

Integrality of the j -invariant of elliptic curves with
complex multiplication

Álvaro Lozano Robledo

November 3, 2003

0.1 Introduction

Consider the following decimal expansion:

$$\xi = e^{\pi\sqrt{163}} = 262537412640768743.999999999999250072597\dots$$

Thus, ξ is an integer to 12 decimal places. This is a very interesting remark since we actually know that ξ is a transcendental number, due to the Gel'fond-Schneider theorem ($e^{\pi\alpha}$ is transcendental whenever α is algebraic over \mathbb{Q} of degree at least 2).

However, this is no curious coincidence. The fact that ξ is so close to a rational integer has a beautiful explanation that involves a deep theorem in the theory of elliptic curves, namely the fact that the j -invariant of an elliptic curve with complex multiplication by the field \mathbf{K} is an algebraic integer in this field.

Let $\mathbf{K}=\mathbb{Q}(\sqrt{-163})$. As we will see (*section 1.2*), given a quadratic imaginary field \mathbf{K} , there is an elliptic curve with complex multiplication by \mathbf{K} . In our case:

$$E_{163} : y^2 + y = x^3 - 2174420x + 1234136692$$

In addition to this, it is a well known fact that $\mathbb{Q}(\sqrt{-163})$ is the “last” quadratic imaginary field with class number 1, i.e. \mathbf{K} is a P.I.D.. The theory of complex multiplication (*Theorem 2.(c)*) tells us that $j(E_{163})$ satisfies $[\mathbb{Q}(j(E_{163})) : \mathbb{Q}] \leq h_K = 1$, therefore $j(E_{163}) \in \mathbb{Q}$. And the strongest statement (*Theorem 6*) implies that $j(E_{163}) \in R_L$, where $\mathbf{L}=\mathbb{Q}(j(E))$, and, in our case $\mathbf{L}=\mathbb{Q}$, so $R_L = \mathbb{Z}$. Hence:

$$j(E_{163}) \in \mathbb{Z}$$

Next, recall that for an elliptic curve E/\mathbb{C} there is a lattice in \mathbb{C} of the form $\Lambda = \langle 1, \tau \rangle$, so that $E/\mathbb{C} \cong \mathbb{C}/\Lambda$. In our case,

$$E_{163}/\mathbb{C} \cong \mathbb{C} / \langle 1, \frac{1 + \sqrt{-163}}{2} \rangle$$

Notice that $j(E)$ has a q -expansion, depending on τ :

$$j(q) = 1/q + 744 + 196884q + 21493760q^2 + \dots, \text{ where } q = e^{2\pi i\tau}$$

If we substitute $\tau = \frac{1+\sqrt{-163}}{2}$, then $q = -e^{-\pi\sqrt{163}} \approx -3.809 \cdot 10^{-18}$ is very small. Thus, $j(E_{163}) \approx 1/q + 744$, so $744 - j(E_{163}) \approx -1/q = \xi = e^{\pi\sqrt{163}}$ must be very close to be a rational integer.

1.1 Basic Definitions and Theorems

Definition 1. Let E be an elliptic curve. The **endomorphism ring** of E is the set:

$$\text{End}(E) = \text{Hom}(E, E) = \{\phi : E \rightarrow E, \text{ morphism s.t. } \phi(0) = 0\} \quad (1.1)$$

The basic theory of complex multiplication tells us that $\text{End}(E) \otimes \mathbb{Q}$ is isomorphic to a quadratic imaginary field, and $\text{End}(E)$ is an order in that field.

Definition 2. If $\text{End}(E) \cong R \subseteq \mathbb{C}$, and $\mathbf{K} = R \otimes \mathbb{Q}$, then we say that the elliptic curve E has complex multiplication by R (or complex multiplication by \mathbf{K}).

The following theorem plays a fundamental role in the theory of elliptic curves.

