ON THE j-INVARIANT AND ITS CONNECTION TO NUMERICAL PHENOMENA

TARUN RAPAKA

ABSTRACT. The numbers $e^{\pi\sqrt{163}}$ and $e^{\pi\sqrt{67}}$ are rather close to integers, despite them being exponential expressions involving π and square roots. This is no coincidence, and this paper will provide intuition into this remarkable fact. Specifically, it will start by establishing an isomorphism between elliptic curves and complex tori, and then introduce the j-invariant as a function of the corresponding lattice. j may also be viewed as a function on the upper half plane under $SL_2(\mathbb{Z})$. For a complex number τ, its corresponding elliptic curve may admit complex multiplication under a quadratic number field's ring of integers. We will show that for such τ, inputting it into j yields an algebraic number with minimal degree over $\mathbb{Q}$ at most the class number of the quadratic number field. In fact, one may further improve this to $j(\tau)$ being an algebraic integer, but we won't discuss the proof. Finally, using the Fourier expansion of j, we will connect this fact to explaining why the above numbers are near-integers.

1. From complex lattices to elliptic curves

Let Λ be a lattice in $\mathbb{C}$, meaning that $\Lambda = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2$ for ω_1, ω_2 with different arguments. In this section, we will establish a bijection between the complex torus $\mathbb{C}/\Lambda$ (which is just $\mathbb{C}$ but numbers are taken modulo ω_1 and ω_2) and a corresponding elliptic curve.

Define the *Weierstrass elliptic function* $\wp(z)$ as given in Section VI.3 of Silverman [1]

$$\wp(z) = \frac{1}{z^2} + \sum_{\lambda \in \Lambda \setminus \{0\}} \left(\frac{1}{(z-\lambda)^2} - \frac{1}{\lambda^2} \right).$$

Notice that this function is defined on $\mathbb{C}/\Lambda$ because $\wp(z+\omega_1) = \wp(z)$ and $\wp(z+\omega_2) = \wp(z)$, as can be checked by slightly rearranging the sum. The way that $\wp$ connects to elliptic curves is through its remarkable differential equation:

Theorem 1.1. *The function $\wp$ satisfies*

$$(\wp'(z))^2 = 4(\wp(z))^3 - g_2(\wp(z)) - g_3,$$

where g_2 and g_3 are constants only dependent on Λ.

Proof. Notice that if the $\frac{1}{z^2}$ term were not there, then $\wp(z)$ would vanish at 0, and would also be holomorphic. Furthermore, note that $\wp(z)$ is even because $\frac{1}{(-z-\lambda)^2} - \frac{1}{\lambda^2} = \frac{1}{(z-(-\lambda))^2} - \frac{1}{(-\lambda)^2}$. Hence we may write the Laurent expansion of $\wp(z)$ as

$$\wp(z) = \frac{1}{z^2} + a_1 z^2 + a_2 z^4 + \dots.$$

This means that

$$\wp'(z) = -\frac{2}{z^3} + 2a_1 z + 4a_2 z^3 + \dots.$$

Date: March 26, 2026.

Squaring, we get

$$(\wp'(z))^2 = \frac{4}{z^6} - \frac{8a_1}{z^2} + \dots,$$

where everything beyond the first two terms have a positive power of z.

On the other hand, if we cube the Laurent expansion of $\wp(z)$, we get

$$(\wp(z))^3 = \frac{1}{z^6} + \frac{3a_1}{z^2} + \dots,$$

where again everything beyond the first two terms have a positive power of z. This means that

$$(\wp'(z))^2 - 4(\wp(z))^3 = -\frac{20a_1}{z^2} + \dots,$$

so

$$(\wp'(z))^2 - 4(\wp(z))^3 + 20a_1\wp(z) = c_0 + c_1z^2 + \dots$$

is a holomorphic function with no poles. Since it is doubly periodic and is uniquely determined by the torus $\mathbb{C}/\Lambda$, it is bounded. By Liouville's Theorem, this implies that it must be a constant, say $-g_3$. Then letting $g_2 = 20a_1$, we get

$$(\wp'(z))^2 = 4(\wp(z))^3 - g_2\wp(z) - g_3$$

for constants g_2 and g_3, as desired. ■

Remark 1.2. In fact,

$$g_2 = 60 \cdot \sum_{\lambda \in \Lambda \setminus \{0\}} \frac{1}{\lambda^4}$$

and

$$g_3 = 140 \cdot \sum_{\lambda \in \Lambda \setminus \{0\}} \frac{1}{\lambda^6}.$$

