The Modular j-Function

Hariharan Senthilkumar

March 27, 2026

Abstract

The modular j-function is a single holomorphic function on the upper half-plane that acts as a "coordinate" for complex elliptic curves: two complex elliptic curves are isomorphic if and only if they determine the same j-value. In this paper we build the j-function from the Eisenstein series and the modular discriminant, explain why it is invariant under the modular group, and describe how its q-expansion turns the theory into something one can compute with.

1 Lattices and the analytic model of elliptic curves

In the simplest sense, an elliptic curve over $\mathbb{C}$ can be viewed as a two-dimensional grid in the complex plane. The grid itself is a lattice, and the elliptic curve is what you get when you identify points that differ by a lattice vector. The point of this perspective is that it turns an algebraic curve into a geometric quotient, and it is exactly this quotient construction that the j-function eventually measures.

1.1 Lattices as "periodic directions"

A lattice in $\mathbb{C}$ is built from two complex numbers that point in "independent" directions.

Definition 1.1. A lattice is a subgroup $\Lambda \subset \mathbb{C}$ of the form

$$\Lambda = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2$$

where $\omega_1, \omega_2 \in \mathbb{C}$ are $\mathbb{R}$-linearly independent (equivalently, $\omega_1/\omega_2 \notin \mathbb{R}$).

The quotient space $\mathbb{C}/\Lambda$ is a torus: moving by a lattice element does not change the class of a point. This is the analytic shadow of an elliptic curve.

Definition 1.2. A complex elliptic curve is a Riemann surface that is analytically isomorphic to $\mathbb{C}/\Lambda$ for some lattice $\Lambda \subset \mathbb{C}$.

Remark 1.1. The same underlying torus can be presented by many different lattices. For instance, multiplying a lattice by any nonzero complex number c rescales the picture without changing the quotient as a complex manifold: $\mathbb{C}/\Lambda \cong \mathbb{C}/(c\Lambda)$ via $z \mapsto cz$.

1.2 Normalizing a lattice by a point in the upper half-plane

Because lattices are only meaningful up to rescaling, it is convenient to encode a lattice by a single complex parameter.

Definition 1.3. The upper half-plane is

$$\mathbb{H} = \{\tau \in \mathbb{C} : \mathrm{Im}(\tau) > 0\}.$$

For $\tau \in \mathbb{H}$ we write

$$\Lambda_\tau = \mathbb{Z}\tau + \mathbb{Z}.$$

Every lattice is homothetic to some Λ_τ with $\tau \in \mathbb{H}$ (choose an oriented basis and divide by one basis vector). So points of $\mathbb{H}$ parametrize lattices up to scaling, but there is still redundancy: different τ may lead to the same lattice up to an integral change of basis.

Example 1.1. Let $\tau = 2i$ and let

$$\tau' = \frac{\tau}{2\tau + 1} = \frac{2i}{4i + 1}.$$

Both τ and τ' lie in $\mathbb{H}$. Consider the integer matrix

$$\gamma = \begin{pmatrix} 1 & 0 \\ 2 & 1 \end{pmatrix}.$$

If we apply γ to τ' by the rule $\gamma \cdot \tau' = \dfrac{1 \cdot \tau' + 0}{2 \cdot \tau' + 1}$, we get $\gamma \cdot \tau' = \tau$. The reason this forces Λ_τ and $\Lambda_{\tau'}$ to be homothetic is that the same computation produces an *explicit scaling factor* relating the two lattices.

Indeed, the equation $\tau = \dfrac{\tau'}{2\tau' + 1}$ can be rewritten as

$$(2\tau' + 1)\tau = \tau'.$$

Now multiply the generators of $\Lambda_\tau = \mathbb{Z}\tau + \mathbb{Z}$ by the nonzero complex number $(2\tau' + 1)$:

$$(2\tau' + 1)\Lambda_\tau = \mathbb{Z}\big((2\tau' + 1)\tau\big) + \mathbb{Z}(2\tau' + 1) = \mathbb{Z}\tau' + \mathbb{Z}(2\tau' + 1).$$

