CONCORDANT NUMBERS WITHIN
ARITHMETIC PROGRESSIONS AND ELLIPTIC CURVES

BO-HAE IM

(Communicated by Matthew A. Papanikolas)

Abstract. If the system of two diophantine equations
\[ X^2 + mY^2 = Z^2 \]
and \[ X^2 + nY^2 = W^2 \]
has infinitely many integer solutions \((X, Y, Z, W)\) with \(\gcd(X, Y) = 1\), equivalently, the elliptic curve \(E_{m,n} : y^2 = x(x + m)(x + n)\) has positive rank over \(\mathbb{Q}\), then \((m, n)\) is called a strongly concordant pair. We prove that for a given positive integer \(M\) and an integer \(k\), the number of strongly concordant pairs \((m, n)\) with \(m, n \in [1, N]\) and \(m, n \equiv k\) is at least \(O(N)\), and we give a parametrization of them.

1. Introduction

The following is known as Euler’s concordant forms problem:

**Problem 1** (Euler’s concordant forms). For nonzero integers \(m\) and \(n\), are there integer solutions \((X, Y, Z, W)\) with \(\gcd(X, Y) = 1\) to the system of equations

\[ X^2 + mY^2 = Z^2 \quad \text{and} \quad X^2 + nY^2 = W^2? \]

In this paper, we consider an infinite family of positive integer pairs \((m, n)\) for which there are infinitely many integer solutions to (1) with \(\gcd(X, Y) = 1\).

When \(m = -n\), this problem is the congruent number problem and if there exist an integer solution \((X, Y, Z, W)\) with \(\gcd(X, Y) = 1\) to \(X^2 - nY^2 = Z^2\), and \(X^2 + nY^2 = W^2\), then such an integer \(n\) is called a congruent number. In [8] Tunnell found a formula under the BSD conjecture for determining whether or not a number is a congruent number by investigating the connection between congruent numbers and elliptic curves. Also Bennet proved the arithmetic progression of congruent numbers in [1], i.e. that for a positive integer \(M\) and an integer \(k\), there are infinitely many congruent numbers \(n\) such that \(n \equiv k \pmod{M}\).

Ono proved in [6] that if \(m = 1\) and \(n = 2k^2 - 1\) with \(k \neq 0, 1\) and \(2\), then there are infinitely many integer solutions \((X, Y, Z, W)\) with \(\gcd(X, Y) = 1\) to (1).

Our main result in this paper is to prove a lower bound of the number of positive integer pairs \((m, n)\) in arithmetic progressions for which there are infinitely many integer solutions to (1) with \(\gcd(X, Y) = 1\) and to give a parametrization of an infinite family of such pairs.

Received by the editors March 8, 2011 and, in revised form, July 19, 2011.

2010 Mathematics Subject Classification. Primary 11G05; Secondary 11D09, 11D45.

The author was supported by the Basic Science Research Program through the National Research Foundation of Korea (NRF), funded by the Ministry of Education, Science and Technology (No. 2009-0087887).

©2012 American Mathematical Society
Reverts to public domain 28 years from publication

791

License or copyright restrictions may apply to redistribution; see https://www.ams.org/journal-terms-of-use
In Section 2, we give a connection between such pairs and the rational points of elliptic curves and prove the main theorem, which shows that the number of such pairs \((m, n)\) in arithmetic progressions and with \(0 < m, n < N\) is at least \(O(N)\) (Theorem 7) and gives parametrizations of such pairs and solutions to (1). In Section 3, we consider the case when \(m = 1\) and give a parametrization of integers \(n\) and solutions to (1) when \(m = 1\) (Theorem 13); in particular, we show that the number of such integers \(n < N\) in arithmetic progressions is at least \(O(\sqrt{N})\). In Section 4, we consider the general case of nonzero distinct \(m\)-tuples \((n_1, \ldots, n_m)\) such that the system \(X^2 + Y^2 = Z^2, X^2 + n_1 Y^2 = Z^2, X^2 + n_m Y^2 = Z^2\) has integer solutions, and give a parametrization of them (Corollary 15).