As such, the lattice Λ has a corresponding elliptic curve E_Λ given by

$$y^2 = 4x^3 - g_2x - g_3.$$

The way it works is as follows: first consider the torus $\mathbb{C}/\Lambda$. Then for z in this torus, map z to $(\wp(z), \wp'(z))$, which lies on the elliptic curve. We may check that $\wp(z)$ is a surjection from $\mathbb{C}/\Lambda$ to $\mathbb{C}$. Furthermore, by some more routine expansion, we may check that the points $(\wp(z), \wp'(z))$, $(\wp(w), \wp'(w))$, and $(\wp(z+w), -\wp'(z+w))$ are collinear, meaning that the group law on the elliptic curve is simply given by addition in $\mathbb{C}/\Lambda$. This means that $\mathbb{C}/\Lambda \cong E_\Lambda$.

2. Definition of the j function

Note that for any complex number c, we get $E_\Lambda \cong E_{c\Lambda}$. This is true because when we scale the lattice by c, the value of g_2 scales down by a factor of c^4 while the value of g_3 scales down by a factor of c^6, thus making the two elliptic curves isomorphic. Thus it makes sense to consider lattices under equivalence:

Definition 2.1. Two lattices Λ_1 and Λ_2 are said to be *homothetic* if there is nonzero $c \in \mathbb{C}$ such that $c\Lambda_1 = \Lambda_2$.

We use the shorthand notation $\sim$ to denote similarity of lattices.

Example. We have that if $\Lambda_1 = \mathbb{Z} + \mathbb{Z}i$ and $\Lambda_2 = \mathbb{Z}(2+i) + \mathbb{Z}(-1+2i)$, then $\Lambda_1 \sim \Lambda_2$, as one can multiply Λ_1 by $2+i$ to obtain Λ_2.

Hence we can assume that the lattice can be written simply as $\mathbb{Z} + \tau\mathbb{Z}$. However, two different values of τ can result in two homothetic lattices and therefore the same elliptic curve up to isomorphism. The values of τ which output the same elliptic curve can be described as follows:

Proposition 2.2. *For complex numbers τ and ω, we have that $\mathbb{Z}+\mathbb{Z}\omega \sim \mathbb{Z}+\mathbb{Z}\tau$ if and only if $\omega = \frac{a\tau+b}{c\tau+d}$ for some $a, b, c, d \in \mathbb{Z}$ with $ad - bc = \pm 1$.*

Proof. We will first deal with one direction: that if $\omega = \frac{a\tau+b}{c\tau+d}$, then $\mathbb{Z}+\tau\mathbb{Z} \sim \mathbb{Z}+\omega\mathbb{Z}$. Indeed, when $ad - bc = 1$, we get

$$\mathbb{Z} + \omega\mathbb{Z} = \mathbb{Z} + \left(\frac{a\tau + b}{c\tau + d}\right)\mathbb{Z}$$

is homothetic to

$$(c\tau + d)\mathbb{Z} + (a\tau + b)\mathbb{Z} = (-c(a\tau + b) + a(c\tau + d))\mathbb{Z} + (d(a\tau + b) - b(c\tau + d))\mathbb{Z} = \mathbb{Z} + \tau\mathbb{Z}.$$

The case where $ad - bc = -1$ can be handled similarly.

