Pontificia Universidad Católica de Chile

Master Thesis

Arithmetic progressions of integral points on congruent elliptic curves of rank two

Author:
Pedro Mendoza

Supervisor:
Natalia García

A thesis submitted in fulfillment of the requirements for the degree of Master in Mathematics in the Faculty of Mathematics of the Pontifical Catholic University of Chile.

Jury: Ricardo Menares
Giancarlo Lucchini

June 2019
Santiago, Chile

Contents

Introduction ii

1 Preliminaries 1

1.1 Basic definitions 1

1.2 Group law of elliptic curves 2

1.3 Some facts about elliptic curves over $\mathbb{Q}$ 5

1.4 Heights of elliptic curves 7

1.4.1 Weil height 7

1.4.2 Canonical height 7

2 Arithmetic progressions of rational points 10

2.1 Known results 11

2.1.1 Mordell curves 11

2.1.2 Edwards curves 12

2.1.3 Congruent curves 12

2.1.3.1 Congruent numbers 13

2.1.3.2 Magic squares of squares 14

2.2 Relationship with ranks of elliptic curves 15

2.3 Main result 16

2.3.1 Strategy of Bremner, Silverman, and Tzanakis result 16

3 Proof of the main result 18

3.1 Height estimates 18

3.2 Proof of main result 21

4 Final remarks 24

Introduction

Elliptic curves are one of the main topics of research in number theory. For example, they play a crucial role in the proof of Fermat's last theorem. Elliptic curves are also of great relevance in applied mathematics, specially in cryptography, and they are useful in algorithms to obtain the prime factorization of big numbers.

The rank of elliptic curves over $\mathbb{Q}$, which is the number of generators of the free part of the finitely generated abelian group of its rational points (see Chapter 1 for more details), has been extensively studied and there are many open questions about it (see [Sil]). It is still unknown if this number is bounded or not; traditionally people expects that this number should be unbounded because Ulmer proved that this is what happens on function fields (see [U]), but recent probabilistic heuristics by Poonen, Park, Voight, and Wood suggest that the rank should be bounded by 21 except for finitely many cases (see [PPVW]). In 2013, Bhargava and Shankar proved that the average rank of elliptic curves over $\mathbb{Q}$ is bounded (see [BS]); the first author was awarded the Fields Medal for this result, among other contributions. One of the Millenium Prize Problems is to prove the Birch and Swinnerton-Dyer conjecture, which asserts that the rank of an elliptic curve is related with the behaviour of its Hasse-Weil L-function.

The problem that motivates this thesis is what can we say about the length of x-arithmetic progressions of rational points on elliptic curves, which are sequences of points whose x-coordinates form an arithmetic progression. For example, the integral points $(-528, 25136)$, $(-363, 22869)$, $(-198, 17424)$ form an x-arithmetic progression of length 3 on the congruent elliptic curve $y^2 = x^3 - 1254^2x$. This problem has been studied by Mohanty for the particular case of Mordell curves (see [Mo1], [Mo2]). Due to a theorem of García and Pastén, there exists a relationship between the rank of an elliptic curve and the length of an x-arithmetic progression of rational points. There is a result of Bremner, Silverman, and Tzanakis which asserts that there are no x-arithmetic progressions of integral points on congruent elliptic curves of rank one (see [BST]).

We are interested on seeing what happens in the rank two case of Bremner, Silverman, and Tzanakis theorem. We obtain the following result:

Theorem 0.1. *Let n be a squarefree integer, and let E_n be the elliptic curve $y^2 = x^3 - n^2x$. Let $P_1, \ldots, P_d$ be integral points in x-arithmetic progression. Suppose also that $x(P_i) \geq n$, $\gcd(x(P_i), n) = 1$, and $h(P_i) > 40$ (where h denotes the Weil height of P_i). If E_n has rank two, then $d \leq 13$.*

Now, we describe the organization of this thesis. On Chapter 1 we recall some definitions and basic facts about elliptic curves, the group law, heights, etc. On Chapter 2 we present the problem of arithmetic progressions of rational points, some motivation and related results. We also present the main theorem of this thesis and we briefly describe the strategy of Bremner, Silverman, and Tzanakis result, which serves as a motivation for the proof of the main theorem. On Chapter 3 we present the proof of the main result. Finally, on Chapter 4 we describe some natural questions that are left unanswered, and present some questions for future work.

Chapter 1

Preliminaries

1.1 Basic definitions

Definition 1.1. An *elliptic curve* is a pair $(E, \mathcal{O})$, where E is a smooth projective curve of genus one over a field K, and $\mathcal{O} \in E$ is an specified point.

Every such curve can be written as the locus on $\mathbb{P}^2$ of a cubic equation with only one point, the base point, on the line at infinity.

When $\text{char}(K) \neq 2, 3$, an elliptic curve E can be described by a *Weierstrass equation*

$$E : y^2 = x^3 + Ax + B.$$

There are similar (but more complicated) equations for elliptic curves over fields with $\text{char}(K) = 2, 3$, but this thesis is focused on elliptic curves over $\mathbb{Q}$, so we will omit them.

Given an elliptic curve E with Weierstrass equation $y^2 = x^3 + Ax + B$, there are two important quantities associated, the discriminant and the j-invariant.

Definition 1.2. The *discriminant* of E is

$$\Delta_E = -16(4A^3 + 27B^2).$$

This number tells us if the curve E is smooth or not; E is smooth if and only if $\Delta_E \neq 0$.

Definition 1.3. The *j-invariant* of E is given by

$$j_E = -1728 \frac{(4A)^3}{\Delta_E}.$$

The j-invariant is important because it characterizes elliptic curves defined over $\mathbb{C}$; two complex elliptic curves are isomorphic if and only if they have the same j-invariant. Nonetheless, in this thesis the j-invariant fulfills the role of classifying elliptic curves (in some sense).

Example 1.4. Let $E_n/\mathbb{Q}$ be the congruent elliptic curve $y^2 = x^3 - n^2x$, where n is a squarefree integer. Then

$$\begin{aligned}\Delta_{E_n} &= -16 \cdot 4A^3 = 64n^6,\\ j_{E_n} &= -1728\frac{(4A)^3}{\Delta_{E_n}} = 1728.\end{aligned}$$

Then, the family of congruent elliptic curves has constant j-invariant.

Definition 1.5. Let d in K which is not a square. The *quadratic twist* E^d/K of E is given by

$$E^d : y^2 = x^3 + d^2Ax + d^3B.$$

The elliptic curves E and E^d are not isomorphic over K, but they are isomorphic over the larger field $K(\sqrt{d})$.

Theorem 1.6. *The map*

$$\begin{array}{rccc}\varphi: & E^d(K(\sqrt{d})) & \to & E(K(\sqrt{d}))\\ & (x,y) & \mapsto & \left(\dfrac{x}{d}, \dfrac{y}{d^{3/2}}\right).\end{array}$$

is an isomorphism.

Proof. Sea Example 2.4 on page 321 of [Si2]. ■

The previous result will be useful later.

1.2 Group law of elliptic curves

Let $E/\mathbb{Q}$ be an elliptic curve defined by a Weierstrass equation

$$y^2 = x^3 + Ax + B,$$

where $A, B \in \mathbb{Z}$ and $4A^3 + 27B^2 \neq 0$. Let $\mathcal{O}$ be the point at infinity, that is, the point $[0 : 1 : 0]$ in the projectivized curve.