2. STRONGLY CONCORDANT PAIRS AND THE MAIN THEOREM

Definition 2. An integer pair \((m, n)\) such that \(mn \neq 0\) and \(m \neq n\) is called a concordant pair if the system (1) has a nontrivial solution, i.e. an integer solution \((X, Y, Z)\) with \(XYZ \neq 0\). Equivalently, a nontrivial integer solution to (1) gives rise to a positive solution \((X, Y, Z, W)\) with \(\gcd(X, Y) = 1\) by dividing by \(\gcd\) and taking the absolute values, which is called a primitive solution. A concordant pair \((m, n)\) is called strong if the system (1) has infinitely many primitive solutions.

Example 3. The pair \((27, -5)\) is concordant but not strongly concordant. In fact, the system

\[ X^2 + 27Y^2 = Z^2, \quad X^2 - 5Y^2 = W^2 \]

has only one primitive solution, \((X, Y, Z, W) = (3, 1, 6, 2)\).

For integers \(m\) and \(n\) such that \(mn \neq 0\) and \(m \neq n\), let

\[ (2) \quad E_{m, n} : y^2 = x(x + m)(x + n). \]

The Euler concordant forms problem can be reduced to the existence of certain rational points of the elliptic curve \(E_{m, n}\) over \(\mathbb{Q}\) given in (2) as follows.

Lemma 4 ([5, Corollary 2]). For nonzero distinct integers \(m\) and \(n\), \((m, n)\) is a concordant pair if and only if there exists a point \(P \in E_{m, n}(\mathbb{Q})\) such that \(4P \neq O\).

Corollary 5. For nonzero distinct integers \(m\) and \(n\), \((m, n)\) is a strongly concordant pair if and only if \(E_{m, n}(\mathbb{Q})\) has positive rank.

Proof. By Lemma 4 for a concordant pair \((m, n)\), a primitive integer solution to (1) corresponds to a point \(P\) such that \(2Q = P \notin E_{m, n}(\mathbb{Q})[2]\) for some point \(Q\). Now we need to show the correspondence between infinitely many primitive solutions and infinitely many points of infinite order in \(E_{m, n}(\mathbb{Q})\).

For nonzero distinct integers \(m\) and \(n\), let \(\{(a_i, b_i, c_i, d_i) | i \in \mathbb{N}\}\) be an infinite set of primitive solutions to (1). Then

\[ P_i = \left( \frac{a_i^2}{b_i^2}, \frac{a_i c_i d_i}{b_i^3} \right) \in E_{m, n}(\mathbb{Q}). \]

Since \(\gcd(a_i, b_i) = 1\) for each \(i\), we have that \(P_i = P_j \iff i = j\). So \(E_{m, n}(\mathbb{Q})\) contains an infinite set \(\{P_i | i \in \mathbb{N}\}\) of points, but since \(E_{m, n}(\mathbb{Q})_{tor}\) is finite, this implies that \(E_{m, n}(\mathbb{Q})\) has a nontorsion point, so has positive rank.
Also, if \( E_{m,n}(\mathbb{Q}) \) has a non-torsion point \( Q \) and we let \( P_k = kQ = (a_k, b_k) \) for each \( k \in \mathbb{Z} \), then \( P_i \neq P_j \) for any \( i \neq j \). Also, for \( Q = (a_1, b_1) \) and \( 2Q = (a_2, b_2) \), by the duplication formula (\textit{[12] III.2.3} (d), p. 59), we get

\[
a_2 = \left( \frac{a_1 - mn}{2b_1} \right)^2 = \frac{u^2}{v^2},
\]

where \( \gcd(u, v) = 1 \).

By \textit{[3]} 4.1, p. 37, \( a_2, a_2 + m, a_2 + n \) are squares in \( \mathbb{Q} \). By multiplying by \( v^2 \), we show that

\[
(|u|, |v|, \sqrt{u^2 + mv^2}, \sqrt{u^2 + nv^2})
\]

is a primitive solution to (1). For each pair \( m, n \), the rank of \( E_{m,n}(\mathbb{Q}) \) is such that \( \gcd(m, n) = 1 \).

For every \( k \in \mathbb{Z} \), \( P_{2k} \) provides only one primitive solution (1). Since \( P_{2k} = \pm P_{2\ell} \), the infinite set \( \{ P_{2k} \in E_{m,n}(\mathbb{Q}) : k \in \mathbb{Z} \} \) provides infinitely many primitive solutions to (1). Hence \( (m, n) \) is a strongly concordant pair.