Theorem 1. (Uniformization Theorem) Let E/\mathbb{C} be an elliptic curve. Then there exists a lattice $\Lambda \subset \mathbb{C}$ and an isomorphism:

$$\varphi : \mathbb{C}/\Lambda \rightarrow E(\mathbb{C}), \varphi(z) = (\wp(z, \Lambda), \wp'(z, \Lambda)) \quad (1.2)$$

Using the Uniformization theorem and the theory of complex multiplication, it can be proved that for E/\mathbb{C} isomorphic to \mathbb{C}/Λ (call it E_Λ):

$$\text{End}(E_\Lambda) \cong \{\alpha \in \mathbb{C} : \alpha\Lambda \subset \Lambda\} \quad (1.3)$$

Next, we consider the set of all elliptic curves with a fixed endomorphism ring.

Definition 3. $ELL(R) = \frac{\{\text{Elliptic curves with } \text{End}(E) \cong R\}}{\{\text{Isomorphism over } \mathbb{C}\}}$

1.2 The group action induced by $CL(R_K)$

Let \mathbf{K} be a quadratic imaginary field. Is there any elliptic curve $E \in ELL(R_K)$? The answer is *yes*. For this, let ϑ be a non-zero fractional ideal of \mathbf{K} , $\vartheta \subset \mathbf{K} \subset \mathbb{C}$, in particular ϑ is a lattice in \mathbb{C} . Moreover:

$$\begin{aligned} \text{End}(E_\vartheta) &\cong \{\alpha \in \mathbb{C} : \alpha\vartheta \subset \vartheta\} \\ &= \{\alpha \in \mathbf{K} : \alpha\vartheta \subset \vartheta\}, \text{ since } \vartheta \subset \mathbf{K} \\ &= R_{\mathbf{K}}, \text{ since } \vartheta \text{ is fractional ideal.} \end{aligned}$$

Hence, $E_\vartheta \in ELL(R_{\mathbf{K}})$. Since homothetic lattices give isomorphic elliptic curves, it turns out that $E_\vartheta \cong E_{\lambda\vartheta}$ for any non-zero $\lambda \in \mathbb{C}$. Therefore it is enough to look at equivalence classes of ideals, i.e. $\bar{\vartheta} \in CL(R_K)$. In other words, there is a well defined map:

$$\begin{aligned} CL(R_K) &\longrightarrow ELL(R_K) \\ \bar{\vartheta} &\longrightarrow E_\vartheta \end{aligned} \tag{1.4}$$

Furthermore, this induces a simply transitive action of $CL(R_K)$ on $ELL(R_K)$.

Proposition 1 (Simply transitive action). *Let Λ be a lattice with $E_\Lambda \in ELL(R_K)$, and let ϑ, θ be non-zero fractional ideals of \mathbf{K} .*

- (i) $\vartheta\Lambda$ is a lattice in \mathbb{C} ;
- (ii) $\text{End}(E_{\vartheta\Lambda}) \cong R_K$;
- (iii) $E_{\vartheta\Lambda} \cong E_{\theta\Lambda}$ if and only if $\bar{\vartheta} = \bar{\theta}$ in $CL(R_K)$;

and this gives a well defined group action $\bar{\vartheta} * E_\Lambda = E_{\vartheta^{-1}\Lambda}$. Moreover, this action is simply transitive. In particular:

$$\sharp ELL(R_K) = \sharp CL(R_K) = h_K \tag{1.5}$$

Suppose E has complex multiplication, so $\text{End}(E)$ is an order in \mathbb{C} , thus, there are two ways to embed it. So we must fix this embedding:

Lemma 1. *Let $E \in ELL(R_K)$. There is a unique isomorphism*

$$[\cdot] : R_K \longrightarrow \text{End}(E)$$

such that $[\alpha]^*\omega = \alpha\omega, \forall \alpha \in R_K, \forall \omega \in \Omega_E$.

From now on, always assume we are using this isomorphism.

