A litte about Ellipse–Integral, Function, Curve and Modular Form

Baizhou Jin 2021011644

Contents

1 Elliptic Integral

1.1 Start from calculating the perimeter of the ellipse

Consider an ellipse on the plane

$$\frac{x^2}{a^2} + \frac{y^2}{b^2} = 1$$

We cam calculate the perimeter of it. Consider the parameterize $x = acost, y = bsint$, there are

$$L = \int_0^{2\pi} \sqrt{x'^2 + y'^2} \mathrm{d}t = \int_0^{2\pi} \sqrt{a^2 sin^2 t + b^2 cos^2 t} \mathrm{d}t$$

Sadly, it cannot be simplify more. By the theorem of Liouville's theorem, L cannot be written as composition of elementary functions. Fortunately, by centuries, people have learned a lot about it.

At first, Guilio Fagnano and Euler studied about it. The study of Euler will be talked later. Now, I would like to show the first beautiful result yielded by Gauss from analyzing the elliptic integral.

1.2 Gauss's AGM method

In 1791, Gauss noticed the interesting property of the Algebraic-Geometric Average. At that time, he got this well-known result. [4]

Theorem 1 *Consider two series*

$$\begin{aligned} a_{n+1} &= \tfrac{a_n + b_n}{2} \\ b_{n+1} &= \sqrt{a_n b_n} \\ a_0 = 1, b_0 &= \tfrac{1}{\sqrt{2}} \end{aligned}$$

For $p_n = \frac{2a_n^2}{1 - \sum_{i=0}^n 2^i \left(a_i^2 - b_i^2\right)}$, *there are* $lim p_n = \pi$

Now I would like to introduce how to get this result by the elliptic integral.

Firstly, it is not difficult to prove that a_n and b_n converges to the same number, denoted by $M\left(a_0, b_0\right)$.

The function M has the following properties:

1.$\lambda M\left(a, b\right) = M\left(\lambda a, \lambda b\right)$ for $\lambda > 0$

2.$M\left(a, b\right) = M\left(\frac{a+b}{2}, \sqrt{ab}\right)$

Define

$$I\left(a,b\right)=\int_{0}^{\infty}\frac{1}{\sqrt{\left(x^2+a^2\right)\left(x^2+b^2\right)}}\mathrm{d}x$$

This integral converges, because

$$\frac{c}{x^2+1}<\frac{1}{\sqrt{\left(x^2+a^2\right)\left(x^2+b^2\right)}}<\frac{C}{x^2+1}\ c,C>0$$

Not difficult to prove that $\frac{\partial I}{\partial a}$ and $\frac{\partial I}{\partial b}$ exist and continuous. Consider the change of variable $x=btan\theta$, there are

$$\begin{aligned}I\left(a,b\right)&=\int_{0}^{\infty}\frac{1}{\sqrt{\left(x^2+a^2\right)\left(x^2+b^2\right)}}\mathrm{d}x\\&=\int_{0}^{\frac{\pi}{2}}\frac{b}{\sqrt{cos^4\theta\left(b^2tan^2\theta+a^2\right)\left(b^2tan^2\theta+b^2\right)}}\mathrm{d}\theta\\&=\int_{0}^{\frac{\pi}{2}}\frac{1}{\sqrt{\left(b^2sin^2\theta+a^2cos^2\theta\right)\left(sin^2\theta+cos^2\theta\right)}}\mathrm{d}\theta\\&=\int_{0}^{\frac{\pi}{2}}\frac{1}{\sqrt{b^2sin^2\theta+a^2cos^2\theta}}\mathrm{d}\theta\\&=\int_{0}^{\frac{\pi}{2}}\frac{1}{\sqrt{a^2-\left(a^2-b^2\right)sin^2\theta}}\mathrm{d}\theta\end{aligned}$$

We samely define that

$$J\left(a,b\right)=\int_{0}^{\infty}\sqrt{b^2sin^2\theta+a^2cos^2\theta}\mathrm{d}x$$

Consider the change of variable I: $y=\frac{\sqrt{ab}}{x}$, there are

$$\int_{0}^{\sqrt{ab}}\frac{1}{\sqrt{\left(x^2+a^2\right)\left(x^2+b^2\right)}}\mathrm{d}x=\int_{\sqrt{ab}}^{\infty}\frac{1}{\sqrt{\left(x^2+a^2\right)\left(x^2+b^2\right)}}\mathrm{d}x$$

Then

$$\int_{\sqrt{ab}}^{\infty}\frac{1}{\sqrt{\left(x^2+a^2\right)\left(x^2+b^2\right)}}\mathrm{d}x=\frac{1}{2}I\left(a,b\right)$$

Now consider $y=x-\frac{\sqrt{ab}}{x}$, we finally get that

$$I\left(a,b\right)=I\left(\frac{a+b}{2},\sqrt{ab}\right)$$

That is,

$$I\left(a_n,b_n\right)=I\left(a_0,b_0\right)$$

Since $\frac{\partial I}{\partial a}$ and $\frac{\partial I}{\partial b}$ exist and continuous, let $n\to\infty$, there are

$$I\left(a,b\right)=I\left(M\left(a,b\right),M\left(a,b\right)\right)$$

By the simple calculation,

$$I\left(M\left(a,b\right),M\left(a,b\right)\right)=\frac{\pi}{2M\left(a,b\right)}$$

That is,

$$2I\left(a,b\right)M\left(a,b\right)=\pi$$

Take $a=1,b=\frac{1}{\sqrt{2}}$, there are

$$M\left(a,b\right)=\frac{\pi}{2I\left(a,b\right)}=\frac{\pi}{2\int_0^{\frac{\pi}{2}}\frac{1}{\sqrt{1-\frac{1}{2}sin^2\theta}}\mathrm{d}\theta}$$

Define

$$K\left(k\right)=\int_0^{\frac{\pi}{2}}\frac{1}{\sqrt{1-k^2sin^2\theta}}\mathrm{d}\theta$$

$$E\left(k\right)=\int_0^{\frac{\pi}{2}}\sqrt{1-k^2sin^2\theta}\mathrm{d}\theta$$

These are some types of the classical elliptic integral.

There are

$$M\left(1,\frac{1}{\sqrt{2}}\right)=\frac{\pi}{2K\left(\frac{1}{\sqrt{2}}\right)}$$

Take derivative about K

$$kK'\left(k\right)=\int_0^{\frac{\pi}{2}}\frac{k^2sin^2\theta}{\left(\sqrt{1-k^2sin^2\theta}\right)^3}\mathrm{d}\theta$$

$$=-K\left(k\right)+\frac{E\left(k\right)}{1-k^2}-\frac{k^2}{1-k^2}\int_0^{\frac{\pi}{2}}\frac{-1+2sin^2\theta-k^2sin^4\theta}{\left(1-k^2sin^2\theta\right)^2}\mathrm{d}\theta$$

Consider $sin^2\theta=\frac{tan\theta}{1+tan^2\theta}$ and consider the change of variable $\theta=\arctan y$, we can finally draw it into a rational integral and prove it vanish, then

$$K'\left(k\right)=\frac{E\left(k\right)}{k\left(1-k^2\right)}-\frac{K\left(k\right)}{k}$$

By the same way, there are

$$E'(k) = \frac{E(k) - K(k)}{k}$$

Then, we can prove directly through $\widetilde{E}(k) = E\left(\sqrt{1-k^2}\right), \widetilde{K}(k) = K\left(\sqrt{1-k^2}\right)$ that,

$$\left(E\widetilde{K} + \widetilde{E}K - K\widetilde{K}\right)' = 0$$

That is $E\widetilde{K} + \widetilde{E}K - K\widetilde{K} = C$ for some C.

