0.1 The Complex Lattice

Theorem 1 *Let ω_1, ω_2 be linearly independent points in C. Then define the lattice*

$$L = Z\omega_1 + Z\omega_2$$

Then there exists an elliptic curve that is isomorphic to $\mathbb{C}/L$.

Define $G_k(L) = \sum_{\omega \in L} \omega^{-k}$. Then define the Weierstrass $\wp(z)$ function as follows:

$$\wp(z) = \frac{1}{z^2} + \sum_{\omega \in L} \left(\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2} \right) \tag{1}$$

Then this function can easily be shown, by applications of complex analysis, to be convergent and meromorphic, as well as periodic. Then the derivative $\wp(z)$ is

$$\wp'(z) = -2 \sum_{\omega \in L} \frac{1}{(z-\omega)^2} \tag{2}$$

Now we have a isomorphism from the additive group on $\mathbb{C}/L$ to the the group of elliptic points on $E(\mathbb{C})$, by the map

$$z \to (\wp(z), \wp'(z)), \quad 0 \to O$$

with E being defined as

$$E : y^2 = 4x^3 - g_2 x - g_3 \tag{3}$$

where $g_2 = 60G_4, g_3 = 140G_6$ Note that the periodicity will give:

$$(\wp(z_1), \wp'(z_1)) \oplus (\wp(z_2), \wp'(z_2)) = (\wp(z_1 + z_2), \wp'(z_1 + z_2)) \tag{4}$$

which gives rise to the corresponding group law on elliptic curves.

Now we relate the j-invariant on curves to the $j-$function of a complex lattice. First, let rescale our lattice L to $Z\tau + Z$ where $\tau = \frac{w_1}{w_2}$. Then the j-invariant related to the lattice parameter is

$$j(\tau) = 1728 \frac{g_2^3}{g_2^3 - 27g_3^2} \tag{5}$$

The proof of all of this we won't go into detail in this paper, but this gives rise to the relationship between the complex lattice and isogenies, mainly integer endomorphisms $[m]$ give rise to $z \to mz$, and for multiplication by a complex number β, we have $z \to \beta z$, which is defined when $\beta L \in L$. A key theorem is that

$$End(E) \cong \{\beta \in C | \beta L \subseteq L\} \tag{6}$$

This can be proved by taking the limit of the action of the endomorphism by approaching a lattice point in [WASH08].

For curves defined on a field K, there is a homomorphism $K \to C$ if we linearly map the finite basis elements of K, $\alpha_1, ..., \alpha_n$ respectively to any algebraically independent set of elements in $\mathbb{C}$, $\tau_1, ..., \tau_n$, so we can regard $E(K)$ as a curve in $\mathbb{C}$.

0.1.1 Using Quadratic Lattices

Theorem 2 *The elements β in the endomorphism ring are algebraic integers that lie in some quadratic field.*

Proof: Note that by the theorem in (6), there exist integers a, b, c, d such that

$$\beta\omega_1 = a\omega_1 + b\omega_2 \qquad \beta\omega_2 = c\omega_1 + d\omega_2 \tag{7}$$

Since this becomes a linear transformation, we can re-write β in a qudratic, i.e.

$$\beta^2 - \beta(a + d) + (ad - bc) = 0 \tag{8}$$

which implies β is an quadratic algebraic integer. □

Such quadratic fields are defined by $Z[\delta]$, of the forms $Z[\frac{1+\sqrt{-D}}{2}]$ if $D \equiv 3 \mod 4$ or $Z[\sqrt{-D}]$ if $D \equiv 1, 2 \mod 4$ where D is squarefree.

Definition: An *order* in an imaginary qudratic field is a ring R that is contained in the field, which will have have the form $Z[f\delta]$.

It is then proved that all such β are in the same order of some quadratic field in [WASH08], or in other words, elliptic curves in $\mathbb{C}$ have endomorphism rings isomorphic to R in some quadratic field.

Now to construct a curve of size N in $\mathbb{F}_p$, we have that $t = p + 1 - N$ due to Hasse's theorem, and find D to be square-free part of $t^2 - 4p$. We will then find an integer polynomial $H_D(x)$ such that the roots will be j-invariants of curves with complex multiplication defined in the actual quadratic field. To do so requires taking Galois conjugates of elements in the field, depicted in [WASH08]. The algorithm is defined in section 3.