CONSTRUCTION OF AN INFINITE FAMILY OF ELLIPTIC CURVES OF 2-SELMER RANK 1 FROM HERON TRIANGLES

DEBOPAM CHAKRABORTY, VINODKUMAR GHALE, AND ANUPAM SAIKIA

Abstract

Given any positive integer $n$, it is well known that there always exist triangles with rational sides $a, b$ and $c$ such that the area of the triangle is $n$. Assuming finiteness of the Shafarevich-Tate group, we first construct a family of infinitely many Heronian elliptic curves of rank exactly 1 from Heron triangles of a certain type. We also explicitly produce a separate family of infinitely many Heronian elliptic curves with 2-Selmer rank lying between 1 and 3.

1. Introduction

The congruent number problem is to determine which positive integers $n$ appear as the area of a right triangle with rational sides. The problem boils down to identifying the elliptic curve $E_n : y^2 = x^3 - n^2x$, known as the congruent number elliptic curve, with positive rank. Currently, there is no algorithm to determine whether a given positive integer $n$ is congruent or not. The Birch and Swinnerton-Dyer conjecture [1] predicts that $n$ should be a congruent number if $n \equiv 5, 6$ or $7 \pmod{8}$. Understanding the 2-Selmer rank plays an important role in the rank computation of an elliptic curve. In [2] and [3], D. R. Heath-Brown examined the size of the 2-Selmer group of the congruent elliptic curve $E_n$. A glimpse of the extensive studies on the congruent number problem can be found in [4], [7], [9] and [13].

An immediate generalization of the congruent number problem is the existence of positive integer $n$ as the area of triangles with rational sides without the constraint of being a right angle triangle. Such triangles are called Heron triangles. In [12], Goins and Maddox have proved that the existence of a Heron triangle of area $n$ is equivalent to the existence of rational points of order greater than 2 on an associated elliptic curve (given by (2.1)). Elliptic curves associated with Heron triangles appear in the works of various
authors. For a given integer \( n \), the existence of infinitely many Heron triangles with the area \( n \) has been studied in [17]. Buchholz and Rathbun [4] proved the existence of infinitely many Heron triangles with two rational medians. Later in [5], Buchholz and Stingley looked into the existence of Heron triangles with three rational medians. In [10], Dujella and Peral have shown the existence of elliptic curves of higher ranks associated with Heron triangles. In [13], Halbeisen and Hungerbühler have shown the existence of elliptic curves of rank at least two associated with Heron triangles. In a recent work of Ghale et al. [11], the authors constructed a family of elliptic curves of rank at most one from a certain Diophantine equation via Heron triangle.

In this article, we consider two primes \( p \) and \( q \) such that \( p \equiv 7 \pmod{8} \) and \( q = 4^m + 1 \).

We examine the group structure of elliptic curves associated with Heron triangles of area \( 2^m p \) having one of the angles as \( \theta \) such that \( \tau = \tan \frac{\theta}{2} = 2^m \). We prove the following theorem.

**Theorem 1.1.** Let \( p \) be a prime congruent to 7 modulo 8 and \( q = 4^m + 1 \) be a prime such that \( \left( \frac{p}{q} \right) = 1 \). Then the 2-Selmer rank of the elliptic curve

\[
E : y^2 = x(x - 4^m p)(x + p)
\]

is 1 when \( m = 1 \). In case \( m \geq 2 \), the 2-Selmer rank of \( E \) lies between 1 and 3.

Here, for an odd prime \( l \) and an integer \( a \) coprime to \( l \), \( \left( \frac{a}{l} \right) \) denotes the Legendre symbol of \( a \) modulo \( l \). We deduce the following corollary under the assumption of the finiteness of the Shafarevich-Tate group.

**Corollary 1.2.** The Mordell-Weil rank of the elliptic curve \( E \) given by (1.1) is at most 1 when \( m = 1 \). Moreover, if we assume the finiteness of the Shafarevich-Tate group \( \text{III}(E/\mathbb{Q}) \), then the rank of \( E(\mathbb{Q}) \) is exactly 1 and the 2-part of \( \text{III}(E/\mathbb{Q}) \) is trivial.

