Weil Pairings on Elliptic Curves

Jose Capco

2003

Contents

Abstract

The main purpose of this thesis is the study of Weil-Pairing on elliptic curves over the complex field. Weil-Pairing has become of particular interest since the development of elliptic curve cryptosystems. For example, it can be used to solve elliptic curve logarithm problems. And it allows us to determine particular elliptic curve cryptosystems that may be insecure towards attacks, thus enabling us to avoid those systems in application. This is however not tackled here, we concentrate here mainly on the theories and properties of Weil-Pairing on elliptic curves over the complex field. In the last section we will be able to develop a formula that makes the computation of Weil-Pairing in the complex field very easy. Thus the last few theorems involved in the last section is the main part of this thesis. The thesis is quite self-contained for the reader who has minimal or even no knowledge about function theory or elliptic curves. The first section involves the basic definitions and properties about elliptic curves, it can be used to motivate the reader who is not familiar, or who has to recall the concepts of elliptic curves. The next section deals with the necessary tools needed from function theory, mostly about the elliptic functions and in particular the Weierstraß $\wp$-function. The section after this involves divisor theories that are proven in the complex field, however most of them may be applied as well in other algebraically closed fields. This section begins to deal with theories needed from algebraic geometry. The last but not least section is the section that concludes the thesis and gives the main theory of the thesis. It involves definition and study of the Weil- Pairing in the complex fields (and in some cases of other algebraically closed fields) using the concepts provided in the former sections.

1 Preliminary Topics

Notation. Throughout this paper, for any group G, by G^* we mean the set $G\backslash\{e\}$, where e is the identity element of the group. In case G is a field (or a ring with unity), e will be the zero element of G. And unless otherwise stated we use the symbol K to denote an algebraically closed field. Unless otherwise stated we use fields K of characteristic not equal to 2 or 3.

Definition. For a field K the *projective plane* is defined by $\mathbb{P}(K) = (K^3)^*/\sim$ where

$$(x_o, x_1, x_2) \sim (y_o, y_1, y_2) \Leftrightarrow \exists \lambda \in K^* \ni x_i = \lambda y_i \quad i = 1, 2$$

We denote the equivalence class of $(x_o, x_1, x_2) \in (K^3)^*$ by $(x_o : x_1 : x_2)$

Definition. $F(x, y, z) \in K[x, y, z]$ is called a *homogenous polynomial of degree d* if it can be expressed as

$$F(x, y, z) = \sum_{k+l+m=d} c_{klm} x^k y^l z^m$$

For some $d \in \mathbb{Z}$. For brevity we sometimes simply call $F(x, y, z)$ *homogenous.*

Remark. If (x_o, x_1, x_2) is a zero of a homogenous polynomial, then it is easy to see that all of the elements belonging to the class $(x_o : x_1 : x_2)$ is a zero of F. So we may say $(x_o : x_1 : x_2)$ solves the homogenous equation $F(x, y, z) = 0$.

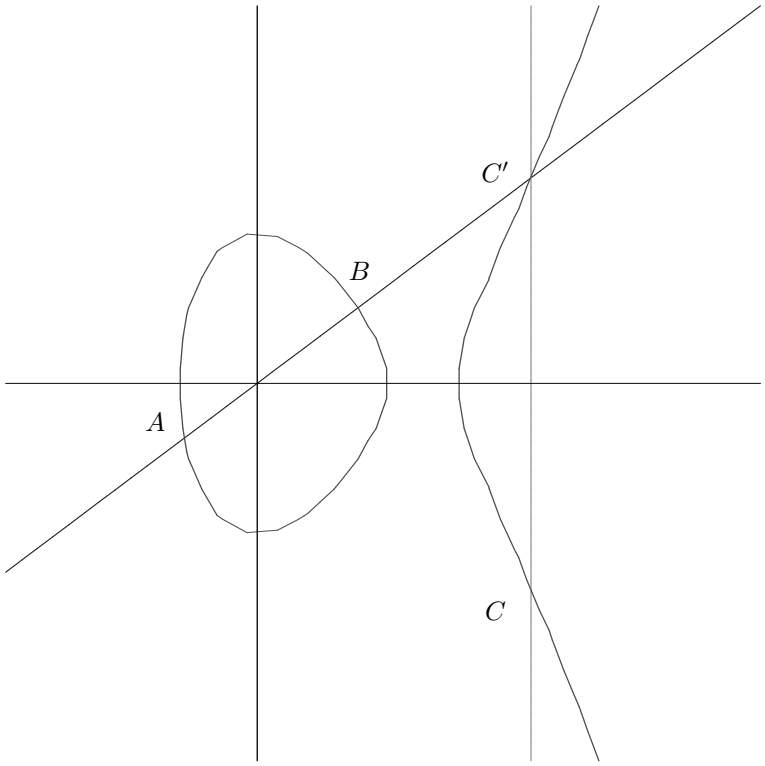
Definition. Given a field K whose characteristic is not 2 or 3 and a homogenous polynomial $F(x, y, z) = zy^2 - x^3 - az^2x - bz^3$, where $a, b \in K$ satisfy the equation $4a^3 + 27b^2 \neq 0$. The *elliptic curve* consists of the points in the projective plane that solves the homogenous equation $F(x, y, z) = 0$. We see that the only point in the elliptic curve that has the form $(\alpha : \beta : 0)$ is $(0 : 1 : 0)$ and we call this point *the point of infinity* of the elliptic curve (this is because we want to reduce the points in the elliptic curve to two coordinate points belongs to the affine plane (this is the plane formed when a "line" consisting of the points $(\alpha : \beta : 0)$ is removed from the projective plane)). Other points of the elliptic curve consists of the points of the form $(\alpha : \beta : 1)$ Points of this form we write shortly as (α, β). And we may therefore redefine the elliptic curve as the points in K^2 satisfying $f(x, y) = F(x, y, 1) = y^2 - x^3 - ax - b = 0$ and a point not in K^2 which we call the *point of infinity* and represent it as $\mathcal{O}$. We denote the elliptic curve by the symbol E and we say that the elliptic curve is defined by $E : f(x, y) = 0$. We notate the points in the elliptic curve by capital letters, and the coordinate pointy by "point notations", like $P = (x_P, y_P)$.

Remark. The elliptic curves can also be defined on fields of characteristic 2 and 3. However we will not go into this topic. It is however interesting to know that the elliptic curve on fields of characteristic 2 (which is very much used in applications) must be defined on the points in the affine plane that solve $f(x, y) = y^2 + a_3y - x^3 - a_4x - a_6 = 0$, where a_3, a_4 and a_6 are constants in the field by which at least one of the partial derivatives of $F(x, y, z) = z^3 f(\frac{x}{z}, \frac{y}{z})$ (namely $\partial F/\partial x, \partial F/\partial y$ and $\partial F/\partial z$) is nonzero at all points of the projective plane. (or in words of algebraic geometry, the curve has no *point of singularity*, or is *smooth*).

Definition. Let $f(x, y) = y^2 - 4x^3 + g_2x - g_3$ be a polynomial in a field of characteristic other than 2 or 3, where g_2 and g_3 are constants in the field, and suppose that an elliptic curve is defined by $E : f(x, y/2)/4 = 0$ then we may also write that it is defined by $E : f(x, y) = 0$ and we say that the polynomial $f(x, y) = y^2 - 4x^3 - g_2x - g_3$ is expressed in *Weierstraß form.*

Remark. The above definition makes a little abuse of notations, but the points of the above elliptic curve must satisfy $f(x, y) = y^2 - 4x^3 - g_2x - g_3 = 0$ and a point of infinity $\mathcal{O}$. Of course we must make sure that $g_2^3 - 27g_3^2 \neq 0$ if we want to say that it is an elliptic curve.

Now we will explain how a group can be formed on the elliptic curves. Let A and B be points in the elliptic curve. We will define the *addition* of these two points. First we may do it geometrically.



Supposing the working field is $\mathbb{R}$ (although in most cases we work with algebraically closed field, this field will help us visualize the situation). Connect the points A and B by a line g, if $A = B$ then take g to be the tangent line to the curve (this will be discussed more mathematically later). If g is parallel to the y-axis, then define $A + B = \mathcal{O}$, else g , must intersect another point $C' = (x_C, -y_C)$ in the elliptic curve we then define $A + B = C = (x_C, y_C)$ that is the sum of A and B will be the reflection of the point C' (note: C also belongs to our elliptic curve!). And lastly for any point A in the elliptic curve, define $A + \mathcal{O} = \mathcal{O} + A = A$.
We now proceed to do these in a more analytic way. Let $A = (x_A, y_A)$ and $B = (x_B, y_B)$ be points other than $\mathcal{O}$ in the elliptic curve (otherwise our addition is defined as above). Suppose $x_A \neq x_B$ then we choose (otherwise $\overline{A}B$ is parallel to the $y - axis$ and we can define $A + B = \mathcal{O}$ as above) $g = \overline{AB} = \{(x_g, y_g) : x_g = x_A + t, y_g = y_A + \mu t \quad t \in K\}$ where $\mu = \frac{y_B - y_A}{x_B - x_A}$. If we extend this line (in the affine plane) to the projective plane we see that it does not meet the point of infinity (i,e, the point $(1 : 0 : 0)$), but it will meet another point (other than A or B) in the elliptic curve. To solve the other point let $P_3(x) = x^3 + ax + b$ and consider the equation

$$(y_A + \mu t)^2 = P_3(x_A + t) \quad (1)$$

This equation must have three solutions (because of the condition of the elliptic curve $4a^3+27b^2 \neq 0$ and from algebra we know that this is equivalent to the statement that $P_3(x)$ has no repeating roots) two of which is when $t = 0$ and $t = x_B - x_A$ We write this in terms of power series

$$(y_A + \mu t)^2 = P_3(x_A) + P_3'(x_A)t + \frac{1}{2}P_3''(x_A)t^2 + \frac{1}{6}P_3'''(x_A)t^3$$

(Note: 1/2 and 1/6 don't disturb us, since we have field of characteristic unequal to 2 or 3) If we expand this and noting that $P(x_A) = y_A^2$ we obtain

$$y_A^2 + 2\mu y_A t + \mu^2 t^2 = y_A^2 + (3x_A^2 + a)t + 3x_A t^2 + t^3$$

We consider then $t \neq 0$ and divide the equation by t (since $t = 0$ correspond to point A which we know already).

$$t^2 + (3x_A - \mu^2)t + (3x_A^2 + a - 2\mu y_A) = 0 \quad (2)$$

And the two solutions for this equation are $t = x_B - x_A$ and $t = x_{-C} - x_A$ where x_{-C} is a coordinate term we need to determine. In a quadratic polynomial of one variable the sum of the two roots is equivalent to the negative of the linear coefficient, i.e.

$$(x_B - x_A) + (x_{-C} - x_A) = -(3x_A - \mu^2)$$

Thus $x_{-C} = \mu^2 - x_A - x_B$, is the x-coordinate of the 3rd point by which g meets the elliptic curve. The y-coordinate would then be $y_{-C} = y_A + \mu(x_{-C} - x_A)$. But as described in the geometric definition of group addition we need the reflection of the point $-C = (x_{-C}, y_{-C})$ and that would be $C = A + B = (x_C, y_C)$ where $x_C = \mu^2 - x_A - x_B$ and $y_C = -y_A - \mu(x_C - x_A)$. Suppose now that $A = B$, but $y_A \neq 0$, then we attempt to find the tangent line on the curve at point A (as discussed in the geometric definition). Then (2) has a solution at $t = 0$ iff $3x_A^2 + a - 2\mu y_A = 0$ iff $\mu = \frac{3x_A^2 + a}{2y_A}$. This is in fact the tangent line at point A which by geometry we know to be

$$\mu = -\frac{\partial f(x,y)/\partial x}{\partial f(x,y)/\partial y}_A$$

The rest of the calculations are similar to above.
Now we notice the following, $\mathcal{O}$ clearly acts as the neutral element of the "group". If $A = (x_A, y_A) \in E$ then $-A = (x_A, -y_A) \in E$ and $A + (-A) = (-A) + A = \mathcal{O}$. The "group" is also clearly commutative. The only difficulty is to prove that the associative law holds here. We shall not tackle this, but mention the fact that this can be done rigorously (but less elegantly) or by the use of Bezout Theorem. However since our main work is with the field $\mathbb{C}$ in a later section in corollary 3.2 we will prove that there is a bijective linear transformation between E over field $\mathbb{C}$ and a certain group (by which the group properties are far easier to prove) and thus the associative law on E will follow from that too.

2 Elliptic Functions and Theta Functions

We begin by noting some basic definitions in function theory. Unless otherwise stated, throughout we use a complex number in the upper half complex plane $\tau \in \mathbb{H}$ that forms a lattice $L = \mathbb{Z}\tau + \mathbb{Z}$ in the complex plane. And throughout this chapter, unless otherwise stated, we use the symbol $\mathcal{F} = \{t_1 + t_2\tau : t_1, t_2 \in [0,1)\}$ for the *cell in L with base* 0 sometimes also called the *funamental parallelogram* and $\mathcal{F}_a = \{a + t_1 + t_2\tau : t_1, t_2 \in [0,1)\}$ is the *cell in L with base a*.

Definition. A meromorphic function $f : \mathbb{C} \to \overline{\mathbb{C}}$ that is doubly periodic on L (i.e. $f(1+z) = f(z)$ and $f(\tau + z) = f(z)$ for all $z \in \mathbb{C}$) is called an *elliptic function on L*.

Definition. Two points $z, w \in \mathbb{C}$ are said to be *equivalent* in the lattice L iff $z - w \in L$, we write $z \equiv w \bmod L$

Notation. We denote the set of meromorphic functions defined on $U \subset \mathbb{C}$ with $\mathcal{M}(U)$, and the set of elliptic functions on L by $\mathcal{M}(\mathbb{C}/L)$.

