

Nagell-Lutz Theorem: Finding Points of Finite Order for Elliptic Curves

Stephen Laffey

Math 466: Abstract Algebra I | Department of Mathematics | Colorado State University | Contact: Stephen.Laffey@colostate.edu

Introduction

Elliptic curves, expressed by the general cubic equation

$$E : y^2 = x^3 + ax^2 + bx + c,$$

where $a, b, c \in \mathbb{Q}$, in addition to being aesthetically interesting due to the symmetry of their graphs, are a powerful tool in modern mathematics, particularly in number theory and its applications to cryptography. These curves have been studied for broad application, including securing communications through elliptic cryptography.

To ensure the curve is non-singular, its discriminant

$$D = -4a^3c + a^2b^2 + 18abc - 4b^3 - 27c^2$$

must satisfy $D \neq 0$. This guarantees that E has three distinct roots, and forms a smooth curve, without cusps.

The focus of this poster is the **Nagell-Lutz Theorem**, which identifies torsion points (points of finite order) on elliptic curves defined over $\mathbb{Q}$. This theorem not only provides a systematic way to determine these points but also shows these points can be calculated in finitely few steps.

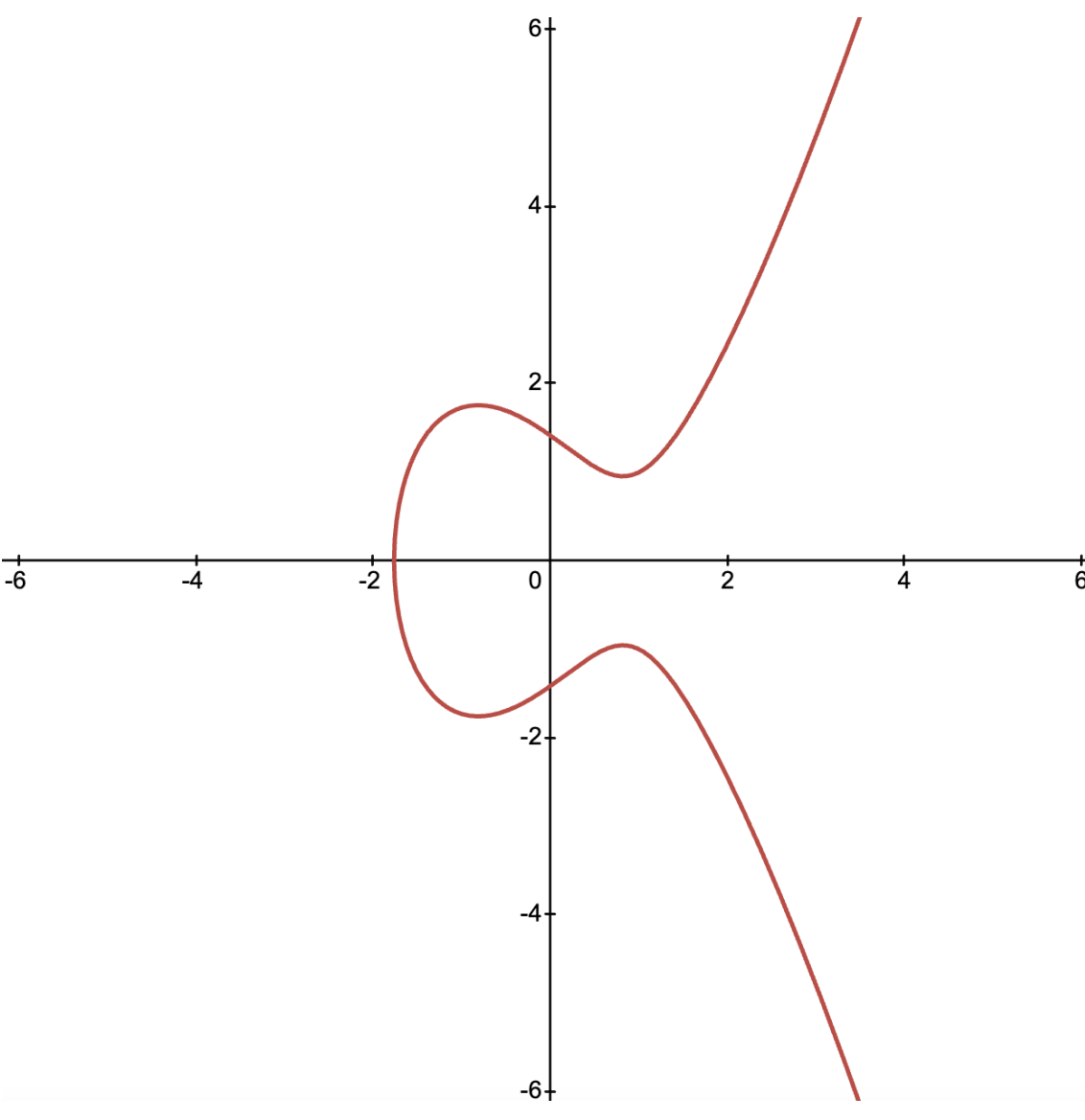


Figure: Graph of the curve:

