MODULAR FORMS 2019: ELLIPTIC FUNCTIONS WEEKS OF MARCH 17, 24, 2019

ZEÉV RUDNICK

Contents

1. Elliptic functions

1.1. **The periods of a meromorphic function.** Let $f(z)$ be a meromorphic function, defined in the entire complex plane $\mathbb{C}$. A complex number $\omega \in \mathbb{C}$ is a *period* of f if

$$f(z+\omega) = f(z), \quad \forall z \in \mathbb{C}$$

in particular z is a pole of f iff $z+\omega$ is a pole.

The set of periods is clearly a subgroup of the additive group of $\mathbb{C}$. Denote it by L_f. It usually consists of just $\{0\}$. Hoever, it can be larger, for instance the period of $\sin z$ are $L_{\sin} = 2\pi\mathbb{Z}$.

Lemma 1.1. *The periods L_f of a non-constant meromorphic function are a discrete subgroup of $\mathbb{C}$.*

Date: April 7, 2019.

Proof. We need to recall that if f is a non-constant meromorphic function, and $a \in \mathbb{C} \cup \infty$, then the set $f^{-1}(a)$ is *discrete*. Indeed, if say $f(0) = a$, then near $z = 0$ we can expand $f(z) - a$ in a Taylor series which converges in a neighborhood of 0, with finite order k of vanishing at 0:

$$f(z) - a = c_k z^k + c_{k+1} z^{k+1} + \cdots = z^k \Big(c_k + c_{k+1} z + \dots \Big) = z^k g(z)$$

with $c_k \neq 0$, so that $g(z) \neq 0$ near $z = 0$, and hence $z_0 = 0$ is an isolated zero of $f(z) - a$.

Therefore the set $f^{-1}(f(0)) = \{z : f(z) = f(0)\} \supseteq L_f$ is discrete, and this includes the group of periods. □

From our classification of discrete subgroups of $\mathbb{C} = \mathbb{R}^2$, we see that there are three possibilities for L_f: Either $L_f = \{0\}$, of $L_f = \mathbb{Z}\Omega$ is rank one ($\Omega \neq 0$), for instance for the trigonometric functions sin, cos, tan, or there are two linearly independent (over $\mathbb{R}$) periods ω_1, ω_2 such that $L_f = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2$. In this case we say that f is *doubly periodic*, or is an *elliptic function*. At this point, we have yet to see such a function!

1.2. **Basic properties.** Let $L = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2 \subset \mathbb{C}$ be a lattice, and D a fundamental parallelogram (Figure 1), which we can take as

$$D = \{t_1\omega_1 + t_2\omega_2 : 0 \leq t_1, t_2 < 1\}$$

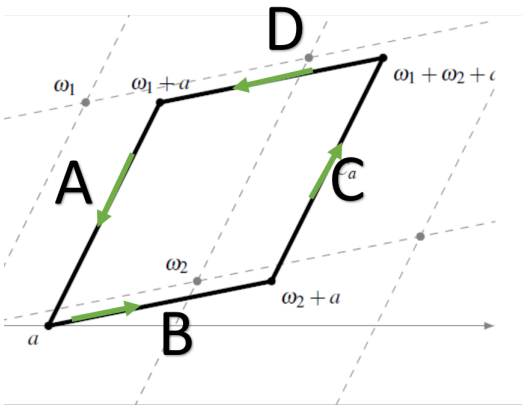

FIGURE 1. A fundamental parallelogram.

Proposition 1.2. *Let f be a non-constant elliptic function*

(1) *f has to have poles.*

(2) *f attains all values in $\mathbb{C} \cup \infty$.*
(3) *Let D be a fundamental parallelogram for L_f so that f has no poles on its boundary ∂D. Then*

$$\oint_{\partial D} f(z)dz = 0$$

(4) *Let $\{p_i\}$ be the set of poles of f in a fundamental parallelogram as above, i.e. a complete set of inequivalent poles (this set is necessarily finite). Then*

$$\sum_{p_j \in D} \mathrm{Res}_{z=p_j} f = 0$$

Proof. (1). Suppose f has no poles, so is entire. Let D be a fundamental parallelogram for the lattice L_f. Then f attains the same values on $\mathbb{C}$ as it does on D. Since D is compact and f continuous, this means that f is bounded on D, hence on $\mathbb{C}$. But by Liouville's theorem, a bounded entire function is constant.

(2). We just saw the case of ∞. Let $a \in \mathbb{C}$, and assume that $f(z) \neq a$. Then the function $1/(f(z) - a)$ is still non-constant and elliptic, but has no poles, contradiction.

(3). Choose a fundamental parallelogram for the lattice so that f has no poles on its boundary, say $D = \{a + t_1\omega_1 + t_2\omega_2 : 0 \leq t_1, t_2 < 1\}$ (Figure 1). Label the edges of the fundamental parallelogram traversed counter-clockwise as A, B, C, D (see Figure 1). Then $C = A + \omega_2$ but traversed in the opposite sense, and likewise $D = B + \omega_1$ and

$$\int_C f(z)dz = \int_{-A+\omega_2} f = \int_{-A} f(z' + \omega_2)dz' = \int_{-A} f(z')dz' = -\int_A f(z)dz$$

and likewise $\int_B f = -\int_D f$. Hence $\int_{\partial D} f(z)dz = 0$.

