

Ramanujan-Nagell Equation and Elliptic Curves

Lale Baylar and Karin Lund
Harvard College '28 and Dartmouth College '29

The Ramanujan-Nagell equation $x^2 + 7 = 2^n$ is a classic Diophantine equation with integer solutions. In this paper, we explore this equation using the theory of elliptic curves and computational techniques. We transform the Ramanujan-Nagell equation into elliptic curves of the forms $y^2 = x^3 - 7$, $y^2 = 2x^3 - 7$, and $y^2 = 4x^3 - 7$, and use the Nagell-Lutz theorem to analyze torsion points and solutions. Our primary research question is: *Can we classify all integer solutions to the Ramanujan-Nagell equation using elliptic curves and computational methods?* We provide an expository presentation on the groups of rational points on elliptic curves, offering insights into their structure and properties. Computational methods using SageMath are employed to verify and explore solutions. Our work reproduces and classifies all integer solutions (2, 1) and (2, -1) for $n = 3$, (2, 3) and (2, -3) for $n = 4$, (2, 5) and (2, -5) for $n = 5$, (4, 11) and (4, -11) for $n = 7$, and (32, 181) and (32, -181) for $n = 15$, which are all solutions of the Ramanujan-Nagell equation. This analysis demonstrates the effectiveness of elliptic curves and computational techniques in solving Diophantine equations.

Introduction

In number theory, the Ramanujan-Nagell equation, named after Indian mathematician Srinivasa Ramanujan and Norwegian mathematician Trygve Nagell, is a specific Diophantine equation of the form $x^2 + 7 = 2^n$, where n and x are natural numbers. This equation has fascinated mathematicians for decades due to its elegant simplicity and the surprising depth of its solutions. Its study connects classical number theory to the rich theory of elliptic curves and arithmetic algebraic geometry.

This particular equation was derived by Ramanujan, and Nagell later proved that the integer solutions for x only occur when $n = 3, 4, 5, 7$, and 15 . There are many methods utilized to understand this equation. For example, in "The Diophantine Equation $x^2 + 7 = 2^n$," published in 1973 by the American Mathematical Society, the solution described uses a direct approach to the Diophantine equation. There are also other similar equations in the literature such as $x^2 + 11 = 3^n$, or more generally, $x^2 + p = k^n$ where k, n , and x are positive integers and p is a prime integer. In this paper, we employ the theory of elliptic curves and computational techniques, particularly using SageMath, to investigate the Ramanujan-Nagell equation. Our approach combines theoretical insights with computation tools to study and classify the solutions of this equation. The goal is to identify all integer solutions of the Ramanujan-Nagell equation by converting the equation into elliptic curves and analyzing their rational and integer points using the Mordell-Weil Theorem, the Nagell-Lutz Theorem, and the Mazur's Theorem. We would like to remark that some of the SageMath computations, such as determining the generator(s) of the Mordell-Weil group and computing higher multiples of the generator(s), are important in our solution. We have used the Mordell-Weil Theorem, the Nagell-Lutz Theorem, and Mazur's Theorem to determine the torsion subgroup of certain elliptic curves are trivial, and the SageMath computations we have provided also verifies our computation. We learned the material and were motivated by the insights from various materials, books, and lectures from (Silverman 2015), (Silverman 2009), (Lang 2012), (Cassels 1991), and (Knapp 2005).

Elliptic Curves and Group Law

Definitions and Theorems

An elliptic curve is a smooth, symmetrical curve defined by an equation like $y^2 = x^3 + Ax^2 + Bx + C$. These curves were central to Professor Andrew Wiles' proof of Fermat's Last Theorem, a famous problem that puzzled mathematicians for over 350 years (Wiles 1995).

Elliptic curves are an essential object of study in modern algebraic geometry and number theory. They exhibit fascinating properties that allow for a rich interplay between geometry and arithmetic. In particular, they form a group with the addition law, making them very important in various applications, including cryptography. In what follows, we review the definitions of elliptic curves, Weierstrass form, Bézout's Theorem, and the Cayley-Bacharach Theorem, which are important for defining the group law on an elliptic curve.

Definition 1 (Elliptic Curve) An elliptic curve is a smooth projective algebraic curve of genus one, defined over a field $\mathbb{C}$, with a specific point at infinity often denoted by O . In affine coordinates, an elliptic curve can be represented by a cubic equation of the form:

$$y^2 = x^3 + Ax^2 + Bx + C$$

where $A, B, C \in \mathbb{C}$ and the discriminant $\Delta = -4A^3C + A^2B^2 - 4B^3 - 27C^2$ is non-zero, ensuring the curve is non-singular.

Elliptic curves are a type of projective curve and have degree $d = 3$. More generally, the form of projective plane curves is defined by their degree. A projective curve includes the coordinates in a projective plane that are defined by $P(X, Y, Z)$ as zeros of a homogeneous polynomial.

Definition 2 (Weierstrass Form) An elliptic curve in Weierstrass form is given by the equation:

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

where A and B are constants, typically over a field $\mathbb{C}$.

The Weierstrass equation captures the essence of elliptic curves, expressing the relationship between the x -coordinate and the y -coordinate through a cubic equation. The smoothness condition ensures that the curve has no cusps or singularities while projectivity allows for the inclusion of points at infinity, which plays a crucial role in the arithmetic of elliptic curves.

Bézout's and Cayley-Bacharach Theorems

Theorem 1 (Bézout for $n = 2$) Let $f(x_0, x_1, x_2)$ and $g(x_0, x_1, x_2)$ be two homogeneous polynomials in three variables over an algebraically closed field k , with degrees d_1 and d_2 , respectively. If these polynomials have only a finite number of common zeros in the projective plane P^2 , then the number of common zeros, counted with multiplicity, is equal to the product of the degrees:

$$d_1 \cdot d_2.$$

In other words, if f and g are homogeneous polynomials in P^2 and

they intersect transversally, then the number of points in the intersection set $V(f) \cap V(g)$ is $d_1 \cdot d_2$.

Note that the algebraically closed field k in the statement above can be taken to be $\mathbb{C}$.

Theorem 2 (Cayley-Bacharach) Let C_1 and C_2 be two plane curves of degrees d_1 and d_2 , respectively, in the projective plane P^2 over an algebraically closed field k . Assume that C_1 and C_2 intersect in exactly $d_1 \cdot d_2$ points (counting multiplicities). Let C be a curve of degree d passing through all but one of these intersection points. Then C passes through the remaining point as well.

Note that the algebraically closed field k in the statement above can be taken to be $\mathbb{C}$.

The Bézout's Theorem and the Cayley-Bacharach Theorem will be used below to define the group law on elliptic curves.

