Arithmetic of Heronian Elliptic Curves

Thesis

Submitted in partial fulfillment
of the requirements for the degree of
DOCTOR OF PHILOSOPHY

by

Ghale Vinodkumar Rajlingappa
ID No. 2018PHXF0465H

Under the Supervision of

Dr. Debopam Chakraborty

BIRLA INSTITUTE OF TECHNOLOGY AND SCIENCE, PILANI
2024

BIRLA INSTITUTE OF TECHNOLOGY AND SCIENCE, PILANI

CERTIFICATE

This is to certify that the thesis entitled "*Arithmetic of Heronian Elliptic Curves*", submitted by **Ghale Vinodkumar Rajlingappa**, ID No. 2018PHXF0465H, in partial fulfillment of the requirements for the degree of DOCTOR OF PHILOSOPHY embodies original work done by him under my supervision.

Debopam Chakraborty

Supervisor
Dr. Debopam Chakraborty
Assistant Professor,
BITS-Pilani, Hyderabad Campus
Date: 20/03/2024

Declaration of Authorship

I, **Ghale Vinodkumar Rajlingappa**, declare that this thesis titled, ‘Arithmetic of Heronian Elliptic Curves’ and the work presented in it are my own. I confirm that:

- This work was done wholly or mainly while in candidature for a research degree at this University.
- No portion of this work referred to in this thesis has been submitted in support of an application for another degree or qualification of this or any other university or other institution of learning.
- Where I have consulted the published work of others, this is always clearly attributed.
- Where I have quoted from the work of others, the source is always given. With the exception of such quotations, this thesis is entirely my own work.

Signed:

Date: 20/03/2024

To

my parents

and

my high school teachers

Acknowledgements

“Plant it — perhaps it will grow. I make no promises.
Perhaps it will grow. Perhaps it will not.”
Miss Moon thanked the old man. “Thank you for my tree.”
“It’s not a tree yet; its only a flower,
and a paper one at that,” he replied as he waved goodbye.

From the book “The Paper-Flower Tree" by Jacqueline Ayer.

Thank you Aai and Pappa for your continuous love, support and belief in me in a village without high school to date! and being courageous enough to face financial difficulties and not let us know in our school days. Thank you Vilas for your love and understanding and for sharing my responsibilities towards our parents. Thank you Dr. Debopam Chakraborty, for being there with me through this journey, for your involvement, for listening to all my nonsense most of the time and for all your suggestions, questions, comments and encouragement. He did not hesitate to show his availability for my unusual meetings and my text messages. I am thankful to him for reading the thesis carefully and for his suggestions. I also express my gratitude to Prof. Anupam Saikia for his advice, suggestions and constant support during the entire tenure of my research work. I thank him for reading the thesis and providing comments and suggestions. I thank Prof. Loïc Merel for reading the thesis and discussions.

I would also like to thank my Doctoral Advisory Committee members, Dr. Pratyusha Chattopadhyay and Dr. Sharan Gopal, for their questions, comments and constant feedback during this research work.

I thank the Head of the Department, Prof. Pradyumn Kumar Sahoo and previous HoD, Prof. Dipak Satpathi; DRC convener, Dr. Sharan Gopal and previous DRC convener, Dr. Jaganmohan Jonnalagadda of the Department of Mathematics, BITS-Pilani, Hyderabad Campus, for their support and encouragement in carrying out my research work. Thanks to my collaborators Prof. Anupam Saikia, Dr. Shamik Das and Mr. Imdadul Islam. Without their efforts, this thesis would not have been in this form. Thanks to all the reviewers and editors of our articles. I acknowledge the financial support from the Council of Scientific and Industrial Research (CSIR), India (File No:09/1026(0029)/2019-EMR-I), during my entire research work. Thanks to Lorenz Halbeisen for replying my emails. I thank Jan Vonk for helpful discussions at ICTS, India. I thank BITS-Pilani, Hyderabad Campus, for providing the necessary facilities. I thank all the faculty members of the Department of Mathematics. The friendly nature of Dr. Murali Reddy made my Ph.D.

days playful. The cordial way of working with Dr. Sharan Gopal, Dr. Nijjwal Karak, Dr. Sumit Vishwakarma, Dr. Manish Kumar and Dr. Deepika made the academic work easy. Friends made my days cheerful and they are encouraging. I mention Onkar, Navnath, Mayureh, Datta, Saurabh, Rekha, Rama, Chinmayee, Vidisha, Soumya from my B.Sc. days. Onkar and Navnath have been great support from then till now. Pabitra, Faiz, Namrata A. from my M.Sc. days. Faiz, Karthik, Panduranga, Revathi, Kshama, Aleena, Amar, Gopal, Tapaswini, Simran and Sanjay were all very cooperative and helpful. Pankaj, Sunita and Amar were very supportive. Discussion in the initial days with the number theory group Dr. Debopam, Pankaj, Imdadul and Prof. Saikia, Shamik, Laxmi from IIT-G was helpful. They are all friendly and supportive. I thank Jaitra Chattopadhyay for sharing general mathematical information. Thank you Onkar, Amrita, Navnath, Pabitra, Pankaj, Sunita and Laxmi who are a call away to listen to my fuss. The algebra study group at BITS-Hyderabad involving Pankaj, Amrutha, Amritanshu, Anshid, Sunil, Rabin, Dr. Pratyusha Chattopadhyay, Dr. Sushil Bhunia brought a healthy atmosphere to the department and helped me to stay connected and motivated. I thank all the cricket and chess club members at BITS-Hyderabad. I thank all the staff of the Mathematics office and AGSRD office at BITS-Hyderabad.

The support from Vidyarthi Sahayak Samiti (Students Welfare Association), Pune, has played a crucial role during my Bachelor's degree. Its teaching brought me a sense of discipline and responsibility. Teachers from Fergusson College, Dr. V.V. Acharya, Dr. Manish Aaglave and Phatangare sir always motivated me and were very helpful. Professors at the University of Hyderabad, Prof. V. Kannan, R. Tondon and Prof. Kumaresan, influenced me to learn more mathematics and made me experience mathematics differently. Prof. Illangvon and Dr. Mohan Chintamani were very supportive and encouraging during my M.Sc. days. I fondly remember my days at IISER Pune as a teaching assistant. The comments and suggestions from Prof. Steven Spallon, Prof. Chandrasheel Bhagwat, Prof. Amit Hogadi and Dr. Rohit Holkar helped me to do better at teaching.

In the end, I would like to thank my grandparents- Amma, Tata, Mamas(uncles) and Mavshis(aunts), who greatly helped me in my primary education. My grandfather used to give me a lot of puzzles, and he used to play logical games with me that engaged my childhood days. I am thankful to my high school teachers, Dr. Sanjay Debadwar, the late V. D. Kendre, P.L. Kavere, Pravin Bhole, Hareshwar Swami, Narsing Pawar, Sanjeev Patil, Ainille Madam, Kumthekar Madam, B.S. Mane (sports teacher) and all the teachers at Shyamlal Memorial Highschool, Udgir whose love and encouragement helped me a lot in pursuing higher education.

Abstract

The arithmetic of elliptic curves has played a crucial role in understanding various classical questions in number theory and arithmetic geometry. In the last few decades, breakthroughs have been made towards solving the congruent number problem using the arithmetic of elliptic curves. The congruent number problem relates to giving a complete description of positive integers that can occur as the areas of rational right triangles. A complete answer to the congruent number problem is still unknown. It is well known in the literature that the existence of congruent numbers is equivalent to the existence of rational points of infinite order on a certain class of elliptic curves known as the congruent number elliptic curves. The works of Goins and Maddox generalized the congruent number problem for rational triangles, known as Heron triangles, through the positivity of rank of a certain class of elliptic curves, known as Heronian elliptic curves.

As of yet, there is no effective way to compute the rank of an elliptic curve. However, for a positive integer m, the study of m-Selmer groups helps to understand the structure of rational points on elliptic curves and, hence, the rank. Selmer groups are finite and effectively computable and act as an upper bound for the rank of an elliptic curve.

Heath-Brown studied the structure of 2-Selmer groups for congruent number elliptic curves, which was fundamental to the understanding of the rank of that class of elliptic curves. Unlike the congruent number elliptic curves, there is comparatively little in the literature regarding the study of 2-Selmer groups of Heronian elliptic curves associated with Heron triangles.

The main focus of the thesis is to analyze the structure of 2-Selmer groups for different classes of Heronian elliptic curves using the method of 2-descent on elliptic curves. This, in turn, provides a better estimate of the ranks of those curves, which is crucial for understanding the numbers occurring as the area of Heron triangles with certain angles. As a consequence of computing 2-Selmer groups, we also delve into the 2-part of the Shafarevich-Tate groups for some of these classes of Heronian elliptic curves through the class number divisibility criteria of certain number fields and solutions to certain Diophantine equations. We provide numerical evidence for each of the studied classes of Heronian elliptic curves at the end of each section.

List of Tables

Contents

List of Notations

E	:	Elliptic curve
$\mathbb{N}$	:	Set of natural numbers
$\mathbb{Z}$	:	Set of integer numbers
$\mathbb{Q}$	:	Set of rational numbers
$\mathbb{Q}^*$	:	Set of nonzero rational numbers
K	:	A number field
$\mathbb{C}$	:	Set of complex numbers
$E/\mathbb{Q}$	:	Elliptic curve over rational numbers
E/K	:	Elliptic curve over number field K
$E(\mathbb{Q})$	:	Mordell-Weil group of E over $\mathbb{Q}$
$E(K)$	:	Mordell-Weil group of E over K
$\lvert A\rvert, \#A$	:	The order of the set A
$\in$	:	belongs to
$\notin$	:	does not belong to
$A \subseteq B$	:	A is subset of B
$A \times B$	:	The cartesian or direct product of A, and B
$\langle a \rangle$	:	The group generated by the element a
$\langle A \rangle$	:	The group generated by the set A
$a \mid b$	:	a divides b
$a \nmid b$	:	a does not divide b
$\sum\limits_{i=1}^{n}$	:	Summation from 1 to n
$a \equiv b \pmod{c}$	:	a is congruent to b modulo c
$a \not\equiv b \pmod{c}$	:	a is not congruent to b modulo c
$A \cong B$	:	A is isomorphic to B
$\left(\frac{a}{p}\right)$	:	The Legendre symbol of a modulo p
G/H	:	Quotient of group G by H
$G \times H$	:	Direct product of G and H
$\longrightarrow$	:	Maps to
$\mathcal{O}_K$	:	Ring of integers of K.
O	:	Point at infinity on E
Δ	:	Discriminant of E
$\mathbb{F}_p$	:	Finite field with p elements
$\mathbb{F}_p^*$	:	Set of units in $\mathbb{F}_p$

v	: discrete valuation on the field K
$\bar{K}$	: an algebraic closure of K
$E(\mathbb{Q})_{tors}$	: Torsion group of $E(\mathbb{Q})$
$E(K)_{tors}$	: Torsion group of $E(K)$
$[m]$	: Multiplication by m map on elliptic curve
$E[m]$	: $m-$ torsion subgroup of the elliptic curve
$G_{\bar{K}/K}$	: The Galois group of $\bar{K}/K$
M_K	: a complete set of equivalent set of absolute values on K
M_K^∞	: The archimedean absolute values in K
M_K^0	: The non archimedean absolute values in K
K_v	: The completion of K at v
$\mathrm{Hom}(E_1,\ E_2)$	: group of isogenies from E_1 to E_2
M^G	: The submodule of M fixed by G
$H^0(G, M)$	: The 0^{th} Cohomology of G-module M
$H^1(G, M)$	: The 1^{st} cohomology of the G-Module M
$\mathrm{Sel}_2(E/K)$	: The 2-Selmer group of E/K
$Ш(E/K)[2]$	: 2-Part of the Shafarevich-Tate group of E/K

Chapter 1

Introduction

A positive integer n is called a *congruent number* if it is the area of a right triangle, with all of its sides' lengths being rational numbers. Given a positive integer n, the celebrated *congruent number problem* asks when n is a congruent number. A *Heron triangle* is a triangle with rational sides and rational area. The problem of determining when a positive integer n appears as the area of a Heron triangle is a direct generalization of the congruent number problem. The main aim of this thesis is to look into the rank computation of a special class of elliptic curves, known as the *Heronian elliptic curves*, associated with Heron triangles. This is essential in identifying a positive integer n as the area of a Heron triangle with a given angle.
The quest for understanding congruent numbers has inspired mathematicians for more than a thousand years (see [6], [28]). Works of Fibonacci, Fermat, and Euler made a significant contribution in describing these numbers (see [4], [11]). Fibonacci showed that 5 and 7 are congruent numbers and claimed 1 is not a congruent number. Fermat's idea (see [6]) of infinite descent proved that 1 is not a congruent number, and hence, the possibility of a congruent number being a perfect square was discarded.
The congruent number problem eventually boils down to whether the rank of a special type of elliptic curve, known as the *congruent number elliptic curve*, is positive, in the following way (see [28], Chapter 1, Proposition 18):

Result 1.0.1. A positive integer n is a congruent number if and only if the rank of the elliptic curve over $\mathbb{Q}$

$$E_n : y^2 = x^3 - n^2x = x(x-n)(x+n) \tag{1.0.1}$$

is at least one. In (1.0.1), E_n denotes the congruent number elliptic curve.

The rank of an elliptic curve, also known as the Mordell-Weil rank, is discussed in detail in the next chapter. It denotes the size of the group of all rational points of the elliptic curve. There is no effective algorithm for finding the rank of elliptic curves yet. Using the equivalent criterion of the congruent number problem involving the congruent number elliptic curve, Heegner proved in [22] that $n = 2p$ are congruent numbers for every n with $p \equiv 3 \pmod 8$. He proved that the congruent number elliptic curves are isogenous to modular curves $X_0(32)$ and then used the theory of complex multiplication to construct a non-torsion point in $\mathbb{Q}(\sqrt{-2p})$. Monsky extended Heegner's method in [38] and showed that primes $p \equiv 5, 7 \pmod 8$ are congruent numbers. The Birch and Swinnerton-Dyer conjecture (see [28]) predicts that a positive integer n is a congruent number if $n \equiv 5, 6$ or $7 \pmod 8$. This is because the sign of the functional equation depends on the equivalence class of $n \pmod 8$ and under these conditions, the $L-$function of E_n must vanish at $s = 1$ (see [28], Chapter 2, Proposition 12). In a recent work, Tian generalized this to a class of highly composite numbers (see [51]) and proved that for any given integer $k \geq 0$, there are infinitely many square-free congruent numbers with exactly $k+1$ odd prime divisors in each residue class of 5, 6 and $7 \pmod 8$. Jaap Top and Noriko Yui did a detailed survey on the congruent number problem and its variants in [52]. One of the most important results regarding the congruent number problem is due to J. Tunnell [53] in 1983. It relates the congruent number problem to the Diophantine equations.

Result 1.0.2. [Tunnell, 1983]: Let n be a square free congruent number. Define A_n, B_n, C_n, D_n as follows:

$$\begin{aligned}
A_n &= \#\{(x,y,z) \in \mathbb{Z}^3 \mid n = 2x^2 + y^2 + 32z^2\}, \\
B_n &= \#\{(x,y,z) \in \mathbb{Z}^3 \mid n = 2x^2 + y^2 + 8z^2\}, \\
C_n &= \#\{(x,y,z) \in \mathbb{Z}^3 \mid n = 8x^2 + 2y^2 + 64z^2\}, \\
D_n &= \#\{(x,y,z) \in \mathbb{Z}^3 \mid n = 8x^2 + 2y^2 + 16z^2\}.
\end{aligned}$$

Then:

$$\begin{aligned}
A_n =& B_n/2 \text{ if } n \text{ is odd; and} \\
C_n =& D_n/2 \text{ if } n \text{ is even.}
\end{aligned}$$

If the Birch-Swinnerton Dyer conjecture is true, the converse of Tunnell's aforementioned result is also true. But the Birch-Swinnerton Dyer conjecture is still an open problem; hence, the complete description of congruent numbers is still unknown.

Like the congruent number problem, many open problems involving elliptic curves are dependent on finding the rank of the elliptic curves. As mentioned earlier, there is no known effective algorithm for rank computation. Initially, Neron had conjectured that the rank of the set of rational points on an elliptic curve is bounded (see [43]). Finding elliptic curves with high ranks is an area of immense interest in number theory. Elliptic curves with rank of four were found in 1945, with rank of seven in 1975, twelve in 1982, and twenty-eight in 2006. Andrej Dujella maintains a database for elliptic curves with high ranks in https://web.math.pmf.unizg.hr/ duje/tors/rankhist.html. At present, the largest known rank of an elliptic curve is twenty-eight, found by Noam Elkies. Another source for data about elliptic curves is due to J. Cremona (https://wstein.org/Tables/cremona/INDEX.html). Due to the difficulties in finding ranks of elliptic curves over rational numbers, mathematicians began looking into the rational numbers "locally," i.e., by their degree of p-divisibility, effectively clubbing together numbers with the same remainder modulo p^n. This technique had the benefit of the operation structure being finite. Working out this analysis for every prime p and then collectively putting it together as a global solution for $\mathbb{Q}$, one can embed $E(\mathbb{Q})/mE(\mathbb{Q})$ into a group known as *m-Selmer group.* $E(\mathbb{Q})/mE(\mathbb{Q})$ contains information about the Mordell-Weil group $E(\mathbb{Q})$ of an elliptic curve E. Hence, the m-Selmer group gives an upper bound for the size of the Mordell-Weil group. Noting that $E(\mathbb{Q})$ denotes the Mordell-Weil group of E over $\mathbb{Q}$, and $r(E/\mathbb{Q})$ the corresponding Mordell-Weil rank, a full p-descent method (see [46], Proposition X.4) generates an exact sequence

$$0 \to E(\mathbb{Q})/pE(\mathbb{Q}) \to \mathrm{Sel}_p(E/\mathbb{Q}) \to Ш(E/\mathbb{Q})[p] \to 0.$$

Here, $\mathrm{Sel}_p(E/\mathbb{Q})$ denotes the p-Selmer group and $Ш(E/\mathbb{Q})$ denotes the Shafarevich-Tate group. The importance of the Selmer and the Shafarevich-Tate group in the rank computation follows from the aforementioned p-descent exact sequence, as $r(E/\mathbb{Q}) = s_p(E/\mathbb{Q}) - \dim_{\mathbb{F}_p} Ш(E/\mathbb{Q})[p]$ where $s_p(E/\mathbb{Q}) = \dim_{\mathbb{F}_p}\mathrm{Sel}_p(E/\mathbb{Q}) - \dim_{\mathbb{F}_p} E(\mathbb{Q})[p]$ denotes the p-Selmer rank of E.

Due to Cassels-Tate pairing (see [5]), the finiteness of the p-primary part of $Ш(E/\mathbb{Q})[p^\infty]$ would imply that $Ш(E/\mathbb{Q})[p]$ has even $\mathbb{F}_p$ dimension, hence $s_p(E/\mathbb{Q})$ and $r(E/\mathbb{Q})$ have the same parity. The finiteness of $Ш(E/\mathbb{Q})[p^\infty]$ implies the *p-Selmer rank one conjecture* which states that $r(E/\mathbb{Q}) = 1$ whenever $s_p(E/\mathbb{Q}) = 1$. This conjecture has been verified for $p \geq 5$ under certain assumptions (see [56], [54], [47]).

Very little is known about the p-Selmer rank one conjecture for $p = 2$ even though the computation of a full 2-descent is easiest in practice and provides as yet the best tool to compute $r(E/\mathbb{Q})$. There has been a growing interest in the 2-Selmer group computation for different families of elliptic curves, as evidenced by the works of Klagsbrun-Mazur-Rubin in [26], [27], and the work of Mazur-Rubin in [35].

The method of descent is used in theory and in practice to find the rank of elliptic curves. However, the method is not always successful. There are examples due to Shafarevich-Tate and Ulmer for elliptic curves over function fields $\mathbb{F}_p(t)$ with arbitrarily large ranks. Recently in ([43]), Park, Poonen, Voight, and Wood gave a heuristic model for elliptic curve ranks that indicates that ranks are bounded. Moreover, it says there are finitely many elliptic curves over $\mathbb{Q}$ having rank ≥ 22. The current record of known rank for a class of infinitely many elliptic curves is nineteen, constructed by Noam Elkies.

We shall define the Selmer group in the next chapter explicitly. The Selmer groups of an arbitrarily large order are known. In a series of works by Heath-Brown in [19], [20], congruent number elliptic curves with large 2-Selmer groups were discussed in detail.

A generalization to the congruent number problem questions for a given positive rational number n, whether a rational triangle $[a, b, c]$ exists with area n with some given angle

θ. One can immediately see that the congruent number problem is a special case with $\theta = \pi/2$. Heron of Alexandria was the first who related the number n occurring as the area of a rational triangle and the sides of a rational triangle by the formula $n = \sqrt{s(s-a)(s-b)(s-c)}$ where s represents semiperimeter, i.e., $s = \dfrac{a+b+c}{2}$, in the first century. In his honor, rational triangles are known as Heron triangles. In [17], the work of Goins and Maddox gave a correspondence analogous to the correspondence between congruent numbers and congruent number elliptic curves. Their correspondence was between the numbers occurring as the area of Heron triangles and the rational points on specific elliptic curves associated with such numbers. Their main result was as follows.

Result 1.0.3. [Goins and Maddox, 2006]: A positive integer n can be expressed as the area of a triangle with rational sides if and only if for some nonzero rational number τ the elliptic curve

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

has a rational point that is not of order 2, where $\tau = \tan\dfrac{\theta}{2}$. Such elliptic curves $E_{\tau,n}$ are called *Heronian elliptic curves.* Moreover, n is a congruent number if and only if we can choose $\tau = 1$.

Given any integer n, the existence of infinitely many Heron triangles with the area n was studied in [17], [44]. Buchholz and Rathbun proved in [1] the existence of infinitely many Heron triangles with two rational medians. Later in [2], Buchholz and Stingley studied eight elliptic curves associated with Heron triangles with two rational medians and showed that none of them can have three rational medians. A Heron triangle with three rational medians is called a perfect triangle and it is a longstanding conjecture that such triangles do not exist. Peng and Zhang [40],[41] showed the existence of infinitely many classes of isosceles Heron triangles whose sides are triangular numbers and infinitely many isosceles Heron triangles whose sides are polygonal numbers. In a recent work, Das, Juyal, and Moody [9] showed the existence of infinitely many Heron triangles and integer rhombuses with common area and perimeter using the arithmetic of elliptic curves. In [12], Dujella and Peral showed the existence of elliptic curves of ranks three, four, and five associated with Heron triangles and found examples of elliptic curves over $\mathbb{Q}$ with ranks nine and ten. Recently, Matilde and Oliver [33] extended the idea of Heron triangles from the Euclidean plane to the hyperbolic plane. They showed a one-one correspondence between Heron triangles with area n and rational points on the corresponding curve. In [18], Halbeisen and Hungerbühler showed the existence of elliptic curves of rank at least two associated with Heron triangles. They modified a few results of Goins and Maddox and related the existence of a Heron triangle to an integral solution of certain Diophantine equations.

We enlist the different objectives of this thesis below which mainly involve the computation of the explicit group structure of the 2-Selmer group for Heronian elliptic curves associated with different types of Heron triangles.

1. Mordell-Weil rank computation of the Heronian elliptic curves associated with Heron triangles with specific angles and odd area n of the form $n^2 + 1 = 2q$ for a prime number q. Such numbers famously appear in Landau's problems (see [42]). A complete group structure of the 2-Selmer group of those elliptic curves.

2. Mordell-Weil rank computation of the Heronian elliptic curves associated with Heron triangles with specific angles and even area. A complete group structure of the 2-Selmer group of those elliptic curves.

3. Correspondence between the existence of Heron triangles and the solvability of Diophantine equations associated with those Heron triangles.

4. Correspondence between the order of the 2-part of the Shafarevich-Tate group of a certain class of Heronian elliptic curves and the solvability of certain Diophantine equations.

The organization of the thesis is done in the following manner.

Chapter 2 includes the necessary background of the arithmetic of elliptic curves, most notably, the structure of the Selmer and the Shafarevich-Tate groups, along with a brief description of known results on Heronian elliptic curves.

In Chapter 3, we look into the arithmetic of the Heronian elliptic curves associated with the Heron triangles of odd area. We first consider the case when n is a prime p such that $p \equiv 3, 5, 7 \pmod{8}$. The latter part of this chapter includes a generalization of the previous result in terms of arbitrary square-free odd integers n, with an explicit computation of the 2-Selmer group using the complete 2-descent method. This chapter's work has been published/accepted in [16], [8].

Chapter 4 describes the arithmetic of Heronian elliptic curves representing the Heron triangles with even area. The beginning of the chapter deals with the 2-Selmer group structure of a special type of Heron triangle with area 2^m. Later in the chapter, we generalize the result for arbitrary even integers. The initial part of this chapter has been published in [7]. The later part of the work mentioned in this chapter is communicated and currently under review and the last part is accepted in [8].

Chapter 5 deals with a one-one correspondence between the solvability of certain Diophantine equations and the existence of Heron triangles using the Mordell-Weil rank. We then highlight the 2-Selmer group structure of Heronian elliptic curves of prime area $p \equiv 1 \pmod 8$ which were left out in Chapter 3. This was due to the possible existence of a non-trivial Shafarevich-Tate group which depends on the solvability of a certain class of Diophantine equations. A part of this chapter's work has been published in [16].

Chapter 6 states a few results connecting the work in this thesis and several works available in the literature. It mentions the limitations of the work clearly and then describes the future scope of further work related to the results presented in this thesis.

Chapter 2

Background

This chapter introduces the necessary preliminaries of the topics covered in the thesis. It primarily gives a short background detail on the elliptic curve over number fields, the primary focus of the thesis. We first recall some notions and results about the classification of finite abelian groups (see [14] as a reference). We start with the definition of a p-group.

Definition 2.1. Let p be a prime. A group G is called p-group if every element of G is of order p^k for some $k \geq 0$.

Theorem 2.2. *A finite group is a p-group if and only if its order is a power of p.*

Definition 2.3. A group G is finitely generated if there is a finite subset $A \subseteq G$ such that $G = \langle A \rangle$ i.e., every $g \in G$, can be written as $g = \sum_{i=1}^{r} k_i g_i$ where $g_i \in A, k_i \in \mathbb{Z}$.

Definition 2.4. For each $0 \leq r \in \mathbb{Z}$, let $\mathbb{Z}^r = \mathbb{Z} \times \ldots \times \mathbb{Z}$ be the direct product of r copies of $\mathbb{Z}$, where we take $\mathbb{Z}^0 = 1$. The group $\mathbb{Z}^r$ is a free abelian group of rank r.
We can now state the following theorem regarding the group structure of finitely generated groups.

Theorem 2.5 (Fundamental theorem of Finitely generated abelian groups)**.** *Every finitely generated abelian group G is isomorphic to a direct product of cyclic groups in the form*

$$\mathbb{Z}^r \times \mathbb{Z}_{p_1^{r_1}} \times \mathbb{Z}_{p_2^{r_2}} \times \ldots \times \mathbb{Z}_{p_k^{r_k}}$$

where the p_i are primes, not necessarily distinct, and the r_i are positive integers. The direct product is unique except for the possible rearrangement of the factors; that is, the number of factors $\mathbb{Z}$ is unique and the prime powers $p_i^{r_i}$ are unique.

A sequence of groups A, B and C and group homomorphisms α, and β such that

$$A \xrightarrow{\alpha} B \xrightarrow{\beta} C$$

is called exact at B if im $\alpha =$ ker β.

Definition 2.6. A short exact sequence of groups is a sequence of groups and group homomorphisms

$$0 \rightarrow A \xrightarrow{\alpha} B \xrightarrow{\beta} C \rightarrow 0$$

which is exact at A, B, and C. That means α is one-one, β is onto, and im $\alpha =$ ker β. In a general setup, an exact sequence can have many terms:

$$A_1 \xrightarrow{\alpha_1} A_2 \xrightarrow{\alpha_2} A_3 \ldots A_{n-1} \xrightarrow{\alpha_{n-1}} A_n$$

and it must be exact at each A_i for $1 < i < n$. Exact sequences can also be of infinite length.

2.1 Number Fields

Throughout this thesis, we consider elliptic curves over rational numbers. But most of the properties of an elliptic curve hold true for *number fields* also. A number field is a finite extension of $\mathbb{Q}$. We use [39] as a reference for this section.

A field extension L/K is a pair of fields with $K \subset L$. In other words, L is a K-vector space, and the number $[L : K] = \dim_K L$ is called the *degree of the field extension* L/K. The extension L/K is said to be finite if the degree of the extension is finite.

Definition 2.7. A finite extension $K/\mathbb{Q}$ is called a *number field.*

Definition 2.8. Let K be a number field. An *algebraic integer* is an element $\alpha \in K$ such that there is some monic polynomial $f \in \mathbb{Z}[x]$ with $f(\alpha) = 0$. We write $\mathcal{O}_K$ for the set of algebraic integers in K.

Example 2.1. *If $K = \mathbb{Q}(i)$, then $\mathcal{O}_K = \mathbb{Z}[i]$.*

For $K = \mathbb{Q}(\sqrt{d})$ where $d \in \mathbb{Z}$, $d \neq 0, 1$, and d is square-free, it is well-known that

$$\mathcal{O}_K = \begin{cases} \mathbb{Z}[\sqrt{d}], & d \not\equiv 1 \pmod 4. \\ \mathbb{Z}[\frac{1}{2}(1+\sqrt{d})], & d \equiv 1 \pmod 4. \end{cases}$$

One can easily observe that if K is a number field, then $K = \mathbb{Q}(\alpha)$ for some algebraic integer α. The following result gives the number of distinct embeddings a number field can possess in $\mathbb{C}$.

Theorem 2.9. *Let K be a number field of degree n. Then there are exactly n distinct embeddings $\sigma_i : K \to \mathbb{C}$, $(i = 1, 2, 3, \ldots, n)$. The element $\sigma_i(\alpha) = \alpha_i$ are all the distinct zeros in $\mathbb{C}$ of the minimal polynomial of α over $\mathbb{Q}$.*

The following result now describes the structure of the unit group $\mathcal{O}_K^*$ of $\mathcal{O}_K$.

Theorem 2.10. *$\mathcal{O}_K^*$ is a finitely generated abelian group of rank $r + s - 1$ where r is the number of real embeddings of K and $2s$ is the number of non-real complex embeddings.*

Definition 2.11. Let K be a number field of degree n and let $\sigma_1, \sigma_2, \ldots \sigma_n$ be the embeddings $K \to \mathbb{C}$. Then for any $\alpha \in K$, the norm is

$$N_K(\alpha) = \prod_{i=1}^{n} \sigma_i(\alpha),$$

and the trace is

$$T_K(\alpha) = \sum_{i=1}^{n} \sigma_i(\alpha).$$

It is well known that unique factorization does not hold for the elements of the ring of integers of a number field. However, the unique factorization of nonzero ideals into prime ideals does hold. To see this, we introduce the notion of fractional ideal first.

Definition 2.12. A fractional ideal of $\mathcal{O}_K$ is a subset $I \subseteq K$ satisfying the following:
(i) I is an abelian group under addition;
(ii) $xI \subseteq I$ for every $x \in \mathcal{O}_K$;
(iii) there exists some nonzero $y \in \mathcal{O}_K$ such that $yI \subseteq \mathcal{O}_K$.
There is a group structure on the set of fractional ideals of $\mathcal{O}_K$. The following theorem tells us that the prime factorization in $\mathcal{O}_K$ is unique if all the ideals of $\mathcal{O}_K$ are principal.

Theorem 2.13. *The non-zero fractional ideals of $\mathcal{O}_K$ form an abelian group under multiplication. Moreover, every non-zero ideal of $\mathcal{O}_K$ can be written as a product of prime ideals, uniquely up to the order of the factors.*

Let $I(\mathcal{O}_K)$ denote the collection of all nonzero fractional ideals of $\mathcal{O}_K$, and $P(\mathcal{O}_K)$ denotes the collection of all nonzero principal fractional ideals of $(\mathcal{O}_K)$. It can be noted that $P(\mathcal{O}_K)$ is a subgroup of $I(\mathcal{O}_K)$.

Definition 2.14. The ideal class group for a number field K is the quotient group $I(\mathcal{O}_K)/P(\mathcal{O}_K)$.
It is well known that the ideal class group of a number field is a finite group. The *class number* of a number field K, denoted by $h(K)$, is defined as the order of the ideal class group of K.
We note that if $\mathcal{O}_K$ itself is a principal ideal domain, then the ideal class group is the trivial group, and vice versa. One can loosely interpret the class number of a number field to be a measure of how far $\mathcal{O}_K$ is from being a principal ideal domain.

Definition 2.15. A prime number p is said to be *ramified* in a number field K if the prime ideal factorization

$$\langle p \rangle = p\mathcal{O}_K = \wp_1^{e1} \ldots \wp_t^{e_t}$$

has some e_i greater than 1. If every e_i equals 1, we say p is unramified in K.

Theorem 2.16 (Hilbert's Class Field). *([39],Proposition (6.9)) The Hilbert class field E of a number field K is the maximal unramified abelian extension of K. Its degree over K equals the class number of K, and $Gal(E/K)$ is canonically isomorphic to the ideal class group of K.*

We can use this fact to show the existence of an unramified abelian extension of degree n of a number field K is equivalent to the class number $h(K) \equiv 0 \pmod{n}$.

2.2 Elliptic Curves

We now introduce the necessary details regarding the group structure of elliptic curves over number fields. Most of the results mentioned here are well-known. For notations and references, we have followed [46].

Definition 2.17. An *elliptic curve over a number field* K is a smooth projective curve (defined over K) of genus one with a distinguished K-rational point. Equivalently, an elliptic curve is an abelian variety of dimension one.
For a field with $\text{char}(K) \neq 2$ or 3, an elliptic curve E/K can be defined by a short Weierstrass equation

$$E : y^2 = x^3 + Ax + B \text{ with } A, B \in K, \text{ with } \Delta \neq 0.$$

The smoothness of an elliptic curve is equivalent to the non-vanishing of the *discriminant*, $\Delta = -(4A^3 + 27B^2)$, of an elliptic curve.