Definition 1.7. The set $E(\mathbb{Q})$ of *rational points* of E is given by

$$E(\mathbb{Q}) = \{(x, y) \in E : x, y \in \mathbb{Q}\} \cup \{\mathcal{O}\}.$$

Remark 1.8. If $P \in E(\mathbb{Q})$ and $P \neq \mathcal{O}$, we denote the x-coordinate and y-coordinate of P by $x(P)$ and $y(P)$ respectively.

We define a binary relation on $E(\mathbb{Q})$ in the following way. Let $P, Q \in E(\mathbb{Q})$, and let L be the line through P and Q (if $P = Q$, the line L is tangent at P). By Bezout's theorem, L must intersect E at a third point R. Let L' be the line through R and $\mathcal{O}$. Again by Bezout's theorem, L' must intersect E at a third point. We define $P + Q$ as that third point.

Example 1.9. Consider the elliptic curve $y^2 = x^3 + 17$ over $\mathbb{Q}$, and the two rational points $P = (-1, 4)$ and $Q = (2, 5)$. The line through P and Q is $y = \frac{1}{3}x + \frac{13}{3}$, and let $R = (x_3, y_3)$ be the third point of intersection. In order to intersect this line with the curve, we replace y in the equation

$$\left(\frac{1}{3}x + \frac{13}{3}\right)^2 = y^2 = x^3 + 17.$$

This is a degree 3 polynomial equation in the variable x, for which we know two solutions already, -1 and 2, so we can factorize it as

$$(x^3 + 17) - \left(\frac{1}{3}x + \frac{13}{3}\right)^2 = (x + 1)(x - 2)(x - x_3).$$

Equating the coefficients of x^2 at both sides we have

$$-\frac{1}{9} = -(-1 + 2 + x_3),$$

so $x_3 = -\frac{8}{9}$. Since (x_3, y_3) lies on the line $y = \frac{1}{3}x + \frac{13}{3}$, we obtain $y_3 = \frac{1}{3}x_3 + \frac{13}{3} = \frac{109}{27}$, so $R = (x_3, y_3) = \left(-\frac{8}{9}, \frac{109}{27}\right)$. Finally, the line through R and $\mathcal{O}$ is just the vertical line $x = \frac{-8}{9}$ so the third point of intersection is just the reflection of R trough the x-axis. All this shows that

$$P + Q = (-1, 4) + (2, 5) = (x_3, -y_3) = \left(-\frac{8}{9}, -\frac{109}{27}\right).$$

If we want to compute $2P = P + P$, we need the line through P and P, which is the tangent line at P. From the equation

$$y^2 = x^3 + 17,$$

defining $f(x) := x^3 + 17$, we have by implicit differentiation that the slope of the tangent line at a point (x_0, y_0) is given by $\frac{f'(x_0)}{2y_0}$ (if $y_0 = 0$, the tangent line is just the vertical line $x = x_0$), so the slope of the tangent line at $(-1, 4)$ is $\frac{f'(-1)}{2 \cdot 4} = \frac{3}{8}$, and this tangent line is given by $y = \frac{3}{8}x + \frac{35}{8}$. Replacing this equation on the curve and equating the coefficients of x^2 as before, we obtain

$$2P = P + P = (-1, 4) + (-1, 4) = \left(\frac{137}{64}, -\frac{2651}{512}\right).$$

The same reasoning can be used to obtain

$$P + \mathcal{O} = P.$$

Remark 1.10. Using the same method as before, we can obtain explicit formulas for this binary relation. If $P = (x_1, x_2)$ and $Q = (x_2, y_2)$, let $y = \lambda x + \nu$ be the line through P and Q (or the tangent line at P in the case that $P = Q$), which intersects E at a third point $R = (x_3, y_3)$. We have different cases

- If $x_1 \neq x_2$, then $\lambda = \frac{y_2 - y_1}{x_2 - x_1}$, $\nu = y_1 - \lambda x_1 = y_2 - \lambda x_2$, and
$$P + Q = (x_3, -y_3) = (\lambda^2 - x_1 - x_2, -\lambda x_3 - \nu).$$
- If $x_1 = x_2$ and $y_1 \neq y_2$, then
$$P + Q = \mathcal{O}.$$
- If $P = Q$ and $y_1 = y_2 = 0$, then
$$2P = P + Q = \mathcal{O}.$$
- If $P = Q$ and $y_1 = y_2 \neq 0$, then
$$\lambda = \frac{f'(x_1)}{2y_1} = \frac{3x_1^2 + A}{2y_1} = \frac{3x_2^2 + A}{2y_2}, \quad \nu = y_1 - \lambda x_1 = y_2 - \lambda x_2,$$
and
$$2P = P + Q = (x_3, -y_3) = (\lambda^2 - x_1 - x_2, -\lambda x_3 - \nu).$$

This binary relation makes $E(\mathbb{Q})$ into a group. The identity element is given by $\mathcal{O}$, and the inverses are given by $-\mathcal{O} = \mathcal{O}$ and $-(x, y) = (x, -y)$. Associativity can be checked directly (in a very tedious way) from the previous formulas, or using again Bezout's theorem. There is a more geometric proof of the fact that $E(\mathbb{Q})$ is a group, which consists of identifying a point with a degree-0 divisor on $\mathrm{Pic}^0(E)$ (see Proposition 3.4 on page 61 of [Si2]).

Since the line that passes through P and Q is the same that the one that passes through Q and P, we have that $E(\mathbb{Q})$ is an abelian group. This fact can also be seen from the explicit equations given above.

We recall that everything said on this section is valid for every field K, with little technical differences when $\operatorname{char}(K) = 2, 3$. We work over $\mathbb{Q}$ for simplicity, and because the main result of this thesis concerns elliptic curves over $\mathbb{Q}$.

1.3 Some facts about elliptic curves over $\mathbb{Q}$

Answering a question apparently posed by Poincaré around 1901, in 1922 Mordell proves the following theorem (see [Mor])

Theorem 1.11. *The abelian group $E(\mathbb{Q})$ is finitely generated.*

Some years later Weil generalizes the previous result to abelian varieties over number fields. Then, by the classification theorem for finitely generated abelian groups, the group $E(\mathbb{Q})$ has the form

$$E(\mathbb{Q}) = \mathbb{Z}^r \oplus C_{p_1^{n_1}} \oplus \ldots \oplus C_{p_k^{n_k}},$$

where $p_1, \ldots, p_k$ are primes, and C_n denotes the cyclic group of order n.

Definition 1.12. The non-negative integer r is called the *rank* of E, and it will be denoted by rk_E.

Definition 1.13. A *torsion* point $P \in E(\mathbb{Q})$ is a point of finite order, i.e., there exists an $m \neq 0$ such that $mP = \underbrace{P + \ldots + P}_{m \text{ times}} = \mathcal{O}$.

The 2-torsion points can be easily computed. First note that $2P = \mathcal{O}$ is equivalent to $(x, y) = P = -P = (x, -y)$, so $y = 0$, and the x-coordinates will be the rational roots of the polynomial $x^3 + Ax + B$.

