The Congruent Number Problem

Debbie D. White

Advisor: Dan Yasaki

University of North Carolina at Greensboro

April 11, 2018

Abstract

In mathematics, especially number theory, one often comes across problems easy to state, but whose solutions require very sophisticated methods. The Congruent Number Problem is one such unsolved problem that goes back thousands of years. A natural number is a congruent number if it is the area of a right triangle with rational length sides. The Congruent Number Problem is to find an algorithm to determine whether a given natural number is congruent or not. There is a conjectural solution, but a proof would require solving a millennium problem worth a million dollars concerning elliptic curves.The goal of this project is to give a summary of connection between the congruent numbers and the rational points of special family of elliptic curves

$$E_N : y^2 = x^3 - N^2 x.$$

After we introduce elliptic curves and the group law of rational points on E_N we find the torsion points by Nagel–Lutz theorem. Then, we show the rational points of these family of elliptic curves finitely generated which proved by Mordell. After introducing rank of elliptic curves, we conclude a natural number N is a congruent number if and only if the corresponding elliptic curve $E_N(\mathbb{Q})$ has non-zero rank.

Contents

Chapter 1

Introduction

> Mathematics is the Queen of the Sciences and Number theory is the Queen of Mathematics.
>
> *Gauss*

A Thousand Year Old Problem

The congruent number problem was first stated by the Persian mathematician Al-Karaji (c.953 - c.1029). See Figure 1.1. He stated the problem another form without mention right triangles. He stated it in terms of square numbers; asked for which whole numbers N, does there exist a square a^2 such that $a^2 - N$ and $a^2 + N$ are also squares? A major influence on Al-Karaji was the Arabic translations of the works of the Greek mathematician Diophantus (c.210 - c.290) who stated similar problems.

Figure 1.1: Page from AL-kitab al-Fakhri[cul].

In the eleventh century, Fibonacci found three rational numbers whose squares form a common difference of 5, he generalized the problem in his 1225 book, *Liber Quadratorum* [Fib08]. Fibonacci referred to a common difference between numbers in arithmetic progression of three squares

$$x^2 - N, \quad x^2, \quad x^2 + N$$

and named it by **congruum** from the Latin *congruere* which means *to meet together* [Cha06] since it is clear to see that these three squares

$$x^2 - N, \quad x^2, \quad x^2 + N$$

are congruent modulo N. He proved 5 and 7 are congruent numbers, but he only stated 1 is not a congruent number without proof. That proof was supplied by Fermat in 1659. Similar argument of Fermat shows 2 and 3 are not either. Fermat also implied that there are no rational (x, y) with $x, y \neq 0$ such that $x^4 + y^4 = 1$ which may led him to claim his famous last theorem which is "there are no non-trivial integer solutions to $x^a + y^a = z^a$ for any integer $a \geq 3$."

In this paper we show how the original version of the congruent number problem connects with rational points on elliptic curves. The connection of the area of a rational right triangle N with the rational solution of special family of elliptic curves allows us to reduce the congruent number problem to find the rational solutions of the corresponding elliptic curve. Then, we show rational points on these special family of elliptic curves with the point addition form an Abelian group. After we find the points of finite order which are called *torsion points* of the corresponding elliptic curve by Nagel–Lutz theorem, we follow Mordell's theorem, and we see that the set of the rational points of corresponding elliptic curve is finitely generated Abelian group; which means we can construct all elements in the set of rational points on this curve. Finally, we show the number of the points of infinite order of corresponding elliptic curve which are called *rank*, determine N is whether or not a congruent number.

Chapter 2

Congruent Numbers

A natural number is a congruent number if it is the area of a right triangle with rational length sides. A right triangle or right-angled triangle is a triangle in which one angle is a right angle. If the lengths of all three sides are integers, the triangle is called a *Pythagorean* triangle and, if the lengths of all sides are rational numbers it is called *rational* triangle. Any rational right triangle has a rational area but not conversely. For example, there is no rational right triangle has the area 1.

We use triples to denote the sides of right-angled triangle such as (α, β, γ).

Example 2.1. $\frac{3}{2}, \frac{20}{3}, \frac{49}{12}$ are the rational numbers which Fibonacci found and the triples $(\frac{3}{2}, \frac{20}{3}, \frac{49}{12})$ represents the right triangle whose area is 5 and implies 5 is a congruent number.

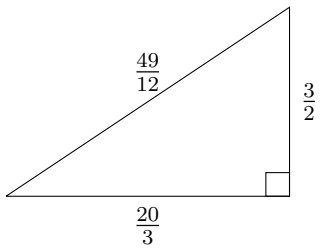

Figure 2.1: 5 is a congruent number.

Example 2.2. $(\frac{24}{5}, \frac{35}{12}, \frac{337}{60})$

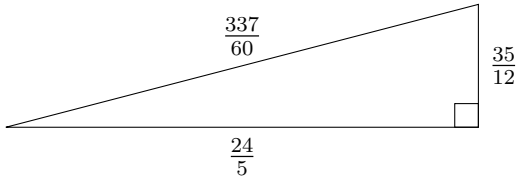

Figure 2.2: 7 is a congruent number.

Definition 2.3. *A Rational Pythagorean triple* is a triple (α, β, γ) where $\alpha, \beta, \gamma \in \mathbb{Q}$ such that

$$\alpha^2 + \beta^2 = \gamma^2.$$

Definition 2.4. *A Primitive Pythagorean triple* is a Pythagorean triple of integers (α, β, γ) such that $\alpha, \beta, \gamma \in \mathbb{Z}$ and $\gcd(\alpha, \beta, \gamma) = 1$.

There are infinitely many primitive triples, but this does not imply every natural number will be the area of a right triangle. For example, 5 is not the area of any primitive Pythagorean triples.

Scaling the sides of a right triangle changes the area by a square factor. Let N be a congruent number which is area of a rational right triangle (a, b, c), when we scale it by k the new rational right triangle (ka, kb, kc) will have area k^2N which is another congruent number. So, we assume without loss of generality, the congruent number N is a square-free number.

Example 2.5. Let $(\frac{3}{2}, \frac{20}{3}, \frac{41}{6})$ represent the sides of a right triangle. The area of this triangle is 5. If we multiply sides by 12, the new triple will be $(18, 80, 82)$ and the new area $720 = 12^2 \cdot 5$. If we multiply sides by 6 the new triple for the triangle is $(9, 40, 41)$ and the area will be $180 = 6^2.5$. All the numbers $5, 180, 720$ are congruent numbers.