Theorem 2.1. (First Liouville's Theorem) Let $f, g \in \mathcal{M}(\mathbb{C}/L)$, with same poles and zeroes. Set S to be the set of poles and zeroes, If $\forall z \in S$ $\operatorname{ord}(f; z) = \operatorname{ord}(g; z)$ then f and g are equal upto a constant (i.e. $\exists\, \alpha \in \mathbb{C}$ such that $f = \alpha g$). In particular an elliptic function that has no pole is a constant.

Proof. If we prove the second statement then the first statement follows automatically, since f/g is in $\mathcal{M}(\mathbb{C}/L)$ and has no pole. Let $f \in \mathcal{M}(\mathbb{C}/L)$ with no pole and set $\mathcal{F} = \{t_1 + t_2\tau : t_1, t_2 \in (0,1)\}$ (i.e. an open cell of the lattice L). Then since f is periodic within that cell and since it is continous we have $f(\overline{\mathcal{F}})$ is compact and so it is bounded in $\mathbb{C}$. By Liouville's (main) theorem it follows that f is constant. □

Theorem 2.2. (Second Liouville's Theorem) Let $f \in \mathcal{M}(\mathbb{C}/L)$ then

$$\sum_{p\in\mathcal{F}} \operatorname{Res}(f;p) = 0$$

Proof. Using residue theorem

$$2\pi i \sum_{p\in\mathcal{F}} \operatorname{Res}(f;p) = \int_{\partial\mathcal{F}} f(z)dz = \int_0^1 f(t)dt + \int_0^1 f(1+t\tau)\tau dt - \int_0^1 f(1+\tau-t)dt - \int_0^1 f(\tau-t\tau)\tau dt$$

But because f has perioids 1 and τ we can easily see that the sum will vanish. □

Theorem 2.3. (Third Liouville's Theorem) Every elliptic function has as many zeroes as poles, when counting each zero and pole by its multiplicity. i.e.

$$\forall f \in \mathcal{M}(\mathbb{C}/L) \qquad \sum_{z\in f^{-1}(0)\cap\mathcal{F}} \mu(f;z) = \sum_{z\in f^{-1}(\infty)\cap\mathcal{F}} \mu(f;z)$$

Proof. We see that clearly $f'/f \in \mathcal{M}(\mathbb{C}/L)$, and that

$$\operatorname{Res}(\frac{f'}{f};a) = \begin{cases} \mu(f;a) & f(a)=0 \\ -\mu(f;a) & f(a)=\infty \\ 0 & \text{otherwise} \end{cases}$$

So by Liouville's 2nd Theorem

$$0 = \sum_{a\in\mathcal{F}} \operatorname{Res}(\frac{f'}{f};a) = \sum_{z\in f^{-1}(0)\cap\mathcal{F}} \mu(f;z) - \sum_{z\in f^{-1}(\infty)\cap\mathcal{F}} \mu(f;z)$$

□

Corollary 2.4.

$$\forall f \in \mathcal{M}(\mathbb{C}/L),\, c \in \overline{\mathbb{C}} \qquad \sum_{z\in f^{-1}(c)\cap\mathcal{F}} \mu(f;z) = \sum_{z\in f^{-1}(\infty)\cap\mathcal{F}} \mu(f;z)$$

Proof. Consider $g = f - c$ and use the same methods as in the proof of Liouville's 3rd theorem. □

Definition. The Weierstraß $\wp$-function is $\wp : \mathbb{C} \to \overline{\mathbb{C}}$ defined by

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

Notation. In literature it is common practice to write the Weierstraß $\wp$-function defined on a lattice L (generated by $(1,\tau)$) by $\wp_L(z)$. In case the lattice is known to us we write in short $\wp(z)$.

Proposition 2.5. The *Eisenstein series of "weight"* $k \geq 3$

$$G_k(\tau) = \sum_{(c,d)\in\mathbb{Z}^{2*}} (c+d\tau)^{-k} \quad (k \geq 3, \tau \in \mathbb{H})$$

converges absolutely and defines an analytic function $G_k : \mathbb{H} \to \overline{\mathbb{C}}$ over the upper halfplane.

Proof. If we show for $k \geq 3$, $G_k : \mathbb{H} \to \overline{\mathbb{C}}$ has a sum representation that is normally convergent with respect to $\mathbb{H}$ then we are done. Set $\tau \in \mathbb{H}$ fixed, and consider the ball $U = B(\tau, \epsilon)$ where $2\epsilon = \text{dist}(\tau, \partial\mathbb{H})$, then

$$m = \text{dist}(0, (1 + (\tau - i\epsilon)\mathbb{R}) \cup (\mathbb{R} + (\tau - i\epsilon))) > 0$$

We first claim

$$\forall c, d \in \mathbb{Z}, |c + d\tau| \geq m \sup\{|c|, |d|\}$$

For $c = d = 0$ it is trivial. For $d \neq 0$, $|c| \geq |d|$ we have

$$|c + d\tau| = |c| \left|1 + \frac{c}{d}\tau\right| \geq m|c| = m \sup\{|c|, |d|\}$$

Analogously for $|d| > |c|$. And so the claim is proved.
Now set $k \geq 3$ fixed. Let $\alpha = -k$ then

$$\sum_{(c,d)\in\mathbb{Z}^{2*}} |c + d\tau|^\alpha = \sum_{r=1}^{\infty} \sum_{\sup\{|c|,|d|\}=r} |c + d\tau|^\alpha \leq \sum_{r=1}^{\infty} 8r(mr)^\alpha = 8m^\alpha \sum_{r=1}^{\infty} r^{\alpha+1} < \infty$$

The second inequality is because there are $8r$ points by which $\sup\{|c|, |d|\} = r$ and each point is less than or equal to mr by definition of m. Thus we have proven the theorem, since we have found a Weirstraß majorant for another representation of $G_k(\tilde{\tau})$ (i.e. the right hand side of the first equality above) for all $\tilde{\tau} \in U$. □

Definition. Let $S_N = \sum_{n=1}^{N} f_n$ be a partial sum of functions defined on a domain $D \subset \mathbb{C}$

$$f_n : D \to \mathbb{C}, \quad n \in \mathbb{N}$$

then the sum $lim_{N\to\infty} S_N$ is *normally convergent* if for all $z_o \in D$ there exists a neighbourhood U of z_o in D and a sequence $\langle M_n \rangle \subset \mathbb{R}^+\backslash\{0\}$ (that is nonnegative numbers) such that

$$|f_n(z)| \leq M_n \quad \forall z \in U, n \in \mathbb{N} \quad \text{such that } \sum_{n=0}^{\infty} M_n < \infty$$

Corollary 2.6.

$$\sum_{\omega\in M} \left[\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2}\right]$$

converges normally in $\mathbb{C}\backslash L$

Proof. We have

$$\left|\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2}\right| = \frac{|z||z-2\omega|}{|\omega|^2|z-\omega|^2}$$

Let $z_o \in \mathbb{C}\backslash L$ and U be a ball containing z_o of radius ϵ. Set $r = \epsilon + |z_o|$ then we can see that

$$\left|\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2}\right| \leq 12r|\omega|^{-3}$$

for all $z \in U$ and $\omega \in L$ such that $|\omega| \geq 2$ □

Remark 2.7. Therefore the Weierstraß $\wp$-function is a meromorphic function with poles only in the lattice L. Moreover it is easy to see that it is an even function. It is also easy to conclude that its derivative is also an elliptic function. The derivative would be then an odd function. We also further observe that $\wp$ takes all values in $\mathbb{C}$, the function is open in $\overline{\mathbb{C}}$ (it is obviously not a constant) so one must only prove that $\wp(\mathbb{C})$ is closed in $\overline{\mathbb{C}}$ to prove that $\wp$ is surjective on $\mathbb{C}$, but this is easy since one need only consider a sequence in $\overline{\mathcal{F}}$ which is compact and use the continuity of $\wp$ in $\overline{\mathbb{C}}$.

Definition. We define the *discriminant* and the *j-function* respectively by

$$\Delta(\tau) = g_2^3(\tau) - 27g_3^2(\tau) \quad , \quad j(\tau) = g_2^3(\tau)/\Delta(\tau)$$

where $g_2(\tau) = 60G_4(\tau)$ and $g_3(\tau) = 140G_6(\tau)$ for $\tau \in \mathbb{H}$ (see [2]).

Theorem 2.8. Given a lattice $L = \mathbb{Z} + \mathbb{Z}\tau$ the Weierstraß $\wp$-function has the following identity

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

Also

$$2\wp_L''(z) = 12\wp_L(z)^2 - g_2(\tau)$$

Proof. Because $\wp$ is even we can take the Laurent series reperesentation

$$\wp(z) = 1/z^2 + a_2z^2 + a_4z^4 \cdots$$

$a_0 = 0$ because the value of $\wp(z) - 1/z^2$ evaluated at zero will be zero due to the sum

$$\sum_{\omega \in L^*} \left[\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2} \right]$$

Thus $\wp(z) = \frac{1}{z^2} + f(z)$ where $f(z) = \sum_{n=1}^{\infty} a_{2n}z^{2n}$. We can use the Taylor series representation of $f(z)$ to get $a_{2n} = \frac{f^{(2n)}(0)}{(2n)!}$ and using the definition of the Weierstraß $\wp$-function for $n > 1$ we have

$$f^{(n)}(z) = (-1)^n(n+1)! \sum_{\omega \in L^*} \frac{1}{(z-\omega)^{n+2}}$$

We can then conclude that

$$a_{2n} = \frac{(2n+1)!}{(2n)!} \sum_{\omega \in L^*} \frac{1}{\omega^{2(n+1)}}$$

Thus

$$\wp(z) = \frac{1}{z^2} + \sum_{n=1}^{\infty} (2n+1)G_{2(n+1)}z^{2n}$$

Thus we know that

$$\wp(z) = z^{-2} + 3G_4z^2 + 5G_6z^4 + \cdots$$
$$\wp'(z) = -2z^{-3} + 6G_4z + 20G_6z^3 + \cdots$$
$$\wp(z)^2 = z^{-4} + 6G_4 + 10G_6z^2 + \cdots$$
$$\wp(z)^3 = z^{-6} + 9G_4z^{-2} + 15G_6 + \cdots$$
$$\wp'(z)^2 = 4z^{-6} - 24G_4z^{-2} - 80G_6 + \cdots$$

So we have

$$\wp'(z)^2 - 4\wp(z)^3 = -60G_4z^{-2} - 140G_6 + \cdots$$

or if we add $60G_4\wp(z)$

$$\wp'(z)^2 - 4\wp(z)^3 + 60G_4\wp(z) = -140G_6 + \cdots$$

The above is an elliptic function without any poles, therefore it is a constant. The first identity is proved.
After differentialing the identity above we obtain

$$2\wp'(z)\wp''(z) = 12\wp(z)^2\wp'(z) - g_2(\tau)\wp'(z)$$

and thus the other result. □

Notation. For the remaining of this section by $G(z)$ we mean the set $G(z) = (L + z) \cup (L - z)$ for $z \in \mathbb{C}$.

Lemma 2.9. $a \in \mathbb{C}$ is a zero of $\wp'$ iff $a \notin L$ and $2a \in L$

Proof. For the sufficiency condition

$$\wp'(a) = \wp'(a - 2a) = \wp'(-a) = -\wp'(a)$$

and the necessity condition is true because of the third Liouville's theorem, since we know that the order of poles of $\wp$ is 2 we know then that

$$\sum_{z \in \wp^{-1}(0) \cap \mathcal{F}} \mu(f; z) = \mu(\wp'; 0) = 3$$

Thus there are at most 3 zeroes of $\wp'$ in $\mathcal{F}$ with multiplicity 1. And they are indeed those in $\frac{1}{2}L$ □

Lemma 2.10.

$$|\mathcal{F} \cap G(z)| = \begin{cases} 1 & \text{if } z \in \frac{1}{2}L \\ 2 & \text{if otherwise} \end{cases}$$

Proof. We know $\exists! \omega_1 \in \mathcal{F}$ so that $\omega_1 = z \bmod L$ and $\exists! \omega_2 \in \mathcal{F}$ with $\omega_2 = -z \bmod L$ Thus $\mathcal{F} \cap G(z) = \{\omega_1, \omega_2\}$ and

$$|\mathcal{F} \cap G(z)| = 1 \Leftrightarrow \omega_1 = \omega_2 \Leftrightarrow z = -z \bmod L \Leftrightarrow 2z \in L$$

□

Lemma 2.11. Let $f \in \mathcal{M}(\mathbb{C})$ be an even function, $a \in \mathbb{C}$ then $\operatorname{ord}(f; a) = \operatorname{ord}(f; -a)$ and $\operatorname{ord}(f; 0) \in 2\mathbb{Z} \cup \{\infty\}$

Proof. For $f \equiv 0$ the result is trivial. Suppose then that $f \not\equiv 0$ and set $\infty \neq n = \operatorname{ord}(f; a)$. We take the Laurent series representation near a,

$$f(a + \zeta) = \sum_{j=n}^{\infty} c_j \zeta^j$$

$$f(a - \zeta) = f(-a + \zeta) = \sum_{j=n}^{\infty} c_j (-1)^j \zeta^j$$

$\Rightarrow \operatorname{ord}(f; a) = \operatorname{ord}(f; -a)$
For a=0 we get

$$\sum_{j=n}^{\infty} c_j \zeta^j = f(\zeta) = f(-\zeta) = \sum_{j=n}^{\infty} c_j (-1)^j \zeta^j$$

$\Rightarrow 0 \neq c_n = c_n(-1)^n \Rightarrow n \in 2\mathbb{Z}$ □

Lemma 2.12. Let $f \in \mathcal{M}(\mathbb{C}/L)$ be even and let $a \in \mathbb{C}$, then $f(z)$, $\operatorname{ord}(f; z)$ and $\mu(f; z)$ are constant in $G(a)$ and if $a \in \frac{1}{2}L$ then $\operatorname{ord}(f; a) \in 2\mathbb{Z} \cup \{\infty\}$ and $\mu(f; a) \in 2\mathbb{N} \cup \{\infty\}$