The corollary guarantees the existence of infinitely many Heron triangles with area \( 2p \) and one angle \( \theta \) such that \( \tau = \tan \frac{\theta}{2} = 2 \), since for \( q = 5 \) we have infinitely primes \( p \equiv 7 \pmod{8} \) such that \( \left( \frac{p}{5} \right) = 1 \) by Dirichlet’s theorem on primes in arithmetic progression.

2. The 2-Selmer Group

We begin this section by recalling the association of a Heron triangle with an elliptic curve. In [12], Goins and Maddox have shown that any triangle \( \Delta_{\tau,n} \) of area \( n \in \mathbb{Z} \) with
rational sides $a, b, c$ and an angle $\theta$ is associated with the elliptic curve

$$E_{\Delta, n} : \quad y^2 = x(x - n\tau)(x + n\tau^{-1}),$$

where $\tau$ denotes $\tan \frac{\theta}{2}$. Moreover, they have shown that the torsion group of $E_{\Delta, n}(\mathbb{Q})$ will be either $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ or $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$, the triangle being isosceles in the latter case. One can identify the elliptic curve given by (1.1) with a Heron triangle of area $2^m p$ and an angle $\theta$ such that $\tau = \tan \frac{\theta}{2} = 2^m$.

By the method of 2-descent (see [19], Section X.1.4), there exists an injective homomorphism

$$b : E(\mathbb{Q})/2E(\mathbb{Q}) \longrightarrow \mathbb{Q}(S, 2) \times \mathbb{Q}(S, 2)$$

defined by

$$b(x, y) = \begin{cases} 
(x, x - 4^m p) & \text{if } x \neq 0, 4^m p, \\
(-1, -p) & \text{if } x = 0, \\
(p, q) & \text{if } x = 4^m p, \\
(1, 1) & \text{if } P = \mathcal{O},
\end{cases}$$

where

$$\mathbb{Q}(S, 2) = \{b \in \mathbb{Q}^*/(\mathbb{Q}^*)^2 : \text{ord}_l(b) \equiv 0 \pmod{2} \text{ for all finite primes } l \neq 2, p, q\}$$

$$= \{\pm 1, \pm 2, \pm p, \pm q, \pm 2p, \pm 2q, \pm pq, \pm 2pq\}.$$

Moreover, if $(b_1, b_2) \in \mathbb{Q}(S, 2) \times \mathbb{Q}(S, 2)$ is a pair that is not in the image of one of the three points $\mathcal{O}, (0, 0), (4^m p, 0)$, then $(b_1, b_2)$ is the image of a point $P = (x, y) \in E(\mathbb{Q})/2E(\mathbb{Q})$ if and only if the equations

$$b_1 z_1^2 - b_2 z_2^2 = 4^m p,$$

$$b_1 z_1^2 - b_1 b_2 z_3^2 = -p,$$

have a solution $(z_1, z_2, z_3) \in \mathbb{Q}^* \times \mathbb{Q}^* \times \mathbb{Q}$. These equations represent a homogeneous space for $E$ ([19]).

The image of $E(\mathbb{Q})/2E(\mathbb{Q})$ under the 2-descent map is contained in a subgroup of $\mathbb{Q}(S, 2) \times \mathbb{Q}(S, 2)$ known as the 2-Selmer group $\text{Sel}_2(E/\mathbb{Q})$, which fits into an exact sequence (see Chapter X, [19])

$$0 \longrightarrow E(\mathbb{Q})/2E(\mathbb{Q}) \longrightarrow \text{Sel}_2(E/\mathbb{Q}) \longrightarrow \text{III}(E/\mathbb{Q})[2] \longrightarrow 0.$$
The elements in $\text{Sel}_2(E/\mathbb{Q})$ correspond to the pairs $(a, b) \in \mathbb{Q}(S, 2)^2$ such that the system of equations (2.3) and (2.4) have non-trivial local solutions in $\mathbb{Q}_l$ at all primes $l$ of $\mathbb{Q}$ including infinity. Note that $\# E(\mathbb{Q})/2E(\mathbb{Q}) = 2^{2+r(E)}$. It is customary to denote $\# \text{Sel}_2(E/\mathbb{Q}) = 2^{2+s(E)}$, and refer to $s(E)$ as the 2-Selmer rank. Clearly, we have

(2.6) $0 \leq r(E) \leq s(E)$.

