(*November 6, 2015*)

Trigonometric functions, elliptic functions, elliptic modular forms

Paul Garrett garrett@math.umn.edu http://www.math.umn.edu/~garrett/

[This document is http://www.math.umn.edu/~garrett/m/mfms/notes_2015-16/09_elliptic.pdf]

---

1. *Reconsideration of* $\sin x$

Although we already know quite a bit about trigonometric functions and their role in calculus, their treatment can be redone to emphasize parallels for *elliptic integrals* and *elliptic functions*.

[1.1] Integral defining $\arcsin x$ The length of arc of a piece of a circle is $x^2 + y^2 = 1$ is

$$\text{arc length of circle fragment from 0 to } x \;=\; \int_0^x \sqrt{1+y'^2}\,dt \;=\; \int_0^x \sqrt{1+\big(\frac{d}{dt}\sqrt{1-t^2}\big)^2}\,dt$$

$$=\; \int_0^x \sqrt{1+\Big(\frac{\frac{1}{2}\cdot(-2t)}{\sqrt{1-t^2}}\Big)^2}\,dt \;=\; \int_0^x \sqrt{1+\frac{t^2}{1-t^2}}\,dt \;=\; \int_0^x \frac{dt}{\sqrt{1-t^2}} \;=\; \arcsin x$$

[1.2] Periodicity The *periodicity* of $\sin x$ comes from the *multi-valuedness* of $\arcsin x$. The multi-valuedness is ascertainable from this integral, since the path from 0 to x can meander through the *complex plane*, going around the two points ± 1 special for the integral. The basic unit of this multi-valuedness is

$$\int_\gamma \frac{d\zeta}{\sqrt{1-\zeta^2}} \;=\; \pm 2\pi \qquad \text{(counter-clockwise circular path } \gamma \text{ enclosing both } \pm 1)$$

That is, a path integral from 0 to x could go from 0 to x along the real axis, but then add to the path a vertical line segment from x out to a circle of radius 2, traverse the circle an arbitrary number of times, come back along the same segment (thus cancelling the contribution from this segment).

There are two single-valued choices for $(1-z^2)^{-\frac{1}{2}}$ on any region complementary to an arc connecting ± 1. For example, it is easy to see a *Laurent expansion* in $|z| > 1$:

$$(1-z^2)^{-\frac{1}{2}} \;=\; \frac{\pm i}{z}\cdot\Big(1-\frac{1}{z^2}\Big)^{-\frac{1}{2}} \;=\; \frac{\pm i}{z}\cdot\Big(1-(-\tfrac{1}{2})\frac{1}{z^2}+\frac{(-\frac{1}{2})(-\frac{3}{2})}{2!}\big(\frac{1}{z^2}\big)^2+\dots\Big) \;=\; \pm\Big(\frac{i}{z}+\frac{1/2}{z^3}+\frac{3/8}{z^5}+\dots\Big)$$

Let γ be a path traversing counterclockwise a circle of radius more than 1 centered at 0. Integrals $\int_\gamma \frac{dz}{z^N}$ are 0 except for $N = 1$, in which case the integral is $2\pi i$. Thus,

$$\int_\gamma \frac{dz}{\sqrt{1-z^2}} \;=\; \pm 2\pi$$

[1.3] Polynomial relation between $\sin x$ and $\sin' x$ Rewriting the integral as

$$\int_0^{\sin x} \frac{dt}{\sqrt{1-t^2}} \;=\; x$$

and taking a derivative, by the fundamental theorem of calculus,

$$\sin' x \cdot \frac{1}{\sqrt{1-\sin^2}} \;=\; 1$$

Thus, $(\sin' x)^2 = 1 - (\sin x)^2$ and the algebraic relation between $\sin x$ and its derivative (we know it is $\cos x$) arises:

$$(\sin x)^2 + (\sin' x)^2 = 1$$

---

2. *Construction of singly-periodic functions*

A *singly-periodic* function f on $\mathbb{C}$ is a (probably holomorphic or meromorphic) function such that for some $\omega \neq 0$

$$f(z+\omega) \;=\; f(z) \qquad\qquad (\text{for all } z \in \mathbb{C})$$

or at least for z away from poles of f. Iterating the condition, for any integer n

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

In other words, f is *invariant* under translation by the group $\mathbb{Z} \cdot \omega$ inside $\mathbb{C}$.

Feigning ignorance of the trigonometric (and exponential) function, whether as inverse functions to integrals or not, as a warm-up to the construction of *doubly*-periodic functions we should try to *construct* some singly-periodic functions.

[2.1] Construction and comparison to $\sin z$ For simplicity, take $\omega = 1$, and make holomorphic or meromorphic functions f such that

$$f(z+1) \;=\; f(z) \qquad\qquad (\text{for all } z \in \mathbb{C})$$

That is, we want $\mathbb{Z}$-periodic functions on $\mathbb{C}$, hypothetically closely related to $\sin 2\pi z$. A fundamental approach to manufacturing such things is *averaging*, also called *periodicization* or *automorphizing*, as follows. For given function φ, consider

$$f(z) \;=\; \sum_{n\in\mathbb{Z}} \varphi(z+n)$$

If this converges nicely it is certainly periodic with period 1, since

$$f(z+1) \;=\; \sum_{n\in\mathbb{Z}} \varphi(z+1+n) \;=\; \sum_{n\in\mathbb{Z}} \varphi(z+n)$$

by replacing n by $n-1$, using the fact that we have summed over the *group* $\mathbb{Z}$, justifying rearrangement by absolute convergence.

An elementary function making the sum converge, apart from poles, is $\varphi(z) = 1/z^2$, so put

$$f(z) \;=\; \sum_{n\in\mathbb{Z}} \frac{1}{(z+n)^2}$$

If we are lucky, this manufactures a function related to the *sine* function. Indeed, $f(z)$ has double poles at the zeros of $\sin \pi z$, so a plausible preliminary guess is that $f(z)$ is $1/(\sin \pi z)^2$.