(4). By Cauchy's residue theorem

$$\sum \mathrm{Res}_{p_j} f = \frac{1}{2\pi i} \oint_{\partial D} f(z)dz$$

which vanishes by the previous claim. □

Corollary 1.3. *Let f be a non-constant elliptic function*

(1) *The number of inequivalent zeros (i.e. lying in a fundamental parallelogram) of f equals the number of inequivalent poles (both counted with multiplicity).*
(2) *f attains any value the same number of times, called the order $\gamma(f)$ of f.*
(3) *The order of f is at least 2: $\gamma(f) \geq 2$.*
(4) *Let $\{z_j\}$ be a full set of inequivalent zeros of f, $\{p_i\}$ of poles, counted with multiplicity. Then*[1]

$$\sum_j z_j - \sum_i p_i \in L_f \tag{1}$$

Proof. (1) For any meromorphic function f, we have

$$\frac{1}{2\pi i}\oint_{\partial D}\frac{f'}{f}(z)dz = \#\{\text{ zeros }\} - \#\{\text{ poles in } D\}$$

Now if f is elliptic and D_f a fundamental parallelogram, then f'/f is still elliptic with period lattice containing L_f, and non-constant, so with fundamental parallelogram tiling D_f, so we still have $\oint_{\partial D} f'/f = 0$ by our previous lemma, hence we are done.

(2) Set $\gamma(f)$ to be the number of poles (with multiplicity) of f in D. Then $\gamma(f-a) = \gamma(f)$ for all $a \in \mathbb{C}$. Let $a \in \mathbb{C}$. Then

$$\begin{aligned}\#\{s \in D : f(z) = a\} &= \#\{\text{ zeros of } f(z) - a \text{ in } D\}\\ &= \#\{\text{ poles of } f(z) - a \text{ in } D\} = \gamma(f)\end{aligned}$$

(3) If $\gamma(f) = 1$, then there would be a single pole of f in D, which would be a simple pole. But we know that the sum of residues of f at the poles in D is zero, while for such a function this cannot be the case. Hence $\gamma(f) \geq 2$.

(4) We have

$$\sum_j z_j - \sum_i p_i = \frac{1}{2\pi i}\oint_{\partial D} z\frac{f'(z)}{f(z)}dz$$

Referring to Figure 1, we have

$$\oint_{\partial D} z\frac{f'(z)}{f(z)}dz = \int_A + \int_B - \int_{\omega_1+A} - \int_{\omega_2+B}$$

Now

$$\int_{\omega_1+A} z\frac{f'(z)}{f(z)}dz = \int_A (z+\omega_1)\frac{f'}{f}(z+\omega_1)dz$$

[1] need this in description of addition law

Now f'/f is elliptic, hence $\frac{f'}{f}(z+\omega_1) = f'/f(z)$ so that

$$\int_A (z+\omega_1)\frac{f'}{f}(z+\omega_1)dz = \int_A z\frac{f'}{f}(z)dz + \omega_1 \int_A \frac{f'}{f}(z)dz$$

and similarly for the integral over $B+\omega_2$. Hence

$$\frac{1}{2\pi i}\oint_{\partial D} z\frac{f'(z)}{f(z)}dz = -\omega_1\frac{1}{2\pi i}\int_A \frac{f'}{f}(z)dz - \omega_2\frac{1}{2\pi i}\int_B \frac{f'}{f}(z)dz$$

It remains to argue that $\frac{1}{2\pi i}\int_A \frac{f'}{f}(z)dz$ is an integer.

Change variable $u = f(z)$, so that

$$\frac{1}{2\pi i}\int_A \frac{f'}{f}(z)dz = \frac{1}{2\pi i}\oint_\Gamma \frac{du}{u}$$

where now the curve Γ is the image of the curve A under $z \mapsto f(z)$. Now A is a straight line between $a+\omega_1$ and a whose endpoints differ by a period of f, and hence under the change of variables $u = f(z)$ is transformed into a *closed* curve Γ. Therefore

$$\frac{1}{2\pi i}\oint_\Gamma \frac{du}{u} = \text{ winding number}$$

is an integer, the winding number of the closed curve Γ. □

1.3. **Construction of elliptic functions.** Until now, we have derived properties of non-constant elliptic functions, with no assurance that they exist. We now construct such functions.

Lemma 1.4. *Let $L \subset \mathbb{C}$ be a lattice. Then the series*

$$\sum_{0\neq\omega\in L} \frac{1}{|\omega|^k}$$

converges for all $k > 2$.

