Math 7359 (Elliptic Curves and Modular Forms)

Lecture #21 of 24 $\sim$ November 27, 2023

Elliptic Curves via the Weierstrass $\wp$-Function

- Elliptic Curves and Elliptic Functions

Recall the Weierstrass $\wp$-Function, I

So now let's define some things:

Definition

Let ω_1, ω_2 are $\mathbb{R}$-linearly independent complex numbers and $\Lambda = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2$ be the associated complex lattice.

The Weierstrass $\wp$-function (with respect to Λ) is defined to be $\wp(z;\Lambda) = \dfrac{1}{z^2} + \displaystyle\sum_{\omega\in\Lambda*}\left[\dfrac{1}{(z-\omega)^2} - \dfrac{1}{\omega^2}\right]$.

The Eisenstein series of weight $2k$ (with respect to Λ) is $G_{2k}(\Lambda) = \displaystyle\sum_{\omega\in\Lambda*}\dfrac{1}{\omega^{2k}}$ *where the sums are over all nonzero $\omega \in \Lambda$.*

- When Λ is clear from context, we will just write $\wp(z)$ in place of $\wp(z;\Lambda)$ and G_{2k} in place of $G_{2k}(\Lambda)$.
- We index as G_{2k} because the G_{2k-1} are all zero.

Recall the Weierstrass $\wp$-Function, II

Theorem (Properties of $\wp$ and G_{2k}, Part 1)

Let Λ be a complex lattice with

$$\wp(z;\Lambda) = \frac{1}{z^2} + \sum_{\omega\in\Lambda*}\left[\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2}\right] \text{ and } G_{2k}(\Lambda) = \sum_{\omega\in\Lambda*}\frac{1}{\omega^{2k}}$$

1. *The Eisenstein series $G_{2k}(\Lambda)$ is absolutely convergent for $k > 1$ but not for $k \leq 1$.*
2. *The series defining $\wp(z)$ converges absolutely and uniformly on compact subsets of $\mathbb{C}\backslash\Lambda$.*
3. *The $\wp$-function is meromorphic on $\mathbb{C}$ with a double pole with residue 0 at each point of Λ (and no other poles).*
4. *The $\wp$-function is an even function: $\wp(-z) = \wp(z)$.*

Recall the Weierstrass $\wp$-Function, III

Theorem (Properties of $\wp$ and G_{2k}, Part 2)

Let Λ be a complex lattice with

$$\wp(z;\Lambda) = \frac{1}{z^2} + \sum_{\omega\in\Lambda*}\left[\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2}\right] \textit{ and } G_{2k}(\Lambda) = \sum_{\omega\in\Lambda*}\frac{1}{\omega^{2k}}$$

5. *The derivative* $\wp'(z) = -2\sum_{\omega\in\Lambda}\frac{1}{(z-\omega)^3}$ *is an odd function with a triple pole at each point of Λ (and no other poles).*
6. *The $\wp$-function and its derivative are elliptic functions with respect to Λ.*
7. *The field of even elliptic functions $\mathbb{C}(\Lambda)$ is equal to $\mathbb{C}(\wp(z))$.*
8. *The field of elliptic functions $\mathbb{C}(\Lambda)$ is equal to $\mathbb{C}(\wp(z), \wp'(z))$.*

Elliptic Curves via $\wp$, I

The goal of this entire construction was to find the analogues of the coordinate functions x and y on $\mathbb{C}/\Lambda$.

- Since $\wp(z)$ has a double pole at 0 and $\wp'(z)$ has a triple pole at 0, these two functions are natural candidates for x and y, following the Riemann-Roch analogy (in which x was constructed as an element of $L(2P)$ not in $L(P)$ and y was constructed as an element of $L(3P)$ not in $L(2P)$).
- We therefore can hope that there exists a relation of the form $\wp'(z)^2 = \wp(z)^3 + A\wp(z) + B$ for some constants A and B (which necessarily will depend on the lattice).

Elliptic Curves via $\wp$, II

Indeed, we know there must be some algebraic relation between $\wp(z)$ and $\wp'(z)$, because $\wp'(z)^2$ is an even elliptic function, hence by (7) in the proposition above it must be a rational function of $\wp(z)$.

- We can use (7) to compute the precise relation, which requires only understanding the zeroes and poles of $\wp'(z)$. This will give us one form of the cubic expression we seek.
- Alternatively, we could simply calculate the Laurent expansions of each of the terms near $z = 0$ and compute an appropriate linear combination that is holomorphic: then it will be a holomorphic elliptic function hence constant. This will give us a second form of the cubic expression.