From the inequality above as well as the exact sequence (2.5), it can be easily seen that the 2-Selmer rank controls both $E(\mathbb{Q})$ and $\text{III}(E/\mathbb{Q})[2]$.

### 3. Local Solutions for the Homogeneous Spaces

In this section, we examine the properties of the $l$-adic solutions for the equations (2.3) and (2.4) that are associated with the 2-Selmer group. In a later section, we use these properties to bound the size of the 2-Selmer group. We use the well-known fact that any $l$-adic number $a$ can be written as $a = l^n \cdot u$ where $n \in \mathbb{Z}$, $u \in \mathbb{Z}_l^*$. We first prove the following result for all odd primes $l$.

**Lemma 3.1.** Suppose the equations (2.3) and (2.4) have a solution $(z_1, z_2, z_3) \in \mathbb{Q}_l \times \mathbb{Q}_l \times \mathbb{Q}_l$ for any odd prime $l$. If $v_l(z_i) < 0$ for any one $i \in \{1, 2\}$, then $v_l(z_1) = v_l(z_2) = v_l(z_3) = -k < 0$ for some integer $k$.

**Proof.** Let $z_i = l^{k_i} u_i$, where $k_i \in \mathbb{Z}$ and $u_i \in \mathbb{Z}_l^*$ for $i = \{1, 2, 3\}$. Then $v_l(z_i) = k_i$ for all $i \in \{1, 2, 3\}$.

Suppose $k_1 < 0$. Then from equation (2.3) one can get that

$$b_1u_1^2 - b_2u_2^2l^{2(k_2-k_1)} = 4^m pl^{-2k_1}.$$ 

If $k_2 > k_1$, then $l^2$ must divide $b_1$, a contradiction as $b_1$ is square-free. Hence $k_2 \leq k_1 < 0$.

Now if $k_2 < k_1 < 0$ then again from equation (2.3) we get

$$b_1u_1^2l^{2(k_1-k_2)} - b_2u_2^2 = 4^m pl^{-2k_2},$$

which implies $l^2$ must divide $b_2$, a contradiction again. Hence if $k_1 < 0$, then we have $k_1 = k_2 = -k < 0$ for some integer $k$. For $k_2 < 0$, one similarly gets $k_1 = k_2 = -k < 0$.

From the equation (2.4), we have

$$b_1u_1^2 - b_1b_2u_3^2l^{2(k_3-k_1)} = -pl^{-2k_1}.$$
If \( k_1 < 0 \) and \( k_3 > k_1 \), then \( l^2 \) must divide \( b_1 \), a contradiction as before. Hence \( k_3 \leq k_1 < 0 \) if \( k_1 < 0 \). For \( k_3 < k_1 < 0 \), we can rewrite the above equation as

\[
(3.1) \quad b_1 u_1^2 l^{2(k_1-k_3)} - b_1 b_2 u_3^2 = -pl^{-2k_3},
\]

which implies \( l^2 \) must divide \( b_1 b_2 \), i.e., \( l = p \) or \( q \) as \( l \) is odd. If \( l = p \), then from equation (3.1) we arrive at the contradiction that \( p^3 \) divides \( b_1 b_2 \) whereas \( b_1 \) and \( b_2 \) are square-free. For \( l = q \), we subtract the equation (2.4) from the equation (2.3) and observe that

\[
b_1 b_2 u_3^2 - b_2 u_2^2 l^{2(k_2-k_3)} = pql^{-2k_3}.
\]

If \( k_2 > k_3 \), we get a contradiction that \( q^3 \) divides \( b_1 b_2 \). Therefore, \( k_2 \leq k_3 < 0 \) but then by the first part, \( k_1 = k_2 \leq k_3 \). Together, we obtain \( k_1 = k_2 = k_3 = -k < 0 \) for some integer \( k \) if \( k_1 < 0 \) or \( k_2 < 0 \).

\[\square\]

**Lemma 3.2.** Suppose the equations (2.3) and (2.4) have a solution \((z_1, z_2, z_3) \in \mathbb{Q}_2^3\). If \( b_1 b_2 \equiv 2 \pmod{4} \), then \( v_2(z_1) = v_2(z_2) = v_2(z_3) = -k < 0 \).