Definition 2.18. Let $E : y^2 = f(x)$ be an elliptic curve over K. The set of K-rational points on E is the set $\{(x, y) \in K \times K \mid y^2 = f(x)\}$. This set is denoted by $E(K)$.
We note that although the curves are represented with affine coordinates, in the variables x and y, in the projective coordinates, the curve looks like

$$E : y^2z = x^3 + Axz^2 + Bz^3.$$

To specify an elliptic curve, we not only need an equation defining the curve but also a distinguished rational point, which acts as the group's identity. For curves in Weierstrass form, the point $O := (0 : 1 : 0)$ acts as the distinguished point, the unique point on the curve E that lies on the line $z = 0$ at infinity. If $z = 0$ then $x = 0$ and we may assume $y = 1$ after scaling the projective point $(0 : y : 0)$ by $1 = y$. We note that $x = z = 0$ gives

$y \neq 0$, since $(0 : 0 : 0)$ is (by definition) not a projective point. Every point $P \neq O$ on the curve E thus has a nonzero z-coordinate which we can scale to be 1, and we use the notation $P = (x_0, y_0) := (x_0 : y_0 : 1)$ to denote these affine points.
Given distinct points $P, Q \in E(K)$, $P * Q$ denotes the third point of intersection between the curve and the line passing through P and Q. Note that $P * Q \in E(K)$. $P + Q$ is defined to be the reflection of $P * Q$ about the x-axis. $P * P$ is defined to be the third intersection point of E with the line tangent to E at P (which is well-defined for every P because E is non-singular). As before, the reflection of $P * P$ about the x-axis defines $P + P$. With this $+$, the set $E(K)$ forms an abelian group, and O acts as the identity element.

Theorem 2.19 (Mordell Theorem)**.** *Let $E/\mathbb{Q}$ be an elliptic curve. Then the group $E(\mathbb{Q})$ is finitely generated.*

So by Theorem 2.5, $E(\mathbb{Q}) \cong \mathbb{Z}^r \oplus E(\mathbb{Q})_{tors}$. r is called the rank of the elliptic curve. The result stands true even if $\mathbb{Q}$ is replaced by any arbitrary number field K. The subgroup of points of finite order having coordinates in K are denoted by $E(K)_{tors}$.

Theorem 2.20 (Mordell-Weil Theorem)**.** *Let E be an elliptic curve over a number field K, then the set of K-rational points $E(K)$ is finitely generated abelian group. i.e. $E(K) \cong \mathbb{Z}^r \oplus E(K)_{tors}$.*

Theorem 2.21. *([46], Theorem II.2.3) Let $\phi : C_1 \to C_2$ be a morphism of curves. Then ϕ is either constant or subjective.*

Let C_1/K and C_2/K be curves and let $\phi : C_1 \to C_2$ be a nonconstant rational map defined over K. Then composition with ϕ induces an injection of function fields fixing K,

$$\phi^* : K(C_2) \to K(C_1), \quad \phi^* f = fo\,\phi.$$

Definition 2.22. Let $\phi : C_1 \to C_2$ be a map of curves defined over K. If ϕ is constant, we define the degree of ϕ to be 0. Otherwise we say that ϕ is a finite map and $deg\ \phi = [(K(C_1) : \phi^* K(C_2)]$.

Theorem 2.23. *([46], Theorem II. 2.4.1) Let C_1 and C_2 be smooth curves and let $\phi : C_1 \to C_2$ be a map of degree one. Then ϕ is an isomorphism.*

Let $E[m] = \{P \in E(\bar{K}) \mid mP = O\}$ refer the set of $m-$torsion points. It can be shown that (see [46], Proposition $VI.6.1$),

$$E[m] \cong \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}.$$

Definition 2.24. The divisor group of a curve C is the free abelian group generated by the points of C denoted by $Div(C)$. Thus a divisor $D \in Div(C)$ is a formal sum

$$D = \sum_{P \in C} n_P(P)$$

where $n_P \in \mathbb{Z}$ and $n_p = 0$ for all but finitely many $P \in C$. The degree of D is defined by

$$deg\ D = \sum_{P \in C} n_P.$$

Definition 2.25. Let C be a smooth curve and let $f \in \bar{K}(C)^*$. Then we can associate to f the divisor,

$$div(f) = \sum_{P \in C} ord_P(f)(P).$$

where $K(C)$ denotes the function field of C over K.

Weil-Pairing: Let $T \in E[m]$. There is a function $f \in \bar{K}(E)$ satisfying

$$div(f) = m(T) - m(O).$$

Taking $T' \in E$ to be a point with $[m]T' = T$, there is a function $g \in \bar{K}(E)$ satisfying

$$div(g) = [m]^*(T) - [m]^*(O) = \sum_{R \in E[m]} (T' + R) - (R).$$

Then there is a pairing

$$e_m : E[m] \times E[m] \to \mu_m$$

by setting

$$e_m(S, T) = \frac{g(X + S)}{g(X)}$$

where $X \in E$ is any point such that $g(X + S)$ and $g(X)$ are both defined and nonzero (μ_m denotes the group of m^th root of unity). This pairing is called the Weil e_m -pairing, which we use in later sections to briefly sketch the proof of *Complete* 2-*Descent*.

Proposition 2.26. *([46], Proposition II.8.1): The Weil e_m-pairing has the following properties:*
(i) It is bilinear:

$$e_m(S_1 + S_2, T) = e_m(S_1, T)e_m(S_2, T),$$

$$e_m(S, T_1 + T_2) = e_m(S, T_1)e_m(S, T_2).$$

(ii) It is alternating:

$$e_m(T, T) = 1.$$

so in particular, $e_m(S, T) = e_m(T, S)^{-1}$.
(iii) It is non-degenerate:

$$\text{If } e_m(S, T) = 1 \text{ for all } S \in E[m], \text{ then } T = O.$$

(iv) It is Galois invariant:

$$e_m(S, T)^\sigma = e_m(S^\sigma, T^\sigma) \;\; \text{for all} \;\; \sigma \in G_{\bar{K}/K}.$$

(v) It is compatible:

$$e_{mm'}(S, T) = e_m([m']S, T) \;\; \text{for all } S \in E[mm'] \;\; \text{and } T \in E[m].$$

We recall a few notions from p-adic valuation that will be needed in later topics.

Definition 2.27. For all $x, y \in \mathbb{Z}$, a valuation $v : \mathbb{Z} \to \mathbb{Z} \cup \{\infty\}$ satisfies following;

(i) $v(xy) = v(x) + v(y)$.

(ii) $v(x + y) \geq \min\{v(x), v(y)\}$.

(iii) $v(0) = \infty$.

Definition 2.28. For a fixed prime number $p \in \mathbb{Z}$, and $x \in \mathbb{Z} - \{0\}$, $v_p(x)$ is the unique non-negative integer which satisfies $x = p^{v_p(x)}u$ with $u \in \mathbb{Z}$ and $p \nmid u$.
For $x \in \mathbb{Q}$ where $x = a/b$, $v_p(x) = v_p(a) - v_p(b)$.

Definition 2.29. On a field K, an absolute value is a function $|\;| : K \to \mathbb{R} \geq 0$ such that
(i) $|x| = 0 \iff x = 0$,
(ii) $|xy| = |x||y|$, and
(iii) $|x + y| \leq |x| + |y|$

Definition 2.30. Let $(K, |\ |)$ be a field with an absolute value. A completion of $(K, |\ |)$ is an absolute-valued field $(L, |\ |_L)$ which is complete as a metric space and has the property that there is some embedding $i : K \to L$ with the image of K dense and $|x| = |i(x)|_L$ for $x \in K$.

Minimal Weierstrass equation

Let E/K be an elliptic curve given by a Weierstrass equation $y^2 = x^3 + ax + b$. We say that a Weierstrass equation is minimal if a and b belong to $R = \{x \in K : v(x) \geq 0\}$ the ring of integers of K and $v(a) < 4$ or $v(b) < 6$ (this is equivalent to $v(\Delta)$ being minimal).

Theorem 2.31. *(Lutz-Nagell) If $E/\mathbb{Q}$ has minimal Weierstrass equation and $P = (x, y) \in E(\mathbb{Q})_{tors}$ then $x, y \in \mathbb{Z}$ and either $y = 0$ or $y^2|D$ where D denotes the discriminant of the curve.*

Let $p \in \mathbb{Z}$ be a prime, E be an elliptic curve over $\mathbb{Q}$ in minimal Weierstrass form. Then the reduction of E modulo p is the (possibly singular) Weierstrass curve over $\mathbb{F}_p$. $\bar{E}(\mathbb{F}_p)$ denotes the group of $\mathbb{F}_p$ rational points of E modulo p.

Definition 2.32. Let $p \in \mathbb{Z}$ prime, and E be an elliptic curve over $\mathbb{Q}$ in minimal Weierstrass form. Then E is said to have a good reduction at p if $\bar{E}$ is non-singular. Otherwise, E has a bad reduction at p.

Theorem 2.33. *([46], Proposition VII.3.1.) Let p be a prime such that E has a good reduction at p. Let $\phi : E(\mathbb{Q})_{tors} \to \bar{E}(\mathbb{F}_p)$ be given by $O \to \bar{O}$ and $(x, y) \to (\bar{x}, \bar{y})$. Then ϕ is a one-one homomorphism, and thus $E(\mathbb{Q})_{tors}$ is isomorphic to a subgroup of $\bar{E}(\mathbb{F}_p)$.*

Corollary 2.34. *The order of $E(\mathbb{Q})_{tors}$ divides the order of $\bar{E}(\mathbb{F}_p)$ for every prime p with good reduction.*

Theorem 2.35 (Mazur's theorem:)**.** *([46], Theorem VIII.7.5) Let E be an elliptic curve defined over $\mathbb{Q}$. The possible torsion subgroups of $E(\mathbb{Q})$ are:*

(i) $\mathbb{Z}/N\mathbb{Z}$*, where* $1 \leq N \leq 10$*, or* $N = 12$.

(ii) $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2N\mathbb{Z}$*, where* $N = 1, 2, 3, 4$.

The Mordell-Weil theorem is vast in nature. It tells us that a finite set is enough to describe the whole structure of rational points on an elliptic curve. One can see the size of $E(K)/mE(K)$ as a measure of how large $E(K)$ is compared to $mE(K)$. The difficulty is finding the inverse of the multiplication by $[m]$ map in $E(K)$. Without the loss of generality, one can assume $E[m] \subset E(K)$ for the next few results.

Definition 2.36. The Kummer pairing

$$\mathrm{k} : E(K) \times G_{\bar{K}/K} \to E[m]$$

is defined as follows. Let $P \in E(K)$ and choose any point $Q \in E(K)$ satisfying $[m]Q = P$. Then $\mathrm{k}(P, \sigma) = Q^{\sigma} - Q$.

We enlist some of the fundamental properties of the Kummer pairing below.

Proposition 2.37. *([46] Proposition VIII.1.2) Let* $\mathrm{k} : E(K) \times G_{\bar{K}/K} \to E[m]$ *is a Kummer pairing. Then*
(i) The Kummer pairing is well-defined.
(ii) The Kummer pairing is bilinear.
(iii) The kernel of the Kummer pairing on the left is $mE(K)$*.*
(iv) The kernel of the Kummer pairing on the right is $G_{\bar{K}/L}$*, where* $L = K([m]^{-1}E(K))$ *is the composition of all fields* $K(Q)$ *as* Q *ranges over the points in* $E(\bar{K})$ *satisfying* $[m]Q \in E(K)$*.*
Hence, the Kummer pairing induces a perfect bilinear pairing

$$E(K)/mE(K) \times G_{L/K} \to E[m], \ \textit{where } L = K([m]^{-1}E(K)).$$

The above proposition tells us that the finiteness of $E(K)/mE(K)$ (which can be proved, is equivalent to the finiteness of the extension L/K.

Proposition 2.38. *([46], Proposition* $VIII.1.5.$*) Let* $L = K([m]^{-1}E(K))$ *be the field as defined above.*
i) The extension L/K *is abelian and has exponent* m *i.e. the Galois group* $G_{L/K}$ *is abelian and every element of* $G_{L/K}$ *has order dividing* m*.*
ii) Let $S = \{v \in M_k^0 : E \textit{ has bad reduction at } v\} \cup \{v \in M_K^0 : v(m) \neq 0\} \cup M_K^{\infty}$*.*

The following proposition proves that the field extension L/K satisfying the conditions in the above proposition is a finite extension.

Proposition 2.39. *([46], Proposition VIII.1.6.) Let* K *be a number field,* $S \subset M_K$ *be a finite set of places containing* M_K^{∞}*, and* $m \geq 2$ *be an integer. Let* L/K *be the maximal abelian extension of* K *having exponent* m *that is unramified outside of* S*. Then* L/K *is a finite extension.*

One can use the results of Proposition 2.37, Proposition 2.38, and Proposition 2.39 above to prove the following theorem, known as the *Weak Mordell-Weil Theorem*. For the brevity of this thesis, we also include a brief sketch of the proof of the Weak Mordell-Weil theorem and its relation to the Mordell-Weil theorem and m-Selmer group.

Theorem 2.40. *(Weak Mordell-Weil Theorem)([46], Theorem VIII.1.1.) Let K be a number field, E/K be an elliptic curve, and $m \geq 2$ be an integer. Then*

$$E(K)/mE(K)$$

is a finite group.

Proof. The perfect pairing at the end of the Proposition 2.37 shows that $E(K)/mE(K)$ is finite if and only if $G_{L/K}$ is finite where $L = K([m]^{-1}E(K))$. Proposition 2.38 ensures that L has certain properties, and Proposition 2.39 implies that any extension L of K having these properties is a finite extension, hence $G_{L/K}$ is finite. This concludes the proof of the Weak Mordell-Weil Theorem. □

Remark 1: We note that the Kummer pairing induces an injection

$$E(K)/mE(K) \to \mathrm{Hom}(G_{L/K}, E[m]).$$

While it is possible to compute the group $\mathrm{Hom}(G_{L/K}, E[m])$ explicitly, the crucial question that remains is of which of those elements come from points of $E(K)/mE(K)$. This last question currently has no effective solution, and what makes the Mordell-Weil theorem ineffective in practice. For this reason, one introduces the concept of *the m-Selmer group*, where $E(K)/mE(K)$ will be injected into a smaller group, and the cokernel of the corresponding map will be explored. The following theorem shows that if the generators of $E(K)/mE(K)$ are known, one can effectively find the generators of $E(K)$. This highlights that the only ineffectiveness in the above proof is finding generators of $E(K)/mE(K)$.

Theorem 2.41 (Descent Theorem)**.** *([46], VIII.3.1.) Let A be an abelian group. Suppose that there exist a height function $h : A \to \mathbb{R}$ with the following three properties:*
(i) Let $\mathbb{Q} \in A$. There is a constant C_1, depending on A and Q, such that

$$h(P+Q) \leq 2h(P) + C_1 \quad \forall\ p \in A.$$

(ii) There are an integer $m \geq 2$ and a constant C_2, depending on A, such that

$$h(mp) \geq m^2 h(P) - C_2 \quad \forall\ P \in A.$$

(iii) For every constant C_3, the set $\{P \in A : h(P) \leq C_3\}$ is finite.

Suppose further that for the integer m in (ii), the quotient group A/mA is finite then A is finitely generated.

Proof. Choose a finite set $S = Q_1, Q_2, \dots \mathbb{Q}_r \in A$ to represent the finitely many cosets in A/mA, and let $P \in A$ be an arbitrary element. Reminiscent of the Euclidean algorithm, let us begin by writing

$$P = mP_1 + Q_{i_1},$$

$$P_1 = mP_2 + Q_{i_2},$$

$$P_{n-1} = mP_n + Q_{i_n}.$$

For any index j, we have

$$h(P_j) \leq \frac{1}{m^2}(h(mP_j) + C_2) \text{ from } (ii)$$

$$= \frac{1}{m^2}(h(P_{j-1} - Q_{i_j}) + C_2)$$

$$\leq \frac{1}{m^2}(2h(P_{j-1} + C_1' + C_2) \text{ from } (i)$$

where C_1' is the maximum of the constants from (i) for $Q \in \{-Q_1, -Q_2, \dots, -Q_r\}$. Using this inequality,

$$h(P_n) \leq \left(\frac{2}{m^2}\right)^n h(P) + \left(\frac{1}{m^2} + \frac{2}{m^2} + \frac{4}{m^2} + \dots + \frac{2^{n-1}}{m^2}\right)(C_1' + C_2)$$

$$< \left(\frac{2}{m^2}\right)^n h(P) + \frac{C_1' + C_2}{m^2 - 2}$$

$$\leq \frac{1}{2^n}h(P) + \frac{1}{2}(C_1' + C_2) \text{ since } m \geq 2.$$

$$\implies h(P_n) \leq 1 + \frac{1}{2}(C_1' + C_2), \text{ for sufficiently large } n$$

As P is a linear combination of P_n and $Q_1, Q_2, \dots, Q_r$,

$$P = m^n P_n + \sum_1^n m^{j-1} Q_{i_j}.$$

It implies that every $P \in A$ is a linear combination of the points in the set

$$\{Q_1, Q_2, \cdots Q_r\} \cup \{Q \in A : h(Q) \leq 1 + \frac{1}{2}(C_1' + C_2)\}.$$

From (iii), it is a finite set. This concludes the proof. □

2.3 Galois Group Cohomology

We give a brief overview of Galois cohomology groups which will be essential in defining the Selmer and Shafarevich-Tate groups later. We refer to ([46], Appendix B) for a detailed discussion.

Definition 2.42. Let G be a group. A $G-$module is a pair (M, G) consisting of an abelian group M together with a $G-$ action that preserves its abelian structure, i.e. for all $\sigma \in G$ and all $m, m' \in M, \sigma(m + m')) = \sigma m + \sigma m'$.

We note that $\sigma \in G$ defines an automorphism of M, so that the $G-$action defines a homomorphism $G \to Aut(M)$, generalizing the notion of a representation and agreeing with the definition of a module over the group ring $\mathbb{Z}[G]$. For example, if L/K is a finite Galois extension with $G = Gal(L/K)$, an elliptic curve $E(L)$ is naturally a $G-$module, with the action given by applying a field automorphism.

Definition 2.43. For a $G-$module M, the 0th cohomology group is the fixed set by

$$G : H^0(G, M) := M^G = \{m \in M | \forall \sigma \in G, gm = m\}.$$

Definition 2.44. A crossed homomorphism is a map $f : G \to M$ such that $\forall \sigma, \tau \in G, f(\sigma\tau) = f(\sigma) + \sigma f(\tau)$.

Definition 2.45. A crossed homomorphism is called principal if it is of the form $\forall \sigma \in G, f(\sigma) = \sigma m - m$, for some $m \in M$.

Definition 2.46. For a $G-$module M, the first cohomology group is (roughly) the set of crossed homomorphisms that aren't principal. More precisely, $H^1(G, M) := \dfrac{\textit{crossed homomorphisms}}{\textit{principal crossed homomorphisms}}$ Note that any crossed homomorphism satisfies $f(1) = f(1 \cdot 1) = f(1) + f(1) \implies f(1) = 0$. Sums and differences of crossed (resp. principal) homomorphisms are crossed (resp. principal), and observe that $H^1(G, M)$ is an abelian group.

Example 2.2. *If G acts on M trivially, then $H^0(G,M) = M^G = M$. The crossed homomorphisms "uncross:" $f(\sigma\tau) = f(\sigma) + f(\tau)$, and principal crossed homomorphisms vanish: $f(\sigma) = \sigma m - m = 0$.*
Therefore $H^1(G,M) = Hom(G,M)$.

2.4 Selmer and Shafarevich-Tate Group

We can now introduce the notion of Selmer and Shafarevich-Tate group to inject $E(K)/mE(K)$ into a smaller group. From Definition 2.36, we know there exists a pairing $\mathrm{k} : E(K) \times G_{\bar{K}/K} \to E[m]$ such that $\mathrm{k}(P,\sigma) = Q^\sigma - Q$, where $Q \in E(\bar{K})$ such that $[m]Q = P$.
From Proposition 2.37, we know that the kernel of k is $mE(K)$. Hence, one may view the map k as a homomorphism

$$\delta_E : E(K)/mE(K) \to \mathrm{Hom}(G_{\bar{K}/K}, E[m]),$$

$$\delta_E(P)(\sigma) = \mathrm{k}(P,\sigma).$$

$E[m] \subset E(K)$ implies that *the group of m-th roots of unity* $\mu_m \subset K^*$ which follows from the basic properties of Weil Pairing

$$e_m : E[m] \times E[m] \to \mu_m$$

mentioned in Proposition 2.26. Since $\mu_m \subset K^*$, Hilbert's Theorem 90 ([14], (17.3)) asserts that every homomorphism $G_{\bar{K}/K} \to \mu_m$ has the form $\sigma \to \frac{\beta^\sigma}{\beta}$ for some $\beta \in \bar{K}^*$ such that $\beta^m \in K^*$. In other words, there is an isomorphism

$$\delta_K : K^*/(K^*)^m \to \mathrm{Hom}(G_{\bar{K}/K}, \mu_m),$$

$$\delta_K(b)(\sigma) = \frac{\beta^\sigma}{\beta}$$

for β as mentioned above. We now describe the theoretical version of the m-descent method through the following theorem.

Theorem 2.47 ([46], Theorem X.1.1.)**.** *With notations as mentioned above,*
(i) There is a bilinear pairing $b : E(K)/mE(K) \to K^*/(K^*)^m$ satisfying $e_m(\delta_E(P), T) = \delta_K(b(P,T))$.
(ii) The pairing in (i) is nondegenerate on the left.
(iii) Let $S \subset M_K$ be the union of the set of infinite places, the set of finite primes at which E has bad reduction and the set of finite primes dividing m. Then the image of the pairing

in (i) *lies in the following subgroup of* $K^*/(K^*)^m$*:*

$$K(S,m) = \{b \in K^*/(K^*)^m : \; v(b) \equiv 0 \pmod{m} \textit{ for all } v \notin S\}.$$

(iv) *The pairing in* (i) *may be computed as follows. for each* $T \in E[m]$*, choose functions* $f_T, g_T \in K(E)$ *such that*

$$\textit{div}(f_T) = m(T) - m(O) \textit{ and } f_T \cdot [m] = g_T^m.$$

Then for any point $P \neq T$*,* $b(P,T) \equiv f_T(P) \pmod{(K^*)^m}$*. For* $P = T$*, one can compute* $b(T,T)$ *using linearity.*

Remark 2: Theorem 2.47 provides formulas for the computation of the Mordell-Weil group. This is because it can be shown that $K(S,m)$ in (iii) is a finite group ([46], VIII.1.6). Secondly, the functions f_T in (iv) are also quite easy to compute ([46], IX.8.1), even for large values of m (we only focus on $m = 2$ here). Now the pairing in (i) is nondegenerate on the left implies that to compute $E(K)/mE(K)$, one only needs to do the following.

Fix two generators T_1 and T_2 for $E[m]$. For each of the finitely many pairs $(b_1, b_2) \in K(S,m) \times K(S,m)$ check whether the simultaneous equations

$$b_1 z_1^m = f_{T_1}(P) \text{ and } b_2 z_2^m = f_{T_2}(P)$$

have a solution $(P, z_1, z_2) \in E(K) \times K^* \times K^*$. One can be even more explicit by expressing the function f_T in terms of Weirstrass coordinates x and y. This reduces the problem into finding a solution $(x, y, z_1, z_2) \in K \times K \times K^* \times K^*$ satisfying

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6,$$

$$b_1 z_1^m = f_T(x,y), \;\; b_2 z_2^m = f_{T_2}(x,y).$$

The above equations define a new curve, called a *homogeneous space*, which we define later. The problem of calculating $E(K)/mE(K)$ now reduces to the existence or non-existence of a single rational point on each of an explicitly given finite set of curves. Many of these curves immediately get discarded from consideration due to the lack of any local solution and, hence, no rational solution. The problem arises when there is a homogeneous space having points defined over every completion K_v, yet having no K-rational points, which we discuss later on.

For $m = 2$, we now give a detailed working description of the method 2-descent below.

Proposition 2.48 (Complete 2-Descent). *([46], Proposition X.1.4.) Let E/K be an elliptic curve given by a Weierstrass equation*

$$y^2 = (x - a_1)(x - a_2)(x - a_3)$$

with $a_1, a_2, a_3 \in K$. Let $S \subset M_K$, be the finite set of places containing all Archimedean places, the set of finite places at which E has bad reduction, and the set of finite places dividing 2. Further let

$$K(S, 2) = \{b \in K^*/(K^*)^2 : v(b) \equiv 0 \pmod 2 \textit{ for all } v \in M_K \backslash S\}.$$

Then, there is an injective homomorphism

$$\beta : E(K)/2E(K) \longrightarrow K(S, 2) \times K(S, 2)$$

defined by

$$\beta(x, y) = \begin{cases} (x - a_1, x - a_2) & \textit{if } x \neq a_1, a_2, \\ \left(\dfrac{a_1 - a_3}{a_1 - a_2}, a_1 - a_2\right) & \textit{if } x = a_1, \\ \left(a_2 - a_1, \dfrac{a_2 - a_3}{a_2 - a_1}\right) & \textit{if } x = a_2 \\ (1, 1) & \textit{if } x = \infty, \ \textit{i.e., if } (x, y) = O, \end{cases}$$

Let $(b_1, b_2) \in K(S, 2) \times K(S, 2)$ be a pair that is not the image of one of the three points $O, (a_1, 0), (a_2, 0)$.Then (b_1, b_2) is the image of a point $P = (x, y) \in E(K)/2E(K)$ if and only if the equations

$$\begin{aligned} b_1 z_1^2 - b_2 z_2^2 &= a_2 - a_1, \\ b_1 z_1^2 - b_1 b_2 z_3^2 &= a_3 - a_1, \end{aligned}$$

have a solution $(z_1, z_2, z_3) \in K^* \times K^* \times K$. If such a solution exists, then we can take $P = (x, y) = (b_1 z_1^2 + a_1, b_1 b_2 z_1 z_2 z_3)$.

We now formally define the homogeneous spaces mentioned after Theorem 2.47.

Definition 2.49. Let C/K be a smooth projective curve. The isomorphism group of C is the group of $\bar{K}$-isomorphism from C to itself. It is denoted by $\mathrm{Isom}(C)$ and its subgroup containing isomorphisms defined over K is denoted by $\mathrm{Isom}_K(C)$.

Definition 2.50. A twist of C/K is a smooth curve C'/K that is isomorphic to C over $\bar{K}$. Two twists, C_1 and C_2, are equivalent if they are isomorphic over K. The set of twists of C/K, modulo K-isomorphism, is denoted by $\text{Twist}(C/K)$.
The following result shows that there is a bijection between $\text{Twist}(C/K)$ and the elements of the cohomology set $H^1(G_{\bar{K}/K}, \text{Isom}(C))$.

Theorem 2.51 ([46], Theorem X.2.2)**.** *Let C/K be a smooth projective curve. For each twist C'/K of C/K, choose a $\bar{K}$-isomorphism $\phi : C' \to C$ and define a map $\xi_\sigma = \phi^\sigma\phi^{-1} \in Isom(C)$-the automorphism group of C. (a) The map ξ is a 1-cocycle, i.e.*

$$\xi_{\sigma\tau} = (\xi_\sigma)^\tau \xi_\tau \quad \textit{for all} \quad \sigma, \tau \in G_{\bar{K}/K}.$$

The associated cohomology class in $H^1(G_{\bar{K}/K}, Isom(C))$ is denoted by $\{\xi\}$.
(b) The cohomology class $\{\xi\}$ is determined by the $K-$ isomorphism class of C' and is independent of the choice of ϕ. We thus obtain a natural map

$$Twist(C/K) \to H^1(G_{\bar{K}/K}, Isom(C)).$$

(c) The map in (b) is a bijection. In other words, the twists of C/K, up to $K-$ isomorphism, are in one-to-one correspondence with the elements of cohomology set $H^1(G_{\bar{K}/K}, Isom(C))$.

Remark 3: The group $\text{Isom}(C)$ is often non-abelian, and definitely so when C is an elliptic curve. Hence, $H^1(G_{\bar{K}/K}, \text{Isom}(C))$ in Theorem 2.51 is generally a pointed set, not a group. This makes one look into a $G_{\bar{K}/K}$-invariant subgroup A of $\text{Isom}(C))$ such that $H^1(G_{\bar{K}/K}, A)$ is a group.

Definition 2.52. A homogeneous space for E/K is a smooth curve C/K together with a simply transitive algebraic group action of E on C defined over K, i.e. it is a pair (C, ν), $\nu : C \times E \to C$ is a morphism over K satisfying the following properties:
(i) $\nu(p, O) = p \ \ \forall p \in C$.
(ii) $\nu(\nu(p, P), Q) = \nu(p, P + Q) \ \ \forall \ p \in C$ and $P, Q \in E$.
(iii) There exists a unique $P \in E$ satisfying $\nu(p, P) = q, \ \forall \ p, q \in C$. The following result shows that a homogeneous space a special case of twists on a curve.

Proposition 2.53 ([46], Proposition X.3.2)**.** *Let E/K be an elliptic curve and let C/K be a homogeneous space for E/K. Fix a point $p_0 \in C$ and define a map*

$$\theta : E \to C, \quad \theta(P) = p_0 + P.$$

(i) The map θ is an isomorphism defined over $K(p_0)$. In Particular, the curve C/K is a twist of E/K.
(ii) for all $p \in C$ and all $P \in E$,

$$p + P = \theta(\theta^{-1}(p) + P).$$

(note: The first + is the action of E on C while the second + is addition on E.)
(iii) For all $p, q \in C$,

$$q - p = \theta^{-1}(q) - \theta^{-1}(p).$$

(iv) The subtraction map

$$v : C \times C \to E, \quad v(q,p) = q - p$$

is a morphism and is defined over K.

Definition 2.54. Let C/K and C'/K be two homogeneous spaces. They are said to be equivalent if there exists an isomorphism $\phi :\ C \to C'$ over K such that $\phi(p+P) = \phi(p)+P$ for all $p \in C$ and all $P \in E$. The equivalence class containing E/K, acting on itself by translation, is called the trivial class. The collection of equivalence classes of homogeneous spaces for E/K is called the *Weil -Chatlet* group for E/K and is denoted by $WC(E/K)$.

Proposition 2.55. *([46], Proposition X.3.3.) A homogeneous space C/K for E/K is in the trivial class if and only if $C(K)$ is not the empty set.*

The above proposition indicates that the triviality of homogeneous space, i.e., being in the equivalence class containing E/K, is equivalent to answering the Diophantine equation question of whether the given curve has any rational points. The following result identifies the Weil-Chatelet group $WC(E/K)$ with a certain cohomology group, which helps solve the Diophantine problems mentioned above.

Theorem 2.56. *([46], Theorem X.3.6.) There is a bijection $WC(E/K) \to H^1(G_{\bar{K}/K}, E)$ in the following way. Choose any point $p \in C$, and then define the map $\{C/K\} \to \{\sigma \to p^\sigma - p\}$.*

The above theorem helps to identify the $WC(E/K)$ with the cohomology group. Let E, E' be elliptic curves defined over K. We consider the isogeny $[m] : E \to E$ over K. Then, there is an exact sequence of $\mathrm{G}_{\bar{K}/K}$-modules

$$\begin{tikzcd} 0 \arrow[r] & E[m] \arrow[r] & E \arrow[r, "m"] & E \arrow[r] & 0 \end{tikzcd}.$$

Considering Galois cohomology, one can now obtain the long exact sequence

$$\begin{tikzcd} 0 \arrow[r] & E(K)[m] \arrow[r] & E(K) \arrow[r] & E(K) \arrow[r] & H^1(G_{\bar{K}/K}, E[m]) \arrow[r] & H^1(G_{\bar{K}/K}, E)[m] \arrow[r] & 0 \end{tikzcd}$$

which yields the following short exact sequence

$$\begin{tikzcd} 0 \arrow[r] & E(K)/mE(K) \arrow[r] & H^1(G_{\bar{K}/K}, E[m]) \arrow[r] & H^1(G_{\bar{K}/K}, E)[m] \arrow[r] & 0\ . \end{tikzcd}$$

After considering the above sequence locally for each $v \in M_K$, the following commutative diagram can be obtained.

$$\begin{tikzcd} 0 \arrow[r] & E(K)/m(E(K)) \arrow[r] \arrow[d] & H^1(G_{\bar{K}/K}, E[m]) \arrow[r] \arrow[d] & H^1(G_{\bar{K}/K}, E)[m] \arrow[r] \arrow[d] & 0 \\ 0 \arrow[r] & \prod_v E(K_v)/m(E(K_v)) \arrow[r] & \prod_v H^1(G_{\bar{K}_v/K_v}, E[m]) \arrow[r] & \prod_v H^1(G_{\bar{K}_v/K_v}, E)[m] \arrow[r] & 0 \end{tikzcd}$$

Definition 2.57. The *m-Selmer group* of E/K is the subgroup of $H^1(G_{\bar{K}/K}, E[m])$ defined by

$$Sel_m(E/K) = ker\left\{H^1(G_{\bar{K}/K}, E[m]) \longrightarrow \prod_v H^1(G_{\bar{K}_v/K_v}, E)\right\},$$

and is finite. The group is effectively computable, certainly in theory and often in practice. The *Shafarevich-Tate group* of E/K is the subgroup of $H^1(G_{\bar{K}/K}, E)$ defined by

$$Ш(E/K) = ker\left\{H^1(G_{\bar{K}/K}, E)) \longrightarrow \textstyle\prod_v H^1(G_{\bar{K}_v/K_v}, E)\right\}.$$

$Ш(E/K)$ is the collection of elements of $WC(E/K)$ that becomes trivial in all completions of K. In other words, $Ш(E/K)$ consists of all homogeneous spaces of E, up to equivalence, which have points everywhere locally. The group $Ш(E/K)$ is conjecturally finite. We conclude this subsection with the following exact sequence between the m-Selmer group and the m-part of the Shafarevich Tate group of an elliptic curve.

$$0 \longrightarrow E(K)/mE(K) \longrightarrow \mathrm{Sel}_m(E/K) \longrightarrow Ш(E/K)[m] \longrightarrow 0.$$

Remark 4: We will compute the above groups when $m = 2$, called the 2-Selmer group and 2 -part of the Shafarevich-Tate group. As defined in the introduction, 2-Selmer rank of $E(K)$ be $s_2(E/K) = dim_{\mathbb{F}_2}Sel_2(E/K) - dim_{\mathbb{F}_2}E(K)[2]$. Let E/K be an elliptic curve with $E[2] \subset E(K)$, let $S \subset M_K$ be the set of places mentioned in Proposition 2.38 and let $K(S, 2)$ be as in Proposition 2.48. We choose a basis for $E[2]$ and use it to identify $E[2]$ with $\mu_\mathbf{2} \times \mu_\mathbf{2}$ as $G_{\bar{K}/K}$ -modules. Then

$$H^1(G_{\bar{K}/K}, E[2]; S) \cong K(S, 2) \times K(S, 2),$$

where this map uses the isomorphism $K^*/(K^*)^2 \xrightarrow{\sim} H^1(G_{\bar{K}/K}, \mu_{\mathbf{2}})$. The homogeneous space associated to a pair $(b_1, b_2) \in K(S,2) \times K(S,2)$ is the curve in $\mathbb{P}^3$ give by the equations in Proposition 2.48,

$$C : b_1 z_1^2 - b_2 z_2^2 = (e_2 - e_1) z_0^2, \ , \ b_1 z_1^2 - b_1 b_2 z_3^2 = (e_3 - e_1) z_0^2.$$

We need to check whether $C(K_v) \neq \phi$ for any pair (b_1, b_2) and any absolute value $v \in S$ to compute the $Sel_2(E/K)$.