There is a useful theorem that allows us to easily compute the torsion points

Theorem 1.14. *(Nagell-Lutz) Let $P = (x, y) \in E(\mathbb{Q})$ be a torsion point. Then $x, y \in \mathbb{Z}$, and either $y = 0$, in which case $2P = \mathcal{O}$, or y divides $-4A^3 - 27B^2$.*

Proof. See Theorem 2.5 on page 56 of [Si1]. ■

Example 1.15. Consider the elliptic curve $y^2 = x^3 + 1$ defined over $\mathbb{Q}$, and let $P = (x, y)$ be a torsion point. We have that $-4A^3 - 27B^2 = -27$, so the only possibilities for y are $0, \pm 1, \pm 3$. Replacing these values on the equation we obtain the values for x. Then the torsion of points are $(-1, 0)$, $(0, 1)$, $(0, -1)$, $(2, 3)$, $(2, -3)$, and $\mathcal{O}$.

Since $E(\mathbb{Q})$ is an abelian group, the set of torsion points forms a subgroup of $E(\mathbb{Q})$, which is called the torsion subgroup of $E(\mathbb{Q})$. There is a theorem that completely classifies the possible torsion subgroups of $E(\mathbb{Q})$ (see [Ma])

Theorem 1.16. *(Mazur) The torsion subgroup of $E(\mathbb{Q})$ is exactly one of the following:*

- *C_n, where $1 \leq n \leq 10$ or $n = 12$.*
- *$C_2 \oplus C_{2n}$, where $1 \leq n \leq 4$.*

On the other hand, there is not much information about the rank (see [Sil] for a summary of known results and open problems about it). Since the rank is unbounded when elliptic curves are defined over function fields (see [U]), it is believed that this number should be unbounded as E varies over all elliptic curves defined over $\mathbb{Q}$, but recent probabilistic heuristics suggest that the rank should be at most 21, except for finitely many cases (see [PPVW]).

Here is a list of some ranks

elliptic curve	rank
$y^2 = x^3 - x$	0
$y^2 = x^3 - 5x$	1
$y^2 = x^3 - 243$	1
$y^2 = x^3 - 17x$	2
$y^2 = x^3 - 34^2x$	2
$y^2 = x^3 - 82x$	3
$y^2 + xy + y = x^3 - x^2 + Ax + B$	19

where

$$A = 31368015812338065133318565292206590792820353345$$

$$B = 302038802698566087335643188429543498624522041683874493555186062568159847$$

The last example was found by Elkies on 2009, and is the greatest exact rank that is known. There is another example of a curve which has rank at least 28, and was found by Elkies on 2006.

1.4 Heights of elliptic curves

During this chapter, we follow [Si1] as the main reference.

1.4.1 Weil height

Definition 1.17. Let $x = \dfrac{m}{n}$ be a rational number written in irreducible form. The *Weil height* of x is

$$h(x) := \log \max\{|m|, |n|\}.$$

The Weil height measures the complexity of a rational number, it is approximately the number of bits needed to store $\dfrac{m}{n}$ in a computer.

Now, let $E/\mathbb{Q}$ be an elliptic curve given by a Weierstrass equation $y^2 = x^3 + Ax + B$, where $A, B \in \mathbb{Z}$.

Definition 1.18. Let $P \in E(\mathbb{Q})$. The *Weil height* of P is the height of its x-coordinate, that is

$$h(P) := h(x(P)).$$

Also, we define $h(\mathcal{O}) = 0$.

The Weil height satisfies the following finiteness result

Theorem 1.19. *(Northcott property for h) For any $B \in \mathbb{R}$, the set*

$$\{P \in E(\mathbb{Q}) : h(P) \leq B\}$$

is finite.

Proof. Write $P = (x, y)$, and $x = \dfrac{m}{n}$ in lowest terms. Since

$$h(P) = h(x) = \log \max\{|m|, |n|\}$$

is bounded, we have finitely many options for m and n, so x has finitely many possible values. Then, since $y^2 = x^3 + Ax + B$, we have finitely many possible values for y. ■

1.4.2 Canonical height

Definition 1.20. Let $P \in E(\mathbb{Q})$. The *canonical height* (or *Néron-Tate height*) of P is

$$\hat{h}(P) := \lim_{n\to\infty} \frac{1}{4^n} h(2^n P),$$

where $2^n P$ denotes the sum $\underbrace{P + \ldots + P}_{2^n \text{ times}}$ according to the group law of $E(\mathbb{Q})$.

The canonical height is a *normalized* version of the Weil height. It has better properties than the first one, but it is more difficult to compute.

Proposition 1.21. *The canonical height has the following properties:*

- $\hat{h}(P) = 0$ *if and only if* P *is a torsion point.*
- $\hat{h}(mP) = m^2 \hat{h}(P)$*, where* $m \in \mathbb{Z}$*.*
- *Parallelogram law:* $\hat{h}(P + Q) + \hat{h}(P - Q) = 2\hat{h}(P) + 2\hat{h}(Q)$*.*

Proof. See Exercises 3.2 and 3.3 on page 111 of [Si1], or Theorem 9.3 on page 243 of [Si2]. ■

Remark 1.22. Due to the parallelogram law, the pairing

$$\begin{array}{cccl} \langle \cdot, \cdot \rangle : & E(\mathbb{Q}) \times E(\mathbb{Q}) & \to & \mathbb{R} \\ & (P, Q) & \mapsto & \frac{1}{2}(\hat{h}(P+Q) - \hat{h}(P) - \hat{h}(Q)) \end{array}$$

defines an inner product on the real vector space $E(\mathbb{Q}) \otimes_{\mathbb{Z}} \mathbb{R}$, so we have a natural notion of an *angle* between points. This fact is a key ingredient in the proof of the main theorem of this thesis.

It results that the two previous heights are the same up to a constant

Proposition 1.23. *There is a constant* C *depending on* A *and* B *such that*

$$\left| \hat{h}(P) - \frac{1}{2} h(P) \right| \leq C, \textit{ for all } P \in E(\mathbb{Q}).$$

Proof. See Exercise 3.3 of [Si1]. ■

As a corollary of this we also have Northcott's property for the canonical height

Theorem 1.24. *(Northcott property for* $\hat{h}$*) For any* $B \in \mathbb{R}$*, the set*

$$\{P \in E(\mathbb{Q}) : \hat{h}(P) \leq B\}$$

is finite.

There are many results about the difference between these two heights.

Theorem 1.25. *Let K be a number field, and let E/K be an elliptic curve given by a Weierstrass equation $y^2 = x^3 + Ax + B$. Then*

$$-\frac{1}{8}h(j_E) - \frac{1}{12}h(\Delta_E) - 0.973 \leq \hat{h}(P) - \frac{1}{2}h(P) \leq \frac{1}{12}h(j_E) + \frac{1}{12}h(\Delta_E) + 1.07.$$

Proof. See Theorem 1.3 of [Si4]. ■

Chapter 2

Arithmetic progressions of rational points

In this chapter we present the problem of arithmetic progressions of rational points, some results about it, and the main result of this thesis.

Definition 2.1. Let $E/\mathbb{Q}$ be an elliptic curve. Recall that a collection of rational points $P_1, \ldots, P_d$ are in *x-arithmetic progression* if their x-coordinates are in arithmetic progression.

Remark 2.2. The previous definition only makes sense when all the points are different from the point at infinity $\mathcal{O}$.