To deal with the other direction, suppose that $\mathbb{Z} + \tau\mathbb{Z} \sim \mathbb{Z} + \omega\mathbb{Z}$. This means there exists a nonzero constant A such that there exist integers $a, b, c, d \in \mathbb{Z}$ such that $A = c + d\omega$ and $A\tau = a + b\omega$. We need $ad - bc = \pm 1$, as otherwise 1 cannot be expressed of the form $A(x + y\tau)$ for $x, y \in \mathbb{Z}$. Hence dividing the two gives $\tau = \frac{a+b\omega}{c+d\omega}$, as needed. ■

For our purposes, we will restrict τ to the upper half plane since $\mathbb{Z}+\tau\mathbb{Z}$ is the same lattice as $\mathbb{Z}+(-\tau)\mathbb{Z}$. As such, since we are moving from $GL_2(\mathbb{Z})$ to $SL_2(\mathbb{Z})$, we can turn the above condition into simply $ad - bc = 1$.

Now, given any complex number τ in the upper half plane, we can construct a lattice $\mathbb{Z} + \mathbb{Z}\tau$, and from this lattice we can construct a corresponding elliptic curve. However, as shown by Proposition 2.1, two different values of τ may result in two isomorphic elliptic curves, so we need a way to distinguish between these isomorphic elliptic curves easily. This is where the j function comes in:

Definition 2.3. Given an elliptic curve E with equation $y^2 = 4x^3 - g_2x - g_3$, its *j-invariant*, as described in section III.1 of Silverman [1], is given by

$$j(E) = 1728 \cdot \frac{g_2^3}{g_2^3 - 27g_3^2}.$$

Likewise, given a complex number τ in the upper half plane, the j function is defined by

$$j(\tau) = j(E_{\mathbb{Z}+\tau\mathbb{Z}}).$$

The key property about the j invariant is that two elliptic curves E_1 and E_2 are isomorphic if and only if their j invariants are equal. This is true because when we multiply x by a factor t^2 and y by a factor t^3, the value of g_2 scales down by a factor of t^4, and the value of g_3 scales down by a factor of t^6. Hence g_2^3 and g_3^2 scale down by the same factor, thus fixing the j invariant. (The reason why we divide by $g_2^3 - 27g_3^2$ on the denominator is because when it vanishes, the elliptic curve is singular, which is bad.)

3. Complex multiplication

The material in the next two sections is adapted from Singh [2].

Let $\Lambda = \mathbb{Z} + \tau\mathbb{Z}$ be a lattice, and let E_Λ be its corresponding elliptic curve. Notice that in the above interpretation of elliptic curves as complex tori, we only explored addition of complex numbers, but we can also multiply complex numbers together. Multiplication by a fixed complex number gives a very special type of map:

Definition 3.1. Let E_1 and E_2 be two elliptic curves. An *isogeny* $f\colon E_1 \to E_2$ is a surjective morphism with finite kernel (i.e. finitely many elements of E_1 are sent to the additive identity of E_2).

Then clearly the map $f\colon E_\Lambda \to E_\Lambda$ defined by $x \xrightarrow{f} ax$, where $x \in \mathbb{C}/\Lambda$ and $a \in \mathbb{C} \setminus \{0\}$ is such that $a\Lambda \subseteq \Lambda$, is an isogeny. (The condition on a ensures that the isogeny is well-defined.) Since f sends E_Λ to itself, it is further called an *endomorphism* on E_Λ.

Now, let $\operatorname{End}(E_\Lambda)$ denote the ring of endomorphisms on E_Λ. This can also be thought of as the endomorphism ring of $\mathbb{C}/\Lambda$. Hence we can describe $\operatorname{End}(E_\Lambda)$ as the ring of $a \in \mathbb{C}$ for which $a\Lambda \subseteq \Lambda$. Indeed, as mentioned above, such a describes an endomorphism in $\mathbb{C}/\Lambda$ by $t \to at$, and an endomorphism in $\mathbb{C}/\Lambda$ must be of the form $t \to bt$ for some $b \in \mathbb{C}$.