In this paper, our focus primarily lies on exploring the properties and behavior of elliptic curves defined over the field of rational numbers, denoted by $\mathbb{Q}$ or with coefficients in $\mathbb{Z}$, and consider their rational or integer solutions only. We will mention important results below on rational points on these curves, particularly examining their integer solutions and their implications.

Elliptic Curve Group Laws

Let us now provide the precise definition of the group law on elliptic curves and explore some of its properties.

Given that (E, O) is an elliptic curve over k , the group law defines how to add points on E , resulting in another point on the curve. We define addition operation on $E(k)$ as follows the follows: $+: E(k) \times E(k) \rightarrow E(k)$

- **Identity Element:** If P is the identity element (denoted as O), then $P + Q = Q$ for any point Q , and vice versa.
- **Inverse Element:** The inverse of a point P is denoted as $-P$ and is defined as the reflection of P across the x -axis.
- **Point Doubling:** If $P = Q$, then $P + P$ is computed by drawing the tangent line to the curve at P and finding its intersection with the curve. The result is then reflected across the x -axis to obtain $P + P = 2P$.
- **Point Addition:** For distinct points P and Q , the line through P and Q intersects the curve at a third point R . The sum $P + Q$ is then defined as the reflection of R across the x -axis.

These operations define a group structure on the set of points of E , with the identity element O and associativity ensured by the geometric properties of elliptic curves, which we will explain below. This group structure on an elliptic curve is fundamental in various cryptographic protocols and number theory applications. In terms of coordinates, the above-defined operation can be given as follows:

- **Identity Element:** $(0 : 1 : 0)$, point at infinity. The point at infinity O serves as the identity element since $P + O = O + P = P$ for any point P on the curve E . Geometrically, adding O to any point P results in P itself, which is consistent with the identity element property.
- **Inverse Element:** Let P be the point with coordinates $(x : y : z)$. Then its inverse is $-P$ with coordinates $(x : -y : z)$. Geometrically, the inverse of P is the reflection of P about the x -axis. Thus, $P + (-P) = O$, ensuring the existence of inverses.
- **Closure:** For any two distinct points P and Q on E , the line passing through P and Q intersects E at a third point R . Geometrically, this is guaranteed by the tangent-secant law. Thus, the sum $P + Q = R$ is well-defined and lies on E , ensuring closure.

- **Commutativity:** Let P and Q be points on the curve. Then $P + Q = Q + P$. The commutativity property $P + Q = Q + P$ follows directly from the geometric construction of the sum point $P + Q$. Regardless of the order of addition, the resulting point remains the same due to the symmetry of the elliptic curve.
- **Associativity:** To prove associativity $(P + Q) + R = P + (Q + R)$ for any points P, Q , and R on an elliptic curve E , we use properties of the curve and Cayley-Bacharach's theorem.

Consider E as an elliptic curve given by a Weierstrass equation, where points on E satisfy this cubic equation. A fundamental property of elliptic curves is that any line intersects E in exactly three points, counting multiplicities. For points P and Q on E , the line through P and Q intersects E at a third point, say R_1 . Reflecting R_1 across the x -axis gives $-(P + Q)$, and thus $P + Q$ is defined as the reflection of R_1 , denoted by R'_1 .

Now consider points P, Q , and R on E . To prove $(P + Q) + R = P + (Q + R)$, we analyze the points of intersection produced by lines connecting these points. The line through P and Q intersects E at P, Q , and $-(P + Q)$. Similarly, the line through Q and R intersects E at Q, R , and $-(Q + R)$.

According to Bézout's theorem, the two lines will intersect E at a total of nine points, counting multiplicities. Recall Cayley-Bacharach theorem in the special case states that if two cubic curves intersect in exactly nine points, any cubic curve passing through eight of these points also passes through the ninth. Here, the cubic curves are the elliptic curve E itself and the union of lines L_1 through P and Q , and L_2 through Q and R .

The nine points of intersection are $P, Q, R, -(P + Q), -(Q + R)$, and additional points that align with the intersection properties of cubic curves. Consider the point $(P + Q) + R$, which lies on E and aligns with the points derived from P, Q , and $-(P + Q)$. Similarly, the point $P + (Q + R)$ lies on E and aligns with Q, R , and $-(Q + R)$. By Cayley-Bacharach, since we can choose eight points on E (out of these nine intersection points) that satisfy the conditions, the ninth point must also lie on the curve.

Hence, both $(P + Q) + R$ and $P + (Q + R)$ must lie on E through the Cayley-Bacharach theorem's implication. Therefore, $(P + Q) + R$ and $P + (Q + R)$ must be the same point, proving associativity. Using Cayley-Bacharach's theorem that we have included below and applying it to the intersection properties of cubic curves, we establish that the points resulting from the associative addition on the elliptic curve E must coincide, confirming $(P + Q) + R = P + (Q + R)$.

This completes the proof of the group law on an elliptic curve.

Mordell's Theorem, Mazur's Theorem, Nagell-Lutz Theorem

The Mordell-Weil theorem states that the rational points on an elliptic curve can be built from a finite set of points using addition. The Mordell-Weil theorem provides insights into the distribution of rational points on abelian varieties, including elliptic curves, over number fields. It states that the group of K -rational points on an abelian variety A defined over a number field K is finitely generated.

Specifically, for an elliptic curve E defined over K , the group $E(K)$ of K rational points, which is known as the Mordell-Weil group, can be expressed as the direct sum of a finite torsion subgroup and a free abelian group of finite rank. In mathematical terms:

$$E(K) \cong \mathbb{Z}^r \oplus T$$

where r is the rank of the elliptic curve and T is a finite torsion subgroup.

Theorem 3 (Mordell-Weil) Let E be an elliptic curve defined over a

number field K . Then, the group of rational points $E(K)$ is finitely generated and can be expressed as the direct sum of a torsion subgroup $E(K)_{\text{tors}}$ and a free abelian group $\mathbb{Z}^r$, where r is the rank of $E(K)$.

Mazur's theorem provides a classification of the possible torsion subgroups of elliptic curves over the rationals. This theorem gives a precise list of the possible structures that the torsion subgroup can take for any elliptic curve defined over $\mathbb{Q}$.

Theorem 4 (Mazur's Theorem) *If E is an elliptic curve defined over the rational numbers $\mathbb{Q}$, then torsion subgroup $E(\mathbb{Q})_{\text{tors}}$ is isomorphic to one of the following 15 groups:*

$$\mathbb{Z}/n\mathbb{Z} \text{ or } \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2m\mathbb{Z}$$

where n and m are positive integers satisfying $1 \leq n \leq 10$ or $n = 12$, and $1 \leq m \leq 4$.

We will use Mazur's Theorem and Nagell-Lutz Theorem to determine the torsion subgroups of a certain family of elliptic curves below.