We finish this section with the following results of Hasse, which gives a bound for the number of solutions of an elliptic curve over finite fields. This result is often used in literature and, indeed, in this thesis to compute the 2-Selmer rank of an elliptic curve.

Theorem 2.58. *(Hasse). Let E be an elliptic curve over $\mathbb{F}_q$. Then there exist complex numbers α and β with $|\alpha| = |\beta| = \sqrt{q}$ such that for each $k \in \mathbb{N}, \#E(\mathbb{F}_{q^k}) = 1 + q^k - \alpha^k - \beta^k$.*

Corollary 2.59. *(Hasse). For an elliptic curve E over $\mathbb{F}_q$, $|\#E(\mathbb{F}_q) - 1 - q| \leq 2\sqrt{q}$.*

More generally, For smooth projective curves defined over $\mathbb{F}_q$, the Hasse-Weil bound relates to the following result.

Theorem 2.60. *(Hasse-Weil bound) For a smooth projective curve C of genus g,*

$$|\#C(\mathbb{F}_q) - q - 1| \leq 2g\sqrt{q}.$$

2.5 Heronian Elliptic Curves

We have already formally defined the Heron triangle and the Heronian elliptic curves in the previous chapter. We now look into some of the already established results regarding these types of curves. For more details of the results in this section, one can see [17], [52]. We start with an example.

Example 2.3. *$n = 1$ is the area of a rational triangle with sides $\left(\frac{3}{2}, \frac{5}{3}, \frac{17}{6}\right)$. However, we have seen in the first chapter that 1 is not a congruent number.*

The following table in [17] gives us the explicit transformation from a Heron triangle to a Heronian elliptic curve and vice versa.

The following result, which is part of a work done by Goins and Maddox (see [17]), relates the area of isosceles Heron triangles and the congruent numbers, along with some more characterizations.

Result 2.5.1. Fix a positive integer n. Then the following are equivalent:
(i) n is the area of an isosceles triangle.

Table 2.1: Transformation between Heron triangle and Heronian elliptic curve

Triangle to Curve	Curve to Triangle
$n = \sqrt{s(s-a)(s-b)(s-c)}$	$E_{\tau,n} = y^2 = x(x-n\tau)(x+n\tau^{-1})$
$\tau = \dfrac{4n}{(a+b)^2-c^2}$	$\mathrm{a} = \dfrac{y}{x}$
$\mathrm{x} = \dfrac{(a+c)^2-b^2}{4}$	$b = n(\tau+\tau^{-1})\dfrac{x}{y}$
$y = a\dfrac{(a+c)^2-b^2}{4}$	$c = \dfrac{(x^2+n^2)}{y}$

(ii) $2n$ is a congruent number.

(iii) $E_{\tau,n}$ has a rational point of order 4 for some nonzero rational τ.

If there is a rational point that is not of order 2, then the Mordell-Weil group of the congruent number elliptic curve is infinite. However, in the case of Heronian elliptic curves, the existence of points of order different from 2 will not necessarily ensure the Mordell-Weil group is infinite. For example, such a situation arises when the triangle is an isosceles Heron triangle. We conclude this section by collecting a few observations about congruent number elliptic curves and Heronian elliptic curves.

Table 2.2: An analogy between Heronian elliptic curves and congruent number elliptic curves

	Heronian elliptic curve	congruent number elliptic curve
$E_{\tau,n}$	$y^2 = x(x-n\tau)(x+n\tau^{-1})$	$y^2 = x(x-n)(x+n)$
Δ	$16n^2(\tau+\tau^{-1})^2$	$64n^2$
E_{tors}	$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ or $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$	$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$

Chapter 3

Heronian Elliptic Curves Associated to Triangles of Odd Area

*This chapter contains the following articles:

Ghale Vinodkumar, Das Shamik, Chakraborty Debopam; “A Heron triangle and a Diophantine equation”, *Periodica Mathematica Hungarica* 2 (2022) 530-537.

Chakraborty Debopam, Ghale Vinodkumar; “Size of the 2-Selmer groups for Heronian elliptic curves” *European Journal of Mathematics* (2023) (Accepted).

In this chapter, we look into the Mordell-Weil group structure of the Heronian elliptic curves associated with the Heron triangles of odd areas. This section primarily includes explicit 2-descent methods for different Heronian elliptic curves to look into their corresponding 2-Selmer ranks, which act as an upper bound of the Mordell-Weil ranks. We start with the particular case when the area of the Heron triangle under consideration is an odd prime and then generalize the result later in this chapter.

3.1 A Special Case of $n = p \not\equiv 1 \pmod 8$:

Given any integer n, the existence of infinitely many Heron triangles with the area n has been studied in [17], [44]. The question becomes interesting when we fix an angle θ and study the associated Heronian elliptic curve, its rank, and Selmer rank, which, as mentioned before, acts as an upper bound for Mordell-Weil rank and is certainly computable in theory and often in practice. We first consider the case of Heronian elliptic curves associated with the Heron triangles with area $n = p \equiv 3, 5, 7 \pmod 8$. We first state the following result regarding the rank of the aforementioned Heron triangles. We prove the result in the upcoming sections via a complete 2-descent. Throughout this chapter, we denote a Heronian elliptic curve associated with a Heron triangle of area n and one of the angles θ such that $\tan\frac{\theta}{2} = \tau$, by E.

Theorem 3.1. *Let p be a prime such that $p^2 + 1 = 2q$ for a prime q. Then the Heronian elliptic curve $E : y^2 = x(x-1)(x+p^2)$ associated with Heron triangles of area p and $\tau = p^{-1}$ for one of the angles θ has rank zero for $n = p \equiv 5 \pmod 8$. Hence, there exists no Heron triangle with area p and an angle θ such that $\tan\frac{\theta}{2} = \frac{1}{p}$. Moreover, E has rank at most one if $n = p \equiv 3, 7 \pmod 8$ and $\tau = \frac{1}{p}$.*

Assuming the finiteness of the Shafarevich-Tate group, we give the precise rank for the cases $p \equiv 3, 7 \pmod 8$ in the later part of this chapter. We start with a brief introduction to this set of Heron triangles. We first recall that the Heronian elliptic curve associated with the Heron triangle of area n and an angle θ is

$$E : y^2 = x(x - n\tau)(x + n\tau^{-1})$$

where τ denotes $\tan\frac{\theta}{2}$. Now we can identify the Heronian elliptic curve with the given set of Heron triangles in Theorem 3.1 as

$$E : y^2 = x(x-1)(x+p^2) \text{ with } \tau = p^{-1}.$$

Throughout this section, we consider $\tau = p^{-1}$. Let S be the set consisting of all finite places at which E has bad reductions, infinite places, and the prime 2. By the method of 2-descent, as explained in Proposition 2.48, there exists an injective homomorphism β such that

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

defined by

$$\beta(x,y) = \begin{cases} (x, x-1) & \text{if } x \neq 0, 1, \\ (-1,-1) & \text{if } x = 0, \\ (1, 2q) & \text{if } x = 1, \\ (1,1) & \text{if } \ P = O, \end{cases}$$

where

$$\begin{aligned} \mathbb{Q}(S,2) &= \left\{ b \in \mathbb{Q}^*/(\mathbb{Q}^*)^2 : v_l(b) \equiv 0 \pmod 2 \text{ for } l \neq 2, p, q \right\} \\ &= \left\{ \pm 1, \pm 2, \pm p, \pm q, \pm 2p, \pm 2q, \pm pq, \pm 2pq \right\}, \end{aligned}$$

and O denotes the *point of infinity* $[0,1,0]$ in the projective plane that acts as the identity element in the group $E(\mathbb{Q})$. 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 $O, (0,0), (1,0)$, 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

$$b_1 z_1^2 - b_2 z_2^2 = 1, \tag{3.1.1}$$

$$b_1 z_1^2 - b_1 b_2 z_3^2 = -p^2, \tag{3.1.2}$$

have a solution $(z_1, z_2, z_3) \in \mathbb{Q}^* \times \mathbb{Q}^* \times \mathbb{Q}$. If (z_1, z_2, z_3) is solution to the equations (3.1.1) and (3.1.2), then the pre-image $P = (x,y) \in E(\mathbb{Q})$ of a point (b_1, b_2) under the map b is given by $x = b_1 z_1^2$ and $y = b_1 b_2 z_1 z_2 z_3$. We note that $\# E(\mathbb{Q})/2E(\mathbb{Q}) = 2^{2+r(E/\mathbb{Q})}$, where $r(E/\mathbb{Q})$ is the Mordell-Weil rank of E.

Remark 5: The brief plan for the proof of Theorem 3.1 is as follows. We first show that the torsion group of the elliptic curve mentioned in the theorem is isomorphic to $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. We note that the existence of a $\mathbb{Q}$-rational (simply rational) solution for the homogeneous space corresponding to (b_1, b_2), defined by (3.1.1) and (3.1.2), identifies them inside the trivial class in the Weil-chatelet group. The method adopted for finding such (b_1, b_2) is as follows.

(i) First, narrow down the choices of (b_1, b_2) for which the corresponding homogeneous spaces given by (3.1.1) and (3.1.2) have rational solutions. This is done by carefully removing (b_1, b_2) with corresponding homogeneous space missing local solutions for some prime p. In the case $n = p \equiv 5 \pmod 8$, a method like this essentially removes all possible pairs of (b_1, b_2), which from the Proposition 2.48 then implies $E(\mathbb{Q})/2E(\mathbb{Q})$ only contains the four torsion points, implying the rank of the elliptic curve to be exactly zero.

(ii) For the case $n = p \equiv 3, 7 \pmod 8$, only one $(b_1, b_2) = (1, q)$ remains that can not be removed by the calculation mentioned above. This (b_1, b_2) remains a possible element for the 2-Selmer group (if one could show the local solutions exist for the corresponding homogeneous spaces at every prime), or for the Mordell-Weil group (in case the rational solution exist for the corresponding homogeneous space). As we fail to compute that, we stop at giving the upper bound for the Mordell-Weil rank as one in this case.

Remark 6: We also note that the idea behind the calculation of various Selmer groups in this chapter and later chapters depends heavily on the process mentioned above. With different curves and more general n with arbitrary prime factors, the calculation varies significantly, sometimes (in Chapter 5) involving methods from the ring of integers of ideal class groups. Still, the general idea remains very similar to the one mentioned above.

3.1.1 Computing the Torsion Group of E :

Here, we explicitly discuss a method for computing the torsion group of elliptic curves. We note that for an elliptic curve given by an equation of the form $y^2 = x^3 + Ax + B$, one may consider the set $\tilde{E}(\mathbb{F}_p)$ of points on the curve with coordinates in $\mathbb{F}_p$. For such points, we have the following result (see [46], Section VII.3, Proposition 3.1):

Theorem 3.2. *Let $E/\mathbb{Q}$ be an elliptic curve and p be a prime of good reduction. Then $E(\mathbb{Q})_{tors}$ injects into $\tilde{E}(\mathbb{F}_p)$.*

By applying the above theorem with several small primes which do not divide Δ, one can get an effective bound on the size of the torsion subgroup. We first note that for $E : y^2 = x(x-1)(x+p^2)$, $\Delta = 64p^4q^2$. Now for $p \neq 3$, we reduce $E : y^2 = x(x-1)(x+p^2)$ to $\tilde{E} \pmod 3$ while simultaneously noticing the fact $q \not\equiv 0 \pmod 3$, we find that $|\tilde{E}(\mathbb{F}_3)| = 4$. Since $E[2] \subseteq E(\mathbb{Q})_{\text{tors}}$ and $E(\mathbb{Q})_{\text{tors}}$ injects into $\tilde{E}(\mathbb{F}_3)$ for any elliptic curve E, one can see that $E(\mathbb{Q})_{\text{tors}} = E[2]$ whenever $p \neq 3$. On the other hand, For $p = 3$ a similar approach shows that $\tilde{E}(\mathbb{Q})_{\text{tors}} \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. Hence we obtain the following isomorphism:

$$E(\mathbb{Q})_{\text{tors}} \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}.$$

3.1.2 Bounding the Mordell-Weil Rank of E for $p \not\equiv 1 \pmod 8$:

We begin with the following result regarding the modifications of the equations (3.1.1) and (3.1.2), which help us to look into nonzero integer solutions of equations rather than nonzero rationals.

Lemma 3.3. *Let $(b_1, b_2) \in \mathbb{Q}(S, 2) \times \mathbb{Q}(S, 2)$ be a pair that is not in the image of points of $E(\mathbb{Q})_{\text{tors}}$. 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*

$$b_1r_1^2 - b_2r_2^2 = s^2, \tag{3.1.3}$$

$$b_1r_1^2 - b_1b_2r_3^2 = -p^2s^2, \tag{3.1.4}$$

have a solution $(r_1, r_2, r_3, s) \in \mathbb{Z}^* \times \mathbb{Z}^* \times \mathbb{Z}^* \times \mathbb{Z}^*$ *with* $\gcd(r_i, s) = 1$, $i \in \{1, 2, 3\}$.

Proof. Assume $z_i = \dfrac{r_i}{s_i}$ where $r_i, s_i \in \mathbb{Z}$ and $\gcd(r_i, s_i) = 1$ for $i \in \{1, 2, 3\}$. The result follows immediately if one assumes $\gcd(b_1, s_1) = \gcd(b_2, s_2) = \gcd(b_1b_2, s_3) = 1$ in addition. In case the additional assumption of $\gcd(b_1, s_1) = \gcd(b_2, s_2) = \gcd(b_1b_2, s_3) = 1$ is not true, a simple calculation for each of the three cases here will yield to a contradiction. We show proof for one of those three cases; the other two follow a similar approach toward their solution. If $\gcd(b_1, s_1) \neq 1$ then there exists a prime number t_1 such that $t_1|b_1$ and $t_1|s_1$. Now, from (3.1.1), we have $r_1^2s_2^2 \equiv 0 \pmod{t_1}$ as b_1 is square-free. This in turn implies that $s_2 \equiv 0 \pmod{t_1}$ as $\gcd(r_1, s_1) = 1$ and $t_1|s_1$. If $t_1 \nmid b_2$, then $b_1r_1^2s_2^2$ is divisible by an odd power of t_1 whereas $b_2r_2^2s_1^2 + s_1^2s_2^2$ is divisible by an even power of t_1, a contradiction because $b_1r_1^2s_2^2 = b_2r_2^2s_1^2 + s_1^2s_2^2$. Similarly if $t_1|b_2$, then an odd power of t_1 divides $b_1r_1^2s_2^2 - b_2r_2^2s_1^2$ whereas an even power of t_1 divides $s_1^2s_2^2$, a contradiction again. □

In total there are 256 different possibilities of $(b_1, b_2) \in \mathbb{Q}(S, 2) \times \mathbb{Q}(S, 2)$. We now show that it is sufficient to focus only on 16 of those pairs. Before we state our next result, for the sake of brevity, we will assume A is the image of the set $E(\mathbb{Q})_{\text{tors}}$ under the map β, that is,

$$A = \{(-1, -1), (1, 2q), (1, 1), (-1, -2q)\}.$$

Lemma 3.4. *Suppose* $(b_1, b_2) \in \mathbb{Q}(S, 2) \times \mathbb{Q}(S, 2)$ *such that* (b_1, b_2) *is the image of a point in the group* $E(\mathbb{Q})/2E(\mathbb{Q})$. *Then*
(i) $b_1b_2 > 0$.
(ii) b_1 *is odd.*
(iii) If $(b_1, b_2) \in \operatorname{Im}(\beta)$ *modulo* A, *then* $b_i \in \{1, p, q, pq\}$ *for* $i = 1, 2$.

Proof. Let us assume $b_1b_2 < 0$. If $b_1 > 0$ and $b_2 < 0$ then (3.1.4) implies $0 < b_1r_1^2 - b_1b_2r_3^2 = -p^2s^2$, a contradiction. Similarly if $b_1 < 0$ and $b_2 > 0$ then (3.1.3) implies $s^2 = b_1r_1^2 - b_2r_2^2 < 0$, a contradiction again. This immediately proves (i).
We now show that b_1 has to be odd. Since p is an odd prime, from (3.1.4) one can get $p^2s^2 = b_1b_2r_3^2 - b_1r_1^2 \equiv 0 \pmod 2$ which implies $s \equiv 0 \pmod 2$ if b_1 is even. Then from (3.1.3) we get, $b_1r_1^2 - b_2r_2^2 = s^2 \equiv 0 \pmod 4$, which implies $b_2 \equiv b_1 \equiv 0 \pmod 2$. This is because $\gcd(r_1, s) = 1 = \gcd(r_2, s)$ and $s \equiv 0 \pmod 2$. So, $r_1 \equiv r_2 \equiv 1 \pmod 2$. Now from (3.1.4) we

get,

$$b_1 r_1^2 = b_1 b_2 r_3^2 - p^2 s^2 \equiv 0 \pmod 4 \text{ and hence } r_1 \equiv 0 \pmod 2$$

as b_1 is square-free. This is a contradiction as otherwise $r_1 \equiv 0 \equiv 1 \pmod 2$. Hence, $b_1 \not\equiv 0 \pmod 2$ and the assertion of part *(ii)* holds.

Now for part *(iii)*, using the fact that β is a homomorphism, we can immediately say that any pair (b_1, b_2) belongs to $\mathrm{Im}(\beta)$ if and only if $(b_1, b_2) \times (a_1, a_2) = (a_1 b_1, a_2 b_2) \in \mathrm{Im}(\beta)$ where $(a_1, a_2) \in A$. Hence without the loss of generality, one can only focus on examining the possibility of $(b_1, b_2) \in \mathrm{Im}(\beta)$ where both b_1 and b_2 belong to $\mathrm{Im}(\beta)/A = \{1, p, q, pq\}$. This proves the statement of part *(iii)*. □

We now systematically look into the rest of the sixteen possibilities for (b_1, b_2) as potential image points under the map β. The next result shows there will be only one point to be concerned with.

Lemma 3.5. *Let* (b_1, b_2) *be a pair such that* $b_i \in \{1, p, q, pq\}$ *for* $i = 1, 2$. *If* $(b_1, b_2) \neq (1, q)$ *then* $(b_1, b_2) \notin \mathrm{Im}(\beta)$ *whenever* $p \equiv 5 \pmod 8$.

Proof. Suppose $\gcd(b_1, b_2) \neq 1$ for some $(b_1, b_2) \in \mathrm{Im}(\beta)$. Then $\gcd(b_1, b_2)$ is p, q or pq. If p divides $\gcd(b_1, b_2)$ then $s \equiv 0 \pmod p$ from (3.1.3). Also from (3.1.4), one can observe that $b_1 b_2 r_3^2 - p^2 s^2 = b_1 r_1^2 \equiv 0 \pmod{p^2}$. Hence, $r_1 \equiv 0 \pmod p$ as b_1 is square-free. This leads us to a contradiction as then p divides $\gcd(r_1, s) = 1$. So $(b_1, b_2) \notin \mathrm{Im}(\beta)$ if $\gcd(b_1, b_2) = p$ or pq. A very similar argument proves that q cannot also divide $\gcd(b_1, b_2)$ if $(b_1, b_2) \in \mathrm{Im}(\beta)$. So $(b_1, b_2) \in \mathrm{Im}(\beta)$ implies that $\gcd(b_1, b_2) = 1$. Now we are left with eight possible pairs of (b_1, b_2), i.e., $(1, p), (1, q), (1, pq), (p, 1), (p, q), (q, 1), (q, p)$ and $(pq, 1)$ (ignoring $(b_1, b_2) = (1, 1)$ which is the image of O under the map β).

If $(b_1, b_2) = (1, pq) \in \mathrm{Im}(\beta)$ then from (3.1.4), one gets that $pqr_3^2 - p^2 s^2 = r_1^2 \equiv 0 \pmod p$. But then (3.1.3) implies p divides $r_1^2 - pqr_2^2 = s^2$, a contradiction as $\gcd(r_1, s) = 1$. So $(1, pq) \notin \mathrm{Im}(\beta)$. A very similar argument shows that $(pq, 1) \notin \mathrm{Im}(\beta)$ either.

Now $(p, q) \in \mathrm{Im}(\beta)$ implies $pr_1^2 - pqr_3^2 = -p^2 s^2$ from (3.1.4). This implies that $2r_1^2 \equiv 2qr_3^2 \equiv r_3^2 \pmod p$, hence either $\left(\frac{2}{p}\right) = 1$ or $r_1 \equiv r_3 \equiv 0 \pmod p$. But $\left(\frac{2}{p}\right) = -1$ as $p \equiv 5 \pmod 8$. Also from (3.1.3), $r_1 \equiv 0 \pmod p$ implies $-qr_2^2 \equiv s^2 \pmod p$. Multiplying both sides by 2, we get $r_2^2 = -2s^2 \pmod p$ as $2q = p^2 + 1$. This implies that either $r \equiv s \equiv 0 \pmod p$ or $\left(\frac{-2}{p}\right) = 1$. But $\left(\frac{-2}{p}\right) = -1$ as $p \equiv 5 \pmod 8$. Hence $r_2 \equiv s \equiv 0 \pmod p$, a contradiction again as $\gcd(r_2, s) = 1$. So, $(p, q) \notin \mathrm{Im}(\beta)$.

If $(q, p) \in \mathrm{Im}(\beta)$, then from (3.1.4), we have $qr_1^2 - pqr_3^2 = -p^2 s^2$ which implies $r_1^2 \equiv 0 \pmod p$. This leads to a contradiction because from (3.1.3), $s^2 = qr_1^2 - pr_2^2$ implies $s \equiv 0 \pmod p$, hence p divides both r_1 and s. So $(q, p) \notin \mathrm{Im}(\beta)$.

Now, we are left with only four possible image points for the homomorphism β. Those points are $(p, 1)$ $(1, p), (q, 1)$ and $(1, q)$.

$(q, 1) \notin \mathrm{Im}(\beta)$ because otherwise $s \equiv 0 \pmod q$ from (3.1.4) and then $r_2 \equiv 0 \pmod q$ from (3.1.3).

This leads to a contradiction as $\gcd(r_2, s) = 1$. Now $(1, p) \in \mathrm{Im}(\beta)$ implies that $r_1 \equiv 0 \pmod{p}$ from (3.1.4). Then from (3.1.3), one can observe that $r_1^2 - pr_2^2 = s_2^2 \equiv 0 \pmod{p}$, hence $s \equiv 0 \pmod{p}$, a contradiction, as $(r_1, s) = 1$. Similarly $(p, 1) \in \mathrm{Im}(\beta)$ implies $pr_3^2 - r_2^2 = 2qs^2$ which implies $pr_3^2 \equiv r_2^2 \pmod{q}$ from (3.1.3) and (3.1.4). This leads to a contradiction if $r_2 \equiv r_3 \not\equiv 0 \pmod{q}$ as $\left(\frac{p}{q}\right) \neq 1$ from the Gauss' quadratic reciprocity law and the fact $p^2 + 1 = 2q$. But if $r_2 \equiv r_3 \equiv 0 \pmod{q}$, then again from the above equation, $2qs^2 = pr_3^2 - r_2^2 \equiv 0 \pmod{q^2}$ which implies $s \equiv 0 \pmod{q}$, a contradiction as $\gcd(r_2, s) = 1$. Hence $(1, p), (p, 1) \notin \mathrm{Im}(\beta)$ and the result follows. □

We have excluded the possibility of every non-trivial pair (b_1, b_2) being in the image of the homomorphism β, apart from the point $(1, q)$. The following lemma now essentially proves Theorem 3.1 for $p \equiv 5 \pmod{8}$.

Lemma 3.6. *If* $p \equiv 5 \pmod{8}$ *then* $(1, q) \notin \mathrm{Im}(\beta)$.

Proof. From (3.1.3) and (3.1.4) we know that if $(1, q) \in \mathrm{Im}(\beta)$, then

$$r_1^2 - qr_2^2 = s^2, \tag{3.1.5}$$
$$r_1^2 - qr_3^2 = -p^2s^2, \tag{3.1.6}$$

for some $(r_1, r_2, r_3, s) \in \mathbb{Z}^* \times \mathbb{Z}^* \times \mathbb{Z}^* \times \mathbb{Z}^*$. From (3.1.6), we get that either $\left(\frac{q}{p}\right) = 1$ or $r_1 \equiv r_3 \equiv 0 \pmod{p}$. But $p \equiv 5 \pmod{8}$ and $2q = p^2 + 1$ implies that $\left(\frac{q}{p}\right) \neq 1$ and hence $r_1 \equiv r_3 \equiv 0 \pmod{p}$. But from (3.1.5), $r_1 \equiv 0 \pmod{p}$ implies either $\left(\frac{-q}{p}\right) = 1 \pmod{p}$ or $r_2 \equiv s \equiv 0 \pmod{p}$, a contradiction in either way as $\left(\frac{-q}{p}\right) \neq 1$ and $\gcd(r_2, s) = 1$. Hence $(1, q) \notin \mathrm{Im}(\beta)$. □

For $p \equiv 3, 7 \pmod{8}$, we first observe that the same proof for $p \equiv 5 \pmod{8}$ works, except for the image points $(b_1, b_2) = (1, q), (p, q)$ and $(p, 1)$ where we have used the fact $p \equiv 5 \pmod{8}$. We now prove the main result by noticing that two of those three points can not appear as image points even for the cases $p \equiv 3, 7 \pmod{8}$.

Proof of Theorem 3.1: We can now conclude the proof of Theorem 3.1 by proving that $(p, q), (p, 1) \notin \mathrm{Im}(\beta)$ if $p \equiv 3 \pmod{4}$. First, let us suppose that $p \equiv 3 \pmod{8}$. Then $(p, q) \notin \mathrm{Im}(\beta)$ as $(p, q) \in \mathrm{Im}(\beta)$ implies $pr_1^2 - pqr_3^2 = -p^2s^2$ from (3.1.4). This implies that $2r_1^2 \equiv 2qr_3^2 \equiv r_3^2 \pmod{p}$, hence either $\left(\frac{2}{p}\right) = 1$ or $r_1 \equiv r_3 \equiv 0 \pmod{p}$, a contradiction in both cases as $\left(\frac{2}{p}\right) = -1$ whenever $p \equiv 3 \pmod{8}$ and $r_1 \equiv r_3 \equiv 0 \pmod{p}$ implies that $-p^2s^2 \equiv 0 \pmod{p^3}$ from (3.1.4) which consequentially implies $s \equiv 0 \pmod{p}$, a contradiction as $\gcd(r_1, s) = 1$. Similarly, when $p \equiv 7 \pmod{8}$, from (3.1.3), one gets $r_2^2 \equiv -2s^2 \pmod{p}$ which implies $r_2 \equiv s \equiv 0 \pmod{p}$ or $\left(\frac{-2}{p}\right) = 1$, contradiction either way as $\gcd(r_2, s) = 1$ and $\left(\frac{-2}{p}\right) = -1$ when $p \equiv 7 \pmod{8}$. Hence $(p, q) \notin \mathrm{Im}(\beta)$ if $p \equiv 3 \pmod{4}$.

Now $(p,1) \in \mathrm{Im}(\beta)$ implies that $pr_1^2 - r_2^2 = s^2$ from (3.1.3). This in turn implies $r_2^2 \equiv -s^2 \pmod{p}$. Hence either $\left(\frac{-1}{p}\right) = 1$ or $r_2 \equiv s \equiv 0 \pmod{p}$, a contradiction either way as $p \equiv 3 \pmod{4}$ and $\gcd(r_2, s) = 1$. Hence $(p,1) \notin \mathrm{Im}(\beta)$ when $p \equiv 3 \pmod{4}$. This implies $(1,q)$ is the only possible image point (modulo the image of the torsion group). Using Lemma 3.6, we can now conclude the proof. □

It is now evident that the rank of the elliptic curve $E(\mathbb{Q})$ is zero when $p \equiv 5 \pmod{8}$. The torsion group is $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ or $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$, triangle being isosceles in the latter case. So unlike the non-congruent numbers, we need to consider other orientations of the triangle and see the rank of corresponding elliptic curves to conclude that there is no Heron triangle.

For the case of non-isosceles Heron triangle, we note that the torsion group of $(E)_{tors} = \{(0,0),(0,1),(0,-p^2),O\}$ and have one-one correspondence between sides of the triangle and points $y \neq 0$ on the elliptic curve. So above argument tells us that we do not have a non-isosceles Heron triangle.

For the isosceles triangle case, we know if p is the area of an isosceles Heron triangle, then $2p$ is a congruent number(see [17]). But $2p$ is the non-congruent number when $p \equiv 5 \pmod{8}$ (see [15]). This implies p can not be an area of an isosceles Heron triangle. Hence there is no Heron triangle with area p and an angle θ such that $\tau = \dfrac{1}{p}$ for $p \equiv 5 \pmod{8}$.

TABLE 3.1: Examples for area $p \equiv 3, 5, 7 \pmod{8}$, $\tau = \frac{1}{p}$ with $p^2 + 1 = 2q$ and corresponding rank distribution

p	$p \pmod{8}$	q	$r(E/\mathbb{Q})$	p	$p \pmod{8}$	q	$r(E/\mathbb{Q})$
3	3	5	1	131	3	8581	1
5	5	13	0	139	3	9661	1
11	3	61	1	199	7	19801	1
19	3	181	1	271	7	36721	1
29	5	421	0	379	3	71821	1
59	3	1741	1	571	3	163021	1
61	5	1861	0	631	7	199081	1
71	7	2521	1	739	3	273061	1

We note that we have not included the case $p \equiv 1 \pmod{8}$ here. This is because we discuss in detail the 2-Selmer group structure and the 2-part of the Shafarevich-Tate group of the corresponding Heronian elliptic curves through the solvability of certain Diophantine equations in Chapter 5.2. We enlist a few examples above of the curve $E : y^2 = x(x-1)(x+p^2)$. The rank is verified at `http://magma.maths.usyd.edu.au/calc/`.

3.2 A Generalization

Now we give an explicit group structure for the 2-Selmer group of Heronian elliptic curve $E : y^2 = x(x-1)(x+n^2)$ associated with a Heron triangle of area n with θ as an angle such that $\tau = \tan\frac{\theta}{2} = n^{-1}$ and $n^2+1 = 2q$ for some prime q. For positive integers k and n, we define $\Omega_{k,n} = \#\{p\ : n \equiv 0 \pmod{p} \text{ and } p \equiv k \pmod{8}\}$. We now state the main result of this section below.

Theorem 3.7. *For a square-free integer n such that $n^2+1 = 2q$ for some prime q, let $E : y^2 = x(x-1)(x+n^2)$ denote the Heronian elliptic curve associated with the non-isosceles Heron triangle of area n and an angle θ such that $\tan(\frac{\theta}{2}) = n^{-1}$. Then,*
(i) $Sel_2(E/\mathbb{Q}) \cong (\mathbb{Z}/2\mathbb{Z})^{\Omega_{1,n}+1}$ if $\Omega_{5,n} = 0$.
(ii) $Sel_2(E/\mathbb{Q}) \cong (\mathbb{Z}/2\mathbb{Z})^{\left(\Omega_{1,n}+\frac{\Omega_{5,n}(\Omega_{5,n}-1)}{2}\right)}$ if $\Omega_{5,n} \neq 0$.

We note that the above results can be used as a tool to compute the Heronian elliptic curve with arbitrarily large 2-Selmer rank. This is because the 2-Selmer rank here is directly related to the number of prime factors of n of the form $1, 5$ modulo 8.

3.2.1 Bounding the 2-Selmer Rank of E :

Let $n = \prod_i p_i$ where p_i's are distinct odd primes. Then, we define

$$\begin{aligned}\mathbb{Q}(S,2) &= \left\{b \in \mathbb{Q}^*/(\mathbb{Q}^*)^2 : v_l(b) \equiv 0 \pmod{2} \text{ for all primes } l \notin S\right\}\\ &= \langle \pm 2,\ \pm p_i,\ \pm q : 2^2 = p_i^2 = q^2 = 1\rangle.\end{aligned}$$

As described in the previous section, by the method of 2-descent (2.48), there exists an injective homomorphism

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

defined by

$$\beta(x,y) = \begin{cases} (x, x-1) & \text{if } x \neq 0, 1,\\ (-1,-1) & \text{if } x = 0,\\ (1, 2q) & \text{if } x = 1,\\ (1,1) & \text{if } x = \infty,\ \text{i.e., if } (x,y) = O,\end{cases}$$

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 $O, (0,0), (1,0)$, 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

$$b_1 z_1^2 - b_2 z_2^2 = 1, \tag{3.2.1}$$

$$b_1 z_1^2 - b_1 b_2 z_3^2 = -n^2, \tag{3.2.2}$$

have a solution $(z_1, z_2, z_3) \in \mathbb{Q}^* \times \mathbb{Q}^* \times \mathbb{Q}$. As mentioned previously, under the 2-descent method, each element (b_1, b_2) in $\mathrm{Sel}_2(E/\mathbb{Q})$ corresponds to the homogeneous space given by (3.2.1) and (3.2.2) with local solutions everywhere.

b_1, b_2 are square-free integers whose only prime factors are $2, q$ and prime factors of n. The image of $E(\mathbb{Q})_{\text{tors}}$ under the 2-descent map is $\{(1,1), (1,2q), (-1,-1), (-1,-2q)\}$. We start with the following result regarding l-adic solutions of the homogeneous space given by (3.2.1) and (3.2.2).