1 Congruent Number Problem

Definition 2.6. Original Version of CNP

For a whole number N, does there exist a square a^2 such that $a^2 - N$ and $a^2 + N$ are also squares?

Definition 2.7. Triangular Version of CNP For a whole number N, does there exist a rational right triangle with the area N?

These two version of the congruent number problem refer to search the same number N.

Let N be the area of the rational triangle represented by (α, β, γ), We have $\alpha, \beta, \gamma \in \mathbb{Q}$ with $\alpha^2 + \beta^2 = \gamma^2$ and $N = \frac{1}{2}\alpha\beta$. If we multiply N by 4 we have

$$(\alpha + \beta)^2 = \gamma^2 - 4N$$

$$(\alpha - \beta)^2 = \gamma^2 + 4N$$

then, if we divide them by 4 again, we have

$$(\frac{\alpha + \beta}{2})^2 = (\frac{\gamma}{2})^2 - N \tag{1.1}$$

$$(\frac{\alpha - \beta}{2})^2 = (\frac{\gamma}{2})^2 + N \tag{1.2}$$

So there exist a square $(\frac{\gamma}{2})^2$ such that $(\frac{\gamma}{2})^2 - N$ and $(\frac{\gamma}{2})^2 + N$ are also squares. Now, we can define a congruent number formally:

Definition 2.8. A natural number N is a *congruent number* if there exists $\alpha, \beta, \gamma \in \mathbb{Q}$ such that

$$\alpha^2 + \beta^2 = \gamma^2 \quad \text{and} \quad N = \frac{1}{2}\alpha\beta.$$

Working with square-free integers and primitive Pythagorean triples reduce the case. We can construct Pythagorean triple which is generated by Euclid's formula.

Theorem 2.9 (Euclid's Formula)**.** *A triple* (α, β, γ) *of integers is a Primitive Pythagorean triple if and only if there exist relatively prime natural numbers,* m *and* n*, such that* $m > n$ *and* $\alpha = 2mn, \beta = m^2 - n^2, \gamma = m^2 + n^2$.

This parametric formula helps to construct some congruent numbers. Taking any relatively prime $m, n \in \mathbb{N}$, with $m > n$ and evaluating them for $\alpha = 2mn$ and $\beta = m^2 - n^2$, $\gamma = m^2 + n^2$. These Primitive Pythagorean triples give a congruent number which is the area of right triangle.

$$N = \text{Area} = \frac{1}{2}\alpha\beta = \text{Congruent Number} = mn(m^2 - n^2).$$

In Table 2.1, we list some of Primitive Pythagorean triples from chosen $m, n < 8$, the area N and square-free part of N.

As seen in the Table 2.1 some of congruent numbers repeated and we do not know which one can repeat again. We can extend the Table 2.1 for increasing values of m and n to find more congruent numbers but, one can **not** tell how long one must wait to get N if it is congruent. Also **if** N **has not appeared, we do not know whether this means that** n **is not a congruent number.** So this table only can help to construct some congruent numbers, but it is not an algorithm.

Example 2.10. 53 is a congruent number, but it shows up for the first time when

$$m = 1873180325$$

and

$$n = 1158313156$$

with the area

$$N = 53 \times (297855654284978790)^2$$

Example 2.11. Searching to determine whether a number is congruent or not from the sides of the right-triangles is not easy calculation. As an example the congruent number $N = 157$ as the area of the right triangle which has the sides

$$\alpha = \frac{411340519227716149383203}{21666555693714761309610}$$

$$\beta = \frac{6803298487826435051217540}{411340519227716149383203}$$

This is the "simplest" triangle for the congruent number 157 and was initially mentioned by Don Zagier in his article. [Zag90]

September 22, 2009 – Mathematicians from North America, Europe, Australia, and South America have resolved the first one trillion cases of an ancient mathematics problem [Har08].

Some of the congruent numbers [Slo11]:

$$5, 6, 7, 13, 14, 15, 20, 21, 22, 23, 24, 28, 29, 30, 31, 34, 37, 38, 39, 41, 45,$$
$$46, 47, 52, 53, 54, 55, 56, 60, 61, 62, 63, 65, 69, 70, 71, 77, 78, 79, 80,$$
$$84, 85, 86, 87, 88, 92, 93, 94, 95, 96, 101, 102, 103, 109,$$
$$110, 111, 112, 116, 117, 118, 119, 120, 124, 125, 126, \ldots$$

2 Arithmetic progressions of three squares

Theorem 2.12. *Let $n > 0$. There is a one to one correspondence between right triangles with area N and 3-term arithmetic progressions of squares with common difference N: the sets*

$$\{(\alpha, \beta, \gamma) : \alpha^2 + \beta^2 = \gamma^2, \frac{1}{2}\alpha\beta = N\} \quad \textit{and} \quad \{(r, s, t) : s^2 - r^2 = t^2 - s^2 = N\}$$

are in one-to-one correspondence by

$$(\alpha, \beta, \gamma) \mapsto (\frac{\beta - \alpha}{2}, \frac{\gamma}{2}, \frac{\beta + \alpha}{2}) \quad \textit{and} \quad (r, s, t) \mapsto (t - r, t + r, 2s).$$

This correspondence preserves rationality and positivity/monotonicity, when $N > 0$.

Example 2.13. The congruent number $N = 21$ is the area of a triangle represented by the triple $(\frac{7}{2}, \frac{24}{2}, \frac{25}{2})$. Using the correspondence in Theorem 2.12, this triple yields $(r, s, t) = (\frac{17}{4}, \frac{25}{4}, \frac{31}{4})$, whose termwise squares are $(\frac{17}{4})^2, (\frac{25}{4})^2, (\frac{31}{4})^2$ with common difference 21.

Theorem 2.14 ([Kob93])**.** *Let N be a fixed square-free positive integer. Let α, β, γ be positive rational numbers $\alpha < \beta < \gamma$ There is one to one correspondence between right-angled triangle with legs α and β, hypotenuse γ and area N; and numbers x for which $x, x + N, x - N$ are each the square of a rational numbers. The correspondence is*

$$\alpha, \beta, \gamma \mapsto x = (\frac{\gamma}{2})^2$$

and

$$x \mapsto \alpha = \sqrt{x + N} - \sqrt{x - N}, \quad \beta = \sqrt{x + N} + \sqrt{x - N}, \quad \gamma = 2\sqrt{x}.$$

Definition 2.15. An integer N is a *congruent number* if and only if there exists a rational number x such that $x, x + N, x - N$ are squares of rational numbers.