Proof. We need to know that the number of lattice points in a ball of radius R is

$$N_L(R) := \#\{\omega \in L : |\omega| \leq R\} \sim c_L R^2, \quad R \to \infty$$

where $c_L = \frac{\pi}{\text{area}(D)}$ with D a fundamental parallelogram for L (in fact, only need the upper bound). From this, we use a dyadic subdivision

to bound

$$\sum_{0\neq\omega\in L}\frac{1}{|\omega|^k} = O(1) + \sum_{j=1}^{\infty}\sum_{2^{j-1}<|\omega|\leq 2^j}\frac{1}{|\omega|^k}$$
$$\ll 1 + \sum_{j=1}^{\infty}\sum_{2^{j-1}<|\omega|\leq 2^j}\frac{N_L(2^j)}{(2^{j-1})^k}$$
$$\ll 1 + \sum_{j=1}^{\infty}\frac{(2^j)^2}{(2^{j-1})^k} \ll 1 + \sum_{j=1}^{\infty}\frac{1}{(2^{k-2})^j}$$

which converges for $k > 2$. □

For $k > 2$ integer, we now consider the series

$$f_k(z) = \sum_{\omega\in L}\frac{1}{(z-\omega)^k}$$

According to Lemma 1.4 this series is absolutely convergent, uniformly on compact subsets of $\mathbb{C}\backslash L$, and so defines a meromorphic function. Indeed, by the triangle inequality, if $|\omega|/2 \geq |z|$ then

$$|z-\omega| \geq ||\omega| - |z|| \geq \frac{1}{2}|\omega|$$

and so

$$\sum_{\omega\in L}|\frac{1}{(z-\omega)^k}| \leq \sum_{|\omega|\leq 2|z|}|\frac{1}{(z-\omega)^k}| + \sum_{|\omega|>2|z|}(\frac{2}{|\omega|})^k$$

which is convergent.

The function f_k is clearly periodic for L:

$$f_k(z+\omega_0) = \sum_{\omega\in L}\frac{1}{(z+\omega_0-\omega)^k} = \sum_{\omega'\in L}\frac{1}{(z-\omega')^k} = f_k(z)$$

by changing the variable of summation $\omega' = \omega - \omega_0$.

The series f_k has a pole of order k at each point of L, so is in particular non-zero. Thus for each $k \geq 3$ we have constructed an elliptic function of order $\gamma(f_k) = 3$.

1.4. **The Weierstrass $\wp$ function.** We now construct an elliptic function of order 2, in fact with a double pole at the points of L. Set

$$\wp(z;L) = \wp(z) := \frac{1}{z^2} + \sum_{0\neq\omega\in L}\Big(\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2}\Big)$$

We have

$$|\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2}| = |\frac{2z\omega - z^2}{\omega^2(z-\omega)^2}| \ll_z \frac{|\omega|}{|\omega|^2|z-\omega|^2} \ll_z \frac{1}{|\omega|^3}$$

locally uniformly in z, and hence by Lemma 1.4 this series is absolutely convergent, and so defines a meromorphic function with double poles at L.

We note that $\wp$ is *even*:

$$\wp(-z) = \wp(z)$$

Indeed, since the lattice L is invariant under $\omega \mapsto -\omega = \omega'$, we have

$$\begin{aligned}\wp(-z) &= \frac{1}{(-z)^2} + \sum_{0\neq\omega\in L} \Big(\frac{1}{(-z-\omega)^2} - \frac{1}{\omega^2}\Big) \\ &= \frac{1}{z^2} + \sum_{0\neq\omega\in L} \Big(\frac{1}{(z+\omega)^2} - \frac{1}{\omega^2}\Big) \\ &= \frac{1}{z^2} + \sum_{0\neq\omega'\in L} \Big(\frac{1}{(z-\omega')^2} - \frac{1}{\omega'^2}\Big) = \wp(z)\end{aligned}$$

We next claim that $\wp$ has all of L as periods. This is trickier, because while $L + \omega = L$, we cannot simply use that in the sum.

Lemma 1.5. *$\wp(z+\omega) = \wp(z)$ for all $\omega \in L$.*

Proof. The result clearly holds for $z \in L$, so we assume $z \notin L$. We differentiate $\wp$, term-by-term as we may due to uniform convergence on compacta

$$\wp'(z) = -\frac{2}{z^3} - 2\sum_{0\neq\omega\in L} \frac{1}{(z-\omega)^3} = -2f_3(z)$$

which is elliptic, so in particular for all $\omega \in L$,

$$\wp'(z+\omega) = \wp'(z)$$

Integrating we find that there is some constant $c(\omega)$ so that

$$\wp(z+\omega) - \wp(z) = c(\omega)$$

Taking $z = -\omega/2$ we obtain

$$c(\omega) = \wp(-\frac{\omega}{2}) - \wp(\frac{\omega}{2})$$

Now recall that $\wp$ is even, so that $\wp(-\frac{\omega}{2}) = \wp(\frac{\omega}{2})$ and hence $c(\omega) = 0$. Thus we find $\wp(z+\omega) = \wp(z)$. □

One reason that $\wp$ is fundamental is that in a sense it generates all elliptic functions:

Theorem 1.6. *a) Every even elliptic function (for L) is a rational function in $\wp(z;L)$.*

b) Every elliptic function is of the form $A(\wp)+B(\wp)\wp'$ with $A,B\in\mathbb{C}(X)$ rational functions.

We refer to [**?**] for a proof.

Exercise 1. Let $L\subset\mathbb{C}$ be a lattice, and $f(z)$ be an elliptic function for L, that is a meromorphic function so that $f(z+\omega)=f(z)$ for all $\omega\in L$. Assume that f is analytic except for double poles at each point of the lattice L. Show that $f=a\wp+b$ for some constants $a\neq 0$, b.