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

Background on Elliptic Curves

An elliptic curve E over the rationals $\mathbb{Q}$ can be written in its general Weierstrass form, with assumed non-singularity:

$$E : y^2 = x^3 + ax^2 + bx + c.$$

The set of rational points $E(\mathbb{Q})$, together with a unique point at infinity $\mathcal{O}$, forms an abelian group under the group law of addition. The addition of points on the curve is defined geometrically:

- For distinct points $P = (x_1, y_1)$ and $Q = (x_2, y_2)$, the slope λ is given by:

$$\lambda = \frac{y_2 - y_1}{x_2 - x_1}.$$

- For the doubling of a point $P = Q$, the slope λ becomes:

$$\lambda = \frac{3x_1^2 + 2ax_1 + b}{2y_1}.$$

- The resulting point $R = (x_3, y_3)$ is calculated as:

$$x_3 = \lambda^2 - a - x_1 - x_2, \quad y_3 = \lambda(x_1 - x_3) - y_1.$$

Points of Finite Order

A (torsion) point P on an elliptic curve is said to be of **order** n if $nP = \mathcal{O}$, where $\mathcal{O}$ is the point at infinity. In simpler terms, repeatedly adding P to itself n times yields the identity element $\mathcal{O}$. Identifying such points is essential to understanding the group structure of elliptic curves.

Points of Order 2: A point P is of order 2 if $2P = \mathcal{O}$, which implies $P = -P$. For a point $P = (x, y)$, this condition is satisfied exactly when $y = 0$. Geometrically, these are the x -intercepts (roots) of the elliptic curve E , so there are a maximum of three such points for any curve.

Points of Order 3: A point P is of order 3 if $3P = \mathcal{O}$, or equivalently, $2P = -P$. Algebraically, this occurs if and only if P is a root of the cubic division polynomial:

$$\psi_3(x) = 3x^4 + 4ax^3 + 6bx^2 + 12cx + 4ac - b^2.$$

This polynomial has at most 4 (rational) roots, corresponding to at most 8 (rational) points of order 3.

Example Determining Order of Given Torsion Point

Take $E : y^2 = x^3 - 43x + 166$

Let's look at the torsion structure of the curve E by starting with a known torsion point $P = (-5, 16)$. Using the group law, we can compute successive multiples of P to determine its order and identify other torsion points.

Step 1: Compute $2P = (x_2, y_2)$ Using the formula for point doubling:

$$\lambda = \frac{3x_1^2 + a}{2y_1}, \quad x_2 = \lambda^2 - 2x_1, \quad y_2 = \lambda(x_1 - x_2) - y_1,$$

where $x_1 = -5$, $y_1 = 16$, and $a = -43$, we find:

$$\lambda = \frac{3(-5)^2 + (-43)}{2(16)} = \frac{75 - 43}{32} = \frac{32}{32} = 1.$$

Substituting $\lambda = 1$:

$$x_2 = 1^2 - 2(-5) = 1 + 10 = 11, \quad y_2 = 1(-5 - 11) - 16 = -32.$$

Thus, $2P = (11, -32)$.

Step 2: Compute $3P = P + 2P = (x_3, y_3)$ For $P_1 = (-5, 16)$ and $P_2 = (11, -32)$: Following the identified steps for point addition, you will find, $3P = (3, 8)$.

Step 3: Continue Successive Additions. Following the same process, compute $4P, 5P$ and $6P$. Following this process, $6P = (-5, -16)$. Now, the slope λ between P and $6P$ is undefined, and their addition is the point at infinity. These computations identify all torsion points of the curve:

$$\{(-5, 16), (11, -32), (3, 8), (-1, -10), \dots, \mathcal{O}\}.$$

Result: The torsion subgroup $E_{\text{tors}}(\mathbb{Q})$ consists of these points and forms a cyclic subgroup. The computations verify that P is a point of order 7, as $7P = \mathcal{O}$. **Note:** In this case, each of the identified points is also of order 7, and starting from any torsion point would yield the remaining torsion points.