Consider $k = \frac{1}{\sqrt{2}}$

$$\begin{aligned}
K(k) &= \int_0^{\frac{\pi}{2}} \frac{1}{\sqrt{1 - \frac{1}{2}sin^2\theta}} \mathrm{d}\theta \\
&\xlongequal{\theta=\arcsin\left(\sqrt{\frac{2x}{1+x^2}}\right)} \int_0^1 \frac{1}{\sqrt{2x(1-x^2)}} \mathrm{d}x \\
&\xlongequal{t=x^2} \frac{1}{2\sqrt{2}} \int_0^1 t^{-\frac{3}{4}} (1-t)^{-\frac{1}{2}} \mathrm{d}t \\
&= \frac{1}{2\sqrt{2}} B\left(\frac{1}{4}, \frac{1}{2}\right)
\end{aligned}$$

and

$$\begin{aligned}
2E(k) - K(k) &= \int_0^{\frac{\pi}{2}} \frac{1 - sin^2\theta}{\sqrt{1 - \frac{1}{2}sin^2\theta}} \mathrm{d}\theta \\
&\xlongequal{\theta=\arcsin\left(\sqrt{\frac{2x}{1+x^2}}\right)} \int_0^1 \frac{1}{\sqrt{2x(1-x^2)}} \frac{1-x}{1+x} \mathrm{d}x \\
&\xlongequal{x=\frac{1-u}{1+u}} \frac{1}{\sqrt{2}} \int_0^1 \sqrt{\frac{u}{1-u^2}} \mathrm{d}u \\
&\xlongequal{t=u^2} \frac{1}{2\sqrt{2}} \int_0^1 t^{-\frac{1}{4}} (1-t)^{-\frac{1}{2}} \mathrm{d}t \\
&= \frac{1}{2\sqrt{2}} B\left(\frac{3}{4}, \frac{1}{2}\right)
\end{aligned}$$

Then

$$C = (2K - E) K = \frac{1}{8} B\left(\frac{3}{4}, \frac{1}{2}\right) B\left(\frac{1}{4}, \frac{1}{2}\right)$$

By the property of Beta function,

$$B(a,b) = \frac{\Gamma(a)\Gamma(b)}{\Gamma(a+b)}$$

$$C = \frac{1}{8}\frac{\Gamma\left(\frac{1}{2}\right)\Gamma\left(\frac{1}{4}\right)}{\Gamma\left(\frac{3}{4}\right)}\frac{\Gamma\left(\frac{1}{2}\right)\Gamma\left(\frac{3}{4}\right)}{\Gamma\left(\frac{5}{4}\right)}$$

$$= \frac{1}{8} \times 4 \times \sqrt{\pi} \times \sqrt{\pi} = \frac{\pi}{2}$$

Above all, we get

$$K\left(k\right) = \frac{1}{1+k}K\left(\frac{2\sqrt{k}}{1+k}\right)$$

Multiplied by $1+k$ and take derivative, denoted by $g\left(k\right) = \frac{2\sqrt{k}}{1+k}$, there are

$$\left(1+k\right)K'\left(k\right) + K\left(k\right) = K'\left(g\left(k\right)\right)g'\left(k\right)$$

By $K'\left(k\right) = \frac{E(k)}{k(1-k^2)} - \frac{K(k)}{k}$ we can cancel K', by $K\left(k\right) = \frac{1}{1+k}K\left(\frac{2\sqrt{k}}{1+k}\right)$ we can cancel $E\left(g\left(k\right)\right)$, we finally get

$$E\left(k\right) = \frac{1+k}{2}E\left(g\left(k\right)\right) + \frac{k'^2}{2}K\left(k\right)$$

Finally, we replace k by $g^{-1}\left(k\right)$, we get

$$E\left(k\right) = \left(1+k'\right)E\left(\frac{1-k'}{1+k'}\right) - k'^2K\left(k\right)$$

Recall that

$$I\left(a,b\right) = \int_0^{\frac{\pi}{2}} \frac{1}{\sqrt{b^2sin^2\theta + a^2cos^2\theta}}\mathrm{d}x$$

$$J\left(a,b\right) = \int_0^{\infty} \sqrt{b^2sin^2\theta + a^2cos^2\theta}\mathrm{d}x$$

We claim that

$$2J\left(a_{n+1}, b_{n+1}\right) - J\left(a_n, b_n\right) = a_nb_nI\left(a_n, b_n\right)$$

This is because $k_n = \frac{c_n}{a_n}, k'_n = \frac{b_n}{a_n}$, where $c_n = \sqrt{a_n^2 - b_n^2}$

There are

$$2J\left(a_{n+1}, b_{n+1}\right) = 2a_{n+1}E\left(\sqrt{1 - \frac{b_{n+1}^2}{a_{n+1}^2}}\right) = 2a_{n+1}E\left(k_{n+1}\right)$$

$$J\left(a_n, b_n\right) = a_nE\left(k_n\right)$$

and $k_{n+1} = \frac{a_n - b_n}{a_n + b_n} = \frac{1-k'_n}{1+k'_n}$

which is equals to

$$2a_{n+1}E\left(k_{n+1}\right) - a_nE\left(k_n\right) = b_nK\left(b_n\right)$$

which is proved before.

Then, we get $2J\left(a_{n+1}, b_{n+1}\right) - J\left(a_n, b_n\right) = a_n b_n I\left(a_n, b_n\right) = a_n b_n I\left(a_0, b_0\right)$, because $4a_{n+1}^2 - 2a^n - 2a_n b_n = -c_n^2$,

$$2^{n+1}[J\left(a_{n+1}, b_{n+1}\right) - a_{n+1}^2 I\left(a_0, b_0\right)] - 2^n[J\left(a_n, b_n\right) - a_n^2 I\left(a_0, b_0\right)]$$
$$= 2^{n-1} c_n^2 I\left(a_0, b_0\right)$$

Add up those, we get $J\left(a_0, b_0\right) = \left(a_0^2 - \sum_{n=0}^{\infty} 2^{n-1} c_n^2\right) I\left(a_0, b_0\right)$.

That is $E\left(k\right) = \left(1 - \sum_{n=0}^{\infty} 2^{n-1} c_n^2\right) K\left(k\right)$,

Now, for $k = \frac{1}{\sqrt{2}}$

$$\lim_{n\to\infty} 1 - \sum_{n=0}^{n} 2^k c_k^2 = 2\frac{E}{K} - 1$$

and $\lim_{n\to\infty} a_n = \frac{\pi}{2K}$

Then, we finally get

$$\lim_{n\to\infty} \frac{2a_n^2}{1 - \sum_{n=0}^{n} 2^k c_k^2} = \frac{\pi^2}{2\left(2EK - K^2\right)} = \pi$$

which proves the upper theorem.

By the way, in 1816, Schumacher write to Gauss about his analysis for the Algebraic-Geometric average, Gauss said candidly that he had studied this series since 1791, and get abundant results that "can fill a whole book". However, according to Klein, these are the simple puzzles Gauss designed for himself at the age of 14. We can have a glance at the great talent of Gauss–the prince of Maths. [17]

Felix Klein said, all those puzzles, firstly designed for seeking interest, would become the first step of seeking great treasure, which was Gauss noticed when he grew up. To put the first dig of the hoe on a buried gold mine looks like a great foresight, which is definitely a part of talent. The foresight coming through one's trails which is firstly used to show his intelligence has great meaning, which is hard to be realized. [6]

1.3 Ramanujan and his functions

In 20th centery, Ramanujan contributed a lot about the theory of elliptic function. Almost all of his work are abstract and gorgeous. [5]

Definition 1 For q complex variable, $|q| < 1$

$$Q = 1 + 240 \sum_{j\geqslant 1} \frac{j^3 q^j}{1 - q^j}$$

$$R = 1 - 504\sum_{j\geqslant 1}\frac{j^5 q^j}{1-q^j}$$

$$P = 1 - 24\sum_{j\geqslant 1}\frac{j q^j}{1-q^j}$$

Theorem 2 *There are Ramanujan Differential Equations:* $\begin{cases} q\frac{dP}{dq} = \frac{P^2-Q}{12} \\ q\frac{dQ}{dq} = \frac{PQ-R}{3} \\ q\frac{dR}{dq} = \frac{PR-Q^2}{2} \end{cases}$

For this, define $\rho_1(z) = \frac{1}{2} + \sum' \frac{z^n}{1-q^n}$

$\rho_2(z) = -\frac{1}{12} + \sum \frac{q^n z^n}{1-q^n}$

They have the following properties:

$\forall \alpha\beta\gamma = 1$, there are $\rho_1(\alpha)\rho_1(\beta) - \rho_1(\alpha\beta)(\rho_1(\alpha) + \rho_1(\beta)) = \rho_2(\alpha) + \rho_2(\beta) + \rho_2(\gamma)$

And

$\begin{cases} \rho_1(z^{-1}) = -\rho_1(z) \\ \rho_1(z) - \rho_1(qz) = -1 \end{cases}$

$\begin{cases} \rho_2(z^{-1}) = \rho_2(z) \\ \rho_2(z) - \rho_2(qz) = \frac{1}{2} + \rho_1(z) \end{cases}$

Then the upper can be written as

$\forall \alpha\beta\gamma = 1$, there are $\rho_1(\alpha)\rho_1(\beta) + \rho_1(\gamma)\rho_1(\alpha) + \rho_1(\beta)\rho_1(\gamma) = \rho_2(\alpha) + \rho_2(\beta) + \rho_2(\gamma)$

Denote by $\phi_1(\theta) = \frac{1}{2i}\rho_1(e^{i\theta}), \phi_2(\theta) = \frac{1}{2}\rho_2(e^{i\theta})$

There are $\frac{1}{16}\left(\frac{\phi_1''(a)-\phi_1''(b)}{\phi_1'(a)-\phi_1'(b)}\right)^2 = \frac{3}{2}\phi_2(0) - \frac{1}{2}(\phi_1'(a) + \phi_1'(b) + \phi_1'(c))$

Here, define $p(a) = 2(\phi_2(0) - \phi_1'(a))$, there are

$\frac{1}{4}\left(\frac{p'(a)-p'(b)}{p(a)-p(b)}\right)^2 = p(a) + p(b) + p(c)$

p is called the Weierstrass Elliptic Function, also known as Weierstrass $\wp-$function. Its property will be specify in next section, here, we just mention some of them.