To prove equality, perhaps after adjusting details, match poles, subtract, check that the difference goes to 0 as the imaginary part of z at infinity goes to ∞, and invoke Liouville. [1]

To do this, first determine the Laurent expansion of $f(z)$ near its poles. By periodicity, we'll understand all the poles if we understand the pole at $z = 0$. This is

$$f(z) \;=\; \frac{1}{z^2} + \sum_{n\neq 0} \frac{1}{(z+n)^2} \;=\; \frac{1}{z^2} + (\text{holomorphic near } z = 0)$$

To understand the nature of each pole of $1/\sin^2 \pi z$, by periodicity it suffices to look near $z = 0$. Since

$$\sin \pi z \;=\; \pi z + (\pi z)^3/3! + \ldots \;=\; \pi z \cdot \big(1 + (\pi z)^2/3! + \ldots\big)$$

the inverse square is [2]

$$\frac{1}{\sin^2 \pi z} \;=\; \frac{1}{\pi z \cdot \big(1 + (\pi z)^2/3! + \ldots\big)} \;=\; \frac{1}{(\pi z)^2} \cdot \big(1 - (\pi z)^2/3! + \ldots\big) \;=\; \frac{1/\pi^2}{z^2} + \text{holomorphic at } 0$$

Correcting by π^2, the poles of $f(z)$ and $\pi^2/\sin^2 \pi z$ cancel:

$$f(z) - \frac{\pi^2}{\sin^2 \pi z} \;=\; \sum_n \frac{1}{(z+n)^2} - \frac{\pi^2}{\sin^2 \pi z} \;=\; \text{entire}$$

As $\text{Im}(z)$ becomes large, $f(z)$ goes to zero. For apparently different reasons, also

$$\frac{\pi^2}{\sin^2 \pi z} \;=\; \Big(\frac{2\pi i}{e^{\pi i z} - e^{-2\pi i z}}\Big)^2 \;\longrightarrow\; 0 \qquad\qquad (\text{as } |\text{Im}(z)| \to \infty)$$

Thus, by Liouville,

$$\sum_{n\in\mathbb{Z}} \frac{1}{(z+n)^2} \;=\; \frac{\pi^2}{\sin^2 \pi z}$$

[2.2] Differential equations for singly-periodic functions

The construction produced a *singly*-periodic function $\sum 1/(z+n)^2$ identifiable in terms of already-familiar items. The analogous discussion for *doubly*-periodic functions does *not* produce familiar objects. For practice, we now take another viewpoint that will also succeed with constructed *doubly*-periodic functions.

---

[1] Liouville's theorem asserts that a *bounded entire function* is *constant*. As an immediate corollary, an entire function which is bounded *and* goes to 0 as the imaginary part of z goes to infinity is 0. Liouville's theorem is a striking instance of *rigidity*, where to prove two things equal, we need not prove something with infinite precision, but only demonstrate *sufficient* closeness to be able to infer equality. A trivial case of *rigidity* is that two integers are equal if they are within distance 1.

[2] The first two terms of the multiplicative inverse of a convergent power series $1 + c_1 z + c_2 z^2 + \ldots$ are easily determined, using $\frac{1}{1-r} = 1 + r + r^2 + \ldots$:

$$\frac{1}{1 + c_1 z + c_2 z^2 + \ldots} \;=\; \frac{1}{1 - (-c_1 z - c_2 z^2 - \ldots)}$$

$$=\; 1 + (-c_1 z - c_2 z^2 - \ldots) + (-c_1 z - c_2 z^2 - \ldots)^2 + \ldots \;=\; 1 - c_1 z + (\text{higher-order})$$

That is, with leading term 1, the coefficient of z changes simply by flipping sign.

The aim is to determine a differential equation satisfied by $f(z) = \sum 1/(z+n)^2$. In terms of Liouville, both f and its derivative

$$f'(z) \;=\; -2\sum \frac{1}{(z+n)^3}$$

go to 0 as $\mathrm{Im}(z) \to \pm\infty$, so if a polynomial $P(f, f')$ in f and f' cancels the poles, then $P(f, f')$ is necessarily *constant*, giving a polynomial relation [3] between f' and f. By periodicity, it suffices to consider the poles at $z = 0$, as before.

Noting that $f(-z) = f(z)$ assures vanishing of odd-order terms, let

$$f(z) \;=\; \frac{1}{z^2} + a + bz^2 + O(z^4) \qquad \text{so} \qquad f'(z) \;=\; \frac{-2}{z^3} + 2bz + O(z^3)$$

To cancel poles by a polynomial $P(f, f')$, the first step is to cancel the worst pole by $f^3 - (f'/-2)^2$: compute (carefully!?) that

$$f(z)^2 \;=\; \frac{1}{z^4} + \frac{2a}{z^2} + O(1) \qquad \text{and} \qquad f(z)^3 \;=\; \frac{1}{z^6} + \frac{3a}{z^4} + \frac{3a^2+3b}{z^2} + O(1)$$

and

$$\left(\frac{f'(z)}{-2}\right)^2 \;=\; \left(\frac{1}{z^3} - bz + O(z^3)\right)^2 \;=\; \frac{1}{z^6} - \frac{2b}{z^2} + O(1)$$

Thus,

$$\left(\frac{f'(z)}{-2}\right)^2 - f(z)^3 \;=\; -\frac{3a}{z^4} - \frac{3a^2+5b}{z^2} + O(1)$$

The $1/z^4$ term can be eliminated by adjusting by a multiple of $f(z)^2$:

$$\left(\frac{f'(z)}{-2}\right)^2 - f(z)^3 + 3a\cdot f(z)^2 \;=\; \frac{-3a^2-5b+6a^2}{z^2} + O(1) \;=\; \frac{3a^2-5b}{z^2} + O(1)$$

Finally, subtract a multiple of $f(z)$ to eliminate the $1/z^2$ term:

$$\left(\frac{f'(z)}{-2}\right)^2 - f(z)^3 + 3a\cdot f(z)^2 - (3a^2-5b)\cdot f(z) \;=\; O(1)$$

In fact, since both f and f' go to zero as $\mathrm{Im}(z) \to \pm\infty$, the $O(1)$ term must be 0. Rearrangement produces a relation anticipating Weierstraß' analogous relation for constructed *doubly*-periodic functions:

$$\boxed{f'^2 \;=\; 4f^3 - 12af^2 + (12a^2 - 20b)f} \qquad (\text{with } f(z) = \sum \frac{1}{(z+n)^2} = \frac{1}{z^2} + a + bz^2 + \ldots)$$

Again, for other reasons, we know $f(z) = \pi^2/\sin^2 \pi z$.