Elliptic Curves via $\wp$, III

Theorem (Elliptic Curves and $\wp$-Functions)

Let $\Lambda = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2$ *be a complex lattice with*

$$\wp(z) = \frac{1}{z^2} + \sum_{\omega \in \Lambda*} \left[\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2} \right], \; G_{2k} = \sum_{\omega \in \Lambda*} \frac{1}{\omega^{2k}}. \text{ Then:}$$

1. *The derivative* $\wp'(z)$ *has three single zeroes, located at the nonzero half-lattice points* $\omega_1/2$, $\omega_2/2$, $(\omega_1+\omega_2)/2$.
2. *We have* $\wp'(z)^2 = 4(\wp(z)-e_1)(\wp(z)-e_2)(\wp(z)-e_3)$ *for* $e_1 = \wp(\omega_1/2)$, $e_2 = \wp(\omega_2/2)$, *and* $e_3 = \wp((\omega_1+\omega_2)/2)$.
3. *The Laurent series for* $\wp(z)$ *around* $z=0$ *is given by* $\wp(z) = z^{-2} + \sum_{k=1}^{\infty}(2k+1)G_{2k+2}z^{2k}$.
4. *We have* $\wp'(z)^2 = 4\wp(z)^3 - 60G_4\wp(z) - 140G_6$.
5. *For* $g_2 = 60G_4$ *and* $g_3 = 140G_6$, *the polynomial* $f(x) = 4x^3 - g_2x - g_3$ *has distinct roots, so* $y^2 = f(x)$ *is an elliptic curve.*

Elliptic Curves via $\wp$, IV

1. The derivative $\wp'(z)$ has three single zeroes, located at the nonzero half-lattice points $\omega_1/2$, $\omega_2/2$, $(\omega_1+\omega_2)/2$.

Proof:

- We have already shown that $\wp'(z)$ has a triple pole at 0, and so it must also have three zeroes.
- From the fact that $\wp'$ is both elliptic and odd, we can see that $\wp'(\omega_1/2) = \wp'(\omega_1/2 - \omega_1) = \wp'(-\omega_1/2) = -\wp'(\omega_1/2)$, and so $\wp'(\omega_1/2) = 0$.
- Likewise we also have $\wp'(\omega_2/2) = 0$ and $\wp'((\omega_1+\omega_2)/2) = 0$, and so $\wp'$ has zeroes at the nonzero half-lattice points $\omega_1/2$, $\omega_2/2$, $(\omega_1+\omega_2)/2$. Since $\wp'$ only has three zeroes, these are all of the zeroes.

Elliptic Curves via $\wp$, V

2. We have $\wp'(z)^2 = 4(\wp(z) - e_1)(\wp(z) - e_2)(\wp(z) - e_3)$ for $e_1 = \wp(\omega_1/2)$, $e_2 = \wp(\omega_2/2)$, and $e_3 = \wp((\omega_1 + \omega_2)/2)$.

Proof:

- Applying the proof of (7), for $e_1 = \wp(\omega_1/2)$, $e_2 = \wp(\omega_2/2)$, and $e_3 = \wp((\omega_1 + \omega_2)/2)$, the function $(\wp(z) - e_1)(\wp(z) - e_2)(\wp(z) - e_3)$ has the same zeroes and same zero multiplicities as $\wp'(z)^2$, and both functions also have a pole of order 6 at 0, so they are equal up to a scalar.
- To find this constant factor observe $\wp(z) = z^{-2} + O(z^{-1})$ while $\wp'(z) = -2z^{-3} + O(z^{-2})$ near $z = 0$, so $(\wp(z) - e_1)(\wp(z) - e_2)(\wp(z) - e_3) = z^{-6} + O(z^{-5})$ while $\wp'(z)^2 = 4z^{-6} + O(z^{-5})$.
- Hence the constant factor is the ratio of the coefficients, which is 4.

Elliptic Curves via $\wp$, VI

3. The Laurent series for $\wp(z)$ around $z = 0$ is given by $\wp(z) = z^{-2} + \sum_{k=1}^{\infty}(2k+1)G_{2k+2}z^{2k}$.

Proof:

- For z closer to 0 than the nearest nonzero $\omega \in \Lambda^*$, we have

$$\begin{aligned}
\wp(z) - z^{-2} &= \sum_{\omega\in\Lambda*}\left[\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2}\right] \\
&= \sum_{\omega\in\Lambda*}\left[\frac{1}{\omega^2}\cdot\frac{1}{(1-z/\omega)^2} - \frac{1}{\omega^2}\right] \\
&= \sum_{\omega\in\Lambda*}\left[\sum_{n=1}^{\infty}(n+1)\frac{z^n}{\omega^{n+2}}\right] \\
&= \sum_{n=1}^{\infty}(n+1)z^n\sum_{\omega\in\Lambda*}\left[\frac{1}{\omega^{n+2}}\right] = \sum_{n=1}^{\infty}(n+1)G_{n+2}z^n
\end{aligned}$$

where we switched the order using absolute convergence.