But $\mathbb{Z}\tau' + \mathbb{Z}(2\tau' + 1)$ is the same as $\mathbb{Z}\tau' + \mathbb{Z}$, because $1 = (2\tau' + 1) - 2\tau'$ lies in the lattice generated by τ' and $(2\tau' + 1)$. Therefore

$$(2\tau' + 1)\Lambda_\tau = \mathbb{Z}\tau' + \mathbb{Z} = \Lambda_{\tau'}.$$

Equivalently,

$$\Lambda_\tau = \frac{1}{2\tau' + 1}\,\Lambda_{\tau'}.$$

That is exactly what "homothetic" means: one lattice is obtained from the other by multiplying by a nonzero complex scalar.

2 The modular group as a change of coordinates

The redundancy in the parameter τ is not a defect; it is a feature. It tells us that the moduli space of lattices (and hence of complex elliptic curves) is not $\mathbb{H}$ itself, but rather a quotient of $\mathbb{H}$ by a group of coordinate changes.

2.1 Fractional linear transformations

Definition 2.1. The modular group is the quotient

$$\Gamma(1) = \mathrm{SL}_2(\mathbb{Z})/\{\pm I\}.$$

An element represented by $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ acts on $\mathbb{H}$ by

$$\gamma \cdot \tau = \frac{a\tau + b}{c\tau + d}.$$

This action is exactly what happens to $\tau = \omega_1/\omega_2$ when we replace a lattice basis (ω_1, ω_2) by another oriented $\mathbb{Z}$-basis.

Remark 2.1. Two especially important transformations are

$$S(\tau) = -\frac{1}{\tau} \qquad \text{and} \qquad T(\tau) = \tau + 1,$$

corresponding to the matrices

$$\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$$

and

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}.$$

They generate $\Gamma(1)$.

2.2 A fundamental region and the two "special" points

A fundamental region gives one representative for almost every orbit.

Definition 2.2. A standard fundamental domain for the $\Gamma(1)$-action is

$$\mathscr{F} = \left\{ \tau \in \mathbb{H} : \ |\tau| \geq 1, \ -\tfrac{1}{2} \leq \mathrm{Re}(\tau) \leq \tfrac{1}{2} \right\}.$$

Points on the boundary can have nontrivial stabilizers (they correspond to lattices with extra symmetry). There are two such points inside $\mathscr{F}$ that matter for j:

$$i \quad \text{and} \quad \rho = e^{2\pi i/3} = \frac{-1 + \sqrt{-3}}{2}.$$

They represent the square lattice and the hexagonal lattice.

Example 2.1. If $\tau = i$, then $\Lambda_\tau = \mathbb{Z}i + \mathbb{Z}$ is preserved by multiplication by i. This gives $\mathbb{C}/\Lambda_i$ an automorphism of order 4 (rotation by 90° on the torus), which is larger than the generic automorphism group.

3 Modular forms that feed into j

To define j we need modular forms of weights 4, 6, and 12. The relationship among these weights is not accidental: it is what allows a weight-0 quotient, and weight 0 is precisely what one needs for an honest function on the quotient $\Gamma(1)\backslash\mathbb{H}$.

3.1 What "weight" means

Definition 3.1. Let $k \in \mathbb{Z}$. A *modular form of weight* k for $\Gamma(1)$ is a holomorphic function $f : \mathbb{H} \to \mathbb{C}$ satisfying

$$f(\gamma \cdot \tau) = (c\tau + d)^k f(\tau) \quad \text{for all} \quad \gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}),$$

together with a holomorphy condition at the cusp $\tau = i\infty$.

A modular form of weight 0 is simply a $\Gamma(1)$-invariant holomorphic function on $\mathbb{H}$ with controlled growth as $\mathrm{Im}(\tau) \to \infty$; such objects are called modular functions.

3.2 Eisenstein series and lattice invariants

The simplest modular forms are the Eisenstein series, which can be written as sums over lattice points.