Remark 6. In Example \textit{[3]} for the pair \((27, -5)\), \( E_{27,-5} : y^2 = x(x + 27)(x - 5) \) has the Mordell-Weil group \( E_{27,-5}(\mathbb{Q}) \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z} \) which has zero rank, and \( Q = (-3, 24) \in E_{27,-5}(\mathbb{Q}) \) has the order 6, so as in \textit{[3]} and \textit{[4]}, \( 2Q = P = (9, 36) \) provides only one primitive solution \((X, Y, Z, W) = (3, 1, 6, 2)\) to (1).

The following is our main result.

**Theorem 7.** For a given integer \( M > 1 \) and an integer \( k \), if \( k' \in \mathbb{Z} \) is such that \( \frac{k}{M} < k' < M - 1 \), then a parametrization of an infinite family of strongly concordant pairs \((m_r(t), n_r(t))\) such that \((m_r(t), n_r(t)) \equiv k \) (mod \( M \)) is

\[
\begin{align*}
m_r(t) &= (k' - Mr)(Mt + 1) \\
n_r(t) &= -(Mt + Mr - k')
\end{align*}
\]

for each pair \((t, r)\) such that \( r \neq 0, 1 \) and \( t \neq 0, -r, \pm(r - 1) \) and for each of such a pair \((m_r(t), n_r(t))\), a primitive solution to (1) is

\[
(X, Y, Z, W) = c(Mt + Mr - k' + 1, \ 2, \ Mt - M + k' + 1, Mt + Mr - k' - 1),
\]

where \( c \) is 1 or 1/2 depending on the parity of \( Mt + Mr - k' + 1 \).

In particular, the number of strongly concordant pairs \((m, n)\) with \( m, n \in [1, N] \) and \( m, n \equiv k \) (mod \( M \)), equivalently, by Corollary \textit{[5]} the rank of \( E_{m,n}(\mathbb{Q}) \) is positive, is at least \( O(N) \).

**Proof.** For given integers \( M > 1 \) and \( k \), let \( k = Mq + k' \) where \( 0 \leq k' \leq M - 1 \). For integers \( t \) and \( r \), we let

\[
\begin{align*}
f_r(t) &= Mt + Mr - k' \\
g_r(t) &= Mt + 1 \\
h_r(t) &= Mt,
\end{align*}
\]

and

\[
\begin{align*}
m_r(t) &= g_r(t)h_r(t) - f_r(t) = (Mt + 1)(k' - Mr) \\
n_r(t) &= f_r(t)h_r(t) - g_r(t) = -(Mt + Mr - k') \\
x_r(t) &= f_r(t)g_r(t) = (Mt + Mr - k')(Mt + 1) \\
y_r(t) &= f_r(t)g_r(t)h_r(t) = (Mt + Mr - k')(Mt + 1)Mt.
\end{align*}
\]
Then, since $M > 1$ and $0 \leq k' \leq M - 1$, if $m_r(t) = 0$, then $r = 0$ when $k' = 0$, and if $n_r(t) = 0$, then $t = -r$ when $k' = 0$. If $n_r(t) = 1$, then $t = -r$ when $k' = 1$ and if $n_r(t) = -1$, then $t = -r + 1$ when $k' = M - 1$. If $m_r(t) = n_r(t)$, then $r = 1$ when $k' = M - 1$, or $t = 0$. Also note that

$$(n_r(t) - 1)^2 + 4m_r(t) = (-Mt + Mr - k' - 1)^2,$$

and if $-Mt + Mr - k' - 1 = 0$, then $t = r - 1$ when $k' = M - 1$. To avoid these zero-conditions, we let

$$T := \{(t, r) \in \mathbb{Z}^2 : r \neq 0, 1 \text{ and } t \neq 0, -r, \pm(r - 1)\}.$$

Then $T$ is an infinite subset of $\mathbb{Z}^2$. For each pair $(t, r) \in T,$

$$m_r(t)n_r(t) \neq 0, \quad n_r(t) \neq \pm 1, \quad m_r(t) \neq n_r(t),$$

and

$$(n_r(t) - 1)^2 + 4m_r(t) = (-Mt + Mr - k' - 1)^2 \neq 0,$$

and

$$m_r(t) \equiv k' \equiv k \pmod{M} \quad \text{and} \quad n_r(t) \equiv k' \equiv k \pmod{M}.$$