The Nagell-Lutz Theorem

Let

$$y^2 = f(x) = x^3 + ax^2 + bx + c$$

be a non-singular cubic curve with integer coefficients a, b, c , and let D be the non-zero discriminant of the cubic polynomial:

$$D = -4a^3c + a^2b^2 + 18abc - 4b^3 - 27c^2.$$

The Nagell-Lutz Theorem states that if $P = (x, y)$ is a rational point of finite order on the curve, then:

- Both x and y are integers.
- Either $y = 0$ (in which case P is a point of order 2), or y^2 divides the discriminant D .

Implications: Although we will not prove this theorem, its implications are significant. It allows us to determine the torsion points of a given curve in a finite number of steps (a significant accomplishment), because these points must have integer coordinates. Also, the divisibility condition on y^2 greatly reduces the anticipated search time for such torsion points.

History: The theorem is named for its two independent discoverers: Norwegian Trygve Nagell (1895-1988) and Frenchwoman Élisabeth Lutz (1914-2008).

Example: Finding Torsion Points

Take $E : y^2 = x^3 - 11x + 6$

Let us use the Nagell-Lutz Theorem to find all torsion points on the curve:

$$y^2 = x^3 - 11x + 6.$$

Step 1: Compute the Discriminant For this curve, $a = -11$, $b = 6$, and $c = 0$. Using the discriminant formula:

$$D = 4(-11)^3 - 27(6)^2,$$

the discriminant simplifies to:

$$D = -6296.$$

Step 2: Identify Possible Values for y^2 By the Nagell-Lutz Theorem, y^2 must equal 0 or divide $D = -6296$. This leaves the following y values to test:

$$0, \pm 1, \pm 4$$

Step 3: Solve for x We start with $y^2 = 0$, and solve for integer roots of

$$0 = x^3 - 11x + 6,$$

which has one integer root, 3. (This can be tested in finitely many steps via the **rational root theorem**.) So, we have found our first torsion point: $(3, 0)$.

Continuing this process gives us all of the torsion points. Substitute each valid y^2 into the curve equation:

$$y^2 = x^3 - 11x + 6.$$

Testing these values gives the torsion points:

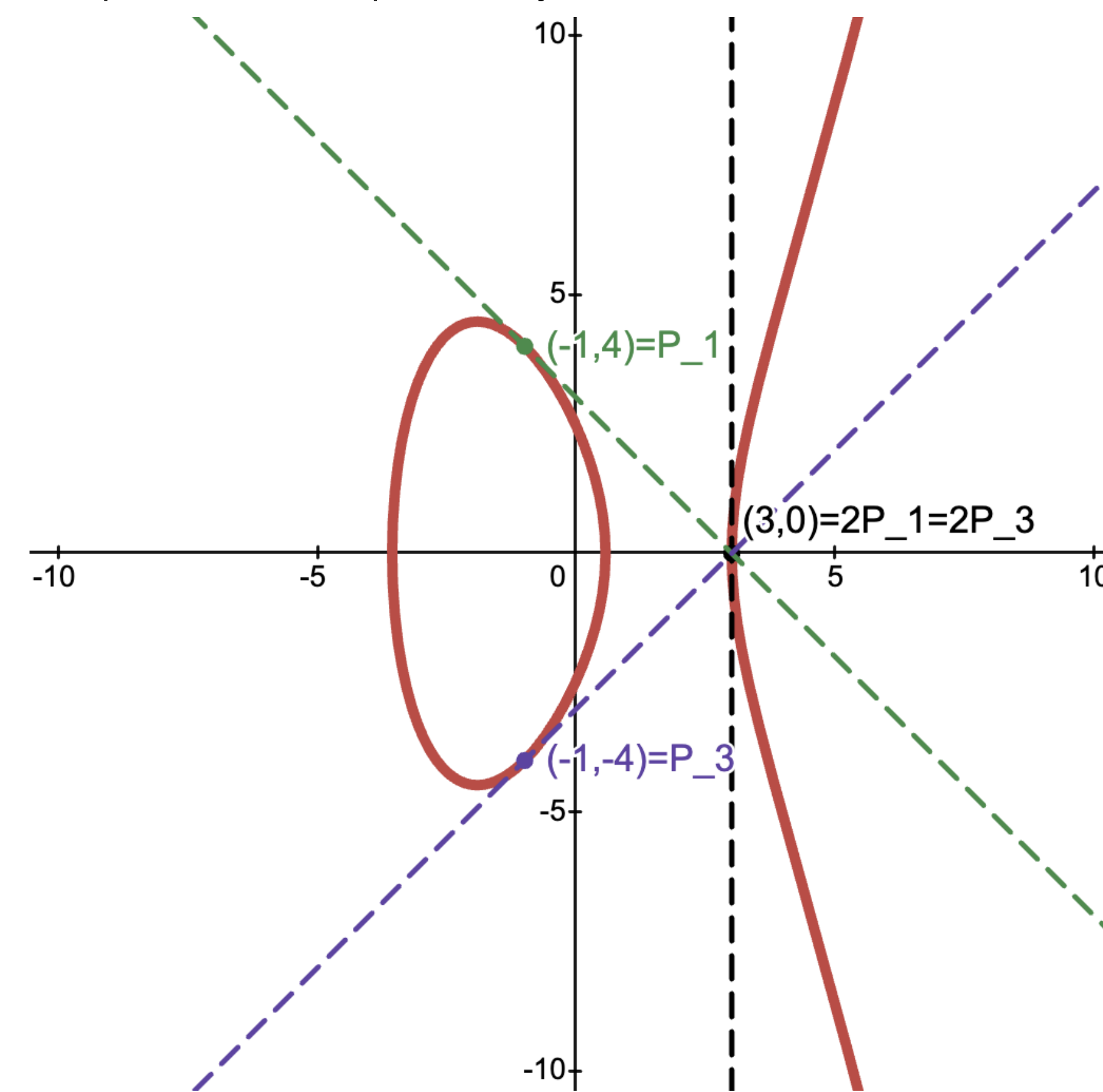
$$(-1, 4), (-1, -4), (3, 0), \mathcal{O}.$$