[2.2.1] Remark: The existence of the relation made no use of higher Laurent coefficients, and at the same time explicitly demonstrates the dependence of the algebraic relation on the coefficients a, b in $f(z) = \frac{1}{z^2} + a + bz^2 + \ldots$. As discussed just below, in fact $a = 2\zeta(2) = \pi^2/3$ and $b = 6\zeta(4) = \pi^4/15$. Thus, miraculously, $12a^2 - 20b = 0$, and the relation is simply

$$\boxed{f'^2 \;=\; 4f^3 - 4\pi^2 f^2} \qquad (\text{with } f(z) = \sum \frac{1}{(z+n)^2})$$

[3] A non-linear polynomial relation between f and f' is a *non-linear*, probably hard-to-solve, differential equation. The difficulty of solving non-linear differential equations in general is not the point, however.

3. *Arc length of ellipses: elliptic integrals and elliptic functions*

One might naturally be interested in the integral for the length of a piece of arc of an ellipse. For example, the arc length of the piece the ellipse

$$x^2 + k^2 y^2 \;=\; 1 \qquad\qquad (\text{with real } k \neq 0)$$

up to x, in the first quadrant, is

$$\int_0^x \sqrt{1+y'^2}\,dt \;=\; \int_0^x \sqrt{1+\frac{1}{k^2}\left(\frac{\frac{-1}{2}\cdot 2t}{\sqrt{1-t^2}}\right)^2}\,dt \;=\; \int_0^x \sqrt{1+\frac{1}{k^2}\frac{t^2}{1-t^2}}\,dt \;=\; \frac{1}{\sqrt{k}}\int_0^x \sqrt{\frac{k^2-(k^2-1)t^2}{1-t^2}}\,dt$$

For the *circle*, $k = 1$, simplifying the numerator, and the value is as above:

$$\int_0^x \frac{1}{\sqrt{1-t^2}}\,dt \;=\; \arcsin x$$

Otherwise, there is no obvious reduction to elementary integrals. This leads to calling this integral an *elliptic integral*. [4] Many people studied the effect of changes of variables to transmute one form into another. [5] The immediate problems of computing arc length or evaluating integrals were eclipsed by the higher-level discovery by Abel and Jacobi (independently) in 1827 of the *double periodicity* [6] of functions $f(z)$ defined implicitly by

$$z \;=\; \int_0^{f(z)} \frac{d\zeta}{\sqrt{\text{quartic in } \zeta \text{ with distinct factors}}}$$

That is, there are *periods* ω_1 and ω_2 in $\mathbb{C}$ such that

$$f(z+\omega_1) \;=\; f(z+\omega_2) \;=\; f(z) \qquad\qquad (\text{for all } z \in \mathbb{C})$$

with ω_1 and ω_2 linearly independent over $\mathbb{R}$. These ω_1 and ω_2 will arise as *integrals* of $1/\sqrt{\text{quartic}}$ over closed paths, which is why these integrals themselves have come to be called *period integrals*, or simply *periods*.

For example, consider

$$z = \int_0^{f(z)} \frac{d\zeta}{\sqrt{1+\zeta^4}}$$

[4] More generally, an *elliptic integral* is of the form

$$\int_a^b \frac{(\text{rational expression in } z)}{\sqrt{\text{cubic or quartic in } z}}\,dz$$

When the expression inside the radical has more than 4 zeros, or if the square root is replaced by a higher-order root, the integral's behavior is yet more complicated. The case of square root of cubic or quartic is the simplest beyond more elementary integrals. Abel and Jacobi and others *did* subsequently consider the more complicated cases, a popular pastime throughout the 19^{th} century.

[5] By 1757 Euler had studied relationships $dx/\sqrt{x^4+1} + dy/\sqrt{y^4+1} = 0$, leading to algebraic relations between x and y. Legendre (about 1811) studied transformations of such integrals, giving special reduced forms.

[6] Gauss later claimed he had found the double periodicity earlier, but had not published it. Abel and Jacobi published in 1827, and Legendre very civilly acknowledged their work in a new edition of his *Exercices de Calcul Intégral*. Later archival work did verify that Gauss had *privately* found the double periodicity in 1809.

The uniform *ambiguities* in the value of this integral viewed as a *path integral* from 0 to w are the values of the integrals along closed paths which circle an *even* number of the bad points $e^{2\pi ik/8}$ with $k = 1, 3, 5, 7$ (primitive 8^{th} roots of 1).

With a denominator decaying like $1/|\zeta|^2$ for large $|\zeta|$, the integral over large circles goes to 0 as the radius goes to $+\infty$. The integral around two points added to the integral around the other two points is equal to that outer circle integral, which is 0, so any two such integrals are merely negatives of each other.

Because of the decay for $|\zeta|$ large, the integral of $1/\sqrt{1+\zeta^4}$ along a path encircling $e^{2\pi i/8}$ and $e^{2\pi i\, 3/8}$ is equal (via a deformation of the path) to the integral along the real axis, namely

$$\lambda \;=\; \int_{-\infty}^{+\infty} \frac{dt}{\sqrt{1+t^4}}$$

Whatever else this may be, it is a positive real number. Similarly, the integral along a path encircling $e^{2\pi i/8}$ and $e^{2\pi i\, 7/8}$ is equal (via a deformation of path) to the path integral along the imaginary axis, namely

$$\int_{-\infty}^{+\infty} \frac{d(it)}{\sqrt{1+(it)^4}} \;=\; i\cdot \int_{-\infty}^{+\infty} \frac{dt}{\sqrt{1+t^4}} \;=\; i\lambda$$

since $i^4 = 1$. Thus, the double periodicity

$$f(z+\lambda) \;=\; f(z+i\lambda) \;=\; f(z)$$

The corresponding *period lattice* is

$$\Lambda \;=\; \mathbb{Z}\cdot\lambda + \mathbb{Z}\cdot i\lambda \subset \mathbb{C}$$

[3.0.1] Remark: In our example, the function $f(z)$ has *poles*. Notice that the integral along the positive real axis

$$\int_0^{+\infty} \frac{dt}{\sqrt{1+t^4}}$$

is absolutely convergent, with value $\lambda/2$, where λ is the *whole* integral on the real line, as just above. That is, $f(\lambda/2) = \infty$, which is to say that f has a pole at $\lambda/2$. Likewise, the integral along the upper imaginary axis is absolutely convergent, to $i\lambda/2$, so another pole is at $i\lambda/2$. And then the periodicity implies that there are poles (at least) at all points

$$\frac{\lambda}{2} + (m+ni)\lambda \qquad \frac{i\lambda}{2} + (m+ni)\lambda \qquad\qquad (\text{for } m,n \in \mathbb{Z})$$

---

4. *Construction of doubly-periodic functions*

Once the existence of doubly-periodic functions is established via inverting elliptic integrals, the possibility of other constructions arises, just as we have alternative expressions for $\sin x$ in addition to $x = \int_0^{\sin x} dt/\sqrt{1-t^2}$.