Also, for each pair $(t, r) \in T$, $E_{m_r(t), n_r(t)}$ defined in (2) is nonsingular and

$$P_t = (x_r(t), y_r(t)) \in E_{m_r(t), n_r(t)}(\mathbb{Q}).$$

By the duplication formula and using (5), we can get the following expressions for points $2P_t$ and $4P_t$ which are well-defined (by (6)):

$$2P_t = \left(\frac{(n_r(t) - 1)^2}{4}, -\frac{(n_r(t) + 1)(n_r(t) - 1)(-Mt + Mr - k' - 1)}{8}\right),$$

$$4P_t = \left\{\begin{array}{l}
A = 16n_r(t)m_r(t) - (n_r(t) - 1)^4, \\
B = 8(n_r(t)^2 + 1)m_r(t) + (n_r(t) - 1)^4, \\
C = 16n_r(t)m_r(t) + (n_r(t)^2 + 6n_r(t) + 1)(n_r(t) - 1)^2.
\end{array}\right.$$
Solving each equation for \( m_r(t) \) implies that
\[
(8) \quad m_r(t) = \frac{-1 - 8n_r(t)^3 + 6n_r(t)^2 + 3n_r(t)^4}{-16n_r(t)}
\]
or
\[
(9) \quad m_r(t) = \frac{n_r(t)^4 - 6n_r(t)^2 + 8n_r(t) - 3}{16}.
\]

Since \( m_r(t) \) is an integer, the case \( (8) \) implies that \( n_r(t) \) divides \((-1 - 8n_r(t)^3 + 6n_r(t)^2 + 3n_r(t)^4) \), which implies that \( n_r(t) \) divides \(-1 \), so \( n_r(t) = \pm 1 \), which is impossible for \((t, r) \in T\) by \( (6) \). The case \( (9) \) implies that
\[
r = -\frac{Mt + 3k'}{3M} + 2\sqrt{M^2t^2 + Mt + 1}.
\]

Since \( r \) is an integer and \( t \neq 0 \), \( M^2t^2 + Mt + 1 \) must be a square but not 1, say \( s^2\) in \( \mathbb{N} \). Then \( s \neq \pm 1 \) and \((2Mt+1-2s)(2Mt+1+2s) = -3\). So \((2Mt+1-2s, 2Mt+1+2s) = (-1, 3), (1, -3), (3, -1), \) or \((-3, 1)\). But each case implies that \( s = \pm 1 \), which is impossible. So we have shown that if \((t, r) \in T\), then \( 6P_t \neq O \).

If \( 8P_t = O \), then the \( y \)-coordinate of \( 4P_t \) is zero, so by \( (7) \), we have
\[
16n_r(t)m_r(t) - (n_r(t) - 1)^4 = 0
\]
or
\[
8(n_r(t)^2 + 1)m_r(t) + (n_r(t) - 1)^4 = 0
\]
or
\[
16n_r(t)m_r(t) + (n_r(t)^2 + 6n_r(t) + 1)(n_r(t) - 1)^2 = 0.
\]

Hence, by solving each equation for \( m_r(t) \),
\[
m_r(t) = \frac{(n_r(t) - 1)^4}{16n_r(t)}
\]
or
\[
m_r(t) = -\frac{(n_r(t) - 1)^4}{8(n_r(t)^2 + 1)}
\]
or
\[
m_r(t) = -\frac{(n_r(t)^2 + 6n_r(t) + 1)(n_r(t) - 1)^2}{16n_r(t)}.
\]

If the first case happens, since \( n_r(t) \) divides \((n_r(t) - 1)^4\), we must have that \( n_r(t) = \pm 1 \), which is impossible for \((t, r) \in T\) by \( (6) \).

If the second case happens, since \( n_r(t)^2 + 1 \) divides \((n_r(t) - 1)^4 = (n_r(t)^2 + 1)(n_r(t)^2 - 4n_r(t) + 5) - 4\), a positive integer \( n_r(t)^2 + 1 \) must divide \(-4\) and so \( n_r(t) = 0 \) or \( \pm 1 \), which is impossible for \((t, r) \in T\) by \( (6) \) again.

If the third case happens, since \( n_r(t) \) divides \((n_r(t)^2 + 6n_r(t) + 1)(n_r(t) - 1)^2\), we must have that \( n_r(t) = \pm 1 \), which is impossible for \((t, r) \in T\) by \( (6) \).