By Definition 2.8, an integer N being Congruent Number is equivalent to the existence of rational numbers α, β, γ such that

$$\gamma^2 = \alpha^2 + \beta^2 \quad \text{and} \quad N = \frac{1}{2}\alpha\beta.$$

If we multiply equations (1.1) and (1.2) from page 5 side by side we get

$$(\frac{\alpha^2 - \beta^2}{4})^2 = (\frac{\gamma}{2})^4 + N^2.$$

Let $v = \frac{\alpha^2-\beta^2}{4}$, and let $u = (\frac{\gamma}{2})$. Then we have

$$v^2 = u^4 - N^2.$$

Multiplying by u^2, we get

$$(uv)^2 = u^6 - N^2u^2.$$

Setting $x = u^2 = (\frac{\gamma}{2})^2$ and $y = uv = \frac{\gamma(\alpha^2-\beta^2)}{8}$, we obtain

$$y^2 = x^3 - N^2x$$

which is the equation of an elliptic curve.

Table 2.1: Congruent Numbers from Pythagorean Triples/

m	n	(α, β, γ)	N = Area	Square-free part of N
2	1	(4, 3, 5)	6	6
3	1	(6, 8, 10)	24	6
3	2	(12, 5 , 13)	30	30
4	1	(8, 15, 17)	60	15
4	3	(24 , 7 , 25)	84	21
4	2	(16, 12, 20)	96	6
5	1	(10 , 24 , 26)	120	30
5	4	(40 , 9 , 41)	180	5
5	2	(21, 20, 29)	210	210
5	4	(9, 40 , 41)	180	5
4	3	(7, 24, 25)	84	21
6	1	(35, 12, 37)	210	210
8	1	(63, 16, 65)	504	6
7	2	(45, 28, 53)	630	70

Chapter 3

Connection of Congruent Numbers with Elliptic Curves

From this point we see that **the number N which is the area of the right triangle with rational sides α, β, γ corresponds a rational point on the special family of the elliptic curves,**

$$E_N := y^2 = x^3 - N^2 x$$

One can prove that, if we have a right-angled triangle with rational sides α, β, γ and area N we can calculate the corresponding rational point (x, y) on the

$$E_N : y^2 = x^3 - (\frac{1}{2}\alpha\beta)^2 x$$

which gives

$$(x, y) = (\frac{\gamma^2}{4}, \frac{(\beta^2 - \alpha^2)\gamma}{8})$$

is on the curve.

Example 3.1. If we choose $(3, 4, 5)$ triangle which has the area 6, the corresponding rational points on the elliptic curve $E_N := y^2 = x^3 - 6^2 x$ is $(x, y) = \left(\frac{25}{4}, \pm\frac{35}{8}\right)$. We have two points since α and β are right legs and interchangeable, and elliptic curves is symmetric about the x-axis.

Example 3.2. If we choose $(16, 63, 65)$ triangle which has the area 504 the rational points $(x, y) = (\frac{4225}{4}, \pm\frac{241345}{8})$ is on the elliptic curve $E_N : y^2 = x^3 - 504^2 x$.

Notice that triangles $(3, 4, 5)$ and $(16, 63, 65)$ show 6 is a congruent number, since square-free part of 504 is 6.

Example 3.3. The triangles $(21, 20, 29)$ and $(35, 12, 37)$ have the same area 210, but each triangle corresponds to different points on the curve $E_N : y^2 = x^3 - 210x$ which are

$$(\frac{841}{4}, \pm\frac{1189}{8}) \quad \text{and} \quad (\frac{1369}{4}, \pm\frac{39997}{8}).$$

Determining whether or not a given natural number is congruent is equivalent to rational solutions of the curve $E_N : y^2 = x^3 - N^2 x$.

Theorem 3.4 ([Con]). *For $N > 0$, there is one to one correspondence between following two sets:*

$$\{(\alpha,\beta,\gamma) : \alpha^2+\beta^2=\gamma^2, N=\frac{1}{2}\alpha\beta\}, \quad \{(x,y) : y^2=x^3-N^2x, \quad y\neq 0\}.$$

Mutually inverse correspondences between these sets are

$$(\alpha,\beta,\gamma)\mapsto\big(\frac{N\beta}{\gamma-\alpha},\frac{2N^2}{\gamma-\alpha}\big), \quad (x,y)\mapsto\big(\frac{x^2-N^2}{y},\frac{2Nx}{y},\frac{x^2+N^2}{y}\big).$$

In the set of triples since $\alpha,\beta,\gamma\in\mathbb{Q}$ for each triple there are 8 possibilities satisfying $\alpha^2+\beta^2=\gamma^2$ and $N=\frac{1}{2}\alpha\beta$.

Four of these points are

$$(\alpha,\beta,\gamma), \quad (-\alpha,-\beta,-\gamma), \quad (-\alpha,-\beta,\gamma), \quad \text{and} \quad (\alpha,\beta,-\gamma).$$

Since α and β are right legs, they are interchangeable to give the remaining four points

$$(\beta,\alpha,\gamma), \quad (-\beta,-\alpha,-\gamma), \quad (-\beta,-\alpha,\gamma), \quad \text{and} \quad \beta,\alpha,-\gamma).$$

Each triple give us a new point on the corresponding elliptic curve. Table 3.1 shows how these points are related each other, for example if we take the point (x,y) and $(0,0)$, the line connecting these two points will intersects with the curve at a third point which gives us with the correspondence the triple $(\alpha,\beta,-\gamma)$.

Table 3.1: 8 Points on E_N Correspond 8 Triples for The Area N.

First Point	Second Point	Third Point	Corresponding Triple
(x,y)			(α,β,γ)
$(x,-y)$			$(\alpha,\beta,-\gamma)$
(x,y)	$(0,0)$	$(\frac{-N^2}{x},\frac{-N^2y}{x^2})$	$(\alpha,\beta,-\gamma)$
$(x,-y)$	$(0,0)$	$(\frac{-N^2}{x},\frac{N^2y}{x^2})$	$(-\alpha,-\beta,\gamma)$
(x,y)	$(N,0)$	$(\frac{N(x+N)}{x-N},\frac{2N^2y}{(x-N)^2})$	(β,α,γ)
$(x,-y)$	$(N,0)$	$(\frac{N(x+N)}{x-N},\frac{-2N^2y}{(x-N)^2})$	$(-\beta,-\alpha,-\gamma)$
(x,y)	$(-N,0)$	$(\frac{-N(x+N)}{x-N},\frac{2N^2y}{(x-N)^2})$	$(-\beta,-\alpha,\gamma)$
$(x,-y)$	$(-N,0)$	$(\frac{-N(x+N)}{x-N},\frac{-2N^2y}{(x-N)^2})$	$(\beta,\alpha,-\gamma)$

The triple of the lengths of rational right triangle with area N with the arithmetic progression produces different points on the corresponding elliptic curve E_N.