**Proof.** Let \( z_i = 2^{k_i} u_i \), where \( k_i \in \mathbb{Z} \) and \( u_i \in \mathbb{Z}_2^* \) for \( i = \{1, 2, 3\} \). Then \( v_2(z_i) = k_i \) for all \( i = \{1, 2, 3\} \).

When \( k_1 < 0 \), the argument in the first part of the proof of Lemma 3.1 also yields \( k_1 = k_2 = -k < 0 \) and \( k_3 \leq k_1 \). From equation (3.1), we can also conclude that \( k_1 = k_3 \) as \( l^2 \nmid b_1 b_2 \) for \( l = 2 \) in this case.

If \( k_1 > 0 \), then \( k_3 \geq 0 \) in equation (2.4) implies \( 2 \) divides \( p \), a contradiction. If \( k_3 < 0 < k_1 \), then equation (2.4) implies \( b_1 b_2 \equiv 0 \pmod{4} \), a contradiction again.

If \( b_1 \) is even, one can show that \( k_1 \neq 0 \) by similar argument. If \( b_2 \) is even and \( k_1 = 0 \), then \( 4 \) divides \( b_1 \) by equation (2.3), a contradiction if \( k_2 \geq 0 \). But \( k_2 < 0 \) contradicts the fact \( k_1 = 0 \) by equation (2.3). Hence the only possibility is \( k_1 = k_2 = k_3 = -k < 0 \) for some integer \( k \).

\[\square\]

4. Bounding the Size of the 2-Selmer Group

In this section, we bound the size of the 2-Selmer group of the Heronian elliptic curve given by (1.1). The 2-Selmer group \( \text{Sel}_2(E/\mathbb{Q}) \) consists of those pairs \((b_1, b_2)\) in \( \mathbb{Q}(S, 2) \times \mathbb{Q}(S, 2) \) for which the equation (2.3) and (2.4) have an \( l \)-adic solution at every place \( l \) of \( \mathbb{Q} \). We now limit the size of \( \text{Sel}_2(E/\mathbb{Q}) \) by ruling out local solutions for certain pairs \((b_1, b_2)\) by exploiting the results of the previous section.
Lemma 4.1. Let \((b_1, b_2) \in \mathbb{Q}(S, 2) \times \mathbb{Q}(S, 2)\). Then

(i) The corresponding homogeneous space will have no \(l\)-adic solution for the case \(l = \infty\) if \(b_1b_2 < 0\).

(ii) If \(b_1b_2 \equiv 2 \pmod{4}\), the corresponding homogeneous space will not have 2-adic solutions.

(iii) If \(b_1 \equiv 0 \pmod{q}\), then the corresponding homogeneous space will not have any \(q\)-adic solution.

Proof. (i) Let the homogeneous space corresponding to \((b_1, b_2) \in \mathbb{Q}(S, 2) \times \mathbb{Q}(S, 2)\) have real solutions. Then \(b_1 > 0\) and \(b_2 < 0\) implies \(-p > 0\) in equations (2.4), which is absurd. Similarly, \(b_1 < 0\) and \(b_2 > 0\) implies \(4^mp < 0\) in equation (2.3), which is absurd. Thus, the homogeneous space corresponding to \((b_1, b_2)\) have no \(l\)-adic solutions for \(l = \infty\) if \(b_1b_2 < 0\).

(ii) Let \(b_1b_2 \equiv 2 \pmod{4}\). Suppose \(b_1\) is even and \(b_2\) is odd. Then \(v_2(z_1) = v_2(z_2) = -k < 0\) for some integer \(k\) from lemma (3.2). This in turn implies

\[
b_1u_1^2 - b_2u_2^2 = 4^mp \cdot 2^{2k} \implies b_2 \equiv 0 \quad \text{(mod 2)},
\]

a contradiction. The case when \(b_1\) is odd follows similarly.

