

Notes on elliptic curves and modular forms

David Pierce

Spring 1999

'In the future, elliptic curves will be as well-known as conics are now.'

Here is a summary of some results expounded in [1] and [2]: ultimately, the uniformization theorem for elliptic curves over \mathbf{C} .

1 A **lattice** is a maximal discrete subgroup of \mathbf{C} . Let Λ be the lattice $\langle \omega_0, \omega_1 \rangle$, so that ω_0 and ω_1 are \mathbf{R} -linearly independent. In the following, the qualification 'with respect to Λ ' is often implicit.

2 An **elliptic function** is meromorphic and well-defined on the torus \mathbf{C}/Λ . Then an entire elliptic function is bounded, hence constant.

3 The **Weierstrass \wp -function** is given by

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

where $\Lambda' = \Lambda \setminus \{0\}$. The series converges normally since $\sum_{\omega \in \Lambda'} 1/|\omega^3|$ converges. The \wp -function is even. Its derivative is given by

$$\wp'(z) = \sum_{\omega \in \Lambda} \frac{1}{(z - \omega)^3},$$

and is elliptic (and odd); therefore \wp is elliptic.

4 If f is an elliptic function, let P be a **fundamental parallelogram**

$$\{b + t_0\omega_0 + t_1\omega_1 : t_0, t_1 \in [0, 1]\}$$

such that no zeros or poles of f or f' are on ∂P . Then

- $\sum_{a \in \mathbf{C}/\Lambda} \text{ord}_a f = \frac{1}{2\pi i} \int_{\partial P} \frac{df}{f} = 0$;
- $\int_{\partial P} (f) = \sum_{a \in \mathbf{C}/\Lambda} (\text{ord}_a f) a = \frac{1}{2\pi i} \int_{\partial P} z \frac{f'(z)}{f(z)} dz \equiv 0 \pmod{\Lambda}$.

5 Let $\omega_2 = \omega_0 + \omega_1$ and let $e_i = \omega_i/2$ for i in $\{0, 1, 2\}$.

- \wp has a double pole at 0 and no other poles; hence it has either a double zero at one of the e_i , or a single zero at some other point and its negative; and \wp has no other zeros.
- \wp' has a triple pole at 0 and no other poles, and has a single zero at each e_i and no other zeros.

6 The field of elliptic functions is $\mathbf{C}(\wp, \wp')$. For, if f is an even elliptic function, then f is a multiple of

$$\prod_{a \in \mathbf{C}/\Lambda} (\wp(z) - \wp(a))^{(\text{ord}_a f)/2},$$

and $\text{ord}_a f$ is even if $2a \in \Lambda$; so $f \in \mathbf{C}(\wp)$.

7 The **Eisenstein series** $G_k(\Lambda)$ is $\sum_{\omega \in \Lambda'} 1/\omega^{2k}$, which converges when $k > 1$. Hence the \wp -function has the series-expansion

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

8 From this expansion follows

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

where $g_2 = 60G_2$ and $g_3 = 140G_3$, since the difference of the members of the equation has no polar or constant term.

9 The **discriminant** Δ is $g_2^3 - 27g_3^2$, and is nonzero since \wp' has three distinct roots.

10 The map $z \mapsto (\wp(z), \wp'(z))$ is an isomorphism of \mathbf{C}/Λ onto an **elliptic curve**. The induced group-structure is given by

$$4(\wp(a) + \wp(b) + \wp(a+b)) = \lambda^2,$$

where $\lambda = (\wp'(b) - \wp'(a))/(\wp(b) - \wp(a))$ if $\wp(a) \neq \wp(b)$. For, each member of the equation will be minus the coefficient of \wp^2 in

$$4\wp^3 - g_2\wp - g_3 - (\lambda(\wp - \wp(a)) + \wp'(a))^2,$$

that is, $\wp'^2 - (\lambda(\wp - \wp(a)) + \wp'(a))^2$, whose factor

$$\wp' - \lambda(\wp - \wp(a)) + \wp'(a)$$

is zero at a , b and c such that $a + b + c \equiv 0 \pmod{\Lambda}$, so $\wp(a+b) = \wp(c)$.

11 Lattices are **homothetic** if one is a multiple of the other. Then in fact lattices are homothetic if and only if the corresponding elliptic curves are isomorphic.

12 Every lattice is homothetic to $\langle \tau, 1 \rangle$ for some τ in the **upper half-plane**, the set \mathfrak{H} comprising z with $\text{Im } z > 0$.