We are interested in the length of such x-arithmetic progressions. In particular, we will focus on the following questions

How large can an x-arithmetic progression be?
Can there be x-arithmetic progressions of arbitrarily large length?

Note that for any point P we have that $P = (x, y)$ and $-P = (x, -y)$ have the same x-coordinate, so we always have the *trivial* x-arithmetic progression $\pm P, \pm P, \pm P, \ldots$, which can be of arbitrarily large length. In order to make the problem interesting we want to avoid this situation. From here and so on, when we mention an *x-arithmetic progression* we are actually speaking about a non-trivial x-arithmetic progression, i.e., the x-coordinates of its points are all distinct.

Example 2.3. Consider the elliptic curve $y^2 = x(x^2 - 1254^2)$ over $\mathbb{Q}$. The rational points

$$(-528, 26136), (-363, 22869), (-198, 17424)$$

form a non-trivial x-arithmetic progression of length 3. Note that these points also have integral coordinates.

Analogously we can define y-arithmetic progressions (in this case we don't have to worry about the $\pm P, \pm P, \pm P, \ldots$ trivial situation).

2.1 Known results

On this section we will present some results about arithmetic progressions on elliptic curves which are related with the thesis main result.

2.1.1 Mordell curves

Definition 2.4. A *Mordell curve* is an elliptic curve given by the equation

$$y^2 = x^3 + b,$$

where $b \in \mathbb{Q}^*$.

In 1975, Mohanty studies the number of integer values of k for which the diophantine equation $y^2 = x^3 + k$, has a given number of consecutive integer solutions either for the x-coordinate, for the y-coordinate, or both (see [Mo1]). He proves that there are infinitely many k's such that there are three integral points in x-arithmetic progression with common difference 1, the same result for both coordinates x and y, and there are no k's such that there are five integral points in y-arithmetic progression with common difference 1. He also conjectured that there are only finitely many k's with four integral points in y-arithmetic progression with common difference 1, and possibly the only k with that property is 1025 with solutions

$$(-5, 30), (-4, 31), (-1, 32), (4, 33).$$

In 1980, Mohanty extends the previous conjecture to arithmetic progressions with common difference not necessarily equal to 1 (see [Mo2]), and conjectures that there are no x-arithmetic progressions of integral points of length greater than four on Mordell curves, and the same for y-arithmetic progressions.

In 1992, Lee and Vélez found examples of y-arithmetic progressions of length four, five and six (see [LV]); so the previous conjecture is false, but it is expected to be true when five is replaced by a greater bound.

Conjecture 2.5. *(Mohanty's conjecture) There exists an absolute bound M such that for any $b \in \mathbb{Q}^*$, there are no length M or greater y-arithmetic progressions of rational points on Mordell curves.*

Under the Bombieri-Lang conjecture for surfaces, in 2016 García-Fritz proved Mohanty's conjecture (see [G-F]).

2.1.2 Edwards curves

The following result deals with elliptic curves given by an equation different than the Weierstrass form.

Definition 2.6. An *Edwards curve* is an elliptic curve $E_d/\mathbb{Q}$ given by the equation

$$x^2 + y^2 = 1 + dx^2y^2,$$

where $d \in \mathbb{Q}\backslash\{0,1\}$.

In 2011, Moody proved the following result (see [Moo])

Theorem 2.7. *There are infinitely many $d \in \mathbb{Q}\backslash \{0,1\}$ such that the Edwards curve E_d has at least nine points in x-arithmetic progression.*

Remark 2.8. It is interesting that the formula for sum of points on curves with these equation becomes a little more *friendly* than the sum on curves with Weierstrass equation

$$(x_1,y_1) + (x_2,y_2) = \left(\frac{x_1y_2 + x_2y_1}{1 + dx_1x_2y_1y_2}, \frac{y_1y_2 - x_1x_2}{1 - dx_1x_2y_1y_2}\right) = \left(\frac{x_1y_1 + x_2y_2}{x_1x_2 + y_1y_2}, \frac{x_1y_1 - x_2y_2}{x_1y_2 - y_1x_2}\right).$$

2.1.3 Congruent curves

On this section we will introduce congruent elliptic curves, which are the main object of study on this thesis.

Definition 2.9. A *congruent curve* is an elliptic curve $E_n/\mathbb{Q}$ given by the equation

$$y^2 = x^3 - n^2x,$$

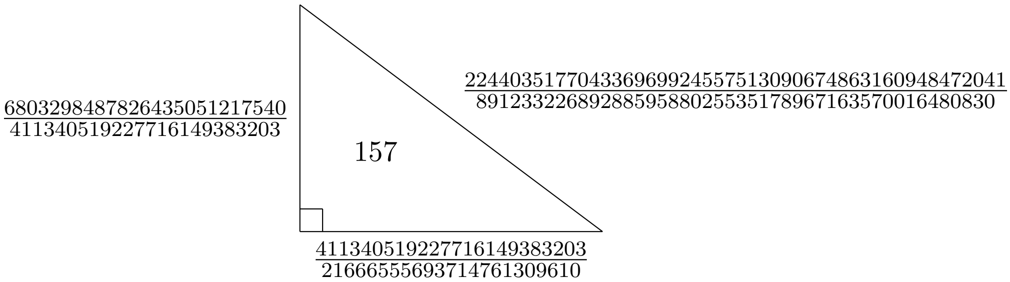
where n is a squarefree integer.

Before we state the result, we present some connections of congruent elliptic curves with other interesting number theory problems.

2.1.3.1 Congruent numbers

Definition 2.10. A positive rational number $q \in \mathbb{Q}_{>0}$ is called *congruent* if it is the area of a right triangle with rational sides.

Example 2.11. 157 is a congruent number, because


$\frac{224403517704336969924557513090674863160948472041}{8912332268928859588025535178967163570016480830}$
$\frac{6803298487826435051217540}{411340519227716149383203}$
157
$\frac{411340519227716149383203}{21666555693714761309610}$

and these rational numbers are in lowest terms.

Suppose that r is congruent and $x, y, z \in \mathbb{Q}$ are the sides of a right triangle with area r. We can find some $s \in \mathbb{Q}$ such that $s^2 r$ is a squarefree integer, then the triangle with sides sx, sy, sz has area $s^2 r$. Thus, when we ask if a certain rational number is congruent or not, without loss of generality we may assume that $q = n$ is a squarefree integer.

We are interested in characterizing squarefree integers wich are congruent.

From now on, n will always be a squarefree integer.