1.5. **The Taylor expansion of $\wp$.** For $n>2$, let

$$G_n(L)=\sum_{0\neq\omega\in L}\frac{1}{\omega^n}$$

Due to the symmetry $\omega\mapsto-\omega$ of L, we have $G_n(L)=0$ for n odd.

Proposition 1.7. *For $z\notin L$, $|z|\ll 1$,*

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

Proof. For $0\neq\omega\in L$ and $|z|<|\omega|$, we expand

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

on using

$$\frac{1}{(1-x)^2}=\sum_{n\geq 0}(n+1)x^n,\quad |x|<1.$$

Hence for $|z|<\min(|\omega|:0\neq\omega\in L)$

$$\begin{aligned}\wp(z)&=\frac{1}{z^2}+\sum_{0\neq\omega\in L}\frac{1}{\omega^2}\sum_{n=1}^{\infty}(n+1)\left(\frac{z}{\omega}\right)^n\\&=\frac{1}{z^2}+\sum_{n=1}^{\infty}(n+1)\Big(\sum_{0\neq\omega\in L}\frac{1}{\omega^{n+2}}\Big)z^n\\&=\frac{1}{z^2}+\sum_{n=1}^{\infty}(n+1)G_{n+2}(L)z^n\end{aligned}$$

Finally, recall that $G_{2k+1}=0$ to obtain the claim. □

1.6. **The differential equation.** We show that $\wp$ satisfies a nonlinear ODE. We set

$$g_2(L) := 60G_4(L), \qquad g_3(L) := 140G_6(L)$$

Theorem 1.8.

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

Note: $(\wp')^2$ is clearly even, hence by Theorem 1.6 we know apriori that it is a rational function of $\wp$.

Proof. We compute the Taylor expansion of $\wp'$ using that of $\wp$:

$$\wp = \frac{1}{z^2} + 3G_4 z^2 + 5G_6 z^4 + \dots$$

and so

$$\wp' = -\frac{2}{z^3} + 6G_4 z + 20G_6 z^3 + \dots$$

Hence

$$(\wp')^2 = \frac{4}{z^6} - 24G_4\frac{1}{z^2} - 80G_6 + O(z^2)$$

which has a pole of order 6 at the origin. Subtracting $4\wp^3$ gives a function with a pole of order ≤ 4 at $z = 0$:

$$\begin{aligned}(\wp')^2 - 4\wp^3 &= \Big(\frac{4}{z^6} - 24G_4\frac{1}{z^2} - 80G_6 + O(z^2)\Big) - 4\Big(\frac{1}{z^6} + 9G_4\frac{1}{z^2} + 15G_6 + O(z^2)\Big) \\ &= -60G_4\frac{1}{z^2} - 140G_6 + O(z^2) = -\frac{g_2}{z^2} - g_3 + O(z^2)\end{aligned}$$

Hence adding $g_2\wp$ gives an analytic function, moreover

$$(\wp')^2 - 4\wp^3 + g_2\wp = -\frac{g_2}{z^2} - g_3 + O(z^2) + g_2\Big(\frac{1}{z^2} + O(z^2)\Big) = -g_3 + O(z^2)$$

so that

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

is an elliptic function, which is entire (the only poles of $\wp$ and $\wp'$ are at L, and can be checked at the origin), which hence must be a constant, and since it vanishes at the origin it must be identically zero. □

Exercise 2. Show that the Weierstrass $\wp$ function satisfies

$$\wp''(z) = 6\wp(z)^2 - \frac{1}{2}g_2$$

Exercise 3. Show that the the Eisenstein series $G_k(L) = \sum_{0\neq\omega\in L} 1/\omega^k$ satisfy

$$G_8 = \frac{3}{7}G_4^2$$

1.7. **Semi-periods.** Let ω_1, ω_2 be a basis of L, so that $L = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2$ and a fundamental parallelogram is $D = \{t_1\omega_1 + t_2\omega_2 : 0 \leq t_1, t_2 < 1\}$. The points $\omega_1/2, \omega_2/2$ and $\omega_3/2 := (\omega_1 + \omega_2)/2$ (which are the points of $(\frac{1}{2}L/L)\backslash\{0\}$, namely the points of order 2 on $\mathbb{C}/L$) are called the semi-periods.

We note that the derivative $\wp'$ vanishes at the semi-periods:

$$\wp'(\frac{1}{2}\omega_i) = 0$$

because $\wp'$ is an odd function, so that

$$-\wp'(\frac{1}{2}\omega_j) = \wp'(-\frac{1}{2}\omega_j) = \wp'(\frac{1}{2}\omega_j)$$

the last equality because $\omega_j/2 \equiv -\omega_j/2 \bmod L$.

We set

$$e_j := \wp(\frac{1}{2}\omega_j)$$

From the differential equation for $\wp$, we find that e_j are zeros of the polynomial $4x^3 - g_2(L)x - g_3(L)$.

Lemma 1.9. *The $e_j := \wp(\frac{1}{2}\omega_j)$ are distinct*

Proof. Assume that $\wp(z) = e_1 := \wp(\omega_1/2)$ then one solution is $z = \omega_1/2$, and we claim it is the only one, and is a double solution (i.e. a double zero of $\wp(z) - e_1$).