Lemma 3.8. *Let (z_1, z_2, z_3) be a solution to the homogeneous space given by equations (3.2.1) and (3.2.2). Then for each prime $l < \infty$ and all $i \in \{1, 2, 3\}$, either $v_l(z_i) \geq 0$ or $v_l(z_i) = -k$ for some positive 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 (3.2.1) one can get that

$$b_1 u_1^2 - b_2 u_2^2 l^{2(k_2 - k_1)} = l^{-2k_1}.$$

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 (3.2.1) we get

$$b_1 u_1^2 l^{2(k_1 - k_2)} - b_2 u_2^2 = l^{-2k_2},$$

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 (3.2.2), we have

$$b_1 u_1^2 - b_1 b_2 u_3^2 l^{2(k_3 - k_1)} = -n^2 \cdot l^{-2k_1}.$$

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

$$b_1 u_1^2 l^{2(k_1 - k_3)} - b_1 b_2 u_3^2 = -n^2 \cdot l^{-2k_3}, \tag{3.2.3}$$

which implies l^2 must divide $b_1 b_2$, i.e., $l = 2, p_i$ or q. If $l = p_i$, then from (3.2.3) we arrive at the contradiction that p^3 divides $b_1 b_2$ whereas b_1 and b_2 are square-free. For $l = 2$ and q, one can notice from (3.2.2) that if $k_3 \leq -2$, then l^3 divides $b_1 b_2$, a contradiction again. This in turn implies $k_3 = -1$ and hence $k_1 \geq 0$ which contradicts the assumption that $k_1 < 0$. Hence

$k_1 < 0 \implies k_3 = k_1$.

Now, suppose $k_3 < 0$. If $k_1 < 0$, then from the previous part we already established $k_1 = k_2 = k_3 = -k$ for some positive integer k. So without loss of generality, we can assume $k_1 \geq k_3$. If $k_3 < k_1$ and $k_3 < 0$, then as mentioned previously in this proof, one can get that $b_1b_2 \equiv 0 \pmod{l^2}$ and $l = 2$ or q. Now we subtract (3.2.2) from (3.2.1) and observe that

$$b_1b_2u_3^2 - b_2u_2^2l^{2(k_2-k_3)} = 2q \cdot l^{-2k_3}.$$

If $k_2 > k_3$, we get a contradiction that l^3 divides b_1b_2 for $l = 2, q$. Therefore, $k_2 \leq k_3 < 0$ but then by the first part, $k_1 = k_2 \leq k_3$, a contradiction to the assumption $k_1 > k_3$. Hence $k_3 < 0 \implies k_1 = k_3$. Together, now we obtain $k_1 = k_2 = k_3 = -k < 0$ for some integer k if $k_1 < 0$ or $k_2 < 0$ or $k_3 < 0$. □

Noting that we will only look into possible $(b_1, b_2) \in \text{Sel}_2(E/\mathbb{Q})/Im(E(\mathbb{Q})_{\text{tors}})$ under the 2-descent map, without loss of generality, we fix the following observations.

i) $b_1 > 0, b_2 > 0$ always (due to $l = \infty$).

ii) b_2 is odd.

Lemma 3.9. *Let $(b_1, b_2) \in Sel_2(E/\mathbb{Q})$. Then for an arbitrary prime p,*

(i) $b_1 \equiv 0 \pmod p \implies p \equiv 1, 5 \pmod 8$.

(ii) $b_2 \in \{1, q\}$. Moreover, $n \equiv 0 \pmod p$, $p \equiv 5 \pmod 8 \implies (1, q) \notin Sel_2(E/\mathbb{Q})$.

(iii) The number of prime factors of b_1 of the form $8k + 5$ must always be even.

Proof. We begin with noticing that $b_1 \not\equiv 0 \pmod q$. Otherwise, from (3.2.2) and (3.2.1), $v_q(z_i) \geq 0 \implies -n^2 \equiv 0 \pmod q$ and, $v_q(z_i) = -k \implies b_1 \equiv 0 \pmod{q^2}$, contradiction in each case. This implies no q-adic solution for the homogeneous space associated with (b_1, b_2) when q divides b_1.

A very similar argument as above shows that b_1 is odd if $(b_1, b_2) \in \text{Sel}_2(E/\mathbb{Q})$. As otherwise, $v_2(z_i) \geq 0$ implies 2 divides $-n^2$ from (3.2.2) and $v_2(z_i) = -k$ leads to b_2 as even from (3.2.1), both contradictions from our assumptions of n and b_2.

We now note that $b_2 \not\equiv 0 \pmod p$ if p divides n. If $v_p(z_i) \geq 0$ then subtracting (3.2.2) from (3.2.1), one can get $2q \equiv 0 \pmod p$, a contradiction. Otherwise, from (3.2.2), we get that p^2 divides b_1, a contradiction. This, along with the assumptions above, narrows down the choices of $b_2 \in \{1, q\}$.

Now $b_1 \equiv 0 \pmod p$ implies p divides n. We note that possible elements of $\text{Sel}_2(E/\mathbb{Q})$ now looks like $(b_1, 1)$ or (b_1, q).

If $p \equiv 3, 7 \pmod 8$, we notice that the homogeneous space corresponding to $(b_1, 1)$ has no p-adic solution. This is because if $p \equiv 3, 7 \pmod 8$ then depending on $v_p(z_i)$, from (3.2.1), either $\left(\frac{-1}{p}\right) = 1$, or $b_2 \equiv 0 \pmod p$, contradiction either way.

Now for homogeneous spaces corresponding to (b_1, q), we first note that $v_p(z_i) = -k \implies q \equiv 0$

$\pmod p$, a contradiction. For $v_p(z_i) \geq 0$, subtracting (3.2.2) from (3.2.1), we get that $\left(\frac{-2}{p}\right) = 1$ which implies $p \not\equiv 7 \pmod 8$. For $p \equiv 3 \pmod 8$, we note that $\left(\frac{q}{p}\right) = -1$ which contradicts (3.2.1). This concludes the proof of part (i).

To conclude the proof of part (ii), we show that whenever n has a prime factor $p \equiv 5 \pmod 8$, the homogeneous space for $(1, q)$ has no p-adic solution. From (3.2.2), we get $\left(\frac{q}{p}\right) = 1$, a contradiction as $\left(\frac{q}{p}\right) = -1$ here.

For part (iii), we notice that the only possible element in the 2-Selmer group is of the form $(b_1, 1)$ with $p \equiv 1, 5 \pmod 8$ its only prime divisors where p varies over all divisors of n. For $p \equiv 5 \pmod 8$, we note that $\left(\frac{p}{q}\right) = -1$ whereas $\left(\frac{p}{q}\right) = 1$ whenever $p \equiv 1 \pmod 8$. Noting that only factors of b_1 are now primes $p \equiv 1, 5 \pmod 8$, one can get that $\left(\frac{b_1}{q}\right) = 1$ if there are even number of factors of $5 \pmod 8$, else $\left(\frac{b_1}{q}\right) = -1$. The result now follows from (3.2.1) and (3.2.2), observing the fact that $\left(\frac{b_1}{q}\right) = 1$ is a necessary condition for the homogeneous space corresponding to $(b_1, 1)$ to have a q-adic solution. □

3.2.2 Everywhere Local Solution

We prove that the homogeneous spaces corresponding to $(p, 1)$ and $(1, q)$ have local solutions everywhere where p is any prime factor of n such that $p \equiv 1 \pmod 8$. We use Hensel's lemma to lift a simple root of a polynomial $f(x)$ modulo a prime l to a solution for $f(x)$ in $\mathbb{Z}_l$. Let C be the homogeneous space given by (3.2.1) and (3.2.2) corresponding to the pairs $(p, 1)$ and $(1, q)$. An application of smoothness of C, the degree-genus formula, and the Hasse-Weil bound give the following.

(i) For $l \geq 5,\ l \neq t$ where $t \equiv 1, 5 \pmod 8$ and t divides n, C is a homogeneous space of genus 1 corresponding to $(p, 1)$ or $(p_1p_2, 1)$ with $\#C(\mathbb{F}_l)\ \geq\ 1 + l - 2\sqrt{l}\ \geq\ 2$ where $p \equiv 1 \pmod 8$, $p_1 \equiv p_2 \equiv 5 \pmod 8$.

(ii) For $l \geq 5,\ l \neq t$ where $t \equiv 1, 3 \pmod 8$ and t divides n, C is a homogeneous space of genus 1 corresponding to $(1, q)$ then $\#C(\mathbb{F}_l)\ \geq\ 1 + l - 2\sqrt{l}\ \geq\ 2$.

Hensel's lemma implies that the homogeneous spaces mentioned above have l-adic solution for all the primes l mentioned above. This reduces the problem to finding local solutions for only finitely many primes.

Lemma 3.10. *Let n be a squarefree integer such that $n^2 + 1 = 2q$ for a prime q. Then for each prime factor, p of n, $p \equiv 1 \pmod 8$, the homogeneous spaces corresponding to $(p, 1)$ have local solutions everywhere for $l \leq \infty$.*

Proof. As mentioned above, we need only to show local solutions exist for $l = 2, 3$ and t where $t \equiv 1, 5 \pmod 8$ is a prime that divides n. Fixing two of the three variables z_1, z_2, z_3, we present a set of simple roots for the system of equations (3.2.1) and (3.2.2) modulo l using Lemma 3.8 that can be lifted to $\mathbb{Q}_l$ using Hensel's lemma.

For $l = 2$, $z_1 = 1$ is a simple root modulo 8 to the system of equations $pz_1^2 - 1 = 2^{2k}$ and

$z_1^2 - 1 = -\frac{n^2}{p} \cdot 2^{2k}$ for $k \geq 2$.
For $l = 3$, $z_1 = 1$ is a simple root modulo 3 to the system of equations $pz_1^2 - 1 = 3^{2k}$ and $z_1^2 - 1 = -\frac{n^2}{p} \cdot 3^{2k}$ when $p \equiv 1 \pmod 3$. When $p \equiv 2 \pmod 3$, one can see that $z_1 = 1$ is a simple root modulo 3 to the simultaneous equations $pz_1^2 - 1 = 1$ and $z_1^2 - 0 = -\frac{n^2}{p}$.
For $l = t$, $t \equiv 1, 5 \pmod 8$ and t divides n, $z_2 = a$ such that $a^2 \equiv -1 \pmod p$ is a simple root modulo p for equations $p \cdot 0^2 - z_2^2 = 1$ and $p \cdot 0^2 - z_2^2 = 2q$. This concludes the proof. □

In a very similar way to that of Lemma 3.10, we can prove the following result for $(p_1p_2, 1)$ where $p_i \equiv 5 \pmod 8$. We only observe that $p_1p_2 \equiv 1 \pmod 8$ in this case.

Lemma 3.11. *Let n be a squarefree integer such that $n^2 + 1 = 2q$ for a prime q. Then if exist, for any two prime factors p_1 and p_2 of n, $p_i \equiv 5 \pmod 8), i = 1, 2$, the homogeneous spaces corresponding to $(p_1p_2, 1)$ have local solutions everywhere for $l \leq \infty$.*

Lemma 3.12. *The homogeneous space corresponding to $(1, q) \in Sel_2(E/\mathbb{Q})$ if n has no prime factor of the form $8k + 5$.*

Proof. We have already established in Lemma 3.9 that if n has a prime divisor of the form 5 modulo 8, then $(1, q) \notin \mathrm{Sel}_2(E/\mathbb{Q})$.
For $l = 2$, we notice $n \not\equiv 1 \pmod 8$ implies $q \equiv 5 \pmod 8$. For homogeneous space associated to $(1, q)$, this implies $z_1 = 1$ is a simple root to $z_1^2 - q \cdot 1^2 = 2^2$ and $z_1^2 - q \cdot 1^2 = -n^2 \cdot 2^2$. Now $n \equiv 1 \pmod 8 \implies q \equiv 1 \pmod 8$. We can immediately now see that $z_1 = 1$ is a simple root modulo 8 of the simultaneous equations $z_1^2 - q = 2^{2k}$ and $z_1^2 - q = -n^2 \cdot 2^{2k}$ for $k \geq 2$.
For $l = 3$, we first note that $q \equiv 1 \pmod 3$ always. Then $z_1 = 1$ is a simple root to the system of equations $z_1^2 - q \cdot 1^2 = 3^{2k}$ and $z_1^2 - q \cdot 1^2 = -n^2 \cdot 3^{2k}$.
For $l = t$, where $t \equiv 1, 3 \pmod 8$ is prime, t divides n, we note that $\left(\frac{-q}{t}\right) = \left(\frac{-2}{t}\right) = 1$. Now we can see that $z_2 = a$ is a simple root to the equations $0^2 - qz_2^2 = 1$ and $0^2 - z_2^2 = 2$ where $a^2 \equiv -2 \pmod t$. This concludes the proof. □

We are now in a position to restrict the size of the 2-Selmer group $\mathrm{Sel}_2(E/\mathbb{Q})$. The proof requires the results obtained in earlier sections.

Proof of Theorem 3.7. From Lemma 3.12, we know that $(1, q) \in \mathrm{Sel}_2(E/\mathbb{Q})$ if n has no prime factor of the form 5 modulo 8. From the group structure of the 2-Selmer group, Lemma 3.9 and Lemma 3.10, we can see that $\mathrm{Sel}_2(E/\mathbb{Q}) = \langle (p_i, 1), (1, q) \rangle$ where $p_i \equiv 1 \pmod 8$ vary over all the prime factors of n. This proves part (i) of Theorem 3.7.
From Lemma 3.9, we know $(1, q) \notin \mathrm{Sel}_2(E/\mathbb{Q})$ if n has a prime factor of the form $8k + 5$. Hence Lemma 3.10 and Lemma 3.11 imply $\mathrm{Sel}_2(E/\mathbb{Q}) = \langle (p_i, 1), (t_it_j, 1) \rangle$ where p_i varies over all the prime factors of n of the form $8k + 1$ and $t_i \neq t_j$ varies over all the prime factors of n of the form $8k + 5$. Because there are $\frac{\Omega_{5,n}(\Omega_{5,n}-1)}{2}$ ways to choose distinct t_i, t_j, the result follows. □

Remark 7: Using the above result, we get that $\text{Sel}_2(E/\mathbb{Q}) = 1$ for $p \equiv 3, 7 \pmod 8$. Hence, using the finiteness of the Shafarevich-Tate group, which implies that $r(E/\mathbb{Q})$ has the same parity as the $p-$Selmer rank for a prime number p, we can conclude that $r(E/\mathbb{Q})$ is exactly one. Hence $\text{Ш}[2]$ is trivial. For $p \equiv 5 \pmod 8$, we have seen $r(E/\mathbb{Q}) = 0$ and $\text{Sel}_2(E/\mathbb{Q}) = 0$ hence $\text{Ш}[2]$ is trivial for this also.

We list odd integers n below with the 2-Selmer ranks of corresponding Heronian elliptic curve E associated with the non-isosceles Heron triangle. The tables are verified using MAGMA [34] and SAGE [49].

Table 3.2: Examples for odd area n, $\tau = \frac{1}{n}$ with $n^2 + 1 = 2q$ and corresponding 2-Selmer rank

n	q	2- Selmer Rank of E	Generators
3	5	1	(1,5)
5	13	0	-
71	2521	1	(1, 2521)
$3 \cdot 5$	113	0	-
$3 \cdot 5 \cdot 7 \cdot 11$	667013	0	-
$5 \cdot 11 \cdot 13$	255613	1	(65,1)
$5 \cdot 17$	3613	1	(17,1)
$17 \cdot 23$	76441	2	(17,1),(1, 76441)
$7 \cdot 11 \cdot 13$	501001	0	-
$3 \cdot 5 \cdot 7 \cdot 11 \cdot 19$	240791513	0	-
$5 \cdot 13 \cdot 3$	19013	1	(65,1)
$17 \cdot 73$	770041	3	(17,1),(73,1),(1,77041)
$17 \cdot 41 \cdot 97$	2285488441	4	(17,1),(41,1),(97,1),(1, 2285488441)

Chapter 4

Heronian Elliptic Curves Associated to Triangles of Even Area

*This chapter contains the following articles:

Chakraborty Debopam, Ghale Vinodkumar, Saikia Anupam; “Construction of an infinite family of elliptic curves of 2-Selmer rank 1 from Heron triangles”, *Research in Number Theory* 8, 101 (2022)

Chakraborty Debopam, Ghale Vinodkumar; “Size of the 2-Selmer groups for Heronian elliptic curves", *European Journal of Mathematics.* (2023) (Accepted).

Ghale Vinodkumar, Islam Imdadul, Chakraborty Debopam; “Elliptic curves associated with Heron triangles with high 2-Selmer rank”, (2023) (In communication).

Chakraboty Debopam, Ghale Vinodkumar, Saikia Anupam; “Heron triangles of even area and associated elliptic curves”, (2023) (In communication).

This chapter consists of the arithmetic of the Heronian elliptic curves associated with triangles with even area. First, we study a special case of triangles with area $n = 2^m p$ where p denotes a prime number. Consequently, we construct a family of infinitely many Heronian elliptic curves of rank 1 arising from Heron triangles. Assuming the finiteness of the Shafarevich-Tate group, we then explicitly produce a separate family of infinitely many Heronian elliptic curves with 2-Selmer rank lying between 1 and 3. Then we generalize the result and analyze the 2-Selmer ranks of the generalized Heronian elliptic curves. We conclude this chapter with the construction of a large class of Heronian elliptic curves with arbitrarily large 2-Selmer ranks.

4.1 Heron Triangles of Area $2^m p$, and $\tau = 2^m$:

For a prime p, and an arbitrary positive integer m, in this section, we consider Heronian elliptic curves associated with triangles of area $2^m p$ and one of the angles θ such that $\tau = \tan\frac{\theta}{2} = 2^m$. The main result regarding this class of Heronian elliptic curves is as follows.

Theorem 4.1. *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 Heronian elliptic curve*

$$E : y^2 = x(x - 4^m p)(x + p) \tag{4.1.1}$$

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

4.1.1 The 2-Selmer Group :

We can identify the Heronian elliptic curve E given by (4.1.1) with a Heron triangle of area $2^m p$ and an angle θ such that $\tau = \tan\frac{\theta}{2} = 2^m$. The discriminant of the elliptic curve E is $16 \cdot 4^{2m} \cdot p^6 \cdot q^2$. Let S be the set consisting of all finite places at which E has bad reduction, the infinite places and the prime 2, i.e., $S = \{p,\, q,\, 2,\, \infty\}$. We define

$$\begin{aligned}\mathbb{Q}(S,2) &= \left\{b \in \mathbb{Q}^*/(\mathbb{Q}^*)^2 : v_l(b) \equiv 0 \pmod 2 \text{ for all primes } l \notin S\right\}\\ &= \{\pm 1,\, \pm 2,\, \pm p,\, \pm q,\, \pm 2p,\, \pm 2q,\, \pm pq,\, \pm 2pq\}\,.\end{aligned}$$

By the method of 2-descent (2.48), there exists an injective homomorphism

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

defined by

$$\beta(x,y)=\begin{cases}(x,x-4^m p) & \text{if } x\neq 0,4^m p,\\ (-1,-p) & \text{if } x=0,\\ (p,q) & \text{if } x=4^m p,\\ (1,1) & \text{if } x=\infty,\ \text{i.e., if } (x,y)=O.\end{cases}$$

The homogeneous space for this curve is

$$b_1z_1^2-b_2z_2^2=4^m p, \tag{4.1.2}$$

$$b_1z_1^2-b_1b_2z_3^2=-p. \tag{4.1.3}$$

4.1.2 Local Solutions for the Homogeneous Spaces :

In this section, we examine the properties of the l-adic solutions for (4.1.2) and (4.1.3) 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 first prove the following result for all odd primes l.

Lemma 4.2. *Suppose (4.1.2) and (4.1.3) 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 (4.1.2) 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 (4.1.2) 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 (4.1.3), 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

$$b_1 u_1^2 l^{2(k_1-k_3)} - b_1 b_2 u_3^2 = -pl^{-2k_3}, \tag{4.1.4}$$

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 (4.1.4) 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 (4.1.3) from (4.1.2) 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 $k_2 < 0$. □

Lemma 4.3. *Suppose equations (4.1.2) and (4.1.3) have a solution* $(z_1, z_2, z_3) \in \mathbb{Q}_2 \times \mathbb{Q}_2 \times \mathbb{Q}_2$. *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 4.2 also yields $k_1 = k_2 = -k < 0$ and $k_3 \leq k_1$. From (4.1.4), 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 (4.1.4) implies 2 divides p, a contradiction. If $k_3 < 0 < k_1$, then reducing (4.1.4) modulo 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 a similar argument. If b_2 is even and $k_1 = 0$, then $k_2 \geq 0$ (resp. $k_2 < 0$) in (4.1.2) implies that 4 divides $b_1 b_2$ (resp. b_2), a contradiction. □

4.1.3 Bounding the Size of the 2-Selmer Group :

We now bound the size of the 2-Selmer group of the Heronian elliptic curves given by (4.1.1). The 2-Selmer group $\mathrm{Sel}_2(E/\mathbb{Q})$ consists of those pairs (b_1, b_2) in $\mathbb{Q}(S, 2) \times \mathbb{Q}(S, 2)$ for which equations (4.1.2) and (4.1.3) have an l-adic solution at every place l of $\mathbb{Q}$. We now limit the size of $\mathrm{Sel}_2(E/\mathbb{Q})$ by ruling out local solutions for certain pairs (b_1, b_2) by exploiting the results of the previous section.

Lemma 4.4. *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* $b_1 b_2 < 0$.

(ii) If $b_1 b_2 \equiv 2 \pmod 4$, *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 (4.1.3), which is absurd. Similarly, $b_1 < 0$ and $b_2 > 0$ implies $4^m p < 0$ in (4.1.2), which is absurd. Thus, the homogeneous space corresponding to (b_1, b_2) has no l-adic solutions for $l = \infty$ if $b_1 b_2 < 0$.
(ii) Let $b_1 b_2 \equiv 2 \pmod 4$. Then $v_2(z_1) = v_2(z_2) = -k < 0$ for some integer k from Lemma 4.3. Hence (4.1.2) can be written as

$$b_1 u_1^2 - b_2 u_2^2 = 4^m p \cdot 2^{2k},$$

which implies that b_1 and b_2 have the same parity, and it contradicts $b_1 b_2 \equiv 2 \pmod 4$.
(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 (4.1.3). If $v_q(z_1) < 0$, then from Lemma 4.2, we have $v_q(z_1) = v_q(z_2) = v_q(z_3) = -k < 0$ for some integer k. Subtracting (4.1.3) from (4.1.2), we get

$$b_1 b_2 u_3^2 - b_2 u_2^2 = pq^{2k+1},$$

where $z_i = u_i q^{-k}$ for $u_i \in \mathbb{Z}_q^*$ and $i \in \{1, 2, 3\}$. This implies that $b_2 \equiv 0 \pmod q$. From (4.1.3), one can now deduce that

$$b_1 u_1^2 - b_1 b_2 u_3^2 = -pq^{2k} \implies b_1 \equiv 0 \pmod{q^2},$$

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 4.2.
So we now suppose $v_q(z_3) < 0$ and $v_q(z_i) \geq 0$ for $i \in \{1, 2\}$. Then from (4.1.3), one can immediately observe $b_1 b_2 \equiv 0 \pmod{q^2} \implies b_2 \equiv 0 \pmod q$ too. From (4.1.2), this in turn implies that $4^m p \equiv 0 \pmod q$, a contradiction again. Hence the result follows. □

With the help of Lemma 4.3 and from the fact that the torsion points $(0, 0), (4^m, 0), (-p, 0)$ and O under the map β are

$$A = \{(-1, -p), (p, q), (-p, -pq), (1, 1)\},$$

we can now solely focus on the seven pairs

$$(1, p),\ (1, q),\ (1, pq),\ (2, 2),\ (2, 2p),\ (2, 2q),\ (2, 2pq).$$

Every other pair (b_1, b_2) will either belong to the same coset of one of those seven points in the torsion group $\mathrm{Im}(\beta)/A$ or the corresponding homogeneous space will not yield local solutions for at least one place l by Lemma 4.3, and consequently will not have rational solutions either. The following result narrows down the possible pairs from seven to three.

Lemma 4.5. *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 $z_1 = p\tilde{z}_1$ one can get the following from (4.1.2).

$$p^2\tilde{z}_1^2 - pz_2^2 = 4^m p \implies -z_2^2 \equiv 4^m \pmod p$$

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 (4.1.2), which in turn implies $v_p(z_1) < 0$ from Lemma 4.2, a contradiction.
If $v_p(z_1) < 0$ then from Lemma 4.2, $v_p(z_1) = v_p(z_2) = -k < 0$ for some integer k. Assuming $z_i = u_i p^{-k}$ for $i \in \{1, 2\}$, (4.1.2) yields $u_1^2 - pu_2^2 = 4^m p^{2k+1} \implies u_1 \equiv 0 \pmod p$, a contradiction.

We now deal with the pair $(2, 2p)$, the argument being similar for $(2, 2pq)$. From (4.1.2) one can see that if $v_p(z_2) \geq 0$ 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 $v_p(z_2) = v_p(z_1) = -k < 0$ for some integer k. Assuming $z_i = u_i p^k$ where $u_i \in \mathbb{Z}_p^*$ for $i \in \{1, 2, 3\}$, one can now observe from (4.1.2) that

$$2u_1^2 - 2pu_2^2 = 4^m p^{2k+1} \implies u_1 \equiv 0 \pmod p,$$

a contradiction again. Hence the result follows. □

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 4.6. *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 (4.1.3) from (4.1.2) 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 $z_2 \equiv z_3 \equiv 0 \pmod 5$, (4.1.3) 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 (4.1.2)

$$2z_1^2 - 10z_2^2 = 4p \implies 2z_1^2 \equiv 4p \pmod 5.$$

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

Lemma 4.7. *Equations (4.1.2) and (4.1.3) have a local solution in $\mathbb{Q}_l$ for every prime l for $(b_1, b_2) = (1, q)$.*

Proof. A twist of a smooth projective curve $C/\mathbb{Q}$ is a smooth curve $C'/\mathbb{Q}$ that is isomorphic to C over $\bar{\mathbb{Q}}$ (see [46], Section X.2). We use Hensel's lemma to show that for $(b_1, b_2) = (1, q)$, equations (4.1.2) and (4.1.3) have a local solution in $\mathbb{Q}_l$ for every place l. Every homogeneous space of E is a twist of E (see [46], Proposition 3.2). First we consider $l \geq 5$, $l \neq q$. Suppose C is the homogeneous space given by (4.1.2) and (4.1.3) 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

$$\#C(\mathbb{F}_l) \ \geq \ 1 + l - 2\sqrt{l} \ \geq \ 2 \qquad \text{for } l \geq 5, \ l \neq q.$$

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 $4^m p$, a contradiction. Similarly, $z_1 \equiv z_3 \equiv 0 \pmod{l}$ implies $-p \equiv 0 \pmod{l^2}$, contradiction again. One can now suitably choose two of z_1, z_2 and z_3 to convert equations (4.1.2) and (4.1.3) into one single equation of one variable with a simple root over $\mathbb{F}_l$. That common solution can then be lifted to $\mathbb{Q}_l$ via Hensel's lemma.

For $l = q$, one can notice that there exists $a \not\equiv 0 \pmod{q}$ such that $-p \equiv a^2 \pmod{q}$. This in turn shows that equations (4.1.2) and (4.1.3) has a simple root $z_1 = a$ modulo q and hence can be lifted to a solution in $\mathbb{Z}_q$ via Hensel's lemma. We also note that any initial choice of integers for z_2 and z_3 will not affect the above choice of z_1 to work in this case.

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 $z_1^2 = 4^m p \equiv 1 \pmod{3}$ from the first equation and $z_1^2 = q - p \equiv 1 \pmod{3}$ from the 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 $z_1^2 = q + 4^m p \equiv 1 \pmod{3}$ from the first equation and $z_1^2 = -p \equiv 1 \pmod{3}$ from the 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 (4.1.2) and (4.1.3) into the following;

$$z_1^2 - 5z_2^2 = 4p \equiv 28 \equiv 4 \pmod{8}, \tag{4.1.5}$$

$$z_1^2 - 5z_3^2 = -p \equiv 1 \pmod{8}. \tag{4.1.6}$$

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. □

Proof of Theorem 4.1. Lemma 4.4 and Lemma 4.5 establish that there are at most three distinct homogeneous spaces with possible local solutions at every prime $l \leq \infty$. This concludes that the 2-Selmer rank of E lies between 0 and 3. Lemma 4.7 ensures the existence of one homogeneous space with local solutions for all prime $l \leq \infty$. These three lemmas conclude that the 2-Selmer rank of E lies between 1 and 3. For $q = 5$, Lemma 4.6 implies that there is at most one homogeneous space with everywhere local solution, and hence, with Lemma 4.7, this proves that the 2-Selmer rank is exactly 1 for $q = 5$, concluding the proof of Theorem 4.1. □

4.1.4 The Mordell-Weil Rank and 2-Part of Shafarevich-Tate Group:

Assuming the finiteness of the Shafarevich-Tate group, one can immediately note that Theorem 4.1 has the following consequence.

Corollary 4.8. *The Mordell-Weil rank of the elliptic curve E given by (4.1.1) is at most 1 when $m = 1$. Moreover, if we assume the finiteness of the Shafarevich-Tate group $Ш(E/\mathbb{Q})$, then the rank of $E(\mathbb{Q})$ is exactly 1 and the 2-part of $Ш(E/\mathbb{Q})$ is trivial.*

Proof: We have seen that the 2-Selmer group has rank 1 in the previous section when $q = 5$. By the exact sequence (2.54), it follows that either $E(\mathbb{Q})$ has rank 0 or $Ш(E/\mathbb{Q})[2] = 0$. If we assume the finiteness of $Ш(E/\mathbb{Q})$ as predicted by Shafarevich, then $Ш(E/\mathbb{Q})$ must have square order by Cassels-Tate pairing (see [3]). Therefore, $Ш(E/\mathbb{Q})[2]$ has to be 0 i.e. the Mordell-Weil rank of E is 1. □

With the help of Theorem 4.1 and Corollary 4.8, we can now state the following regarding the existence of infinitely many Heron triangles of a certain type.

Corollary 4.9. *There exist infinitely many primes p congruent to 7 modulo 8 such that $2p$ is the area of infinitely many Heron triangles with one angle θ given by $\tan\frac{\theta}{2} = 2$.*

Proof: For $q = 5$ we have infinitely many primes $p \equiv 7 \pmod 8$ such that $\left(\frac{p}{5}\right) = 1$ by Dirichlet's theorem on primes in arithmetic progression. This ensures the existence of a Heronian elliptic curve E as in Theorem 4.1 with a rank of exactly 1, for each such prime p (Theorem 4.1 and Corollary 4.8). This is equivalent to the existence of infinitely many Heron triangles with area $2p$ and one angle θ such that $\tau = \tan\frac{\theta}{2} = 2$ due to the work of Goins and Maddox in [17] for each such prime p. This concludes the proof. □

We now include a list of Heronian elliptic curves satisfying the properties mentioned in the Theorem 4.1 with the corresponding rank, 2-Selmer rank, and Shafarevich-Tate group in the table below. The computations have been done in Magma [34] and SageMath [49] software.

TABLE 4.1: Examples for area $n = 2^m p, \tau = 2^m$ with $4^m + 1 = q$ and corresponding rank distribution

p	q	$r(E/\mathbb{Q})$	$s_2(E)$	Ш$(E/\mathbb{Q})[2]$	p	q	$r(E/\mathbb{Q})$	$s_2(E)$	Ш$(E/\mathbb{Q})[2]$
31	5	1	1	trivial	47	17	0	2	no information
71	5	1	1	trivial	127	17	2	2	trivial
79	5	1	1	trivial	151	17	0	no information	no information
151	5	1	1	trivial	191	17	0	2	no information
191	5	1	1	trivial	223	17	0	2	no information
199	5	1	1	trivial	239	17	0	2	no information

4.2 Heron Triangles of Area $2^m n$ and $\tau = n$:

As a generalization to the triangle considered above, we focus on Heron triangles of area $2^m \cdot n$ for square-free odd integer n and with one of the angles θ such that $\tau = \tan\frac{\theta}{2} = n$. The Heronian elliptic curve $E : y^2 = x(x - 2^m n^2)(x + 2^m)$ is associated with such triangles. Let S denote the set consisting of all finite places at which E has bad reductions, infinite places, and prime 2. We define

$$\begin{aligned}\mathbb{Q}(S, 2) &= \left\{b \in \mathbb{Q}^*/(\mathbb{Q}^*)^2 : v_l(b) \equiv 0 \pmod 2 \text{ for all primes } l \notin S\right\}\\ &= \langle \pm 2,\ \pm p_i,\ \pm q\rangle\end{aligned}$$

where $n = p_1 p_2 ... p_k$ is a square-free odd number such that $n^2 + 1 = 2q$ for some prime q. By the method of 2-descent (2.48), there exists an injective homomorphism

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

defined by

$$\beta(x, y) = \begin{cases} (x, x - 2^m n^2) & \text{if } x \neq 0, 2^m n^2,\\ (-1, -2^{\delta(m)}) & \text{if } x = 0,\\ (2^{\delta(m)}, 2q) & \text{if } x = 2^m n^2,\\ (1, 1) & \text{if } x = \infty, \text{ i.e., if } (x, y) = O,\end{cases}$$

where O is the fixed base point and $\delta(m) = 0$ for even m and $\delta(m) = 1$ otherwise. If (b_1, b_2) is a pair which is not in the image of $O, (0, 0), (2^m n^2, 0)$, 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

$$b_1 z_1^2 - b_2 z_2^2 = 2^m \cdot n^2, \tag{4.2.1}$$

$$b_1 z_1^2 - b_1 b_2 z_3^2 = -2^m, \tag{4.2.2}$$

$$b_1 b_2 z_3^2 - b_2 z_2^2 = 2^{m+1} \cdot q \tag{4.2.3}$$

have a solution $(z_1, z_2, z_3) \in \mathbb{Q}^* \times \mathbb{Q}^* \times \mathbb{Q}$. We note that (4.2.3) is obtained by subtracting (4.2.2) from (4.2.1) and is only included here due to its use later in this section. Throughout the work, b denotes all possible products of the prime factors of n. By p, we denote an arbitrary factor of n, unless otherwise mentioned. The main results of this work are now as follows;

Theorem 4.10. *Let $E : y^2 = x(x - 2^m n^2)(x + 2^m)$ be the elliptic curve corresponding to non-isosceles Heron triangles of area $2^m \cdot n$ and one of the angles θ such that $\tau = \tan\frac{\theta}{2} = n$. We assume $n = p_1 p_2 .. p_k$ as a square-free odd number and $n^2 + 1 = 2q$ for some prime number q. Then for odd m,*

$$Sel_2(E) = \begin{cases} \langle(2,2)\rangle & \text{if } p_i \equiv \pm 3 \pmod 8, q \equiv 1 \pmod 8, \\ 0 & \text{if } p_i \equiv \pm 3 \pmod 8, q \equiv 5 \pmod 8, \\ \langle(b,b),(2b,b),(2,2)\rangle & \text{if } p_i \equiv \pm 1 \pmod 8, q \equiv 1 \pmod 8, \end{cases}$$

for all $i \in \{1, 2, ..., k\}$, where $(b, b) \in Sel_2(E)$ implies $b \equiv 1 \pmod 8$ and $(2b, b) \in Sel_2(E)$ implies $b \equiv 7 \pmod 8$.