Note that the right triangles with area n are parametrized by rational points with non-zero y-coordinate on the curve E_n. Suppose that n is a congruent number, and let $a, b, c \in \mathbb{Q}$ such that $a^2 + b^2 = c^2$ and $\frac{ab}{2} = n$. If we set $x = \frac{n(a+c)}{b}$ and $y = \frac{2n^2(a+c)}{b^2}$ we have $y^2 = x(x^2 - n^2)$, so a right triangle with area n takes us to a rational point with non-zero y-coordinate on the elliptic curve $y^2 = x(x^2 - n^2)$. Reciprocally, if (x, y) is a rational point on the curve with non-zero y-coordinate, we have the right triangle with area n with sides $a = \frac{x^2 - n^2}{y}$, $b = \frac{2nx}{y}$, and $c = \frac{x^2 + n^2}{y}$. Summarizing, we have a bijection between the sets

$$\left\{(a, b, c) \in (\mathbb{Q}_{>0})^3 : a^2 + b^2 = c^2, \frac{ab}{2} = n\right\} \text{ and } \left\{(x, y) \in \mathbb{Q}^2 : y^2 = x^3 - n^2 x, y \neq 0\right\}.$$

Furthermore, the elliptic curve $y^2 = x^3 - n^2 x$ has $(-n, 0), (0, 0), (n, 0)$, and $\mathcal{O}$ as torsion points (see Proposition 6.1 on page 346 of [Si2]), so we have the following result (see Proposition 18 on page 46 of [Ko])

Theorem 2.12. *A squarefree integer n is congruent if and only if the elliptic curve $y^2 = x^3 - n^2x$ has positive rank.*

In 1983, Tunnel found an *almost* characterization for these numbers (see [Tu])

Theorem 2.13. *For a given congruent number n, define*

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

If n is odd, then $2A_n = B_n$. If n is even, then $2C_n = D_n$. Moreover, under the Birch and Swinnerton-Dyer conjecture, the previous equalities are enough to conclude that n is a congruent number.

2.1.3.2 Magic squares of squares

LaBar propose the following problem (see [La])

> *Does there exist a 3×3 magic square with nine distinct perfect squares as entries?*

Bremner found the following example with seven squares (see [Br2])

373^2	289^2	565^2
360721	425^2	23^2
205^2	527^2	222121

and, as of today, it is not known if there exists an example with eight.

Robertson found the following characterization (see [Ro])

Theorem 2.14. *The following problems are equivalent*

- *Prove or disprove that a 3×3 magic square can be constructed with nine distinct perfect squares.*

- *Prove or disprove that there are three rational triangles with the same area, such that the squares of the hypotenuses are in arithmetic progression.*
- *Prove or disprove that there is an elliptic curve $y^2 = x^3 - n^2x$, where n is a congruent number, with three rational points which are the double of another rational points (in the sense of the group structure), whose x-coordinates are in arithmetic progression.*

Following the third characterization, in 2000, Bremner, Silverman, and Tzanakis proved the following result (see [BST])

Theorem 2.15. *Let n be a squarefree integer, and let E_n be the elliptic curve $y^2 = x^3 - n^2x$. If E_n has rank one, then E_n has no arithmetic progressions of integral points.*

This is the theorem that motivates this thesis. The main result of this thesis may be viewed as an extension of this theorem to the rank two case.

2.2 Relationship with ranks of elliptic curves

After proving the result together with Silverman and Tzanakis, Bremner made the following *commentary/conjecture* (see [Br1])

> *It seems that points of an arithmetic progression have a tendency*
> *to be linearly independent in the group of rational points.*

In 2018, García-Fritz and Pastén proved the following result (unfortunately this has not been published yet, so we don't have a proper reference)

Theorem 2.16. *Given $r \in \mathbb{N}$ and $j \in \mathbb{Q}$, there exist a constant $M = M(r, j) > 0$ such that for every elliptic curve $E/\mathbb{Q}$ with $\mathrm{rk}_E \leq r$ and $j_E = j$, the x-arithmetic progressions on E have length at most M.*

thus, at least for a fixed j-invariant, there exists a relationship between the rank of elliptic curves and the maximal length of x-arithmetic progressions.

Remark 2.17. One of the most important unsolved problems about elliptic curves is the question about boundedness of the rank. Traditionally, most people expects that the rank should be unbounded (see [U]), but recent probabilistic heuristics suggest that the rank should be at most 21, except for finitely many cases (see [PPVW]); including the record curve found by Elkies on 2006 which has rank at least 28. García-Fritz and Pastén proved that the question of the length of x-arithmetic progressions *may* be used to attack the central problem of the rank (at least for the case of a fixed j-invariant).

2.3 Main result

To see what happens in the rank two case in the theorem of Bremner, Silverman, and Tzanakis, we obtain the following result

Theorem 2.18. *Let n be a squarefree integer, and let E_n be the elliptic curve $y^2 = x^3 - n^2x$. Let $P_1, \dots, P_d$ be integral points in x-arithmetic progression. Suppose also that $x(P_i) \geq n$, $\gcd(x(P_i), n) = 1$, and $h(P_i) > 40$. If E_n has rank two, then $d \leq 13$.*

Note that the family of congruent elliptic curves has constant j-invariant equal to 0, so we are giving a sharp explicit bound which the theorem of García-Fritz and Pastén does not provide.

2.3.1 Strategy of Bremner, Silverman, and Tzanakis result

Roughly speaking, the proof starts with height estimates for congruent elliptic curves; these estimates are general and they have nothing to do (at first) with x-arithmetic progressions. The proof of their theorem has two cases. Assuming that such x-arithmetic progressions exists, the height estimates are used to get a contradiction when $n \geq 72$. The $n < 72$ case is just a *brute-force attack*.

First of all, they proved the following estimates for the canonical height (Proposition 2.1 in [BST])

Proposition 2.19. *Let n be a fixed squarefree integer. Let $P \in E_n(\mathbb{Q})$ be a rational point such that $2P \neq \mathcal{O}$, and write the x-coordinate of P as $x = \dfrac{a}{d^2}$. Then*

$$\begin{aligned}
\hat{h}(P) &\geq \frac{1}{16}\log(2n^2), \\
\hat{h}(P) &\geq \frac{1}{4}\log\left(\frac{a^2+n^2d^4}{2n^2}\right), \\
\hat{h}(P) &\leq \frac{1}{4}\log(a^2+n^2d^4) + \frac{1}{12}\log(2).
\end{aligned}$$

Since E_n has rank 1, let $P \in E_n(\mathbb{Q})$ be a generator of the free part of the group of rational points, i.e., write $E_n(\mathbb{Q}) = \langle P \rangle \oplus E_n(\mathbb{Q})_{\text{tors}}$. Let P_1, P_2, P_3 be an arithmetic progression of integral points. For $i = 1, 2, 3$ write $P_i = m_iP + T_i$, where $m_i \in \mathbb{Z}$ and T_i are torsion points. Under the aditional hypothesis of $n \geq 72$ and using the property $\hat{h}(mP) = m^2\hat{h}(P)$, they proved that there are very few possible values for m_i's (see Corollary 3.2 in [BST]).

Then, for each possible combination of m_i's, the x-arithmetic progression condition gives rational roots of certain polynomials which do not have rational roots (see Section 4.1 in [BST]).

Finally, the case $n < 72$ is just a *brute-force attack*. By Siegel's Theorem, elliptic curves have only finitely many integral points, and they have explicit found all integral points and verify that there is no such x-arithmetic progression (see Section 4.2 in [BST]).

Chapter 3

Proof of the main result

In this chapter we prove the main result of this thesis. For completeness, let us recall the statement

Theorem 3.1. *Let n be a squarefree integer, and let E_n be the elliptic curve $y^2 = x^3 - n^2x$. Let $P_1, \dots, P_d$ be integral points in x-arithmetic progression. Suppose also that $x(P_i) \geq n$, $\gcd(x(P_i), n) = 1$, and $h(P_i) > 40$. If E_n has rank two, then $d \leq 13$.*

Remark 3.2. There are congruent elliptic curves of rank two, for example $n = 34, 41, 65, \dots$ In fact, there are 376 values of n between 1 and 10000 such that E_n has rank two (see [WT] and [NW]).