Let E be an elliptic curve. For $m \in \mathbb{N}$, it is always possible to define the torsion subgroup:

$$E[m] = \{P \in E : [m]P = 0\}$$

If E has complex multiplication, there are other natural subgroups to look at. Suppose $E \in ELL(R_K)$ and let ϑ be an integral ideal of R_K :

$$E[\vartheta] = \{P \in E : [\alpha]P = 0 \forall \alpha \in \vartheta\}$$

Moreover, if $E(\mathbb{C}) \cong \mathbb{C}/\Lambda$, then, by (1.3), $R_K\Lambda = \Lambda$, and since $\vartheta \in R_K$, we have $\Lambda \subset \vartheta^{-1}\Lambda$. So there is a natural homomorphism:

$$\begin{aligned} \mathbb{C}/\Lambda &\longrightarrow \mathbb{C}/\vartheta^{-1}\Lambda \\ z &\longrightarrow z \end{aligned}$$

which corresponds to a natural map:

$$E_\Lambda \longrightarrow \bar{\vartheta} * E_\Lambda \tag{1.6}$$

Proposition 2. *Let $E_\Lambda \in ELL(R_K)$, and let $\vartheta \in R_K$ be an integral ideal. Then:*

- (a) $E[\vartheta] = \text{Ker}(E_\Lambda \longrightarrow \bar{\vartheta} * E_\Lambda)$
- (b) $E[\vartheta]$ is a free R_K/ϑ -module of rank 1.

1.3 $j(\mathbf{E}) \in \bar{\mathbb{Q}}$

Theorem 2.

(a) *Let E/\mathbb{C} be an elliptic curve, and let $\sigma : \mathbb{C} \longrightarrow \mathbb{C}$ be a field automorphism. Then, $\text{End}(E^\sigma) \cong \text{End}(E)$.*

(b) *If $E \in ELL(R_K)$ then $j(E) \in \bar{\mathbb{Q}}$.*

(c) $[\mathbb{Q}(j(E)) : \mathbb{Q}] \leq h_K$.

Proof. (a) Let $\phi : E \longrightarrow E$ be an endomorphism of E . Since E^σ is defined by letting σ act on the coefficients of the Weierstrass equation for E , and since ϕ is a morphism, we can define $\phi^\sigma : E^\sigma \longrightarrow E^\sigma$ just by letting σ act on the coefficients of the defining equations for the morphism ϕ . Then it is trivial to check that the map:

$$\begin{aligned} \text{End}(E) &\longrightarrow \text{End}(E^\sigma) \\ \phi &\longrightarrow \phi^\sigma \end{aligned}$$

is an isomorphism.

(b) Let $\sigma \in \text{Aut}(\mathbb{C})$. The j -invariant $j(E)$ is given by a rational combination of the coefficients of E , and the Weierstrass equation of E^σ is given by letting σ act on the coefficients of the equation for E . Thus:

$$j(E^\sigma) = j(E)^\sigma \tag{1.7}$$

By (a), we know that $End(E^\sigma) \cong End(E) \cong R_K$, so $E^\sigma \in ELL(R_K)$. Now, *Proposition 1* says that $\sharp ELL(R_K) = \sharp CL(R_K) = h_K$, in particular there is a finite number of isomorphism classes of elliptic curves with complex multiplication by \mathbf{K} . Since the \mathbb{C} -isomorphism class of an elliptic curve is determined by its j -invariant, $j(E)^\sigma$ can only take finitely many different values as σ ranges over $Aut(\mathbb{C})$.

Hence $[\mathbb{Q}(j(E)) : \mathbb{Q}]$ is finite ($\leq h_K$, which proves part (c)), so $j(E)$ is an algebraic number over \mathbb{Q} .

Q.E.D.

1.4 Extension by torsion

First a technical lemma:

Lemma 2.

(i) Let $E/\mathbb{C} \in ELL(R_K)$. Then $([\alpha]_E)^\sigma = [\alpha^\sigma]_{E^\sigma} \forall \alpha \in R_K, \forall \sigma \in Aut(\mathbb{C})$.

(ii) Let \mathbf{L} be a number field, let E be defined over \mathbf{L} , and $E \in ELL(R_K)$. Then every endomorphism is defined over \mathbf{LK} .

