TORI ARE ELLIPTIC CURVES

ASHLEY NEAL

Lattice
Let ω_1, ω_2 be complex numbers that are linearly independent over $\mathbb{R}$. Then

$$L = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2 = \{n_1\omega_1 + n_2\omega_2 \mid n_1, n_2 \in \mathbb{Z}\}$$

is called a lattice, and C/L is a torus.

Fundamental Parallelogram
The set

$$F = \{a_1\omega_1 + a_2\omega_2 \mid 0 \leq a_i < 1,\ i = 1, 2\}$$

is called a fundamental parallelogram for L.

Doubly Periodic Function
A doubly periodic function is a meromorphic function

$$f : \mathbb{C} \longrightarrow \mathbb{C} \cup \infty$$

such that

$$f(z + \omega) = f(z)$$

for all $z \in \mathbb{C}$ and all $\omega \in L$, where L is a lattice.

Divisor of a Function
If f is a not identically zero meromorphic function and $\omega \in \mathbb{C}$, then we can write

$$f(z) = a_r(z - w)^r + a_{r+1}(z - w)^{r+1} + \cdots ,$$

with $a_r \neq 0$. The residue of f at w is $r = \text{ord}_w f$, which can be positive, negative, or zero. The **divisor of a function** f is defined as

$$\text{div}(f) = \sum_{w \in F} (\text{ord}_w f)[w]$$

where F is the fundamental parallelogram for L.

Theorem 9.1. *Let f be a doubly periodic function for the lattice L and let F be a fundamental parallelogram for L.*
1. If f has no poles, then f is constant.
2. $\sum_{w \in F} \text{Res}_w f = 0$
3. If f is not identically 0,

$$\deg(\text{div}(f)) = \sum_{w \in F} \text{ord}_w f = 0$$

4. If f is not identically 0,

$$\sum_{w \in F} w \cdot \text{ord}_w f \in L$$

5. If f is not constant, then $f : \mathbb{C} \longrightarrow \mathbb{C} \cup \infty$ is surjective. If n is the sum of the orders of the poles of f in F and $z_0 \in \mathbb{C}$, then $f(z) = z_0$ has n solutions (counting multiplicities).

6. If f has only one pole in F, then this pole cannot be a simple pole.
All of the above sums over $w \in F$ have only finitely many nonzero terms.

Theorem 9.3. *Given a lattice L, define the Weirstrass $\wp$-function by*

$$\wp(z) = \wp(z; L) = \frac{1}{z^2} + \sum_{\omega \in L,\, \omega \neq 0} \left(\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2} \right).$$

Then
1. The sum defining $\wp(z)$ converses absolutely and uniformly on compact sets not containing elements of L.
2. $\wp(z)$ is meromorphic in $\mathbb{C}$ and has a double pole at each $\omega \in L$.
3. $\wp(-z) = \wp(z)$ for all $z \in \mathbb{C}$.
4. $\wp(z+\omega) = \wp(z)$ for all $\omega \in L$.
5. The set of doubly periodic functions for L is $\mathbb{C}(\wp, \wp')$. In other words, every doubly periodic function is a rational function of $\wp$ and its derivative $\wp'$.

Eisenstein Series

Let L be a lattice. For integers $k \geq 3$, define the **Eisenstein series**

$$G_k = G_k(L) = \sum_{\omega \in L,\, \omega \neq 0} \omega^{-k}.$$

The sum converses. When k is odd, the terms for ω and $-\omega$ cancel, so $G_k = 0$.

Proposition 9.7. *For $0 < |z| < \min_{0 \neq \omega \in L}(|\omega|)$,*

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

Proof. By definition,

$$\wp(z) = \frac{1}{z^2} + \sum_{\omega \in L,\, \omega \neq 0} \left(\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2} \right).$$

When $|z| < |\omega|$,

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

We know

$$\frac{1}{1-\frac{z}{\omega}} = \sum_{n=0}^{\infty} \left(\frac{z}{\omega}\right)^n$$

for $|\frac{z}{\omega}| < 1$. Differentiation both sides we get

$$\frac{\frac{1}{\omega}}{(1-\frac{z}{\omega})^2} = \sum_{n=0}^{\infty} \left(\frac{1}{\omega}\right)^n n(z)^{n-1} = \sum_{n=1}^{\infty} n \frac{z^{n-1}}{\omega^n}.$$

Therefore,

$$\frac{1}{(1-\frac{z}{\omega})^2} = \sum_{n=1}^{\infty} n \frac{z^{n-1}}{\omega^{n-1}} = \sum_{n=0}^{\infty} (n+1) \frac{z^n}{\omega^n}.$$