3.1 Height estimates

Before proving Theorem 3.1, we will prove some height estimates for congruent elliptic curves that will be useful later.

First of all, note that all the curves E_n's are quadratic twists by n of the curve E_1, and there is an isomorphism over $\mathbb{Q}(\sqrt{n})$ between E_n and E_1 (see Theorem 1.6)

$$\begin{array}{rcl} \varphi : E_n(\mathbb{Q}(\sqrt{n})) & \to & E_1(\mathbb{Q}(\sqrt{n})) \\ (x, y) & \mapsto & \left(\dfrac{x}{n}, \dfrac{y}{n^{3/2}} \right). \end{array}$$

Lemma 3.3. *Let $P = (X, Y), Q = (x, y) \in E_n(\mathbb{Q})$. Then*

$$x(\varphi(P) + \varphi(Q)) = \frac{X^2x + Xx^2 - 2Yy - n^2(X + x)}{n(X - x)^2}.$$

Proof. Using the formula for the sum of points on an elliptic curve (see Remark 1.10), we have

$$\begin{aligned} x(\varphi(P)+\varphi(Q)) &= x(\varphi(P+Q)) \\ &= \frac{x(P+Q)}{n} \\ &= \frac{1}{n}\left\{\left(\frac{Y-y}{X-x}\right)^2 - X - x\right\} \\ &= \frac{Y^2-2Yy+y^2+X^2x-X^3-x^3+Xx^2}{n(X-x)^2} \\ &= \frac{X^2x+Xx^2-2Yy-n^2(X+x)}{n(X-x)^2}. \end{aligned}$$

■

Lemma 3.4. *Let $P, Q \in E_n(\mathbb{Q})$ be integral points such that $x(P), x(Q) \geq n$. If $x(P) > x(Q)$, then:*

$$h(\varphi(P)+\varphi(Q)) \leq 2h(P) + h(Q) + 4\log(2).$$

Proof. This proof is based on Lemma 4.5 of [Al]. Write $P = (X, Y)$ and $Q = (x, y)$. Since $X > x \geq n$, the quantities that appear on Lemma 3.3 are bounded as follows

$$\begin{aligned} \log|2Yy| &= \frac{1}{2}\log|X^3-n^2X| + \frac{1}{2}\log|x^3-n^2x| + \log(2) \\ &\leq \frac{1}{2}\log|2X^3| + \frac{1}{2}\log|2x^3| + \log(2) \\ &= \frac{3}{2}h(P) + \frac{3}{2}h(Q) + 2\log(2). \end{aligned}$$

Similarly

$$\log|n^2(X+x)| \leq h(P) + 2\log(n) + \log(2),$$

and

$$\log|n(X-x)^2| = \log(n) + 2\log|X-x| \leq 2h(P) + \log(n) + 2\log(2).$$

Putting together all these estimates and using Lemma 3.3

$$\begin{aligned}
h(\varphi(P)+\varphi(Q)) &\leq \max\{\log|X^2x+Xx^2-2Yy-n^2(X+x)|, \log|n(X-x)^2|\}\\
&\leq \max\Big\{ \max\{\log|X^2x|, \log|Xx^2|, \log|2Yy|, \log|n^2(X+x)|\}+\log(4),\\
&\qquad\qquad 2h(P)+\log(n)+2\log(2)\Big\}\\
&\leq \max\Big\{2h(P)+h(Q), h(P)+2h(Q), \frac{3}{2}h(P)+\frac{3}{2}h(Q)+2\log(2),\\
&\qquad\qquad h(P)+2\log(n)+\log(2), 2h(P)+\log(n)\Big\}+2\log(2)\\
&\leq \max\Big\{2h(P)+h(Q), h(P)+2h(Q), \frac{3}{2}h(P)+\frac{3}{2}h(Q),\\
&\qquad\qquad h(P)+2\log(n), 2h(P)+\log(n)\Big\}+4\log(2)\\
&= 2h(P)+h(Q)+4\log(2).
\end{aligned}$$

■

Lemma 3.5. *For all $P \in E_1(\mathbb{Q}(\sqrt{n}))$ we have*

$$-\frac{5}{4}\log(2)-\frac{3}{8}\log(3)-0.973 \leq \hat{h}(P)-\frac{1}{2}h(P) \leq \log(2)+\frac{1}{4}\log(3)+1.07.$$

Proof. Since its discriminant is $\Delta_{E_1}=64$ and its j-invariant is $j_{E_1}=1728$ (see Example 1.4), by Theorem 1.25 we have the following estimate for the difference between the Weil height and the canonical height

$$-\frac{1}{8}h(1728)-\frac{1}{12}h(64)-0.973 \leq \hat{h}(P)-\frac{1}{2}h(P) \leq \frac{1}{12}h(1728)+\frac{1}{12}h(64)+1.07$$

for all $P \in E_1(\mathbb{Q}(\sqrt{n}))$. Then, for all $P \in E_1(\mathbb{Q}(\sqrt{n}))$ we have

$$-\frac{5}{4}\log(2)-\frac{3}{8}\log(3)-0.973 \leq \hat{h}(P)-\frac{1}{2}h(P) \leq \log(2)+\frac{1}{4}\log(3)+1.07.$$

■

Lemma 3.6. *Let $P, Q \in E_n(\mathbb{Q})$ be integral points such that $x(P), x(Q) \geq n$, satisfying that* $\gcd(x(P), n)=\gcd(x(Q), n)=1$. *If $x(P) \geq x(Q)$, then*

$$\hat{h}(P+Q) \leq 2\hat{h}(P)+\hat{h}(Q)+\frac{27}{4}\log(2)+\frac{11}{8}\log(3)+3.989.$$

Proof. Since $\gcd(x(P), n)=1$ we have

$$h(\varphi(P))=h\left(\frac{x(P)}{n}\right)=\max\{\log(x(P)), \log(n)\}=\log(x(P))=h(P).$$

Using the fact that the canonical height is invariant under isomorphism and Lemma 3.5 we have

$$h(P) \leq 2\hat{h}(P) + \frac{5}{2}\log(2) + \frac{3}{4}\log(3) + 1.946,$$

and the same for Q. Using again the invariance of the canonical height, Lemma 3.5 and Lemma 3.4, we have

$$\begin{aligned}\hat{h}(P+Q) - \log(2) - \frac{1}{4}\log(3) - 1.07 &= \hat{h}(\varphi(P+Q)) - \log(2) - \frac{1}{4}\log(3) - 1.07\\ &\leq \frac{1}{2}h(\varphi(P) + \varphi(Q))\\ &\leq h(P) + \frac{1}{2}h(Q) + 2\log(2)\\ &\leq 2\hat{h}(P) + \hat{h}(Q) + \frac{23}{4}\log(2) + \frac{9}{8}\log(3) + 2.919\end{aligned}$$

so

$$\hat{h}(P+Q) \leq 2\hat{h}(P) + \hat{h}(Q) + \frac{27}{4}\log(2) + \frac{11}{8}\log(3) + 3.989.$$

■

3.2 Proof of main result

Before proving Theorem 3.1, we will prove a lemma about arithmetic progressions, and other about angles between points