Proof. Let $b \in G(a)$ then $b \equiv \pm a \bmod L$. We thus have

$$f(b) = f(\pm a) = f(a) =: c$$

where c is a constant. Also we have by the previous lemma

$$\operatorname{ord}(f; b) = \operatorname{ord}(f; \pm a) = \operatorname{ord}(f; a)$$

Now if $c = \infty$ then

$$\mu(f;b) = |\operatorname{ord}(f;b)| = |\operatorname{ord}(f;a)| = \mu(f;a)$$

and if $c \neq \infty$ then

$$\mu(f;b) = \operatorname{ord}(f-c;b) = \operatorname{ord}(f-c;a) = \mu(f;a)$$

Let $a \in \frac{1}{2}L \Rightarrow 2a \in L$. Thus for the function $g(z) := f(z-a)$ we have

$$g(z) = f(z-a) = f(z-a+2a) = f(z+a) = g(-z)$$

$\Rightarrow g$ is even $\Rightarrow$ by the preceding lemma $\operatorname{ord}(f;a) = \operatorname{ord}(g;0) \in 2\mathbb{Z} \cup \{\infty\}$. Since $\mu(f;a) = |\operatorname{ord}(f-c_o;a)|$, where c_o is the constant term in the Laurent series representation of f, the last result $\mu(f;a) \in 2\mathbb{N} \cup \{\infty\}$ is also clear. □

Theorem 2.13.

$$\wp'(z)^2 = 4(\wp(z)-e_1)(\wp(z)-e_2)(\wp(z)-e_3)$$

Where $e_1 = \wp(\frac{1}{2})$, $e_3 = \wp(\frac{\tau}{2})$ and $e_3 = \wp(\frac{1+\tau}{2})$. Moreover the values of $\wp(\frac{1}{2})$, $\wp(\frac{\tau}{2})$ and $\wp(\frac{1+\tau}{2})$ are distinct.

Proof. Because of theorem 2.8 we know that $\wp'(z)^2 = 4\wp(z)^3 - g_2(\tau)\wp(z) - g_3(\tau)$ which implies that $\wp'^2$ is a cubic equation with respect to $\wp$ in $\mathbb{C}$. We know that a cubic equation in a closed algebraic field must contain at most 3 distinct zeroes. Thus we need only show that e_j , $j = 1,2,3$ are the zeroes (which we will know to be also distinct). Since for $w \in \{1, \tau, 1+\tau\} \Rightarrow w/2 \notin \wp^{-1}(\infty)$ $\Rightarrow w/2 \notin \wp'^{-1}(\infty)$. Moreover since $\wp'$ is an odd function and $w \in L$ we have

$$\wp'(w/2) = \wp'(w/2 - w) = \wp'(-w/2) = -\wp'(w/2) \Leftrightarrow \wp'(w/2) = 0$$

Thus e_j for $j = 1,2,3$ are the zeroes of the polynomial $4x^3 - g_2x - g_3$
The last statement is true becuase of corollary 2.4

$$2 = \sum_{z \in \wp^{-1}(\infty) \cap \mathcal{F}} \mu(\wp;z) = \sum_{z \in \wp^{-1}(c) \cap \mathcal{F}} \mu(\wp;z)$$

where the first equality is due to the fact that there is only one pole of $\wp$ in $\mathcal{F}$, and for the second equality we take $c \in \{\wp(\frac{1}{2}), \wp(\frac{\tau}{2}), \wp(\frac{1+\tau}{2})\}$ and suppose $|\wp^{-1}(c) \cap \mathcal{F}| = 2$ then $\mu(\wp;z) = 1$ for each $z \in \wp^{-1}(c) \cap \mathcal{F}$, but we know that there is at least one z such that $z \in \frac{1}{2}L \Rightarrow$ by the preceding lemma there is at least one z such that $\mu(\wp;z) \in 2$ (not ∞ because $\wp$ is a nonconstant elliptic function). But this implies that $\sum_{z \in \wp^{-1}(c) \cap \mathcal{F}} \mu(\wp;z) > 2$, because for any $z \in \wp^{-1}(c) \cap \mathcal{F}$ $\mu(\wp;z) > 0$, so we have a contradiction. Therefore we can conclude that $|\wp^{-1}(c) \cap \mathcal{F}| = 1$ for $c \in \{\wp(\frac{1}{2}), \wp(\frac{\tau}{2}), \wp(\frac{1+\tau}{2})\}$ which means that the values of e_1, e_2 and e_3 must be distinct.
And because the e_j's are distinct for $j = 1,2,3$ we have all the zeroes of $4x^3 - g_2x - g_3$ thus we have the algebraic equation $4x^3 - g_2x - g_3 = 4(x-e_1)(x-e_2)(x-e_3)$. This however implies $\wp'(z)^2 = 4\wp(z)^3 - g_2(\tau)\wp(z) - g_3(\tau) = 4(\wp(z)-e_1)(\wp(z)-e_2)(\wp(z)-e_3)$ □

Notation. We will keep in mind the parameters e_1, e_2 and e_3 used in the proposition above for the remaining of this section. Since these parameters are dependent on τ we sometimes write them as $e_i(\tau)$, $i = 1,2,3$

Proposition 2.14. $\Delta(\tau) \neq 0 \, \forall \tau \in \mathbb{H}$

Proof. From the preceding theorem and theorem 2.8 we know the

$$\wp'(z)^2 = 4\wp(z)^3 - g_2(\tau)\wp(z) - g_3(\tau) = 4(\wp(z)-e_1)(\wp(z)-e_2)(\wp(z)-e_3)$$

We can write this as polynomials

$$x^3 + px + q = (x-e_1)(x-e_2)(x-e_3)$$

where $x = \wp(z)$, $p = -g_2/4$ and $q = -g_3/4$. Then we get the following symmetric function of the roots

$$e_1 + e_2 + e_3 = 0 \quad e_1e_2 + e_1e_3 + e_2e_3 = p \quad e_1e_2e_3 = -q$$

From the above equations we get

$$(e_1 - e_2)^2 = (e_1 + e_2)^2 - 4e_1e_2 = -e_3(e_1 + e_2) - 4e_1e_2 = -p - 3e_1e_2$$

similarly $(e_1 - e_3)^2 = -p - 3e_1e_3$ and $(e_2 - e_3)^2 = -p - 3e_2e_3$.
Multiplying the last three equations we get

$$(e_1 - e_2)^2(e_1 - e_3)^2(e_2 - e_3)^2 = -(p + 3e_1e_2)(p + 3e_1e_3)(p + 3e_2e_3)$$

$$-p^3 - 3p^2(e_1e_2 + e_1e_3 + e_2e_3) - 9pe_1e_2e_3(e_1 + e_2 + e_3) - 27e_1^2e_2^2e_3^2$$

$$= -p^3 - 3p^3 - 0 - 27q^2 = -(4p^3 + 27q^2)$$

Thus we can write

$$\Delta(\tau) = g_2^3(\tau) - 27g_3^2(\tau) = 16(e_1(\tau) - e_2(\tau))^2(e_1(\tau) - e_3(\tau))^2(e_2(\tau) - e_3(\tau))^2$$

And by previous theorem for any $\tau \in \mathbb{H}$ none of the values e_1, e_2 and e_3 are equal. (This we can see is also true for any $\tau \in \mathbb{C}^*$) □

Corollary 2.15. $\Delta : \mathbb{H} \to \overline{\mathbb{C}}$ and $j : \mathbb{H} \to \overline{\mathbb{C}}$ are thus meromorphic on $\mathbb{H}$

Definition. The *elliptic modular group* is the group

$$\Gamma = SL(2, \mathbb{Z}) = \{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} | a, b, c, d \in \mathbb{Z}\,,\ ad - bc = 1 \}$$

Notation. For $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma$ and $\tau \in \mathbb{C}$, by $M\tau$ we mean $M\tau := \frac{a\tau+b}{c\tau+d}$

Lemma 2.16.

$$G_k\left(\frac{a\tau + b}{c\tau + d}\right) = (c\tau + d)^k G_k(\tau) \quad \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma$$

Proof. $n\frac{a\tau+b}{c\tau+d} + m = \frac{j\tau+l}{c\tau+d}$, where $j = na + mc$ and $l = nb + md$. So

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} m \\ n \end{pmatrix} = \begin{pmatrix} j \\ l \end{pmatrix}$$

Which means (since the determinant of matrices in Γ are 1)

$$\begin{pmatrix} m \\ n \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix}^{-1} \begin{pmatrix} j \\ l \end{pmatrix}$$

Which means that (j, l) will run thru each value of $\mathbb{Z}^2\backslash\{(0, 0)\}$ exactly once when (m, n) runs once thru each value of $\mathbb{Z}^2\backslash\{(0, 0)\}$. Thus we may write

$$G_k\left(\frac{a\tau + b}{c\tau + d}\right) = \sum_{n,m} \left(n\frac{a\tau + b}{c\tau + d} + m\right)^{-k} = \sum_{j,l} \left(\frac{j\tau + l}{c\tau + d}\right)^{-k} = (c\tau + d)^k G_k(\tau)$$

where the last equality is due to the statement above. □

Lemma 2.17. For all $k \geq 2$ we have

$$\lim_{\mathrm{Im}\tau \to \infty} G_{2k} = 2\zeta(2k) = 2\sum_{n=1}^{\infty} n^{-2k}$$

Proof. We work with $\tau \in \mathbb{H}$ where G_{2k} converges uniformly, then clearly $\lim_{\mathrm{Im}\tau\to\infty}(c\tau+d)^{-1}=0$ for $c\neq 0$ and we have

$$\lim_{\mathrm{Im}\tau\to\infty} G_{2k}(\tau)=\sum_{d\in\mathbb{Z}^*} d^{-2k}=2\sum_{d=1}^{\infty} d^{-2k}$$

□

Theorem 2.18. The j-function is analytic and is invariant under the elliptic modular group transformation i.e.

$$j\left(\frac{a\tau+b}{c\tau+d}\right)=j(\tau) \quad \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma$$

Moreover $\lim_{\mathrm{Im}\tau\to\infty}|j(\tau)|=\infty$

Proof. The first statement is true because from lemma 2.16

$$j\left(\frac{a\tau+b}{c\tau+d}\right)=\left(\frac{g_2^3}{g_2^3-27g_3^2}\right)\left(\frac{a\tau+b}{c\tau+d}\right)=\frac{(c\tau+d)^{12}}{(c\tau+d)^{12}}\left(\frac{g_2^3}{g_2^3-27g_3^2}\right)(\tau)=j(\tau)$$

We now attempt to prove the second statement

$$\lim_{\mathrm{Im}\tau\to\infty}\Delta(\tau)=\lim_{\mathrm{Im}\tau\to\infty} g_2(\tau)^3-g_3(\tau)^2=(60\cdot 2\zeta(4))^3-27\cdot(140\cdot 2\zeta(6))^2$$

substituting, from analytic number theory, the fact that $\zeta(4)=\frac{\pi^4}{90}$ and $\zeta(6)=\frac{\pi^6}{945}$ we see that the above value vanishes. And because $g_2(\tau)$ converges to a nonzero value, we have proved the theorem. □

Definition. By the *fundamental domain* in $\mathbb{C}$ we mean the set $\{\tau\in\mathbb{H}:|\tau|\geq 1,|\mathrm{Re}\tau|\leq 1/2\}$

Lemma 2.19. For every $\tau\in\mathbb{H}$ there exists $M\in\Gamma$ such that $M\tau$ is in the fundamental domain

Proof. Let $M=\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ then $c\tau+d\neq 0$ since $\mathrm{Im}\tau\neq 0$ and either $c\neq 0$ or $d\neq 0$ if $M\in\Gamma$. Then we have

$$\mathrm{Im}\frac{a\tau+b}{c\tau+d}=\frac{1}{2i}\left(\frac{a\tau+b}{c\tau+d}-\frac{a\overline{\tau}+b}{c\overline{\tau}+d}\right)$$

$$=\frac{1}{2i}\frac{(a\tau+b)(c\overline{\tau}+d)-(a\overline{\tau}+b)(c\tau+d)}{|c\tau+d|^2}=(ad-bc)\frac{\mathrm{Im}\tau}{|c\tau+d|^2}=\frac{\mathrm{Im}\tau}{|c\tau+d|^2}$$

Thus $\mathrm{Im}M\tau>0$ or $M\tau\in\mathbb{H}$ for all $M\in\Gamma$ and $\tau\in\mathbb{H}$. And for $c\in\mathbb{Z}\backslash\{0\}$ we have

$$|c\tau+d|^2=|c\mathrm{Re}\tau+d|^2+|c\mathrm{Im}\tau|^2\geq|c\mathrm{Im}\tau|^2\geq|\mathrm{Im}\tau|^2$$

and for $c=0$ we have necessarily $|d|=1$ thus the minimum of the denominator $|c\tau+d|^2$ is less than $|\mathrm{Im}\tau|^2$ or 1 depending on τ.
If $|\mathrm{Im}\tau|\leq 1$ then with $M_o=\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ we have $\mathrm{Im}M_o\tau\geq\mathrm{Im}M\tau$ for all $M\in\Gamma$. If however $|\mathrm{Im}\tau|\geq 1$ then with $M_o=\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ we have again $\mathrm{Im}M_o\tau\geq\mathrm{Im}M\tau$ for all $M\in\Gamma$. Thus $\forall\tau\mathbb{H}\quad\exists M_o\in\Gamma\quad\mathrm{Im}M_o\tau\geq\mathrm{Im}M\tau\quad\forall M\in\Gamma$.
Set now $\tau_o=M_o\tau$ for a fixed τ (M_o as described above). Here we may assume $|\mathrm{Re}\tau_o|\leq\frac{1}{2}$ because

$$\tau_o+n=M_o\tau+n=\left[\begin{pmatrix} a & b \\ c & d \end{pmatrix}M_o\right]\tau \quad \forall n\in\mathbb{Z}$$

and

$$\mathrm{Im}\left[\begin{pmatrix} a & b \\ c & d \end{pmatrix}M_o\right]\tau=\mathrm{Im}M_o\tau \quad \forall n\in\mathbb{Z}$$