A *lattice* in $\mathbb{C}$ is a subgroup of $\mathbb{C}$ of the form

$$\Lambda \;=\; \mathbb{Z}\cdot\omega_1 + \mathbb{Z}\cdot\omega_2 \qquad\qquad (\text{with } \omega_1,\omega_2 \text{ linearly independent over } \mathbb{R})$$

We want Λ-*periodic* functions, meaning meromorphic functions f on $\mathbb{C}$ such that

$$f(z+\lambda) \;=\; f(z) \qquad\qquad (\text{for all } z \in \mathbb{C} \text{ and } \lambda \in \Lambda)$$

These are *elliptic functions* with *period lattice* Λ. For a construction by *averaging*, just as we constructed $\pi^2/\sin^2 \pi z$, consider sums

$$\sum_{\lambda\in\Lambda} \frac{1}{(z+\lambda)^k}$$

For $k > 2$, these are absolutely convergent and uniformly on compacta, and visibly invariant under $z \to z+\lambda$ for $\lambda \in \Lambda$. The smallest exponent for which this sum converges (for z not in Λ) is $k = 3$, but Weierstraß discovered [7] that it is best, to try to repair the convergence in the $k = 2$ case. The *Weierstraß $\wp$-function* is

$$\wp(z) \;=\; \wp_\Lambda(z) \;=\; \frac{1}{z^2} + \sum_{0\neq\lambda\in\Lambda} \left(\frac{1}{(z+\lambda)^2} - \frac{1}{\lambda^2} \right)$$

This *does* converge absolutely, but the argument for double periodicity is more complicated. Still, its derivative

$$\wp'(z) \;=\; \wp'_\Lambda(z) \;=\; -2 \sum_{\lambda\in\Lambda} \frac{1}{(z+\lambda)^3}$$

is nicely convergent *and* admits the easy change-of-variables argument for its periodicity.

[4.0.1] Claim: The function $\wp_\Lambda(z)$ is doubly-periodic, with period lattice Λ.

Proof: For $0 \neq \mu \in \Lambda$ the difference $\wp(z+\mu) - \wp(z)$ has derivative $\wp'(z+\mu) - \wp'(z) = 0$, by periodicity of $\wp'(z)$, so there is a constant C_μ such that $\wp(z+\mu) = \wp(z) + C_\mu$ for all z. Note that $\wp$ is an *even* function, because the term $1/z^2$ is invariant under $z \to -z$, and the other summands occur in pairs $(z \pm \lambda)^2 - \lambda^2$, interchanged by $z \to -z$. Take $z = -\mu/2$ to see that

$$C_\mu \;=\; \wp(-\mu/2 + \mu) - \wp(\mu/2) \;=\; 0$$

proving the periodicity of $\wp$. ///

[4.0.2] Claim: An *entire* doubly-periodic function is *constant*.

Proof: Let ω_1, ω_2 be $\mathbb{Z}$-generators for Λ. Since the ω_i are linearly independent over $\mathbb{R}$, every $z \in \mathbb{C}$ is an $\mathbb{R}$-linear combination of them. Given $z = a\omega_1 + b\omega_2$ with $a, b \in \mathbb{R}$, let m, n be integers such that $0 \leq a - m < 1$ and $0 \leq b - n < 1$. Then

$$z \;=\; a\omega_1 + b\omega_2 \;=\; (a-m)\omega_1 + (b-n)\omega_2 + (m\omega_1 + n\omega_2)$$

Since $m\omega_1 + n\omega_2$ is in the lattice Λ, this shows that every Λ-orbit on $\mathbb{C}$ has a unique representative inside the so-called *fundamental domain*

$$F \;=\; \{r\omega_1 + s\omega_2 : 0 \leq r < 1,\ 0 \leq s < 1\}$$

for Λ. A Λ-periodic function's values on the whole plane are determined completely by its values on F. The set F has *compact* closure

$$\overline{F} \;=\; \{r\omega_1 + s\omega_2 : 0 \leq r \leq 1,\ 0 \leq s \leq 1\}$$

Thus, a continuous Λ-periodic function is *bounded* on $\overline{F}$, so bounded on $\mathbb{C}$. Thus, an entire Λ-periodic function is bounded. By Liouville's theorem, it is constant. ///

*[... iou ...]*pictures

[7] We follow Weierstraß's work on elliptic functions that came somewhat after Abel's and Jacobi's.

[4.0.3] Claim: Fix a lattice Λ. The Weierstraß P-function $\wp(z)$ and its derivative $\wp'(z)$ (attached to lattice Λ) satisfy the algebraic relation

$$\boxed{\wp'^2 \;=\; 4\wp^3 - 60g_2\wp - 140g_3}$$

where

$$g_2 \;=\; g_2(\Lambda) = 60 \sum_{0\neq\lambda\in\Lambda} \frac{1}{\lambda^4} \qquad g_3 \;=\; g_3(\Lambda) = 140 \sum_{0\neq\lambda\in\Lambda} \frac{1}{\lambda^6}$$

[4.0.4] Remark: We will *find* the relation satisfied by $\wp$ and $\wp'$, not merely *verify* Weierstraß' relation, much as we did for singly-periodic functions.

Proof: The poles of both $\wp$ and $\wp'$ are just on the lattice Λ, so if we can make a linear combination of powers of $\wp$ and $\wp'$ whose Laurent expansion at 0 has no negative terms or constant term, then that linear combination of powers is identically 0.