Definition 3.5 (**Elliptic Curve Version of CNP**). For a whole number N, does there exists a rational point(x, y) with $y \neq 0$ on the elliptic curve $E_N : y^2 = x^3 - N^2$?

Notice that, given a right triangle with rational sides and area N, we obtain a point (x, y) in the xy-plane having rational coordinates and lying on the curve $E_N : y^2 = x^3 - N^2x$. Conversely, we can not say that *any point* (x, y) *with* $x, y \in \mathbb{Q}$ *which lies on the cubic curve must necessarily come from such a right triangle with rational sides.*

Example 3.6. Consider the right triangle $(\frac{3}{2}, \frac{20}{3}, \frac{41}{6})$ with area 5. By Theorem 3.4, we can find the corresponding point (x, y) on the elliptic curve $E_N := y^2 = x^3 - 25x$. If we allow sign changes of (α, β, γ) we get different points for each triples, as show in Table 3.2.

Table 3.2: Solutions to $y^2 = x^3 - 25x$.

Triples for triangle	Points on E_N
$(\frac{3}{2}, \frac{20}{3}, \frac{41}{6})$	$(\frac{25}{4}, \frac{75}{8})$
$(\frac{-3}{2}, \frac{-20}{3}, \frac{-41}{6})$	$(\frac{25}{4}, \frac{-78}{8})$
$(\frac{3}{2}, \frac{20}{3}, \frac{-41}{6})$	$(-4, -6)$
$(\frac{-3}{2}, \frac{-20}{3}, \frac{41}{6})$	$(-4, 6)$
$(\frac{20}{3}, \frac{3}{2}, \frac{41}{6})$	$(45, 300)$
$(\frac{-20}{3}, \frac{-3}{2}, \frac{-41}{6})$	$(-45, 300)$
$(\frac{-20}{3}, \frac{-3}{2}, \frac{41}{6})$	$(\frac{-5}{9}, \frac{100}{27})$
$(\frac{20}{3}, \frac{3}{2}, \frac{-41}{6})$	$(\frac{-5}{9}, \frac{-100}{27})$

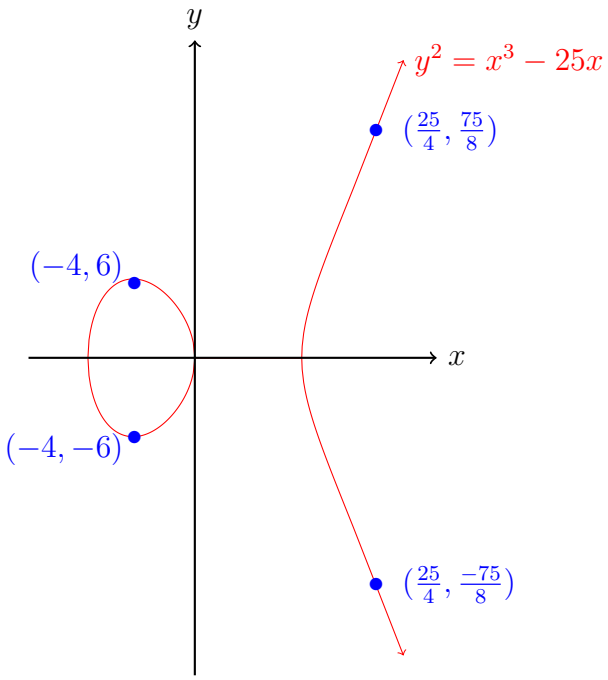

Figure 3.1: Some rational points on $y^2 = x^3 - 25x$.

Chapter 4

Projective Plane

An elliptic curve can be viewed as a curve in projective space.In order to understand elliptic curves we need some basic knowledge about projective plane.The projective plane contains triples $(x, y, z) \neq (0, 0, 0)$. We denote the line through the vector (x, y, z) by $[x : y : z]$ which represent all the points of the form $[\lambda x : \lambda y : \lambda z]$ for some nonzero λ with the equivalence relation $\sim$ on all triples. This allows us to define $\mathbb{P}^2_{\mathbb{Q}}$ as

$$\mathbb{P}^2_{\mathbb{Q}} = \{(x, y, z) \mid (x, y, z) \neq (0, 0, 0) \quad \text{and} \quad x, y, z \in \mathbb{Q}\}/\sim .$$

Elliptic curves in the affine plane $\mathbb{A}^2$ are projections of the cubic curves in the projection plane $\mathbb{P}^2$.The affine and projective space are defined over a field.The coordinates of the points of elliptic curves can belong to such as $\mathbb{C}$, $\mathbb{R}$, $\mathbb{Q}$. The properties of the curve may change depending on the field over where it is defined.In this paper, we work over $\mathbb{Q}$.In an affine plane $\mathbb{A}^2$ parallel lines never meet but in a projective plane $\mathbb{P}^2$, there are no parallel lines at all; all lines must intersect, and this intersection point is the basic idea for the notion of a **point at infinity**. Projective space can be defined as

$$\mathbb{P}^2 = \mathbb{A}^2 \cup \mathcal{O}$$

The projective plane is generalization of the ordinary xy-plane. In each equivalence class where $z \neq 0$ there is a unique point $(x, y, 1)$ which is obtained by normalizing by multiplication by z^{-1}.The new points we gain are the ones $z = 0$; the line at infinity. We are interested in the point $[0 : 1 : 0]$ which is the only point on the line at infinity that lies on the curve E_N.

1 Point Addition Of Elliptic Curve

The fact that the equation of the elliptic curves E_N implies that any line intersects with the curve must intersect in a third point. We can define an addition on the points of an elliptic curve with the third point as the sum of these two points. Unfortunately, associativity property does not hold with this operation, but by reflecting the third point over x axis, we obtain nice operation for the point addition of the elliptic curves.This geometric construction is also algebraic. An elliptic curve has one point at infinity, and is counted as a rational point.

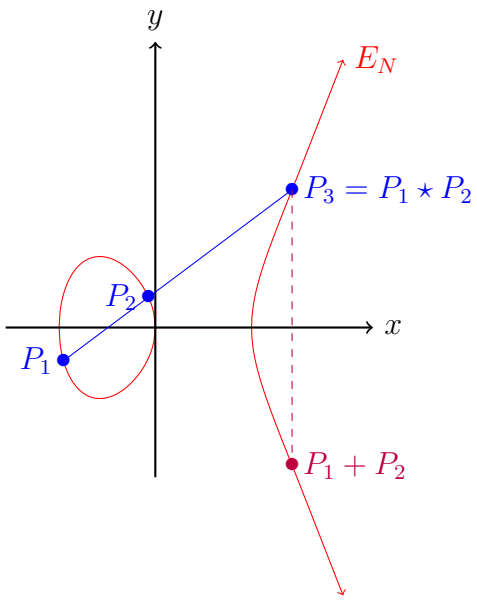

Figure 4.1: The sum of points P_1 and P_2.