Proof. (i) For this, we need to use that the map:

$$End(E^\sigma) \longrightarrow End(\Omega_{E^\sigma}), \omega \longrightarrow \omega^* \quad (1.8)$$

is injective, and that for any $\alpha \in R$, $\sigma \in Aut(\mathbb{C})$, and for $\omega \in \Omega_E$:

$$(([\alpha]_E)^\sigma)^*(\omega^\sigma) = (([\alpha]_E)^*\omega)^\sigma = (\alpha\omega)^\sigma = \alpha^\sigma\omega^\sigma = ([\alpha^\sigma]_{E^\sigma})^*(\omega^\sigma) \quad (1.9)$$

to deduce the desired result.

(ii) Let $\sigma \in Aut(\mathbb{C})$ that fixes \mathbf{L} . Since E is defined over \mathbf{L} , there exists a Weierstrass equation for E with coefficients over \mathbf{L} . Since σ fixes \mathbf{L} , $E^\sigma = E$. So, by (i):

$$([\alpha]_E)^\sigma = [\alpha^\sigma]_{E^\sigma} = [\alpha^\sigma]_E \quad (1.10)$$

Now suppose σ also fixes \mathbf{K} , i.e. σ fixes \mathbf{LK} , then $\alpha^\sigma = \alpha \forall \alpha \in R_K$, and (1.10) reads:

$$([\alpha]_E)^\sigma = [\alpha]_E, \forall \sigma \text{ that fix } \mathbf{LK} \quad (1.11)$$

Therefore, $[\alpha]$ is defined over \mathbf{LK} .

Q.E.D.

Theorem 3 (Abelian extension generated by torsion points).

Let $E \in ELL(R_K)$, and let $\mathbf{L} = \mathbf{K}(j(E), E_{tors})$, where E_{tors} is the set of coordinates of torsion points. Then \mathbf{L} is an abelian extension of $\mathbf{K}(j(E))$.

Proof. Put $\mathbf{H} = \mathbf{K}(j(E))$, and $\mathbf{L}_m = \mathbf{K}(j(E), E[m]) = \mathbf{H}(E[m])$. \mathbf{L} is the compositum of all \mathbf{L}_m , when m runs over \mathbf{N} , so it is enough to show that \mathbf{L}_m/\mathbf{H} is an abelian extension.

Next, notice that E is defined over \mathbf{H} , and $\text{Gal}(\overline{\mathbf{K}}/\mathbf{H})$ acts on $E[m]$:

$$[m]P = 0 \Rightarrow [m](P^\sigma) = ([m]P)^\sigma = 0, \forall \sigma \in \text{Gal}(\overline{\mathbf{K}}/\mathbf{H}) \quad (1.12)$$

and we can define a representation by:

$$\begin{aligned} \rho : \text{Gal}(\overline{\mathbf{K}}/\mathbf{H}) &\longrightarrow \text{Aut}(E[m]) \cong GL_2(\mathbb{Z}/m\mathbb{Z}) \\ \sigma &\longrightarrow \rho(\sigma), \rho(\sigma)(T) = T^\sigma \end{aligned} \quad (1.13)$$

By Lemma 2.ii every endomorphism of E is defined over \mathbf{H} ($\mathbf{K} \subseteq \mathbf{H}$, so $\mathbf{H}\mathbf{K} = \mathbf{H}$). By Lemma 2.i, $[\alpha]^\sigma = [\alpha^\sigma]$, so if $\alpha \in R_K$ and σ fixes \mathbf{H} then $[\alpha]^\sigma = [\alpha]$. Thus:

$$([\alpha]T)^\sigma = [\alpha]^\sigma T^\sigma = [\alpha]T^\sigma, \forall \sigma \in \text{Gal}(\mathbf{L}_m/\mathbf{H}), T \in E[m], \alpha \in R_K$$

So, if $\alpha = m\beta \in mR_K$, then $([m\beta]T)^\sigma = [m\beta]T^\sigma = [m\beta]T^\sigma = 0$. Therefore, ρ induces an injection:

$$\phi : \text{Gal}(\mathbf{L}_m/\mathbf{H}) \hookrightarrow \text{Aut}_{R_K/mR_K}(E[m]) \quad (1.14)$$

Last, Proposition 2.(b) says that $E[m]$ is a free R_K/mR_K -module of rank one, so:

$$\text{Aut}_{R_K/mR_K}(E[m]) \cong (R_K/mR_K)^* \quad (1.15)$$

and, clearly $(R_K/mR_K)^*$ is an abelian group. Therefore $\text{Gal}(\mathbf{L}_m/\mathbf{H})$ is abelian.