Thus, we have proved that \( 8P_t \neq O \) for each \((t, r) \in T\).

Therefore, for every pair \((t, r) \in T\), \( P_t \) is a nontorsion point of \( E_{m_r(t), n_r(t)}(\mathbb{Q}) \), so \( E_{m_r(t), n_r(t)}(\mathbb{Q}) \) is of positive rank and, by Corollary 5 \((m_r(t), n_r(t))\) is a strongly concordant pair.

Referring to \( (3) \) and \( (4) \) in Corollary 5 and \( (7) \), for each \((t, r) \in T\), the \( x \)-coordinate of \( 2P_t \) is
\[
a_r(t) = \frac{(Mt + Mr - k' + 1)^2}{4},
\]
so a primitive solution to \( (1) \) is \( c_r(Mt + Mr - k' + 1, 2, Mt - Mr + k' + 1, Mt + Mr - k' - 1) \), where \( c_r = 1 \) if \( Mt + Mr - k' + 1 \) is odd and \( c_r = 1/2 \) if \( Mt + Mr - k' + 1 \) is even.
Now we estimate a lower bound on the number of positive strongly concordant pairs.

For a positive integer \( N \), if \( \left( \frac{k' - \sqrt{N}}{M} \leq 1 - \frac{\sqrt{N}}{M} \right) \) and \( 0 < t < -r \left( \leq -r + \frac{k'}{M} \right) \), then \( 0 < m_r(t), n_r(t) \leq N \) and \((t, r) \in T\) and \((m_r(t), n_r(t))\) is a strongly concordant pair as we have discussed above.

Moreover, for each \( t \) where \((t, r) \in T\), the point \((m_r(t), n_r(t)) = (Mt + 1)(k' - Mr), -(Mt + Mr - k')\) lies in the straight line \( \ell_{t,r} : y = \frac{1}{Mr - k'}x + 1 - k' - Mr. \)

For \( i = 1, 2 \), if \( 0 < t_i < -r_i \) and \( 1 - \frac{\sqrt{N}}{M} < r_i < 0 \), then the intersection point of two lines \( \ell_{t_1, r_1} \) and \( \ell_{t_2, r_2} \) has the coordinates
\[
\begin{align*}
x &= -(Mr_1 - k')(Mr_2 - k') < 0, \\
y &= -(Mr_2 - k') + 1 - k' - Mr_1 \geq 1,
\end{align*}
\]
and so it lies in the second quadrant of the \((x, y)\)-plane. This implies that if \( 0 < t < -r \) and \( 1 - \frac{\sqrt{N}}{M} < r < 0 \), then \((t, r) \in T\) and the corresponding positive integer pairs \((m_r(t), n_r(t))\) are all distinct.

Hence, the number
\[
A(N) := \#\{(m, n) \in \mathbb{N}^2 : (m, n) \text{ is a strongly concordant pair} \}
\]
\[
\text{and } 0 < m, n \leq N \}
\]
\[
\geq \#\left\{(t, r) \in T : 1 - \frac{\sqrt{N}}{M} < r < 0, 0 < t < -r \right\}
\]
\[
(\text{10})
\]
\[
= \#\left\{(t, r) \in \mathbb{Z}^2 : 1 - \frac{\sqrt{N}}{M} < r < 0, 0 < t < -r \right\}
\]
\[
(\text{11})
\]
\[
= \frac{(\lfloor N/M - 1 \rfloor - 1)(\lfloor \sqrt{N}/M - 1 \rfloor)}{2}
\]
\[
> \frac{(\sqrt{N}/M - 3)(\sqrt{N}/M - 2)}{2}
\]
\[
> N/(9M^2) \text{ for every } N > 24M^2
\]
\[
= O(N).
\]

\textbf{Example 8.} When \( M = 8 \), by \textbf{(10)}, we can give a list of examples of positive strongly concordant pairs \((m, n)\) such that \( m, n \equiv k \pmod{8}, 0 < m, n < 3000 \); i.e. we list some pairs \((m_r(t), n_r(t))\), where \(-5.9 < 1 - \sqrt{3000}/8 < r < 0 \) and \( 0 < t < -r \). Note that we get at least \( 10 = \frac{(\lfloor N/M - 1 \rfloor - 1)(\lfloor \sqrt{N}/M - 1 \rfloor)}{2} \) pairs for each \( k \) as in \textbf{(11)}, where \( N = 3000 \). A list of examples of concordant pairs modulo 8 is given in Table 1.
3. STRONGLY CONCORDANT NUMBERS: WHEN \( m = 1 \)

**Definition 9.** An integer \( n \neq 0, 1 \) is a concordant number if the system (11) when \( m = 1 \) has a primitive solution, and \( n \) is called a strongly concordant number if the system (11) when \( m = 1 \) has infinitely many primitive solutions.