There are

$\frac{1}{4}\left(\frac{p'(a)-p'(b)}{p(a)-p(b)}\right)^2 - p(a) - p(b) = p(a+b)$

which is the addition principal of Weierstrass $\wp-$function.

Define $\phi_{m,n} = \sum_{j\geqslant 1}\sum_{k\geqslant 1} j^m k^n q^{jk}$, we have ϕ converges absolutely if $|q| < 1$

Consider the equality

$$(\phi_1(a)+\phi_1(b))\,\phi_1(a+b)-\phi_1(a)\,\phi_1(b)=\frac{1}{2}\left(\phi_2(a)+\phi_2(b)+\phi_2(a+b)\right)$$

we can view this equality as function of b, then we can expand the both sides in powers of b, then compare the coef. of b^2, we get the equality

$$2\phi_1^2(a)\,\phi_1''(a)-\frac{P}{6}\phi_1'(a)+\frac{1}{3}\phi_1'''(a)=\phi_2''(a)-\phi_{1,2}(a)$$

Also, there are $\phi_1^2(a)+\frac{1}{2}\phi_1'(a)=\phi_2(a)+\frac{1}{2}\phi_2(0)$, take the 2nd derivative, we get

$$2\left(\phi_1'(a)\right)^2+2\phi_1(a)\,\phi_1''(a)+\frac{1}{2}\phi_1'''(a)=\phi_2''(a)$$

Now, by cancelling the term $\phi_2''(a)$, we get

$$4\left(\phi_1'(a)\right)^2+\frac{P}{3}\phi_1'(a)+\frac{1}{3}\phi_1'''(a)=2\phi_{1,2}+\frac{P^2}{144}$$

That is, $p^2-\frac{1}{6}p''=2\phi_{1,2}+\frac{P^2}{144}$

We will show later that $2\phi_{1,2}+\frac{P^2}{144}=\frac{Q}{144}$

Then, since $12p'(a)\left(p^2(a)-\frac{1}{6}p''(a)\right)=\frac{Q}{144}\cdot 12p'(a)$, we get

$$4p^3-\left(p'(a)\right)^2=\frac{Qp(a)}{12}+k$$

Also, $k=-\frac{R}{216}$,

$$\left(p'\right)^2=4p^3-\frac{Q}{12}p-\frac{R}{216}$$

Now, put $g_2=\frac{Q}{12}, g_3=\frac{R}{216}$, we see it is the form of Weierstrass $\wp-$function.

Remark 1 In fact,

$$p(\theta)=\frac{1}{\theta^2}-\sum_{m,n}{}'\left(\frac{1}{(\theta-2\pi n-2\pi\tau m)^2}-\frac{1}{(2\pi n+2\pi\tau m)^2}\right)$$

with some $Im\tau>0$

Now, look back to the Ramanujan's DE

$$\begin{cases} q\frac{dP}{dq} = \frac{P^2-Q}{12} \\ q\frac{dQ}{dq} = \frac{PQ-R}{3} \\ q\frac{dR}{dq} = \frac{PR-Q^2}{2} \end{cases}$$

Proof: $\phi_{m,n}=\sum_j\sum_k j^m k^n q^{jk}$

Denote $S_r=\frac{B_{r+1}}{2(r+1)}+\phi_{0,r}$, B the Bernoulli number.

We have $S_1=-\frac{P}{24}, S_3=\frac{Q}{240}, S_5=-\frac{R}{504}$

With

$$\phi_1(\theta) = \frac{1}{2\theta} + \sum_n \frac{(-1)^{n-1}}{(2n-1)!} S_{2n-1}\theta^{2n-1}$$

$$\phi_2(\theta) = \frac{1}{24} + \sum_n \frac{(-1)^{n+1}}{(2n)!} \phi_{1,2n}\theta^{2n}$$

$$p(\theta) = \frac{1}{\theta^2} + 2\sum_n \frac{(-1)^{n+1}}{(2n)!} S_{2n+1}\theta^{2n}$$

And $p''(\theta) = 6p^2(\theta) - \frac{Q}{24}$

With $S_{2n+3} = \frac{12(n+1)(2n+1)}{(n-1)(2n+5)} \sum_{j=1}^{n-1} \binom{2n}{2j} S_{2j+1}S_{2n+1-2j}$. For this, we observe that if $r \geqslant 1$, $S_{2r+1} \in \mathbb{Q}[Q,R]$.

Then $S_{2n-1} = \sum_{2i+3j=n} K_{ij}Q^iR^j, K_{ij} \in \mathbb{Q}$

We have proved that $\phi_1^2 + \frac{1}{2}\phi_1' = \phi_2(\theta) + \frac{S_1}{2}$

$$LHS = \left(\frac{1}{2\theta} + \sum_n \frac{(-1)^{n-1}}{(2n-1)!} S_{2n-1}\theta^{2n-1}\right)\left(\frac{1}{2\theta} + \sum_n \frac{(-1)^{n-1}}{(2n-1)!} S_{2n-1}\theta^{2n-1}\right)$$

$$+ \frac{1}{2}[\frac{1}{2\theta} + \sum_n \frac{(-1)^{n-1}}{(2n-1)!} S_{2n-1}\theta^{2n-1}]'$$

$$= \frac{1}{4\theta^2} + \sum_a \frac{(-1)^{a-1}}{(2a-1)!} S_{2a-1}\theta^{2a-2} + \sum_{a,b} \frac{(-1)^{a+b-2}}{(2a-1)!\,(2b-1)!} S_{2a-1}S_{2b-1}$$

$$\theta^{2a+2b-2} + [-\frac{1}{4\theta^2} + \frac{1}{2}\sum_m \frac{(-1)^{m-1}}{(2m-2)!} S_{2m-1}\theta^{2m-2}]$$

$$= \sum_n \frac{(-1)^{n-1}}{(2n-1)!} S_{2n-1}\theta^{2n-2} + \sum_n \left(\sum_{j=1}^{n} \frac{(-1)^{n-1}}{(2j-1)!\,(2n+1-2j)!} S_{2j-1}S_{2n+1-2j}\right)$$

$$\theta^{2n} + \frac{1}{2}\sum_n \frac{(-1)^n}{(2n)!} S_{2n+1}\theta^2 n$$

Noticed that $\phi_{1,2n} = \frac{2n+3}{2(2n+1)} S_{2n+1} - \sum_{j=1}^{n} \binom{2n}{2j-1} S_{2j-1}S_{2n+1-2j}$

We have $\begin{cases} \phi_{1,2} = \frac{5}{6}S_3 - 2S_1^2 \\ \phi_{1,4} = \frac{7}{10}S_5 - 8S_1S_3 \\ \phi_{1,6} = S_3^2 - 12S_1S_5 \end{cases}$

That is, $\begin{cases} 288\phi_{1,2} = Q - P^2 \\ 720\phi_{1,4} = PQ - R \\ 1008\phi_{1,6} = Q^2 - PR \end{cases}$

And it is easy to check that $q\frac{d}{dq}\phi_{m,n} = \phi_{m+1,n+1}$

Then $\begin{cases} 288q\frac{d}{dq}\phi_{0,1}\phi_{1,2} = Q - P^2 \\ 720q\frac{d}{dq}\phi_{0,3} = PQ - R \\ 1008q\frac{d}{dq}\phi_{0,5} = Q^2 - PR \end{cases}$ □