The Nagell-Lutz Theorem is a fundamental result in the theory of elliptic curves and plays a significant role in the study of rational points on these curves. It provides a way to find the integer points of finite order (torsion points) on an elliptic curve. The torsion points are points on an elliptic curve with finite order, meaning they return to identity after a finite number of self additions. The following Nagell-Lutz helps identify these points by checking if the y -coordinate divides the discriminant of the elliptic curve.

Theorem 5 (Nagell-Lutz Theorem) *If E is an elliptic curve given by the equation $y^2 = x^3 + Ax + B$, where A and B are integers, and if $P = (x, y)$ is a rational point of finite order on E , then either:*

1. $y = 0$, in which case the point $P = (x, y)$ has order two, or
2. y is an integer that divides $D = 4A^3 + 27B^2$, which immediately implies that y^2 divides D , which is the discriminant of the elliptic curve E .

It follows from the Nagell-Lutz Theorem that, if a rational point $P = (x, y)$ with $y \neq 0$ lies on an elliptic curve, either it corresponds to an integral solution of the equation defining the curve or it satisfies a special divisibility condition related to the coefficients of the curve equation.

Rational Points on Elliptic Curves

Let E be an elliptic curve defined over a field k , given by the Weierstrass equation

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

where $A, B \in k$ and the discriminant $\Delta = -16(4A^3 + 27B^2) \neq 0$. The set of rational points on E over k , denoted $E(k)$, consists of solutions $(x, y) \in k \times k$ that satisfy the Weierstrass equation. Our field k will be $\mathbb{C}$, $\mathbb{R}$, or $\mathbb{Q}$, but the formulas below hold for general field k .

Addition Formula

Given two rational points $P = (x_1, y_1)$ and $Q = (x_2, y_2)$ on E , the formula for the sum $P + Q$ is given by the following:

$$x_3 = \lambda^2 - x_1 - x_2,$$

$$y_3 = \lambda(x_1 - x_3) - y_1,$$

where $\lambda = (y_2 - y_1)/(x_2 - x_1)$ if $P \neq Q$, and $\lambda = (3x_1^2 + A)/2y_1$ if $P = Q$.

Doubling Formula

Using the above, the doubling formula for a rational point $P = (x_1, y_1)$ on E is given by:

$$x_3 = \lambda^2 - 2x_1,$$

$$y_3 = \lambda(x_1 - x_3) - y_1,$$

where $\lambda = (3x_1^2 + A)/2y_1$.

In what follows, we will apply the above formulas to analyze the groups of rational points of some examples.

Example 1 Let us consider the elliptic curve E_1 defined by the equation $Y^2Z = X^3 - 4XZ^2 + 4Z^3$. To check for nonsingularity of E_1 , we analyze the partial derivatives:

$$\partial F/\partial X = 3X^2 - 4Z^2, \partial F/\partial Y = 2YZ, \partial F/\partial Z = Y^2 + 8XZ + 12Z^2$$

Setting each partial derivative equal to zero and solving the resulting system of equations, we find the following solutions:

$$\partial F/\partial X = 0 \rightarrow 3X^2 - 4Z^2 = 0 \rightarrow X^2 = 4Z^2/3$$

$$\partial F/\partial Y = 0 \rightarrow Y = 0 \text{ or } Z = 0$$

$$\partial F/\partial Z = 0 \rightarrow Y^2 + 8XZ + 12Z^2 = 0.$$

The first equation implies that either $X = \pm 2Z/\sqrt{3}$ or $X = 0$. The second equation indicates that either $Y = 0$ or $Z = 0$. The third equation yields a quadratic equation in X , Y , and Z , which can be solved for Y^2 to obtain solutions in terms of X and Z . By further analysis, we find that the only common solutions satisfying all three equations are when $X = 0$, $Y = 0$, and $Z = 0$, which can not be on our curve because it can not be on a projective space. Thus, there are no nontrivial common solutions. Therefore, E_1 is nonsingular.

Next, we will consider the torsion rational points on elliptic curve E_1 . To compute the torsion points, we first transform the equation into its Weierstrass form: $y^2 = x^3 - 4x + 4$, and then apply the Nagell-Lutz theorem to find the torsion points. Recall that Nagell-Lutz Theorem states that if (x, y) is a rational point on an elliptic curve E given by $y^2 = x^3 + ax + b$, where $a, b \in \mathbb{Z}$, then either $y = 0$ or y^2 is a perfect square that divides D , and x and y are integers with $|x| \leq \max(1, |2b|)$.

In our case, the Weierstrass form of E_1 is $y^2 = x^3 - 4x + 4$. Here, $a = -4$ and $b = 4$. We have either $y = 0$ or y^2 divides $D = 4^2 \cdot 11$. It follows that we have one of the following possibilities for y : $y = 0, \pm 1, \pm 2, \pm 4$. If $y = 0$, then $x^3 - 4x + 4 = 0$, which has no integer solutions. If $y = \pm 1$, then $x^3 - 4x + 4 = 1$, which has solution $(x, y) = (1, \pm 1)$. If $y = \pm 2$, then $x^3 - 4x + 4 = 4$, which has three solutions $(x, y) = (0, \pm 2)$, $(x, y) = (-2, \pm 2)$, $(x, y) = (2, \pm 2)$. If $y = \pm 4$, then $x^3 - 4x + 4 = 16$, which has no integer solutions.

Thus, it follows that the torsion subgroup $E_1(\mathbb{Q})_{\text{tors}}$ is trivial, meaning it contains only the identity element. We have also provided SAGE computation verifying the triviality of the torsion subgroup $E_1(\mathbb{Q})_{\text{tors}}$ and computed its rank (**S1**).

Example 2 Let C be the following non-singular cubic curve with the form $y^2 = x^3 + ax^2 + bx + c$:

$$C: y^2 = f(x) = x^3 + 1.$$

Let us take points $P = (x_1, y_1) = (-1, 0)$ and $Q = (x_2, y_2) = (2, 3)$ on curve C . Using the formulas from (1), we have that:

$$\lambda = (y_2 - y_1)/(x_2 - x_1) = (3 - 0)/(2 - (-1)) = 1$$

$$x_3 = \lambda^2 - x_1 - x_2 = 1^2 - (-1) - 2 = 0$$

$$y_3 = \lambda(x_1 - x_3) - y_1 = 1((-1) - 0) - 0 = -1$$

$$P + Q = (x_3, y_3) = (0, -1)$$

Using point $R = (x_2, y_2) = (2, 3)$ on our previous curve C and the formula

$$\lambda = dy/dx = f'(x)/2y$$

we obtain:

$$\lambda = 3x^2/2y = 3(2)^2/2(3) = 2.$$

Using the fact that $\lambda = 2$ and the equations from (2), we have:

$$x_4 = \lambda^2 - 2x_2 = 2^2 - 2(2) = 0$$

$$y_4 = \lambda \cdot (x_2 - x_4) - y_2 = 2(2 - 0) - 3 = 1$$

To continue with point doubling with curve $C: y^2 = x^3 + 1$, we

can conclude whether $(2, 3)$ is a point of finite order. To do so, we'll use the methods of point doubling and point addition:

We left off on the point $(x_4, y_4) = (0, 1)$ in our previous example. Adding $(0, 1)$ and $(2, 3)$, we have:

$$\begin{aligned}\lambda &= (3 - 1)/(2 - 0) = 1 \\ x_5 &= \lambda^2 - 0 - 2 = -1 \\ y_5 &= 1 \cdot (0 - (-1)) - 1 = 0\end{aligned}$$

Now we have the point $(x_5, y_5) = (-1, 0)$. Once again, we repeat the process above:

$$\begin{aligned}\lambda &= (3 - 0)/(2 - (-1)) = 1 \\ x_6 &= \lambda^2 - (-1) - 2 = 0 \\ y_6 &= 1(-1 - 0) - 0 = -1\end{aligned}$$

We can also see this from our previous example of point addition above. Now, we have point $(x_6, y_6) = (0, -1)$.

$$\begin{aligned}\lambda &= (3 - (-1))/(2 - 0) = 2 \\ x_7 &= \lambda^2 - 0 - 2 = 2 \\ y_7 &= 2(0 - 2) - (-1) = -3\end{aligned}$$

Now, we have the point $(x_7, y_7) = (2, -3)$. The example concludes here because, when attempting to compute our next point, the denominator of λ will be zero. Thus, we stop calculating points here, as we've arrived at the origin point.

We have also provided SAGE computation verifying the torsion subgroup $E_1(\mathbb{Q})_{\text{tors}}$ and computed its rank (S2).

Example 3 For this example, let our curve be $C: y^2 = x^3 + 8$. Using the following discriminant formula:

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

we have that the discriminant of this curve is -1728 since $a = 0$, $b = 0$, and $c = 8$. Thus, the possibilities for the y -coordinate are:

$$\{0, \pm 1, \pm 2, \pm 3, \pm 4, \pm 6, \pm 8, \pm 12, \pm 24\}$$

Then, we can calculate the x -coordinates for each of these y -values:

$$\begin{aligned}0 &= x^3 + 8 \rightarrow x = -2 \\ 1 &= x^3 + 8 \rightarrow x = -7^{1/3} \\ 4 &= x^3 + 8 \rightarrow x = -4^{1/3} \\ 9 &= x^3 + 8 \rightarrow x = 1 \\ 16 &= x^3 + 8 \rightarrow x = 2 \\ 36 &= x^3 + 8 \rightarrow x = 28^{1/3} \\ 64 &= x^3 + 8 \rightarrow x = 56^{1/3} \\ 144 &= x^3 + 8 \rightarrow x = 136^{1/3} \\ 576 &= x^3 + 8 \rightarrow x = 568^{1/3}\end{aligned}$$

(Note that the sign of y does not alter the x -coordinates)

Note that the point $(-2, 0)$ is a torsion point, and in fact it generates the torsion subgroup of the elliptic curve $C: y^2 = x^3 + 8$.

The x -coordinates are integers when $y = 3$ and $y = 4$. Thus, our possible points are $P_1 = (1, 3)$ and $P_2 = (2, 4)$. Next, calculating $2P_1$ and $2P_2$, we compute that the x -coordinates of $2P_1$ and $2P_2$ are not integers. Thus, they are not points of finite order, meaning they are of infinite order. In fact, any of these two points generates an infinite part of the Mordell-Weil group of the elliptic curve $C: y^2 = x^3 + 8$.

We have also provided SAGE computation verifying the torsion subgroup $E_C(\mathbb{Q})_{\text{tors}} \cong \mathbb{Z}_2$ and computed its rank (S3).

Solving Ramanujan-Nagell Equation Using Elliptic Curves and SAGE Computations

In this section, we consider the Ramanujan-Nagell equation

$$y^2 + 7 = 2^n \quad (*)$$

and provide its solution using the theory of elliptic curves:

To solve this equation, let us first rewrite $(*)$ as follows to identify its solutions among the integer points of one of three elliptic curves.

We will consider the cases $n = 3k$, $n = 3k + 1$, and $n = 3k + 2$ separately.

For $n = 3k$:

$$y^2 + 7 = (2^k)^3 \rightarrow y^2 = x^3 - 7 \quad \text{Case (1)}$$

For $n = 3k + 1$:

$$y^2 + 7 = 2(2^k)^3 \rightarrow y^2 = 2x^3 - 7 \quad \text{Case (2)}$$

For $n = 3k + 2$:

$$y^2 + 7 = 4(2^k)^3 \rightarrow y^2 = 4x^3 - 7 \quad \text{Case (3)}$$

where in each case above, we set $x = 2^k$.

Recall that the set of rational solutions on these elliptic curves forms a finitely generated abelian group of finite rank. Furthermore, this group is the direct sum of the subgroups of points of finite order (the torsion subgroup) and the subgroup of points of infinite order, according to the Mordell-Weil Theorem:

$$E(\mathbb{Q}) = E_{\text{finite}} \oplus E_{\text{infinite}}.$$

Remark: While we will initially apply the Nagell-Lutz Theorem to identify potential torsion points with integer coordinates on the elliptic curves under consideration, it is crucial to emphasize the role of Mazur's Theorem in concluding the structure of the torsion subgroup. The Nagell-Lutz Theorem provides necessary conditions for a point to be torsion: namely, that the coordinates are integers and that the y -coordinate (when non-zero) divides the discriminant of the curve. This allows us to generate a finite list of candidate torsion points, such as $P = (2, 1)$ and $Q = (2, -1)$ and $2P = (32, 181)$ and $2Q = (32, -181)$ on the curve $E: y^2 = x^3 - 7$ (see below).

However, determining whether these points are indeed of finite order requires further analysis. Here, Mazur's Theorem plays a key role. It classifies all possible torsion subgroups of elliptic curves over the rational numbers $\mathbb{Q}$ and states that the torsion subgroup $E(\mathbb{Q})_{\text{tors}}$ must be isomorphic to one of the following fifteen groups: $\mathbb{Z}/n\mathbb{Z}$ for $1 \leq n \leq 10$ or $n = 12$, or $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2m\mathbb{Z}$ for $1 \leq m \leq 4$.

By computing several multiples of P using SageMath (from $2P$ up to $12P$ and $2Q$ up to $12Q$), and observing that none of these yield the identity point O or repeat earlier points, we conclude that P and Q do not lie in any of the allowable finite torsion subgroups classified by Mazur's Theorem. Thus, P and Q must be points of infinite order.