Q.E.D.

1.5 Criterion of Néron-Ogg-Shafarevich

In this section, we use the following notation:

- \mathbf{K} local field, complete with respect to a discrete valuation ν
- \mathbf{R} the ring of integers of \mathbf{K}
- M the maximal ideal of \mathbf{R}
- k the residue field of \mathbf{R}

Definition 4. Let Ξ be a set on which $\text{Gal}(\overline{\mathbf{K}}/\mathbf{K})$ acts. We say that Ξ is unramified at ν if the action of I_ν on Ξ is trivial, i.e. $\zeta^\sigma = \zeta \forall \sigma \in I_\nu, \forall \zeta \in \Xi$.

Theorem 4 (Criterion of Néron-Ogg-Shafarevich).

Let E/\mathbf{K} be an elliptic curve. The following are equivalent:

- (a) E has good reduction over \mathbf{K} ;
- (b) $E[m]$ is unramified at ν for all $m \geq 1, (m, \text{char}(k))=1$;
- (c) The Tate module $T_l(E)$ is unramified at ν for some (all) $l, l \neq \text{char}(k)$;
- (d) $E[m]$ is unramified at ν for infinitely many integers $m \geq 1, (m, \text{char}(k))=1$.

Corollary 1. Let E/\mathbf{K} be an elliptic curve. Then E has potential good reduction if and only if the inertia group I_ν acts on $T_l(E)$ through a finite quotient for some prime $l \neq \text{char}(k)$.

Proof of Corollary. (\Rightarrow) Assume that E has potential good reduction. By definition, there exists a finite extension of \mathbf{K}, \mathbf{K}' , such that E/\mathbf{K}' has good reduction. We can extend \mathbf{K}' so \mathbf{K}'/\mathbf{K} is a Galois finite extension.

Let ν' and $I_{\nu'}$ be the corresponding valuation and inertia group for \mathbf{K}' . Then the theorem above ((a) \Rightarrow (c)) implies that $T_l(E)$ is unramified at ν' for all $l, l \neq \text{char}(k) = \text{char}(k')$ (since k' is a finite extension of k). So $I_{\nu'}$ acts trivially on $T_l(E) \forall l \neq \text{char}(k')$. Thus $I_\nu \hookrightarrow T_l(E)$ factors through the finite quotient $I_\nu/I_{\nu'}$.

(\Leftarrow) Let $l \neq \text{char}(k)$, and assume $I_\nu \hookrightarrow T_l(E)$ factors through a finite quotient, say I_ν/J . Let $\overline{\mathbf{K}}^J$ be the fixed field of J , then $\overline{\mathbf{K}}^J/\overline{\mathbf{K}}^{I_\nu}$ is a finite extension, so we can find a finite extension \mathbf{K}'/\mathbf{K} so that $\overline{\mathbf{K}}^J = \mathbf{K}'\overline{\mathbf{K}}^{I_\nu}$.

So the inertia group of \mathbf{K}' is equal to J , and J acts trivially on $T_l(E)$. Hence the criterion ((c) \Rightarrow (a)) implies that E has good reduction over \mathbf{K}' , and since \mathbf{K}'/\mathbf{K} is finite, E has potential good reduction.

Q.E.D.

Proposition 3. Let E/\mathbf{K} be an elliptic curve. Then E has potential good reduction if and only if its j -invariant is integral (i.e. $j(E) \in \mathbf{R}$).

Proof. (\Leftarrow) Assume $\text{char}(k) \neq 2$, it is easy to prove that we can extend \mathbf{K} to a finite extension \mathbf{K}' so that E has a Weierstrass equation:

$$E : y^2 = x(x-1)(x-\lambda) \quad \lambda \neq 0, 1 \quad (1.16)$$

Since we are assuming $j(E) \in R$, and:

$$(1 - \lambda(1 - \lambda))^3 - j\lambda^2(1 - \lambda)^2 = 0 \quad (1.17)$$

then $\lambda \in R$ and $\lambda \neq 0, 1 \pmod{M'}$ ($\Rightarrow \Delta' \in (R')^*$). Hence E/\mathbf{K}' has good reduction, i.e. E has potential good reduction.