(iii) Let us assume \(b_1 \equiv 0 \pmod{q}\). Then one of \(v_q(z_1)\) or \(v_q(z_3)\) has to be negative in equation (2.4). If \(v_q(z_1) < 0\), then from lemma (3.1), we have \(v_q(z_1) = v_q(z_2) = v_q(z_3) = -k < 0\) for some integer \(k\). Subtracting equation (2.4) from the equation (2.3), we get

\[
b_1b_2u_3^2 - b_2u_3^2 = pq^{2k+1},
\]

where \(z_i = u_iq^i\) for \(u_i \in \mathbb{Z}_q^*\) and \(i \in \{1, 2, 3\}\). This implies that \(b_2 \equiv 0 \pmod{q}\). From equation (2.4), one can now deduce that

\[
b_1u_1^2 - b_1b_2u_3^2 = -pq^{2k} \implies b_1 \equiv 0 \quad \text{(mod } q^2)\),
\]

a contradiction. For the case \(v_q(z_3) < 0\), if additionally one of \(v_q(z_i) < 0\) for \(i \in \{1, 2\}\), we are back to the previous case due to lemma (3.1).

So we now suppose \(v_q(z_3) < 0\) and \(v_q(z_i) \geq 0\) for \(i \in \{1, 2\}\). Then from equation (2.4), one can immediately observe \(b_1b_2 \equiv 0 \pmod{q^2} \implies b_2 \equiv 0 \pmod{q}\) too. From equation (2.3), this in turn implies that \(4^mp \equiv 0 \pmod{q}\), a contradiction again. Hence the result follows. \(\square\)
With the help of the lemma (4.1) and noting that the image of the torsion points \((0, 0), (4^m, 0), (−p, 0)\) and \(O\) under the map \(b\) is

\[ A = \{ (−1, −p), (p, q), (−p, −pq), (1, 1) \}, \]

we can now solely focus on the seven pairs

\[(4.4) \quad (1, p), (1, q), (1, pq), (2, 2), (2, 2p), (2, 2q), (2, 2pq).\]

Every other pair \((b_1, b_2)\) will either belong to the same coset of one of those seven points in the torsion group \(Im(b)/A\) or the corresponding homogeneous space will not yield local solutions for at least one prime \(l ≤ 7\) by the lemma (4.1) and consequently will not have rational solutions either. The following result narrows down the possible pairs from seven to three.

**Lemma 4.2.** There are no \(p\)-adic solutions to the homogeneous spaces corresponding to \((1, p), (1, pq), (2, 2p)\) and \((2, 2pq)\).

**Proof.** First we prove the result for the case \((b_1, b_2) = (1, p)\). A very similar proof can also be carried out for the case \((b_1, b_2) = (1, pq)\).

If \(v_p(z_1) > 0\) then assuming \(z_1 = p\overline{z}_1\) one can get the following from equation (2.3).

\[(4.5) \quad p^2\overline{z}_1^2 - p\overline{z}_2^2 = 4^mp \implies -\overline{z}_2^2 \equiv 4^m \pmod{p}\]

which implies that \(\left( \frac{-1}{p} \right) = 1\), a contradiction as \(p \equiv 7 \pmod{8}\).

Now \(v_p(z_1) = 0\) implies \(v_p(z_2) < 0\) from equation (2.3), which in turn implies \(v_p(z_1) < 0\) from lemma (3.1), a contradiction.

If \(v_p(z_1) < 0\) then from lemma (3.1), \(v_p(z_1) = v_p(z_2) = −k < 0\) for some integer \(k\).

Assuming \(z_i = u_ip^{-k}\) for \(i \in \{1, 2\}\), equation (2.3) yields \(u_1^2 − pu_2^2 = 4^mp^{2k+1} \implies u_1 \equiv 0 \pmod{p}\), a contradiction.