So

$$\frac{1}{(1-\frac{z}{\omega})^2} - 1 = \left(\sum_{n=0}^{\infty} (n+1) \frac{z^n}{\omega^n} \right) - 1 = \left(1 + \sum_{n=1}^{\infty} (n+1) \frac{z^n}{\omega^n} \right) - 1 = \sum_{n=1}^{\infty} (n+1) \frac{z^n}{\omega^n}.$$

Then

$$\wp(z) = \frac{1}{z^2} + \sum_{\omega \in L,\, \omega \neq 0} \omega^{-2} \sum_{n=1}^{\infty} (n+1) \frac{z^n}{\omega^n} = \frac{1}{z^2} + \sum_{\omega \in L, \omega \neq 0} \sum_{n=1}^{\infty} (n+1) \frac{z^n}{\omega^{n+2}}.$$

Switching the order of the summations an factoring out constants yields

$$\wp(z) = \frac{1}{z^2} + \sum_{n=1}^{\infty} (n+1) z^n \sum_{\omega \neq 0, \omega \in L} \omega^{-(n+2)} = \frac{1}{z^2} + \sum_{n=1}^{\infty} (n+1) z^n G_{n+2}.$$

Since when k is odd, $G_k = 0$, we can let $n = 2j$, so

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

□

Theorem 9.8. *Let $\wp(z)$ be the Weierstrass $\wp$-function for a lattice L. Then,*

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

Proof. From Proposition 9.7, we know

$$\wp(z) = z^{-2} + 3G_4 z^2 + 5G_6 z^4 + \cdots .$$

Differentiating, we get

$$\wp'(z) = -2z^{-3} + 6G_4 z + 20G_6 z^3 + \cdots .$$

So

$$\wp(z)^3 = z^{-6} + 9G_4 z^{-2} + 15G_6 + \cdots$$

and

$$\wp'(z)^2 = 4z^{-6} - 24G_4 z^{-2} - 80G_6 + \cdots .$$

Let

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

$$= (4z^{-6} - 24G_4 z^{-2} - 80G_6 + \cdots) + (-4z^{-6} - 36G_4 z^{-2} - 60G_6 + \cdots) + (60G_4 z^{-2} + 180G_4 z^2 + 300G_6 z^4 + \cdots) + (140G_6)$$

$$= 0z^{-6} + 0z^{-2} + 0 + c_1 z + c_2 z^2 + \cdots$$

Therefore $f(z)$ is a power series with no constant term and no negative powers of z. The only possible poles of $f(z)$ are the poles of $\wp(z)$ and $\wp'(z)$, which are each $\omega \in L$. $f(z)$ has no pole at 0. By 9.3, $f(z)$ is doubly periodic, so $0 \in L \implies f(\omega) = f(0)$ for all $\omega \in L$. Therefore $f(z)$ has no poles. By theorem 9.1, $f(z)$ is constant. Since $f(z)$ has no constant term, $f(0) = 0$. Therefore $f(z)$ is identically 0. Hence,

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

□

Setting $g_2 = 60G_4$ and $g_3 = 140G_6$ gives

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

therefore, $(\wp(z), \wp'(z))$ lie on the curve

$$y^2 = 4x^3 - g_2 x - g_3.$$

Proposition 9.9. $\triangle \neq 0$

Proof. $\triangle = 16(g_2^3 - 27g_3^2)$ so we need to show $g_2^3 - 27g_3^2 \neq 0$. $\wp'(z)$ is doubly periodic and $w_i \in L$, so letting $z = -\frac{\omega_i}{2}$ gives

$$\wp'\left(\frac{\omega_i}{2}\right) = \wp'\left(w_i - \frac{\omega_i}{2}\right) = \wp\left(-\frac{\omega_i}{2}\right).$$

Since $\wp'(-z) = -\wp'(z)$,

$$\wp'\left(\frac{\omega_i}{2}\right) = \wp\left(-\frac{\omega_i}{2}\right) = -\wp'\left(\frac{\omega_i}{2}\right).$$