Recall that $\wp$ has order $\gamma(\wp) = 2$, so if $\wp(z) = e_1 := \wp(\omega_1/2)$ then if z is not a double solution there is exactly one other (necessarily simple) solution z_1. Now use the fact that the sum of zeros minus the sum of poles of the elliptic function $f(z) = \wp(z) - e_1$ is 0 mod L:

$$z_1 + \frac{1}{2}\omega_1 - \sum p_j \in L$$

Now $f(z)$ has a double pole at $z = 0$ and no other poles mod L, so that

$$z_1 + \frac{1}{2}\omega_1 - (0 + 0) = 0 \bmod L$$

or

$$z_1 = -\frac{1}{2}\omega_1 \bmod L = \frac{1}{2}\omega_1 \bmod L$$

so that $\omega_1/2$ is the a double zero of f, and there are no other zeros. In particular $\wp(\omega_i/2) \neq \wp(\omega_j/2)$ if $i \neq j$, as claimed. □

1.8. **The modular discriminant Δ.** Due to the differential equation and the vanishing of $\wp'$ at the half periods, we must have that e_j are zeros of the polynomial $4x^3 - g_2x - g_3$, and since by Lemma 1.9 they are distinct, they are the only zeros of this cubic polynomial. Thus we may factor

$$4x^3 - g_2x - g_3 = 4(x - e_1)(x - e_2)(x - e_3)$$

We define the modular discriminant $\Delta(L)$ by

$$\Delta(L) = \frac{1}{16}\operatorname{disc}(4x^3 - g_2(L)x - g_3) = 16\prod_{1\le i<j\le 3}(e_i - e_j)^2$$

It is nonzero because we saw that e_j are *distinct*.

Recall that the discriminant of any polynomial $f(x) = a_dx^d + \cdots + a_1x + a_0 = a_d\prod_{j=1}^d(x - e_j)$, $a_d \neq 0$, is defined as

$$\operatorname{disc} f = a_d^{2(d-1)}\prod_{1\le i<j\le d}(e_i - e_j)^2$$

It is a polynomial in the coefficients, and for a cubic polynomial of the form (WLOG) $x^3 - px - q$ it is given by

$$\operatorname{disc}(x^3 - px - q) = 4p^3 - 27q^2$$

and hence

$$\operatorname{disc}(4x^3 - g_2(L)x - g_3) = 4^{2(3-1)}\operatorname{disc}(x^3 - \frac{1}{4}g_2(L)x - \frac{1}{4}g_3) = 16(g_2^3 - 27g_3^2)$$

Thus we have a formula

$$\boxed{\Delta(L) = g_2(L)^3 - 27g_3(L)^2}$$

1.8.1. *Reminder about discriminants.* Set $s_k = \sum_j e_j^k$ the elementary power sums. Then by the Vandermonde formula

$$\prod_{j>i}(e_j - e_i) = \det V = \det\begin{pmatrix} 1 & 1 & \dots & 1 \\ e_1 & e_2 & \dots & e_d \\ e_1^2 & e_2^2 & \dots & e_d^2 \\ \vdots & & & \\ e_1^{d-1} & e_2^{d-1} & \dots & e_d^{d-1} \end{pmatrix}$$

and hence

$$\prod_{i<j}(e_i - e_j)^2 = \det VV^T = \det\begin{pmatrix} d & s_1 & s_2 & \dots & s_{d-1} \\ s_1 & s_2 & s_3 & \dots & s_d \\ \vdots & & & & \\ s_{d-1} & s_d & s_{d+1} & \dots & s_{2(d-1)} \end{pmatrix}$$

Recall that by Newton's formulas, the elementary power sums s_k may be expressed in terms of the elementary symmetric functions c_k of the roots

$$\prod(x-e_j) = x^d - c_1x^{d-1} + c_2x^{d-2} - \cdots + (-1)^d c_d$$

$$c_k = \sum_{i_1<i_2<\cdots<i_k} e_{i_1}e_{i_2}\dots e_{i_k}$$

and this allows us to express the discriminant in terms of the coefficients of the polynomial.

For instance, for the quadratic monic polynomial $f(x) = x^2+Bx+C$, we have $-B = e_1+e_2 = s_1$, $C = e_1e_2$,

$$s_2 = e_1^2+e_2^2 = (e_1+e_2)^2 - 2e_1e_2 = B^2-2C$$

and

$$\begin{aligned}\operatorname{disc}(x^2+Bx+C) = (e_1-e_2)^2 &= \det\begin{pmatrix} 2 & s_1 \\ s_1 & s_2\end{pmatrix} \\ &= \det\begin{pmatrix} 2 & -B \\ -B & B^2-2C\end{pmatrix} = B^2-4C\end{aligned}$$

For the cubic case, a similar computation gives

$$\operatorname{disc}(x^3-px-q) = 4p^3-27q^2$$

1.9. **Elliptic curves.** Using the differential equation for $\wp$, we obtain a map ϕ from $\mathbb{C}/L\backslash\{0\}$ to the curve

$$E = \{y^2 = 4x^3-g_2x-g_3\}\cup\infty$$

by taking

$$\phi : z\mapsto (x,y) = (\wp(z),\wp'(z)), \quad z\neq 0 \bmod L$$

and extend it to a map $\mathbb{C}/L\to E$ by taking $0\mapsto\infty$. We now have a map of $\mathbb{C}/L$ to the plane projective curve (still denoted by E) (Figure 2)

$$E = \{(X:Y:Z) : ZY^2 = 4X^3-g_2XZ^2-g_3Z^3\}\subset\mathbb{P}^2(\mathbb{C})$$

defined by

$$\phi : 0\neq z\in\mathbb{C}/L\mapsto(\wp(z):\wp'(z):1)$$

and $\phi(0) = (0:1:0)$ which is the point at infinity on E.