Now, we may consider the deg-3 eqn $4t^3 - \frac{Q}{12}t - \frac{R}{216} = 0$, it has the discriminant $Q^3 - R^2$

By using the R-DE, we get $q\frac{d}{dq}[\log(Q^3 - R^2)] = P = 1 - 24\sum_n \frac{nq^n}{1-q^n}$

Then, $\log(Q^3 - P^2) = \int \frac{1}{q} - 24\sum_n \frac{nq^{n-1}}{1-q^n}dq = \log q + 24\sum\log(1-q^n) + C$

In fact, there are $Q^3 - R^2 = 1728q\prod_n (1-q^n)^{24}$

Remark 2 $q\prod_n(1-q^n)^{24} = \sum_n \tau(n)\,q^n$, and $\tau(n) \equiv \sigma_{11}(n)\,[691]$, where $\sigma_r(n) = \sum_{d|n} d^r$

This isn't a mystery thing: in fact, the equality holds:

$$691 + 65520\sum_n \frac{n^{11}q^n}{1-q^n} = 411Q^3 + 250R^2$$

Ramanujan studied lots of property about the tau functions. Here are some other result:

$$\tau(5n) = 0[5]$$

$$\tau(7n), \tau(7n-1), \tau(7n-2), \tau(7n-4) = 0[7]$$

$$\tau(23n+m) = 0[5], m = -1, -2, -3, -4, 5, -6, 7, -8, -9, 10, 11$$

$$\tau(n) = \sigma_{11}(n)\,[4068608], for\ n\ odd$$

The last equality is simply hold because 4068608 = 23 × 256 × 691 [1]

However, whether $\tau \neq 0$ always holds is still a conjecture. In 2013, Derickx, van Hoeij and Zeng verified the conjecture for n up to 816 212 624 008 787 344 127 999. [13]

1.4 Jacobi Identity

1.4.1 First proof from Ramanujan

Let $|q| < 1, z \neq 0,\ f(z) = \prod_{n=1}^{\infty} \left(1 + zq^{2n-1}\right)\left(1 + z^{-1}q^{2n-1}\right)$, we have the product converges absolutely and uniformly on cpt subsets of $0 < |z| < \infty$.

Denote the Laurent expansion $f(z) = \sum_{-\infty}^{\infty} c_n z^n$, $\frac{f(z)}{f(q^2z)} = \frac{1+zq}{1+z^{-1}q^{-1}} = zq$. Then $qzf\left(q^2z\right) = f(z)$, we obtain $c_n = q^{n^2}c_0$. That is $f(z) = c_0 \sum_{-\infty}^{\infty} q^{n^2}z^n$.

Everything goes well, except a small question: How to calculate c_0? However, calculating c_0 is extremely hard, for we can hardly let z be something and calculate the things directly.

Ramanujan gave this way:

For $\Phi(z, \alpha, \beta) = \prod_{n=1}^{\infty} \frac{\left(1+zq^{2n-1}\right)\left(1+z^{-1}q^{2n-1}\right)}{\left(1+\alpha zq^{2n-1}\right)\left(1+\beta z^{-1}q^{2n-1}\right)}$

There are $\Phi(z, \alpha, \beta) = \sum c_n(\alpha, \beta) z^n$.

Since $\frac{\Phi\left(q^2z,\alpha,\beta\right)}{\Phi(z,\alpha,\beta)} = \frac{(1+\alpha qz)\left(1+q^{-1}z^{-1}\right)}{\left(1+\beta q^{-1}z^{-1}\right)(1+qz)}$

Then, $(1 + \alpha qz)\Phi(z, \alpha, \beta) = (\beta + qz)\Phi\left(q^2z, \alpha, \beta\right)$

Then, we can get the recurrence relation:

$$c_n(\alpha, \beta) = \frac{q^{2n-2} - \alpha}{1 - \beta q^{2n}} qc_{n-1}$$

That is,

$$c_n(\alpha, \beta) = \frac{(1-\alpha)\left(q^2 - \alpha\right)\cdots\left(q^{2n-2} - \alpha\right)}{\left(1 - \beta q^2\right)\left(1 - \beta q^4\right)\cdots\left(1 - \beta q^{2n}\right)} q^n c_0(\alpha, \beta)$$

with $c_{-n}(\alpha, \beta) = c_n(\beta, \alpha)$

Now, we can calculate the residue at $z = -(\alpha q)^{-1}$

$$\begin{aligned}
&\lim_{z\to-(\alpha q)^{-1}} (1 + \alpha qz)\Phi(z, \alpha, \beta) \\
=& \lim_{z\to-(\alpha q)^{-1}} (1 + \alpha qz) \prod_{n=1}^{\infty} \frac{\left(1 + zq^{2n-1}\right)\left(1 + z^{-1}q^{2n-1}\right)}{\left(1 + \alpha zq^{2n-1}\right)\left(1 + \beta z^{-1}q^{2n-1}\right)} \\
=& \prod_{n=1}^{\infty} \frac{\left(1 + zq^{2n-1}\right)\left(1 + z^{-1}q^{2n-1}\right)}{\left(1 + \alpha zq^{2n+1}\right)\left(1 + \beta z^{-1}q^{2n-1}\right)}\Bigg|_{z=-(\alpha q)^{-1}} \\
=& \prod_{n=1}^{\infty} \frac{\left(1 - \alpha^{-1}q^{2n-2}\right)\left(1 - \alpha q^{2n}\right)}{\left(1 - q^{2n}\right)\left(1 - \alpha\beta q^{2n}\right)}
\end{aligned}$$

And

$$\lim_{z\to-(\alpha q)^{-1}}(1+\alpha qz)\,\Phi(z,\alpha,\beta)$$

$$=\lim_{N\to\infty}c_0(\alpha,\beta)+\sum_{i=1}^{N}(\alpha qc_{n-1}+c_n)(-\alpha q)^{-n}$$

$$=\lim_{N\to\infty}c_N(-\alpha q)^{-N}$$

$$=\lim_{N\to\infty}\frac{(1-\alpha^{-1})\cdots(1-\alpha^{-1}q^{2N-2})}{(1-\beta q^2)\cdots(1-\beta q^{2N})}c_0(\alpha,\beta)$$

$$=c_0(\alpha,\beta)\prod_{n=1}^{\infty}\frac{1-\alpha^{-1}q^{2n-2}}{1-\beta q^{2n}}$$

Then, $c_0(\alpha,\beta)=\prod_{n=1}^{\infty}\frac{(1-\alpha q^{2n})(1-\beta q^{2n})}{(1-q^{2n})(1-\alpha\beta q^{2n})}$ That is,

$$\prod_{n=1}^{\infty}\frac{(1+zq^{2n-1})(1+z^{-1}q^{2n-1})(1-q^{2n})(1-\alpha\beta q^{2n})}{(1+\alpha zq^{2n-1})(1+\beta z^{-1}q^{2n-1})(1-\alpha q^{2n})(1-\beta q^{2n})}=1$$

$$+\sum_{n=1}^{\infty}\frac{(1-\alpha)(q^2-\alpha)\cdots(q^{2n-2}-\alpha)}{(1-\beta q^2)(1-\beta q^4)\cdots(1-\beta q^{2n})}q^nz^n$$

$$+\sum_{n=1}^{\infty}\frac{(1-\alpha)(q^2-\alpha)\cdots(q^{2n-2}-\alpha)}{(1-\beta q^2)(1-\beta q^4)\cdots(1-\beta q^{2n})}q^nz^{-n}$$

Now, let $\alpha,\beta\to0$, we get

$$\prod_{n=1}^{\infty}\left(1+zq^{2n-1}\right)\left(1+z^{-1}q^{2n-1}\right)\left(1-q^{2n}\right)=\sum_{-\infty}^{\infty}q^{n^2}z^n$$

This is called the Jacobi triple product identity.

1.4.2 Second proof from Euler

Define $(a;q)_0=1,(a;q)_n=(1-a)(1-aq)\cdots(1-aq^{n-1})$, for $|q|<1$, $(a;q)_\infty=\prod_{k=0}^{\infty}\left(1-aq^k\right)$

Define $0!_q=1,n!_q=1\cdot(1+q)\cdot\cdots\cdot(1+q+q^2+\cdots+q^{n-1})$

Remark 3 For $q=1$, $n!_q=n!$

$n!_q=\frac{(q;q)_n}{(1-q)^n}$

Define $\begin{bmatrix}n\\j\end{bmatrix}_q=\frac{n!_q}{j!_q(n-j)!_q}=\frac{(q;q)_n}{(q;q)_j(q;q)_{n-j}}$

Here we denote $\begin{bmatrix} n \\ j \end{bmatrix}_q$ by Q_j^n

Theorem 3 *(Cauchy) n positive integer, z, q complex number*

$$(-z;q)_n = \sum_{j=0}^{n} Q_j^n q^{j(j-1)/2} z^j$$

Only need to notice that for $f(z) = (-z;q)_n$, $f(z) = \sum Q_j(q) z^j$, we have $(1+z) f(qz) = f(z)(1+q^n z)$, then we obtain the recurrence about Q_j.