13 The **modular group** Γ is $\text{SL}_2(\mathbf{Z})/\langle -I \rangle$, and acts on \mathfrak{H} by the rule

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} z = \frac{az + b}{cz + d}.$$

14 $\Gamma = \langle S, T \rangle$, where $S = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ and $T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$. For, this group carries every element of \mathfrak{H} into the set D comprising z such that $|\text{Re } z| \leq 1/2$ and $|z| \geq 1$; moreover, if $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma$, then

$$\text{Im} \left(\begin{pmatrix} a & b \\ c & d \end{pmatrix} z \right) = |cz + d|^{-2} \text{Im } z,$$

so only S and T can take one element of D to another.

15 The set D is a **fundamental domain** for the action of Γ on \mathfrak{H} . Two distinct elements of D are congruent *modulo* Γ if and only if they are on ∂D and have the same absolute value and imaginary part. The stabilizer $I(z)$ of a point z of D is trivial, except:

- $I(i) = \langle S \rangle$, which has order 2;
- $I(\rho) = \langle ST \rangle$, which has order 3, where $\rho = e^{2\pi i/3}$;
- $I(-\bar{\rho}) = \langle TS \rangle$, which has order 3.

16 The map $\tau \mapsto \langle \tau, 1 \rangle$ is a bijection of $\Gamma \backslash \mathfrak{H}$ onto the set of homothety-classes of lattices.

17 A **modular function** f of weight k (or $2k$) is meromorphic on $\mathfrak{H} \cup \{\infty\}$ and satisfies

$$f \left(\begin{pmatrix} a & b \\ c & d \end{pmatrix} z \right) = (cz + d)^{2k} f(z).$$

That f is meromorphic at ∞ means that the function f^* is meromorphic at 0, where $f^*(e^{2\pi iz}) = f(z)$.

18 A **modular form** is a modular function that is holomorphic on $\mathfrak{H} \cup \{\infty\}$. The modular forms of weight k compose the \mathbf{C} -vector space M_k . The direct sum of these spaces is a graded algebra.

19 Let $G_k(\tau)$ be $G_k(\langle \tau, 1 \rangle)$. Then $G_k \in M_k$. In fact, $G_k(\infty) = 2\zeta(2k)$, where ζ is the Riemann ζ -function.

20 A **cusp form** is a modular form that is zero at ∞ ; those of weight k compose a subspace M_k^0 of M_k .

21 $\Delta \in M_6^0$, since $g_2(\infty) = 2\zeta(4) = 4\pi^4/3$ and $g_3(\infty) = 2\zeta(6) = 8\pi^6/27$.

22 If $f \in M_k$, then

$$\text{ord}_\infty f + \frac{1}{2} \text{ord}_i f + \frac{1}{3} \text{ord}_\rho f + \sum \text{ord}_a f = \frac{k}{6},$$

where the sum is over points of $\Gamma \backslash \mathfrak{H}$ distinct from i and ρ . If there are no other singular points on ∂D , then take $(1/2\pi i) \int df/f$ along ∂D and small arcs around ∞ , ρ , i and $-\bar{\rho}$. This gives the sum of the orders at the other points. It also gives $-(\text{ord}_\infty f + \frac{1}{2} \text{ord}_i f + \frac{1}{3} \text{ord}_\rho f)$, plus $(1/2\pi i)$ times the integral from ρ to $-\bar{\rho}$; for this part, use $f(Sz) = z^{2k} f(z)$.

23 The graded algebra of modular forms is $\mathbf{C}[g_2, g_3]$; and g_2 and g_3 are algebraically independent. In fact,

$$\sum_{k=0}^5 M_k = (1) \oplus (0) \oplus (g_2) \oplus (g_3) \oplus (g_2^2) \oplus (g_2 g_3),$$

while $M_{k+6} = \Delta M_k \oplus (g_2^\alpha g_3^\beta)$ if $2\alpha + 3\beta = k + 6$, since $(f - c g_2^\alpha g_3^\beta)/\Delta \in M_k$ for some c if $f \in M_{k+6}$. If $\{g_2, g_3\}$ were algebraically dependent, then distinct monomials in one of the M_k would be linearly dependent, so g_2^3/g_3^2 would be algebraic, hence constant.

24 The **modular invariant** j is $1728g_2^3/\Delta$, where $1728 = 2^6 3^3$. It is a modular function of weight 0 with a single pole at ∞ .

25 j gives a bijection of $\Gamma \backslash \mathfrak{H}$ onto \mathbf{C} . Indeed, if $\alpha \in \mathbf{C}$, then $1728g_2^3 - \alpha\Delta \in M_6$, so it has a double zero at i , a triple zero at ρ , or a single zero somewhere else, and no other zeros modulo Γ .

26 If $a, b \in \mathbf{C}$ and $a^3 - 27b^2 \neq 0$, then $a = g_2(\Lambda)$ and $b = g_3(\Lambda)$ for some lattice Λ .

References

- [1] Serge Lang, *Elliptic Functions*, Springer, 1987.
- [2] Jean-Pierre Serre, *A Course in Arithmetic*, Springer, 1973.