Therefore,

$$\wp'\left(\frac{\omega_i}{2}\right) = 0,\ i = 1, 2, 3.$$

Since $\wp'(z)^2 = 4\wp(z)^3 - g_2\wp(z) - g_3$ we see $\wp'(\frac{\omega_i}{2})$ is a root of $4x^3 - g_2x - g_3$. If we can show the 3 roots are distinct, then $\triangle \neq 0$. Let

$$h_i(z) = \wp(z) - \wp(\frac{\omega_i}{2}).$$

Then

$$h_i\left(\frac{\omega_i}{2}\right) = \wp\left(\frac{\omega_i}{2}\right) - \wp\left(\frac{\omega_i}{2}\right) = 0$$

and $h_i'(z) = \wp'(z)$ implies

$$h_i'\left(\frac{\omega_i}{2}\right) = \wp'\left(\frac{\omega_i}{2}\right) = 0.$$

Therefore h_i vanishes to order at least 2 at $\frac{\omega_i}{2}$, so $\frac{\omega_i}{2}$ is a double root of h_i. But by 9.1 (5), h_i only has 2 zeros counting multiplicities (since $h_i(z)$ only has a double pole at $z = 0$). Thus $\frac{\omega_i}{2}$ is the only zero of $h_i(z)$. So

$$h_i\left(\frac{\omega_j}{2}\right) \neq 0$$

when $j \neq i$. Therefore $\wp(\frac{\omega_i}{2})$ are distinct. □

The proposition implies $E : y^2 = 4x^3 - g_2x - g_3$ is the equation of an elliptic curve. Since $\wp(z), \wp'(z)$ depend only on $z \mod L$, we have a function from $\mathbb{C}/L$ to $E(\mathbb{C})$.

Theorem 9.10. *Let L be a lattice and let E be the elliptic curve $y^2 = 4x^3 - g_2x - g_3$. The map*

$$\Phi : \mathbb{C}/L \longrightarrow E(\mathbb{C})$$

$$z \longmapsto (\wp(z), \wp'(z))$$

$$0 \longmapsto \infty$$

is an isomorphism of groups.

Proof. To show Φ is an isomorphism of groups, we must show it is (1) onto, (2) one to one, and a (3) homomorphism.

(1) We will start by showing Φ is onto. Let $(x, y) \in E(\mathbb{C})$. Then $\wp(z) - x$ has a double pole by by 9.3 (2), and therefore has zeros by 9.1 (5). So there exists $z \in \mathbb{C}$ such that $\wp(z) = x$. Since $(x, y) \in E(\mathbb{C})$ and $y^2 = 4x^3 - g_2x - g_2$, by 9.8,

$$\wp'(z)^2 = 4\wp(z)^3 - g_2\wp(z) - g_3 = 4x^3 - g_2x - g_3 = y^2.$$

Therefore $y^2 = \wp'(z)^2$, so $\wp'(z) = \pm y$. If $\wp'(z) = y$, then there exist z such that $(x, y) = (\wp(z), \wp'(z))$, so $z \longmapsto (x, y)$. If $\wp'(z) = -y$, then $\wp(-z) = \wp(z) = x$ since $\wp$ is even and $\wp'(-z) = -\wp(z) = -(-y) = y$ since $\wp'$ is odd. Therefore, there exists z such that $(x, y) = (\wp(-z), \wp'(-z))$, so $-z \longmapsto (x, y)$.

(2) Next we will show Φ is one to one. Assume $(\wp(z_1), \wp'(z_1)) = (\wp(z_2), \wp'(z_2))$ for $z_1, z_2 \in \mathbb{C}$. Then $\wp(z_1), \wp(z_2)$ and $\wp'(z_1) = \wp'(z_2)$. $\wp(z)$ only has poles at $z \in L$. Therefore, if z_1 is a pole of p, then $z_1 \in L$ and $z_2 \in L$, so $z_1 \equiv z_2 \mod L$.

Now assume z_1 is not a pole of $\wp$, so $z_1 \notin L$. Consider the function

$$h(z) = \wp(z) - \wp(z_1).$$

It has a double pole at $z = 0$ and no other poles in F (the fundamental parallelogram). Therefore $h(z)$ has exactly 2 zeros by 9.1 (5).

Suppose $z_1 = \frac{\omega_i}{2}$ for some i. Since $\wp'(\frac{\omega_i}{2}) = 0$ for $i = 1, 2, 3$ by the proof of 9.9, so $\wp'(z_1) = \wp'(\frac{\omega_i}{2}) = 0$ implies z_1 is a double root of $h(z)$. Therefore z_1 is the only root. $0 = \wp(z_1) = \wp(z_2)$ implies z_2 is a root, therefore $z_1 = z_2$.