We will first find the points of finite order using the Nagell-Lutz Theorem, considering each case:

Case (1): No Torsion $\rightarrow$ No Points of Finite Order

We use the Nagell-Lutz Theorem to find finite order points on the elliptic curve $y^2 = x^3 - 7$. In fact, using the Nagell-Lutz Theorem, Mazur's Theorem, and some SageMath computations, we show the torsion subgroup of this elliptic curve is trivial. First, we check whether the curve has points of order 2:

$$x^3 - 7 = 0 \rightarrow x = 7^{1/3} \notin \mathbb{Z}$$

Since the equation above does not have an integer solution, it follows that the elliptic curve does not have a point of order 2. Next, we compute the discriminant of the elliptic curve $y^2 = x^3 - 7$ using the formula below. We then apply the Nagell-Lutz Theorem to find all torsion points of this elliptic curve.

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

where $a = 0$, $b = 0$, and $c = -7$:

$$D = 0 + 0 + 0 + 0 - 27(-7)^2 = -1323 = -3^3 \cdot 7^2.$$

It follows that the possible candidates for y are:

$$\{\pm 1, \pm 3, \pm 7, \pm 21\}$$

We then calculate the x -coordinates for these y -values:

$$\begin{aligned}1 &= x^3 - 7 \rightarrow x = 8^{1/3} \notin \mathbb{Z} \\ 9 &= x^3 - 7 \rightarrow x = 16^{1/3} \notin \mathbb{Z} \\ 49 &= x^3 - 7 \rightarrow x = 56^{1/3} \notin \mathbb{Z}\end{aligned}$$

$$441 = x^3 - 7 \rightarrow x = 448^{1/3} \notin \mathbb{Z}$$

We get integer x -coordinates when $y = \pm 1$. Thus, our possible points are $P_1 = (2, 1)$ and $P_2 = (2, -1)$. To ensure that these candidates are solutions to the original equation (*), we must check that the x -coordinate is a power of 2, which it is ($2 = 2^1$). We use SageMath commands in **S4** to check whether P_1 and P_2 are points of finite or infinite order, determine the torsion subgroup, the rank of the given elliptic curve, and the generators of the Mordell-Weil group.

Using the SageMath computation (**S4**), we see that nP_1 are all different points for any $1 \leq n \leq 12$, and we have $-P_1 = P_2$. From Mazur's Theorem, it follows that the torsion subgroup of this elliptic curve consists of only the identity element. This has also been verified by the SageMath commands (**S4**). Since there are no torsion points on the elliptic curve $y^2 = x^3 - 7$, P_1 and P_2 must be points of infinite order. Furthermore, the SageMath commands in **S4** also verify that P_1 (and P_2) are points of infinite order, and they are each generators of the Mordell-Weil group, which is isomorphic to $\mathbb{Z}$.

Since the elliptic curve in Case (1) does not have any torsion points, we can only use the points of infinite order, the generators P_1 and P_2 of the Mordell-Weil group, to potentially identify more integer solutions on this elliptic curve. Let us take points $P = P_1 = (2, 1)$ (or equally $Q = P_2 = (2, -1)$, which is the same as the point $-P$). Knowing that P and Q are of infinite order and since they both are generators of the Mordell-Weil group, we can use them to generate more solutions. Using SageMath, we compute $2P, 2Q, 3P, 3Q, 4P, 4Q, \dots, 12P, 12Q$.

We find additional solutions: $2P = (32, 181)$ and $2Q = (32, -181)$. Since nP and nQ ($|n| > 2$) involve fractions, we will show that Case (1) does not have any additional integer solutions.

Theorem 6 Let $E/\mathbb{Q}$ be the elliptic curve defined by $y^2 = x^3 - 7$, and let $P = (2, 1)$ denote a generator of the Mordell-Weil group $E(\mathbb{Q}) \cong \mathbb{Z}$. Then the integral points on E satisfy the following:

1. The complete set of integral points is $E(\mathbb{Z}) = \{O, (2, \pm 1), (32, \pm 181)\}$.
2. For all integers n with $|n| \geq 3$ the multiple nP does not have integral coordinates; that is, $nP \notin \mathbb{Z}^2$ for all $|n| \geq 3$.

Proof. (I) By Siegel's theorem, the set $E(\mathbb{Z})$ is finite. Moreover, Baker's method using linear forms in logarithms yields effective bounds for the size of integral points. In particular, Baker (1968) showed that if P generates $E(\mathbb{Q})$, then there exists an explicit constant C such that any integral point (x, y) satisfies

$$\max(|x|, |y|) < \exp(C),$$

where C depends on the canonical height of P and the minimal Weierstrass model. This result was further refined by Baker-Coates and later by Bugeaud, Mignotte, and Siksek.

For the curve $E: y^2 = x^3 - 7$, computations (using Magma or Sage) show that $C < 10^{10}$, allowing one to exhaustively search for integral points by checking nP for small values of $|n|$. Since $P = (2, 1)$ generates $E(\mathbb{Q})$, every rational point on E is of the form nP for some $n \in \mathbb{Z}$. A direct computation yields:

$$\begin{aligned} P &= (2, 1), \\ -1 \cdot P &= (2, -1), \\ 2P &= (32, 181), \\ -2P &= (32, -181). \end{aligned}$$

All other multiples nP with $|n| < 100$ yields non-integral coordinates, and by the aforementioned bound, no further integral points exist. Hence,

$$E(\mathbb{Z}) = \{O, (2, \pm 1), (32, \pm 181)\}.$$

(II) Suppose $|n| \geq 3$. We present two independent arguments.

Height argument: The canonical Néron-Tate height satisfies $\hat{h}(nP) = n^2 \hat{h}(P)$, where $\hat{h}(P) \approx 0.76009$. From Silverman's inequality (see Advanced Topics in the Arithmetic of Elliptic Curves, Thm. 1.1), we have:

$$\log|x(nP)| \geq 2\hat{h}(nP) - C_E = 2n^2 \hat{h}(P) - C_E,$$

where C_E is an explicit constant depending on E . Since $\hat{h}(P) > 0$, this lower bound grows quadratically in n , showing that $|x(nP)|$ becomes arbitrarily large as $|n|$ increases. Thus, integrality of $x(nP)$ is ruled out for large n , unless exceptional cancellation occurs.