Summary: The torsion points on the curve $y^2 = x^3 - 11x + 6$ are:

$$\{E_{\text{tors}}(\mathbb{Q}) = (-1, 4), (-1, -4), (3, 0), \mathcal{O}\}.$$

These points form a finite subgroup under the group law, as predicted by the Nagell-Lutz Theorem. In this case, we can also state $E_{\text{tors}}(\mathbb{Q}) \cong \mathbb{Z}/4\mathbb{Z}$. (See Applications Section).

Figure: Graph, with torsion points, of $y^2 = x^3 - 11x + 6$:



Applications: Torsion Points Form a Subgroup

One of the key applications of the Nagell-Lutz Theorem is its role in understanding the group structure of elliptic curves. The torsion points on an elliptic curve, identified as points of finite order, form a finite subgroup of the larger group of rational points, $E(\mathbb{Q})$.

Subgroup Properties:

- The torsion subgroup, denoted $E_{\text{tors}}(\mathbb{Q})$, is closed under the group law defined on the curve. This means that the sum of any two torsion points is also a torsion point.
- The torsion subgroup is abelian, meaning the addition operation is commutative: $P + Q = Q + P$ for all $P, Q \in E_{\text{tors}}(\mathbb{Q})$.
- The structure of $E_{\text{tors}}(\mathbb{Q})$ is given by the **Mazur's theorem**, which states that it is isomorphic to one of 15 possible groups, such as $\mathbb{Z}/m\mathbb{Z}$, where $1 \leq m \leq 10$ or $m=12$, or $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2n\mathbb{Z}$, where n is an integer between 1 and 4.

Significance:

The fact that torsion points form a subgroup is of interest in several fields, notably elliptic curve cryptography. Silverman and Tate note that a well-defined torsion subgroup is a consideration in selecting a curve for elliptic curve cryptography.

Conclusion

The Nagell-Lutz Theorem is a powerful tool in the study of elliptic curves, providing a method of finitely many steps to determine which torsion points exist on an elliptic curve with rational coordinates.

Acknowledgments

Special thanks to Prof. Dr. Rachel Pries for her guidance and support throughout this project.

References

- Desmos Graphing Calculator: (Desmos, Amherst, 2011), WWW Document, (<https://www.desmos.com/calculator>)
- Silverman, J. H., Tate, J. T. (2015). Rational points on elliptic curves (2nd ed.). Springer
- JPAAnderson. [Dr. John Anderson]. (2023, October 14). Elliptic Curves videos 1-6 [Video]. YouTube. <https://www.youtube.com/watch?v=n6H5Je2cFss>