Proposition 1.10. *The map $\phi:\mathbb{C}/L\to E$ is a bijection*

Proof. First of all, the point at infinity is the image of 0 and all $z\in\mathbb{C}/L\backslash\{0\}$ are not mapped to infinity. Thus infinity is hit exactly once.

For the finite points of E: Given $x\in\mathbb{C}$, there are exactly two values of z with $\wp'(z) = x$, and then there are two values of y solving $y^2 = 4x^3-g_2x-g_3$ (unless the RHS is zero, in which case take $y=0$),

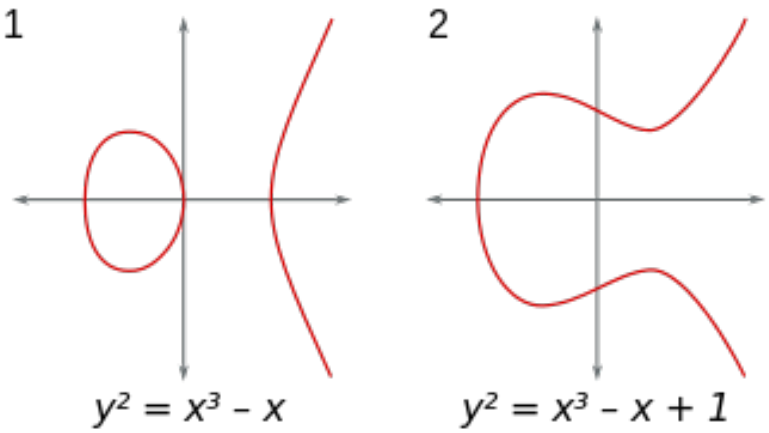

FIGURE 2. Graphs (in the real plane) of the curves $y^2 = x^3 - x$ and $y^2 = x^3 - x + 1$.

and using the ODE, if one of them is $\wp'(z) = y$, then the other is $\wp'(-z) = -\wp'(z) = -y$. Thus the map is surjective.

In fact the analysis shows that it is one-to-one, except possibly when $y = 0$. When $y = 0$, we saw that taking z to be one of the three half periods $\omega_j/2 \in \frac{1}{2}L/L$ gives $\wp'(z) = 0$ and these give exactly the three zeros $e_j = \wp(\omega_j/2)$, that is the three points $(e_j, 0) \in E$ on the intersection of E with the line $y = 0$, and this is the only solution. Hence the map ϕ is one to one. □

Therefore for E of the form $y^2 = 4x^3 - g_2(L)x - g_3(L)$ we have a uniformization map $\phi : \mathbb{C}/L \simeq E$. In fact any E with $g_2^3 - 27g_3^2 \neq 0$ is of this form:

Theorem 1.11. *Suppose we are given $g_2, g_3 \in \mathbb{C}$ such that $g_2^3 - 27g_3^2 \neq 0$. Then there is a lattice $L \subset \mathbb{C}$ so that these are its invariants: $g_2(L) = g_2$ and $g_3(L) = g_3$.*

We refer to the section on the j-invariant **??** for a proof.

1.10. **The addition law.** Consider the elliptic curve in Weierstrass form

$$E : y^2 = 4x^3 - g_2x - g_3$$

and a lattice $L \subset \mathbb{C}$ such that $g_2(L) = g_2$, $g_3(L) = g_3$. We define an addition law on E: We uniformize

$$\mathbb{C}/L \to E, \qquad z \mapsto P(z) := (\wp(z), \wp'(z))$$

and $P(0) = \infty$, which is a bijection, and hence we can use the group structure of $\mathbb{C}/L$ to induce a group structure on E by

$$P(z) \oplus P(w) := P(z + w)$$

As defined above, this addition law is difficult to work with because it requires solving a transcendental inversion problem, namely given two points $P_1, P_2 \in E$, to find $z_1, z_2 \in \mathbb{C}/L$ such that $P(z_i) = P_i$, and only then can we carry out the addition by computing $P(z_1 + z_2)$. However, it turns out that the addition law can be described in geometric and purely algebraic terms as follows:

- The identity element is the point at infinity (corresponding to $z = 0$).
- The negative of a point $P = (x, y) \neq \infty$ is $\ominus P := (x, -y)$ since $P(-z) = (\wp(-z), \wp'(-z)) = (\wp(z), -\wp'(z))$ as $\wp$ is even and $\wp'$ is odd.
- If $P_1 = (x_1, y_1) = P(z_1)$, $P_2 = (x_2, y_2) = P(z_2)$ with both $y_1, y_2 \neq 0$, then the line through P_1 and P_2 will intersect the cubic E in one extra point P_3, which by Proposition 1.12 equals $P_3 = P(-z_1 - z_2) = (x_3, y_3)$, and then set

  $$P_1 \oplus P_2 := \ominus P_3 = (x_3, -y_3) = P(z_2 + z_2)$$

  Now clearly the coordinates of P_3 can be found as algebraic expressions from those of P_1, P_2, e.g. they are the third solution of the equation

  $$\det \begin{pmatrix} x_1 & y_1 & 1 \\ x_2 & y_2 & 1 \\ x & y & 1 \end{pmatrix} = 0$$

- Doubling: A limiting case of the addition formula is to take $P_1 = P_2$, and then $\ominus 2P_1$ is the second intersection of the tangent through P_1 to the curve E with the curve.

