The j-invariant

Jules Gardner

March 2026

Abstract

After a quick review of elliptic curves, we define the j-invariant. The j-invariant is a function of an elliptic curve $y^2 = x^3 + ax^2 + bx + c$, defined as $j(E) = 1728\dfrac{4A^3}{4A^3 + 27B^2}$. The values of A and B are the coefficients of the short Weierstraß form $y^2 = x^3 + Ax + B$, obtained from variable substitutions that preserve rational coordinates. We will look at the group law, which gives a group structure on any elliptic curve. This helps give a motivation for the j-invariant. After we make note of a few small results, review some group theory, and take a look at an important topic regarding the j-invariant, we'll look at the connection between the j-invariant and the number $e^{\pi\sqrt{167}}$, allowing us to use a Laurent series to prove that $e^{\pi\sqrt{167}}$ is close to an integer.

1 Introduction

We begin by defining elliptic curves, the basic preliminaries for the j-function's definition.

Definition 1. *An elliptic curve is a plane curve $y^2 = x^3 + ax^2 + bx + c$, potentially in a field other than $\mathbb{R}$.*

An elliptic curve does not have to be over $\mathbb{R}$. For example, there is an elliptic curve $y^2 = x^3 + (2,3)\,x^2 + (4,1)\,x + (4,2)$ in $\mathbb{F}_7 \times \mathbb{F}_5$, where $\mathbb{F}_5$ is the finite field of integers modulo 5. Now for two simple observations regarding the geometry of an elliptic curve over $\mathbb{R}$.

Proposition 1. *Elliptic curves are symmetrical over the x-axis, and intersect the y-axis at $y = \pm\sqrt{c}$.*

The first of the two can be extended to other fields: Negating y does not change whether $(x, y) \in E$.

Definition 2. *When certain substitutions, which preserve rationality, are applied, the curve can be transformed into short Weierstraß form $y^2 = x^3 + Ax + B$.*

Different elliptic curves can have the same short Weierstraß form. This is important later, for the justification of the j-function's name.

Definition 3. *If we take an elliptic curve E with short Weierstraß form $y^2 = x^3 + Ax + B$, we define $j(E) = 1728\dfrac{4A^3}{4A^3 + 27B^2}$.*

Proposition 2. *One might note that the j-function effectively acts only on certain "equivalence classes" of elliptic curves; specifically, j depends only on the short Weierstraß form.*

This is, of course, true, but a stronger version also applies.

2 The Group Law

Suppose we have an elliptic curve over $\mathbb{Q}$. We can define a group structure on $E \cup \{\mathcal{O}\}$, where $\mathcal{O}$ is a special element called the "point at infinity." We call this the "Group Law."

Definition 4. *Given an elliptic curve over $\mathbb{Q}$, there is a group structure on $E \cup \{\mathcal{O}\}$.*

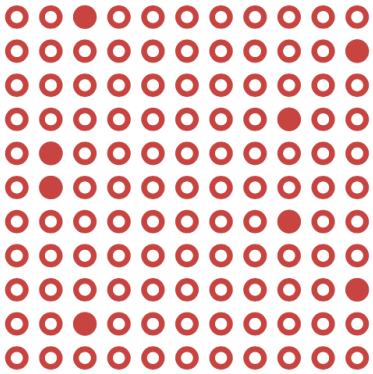

Figure 1: The curve $y^2 = x^3 + 3x^2 + 4x + 6$ over F_{11}, depicted visually[1].

1. *Take points $P, Q \in E$. If $P \neq Q$, and if the line through P and Q intersects E at some other point R, then $P + Q$ is the reflection of R across the x-axis.*
2. *If the tangent line to E at P intersects E at some other point R, then $P + P$ is the reflection of R across the x-axis.*
3. *Otherwise, $P + Q = \mathcal{O}$.*
4. *The identity is $\mathcal{O}$.*

The Group Law can be extended to other fields, though it is most commonly used on curves over $\mathbb{Q}$. It gives us group structures on a range of subsets of K^2 for any field K. However, many are isomorphic, as we will soon see.

Proposition 3. *Negation is reflection across the x-axis.*

Proof. If we reflect P across the x-axis to get P', and then add the two, we find that the line through them is a vertical line that cannot intersect E at any other point. So $P + P' = \mathcal{O}$ and thus $-P = P'$. □

Since elliptic curves in $\mathbb{R}$ have a wide variety of shapes, we can get a range of new group structures on subsets of $\mathbb{R}^2 \cup \mathcal{O}$. One for each equivalence class of elliptic curves. These equivalence classes are based on what we call an isogeny.

3 Isogeny

Since elliptic curves in $\mathbb{R}$ have a wide variety of shapes, we can get a range of new group structures on subsets of $\mathbb{R}^2 \cup \mathcal{O}$. One for each equivalence class of elliptic curves. These equivalence classes are based on what we call an isogeny.

Definition 5. *An isogeny is a group homomorphism between two elliptic curves over $\mathbb{Q}$.*

[1] This image was made using `https://www.desmos.com/calculator/qljdq8y9ru`. The reflective symmetry is due to the fact that elliptic curves are symmetrical over the y-axis. Reflecting a point over the line $y = \frac{p}{2}$ negates the y-coordinate, and so this is the equivalent of vertical symmetry.