We now deal with the pairs \((2, 2p)\), the argument being similar for \((2, 2pq)\). From the equations (2.3) one can see that if \(v_p(z_2) ≥ 0\) then \(v_p(z_1) > 0\). Now \(v_p(z_1) > 0\) implies \(\left( \frac{-2}{p} \right) = 1\), a contradiction as \(p \equiv 7 \pmod{8}\). If \(v_p(z_2) < 0\), then \(v_p(z_1) = v_p(z_2) = −k < 0\) for some integer \(k\). Assuming \(z_i = u_ip^k\) where \(u_i \in \mathbb{Z}_p^*\) for \(i \in \{1, 2, 3\}\), one can now observe from equation (2.3) that

\[(4.6) \quad 2u_1^2 − 2pu_2^2 = 4^mp^{2k+1} \implies u_1 \equiv 0 \pmod{p},\]

a contradiction again. Hence the result follows. \(\square\)
We can reduce the possibilities for \((b_1, b_2)\) further down from three to one if 2 is not a quadratic residue modulo \(q\), i.e., \(q = 5\).

**Lemma 4.3.** Suppose \(m = 1\), i.e., \(q = 5\). Then the homogeneous spaces corresponding to \((b_1, b_2) \in \{(2, 2), (2, 2q)\}\) will not have \(q\)-adic solution.

**Proof:** First consider \((b_1, b_2) = (2, 2)\). Subtracting equation (2.4) from equation (2.3) we get

\[
4z_3^2 - 2z_2^2 = 5p.
\]

This implies either \(z_2 \equiv z_3 \equiv 0 \pmod{5}\) or \(\left(\frac{2}{5}\right) = 1\), the latter being an immediate contradiction. If \(z_2 \equiv z_3 \equiv 0 \pmod{5}\), equation (2.4) implies \(2z_1^2 \equiv -p \pmod{5}\), which is a contradiction again as \(\left(\frac{-p}{5}\right) = 1\) but \(\left(\frac{2}{5}\right) = -1\). Hence the result follows for \((b_1, b_2) = (2, 2)\). For the case \((b_1, b_2) = (2, 2q)\) the result follows from equation (2.3)

\[
2z_1^2 - 10z_2^2 = 4p \implies 2z_1^2 \equiv 4p \pmod{5}.
\]

This in turn implies \(\left(\frac{2}{5}\right) = 1\), a contradiction. \(\square\)

**Lemma 4.4.** The equations (2.3) and (2.4) have a local solution in \(\mathbb{Q}_l\) for every prime \(l\) for \((b_1, b_2) = (1, q)\).

**Proof.** First we consider \(l \geq 5\). Suppose \(C\) is the homogeneous space given by the equations (2.3) and (2.4) corresponding to the pair \((1, q)\). Then \(C\) is a twist of \(E\), and in particular, it has genus 1. By the Hasse-Weil bound, we have

\[
\#C(\mathbb{F}_l) \geq 1 + l - 2\sqrt{l} \geq 2 \quad \text{for } l \geq 5.
\]

We can choose a solution \((z_1, z_2, z_3) \in \mathbb{F}_l \times \mathbb{F}_l \times \mathbb{F}_l\) such that not all three of them are zero modulo \(l\). Now \(z_1 \equiv z_2 \equiv 0 \pmod{l}\) implies \(l^2\) divides \(4^mp\), a contradiction. Similarly, \(z_1 \equiv z_3 \equiv 0 \pmod{l}\) implies \(-p \equiv 0 \pmod{l^2}\), contradiction again. Hence for \(l \geq 5\), there exists solution to the simultaneous equations (2.3) and (2.4) in \(\mathbb{F}_l\) that can be lifted to \(\mathbb{Q}_l\) via Hensel’s lemma.