Elliptic Curves via $\wp$, VII

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

Proof:

- Using $\wp(z) = z^{-2} + \sum_{k=1}^{\infty}(2k+1)G_{2k+2}z^{2k}$ we see that

$$\begin{aligned}
\wp(z) &= z^{-2} + 3G_4z^2 + 5G_6z^4 + \cdots \\
\wp(z)^2 &= z^{-4} + 6G_4 + 10G_6z^2 + \cdots \\
\wp(z)^3 &= z^{-6} + 9G_4z^{-2} + 15G_6 + \cdots \\
\wp'(z) &= -2z^{-3} + 6G_4z + 20G_6z^3 + \cdots \\
\wp'(z)^2 &= 4z^{-6} - 24G_4z^{-2} - 40G_6 + \cdots
\end{aligned}$$

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

- Hence the difference is a holomorphic elliptic function hence constant hence equal to $140G_6$, its value at 0.

Elliptic Curves via $\wp$, VIII

5. For $g_2 = 60G_4$ and $g_3 = 140G_6$, the polynomial $f(x) = 4x^3 - g_2x - g_3$ has distinct roots, so $y^2 = f(x)$ is an elliptic curve.

Proof:

- From (2) the roots of $f(x)$ are the values $e_1 = \wp(\omega_1/2)$, $e_2 = \wp(\omega_2/2)$, and $e_3 = \wp((\omega_1 + \omega_2)/2)$, so we need only see they are distinct.
- For this we observe that $\wp(z) - \wp(\omega_i/2)$ is even hence has a double zero at ω_i, but since its total pole order is 2, we see it only vanishes at ω_i. In particular, it does not vanish at the other two half-lattice points, and so e_1, e_2, e_3 are distinct.

Elliptic Curves via $\wp$, X

The proposition above establishes an explicit correspondence between complex tori $\mathbb{C}/\Lambda$ and complex elliptic curves E, via the Weierstrass $\wp$-function and its derivative. In fact, this correspondence is natural, in both the category of Riemann surfaces and in the category of groups.

Theorem (Elliptic Curves and $\wp$-Functions)

Let Λ be a complex lattice with $g_2 = 60G_4$ and $g_3 = 140G_6$ and let E be the elliptic curve $y^2 = 4x^3 - g_2x - g_3$. Define the map $\Phi : \mathbb{C}/\Lambda \to E(\mathbb{C})$ via $\Phi(z) = (\wp(z), \wp'(z))$, with $\Phi(0) = \infty$.

1. *The map Φ is a bijection.*
2. *The map Φ is a globally analytic isomorphism of Riemann surfaces.*
3. *The map Φ is a group isomorphism.*

Elliptic Curves via $\wp$, XI

1. The map $\Phi(z) = (\wp(z), \wp'(z))$ is a bijection from $\mathbb{C}/\Lambda \to E(\mathbb{C})$.

Proof (surjection):

- Since $\wp'(z)^2 = 4\wp(z)^3 - g_2\wp(z) - g_3$, the image of Φ is a subset of $E(\mathbb{C})$.
- To show Φ is onto, choose a finite point $(x, y) \in E(\mathbb{C})$: then $\wp(z) - x$ is a nonconstant elliptic function hence has a zero, say at $z = a$.
- Then $\wp'(a)^2 = 4a^3 - g_2a - g_3 = y^2$ so (swapping a for $-a$ if needed) we have $\wp'(a) = y$: then $\Phi(a) = (x, y)$.

Elliptic Curves via $\wp$, XI

1. The map $\Phi(z) = (\wp(z), \wp'(z))$ is a bijection from $\mathbb{C}/\Lambda \to E(\mathbb{C})$.

Proof (injection):

- To show Φ is one-to-one, if $\Phi(z_1) = \Phi(z_2)$ then $\wp(z) - \wp(z_1)$ is an elliptic function vanishing at z_1, $-z_1$, and z_2. Since it only has order 2, two of these points must be equivalent modulo Λ.
- If $2z_1 \notin \Lambda$ then we see $z_2 \equiv \pm z_1 \pmod{\Lambda}$, in which case $\wp'(z_1) = \wp'(z_2) = \wp'(\pm z_1) = \pm\wp'(z_1)$ so we must have the plus sign, and so $z_2 = z_1$ in $\mathbb{C}/\Lambda$.
- If $2z_1 \in \Lambda$ then as noted in (5), $\wp(z) - \wp(z_1)$ has a double zero at z_1, so since it vanishes also at z_2, we again have $z_2 = z_1$ in $\mathbb{C}/\Lambda$.