Since $\wp(z)$ is *even*, the Laurent expansion of $\wp$ at 0 has no odd-degree terms. Because of the convergence trick, the constant Laurent coefficient of $\wp(z)$ at 0 is 0, so the expansion is of the form

$$\wp(z) \;=\; \frac{1}{z^2} + az^2 + bz^4 + O(z^6) \qquad \text{and} \qquad \wp'(z) \;=\; \frac{-2}{z^3} + 2az + 4bz^3 + O(z^5)$$

Then

$$\left(\frac{\wp'(z)}{-2}\right)^2 \;=\; \frac{1}{z^6} - \frac{2a}{z^2} - 4b + O(z) \qquad \text{and} \qquad \wp(z)^3 = \frac{1}{z^6} + \frac{3a}{z^2} + 3b + O(z)$$

so

$$\left(\frac{\wp'}{-2}\right)^2 - \wp^3 \;=\; \frac{-5a}{z^2} - 7b + O(z)$$

Then

$$\left(\frac{\wp'}{-2}\right)^2 - \wp^3 + 5a\,\wp + 7b = O(z)$$

As remarked at the beginning, this linear combination of powers is a doubly-periodic function without poles, so by Liouville is constant, yet vanishes at $z = 0$, so is 0. That is,

$$\wp'(z)^2 \;=\; 4\wp(z)^3 - 20a\,\wp(z) - 28b$$

With $\wp_o(z) = \wp(z) - \frac{1}{z^2}$,

$$a \;=\; \frac{\wp_o''(0)}{2!} \;=\; \frac{1}{2!}\cdot \sum_{0\neq\lambda\in\Lambda} \frac{(-2)(-3)}{\lambda^4} \;=\; 3\sum_{0\neq\lambda\in\Lambda} \frac{1}{\lambda^4}$$

and

$$b \;=\; \frac{\wp_o''''(0)}{2!} \;=\; \frac{1}{4!}\cdot \sum_{0\neq\lambda\in\Lambda} \frac{(-2)(-3)(-4)(-5)}{\lambda^6} \;=\; 5\sum_{0\neq\lambda\in\Lambda} \frac{1}{\lambda^6}$$

we have the Weierstraß equation

$$\wp'^2 \;=\; 4\wp^3 - 60g_2\wp - 140g_3$$

as anticipated. ///

[4.0.5] Remark: There is at least one other way to construct doubly-periodic functions directions, due to Jacobi, who expressed doubly-periodic functions as ratios of *entire* functions (*theta functions*) which are genuinely singly-periodic with periods (for example) $\mathbb{Z}$, and nearly (but not quite) periodic in another direction. (Indeed, we saw just above that entire functions that are genuinely doubly-periodic are constant!)

5. *Complex tori, elliptic curves, the modular curve*

Just as *sine* and its derivative *cosine* map $\mathbb{R}$ to a circle [8]

$$z \longrightarrow (\sin z, \sin' z) \in \{(x,y) \in \mathbb{R}^2 : x^2 + y^2 = 1\}$$

the Weierstraß $\wp$ and $\wp'$ attached to a lattice Λ map $\mathbb{C}$ to a cubic algebraic curve

$$z \longrightarrow (\wp(z), \wp'(z)) \in \{(x,y) \in \mathbb{C}^2 : y^2 = 4x^3 - 60g_2x - 140g_3\}$$

Just as the map $z \to (\sin z, \cos z)$ *factors through* the quotient $\mathbb{R}/2\pi\mathbb{Z}$

$$\begin{array}{ccc} \mathbb{R} & \longrightarrow & \{x^2+y^2=1\} \\ & \searrow \quad \nearrow & \\ & \mathbb{R}/2\pi\mathbb{Z} & \end{array} \qquad \text{by} \qquad \begin{array}{ccc} z & \longrightarrow & (\sin z, \cos z) \\ & \searrow \quad \nearrow & \\ & z + 2\pi\mathbb{Z} & \end{array}$$

the map given by $\wp$ and its derivative factor through the quotient $\mathbb{C}/\Lambda$:

$$\begin{array}{ccc} \mathbb{C} & \longrightarrow & \{y^2 = 4x^3 - 60g_2x - 140g_3\} \\ & \searrow \quad \nearrow & \\ & \mathbb{C}/\Lambda & \end{array} \qquad \text{by} \qquad \begin{array}{ccc} z & \longrightarrow & (\wp(z), \wp'(z)) \\ & \searrow \quad \nearrow & \\ & z + \Lambda & \end{array}$$

The quotient $\mathbb{C}/\Lambda$ is a *complex torus*, and the cubic curve $\{(x,y) \in \mathbb{C}^2 : y^2 = 4x^3 - 60g_2x - 140g_3\}$ is an *elliptic curve*. Thus, the algebraic relation between $\wp = \wp_\Lambda$ and $\wp' = \wp'_\Lambda$ implies that $\wp, \wp'$ map the complex torus $\mathbb{C}/\Lambda$ to the corresponding elliptic curve.

Any subgroup $\mathbb{Z} \cdot \omega$ can be converted to $\mathbb{Z} \cdot 1$ by the holomorphic map $z \to \omega^{-1}z$, so all the quotients $\mathbb{C}/\mathbb{Z}\omega$ are *isomorphic*.

In contrast, we will see now that there are many non-isomorphic complex tori $\mathbb{C}/\Lambda$, even though *topologically* these are all cartesian products of two circles. We can only prove a limited form of this in the present context. First, a given lattice $\Lambda = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2$ can be adjusted by multiplying the ambient $\mathbb{C}$ by any complex scalar. It is traditional to consider two cases: if ω_1/ω_2 lies in the *upper* half-plane $\mathfrak{H}$, then let $z = \omega_1/\omega_2$, and multiplication by ω_2^{-1} changes the lattice to $\mathbb{Z} \cdot z + \mathbb{Z} \cdot 1$. If ω_1/ω_2 is in the *lower* half-plane, reverse the roles of ω_1, ω_2 to reduce to the previous case. Thus, every $\mathbb{C}/\Lambda$ is isomorphic [9] to at least one complex torus of the form $\mathbb{C}/(\mathbb{Z}z + \mathbb{Z})$.