Now consider $M = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} M_o$ and we use our derived inequality

$$\mathrm{Im}\tau_o \geq \mathrm{Im}M\tau = \frac{\mathrm{Im}\tau_o}{|\tau_o|^2}$$

We thus conclude that because $\mathrm{Im}\tau_o > 0$ we have that $|\tau_o| \geq 1$ □

Theorem 2.20. $j(\mathbb{H}) = \mathbb{C}$

Proof. Because Δ is holomorphic and has no zero values in $\mathbb{H}$, j is holomorphic in $\mathbb{H}$. Because $\mathbb{H}$ is open and nonconstant holomorphic functions are open, then $j(\mathbb{H})$ is open. Since $\mathbb{C}$ is connected, we need only show that $j(\mathbb{H})$ is closed.
Let b be a closure point of $j(\mathbb{H})$. Choose a sequence $\langle j(\tau_n)\rangle \subset j(\mathbb{H})$ such that $j(\tau_n) \to b$.
Suppose that there is a subsequence of $\langle \tau_n \rangle$ such that the imaginary part converges to ∞. Which means by the preceding theorem, the j image of this subsequence converges to infinity. But this is a contradiction since it means that the sequence $\langle j(\tau_n)\rangle$ does not converge.
Thus there must be a number $C \geq 0$ so that $\mathrm{Im}\tau_n \leq C$, $\forall n \in \mathbb{N}$. Because of the above theorem (i.e. j-function is invariant under elliptic modular group transformations), and the above lemma, we need only to consider the fundamental domain in $\mathbb{C}$ which we set to be S.
Now let $K := \{\tau \in \overline{S} : \mathrm{Im}\tau \leq C\}$, then K is clearly compact and so there is a subsequence of $\langle \tau_n \rangle$ that converges to a point τ, without loss of generality let this subsequence be the sequence itself. Then by the continuity of j we have $j(\tau) = b \in j(\mathbb{H})$ □

Until now we have only considered lattices of the form $L = \mathbb{Z} + \tau\mathbb{Z}$ but the reader must be aware that all of the results proven are also valid for lattices of the form $L = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2$ where $\omega_1, \omega_2 \in \mathbb{C}$ are $\mathbb{R}$ linearly independent values. However unlesss otherwise stated we will always use our original form of L throughout this paper. It is not hard to show that in fact for any lattice L there exist a constant $a \in \mathbb{C}$ such that aL is of the first form.

Notation. Originally we we wrote the Eisenstein series of weight $k \geq 3$ by

$$G_k(\tau) = \sum_{(c,d)\in\mathbb{Z}^{2*}} (c + d\tau)^{-k}$$

however if we want to represent it in general for lattices of the form $L = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2$ we usually write it as

$$G_k(L) = \sum_{(c,d)\in\mathbb{Z}^{2*}} (c\omega_1 + d\omega_2)^{-k} = \sum_{\omega\in L^*} \omega^{-k}$$

Similarly we can write $g_2(L)$, $g_3(L)$

Remark 2.21. It is easy to see that for any lattice L and $a \in \mathbb{C}$ we get $G_k(aL) = a^{-k}G_k(L)$

Corollary 2.22. $g_2, g_3 \in C$ satisfies $g_2^3 - 27g_3^2 \neq 0$ iff there is a lattice L such that $g_2(L) = g_2$ and $g_3(L) = g_3$

Proof. The sufficiency is the result of the fact that Δ does not attain a zero in $\mathbb{H}$ and thus any lattice of the form $L = \mathbb{Z} + \tau\mathbb{Z}$, $\tau \in \mathbb{H}$ and its multiple aL where $a \in \mathbb{C}$ have this property (that's actually because $\Delta(aL) = a^{-12}\Delta(L) \neq 0$)
For the necessity condition, first suppose that g_2 is not zero. Because j is surjective, there is a $\tau \in \mathbb{H}$ such that

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

Since $g_2 \neq 0$ and $g_2^3 - 27g_3^2 \neq 0$ we also have $g_2(\tau), j(\tau) \neq 0$, and by algebraic manipulation we arrive to $\dfrac{g_3^2}{g_2^3} = \dfrac{g_3(\tau)^2}{g_2(\tau)^3}$. This implies that

$$g_3^2 = g_3(\tau)^2 \left(\frac{g_2}{g_2(\tau)}\right)^3 \Rightarrow g_3 = g_3(\tau)\left(\frac{g_2}{g_2(\tau)}\right)^{3/2}$$

Where $\left(\frac{g_2}{g_2(\tau)}\right)^{3/2}$ is one of the square roots by which the equality above holds. And by the remark above this can be written as $g_3 = g_3(\tau(g_2/g_2(\tau))^{-1/4})$ (and this is independent of the choice of which fourth root of $\frac{g_2}{g_2(\tau)}$). Allowing $a := (g_2/g_2(\tau))^{-1/4}$ we claim that our lattice $L = a(\mathbb{Z} + \tau\mathbb{Z})$ has the desired property.
We need only check that $a^{-4}g_2(\tau) = g_2$, but this is indeed true since

$$a^{-4}g_2(\tau) = (g_2/g_2(\tau))g_2(\tau) = g_2$$

For the case that $g_2 = 0$ we have $g_3 \neq 0$ because $g_2^3 - 27g_3^2 \neq 0$, and we can similarly prove our result using the equation $\frac{g_2^3}{g_3^2} = \frac{g_2(\tau)^3}{g_3(\tau)^2}$. □

Remark. We know from function theory, that given a lattice $L = \mathbb{Z}+\mathbb{Z}\tau$ the Weierstraß $\wp$-function has the following identity

$$\wp_L'(z)^2 = 4\wp_L(z)^3 - g_2(\tau)\wp_L(z) - g_3(\tau) \tag{1}$$

also (by Corollary 2.22) given $g_2, g_3 \in \mathbb{C}$ we can find $\tau \in \mathbb{H}$ that forms a lattice $L = \mathbb{Z} + \mathbb{Z}\tau$ and defines a Weierstraß $\wp$-function satisfiying the identity above.

Definition. A *theta function* defined on a lattice $L = \mathbb{Z}\tau + \mathbb{Z}$ of $\mathbb{C}$ is a non-constant analytic function $\theta : \mathbb{C} \to \mathbb{C}$ satisfying $\theta(z + \omega) = e^{a_\omega z + b_\omega}\theta(z)$. Where $a_\omega = a(\omega), b_\omega = b(\omega)$ are functions taking values $\omega \in L$. We call $\mu(\omega, z) = e^{a_\omega z + b_\omega}$ the *factor of automorphy.*

Notation. The reader should not confuse the factor of automorphy with the multiplicity of a function, for the latter we always have a semicolon involved. (i.e. we write $\mu(f; z)$ if we refer to the multiplicity of f at z)

Proposition 2.23. The function

$$G(z) = e^{az^2+bz+c}$$

where $a, b, c \in \mathbb{C}$, is a theta function (on any lattice L), and it is called a *trivial theta function*

Proof. Let $Q(z) = az^2 + bz + c$ then $Q(z + \omega) = Q(z) + (2a\omega z + a\omega^2 + b\omega)$ for $\omega \in L$. This shows that G satisfies the properties that define a theta function with $a_\omega = 2a\omega$ and $b_\omega = a\omega^2 + +b\omega$

Proposition 2.24. The function

$$\theta(\tau, z) = \sum_{n\in\mathbb{Z}} e^{\pi i(n^2\tau+2nz)}$$

is a theta function and has a zero at $\frac{\tau+1}{2}$ of order 1. Morever it satisfies $\theta(\tau, z + 1) = \theta(\tau, z)$ and $\theta(\tau, z + \tau) = e^{-\pi i(\tau+2z)}\theta(\tau, z)$.

Proof. We first need to show that the sum is absolutely convergent. Let $\tau = u + iv$ with $u, v \in \mathbb{R}$ and $v > 0$. Also write $z = x + iy \in \mathbb{C}$ with $x, y \in \mathbb{R}$. Then $|e^{\pi i(n^2\tau+2nz)}| = e^{\pi(n^2v+2ny)}$, and for all except finitely many n we have $n^2v+2ny \leq \frac{1}{2}n^2v$. Those n that does not satisfy the inequality above are those that satisfy $|n| < 4\frac{|y|}{v}$. We also know that the summation $\sum_{n\in\mathbb{Z}} q^{n^2}$, $q = e^{-\frac{\pi}{2}v}$ converges. The properties of a theta function is easily verified. □

Lemma 2.25. Let $\theta : \mathbb{C} \to \mathbb{C}$ be a theta function so that $\theta(0) \neq 0$ then $\forall\omega_1, \omega_2 \in L$ we have $\exp(a(\omega_1).\omega_2) = \exp(a(\omega_2).\omega_1)$, where $a, b : L \to \mathbb{C}$ are functions found in the factor of automorphy $\mu(\omega, z) = e^{a(\omega)z+b(\omega)}$ of our theta function.

Proof.

$$\theta(\omega_1+\omega_2)=\theta(\omega_1)\exp(a(\omega_2).\omega_1+b(\omega_2))=\theta(0)\exp(a(\omega_2).\omega_1+b(\omega_2)+b(\omega_1))$$

Similary

$$\theta(\omega_1+\omega_2)=\theta(0)\exp(a(\omega_1).\omega_2+b(\omega_1)+b(\omega_2))$$

Thus $\exp(a(\omega_1).\omega_2)=\exp(b(\omega_1).\omega_2)$ □

Theorem 2.26. (Abel's Theorem) $\exists f\in\mathcal{M}(\mathbb{C}/L)$ with zeroes $a_1,\cdots,a_n\in\mathbb{C}$ and poles $b_1,\cdots,b_n\in\mathbb{C}$ iff $\sum_{i=1}^{n}a_i\equiv\sum_{i=1}^{n}b_i \bmod L$ (here the number of equal a_i's is exactly $\mu(f;a_i)$, and similarly for b_i's)

Proof. For the proof sufficiency we take the open cell $\mathcal{F}_a^\circ=\{a+t_1\omega_1+t_2\omega_2 : t_1,t_2\in(0,1)\}$ so that the boundary of the cell does not touch any of the a_i's and b_i's. Then we make use of the Residue theorem and take the path integral of $z\frac{f'(z)}{f(z)}$ over the boundary of $\mathcal{F}_a^\circ$ to arrive at our result. We do not go much into detail since this side of the proof is the easy side. For the proof of necessity we can make use of proposition 2.24 we see that there is a theta function with zero z_o whose order is 1 and by which $\theta(0)\neq 0$. One can then use the function

$$f(z)=\mu(A-B,z)\prod_{j=1}^{n}\frac{\theta(z_o+z-a_j)}{\theta(z_o+z-b_j)}$$

where with $A=\sum_{j=1}^{n}a_j$ and $B=\sum_{j=1}^{n}b_j$. Here we claim that $f(z)\in\mathcal{M}(\mathbb{C}/L)$.
Let then $\omega\in L$ and we attempt to consider $f(z+\omega)$. First set

$$h(z)=\frac{\theta(z_o+z-a_j)}{\theta(z_o+z-b_j)}$$

then

$$f(z+\omega)=\mu(A-B,z+\omega)h(z)\prod_{j=1}^{n}\frac{\exp(a(\omega)(z_o+z-a_j)+b(\omega))}{\exp(a(\omega)(z_o+z-b_j)+b(\omega))}$$

$$=\mu(A-B,z)e^{a(A-B).\omega}h(z)\exp(a(\omega).(B-A))=\mu(A-B,z)h(z)$$

wherein the last equality is due to the preceding lemma. □

It is easy to see that $\mathcal{M}(\mathbb{C}/L)$ is a field. Moreover given a polynomial $p(z)=a_0+a_1z+\cdots+a_nz^n$, we write $p(f)$ as the elliptic function produced by the composition of p with f. Also if $r(z)\in\mathbb{C}(Z)$ (i.e. the ratio of two polynomial), we define $r(f)$ analogously.

Notation. If $f\in\mathcal{M}(\mathbb{C}/L)$ then we set a notation of the subfield of $\mathcal{M}(\mathbb{C}/L)$ produced by composition of rational functions with f by $\mathbb{C}(f)=\{p(f) : p(z)\in\mathbb{C}(z)\}$.