We note that the case of $p_i \equiv \pm 1 \pmod 8$, $q \equiv 5 \pmod 8$ is not included above, since $\left(\frac{n^2+1}{p_i}\right) = \left(\frac{2}{p_i}\right)\left(\frac{q}{p_i}\right) \implies q \equiv 1 \pmod 8$. The result for even m is as follows.

Theorem 4.11. *Let $E : y^2 = x(x - 2^m n^2)(x + 2^m)$ be the Heronian elliptic curve as mentioned above. Then for even m, $Sel_2(E) = \langle(b,b),(1,2)\rangle$ where*
(i) $(b, b) \in Sel_2(E) \implies b \equiv \pm 1 \pmod 8$.
(ii) $(1, 2) \in Sel_2(E)$ implies every prime factor of n is of the form ± 1 modulo 8.

4.2.1 Local Solution to the Homogeneous Spaces :

We focus on l-adic solutions that are not in $\mathbb{Z}_l$, i.e. $t_i < 0$ for all $i = 1, 2, 3$. We start with the following result relating t_1 and t_2.

Lemma 4.12. *Suppose (4.2.1) and (4.2.2) have a solution $(z_1, z_2, z_3) \in \mathbb{Q}_l \times \mathbb{Q}_l \times \mathbb{Q}_l$ for any prime l. If $v_l(z_i) < 0$ for any one $i \in \{1, 2\}$, then $v_l(z_1) = v_l(z_2) = -t < 0$ for some integer t.*

Proof. With the notations above, for $t_1 < 0$, (4.2.1) implies $b_1 \cdot u_1^2 - b_2 \cdot u_2^2 \cdot l^{2(t_2 - t_1)} = 2^m \cdot n^2 \cdot l^{-2t_1} \implies b_1 \equiv 0 \pmod{l^2}$ if $t_2 > t_1$, a contradiction as b_1 is square-free. Hence $t_2 \leq t_1 < 0$. Now if $t_2 < t_1 < 0$ then again from (4.2.1) one gets

$$b_1 \cdot u_1^2 \cdot l^{2(t_1 - t_2)} - b_2 \cdot u_2^2 = 2^m \cdot n^2 \cdot l^{-2t_2},$$

which implies l^2 must divide b_2, a contradiction again. Hence if $t_1 < 0$, then we have $t_1 = t_2 = -t < 0$ for some integer t. For $t_2 < 0$, one similarly gets $t_1 = t_2 = -t < 0$. □

The following result gives a correspondence between $v_l(z_1)$ and $v_l(z_3)$ for all primes l.

Lemma 4.13. *Suppose (4.2.1) and (4.2.2) have a solution* $(z_1, z_2, z_3) \in \mathbb{Q}_l \times \mathbb{Q}_l \times \mathbb{Q}_l$ *for any prime* l*. Then* $v_l(z_1) < 0 \implies v_l(z_3) = v_l(z_1) = -t < 0$.

Proof. For $t_1 < 0$, from (4.2.2), we have

$$b_1 \cdot u_1^2 - b_1 b_2 \cdot u_3^2 \cdot l^{2(t_3 - t_1)} = -2^m \cdot l^{-2t_1}.$$

If $t_3 > t_1$, then l^2 must divide b_1, a contradiction. Hence $t_3 \leq t_1 < 0$. Now for $t_3 < t_1 < 0$, one can see from above that

$$b_1 \cdot u_1^2 \cdot l^{2(t_1 - t_3)} - b_1 b_2 \cdot u_3^2 = -2^m \cdot l^{-2t_3}, \tag{4.2.4}$$

which implies l^2 must divide $b_1 b_2$, i.e., $l = 2, p$ or q where p denotes any of the primes that divide n. Noting b_1, b_2 are square-free, one can get that $t_3 \leq -2 \implies b_1 b_2 \equiv 0 \pmod{l^3}$, a contradiction from the above equation. Hence, $t_3 = -1$, but then $t_3 < t_1 \implies t_1 \geq 0$, contradiction again as $t_1 < 0$. Together, now we obtain $t_1 = t_3 = -t < 0$ if $t_1 < 0$. □

Lemma 4.14. *Suppose (4.2.1) and (4.2.2) have a solution* $(z_1, z_2, z_3) \in \mathbb{Q}_l \times \mathbb{Q}_l \times \mathbb{Q}_l$ *for any prime* l*. If* p *denotes an arbitrary prime factor of* n*, then*
(i) For all primes $l \neq p$, $v_l(z_3) < 0 \implies v_l(z_3) = v_l(z_1)$*. The same conclusion holds true for* $l = p$ *also if* $b_1 b_2 \not\equiv 0 \pmod{p^2}$.
(ii) For $l = p$, $b_1 b_2 \equiv 0 \pmod{p^2}$*, and* $v_l(z_3) < 0$*, either* $v_l(z_3) = -1$ *and* $v_l(z_1) = v_l(z_2) = 0$*, or* $v_l(z_3) = v_l(z_1) = -t < 0$.

Proof. (i) For $v_l(z_3) = t_3 < 0$, from (4.2.2), we get

$$b_1 \cdot u_1^2 \cdot l^{2(t_1 - t_3)} - b_1 b_2 \cdot u_3^2 = -2^m \cdot l^{-2t_3}.$$

Hence $t_1 > t_3$ implies l^2 divides $b_1 b_2$ i.e. $l = 2, p$ or q. $l = 2$ will imply 2^3 divides $b_1 b_2$, a contradiction. For $l = q$, from (4.2.3), we again get q^3 divides $b_1 b_2$ if $t_2 > t_3$, a contradiction. Hence $t_2 \leq t_3 < 0 \implies t_2 = t_1 \leq t_3$ from Lemma 4.12. Now $t_1 < t_3 \implies b_1 \equiv 0 \pmod{l^2}$ from (4.2.2), a contradiction. Hence $t_3 < 0 \implies t_3 = t_1 = -t < 0$. This proves the first part of the result.
(ii) For the second part, $l = p, b_1 b_2 \equiv 0 \pmod{p^2}$, and $t_1 > t_3$ will imply $t_3 = -1$ from (4.2.2), and hence $t_1 \geq 0$. This, in turn, will also imply $t_2 \geq 0$. As $v_p(2^m \cdot n^2) = 2$, one can easily observe that $t_1, t_2 \geq 0 \implies t_1 = t_2 = 0$ from (4.2.1). Hence for $l = p$ and $t_1 > t_3$ implies $t_3 = -1$, and $t_1 = t_2 = 0$. For $l = p$ and $t_1 \leq t_3 < 0 \implies t_1 < 0$, and hence from Lemma 4.13, we conclude $t_1 = t_3$. This concludes the proof. □

The following result discusses the non-existence of l-adic solutions for different homogeneous spaces and different l. This, in turn, makes the upper bound of the size of $\mathrm{Sel}_2(E)$ smaller. Without loss of generality, we assume $b_2 \not\equiv 0 \pmod q$, as $(2^{\delta(m)}, 2q)$ belongs in the image of the $E(\mathbb{Q})_{tors}$ under the 2-descent map β.

Lemma 4.15. *Let $(b_1, b_2) \in \mathbb{Q}(S,2) \times \mathbb{Q}(S,2)$. Then*
(i) The corresponding homogeneous space has no l-adic solution for the case $l = \infty$ if $b_1 b_2 < 0$.
(ii) If $b_1 \equiv 0 \pmod q$, then the corresponding homogeneous space has no q-adic solution.
(iii) The homogeneous space corresponding to (b_1, b_2) has no p-adic solution if $b_1 b_2 \equiv 0 \pmod p$ but $b_1 b_2 \not\equiv 0 \pmod{p^2}$.

Proof. (i) Let the homogeneous space corresponding to $(b_1, b_2) \in \mathbb{Q}(S,2) \times \mathbb{Q}(S,2)$ has real solutions. Then $b_1 > 0$ and $b_2 < 0$ implies $-2^m > 0$ in (4.2.2), which is absurd. Similarly, $b_1 < 0$ and $b_2 > 0$ implies $2^m \cdot n^2 < 0$ in (4.2.1), a contradiction. Thus, the homogeneous space corresponding to (b_1, b_2) has no l-adic solutions for $l = \infty$ if $b_1 b_2 < 0$.
(ii) Let us assume $b_1 \equiv 0 \pmod q$. From (4.2.3), we notice that $v_q(z_i) < 0 \implies b_2 \equiv 0 \pmod q$, a contradiction. Now for $v_q(z_i) \geq 0$, (4.2.2) will imply that $-2^m \equiv 0 \pmod q$, a contradiction again. Hence the result follows.
(iii) Assuming $b_1 \equiv 0 \pmod p$, we get $b_2 \not\equiv 0 \pmod p$ from the given condition. If $v_p(z_i) < 0$, from (4.2.1), we get $b_2 \cdot u_2^2 \equiv 0 \pmod p$ where $u_2 \in \mathbb{Z}_p^*$, a contradiction. Hence $v_p(z_i) \geq 0$, but then (4.2.2) implies $-2^m \equiv 0 \pmod p$, a contradiction. The case $b_2 \equiv 0 \pmod p$, $b_1 \not\equiv 0 \pmod p$ can be done in a similar manner. □

4.2.2 Size of the 2-Selmer Group When m is an Odd Integer :

We start this section under the assumption m is odd. From Lemma 4.15, it is evident that $(b, b), (2b, b), (b, 2b), (2b, 2b)$ are the only possible elements of $\mathrm{Sel}_2(E)$ where b runs over all possible square-free combinations of prime factors of n and 1.

Lemma 4.16. *Let $(b_1, b_2) \in \mathbb{Q}(S,2) \times \mathbb{Q}(S,2)$. Then*
(i) The homogeneous spaces corresponding to $(2b, b)$ and $(b, 2b)$ have no 2-adic solutions if $b \not\equiv 7 \pmod 8$. The homogeneous space corresponding to $(2b, 2b)$ has no 2-adic solution if $b \not\equiv 1 \pmod 8$.
(ii) For $p \equiv \pm 3 \pmod 8$, the homogeneous spaces corresponding to $(b, b), (2b, b), (b, 2b)$ and $(2b, 2b)$ have no p-adic solutions where p is any prime factor of b.
(iii) For $q \equiv 5 \pmod 8$, the homogeneous space corresponding to $(2, 2)$ has no q-adic solution.

Proof. (i) For the case $(2b, b)$, one can immediately observe $v_2(z_i) \geq 0$, as otherwise $b \equiv 0 \pmod 2$ from (4.2.1). For $v_2(z_i) \geq 0$, looking into the parity of $v_2(z_i)$ from (4.2.1) and (4.2.3), we get $v_2(z_1) = \frac{m-1}{2}$ and $v_2(z_2) = \frac{m+1}{2}$. Using (4.2.1), this, in turn, implies

$$b \cdot u_1^2 - 2b \cdot u_2^2 \equiv b - 2b = n^2 \equiv 1 \pmod 8 \implies b \equiv 7 \pmod 8.$$

For the case $(b, 2b)$, in a similar way, we note that from (4.2.1) and (4.2.2), $v_2(z_2) = \frac{m-1}{2} = v_2(z_3)$. From (4.2.3), we can now observe that $b^2 \cdot u_3^2 - b \cdot u_2^2 = 2q \implies b^2 - b \equiv 2 \pmod 8 \implies b \equiv 7 \pmod 8$. Hence the result follows.

Now for the case $(2b, 2b)$, $v_2(z_i) < 0 \implies 2b \cdot u_1^2 \equiv 0 \pmod 4$ from (4.2.2), a contradiction. Hence $v_2(z_i) \geq 0$ for all $i = 1, 2, 3$. Now from (4.2.2) and (4.2.3), one can immediately observe that $v_2(z_1) = v_2(z_3) = \frac{m-1}{2}$, which in turn, implies $b \cdot u_1^2 - 2b^2 \cdot u_3^2 = -1 \implies b \equiv 1 \pmod 8$ from (4.2.2). Hence the result follows.

(ii) For all the four types of pairs, in this case, one can first note from Lemma 4.14 that $v_p(z_3) = -1$, and $v_p(z_1) = v_p(z_2) = 0$, as otherwise from (4.2.2), either $2^m \equiv 0 \pmod p$ or $b \equiv 0 \pmod{p^2}$. Now from (4.2.3), for (b, b) and $(2b, 2b)$, we get $\left(\frac{2^{m+1}q}{p}\right) = 1$, a contradiction as $n^2 + 1 = 2q \implies \left(\frac{2q}{p}\right) = 1$ whereas m is odd, and $\left(\frac{2}{p}\right) = -1$ as $p \equiv \pm 3 \pmod 8$.

For $(2b, b)$ and $(b, 2b)$, noting again that $v_p(z_3) = -1$, and $v_p(z_1) = v_p(z_2) = 0$, one gets $\left(\frac{2}{p}\right) = 1$ from (4.2.1), a contradiction again as $p \equiv \pm 3 \pmod 8$. Hence the result follows.

(iii) For $(2, 2)$, from (4.2.3), we obtain $v_q(z_i) > 0 \implies 2^{m+1} \equiv 0 \pmod q$, $v_p(z_2) = v_p(z_3) = 0 \implies \left(\frac{2}{q}\right) = 1$ contradiction both the time. Also, one can trivially observe from (4.2.3) that $v_p(z_2) = 0$ if and only if $v_p(z_3) = 0$. Hence $v_q(z_i) < 0$ for all $i \in \{1, 2, 3\}$, and from Lemma 4.12, one now gets $\left(\frac{2}{q}\right) = 1$, a contradiction when $q \equiv 5 \pmod 8$. □

4.2.3 Size of 2-Selmer Group When m is Even :

We focus on the elliptic curve E and its corresponding 2-Selmer group $\mathrm{Sel}_2(E)$ with the assumption m is an even integer in this section. From Lemma 4.14 and Lemma 4.15, it is again evident that $\{(b, b), (b, 2b), (2b, b), (2b, 2b)\}$ are the only possible elements in $\mathrm{Sel}_2(E)$.

Lemma 4.17. *Let $(b_1, b_2) \in \mathbb{Q}(S, 2) \times \mathbb{Q}(S, 2)$. Then*

(i) The homogeneous spaces corresponding to $(2b, b)$ and $(2b, 2b)$ have no 2-adic solutions.

(ii) If $p \not\equiv \pm 1 \pmod 8$ and $n \equiv 0 \pmod p$, then the homogeneous spaces corresponding to $(b, 2b)$ has no p-adic solutions.

(iii) The homogeneous space corresponding to (b, b) has no 2-adic solution if $b \not\equiv \pm 1 \pmod 8$.

Proof. (i) For $l = 2$ and $(b_1, b_2) = (2b, b)$, it is evident from Lemma 4.12 and Lemma 4.13 that $v_2(z_i) \geq 0$ for the homogeneous space described by (4.2.1) and (4.2.2). Noting that m is even and comparing the parity of the exponent of 2 on both sides of (4.2.1) and (4.2.3), we get $v_2(z_3) = v_2(z_2) = \frac{m}{2}$. From (4.2.3), we now get $2b \cdot u_3^2 - b \cdot u_2^2 = 2q \implies b \equiv 2 \pmod 8$, hence a contradiction and the result then follows for the case $(b_1, b_2) = (2b, b)$.

For the case $(b_1, b_2) = (2b, 2b)$ a similar method shows from (4.2.2) and (4.2.3) that $v_2(z_2) =$

$\frac{m}{2}, v_2(z_3) = \frac{m-2}{2}$. From (4.2.3), one can now get $2b \equiv 7 \pmod 8$, a contradiction. Hence the result follows.

(ii) We first prove the case when $b \equiv 0 \pmod p$. If $v_p(z_i) \geq 0$ for all i, then from (4.2.2) for $(b_1, b_2) = (b, 2b)$, one can observe that $2^m \equiv 0 \pmod p$, a contradiction. Similarly if $v_p(z_i) = -t < 0$ for all i, again from (4.2.2), one can see $b \cdot u_1^2 \equiv 0 \pmod{p^2}$, a contradiction. From Lemma 4.14, now the only remaining case is $v_p(z_3) = -1$, and $v_p(z_1) = v_p(z_2) = 0$. Noting m is even, from (4.2.2), this implies $\left(\frac{2}{p}\right) = 1 \implies p \equiv \pm 1 \pmod 8$.

Now for the case when $p \not\equiv \pm 1 \pmod 8$ divides n but not b, one can immediately observe that $v_p(z_i) \geq 0$ as otherwise $\left(\frac{2}{p}\right) = 1$ from (4.2.1), a contradiction if $p \not\equiv \pm 1 \pmod 8$. Now for $v_p(z_i) \geq 0$, from (4.2.1), we get that $v_p(z_2) = 0 \implies v_p(z_1) = 0 \implies \left(\frac{2}{p}\right) = 1$, a contradiction. Hence $v_p(z_2) > 0$ which implies $v_p(z_1) > 0$ and that leads to $v_p(z_3) = 0$. Now from (4.2.3), we get

$$2b^2 \cdot u_3^2 - 2b \cdot z_2^2 = 2^m \cdot 2q \implies b^2 \cdot u_3^2 \equiv 2^{m-1} \pmod p \implies \left(\frac{2}{p}\right) = 1.$$

The result now follows as 2 is a quadratic non-residue modulo p here.

(iii) For homogeneous space corresponding to (b, b), if $v_2(z_i) < 0$ in (4.2.1) and (4.2.2), then from (4.2.2), it is evident that $b \equiv 1 \pmod 8$. Otherwise, for the case $v_2(z_i) \geq 0$, from (4.2.3), one can notice that

$$v_2(z_2) = v_2(z_3) \implies b^2 \cdot u_3^2 - b \cdot u_2^2 \equiv 2q \text{ or } 0 \equiv 2 \text{ or } 0 \pmod 8.$$

This implies $b \equiv \pm 1 \pmod 8$, and the result follows. □

4.2.4 Everywhere Local Solution :

We now look into concluding the computation of the 2-Selmer rank for E. The following result focuses on the homogeneous spaces with local solutions everywhere.

Lemma 4.18. *Equations (4.2.1) and (4.2.2) have a local solution in $\mathbb{Q}_l$ for every prime l for $(b_1, b_2) = (2, 2)$ when m is odd, $q \equiv 1 \pmod 8$.*

Proof. The Jacobian of the intersection of (4.2.1) and (4.2.2) for $(2, 2)$ is

$$\begin{pmatrix} 4 \cdot z_1 & -4 \cdot z_2 & 0 \\ 4 \cdot z_1 & 0 & -8 \cdot z_3 \end{pmatrix}$$

which one can easily observe has rank 2 whenever $l \neq 2, p, q$ where $p \equiv \pm 1 \pmod 8$, $q \equiv 1 \pmod 8$. Hence except for those l's, the topological genus becomes the same as the arithmetic genus, which is 1 by the degree-genus formula, and Hasse-Weil bound for a genus one curve can be used for all but finitely many primes. For small primes $l = 2, 3$ and for $l = p, q$ we check directly for the local solutions.

For $l \neq p, q, l \geq 5$, using Hasse bound we 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 $2^m \cdot n^2 \implies l = p$, a contradiction. Similarly, $z_1 \equiv z_3 \equiv 0 \pmod{l}$ implies $-2^m \equiv 0 \pmod{l} \implies l = 2$, contradiction again. One can now suitably choose two of z_1, z_2 and z_3 to convert equations (4.2.1) and (4.2.2) into one single equation of one variable with a simple root over $\mathbb{F}_l$. That common solution can then be lifted to $\mathbb{Q}_l$ via Hensel's lemma.

For $l = 2$, we first note that any solution (z_1, z_2, z_3) of (4.2.1) and (4.2.3) implies $v_2(z_1) = v_2(z_3) = \frac{m-1}{2}$. Using these we convert the equations (4.2.1) and (4.2.2) into the following;

$$u_1^2 - z_2^2 = n^2,$$
$$u_1^2 - 2u_3^2 = -1.$$

Fixing $z_2 = 0$ and $u_3 = 1$, one can see that $u_1^2 \equiv 1 \pmod{8}$ is a solution to the above equations and can be lifted to $\mathbb{Z}_2$ via Hensel's lemma. Multiplying both sides by 2^m then gives rise to a solution of (4.2.1) and (4.2.2) in $\mathbb{Z}_2$.

For $l = 3$, if $n \equiv 0 \pmod{3}$, fixing $z_2 = z_3 = 1$ gives rise to $z_1 \not\equiv 0 \pmod{3}$ as a solution to (4.2.1) and (4.2.2), that can be lifted to $\mathbb{Z}_3$ via Hensel's lemma. If 3 does not divide n, fixing $z_2 = 0$ and $z_3 = 1$ implies $z_1 \not\equiv 0 \pmod{3}$ is a solution that Hensel's lemma can again lift.

For $l = p \equiv \pm 1 \pmod{8}$, instead of looking for p-adic solution of (4.2.1) and (4.2.2), we focus on equations (4.2.2) and (4.2.3). Fixing $z_1 = z_2 = 0$, and noting that $\left(\frac{2}{p}\right) = 1$, one can choose z_3 such that $z_3^2 \equiv 2^{m-2} \pmod{p}$, as a solution that can be lifted to $\mathbb{Z}_p$ via Hensel's lemma.

For $l = q \equiv 1 \pmod{8}$, a very similar argument as for $l = p$, shows that $z_1 = z_2 = 0$ gives rise to z_3 as a solution such that $z_3^2 \equiv -2^{m-1} \pmod{q}$, that can lifted to $\mathbb{Z}_q$ via Hensel's lemma. This concludes the proof. □

The following result now completely determines the 2-Selmer group of E for odd integer m when all the prime factors of n is of the form ± 1 modulo 8.

Lemma 4.19. *Let $p_i \equiv \pm 1 \pmod{8}$ for all $i \in \{1, 2, ..., k\}$. Then for odd m, the equations (4.2.1) and (4.2.2) have a local solution in $\mathbb{Q}_l$ for*

(i) every prime l for $(b_1, b_2) = (b, b)$, when $b \equiv 1 \pmod{8}$.

(ii) every prime l for $(2b, b)$ when $b \equiv 7 \pmod{8}$ if $q \equiv 1 \pmod{8}$.

Proof. The method adopted to prove the result is similar to that used in the proof of Lemma 4.18. Hence, we mostly provide direct solutions that can be lifted to l-adic rational numbers via Hensel's lemma. Like the previous case, we explicitly check the cases $l = 2, 3, q,\ p \equiv \pm 1 \pmod{8}$, and the case $q \equiv 1 \pmod{8}$ if q is of such form. For all other primes l, we use the Hasse-Weil bound and can immediately observe that there exists a solution (z_1, z_2, z_3) for homogeneous spaces corresponding to both (b, b) and $(2b, b)$ modulo l such that $z_1 \equiv z_2 \equiv 0 \pmod{l}$ or $z_1 \equiv z_3 \equiv 0 \pmod{l}$ is not possible. Hence can be lifted to $\mathbb{Q}_l$ via Hensel's lemma. We now start with the case (b, b).

(i) For $l = 2$, choosing $v_2(z_i) < 0$, one can immediately see $z_1^2 \equiv 1 \pmod 8$ is a solution if $z_2 = z_3 = 1$ and hence can be lifted to $\mathbb{Z}_2$.

For $l = 3$, we note that $n \not\equiv 0 \pmod 3$ in this case, and so is true for b. For $b \equiv 1 \pmod 3$, we look for solutions such that $v_q(z_i) < 0$. Fixing $z_2 = z_3 = 1$, one can see $z_1 \not\equiv 0 \pmod 3$ is then a solution modulo 3 that can be lifted to $\mathbb{Q}_3$ via Hensel's lemma. For $b \equiv 2 \pmod 3$, fixing $z_2 = 0$ and $z_3 = 1$ gives rise to $z_1 \not\equiv 0 \pmod 3$, a solution that can again be lifted by Hensel's lemma.

For $l = p$, where p varies over all prime factors of n, we start with noting $\left(\frac{2}{p}\right) = 1$ in this case. We start with those primes p such that $b \equiv 0 \pmod p$. Using Lemma 4.14, we look for solutions (z_1, z_2, z_3) such that $v_p(z_3) = -1$ and $v_p(z_1) = v_p(z_2) = 0$. Fixing $z_1 = z_2 = 1$, we get $\frac{b^2}{p^2} \cdot z_3^2 = 2^m$. This z_3 can be lifted to p-adic solutions using Hensel's lemma.

Now for $l = p$, such that p divides n but not b, noting that $\left(\frac{2}{p}\right) = 1$, we observe that $(0, 0, z_3)$ is a solution for (4.2.2) and (4.2.3) where $b^2 z_3^2 \equiv 2^m \pmod p$. This solution can be lifted to $\mathbb{Z}_p$ using Hensel's lemma.

For $l = q$, we first note that $q \equiv 5 \pmod 8$ implies the Jacobian described earlier has rank 2 and hence is already considered using Hasse-Weil bound. So $q \equiv 1 \pmod 8$, and $\left(\frac{b}{q}\right) = 1$ here. Now $(z_1, 0, 0)$ gives rise to a solution that can be lifted by Hensel's lemma, where $b \cdot z_1^2 \equiv -2^m \pmod q$. This concludes the proof for the case $(b_1, b_2) = (b, b)$.

(ii) We now look into the case $(b_1, b_2) = (2b, b)$ where $b \equiv -1 \pmod 8$. As above, we will only focus on the primes $l = 2, 3, p$ and q where $p \equiv \pm 1 \pmod 8$. $q \equiv 1 \pmod 8$ is a necessary condition in this case, as otherwise, the corresponding homogeneous space does not have any q-adic solution from Lemma 4.16 and hence does not belong to $\mathrm{Sel}_2(E)$.

For $l = 2$, we again notice that $v_2(z_1) = v_2(z_2) - 1 = \frac{m-1}{2}$ which implies dividing both sides of (4.2.1) and (4.2.2) by 2^m, $(z_1, 1, 0)$ is a solution modulo 8, where $z_1^2 \equiv 1 \pmod 8$, and hence can be lifted to $\mathbb{Q}_2$ via Hensel's lemma.

For $l = 3$, we again note that $n \not\equiv 0 \pmod 3$, and hence so is b. For $b \equiv 1 \pmod 3$, fixing $z_1 = 0$ gives rise to $z_2, z_3 \not\equiv 0 \pmod 3$ as solutions that can be lifted. For $b \equiv 2 \pmod 3$, Fixing $z_2 = 1, z_3 = 0$, we get $z_1 \not\equiv 0 \pmod 3$ as a solution that Hensel's lemma can lift.

For $l = p$, when $p \equiv \pm 1 \pmod 8$, p divides n but not b, fixing $z_1 = z_2 = 0$, one can choose z_3 such that $b^2 z_3^2 \equiv 2^{m-1} \pmod p$. If $b \equiv 0 \pmod p$, we look for the solution with $v_p(z_1) = v_p(z_2) = 0, v_p(z_3) = -1$. Now fixing z_1, z_2 to any arbitrary values modulo p, one can see (z_1, z_2, z_3) is a solution where $\frac{b^2}{p^2} \cdot z_3^2 \equiv 2^{m-1} \pmod p$. The solution then can be lifted to $\mathbb{Q}_p$ by Hensel's lemma.

For $l = q \equiv 1 \pmod 8$, noting $\left(\frac{b}{q}\right) = 1$ here, one can fix $z_2 = z_3 = 0$ and get z_1 as a solution to (4.2.1) and (4.2.2) such that $b \cdot z_1^2 \equiv -2^m \pmod q$. This can be lifted to $\mathbb{Q}_q$ via Hensel's lemma. This concludes the proof for this case. □

Now we focus on the 2-Selmer group $\mathrm{Sel}_2(E)$ of the elliptic curve E when m is an even integer. Before proving the results below, we first note that $b \equiv \pm 1 \pmod 8$ implies $\left(\frac{b}{q}\right) = 1$ here.

Lemma 4.20. *Equations (4.2.1) and (4.2.2) have a local solution in $\mathbb{Q}_l$ for every prime l for $(b_1, b_2) = (b, b)$ when m is even, $b \equiv \pm 1 \pmod 8$.*

Proof. The Jacobian of the intersection of (4.2.1) and (4.2.2) for (b, b) is

$$\begin{pmatrix} 2b \cdot z_1 & -2b \cdot z_2 & 0 \\ 2b \cdot z_1 & 0 & -2b^2 \cdot z_3 \end{pmatrix}$$

For $l \notin \{2, p, q\}$, the Jacobian has rank 2 modulo l and hence represent a smooth curve of genus one. Using Hasse-Weil bound for such $l \geq 5$, one can guarantee the existence of at least two solutions (z_1, z_2, z_3) for (4.2.1) and (4.2.2) modulo l. It is now a simple observation that either of $z_1 \equiv z_2 \equiv 0 \pmod l$ or $z_1 \equiv z_3 \equiv 0 \pmod l$ implies $l \in \{2, p, q\}$. Hence, the solutions can not be pairwise zero. Fixing two of z_1, z_2 and z_3 suitably, now one can use Hensel's lemma to lift the solutions modulo l to $\mathbb{Q}_l$ for all such primes l.

For $l = 2$, we start with the case $b \equiv 1 \pmod 8$. Fixing $z_2 = z_3 = 1$ for $v_2(z_i) < 0$, $z_1^2 \equiv 1 \pmod 8$ is a solution that can be lifted to $\mathbb{Q}_2$ by Hensel's lemma. For $b \equiv -1 \pmod 8$, we first observe from (4.2.1) and (4.2.3) that $\frac{m}{2} = v_2(z_2) = v_2(z_3) < v_2(z_1)$ is the only possibility in this case for equations (4.2.1) and (4.2.2). Dividing both sides of (4.2.1) and (4.2.2) by 2^m then yields in

$$\begin{aligned} b \cdot z_1^2 - b \cdot u_2^2 = n^2 \equiv 1 \pmod 8, \\ b \cdot z_1^2 - b^2 \cdot u_3^2 = -1 \equiv -1 \pmod 8. \end{aligned}$$

Fixing $z_1 = 0$ results in $u_2 = u_3 = 1$ as solutions that can be lifted to $\mathbb{Q}_2$ via Hensel's lemma.

For $l = 3$ and $b \equiv 1 \pmod 3$, one can note that fixing $z_2 = z_3 = 1$ for $v_3(z_i) < 0$ gives rise to $z_1 = 1$ as a solution that can be lifted to $\mathbb{Q}_3$. Similarly for $b \equiv 2 \pmod 3$, if $n \not\equiv 0 \pmod 3$, fixing $z_1 = 0$ leads to $z_2 = z_3 = 1$ as solutions that can be lifted. In case $b \equiv 2 \pmod 3$ and $n \equiv 0 \pmod 3$, fixing $z_2 = 1, z_3 = 0$ gives rise $z_1 \not\equiv 0 \pmod 3$ as a solution that can be lifted to $\mathbb{Z}_3$.

For $l = p$ where p divides b, it can be seen that fixing z_1 and z_2 to any arbitrary values modulo p and choosing z_3 as the solution of $\frac{b^2}{p^2} \cdot z_3^2 \equiv 2^m \pmod p$ gives the required solution of (4.2.1) and (4.2.2) that can be lifted to $\mathbb{Q}_p$ for $v_p(z_1) = v_p(z_2) = 0, v_p(z_3) = -1$. For $l = p$ where p divides n but not b, $(0, 0, z_3)$ is a solution of (4.2.2) and (4.2.3), that can be lifted to $\mathbb{Q}_p$ where z_3 satisfies $b^2 \cdot z_3^2 \equiv 2^m \pmod p$.

For $l = q$, fixing $z_2 = z_3 = 0$ in (4.2.1) and (4.2.2), we can see that $(z_1, 0, 0)$ is a solution that can be lifted to $\mathbb{Q}_q$ where $b \cdot z_1^2 \equiv -2^m \pmod q$. This follows from the fact $\left(\frac{b}{q}\right) = 1$. Now the result follows. □

Lemma 4.21. *Equations (4.2.1) and (4.2.2) have a local solution in $\mathbb{Q}_l$ for every prime l for $(b_1, b_2) = (b, 2b)$ when m is even, and the the prime factors of n are of the form ± 1 modulo 8.*

Proof. The Jacobian of the intersection of (4.2.1) and (4.2.2) for (b, b) is

$$\begin{pmatrix} 2b \cdot z_1 & -4b \cdot z_2 & 0 \\ 2b \cdot z_1 & 0 & -4b^2 \cdot z_3 \end{pmatrix}$$

Similar to the method used in Lemma 4.20, we note that for $l \notin \{2, p, q\}$, the Jacobian has rank 2 modulo 2 and hence represent a curve of genus one modulo such primes. Using the Hasse-Weil bound, in a similar way, one can then notice the homogeneous space corresponding to $(b, 2b)$ represented by (4.2.1) and (4.2.1) has l-adic solution for all $l \geq 5$ and $l \neq 2, p, q$.