Lemma 3.7. *Let $x_1 < x_2 < \ldots < x_m$ be an arithmetic progression of positive numbers. Then, for $2 \leq i < j$ we have*

$$x_j < (j - i + 1)x_i.$$

Proof. For a fixed $i \geq 2$, we will prove this by strong induction on j. For $j = i+1$, the arithmetic progression condition implies $x_{i+1} + x_{i-1} = 2x_i$, so the result holds since $x_{i-1} > 0$. Now suppose we have the result for all $i+1, \ldots, j$. For $j+1$ we have $x_{j+1} = x_j + (x_{i+1} - x_i) < (j-i+1)x_i + 2x_i - x_i = ((j+1) - i + 1)x_i$. ■

Lemma 3.8. *Let $P, Q \in E_n(\mathbb{Q})$ be such as in Lemma 3.6. Let $\theta_{P,Q}$ be the angle between P and Q induced by the inner product*

$$\langle P, Q\rangle = \frac{1}{2}\left\{\hat{h}(P+Q) - \hat{h}(P) - \hat{h}(Q)\right\}$$

on the real vector space $E_n(\mathbb{Q}) \otimes_{\mathbb{Z}} \mathbb{R}$. Then

$$\cos(\theta_{P,Q}) \leq \frac{\|P\|}{2\,\|Q\|} + \frac{C}{2\,\|P\|\,\|Q\|},$$

where the norm $\|P\| = \sqrt{\hat{h}(P)}$ *is induced by the inner product, and*

$$C = \frac{27}{4}\log(2) + \frac{11}{8}\log(3) + 3.989$$

Proof. From Lemma 3.6 we have the following estimate for $\theta_{P,Q}$

$$\begin{aligned}\cos(\theta_{P,Q}) &= \frac{\langle P,Q\rangle}{\|P\|\,\|Q\|} \\ &= \frac{\hat{h}(P+Q) - \hat{h}(P) - \hat{h}(Q)}{2\,\|P\|\,\|Q\|} \\ &\leq \frac{\hat{h}(P) + C}{2\,\|P\|\,\|Q\|} \\ &= \frac{\|P\|}{2\,\|Q\|} + \frac{C}{2\,\|P\|\,\|Q\|}.\end{aligned}$$

■

Now we present the proof of Theorem 3.1.

Proof. Let $\theta = \frac{\pi}{6}$. Let $P_1, \ldots, P_{14} \in E_n(\mathbb{Q})$ be integral points in x-arithmetic progression, that is $x_1 < \ldots < x_{14}$ and $x_2 - x_1 = \ldots = x_{14} - x_{13}$, where $x_i := x(P_i)$. Suppose also that $x_i \geq n$ and $\gcd(x_i, n) = 1$. We consider the thirteen points $P_2, \ldots, P_{14}$. Since $E_n(\mathbb{Q})$ has rank two, $E_n(\mathbb{Q}) \otimes_{\mathbb{Z}} \mathbb{R}$ is a two-dimensional real vector space, so by pigeonhole principle, there exist points $P_i \neq P_j$, with $1 \neq i < j$, with angle less than $\frac{\pi}{6}$.

From lemma 3.5 we have

$$\frac{1}{2}h(P_i) - \frac{5}{4}\log(2) - \frac{3}{8}\log(3) - 0.973 \leq \hat{h}(P_i) \leq \frac{1}{2}h(P_i) + \log(2) + \frac{1}{4}\log(3) + 1.07.$$

Since $h(P_i) > 40$ the left hand side is non negative, so

$$\sqrt{\frac{1}{2}h(P_i) - \frac{5}{4}\log(2) - \frac{3}{8}\log(3) - 0.973} \leq \|P_i\| \leq \sqrt{\frac{1}{2}h(P_i) + \log(2) + \frac{1}{4}\log(3) + 1.07}.$$

By Lemma 3.7, we have $x_j < (j - i + 1)x_i$, so

$$h(P_j) = \log(x_j) < \log(x_i) + \log(j - i + 1) \leq h(P_i) + \log(13).$$

Also, since $i < j$ we have

$$h(P_i) < h(P_j).$$

Then, by the previous estimates and Lemma 3.8 we can estimate the angle $\theta_{i,j}$ between P_i and P_j

$$
\begin{aligned}
\cos(\theta_{i,j}) &\leq \frac{\|P_j\|}{2\,\|P_i\|} + \frac{C}{2\,\|P_j\|\,\|P_i\|} \\
&\leq \frac{\sqrt{\frac{1}{2}h(P_j) + \log(2) + \frac{1}{4}\log(3) + 1.07}}{2\sqrt{\frac{1}{2}h(P_i) - \frac{5}{4}\log(2) - \frac{3}{8}\log(3) - 0.973}} \\
&\quad + \frac{C}{2\sqrt{\frac{1}{2}h(P_j) - \frac{5}{4}\log(2) - \frac{3}{8}\log(3) - 0.973}\sqrt{\frac{1}{2}h(P_i) - \frac{5}{4}\log(2) - \frac{3}{8}\log(3) - 0.973}} \\
&\leq \frac{\sqrt{\frac{1}{2}h(P_i) + \frac{1}{2}\log(13) + \log(2) + \frac{1}{4}\log(3) + 1.07}}{2\sqrt{\frac{1}{2}h(P_i) - \frac{5}{4}\log(2) - \frac{3}{8}\log(3) - 0.973}} \\
&\quad + \frac{C}{2\sqrt{\frac{1}{2}h(P_i) - \frac{5}{4}\log(2) - \frac{3}{8}\log(3) - 0.973}\sqrt{\frac{1}{2}h(P_i) - \frac{5}{4}\log(2) - \frac{3}{8}\log(3) - 0.973}} \\
&\leq \frac{1}{2}\sqrt{1 + \frac{\frac{1}{2}\log(13) + \frac{9}{4}\log(2) + \frac{5}{8}\log(3) + 2.043}{\frac{1}{2}h(P_i) - \frac{5}{4}\log(2) - \frac{3}{8}\log(3) - 0.973}} \\
&\qquad\qquad + \frac{C}{h(P_i) - \frac{5}{2}\log(2) - \frac{3}{4}\log(3) - 1.946}.
\end{aligned}
$$

Since $\theta_{i,j} < \frac{\pi}{6}$, we have $\cos(\theta_{i,j}) > \frac{\sqrt{3}}{2}$. On the other hand, since $h(P_i) > 40$, the previous inequality gives $\cos(\theta_{i,j}) < \frac{\sqrt{3}}{2}$ which is a contradiction. ■

Chapter 4

Final remarks

Let us recall the main theorem of this thesis

Theorem 4.1. *Let n be a squarefree integer, and let E_n be the elliptic curve $y^2 = x^3 - n^2x$. Let $P_1, \ldots, P_d$ be integral points in arithmetic progression. Suppose also that $x(P_i) \geq n$, $\gcd(x(P_i), n) = 1$, and $h(P_i) > 40$. If E_n has rank two, then $d \leq 13$.*

This theorem may be viewed as an extension of Bremner, Silverman, and Tzanakis result for the rank two case; and also as an explicit bound for the length of arithmetic progressions which García-Fritz, and Pastén theorem for congruent elliptic curves (a family which has constant j-invariant) does not give.

There are some questions that arise naturally from this work.