Elliptic Curves via $\wp$, XI

2. The map $\Phi(z) = (\wp(z), \wp'(z))$ is a globally analytic isomorphism of Riemann surfaces $\mathbb{C}/\Lambda \to E(\mathbb{C})$.

Proof:

- To show Φ is an analytic isomorphism, observe that $\Phi^*(\frac{dx}{y}) = \frac{d\wp(z)}{\wp'(z)} = \frac{\wp'(z)\,dz}{\wp'(z)} = dz$, so Φ^* maps the invariant differential of $E(\mathbb{C})$ to the invariant differential dz of $\mathbb{C}/\Lambda$.
- This means Φ is locally an analytic isomorphism, and since Φ is a bijection from (1), it is a global isomorphism.

Elliptic Curves via $\wp$, XI

3. The map $\Phi(z) = (\wp(z), \wp'(z))$ is a group isomorphism from $\mathbb{C}/\Lambda \to E(\mathbb{C})$.

Proof (part 1):

- By (1) we need only show that Φ is a homomorphism. Let $z_1, z_2 \in \mathbb{C}$: per the geometric group law, this requires showing that $\Phi(z_1)$, $\Phi(z_2)$, $\Phi(-z_1 - z_2)$ are the three intersection points of a line with E.
- If $z_1 = 0$ or $z_2 = 0$ then the result follows by noting $\Phi(-z) = (\wp(-z), \wp'(-z)) = (\wp(z), -\wp'(z)) = -\Phi(z)$, and the case $z_1 = -z_2$ follows in the same way.

Elliptic Curves via $\wp$, XI

3. The map $\Phi(z) = (\wp(z), \wp'(z))$ is a group isomorphism from $\mathbb{C}/\Lambda \to E(\mathbb{C})$.

Proof (part 2):

- Otherwise, if the line through $\Phi(z_1)$ and $\Phi(z_2)$ is $y = mx + b$ then the elliptic function $\wp'(z) - m\wp(z) - b$ has a triple pole at 0 hence has exactly three zeroes, two of which are z_1 and z_2. (If $z_1 = z_2$ this argument is still valid, as long as we use the tangent line and count with multiplicity.)
- But by property (5) of elliptic functions, summing the coordinates of all zeroes and poles yields an element of Λ: hence the remaining zero must be $-z_1 - z_2$ modulo Λ, so the third point is indeed $\Phi(-z_1 - z_2)$ as required.

So What Was The Point Of This?, I

The point of all of this discussion is that we now have an explicit parametrization of the points on the elliptic curve $E/\mathbb{C}$ having Weierstrass equation $y^2 = 4x^3 - g_2x - g_3$, namely as $(x, y) = (\wp(z), \wp'(z))$ for $z \in \mathbb{C}/\Lambda$.

- Indeed, this was Weierstrass' initial motivation for constructing $\wp(z)$ in the first place: to give a parametrization of the points on an elliptic curve.
- This is essentially the nicest possible form of a parametrization for the points on $E/\mathbb{C}$, since the parameter functions are meromorphic.
- Really, the only thing nicer would be if they were actually rational functions, but a rational parametrization would give an isomorphism with $\mathbb{P}^1(\mathbb{C})$ hence is only possible in genus 0.

So What Was The Point Of This?, II

Indeed, this development nicely parallels the genus-0 case for the circle $x^2 + y^2 = 1$, which has a parametrization $x = \cos z$, $y = \sin z$ for $x \in \mathbb{C}/2\pi i\mathbb{Z}$.

- In the genus-0 case, the parameter functions are also obtained by inverting the integrals of the differential $\omega = dx/y$: here $\int_C dx/y = \int_C \frac{dx}{\sqrt{1-x^2}}$ is the well-understood inverse sine integral that can be made well-defined using a branch cut from -1 to 1. (Then, up to sign, the other parameter function is obtained as the derivative of the first.)
- In our genus-1 case, the parameter function $\wp$ (up to a minus sign) is obtained instead by inverting the elliptic integral $\int_C dx/y = \int_C \frac{dx}{\sqrt{4x^3-g_2x-g_3}}$.

Let's Do Isogenies!, I

Our next task is to bring isogenies into the discussion.

- We have a very robust correspondence between $\mathbb{C}$ modulo lattices and elliptic curves over $\mathbb{C}$, so we should expect that the natural morphisms in the category of elliptic curves (namely, isogenies) should have an equally natural counterpart for lattices.
- Since the correspondence respects the group structures, we are seeking an analytic mapping that sends lattices to other lattices.
- The only obvious analytic maps with this property are linear transformations (as any nonlinear function will distort the lattice structure), and since they must be analytic and preserve 0, they could only be scalings $\varphi_\alpha(z) = \alpha z$ for some $\alpha \in \mathbb{C}$.
- We now show that indeed, complex scalings on lattices correspond to isogenies of elliptic curves.