ELLIPITIC CURVES WITH COMPLEX MULTIPLICATION

YIFENG HUANG

Abstract. This is a note for the Student Arithmetic learning seminar at the University of Michigan, aimed at presenting the important properties of CM elliptic curves and fixing a gap in the proof of [AEC2, Chapter II, Theorem 4.1]. This note can be used as a supplementary to [AEC2, Chapter II] for readers familiar with the basics of elliptic curves [AEC1, Chapter III] and algebraic number theory.

1. References

(a) [AEC1] Arithmetic of Elliptic Curves by J. Silverman
(b) [AEC2] Advanced Topics in the Arithmetic of Elliptic Curves by J. Silverman
(c) [CFT] Class Field Theory by J. Milne

2. Introduction

Recall div $f$ that for an elliptic curve $E$ over $\mathbb{C}$, the endomorphism group $R = \text{End}(E)$ is either $\mathbb{Z}$ or an order of an imaginary quadratic field. Say $E$ has CM if the latter holds, i.e. the curve has extra “multiplications” apart from multiplication by integers. Focus on the case $R = O_K$ where $K$ is an imaginary quadratic field.

Any elliptic curve over $\mathbb{C}$ is of the form $E_\Lambda := \mathbb{C}/\Lambda$ (analytic picture), where $\Lambda$ is a lattice in $\mathbb{C}$. The equation of $E_\Lambda$ is

$$E_\Lambda : y^2 = 4x^3 - g_2(\Lambda) - g_3(\Lambda)$$

(algebraic picture)

where $g_2, g_3$ are given by infinite series. So it is hard in general to go between analytic and algebraic picture.

Example 2.1. Let $a$ be a fractional ideal of $R = O_K$, then $a$ is a lattice in $\mathbb{C}$. Consider $E = \mathbb{C}/a$, then $\text{End}(E) = \{\alpha \in \mathbb{C} : \alpha a \subseteq a\}$ (true for any lattice). Multiply by $a^{-1}$ at both sides, we get $\alpha \in R$,
so \( \text{End}(E) = R \). Any \( \alpha \in R \) gives a canonical “multiplication-by-\( \alpha \)” endomorphism
\[
[\alpha] : \mathbb{C}/a \rightarrow \mathbb{C}/a
\]
\[
z \mapsto \alpha z
\]
For the invariant differential \( \omega = dz \), we have
\[
[\alpha]^* (dz) = d([\alpha] \circ z) = d(\alpha z) = \alpha dz
\]
So \( [\alpha]^* \omega = \alpha \omega \) (\( * \)).

Note that the multiplication map by \( \alpha \) is constructed analytically. However, \( * \) gives a purely algebraic characterization of the action of \( R \) on \( E \): for an abstract CM curve \( E \) by \( R \) and \( \alpha \in R \), the normalized multiplication-by-\( \alpha \) map is the unique endomorphism \([\alpha]\) of \( E \) such that \( * \) holds for one (and all) invariant differential \( \omega \in \Gamma(E, \Omega^1_{E/\mathbb{C}}) \). Normalized multiplication commutes with isogeny (the proof is formal using \( * \)).

**Example 2.2.** Consider \( E : y^2 = x^3 + 1, \ j = 0 \). It has an endomorphism
\[
\rho : (x, y) \mapsto (\zeta_3 x, y)
\]
Check: \((\zeta_3 x)^3 + 1 = x^3 + 1 = y^2\)
Is it an integer multiplication? Look at the effect of \( \rho \) on invariant differential \( \omega = \frac{dx}{y} \)
\[
\rho^* \frac{dx}{y} = \frac{d(x \circ \rho)}{y \circ \rho} = \frac{d(\zeta_3 x)}{y} = \zeta_3 \frac{dx}{y}
\]
Thus \( \rho \) is the multiplication map by \( \zeta_3 \), and in particular it is complex! Thus the endomorphism ring of \( E \) contains \( \mathbb{Z}[\zeta_3] \), which is already a maximal order of \( \mathbb{Q}(\sqrt{-3}) \), so \( \text{End}(E) \) is exactly \( R = \mathbb{Z}[\zeta_3] \).
Upshot: I computed the endomorphism ring and give the normalized multiplication map without rewriting \( E \) analytically.