On Bremner, Silverman, and Tzanakis work, there is no hypothesis of $\gcd(x(P_i), n) = 1$. In the rank one case, the property $\hat{h}(mP) = m^2\hat{h}(P)$ is very useful, but in the rank two case there is no such easy formula for $\hat{h}(mP + nQ)$, so we have to add an aditional hypothesis of the $\gcd$. This motivates the following question:

Question 4.2. Can we drop the $\gcd(x(P_i), n) = 1$ hypothesis?

Note that if n is large enough the condition $x(P_i) \geq n$ implies $h(P_i) > 65$, but it is still unknown that happens when $-n \leq x(P_i) \leq 0$. This motivates the following question:

Question 4.3. What can be say about arithmetic progressions of rational points which has x-coordinates on $[-n, 0]$?

The arithmetic progression of rational points question still makes sense when the elliptic curve is defined over a number field instead of just $\mathbb{Q}$. One of the main ingredients of the work of Bremner, Silverman, and Tzanakis is the height estimates that they obtain, which are the following

Proposition 4.4. *Let n be a fixed squarefree integer. Let $P \in E_n(\mathbb{Q})$ be a rational point such that $2P \neq \mathcal{O}$, and write the x-coordinate of P as $x = \dfrac{a}{d^2}$. Then*

$$\begin{aligned}
\hat{h}(P) &\geq \frac{1}{16}\log(2n^2), \\
\hat{h}(P) &\geq \frac{1}{4}\log\left(\frac{a^2+n^2d^4}{2n^2}\right), \\
\hat{h}(P) &\leq \frac{1}{4}\log(a^2+n^2d^4) + \frac{1}{12}\log(2).
\end{aligned}$$

The proof of this result is based on the decomposition of the canonical height of an elliptic curve $E/\mathbb{Q}$ into *local heights*

$$\hat{h} = \sum_{p \in M_{\mathbb{Q}}} \hat{\lambda}_p,$$

where $M_{\mathbb{Q}} = \{\text{primes}\} \cup \{\infty\}$ is the set of places of $\mathbb{Q}$, and $\tilde{\lambda}_p : E(\mathbb{Q}_p) \to \mathbb{R}$ are height functions on the curve E defined over the completions of $\mathbb{Q}$ with respect to all its absolute values (see Chapter VI of [Si3] for more details).

In the case of a number field K, there is a similar decomposition of the canonical height, but the set of places M_K is more difficult to describe.

Question 4.5. Using the previous decomposition of the canonical height, can we find an analogue of the height estimates obtained by Bremner, Silverman, and Tzanakis over number fields? If this is possible, can we use these estimates to obtain explicit bounds for the length of arithmetic progressions of rational points in terms of the rank over number fields?

The family of congruent elliptic curves has constant j-invariant, so García-Fritz and Pastén's theorem tell us that there must exist a effectively computable but non-explicit bound for the length arithmetic progressions of rational points

Question 4.6. Can we find an analogue of the main theorem for other families of elliptic curves with constant (or bounded) j-invariant? For example, what can be said about Mordell curves?

Bibliography

[Al] Alpoge, L. The average elliptic curve has few integral points. Senior Thesis, Harvard University, 2014. Available online at `http://www.princeton.edu/  lalpoge/papers/my%20senior%20thesis.pdf`

[Br1] Bremner, A. On arithmetic progressions on elliptic curves. Experiment. Math. 8 (1999), no. 4, 409-413.

[Br2] Bremner, A. On squares of squares. Acta Arith. 88 (1999), no. 3, 289-297.

[BS] Bhargava, M.; Shankar, A. Binary quartic forms having bounded invariants, and the boundedness of the average rank of elliptic curves. Ann. of Math. (2) 181 (2015), no. 1, 191-242.

[BST] Bremner, A.; Silverman, J. H.; Tzanakis, N. Integral points in arithmetic progression on $y^2 = x(x^2 - n^2)$. J. Number Theory 80 (2000), no. 2, 187-208.

[G-F] García-Fritz, N. Quadratic sequences of powers and Mohanty's conjecture. Int. J. Number Theory 14 (2018), no. 2, 479-507.

[Ko] Koblitz, N. Introduction to elliptic curves and modular forms. Second edition. Graduate Texts in Mathematics, 97. Springer-Verlag, New York, 1993.

[La] LaBar, M. Problem 270, College Math. J. 15 (1984), 69.

[LV] Lee, J.-B.; Vélez, W. Y. Integral solutions in arithmetic progression for $y^2 = x^3 + k$. Period. Math. Hungar. 25 (1992), no. 1, 31-49.

[Ma] Mazur, B. Modular curves and the Eisenstein ideal. Inst. Hautes tudes Sci. Publ. Math. No. 47 (1977), 33-186 (1978).

[Mo1] Mohanty, S. P. On consecutive integer solutions for $y^2 - k = x^3$. Proc. Amer. Math. Soc. 48 (1975), 281-285.

[Mo2] Mohanty, S. P. Integer solutions in arithmetic progression for $y^2 - k = x^3$. Acta Math. Acad. Sci. Hungar. 36 (1980), no. 3-4, 261-265.

[Moo] Moody, D. Arithmetic progressions on Edwards curves. J. Integer Seq. 14 (2011), no. 1, Article 11.1.7, 4 pp.

[Mor] Mordell, L. J. On the rational solutions of the indeterminate equations of the third and fourth degrees. Proc. Camb. Phil. Soc. 21 (1922), 179-192.

[NW] Noda, K.; Wada, H. All congruent numbers less than 10000. Proc. Japan Acad. Ser. A Math. Sci. 69 (1993), no. 6, 175-178.

[PPVW] Park, J.; Poonen, B.; Voight, J.; Wood, M. M. (2016). A heuristic for boundedness of ranks of elliptic curves. Prepint arXiv:1602.01431.

[Ro] Robertson, J. P. Magic squares of squares. Math. Mag. 69 (1996), no. 4, 289-293.

[Sil] Silverberg, A. Ranks "cheat sheet". Women in numbers 2: research directions in number theory, 101-110, Contemp. Math., 606, Centre Rech. Math. Proc., Amer. Math. Soc., Providence, RI, 2013.

[Si1] Silverman, J. H.; Tate, J. T. Rational points on elliptic curves. Second edition. Undergraduate Texts in Mathematics. Springer, Cham, 2015.

[Si2] Silverman, J. H. The arithmetic of elliptic curves. Second edition. Graduate Texts in Mathematics, 106. Springer, Dordrecht, 2009.

[Si3] Silverman, J. H. Advanced topics in the arithmetic of elliptic curves. Graduate Texts in Mathematics, 151. Springer-Verlag, New York, 1994.

[Si4] Silverman, J. H. The difference between the Weil height and the canonical height on elliptic curves. Math. Comp. 55 (1990), no. 192, 723-743.

[Tu] Tunell, J. A classical diophantine problem and modular forms of weight $3/2$. Invent. Math. 72 (1983), pp. 323-334.

[U] Ulmer, D. Elliptic curves with large rank over function fields. Ann. of Math. (2) 155 (2002), no. 1, 295-315.

[WT] Wada, H.; Taira, M. Computations of the rank of elliptic curve $y^2 = x^3 - n^2x$. Proc. Japan Acad. Ser. A Math. Sci. 70 (1994), no. 5, 154-157.