Theorem 2.27. $\mathbb{C}(\wp)$ is the subfield of $\mathcal{M}(\mathbb{C}/L)$ consisting of all the even functions in $\mathcal{M}(\mathbb{C}/L)$

Proof. Set $f\in\mathcal{M}(\mathbb{C}/L)$, we may suppose here that $f\not\equiv 0$. Set

$$\mathfrak{B}=\{G(z) : z\in\mathcal{F}\backslash L\ \ni \operatorname{ord}(f;z)\neq 0\}$$

$|\mathfrak{B}|<\infty$ because in the cell there are finitely many poles and zeroes of f (which we assumed to be not equivalent to the zero function). Now for $z\in B\in\mathfrak{B}$ define

$$m_B=\begin{cases}\operatorname{ord}(f;z) & \text{if } B\not\subset\frac{1}{2}L\\ \frac{1}{2}\operatorname{ord}(f;z) & \text{if } B\subset\frac{1}{2}L\end{cases}$$

Note that m_B is only dependent on B and it does not matter which $z \in B$ we choose since $\operatorname{ord}(f;z)$ is constant in B by lemma 2.12. So by lemma 2.12 $\wp$ is constant in B and we denote this by $\wp(B)$, Now define

$$F(z) = \prod_{B\in\mathfrak{B}} (\wp(z) - \wp(B))^{m_B}$$

and we claim that this differs with $f(z)$ by only a constant, i.e. $f(z) = cF(z)$ for some $c \in \mathbb{C}^*$ First we claim $\forall z \in \mathbb{C}$, $\operatorname{ord}(F;z) = \operatorname{ord}(f;z)$. Let $z \in \mathbb{C}/L$ then

$$\forall B \in \mathfrak{B} \quad \operatorname{ord}(\wp - \wp(B); z) = \begin{cases} 1 & \text{if } z \in B \not\subset \frac{1}{2}L \\ 2 & \text{if } z \in B \subset \frac{1}{2}L \\ 0 & \text{if } z \notin B \end{cases}$$

So then

$$\forall B \in \mathfrak{B} \quad \operatorname{ord}((\wp - \wp(B))^{m_B}; z) = \begin{cases} m_B & \text{if } z \in B \not\subset \frac{1}{2}L \\ 2m_B & \text{if } z \in B \subset \frac{1}{2}L \\ 0 & \text{if } z \notin B \end{cases}$$

Thus

$$\operatorname{ord}(F;z) = \sum_{B\in\mathfrak{B}} \operatorname{ord}((\wp - \wp(B))^{m_B}; z) = \operatorname{ord}(f;z)$$

This is in general true, because even if there is no such $B_o \in \mathfrak{B}$ such that $z \in B_o$ we have by definition of $\mathfrak{B}$ that $\operatorname{ord}(F;z) = 0 = \operatorname{ord}(f;z)$. Thus $\forall z \in \mathbb{C}\backslash L$ $\operatorname{ord}(f;z) = \operatorname{ord}(F;z)$
Take now $z \in L$ and for $\forall B \in \mathfrak{B}$ fix an $a_B \in B$ then we have

$$\operatorname{ord}(F;z) = \operatorname{ord}(F;0) = \sum_{B\in\mathfrak{B}} m_B \operatorname{ord}(\wp - \wp(B); 0) = -2\sum m_B =$$

$$-\sum_{*} 2\operatorname{ord}(f;a_B) - \sum_{**} 2\cdot\frac{1}{2}\operatorname{ord}(f;a_B) = -\sum_{*}\sum_{a\in B\cap\mathcal{F}} \operatorname{ord}(f;a) - \sum_{**}\sum_{a\in B\cap\mathcal{F}} \operatorname{ord}(f;a)$$

where we have
$*$: $B \in \mathfrak{B}$ such that $B \not\subset L$
$**$: $B \in \mathfrak{B}$ such that $B \subset L$
The last equality holds because for $B \in \mathfrak{B}$, $|B \cap \mathcal{F}| = 2$ for condition $(*)$ and $|B \cap \mathcal{F}| = 1$ for condition $(**)$ (This is due to lemma 2.10). Thus the above would be equivalent to (here we use the definition of $\mathfrak{B}$)

$$-\sum_{B\in\mathfrak{B}}\sum_{a\in B\cap\mathcal{F}} \operatorname{ord}(f;a) = -\sum_{a\in\mathcal{F}} \operatorname{ord}(f;a) + \sum_{a\in L\cap\mathcal{F}} \operatorname{ord}(f;a) = \sum_{a\in L\cap\mathcal{F}} \operatorname{ord}(f;a) = \operatorname{ord}(f;0)$$

Where the first term in the middle vanishes due to Liouville's third theorem. Thus we have shown $\forall z \in \mathcal{F}$ $\operatorname{ord}(f;z) = \operatorname{ord}(F;z)$ and since the functions are elliptic we have f/F is an elliptic function without any pole which implies that it is a constant. □

Theorem 2.28. $\mathcal{M}(\mathbb{C}/L) = \mathbb{C}(\wp) + \mathbb{C}(\wp)\wp'$

Proof. Clearly the right hand side of the equality is a subset of the left hand side. Now suppose $f \in \mathcal{M}(\mathbb{C}/L)$ and set $f_\pm = \frac{1}{2}(f(z) \pm f(-z))$. Then $f_+ + f_- = f$ with $f_\pm \in \mathcal{M}(\mathbb{C}/L)$. We also see that f_+ is even and f_- is odd. We also know that $\wp'$ is odd so we have $f_-/\wp'$ is even. Thus

$$f = f_+ + \wp'\frac{f_-}{\wp'} \in \mathbb{C}(\wp) + \mathbb{C}(\wp)\wp'$$

□

Remark. From the theorem above one can see that the polynomial $x^2 - \wp'^2 \in \mathbb{C}(\wp)[x]$ is the minimal polynomial to extend the field $\mathbb{C}(\wp)$ to the field $\mathcal{M}(\mathbb{C}/L)$ (we may write $\mathcal{M}(\mathbb{C}/L)$ as $\mathbb{C}(\wp,\wp')$). Thus $\mathcal{M}(\mathbb{C}/L)$ is an algebraic extension of $\mathbb{C}(\wp)$ and also a vector space over it with linearly indendent basis $\{1,\wp'\}$. And so by this we have shown that for every $f \in \mathcal{M}(\mathbb{C}/L)$ there is a unique $p, q \in \mathbb{C}(\wp)$ such that $f = p + q\wp'$.

3 Divisors of Elliptic Curves and Elliptic Functions

Unless otherwise stated, throughout we use an elliptic curve defined by $E : f(x, y) = 0$ on the field $\mathbb{C}$. For most purpose we treat the Weierstraß form $f(x, y) = y^2 - 4x^3 + g_2x + g_3$, where $g_2, g_3 \in \mathbb{C}$ satisfying $g_2^3 - 27g_3^2 \neq 0$. Now we provide a relation between the elliptic curves, divisors and elliptic functions. We note that throughout we use the same assumptions about the elliptic curve E and the lattice L as discussed in the beginning of the previous sections.

Theorem 3.1. (Theorem of Addition of $\wp$-Function). If $z, w \in C$ with $z, w, z+w, z-w \notin L$ then

$$\wp(z + w) = \frac{1}{4}\left[\frac{\wp'(z) - \wp'(w)}{\wp(z) - \wp(w)}\right]^2 - \wp(z) - \wp(w)$$

Proof. We will use basic concepts in projective geometry here. For $u, v \in \mathbb{C}$ such that $u, v, u + v, u - v \notin L$. Consider the following points

$$(1 : \wp(u) : wp'(u))$$

$$(1 : \wp(v) : wp'(v))$$

$$(1 : \wp(u + v) : -wp'(u + v))$$

in the projective plane. We clain first that these points are collinear in the projective plane, that is we clain

$$\det \begin{pmatrix} 1 & \wp(u) & \wp'(u) \\ 1 & \wp(v) & \wp'(v) \\ 1 & \wp(u+v) & -\wp'(u+v) \end{pmatrix} = 0$$

Consider first

$$f(z) = \det \begin{pmatrix} 1 & \wp(u) & \wp'(u) \\ 1 & \wp(v) & \wp'(v) \\ 1 & \wp(z) & -\wp'(z) \end{pmatrix}$$

this function is elliptic, and by the required conditions of u and v we have distinct values of $\wp(u)$ and $\wp(v)$. By this we conclude that we can write $f(z)$ as $a+b\wp(z)+c\wp'(z)$, with $a, b, c \in \mathbb{C}$ and in particular $c \neq 0$. Thus $f(z)$ has poles only in the lattice of order 3, moreover one sees immediately that u, v are two distinct zeroes of this function. By Abel's Theorem (theorem 2.26) one arrives to a third zero $z \equiv -(u + v) \bmod L$. Thus we prove our claim.
Now by the identity of $\wp$ proven in theorem 2.8 we see that $(\wp(u), \wp'(v)), (\wp(u), \wp'(u))$ and $(\wp(u + v), -\wp'(u + v))$ are solutions of the elliptic curve define by $E : y^2 - 4x^3 + g_2(\tau)x + g_3(\tau)$. Thus they are the three distinct collinear points in the affine plane that are also in the elliptic curve. The equality in this theorem is obtained by the solution to the first coordinate of the addition operation defined on the elliptic curves (ie we add points $(\wp(u), \wp'(v))$ and $(\wp(u), \wp'(u))$, whose line has the slope $\frac{\wp'(z)-\wp'(w)}{\wp(z)-\wp(w)}$. □

We can do away with the conditions for z, w given above, by allowing limits and infinity. Now in addition to our assumption that $E : f(x, y) = 0$ is our elliptic curve. We require throughout that the equation of the elliptic curve be in Weierstraß form, in other words $f(x, y)$ has the form $f(x, y) = y^2 - 4x^3 + g_2x + g_3$, ($g_2, g_3 \in \mathbb{C}$ satisfying the conditions of elliptic curves). Thus to every lattice L we associate an elliptic curve $E : f(x, y) = 0$ by considering $g_2 = g_2(L)$ and $g_3 = g_3(L)$ and conversely to every elliptic curve $E : f(x, y) = 0$ we asssociate a lattice L as in corollary 2.22.

Corollary 3.2. There is a natural group isomorphism between the torus $\mathbb{C}/L$ and the elliptic curve $E : f(x, y) = 0$ associated to the lattice L, given by:

$$\phi : \mathbb{C}/L \xrightarrow{\sim} E \quad , \quad \phi([z]) = \begin{cases} (\wp(z), \wp'(z)) & z \notin L \\ \mathcal{O} & z \in L \end{cases}$$

Proof. We wish to prove for $u, v \in \mathbb{C}$ we have

$$\phi([u]) + \phi([v]) = \phi([u+v])$$

Let $u, v, u+v, u-v \notin L$, following the method of proof of previous theorem we obtain three distinct points $(\wp(u), \wp'(v)), (\wp(u), \wp'(u))$ and $(\wp(u+v), -\wp'(u+v))$ that are collinear and in the elliptic curve, one has the above. Now if u or v is $0 \bmod L$ the result is obvious. We have to then only consider the case when $u+v, u-v \in L$. When $u-v \in L$ the result is again trivial by definition of ϕ, but when $v \equiv u \bmod L$ we need to compute the doubling of points in the elliptic curve. We consider that $v \equiv u \not\equiv -v \bmod L$, then we have points in the elliptic curve that must be doubled and by which they are not their own additive inverse. Now note that

$$\lim_{z \to v} \frac{\wp'(z) - \wp'(v)}{\wp(z) - \wp(v)} = \frac{\wp''(v)}{\wp'(v)}$$

and that one may substitute the second identity in theorem 2.8 on the Weierstraß $\wp$-function

$$2\wp''(z) = 12\wp(z)^2 - g_2(\tau)$$

One can then use the doubling of two points in the elliptic curve and follows an analogous step as the the first case and that of the previous theorem. This proves that ϕ is a homomorphism.
ϕ is also surjective since $\wp$ takes all values in $\mathbb{C}$ (see remark 2.7), and any point in the elliptic curve with fixed first coordinate has at most two solutions which are both taken by ϕ (see theorem 2.8). The mapping is also injective since if $(\wp(v), \wp'(v)) = (\wp(u), \wp'(u))$ for some $u, v \in \mathbb{C}$ we have

$$\wp(v) = \wp(u) \Rightarrow v \equiv u \bmod L \ \vee \ v \equiv -u \bmod L$$

But because also $\wp'(v) = \wp'(u)$, if $v \equiv -u$ then $\wp'(u) = \wp'(-u) = -\wp'(u) = 0$ and so by lemma 2.9

$$2u \in L \Rightarrow u \equiv -u \equiv v$$

□

Remark. There is a way to find $\phi^{-1}(P)$ for $P \in E$ by using the *elliptic integral of the first kind*. This method is the way one determines the *local inverse* of the Weierstraß $\wp$-function.

Definition. A divisor D is a family $\{n_P\}_{P \in E}$ of whole numbers, such that all but finitely many elements of the family are zero. For brevity, we write divisors as a formal sum (as done by most literatures)

$$D = \sum_{P \in E} n_P(P)$$

Notation. We denote the set of all divisors of D as $\mathbf{D}$. Also if it is clear, we avoid writing the suffix of the formal sum, i.e. we simply write $D = \sum n_P(P)$ for a divisor $D = \sum_{P \in E} n_P(P)$

Remark. It is easy to see that if $D, D' \in \mathbf{D}$ with $D = \sum n_P(P)$ and $D' = \sum m_P(P)$ then by setting their *sum* to be $D + D' = \sum (n_P + m_P)(P)$ we embed an abelian group structure into $\mathbf{D}$

Definition. Let $D = \sum n_P(P)$ be a divisor. The *degree* of D is the integer $\deg(D) = \sum_{P \in E} n_P$, and the *support* of D is the set $\operatorname{supp}(D) = \{P \in E : np \neq 0\}$

Lemma 3.3. Let K be an arbitrary field, $f \in K[x, y]$ an irreducible polynomial and $g \in K[x, y]$. If $f \nmid g$ then $\{(x, y) \in K^2 : f(x, y) = g(x, y) = 0\}$ is a finite set.