**Example 2.3.** \( E : y^2 = x^3 + x, j = 1728, \ \rho(x, y) = (-x, iy). \)
\[
\rho^* \frac{dx}{y} = \frac{d(-x)}{iy} = i \frac{dx}{y}
\]

**Proposition 2.4.** Any CM curve by \( R = \mathcal{O}_K \) is isomorphic to \( \mathbb{C}/a \) for some fractional ideal \( a \) of \( K \).

**Proof.** WLOG \( E = \mathbb{C}/\Lambda, \ \Lambda = \mathbb{Z} \oplus \mathbb{Z} \tau, \ \tau \in \mathbb{C} - \mathbb{R} \). Choose \( \alpha \in R - \mathbb{Z} \), then
\[
\alpha \Lambda \subseteq \Lambda \implies \alpha \tau \in \Lambda \implies \alpha \tau = a + b \tau, a, b \in \mathbb{Z} \implies \tau = \frac{a}{\alpha - b}
\]
Note that $\alpha - b \neq 0$ since $\alpha \notin \mathbb{Z}$. So $\tau \in K$, and $\Lambda$ is itself a fractional ideal of $K$.

Upshot: the number of isomorphic classes of CM curves by $R$ is finite. In fact it equals to $h_K = \text{class number of } K$.

Corollary 2.5. If $E$ has CM, then the $j$-invariant $j(E) \in \overline{\mathbb{Q}}$. Moreover, $[\mathbb{Q}(j(E)) : \mathbb{Q}] \leq h_K$. (In fact we will show that equality holds.)

Proof. Recall for an elliptic curve $E : y^2 = x^3 + Ax + B$, the $j$-invariant is $j = \frac{1728}{4A^3 + 27B^2}$, and two elliptic curves defined over any algebraically closed field $L$ are isomorphic over $L$ iff they have the same $j$-invariant.

Now consider an arbitrary field automorphism $\sigma \in \text{Aut}(\mathbb{C})$. For an elliptic curve $E : y^2 = x^3 + Ax + B$, consider $E^\sigma : y^2 = x^3 + \sigma(A)x + \sigma(B)$. We have an isomorphism $\text{End}(E) \to \text{End}(E^\sigma) : f \mapsto f^\sigma$, so $\text{End}(E^\sigma) = R$. By finiteness result, the isomorphic classes of $\text{End}(E^\sigma)$ have at most $h_K$ choices. Note $\sigma(j(E)) = j(E^\sigma)$ because it is a rational function of $A, B$ with rational coefficient. So $\sigma(j(E))$ has at most $h_K$ choices.

For example, if $K = \mathbb{Q}(\sqrt{-163})$, then $h_K = 1$, so $j(C/O_K)$ is rational. In fact it will be an integer (see the last section).

Remark 2.6. I concluded the finiteness using analytic picture, but I applied this result in algebraic picture.

Upshot: when studying CM curves, can assume they are all defined on a number field $L$. Moreover, given two elliptic curves $E_1, E_2$ defined over $L$, any given isogeny $E_1 \to E_2$ is defined over a finite field extension of $L$ (since isogeny is given by a rational formula, which involves only finitely many coefficients). As $\text{Hom}(E_1, E_2)$ is finitely generated, we can enlarge $L$ to make every isogeny $E_1 \to E_2$ defined over $L$.

3. Analytic action vs Algebraic action

Let $\mathcal{E}_{\ell}(R) = \{ \mathbb{C}\text{-isomorphic classes of CM curves by } R \}$.

We have $\mathcal{E}_{\ell}(R)$ consists of elliptic curves $E_\Lambda = \mathbb{C}/\Lambda$ such that $\alpha \Lambda \subseteq \Lambda$ iff $\alpha \in R$. Note that $\Lambda$ is determined up to $\mathbb{C}^*$ scaling.