For $l = 2$, $b \equiv 1 \pmod 8$, we first note that $\frac{m}{2} = v_2(z_1) < v_2(z_2)$ is the only possibility. Dividing both sides of (4.2.1) and (4.2.2) by 2^m, we can see that $(z_1, 0, 1)$ where $z_1^2 \equiv 1 \pmod 8$ is a solution to the reduced equations and can be lifted to $\mathbb{Q}_2$ by Hensel's lemma. For $b \equiv -1 \pmod 8$, again one can note that $\frac{m}{2} = v_2(z_1) < v_2(z_3)$. This gives rise to $(z_1, 1, 0)$ as a solution modulo 8 such that $z_1^2 \equiv 1 \pmod 8$ and can be lifted to $\mathbb{Z}_2$.

For $l = 3$, for $z_1 \not\equiv 0 \pmod 3$, we get $(z_1, 0, 1)$ as solution modulo l to (4.2.1) and (4.2.2) when $b \equiv 1 \pmod 3$ that can be lifted to $\mathbb{Q}_3$ via Hensel's lemma. For $b \equiv 2 \pmod 3$, the solution $(z_1, 1, 0)$ with $z_1 \not\equiv 0 \pmod 3$ does the same thing.

For $l = p$, if $b \equiv 0 \pmod p$, then fixing z_1, z_2 to any arbitrary non-zero values modulo l, (z_1, z_2, u_3) becomes a solution for the case $v_l(z_1) = v_l(z_2) = 0, v_l(z_3) = -1$ where u_3 satisfies $\frac{b^2}{p^2} \cdot u_3^2 \equiv 2^{m-1} \pmod p$. This happens as $\left(\frac{2}{p}\right) = 1$. Hensel's lemma can lift the solution because after fixing z_1 and z_2, u_3 becomes a simple root for equations (4.2.1) and (4.2.2). For the case when p divides n but not b, $(0, 0, z_3)$ is a solution to (4.2.2) and (4.2.3) that can be lifted to $\mathbb{Q}_p$ where $2b^2 \cdot z_3^2 \equiv 2^m \pmod p$.

Now for $l = q$, noting that m is even and $\left(\frac{b}{q}\right) = 1$, $(z_1, 0, 0)$ is a solution modulo q that can be lifted to $\mathbb{Q}_q$ where z_1 satisfies $b \cdot z_1^2 \equiv -2^m \pmod q$. This concludes the proof. □

4.2.5 Elliptic Curves with Arbitrarily Large 2-Selmer Rank :

Now we are in a position to prove Theorem 4.10 and Theorem 4.11. We note that these theorems give rise to a construction of elliptic curves with arbitrarily high 2-Selmer ranks.

Proof of Theorem 4.10: From Lemma 4.16, one can immediately conclude that for $p \equiv \pm 3 \pmod 8$, $\mathrm{Sel}_2(E) = 0$ if $q \equiv 5 \pmod 8$ and for $q \equiv 1 \pmod 8$, the 2-Selmer group can possibly only be generated by $(2, 2)$ which was proved in Lemma 4.18.

For the case $p \equiv \pm 1 \pmod 8$, from Lemma 4.16, one can identify (b, b) as only possible generators of $\mathrm{Sel}_2(E)$ if $q \equiv 5 \pmod 8$ and $b \equiv 1 \pmod 8$, the assertion later verified in Lemma 4.19. For $q \equiv 1 \pmod 8$, again from Lemma 4.16, the possible elements of $\mathrm{Sel}_2(E)$ are identified as $(2, 2), (b, b), (2b, b), (b, 2b), (2b, 2b)$. In Lemma 4.19, the existence of $(b, b), (2b, b)$ in the 2-Selmer group is proved, which along with the existence of $(2, 2) \in \mathrm{Sel}_2(E)$ proved in Lemma 4.18, proves the result of Theorem 4.22.

Table 4.2: Examples for area $2^m n, \tau = n$ with $n^2 + 1 = 2q$ when m is odd and corresponding 2-Selmer rank

n	m	q	2-Selmer rank of E	Generators of $\mathrm{Sel}_2(E)$
3	$1, 3, 5$	5	0	-
$3 \cdot 5$	$1, 3, 5$	113	1	$(2, 2)^*$
$11 \cdot 19$	$1, 3, 5$	21841	1	$(2, 2)$
$3 \cdot 5 \cdot 11$	$1, 3, 5$	13613	0	-
$3 \cdot 5 \cdot 13$	$1, 3, 5$	19013	0	-
79	$1, 3, 5$	3121	2	$(2, 2)^*$, $(79, 2 \cdot 79)^*$
$17 \cdot 23$	$1, 3, 5$	76441	3	$(2, 2)$, $(34, 34)^*$, $(23, 46)$
$7 \cdot 17 \cdot 31$	$1, 3, 5$	6804361	4	$(2, 2), (17, 17), (14, 7), (62, 31)$

Proof of Theorem 4.11: From Lemma 4.17, we conclude that $\mathrm{Sel}_2(E)$ possibly only contain (b, b) or $(b, 2b)$ when $b \equiv \pm 1 \pmod 8$ if $(b, b) \in \mathrm{Sel}_2(E)$, and every prime factors of b is of the form ± 1 modulo 8 if $(b, 2b) \in \mathrm{Sel}_2(E)$. Lemma 4.20 and Lemma 4.21 proves that $\mathrm{Sel}_2(E)$ contains $(b, b), (b, 2b)$ by showing the existence of l-adic solution for all primes l. Now the result follows from the observation that $(1, 2) = (b, b) \cdot (b, 2b)$.

Table 4.3: Examples for area $2^m n, \tau = n$ with $n^2 + 1 = 2q$ when m is even and corresponding 2-Selmer rank

n	m	q	2-Selmer rank of E	Generators of $\mathrm{Sel}_2(E)$
3	$2, 4, 6$	5	0	-
$3 \cdot 5$	$2, 4, 6$	113	1	$(3 \cdot 5, 3 \cdot 5)^*$
$11 \cdot 19$	$2, 4, 6$	21841	1	$(11 \cdot 19, 11 \cdot 19)^*$
$3 \cdot 5 \cdot 11$	$2, 4, 6$	13613	2	$(15, 15), (55, 55)$
$3 \cdot 5 \cdot 13$	$2, 4, 6$	19013	2	$(15, 15), (65, 65)$
71	$2, 4, 6$	2521	2	$(71, 71), (1, 2)$
79	$2, 4, 6$	3121	2	$(79, 79)^*, (1, 2)^*$
$17 \cdot 23$	$2, 4, 6$	76441	3	$(17, 17)^*$, $(23, 23), (1, 2)$
$5 \cdot 7 \cdot 11 \cdot 17$	$2, 4, 6$	21418513	3	$(7, 7), (17, 17), (55, 55)$
$7 \cdot 17 \cdot 31$	$2, 4, 6$	6804361	4	$(7, 7), (17, 17), (31, 31), (1, 2)$

$(b_1, b_2)^*$ denotes the pairs that were verified via SAGEMATH and MAGMA. The run time for the rest was too long to verify.

4.3 Heron Triangles of Area $2^m n$ and $\tau = 2^m$:

Here, we look into the Selmer and Shafarevich-Tate group structure of the Heronian elliptic curves associated with Heron triangles of area $2^m \cdot n$ for square-free odd n, and one of the angles θ such that $\tau = \tan \frac{\theta}{2} = 2^m$. The main result of this section is as follows.

Theorem 4.22. *Let $E : y^2 = x(x - 4^m n)(x + n)$ be a Heronian elliptic curve for $n = p_1 p_2 .. p_k$, where p_i are primes congruent to 1 modulo 8. If $\left(\frac{p_i}{p_j}\right) = 1$, and $\left(\frac{q}{p_i}\right) = -1$, then the 2-Selmer rank of E is $k + 1$ for $m \geq 3$ and k for $m = 2$.*

We prove the above result as a special case for triangles of area $2^m \cdot n$ for square-free odd n. For this reason, throughout this section, we consider the more general elliptic curve $E : y^2 = x(x - 4^m n)(x + n)$ where n is only a square-free odd integer.

4.3.1 The 2-Selmer Group

We identify the elliptic curve $E : y^2 = x(x - 4^m n)(x + n)$ with a Heron triangle of area $2^m n$ and an angle θ such that $\tau = \tan \frac{\theta}{2} = 2^m$. Moreover, in case the associated Heron triangles are non-isosceles, it is known that $E(\mathbb{Q})_{\text{tors}}$ is isomorphic to Klein's four group. The discriminant of the elliptic curve E can be observed to be $16 \cdot 4^{2m} \cdot n^6 \cdot q^2$ where $q = 4^m + 1$ is a prime number. Let S be the set consisting of all finite places at which E has bad reduction, the infinite places, and the prime 2. We define

$$\begin{aligned} \mathbb{Q}(S, 2) &= \left\{ b \in \mathbb{Q}^*/(\mathbb{Q}^*)^2 : v_l(b) \equiv 0 \pmod 2 \text{ for all primes } l \notin S \right\} \\ &= \langle \pm 2,\ \pm p_i,\ \pm q \rangle, \end{aligned} \tag{4.3.1}$$

where $n = p_1 p_2 ... p_k$ is a square-free odd number. By the method of 2-descent (2.48, there exists an injective homomorphism

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

defined by

$$\beta(x, y) = \begin{cases} (x, x - 4^m n) & \text{if } x \neq 0, 4^m p, \\ (-1, -n) & \text{if } x = 0, \\ (n, q) & \text{if } x = 4^m n, \\ (1, 1) & \text{if } x = \infty, \text{ i.e., if } (x, y) = O, \end{cases}$$

corresponding homogeneous space is

$$b_1 z_1^2 - b_2 z_2^2 = 4^m n, \tag{4.3.2}$$

$$b_1 z_1^2 - b_1 b_2 z_3^2 = -n, \tag{4.3.3}$$

$$b_1 b_2 z_3^2 - b_2 z_2^2 = nq. \tag{4.3.4}$$

We note that (4.3.4) can be obtained by subtracting (4.3.3) from (4.3.2), and only mentioned here because of its use in the later part of this work.

We now examine the properties of the l-adic solutions for (4.3.2) and (4.3.3) that are associated with the 2-Selmer group. We start with the following result for all finite primes l.

Lemma 4.23. *Suppose (4.3.2) and (4.3.3) have a solution* $(z_1, z_2, z_3) \in \mathbb{Q}_l \times \mathbb{Q}_l \times \mathbb{Q}_l$ *for any prime* l*. If* $v_l(z_i) < 0$ *for any one* $i \in \{1, 2\}$*, then* $v_l(z_1) = v_l(z_2) = -t < 0$ *for some integer* t*.*

Proof. Let $z_i = l^{t_i} u_i$, where $t_i \in \mathbb{Z}$ and $u_i \in \mathbb{Z}_l^*$ for $i = \{1, 2\}$. Then $v_l(z_i) = t_i$ for all $i \in \{1, 2\}$. Suppose $t_1 < 0$. Then from (4.3.2) one can get that

$$b_1 u_1^2 - b_2 u_2^2 l^{2(t_2 - t_1)} = 4^m n l^{-2t_1}.$$

If $t_2 > t_1$, then l^2 must divide b_1, a contradiction as b_1 is square-free. Hence $t_2 \leq t_1 < 0$. Now if $t_2 < t_1 < 0$ then again from (4.3.2) we get

$$b_1 u_1^2 l^{2(t_1 - t_2)} - b_2 u_2^2 = 4^m n l^{-2t_2},$$

which implies l^2 must divide b_2, a contradiction again. Hence if $t_1 < 0$, then we have $t_1 = t_2 = -t < 0$ for some integer t. For $t_2 < 0$, one similarly gets $t_1 = t_2 = -t < 0$. □

The following result gives a correspondence between $v_l(z_1)$ and $v_l(z_3)$ for all primes l.

Lemma 4.24. *Suppose (4.3.2) and (4.3.3) have a solution* $(z_1, z_2, z_3) \in \mathbb{Q}_l \times \mathbb{Q}_l \times \mathbb{Q}_l$ *for any prime* l*. Then* $v_l(z_1) < 0 \implies v_l(z_3) = v_l(z_1)$*.*

Proof. We start with the assumption that $v_l(z_i) = t_i$ for all $i \in \{1, 3\}$. For $t_1 < 0$, from (4.3.3), we have

$$b_1 u_1^2 - b_1 b_2 u_3^2 l^{2(t_3 - t_1)} = -n l^{-2t_1}.$$

If $t_3 > t_1$, then l^2 must divide b_1, a contradiction. Hence $t_3 \leq t_1 < 0$. For $t_3 < t_1 < 0$, we can rewrite the above equation as

$$b_1 u_1^2 l^{2(t_1 - t_3)} - b_1 b_2 u_3^2 = -n l^{-2t_3}, \tag{4.3.5}$$

which implies l^2 must divide $b_1 b_2$, i.e., $l = 2, p$ or q where p denotes any of the prime p_i's. For $l = 2, p, q$, we note that $t_3 \leq -2 \implies b_1 b_2 \equiv 0 \pmod{l^3}$, a contradiction from the above equation. Hence, $t_3 = -1$ if $l = 2, p, q$, but then $t_3 < t_1 \implies t_1 \geq 0$, contradiction again as $t_1 < 0$. Together, now we obtain $t_1 = t_3 = -t < 0$ if $t_1 < 0$. □

Lemma 4.25. *Suppose (4.3.2) and (4.3.3) have a solution* $(z_1, z_2, z_3) \in \mathbb{Q}_l \times \mathbb{Q}_l \times \mathbb{Q}_l$ *for any prime* l*. Then*

(i) For all primes $l \neq 2$, $v_l(z_3) < 0 \implies v_l(z_3) = v_l(z_1)$*. The same conclusion holds true for* $l = 2$ *also if* $b_1 b_2 \not\equiv 0 \pmod 4$*.*

(ii) For $l = 2$, $b_1b_2 \equiv 0 \pmod 4$, and $v_l(z_3) < 0$, either $v_l(z_3) = -1$ and $v_l(z_1) = v_l(z_2) \geq 0$, or $v_l(z_3) = v_l(z_1)$.

Proof. Borrowing the same notation, for the case $v_l(z_3) = t_3 < 0$, from (4.3.3), we observe that

$$b_1u_1^2l^{2(t_1-t_3)} - b_1b_2u_3^2 = -nl^{-2t_3}.$$

Hence $t_1 > t_3$ implies l^2 divides b_1b_2 i.e. $l = 2, p_i$ or q. As mentioned previously, $l = p_i$ will imply l^3 divides b_1b_2, a contradiction. For $l = q$, subtracting (4.3.3) from (4.3.2), we again get q^3 divides b_1b_2, a contradiction if $t_2 > t_3$. Hence $t_2 \leq t_3 < 0 \implies t_2 = t_1 \leq t_3$. Now $t_1 < t_3 \implies b_1 \equiv 0 \pmod{l^2}$, a contradiction. Hence $t_3 < 0 \implies t_3 = t_1 = -t < 0$. This proves the first part of the result.

$l = 2, b_1b_2 \equiv 0 \pmod 4$, and $t_1 > t_3$ will imply $t_3 = -1$, and hence $t_1 \geq 0$. This, in turn, will also imply $t_2 \geq 0$. If $t_1 \neq t_2$, it will then lead to a contradiction from (4.3.2), as $v_2(b_1z_1^2 - b_2z_2^2)$ will be an odd number now whereas $v_2(4^mn)$ will always be an even number. Hence $l = 2$ and $t_1 > t_3$ implies $t_3 = -1$, and $t_1 = t_2 \geq 0$. For $l = 2$ and $t_1 \leq t_3 < 0 \implies t_1 < 0$, and hence from Lemma 4.24, we conclude $t_1 = t_3$. This concludes the proof. □

4.3.2 Bounding the Size of the 2-Selmer Group

We now bound the size of the general 2-Selmer group of the Heronian elliptic curve $E : y^2 = x(x-4^mn)(x+n)$. The 2-Selmer group $\mathrm{Sel}_2(E/\mathbb{Q})$ consists of those pairs (b_1, b_2) in $\mathbb{Q}(S, 2)\times\mathbb{Q}(S, 2)$ for which equations (4.3.2) and (4.3.3) have an l-adic solution at every place l of $\mathbb{Q}$. Before proving Theorem 4.22, we define the following subgroup of $\mathbb{Q}(S, 2) \times \mathbb{Q}(S, 2)$.

Notation: We define the the group $G_E \subset \mathbb{Q}(S, 2) \times \mathbb{Q}(S, 2)$ as follows. For $(b_1, b_2) \in G_E$,
(i) $b_1b_2 \equiv 0 \pmod 2 \implies b_1b_2 \equiv 0 \pmod 4$ with $\frac{b_1b_2}{4} \equiv n$ or $n + b_1 \pmod 8$.
(ii) $b_1b_2 \not\equiv 0 \pmod 2$ implies one of $b_1 \equiv b_2 \equiv 1 \pmod 8$, $b_1b_2 \equiv n \pmod 4$, and $b_1 \equiv b_2 \equiv -n, 4 - n \pmod 8$ must hold true.
(iii) $b_1b_2 \equiv 0 \pmod{p^2}$ implies $\left(\frac{b_1/p}{p}\right) = \left(\frac{-n/p}{p}\right)$ and $\left(\frac{b_2/p}{p}\right) = \left(\frac{-nq/p}{p}\right)$.
$b_1b_2 \not\equiv 0 \pmod{p^2}$, $b_1 \equiv 0 \pmod p$ implies $\left(\frac{b_1/p}{p}\right) = \left(\frac{n/p}{p}\right)$ and $\left(\frac{b_2}{p}\right) = \left(\frac{q}{p}\right)$.
$b_1b_2 \not\equiv 0 \pmod{p^2}$, $b_2 \equiv 0 \pmod p$ implies $\left(\frac{-b_1}{p}\right) = 1$ and $\left(\frac{-b_2/p}{p}\right) = \left(\frac{n/p}{p}\right)$.
(iv) $\left(\frac{b_1}{q}\right) = 1$ or $\left(\frac{b_1}{q}\right) = \left(\frac{-n}{q}\right)$.
We first prove the following general result binding the size of $\mathrm{Sel}_2(E/\mathbb{Q})$ for $E : y^2 = x(x - 4^mn)(x + n)$ where n is a square-free odd integer. We use this result later in proving Theorem 4.22.

Lemma 4.26. *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 $b_1b_2 \equiv 0 \pmod 4$, the corresponding homogeneous space has no 2-adic solution if $\frac{b_1b_2}{4} \not\equiv n$ or $n + b_1 \pmod 8$. Moreover, for $m = 2$, and $b_1 \equiv b_2 \pmod 8$, if $\frac{b_1b_2}{4} \not\equiv n + b_1 \pmod 8$, the same conclusion holds.
(iv) If $\left(\frac{b_1}{q}\right) \neq 1$, 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 $-n > 0$ in (4.3.3), which is absurd. Similarly, $b_1 < 0$ and $b_2 > 0$ implies $4^m n < 0$ in (4.3.2), which is absurd. Thus, the homogeneous space corresponding to (b_1, b_2) has no l-adic solutions for $l = \infty$ if $b_1b_2 < 0$.
(ii) For $b_1b_2 \equiv 2 \pmod 4$, we start with the case b_1 even and b_2 odd. $v_2(z_i) < 0 \implies b_2 \equiv 0 \pmod 2$ from (4.3.2) and Lemma 4.25, a contradiction. Hence $v_2(z_i) \geq 0$ which in turn implies $v_2(z_2) > 0$ from (4.3.2). Then from (4.3.4), we get $nq = b_1b_2z_3^2 - b_2z_2^2 \equiv 0 \pmod 2$, a contradiction.
A very similar approach as above shows that $v_2(z_i) \geq 0$ and $v_2(z_1) > 0$ when b_1 is odd and b_2 is even. This in turn implies $-n = b_1z_1^2 - b_1b_2z_3^2 \equiv 0 \pmod 2$, a contradiction.
(iii) For $b_1b_2 \equiv 0 \pmod 4$, we prove that the only possibility is $0 \leq v_2(z_1) = v_2(z_2) \leq m - 1, v_2(z_3) = -1$. From Lemma 4.23, one can immediately notice from (4.3.3) that $v_2(z_i) < 0$ for all $i \in \{1, 2, 3\}$ is not possible. Now for the case $v_2(z_3) \geq 0$, from (4.3.3), one gets that $v_2(z_1) \geq 0 \implies n \equiv 0 \pmod 2$, a contradiction. Hence, $v_2(z_1) < 0$, which in turn implies $v_2(z_3) < 0$ from Lemma 4.24, a contradiction again. Hence $v_2(z_3) = -1$, and $0 \leq v_2(z_1) = v_2(z_2) \leq m - 1$. Now the result follows from (4.3.3). Here, from (4.3.2) and (4.3.3), we also note that $\frac{b_1b_2}{4} \equiv n \pmod 8 \implies v_2(z_1) \geq 1 \implies m \geq 3$ if $b_1 \equiv b_2 \equiv \pmod 8$. This concludes the proof.
(iv) Let us first assume $b_1 \equiv 0 \pmod q$. From (4.3.4), we notice that $v_q(z_i) < 0 \implies b_2 \equiv 0 \pmod q$, a contradiction. Now for $v_q(z_i) \geq 0$, it is an immediate observation from (4.3.4) that $v_q(z_2) > 0$ which implies $4^m n \equiv 0 \pmod q$ from (4.3.2), a contradiction. Hence $b_1 \not\equiv 0 \pmod q$. Now from (4.3.4) if $v_q(z_i) < 0$ or $v_q(z_2) = v_q(z_3) = 0$, one gets $\left(\frac{b_1}{q}\right) = 1$. From (4.3.4), $v_q(z_2) > 0 \iff v_q(z_3) > 0 \implies n \equiv 0 \pmod q$, a contradiction. Hence the result follows. □

We note that the torsion points $(0, 0), (4^m, 0), (-n, 0)$ and O under the map β are $A = \{(-1, -n), (n, q), (-n, -nq), (1, 1)\}$. So without the loss of generality, we assume $b_2 \not\equiv 0 \pmod q$, as (n, q) belongs to the image of the $E(\mathbb{Q})_{tors}$. Hence we can now solely focus on the pairs of the form (b_1, b_2) such that 2 and p are the only possible factors of b_i's where p varies over all prime factors of n. We first start with the 2-adic solutions. We note that from Lemma 4.26, b_1b_2 is either odd or $0 \pmod 4$.

Lemma 4.27. *Let $(b_1, b_2) \in \mathbb{Q}(S,2) \times \mathbb{Q}(S,2)$. Then for b_1b_2 odd and $m \geq 2$, if the corresponding homogeneous space has 2-adic solution (z_1, z_2, z_3) then one of the following conditions occurs.*
(i) $b_1 \equiv b_2 \equiv 1 \pmod 8$.
(ii) $b_1 \equiv b_2 \equiv -n, 4-n \pmod 8$.
(iii) $b_1b_2 \equiv n \pmod 4$.

Proof. (i) Assuming (z_1, z_2, z_3) is a solution, one can immediately observe that if $v_2(z_i) < 0$ then (4.3.2) and (4.3.3) imply $b_1 \equiv b_2 \equiv 1 \pmod 8$.
(ii) For $v_2(z_1) = v_2(z_2) = 0 < v_2(z_3)$, $b_1 \equiv b_2 \pmod 8$ from (4.3.2) as $m \geq 2$. Now from (4.3.3), one can get $b_1 \equiv -n, 4-n \pmod 8$ which proves the result.
(iii) Let us suppose that $0 < v_2(z_1) = v_2(z_2) \leq m-1$ and $v_2(z_3) = 0$. Now (4.3.3) implies $b_1b_2 - n \equiv 0, 4 \pmod 8$. For $v_2(z_1) = m \implies v_2(z_2) > m$ and $v_2(z_3) = 0$. From (4.3.3), one can now obtain $b_1b_2 \equiv n \pmod 8$ as $m \geq 2$. Similarly, $v_2(z_2) = m \implies b_1b_2 \equiv n \pmod 8$ from (4.3.4). □

We now look into the p-adic solutions of (4.3.2) and (4.3.3). Note that p runs over all prime factors of n.

Lemma 4.28. *Let $(b_1, b_2) \in \mathbb{Q}(S,2) \times \mathbb{Q}(S,2)$. Then*
(i) if $b_1b_2 \equiv 0 \pmod{p^2}$, the corresponding homogeneous space has no p-adic solution if $\left(\frac{b_1/p}{p}\right) \neq \left(\frac{-n/p}{p}\right)$ or $\left(\frac{b_2/p}{p}\right) \neq \left(\frac{-nq/p}{p}\right)$.
(ii) if $b_1b_2 \not\equiv 0 \pmod{p^2}$, $b_1 \equiv 0 \pmod p$, the corresponding homogeneous space has no p-adic solution if $\left(\frac{b_2}{p}\right) \neq \left(\frac{q}{p}\right)$ or $\left(\frac{b_1/p}{p}\right) \neq \left(\frac{n/p}{p}\right)$.
(iii) if $b_1b_2 \not\equiv 0 \pmod{p^2}$, $b_2 \equiv 0 \pmod p$, the corresponding homogeneous space has no p-adic solution if $\left(\frac{-b_1}{p}\right) \neq 1$ or $\left(\frac{-b_2/p}{p}\right) \neq \left(\frac{n/p}{p}\right)$.

Proof. (i) We first note that if $b_1b_2 \equiv 0 \pmod{p^2}$, then from (4.3.2), either $v_p(z_i) < 0$ or $v_p(z_1) = v_p(z_2) = 0, v_p(z_3) \geq 0$. In either cases, from (4.3.3), it is now evident $\left(\frac{b_1/p}{p}\right) = \left(\frac{-n/p}{p}\right)$. Similarly, from (4.3.4), one can get $\left(\frac{b_2/p}{p}\right) = \left(\frac{-nq/p}{p}\right)$. Now the result follows.
(ii) For $b_1b_2 \not\equiv 0 \pmod{p^2}$, $b_1 \equiv 0 \pmod p$, we first note that $v_p(z_i) < 0 \implies b_2 \equiv 0 \pmod p$ from (4.3.2), a contradiction. Now $v_p(z_i) \geq 0$ implies $v_p(z_1) = v_p(z_3) = 0$ and $v_p(z_2) > 0$ from (4.3.2) and (4.3.4). Hence from (4.3.2), one can get $\left(\frac{b_1/p}{p}\right) = \left(\frac{n/p}{p}\right)$, whereas (4.3.4) implies $\left(\frac{b_1b_2/p}{p}\right) = \left(\frac{nq/p}{p}\right)$, together which then implies $\left(\frac{b_2}{p}\right) = \left(\frac{q}{p}\right)$.
(iii) For $b_1b_2 \not\equiv 0 \pmod{p^2}$, $b_2 \equiv 0 \pmod p$, in a similar way to the previous case one can show that $v_p(z_i) \geq 0$, which then implies $v_p(z_2) = v_p(z_3) = 0$ and $v_p(z_1) > 0$. Now from (4.3.2), we get $\left(\frac{-b_2/p}{p}\right) = \left(\frac{n/p}{p}\right)$, and from (4.3.3), we get, $\left(\frac{b_1b_2/p}{p}\right) = \left(\frac{n/p}{p}\right)$. Together one then gets $\left(\frac{-b_1}{p}\right) = 1$. Hence the result follows. □

We are now in a position to prove the following general result regarding the size of $\mathrm{Sel}_2(E)$.

Proposition 4.29. *Let $E : y^2 = x(x - 4^m n)(x + n)$ be the Heronian elliptic curve corresponding to non-isosceles Heron triangles of area $2^m \cdot n$ and one of the angles θ such that $\tau = \tan\frac{\theta}{2} = 2^m$, where $n = p_1 p_2 \dots p_k$ is a square-free odd number, $q = 4^m + 1$ is a prime. Then for $m \geq 2$ and $n \not\equiv 0 \pmod 3$, $Sel_2(E) = G_E$.*

Proof. We have already established that $\mathrm{Sel}_2(E) \subset G_E$ through the Lemma 4.26, Lemma 4.27, and Lemma 4.28. We now show that $G_E \subset \mathrm{Sel}_2(E)$. In that regard, we first note that the Jacobian of the intersection of (4.3.2) and (4.3.3) for (b_1, b_2) is

$$\begin{pmatrix} 2b_1 z_1 & -2b_2 z_2 & 0 \\ 2b_1 z_1 & 0 & -2b_1 b_2 z_3 \end{pmatrix} \tag{4.3.6}$$

which has rank 2 modulo any prime $l \neq 2, p$, and $l = q$ in case $z_2 \equiv z_3 \equiv 0 \pmod q \implies \left(\frac{b_1}{q}\right) = \left(\frac{-n}{q}\right)$. Hence for $l \neq 2, p$, and for $\left(\frac{b_1}{q}\right) = \left(\frac{-n}{q}\right)$, $l \neq q$, the topological genus becomes the same as the arithmetic genus, which is 1 by the degree-genus formula, and Hasse-Weil bound ensures the existence of at least two sets of solutions modulo l for all such primes l.

For $l = 2$, $(b_1, b_2) \in G_E$, we go case by case depending on the relations between b_1 and b_2. We start with the case $b_1 b_2$ odd.

If $b_1 \equiv b_2 \equiv 1 \pmod 8$, $(u_1, 1, 1)$ is a solution modulo 8 with $u_1^2 \equiv 1 \pmod 8$, that can be lifted to $\mathbb{Q}_2$ as a solution of (4.3.2) and (4.3.3) with $v_2(z_i) < 0$ by Hensel's lemma.

If $b_1 b_2 \equiv n \pmod 8$, then one can immediately observe that $(0, 0, u_3)$ is a solution to (4.3.3) and (4.3.4) with $u_3^2 \equiv 1 \pmod 8$, that can be lifted to $\mathbb{Q}_2$ as a solution with either $v_2(z_1) = m$ or $v_2(z_2) = m$.

If $b_1 \equiv b_2 \equiv -n, 4 - n \pmod 8$, $(u_1, 1, 0)$ is a solution to (4.3.2) and (4.3.3) with $u_1^2 \equiv 1 \pmod 8$ that can be lifted to $\mathbb{Q}_2$ via Hensel's lemma.

For $b_1 b_2$ even, we have $b_1 b_2 \equiv 0 \pmod 4$ and $\frac{b_1 b_2}{4} \equiv n$ or $n + b_1 \pmod 8$. One can now see that $(0, 0, u_3)$ and $(1, 1, u_3)$ are the respective solutions for the two cases with $u_3^2 \equiv 1 \pmod 8$ and hence can be lifted to $\mathbb{Q}_2$ for a solution with $v_2(z_3) = -1$.

Now for $l = 3$, noting that $n \not\equiv 0 \pmod 3$, we enlist the solutions below that can be lifted to $\mathbb{Q}_3$ via Hensel's lemma. For $n \equiv 1 \pmod 3$, if $b_1 \equiv b_2 \equiv 1 \pmod 3$, $(u, 1, 1)$ is such a solution with $u^2 \equiv 1 \pmod 3$ that can be lifted for $v_3(z_i) < 0$, if $b_1 \equiv b_2 \equiv 2 \pmod 3$, $(0, 1, u)$ is the required solution, $(u, 0, 1)$ works for the case $b_1 \equiv 1 \pmod 3, b_2 \equiv 2 \pmod 3$, while $(u, 1, 0)$ works for the case $b_1 \equiv 2 \pmod 3, b_2 \equiv 1 \pmod 3$. For $n \equiv 2 \pmod 3$, if $b_1 \equiv b_2 \equiv 1 \pmod 3$, again $(u, 1, 1)$ works as a solution for $v_3(z_i) < 0$, $(u, 0, 1)$ works as a solution that can be lifted for $b_1 \equiv b_2 \equiv 2 \pmod 3$, while if $b_1 \equiv 1 \pmod 3, b_2 \equiv 2 \pmod 3$, $(u, 1, 0)$ is a solution that can be lifted, and for the case $b_1 \equiv 2 \pmod 3, b_2 \equiv 1 \pmod 3$, $(0, 1, u)$ is such a solution.

For $l = p$, $b_1 b_2 \equiv 0 \pmod{p^2} \implies \left(\frac{b_1/p}{p}\right) = \left(\frac{-n/p}{p}\right)$ and $\left(\frac{b_2/p}{p}\right) = \left(\frac{-nq}{p}\right)$ as $(b_1, b_2) \in G_E$. Fixing $z_2 = u_2, z_3 = 1$ such that $\frac{b_2}{p} u_2^2 \equiv -\frac{nq}{p} \pmod p$, one can get $z_1 = u_1$ as a solution that can be lifted to $\mathbb{Q}_p$ where $\frac{b_1}{p} u_1^2 \equiv -\frac{n}{p} \pmod p$. Otherwise, for $b_1 \equiv 0 \pmod p$, we have

$\left(\frac{b_1/p}{p}\right) = \left(\frac{n/p}{p}\right)$ and $\left(\frac{b_2}{p}\right) = \left(\frac{q}{p}\right)$. We first note that $v_p(z_2) > 0$ always in this case, and hence without loss of generality, one can solve (4.3.2) and (4.3.3) after dividing by p on both sides. Now fixing $z_2 = 0, z_3 = u_3$ such that $\frac{b_1 b_2}{p} u_3^2 \equiv \frac{nq}{p} \pmod{p}$, one can see $z_1 = u_1$ is a solution that can be lifted by Hensel's lemma for the modified equations, where $\frac{b_1}{p} u_1^2 \equiv \frac{4^m n}{p} \pmod{p}$. For $b_2 \equiv 0 \pmod{p}$, one can similarly find a solution that can be lifted to $\mathbb{Q}_p$ via Hensel's lemma.
For $l = q$, we only focus on the case of $\left(\frac{b_1}{q}\right) = \left(\frac{-n}{q}\right)$, and $(u, 0, 0)$ becomes a solution that can be lifted to $\mathbb{Q}_q$ via Hensel's lemma where $b_1 u^2 \equiv -n \pmod{q}$.
For any other primes l, the Hasse-Weil bound now guarantees one set of solutions (z_1, z_2, z_3) of (4.3.2) and (4.3.3) that does not satisfy $z_1 \equiv z_2 \equiv 0 \pmod{l}$ or $z_1 \equiv z_3 \pmod{l}$. Fixing any two of them suitably, the other one then can be lifted by Hensel's lemma as an l-adic solution of (4.3.2) and (4.3.3). This completes the proof. □

We now conclude this article with the proof of Theorem 4.22, which is a special case of the general result in Proposition 4.29.