The Jacobi Triple Product Identity is to say that

$$\sum_{j=-\infty}^{\infty} q^{j^2} z^j = \left(-zq;q^2\right)_\infty \left(-z^{-1}q;q^2\right)_\infty \left(q^2;q^2\right)_\infty$$

The ingredient of the proof is from Euler:

Lemma 4

$$(-z;q)_\infty = \sum_{j=0}^{\infty} \frac{q^{j(j-1)/2}}{(q;q)_j} z^j$$

Noticed that

$$(-z;q)_n = \sum_{j=0}^{n} Q_j^n q^{j(j-1)/2} z^j$$

You may notice that this holds immediately by letting $n \to \infty$, but there's an obstruction: In general, $\lim_i \sum_j v_{ij} \neq \sum_j \lim_i v_{ij}$. The following thm allows us to do so.

Theorem 5 *(Tannery) $\forall$ positive integer n, let $\sum_{j=0}^{P_n} V_j(n)$ be a finite sum, as $n \to \infty$, $P_n \to \infty$.*

If $\forall j$, $\lim V_j(n)$ exists, and there is a convergent series $\sum M_j$ of non-neg real num s.t. $\forall j \geqslant 0, n \geqslant 1$, $|V_j(n)| \leqslant M_j$

Then, $\lim \sum V_j(n) = \sum \lim V_j(n)$

Lemma 6

$$\sum_{j=0}^{\infty} \frac{z^j}{(q;q)_j} = \frac{1}{(z;q)_\infty}$$

Denote the RHS by $A(z)$, $B(z) = \sum_j \frac{(-1)^j q^{j(j-1)/2}}{(q;q)_j} z^j = (z;q)_\infty$

Then, we only need to verify $A\left(z\right)B\left(z\right)=\sum_{n=0}^{\infty}\left(\sum_{j=0}^{n}\frac{(-1)^{j}q^{j(j-1)/2}}{(q;q)_{n-j}(q;q)_{j}}\right)z^{n}=1$. This is not very difficult.

Now, consider $\left(-zq;q^{2}\right)_{\infty}=\sum_{n=0}^{\infty}\frac{q^{l^{2}}}{\left(q^{2};q^{2}\right)_{l}}z^{l}$

Noticed that $\frac{1}{\left(q^{2};q^{2}\right)_{l}}=\frac{\left(q^{2l+2};q^{2}\right)_{\infty}}{\left(q^{2};q^{2}\right)_{\infty}}$

We have $\left(-zq;q^{2}\right)_{\infty}\left(q^{2};q^{2}\right)_{\infty}=\sum_{n=0}^{\infty}\left(q^{2l+2};q^{2}\right)_{\infty}q^{l^{2}}z^{l}$

Then, $\left(q^{2l+2};q^{2}\right)_{\infty}=\sum_{v=0}^{\infty}\left(-1\right)^{v}\frac{q^{v^{2}+v+2vl}}{\left(q^{2};q^{2}\right)_{v}}$

Then,

$$\begin{aligned}\left(-zq;q^{2}\right)_{\infty}\left(q^{2};q^{2}\right)_{\infty}&=\sum_{n=0}^{\infty}\sum_{v=0}^{\infty}\left(-1\right)^{v}\frac{q^{v^{2}+v+2vl}}{\left(q^{2};q^{2}\right)_{v}}q^{l^{2}}z^{l}\\&=\sum_{k\geqslant 0}\sum_{v\geqslant 0}\frac{z^{k}q^{k^{2}}z^{-v}\left(-1\right)^{v}q^{v}}{\left(q^{2};q^{2}\right)_{v}}\\&=\frac{1}{\left(-z^{-1}q;q^{2}\right)_{\infty}}\sum_{n=0}^{\infty}q^{l^{2}}z^{l}\end{aligned}$$

1.4.3 The third proof: power of combination

Please be charitable about my costing lots of time in this simple identity, because this proof is much more elegant than the previous 2. [15]

Now, we look back to the identity of Jacobi

$$\prod_{n=1}^{\infty}\left(1-q^{2n}\right)\left(1+q^{2n-1}z\right)\left(1+q^{2n-1}z^{-1}\right)=\sum_{-\infty}^{\infty}q^{n^{2}}z^{n}$$

If we put $X=qz$ and $Y=qz^{-1}$, the identity becomes

$$\prod_{n=1}^{\infty}\left(1+X^{n}Y^{n-1}\right)\left(1+X^{n-1}Y^{n}\right)=\sum_{n=-\infty}^{\infty}X^{r(r+1)/2}Y^{r(r-1)/2}\prod_{n=1}^{\infty}\left(1-X^{n}Y^{n}\right)^{-1}$$

Here, the left hand side is the generating function of $\alpha\left(n,m\right)$ as the number of partitions of $\left(n,m\right)$ into different parts $\left(a,a-1\right),\left(b-1,b\right)$.

Again, we have $\prod_{n=1}^{\infty}\left(1-X^{n}Y^{n}\right)^{-1}=\sum_{n=0}^{\infty}p\left(n\right)X^{n}Y^{n}$, where $p\left(n\right)$ is the number of unrestricted partitions of n with $p\left(0\right)=1$.

Compare each sides of the Jacobi Triple Product Identity, we have the identity is equals to show that

$$\alpha\left(n,m\right)=p\left(n-\frac{1}{2}\left(n-m\right)\left(n-m+1\right)\right)$$

where $p\left(k\right)=0$ if $k<0$.

The equality is combinatorial, and the proof is following:

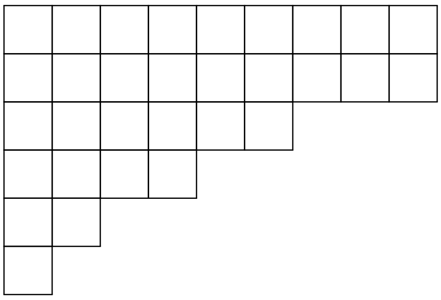
We may assume $n\geqslant m$, write $r=n-m$, write the partition of $\left(n,n-r\right)$ is equals to write n as

$$n=\sum_{l=1}^{v+r}a_l+\sum_{l=1}^{v}\left(b_l-1\right),1\leqslant a_1<a_2<\cdots,1\leqslant b_1<b_2<\cdots(*)$$

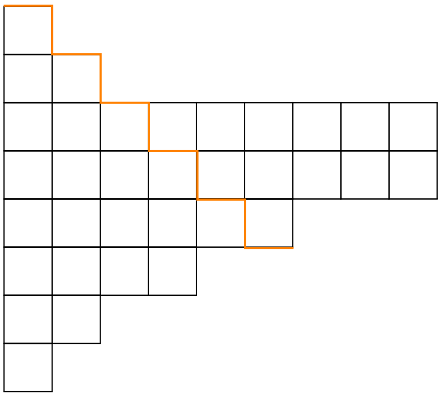
Let $k=n-\frac{r(r+1)}{2}$ so that the RHS of the equality we want is $p\left(k\right)$. If $k<0$ i.e. $n<\frac{1}{2}r\left(r+1\right)$, then $p\left(k\right)=0$ and there is no soln because we can easily verify that in $(*)$, $RHS>n$.

If $k=0$, samely we have $p\left(k\right)=0$ and there is just one soln of $(*)$.

We may assume $k>0$, for any unrestricted partition of k, we may represent it into the form of Young diagram, for example:



For the r, add an $r-$triangle on the upside of the left-left corner and draw a $\frac{\pi}{2}-$fold line, like this:



There are n blocks totally, with $r+v$ columns totally under the fold line, we may let them be $a_{v+r},a_{v+r-1},\cdots,a_1$. Similarly, there are v rows at the right side of the fold line (with mostly 1 row being 0), we may let them be $b_v-1,\cdots,b_1-1$.

Since we can check that the process can be carried reversely, we have proven that $\alpha(n,m) = p(k)$.