Division polynomial argument: Let $x(nP) = \Phi_n(2)/\Psi_n^2(2)$, where Φ_n and Ψ_n are the classical division polynomials. The denominator $\Psi_n^2(2)$ is a square of an integer, and its prime factors are governed by a recurrence:

$$\Psi_{m+2}(\Psi_{m-1})^2 \equiv \Psi_{m-2}(\Psi_{m+1})^2 \pmod{p}$$

valid for any prime p . In particular, for all $|n| \geq 3$, one finds that $\Psi_n(2)$ has nontrivial prime divisors. Moreover, $\Phi_n(2)$ and $\Psi_n^2(2)$ are coprime in $\mathbb{Z}$, since their zero sets correspond to distinct algebraic loci.

Hence, the denominator of $x(nP)$ cannot cancel, so $x(nP)$ is not an integer. This can be checked explicitly by computing valuations at bad primes. Thus, $nP \notin \mathbb{Z}^2$ for all $|n| \geq 3$.

n	$\hat{h}(nP)$
1	0.76009
2	3.04036
3	6.84084
4	12.16150
5	19.00234
6	27.36338

The table above confirms the quadratic growth of $\hat{h}(nP) = n^2 \hat{h}(P)$ and supports the claim that integral points cannot occur for $|n| \geq 3$.

We next use the integer points obtained to find the solutions of the Ramanujan-Nagell equation:

For $P = (2, 1)$ and $Q = (2, -1)$, we can set $x = 2$ and $y = 1$ or $y = -1$ in Case (1)'s equation for $y^2 + 7 = (2^k)^3$ with $n = 3k$:

$$(\pm 1)^2 + 7 = (2^k)^3 \rightarrow k = 1 \rightarrow n = 3$$

Similarly, for $2P = (32, 181)$ and $2Q = (32, -181)$:

$$(\pm 181)^2 + 7 = (2^k)^3 \rightarrow k = 5 \rightarrow n = 15$$

The integer solutions to the equation $y^2 + 7 = 2^n$ in this case are:

$$(2, 1), (2, -1), (32, 181), (32, -181)$$

The points $(2, 1)$ and $(2, -1)$ correspond to $n = 3$, and the points $(32, 181)$ and $(32, -181)$ correspond to $n = 15$.

Case (2): No Torsion Points

We use the Nagell-Lutz Theorem to find finite order points on the elliptic curve $y^2 = 2x^3 - 7$. Similarly, using the Nagell-Lutz Theorem, Mazur's Theorem, and some SageMath computations, we show the torsion subgroup of this elliptic curve is also trivial. First, we check whether the curve has points of order 2:

$$2x^3 - 7 = 0 \rightarrow x = (7/2)^{1/3} \notin \mathbb{Z}.$$

Thus, there is no point of order 2. Next, we compute the discriminant of $y^2 = 2x^3 - 7$ and determine the torsion points:

$$4y^2 = 8x^3 - 28 \rightarrow (2y)^2 = (2x)^3 - 28.$$

Letting $y' = 2y$ and $x' = 2x$, we have:

$$(y')^2 = (x')^3 - 28.$$

The discriminant is:

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

where $a = 0$, $b = 0$, and $c = -28$:

$$D = -27(-28)^2 = -21168 = -2^4 \cdot 3^3 \cdot 7^2.$$

The possible candidates for y' are:

$$\{\pm 1, \pm 2, \pm 3, \pm 4, \pm 6, \pm 7, \pm 14, \pm 21, \pm 42\}$$

We calculate x -coordinates for these y -values:

$$\begin{aligned} 1 &= (x')^3 - 28 \rightarrow x' = 29^{1/3}, \\ 4 &= (x')^3 - 28 \rightarrow x' = 32^{1/3}, \\ 9 &= (x')^3 - 28 \rightarrow x' = 37^{1/3}, \\ 16 &= (x')^3 - 28 \rightarrow x' = 44^{1/3}, \\ 36 &= (x')^3 - 28 \rightarrow x' = 4, \\ 49 &= (x')^3 - 28 \rightarrow x' = 77^{1/3}, \\ 196 &= (x')^3 - 28 \rightarrow x' = 224^{1/3}, \\ 441 &= (x')^3 - 28 \rightarrow x' = 469^{1/3}, \\ 1764 &= (x')^3 - 28 \rightarrow x' = 1792^{1/3}. \end{aligned}$$

We get integer coordinates when $y' = \pm 6$. Thus, the possible points are $P_1 = (4, 6)$ and $P_2 = (4, -6)$. We must ensure that these candidates satisfy the original equation (*) with x -coordinate a power of 2, which it is ($4 = 2^2$). Again, we use SageMath commands in S5 to check whether P_1 and P_2 are points of finite or infinite order, determine the torsion subgroup, the rank of the given elliptic curve, and the generators of the Mordell-Weil group.

Using the SageMath computation (S5), we see that nP_1 are all different points for any $1 \leq n \leq 15$, and we have $-P_1 = P_2$. From Mazur's Theorem, it follows that the torsion subgroup of this elliptic curve consists of only the identity element. This has also been verified by the SageMath commands (S5). Since there are no torsion points on the elliptic curve $(y')^2 = (x')^3 - 28$, P_1 and P_2 must be points of infinite order. Furthermore, the SageMath commands in S5 also verify that P_1 (and P_2) are points of infinite order, and they are each generators of the Mordell-Weil group, which is isomorphic to $\mathbb{Z}$.

Since the elliptic curve in Case (2) does not have any torsion points, we can only use the points of infinite order, the generators P_1 and P_2 of the Mordell-Weil group, to potentially identify more integer solutions on this elliptic curve. Let us take points $P = P_1 = (4, 6)$ (or equally $Q = P_2 = (4, -6)$), which is the same as the point $-P$. Knowing that P and Q are of infinite order and since they both are generators of the Mordell-Weil group, we can use them to generate more solutions. Using SageMath, we compute $2P, 2Q, 3P, 3Q, 4P, 4Q, \dots, 12P, 12Q$.

We find additional solutions: $2P = (8, 22)$, $2Q = (8, -22)$, $3P = (37, 225)$, and $3Q = (37, -225)$. Since nP and nQ ($|n| > 3$) involve fractions, we can similarly show that Case (2) does not have any additional integer solutions. We have that the following theorem holds:

Theorem 7 Let $E/\mathbb{Q}$ be the elliptic curve defined by $y^2 = x^3 - 28$, and let $P = (4, 6)$ denote a generator of the Mordell-Weil group $E(\mathbb{Q}) \cong \mathbb{Z}$. Then the integral points on E satisfy the following:

1. The complete set of integral points is $E(\mathbb{Z}) = \{O, (4, \pm 6), (8, \pm 22), (37, \pm 225)\}$.
2. For all integers n with $|n| \geq 4$, the multiple nP does not have integral coordinates; that is, $nP \notin \mathbb{Z}^2$ for all $|n| \geq 4$.

Proof. The proof is similar to the proof of Theorem 6 above.