The set of rational points on the elliptic curve corresponding to N; denoted by $E(\mathbb{Q})$ forms an Abelian group.

We take the point at infinity, $\mathcal{O}$, as the identity element. Let P_1 and P_2 be two distinct points on the curve, the line passing through P_1 and P_2 must intersects with the curve at a third point $P_1 \star P_2$.

Then we will draw the line through $\mathcal{O}$ and $P_1 \star P_2$. This is the vertical line through $P_1 \star P_2$. since elliptic curves are symmetric about the x-axis, so the intersection of this line with the curve in a second time will be reflection point of $P_1 \star P_2$. If we define the binary operation $\star$ such that $P_1 \star P_2$ is the third intersection point of the line connecting P_1 and P_2 with the curve, then the addition of points of the elliptic curve can be defined

$$P_1 + P_2 = \mathcal{O} \star (P_1 \star P_2)$$

where $\mathcal{O}$ is the point at infinity with $\mathcal{O} \star \mathcal{O} := \mathcal{O}$.

Suppose E has equation

$$y^2 = x^3 - N^2 x.$$

Let $P_1 = (x_1, y_1)$, and let $P_2 = (x_1, y_2)$. The line through P_1 and P_2 intersects the curve in a third point $P_3 = P_1 \star P_2 = (x_3, y_3)$. Then from the construction, it follows $P_1 + P_2 = (x_3, -y_3)$, the reflection of the point P_3. See Figure 4.1.

The inverse a point P is the reflection across the x-axis of the point P. Let $-P = Q$, the line through P and Q is vertical; $P \star Q = \mathcal{O}$. See Figure 4.2.

$$\begin{aligned} P + Q &= \mathcal{O} \star (P \star Q) \\ &= \mathcal{O} \star \mathcal{O} \\ &= \mathcal{O} \end{aligned}$$

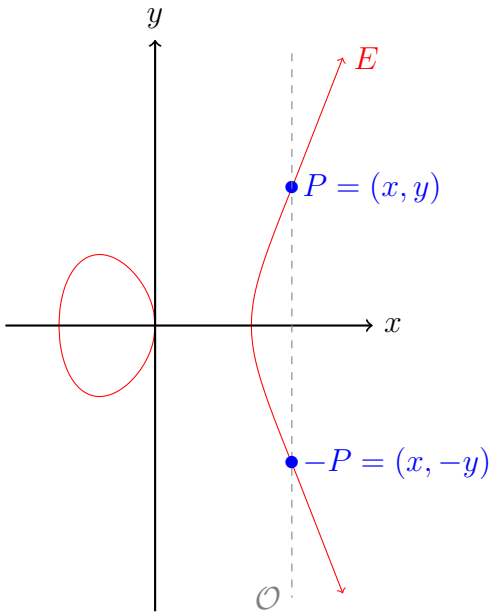

Figure 4.2: The inverse of a point P is the reflection acorss the x-axis of P.

We can see easily $\mathcal{O} = -\mathcal{O}$ since $(P) + (-P) = \mathcal{O}$ and if three distinct points on an elliptic curve are colinear if and only if $P_1 + P_2 + P_3 = \mathcal{O}$.

Algebraically the line connecting P_1 , P_2, and P_3 is

$$y = mx + n, \tag{1.1}$$

where

$$m = \frac{y_2 - x_2}{x_2 - x_1} \quad \text{and} \quad n = y_1 - mx_1 = y_2 - mx_2.$$

We can compute the third intersection point P_3; when we substitute the equation (1.1) into the equation for $E_N : y^2 = x^3 - N^2x$, we have

$$\begin{aligned} x^3 - N^2x &= y^2 \\ &= (mx + n)^2 \\ &= m^2x^2 + 2mnx + n^2. \end{aligned}$$

Then

$$\begin{aligned} x^3 - N^2x - m^2x^2 - 2mnxnv^2 &= 0 \\ x^3 - m^2x^2 - (N^2 + 2mn)x - n^2 &= (x - x_1)(x - x_2)(x - x_3). \end{aligned}$$

Simplifying, we see

$$-m^2 = -x_1 - x_2 - x_3$$

and so

$$x_3 = m^2 - x_1 - x_2 \quad \text{and} \quad y_3 = mx_3 + n.$$

Thus, in order to find $P_1 + P_2$ first we will find the coordinates of P_3 and then reflect over the x-axis which is $(x_3, -y_3)$.

If the points are the same, we use the tangent line to define this addition. Since $P_1 + P_1 = 2P_1 := P$ we draw the tangent line to P and then find the third point of intersection with the curve and then reflect about x-axis.

2 $(E(\mathbb{Q}), +)$ is an Abelian group.

Commutativity

For any two points P_1, P_2 on $E(\mathbb{Q})$,

$$P_1 + P_2 = P_2 + P_1.$$

Since there is a unique line through P_1 and P_2 , then third point of intersection with the curve is the same for the line through P_2 and P_1.

Closure

$E(\mathbb{Q})$ is closed under the binary operation $+$. Since for all $P_1, P_2 \in E(\mathbb{Q})$, $P_1 + P_2 \in E(\mathbb{Q})$.

Identity element

The identity element for the binary operation $+$ is the point at the infinity, $\mathcal{O}$, since for all P_1, P_2 on the elliptic curve $E(\mathbb{Q})$

$$P_1 + P_2 = \mathcal{O} \star (P_1 \star P_2).$$

Thus, for any point P on the elliptic curve

$$\mathcal{O} + P = \mathcal{O} \star (\mathcal{O} \star P) = P$$

since if $P = (x, y)$ then $\mathcal{O} \star P = -P = (x, -y)$ so $\mathcal{O} \star (\mathcal{O} \star P) = (x, y) = P$. Thus there exists an identity element for the group.

Inverse Element

For any point P on the elliptic curve there exists $-P$ such that $P + (-P) = \mathcal{O}$. Define $-P := P \star (\mathcal{O} \star \mathcal{O})$. Then

$$\begin{aligned} P + (-P) &= \mathcal{O} \star (P \star (-P)) \\ &= \mathcal{O} \star (P \star (P \star (\mathcal{O} \star \mathcal{O})) \\ &= \mathcal{O}. \end{aligned}$$

This means there is no third point on the E which intersects the line through P and $-P$.