This proof is wrote by E.M.Wright in 1965. Obviously, it is easier and more elegant than any analytical proof.

1.5 Application

For $z = 1$, we have $\sum q^{j^2} = (-q;q^2)_\infty^2 (q^2;q^2)_\infty$

For $z = q$, we have $\sum q^{j^2+j} = (-q^2;q^2)(q^2;q^2)(-1;q^2)$

And $(q;q) = (q;q^3)(q^2;q^3)(q^3;q^3) = \sum (-1)^j q^{j(3j-1)/2}$

Now, we can define the Jacobi theta function:

$$\Theta_2(q) = \sum_{j\in\mathbb{Z}} q^{\left(j+\frac{1}{2}\right)^2}$$

$$\Theta_3(q) = \sum_{j\in\mathbb{Z}} q^{j^2}$$

$$\Theta_4(q) = \sum_{j\in\mathbb{Z}} (-1)^j q^{j^2}$$

They have the following properties:

1. $\Theta_3^2(q) + \Theta_4^2(q) = 2\Theta_3^2(q^2)$

One can calculate this directly

2. $\Theta_4^2(q^2) = \Theta_3(q)\Theta_4(q)$

Noticed that $\Theta_3(q) + \Theta_4(q) = 2\Theta_3(q^4)$, take square of the both sides and use 1.

Remark 4 This is equvalent to the Jacobi Triple Product Identity.

3. $\Theta_3^4(q) = \Theta_2^4(q) + \Theta_4^4(q)$

To show this, we only need to show

$\sum_{m,n\in\mathbb{Z};m\equiv n[2]} q^{m^2+n^2} = \sum_{m,n\in\mathbb{Z};m\equiv n\equiv 1[2]} q^{m^2+n^2} + \sum_{m,n\in\mathbb{Z};m\equiv n\equiv 0[2]} q^{m^2+n^2}$

Which is trivial.

4. Quintuple product identity

$$\left(q^2;q^2\right)_\infty \left(tq^2;q^2\right)_\infty \left(t^{-1};q^2\right)_\infty \left(t^2q^2;q^4\right)_\infty \left(t^{-2}q^2;q^4\right)_\infty = \sum_{j\in\mathbb{Z}} q^{3j^2+j}\left(t^{3j} - t^{-3j-1}\right)$$

1.5.1 Some special value

Denote the theta function $\Theta(q) = \sum_{n=-\infty}^{\infty} q^{n^2}$

Here are some special value of the theta function: [16]

$$\Theta\left(e^{-\pi}\right)=\frac{\sqrt[4]{\pi}}{\Gamma\left(\frac{3}{4}\right)}$$

$$\Theta\left(e^{-2\pi}\right)=\frac{\sqrt[4]{\pi}}{\Gamma\left(\frac{3}{4}\right)}\frac{\sqrt{2+\sqrt{2}}}{2}$$

$$\Theta\left(e^{-3\pi}\right)=\frac{\sqrt[4]{\pi}}{\Gamma\left(\frac{3}{4}\right)}\frac{\sqrt{1+\sqrt{3}}}{\sqrt[8]{108}}$$

$$\Theta\left(e^{-4\pi}\right)=\frac{\sqrt[4]{\pi}}{\Gamma\left(\frac{2+\sqrt[4]{8}}{4}\right)}$$

$$\Theta\left(e^{-\sqrt{3}\pi}\right)=\pi^{-1}\Gamma\left(\frac{4}{3}\right)^{\frac{3}{2}}2^{-2/3}3^{13/8}$$

$$\Theta\left(e^{-2\sqrt{3}\pi}\right)=\pi^{-1}\Gamma\left(\frac{4}{3}\right)^{\frac{3}{2}}2^{-2/3}3^{13/8}\cos\left(\frac{1}{24}\pi\right)$$

$$\Theta\left(e^{-\sqrt{2}\pi}\right)=\pi^{-1/2}\Gamma\left(\frac{9}{8}\right)\Gamma\left(\frac{5}{4}\right)^{-1/2}2^{7/8}$$

$$\Theta\left(e^{-2\sqrt{2}\pi}\right)=\pi^{-1/2}\Gamma\left(\frac{9}{8}\right)\Gamma\left(\frac{5}{4}\right)^{-1/2}2^{1/8}\left(1+\sqrt{\sqrt{2}-1}\right)$$

2 Elliptic curve

2.1 Lemniscate

Definition 2 A lemniscate is the locus of a point η in a plane satisfying the product of its distance from two fixed points has constant value c^2

Denote the two points $(a,0),(-a,0)$, one can easily identify the equation of the curve to be $x^2+y^2+a^2=\sqrt{c^4+4a^2x^2}$

One may assume it to pass through the origin, and $2a^2=1$, then we obtain the equation

$$r^4+r^2=2x^2$$

Then, this lemniscate can be described by

$$\begin{cases} 2x^2 = r^2 + r^4 \\ 2y^2 = r^2 - r^4 \end{cases}$$

We want to compute the length of an arc restricted in the first quadrant i.e. $r \in [0,1]$, by direct compute

$$\begin{cases} \dot{x}^2 = \frac{4r^4+4r^2+1}{2(r^2+1)} \\ \dot{y}^2 = \frac{4r^4-4r^2+1}{2(-r^2+1)} \end{cases}$$

Then, $\dot{x}^2 + \dot{y}^2 = \frac{1}{1-r^4}$, $\frac{ds}{dr} = \frac{1}{\sqrt{1-r^4}}$

Hence $s = s\left(t\right) = \int_0^t \frac{dr}{\sqrt{1-r^4}}$

By letting $r^2 = \frac{2t^2}{1+t^4}$, we have $\int_0^R \frac{dr}{\sqrt{1-r^4}} = \sqrt{2}\int_0^T \frac{dt}{\sqrt{1+t^4}}$.

Then, by letting $t^2 = \frac{2u^2}{1-u^4}$, we get $\int_0^T \frac{dt}{\sqrt{1+t^4}} = \sqrt{2}\int_0^U \frac{du}{\sqrt{1-u^4}}$

That is, we get $s\left(r\right) = 2s\left(u\right)$, where $r^2 = \frac{4u^2\left(1-u^4\right)}{\left(1+u^4\right)^2}$, this is obtained by Fagnano in 1718.

Please notice that this also hold for an easier function: for $\arcsin R = \int_0^R \frac{dr}{\sqrt{1-r^2}}$, there are $\sin 2x = 2\sin x\cos x$, that is, for $R = 2U\sqrt{1-U^2}$, $\int_0^R \frac{dr}{\sqrt{1-r^2}} = 2\int_0^U \frac{du}{\sqrt{1-u^2}}$.

However, for $\sin x$, there is a well-known result that generalizes the upper one: $\sin\left(x+y\right) = \sin x\cos y + \cos x\sin y$, that is, for $r = u\sqrt{1-v^2} + \sqrt{1-u^2}v$,

$$\int_0^u \frac{du}{\sqrt{1-u^2}} + \int_0^v \frac{dv}{\sqrt{1-v^2}} = \int_0^r \frac{dr}{\sqrt{1-r^2}}$$

Then, there may be an addition theorem like this for the lemniscate integral. In fact, there is: for $r = \frac{u\sqrt{1-v^4}+v\sqrt{1-u^4}}{1+u^2v^2}$

$$\int_0^u \frac{du}{\sqrt{1-u^4}} + \int_0^v \frac{dv}{\sqrt{1-v^4}} = \int_0^r \frac{dr}{\sqrt{1-r^4}}$$

To prove this, we only need to let r be const, and proof that $\frac{du}{\sqrt{1-u^4}} + \frac{dv}{\sqrt{1-v^4}} = 0$. The proof is complex but not difficult, so omitted.

Furthermore, the following are generalized by Euler.

1. If we set $1 + au^2 - u^4 = P\left(u\right)$ instead of $1 - u^4$, where a arbitary const, then $r = \frac{u\sqrt{P(v)}+v\sqrt{P(u)}}{1+u^2v^2}$ still holds the addition theorem.

2. Now, how about the case that $P\left(u\right)$ is an arbitary polynomial of deg 4? Roughly, we can set $u = \frac{\alpha w+\beta}{\gamma w+\delta}, \alpha\delta - \beta\gamma \neq 0$, we may want to find proper $\alpha, \beta, \gamma, \delta$ s.t. for $H\left(w\right) = \left(\gamma w + \delta\right)^4 P\left(u\right)$ is of the form $1 + aw^2 - w^4$. Then, since $du = \frac{\alpha\delta-\beta\gamma}{\left(\gamma w+\delta\right)^2}dw$,

$C\frac{du}{\sqrt{P(u)}} = \frac{dw}{\sqrt{H(w)}}$, where C constant.