For \(l = 3\), first let us observe that \(q \equiv 2 \pmod{3}\) always. If \(p \equiv 1 \pmod{3}\), choose \(z_2 = 0\) and \(z_3 = 1\). Then \(z_1^2 = 4^mp \equiv 1 \pmod{3}\) from first equation and \(z_1^2 = q - p \equiv 1 \pmod{3}\) from second equation. Hence \(z_1 \not\equiv 0 \pmod{3}\) is a solution that can be lifted by Hensel’s lemma. If \(p \equiv 2 \pmod{3}\), choose \(z_2 = 1\), \(z_3 = 0\). Then \(z_1^2 = q + 4^mp \equiv 1\)
(mod 3) from first equation and \( z_1^2 = -p \equiv 1 \pmod{3} \) from second equation. Hence \( z_1 \not\equiv 0 \pmod{3} \) is a solution that can be lifted by Hensel’s lemma.

Finally for the case \( l = 2 \), choose \( z_2 = 1 \) and \( z_3 = 0 \). For \( m = 1 \), this turns equation (2.3) and equation (2.4) into the following;

\[
\begin{align*}
(4.9) \quad z_1^2 - 5z_2^2 &= 4p \equiv 28 \equiv 4 \pmod{8}, \\
(4.10) \quad z_1^2 - 5z_3^2 &= -p \equiv 1 \pmod{8}.
\end{align*}
\]

In both the cases we now have \( z_1^2 \equiv 1 \pmod{8} \) which by Hensel’s lemma can be lifted to \( \mathbb{Q}_2 \). Similarly for \( m \geq 2 \), one can immediately observe that \( z_1^2 \equiv 1 \pmod{8} \) again, and hence can be lifted similarly to \( \mathbb{Q}_2 \) via Hensel’s lemma. Hence proved. \( \square \)

By Lemmas 4.1, 4.2 and 4.4 we can conclude that the the 2-Selmer rank of \( E \) lies between 1 and 3 as stated in Theorem 1.1. For \( q = 5 \), it follows from Lemma 1.3 that the 2-Selmer rank is exactly 1, concluding the proof of Theorem 1.1.

5. THE MORDELL-WEIL RANK AND \( \text{III}(E/\mathbb{Q})[2] \)

We have seen that the 2-Selmer group has rank 1 in the previous section when \( q = 5 \). By the exact sequence (2.5), it follows that either \( E(\mathbb{Q}) \) has rank 0 or \( \text{III}(E/\mathbb{Q})[2] = 0 \). If we assume the finiteness of \( \text{III}(E/\mathbb{Q}) \) as predicted by Shafarevich, then \( \text{III}(E/\mathbb{Q}) \) must have square order by Cassels-Tate pairing. Therefore, \( \text{III}(E/\mathbb{Q})[2] \) has to be 0 i.e. the Mordell-Weil rank of \( E \) is 1 as stated in Corollary 1.2. This also proves the existence of infinitely many Heron triangles with the previously mentioned properties.

We include a list of Heronian elliptic curves satisfying the properties mentioned in the Theorem 1.1 with the corresponding rank, 2-Selmer rank and Shafarevich-Tate group in the below table. The computations have been done in Magma and SageMath software. There is a disparity between the definition of the 2-Selmer rank defined in this work and that in Magma and SageMath. While we define \( \# \text{Sel}_2(E/\mathbb{Q}) = 2^{2+s(E)} \), and refer to \( s(E) \) as the 2-Selmer rank in the following table, \( 2 + s(E) \) will denote the 2-Selmer rank in Magma or SageMath.
| $p$ | $q$ | $r(E)$ | $s(E)$ | $\text{III}(E/\mathbb{Q})[2]$ | $p$ | $q$ | $r(E)$ | $s(E)$ | $\text{III}(E/\mathbb{Q})[2]$ |
|---|---|---|---|---|---|---|---|---|---|
| 31 | 5 | 1 | 1 | trivial | 47 | 17 | 0 | 2 | no information |
| 71 | 5 | 1 | 1 | trivial | 127 | 17 | 2 | 2 | no information |
| 151 | 5 | 1 | 1 | trivial | 191 | 17 | 0 | 2 | no information |

**Acknowledgement:** The first author would like to acknowledge DST-SERB for providing the grant through the Start-Up Research Grant (SRG/2020/001937) as well as BITS-Pilani, Hyderabad Campus for providing amenities. The second author would like to acknowledge the fellowship (File No:09/1026(0029)/2019-EMR-I) and amenities provided by the Council of Scientific and Industrial Research, India (CSIR) and BITS-Pilani, Hyderabad. The third author would like to thank MATRICS, SERB for their research grant MTR/2020/000467.