Definition 3.2. For an integer $k \geq 2$, the (unnormalized) Eisenstein series of weight $2k$ is

$$G_{2k}(\tau) = \sum_{(m,n) \in \mathbb{Z}^2 \setminus \{(0,0)\}} \frac{1}{(m\tau + n)^{2k}}.$$

These series converge absolutely for $k \geq 2$, and the invariance under $\Gamma(1)$ is ultimately a repackaging of the fact that $\mathbb{Z}^2$ is stable under $\mathrm{SL}_2(\mathbb{Z})$.

The invariants that appear in elliptic curve theory are scalar multiples of G_4 and G_6.

Definition 3.3. Define

$$g_2(\tau) = 60\, G_4(\tau) \qquad \text{and} \qquad g_3(\tau) = 140\, G_6(\tau).$$

These normalizations are chosen so that g_2 and g_3 match the classical coefficients in the Weierstrass model coming from the $\wp$-function attached to Λ_τ.

3.3 The discriminant

The discriminant is the quantity that detects whether a cubic has a repeated root, and the same expression controls singularities for elliptic curves written in Weierstrass form.

Definition 3.4. The modular discriminant is the weight-12 modular form

$$\Delta(\tau) = g_2(\tau)^3 - 27 g_3(\tau)^2.$$

Remark 3.1. If one writes an elliptic curve as $y^2 = 4x^3 - g_2 x - g_3$, then the curve is nonsingular exactly when $g_2^3 - 27g_3^2 \neq 0$. So $\Delta(\tau) \neq 0$ is the analytic statement that the associated Weierstrass model really is an elliptic curve.

4 Definition and basic structure of the j-function

We are now ready to define the main character.

4.1 The definition

Definition 4.1. The modular j-function is the weight-0 quotient

$$j(\tau) = 1728\,\frac{g_2(\tau)^3}{\Delta(\tau)}.$$

Because g_2^3 and Δ both have weight 12, the factor $(c\tau + d)^{12}$ cancels in the transformation law, so $j(\gamma \cdot \tau) = j(\tau)$ for every $\gamma \in \Gamma(1)$.

4.2 Why j classifies complex elliptic curves

The slogan is that τ describes a lattice and $j(\tau)$ describes the corresponding elliptic curve. More precisely, if we write $E_\tau = \mathbb{C}/\Lambda_\tau$, then the map $\tau \mapsto j(\tau)$ is constant on $\Gamma(1)$-orbits, so it makes sense on the quotient $\Gamma(1)\backslash\mathbb{H}$.

Theorem 4.1. *If $\tau_1, \tau_2 \in \mathbb{H}$, then the elliptic curves E_{τ_1} and E_{τ_2} are isomorphic over $\mathbb{C}$ if and only if $j(\tau_1) = j(\tau_2)$.*

Remark 4.1. A concrete algebraic reformulation is the following. Suppose an elliptic curve is written in short Weierstrass form

$$E : y^2 = x^3 + Ax + B \quad (4A^3 + 27B^2 \neq 0).$$

Then the classical formula

$$j(E) = 1728\,\frac{4A^3}{4A^3 + 27B^2}$$

produces the same invariant as the analytic $j(\tau)$ attached to any period lattice of E.

4.3 Scaling and why j ignores coordinate choices

The j-invariant is designed to be insensitive to the particular Weierstrass equation we choose for an elliptic curve. The reason is that changing coordinates rescales A and B in a predictable way, and the quotient defining j is built to cancel that rescaling.

Lemma 4.1. *Let E be given by $y^2 = x^3 + Ax + B$ with $4A^3 + 27B^2 \neq 0$, and let $u \in \mathbb{C}^\times$. Under the change of variables*

$$x = u^2 x', \qquad y = u^3 y',$$

the equation becomes $y'^2 = x'^3 + A'x' + B'$ with

$$A' = u^{-4}A, \qquad B' = u^{-6}B.$$

Consequently,

$$\frac{4(A')^3}{4(A')^3 + 27(B')^2} = \frac{4A^3}{4A^3 + 27B^2},$$

so j does not change under this scaling.