Proof. Suppose x appears in f with positive degree, otherwise we see clearly that there are finitely many values of the second coordinate β such that $f(x, \beta) = f(\beta) = 0$ and for each of those values, there are finitely many values of the zeroes for the polynomial $g(x, \beta) \in K[x]$. Let us view f and g as elements of $K(Y)[X]$ (i.e. polynomials of one variable whose coffecients are rational functions of y). Suppose f is reducible in $K(Y)[X]$ then $f = ab/c$ for some $a, b \in K[x, y]$ and

$c \in K[y]$. If $c \mid a$ or $c \mid b$ in $K[x,y]$ then this contradicts the irreducibility of f. If $c \nmid a$ and $c \nmid b$ in $K[x,y]$ then because $ab/c \in K[x,y]$, c must be reducible, i.e. $\exists c_1, c_2 \in K[x]$ so that $c_1 \mid a$, $c_1 \mid b$ in $K[x,y]$ and $c_1 c_2 = c$. Thus we can conclude that f is irreducible in $K(y)[X]$. In a similar manner, we see that $f \nmid g$ in the new ring $K(y)[X]$. Hence there exists $\tilde{u}, \tilde{v} \in K(Y)[X]$ such that $f\tilde{u} + g\tilde{v} = 1$. This implies that $\exists\, a \in K[y]\backslash\{0\}$ such that $fu + gv = a$, where $u = a\tilde{u}$ and $v = a\tilde{v}$ with $u, v \in K[x,y]$. We notice that if for $\alpha, \beta \in K$, $f(\alpha,\beta) = g(\alpha,\beta) = 0$ then $a(\beta) = 0$. Since a is a polynomial of one variable, there are finitely many values for the second coordinate β such that $f(\alpha,\beta) = g(\alpha,\beta) = 0$, Now, the polynmial $f(x,\beta) \in K[x]$ is not 0, otherwise $f(x,y)$ would be divisible by $y - \beta$, and hence there are finite number of possibilities for α. □

Definition. Let E be an elliptic curve on $\mathbb{C}$ given by $f(x,y) = 0$. Consider $u(x,y) = p(x,y)/q(x,y)$, where $p, q \in \mathbb{C}[x,y]$ and $f \nmid q$. Then u is called a *rational function defined on* E. Two rational functions p/q and p_1/q_1 defined on E are *equal on* E iff $f \mid (pq_1 - qp_1)$.

Notation. We denote the set of all rational functions defined above, with the given equivalence by $\mathbb{C}(E)$

Remark 3.4. Because $f \in \mathbb{C}[x,y]$ is irreducible. The set of all rational functions on E, with equivalence defined above, form a field. This field is called *function field* or *field of rational functions of* E denoted by $\mathbb{C}(E)$. Another thing that is worth noticing is that $\mathbb{C}(x,y)/\langle f\rangle = \mathbb{C}(x) + y\mathbb{C}(y)$. To see this let $g \in \mathbb{C}(x,y)/\langle f\rangle$, then g can be written as $g(x,y) = \frac{p_1(x)+yp_2(x)}{q_1(x)+yq_2(x)}$ where $q_1, q_2, p_1, p_2 \in \mathbb{C}[x]$. We only have to make $\frac{yp_2(x)}{q_1(x)+yq_2(x)}$ of the form that is in $\mathbb{C}(X)+y\mathbb{C}(X)$, but this is easily done by multiplying the numerator and denominator by $q_1(x) + yq_2(x)$ and substituting $4x^3 - g_2x - g_3$ for y^2

Definition. Let $g(x,y) \in \mathbb{C}[x,y]/\langle f\rangle$. Then we can write $g(x,y) \equiv p_1(x) + yp_2(x)$. We then define the degree of g denoted by $\deg(g)$ to be $\deg(g) = \max\{2\deg(p_1), 2\deg(p_2) + 3\}$. Take note that $\deg(p_1)$ and $\deg(p_2)$ are the usual degrees on polynomial of one variable, with nonzero constants having degree 0 and zero having degree $-\infty$. We define the *highest degree term* to be the highest degree term in $p_1(x)$ if $\deg(p_1) > \deg(p_2) + 3$, otherwise it is the highest degree term in $p_2(x)$ multiplied by y. We make note that $y^2 - x^3$ will no longer be of degree 6 but will be of degree 2 or less (we consider g to belong to the classes modulo f).

Remark. We know that the points of an elliptic curve have the form $(\wp(z), \wp'(z))$ for some $z \in \mathbb{C}$, thus we can define x to have degree 2 (That is just the order of $\wp$ at 0 which is isomorphic to the point of infinity $\mathcal{O}$) and y to have degree 3 (order of $\wp'$ at 0). Thus the definition above makes sense because $\deg(p_1) \neq \deg(p_2) + 3$ since $p_1(x)$ has degrees $0, 2, 4, \cdots$ in $\mathbb{C}[x,y]/\langle f\rangle$ and $yp_2(x)$ has degrees $3, 5, 7, \cdots$.

Definition. (The value of a rational function on E at a point in E). Let $u = p/q \in \mathbb{C}(E)$, then $f \nmid q$ and by Lemma 3.3 the set $\{P \in E : q(P) = 0\}$ is finite (i.e. the set of points by which u is undefined). Now let $P \in E\backslash\{\mathcal{O}\}$ be given. If there is $\tilde{p}, \tilde{q} \in \mathbb{C}[x,y]$ such that $u \equiv \tilde{p}/\tilde{q}$ and $\tilde{q}(P) \neq 0$ then we say u *is regular at* P and the value of u at P is written as $u(P) = \tilde{p}(P)/\tilde{q}(P)$. Now we define the value of $u(\mathcal{O})$. If $\deg(p) < \deg(q)$ then define $u(\mathcal{O}) = 0$, if $\deg(p) > \deg(q)$ then define $u(\mathcal{O}) = \infty$. If however $\deg(p) = \deg(q)$, then let the highest degree terms of p and q have coefficients a and b respectively, we define $u(\mathcal{O}) = a/b$.

Definition. If $u \in \mathbb{C}(E)$ is regular at $P \in E$ and $u(P) = 0$ then we say P is a zero of u. If however $u \in \mathbb{C}(E)$ is not regular at $P \in E$ then we say P is a pole of u and we write $u(P) = \infty$.

Theorem 3.5. At any point $P \in E$, there is rational function $t \in \mathbb{C}(E)$ regular at P with $t(P) = 0$ and for all $u \in \mathbb{C}(E)^*$ there exists $v \in \mathbb{C}(E)$ regular at P with $v(P) \neq 0$ and $u = t^k v$ for some $k \in \mathbb{Z}$. Moreover, the number k is independent of the choice of t, with u being regular at P iff $k \geq 0$.

Remark. In general the above theorem can be extended for any algebraic curve C defined on any field K, by replacing the word "regular" with "nonsingular". Nonsingular at a point means that the one of the first partial derivative of the equation of the curve will not vanish at that point.

Proof. Without loss of generality let $P = (0, 0)$ (otherwise we may as well work with variables $x - x_o$ and $y - x_o$ for $P = (x_o, y_o)$ without changing much of the method of our proof). We can write $f = \alpha x + \beta y + g$, with $\alpha, \beta \in K$, $g \in K[x, y]$ containing x and y terms of degree ≥ 2. The curve is nonsingular at P, without loss of generality let $f_y(P) \neq 0$, then necessarily we have $\beta \neq 0$. We may rewrite f by grouping terms that involve only x, $f = x\phi(x) + y\beta + yh(x, y)$. Here $h(0, 0) = 0$, and so $w = -\phi(x)/(\beta + h)$ is regular at P. Now because P is a point of the curve, we have $y = xw$. Now let u be a rational function regular at P. If $u(P) \neq$, we have a trivial case where we choose $k = 0$. If $u(P) = 0$, then we may write $u = p/q$ with $p, q \in K[x, y]$ and $p(P) = 0$, $q(P) \neq 0$. p has no constant terms because $p(0, 0) = 0$, thus $p(x, y) = p(x, xw) = xr$ for some $r \in K[x, y]$. Thus $u = xr/q = xu_1$ where $u_1(P) = 0$. u_1 is regular at P, so we can repeat the argument if $u_1(P) = 0$, obtaining $u = x^2u_2$. We claim that this process stops after a finite number of steps k.
Since we assumed $u \neq 0$, then we have $f \nmid p$. Hence, by a similar manner used the proof of lemma 3.3, we see that $f \nmid p$ also in $K(x)[y]$ and so $\exists \xi, \eta \in K[x, y], a \in K[x]$ such that $a \neq 0$ and $f\xi + p\eta = a$ Since a is a polynomial of one variable, we may write $a = x^k a_o$ with $a_o(P) = a_o(0) \neq 0$. Then $p\eta = a$ in $K(E)$. We claim that it is not possible to write $p = x^l w_o$ for $l > k$ and $w_o \in K[x, y]$. Otherwise, $x^k(x^{l-k}w_o - a_o) = 0$ in $K(E)$ and so $x^{l-k}w_o - a_o = 0$ in $K(E)$ which means $f \mid x^{l-k}w_o - a_o$. But now $w_o = c/d$ for some $c, d \in K[x, y]$ with $d(P) \neq 0$. And so $f \mid x^{l-k}c - a_o d$, but then $x^{l-k}c$ vanishes on P and $a_o d$ does not. □

Definition. The number k in theorem 3.5 is called the *order of u at P* and we write $k = \mathrm{ord}(u; P)$. The function t in the theorem 3.5 is called the *local parameter on the curve at P*.

Remark. We can see that for $g \in \mathbb{C}(E)$ and $P \in E$, $g(P) = \infty$ iff $\mathrm{ord}(g; P) < 0$ and $g(P) = 0$ iff $\mathrm{ord}(g; P) > 0$

Definition. The *divisor of a rational function* $g \in \mathbb{C}(E)$ is the divisor $\mathrm{div}(g) = \sum \mathrm{ord}(g; P)(P)$. And if for $D \in \mathbf{D}$ there is a rational function $g \in \mathbb{C}(E)$ so that $\mathrm{div}(g) = D$ then we say D is a *principal divisor*. The set of all principal divisors is denoted with $\mathbf{D}_l$

Now throughout, unless otherwise stated, we fix our elliptic curve E and the lattice L associated to it. So we may be able to speak of divisors and principal divisors without any sense of ambiguity. We also keep the isomorphism ϕ in mind.

Lemma 3.6. For a nonzero $g(z) \in \mathcal{M}(\mathbb{C}/L)$ $\exists\, r_1(z), r_2(z) \in \mathbb{C}(z)$ such that $g(z) = r_1(\wp(z)) + \wp'(z)r_2(\wp(z))$. Now consider $\tilde{g}(x, y) = r_1(x) + yr_2(x)$, then z is a zero (pole) of g iff $P = \phi([z])$ is a zero (pole) of $\tilde{g}$. Moreover $\mathrm{ord}(g; w) = \mathrm{ord}(\tilde{g}; \phi([w]))$

Proof. z is a pole of g $\Leftrightarrow$ $g(z) = r_1(\wp(z)) + \wp'(z)r_2(\wp(z)) = 0$ $\Leftrightarrow$ now if $z \neq 0 \bmod L$ then $\phi([z]) = (\wp(z), \wp'(z)) \in E$ and so $\tilde{g}(P) = 0$ and we are done. Otherwise $\wp(z), \wp'(z) = \infty$, and by considering $g(z), \tilde{g}(x, y)$ to be rational functions and noting that taking the torus as our space we have $\lim_{z\to 0} \frac{\wp(z)}{\wp'(z)} \neq \infty$, then $g(z)$ can only be zero if the highest degree of denominator of $\tilde{g}(x, y)$ is greater than the highest degree of the numerator of $\tilde{g}(x, y)$. But this only means that $\tilde{g}(\mathcal{O}) = 0$. The second part of this lemma is quite clear, because of theorem 3.5 and the way the order of a function is defined (we need only divide $g(z), \tilde{g}$ by the function $h(z) = (z - w)^{\mathrm{ord}(g;z)}$ and $\tilde{h}$ respectively and use the remarks of theorem 3.5 to conclude that both are nonzero at z and $\phi([z])$ respectively and that the local parameter is $\tilde{t}$ where $t(z) = z - w$). □

Theorem 3.7. The mapping $\mathrm{Quot}(\mathbb{C}(x, y)/\langle f \rangle) \to \mathcal{M}(\mathbb{C}/L)$ defined by $g(x, y) \mapsto g(\wp(z), \wp'(z))$ is an isomorphism of fields.

Proof. The mapping is clearly a homomorphism. We can also see that all polynomials that are multiples of f are mapped to the zero function, since $f(\wp(z), \wp'(z)) = 0$. Conversely, any function in the kernel of the mapping will be multiples of f (Note that f has no multiple roots so if a rational function is mapped to zero it must have a multiple which is a root of $f(\wp(z), \wp'(z))$ by doing manipulation on the denominator and numerator of the rational function it can be written also as multiples of $f(\wp(z), \wp'(z))$). Thus the mapping is one-to-one. And by theorem 2.28 and its succeeding remark we can also immediately conclude that the mapping is onto. □

Notation. So we can associate a rational function $\tilde{g} \in \mathbb{C}(E)$ for a function $g \in \mathcal{M}(\mathbb{C}/L)$. For simplicity we sometimes write $\operatorname{div}(g)$ for the divisor $\operatorname{div}(\tilde{g})$.

Lemma 3.8. For $D = \sum n_P(P) \in \mathbf{D}_l$, we have $\deg(D) = 0$ and $\sum n_P P = \mathcal{O}$ (the last summation is using the group operation of the elliptic curve)

Proof. Let $\tilde{g}(x, y) \in \mathbb{C}(E)$ such that $\operatorname{div}(\tilde{g}) = D$. Consider $g(z) = \tilde{g}(\wp(z), \wp'(z))$ then, by remark 3.4 and theorem 2.28, $g \in \mathcal{M}(\mathbb{C}/L)$. Moreover by lemma 3.6 $P \in E$ is a pole (zero) of $\tilde{g}$ iff $z = \phi^{-1}(P)$ is a pole (zero) of g. By theorem 2.3 we can conclude that $\deg(\operatorname{div}(g)) = 0$. Using this with Abel's theorem (2.26) and corollary 3.2 we can easily conclude that for the divisor $D = \operatorname{div}(g) = \sum n_P(P) \in \mathbf{D}_l$ we have $\sum z\mu(g; z) \equiv 0$ and so $\sum n_P P = \mathcal{O}$. □

Notation. From theorem 2.1 (Liouville's First Theorem), we can produce an equivalence relation of elliptic functions (i.e. $f \sim g$ if $\exists \alpha \in \mathbb{C}^*$ so that $f = \alpha g$). We write the set of elliptic functions with this equivalence relation with $\mathcal{T}(\mathbb{C}/L)$. And by $\operatorname{div}(g)$ for $g \in \mathcal{T}(\mathbb{C}/L)$ we mean the divisor of one of the functions that represent g (functions belonging to the same class have the same divisor).