Equip $\mathcal{E}_{\ell}(R)$ with $\mathcal{C}_\ell(K)$ action

$$\bar{a} \ast E_\Lambda = E_{a^{-1} \Lambda}$$

Since $\Lambda$ is determined up to $\mathbb{C}^*$, the choice of $\Lambda$ does not matter. Also principal ideals act on $\Lambda$ by scaling, so the action is well-defined on the
class group. Finally, \( \text{End}(E_{a^{-1} \Lambda}) = R \) as well: \( \alpha a^{-1} \Lambda \subseteq a^{-1} \Lambda \implies \alpha \Lambda \subseteq \Lambda \) by multiplying by \( a \) at both sides.

Since every EC with CM by \( R \) has the form \( \mathbb{C}/a \), \( a \) a fractional ideal, we have

**Proposition 3.1.** There is an isomorphism of \( \mathcal{C}(K) \)-sets

\[
\mathcal{C}(K) \to \mathcal{E}(R)
\]

\( \bar{a} \mapsto \mathbb{C}/a^{-1} \)

In other words, \( \mathcal{C}(K) \) acts on \( \mathcal{E}(R) \) freely and transitively. To write down this action for an abstract elliptic curve, we need its analytic picture.

Recall from the proof of rationality that \( \text{Aut}(\mathbb{C}) \) also acts on \( \mathcal{E}(R) \). To write down this action for an abstract elliptic curve, we need to find its equation (algebraic picture).

**Proposition 3.2.** Let \( \bar{a} \in \mathcal{C}(K), \sigma \in \text{Aut}(\mathbb{C}), E \in \mathcal{E}(R) \). Then

\[
(\bar{a} \ast E)^\sigma = \sigma(\bar{a}) \ast E^\sigma
\]

(Note \( \sigma(\bar{a}) \) is in \( \sigma(K) \), which is \( K \) since \( K \) is normal over \( \mathbb{Q} \).)

This statement sounds vacuous, but it is not trivial. Start with an abstract elliptic curve \( E \in \mathcal{E}(R) \), to check the statement, compute

LHS: Find a lattice for \( E \), compute \( \bar{a} \ast E \), find the equation, apply \( \sigma \) to its coefficients, get an algebraic representation;

RHS: Find an equation for \( E \), apply \( \sigma \) to coefficients, find the lattice, apply \( \sigma(\bar{a}) \) action, get an analytic representation

and finally compare the algebraic picture in LHS and analytic picture in RHS.

**Proof.** The key is to find an algebraic description of the analytic action.

Claim: \( \bar{a} \ast E = \text{Hom}_R(\bar{a}, E) \). Write \( E = \mathbb{C}/\Lambda \). Recall that \( a \) is an invertible sheaf over \( R \), thus

\[
\text{Hom}_R(\bar{a}, E) = a^{-1} \otimes_R \mathbb{C}/\Lambda = a^{-1} \otimes_R \mathbb{C}/a^{-1} \Lambda
\]

Now \( \mathbb{C} \) is flat over \( K \) flat over \( R \), so the \( \mathbb{C} \) vector space \( a^{-1} \otimes_R \mathbb{C} \hookrightarrow K \otimes_R \mathbb{C} = K \otimes_K \mathbb{C} = \mathbb{C} \). Thus \( a^{-1} \otimes_R \mathbb{C} \cong \mathbb{C} \), and

\[
\text{Hom}_R(\bar{a}, E) = \mathbb{C}/a^{-1} \Lambda = \bar{a} \ast E
\]

Now fix a finite presentation of \( \bar{a} \) as \( R \)-module:

\[
R^n \xrightarrow{A} R^n \to \bar{a} \to 0
\]

Apply \( \text{Hom}_R(-, E) \), we get

\[
0 \to \text{Hom}_R(\bar{a}, E) \to \text{Hom}_R(R^m, E) = E^n \xrightarrow{A^t} \text{Hom}_R(R^n, E)
\]
Therefore
\[ \bar{a} \ast E \cong \ker(E^n \xrightarrow{A^T} E^m), \]
the kernel of a homomorphism of abelian varieties.