Proof. Substitute $x = u^2 x'$ and $y = u^3 y'$ into $y^2 = x^3 + Ax + B$ and divide by u^6:

$$y'^2 = x'^3 + (u^{-4}A)x' + u^{-6}B.$$

The displayed identity for the j-ratio is immediate from the exponents -4 and -6. □

Remark 4.2. Analytically, this lemma mirrors the fact that multiplying a lattice by u rescales the Weierstrass invariants by u^{-4} and u^{-6}. The same cancellation is taking place, but on the lattice side rather than the equation side.

Example 4.1. Two quick computations illustrate what the algebraic formula is really measuring.

First consider $E_1 : y^2 = x^3 - 3x + 2$. Here $A = -3$ and $B = 2$, so

$$4A^3 + 27B^2 = 4(-27) + 27 \cdot 4 = -108 + 108 = 0.$$

The vanishing of the denominator is not an arithmetic accident: it is a certificate that the cubic $x^3 - 3x + 2$ has a repeated root, hence E_1 is singular and therefore not an elliptic curve.

Now consider $E_2 : y^2 = x^3 - 3x + 1$. In this case $4A^3 + 27B^2 = -108 + 27 = -81 \neq 0$, and

$$j(E_2) = 1728 \cdot \frac{4(-3)^3}{4(-3)^3 + 27 \cdot 1^2} = 1728 \cdot \frac{-108}{-81} = 2304.$$

So E_2 is nonsingular and has j-invariant 2304.

4.4 j as a global coordinate on the modular curve

The set $\Gamma(1)\backslash\mathbb{H}$ is not compact. Analytically one adds a single cusp (often denoted $i\infty$) to obtain the compact Riemann surface $X(1)$. The function j is holomorphic on $\mathbb{H}$ and has a single pole at the cusp. This forces $X(1)$ to look like a sphere with j as a meromorphic coordinate.

Theorem 4.2. *The function j extends to a meromorphic function on $X(1)$, and the induced map*

$$j : X(1) \longrightarrow \mathbb{P}^1(\mathbb{C})$$

is an isomorphism of compact Riemann surfaces.

One useful consequence is that every modular function for $\Gamma(1)$ is built from j and rational operations.

Corollary 4.1. *If f is a modular function of weight 0, then f can be written as a rational function in j. If, in addition, f is holomorphic on $\mathbb{H}$, then f is actually a polynomial in j.*

5 The q-expansion

The definition of j is conceptually clean but not computationally friendly: it is a quotient of series built from infinite sums over $\mathbb{Z}^2$. The q-expansion converts these objects into power series in one variable.

5.1 From τ to a small parameter

Definition 5.1. Let

$$q = e^{2\pi i\tau}.$$

When τ lies high in the upper half-plane, $\mathrm{Im}(\tau)$ is large and hence $|q| = e^{-2\pi\,\mathrm{Im}(\tau)}$ is small.

Because $T(\tau) = \tau + 1$ leaves q unchanged, any modular form admitting a reasonable growth condition at the cusp has a Fourier expansion in powers of q.

5.2 Normalized Eisenstein series

A standard normalization factors out the constant term.

Definition 5.2. For $k \geq 2$, define

$$E_{2k}(\tau) = \frac{G_{2k}(\tau)}{2\zeta(2k)},$$

so that $E_{2k}(\tau) = 1 + (\text{higher powers of } q)$.

The first two relevant cases are

$$E_4(\tau) = 1 + 240 \sum_{n \geq 1} \sigma_3(n)\, q^n, \qquad E_6(\tau) = 1 - 504 \sum_{n \geq 1} \sigma_5(n)\, q^n,$$

where $\sigma_r(n) = \sum_{d|n} d^r$ is the rth-power divisor sum.

5.3 A product viewpoint via the Dedekind η-function

Definition 5.3. The Dedekind η-function is

$$\eta(\tau) = q^{1/24} \prod_{n \geq 1} (1 - q^n), \qquad q = e^{2\pi i \tau}.$$

One then has the identity

$$\Delta(\tau) = (2\pi)^{12}\, \eta(\tau)^{24}.$$

In this form the exponent 24 is extremely visible, and it explains why Δ has a simple zero at the cusp: the factor q inside $\eta(\tau)^{24}$ contributes exactly one power of q.