(\Rightarrow) Assume that E has potential good reduction, so there exists \mathbf{K}' so that E/\mathbf{K}' has good reduction. Let Δ', c_4' the usual quantities associated to the Weierstrass equation over \mathbf{K}' .

Since E/\mathbf{K}' has good reduction, $\Delta' \in (R')^*$, and so $j(E) = \frac{(c_4')^3}{\Delta'} \in R'$. But since E is defined over \mathbf{K} , $j(E) \in \mathbf{K}$, so $j(E) \in \mathbf{K} \cap R' = R$.

Q.E.D.

1.6 Integrality of the j-invariant

The strategy of the proof is the following. We will prove that for all prime ideals \wp of R_K , $j(E)$ is \wp -integral, i.e. $j(E) \in R_\wp$ and $j(E) \in \bigcap R_\wp = R_K$. In order to show that it is \wp -integral, we use the Criterion of Néron-Ogg-Shafarevich to prove that E has potential good reduction over K_\wp , and then use *Proposition 3* to deduce the desired result.

Theorem 5. *Let \mathbf{L} be a number field and E/\mathbf{L} an elliptic curve with complex multiplication. Then E has potential good reduction at every prime of \mathbf{L} .*

Proof. By *Lemma 2.ii*, we can consider a finite extension of \mathbf{L} so that every endomorphism is defined over that extension. Assume \mathbf{L} has this property, so $\text{End}_{\mathbf{L}}(E) \neq \mathbb{Z}$.

Fix a prime \wp of \mathbf{L} . Let \mathbf{L}_\wp be the completion of \mathbf{L} at \wp , and, consider as usual $R_\wp, M_\wp, p = \text{char}(R_\wp/M_\wp), l$ prime $\neq 2, p$. Also, let \mathbf{L}_\wp^{ab} be the maximal abelian extension of \mathbf{L}_\wp ; I_\wp is the inertia subgroup for $G = \text{Gal}(\overline{\mathbf{L}}_\wp/\mathbf{L}_\wp)$, and I_\wp^{ab} the inertia for $G^{ab} = \text{Gal}(\overline{\mathbf{L}}_\wp^{ab}/\mathbf{L}_\wp)$.

Since $\text{End}_{\mathbf{L}}(E) \neq \mathbb{Z}$ then also $\text{End}_{\mathbf{L}_\wp}(E) \neq \mathbb{Z}$, and we can apply *Theorem 3* to deduce that the action of G on $T_l(E)$ is abelian, so, in particular, I_\wp acts through the quotient I_\wp^{ab} . Moreover, local class field theory says that there is an isomorphism $I_\wp^{ab} \cong R_\wp^*$. This is very useful since we can

write the exact sequence:

$$\begin{array}{ccccccc}
1 & \longrightarrow & R_{\varphi,1}^* & \longrightarrow & R_{\varphi}^* & \longrightarrow & (R_{\varphi}/M_{\varphi})^* \longrightarrow 1 \\
& & & & \parallel \wr & & \\
& & & & I_{\varphi}^{ab} & &
\end{array} \quad (1.18)$$

where $R_{\varphi,1}^* = \{u \in R_{\varphi}^* : u \equiv 1 \pmod{M_{\varphi}}\}$. $R_{\varphi,1}^*$ is a pro-p group, that is, it is the inverse limit of finite groups of p-power order, since it is isomorphic to the formal multiplicative group $\hat{G}_m(M_{\varphi})$.