Proposition 1.12. *Suppose that $z_1 \neq \pm z_2 \bmod L$, $z_1, z_2 \notin L$. Then the points $P(z_1)$, $P(z_2)$ and $\ominus P(z_1 + z_2) = P(-z_1 - z_2)$ are co-linear.*

Thus we find that the line through the points $P(z_1)$, $P(z_2)$ intersects the elliptic curve E at the point $P(-z_1 - z_2)$.

Proof. Consider the line through the two points $P_1 = P(z_1)$ and $P_2 = P(z_2)$ (since $z_i \notin L$ then both points P_1, P_2 are finite). Since $z_1 \neq \pm z_2 \bmod L$, the points are distinct and $x_2 = \wp(z_2) \neq \wp(\pm z_1) = x_1$ (since $\wp(z_2) = \wp(z_1)$ iff $z_2 = \pm z_1$). Thus the line through them has a unique equation of the form $y = Ax + B$, with $A, B \in \mathbb{C}$.

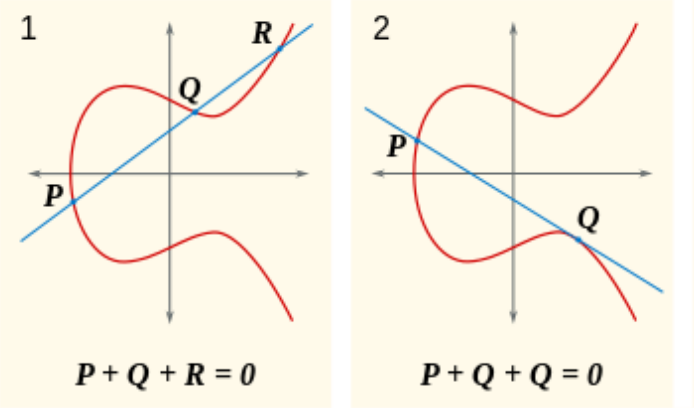

FIGURE 3. The addition law on an elliptic curve $y^2 = 4x^3 - g_2x - g_3$. LHS: for two points P, Q in general position, the third point R on the intersection of the curve E and the line through P, Q satisfies $P \oplus Q \oplus R = 0$. RHS: Doubling a generic point Q. The second point P on the intersection of the curve and the tangent to the curve through Q satisfies $P \oplus 2Q = 0$.

We have found two solutions $z = z_1, z_2$, which are distinct modulo L, of the equation

$$f(z) := \wp'(z) - A\wp(z) - B = 0$$

The function $f(z)$ is a non-constant elliptic function, with a triple pole at $z = 0$, and no other poles mod L, so it has order $\gamma(f) = 3$, and so has three zeros, so in addition to z_1, z_2 it has a third zero z_3. Now we use (1) that for any elliptic function, if z_i are its zeros and p_j its poles mod L, then

$$\sum_i z_i - \sum p_j \in L$$

Hence for f, where the pole is 0 repeated three times, we must have

$$z_1 + z_2 + z_3 - 3 \cdot 0 \in L$$

or

$$z_3 = -z_1 - z_2 \bmod L$$

as claimed. □

Given distinct points $P_i = (x_i, y_i) \in E$, $P_i \neq \infty$, $P_1 \neq \ominus P_2$, the fact that their sum $P_1 \oplus P_2$ is described as the (negative of the) intersection (x_3, y_3) of the line through these point with the curve E allows us to

obtain an algebraic formula for the coordinates of $P_1 \oplus P_2 = (x_3, -y_3)$. The end result is: If $P_1 \neq \pm P_2$

$$\begin{aligned} x_3 &= -x_1 - x_2 + \frac{1}{4}\Big(\frac{y_1 - y_2}{x_1 - x_2}\Big)^2 \\ y_3 &= y_1 + \Big(\frac{y_1 - y_2}{x_1 - x_2}\Big)(x_3 - x_1) \end{aligned} \tag{2}$$

Doubling: When $P_1 = P_2 \neq (0)$, $P_1 = \phi(z_1)$, then we want a formula for the double $P_1 + P_1 = 2P_1 = \phi(2z_1)$. We claim that $2P_1 = \phi(2z_1)$ is the intersection of E with the line tangent to E through the point P_1. This is just the limiting case of the rule for adding two distinct points. Instead of the line through the two distinct points P_1 and P_2, we now take the tangent to the curve at the point P, find the other point R of the intersection (Figure 4), and then $2P = \ominus R$.