Remark 5.1. We will not derive the full transformation law of $\eta(\tau)$ here. The important point for us is that the product is so explicit that it becomes a computational tool: truncating the product gives controlled approximations of Δ, and hence of j.

The discriminant has a q-expansion with integer coefficients,

$$\Delta(\tau) = (2\pi)^{12} \sum_{n \geq 1} \tau(n)\, q^n,$$

where $\tau(1) = 1$ and $\tau(n) \in \mathbb{Z}$ (Ramanujan's τ-function). It also admits the product expansion

$$\Delta(\tau) = (2\pi)^{12}\, q \prod_{n \geq 1} (1 - q^n)^{24}.$$

Combining the definition of j with the expansions of E_4 and Δ yields a Laurent series beginning with q^{-1}:

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

All coefficients in this expansion are integers.

Example 5.1. Take $\tau = 2i$. Then $q = e^{-4\pi} \approx 3.49 \times 10^{-6}$, so

$$j(2i) \approx q^{-1} + 744 \approx e^{4\pi} + 744 \approx 287\,495.$$

Keeping one more term changes this by about $196884\, q \approx 0.69$, so the approximation is already accurate to within a unit.

Remark 5.2. The point of the q-expansion is that it separates ideas from computation. The invariance $j(\tau) = j(\tau + 1)$ is built in, and the map $\tau \mapsto q$ turns the difficult limit $\operatorname{Im}(\tau) \to \infty$ into the familiar limit $q \to 0$.

6 Special values and geometric meaning

The values $j(i) = 1728$ and $j(\rho) = 0$ are famous, but the reason they occur is more informative than the numerical fact itself: these are exactly the lattices with extra rotational symmetry, and the extra symmetry forces branching in the quotient map.

6.1 Automorphisms and the two exceptional j-values

Proposition 6.1. *Let $E/\mathbb{C}$ be a complex elliptic curve.*

1. *If $j(E) \neq 0, 1728$, then $\mathrm{Aut}(E)$ has order 2 (generated by $[-1]$).*
2. *If $j(E) = 1728$, then $\mathrm{Aut}(E)$ has order 4.*
3. *If $j(E) = 0$, then $\mathrm{Aut}(E)$ has order 6.*

Example 6.1. The curve $E_1 : y^2 = x^3 - x$ has $j(E_1) = 1728$ and admits the automorphism $(x, y) \mapsto (-x, iy)$ of order 4. On the other hand, $E_2 : y^2 = x^3 + 1$ has $j(E_2) = 0$ and admits $(x, y) \mapsto (\zeta_3 x, y)$ of order 3, hence a full automorphism group of size 6 after including $[-1]$.

6.2 A real slice of the j-function

The q-expansion has real coefficients, so whenever $q = e^{2\pi i\tau}$ happens to be real, the value $j(\tau)$ must also be real. Two simple families of points in $\mathbb{H}$ make q real:

$$\tau = it \quad (t > 0) \quad \Rightarrow \quad q = e^{-2\pi t} \in (0, 1),$$

and

$$\tau = \tfrac{1}{2} + it \quad (t > 0) \quad \Rightarrow \quad q = e^{\pi i} e^{-2\pi t} = -e^{-2\pi t} \in (-1, 0).$$

Along these vertical lines, the Fourier series

$$j(\tau) = q^{-1} + 744 + \sum_{n \geq 1} c(n) q^n$$

is literally a real Laurent series in a real variable.

A pleasant geometric consequence is that as $t \to \infty$ one has $q \to 0$ and hence $j(it) \to +\infty$, while $j(\frac{1}{2} + it) \to -\infty$ because q^{-1} approaches $-\infty$ on the negative real axis. By continuity, j assumes every real value somewhere on the boundary of a fundamental region. This observation is one of the inputs in the classification of elliptic curves over $\mathbb{R}$: the real number $j(E)$ determines the isomorphism class of E over $\mathbb{C}$, and varying τ along a suitable curve in the standard fundamental domain produces exactly one representative for each possible real j-value.