Denote \( E_{1,n} := E_n \) for an integer \( n \neq 0, 1 \), i.e.

\[
E_n = E_{1,n} : y^2 = x(x + 1)(x + n).
\]

**Theorem 10** ([5 Main Theorem 1]). For nonzero distinct integers \( m \) and \( n \),

1. \( E_{m,n}(\mathbb{Q})_{\text{tor}} \supseteq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z} \) if \( m \) and \( n \) are both squares, or \(-m\) and \( n - m \) are both squares.

2. \( E_{m,n}(\mathbb{Q})_{\text{tor}} \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z} \) if there exists a nonzero integer \( d \) such that \( m = d^2u^4 \) and \( n = d^2v^4 \), or \( m = -d^2u^4 \) and \( n = -d^2(u^4 - v^4) \), or \( m = d^2(u^4 - v^4) \) and \( n = -d^2v^4 \), where \( u^2 + v^2 = w^2 \).

3. \( E_{m,n}(\mathbb{Q})_{\text{tor}} \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z} \) if there exist integers \( a \) and \( b \) such that \( a/b \notin \{ -2, -1, -1/2, 0, 1 \} \) and \( m = a^4 + 2a^3b \) and \( n = 2ab^2 + b^4 \).

4. In all other cases, \( E_{m,n}(\mathbb{Q})_{\text{tor}} \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \).

**Lemma 11.** The torsion subgroup \( E_n(\mathbb{Q})_{\text{tor}} \) is isomorphic to \( \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \) or \( \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z} \).

**Proof.** This follows from Theorem 10 with \( m = 1 \). In other words, the cases (2) and (3) of Theorem 10 cannot occur when \( m = 1 \).

The following are necessary and sufficient conditions to a (strongly) concordant number \( n \) corresponding to \( E_n : y^2 = x(x + 1)(x + n) \).

**Corollary 12.** For an integer \( n \neq 0, 1 \), the following are equivalent:

1. \( n \) is a concordant number.

2. The rank of \( E_n(\mathbb{Q}) \) is positive.

3. \( n \) is a strongly concordant number.

**Proof.** By the proof of Lemma 11 \( n \) is a concordant number if and only if there exists a point \( P \in E_n(\mathbb{Q}) \) such that \( 4P \neq O \). But if \( P \) is a torsion point, then since the order of \( P \) is 1, 2 or 4 by Lemma 11 we must have that \( 4P = O \). So such a point \( P \) cannot be torsion. Therefore, if \( n \) is a concordant number, then the rank

---

**Table 1.** Examples of concordant pairs modulo 8

<table>
<thead>
<tr>
<th>( k )</th>
<th>((m, n)) such that ( m, n \equiv k \pmod{8}, 0 &lt; m, n &lt; 3000 )</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>(32, 360), (24, 680), (16, 1000), (8, 1320), (24, 288), (16, 544), (8, 880), (16, 216), (8, 408), (8, 144), …</td>
</tr>
<tr>
<td>1</td>
<td>(35, 369), (25, 697), (17, 1025), (9, 1353), (25, 297), (17, 561), (9, 825), (17, 225), (9, 425), (9, 153), …</td>
</tr>
<tr>
<td>2</td>
<td>(34, 378), (26, 714), (18, 1050), (10, 1386), (26, 306), (18, 578), (10, 850), (18, 234), (10, 442), (10, 162), …</td>
</tr>
<tr>
<td>3</td>
<td>(35, 387), (27, 731), (19, 1067), (11, 1419), (27, 315), (19, 595), (11, 875), (19, 243), (11, 459), (11, 171), …</td>
</tr>
<tr>
<td>4</td>
<td>(36, 396), (28, 748), (20, 1100), (12, 1432), (28, 324), (20, 612), (12, 900), (20, 252), (12, 476), (12, 180), …</td>
</tr>
<tr>
<td>5</td>
<td>(37, 405), (29, 765), (21, 1125), (13, 1486), (29, 333), (21, 629), (13, 925), (21, 261), (13, 493), (13, 189), …</td>
</tr>
<tr>
<td>6</td>
<td>(38, 414), (30, 782), (22, 1150), (14, 1518), (30, 342), (22, 646), (14, 950), (22, 270), (14, 510), (14, 198), …</td>
</tr>
<tr>
<td>7</td>
<td>(39, 423), (41, 799), (23, 1163), (15, 1551), (41, 351), (23, 663), (15, 975), (23, 279), (15, 527), (15, 207), …</td>
</tr>
</tbody>
</table>
of $E_n(\mathbb{Q})$ is positive. Conversely, if $E_n(\mathbb{Q})$ has a nontorsion point $Q$, then $4P \neq O$, so $n$ is a concordant number. Hence (1) and (2) are equivalent.