Now, for $R(x,y)$ rational function of two variables, $I(x) = \int_a^x R\left(x, \sqrt{P(x)}\right) dx$ is called the elliptic integral, with $\deg P(x) = 3, 4$

2.2 elliptic function

In fact, for the existence of two branches of $\sqrt{P(x)}$, to make the elliptic integral 'make sence', we must talk about the meromorphic function on the Riemann surface $R \simeq T^2$, but the definition, properties and history are omitted due to the limitation of space. More about this is in [10].

Now, we may consider $\left(\frac{dz}{dw}\right)^2 = P(z) = (z-a)(z-b)(z-c)(z-d)$, for A a loop based at ζ_0 on R, define $w(A) = \int_A Q(\zeta)\,d\zeta$, $Q(z) = \frac{1}{\sqrt{P(z)}}$.

Theorem 7 *If C_1, C_2 two curves on R, ζ_0, then $w(C_1) = W(C_2) \iff C_1, C_2$ are homotopic.*

'If' side is trivial, the 'only if' side is because the $w-$plane is simply-connected, w is local homeomorphism.

Then, we may assume A a loop that $[A] \neq 0$, $w(A)$ is a period of the inverse function. Then, the set of nonzero period is nonempty. choose w_1 a period of minimal absolute value. Trivially if w' is another period, with $\frac{w'}{w}$ real, then $w' = mw$ with $m \in \mathbb{Z}$.

Are there another period? Consider $v = e^{(2\pi i/w_1)w}$, suppose they are all period, then v is a single-valued function on R. Since R is compact, there exists a maximal value of $|v|$, hence v is constant, contradict!

Hence f is doubly periodic. Since the periods are discrete, all the periods forms a lattice in $\mathbb{C}$.

2.3 Weierstrass p-function

Now, I'll introduce the Weierstrass p-function. It is also known as $\wp-$function, for the convinence, we use the donation of $p-$function. They play an important role in the theory of elliptic functions. A $\wp$-function together with its derivative can be used to parameterize elliptic curves and they generate the field of elliptic functions with respect to a given period lattice. [14]

$\wp$, the fancy uniquely fancy script p was used already at least in 1890. The first edition of the book A Course of Modern Analysis by E.T. Whittaker in 1902 also used it.

Here, for the $z = f(s) = \frac{\alpha s+\beta}{\gamma s+\delta}$, $w(C) = \int_C Q(z)\,dz, Q(z) = \frac{1}{\sqrt{P(z)}}$, where $P(z) = (z-a)(z-b)(z-c)(z-d)$

By the study of Lorentz transformation, we can reduce it to the Weierstrass normal form $f(\infty) = a$, then $P(z) = F(s)$, where $F(s) = a_0s^3 + a_1s^2 + a_2s + a_3, a_0 \neq 0$. Then, by letting $s_1 = \frac{4}{a_0}s - \frac{a_1}{3a_0}$, we can finally reduce to the form

$$w = \int_\infty^s \frac{d\sigma}{\sqrt{4\sigma^3 - g_2\sigma - g_3}}$$

Note that $4\sigma^3 - g_2\sigma - g_3$ should have three distince roots, $g_2^2 - 27g^3 \neq 0$.

Now, we may consider the inverse function of the function $w = f(s)$ to be $s = p(w)$.

p has the following properties:

1. p is doubly periodic

2. p has exactly one pole $w = 0$. That is, if $s = \infty$, $z = a$, $w = 0$.

And consider the Laurent decomposition $p(w) = \frac{c_{-n}}{w^n} + \cdots + c_0 + \cdots$

Since $\left(\frac{dw}{ds}\right)^2 = \frac{1}{4s^3-g_2s-g_3}$, $\left(\frac{dp}{dw}\right)^2 = 4p^3 - g_2p - g_3$, then consider the lowest term of the both sides, we have $n = 2, c_{-2} = 1$

3. p is even, because locally, we can take the positive branch or the negative branch, these two ways gives two integral with sum 0. Then, $p(w) = w^{-2} + b_0 + b_1w^2 + b_2w^4 + \cdots$.

Once again, we can use $\left(\frac{dp}{dw}\right)^2 = 4p^3 - g_2p - g_3$ to compare the coefficients, then we get $\begin{cases} b_0 = 0 \\ b_1 = \frac{g_2}{20} \\ b_2 = \frac{g_3}{28} \end{cases}$

Then, the question is left: how to calculate the rest coefficients?

Take the differential of $\left(\frac{dp}{dw}\right)^2 = 4p^3 - g_2p - g_3$, we get $2p'p'' = 12p^2p' - g_2p'$, then $p'' = 6p^2 - \frac{g_2}{2}$, then we get the recurrence:

$$2n(2n-1)b_n = 6(2b_n + b_1b_{n-2} + b_{n-2}b_1)$$

Theorem 8 *$p(w) = w^{-2} + \sum_{\omega\neq 0}\left((w-\omega)^{-2} - \omega^{-2}\right)$, ω a lattice.*

we have p is doubly periodic, hence $\frac{1}{2}p'$ is meromorphic. Notice that $g = \sum_{\omega} (w-\omega)^{-3}$ is meromorphic, then we can proof that $\frac{1}{2}p' + g$ is entire and periodic, hence const, hence $LHS - RHS$ is const.

The inverse problem is also interesting: given two complex number w_1, w_2, with w_2/w_1 not real, could they be basic periods of the elliptic integral of the form $w = \int_{\infty}^{s} \frac{d\sigma}{4\sigma - g_2\sigma - g_3}, g_2^3 - 27g_3^2 \neq 0$.

Theorem 9 *Let w_1 and w_2 be given number s.t. w_1/w_2 not real, put $p(w) = w^{-2} + \sum_{\omega \neq 0} (w-\omega)^{-2} - w^{-2}$*

Then $p(w)$ is a doubly periodic meromorphic function which has precisely the ω as period.

If we then put $g_2 = 60 \sum_{\omega \neq 0} \omega^{-4}, g_3 = 140 \sum_{\omega \neq 0} \omega^{-6}$, then $g_2^3 - 27g_3^2 \neq 0$, and p is the inverse function of $w = \int_{\infty}^{z} \frac{d\sigma}{\sqrt{4\sigma^3 - g_2\sigma - g_3}}$. The key is to proof $\left(\frac{dp}{dw}\right)^2 = 4p^3 - g_2 p - g_3$.

2.4 Elliptic function

Definition 3 A meromorphic doubly periodic function is called an elliptic function

We denote $\{\alpha_1 w_1 + \alpha_2 w_2 | 0 \leqslant \alpha_1, \alpha_2 \leqslant 1\}$ the fundamental parallelogram.

Since all the finite singular points are isolated, the fundamental parallelogram contains only finitely many singular points. With a parallel transport, we may assume there is no singular points on its sides.

1. The sum of the residue of the elliptic function at ssingular points inside P equals to 0

Only need to integral over ∂P.

2. For a_i those zeros and poles lie in P, r_i the order of a_i, then $\sum r_i = 0$, $\sum a_i r_i \equiv 0, mod \wedge$.

Integrate $\frac{f'}{f}$ and $\frac{zf'}{f}$ over ∂P

Corollary 10 *A nonconstant elliptic function cannot have exactly one pole of order 1 in the fundamental parallelogram.*

For an elliptic function, its order is defined to be the number of poles in the fundamental parallelogram.

If it has one pole of order 2, then it is the Weiertrass function. And if it has two simple poles, then it belongs to the Jacobi ellipic function.

REMARK 5 For P has double poles, then the sum of poles of P is congruent to 0, *mod* $\wedge$

Then, suppose 0 be a pole of degree 2, then, for all c, $p-c$ still has the same poles as p, since $\sum r_i = 0$, there is exactly two points u and v s.t. $p(u) = p(v) = c, u+v = 0$.

Specially, for $u \equiv -u[\wedge]$, that is, $u = 0(\text{pole})$, $u = w_1/2$, $u = w_2/2$, $u = (w_1+w_2)/2$. The last three are the zero of degree 2 of $p - p(u)$, hence are the zero of p'. Hence we get, in the parallelogram

$$p'(z) = 0 \iff z = \frac{1}{2}w_1, \frac{1}{2}(w_1+w_2), \frac{1}{2}w_2$$

Theorem 11 *Let $f(z)$ be an arbitrary elliptic function with same periods of $p(z)$, then there exists rational function R_1, R s.t.*

$$f(z) = R(p) + R_1(p)p'$$

We have p' is odd, write $f = g+h$, g odd, h even, then g/h even, there is left to prove that even elliptic function could be written as a rational function of p.