**References**

[1] B.J.Birch, H.P.F. Swinnerton-Dyer. "Notes on elliptic curves. II." Journal für die reine und angewandte Mathematik, 218 (1965), 79-108.

[2] Heath-Brown D.R. "The size of Selmer groups for the congruent number problem." Inventiones Mathematicae 111.1 (1993): 171-195.

[3] Heath-Brown, D. R."The size of Selmer groups for the congruent number problem, II." Inventiones Mathematicae 118 (1994): 331-370.

[4] Buchholz, Ralph H., and Randall L. Rathbun. "An infinite set of Heron triangles with two rational medians." The American Mathematical Monthly 104.2 (1997): 107-115.

[5] Buchholz, Ralph H., and Robert P. Stingley. "Heron triangles with three rational medians." The Rocky Mountain Journal of Mathematics 49.2 (2019): 405-417.

[6] Chahal, Jasbir S. "Congruent numbers and elliptic curves." The American Mathematical Monthly 113.4 (2006): 308-317.

[7] Coates, John H. "Congruent number problem." Pure and Applied Mathematics Quarterly 1.1 (2005): 14-27.

[8] Connell, Ian. "Calculating root numbers of elliptic curves over $\mathbb{Q}$." Manuscripta Mathematica 82.1 (1994): 93-104.

[9] Conrad, Keith. "The congruent number problem." The Harvard College Mathematics Review 2.2 (2008): 58-74.

[10] Dujella, Andrej, and Juan Carlos Peral. "Elliptic curves coming from Heron triangles." The Rocky Mountain Journal of Mathematics 44.4 (2014): 1145-1160.

[11] Ghale, Vinodkumar, Shamik Das, and Debopam Chakraborty. "On the Diophantine equation $(x^2 + y^2)^2 + (2pxy)^2 = z^2."$ arXiv e-prints (2021): arXiv-2105.
[12] Goins, Edray Herber, and Davin Maddox. "Heron triangles via elliptic curves." The Rocky Mountain Journal of Mathematics (2006): 1511-1526.

[13] Halbeisen, Lorenz, and Norbert Hungerbühler. "Heron triangles and their elliptic curves." Journal of Number Theory 213 (2020): 232-253.

[14] Johnstone, Jennifer A., and Blair K. Spearman. "Congruent number elliptic curves with rank at least three." Canadian Mathematical Bulletin 53.4 (2010): 661-666.

[15] Kramer, A. V., and F. Luca. "Some remarks on Heron triangles." Acta Acad. Paed. Agriensis, Sectio Mathematicae 27 (2000) 25-38.

[16] Rhoades, Robert C. "2-Selmer groups and the Birch–Swinnerton-Dyer Conjecture for the congruent number curves." Journal of Number Theory 129.6 (2009): 1379-1391.

[17] Rusin, David J. "Rational triangles with equal area." New York J. Math 4.1 (1998): 15..

[18] Sierpinski, Waclaw. Pythagorean triangles. Vol. 9. Courier Corporation, 2003.

[19] Silverman, Joseph H. The arithmetic of elliptic curves. Vol. 106. New York: Springer, 2009.

[20] Yan, Xiao-Hui. "The Diophantine equation \((m^2 + n^2)^x + (2mn)^y = (m + n)^2z\)." International Journal of Number Theory 16.08 (2020): 1701-1708.

Department of Mathematics, BITS-Pilani, Hyderabad campus, Hyderabad, INDIA

Email address: debopam@hyderabad.bits-pilani.ac.in

Department of Mathematics, BITS-Pilani, Hyderabad campus, Hyderabad, INDIA

Email address: p20180465@hyderabad.bits-pilani.ac.in

Department of Mathematics and Computation, IIT Guwahati, Guwahati, INDIA

Email address: a.saikia@iitg.ac.in