Theorem 3.9. $\exists \Phi : \mathcal{T}(\mathbb{C}/L) \rightarrowtail \mathbf{D}_l$ such that $\forall D \in \mathbf{D}_l \ \exists \tilde{g} \in \mathbb{C}(x, y), g \in \mathcal{M}(\mathbb{C}/L)$ such that $D = \operatorname{div}(\tilde{g})$ and $\Phi^{-1}(D) = [g]$ with $g(z) = \tilde{g}(\phi([z])) \ \forall [z] \in \mathbb{C}/L$

Proof. Let $g \in \mathcal{T}(\mathbb{C}/L)$, then define $\Phi(g) = \operatorname{div}(g)$.
We claim:

1. Φ is injective
   Let $g, h \in \mathcal{T}(\mathbb{C}/L)$ with $\operatorname{div}(g) = \operatorname{div}(h)$, then $\operatorname{ord}(g; z) = \operatorname{ord}(h; z) \forall z \in \mathbb{C}$. And so we must have $g = h$

2. Φ is surjective
   Let $D \in \mathbf{D}_l$ and $\tilde{g} \in \mathbb{C}(E)$ with $D = \operatorname{div}(\tilde{g})$. Consider $g(z) = \tilde{g}(\wp(z), \wp'(z))$ then by remark 3.4 and theorem 2.28 $g \in \mathcal{M}(\mathbb{C}/L)$. Now g then must have finite zeroes $a_1, \cdots, a_n \in \mathbb{C}$ and poles $b_1, \cdots, b_n \in \mathbb{C}$ (There are as many repetition of a_i's and b_i's as $\mu(g; a_i)$, $\mu(g; b_i)$ respectively) and by theorem 2.3 and Abel's theorem (2.26) and the remark that follows it, we realize that
   $$h(z) = \mu(A - B, z) \prod_{i=1}^{n} \frac{\theta(z_o + z - a_i)}{\theta(z_o + z - b_i)} \quad z_o = \frac{\tau + 1}{2}$$
   where $A = \sum_{i=1}^{n} a_i$ and $B = \sum_{i=1}^{n} b_i$ with $\mu(A - B, z)$ being the automorphy factor, satisfies $\operatorname{div}(h) = \operatorname{div}(g)$. Therefore $D \in \Phi(\mathcal{T}(\mathbb{C}/L))$

3. The last statement of the theorem is just a restatement of lemma 3.6. □

Remark. The converse of lemma 3.8 is also true.

Corollary 3.10. For $g \in \mathcal{M}(\mathbb{C}/L)$ we have $\operatorname{div}(g) = 0$ iff g is a constant

4 Weil Pairing

We keep in mind the mappings $\phi : \mathbb{C}/L \to E$ and $\Phi : \mathcal{T}(\mathbb{C}/L) \to \mathbf{D}_l$ worked on the previous section. In this section we deal a lot with the torus, therefore it is worthy of having a notation of it.

Notation. We denote the torus by $\mathcal{F} = \mathbb{C}/L$.
For $P \in E$ and $m \in \mathbb{N}$, by mP we mean

$$mP = \underbrace{P + \cdots + P}_{m-times}$$

using the elliptic curve group addition.
For $D \in \mathbf{D}$ and $m \in \mathbb{N}$, by mD we mean

$$mD = \underbrace{D + \cdots + D}_{m-times}$$

using the divisor group addition. So similarly we understand mz for $z \in \mathcal{F}$
From the previous section we see that it makes sense to define divisors as a formal linear combination of points in $\mathbb{C}/L$. Thus we may define a divisor D as a formal linear combination

$$D = \sum_{z \in \mathcal{F}} n_z(z)$$

so that the family $\{n_z\}_z$ consists of finitely many nonzero terms. Thus we make free use of either divisors defined on $\mathcal{F}$ or those on the elliptic curve E.

Definition. Let $m \in \mathbb{N}$, then we define $E[m] = \{P \in E : mP = \mathcal{O}\}$ and $\mu_m = \{z \in \mathbb{C} : z^m = 1\}$, the elements of this set are called the *m division points of the elliptic curve.* Similary we define $\mathcal{F}[m] = \{z \in \mathbb{C}/L : z = 0\}$ (We avoid writing $[z]$).

Definition. Suppose $g \in \mathcal{M}(\mathbb{C}/L)$ and $D = \sum n_z(z) \in \mathbf{D}$ with $\operatorname{supp}(\operatorname{div}(g)) \cap \operatorname{supp}(D) = \emptyset$ then we define g *evaluated at* D to be

$$g(D) = \prod_{z \in \operatorname{supp}(D)} g^{n_z}(z)$$

Definition. We say divisors $D_1, D_2 \in \mathbf{D}$ are *equivalent*, and write $D_1 \sim D_2$, if $D_1 - D_2 \in \mathbf{D}_l$.

Definition. Let $m \in \mathbb{N}$ and $z_1, z_2 \in \mathcal{F}[m]$, consider the function $g \in \mathcal{M}(\mathbb{C}/L)$ such that

$$\operatorname{div}(g) = \sum_{z \in \mathcal{F}[m]} [(z_2/m + z) - (z)]$$

This function exist because of lemma 3.8. Now we define the *Weil pairing of the m division points of the elliptic curve* or simply *The Weil e_m-pairing* as the function

$$e_m : \mathcal{F}[m] \times \mathcal{F}[m] \to \mu_m$$

So that given $(z_1, z_2) \in \mathcal{F}[m] \times \mathcal{F}[m]$ as defined above, and for an arbitrary $w \in \mathcal{F}$ so that $g(z_1 + w), g(w) \in \mathbb{C}^*$, we obtain $e_m(z_1, z_2) = g(z_1 + w)/g(w)$

Remark. The Weil e_m-pairing defined above is a well-defined function. One can easily verify this by working with a function $f \in \mathcal{M}(\mathbb{C}/L)$ such that $\operatorname{div}(f) = m(z_2) - m(0)$, without loss of generality we can choose f to be such that $f(mD) = g(D)^m$ for all $D \in \mathbf{D}$ such that $f(mD)$ and $g(D)$ is defined. By this we can see that $g(z_1+w)^m = f(mz_1+mw) = f(mw) = g(w)^m$ for all w such that $g(z_1+w), g(w) \in \mathbb{C}^*$, thus $g(z_1+w)/g(w)$ is a root of unity. Also we see that this is all independent of the choice w. Consider for instance the function $g_o(w) = g(z_1 + w)/g(w)$, this is an elliptic

function without any poles or zeroes because the zeroes of $g(w)$ are those of the form $z_2/m + z$ for any z in $\mathcal{F}[m]$, and those are also the zeroes of $g(w+z_1)$, since $\{z : z \in \mathcal{F}[m]\} = \{z+z_1 : z \in \mathcal{F}[m]\}$. We can argue similarly for the poles. Thus g_o must be a constant. And so the Weil e_m-pairing is a well-defined function.

Proposition 4.1. Given $m, n \in \mathbb{N}\backslash\{1\}$, the Weil pairing has the following properties

(i) Bilinear, i.e. For all $z_1, z_2, z_3 \in \mathcal{F}[m]$
$e_m(z_1 + z_2, z_3) = e_m(z_1, z_3)e_m(z_2, z_3)$ and $e_m(z_1, z_2 + z_3) = e_m(z_1, z_2)e_m(z_1, z_3)$

(ii) Alternative, i.e. For all $w, z \in \mathcal{F}[m]$
$e_m(w, z) = e_m(z, w)^{-1}$ in particular $e_m(w, w) = 1$

(iii) Compatible, i.e. if $w \in \mathcal{F}[mn]$ and $z \in \mathcal{F}[m]$ then $e_{mn}(w, z) = e_m(nw, z)$

(iv) Non-degenerate, i.e. given $w \in \mathcal{F}[m]$ if for all $z \in \mathcal{F}[m]$ $e_m(z, w) = 1$ then $w \equiv 0$

(v) Surjective

Proof. (i) $e_m(z_1 + z_2, z_3) = \dfrac{g(z_1 + z_2 + w)}{g(z_1 + w)} \dfrac{g(z_1 + w)}{g(w)} = e_m(z_1, z_3)e_m(z_2, z_3)$
Now choose $f_1, g_1 \in \mathcal{M}(\mathbb{C}/L)$ such that $\operatorname{div}(f_1) = m(z_2) - m(0)$, with $g_1^m(\cdot) = f_1(m\cdot)$ (as in the preceding remark). Similarly choose $f_2, g_2, f_3, g_3 \in \mathcal{M}(\mathbb{C}/L)$ for $z_3, z_2 + z_3 \in \mathcal{F}[m]$ respectively. Now choose $h \in \mathcal{M}(\mathbb{C}/L)$ so that $\operatorname{div}(h) = (z_2 + z_3) - (z_2) - (z_3) + (0)$ (can be done by 3.8). Then $\operatorname{div}(f_3/f_1f_2) = m \operatorname{div}(h)$, so $f_3 = \alpha f_1 f_2 h^m$ for some $\alpha \in \mathbb{C}^*$.
Thus we find $\beta \in \mathbb{C}^*$ such that $g_3(\cdot) = \beta g_1(\cdot)g_2(\cdot)h(m\cdot)$ And so

$$e_m(z_1, z_2 + z_3) = \frac{g_3(w + z_1)}{g_3(w)} = \frac{g_1(w + z_1)g_2(w + z_1)h(mw + mz_1)}{g_1(w)g_2(w)h(mw)} = e_m(z_1, z_2)e_m(z_1, z_3)$$

(ii) From (i) we have $e_m(z + w, z + w) = e_m(z, z)e_m(z, w)e_m(w, z)e_m(w, w)$. Thus it suffices to show that $e_m(w, w) = 1$ for all $w \in \mathcal{F}[m]$. Then since the composition of a translation with an elliptic function is again an elliptic function we have

$$\operatorname{div}(\prod_{i=0}^{m-1} f(\cdot + iw)) = m \sum_{i=0}^{m-1} [((1 - i)w) - (-iw)] = 0$$

Hence $\prod_{i=0}^{m-1} f(z + iw)$ evaluated at z is a constant. Obtaining g from f analagous from the preceding remark, we also conclude that $\prod_{i=0}^{m-1} g(\frac{z+iw}{m})$ (evaluated at z) is a constant. Therefore we can write

$$\prod_{i=0}^{m-1} g(z + iw/m) = \prod_{i=0}^{m-1} g(z + (i + 1)w/m)$$

And this gives $g(z) = g(z + w)$ for all $z \in \mathcal{F}$ and so $e_m(w, w) = g(z + w)/g(z) = 1$

(iii) Taking f and g as in the preceding remark ((z, w) instead of (z_1, z_2)), we have

$$\operatorname{div}(f^n) = mn(w) - mn(0)$$

and

$$g^{mn}(n\cdot) = f^n(mn\cdot)$$

Then from the definition of e_{mn} and e_m we obtain

$$e_{mn}(w, z) = \frac{g(n(z_o + w))}{g(nz_o)} = \frac{g(w_o + nw)}{g(w_o)} = e_m(nw, z)$$

where $z_o, w_o = z_o/n \in \mathcal{F}$ or chosen so that the fractions above are well defined.

(iv) This follows directly from the coming theorem 4.4, whose proof only made use of properties (i)-(iii)

(v) This is also the result of the same theorem.

□

Remark 4.2. It is easy to see that $\mathcal{F}[m]$ has m^2 number of points, in fact

$$\mathcal{F}[m] = \{\frac{j\tau + k}{m} : j, k = 0, \cdots, m-1\}$$

Moreover to create the function g used in the definition of the Weil Pairing $e_m(z_1, z_2)$ with

$$\text{div}(g) = \sum_{z \in \mathcal{F}[m]} [(z_2/m + z) - (z)]$$

We make use of any theta function $\theta : \mathbb{C} \to \mathbb{C}$ with zero z_o of order 1. And we can allow g to be

$$g(z) = \mu(mz_2, z) \prod_{w \in \mathcal{F}[m]} \frac{\theta(z_o + z - z_2/m - w)}{\theta(z_o + z - w)}$$

Take note that mz_2 is in $\mathbb{C}^2$ and not in $\mathcal{F}$. Now if we set

$$h(z) = \prod_{w \in \mathcal{F}[m]} \frac{\theta(z_o + z - z_2/m - w)}{\theta(z_o + z - w)}$$

and if our factor of automorphy is $\mu(\omega, z) = \exp(a(\omega) + b(\omega)z)$, then clearly the Weil e_m-pairing of (z_1, z_2) would be $e_m(z_1, z_2) = e^{z_1 a(mz_2)} h(z_1 + w)/h(w)$ for all $w \in \mathcal{F}$ such that $h(z_1 + w), h(w) \in \mathbb{C}^*$

Now from the definition of the Weil pairing let us study how we can approximate the Weil pairing using only finite sums in the theta functions. We make use of the theta function with zero of order 1, that we know from proposition 2.24 and we may from now on refer to it as the *canonical theta function*. And unless otherwise stated we shall make use of this as our working theta function. Set

$$\theta_N(z) = \sum_{n=-N}^{N} e^{\pi i(n^2 z + 2nz)}$$

Suppose we know the least $N = N(\epsilon)$ such that $|\theta(z) - \theta_N(z)| < \epsilon < 1$ and $|\frac{1}{\theta}(z) - \frac{1}{\theta_N}(z)| < \epsilon < 1$ for all $z \not\equiv \frac{1+\tau}{2}$. Now because the function g as defined in Weil pairings above involves $2m^2$ theta functions (namely the numerator and denominator), then to calculate $e_m(z_1, z_2)$ we are dealing with $4m^2$ theta functions. And so if we use θ_N instead of θ, we are sure that we can approximate the Weil pairing within an error of $4m^2\epsilon$.