Replacing the ordered basis ω_1, ω_2 in a lattice $\mathbb{Z}\omega_1 + \mathbb{Z}\omega_2$ by another ordered basis ω_1', ω_2' does not change the lattice itself, so surely $\mathbb{C}/(\mathbb{Z}\omega_1 + \mathbb{Z}\omega_2) \approx \mathbb{C}/(\mathbb{Z}\omega_1' + \mathbb{Z}\omega_2')$. A change of ordered basis is given by

$$\begin{pmatrix} \omega_1' \\ \omega_2' \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot \begin{pmatrix} \omega_1 \\ \omega_2 \end{pmatrix} \qquad \text{(for some } \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z})\text{)}$$

where *the modular group* $SL_2(\mathbb{Z})$ is two-by-two integer matrices with determinant 1. Thus, in terms of a *normalized* ordered basis $z, 1$ with $z \in \mathfrak{H}$, a new ordered basis is of the form $az + b, cz + d$. *Renormalize* to

[8] The messier function $f(z) = \sum_n 1/(z+n)^2 = \pi^2/\sin^2 \pi z$ and its derivative satisfy $f'^2 = 4f^2(f - \pi)$, so $z \to (f(z), f'(z))$ maps $\mathbb{C}$ to $\{(x,y) \in \mathbb{C} : y^2 = 4x^2(x - \pi)\}$. Replacing y by xy and dividing through puts this into the form $y^2 = 4(x - \pi)$, showing that $y^2 = 4x^2(x - \pi)$ is a *degenerate* cubic.

[9] The notion of *isomorphism* should be *as Riemann surface*, but elaboration of this would take us too far afield.

make the second element of the ordered basis be 1 by multiplying by $(cz+d)^{-1}$, giving a new ordered basis $\frac{az+b}{cz+d}, 1$.

These *linear fractional transformations*

$$\gamma(z) \;=\; \frac{az+b}{cz+d} \qquad\qquad (\text{for } \gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z}))$$

send $\mathfrak{H}$ to itself, since in fact $SL_2(\mathbb{R})$ does so. [10] Thus, for $z, z' \in \mathfrak{H}$, if there is $\gamma \in SL_2(\mathbb{Z})$ such that $\gamma(z) = z'$, then the complex tori $\mathbb{C}/(\mathbb{Z}z + \mathbb{Z})$ and $\mathbb{C}/(\mathbb{Z}z' + \mathbb{Z})$ are *isomorphic*. We have not proven the converse here, but it holds.

The *quotient* of $\mathfrak{H}$ by $\Gamma = SL_2(\mathbb{Z})$ is denoted $\Gamma\backslash\mathfrak{H}$. This quotient is *the modular curve*, since it parametrizes isomorphism classes of complex tori.

---

6. *Elliptic modular forms*

[6.1] Functions of lattices The functions traditionally denoted $g_2 = g_2(\Lambda)$ and $g_3 = g_3(\Lambda)$ in the Weierstraß equation relating $\wp$ and $\wp'$ certainly depend on the lattice, or *module*, Λ. It is in this sense that they are *modular forms*. [11] That is, as they arose historically, *modular forms* are functions on the set of lattices in $\mathbb{C}$.

The functions g_2 and g_3 have the further property of *homogeneity*, meaning that for any non-zero complex number α

$$g_2(\alpha \cdot \Lambda) = \alpha^{-4}\, g_2(\Lambda) \qquad \text{and} \qquad g_3(\alpha \cdot \Lambda) = \alpha^{-6}\, g_3(\Lambda)$$

since

$$\sum_{0 \neq \lambda \in \Lambda} \frac{1}{(\alpha\lambda)^{2k}} \;=\; \alpha^{-2k} \sum_{0 \neq \lambda \in \Lambda} \frac{1}{\lambda^{2k}}$$

Thus, more precisely, *modular forms* are *homogeneous* functions on lattices in $\mathbb{C}$.

[6.2] From lattices to the upper half-plane We would be happier if the inputs to these functions-of-lattices were more familiar, rather than *lattices*, since initially we might see no helpful structure on the set of lattices. The homogeneity allows a more tangible viewpoint, as follows. Let F be a *homogeneous* function F of degree $-k$ on lattices, meaning that [12]

$$F(\alpha \cdot \Lambda) \;=\; \alpha^{-k} \cdot F(\Lambda)$$

As in the previous section, for a $\mathbb{Z}$-basis ω_1, ω_2 for a lattice Λ, *ordered* so that $\omega_1/\omega_2 \in \mathfrak{H}$, *normalize* the second basis element to 1, by multiplying Λ by ω_2^{-1} and using basis $z = \omega_1/\omega_2$, 1 for the dilated-and-rotated lattice $\omega_2^{-1} \cdot \Lambda$. By homogeneity,

$$F(\omega_2^{-1} \cdot \Lambda) \;=\; \omega_2^{k} \cdot F(\Lambda)$$

[10] As usual, for a commutative ring R, the group $SL_2(R)$ is the group of invertible 2-by-2 matrices with entries in R and determinant 1.

[11] Why *modular form* rather than *modular function*? After all, these functions *are* literal functions (in our modern sense) on the set of lattices in $\mathbb{C}$. There was historical hesitancy to refer to functions on exotic spaces, since there was no abstract notion of *function* in the 19^{th} century.

[12] Yes, g_2 is homogeneous of degree -4 and g_3 is homogeneous of degree -6. Yes, it would have been better if their indices matched their degrees of homogeneity, at least up to sign, but the tradition developed otherwise.

allowing recovery of the value of F on the original lattice from the value on the adjusted one.

Further, a function of lattices does not depend upon *choice of ordered basis*. That is, for $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ in $SL_2(\mathbb{Z})$ the new ordered basis

$$\begin{bmatrix} \omega_1' \\ \omega_2' \end{bmatrix} \;=\; \begin{bmatrix} a\omega_1 + b\omega_2 \\ c\omega_1 + d\omega_2 \end{bmatrix} \;=\; \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{bmatrix} \omega_1 \\ \omega_2 \end{bmatrix}$$

gives the same lattice, that is,

$$\mathbb{Z} \cdot \omega_1' + \mathbb{Z} \cdot \omega_2' \;=\; \mathbb{Z} \cdot \omega_1 + \mathbb{Z} \cdot \omega_2$$

As before, the normalization and change-of-basis can be combined, as follows. For $\mathbb{R}$-linearly-independent ω_1 and ω_2, and without loss of generality with ω_1/ω_2 in the upper half-plane $\mathfrak{H}$, let $z = \omega_1/\omega_2 \in \mathfrak{H}$ and put

$$f(z) \;=\; F(\mathbb{Z} \cdot z + \mathbb{Z} \cdot 1)$$

For $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ in $SL_2(\mathbb{Z})$,

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{bmatrix} z \\ 1 \end{bmatrix} \;=\; \begin{bmatrix} az + b \\ cz + d \end{bmatrix}$$

Since change-of-basis does not alter the value of a function of lattices, using homogeneity,

$$f(z) \;=\; F(\mathbb{Z} \cdot z + \mathbb{Z} \cdot 1) \;=\; F(\mathbb{Z} \cdot (az+b) + \mathbb{Z} \cdot (cz+d))$$

$$=\; (cz+d)^{-k}\, F(\mathbb{Z} \cdot \frac{az+b}{cz+d} + \mathbb{Z} \cdot 1) \;=\; (cz+d)^{-k}\, f(\frac{az+b}{cz+d})$$

Thus, the action of $SL_2(\mathbb{Z})$ by linear fractional transformations [13]

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

arises through renormalization of generators for lattices.