The statements (2) and (3) are equivalent by Corollary 5 when $m = 1$. □

**Theorem 13.** For a given positive integer $M > 1$ and an integer $k$, if $k' \in \mathbb{Z}$ is such that $k = Mq + k'$ and $0 \leq k' \leq M - 1$, a parametrization of an infinite family of positive strongly concordant numbers $n$ such that $n \equiv k \pmod{M}$ is

$$n = (Mr - k')((Mr - k' + 1)M^2t^2 - 1),$$

for $t \neq 0 \in \mathbb{Z}$ and $r \neq k'/M, k'/M - 1 \in \mathbb{Z}$, and for each $n$, a primitive positive integer solution to (1) when $m = 1$ is

$$(X, Y, Z, W) = c(M^2t^2 - 1, 2Mt, M^2t^2 + 1, (2Mr - 2k' + 1)M^2t^2 - 1),$$

where $c = 1$ or $1/2$ depending on the parity of $M^2t^2 - 1$.

In particular, the number of strongly concordant numbers $n$ such that $n \in [1, N]$ and $n \equiv k \pmod{M}$, equivalently by Corollary 12 such that the rank of $E_n(\mathbb{Q})$ is positive, is at least $O(\sqrt{N})$.

**Proof.** For each integer $r \neq k'/M, k'/M - 1$ (in fact, since $0 \leq k' \leq M - 1$, this is equivalent to $r \neq 0$ when $k' = 0$ or $1$) and each integer $t \neq 0$, we set the following:

$$\begin{cases} 
  n_r(t) = (Mr - k')((Mr - k' + 1)M^2t^2 - 1) \\
  x_r(t) = (Mr - k' + 1)M^2t^2 - 1 \\
  y_r(t) = (Mr - k' + 1)Mt ((Mr - k' + 1)M^2t^2 - 1) . 
\end{cases}$$

Then, since $M > 1$ and $r \neq k'/M, k'/M - 1$ are integers, we have that

$$n_r(t) \neq 0, 1,$$

so $E_{n_r(t)}$ is nonsingular. Also we can check that

$$P_t = (x_r(t), y_r(t)) \in E_{n_r(t)}(\mathbb{Q}(t)).$$

Referring to (3) in Corollary 5 for $r \neq k'/M, k'/M - 1$, and $t \neq 0$, the $x$-coordinate of $2P_t$ is

$$a_t = \frac{(M^2t^2 - 1)^2}{(2Mt)^2},$$

so a primitive solution to

$$X^2 + Y^2 = Z^2, \quad X^2 + n_r(t)Y^2 = W^2$$

is $c(M^2t^2 - 1, 2Mt, M^2t^2 + 1, (2Mr - 2k' + 1)M^2t^2 - 1)$, where $c = 1$ if $M^2t^2 - 1$ is odd and $c = 1/2$ if $M^2t^2 - 1$ is even.

This implies that $n_r(t)$ is a concordant number for every integer $r \neq k'/M, k'/M - 1$ and $t \neq 0$. By Corollary 12 $n_r(t)$ is a strongly concordant number and $E_{n_r(t)}(\mathbb{Q})$ has positive rank.

Now we estimate a lower bound of positive strongly concordant numbers. For a positive integer $N$, if $r > k'/M$, $t \neq 0$ and $-\frac{\sqrt{N}}{M(Mr - k' + 1)} < t < \frac{\sqrt{N}}{M(Mr - k' + 1)}$, then $0 < n_r(t) \leq N$. 