Now everything is algebraic, so it is routine to check that everything
commutes with field automorphisms of \( \mathbb{C} \). \( \square \)

**Corollary 3.3.** The subgroup \( \text{Aut}(\mathbb{C}/K) \) acts on \( \mathcal{E}_\ell \ell(R) \) as a \( \mathcal{C}_\ell(K) \)-sets.

**Proof.** When \( \sigma \) fixes \( K \), \( (\bar{a} \ast E)^\sigma = \sigma(\bar{a}) \ast E^\sigma = \bar{a} \ast E^\sigma. \) \( \square \)

Hence from now on, we only study the action of \( \text{Aut}(\mathbb{C}/K) \) (instead of the whole \( \text{Aut}(\mathbb{C}/\mathbb{Q}) \)) on \( \mathcal{E}_\ell \ell(R) \). We have a striking formula to compute the analytic action in terms of algebraic action:

Let \( E, \bar{a} \) be as above, and \( \sigma \) is any automorphism of \( \mathbb{C} \) that extends the Frobenius element \( (a, K_{nr}/K) \) on the maximal unramified extensions \( K_{nr} \) of \( K \), then
\[ \bar{a} \ast E = E^\sigma. \]

We will give a much stronger form of this statement and prove it using class field theory.

Note the definition of \( E^\sigma \) is independent of the equation: if \( E_1, E_2 \) are two isomorphic models over \( \mathbb{C} \), we have isomorphism \( \varphi : E_1 \to E_2 \), then there is isomorphism \( \varphi^\sigma : E_1^\sigma \to E_2^\sigma \). Therefore, if \( E \) has a model defined over \( L \) (Galois over \( K \)), and \( \sigma \) fixes \( L \), then \( E^\sigma = E \). We get

**Proposition 3.4.** If \( L \) is a Galois extension of \( K \) that contains \( j(E) \), then the algebraic action factors through
\[ F : \text{Gal}(L/K) \to \text{Aut}_{\mathcal{C}_\ell(K)} \mathcal{E}_\ell \ell(R) \cong \mathcal{C}_\ell(K) \]

Since RHS is abelian, it further factors through
\[ F : \text{Gal}(L_{ab}/K) \to \mathcal{C}_\ell(K) \]
where \( L_{ab} \) is the maximal abelian subextension of \( L/K \).

From now on, we can talk about \( E^\sigma \) for \( \sigma \in \text{Gal}(L/K) \) where \( L \) is as above.

### 4. Hilbert Class Field

**Theorem 4.1** (Main Theorem, AEC2 II.4.1). Define \( H = K(j(E)) \) where \( E \in \mathcal{E}_\ell \ell(R) \). Then \( H \) is Galois, abelian and unramified over \( K \) (so the Frobenius map \( \text{I} \to \text{Gal}(H/K), a \mapsto (a, H/K) \) is defined) and we have
\[ \bar{a} \ast E = E^{(a,H/K)} \] \((*)\)
Moreover $H$ is the maximal abelian unramified extension over $K$, i.e. the Hilbert class field of $K$. In particular $[K(j(E)) : K] = [H : K] = h_K$.

**Remark 4.2.** This explains the $a^{-1}$ in the definition of analytic action.

We start with proving (*) for a density one set of primes in $K$, then use Dirichlet theorem saying that every ideal class contains a prime in the set. The following relation between analytic and algebraic actions is the starting point of class field theory of CM curves.

**Theorem 4.3** (Key Lemma, AEC2 II.4.2). For all but finitely degree one primes $p$ in $K$, we have

$$\overline{p} \ast E = E^{\sigma_p}$$

where $E$ is any elliptic curve in $\mathcal{E}(\mathcal{O}_K)$, and $\sigma_p$ is the Frobenius element of $p$ (which has ambiguity that does not matter).

**Proof.** Idea: For elliptic curves $E_1, E_2$ over a finite field of characteristic $p$, any nonseparable map $E_1 \rightarrow E_2$ of degree $p$ is the Frobenius map $E_1 \rightarrow E_1^{(p)}$ up to automorphism. But degree and nonseparability can be obtained from analytic picture.