It is clear that all integers are elements of $\operatorname{End}(E_\Lambda)$, so for most Λ, we simply have $\operatorname{End}(E_\Lambda) \cong \mathbb{Z}$. However, for special lattices, there exist non-integral a for which $a\Lambda \subseteq \Lambda$. We can classify exactly when this happens:

Proposition 3.2. $\operatorname{End}(\mathbb{C}/\Lambda) \ncong \mathbb{Z}$ *if and only if* $\mathbb{Q}(\tau)$ *is an imaginary quadratic number field.*

Proof. For one direction, assume that there exists $c \in \mathbb{C} \setminus \mathbb{Z}$ such that for all $a + b\tau \in \Lambda$, there exist $x, y \in \mathbb{Z}$ for which $c(a + b\tau) = x + y\tau$. Using $a + b\tau = 1$, we get $c = x_1 + y_1\tau$ for some $x_1, y_1 \in \mathbb{Z}$. Note that $y_1 \neq 0$ as otherwise $c = x_1$ is an integer. Plugging this in and instead using $a + b\tau = \tau$, we get

$$(x_1 + y_1\tau)(\tau) = x_1\tau + y_1\tau^2 = x_2 + y_2\tau$$

for some $x_2, y_2 \in \mathbb{Z}$. This means that τ is a root of a quadratic polynomial with integer coefficients. If τ is real, then Λ collapses onto the real line, which is bad. Hence τ is nonreal, meaning it is of the form $\frac{a+\sqrt{-d}}{b}$ for some integers a, b, d with $d > 0$. This means that $\mathbb{Q}(\tau) = \mathbb{Q}(\sqrt{-d})$ is an imaginary quadratic number field. The other direction holds since all these steps are reversible. This concludes the proof. ∎

We can go even further:

Proposition 3.3. *If* $\mathbb{Q}(\tau) = K$ *is an imaginary quadratic number field, then* $\operatorname{End}(\mathbb{C}/\Lambda)$ *is isomorphic to some subring of* $\mathcal{O}_K$*, the ring of integers of* K*.*

Proof. It suffices to show that if $c \in \mathbb{C} \setminus \mathbb{Z}$ is such that for all $a + b\tau \in \Lambda$, there exist $x, y \in \mathbb{Z}$ for which $c(a + b\tau) = x + y\tau$, then c is the root of some monic quadratic polynomial. As before, we get that $c = x + y\tau$ and $c\tau = z + t\tau$ for integers x, y, z, t with $y, z \neq 0$. We now note that $\begin{pmatrix} 1 \\ \tau \end{pmatrix}$ is an eigenvector with eigenvalue c for the matrix $\begin{pmatrix} x & y \\ z & t \end{pmatrix}$, which means that c satisfies the characteristic equation of this matrix. This characteristic equation is our monic quadratic polynomial, as needed. ∎

So for certain elliptic curves, the ring of isogenies onto itself behaves like a subring R of the ring of integers for some imaginary quadratic number field, for which $R \neq \mathbb{Z}$.

Definition 3.4. If E is an elliptic curve with $\mathbb{Z} \subsetneq \mathrm{End}(E) = R \subseteq \mathcal{O}_K$ for some imaginary quadratic number field K, then E is said to have *complex multiplication* by R.

4. Connecting the j function to complex multiplication

In order to prove that $j(\tau)$ is algebraic for certain τ, it will help to examine the set of all elliptic curves with complex multiplication by $R \subseteq \mathcal{O}_K$ for some imaginary quadratic number field K, under isomorphism. We call this set of isomorphism classes $\mathrm{Ell}(R)$, taken from Singh [2].

Notice that any fractional ideal I of $\mathcal{O}_K$ can be treated like a lattice. Hence $\mathrm{End}(\mathbb{C}/I) = \{c \in \mathbb{C} \colon cI \subseteq I\}$. Since any c in this set must clearly also be in K, the set must be

$$\{c \in L \colon cI \subseteq I\} = \mathcal{O}_K$$

by the definition of a fractional ideal. Thus for all fractional ideals I of $\mathcal{O}_K$, we get $E_I \in \mathrm{Ell}(\mathcal{O}_K)$.