Finally suppose z_1 is not of the form $\frac{\omega_i}{2}$. We see that $h(-z_1) = \wp(-z_1) - \wp(z_1) = \wp(z_1) - \wp(z_1) = 0$ because $\wp$ is even and $h(z_1) = \wp(z_1) - \wp(z_1) = 0$. Since $h(-z_1) = h(z_1) = 0$, and since $z_1 \not\equiv -z_1 \mod L$, the two zeros of h are z_1 and $-z_1 \mod L$. But $h(z_2) = \wp(z_2) - \wp(z_1) = \wp(z_1) - \wp(z_1) = 0$ implies that $z_2 \equiv -z_1 \mod L$ which means

$$y = \wp'(z_2) = \wp'(-z_1) = -\wp'(z_1) = -y.$$

So $\wp'(z_1) = y = 0$. But $\wp(z)$ only has a triple pole, so it only has 3 zeros in F. From the proof of 9.9 we know these zeros occur at $\frac{\omega_i}{2}$. Since z_1 is not of the form $\frac{\omega_i}{2}$, this is a contradiction. Hence in all cases $z_1 \equiv z_2 \mod L$ and Φ is injective.

(3) We will now show that Φ is a group homomorphism. Let $z_1, z_2 \in \mathbb{C}$ and let

$$\Phi(z_i) = P_i.$$

First we will only worry about when P_1, P_2 are finite and the line through P_1, P_2 intersects E in 3 distinct finite points (this means that $P_1 \neq \pm P_2$, that $2P_1 + P_2 \neq \infty$, and that $P_1 + 2P_2 \neq \infty$). For a fixed z_1, this excludes only finitely many values of z_2.

Let $y = ax + b$ be the line though P_1, P_2. Let P_3 be the third point of intersection of this line with E and let $P_3 = \Phi(z_3)$ with $z_3 \in \mathbb{C}$. Then consider

$$\ell(z) = \wp'(z) - \wp(z) - b.$$

$\ell(z)$ has zeros at the intersection points of the line $y = ax + b$ and E. Therefore, $\ell(z)$ has zeros at z_1, z_2, z_3. Since $\ell(z)$ has a triple pole at 0, and no other poles, it has 3 zeros in F by 9.1(5). Therefore,

$$div(\ell) = [z_1] + [z_2] + [z_3] - 3[0].$$

Then by 9.1(4), $z_1 + z_2 + z_3 \in L$. So

$$\wp(z_1 + z_2) = \wp(z_1 + z_2 + z_3 - z_3) = \wp((z_1 + z_2 + z_3) + (-z_3)) = \wp(-z_3) = \wp(z_3)$$

since $\wp$ is doubly periodic and even. Also,

$$\wp'(z_1 + z_2) = \wp'(z_1 + z_2 + z_3 - z_3) = \wp'((z_1 + z_2 + z_3) + (-z_3)) = \wp'(-z_3) = -\wp'(z_3)$$

since $\wp$ is doubly periodic and odd. Then

$$\Phi(z_1 + z_2) = (\wp(z_1 + z_2), \wp'(z_1 + z_2)) = (\wp(z_3), -\wp'(z_3)) = -P_3 = P_1 + P_2 = \Phi(z_1) + \Phi(z_2).$$

Therefore Φ is a group homomorphism. Although we excluded certain values of z_i, continuity ensures that this holds for all values of z_i.

The cases involving infinity are easily verified. Then we will consider the case when $P_1 = P_2$ and $y_1 \neq 0$.

Let $y = ax + b$ be the line tangent to E at P_1. Let P_3 be the other point of intersection of this line with E and let $P_3 = \Phi(z_3)$ with $z_3 \in \mathbb{C}$. Then

$$\ell(z) = \wp'(z) - \wp(z) - b.$$

has zeros at z_1, z_3 and z_1 has order 2 since $y = ax + b$ is the line tangent to E at P_1. $\ell(z)$ still has 3 zeros in F. Therefore,

$$div(\ell) = 2[z_1] + [z_3] - 3[0].$$

Then by 9.1(4), $2z_1 + z_3 \in L$. So

$$\wp(2z_1) = \wp(2z_1 + z_3 - z_3) = \wp(-z_3) = \wp(z_3)$$

and

$$\wp'(2z_1) = \wp'(2z_1 + z_3 - z_3) = \wp'(-z_3) = -\wp'(z_3).$$

Then

$$\Phi(z_1 + z_1) = (\wp(2z_1), \wp'(2z_1)) = (\wp(z_3), -\wp'(z_3)) = -P_3 = P_1 + P_1 = \Phi(z_1) + \Phi(z_1).$$

□

References: Elliptic Curves: Number Theory and Cryptography by Lawrence C. Washington