Now pick a finite Galois field extension $L/K$ and a model $E_i$ over $L$ for each isomorphic class in $\mathcal{E}(\mathcal{O}_K)$, and assume that all isogenies between these $E_i$’s are defined over $L$. Define $\varphi : E \rightarrow \overline{p} \ast E$ analytically by $E/\Lambda \rightarrow E/p\Lambda, z \mapsto z$. Let $\mathfrak{P}$ is a prime of $L$ lying over $p$. For $p$ large enough, $p$ is unramified in $L$ and all $E_i$ have good reduction mod $\mathfrak{P}$.

**Claim:** the mod-$\mathfrak{P}$ reduction $\overline{\varphi} : \overline{E} \rightarrow \overline{\mathfrak{p} \ast E}$ has degree $p$ and is nonseparable, so it is essentially the Frobenius.

Given the claim,

$$\overline{p} \ast E \cong \overline{E}^{(p)}$$

and

$$j(\overline{p} \ast E) = j(\overline{E})^p$$

Now $E^{\sigma_p}$ only depends on $\sigma_p|L_{ab}$, which has no ambiguity since $L_{ab}$ is abelian and unramified at $p$ over $K$. So we can as well choose $\sigma_p = (\mathfrak{P}, L/K)$, and

$$j(\overline{p} \ast E) \equiv j(E)^p \equiv j(E^{\sigma_p}) \mod \mathfrak{P}$$

If we pick $p$ large enough so that $\{j(E) \mod \mathfrak{P} : E \in \mathcal{E}( \mathcal{O}_K)\}$ has no repetition, we conclude that $\overline{p} \ast E = E^{\sigma_p}$.

To prove the claim, we need two facts:
(a) For fractional ideals \( a \subseteq b \) and \( c \), we have \((bc : ac) = (b : a)\).

For a proof, note \( ab \cong a \otimes_R b \) as \( R \)-modules, so
\[
\frac{bc}{ac} = \frac{b}{a} \otimes_R \frac{c}{a}
\]
Since \( c \) is an invertible sheaf over \( R \), tensoring with \( c \) does not change the stalks. As \( \frac{b}{a} \) is supported at finitely many points,
\[
\frac{b}{a} \otimes_R c \cong \frac{b}{a} \text{ as } R \text{-modules}.
\](b) For two elliptic curves \( E_1, E_2 \) defined over a local field \( (L, \mathfrak{P}) \) with good reduction, the reduction is functorial:
\[
\begin{array}{ccc}
E_1 & \xrightarrow{\varphi} & E_2 \\
\downarrow & & \downarrow \\
\tilde{E}_1 & \xrightarrow{\tilde{\varphi}} & \tilde{E}_2
\end{array}
\]
Moreover, the degree is preserved: \( \deg \tilde{\varphi} = \deg \varphi \).

For the proof of degree preserving, pick a prime \( \ell \neq \text{char } (L/\mathfrak{P}) \), take Tate modules for the diagram above, we get
\[
\begin{array}{ccc}
T_\ell E_1 & \xrightarrow{\varphi_\ell} & T_\ell E_2 \\
\cong & & \cong \\
T_\ell \tilde{E}_1 & \xrightarrow{\tilde{\varphi}_\ell} & T_\ell \tilde{E}_2
\end{array}
\]
Thus \( \deg \varphi = \det \phi_\ell = \det \tilde{\varphi}_\ell = \deg \tilde{\varphi}_\ell \).

Now write \( E = C/a \) for a fractional ideal \( a \) of \( K \), and consider
\[
E = C/a \xrightarrow{\varphi_\ell} C/p^{-1}a \xrightarrow{\varphi_\ell} E
\]
where \( \alpha \in p \).

Check: Well-defined, and find the kernel and degree. (\( \deg \varphi = Np = p \) since \( p \) is a degree one prime over \( \mathbb{Q} \).)