[6.3] Modular forms of weight k

The next incarnation of *modular forms* is as *elliptic modular forms of weight k*: these are *holomorphic* function f of a complex variable z on $\mathfrak{H}$, meeting the *automorphy condition* [14]

$$f(\begin{pmatrix} a & b \\ c & d \end{pmatrix}(z)) \;=\; (cz+d)^k\, f(z) \qquad\qquad (\text{where } \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z}),\ z \in \mathfrak{H})$$

For example, up to normalizations, the functions associated to g_2 and g_3 above fit into a family of explicitly-constructable elliptic modular forms

$$\text{Eisenstein series} \;=\; \sum_{c,d} \frac{1}{(cz+d)^k} \qquad\qquad (\text{summed over } c, d \text{ not both } 0)$$

[13] Linear fractional transformations are sometimes called *Möbius* transformations. That this action is a genuine group action, including associativity, is not obvious from an *ad hoc* presentation. As we see later, this action is descended from a reasonable *linear* action on *projective space*, giving a conceptual explanation. In general, linear fractional transformations truly act on the *Riemann sphere*, that is, on complex projective one-space $\mathbb{P}^1$, which is $\mathbb{C}$ with an additional point.

[14] The function $j(\begin{pmatrix} a & b \\ c & d \end{pmatrix}, z) = (cz+d)^{-k}$ is a *cocycle*, because it satisfies the condition $j(\gamma\delta, z) = j(\gamma, \delta(z))j(\delta, z)$.

Since $cz+d$ is complex, we must take $k \in \mathbb{Z}$. This series converges for $k > 2$. The series is identically 0, by obvious cancellation, for k odd. Verification of the automorphy condition is direct, and is really just repeating the conversion of homogeneous functions-of-lattices to functions on $\mathfrak{H}$:

$$\sum_{m,n} \frac{1}{(m\frac{az+b}{cz+d}+n)^k} \;=\; (cz+d)^k \sum_{m,n} \frac{1}{\big(m(az+b)+n(cz+d)\big)^k}$$

$$=\; (cz+d)^k \sum_{m,n} \frac{1}{\big((ma+nc)z+(mb+nd)\big)^k} \;=\; (cz+d)^k \sum_{m,n} \frac{1}{(m'z+n')^k}$$

$$(\text{with } (m',n') = (ma+nc,\ mb+nd) = (m,\ n)\begin{pmatrix} a & b \\ c & d \end{pmatrix})$$

Since right multiplication by any element of $SL_2(\mathbb{Z})$ is a bijection of $\mathbb{Z}^2 - \{0\}$ to itself, the sum is again exactly over pairs of integers not both 0, recovering the Eisenstein series.

[6.4] Normalizations of Eisenstein series In the sum $\sum_{c,d}(cz+d)^{-k}$ over all pairs $(c,d) \neq (0,0)$, we could take out *common divisors* $\ell = \gcd(c,d)$:

$$\sum_{c,d} \frac{1}{(cz+d)^k} \;=\; \sum_{c,d} \frac{1}{\ell^k} \frac{1}{(\frac{c}{\ell}z+\frac{d}{\ell})^k} \;=\; \sum_{c,d} \frac{1}{\ell^k} \frac{1}{(\frac{c}{\ell}z+\frac{d}{\ell})^k} \;=\; \sum_{\ell \geq 1} \frac{1}{\ell^k} \sum_{c,d:\, \gcd(c,d)=\ell} \frac{1}{(\frac{c}{\ell}z+\frac{d}{\ell})^k}$$

$$=\; \sum_{\ell \geq 1} \frac{1}{\ell^k} \sum_{c',d':\, \gcd(c',d')=1} \frac{1}{(c'z+d')^k} \;=\; \zeta(\ell) \sum_{c',d':\, \gcd(c',d')=1} \frac{1}{(c'z+d')^k}$$

That is, up to the constant $\zeta(\ell)$, the sum over *all* c,d gives the same thing as the sum over *coprime* c,d. Some sources create notations that attempt to distinguish these variations, but there is no universal notational convention.

[6.5] Group-theoretic version of Eisenstein series Further, noticing that for $k \in 2\mathbb{Z}$ the pairs $\pm(c,d)$ give the same outcome $(cz+d)^k$, we might declare the weight-k Eisenstein series to have a leading coefficient $\frac{1}{2}$:

$$\text{Eisenstein series} \;=\; \tfrac{1}{2} \sum_{\text{coprime } c,d} \frac{1}{(cz+d)^k}$$

Indeed, this is exactly a *group-theoretic* version of an Eisenstein series: with $\Gamma_\infty = \begin{pmatrix} * & * \\ 0 & * \end{pmatrix} \subset \Gamma$, the coset space $\Gamma_\infty \backslash \Gamma$ is in bijection with the set of coprime pairs (c,d) modulo ± 1, by

$$\Gamma_\infty \cdot \begin{pmatrix} a & b \\ c & d \end{pmatrix} \;\longrightarrow\; \{\pm 1\} \cdot (c,d)$$

