 \\
225,722,120,463,840 & 13 \cdot 19 \cdot 31 & 505 & 7,392 & 7,897 \\
457,485,316,904,280 & 7 \cdot 31 \cdot 37 & 895 & 7,544 & 8,439 \\
5,117,352,889,729,080 & 67 \cdot 223 & 1,551 & 14,105 & 15,656 \\
281,692,457,452,791,000 & 79 \cdot 409 & 9,064 & 26,811 & 35,875 \\
24,666,188,870,481,576,600 & 13 \cdot 31 \cdot 223 & 46,169 & 57,400 & 103,569 \\
\end{array}
\]

Of special interest might be values of \( A \) which are related to an \( m \) with few factors, especially to primes \( m \). Recall that if \( m \) is prime, then the integers \( n, l, n + l \) such that \( m^2 = n^2 + nl + l^2 \) are unique, and therefore, \( A(m) := (n+l)lmn \) is determined by \( m \). Among the 666 prime numbers \( m \leq 11,113 \) with \( m \equiv 1 \pmod{6} \), we found the following 30 values of \( m \) such that \( C_{A(m)} \) has rank 4:

\[
127, 139, 181, 277, 337, 709, 769, 823, 829, 883, 1051, 1087, 1213, \\
1747, 1777, 1873, 2137, 2287, 2377, 2467, 2521, 3529, 3877, 3931, \\
4129, 4999, 5521, 7573, 9601, 10711.
\]

However, we did not find any prime \( m \equiv 1 \pmod{6} \) such that \( C_{A(m)} \) has rank 5.

The preceding observations might indicate that the congruent number curves \( C_A \) constructed in Theorem 3 are candidates for high rank congruent number elliptic curves (for another approach, see Dujella, Janfada, Salami [2]).

### 4 Acknowledgment

We would like to thank the referee for his or her valuable remarks which greatly helped to improve this article.
References


2010 Mathematics Subject Classification: Primary 11G05; Secondary 11D09.

Keywords: congruent number elliptic curves, Pythagorean triples.

(Concerned with sequence [A003273](https://oeis.org/A003273).)

Received October 29 2018; revised versions received January 25 2019; February 19 2019; May 15 2019; May 16 2019. Published in *Journal of Integer Sequences*, May 16 2019.

Return to *Journal of Integer Sequences* home page.