The composition is \([\alpha]\), so after reduction mod \( \mathfrak{P} \), we have
\[
[\alpha]^* \omega = [\alpha]^* \omega = \tilde{\alpha} \omega = 0
\]
since \( \alpha \in p \subseteq \mathfrak{P} \). So \([\alpha]\) is not separable.

Write \( b = \alpha p^{-1} \), an integral ideal. Choose \( \alpha \) such that \( b \) is coprime to \( b \). Hence the second map, having degree \( N\alpha \), is separable, so \( \tilde{\varphi} \) is not separable.
Proof of Main Theorem. Write $H = K(j(E))$. Recall the action $F : \text{Gal}(\overline{K}/K) \to \mathcal{C}\ell(K)$. Then

$$\ker F = \{\sigma : E^\sigma = E\} = \{\sigma \text{ fixing } j(E)\} = \text{Gal}(\overline{K}/H)$$

In particular $H$ is normal over $K$ and we have $F : \text{Gal}(H/K) \hookrightarrow \mathcal{C}\ell(K)$, so $H$ is abelian over $K$. Claim $F$ is surjective. For any $\alpha \in \mathcal{C}\ell(K)$, we shall construct an element of $\text{Gal}(H/K)$, using Frobenius, that is mapped to $\alpha$. Recall class field theory:

**Theorem 4.4** (Reciprocity law, CFT V.3.5). Let $L/K$ be any abelian extension of number fields, then there is a modulus $m$ (which is just an integral ideal when $K$ is totally complex) such that $L/K$ is unramified outside $m$ and the Artin map $I^m \to \text{Gal}(L/K)$ vanishes at $K_{m,1} = \{(\alpha) : \alpha \equiv 1 \mod m\}$. Here $I^m$ is the group of fractional ideals coprime to $m$. Moreover, there is a smallest such $m$, called the conductor of $L/K$.

Back to the proof of of the main theorem. Now let $m$ be the conductor of $H/K$. By moving lemma, we can assume $a$ is coprime to $m$. By Dirichlet theorem, every ray class (cosets of $K_{m,1}$ in $I^m$) contains a positive density of primes. Since only degree one primes contribute to density, every ray class contains infinitely many degree one primes, and we may pick one $p$ as in Key Lemma that has the same ray class as $a$. By the definition of $m$, $(a, H/K) = (p, H/K)$, thus

$$F(a, H/K) = F(p, H/K) = \overline{p} = \overline{a}$$

finishing the proof of surjectivity and (*) for certain choice of representative $a$. Thus we have $F : \text{Gal}(H/K) \cong \mathcal{C}\ell(K)$ and $[H : K] = h_K$.

More importantly, we have a commutative diagram

$$\begin{array}{ccc}
I^m & \xrightarrow{\sim} & \mathcal{C}\ell(K) \\
\downarrow (-,H/K) & & \downarrow F \\
\text{Gal}(H/K) & & \\
\end{array}$$

Since the Hilbert class field of $K$ also has degree $h_K$, it suffices to show that $H$ contains in it, that is, $H$ is unramified over $K$. Silverman says that for any $\alpha \in K^*$, $(\alpha, H) = F^{-1}(\overline{\alpha}) = 1$, so the Artin map vanishes at $K_{m,1}$ even when $m = (1)$, thus the conductor has to be $(1)$. But we don’t know $H/K$ is unramified yet, so the argument is cyclic (as the conductor is smallest $m$ divided by all ramified primes such that Artin map vanishes on $K_{m,1}$). **How to fix Silverman’s gap?** Tell me if you have a direct way, but I came up with a solution to get around this:
Let $K^h$ be the Hilbert class field of $K$, then we have an isomorphism $\mathcal{C} \ell(K) \to \text{Gal}(K^h/K)$ given by Artin map. Thus we have

\[
\begin{array}{ccc}
I^m & \xrightarrow{\cong} & \mathcal{C} \ell(K) \\
\downarrow & & \downarrow \\
(-,K^h/K) & \cong & \text{Gal}(K^h/K)
\end{array}
\]