However, some ideals give the same lattice up to homothety, resulting in isomorphic elliptic curves. Hence we have one elliptic curve in $\mathrm{Ell}(\mathcal{O}_K)$ for each element of the ideal class group of K. In fact, these are all the elements of K, and we will prove this by identifying a group action on $\mathrm{Ell}(\mathcal{O}_K)$ by the ideal class group. Recall that the ideal class group $\mathrm{Cl}(K)$ of a number field K is the group of its ideals under equivalence/homothety. For example, the ideal class group of $\mathbb{Q}[i]$ contains just one element since every ideal in $\mathbb{Q}[i]$ is principal.

Proposition 4.1. *Let $E_\Lambda \in \mathrm{Ell}(\mathcal{O}_K)$, and let I be a fractional ideal in $\mathcal{O}_K$. Then $I\Lambda$ is a lattice, and $E_{I\Lambda}$ has complex multiplication by $\mathcal{O}_K$.*

Proof. We first prove that $I\Lambda$ is a lattice. By definition, there exists $\alpha \in \mathcal{O}_K$ such that αI is an ideal in $\mathcal{O}_K$. This means that $\alpha(I\Lambda) = (\alpha I)\Lambda \subseteq \Lambda$, where we use the fact that $a\Lambda \subseteq \Lambda$ for $a \in \mathcal{O}_K$ (follows from $E_\Lambda \in \mathrm{Ell}(\mathcal{O}_K)$). Hence we get $I\Lambda \subseteq \alpha^{-1}\Lambda$, meaning that $I\Lambda$ is contained in a lattice. Since it is closed under addition and clearly doesn't have rank 1, we conclude that it is indeed a lattice.

Now we will show that $I\Lambda$ has complex multiplication by $\mathcal{O}_K$. Again, we must show that for all $a \in \mathcal{O}_K$, that $a(I\Lambda) \subseteq I\Lambda$, but this follows from above because $a(I\Lambda) = I(a\Lambda) \subseteq I\Lambda$ because $a\Lambda \subseteq \Lambda$, which follows from $E_\Lambda \in \mathrm{Ell}(\mathcal{O}_K)$. So we get $E_{I\Lambda} \in \mathrm{Ell}(\mathcal{O}_K)$ as well, and we are done. ■

This introduces a group action on $\mathrm{Ell}(\mathcal{O}_K)$ by the ideal class group, defined by $[I] \cdot E_\Lambda = E_{[I]\Lambda}$. Notice that we are using classes of ideals because if $I \sim J$, then $I\Lambda \sim J\Lambda$, giving $E_{I\Lambda} \cong E_{J\Lambda}$. One can show (we omit the proof) that this action is transitive (meaning there is always a class of ideals sending one E_Λ to another $E_{\Lambda'}$) and free (meaning that the only way to fix an E_Λ is by using the identity).

Using this, we can establish a bijection $f \colon \mathrm{Cl}(K) \to \mathrm{Ell}(\mathcal{O}_K)$ defined by $f([I]) = [I] \cdot E_\Lambda$ for a fixed $E_\Lambda \in \mathrm{Ell}(\mathcal{O}_K)$. This map is surjective because the group action is transitive, and it is injective because if $[I] \cdot E_\Lambda = [J] \cdot E_\Lambda$, then $E_\Lambda = ([I]^{-1} \cdot [J]) \cdot E_\Lambda$, giving $[I] = [J]$ since the group action is free. Hence this map is indeed a bijection, which immediately gives $|\mathrm{Ell}(\mathcal{O}_K)| = |\mathrm{Cl}(K)|$, which we will call h_K.

Thus we get our main theorem:

Theorem 4.2. *If E is an elliptic curve which admits complex multiplication by $\mathcal{O}_K$, then $j(E)$ is an algebraic number with $[\mathbb{Q}(j(E)) : \mathbb{Q}] \leq h_K$.*