Associativity

For all the points P_1, P_2, P_3 on the curve

$$(P_1 + P_2) + P_3 = P_1 + (P_2 + P_3).$$

See [ST15, pg 14].

3 Torsion Points

For the rational points on a non-singular elliptic curve, we could assign an order for each element P with the point addition.

Definition 4.1. An element P of any group has an *order* n if n is the minimum positive integer satisfying

$$nP = \underbrace{P + P + ... + P}_{\text{the sum of } n \text{ } P\text{s}} = \mathcal{O}.$$

If such n exists for P, then P has *finite order*. Otherwise it has *infinite order*.

In the Abelian group $E(\mathbb{Q})$, the set of elements of finite order form a subgroup, called the *torsion subgroup*.

We have the following result of Nagell–Lutz [SZ03, Theorem 6.26] that allows us to compute the torsion points of an elliptic curve over $\mathbb{Q}$.

4 Nagel–Lutz theorem

Theorem 4.2 (Nagell–Lutz Theorem)**.** *Let E be an elliptic curve in short Weierstrass normal form*

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

with integral coefficients $A, B \in \mathbb{Z}$. Let $\mathcal{O} \neq P = (x, y) \in E(\mathbb{Q})_{\text{tors}}$. Then

1. *$x, y \in \mathbb{Z}$ and*
2. *either $2P = \mathcal{O}$ or y^2 divides $\Delta_0 = \frac{-\Delta}{16} = 4A^3 + 27B^2$.*

We are interested only in the special family of the elliptic curves of the form $E_N := y^2 = x^3 - N^2x$.

Corollary 4.3. *If E_N be an elliptic curve of the form*

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

and let $\Delta_0 = 4N^6$. Then the torsion points of E_N are either $y = 0$ or $y^2 \mid 4N^6$.

Lemma 4.4. *$\#E_N(\mathbb{Q})_{\text{tors}} = 4$.*

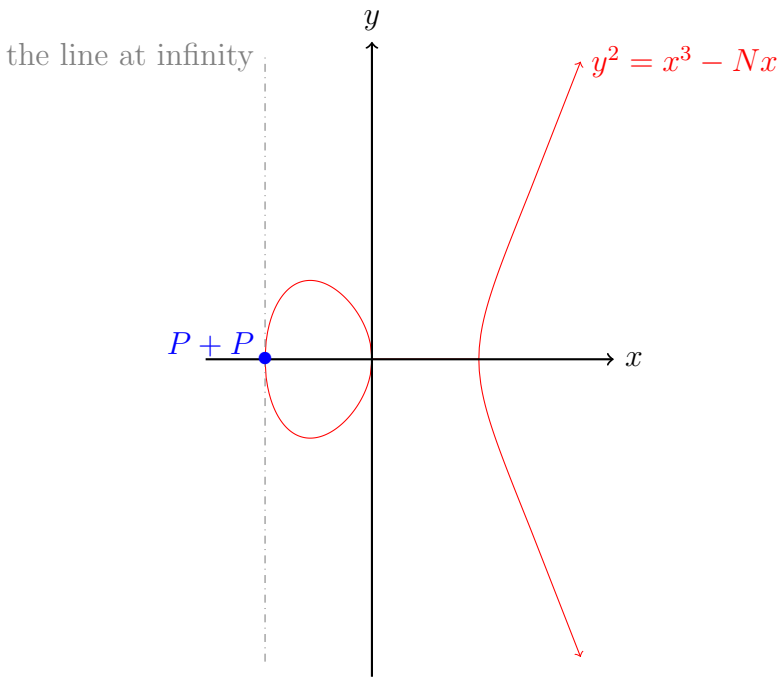

Figure 4.3: $P + P = 2P = \mathcal{O}$, P has order two.

Proof. The point P has order 2 if $P + P = 2P = \mathcal{O}, \quad$ but $\quad P \neq \mathcal{O}$.

Since $P = -P$, these points are the solutions of the curve when $y = 0$, i.e.,

$$P_1 = (0, 0), \quad P_2 = (N, 0), \quad P_3 = (-N, 0).$$

Thus, all the points of order 2 which satisfy $y^2 = x^3 - N^2x = 0$ and the point at infinity determine the full torsion subgroup of $E_N(\mathbb{Q})$.

Since $y^2 = x^3 - N^2x$ has no integer solution when $y = 0$ and $y^2 \mid 4N^6$

$$E_N(\mathbb{Q})_{\text{tors}} = \{\mathcal{O}, (0, 0), (N, 0), (-N, 0)\}.$$

Using the group law, one can show

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

For any n, the set of solutions to $nP = \mathcal{O}$ forms a subgroup of the Abelian group, so the set $\{\mathcal{O}, P_1, P_2, P_3\}$ is the torsion subgroup of the Abelian group $(E_N(\mathbb{Q}), +)$. □

Nagell–Lutz theorem gives information about an elliptic curve defined over $\mathbb{Q}$ has integer coordinates, but not about the structure of $E_N(\mathbb{Q})_{\text{tors}}$. In 1977, Mazur stated explicitly the possibilities for $E_N(\mathbb{Q})_{\text{tors}}$ for any elliptic curve over the rationals.

Nagell–Lutz theorem allows us to find all of rational the points of finite order for an elliptic curve. Suppose P is a rational point on $E_N(\mathbb{Q})$ that is not in $\{\mathcal{O}, (0, 0), (N, 0), (-N, 0)\}$. Then P is not be a torsion point so all the multiple of Ps are different.

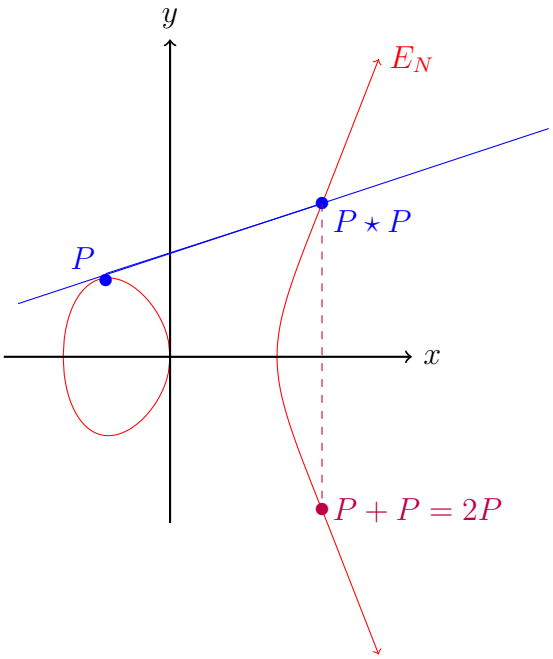

Figure 4.4: P has not finite order.