We verify the results:

For $P = (4, 6)$ and $Q = (4, -6)$, we can set $x' = 4$ and $y' = 6$ or $y = -6$ in Case (2)'s equation for $y^2 + 7 = 2(2^k)^3$ with $n = 3k + 1$.

Because $x' = 2x$ and $y' = 2y$, we have that $x = 2$ and $y = 3$ or $y = -3$:
 $(\pm 3)^2 + 7 = 2(2^k)^3 \rightarrow k = 1 \rightarrow n = 4$

For $2P = (8, 22)$ and $2Q = (8, -22)$, we can set $x' = 8$ and $y' = 22$ or $y = -22$.

Because $x' = 2x$ and $y' = 2y$, we have that $x = 4$ and $y = 11$ or $y = -11$:
 $(\pm 11)^2 + 7 = 2(2^k)^3 \rightarrow k = 2 \rightarrow n = 7$

For $3P = (37, 225)$ and $3Q = (37, -225)$, we can set $x' = 37$ and $y' = 225$ or $y = -225$.

Because $x' = 2x$ and $y' = 2y$, we have that $x = 18.5$ and $y = 112.5$ or $y = -112.5$.

Since y is not an integer, we cannot find a power of 2 for which the equation $y^2 + 7 = 2(2^k)^3$ is solvable. Therefore, $(37, 225)$ and $(37, -225)$ are not solutions.

The integer solutions to the equation $y^2 + 7 = 2^n$ in this case are:

$$(2, 3), (2, -3), (4, 11), (4, -11).$$

The points $(2, 3)$ and $(2, -3)$ correspond to $n = 4$, and the points $(4, 11)$ and $(4, -11)$ correspond to $n = 7$.

Case (3): No Torsion

Similarly, we use the Nagell-Lutz Theorem to find finite order points on the elliptic curve. Again, using the Nagell-Lutz Theorem, Mazur's Theorem, and some SageMath computations, we determine the torsion subgroup of this elliptic curve to be trivial. We first check if the elliptic curve $y^2 = 4x^3 - 7$ for points of order 2:

$$4x^3 - 7 = 0 \rightarrow x = (7/4)^{1/3} \notin \mathbb{Z}.$$

Thus, there is no point of order 2.

Letting $y' = 4y$ and $x' = 4x$, we have:

$$(y')^2 = (x')^3 - 112$$

We find the discriminant of $(y')^2 = (x')^3 - 112$:

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

where $a = 0$, $b = 0$, and $c = -112$:

$$D = -27(-112)^2 = -338688 = -2^8 \cdot 3^3 \cdot 7^2.$$

The possible candidates for torsion $(y')^2$ are:

$$\{1, 4, 9, 16, 36, 49, 64, 144, 196, 256, 441, 576, 784, 1764, 12544, 28224, 112896\}.$$

We can then calculate the x' -coordinates for each of these y' -values:

$$\begin{aligned} 1 &= (x') - 112 \rightarrow x' = 113^{1/3}, \\ 4 &= (x') - 112 \rightarrow x' = 116^{1/3}, \\ 9 &= (x') - 112 \rightarrow x' = 121^{1/3}, \\ 16 &= (x') - 112 \rightarrow x' = 128^{1/3}, \\ 36 &= (x') - 112 \rightarrow x' = 148^{1/3}, \\ 49 &= (x') - 112 \rightarrow x' = 161^{1/3}, \\ 64 &= (x') - 112 \rightarrow x' = 176^{1/3}, \\ 144 &= (x') - 112 \rightarrow x' = 256^{1/3}, \\ 196 &= (x') - 112 \rightarrow x' = 308^{1/3}, \\ 256 &= (x') - 112 \rightarrow x' = 368^{1/3}, \\ 441 &= (x') - 112 \rightarrow x' = 553^{1/3}, \\ 576 &= (x') - 112 \rightarrow x' = 688^{1/3}, \\ 784 &= (x') - 112 \rightarrow x' = 4314^{1/3}, \\ 1764 &= (x') - 112 \rightarrow x' = 1876^{1/3}, \\ 7056 &= (x') - 112 \rightarrow x' = 8167^{1/3}, \\ 12544 &= (x') - 112 \rightarrow x' = 12656^{1/3}, \\ 28224 &= (x') - 112 \rightarrow x' = 28336^{1/3}, \\ 112896 &= (x') - 112 \rightarrow x' = 113008^{1/3}, \end{aligned}$$

We get integer coordinates when $y' = \pm 20$. Thus, the possible points are $P_1 = (8, 20)$ and $P_2 = (8, -20)$. We must ensure these points satisfy the original equation (*) with x -coordinate a power of 2. Again, we use SageMath commands in S6 to check whether P_1 and P_2 are points of finite or infinite order, determine the torsion subgroup, the rank of the given elliptic curve, and the generators of the Mordell-Weil group.

Using the SageMath computation (S6), we see that nP_1 are all different points for any $1 \leq n \leq 15$, and we have $-P_1 = P_2$. From Mazur's Theorem, it follows that the torsion subgroup of this elliptic curve consists of only the identity element. This has also been verified by the SageMath commands (S6). Since there are no torsion points on the

elliptic curve $(y')^2 = (x')^3 - 112$, P_1 and P_2 must be points of infinite order. Furthermore, the SageMath commands above also verify that P_1 (and P_2) are points of infinite order, and they are each generators of the Mordell-Weil group, which is isomorphic to $\mathbb{Z}$.

Since the elliptic curve in Case (3) does not have any torsion points, we can only use the points of infinite order, the generators P_1 and P_2 of the Mordell-Weil group, to potentially identify more integer solutions on this elliptic curve. Let us take points $P = P_1 = (8, 20)$ (or equally $Q = P_2 = (8, -20)$, which is the same as the point $-P$). Knowing that P and Q are of infinite order and since they both are generators of the Mordell-Weil group, we can use them to generate more solutions. Using SageMath, we compute $2P, 2Q, 3P, 3Q, 4P, 4Q, \dots, 12P, 12Q$.

Since nP and nQ ($|n| > 1$) involve fractions, we have that Case (3) does not have any additional integer solutions.

Theorem 8 Let $E/\mathbb{Q}$ be the elliptic curve defined by $y^2 = x^3 - 112$, and let $P = (8, 20)$ denote a generator of the Mordell-Weil group $E(\mathbb{Q}) \cong \mathbb{Z}$. Then the integral points on E satisfy the following:

1. The complete set of integral points is $E(\mathbb{Z}) = \{O, (8, \pm 20)\}$.
2. For all integers n with $|n| \geq 2$, the multiple nP does not have integral coordinates; that is, $nP \notin \mathbb{Z}^2$ for all $|n| \geq 2$.

Proof. The proof is similar to the proof of Theorem 6 above.