Proof. Let σ be an automorphism of $\mathbb{C}$, and construct E^σ by turning $y^2 = 4x^3 - g_2x - g_3$ into $y^2 = 4x^3 - \sigma(g_2)x - \sigma(g_3)$. Clearly note that $\text{End}(E) \cong \text{End}(E^\sigma)$ because $(x, y) \in E$ if and only if $(\sigma(x), \sigma(y)) \in E^\sigma$, so an isogeny from E to itself corresponds with an isogeny from E^σ to itself. Hence E^σ has complex multiplication by $\mathcal{O}_K$ as well. Then

$$j(E^\sigma) = 1728 \cdot \frac{\sigma(g_2)^3}{\sigma(g_2)^3 - 27\sigma(g_3)^2} = \sigma\left(1728 \cdot \frac{g_2^3}{g_2^3 - 27g_3^2}\right) = \sigma(j(E))$$

by the definition of an automorphism. Therefore, $\sigma(j(E))$ can only take on h_K values as σ varies. These $\sigma(j(E))$ are the Galois conjugates of $j(E)$, which means that $[\mathbb{Q}(j(E)) : \mathbb{Q}] \leq h_K$, as desired. ∎

Corollary 4.3. *If K has class number 1 and E is an elliptic curve with complex multiplication by K, then $j(E)$ is a rational number.*

In fact, the above theorem may be strengthened:

Theorem 4.4. *If E is an elliptic curve which admits complex multiplication by $\mathcal{O}_K$, then $j(E)$ is an algebraic **integer** with $[\mathbb{Q}(j(E)) : \mathbb{Q}] \leq h_K$.*

The proof of this theorem is beyond the scope of this paper. This implies that $j(E)$ is an integer when E has complex multiplication by K such that $h_K = 1$.

5. Connection to numerical approximations

The numbers 163 and 67 are both Heegner numbers, meaning that $K = \mathbb{Q}\left[\sqrt{-D}\right]$ satisfies $h_K = 1$ for $D = 67, 163$. Also, if $\tau = \frac{1+i\sqrt{D}}{2}$ and $\Lambda = \mathbb{Z} + \tau\mathbb{Z} = \mathcal{O}_K$, then $\mathbb{C}/\Lambda$ has complex multiplication by $\mathcal{O}_K$ as $\mathcal{O}_K$ is a ring. Hence by Theorem 4.4, $j\left(\frac{1+i\sqrt{D}}{2}\right)$ is an integer.

To finish, we use the Fourier expansion of the j function:

$$j(\tau) = e^{-2\pi i\tau} + 744 + 196884e^{2\pi i\tau} + \ldots.$$

Plugging in $\tau = \frac{1+i\sqrt{D}}{2}$, we get

$$j\left(\frac{1+i\sqrt{D}}{2}\right) = e^{-2\pi i\left(\frac{1+i\sqrt{D}}{2}\right)} + 744 + 196884e^{2\pi i\left(\frac{1+i\sqrt{D}}{2}\right)} + \ldots.$$

Simplifying the exponents, we get

$$j\left(\frac{1+i\sqrt{D}}{2}\right) = -e^{\pi\sqrt{D}} + 744 - 196884e^{-\pi\sqrt{D}} + \ldots.$$

This means that

$$e^{\pi\sqrt{D}} = 744 - j\left(\frac{1+i\sqrt{D}}{2}\right) - 196884e^{-\pi\sqrt{D}} + \ldots.$$

The first two terms are both integers, and all subsequent terms are extremely small, giving that $e^{\pi\sqrt{D}}$ is very close to an integer for all D which are Heegner numbers. Indeed, we get

$$e^{\pi\sqrt{67}} \approx 147197952743.9999987$$

and

$$e^{\pi\sqrt{163}} \approx 262537412640768743.99999999999925.$$

6. Acknowledgments

The author would like to thank Shoshana Elgart and Simon Rubinstein-Salzedo for their feedback and insights on this paper. The author would also like to thank Simon Rubinstein-Salzedo and Euler Circle for offering the Infinite Series course, for which this paper was written.

References

[1] J. H. Silverman, *The Arithmetic of Elliptic Curves*. Springer, 2009.

[2] J. Singh, "Complex multiplication of elliptic curves and class field theory." `https://www.math.ucla.edu/~jas/writings/cm-elliptic-curves-cft.pdf`. Accessed on 2026-03-25.

Email address: `tarun.rapaka@gmail.com`