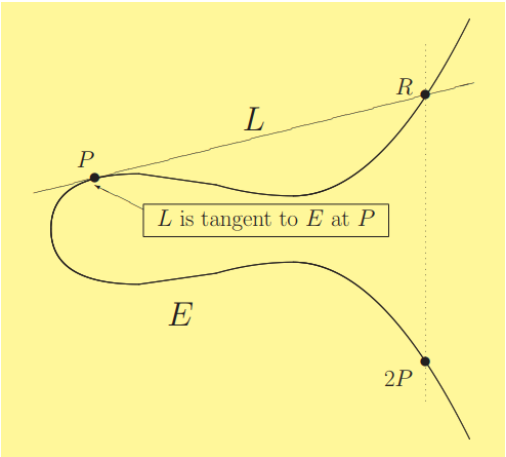

FIGURE 4. Doubling a generic point P. The second point R on the intersection of the curve and the tangent L to the curve through P satisfies $2P \oplus R = 0$.

The algebraic formula is as follows: Write the equation of the curve as $y^2 = f(x)$, $f(x) = 4x^3 - g_2 x - g_3$. If $P_1 = (x_1, y_1)$ with $y_1 \neq 0$, then the slope of tangent to the curve at P_1 is $\frac{f'(x_1)}{2y_1}$, because differentiation gives $2yy' = f'(x)$ hence $y' = f'(x)/2y$ which gives the slope. Then $2P_1 = (x_3, -y_3)$ with

$$\begin{aligned} x_3 &= -2x_1 + \frac{1}{4}(\frac{f'(x_1)}{2y_1})^2 \\ y_3 &= y_1 + \frac{f'(x_1)}{2y_1}(x_3 - x_1) \end{aligned} \tag{3}$$

Formulas (2) and (3) in fact are the same, if one notices that $\frac{y_1-y_2}{x_1-x_2}$ and $\frac{f'(x_1)}{2y_1}$ are just the slopes of the lines involved.

Remark. One can start by defining the addition law either in terms of the geometric construction or the algebraic formulas. The latter have the advantage that they make sense for base fields other than the complex numbers. One then has to check that the formulas define a group law, in particular are associative. This is obvious in the transcendental definition. However, looking at the algebraic definition, it is clear that given a subfield $K \subset \mathbb{C}$, and if $g_2, g_3 \in K$, then if two points $P_1, P_2 \in E(K) = \{(x,y) \in E, x, y \in K\} \cup \infty$ whose x and y coordinates lie in the field K, then also their sum $P_1 \oplus P_2 \in E(K)$ has coordinates in K. In particular this holds for $K = \mathbb{Q}$ the field of rational numbers. Thus if $g_2, g_3 \in \mathbb{Q}$ then $E(\mathbb{Q})$ is a subgroup. Poincaré (1901) suggested that in this case $E(\mathbb{Q})$ is *finitely generated*, which was proved by L.J. Mordell in 1922-23 (A. Weil (1929) handled the case of a general number field).

1.11. **Example: Bachet's problem.** Lets see the doubling law in a classical case, first studied by Bachet in 1621. The problem is: given an integer $c \in \mathbb{Z}$, to express c as a difference of a rational square and a rational cube, that is to solve

$$Y^2 - X^3 = c$$

We rewrite it in Weierstrass form by substituting $(X, Y) = (x, \frac{y}{2})$ (which clearly preserves rationality)

$$y^2 = 4x^3 + 4c$$

and writing it as $y^2 = f(x)$ we may apply the doubling formula (3) to produce, starting with any rational solution $P_1 = (x_1, y_1)$, other rational solutions $P_2 = 2P_1 = (x_2, y_2)$, $P_4 = 2P_2 = 4P_1 = (x_4, y_4)$, etc.

For instance, taking $c = -2$, we want to find rational solutions of $Y^2 - X^3 = -2$. We guess the (integer) solution $P_1 = (X_1, Y_1) = (3, 5)$, which gives the point $(x_1, y_1) = (X_1, 2Y_1) = (3, 10)$ on the curve $y^2 = 4x^3 - 8$, and then using (3) we obtain other solutions

$$P_2 = 2P_1 = (x_2, y_2) = (\frac{129}{10^2}, -\frac{383}{500})$$
$$P_4 = 2P_2 = (x_4, y_4) = (\frac{2340922881}{7660^2}, \frac{113259286337279}{22472754800})$$

giving the following solutions of the original equation $Y^2 - X^3 = -2$:

$$(X_2, Y_2) = (\frac{129}{10^2}, -\frac{383}{10^3}), \quad (X_4, Y_4) = (\frac{2340922881}{7660^2}, \frac{113259286337279}{7660^3})$$

(this example is taken from [1, page 2], which contains a misprint for the value of Y_4, corrected in the second edition).

We can also add $P_1 \oplus P_2$ to get the following solution of $Y^2 - X^3 = -2$

$$(X_3, Y_3) = (\frac{164323}{29241}, \frac{66234835}{5000211})$$

The general formula for the double of a point $P = (X, Y)$ on the curve $Y^2 - X^3 = c$ with $Y \neq 0$ is [1]

$$2P = (\frac{X^4 - 8cX}{4Y^2}, \frac{-X^6 - 20cX^3 + 8c^2}{8Y^3})$$

Exercise 4. Find three rational solutions of $Y^2 - X^3 = -1$ with $Y \geq 0$.

References

[1] J. H. Silverman and J. Tate. Rational points on elliptic curves. Undergraduate Texts in Mathematics. Springer-Verlag, New York, 1992.