Combining the two diagrams above, we get

\[
\begin{array}{ccc}
I^m & \xrightarrow{(-,H/K)} & \text{Gal}(H/K) \\
\downarrow & & \downarrow \\
(-,K^h/K) & \cong & \text{Gal}(K^h/K)
\end{array}
\]

Since $K^h, H$ are both unramified outside $m$, so is $HK^h$ and we can insert $\text{Gal}(HK^h/K)$ into the diagram:

\[
\begin{array}{ccc}
I^m & \xrightarrow{(-,HK^h/K)} & \text{Gal}(HK^h/K) \\
\downarrow & & \downarrow \\
(-,H/K) & \xrightarrow{\pi_H} & \text{Gal}(H/K) \\
\downarrow & & \downarrow \\
(-,K^h/K) & \xrightarrow{\pi_{K^h}} & \text{Gal}(K^h/K) \\
\end{array}
\]

The top left and bottom left triangles commute because they are all Artin maps. By previous diagram, the outer triangle commutes, i.e. $q \circ (-,H/K) = (-,K^h/K)$. Now we have $q \circ \pi_H \circ (-,HK^h/K) = \pi_{K^h} \circ (-,HK^h/K)$. Class field theory says Artin map $(-,HK^h)$ is surjective, so we can cancel $(-,HK^h/K)$ and the right hand side triangle commutes! As $q$ is an isomorphism,

$$\ker \pi_H = \ker \pi_{K^h}$$

and thus

$$\text{Gal}(HK^h/H) = \text{Gal}(HK^h/K^h)$$

as subgroups of $\text{Gal}(HK^h/K)$. Hence $H = K^h$ is the Hilbert class field of $K$. □
5. Maximal Abelian Extension

See [AEC2, Chapter II, §5], especially Corollary 5.7

Quick summary:

<table>
<thead>
<tr>
<th>Cyclomotic Theory</th>
<th>CM theory</th>
</tr>
</thead>
<tbody>
<tr>
<td>(\mathbb{G}_m(\mathbb{C}))</td>
<td>(E(\mathbb{C}))</td>
</tr>
<tr>
<td>(\text{End} = \mathbb{Z}), study the field (\mathbb{Q})</td>
<td>(\text{End} = \mathcal{O}_K), study the field (K)</td>
</tr>
<tr>
<td>(\mathbb{Q}^{ab} = \mathbb{Q}(\zeta_n) = \mathbb{Q}(\mathbb{G}<em>m(\mathbb{C})</em>{\text{tor}}))</td>
<td>(K^{ab} = K(j(E), h(E_{\text{tor}})))</td>
</tr>
</tbody>
</table>

Here \(h(x, y) = x\) in usual except \(h(x, y) = x^2\) when \(j = 1728\) and \(h(x, y) = x^3\) when \(j = 0\). The key property is that \(h\) must commute with automorphisms of \(E\) and for these special \(j\)'s, \(E\) has more symmetry.

6. Integrality of \(j\)

See [AEC2, II.6.4]. The proof uses local class field theory, Neron–Ogg–Shafaverich criterion, and the fact that having potential good reduction implies \(j\)-invariant is integral.

Application:

Now there are nine integers (Heegner numbers) \(n\) such that \(\mathbb{Q}(\sqrt{-n})\) has class number one. The largest three are \(n = 43, 67, 163\), all having \(n \equiv 3 \mod 4\). Now \(j(\mathcal{O}_{\mathbb{Q}(\sqrt{-n})})\) is integer for \(n = 43, 67, 163\). On the other hand,

\[
j = \frac{1}{q} + 744 + 196884q + \cdots
\]

where \(q = \exp(2\pi i \tau)\).

Let \(\tau = \frac{1 + \sqrt{n}i}{2}\), then \(q = \exp(\pi i - \pi \sqrt{n}) = -\exp(-\pi \sqrt{n})\), which is a negative number very close to 0.

Thus \(j \approx \frac{1}{q} + 744\), so \(1/q = -\exp(\pi \sqrt{n})\) is almost an integer.