Proof of Theorem 4.22: Under the given assumptions, as $\left(\frac{-1}{p}\right) = \left(\frac{n}{p}\right) = 1$, and $\left(\frac{q}{p}\right) = -1$, one can see $(b_1, b_2) \in G_E \implies b_1 = 1$, or 2. Also it is evident here that if $b_1 b_2 \not\equiv 0 \pmod{2}$, then $b_1 \equiv b_2 \equiv 1 \pmod{8}$, and when $b_1 b_2 \equiv 0 \pmod{4}$, then $\frac{b_1 b_2}{4} \equiv 1 \equiv n \pmod{8}$. Hence $\mathrm{Sel}_2(E) = G_E = \langle (1, p_i), (2, 2) \rangle$ for $m \geq 3$. For $m = 2$, one can see from Lemma 4.26 that $\langle (2, 2) \rangle \leq \mathrm{Sel}_2(E) \implies 1 = \frac{b_1 b_2}{4} \equiv n + b_1 \equiv 3 \pmod{8}$, a contradiction. Hence the result follows.

TABLE 4.4: Examples for area $2^m n, \tau = 2^m$ with $4^m + 1 = q$ and corresponding 2-Selmer rank

n	q	$s_2(E)$	Generators of $\mathrm{Sel}_2(E)$
$41 \cdot 73$	17	2	(1, 41),(1,73)
$41 \cdot 113$	17	2	(1,41), (1,113)
$41 \cdot 73$	65537	3	(1, 41), (1,73), (2,2)
$41 \cdot 113$	65537	3	(1,41), (1,113), (2,2)
$113 \cdot 137 \cdot 313$	65537	4	(1, 113), (1,137), (1,313), (2,2)
$113 \cdot 137 \cdot 313 \cdot 337$	65537	5	(1, 113), (1,137), (1,313), (1, 337), (2,2)

4.4 Heron Triangles of Even Area n and $\tau = \frac{1}{n}$:

In this section, we discuss the Heronian elliptic curve associated with the Heron triangles of even area n such that $n^2 + 1 = q$ for a prime q, and one of the angles θ with $\tau = \tan \frac{\theta}{2} = n^{-1}$. For positive integers k and n, we define $\Omega_{k,n} = \#\{p \ : n \equiv 0 \pmod{p} \text{ and } p \equiv k \pmod{8}\}$. The main result of this section is now the following.

Theorem 4.30. *For a square-free integer n such that $n^2+1=q$ for some prime q, let $E: y^2 = x(x-1)(x+n^2)$ be the Heronian elliptic curve associated with the non-isosceles Heron triangle of area n and an angle θ such that tan$(\frac{\theta}{2}) = n^{-1}$. Then Sel$_2(E/\mathbb{Q}) \cong (\mathbb{Z}/2\mathbb{Z})^{(\Omega_{1,n}+\Omega_{5,n})}$.*

We again note that the above result can be used as a tool to compute the Heronian elliptic curve with arbitrarily large 2-Selmer rank. This is because the 2-Selmer rank here is directly related to the number of prime factors of n of the form $1,5$ modulo 8. We first associate the Heronian elliptic curve E in Theorem 4.30 with a Heron triangle of area n and an angle θ such that $\tau = \tan\frac{\theta}{2} = \frac{1}{n}$. Assuming $\frac{n}{2} = \prod_i p_i$, we define

$$\begin{aligned}\mathbb{Q}(S,2) &= \left\{b \in \mathbb{Q}^*/(\mathbb{Q}^*)^2 : v_l(b) \equiv 0 \pmod 2 \text{ for all primes } l \notin S\right\}\\ &= \langle \pm 2,\ \pm p_i,\ \pm q : 2^2 = p_i^2 = q^2 = 1\rangle.\end{aligned}$$

By the method of 2-descent (2.48), there exists an injective homomorphism

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

defined by

$$\beta(x,y) = \begin{cases}(x, x-1) & \text{if } x \neq 0,1,\\ (-1,-1) & \text{if } x = 0,\\ (1,q) & \text{if } x = 1,\\ (1,1) & \text{if } x = \infty, \text{ i.e., if } (x,y) = O.\end{cases}$$

4.4.1 Bounding the 2-Selmer Rank :

We first look into the 2-Selmer group Sel$_2(E/\mathbb{Q})$. As mentioned previously, under the 2-descent method, each element (b_1, b_2) in Sel$_2(E/\mathbb{Q})$ corresponds to the following homogeneous space with local solutions everywhere.

$$b_1 z_1^2 - b_2 z_2^2 = 1, \tag{4.4.1}$$

$$b_1 z_1^2 - b_1 b_2 z_3^2 = -n^2, \tag{4.4.2}$$

such that $(z_1, z_2, z_3) \in \mathbb{Q}^* \times \mathbb{Q}^* \times \mathbb{Q}$, b_1, b_2 are square-free integers whose only prime factors are $2, q$ and prime factors of n. The image of $E(\mathbb{Q})_{\text{tors}}$ under the 2-descent map is $\{(1,1),(1,q),(-1,-1),(-1,-q)\}$. We start with the following result regarding l-adic solutions of the homogeneous space given by equations (4.4.1) and (4.4.2). The proof is similar to the previous chapter.

Lemma 4.31. *Let (z_1, z_2, z_3) be a solution to the homogeneous space given by equations (4.4.1) and (4.4.2). Then for each prime $l < \infty$ and all $i \in \{1, 2, 3\}$, either $v_l(z_i) \geq 0$ or $v_l(z_i) = -k$ for some positive integer k.*

Proof. For $i \in \{1, 2\}$, $v_l(z_i) < 0$ immediately implies $v_l(z_i) = -k$ for some positive integer k . If $v_l(z_3) < 0$ and $v_l(z_1) > v_l(z_3)$, then either from (4.4.2) or from subtracting (4.4.2) from (4.4.1), we get l^3 divides $b_1 b_2$, an absurdity. Hence $v_l(z_1) \leq v_l(z_3) < 0$, and using the first case of the proof, we conclude. □

Noting that we will only look into possible $(b_1, b_2) \in \text{Sel}_2(E/\mathbb{Q})/Im(E(\mathbb{Q})_{\text{tors}})$ under the 2-descent map, without loss of generality, we fix the following observations.
1) $b_1 > 0, b_2 > 0$ always (due to $l = \infty$). 2) $b_2 \not\equiv 0 \pmod{q}$.

Lemma 4.32. *Let $(b_1, b_2) \in Sel_2(E/\mathbb{Q})$. Then $b_2 = 1$ always and for an arbitrary prime p, $b_1 \equiv 0 \pmod{p} \implies p \equiv 1, 5 \pmod{8}$ and $p \neq q$.*

Proof. We first note that $b_1 \not\equiv 0 \pmod{q}$ here, and the proof is the same as in the n odd case. Similarly, we can also see that if p is an odd prime that divides n, then $b_2 \not\equiv 0 \pmod{p}$.
We now notice that b_2 is odd if $(b_1, b_2) \in \text{Sel}_2(E/\mathbb{Q})$. One can trivially observe that $\gcd(b_1, b_2) \not\equiv 0 \pmod{2}$. Now b_2 is even either implies 2 divides q when $v_2(z_i) \geq 0$ or 2 divides b_1 when $v_2(z_i) = -k$, contradiction either way.
We have now established that $b_1 \not\equiv 0 \pmod{q}$ and $b_2 = 1$ if $(b_1, b_2) \in \text{Sel}_2(E/\mathbb{Q})$.
From (4.4.1), it is evident that $b_1 \equiv 0 \pmod{p} \implies p \equiv 1, 5 \pmod{8}$. This is because (4.4.1) implies $\left(\frac{-1}{p}\right) = 1$ for the pair $(b_1, 1)$. $n^2 + 1 = q$ implies $q \equiv 5 \pmod{8}$. Subtracting (4.4.2) from (4.4.1) for homogeneous space corresponding to $(2, 1)$, we get $\left(\frac{2}{q}\right) = 1$, a contradiction for $q \equiv 5 \pmod{8}$. Hence the homogeneous space corresponding to $(2, 1)$ has no q-adic solution. This concludes the proof. □

4.4.2 Everywhere Local Solution

We prove that the homogeneous spaces corresponding to $(p, 1)$ has local solutions everywhere where p is any prime factor of n such that $p \equiv 1, 5 \pmod{8}$. We use Hensel's lemma to lift a simple root of a polynomial $f(x)$ modulo a prime l to a solution for $f(x)$ in $\mathbb{Z}_l$. Let C be the homogeneous space given by (4.4.1) and (4.4.2) corresponding to the pair $(p, 1)$. An application of smoothness of C, the degree-genus formula, and the Hasse-Weil bound give the following.
For $l \geq 5$, $l \neq t$ where $t \equiv 1, 5 \pmod{8}$ and t divides n, C is a homogeneous space of genus 1 corresponding to $(p, 1)$ or $(p_1 p_2, 1)$ with $\#C(\mathbb{F}_l) \geq 1 + l - 2\sqrt{l} \geq 2$ where $p \equiv 1, 5 \pmod{8}$. Hensel's lemma implies that the homogeneous spaces mentioned above have l-adic solution for all the primes l mentioned above. This reduces the problem to finding local solutions for only finitely many primes.

Lemma 4.33. *Let n be a integer such that $n^2+1=q$ for a prime q. Then for each prime factor, p of n, $p \equiv 1,5 \pmod 8$, the homogeneous spaces corresponding to $(p,1)$ have local solutions everywhere for $l \leq \infty$.*

Proof. As mentioned above, we need only to show local solutions exist for $l = 2,3$ and t where $t \equiv 1,5 \pmod 8$ is a prime that divides n. Fixing two of the three variables z_1, z_2, z_3, we present a set of simple roots for the system of equations (4.4.1) and (4.4.2) modulo l using Lemma 4.31 that can be lifted to $\mathbb{Q}_l$ using Hensel's lemma.
For $l=2$, For $p \equiv 5 \pmod 8$, we note that $z_1 = 1$ is a simple root modulo 8 to the system of equations $pz_1^2 - 1 = 2^2$ and $z_1^2 - 1 = -\frac{n^2}{p} \cdot 2^2$. For $l = 3$, $z_1 = 1$ is a simple root modulo 3 to the system of equations $pz_1^2 - 1 = 3^{2k}$ and $z_1^2 - 1 = -\frac{n^2}{p} \cdot 3^{2k}$ when $p \equiv 1 \pmod 3$. When $p \equiv 2 \pmod 3$, one can see that $z_1 = 1$ is a simple root modulo 3 to the simultaneous equations $pz_1^2 - 1 = 1$ and $z_1^2 - 0 = -\frac{n^2}{p}$.
For $l = t$, $t \equiv 1,5 \pmod 8$ and t divides n, $z_2 = a$ such that $a^2 \equiv -1 \pmod p$ is a simple root modulo p for equations $p \cdot 0^2 - z_2^2 = 1$ and $p \cdot 0^2 - z_2^2 = 2q$. This concludes the proof. □

We are now in a position to restrict the size of the 2-Selmer group $\mathrm{Sel}_2(E/\mathbb{Q})$. The proof requires the results obtained in earlier sections.

Proof of Theorem 4.30. We observe that from Lemma 4.32, $(b_1, b_2) \in \mathrm{Sel}_2(E/\mathbb{Q})$ implies $(b_1, b_2) = (p, 1)$ such that $p \equiv 1,5 \pmod 8$ divides n are the only possibilities. In Lemma 4.33, we established the homogeneous spaces corresponding to those pairs have local solutions everywhere; hence, the result follows. □

We conclude this section with a table of examples that support the aforementioned result.

TABLE 4.5: Examples for area $n, \tau = \frac{1}{n}$ with $n^2+1=q$ and corresponding 2-Selmer rank

n	q	2- Selmer Rank of E	Generators
2	5	0	-
$2 \cdot 5$	101	1	(5,1)
$2 \cdot 3 \cdot 11$	4357	0	-
$2 \cdot 5 \cdot 13$	16901	2	(5,1),(13,1)
$2 \cdot 7 \cdot 29$	164837	1	(29,1)
$2 \cdot 5 \cdot 17$	28901	2	(5,1),(17,1)
$2 \cdot 7 \cdot 17 \cdot 23$	29964677	1	(17,1)
$2 \cdot 3 \cdot 5 \cdot 7 \cdot 11$	5336101	1	(5,1)
$2 \cdot 3 \cdot 5 \cdot 7 \cdot 13$	7452901	2	(5,1),(13,1)
$2 \cdot 3 \cdot 5 \cdot 7 \cdot 37$	7452901	2	(5,1),(37,1)
$2 \cdot 3 \cdot 5 \cdot 7 \cdot 41$	74132101	2	(5,1), (41,1)
$2 \cdot 5 \cdot 13 \cdot 17$	4884101	3	(5,1),(13,1),(17,1)

Chapter 5

Diophantine Equation and Heron Triangle

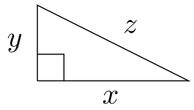
*This chapter contains the following article:

Ghale Vinodkumar, Das Shamik, Chakraborty Debopam; "A Heron triangle and a Diophantine equation", *Periodica Mathematica Hungarica* 2 (2022) 530-537.

Chakraborty Debopam, Ghale Vinodkumar; "A Family of Heronian elliptic curves with non-trivial Shafarevich-Tate group", (2023) (In communication).

Diophantine equations and their solvability have played a key role in Number theory. Understanding the solution of a certain Diophantine equation directly affects the arithmetic of number-theoretic objects frequently. Sierpinsky had proved that the only positive solution (x, y, z) to the non-linear Diophantine equation $3^x + 4^y = 5^z$ is $(2, 2, 2)$ in [45]. Later, L. Jeśmanowicz extended Sierpinsky's result in [25] and conjectured that for fixed coprime integers m, n with $m > n$ and of different parity, the exponential Diophantine equation $(m^2 - n^2)^x + (2mn)^y = (m^2 + n^2)^z$ has only one positive integer solution $(2, 2, 2)$. Many particular cases of this conjecture have been proved over the years in [10], [30], [32], [36], [37], and [50], including a non-coprimality case of the Jeśmanowicz conjecture. The works of Kramer and Luca in [29] showed a pathway regarding understanding a Diophantine equation arising from *Heron triangles*. In [55], X. Yan showed that for fixed coprime positive integers m and n with different parity, the Diophantine equation $(m^2 + n^2)^x + (2mn)^y = (m + n)^{2z}$ has no solution with $y \geq 2$. We show that the Diophantine equation $(x^2 + y^2)^2 + (2pxy)^2 = z^2$ with $\gcd(x, y) = 1$ is solvable if and only if there exists a Heron triangle with area p and an angle θ such that $\tau = \tan\frac{\theta}{2} = \frac{1}{p}$. Hence, We conclude that there is no solution to the aforementioned Diophantine equation when $p \equiv 1,\ 5 \pmod 8$ with the help of Theorem 3.1 from the third chapter. Then, we generalize the result for the area being any squarefree integer n and $\tau = \frac{1}{n}$.

Pythagoras' theorem enables us to see the existence of the right triangle with the area n is equivalent to the solvability of Diophantine equation $x^2 + y^2 = z^2$ and $\dfrac{xy}{2} = n$ with $x, y, z \in \mathbb{Q}$.



i.e., n is a congruent number if and only if the two equations $x^2 + y^2 = z^2$ and $\dfrac{xy}{2} = n$ have solutions with $x, y, z \in \mathbb{Q}$.

5.1 Heron Triangle of Area $n = p$:

We first establish a one-one correspondence between *Heron triangles* and the solvability of certain Diophantine equations. The existence of such *Heron triangles* was already discussed in Chapter 3 via the algebraic rank computation of corresponding elliptic curves.

Theorem 5.1. *For every fixed odd prime p, there is a one-one correspondence between the solvability of the Diophantine equation $(x^2 + y^2)^2 + (2pxy)^2 = z^2$ with $\gcd(x, y) = 1$ and the existence of a Heron triangle with area p and an angle θ such that $\tan\frac{\theta}{2} = \frac{1}{p}$. Hence, if $p \equiv 5 \pmod 8$, then $(x^2 + y^2)^2 + (2pxy)^2 = z^2$ has no solution if $p^2 + 1 = 2q$ for some prime q.*

Proof: We first notice that both $\sin\theta$ and $\cos\theta$ will be rational. From the laws of sines and cosines for a triangle, we get the following;

$$\cos\theta = \frac{a^2 + b^2 - c^2}{2ab}, \quad \sin\theta = \frac{2p}{ab}, \quad \tan\frac{\theta}{2} = \frac{4p}{(a + b)^2 - c^2}. \tag{5.1.1}$$

From (5.1.1) and the fact that we have assumed $\tan\frac{\theta}{2} = \frac{1}{p}$, we arrived at the following conclusion;

$$(a+b)^2 = c^2 + 4p^2 = c^2 + (2p)^2. \tag{5.1.2}$$

Also from (5.1.1) and the fact that $\sin^2\theta + \cos^2\theta = 1$, we get the following;

$$\Big(\frac{a^2+b^2-c^2}{2ab}\Big)^2 + \Big(\frac{2p}{ab}\Big)^2 = 1 \text{ which implies } ab = 1 + p^2. \tag{5.1.3}$$

Equations (5.1.2) and (5.1.3) together implies that $(a-b)^2 = (a+b)^2 - 4ab = c^2 - 4$. Assuming $a - b = u = \frac{u_1}{u_2}$ and $c = w = \frac{w_1}{w_2}$, where both the representations are in their lowest forms, we observe that $\frac{w_1^2 - 4w_2^2}{w_2^2} = \frac{u_1^2}{u_2^2}$. Since $\gcd(w_1^2 - 4w_2^2, w_2^2) = 1$, we can write $u_2^2 = w_2^2$ and $u_1^2 = w_1^2 - 4w_2^2$ which then implies $w_1^2 = u_1^2 + 4w_2^2$. From the fact that $\gcd(w_1, w_2) = 1$, it can be immediately seen $w_1, 2w_2$ and u_1 are all pairwise coprime and they form a *Pythagorean primitive triplet*. Hence, there exist integers m, n with $m > n$ such that $\gcd(m,n) = 1$ and $u_1 = m^2 - n^2$, $2w_2 = 2mn$ and $w_1 = m^2 + n^2$. This implies $c = \frac{w_1}{w_2} = \frac{m^2+n^2}{mn} = \frac{m}{n} + \frac{n}{m}$. Similarly from the fact that $(a-b)^2 = \frac{u_1^2}{w_2^2}$, one can observe that $a - b = \frac{m}{n} - \frac{n}{m}$, under the assumption $a \geq b$ which implies that $b = a - (\frac{m}{n} - \frac{n}{m})$. If $b \geq a$, one can change $a - b$ suitably. Now from (5.1.2), we know that $(a+b)^2 = 4p^2 + c^2 = 4p^2 + (\frac{m}{n} + \frac{n}{m})^2$, where replacing b as in the previous line, we get the following;

$$a = \frac{\frac{m}{n} - \frac{n}{m} \pm \sqrt{(\frac{m}{n} + \frac{n}{m})^2 + 4p^2}}{2} = \frac{m^2 - n^2 \pm \sqrt{(m^2+n^2)^2 + (2pmn)^2}}{2mn}.$$

This immediately gives us a solution to the Diophantine equation $z^2 = (x^2+y^2)^2 + (2pxy)^2$ with $\gcd(x,y) = 1$ in the form of

$$z = 2mna - (m^2 - n^2), \;\; x = m \text{ and } y = n.$$

For the converse implication, we begin with the assumption that there exist positive integers x, y and z such that $\gcd(x,y) = 1$ and $z^2 = (x^2+y^2)^2 + (2pxy)^2$. Define

$$a = \frac{\frac{x}{y} - \frac{y}{x} + \sqrt{(\frac{x}{y} + \frac{y}{x})^2 + 4p^2}}{2} = \frac{\frac{x}{y} - \frac{y}{x} + \frac{z}{xy}}{2}, \;\; b = a - (\frac{x}{y} - \frac{y}{x}) \text{ and } c = \frac{x}{y} + \frac{y}{x}.$$

Then a, b, c are all positive integers. Also, $ab = 1 + p^2$ and $a - b = \frac{y}{x} - \frac{x}{y}$. Now suppose we have a triangle with sides a, b and c and the angle θ between the sides of the length a and b. Then by the law of cosines,

$$\cos\theta = \frac{a^2+b^2-c^2}{2ab} = \frac{(a-b)^2 - c^2}{2ab} + 1 = \frac{p^2-1}{p^2+1} \in \mathbb{Q}.$$

Similarly, from the formula of $\sin\theta = \sqrt{1 - \cos^2\theta}$ we get, $\sin\theta = \frac{2p}{p^2+1} = \frac{2p}{ab}$. This implies that the triangle have area $\frac{1}{2}ab\sin\theta = p$. Substituting the values of a, b and c in terms of

x, y and z and observing the fact that $z^2 = (x^2+y^2)^2 + (2pxy)^2$, one can easily observe that $\tan\frac{\theta}{2} = \frac{4p}{(a+b)^2-c^2} = \frac{1}{p}$ too. This concludes the proof of the statement. □

The following result looks into the solution of the Diophantine equation $x^2 + y^2 + x^2y^2 = p^2$ for some odd prime number p. The result follows directly from Theorem 5.1.

Corollary 5.2. *For an odd prime p, there exists a Heron triangle with area p and an angle θ such that $\tan\frac{\theta}{2} = \frac{1}{p}$ whenever the Diophantine equation $p^2 = x^2 + y^2 + x^2y^2$ is solvable.*

Proof: By the Pythagorean primitive element theorem, any solution (m, n, l) of $(x^2+y^2)^2 + (2pxy)^2 = z^2$ with $\gcd(m, n) = 1$ implies that there exist co-prime natural numbers r and s such that $m^2+n^2 = r^2-s^2$, $2pmn = 2prs$ and $l = r^2+s^2$. Hence $r = p$ and $s = mn$ will be a possible solution if $r^2 - s^2 = p^2 - m^2n^2 = m^2 + n^2$. This concludes the proof of the statement.

5.1.1 A Generalization

Observing the simple fact that we are not using any of the properties of prime p in the above theorem, we generalize the result using the same technique.

Theorem 5.3. *For every squarefree integer n, there is a one-one correspondence between the solvability of the Diophantine equation $(x^2+y^2)^2 + (2nxy)^2 = z^2$ with $\gcd(x, y) = 1$ and the existence of a Heron triangle with area n and an angle θ such that $\tan\frac{\theta}{2} = \frac{1}{n}$.*

Proof: From the laws of sines and cosines for a triangle, we get the following;

$$\cos\theta = \frac{a^2+b^2-c^2}{2ab}, \quad \sin\theta = \frac{2n}{ab}, \quad \tan\frac{\theta}{2} = \frac{4n}{(a+b)^2-c^2}. \tag{5.1.4}$$

From (5.1.4) and the fact that we have assumed $\tan\frac{\theta}{2} = \frac{1}{n}$, we get;

$$(a+b)^2 = c^2 + 4n^2 = c^2 + (2n)^2. \tag{5.1.5}$$

Using (5.1.4) and the fact that $\sin^2\theta + \cos^2\theta = 1$, we get the following;

$$\left(\frac{a^2+b^2-c^2}{2ab}\right)^2 + \left(\frac{2n}{ab}\right)^2 = 1 \text{ which implies } ab = 1 + n^2. \tag{5.1.6}$$

Equations (5.1.5) and (5.1.6) together implies that $(a-b)^2 = (a+b)^2 - 4ab = c^2 - 4$. Assuming $a - b = u = \frac{u_1}{u_2}$ and $c = w = \frac{w_1}{w_2}$, where both the representations are in their lowest forms, we observe that $\frac{w_1^2-4w_2^2}{w_2^2} = \frac{u_1^2}{u_2^2}$. Since $\gcd(w_1^2 - 4w_2^2, w_2^2) = 1$, we can write $u_2^2 = w_2^2$ and $u_1^2 = w_1^2 - 4w_2^2$ which then implies $w_1^2 = u_1^2 + 4w_2^2$. From the fact that $\gcd(w_1, w_2) = 1$, it can be immediately seen $w_1, 2w_2$ and u_1 are all pairwise coprime and they form a *Pythagorean primitive triplet*. Hence, there exist integers m, k with $m > k$ such that $\gcd(m, k) = 1$ and $u_1 = m^2 - k^2$, $2w_2 = 2mk$ and $w_1 = m^2 + k^2$. This implies $c = \frac{w_1}{w_2} = \frac{m^2+k^2}{mk} = \frac{m}{k} + \frac{k}{m}$. Similarly from the fact that $(a-b)^2 = \frac{u_1^2}{w_2^2}$, one can observe that $a - b = \frac{m}{k} - \frac{k}{m}$, under the assumption $a \geq b$ which implies that $b = a - (\frac{m}{k} - \frac{k}{m})$. If $b \geq a$, one can change $a - b$ suitably. Now from (5.1.5), we know that $(a+b)^2 = 4n^2 + c^2 = 4n^2 + (\frac{m}{k} + \frac{k}{m})^2$, where replacing b as in the previous line, we get the following;

$$a = \frac{\frac{m}{k} - \frac{k}{m} \pm \sqrt{(\frac{m}{k} + \frac{k}{m})^2 + 4n^2}}{2} = \frac{m^2 - k^2 \pm \sqrt{(m^2+k^2)^2 + (2nmk)^2}}{2mk}. \tag{5.1.7}$$

This immediately gives us a solution to the Diophantine equation $z^2 = (x^2+y^2)^2 + (2nxy)^2$ with $\gcd(x, y) = 1$ in the form of

$$z = 2mka - (m^2 - k^2),\ \ x = m \text{ and } y = k. \tag{5.1.8}$$

For the converse implication, we begin with the assumption that there exist positive integers x, y and z such that $\gcd(x, y) = 1$ and $z^2 = (x^2 + y^2)^2 + (2nxy)^2$. Define

$$a = \frac{\frac{x}{y} - \frac{y}{x} + \sqrt{(\frac{x}{y} + \frac{y}{x})^2 + 4n^2}}{2} = \frac{\frac{x}{y} - \frac{y}{x} + \frac{z}{xy}}{2},\ b = a - (\frac{x}{y} - \frac{y}{x}) \text{ and } c = \frac{x}{y} + \frac{y}{x}. \tag{5.1.9}$$

Then a, b, c are all positive integers. Also, $ab = 1 + n^2$ and $a - b = \frac{y}{x} - \frac{x}{y}$. Now suppose we have a triangle with sides a, b and c and the angle θ between the sides of the length a and b. Then by the law of cosines,

$$\cos\theta = \frac{a^2 + b^2 - c^2}{2ab} = \frac{(a-b)^2 - c^2}{2ab} + 1 = \frac{n^2 - 1}{n^2 + 1} \in \mathbb{Q}.$$

Similarly, from the formula of $\sin\theta = \sqrt{1 - \cos^2\theta}$ we get, $\sin\theta = \frac{2n}{n^2+1} = \frac{2n}{ab}$. This implies that the triangle have area $\frac{1}{2}ab\sin\theta = p$. Substituting the values of a, b and c in terms of x, y and z and observing the fact that $z^2 = (x^2 + y^2)^2 + (2nxy)^2$, one can easily observe that $\tan\frac{\theta}{2} = \frac{4n}{(a+b)^2 - c^2} = \frac{1}{n}$. □

With the help of results in the previous chapters, we get the Heronian elliptic curves with positive ranks. We conclude this section by enlisting examples for such Heron triangles and corresponding solutions of Diophantine equations below.

Table 5.1: Transformation between Heron triangle and solutions of Diophantine equation

Sides to Solution Triplet	Solution Triplet to Sides
$c = \dfrac{w_1}{w_2} = \dfrac{x^2+y^2}{xy}$	$a = \dfrac{\dfrac{x}{y} - \dfrac{y}{x} + \dfrac{z}{xy}}{2}$
$a - b = \dfrac{u_1}{u_2} = \dfrac{x^2-y^2}{xy}$	$b = a - \left(\dfrac{x}{y} - \dfrac{y}{x}\right)$
adding u_1 and w_1, we get x and y	$c = \dfrac{x}{y} + \dfrac{y}{x}$
$z = 2xya - (x^2 - y^2)$	

Table 5.2: Examples of Heron triangles and solution of corresponding Diophantine equation

n	Point on elliptic curve	Sides of triangle	Solution triplet
3	(9, 36)	$\left[4, \dfrac{5}{2}, \dfrac{5}{2}\right]$	(2, 1, 13)
$2 \cdot 5$	$\left(\dfrac{5}{4}, \dfrac{45}{8}\right)$	$\left[\dfrac{202}{9}, \dfrac{9}{2}, \dfrac{325}{18}\right]$	(18, 1, 485)
11	$\left(\dfrac{121}{49}, \dfrac{7260}{343}\right)$	$\left[\dfrac{427}{30}, \dfrac{60}{7}, \dfrac{1261}{210}\right]$	$(35, 6, 4789)$
$5 \cdot 17$	$\left(\dfrac{425}{64}, \dfrac{266475}{512}\right)$	$\left[\dfrac{57808}{627}, \dfrac{627}{8}, \dfrac{70057}{5016}\right]$	(264, 19, 855593)

5.2 The 2-Selmer group of E for $p \equiv 1 \pmod 8$:

We now look into the 2-part of the Shafarevich-Tate group of elliptic curves associated with the Heron triangles with area $p \equiv 1 \pmod 8$. We note that we have already discussed in detail the Mordell-Weil group structure for similar Heronian elliptic curves in Chapter 3 , Section 3.1, when $p \not\equiv 1 \pmod 8$. The main result of this section is as follows.

Theorem 5.4. *Let $E : y^2 = x(x-1)(x+p^2)$ denote a Heronian elliptic curve associated with a Heron triangle of area p and one of the angles θ such that $\tan\frac{\theta}{2} = p^{-1}$ where $p \equiv 1 \pmod 8$ is a prime, $p^2 + 1 = 2q$ for a prime q. Then $r(E/\mathbb{Q}) = 2$ if the Diophantine equation $p(x^2 - py^2)^2 - 4x^2y^2 = z^2$ has solution for odd integer z. Otherwise, $r(E/\mathbb{Q}) = 0$, and $\text{Ш}(E/\mathbb{Q})[2] \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.*

5.2.1 Local Solutions for the Homogeneous Spaces

A background of the full 2-descent method for similar elliptic curves is elaborately described in Chapter 3.1 for $p \not\equiv 1 \pmod 8$. For brevity, we include a brief background below for the case $p \equiv 1 \pmod 8$.

Let S be the set consisting of all finite places at which E has a bad reduction, the infinite places, and the prime 2. We define

$$\begin{aligned}\mathbb{Q}(S,2) &= \left\{b \in \mathbb{Q}^*/(\mathbb{Q}^*)^2 : v_l(b) \equiv 0 \pmod 2 \text{ for all primes } l \notin S\right\} \\ &= \langle \pm 2,\ \pm p,\ \pm q\rangle.\end{aligned} \tag{5.2.1}$$

If β denotes the 2-descent map, then from (2.48), we can say that $\beta(E(\mathbb{Q})_{\text{tors}}) = \{(1,1),(-1,-1),(1,2q),(-1,-2q)\}$. 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 $O,(0,0),(1,0)$ under β, where $\mathbb{Q}(S,2) = \{\pm 1,\ \pm 2,\ \pm p,\ \pm q,\ \pm 2p,\ \pm 2q,\ \pm pq,\ \pm 2pq\}$, 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

$$b_1 z_1^2 - b_2 z_2^2 = 1, \tag{5.2.2}$$

$$b_1 z_1^2 - b_1 b_2 z_3^2 = -p^2, \tag{5.2.3}$$

have a solution $(z_1,z_2,z_3) \in \mathbb{Q}^* \times \mathbb{Q}^* \times \mathbb{Q}$.

5.2.2 Bounding the Size of 2-Selmer Group of E

We are now in a position to look into the Selmer group structure of E for $p \equiv 1 \pmod 8$. We first prove the following result for all prime l.