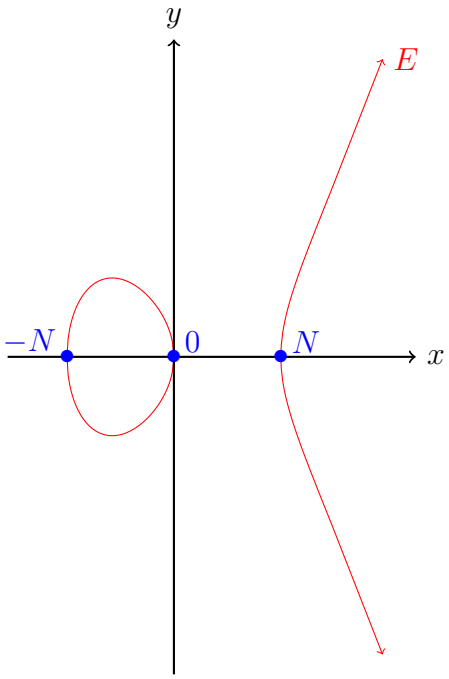

Figure 4.5: Torsion Points of $E_N : y^2 = x^3 - N^2x$.

5 Mordell–Weil theorem

One of the goals of the Number theory from the ancient times to solve Diophantine equations. In general the question is *how we can describe the set of rational numbers on any curve.*

Mordell (1992) proved that over rationals then Weil (1929) extended result for arbitrary number field.

Theorem 4.5 (Mordell–Weil)**.** *$E(\mathbb{Q})$ is a finitely generated Abelian group.*

The proof consist of two steps, which can be found in [SZ03, pg 88] and [Sil09].

Proposition 4.6. *The group of rational points $E_N(\mathbb{Q})$ is isomorphic to the direct sum of $E_N(\mathbb{Q})_{\text{tors}}$ and a finite number of copies of $\mathbb{Z}$*

$$E_N(\mathbb{Q}) \approx E_N(\mathbb{Q})_{\text{tors}} \oplus \mathbb{Z}^r$$

*where the nonnegative integer r is **rank** of $E_N(\mathbb{Q})$.*

For specific cases the rank has been determined but still it is an open problem to compute rank in general. (The current record for rank of a rational elliptic curve was found by Noam Elkies, in 2006, when he produced an elliptic curve of rank at least 28 [Duj].)

When the rank of $E_N(\mathbb{Q})$ is zero, $E_N(\mathbb{Q})$ has only torsion points. In this case, there are no points of infinite order so there are no corresponding rational triangles. If the rank $r > 0$, then the correspondence between these points on the $E_N(\mathbb{Q})$ and Pythagorean triples yields the following result.

Proposition 4.7 ([Kob93, pg.46])**.** *An integer N is a congruent number if and only if the elliptic curve*

$$E_N(\mathbb{Q}) : y^2 = x^3 - N^2x$$

has nonzero rank.

Chapter 5

5 is Congruent Number

In this chapter, we examine in detail the general results above in the specific example $N = 5$.

The triple $(\frac{3}{2}, \frac{20}{3}, \frac{49}{12})$ shows that 5 is a congruent number. See Figure 5.1.

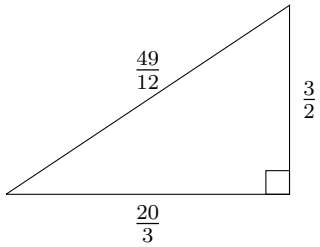

Figure 5.1: 5 is a congruent number.

Since 5 is a congruent number, there exists a right-angled triangle with rational sides which has area 5. Using the correspondence in Theorem 3.4, we find a rational point on the special elliptic curve $E_5 : y^2 = x^3 - 5^2x$.

By the Nagell–Lutz theorem $E_5(\mathbb{Q})$ has torsion subgroup

$$E_5(\mathbb{Q})_{\text{tors}} = \{\mathcal{O}, T_1, T_2, T_3\},$$

where $T_1 = (0, 0)$, $T_2 = (-5, 0)$, and $T_3 = (5, 0)$. Each T_i has order 2, and

$$T_1 + T_2 + T_3 = \mathcal{O},$$

so

$$E_5(\mathbb{Q})_{\text{tors}} \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}.$$

By the Mordell–Weil Theorem, $E_5(\mathbb{Q})$ is finitely generated. Using magma, we find the rank of $E_5(\mathbb{Q})$ is 1, so

$$E_5(\mathbb{Q}) \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}^1,$$

and the point $P = (-4, 6)$ is a generator for the free part of $E_5(\mathbb{Q})$.

Table 5.1: All the points in the table on the left give rise to one triangle whose area is 5 using Theorem 3.4.

P	$(-4, 6)$
$P + T_1$	$(\frac{25}{4}, \frac{75}{8})$
$P + T_2$	$(\frac{-5}{9}, \frac{-100}{27})$
$P + T_3$	$(45, -300)$
$-P$	$(-4, -6)$
$-P + T_1$	$(\frac{25}{4}, \frac{-75}{8})$
$-P + T_2$	$(\frac{-5}{9}, \frac{100}{27})$
$-P + T_3$	$(45, 300)$

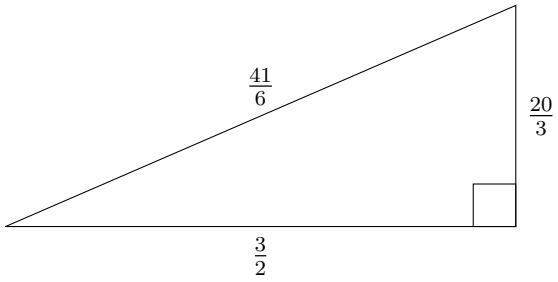

Table 5.2: All the point in the table on the left give rise to the one triangle whose area is 5 using Theorem 3.4.