We deal with the question of how accurate we should be in our approximation of theta function in order to arrive to the correct value of the Weil pairing. Because $e_m : E[m] \times E[m] \to \mu_m$, and that the minimum distance between two points in μ_m is $2\sin(\pi/m)$. We must choose our ϵ to be $\frac{\sin(\pi/m)}{2m^2}$

Let $z_i \in \mathcal{F}$ with $i = 1 \cdots 4m^2$ be all the values by which we want to evaluate our theta functions. Now we determine a way to compute N in case our theta function is the one in proposition 2.24. We take note of proposition 2.24 and its proof with $\tau = u + iv$. Let $y_i = \text{Im} z_i/2$, compute $y = \max\{|y_i|\}$. Also compute $m = \lceil 4\frac{y}{v} \rceil$ Let $c_i = \sum_{n=-m}^{m} e^{-\pi(n^2 v + 2ny_i)}$ for $i = 1 \cdots 4$. From the proof of proposition 2.24 we know that $|\theta(z_i) - c_i| < \frac{2}{1-q}$ where $q = e^{-\frac{\pi}{2}v}$. Now set $m_o = \min\{||c_i| - \frac{2}{1-q}|\}$. It is very likely that $m_o \neq 0$ (which is what we are hoping for, otherwise we can always play around with the values, by increasing the value of $|m|$ which plays a role on

the index of summation by which c_i are defined, to get it to be nonzero due to the fact that we know $\theta(z_i) \neq 0$ for any z_i). By this we can see that $m_o < |\theta(z_i)| \quad \forall i = 1 \cdots 4$. Now let $\epsilon' = \min\{\epsilon, \epsilon m_o | m_o - \epsilon|\}$ and choose $N = N(\epsilon')$ such that $|\theta(z_i) - \theta_N(z_i)| < \epsilon'$ (this N can be calculated to be $|\lceil[\log(\epsilon'(1-q)/2))/\log(q)]^{1/2}\rceil|$, because for $N > m$ we have $|\theta - \theta_N|(z_i) < \frac{2q^{n^2}}{1-q}$).

Notation. If we know $m \in \mathbb{N}\backslash\{1\}$ for simplicity we write $e(w, z)$ instead of $e_m(w, z)$ to denote the Weil e_m-pairing of the pair $(w, z) \in \mathcal{F}[m] \times \mathcal{F}[m]$

Example. Consider $\mathcal{F}[2] = \{0, z_1, z_2, z_3\}$ where $z_1 = 1/2, z_2 = \tau/2$ and $z_3 = z_1 + z_2$. We claim that it is necessary that $e(z_1, z_2) = -1$, otherwise we have $e(z_1, z_2) = 1$ and so $e(z_1, z_3) = e(z_1, z_1)e(z_1, z_2) = 1$ and $e(0, z_i) = 1$ for $i = 1, 2, 3$ but then we also know that the Weil pairing is a surjective map. A contradiction since we have no map to $-1 \in \mu_2$. We compute the Weil e_2-Pairing now for a specific case, using the method of approximation discussed above. Consider $\tau = i$, then we expect $e(z_1, z_2) = e(\frac{1}{2}, \frac{i}{2}) = -1$. We have

$$h(z) = \frac{\theta(z_1 + z_2/2 + z)\theta(z_2/2 + z)\theta(z_1 - z_2/2 + z)\theta(-z_2/2 + z)}{\theta(z_1 + z_2 + z)\theta(z_2 + z)\theta(z_1 + z)\theta(z)}$$

Now knowing that $e(z_1, z_2) = e^{-2\pi i z_1} h(z_1 + w)/h(w)$ for any $w \in \mathcal{F}$ so that $h(z_1 + w), h(w) \neq 0$, we choose $w = -z_1/2 = -1/2$. We can easily verify that $h(z_1 + w) = h(z_1/2)$ and $h(w) = h(-z_1/2)$ are nonzero. We now compute $h(z_1/2)$

$$h(z_1/2) = \frac{\theta(3z_1/2 + z_2/2)\theta(z_1/2 + z_2/2)\theta(3z_1/2 - z_2/2)\theta(z_1/2 - z_2/2)}{\theta(3z_1/2 + z_2)\theta(z_1/2 + z_2)\theta(3z_1/2)\theta(z_1/2)}$$

Also

$$h(-z_1/2) = \frac{\theta(z_1/2 + z_2/2)\theta(-z_1/2 + z_2/2)\theta(z_1/2 - z_2/2)\theta(-z_1/2 - z_2/2)}{\theta(z_1/2 + z_2)\theta(-z_1/2 + z_2)\theta(z_1/2)\theta(-z_1/2)}$$

Using the property of the canonical theta function ($\theta(3z_1/2 + z) = \theta(-z_1/2 + z)$, since $z_1 = 1/2$) and the fact that it is an even function. We can cancel some terms and obtain $\frac{h(z_1/2)}{h(-z_1/2)} = 1$ which clearly implies $e(z_1, z_2) = e^{-2\pi i z_1} = e^{-\pi i} = -1$ as we expected.

Remark 4.3. It can be seen from the example above that we need not have the value of τ to compute the Weil e_2-pairing, we just needed the proportion of the parameters with respect to τ. We can in fact generalize this for the Weil e_m-pairing and arrive at an interesting result. Take note that due to bilinearity and alternative property of the Weil pairing, we need only calculate $e_m(\frac{1}{m}, \frac{\tau}{m})$ to know the pairing of any two points in $\mathcal{F}[m]$ (Due to bilinearity and alternativity $e(z_1 + z_2, z_1) = e(z_2, z_1)$ and all points in $\mathcal{F}[m]$ are linear combinations of $\frac{1}{m}$ and $\frac{\tau}{m}$). The following theorem will in fact help us calculatee the Weil e_m-pairing without much difficulty.

Theorem 4.4. $e_m(\frac{1}{m}, \frac{\tau}{m}) = e^{-2\pi i/m}$ for $m \geq 2$

Proof. Let $z_1 = \frac{1}{m}$ and $z_2 = \frac{\tau}{m}$. Label elements of $\mathcal{F}[m]$ by $\mathcal{F}[m] = \{z_{jk} = \frac{j\tau + k}{m} : j, k = 0 \cdots m - 1\}$. Then $z_1 = z_{01}$ and $z_2 = z_{10}$. Now consider the function

$$h(z) = \prod_{j,k=1}^{m} \frac{\theta(z_o + z - z_2/m - z_{jk})}{\theta(z_o + z - z_{jk})} = \prod_{j=1}^{m}\prod_{k=1}^{m} \frac{\theta(z_o + z - z_2/m - z_{jk})}{\theta(z_o + z - z_{jk})}$$

Now without loss of generality we can assume that there is a $w \in \mathcal{F}$ so that $h(z_1 + w), h(w) \in \mathbb{C}^*$. We wish now to compare the two values $h(z_1 + w)$ and $h(w)$. If we denote the numerators of $h(z_1 + w)$ and $h(w)$ as $N(z_1 + w)$ and $N(w)$ respectively we see that

$$N(z_1 + w) = \prod_{j,k=1}^{m} \theta(z_o + z_1 + w - z_2/m - z_{jk}) = \prod_{j=1}^{m}\prod_{k=1}^{m} \theta(z_o + w - z_2/m - (z_{jk} - z_1)) =$$

$$\prod_{j=1}^{m}\prod_{k=1}^{m}\theta(z_o+w-z_2/m-z_{jk})=\prod_{j,k=1}^{m}\theta(z_o+w-z_2/m-z_{jk})=N(w)$$

Here we used the fact that the canonical theta function is 1-periodic on a horizantal line of the complex plane and that for a fixed $j\in\mathbb{Z}_m$ we have $\{z_{jk}:k\in\mathbb{Z}_m\}=\{z_{jk}-z_1:k\in\mathbb{Z}_m\}$ (equality taken in $\mathcal{F}$). Similarly for the denominators, thus arriving to the conclusion that $h(z_1+w)=h(w)$. So what now remains is $e^{z_1a(mz_2)}$ due to the factor of automorphy $\mu(\omega,z)=\exp(a(\omega).z+b(\omega))$. For our theta function $a(\omega)$ is dependent on the multiples of τ of $\omega\in L$. In general for $\omega=n_1\tau+n_2$ we have $a(\omega)=-2n_1\pi i$. In our case $mz_2=\tau$, so $e^{z_1a(mz_2)}=e^{-2\pi iz_1}=e^{-2\pi i/m}$. □

Corollary 4.5. Let $z_1=\frac{j_1\tau+k_1}{m},z_2=\frac{j_2\tau+k_2}{m}\in\mathcal{F}[m]$, $N=j_2k_1-j_1k_2 \bmod m$ and $\alpha=e^{-2\pi i/m}$ then $e(z_1,z_2)=\alpha^N$

Proof. It follows directly (from the alternative and bilinear property of the Weil pairing and the fact that any point of $\mathcal{F}[m]$ is a linear combination of $\frac{1}{m}$ and $\frac{\tau}{m}$) that

$$e(z_1,z_2)=e^{j_1}(\frac{\tau}{m},\frac{j_2\tau+k_2}{m})e(\frac{k_1}{m},z_2)=e^{j_1}(\frac{\tau}{m},\frac{k_2}{m})e^{k_1}(\frac{1}{m},\frac{j_2\tau+k_2}{m})$$

$$=\alpha^{-j_1k_2}e^{k_1}(\frac{1}{m},\frac{j_2\tau}{m})=\alpha^{-j_1k_2}\alpha^{k_1j_2}=\alpha^{j_2k_1-j_1k_2}=\alpha^N$$

Since α has order m. □

Corollary 4.6. From the above corollary it follows directly that since $\mathcal{F}[m]\times\mathcal{F}[m]\cong\mathbb{Z}_m^2\times\mathbb{Z}_m^2$, the Weil pairing is thus equivalent to the mapping

$$\mathbb{Z}_m^2\times\mathbb{Z}_m^2\to\mathbb{Z}_m\quad,\quad M\mapsto\det(M)$$

Moreover this mapping preserves all the properties (disregarding compatibility) listed in proposition 4.1

Remark 4.7. We can write a more general definition of divisors of elliptic curves by using an arbitrary field K as formal sum of points in the elliptic curve (instead of the fundamental parallelogram). We can also similarly make a general definition of the principal divisors (i.e. we define them as divisors of polynomials of K). Most of the results we obtained for $\mathbb{C}$ also applies for general divisors. For instance it is also true that a divisor is principal if and only if it is a zero divisor and the actual sum (based on elliptic curve group structure) of the points representing the divisor is zero.
Moreover we can generalize Weil pairings for m-torsion points of elliptic curves (instead of the points of the fundamental parallelogram) defined on any field K. Note that all the properties discussed in proposition 4.1 will still hold.

If F_q is the finite field of prime power order $q=p^k$, there is a finite extension $F_q\leq K$ such that all the m-torsion points of $E(\overline{F_q})$ are contained in $E(K)$.
Now our objective is to relate the Weil e_m-pairing of an elliptic curve defined on $\mathbb{C}$ and that defined on K. Firstly we can say that again $E(K)[m]\times E(K)[m]$ is isomorphic to $\mathbb{Z}_m^2\times\mathbb{Z}_m^2$. Let us denote the two generators of $E(K)[m]$ by g_1 and g_2 and that of $E(\mathbb{C})[m]$ by z_1 and z_2. As has been seen in corollary 4.5 the entire mapping of the pairing is determined by only knowing the pairing of each of the generator pairs mentioned above. To relate the Weil-Pairings, we thus need to relate the mappings of the generator pairs of the maps $\mathbb{Z}_m^2\times\mathbb{Z}_m^2\to\mathbb{Z}_m$. These maps must have the property mentioned in proposition 4.1.

Notation. Define the *generalized pairings* $\mathcal{W}$ as the set of the maps $e:\mathbb{Z}_m^2\times\mathbb{Z}_m^2\to\mathbb{Z}_m$ satisfying the first two (the fourth property follow by them) of proposition 4.1.

We can then immediately see

Corollary 4.8. Let $e_1, e_2 \in \mathcal{W}$, $x = (x_1, x_2), y = (y_1, y_2)$ be a generator pair of $\mathbb{Z}_m^2$ (i.e. $\langle x, y \rangle = \mathbb{Z}_m^2$). Set $g_1 = e_1(x, y)$ and $g_2 = e_2(x, y)$ with $k = g_2 g_1^{-1}$ (g_1 has a multiplicative inverse in Z_m because it will also be a generator in $\mathbb{Z}_m$). Then given $a, b \in Z_m^2$, with

$$a = j_1 x + k_1 y, b = j_2 x + k_2 y \quad \text{for some } j_1, j_2, k_1, k_2 \in \mathbb{Z}_m$$

we have the following

$$e_2(a, b) = k e_1(a, b)$$

Thus we get a relation between two Weil pairings defined on different curves and different working fields. Even though the value of k in the above corollary isn't always known in practice, we can at least know the value of a "pseudo Weil-pairing", one that satisfies the first two properties of proposition 4.1.

References

[1] **I.R. Shafarevich**, Basic Algebraic Geometry, *Varieties in Projective Space*, Springer-Verlag, 2nd Edition 1994

[2] **E. Freitag, R. Busam** Funktionentheorie, Springer-Verlag, 2.Aufl.

[3] **J.H. Silverman**, The Arithmetic of Elliptic Curves. Springer-Verlag, New York, 1986 Springer-Verlag, New York, 1986

[4] **A.J. Menezes**, Elliptic Curve Public Key Cryptosystems Springer-Verlag, 1993