Because the stabilizer of i in $\Gamma(1)$ has order 2 and the stabilizer of ρ has order 3, the map $j : X(1) \to \mathbb{P}^1$ is ramified at those points with respective branching indices 2 and 3. A useful way to remember this is to think of $X(1)$ as an orbifold: the points i and ρ behave like cone points, while the cusp behaves like a puncture that has been filled in.

7 Arithmetic of j

Even though j is defined analytically, its values at certain special points are algebraic and structured.

7.1 Modular polynomials as elimination of τ

Fix an integer $N \geq 1$. An elliptic curve may admit many distinct degree-N isogenies. From the lattice viewpoint, these correspond to index-N sublattices of Λ_τ. The modular polynomial is what you get when you try to describe all those isogenies using only the two numbers $j(\tau)$ and $j(\tau')$.

A concrete construction goes as follows. Choose a finite set $\mathcal{S}_N$ of integer matrices

$$\alpha = \begin{pmatrix} a & b \\ 0 & d \end{pmatrix}, \qquad ad = N, \qquad 0 \leq b < d,$$

representing the distinct $\Gamma(1)$-orbits of index-N sublattices. For such a matrix we have $\alpha \cdot \tau = \frac{a\tau+b}{d}$, which corresponds to the sublattice $\mathbb{Z}(a\tau + b) + \mathbb{Z}d \subset \mathbb{Z}\tau + \mathbb{Z}$. Now form the monic polynomial in an auxiliary variable X,

$$\Phi_N(X; j(\tau)) = \prod_{\alpha \in \mathcal{S}_N} \big(X - j(\alpha \cdot \tau)\big).$$

Its coefficients are symmetric polynomials in the values $j(\alpha \cdot \tau)$ and therefore are invariant under $\Gamma(1)$, hence they are modular functions of weight 0.

A key fact is that these coefficients have integral q-expansions, so after identifying modular functions with rational functions in j, one can normalize to obtain a polynomial

$$\Phi_N(X, Y) \in \mathbb{Z}[X, Y]$$

with the property that

$$\Phi_N\big(j(\tau), j(\tau')\big) = 0 \quad \Longleftrightarrow \quad E_\tau \text{ and } E_{\tau'} \text{ are linked by a cyclic isogeny of degree } N.$$

Geometrically, Φ_N is the equation of the Hecke correspondence inside $X(1) \times X(1)$.

Remark 7.1. The theme is the same as elsewhere in this paper: τ carries analytic data, while $j(\tau)$ carries moduli data. The modular polynomial is an explicit certificate that certain analytic constructions (isogenies) are actually algebraic over the j-line.

7.2 Singular moduli and integrality

Definition 7.1. A point $\tau \in \mathbb{H}$ is called quadratic imaginary if it satisfies a quadratic equation with rational coefficients and $\text{Im}(\tau) > 0$. Equivalently, τ generates an imaginary quadratic field. The value $j(\tau)$ is then called a singular modulus.

A central fact is that singular moduli are algebraic integers. In the language of complex multiplication, one proves much more: adjoining $j(\tau)$ to the imaginary quadratic field it generates produces a class field.

Example 7.1. The imaginary quadratic discriminants -3 and -4 have class number 1, and their distinguished lattices are represented by ρ and i. Accordingly,

$$j(\rho) = 0 \qquad \text{and} \qquad j(i) = 1728,$$

and both values are algebraic integers. More subtly, for discriminant -7 one finds the integer value $j\big(\frac{1+\sqrt{-7}}{2}\big) = -3375$, which already hints that special j-values can be unexpectedly integral.

References

[1] J. H. Silverman, *Advanced Topics in the Arithmetic of Elliptic Curves*, Graduate Texts in Mathematics 151, Springer, 1994.

[2] T. M. Apostol, *Modular Functions and Dirichlet Series in Number Theory*, Graduate Texts in Mathematics 41, Springer, 2nd ed., 1990.

[3] J.-P. Serre, *A Course in Arithmetic*, Graduate Texts in Mathematics 7, Springer, 1973.

[4] S. Lang, *Elliptic Functions*, Graduate Texts in Mathematics 112, Springer, 1987.