Lemma 5.5. *Suppose (5.2.2) and (5.2.3) have a solution $(z_1,z_2,z_3) \in \mathbb{Q}_l \times \mathbb{Q}_l \times \mathbb{Q}_l$ for any prime l. If $v_l(z_i) < 0$ for any one $i \in \{1,2,3\}$, 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 (5.2.2) one can get that

$$b_1 u_1^2 - b_2 u_2^2 l^{2(k_2-k_1)} = l^{-2k_1}.$$

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 (5.2.2) we get

$$b_1 u_1^2 l^{2(k_1-k_2)} - b_2 u_2^2 = l^{-2k_2},$$

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 (5.2.3), we have

$$b_1 u_1^2 - b_1 b_2 u_3^2 l^{2(k_3-k_1)} = -p^2 \cdot l^{-2k_1}.$$

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

$$b_1 u_1^2 l^{2(k_1-k_3)} - b_1 b_2 u_3^2 = -p^2 \cdot l^{-2k_3}, \tag{5.2.4}$$

which implies l^2 must divide $b_1 b_2$, i.e., $l = 2, p$ or q. If $l = p$, then from (5.2.4) we arrive at the contradiction that p^3 divides $b_1 b_2$ whereas b_1 and b_2 are square-free. For $l = 2$ and q, one can notice from (5.2.3) that if $k_3 \leq -2$, then l^3 divides $b_1 b_2$, a contradiction again. This in turn implies $k_3 = -1$ and hence $k_1 \geq 0$ which contradicts the assumption that $k_1 < 0$. Hence $k_1 < 0 \implies k_3 = k_1$.
Now, suppose $k_3 < 0$. If $k_1 < 0$, then from the previous part we already established $k_1 = k_2 = k_3 = -k$ for some positive integer k. So without loss of generality, we can assume $k_1 \geq k_3$. If $k_3 < k_1$ and $k_3 < 0$, then as mentioned previously in this proof, one can get that $b_1 b_2 \equiv 0 \pmod{l^2}$ and $l = 2$ or q. Now we subtract (5.2.3) from (5.2.2) and observe that

$$b_1 b_2 u_3^2 - b_2 u_2^2 l^{2(k_2-k_3)} = 2q \cdot l^{-2k_3}.$$

If $k_2 > k_3$, we get a contradiction that l^3 divides $b_1 b_2$ for $l = 2, q$. Therefore, $k_2 \leq k_3 < 0$ but then by the first part, $k_1 = k_2 \leq k_3$, a contradiction to the assumption $k_1 > k_3$. Hence $k_3 < 0 \implies k_1 = k_3$. Together, now we obtain $k_1 = k_2 = k_3 = -k < 0$ for some integer k if $k_1 < 0$ or $k_2 < 0$ or $k_3 < 0$. □

We can now bound the size of the 2-Selmer group of the Heronian elliptic curve E for $p \equiv 1 \pmod 8$. Without loss of generality, we can only focus on the homogeneous spaces corresponding to pairs (b_1, b_2) such that $b_1 > 0, b_2 > 0$ if $b_1 b_2 > 0$. This is because every pair (b_1, b_2) such that $b_1 b_2 > 0$ will belong to the same coset of $(-b_1, -b_2)$ in the quotient group $\mathrm{Im}(\beta)/A$ where $A = \{(-1,-1), (1, 2q), (-1, -2q), (1,1)\}$. Using the exactly similar argument, without loss of generality, we can only focus on the local solutions of the homogeneous spaces corresponding to (b_1, b_2) such that b_2 is odd.

Lemma 5.6. *Let $(b_1, b_2) \notin \{(1,1),(1,q),(p,1),(p,q)\}$. Then the corresponding homogeneous space can not have local solutions for all primes $l \leq \infty$.*

Proof. 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 $-p^2 > 0$ in (5.2.3), which is absurd. Similarly, $b_1 < 0$ and $b_2 > 0$ implies $1 < 0$ in (5.2.2), contradiction again. Thus, the homogeneous space corresponding to (b_1, b_2) has no l-adic solutions for $l = \infty$ if $b_1 b_2 < 0$.

If $\gcd(b_1, b_2) \equiv 0 \pmod p$ and $v_p(z_i) < 0$ for any $i \in \{1,2,3\}$, then from Lemma 5.5 and (5.2.3), one can get p^2 divides b_1, a contradiction. If $\gcd(b_1, b_2) \equiv 0 \pmod p$ and $v_p(z_i) \geq 0$ for all $i \in \{1,2,3\}$, then from Lemma 5.5 and (5.2.2), one can get p divides 1, again a contradiction. Hence $\gcd(b_1, b_2) \not\equiv 0 \pmod p$. Now moreover, if p divides b_2 then $v_p(z_i) \geq 0$ implies p divides b_1 or z_1 from (5.2.3), a contradiction as then either $\gcd(b_1, b_2) \equiv 0 \pmod p$ or p divides 1 from (5.2.2). If $v_p(z_i) < 0$, then also from Lemma 5.5 and (5.2.2), one gets p divides b_1, a contradiction again.

If q divides b_1, then from the equation $b_1 b_2 z_3^2 - b_2 z_2^2 = 2q$, one get that q divides b_2 if $v_q(z_3) \geq 0$ and $v_q(z_2) \geq 0$. This, in turn, implies q divides 1 from (5.2.2) and Lemma 5.5, a contradiction. Otherwise, again from Lemma 5.5 and (5.2.2), one gets that q divides b_2 and hence from (5.2.3), $b_1 \equiv 0 \pmod{q^2}$, a contradiction.

We now show that for the existence of local solutions everywhere, b_1 needs to be odd always. Otherwise, b_1 even and $v_2(z_i) < 0$ implies that $p^2 \equiv 0 \pmod 2$ from (5.2.3), a contradiction. Else, from Lemma 5.5 and (5.2.2), one can see that b_2 is even, a contradiction from the assumption made above.

Now we can see for a homogeneous space corresponding to (b_1, b_2) to have local solution everywhere $b_1 \in \{1, p\}$ and $b_2 \in \{1, q\}$. □

5.2.3 Everywhere Local Solution :

Now we prove that the homogeneous spaces corresponding to $(p,1)$ and $(1,q)$ have local solutions everywhere. We use Hensel's lemma to lift a solution modulo a prime l to a solution in $\mathbb{Q}_l$.

Lemma 5.7. *The homogeneous spaces corresponding to $(p,1)$ and $(1,q)$ have local solutions everywhere for $l \leq \infty$.*

Proof. Suppose C is the homogeneous space given by (5.2.2) and (5.2.3) corresponding to the pair $(p,1)$. Then C is a twist of E. The Jacobian of the intersection of (5.2.2) and (5.2.3) for $(p,1)$ is

$$\begin{pmatrix} 2p \cdot z_1 & -2 \cdot z_2 & 0 \\ 2p \cdot z_1 & 0 & -2p \cdot z_3 \end{pmatrix}$$

one can easily observe has rank 2 whenever $l \neq 2, p, q$. Hence except for those l's, the topological genus becomes the same as the arithmetic genus, which is 1 by the degree-genus formula. By the Hasse-Weil bound, we have

$$\#C(\mathbb{F}_l) \;\geq\; 1 + l - 2\sqrt{l} \;\geq\; 2 \qquad \text{for } l \geq 5,\; l \neq p.$$

Hence, 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 1 from (5.2.2), a contradiction. Similarly, $z_1 \equiv z_3 \equiv 0 \pmod{l}$ implies $-p \equiv 0 \pmod{l^2}$ from (5.2.3), contradiction again. Fixing two of z_1, z_2 and z_3, one can now convert equations (5.2.2) and (5.2.3) into a system of equations in one variable with a simple root over $\mathbb{F}_l$. That common solution can be lifted to $\mathbb{Z}_l$ via Hensel's lemma.

For $l = p$, we first notice that $\left(\frac{-1}{p}\right) = 1$ as $p \equiv 1 \pmod{8}$. Hence there exists $a \in \mathbb{Z}$ such that $a^2 \equiv -1 \pmod{p}$. Now fixing $z_1 = 1$ in equations (5.2.2) and (5.2.3), we can see that $z_2 = a$ and $z_3 = 1$ are two simple roots of two single variable polynomials and hence can be lifted to $\mathbb{Z}_p$.

For $l = q$, we first note that $p \equiv 1 \pmod{8} \implies \left(\frac{p}{q}\right) = \left(\frac{q}{p}\right) = 1$. Now fixing $z_1 = z_3 = 1$, one can immediately notice that $(1, a, 1)$ where $a^2 \equiv p \pmod{q}$, is a solution modulo q to (5.2.2) and (5.2.3) with $v_q(z_i) < 0$ that can be lifted to $\mathbb{Q}_q$ by Hensel's lemma.

For $l = 3$ and $p \equiv 1 \pmod{3}$, using Lemma 5.5, we look into solutions for the equations $pz_1^2 - z_2^2 = 3^{2k}$ and $z_1^2 - z_3^2 = -p \cdot 3^{2k}$ in $\mathbb{Z}_3$. Fixing $z_1 = 1$, one can notice that $z_2 = z_3 = 1$ are two simple solutions and hence can be lifted to solution in $\mathbb{Z}_3$ for the equations mentioned above. Diving by 3^{2k}, it gives rise to solutions in $\mathbb{Q}_3$ for equations (5.2.2) and (5.2.3). For $p \equiv 2 \pmod{3}$, fixing $z_2 = 1$ and $z_3 = 0$ in (5.2.2) and (5.2.3) respectively will give $z_1 = 1$ as a simple solution modulo 3 and hence can be lifted to $\mathbb{Z}_3$ via Hensel's lemma.

For the case $l = 2$, just as in the beginning of the case $l = 3$, using Lemma 5.5, we find solutions in $\mathbb{Z}_2$ for the equations $pz_1^2 - z_2^2 = 2^{2k}$ and $z_1^2 - z_3^2 = -p \cdot 2^{2k}$ such that $k \geq 2$. Fixing $z_2 = z_3 = 1$ gives rise to $z_1 \equiv 1 \pmod{8}$ as a solution modulo 8 to both those equations that can be lifted to a solution in $\mathbb{Z}_2$. This ensures a solution for the homogeneous space corresponding to $(p, 1)$ in $\mathbb{Q}_2$ also.

$\underline{\text{For the case } (b_1, b_2) = (1, q),}$ the proof follows a very similar way as in the case $(b_1, b_2) = (p, 1)$. For $l \geq 5, l \neq p, q$, the homogeneous spaces C corresponding to $(1, q)$ given by equations (5.2.2) and (5.2.3) are of genus 1 and have solutions in $\mathbb{F}_l$ by Hasse-Weil bound and can be lifted to $\mathbb{Z}_l$ via a similar argument used in the previous case.

For $l = q$, because $-p^2 \equiv 1 \pmod{q}$, fixing $z_2 = z_3 = 0$ in equations (5.2.2) and (5.2.3) gives $z_1 = 1$ as a solution to the homogeneous space modulo q that can be lifted to $\mathbb{Z}_l$ via Hensel's lemma.

For $l = p$, we give a solution for the case $v_p(z_i) < 0$. Because $2q \equiv 1 \pmod{p}$, one can notice that fixing $z_1 = 1$ and then choosing $z_2 = 1$ and $z_3 = a$ is a solution that can be lifted to $\mathbb{Z}_l$ via Hensel's lemma where $a^2 \equiv 2 \pmod{p}$.

For the case $l = 3$, fixing $z_1 = 1$ and choosing $z_2 \equiv z_3 \not\equiv 0 \pmod 3$ gives rise to solutions for the equations $z_1^2 - qz_2^2 = 3^{2k}$ and $z_1^2 - qz_2^2 = -p^2 \cdot 3^{2k}$. This solution can be lifted to $\mathbb{Z}_l$ and then give solution for (5.2.2) and (5.2.3) in $\mathbb{Q}_l$ as mentioned in the previous part.
For the case $l = 2$, noticing the fact $p \equiv 1 \pmod 8 \implies q \equiv 1 \pmod 8$, the proof follows the same way with the same choice of solutions modulo 8 for the case $(b_1, b_2) = (p, 1)$. □

5.2.4 2-Part of the Shafarevich-Tate Group :

In this section, we cover the pairs $(p, 1)$ and $(1, q)$. We use the fact that due to Hilbert's class field theorem, the existence of an unramified abelian extension of degree n of a number field K is equivalent to the class number $h(K) \equiv 0 \pmod n$. We are now in a position to prove the following result.

Proof of Theorem 5.4: We start with the possibility of the homogeneous space corresponding to $(p, 1)$ in $Ш(E/\mathbb{Q})[2]$. Let $z_i = \frac{a_i}{d_i}$ for $i = 1, 2, 3$ is a rational solution set for equations (5.2.2) and (5.2.3) where the rational numbers z_i are in their lowest form i.e. $\gcd(a_i, d_i) = 1$ for all $i = 1, 2, 3$. It can be shown easily that $d_1^2 = d_2^2 = d_3^2 = d^2$ for some integer d. So now we have the following three equations for the case $(p, 1)$;

$$pa_1^2 - a_2^2 = d^2, \tag{5.2.5}$$

$$pa_1^2 - pa_3^2 = -p^2 \cdot d^2, \tag{5.2.6}$$

$$pa_3^2 - a_2^2 = 2q \cdot d^2. \tag{5.2.7}$$

We first claim that d is even; hence, a_i is odd for each $i = 1, 2, 3$. Otherwise, from (5.2.7), noticing the fact that $q \equiv 1 \pmod 8$, one can observe $a_3^2 - a_2^2 \equiv 2 \pmod 8$, a contradiction. From (5.2.6), one can actually see that $d^2 \equiv a_1^2 - a_3^2 \equiv 0 \pmod 8 \implies d \equiv 0 \pmod 4$.
A straightforward calculation shows that there are no common odd prime factors of $a_1 + a_3$ and $a_1 - a_3$. Assuming $a_i \geq 0$ for all $i = 1, 2, 3$, (5.2.6) then implies that one of the two possibilities of $a_1 + a_3$ and $a_1 - a_3$ is

$$a_1 + a_3 = p \cdot 2^{n_1} \cdot m_1^2, \; a_1 - a_3 = -2^{n_2} \cdot m_2^2$$

where $m = m_1 m_2$ is odd, $n = n_1 + n_2 \geq 4$ and $d^2 = 2^n \cdot m^2$. The fact that a_3 is odd and $2a_3 = p \cdot 2^{n_1} \cdot m_1^2 + 2^{n_2} \cdot m_2^2$ now implies that either $a_3 = p \cdot 2^{n-2} \cdot m_1^2 + m_2^2$ or $a_3 = p \cdot m_1^2 + 2^{n-2} \cdot$. In either way, $a_3 \equiv 1 \pmod 4$. Same is true for the case when $a_1 + a_3 = 2^{n_1} \cdot m_1^2, \; a_1 - a_3 = -p \cdot 2^{n_2} \cdot m_2^2$. Now if one defines $\alpha = a_3 + d\sqrt{p} \in \mathbb{Q}(\sqrt{p})$, then from (5.2.6) we get $N_{K/\mathbb{Q}}(\alpha) = a_1^2$ where $K = \mathbb{Q}(\sqrt{p})$. Because $\gcd(a_1, a_3) = 1$ can be proved easily, one can also observe that $\gcd(\alpha, \bar{\alpha}) = 1$ in O_K, the ring of integers of K, where $\bar{\alpha} = a_3 - d\sqrt{p}$. This in turn implies that $\alpha \mathrm{O}_K = \mathfrak{a}^2$ for some ideal $\mathfrak{a}$ which implies no finite primes except possibly primes above 2 ramifies in $K(\sqrt{\alpha})/K$. But $\alpha = a_3 + d\sqrt{p} \equiv 1 \pmod 4$ implies 2 also does not ramify in $K(\sqrt{\alpha})/K$. It is also clear that infinite primes also do not ramify in $K(\sqrt{\alpha})/K$ as $K(\sqrt{\alpha}) \subset \mathbb{R}$. Hence from Hilbert's class field theorem, we can conclude that $K = \mathbb{Q}(\sqrt{p})$ has an even class number whenever the homogeneous space corresponding to $(p, 1)$ has a rational solution. But it is well known that the class number of $\mathbb{Q}(\sqrt{p})$ is always odd [13]. Hence $(p, 1) \in Ш(E/\mathbb{Q})[2]$ if $\sqrt{\alpha} \notin \mathbb{Q}(\sqrt{p})$. Assuming the finiteness of $Ш(E/\mathbb{Q})$, as predicted by Shafarevich, the order of the group must be square. As $(1, q)$ is the only other possibility, we conclude that $(1, q) \in Ш(E/\mathbb{Q})[2]$ and hence conclude that $Ш(E/\mathbb{Q})[2] \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ if $\sqrt{\alpha} \notin \mathbb{Q}(\sqrt{p})$.

Now $\sqrt{\alpha} \in K \implies \alpha = (x + y\sqrt{p})^2 \implies a_3 = x^2 + py^2, a_1^2 = (x^2 - py^2)^2$, and $d = 2xy$. This, in turn, implies that $a_2^2 = p(x^2 - py^2)^2 - 4x^2y^2$, a solution to the Diophantine equation $p(x^2 - py^2)^2 - 4x^2y^2 = z^2$ for odd z. This implies that the homogeneous space corresponding to $(p, 1)$ has a rational solution $\left(\frac{\pm(x^2-py^2)}{2xy}, \frac{\pm z}{2xy}, \frac{x^2+py^2}{2xy}\right)$. Hence the Mordell-Weil rank is at least one. Knowing the Selmer rank is two, we can then conclude that $r(E/\mathbb{Q}) = 2$ and the 2-part of the Shafarevich-Tate group is trivial. We note that even though the ring of integer $\mathrm{O}_K = \mathbb{Z}[\frac{1+\sqrt{p}}{2}]$, $\alpha = \left(\frac{x+y\sqrt{p}}{2}\right)^2 \implies a_3 = \frac{x^2+py^2}{4} \in \mathbb{Z} \implies x, y$ both are even as $p \equiv 1 \pmod 8$. Hence, without the loss of generality, one can assume x, y as integers. This concludes the proof. □

Table 5.3: Examples for area $p \equiv 1 \pmod 8$, $\tau = \frac{1}{p}$ with $p^2+1 = 2q$ and corresponding rank distribution

p	$r(E/\mathbb{Q})$	$s_2(E/\mathbb{Q})$	$Ш(E/\mathbb{Q})[2]$
409	0	2	$(\mathbb{Z}/2\mathbb{Z})^2$
449	0	2	$(\mathbb{Z}/2\mathbb{Z})^2$
521	0	2	$(\mathbb{Z}/2\mathbb{Z})^2$
569	0	2	$(\mathbb{Z}/2\mathbb{Z})^2$
641	0	2	$(\mathbb{Z}/2\mathbb{Z})^2$

We provide a table of examples above in support of our result. Computations for the table have been done in Magma software (see [34]).

Chapter 6

Final Remarks and Future Perspectives

6.1 Limitations

1. The main theme of the thesis is to compute the 2-part of the Selmer group for Heronian elliptic curves, which also helps to get an upper bound for the Mordell-Weil rank of the curve. However, it does not give the exact value of the Mordell-Weil rank. Knowing the 2-part of the Shafarevich-Tate group helps in that regard. But as evident in the previous chapters, that information came in a conditional way, mostly via class number divisibility of certain number fields. Because of this, there are practical difficulties while dealing with the Mordell-Weil group of different types of Heronian elliptic curves.

2. The 2-Selmer rank computation for congruent number elliptic curve was done extensively in a series of works by Heath-Brown (see [19] and [20]). As an appendix to his works, Monsky introduced a matrix whose rank is directly related to the 2-Selmer rank of an arbitrary congruent number elliptic curve. This gave an alternative to the 2-descent method for computing the 2-Selmer rank via an approach motivated by elementary linear algebra. There is still a lack of similar results in the case of Heronian elliptic curves.

6.2 Future Perspectives

1. As mentioned in the introduction, Heegner [22] developed a method to conclude $2p$ is congruent for certain numbers, and then Monsky and Tian [51] generalized the results for congruent numbers using Heegner's method. This method can be used to construct rational points, known as Heegner points, which turn out to be of infinite order on the modular elliptic curves. Gross-Zagier and Kolyvagin made remarkable contributions towards BSD conjecture using this method. So, using the Modularity theorem, one can look into the construction of Heegner points on Heronian elliptic curves.

2. The class number divisibility problem is one of the contemporary problems in the field of number theory. There are works available in literature by Soleng [48] and Lemmermayer [31] where authors have used rational points of an elliptic curve with positive rank to construct an unramified abelian extension of certain number fields. Hilbert class field theorem then implies the class number of those number fields divisible by the degree of the aforementioned unramified abelian extension. As we have already constructed Heronian elliptic curves with positive ranks in the previous chapters, the class number divisibility problem for number fields generated from points of those elliptic curves can be looked into.

3. Izadi, Farzali, Khoshnam, and Moody [24] extended the idea of Goins and Maddox to Heron quadrilaterals. So, one can think of extending those ideas to generalize the connection between n-polygon and elliptic curves and Diophantine equations.

4. Harron-Snowden [21] computed the density of elliptic curves associated with each of the torsion subgroups classified by Mazur's theorem. Then Im and Kim [23] extended those

results to elliptic curves over number fields. Using the same method, the density of isosceles Heron triangles can be looked into.

5. An algorithm to compute the Mordell-Weil rank of an elliptic curve is famously unavailable in number theory. However, one can look into the possibility of the same for the subclass of all Heronian elliptic curves.

Appendix A

MAGMA and SAGE Commands

1. Code for Mordell-Weil group information (MAGMA):

   First, go to `http://magma.maths.usyd.edu.au/calc/` and run the following code. Here, a_i's denote the coefficients of an Elliptic curve in generalized Weierstrass form.

   E:=EllipticCurve($[a_1, a_2, a_3, a_4, a_6]$);
   E;
   MordellWeilShaInformation(E);
   time rank, gens, sha :=MordellWeilShaInformation(E : ShaInfo);

2. Code for Mordell-Weil group information (SAGE):

   Go to `http://www.sagemath.org`, and run the following code.

   sage:E=EllipticCurve($[a_1, a_2, a_3, a_4, a_6]$)
   sage: E
   sage:E.rank()
   sage:E.selmer_rank()

3. Code for the Class number of Biquadratic number field $\mathbb{Q}(\sqrt{m}, \sqrt{n})$ (MAGMA):

   $R < X >$:= PolynomialRing(Integers());
   K := NumberField ($[X^2 - m, X^2 - n]$:Abs);
   K;
   ClassNumber (K);

4. Code for quadratic fields $\mathbb{Q}(\sqrt{m})$ (MAGMA):

   $R < X >$:= PolynomialRing(Integers()); K := NumberField($X^2 - m$);
   K;
   ClassNumber (K);

References

[1] Buchholz R.H., Rathbun R.L; "An infinite set of Heron triangles with two rational medians", *The American Mathematical Monthly.* 104(2) (1997), 107-115.

[2] Buchholz R.H., Stingley R.P; " Heron triangles with three rational medians", *The Rocky Mountain Journal of Mathematics.* 49(2) (2019), 405-417.

[3] Cassels J.W.S; "Arithmetic on curves of genus 1. IV. Proof of the Hauptvermutung", *Journal für die Reine und Angewandte Mathematik.* 211 (1962), 95-112.

[4] Chandrasekar V; "The congruent number problem", *Resonance.* 3 (1998), 33–45.

[5] Chao L; "2-Selmer groups, 2-class groups and rational points on elliptic curves", *Transactions of the American Mathematical Society.* 371 (2019), 4631-4653.

[6] Conrad K; "The congruent number problem", *The Harvard College Mathematics Review.* 2(2) (2008), 58-74.

[7] Chakraborty D., Ghale V., Saikia A; "Construction of an infinite family of elliptic curves of 2-Selmer rank 1 from Heron triangles", *Research in Number Theory.* 8, 101 (2022).

[8] Chakraborty Debopam, Ghale Vinodkumar; "Size of the 2-Selmer groups for Heronian elliptic curves", *European Journal of Mathematics.* (2023) (Accepted)

[9] Das P., Juyal A., and Moody D; "Integral isosceles triangle-parallelogram and Heron triangle-rhombus pairs with a common area and common perimeter", *Journal of Number Theory.* 180 (2017), 208-218.

[10] Demyanenko V.A; "On Yesmanowciz problem for Pythagorean numbers", *Izvestiya Vysshikh Uchebnykh Zavedenii. Matematika.* (5) (1965), 52-56.

[11] Dickson L.E; "History of the theory of numbers. Vol. II: Diophantine analysis", *Chelsea Publishing Co., New York.* (1966).

[12] Dujella A., Peral J.C; " Elliptic curves coming from Heron triangles",*The Rocky Mountain Journal of Mathematics.* 44(4) (2014), 1145-1160.

[13] Dujella A., Luca F; “On fundamental units of real quadratic fields of class number 1”, *Archiv der Mathematik.* 113 (2019), 349-353.

[14] Dummit D.S., Foote R.M; “Abstract Algebra” *John Wiley and Sons, Inc., Hoboken, NJ.* (3) (2004).

[15] Genocchi A; “Note analitiche sopra tre scritti”, *Annali di Scienze Matematiche e Fisiche.* 6 (1855), 273–317.

[16] Ghale V., Das S., Chakraborty D; “A Heron triangle and a Diophantine equation”, *Periodica Mathematica Hungarica.* 86 (2023), 530–537.

[17] Goins E.H., Maddox D; “Heron triangles via elliptic curves”, *The Rocky Mountain Journal of Mathematics.* 36(5) (2006), 1511-1526.

[18] Halbeisen L., Hungerbühler N; “Heron triangles and their elliptic curves”, *Journal of Number Theory.* 213 (2020), 232-253.

[19] Heath-Brown D.R; “The size of Selmer groups for the congruent number problem”, *Inventiones Mathematicae.* 111 (1993), 171-195.

[20] Heath-Brown D.R; “The size of Selmer groups for the congruent number problem, II”, *Inventiones Mathematicae.* 118 (1994), 331-370.

[21] Harron R., Snowden A; “Counting elliptic curves with prescribed torsion”, *Journal für die reine und angewandte Mathematik (Crelles Journal).* 729 (2017), 151-170.

[22] Heegner K; “Diophantische analysis und modulfunktionen”, *Mathematische Zeitschrift.* 56(3) (1952), 227-253.

[23] Im B., Kim H; “Density of elliptic curves over number fields with prescribed torsion subgroups”. arXiv: 2209.02889, (2022).

[24] Izadi F., Khoshnam F; “Moody D. Heron quadrilaterals via elliptic curves”, *The Rocky Mountain Journal of Mathematics.* 47(4) (2017), 1227–1258

[25] Jesmanowicz L; “Several remarks on Pythagorean numbers”, *Wiadomości Matematyczne* 1(2) (1955), 196-202.

[26] Klasbrun Z., Mazur B; “Rubin K. Disparity in Selmer ranks of quadratic twists of elliptic curves”, *Annals of Mathematics.* (2013), 287-320.

[27] Klagsbrun Z., Mazur B., Rubin K; “A Markov model for Selmer ranks in families of twists”, *Compositio Mathematica.* 150 (2014), 1077-1106.

[28] Koblitz N.I; “Introduction to elliptic curves and modular forms”, *Springer Science and Business Media.* (97) 2012.

[29] Kramer A.V., Luca F; “Some remarks on Heron triangles”, *Acta Academiae Paedagogicae Agriensis Nova Series. Sectio Mathematicae.* 27 (2000), 25–38.

[30] Le M; “A Note on Jeśmanowicz’ Conjecture Concerning Pythagorean Triples”, *Bulletin of the Australian Mathematical Society.* 59(3) (1999), 477–480.

[31] Lemmermeyer F; “Why is the class number of $\mathbb{Q}(\sqrt[3]{11})$ even?”, *Mathematica Bohemica.* 138 (2013), 149-163.

[32] Ma MM., Chen YG; “Jeśmanowicz’conjecture on Pythagorean triples”, *Bulletin of the Australian Mathematical Society.* 96(1) (2017), 30-35.

[33] Matilde L., Olivier M; “Hyperbolic Heron triangles and elliptic curves”, *Journal of Number Theory.* 240 (2022), 272-295.

[34] The MAGMA algebra system, available at `http://magma.maths.usyd.edu.au/calc/`

[35] Mazur B., Rubin K; “Ranks of twists of elliptic curves and Hilbert’s tenth problem”, *Inventiones Mathematicae.* 181 (2010), 541-575.

[36] Miyazaki T; “Generalizations of classical results on Jesmanowicz conjecture concerning Pythagorean triples”, *Journal of Number Theory.* 133(2) (2013), 583-595.

[37] Miyazaki T., Terai N; “On Jeśmanowicz’ conjecture concerning primitive Pythagorean triples. II”, *Acta Mathematica Hungarica.* 147(2) (2015), 286-293.

[38] Monsky P; “Mock Heegner points and congruent numbers”, *Mathematische Zeitschrift.* 204 (1990), 45–67.

[39] Neukirch J; “Algebraic number theory”, *Springer Science and Business Media.* (322) (2013).

[40] Peng J., Zhang Y; “Heron triangles with figurate number sides”, *Acta Mathematica Hungarica.* 157 (2019), 478–488.

[41] Peng J., Zhang Y; “Corrigendum to: Heron triangles with figurate number sides”, *Acta Mathematica Hungarica.* 159 (2019), 689.

[42] Pintz J; “Landau’s problems on primes”, *Journal de théorie des nombres de Bordeaux.* 21(2) (2009), 357-404.

[43] Park J., Poonen B., Voight J., Wood M; “A heuristic for boundedness of ranks of elliptic curves”, *Journal of European Mathematical Society.* 21 (2019), 2859–2903.

[44] Rusin D.J; “Rational triangles with equal area”, *New York Journal of Mathematics.* 4 (1998), 1-15.

[45] Sierpiński W; “On the Diophantine equation $3^x + 4^y = 5^z$”, *Wiadomości Matematyczne.* 1 (1955/56), 194–195.

[46] Silverman J.H; “The arithmetic of elliptic curves”, *Springer Science and Business Media.* (2009).

[47] Skinner C; “A converse to a theorem of Gross, Zagier, and Kolyvagin”, *Annals of Mathematics.* 191 (2020), 329-354.

[48] Soleng, R; “Homomorphisms from the group of rational points on elliptic curves to class groups of quadratic number fields”, *Journal of Number Theory.* 46 (1994), 214-229.

[49] Stein W. Sage: Open source mathematical software, available at `http://www.sagemath.org`.

[50] Terai N; “On Jesmanowicz’s conjecture concerning primitive Pythagorean triples”, *Journal of Number Theory.* 141 (2014), 316-323.

[51] Tian Y; “Congruent numbers and Heegner points”, *Cambridge Journal of Mathematics.* 2 (2014), 117–161.

[52] Top J., Yui N; “Congruent number problems and their variants”, *Algorithmic number theory: lattices, number fields, curves and cryptography.* 44 (2008), 613–639.

[53] Tunnell J.B; “A classical Diophantine problem and modular forms of weight 3/2”, *Inventiones Mathematicae.* 72 (1983), 323–334.

[54] Xin W; “Heegner point Kolyvagin system and Iwasawa main conjecture”, *Acta Mathematica Sinica, English Series.* 37 (2021), 104-120.

[55] Yan X; “The Diophantine equation $(m^2 + n^2)^x + (2mn)^y = (m + n)^{2z}$”, *International Journal of Number Theory.* 16(08) (2020), 1701-1708.

[56] Zhang W; “Selmer groups and the indivisibility of Heegner points”, *Cambridge Journal of Mathematics.* 2 (2014), 191-253.

List of Publications

List of published/accepted papers in thesis

1 Ghale Vinodkumar, Das Shamik, Chakraborty Debopam; “A Heron triangle and a Diophantine equation", *Periodica Mathematica Hungarica.* 86 (2023), 530–537.
`https://doi.org/10.1007/s10998-022-00491-5`

2 Chakraborty Debopam, Ghale Vinodkumar, Saikia Anupam; “Construction of an infinite family of elliptic curves of 2-Selmer rank 1 from Heron triangles", *Research in Number Theory.* 8, 101 (2022).
`https://doi.org/10.1007/s40993-022-00411-z`

3 Chakraborty Debopam, Ghale Vinodkumar; “Size of the 2-Selmer groups for Heronian elliptic curves", *European Journal of Mathematics.* (2023) (Accepted).

List of submitted papers included in thesis

1 Ghale Vinodkumar, Islam Imdadul, Chakraborty Debopam; “Elliptic curves associated with Heron triangles with high 2-Selmer rank", (2023).

2 Chakraborty Debopam, Ghale Vinodkumar; “A Family of Heronian elliptic curves with non-trivial Shafarevich-Tate group", (2023) .

3 Chakraboty Debopam, Ghale Vinodkumar, Saikia Anupam; “Heron triangles of even area and associated elliptic curves", (2023).

Conferences

1 Presented a talk on “Congruent numbers, Heron triangles and elliptic curves" in the Young Researchers in Algebraic Number Theory III (online), University of Bristol, August 2021.

2 Presented a talk on “Heron triangles and elliptic curves" in the International Conference on Class Groups of Number Fields and Related Topics-2022 (ICCGNFRT-2022) at Kerala School of Mathematics, Calicut, November 2022.

3 Presented a talk on “ On the 2 Selmer ranks of Heronian elliptic curves" in the COmbinatorial Number Theory And Connected Topics II (CONTACT-II) (online) February 2023.

Biography

Brief Biography of Candidate

Mr. Vinodkumar Ghale studied at Ferguson College, Pune, and earned his bachelor of science degree from Savitribai Phule Pune University. He earned his master's degree from the University of Hyderabad. He worked with Dr. Mohan Chintamani as a Project assistant at the University of Hyderabad. Later, he worked as a teaching assistant for a year at the Indian Institute of Science Education and Research, Pune. He worked for a year as an assistant professor at the Singhgad Institute, Pune and Pune Institute of Computer Technology. He qualified for the SET examination held for assistant professorship by Savitribai Phule Pune University. He qualified for the CSIR-UGC NET exam held in India, and he earned the Council for Scientific and Industrial Research (CSIR), India fellowship for his Ph.D. degree and joined as a research fellow to work with Dr. Debopam Chakraborty at Birla Institute of Technology and Sciences -Pilani, Hyderabad Campus. He published scientific articles on the rank computation of Heronian elliptic curves during his Ph.D. days and attended national and international workshops and conferences. He presented talks on his research at international conferences. He acted as a volunteer and Ph.D. representative for mathematical events in the school. He is a sports, music and travel enthusiast. He played chess at the state level. He played chess throughout his education and won medals at various levels. He organized chess tournaments for the people in the institutes and places he was part of.

Brief Biography of Supervisor

Dr. Debopam Chakraborty is currently serving as an assistant professor in the Department of Mathematics at the Hyderabad campus of Birla Institute of Technology and Science Pilani. He received his Ph.D. degree from the Indian Institute of Technology, Guwahati, in 2016. His research work mainly involves class number divisibility problems for number fields and rank computation of elliptic curves. Post his Ph.D., he was a visiting scientist at the Delhi Center of the Indian Statistical Institute. Dr. Chakraborty was an invited resource person in the Advanced Instructional School on Algebraic Number Theory, held at IIT Guwahati in 2018. He was also an invited speaker at ICCGNFRT-2017 (International Conference on Class Groups of Number Fields and related topics), held at the HRI-Allahabad in 2017. Apart from these, he took part in various other conferences and workshops on Algebraic Number Theory over the years and several times acted as a resource person for the MTTS program (Mathematics Training and Talent Search).