So the number of strongly congruent numbers in the interval \([1, N]\) is at least
\[
2 \cdot \# \left\{ (t, r) \in \mathbb{Z}^2 : r > \frac{k'}{M}, \ 1 < t < \frac{\sqrt{N}}{M(Mr - k' + 1)} \right\}
\]
\[
= 2 \cdot \sum_{r=1}^{\lfloor \sqrt{N}/M^2 + (k'-1)/M \rfloor} \frac{\sqrt{N}}{M(Mr - k' + 1)}
\]
\[
\geq \frac{2\sqrt{N}}{M(M - k' + 1)} = O(\sqrt{N}).
\]

4. Concordant tuples: A system of more than two equations

We generalize the definitions of a concordant number and a concordant pair (Definition 2 and Definition 9).

**Definition 14.** Let \(m \in \mathbb{N}\). An integer \(m\)-tuple \((n_1, n_2, \ldots, n_m)\) such that \(n_i \neq 0, 1\) and the \(n_i\) are distinct is called a **concordant \(m\)-tuple** if the system of \(m+1\) equations
\[
X^2 + Y^2 = Z^2, \ X^2 + n_1Y^2 = Z_1^2, \ldots, \ X^2 + n_mY^2 = Z_m^2
\]
has an integer solution \((X, Y, Z, Z_1, Z_2, \ldots, Z_m)\) with \(XYZZ \neq 0\), which is called a nontrivial solution. Equivalently, a nontrivial integer solution to (13) is a solution \((X, Y, Z, Z_1, Z_2, \ldots, Z_m)\) with gcd\((X, Y) = 1\) by dividing by gcd, which is called **primitive**.

**Corollary 15.** Let \(m \in \mathbb{N}\). For an integer \(M > 1\) and any integers \(k_1, k_2, \ldots, k_m\), there is an infinite family of concordant \(m\)-tuples \((n_1, n_2, \ldots, n_m)\) such that \(n_i \equiv k_i \pmod{M}\).

In particular, a parametrization of concordant \(m\)-tuples \((n_1(t), n_2(t), \ldots, n_m(t))\) such that \(n_i(t) \equiv k_i \pmod{M}\) can be given by
\[
n_i(t) = (Mr_i - k_i')((Mr_i - k_i' + 1)M^2t^2 - 1),
\]
where \(k_i = Mr_i + k_i'\) with \(0 \leq k_i' < M\) and for each \(t \neq 0\), \(r_i\) is such that \((Mr_i - k_i')((Mr_i - k_i' + 1)M^2t^2 - 1)\) are distinct. A corresponding primitive solution to (13) is given by
\[
(X, Y, Z, Z_1, \ldots, Z_m) = c(M^2t^2 - 1, 2Mt, M^2t^2 + 1, (2Mr_1 - 2k_1' + 1)M^2t^2 - 1, \ldots, (2Mr_m - 2k_m' + 1)M^2t^2 - 1),
\]
where \(c = 1\) or \(1/2\) depending on the parity of \(M^2t^2 - 1\).

Also, the number of concordant \(m\)-tuples \((n_1, n_2, \ldots, n_m)\) such that \(n_i \equiv k_i \pmod{M}\) and \(0 < n_i \leq N\) is at least \(O(\sqrt{N})\).

**Proof.** This follows from Theorem 13. In particular, for an integer \(s \geq 2\), \(n_i(t) > 0\) for \(r_i > 0\) and if we choose \(r_i = s + i\) for each \(i = 1, 2, \ldots, m\), then \(n_m(t) > \cdots > m_1(t)\). So \(n_i(t) \leq N\) for each \(i = 1, 2, \ldots, m\) if and only if \(n_m(t) \leq N\). So by Theorem 13 the number of concordant \(m\)-tuples \((n_1, n_2, \ldots, n_m)\) such that \(n_i \equiv k_i \pmod{M}\) and \(0 < n_i \leq N\) is at least \(O(\sqrt{N})\).

**Acknowledgement**

The author would like to thank the anonymous referees for pointing out that Theorem 13 can be generalized to Corollary 15 and for valuable suggestions and comments.
REFERENCES


Department of Mathematics, Chung-Ang University, 221, Heukseok-dong, Dongjak-gu, Seoul, 156-756, South Korea

E-mail address: bohaeim@gmail.com, imbh@cau.ac.kr