We verify the results:

For $P = (8, 20)$ and $Q = (8, -20)$, we can set $x' = 8$ and $y' = 20$ or $y = -6$ in Case (3)'s equation for $y^2 + 7 = 4(2^k)^3$ with $n = 3k + 2$.

Since $x' = 4x$ and $y' = 4y$ for Case 3, we have $x = 2$ and $y = 5$ or $y = -5$:

$$(\pm 5)^2 + 7 = 4(2^k)^3 \rightarrow k = 1 \rightarrow n = 5$$

The integer solutions to the equation $y^2 + 7 = 2^n$ in this case are: $(2, 5), (2, -5)$

The points $(2, 5)$ and $(2, -5)$ correspond to $n = 5$.

Conclusion

In this study, we have explored the Ramanujan-Nagell equation $y^2 + 7 = 2^n$ using the theory of elliptic curves and SageMath computations. We analyzed three distinct cases by converting the equation into elliptic curves of the forms $y^2 = x^3 - 7$, $y^2 = 2x^3 - 7$, and $y^2 = 4x^3 - 7$.

For each case, we employed the Nagell-Lutz Theorem to investigate possible torsion points, confirming that none of the elliptic curves have torsion points of order 2. By analyzing the torsion subgroups and computing solutions of infinite order using SageMath, we identified all possible integer solutions to the equation.

The comprehensive results are summarized as follows:

1. For the elliptic curve $y^2 = x^3 - 7$:
 - Solutions include $(2, 1)$ and $(2, -1)$ and $(32, 181)$ and $(32, -181)$, corresponding to the $n = 3$ and $n = 15$ cases, respectively, of the Ramanujan-Nagell equation.
2. For the elliptic curve $y^2 = 2x^3 - 7$:
 - Solutions include $(4, 6)$ and $(4, -6)$ and $(8, 22)$ and $(8, -22)$, corresponding to the $n = 4$ and $n = 7$ cases, respectively, of the Ramanujan-Nagell equation.
3. For the elliptic curve $y^2 = 4x^3 - 7$:
 - Solutions include $(8, 20)$ and $(8, -20)$ corresponding to the $n = 5$ case of the Ramanujan-Nagell equation.

Combining results from all three cases, all the integer solutions to the equation $y^2 + 7 = 2^n$ are:

$$(2, 1), (2, -1), (2, 3), (2, -3), (2, 5), (2, -5), (4, 11), (4, -11), (32, 181), (32, -181),$$

where $(2, 1)$ and $(2, -1)$ correspond to $n = 3$, $(2, 3)$ and $(2, -3)$ correspond to $n = 4$, $(2, 5)$ and $(2, -5)$ correspond to $n = 5$, $(4, 11)$ and $(4, -11)$ correspond to $n = 7$, and $(32, 181)$ and $(32, -181)$ correspond to $n = 15$. The integer solutions to $y^2 + 7 = 2^n$ are:

x	y	n
2	± 1	3
2	± 3	4
2	± 5	5
4	± 11	7
32	± 181	15

Our results confirm all the solutions and demonstrate the effectiveness of combining theory and computation.

Appendix

Supplementary materials are available online at thurj.org.

References

- Anthony W. Knapp, Elliptic Curves, *Mathematical Surveys and Monographs*, 2005, Volume 40.
- Cassels, J. W. S. (1991). Lectures on elliptic curves. *London Mathematical Society Student Texts*, vol. 24. Cambridge University Press, Cambridge. George Green Library, QA565 CAS.
- D. Zagier, Large Integral Points on Elliptic Curves, *Mathematics of Computation*, Volume 48, Number 177, January 1987, Pages 425–436.
- Ebbinghaus, H.-D., Hermes, H., Hirzebruch, F., Koecher, M., Mainzer, K., Neukirch, J., Prestel, A., and Remmert, R. (1991). Numbers. *Graduate Texts in Mathematics*, vol. 123. Springer-Verlag.
- Eisenbud, D., Green, M., and Harris, J. (1996). Cayley-Bacharach theorems and conjectures. *Bulletin of the American Mathematical Society*, 33(3), 295–324.
- Ireland, K., and Rosen, M. (1990). A classical introduction to modern number theory. Second ed. *Graduate Texts in Mathematics*, vol. 84. Springer Verlag, New York.
- Lemmeryer, F. (2018). Elliptic curves, historical remarks. Available at <http://www.fen.bilkent.edu.tr/~franz/ta/ta01.pdf>, last visited Sep 2018.
- Lynn, B. (n.d.-a). Elliptic curves - the weierstrass form. <https://crypto.stanford.edu/pbc/notes/elliptic/weier.html>
- Mead, D. G. (1973). The Equation of Ramanujan-Nagell and [y2]. *Proceedings of the American Mathematical Society*, 41(2), 333–341. <https://doi.org/10.2307/2039090>
- P. Ingram, Multiples of Integral Points on Elliptic Curves, *Journal of Number Theory*, Volume 129, Issue 1, January 2009, Pages 182–208.
- SageMath documentation: https://doc.sagemath.org/html/en/reference/arithmetic_curves/sage/schemes/elliptic_curves/ell_point.html
- SageMath documentation: https://doc.sagemath.org/html/en/reference/arithmetic_curves/sage/schemes/elliptic_curves/ell_torsion.html
- Serge Lang, Elliptic Curves, Springer, 2012, *Graduate Texts in Mathematics*, Volume 231.
- Silverman, J. H., and Tate, J. T. (2015). Rational points on elliptic curves. Second ed. *Undergraduate Texts in Mathematics*. Springer, Cham. George Green Library, QA565 SIL.
- Silverman, J. H. (1994). *Advanced topics in the arithmetic of elliptic curves* (Vol. 151). Springer.
- Silverman, J. H. (1999). Computing rational points on rank 1 elliptic curves via L-series and canonical heights. *Mathematics of Computation*, 68(226), 835–858.
- Silverman, J. H. (2009). *The arithmetic of elliptic curves* (2nd ed., Vol. 106). Springer.
- Sutherland, A. (2021, February 17). 18.783 S2021 Lecture 1: Introduction to elliptic curves: Elliptic curves: Mathematics. MIT OpenCourseWare. https://ocw.mit.edu/courses/18-783-elliptic-curves-spring-2021/resources/mit18_783s21_slides1/
- Washington, L. C. (2008). Elliptic curves. Second ed. *Discrete Mathematics and its Applications* (Boca Raton). Chapman Hall/CRC, Boca Raton, FL. George Green Library, QA565 WAS and QA567.2.E44 WAS.
- Wiles, A. (1995). Modular Elliptic Curves and Fermat's Last Theorem. *Annals of Mathematics*, 141(3), 443–551. <https://doi.org/10.2307/2118559>