Similarly, if we fix a basis for $T_l(E)$, we have $Aut(T_l(E)) \cong GL_2(\mathbb{Z}_l)$, and there is an exact sequence:

$$\begin{array}{ccccccc}
1 & \longrightarrow & GL_2(\mathbb{Z}_l)_1 & \longrightarrow & GL_2(\mathbb{Z}_l) & \longrightarrow & GL_2(\mathbb{Z}/l\mathbb{Z}) \longrightarrow 1 \\
& & & & \parallel \wr & & \parallel \wr \\
& & & & Aut(T_l(E)) & \longrightarrow & Aut(E[l])
\end{array} \quad (1.19)$$

where $GL_2(\mathbb{Z}_l)_1$ is the group of matrices congruent to the identity matrix modulo l, and it is also a pro-l group, since it is isomorphic to the additive group $M_2(l\mathbb{Z}_l)$.

We can put all diagrams together, and fit the map $I_{\varphi} \longrightarrow Aut(T_l(E))$ in the following fashion:

$$\begin{array}{ccccccc}
& & & & I_{\varphi} & & \\
& & & & \downarrow & & \\
& & & & I_{\varphi}^{ab} & & \\
& & & & \parallel \wr & & \\
1 & \longrightarrow & R_{\varphi,1}^* & \longrightarrow & R_{\varphi}^* & \longrightarrow & (R_{\varphi}/M_{\varphi})^* \longrightarrow 1 \\
& & & & \downarrow & & \\
1 & \longrightarrow & GL_2(\mathbb{Z}_l)_1 & \longrightarrow & Aut(T_l(E)) & \longrightarrow & GL_2(\mathbb{Z}/l\mathbb{Z}) \longrightarrow 1
\end{array} \quad (1.20)$$

Next consider the images of $R_{\varphi,1}^*$ and $GL_2(\mathbb{Z}_l)_1$ in $Aut(T_l(E))$ by following diagram (1.20). The images are pro-p and pro-l groups, respectively, and since there can be no non-trivial homomorphism from a pro-p group to a pro-l group ($p \neq l$ by assumption), those groups must have trivial intersection in $Aut(T_l(E))$. But the image of $GL_2(\mathbb{Z}_l)_1$ is $Ker(Aut(T_l(E)) \longrightarrow GL_2(\mathbb{Z}/l\mathbb{Z}))$, therefore there is an injection:

$$Image(R_{\varphi,1}^* \longrightarrow Aut(T_l(E))) \hookrightarrow GL_2(\mathbb{Z}/l\mathbb{Z})$$

and $GL_2(\mathbb{Z}/l\mathbb{Z})$ is obviously finite. But, since also $(R_\varphi/M_\varphi)^*$ is finite, it follows that $Image(R_\varphi^* \rightarrow Aut(T_l(E)))$ is finite (since it consists of finitely many cosets of $Image(R_{\varphi,1}^* \rightarrow Aut(T_l(E)))$).

Hence the image of I_φ in $Aut(T_l(E))$ is finite, so I_φ acts through a finite quotient. Finally, by *Corollary 1* to the Criterion of Néron-Ogg-Shafarevich, E has potential good reduction at φ .

Q.E.D.

Theorem 6 (INTEGRALITY OF THE j-INVARIANT). *Let E/\mathbb{C} be an elliptic curve with complex multiplication. Then $j(E)$ is an algebraic integer, $j(E) \in R_{\mathbf{L}}$, where $\mathbf{L} = \mathbb{Q}(j(E))$.*

Proof. By *Theorem 2*, $j(E)$ is an algebraic number, so we can find a Weierstrass equation for E with coefficients in $\mathbf{L} = \mathbb{Q}(j(E))$.

Theorem 5 says that E has potential good reduction at every prime φ of \mathbf{L} , and *Proposition 3* concludes that $j(E)$ is integral at every prime φ of \mathbf{L} , i.e. $j(E) \in R_\varphi \forall \varphi$. Hence $j(E) \in \bigcap R_\varphi = R_L$.

Q.E.D.

Bibliography

- [1] Joseph H. Silverman, *The Arithmetic of Elliptic Curves*. Springer-Verlag, New York, 1986.
- [2] Joseph H. Silverman, *Advanced Topics in the Arithmetic of Elliptic Curves*. Springer-Verlag, New York, 1994.
- [3] Goro Shimura, *Introduction to the Arithmetic Theory of Automorphic Functions*. Princeton University Press, Princeton, New Jersey, 1971.