It is somewhat interesting that we use a homomorphism instead of an isomorphism. However, this version allows some stronger proofs, and when needed we have an equivalence relation that does use isomorphisms.

Definition 6. *We say $E \cong E'$ if there is an invertible isogeny between the two.*

If E and E' are elliptic curves over $\mathbb{Q}$, then saying $E \cong E'$ is the same as saying the group structures on E and E' are isomorphic.

Theorem 1. *If E and E' are elliptic curves over $\mathbb{Q}$, then $j(E) = j(E')$ if and only if $E \cong E'$.*

This theorem is the reason why $j(E)$ is called the "j-invariant;" it is what we call an isogeny invariant. Thus, we also know that, if two elliptic curves have the same short Weierstraß form, they have the same j-invariant and are thus equivalent. If two curves are equivalent under this relation, we call them "isogenous".

4 Modular functions and forms

This section begins with two closely-related terms: Holomorphic and meromorphic. These are both types of complex functions. Meromorphic functions are like holomorphic ones, but they have discrete points, called "poles," that act as exceptions.

Definition 7. *A holomorphic function f is a complex function such that, for each $z \in \mathbb{C}$, f has a complex derivative in some open region containing z.*

Definition 8. *A meromorphic function f is a complex function such that there is some set $S \subseteq$ of discrete complex numbers (these are called poles), such that for each $z \in \mathbb{C} \setminus S$, f has a complex derivative in some open region containing z.*

We now will make use of a rather simple definition:

Definition 9. *The upper half plane is $\mathbb{H} = \left\{x \in \mathbb{C} \middle| \operatorname{im}(x) > \mathbb{C}\right\}$*

This name makes intuitive sense: $\mathbb{H}$ is just the upper half of the typical complex plane.

Definition 10. *We define $SL_2(\mathbb{Z}) = \left\{\begin{bmatrix} a & b \\ c & d \end{bmatrix} \middle| ad - bc = 1 \ \& \ a, b, c, d \in \mathbb{Z}\right\}$.*

This simply means the set of all 2×2 matrices with determinant 1. These can also be represented as ideals of $\mathbb{Z}[i]$ with norm 1, linear transformations that do not affect areas, or lattices with fundamental parallelograms of area 1. A function f is weakly modular of weight $2k$ if it is meromorphic on $\mathbb{H}$ and has $f(z) = (cz - d)^{-2k} f\left(\frac{az + b}{cz + d}\right)$ for all $\begin{bmatrix} a & b \\ c & d \end{bmatrix} \in SL_2(\mathbb{Z})$. If f is meromorphic at infinity it is a modular function, and if it is holomorphic, including at infinity, it is a modular form.

Definition 11. *For $k \geq 1$, we define the Eisenstein series of weight $2k$ by $G_{2k}(\tau) = \sum_{(m,n) \neq (0,0)} \frac{1}{(m + n\tau)^{2k}}$.*

Theorem 2. *The Eisenstein series is a modular form of weight $2k$.*

This all paves the way for the following:

Given an elliptic curve E with short Weierstraß form $y^2 = x^3 + Ax + B$, we have two important numbers: $\Delta(E)$ and $j(E)$. The j-invariant has already been discussed. Δ, on the other hand, is new, and equal to $-16\left(4A^3 + 27B^2\right)$. We have $j(E) = -1728\frac{64A^3}{\Delta}$.

We write $g_2 = 60G_4(\tau)$ and $g_3 = 140G_6(\tau)$, then consider the elliptic curve $y^2 = 4x^3 - g_2 x - g_3$. Now the short Weierstraß form is $y^2 = x^3 - \frac{1}{4}g_2 x - \frac{1}{4}g_3$, giving $\Delta(\tau) = g_2^3 - 27g_3^2$ and $j(\tau) = 1728\frac{g_2^3}{g_2^3 - 27g_3^2}$.

Because sums and products of holomorphic functions are holomorphic, Δ is a modular form of weight 12. Since g_2^3 is also weight 12, we know j is a modular function of weight 0.

But there is more to the j-invariant. A new bit of motivation will be discussed promptly, explaining the factor of 1728 and paving the way for the connection to the Monster Group.

5 Lattices

Let Λ be any lattice. Define $G_{2k}(\Lambda) = \sum_{\omega\in\Lambda\setminus 0} \frac{1}{\omega^{2k}}$. Now we take E_Λ, using the method outlined in the previous section.

Theorem 3. *Given a lattice $\Lambda \subset \mathbb{C}$, we have $\mathbb{C}/\Lambda \cong E_\Lambda(\mathbb{C})$ as groups. Given an elliptic curve E, there is a lattice Λ_E such that $\mathbb{C}/\Lambda_E \cong E(\mathbb{C})$.*

This combines with a simple observation to help justify the term j-invariant:

Theorem 4. *E_Λ and $E_{\Lambda'}$ are isomorphic if and only if Λ and Λ' are homothetic.*

Now, let $j(\Lambda) = j(E_\Lambda)$. So $j(\Lambda) = j(\Lambda')$ if and only if Λ and Λ' are homothetic, making j a homothety invariant.