$2P$	$(\frac{1681}{144}, \frac{-62279}{1728})$
$2P + T_1$	$(\frac{-3600}{1681}, \frac{-455700}{68921})$
$2P + T_2$	$(\frac{12005}{961}, \frac{1205400}{29791})$
$2P + T_3$	$(\frac{-4805}{2401}, \frac{762600}{117649})$
$-2P$	$(\frac{1681}{144}, \frac{62279}{1728})$
$-2P + T_1$	$(\frac{-3600}{1681}, \frac{455700}{68921})$
$-2P + T_2$	$(\frac{12005}{961}, \frac{-1205400}{29791})$
$-2P + T_3$	$(\frac{-4805}{2401}, \frac{-762600}{117649})$

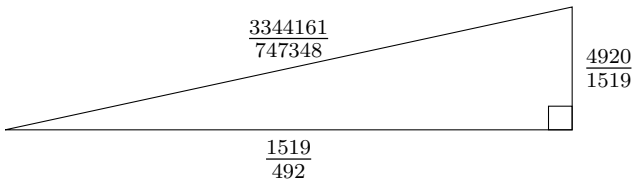

Table 5.3: All the point in the table on the left give rise to the one triangle whose area is 5 using Theorem 3.4.

$3P$	$(\frac{-2439844}{5094049}, \frac{39601568754}{11497268593})$
$3P + T_1$	$(\frac{127351225}{2439844}, \frac{1430549626725}{3811036328})$
$3P + T_2$	$(\frac{-115152005}{27910089}, \frac{845927888300}{147449000187})$
$-3P$	$(\frac{-2439844}{5094049}, \frac{-39601568754}{11497268593})$
$-3P + T_1$	$(\frac{127351225}{2439844}, \frac{-1430549626725}{3811036328})$
$-3P + T_2$	$(\frac{-115152005}{27910089}, \frac{845927888300}{147449000187})$
$-3P + T_3$	$(\frac{139550445}{23030401}, \frac{931243391100}{110522894399})$

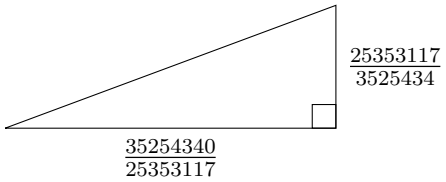

Table 5.4: 5 is a Congruent Number.

Point	(x, y)	(α, β, γ)	Area	N
P	$(-4, 6)$	$(\frac{-3}{2}, \frac{-20}{3}, \frac{41}{6})$	$(\frac{-3}{2})(\frac{-20}{3})(\frac{1}{2})$	5
$2P$	$(\frac{1681}{144}, \frac{-62279}{1728})$	$(\frac{-1519}{492}, \frac{-4920}{1519}, \frac{-3344161}{747348})$	$(\frac{-1519}{492})(\frac{-4920}{1519})(\frac{1}{2})$	5
$3P$	$(\frac{-2439844}{5094049}, \frac{39601568754}{11497268593})$	$(\frac{-25353117}{3525434}, \frac{-35254340}{25353117}, \frac{654686219104361}{89380740677778})$	$(\frac{-2439844}{5094049})(\frac{-35254340}{25353117})(\frac{1}{2})$	5
$P + T_1$	$(\frac{25}{4}, \frac{20}{3})$	$(\frac{3}{2}, \frac{20}{3}, \frac{41}{6})$	$(\frac{3}{2})(\frac{20}{3})(\frac{1}{2})$	5
$P + T_3$	$(\frac{-5}{9}, \frac{-100}{27})$	$(\frac{20}{3}, \frac{3}{2}, \frac{-41}{6})$	$(\frac{20}{3})(\frac{3}{2})(\frac{1}{2})$	5
$2P + T_2$	$(\frac{-4805}{2401}, \frac{762600}{117649})$	$(\frac{-4920}{1519}, \frac{-1519}{492}, \frac{3344161}{747348})$	$(\frac{-4920}{1519})(\frac{-1519}{492})(\frac{1}{2})$	5
$-2P$	$(\frac{1681}{144}, \frac{62279}{1728}$	$(\frac{1519}{492}, \frac{4920}{1519}, \frac{3344161}{747348})$	$(\frac{1519}{492})(\frac{4920}{1519})(\frac{1}{2})$	5
$4P$	$(\frac{11183412793921}{2234116132416}, \frac{1791076534232245919}{3339324446657665536})$	$(\frac{535583225279}{4998504070056}, \frac{49985040700560}{535583225279}, \frac{24985059404727155836448064 1}{26771149314108010461456 24})$	$(\frac{-3}{2})(\frac{-20}{3})(\frac{1}{2})$	5

Bibliography

[Cha06] Jasbir S. Chahal, *Congruent numbers and elliptic curves*, The American Mathematical Monthly **113** (2006), no. 4, 308–317.

[Con] Kevin Conrad, *The congruent number problem*, www.math.uconn.edu/~kconrad/blurbs/ugradnumthy/congnumber.pdf, [Online; accessed 2-4-2018.

[cul] cultureMATH, *Iconographie commentée et petits problèmes*, http://culturemath.ens.fr/video/html/Djebbar/icono.htm, [Online; accessed 4-4-2018].

[Duj] Sndrej Dujella, *History of elliptic curves rank records*, https://web.math.pmf.unizg.hr/~duje/tors/rankhist.html, [Online; accessed 3-5-2018.

[Fib08] Leonardo Pisano Fibonacci, *Fibonacci's de practica geometrie*, Sources and Studies in the History of Mathematics and Physical Sciences, Springer, New York, 2008, Translated from the Latin, edited and with a commentary by Barnahas Hughes, With a foreword by Frank Swetz. MR 2364574

[Har08] Bill Hart, *A trillion triangles*, https://aimath.org/news/congruentnumbers/, 2008, [Online; accessed 3-4-2018.

[Kob93] Neal Koblitz, *Introduction to elliptic curves and modular forms*, second ed., Graduate Texts in Mathematics, vol. 97, Springer-Verlag, New York, 1993. MR 1216136

[Sil09] Joseph H. Silverman, *The arithmetic of elliptic curves*, second ed., Graduate Texts in Mathematics, vol. 106, Springer, Dordrecht, 2009. MR 2514094

[Slo11] N.J.A. Sloane, *Index to oeis*, https://oeis.org/search?q=A003273+-id:A003273/, 2011, [Online; accessed 3-15-2018.

[ST15] Joseph H. Silverman and John T. Tate, *Rational points on elliptic curves*, second ed., Undergraduate Texts in Mathematics, Springer, Cham, 2015. MR 3363545

[SZ03] Susanne Schmitt and Horst G. Zimmer, *Elliptic curves*, De Gruyter Studies in Mathematics, vol. 31, Walter de Gruyter & Co., Berlin, 2003, A computational approach, With an appendix by Attila Pethö. MR 2025384

[Zag90] D. Zagier, *Elliptische Kurven: Fortschritte und Anwendungen*, Jahresber. Deutsch. Math.-Verein. **92** (1990), no. 2, 58–76. MR 1056202