Indeed, since $ad-bc=1$, necessarily the c,d in a lower row of an element of $SL_2(\mathbb{Z})$ are mutually prime. Conversely, given coprime c,d, there exist a,b such that $ad-bc=1$, creating an element of $SL_2(\mathbb{Z})$. Thus, another presentation of an Eisenstein series, perhaps optimally explanatory:

$$E_k(z) \;=\; \sum_{\gamma \in \Gamma_\infty \backslash \Gamma} \frac{1}{(c_\gamma z + d_\gamma)^k} \;=\; \tfrac{1}{2} \sum_{\text{coprime } c,d} \frac{1}{(cz+d)^k} \qquad (\text{where } \gamma = \begin{pmatrix} * & * \\ c_\gamma & d_\gamma \end{pmatrix})$$

[6.6] Congruence subgroups There are Eisenstein series with *congruence conditions*: for fixed positive integer N and integers c_o, d_o, define Eisenstein series with *congruence conditions*

$$E(z) \;=\; \sum_{(c,d)=(c_o,d_o) \bmod N} \frac{1}{(cz+d)^k} \quad (c,d \text{ not both } 0)$$

This is an example of a modular form *of level* N, meaning that a condition such as

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \mod N \quad \text{(elementwise)}$$

is necessary to have[15] this Eisenstein series satisfy the *automorphy* condition

$$E(\begin{pmatrix} a & b \\ c & d \end{pmatrix}(z)) \;=\; (cz+d)^k\, E(z)$$

The first examples were tacitly of level 1. Such considerations motivate attention to natural subgroups of $SL_2(\mathbb{Z})$, with traditional notations: for a positive integer N,

$$\begin{aligned}
\Gamma(N) &= \{\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z}) \;:\; a = 1 \bmod N, b = 0 \bmod N, c = 0 \bmod N, d = 1 \bmod N\} \\
&= \{\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z}) \;:\; \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \mod N\} \\
\Gamma_0(N) &= \{\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z}) \;:\; \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{bmatrix} * & * \\ 0 & * \end{bmatrix} \mod N\} \\
\Gamma_1(N) &= \{\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z}) \;:\; \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{bmatrix} 1 & * \\ 0 & 1 \end{bmatrix} \mod N\}
\end{aligned}$$

In particular, the frequently occurring subgroup $\Gamma(N)$ is also denoted Γ_N for reasons of economy:

$$\Gamma_N = \Gamma(N) = \textit{ principal} \text{ congruence subgroup of level } N$$

[6.7] Preview: a less-elementary modular form

Up to a normalizing constant, the *discriminant*[16] of Weierstraß' cubic $4x^3 - g_2x - g_3$ is $g_2^3 - 27g_3^2$. For the lattice $\Lambda_z = \mathbb{Z}\cdot z + \mathbb{Z}\cdot 1 \subset \mathbb{C}$, the discriminant is an elliptic modular form of weight 12, usually normalized as

$$\Delta(z) \;=\; \frac{1}{(2\pi)^{12}}\,(g_2^3 - 27g_3^2)$$

We'll later prove the surprising factorization

$$\Delta(z) \;=\; e^{2\pi iz}\prod_{n=1}^{\infty}(1-e^{2\pi inz})^{24}$$

This factorization suggests combinatorial applications, in light of the generating function identity

$$\prod_{n=1}^{\infty}\frac{1}{1-q^n} \;=\; \sum_{n=0}^{\infty} p(n)\cdot x^n$$

[15] Some choices of the data c_o, d_o modulo N may allow larger groups than $\Gamma(N)$. For example, $c_o = d_o = 0$ does not require any congruence condition at all (and yields N^{-k} times the simplest Eisenstein series $E(z) = \sum_{c,d} 1/(cz+d)^k$ summed over all c, d not both 0.

[16] The *discriminant* of a cubic $(x-\alpha)(x-\beta)(x-\gamma)$ is $\Delta = (\alpha-\beta)^2(\alpha-\gamma)^2(\beta-\gamma)^2$. Invariant under permutations of the roots, it is expressible in terms of the *elementary* symmetric functions $s_1 = \alpha+\beta+\gamma$, $s_2 = \alpha\beta+\beta\gamma+\gamma\alpha$, and $s_3 = \alpha\beta\gamma$. After some work, one finds

$$\Delta \;=\; (s_1^2 - 4s_2)s_2^2 + s_3(-4s_1^3 + 18s_1s_2 - 27s_3)$$

For a cubic $x^3 + px + q$ this simplifies to the more-familiar $-4p^3 - 27q^2$.

where $p(n)$ is the number of *partitions* $n_1 + \ldots + n_k = n$, with $n_1 \leq n_2 \leq \ldots \leq n_k$. Even more profoundly, as it turns out, the Fourier expansion

$$\Delta(z) \;=\; e^{2\pi iz} + \sum_{n\geq 2} \tau(n)\, e^{2\pi inz}$$

has coefficients $\tau(n)$ with properties conjectured by S. Ramanujan: *weak multiplicativity* $\tau(mn) = \tau(m)\tau(n)$ for coprime m, n was proven by L. J. Mordell soon after, but the estimate $|\tau(p)| \leq 2p^{\frac{11}{2}+\varepsilon}$ for every $\varepsilon > 0$ was proven only in 1974 by P. Deligne, as a striking corollary of the Grothendieck-Deligne-*et al* proof of Weil's conjectures on Hasse-Weil zeta functions of algebraic varieties. E. Hecke had proven $|\tau(p)| \leq 2p^{\frac{12}{2}}$ in fairly straightforward fashion decades earlier, but that last $\frac{1}{2} + \varepsilon$ was much larger, and more meaningful, than it may seem.

[6.8] Preview: the j-invariant and parametrization of elliptic curves As above, a reasonable notion of isomorphism of elliptic curves $\mathbb{C}/\Lambda$ leads to identifying the collection of isomorphism classes with the quotient $\Gamma\backslash\mathfrak{H}$, with $\Gamma = SL_2(\mathbb{Z})$.

The j-function is

$$j(z) \;=\; 1728\frac{g_2^3}{g_2^3 - 27g_3^2}$$

The numerator and denominator are both weight 12 level one modular forms, so $j(z)$ is weight 0, that is, *invariant* under $SL_2(\mathbb{Z})$.

We will see that $z \to j(z)$ *injects* the quotient $SL_2(\mathbb{Z})\backslash\mathfrak{H}$ to complex projective one-space $\mathbb{P}^1$, so $j(z)$ is a sufficient invariant for isomorphism classes of elliptic curves over $\mathbb{C}$.

[6.8.1] Remark: There is much more to be said about modular forms, even from an elementary viewpoint! The above preview neglects many aspects!