This is the final form of the j-invariant that will be discussed here.

6 Monstrous Moonshine

Consider this number.

$$8080,17424,79451,28758,86459,90496,17107,57005,75436,80000,00000$$

That number is the order, or cardinality, of the Monster group. The group was conjectured to have a representation of order 196883. Let $q = e^{2\pi i\tau}$. Now, $j(\tau)$ can be written as a power series in terms of q. We have $\tau = \frac{\ln(q)}{2\pi i}$. Now, $j(q)$ is meromorphic with a pole at $q = 0$. Because of this we can get a Laurent series by simply multiplying by a power of q, in this case simply q itself, taking the Taylor series, and dividing by q. In the end, we get the following:

$$j(\tau) = \frac{1}{q} + 744 + 196884q + 21493760q^2 + \dots$$

. This power series contains the term $196884q$. Note that $196883 + 1 = 196884$. When numbers this big are involved, coincidences are unlikely, so the mathematical community decided tosearch for a reason why.

Definition 12. *A simple group is a nontrivial group whose only normal subsets are trivial .*

The Monster group $\mathbb{M}$ is the largest finite simple group. Simple groups can be composed using semi-direct products to make all other finite groups.

Definition 13. *The automorphism group of some mathematical object (this can a group, a field, a vector field, a polytope, or anything else with a notion of "isomorphism") is the set of automorphisms under the composition operation: Given automorphisms f and g, we let $f \oplus g b$ be $f \circ g$, which is another automorphism.*

There is a vertex operator algebra $V^\natural$ called the Moonshine Module, which connects the two. Its automorphism group is the Monster group, and its graded dimension is the j-invariant. However, the phenomenon is not fully understood.

7 Algebraic Numbers and $e^{\pi\sqrt{163}}$

Definition 14. *An algebraic integer is a complex root of a monic (i.e. having leading coefficient 1) polynomial with integer coefficients, such as $x^3 - x^2 + 2x + 7$.*

Definition 15. *An elliptic curve E is said to have complex multiplication if $\mathbb{Z} \subsetneq \mathrm{End}(E)$. An elliptic curve E is said to have complex multiplication by a ring R if $R \cong \mathrm{End}(E)$.*

This concept allows us to define a special complex monic polynomial corresponding to each complex quadratic field.

Definition 16. *The Hilbert class polynomial of* $\mathbb{Q}\left(\sqrt{-d}\right)$ *is defined as* $\prod_{\mathfrak{a}\in \mathrm{Cl}\left(\mathbb{Q}\left(\sqrt{-d}\right)\right)} \left(x - j\left(\tau_{\mathfrak{a}}\right)\right)$*, where* $\tau_{\mathfrak{a}}$ *is a complex number in the upper half plane, corresponding to each equivalence class of ideals. The roots are the* j*-invariants of elliptic curves with complex multiplication by* $\mathbb{Q}\left(\sqrt{-d}\right)$.

Since this is a monic polynomial, and the roots are the j-invariants of complex curves, it makes sense that this lets us connect the j-invariant to algebraic integers.

It turns out $j(E)$ is an algebraic integer when E has complex multiplication, and $j(\tau)$ is an algebraic integer when τ is a quadratic imaginary number.

This result has many consequences, including one that at first glance doesn't seem like the sort of thing mathematics can talk about, let alone prove. However, it turns out that it can, using the j-function's Laurent series.

We wish to prove that $e^{\pi\sqrt{163}}$ is very close to an integer. Take $\tau = \dfrac{1+\sqrt{163}}{2}$. Now we have $q = e^{i\pi+\pi\sqrt{163}} = \dfrac{1}{e^{\pi\sqrt{163}}}$. Note that q is a rather small number. So

$$j(\tau) = \frac{1}{q} + 744 + 196884q + 21493760q^2 + \cdots =$$

$$e^{\pi\sqrt{163}} + 744 + 196884q + 21493760q^2 + \cdots \approx$$

$$e^{\pi\sqrt{163}} + 744$$

. Now, the class number of $\mathbb{Q}\left(\sqrt{-163}\right)$ is 1. And the Hilbert class polynomial thus has degree 1. So $j(\tau)$ is an integer, implying $e^{\pi\sqrt{163}}$ is almost an integer.

8 Conclusion

The j-invariant, or j-function, takes many forms while retaining the same underlying structure. At its core it is a function of elliptic curves, and yet it can also be a function of complex numbers, and even of complex lattices. As a complex function, it is a modular function. The name "j-invariant" comes from the operations, including isogenies and homotheties that can be performed on the input to leave the output unchanged. All these forms are different, yet they are all closely related and generally treated as the same function: j. The j-function is an interesting function with many applications in a wide range of fields.

References

[1] Dylan Pentland *The j-invariant of an Elliptic Curve.*

[2] Raiann Rahman *Elliptic Curves, the Group Law, and the J Invariant*

[3] John Horton Conway and Simon Phillips Norton *Monstrous Moonshine*

[4] Terry Gannon *Monstrous Moonshine: The first twenty-five years*