For u zero of f, the order of $u \geqslant 2$. If $u \equiv \frac{1}{2}w_1, \frac{1}{2}(w_1+w_2), \frac{1}{2}w_2$, consider $F(z) = p(z) - p(u)$ has a zero of order 2 at u

If $u \equiv 0[\wedge]$, consider $F(z) = \frac{1}{p(z)}$ has a zero of order 2 at u.

By continously dividing $F(z)$, we finallly divide all the zeros or poles into the form $(x_1 - x)$. Then, choose a representation from each pair

$$\begin{cases} a_1 \cdots a_k & zeros \\ b_1 \cdots b_k & poles \end{cases}$$

Then, for $Q(z) = \frac{\prod(p(z)-p(a_i))}{\prod(p(z)-p(b_i))}$

Then, f/Q is doubly periodic without poles, hence const. $f(z) = cQ$.

Denote $e_1 = \frac{1}{2}w_1, e_2 = \frac{1}{2}w_2, e_3 = \frac{1}{2}(w_1+w_2)$. We have

$$p'^2 = C(p-e_1)(p-e_2)(p-e_3)$$

From $p(w) = w^{-2} + \sum_{\omega\neq 0}(w-\omega)^{-2} - w^{-2}$ and $\frac{1}{(1-z/l)^2} = 1 + 2\frac{z}{l} + 3\frac{z^2}{l^2} + \cdots$, we obtain

$$p(z) = \frac{1}{z^2} + 3G_4z^2 + 5G_6z^4 + 7G_8z^6 + \cdots$$

with $G_i = \sum_{l\in L} l^{-k}$. And $g_2 = 60G_4, g_3 = 140G_6$.

3 Elliptic curve-Start from an old question in Number Theory

3.1 Talking from Weierstrass p-function

Consider the homogeneous coordinates, consider

$$f : \mathbb{C}/\wedge \to \mathbb{C}P^2$$

$$z \mapsto \left(z^3 p\left(z\right), z^3 p'\left(z\right), z^3\right)$$

Remark 6 f is one-to-one of the torus $\mathbb{C}/\wedge$ to the cubic curve

$$y^2 z = 4x^3 - g_2 xz - g_3 z^3$$

Now, we can define the addition law of points in the cubic curve:

Recall that in 2.1, we have proven that

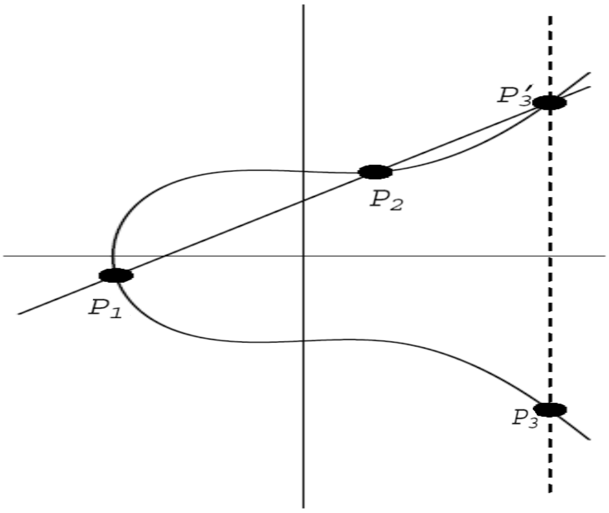
$$p\left(a+b\right) = \frac{1}{4}\left(\frac{p'\left(a\right) - p'\left(b\right)}{p\left(a\right) - p\left(b\right)}\right)^2 - p\left(a\right) - p\left(b\right)$$

This is called the addition law of Weierstrass p-function. It induces a addition structure on the torus $\mathbb{C}/\wedge$: for z, the point of $f\left(z+\wedge\right)$ is denoted as P_z, then $P_{z_1} + P_{z_2} = P_{z_1+z_2}$

How to understand the addition law of points in the cubic curve?

Consider $f\left(z\right) = p'\left(z\right) - ap\left(z\right) - b$, f is a elliptic function with a unique pole of degree 3 at 0. Hence for z_1, z_2, z_3 zeros, we have $z_1 + z_2 + z_3 = 0[\wedge]$.

Hence, $p\left(z_3\right) = p\left(z_1+z_2\right), p'\left(z_3\right) = -p'\left(z_1+z_2\right)$. P_{z_3} is the reflection point of P'_{z_3}, which lies in the same line of P_{z_1} and P_{z_2}



For $(ax+b)^2 = 4x^3 - g_2x - g_3$, there are $4x^3 - a^2x^2 - * = 0$, hence $p(z_1) + p(z_2) + p(z_1 + z_2) = \frac{a^2}{4}$, where $a = \frac{p'(z_1) - p'(z_2)}{p(z_1) - p(z_2)}$.

3.2 "Digression" to the Number theory

There is a small question: given n, can one find a rational number x s.t. both $x^2 + n$ and $x^2 - n$ are squares of rational numbers? [7]

Those numbers are called congruent number. Euler showed that $n = 7$ is congruent, and Fermat showed that $n = 1$ is not: this is equvalent to Fermat's Last Theorem for the exponent 4, that is, $x^4 + y^4 = z^4$ has no nontrivial integer solutions.

Nowadays, We know that the smallest 10 congruent numbers are

$$5, 6, 7, 13, 14, 15, 20, 21, 22, 23$$

By simple Number Theory technique, we can show that n is congruent equals to that there exists a right triangle with the length of the three sides are rational has the area n. For example, for $n = 5$, we can consider the triangle with length $\frac{3}{2}, \frac{20}{3}, \frac{41}{6}$, and for $n = 157$, by the result of D.Zagier, it is congruent because of the triangle with length

$$\frac{411340519227716149383203}{21666555693714761309610}, \frac{6803298487826435051217540}{411340519227716149383203},$$
$$\frac{224403517704336969924557513090674863160948472041}{8912332268928859588025535178967163570016480830}$$

.

Fermat stated that the area of right triangle with length 2896804, 7216803, 7776485 is of the form $6u^2$, like the triangle with sides $3, 4, 5$. And E.Lucas noted that the area of a right triangle is never a square, nor the double, triple or quintuple of a square. [3]

It looked hopeless to find a criterion to tell whether a given n is congruent. However, J.B.Tunnell show that the following theorem.

Theorem 12 *(Tunnell) Let n be an odd squarefree natural number. Consider the two conditions:*

(A) n is congruent;

(B) the number of triples of integers (x, y, z) satisfying $2x^2 + y^2 + 8z^2 = n$ is equals to twice the number of triples satisfying $2x^2 + y^2 + 32z^2 = n$.

Then(A) implies (B), and, if a weak form of the so-called Birch-Swinnerton-Dyer conjecture is true, then (B) also implies (A).

The proof of the whole Tunnell's theorem takes many pages. Fortunately, we exactly have the large volume!

First of all, we may generalize the definition of the "congruent number" to the rational numbers. Consider the multiplicative group $\mathbb{Q}^*$, each coset in $\mathbb{Q}^*/\left(\mathbb{Q}^*\right)^2$ contains a unique squarefree natural number. Now, when talking about congruent number, we always talk about squarefree number.

For $\left(\frac{X\pm Y}{2}\right)^2 = \left(\frac{Z}{2}\right)^2 \pm n$ whenever X, Y, Z are sides of a triangle with area n. If we multiply together these, we obtain $\left(\frac{X^2-Y^2}{4}\right)^2 = \left(\frac{Z}{2}\right)^4 - n^2$. That is, $u^4 - n^2 = v^2$ has a rational solution $u = Z/2, v = \left(X^2 - Y^2\right)/4$. If we set $x = (Z/2)^2$ and $y = \left(X^2 - Y^2\right)Z/8$, then we have a pair of rational number (x, y) satisfying the cubic equation

$$y^2 = x^3 - n^2 x$$

Then, we obtain a point (x, y) with rational coordinates lying on $y^2 = x^3 - n^2 x$. By assuming they correspond to a primitive Pythagorean triple, (x, y) has the following properties:

1. $x = (Z/2)^2$ has denominator divisible by 2.

2. the power of 2 dividing Z is equals to the power of 2 dividing the denominator of one of the two sides, while a strictly lower power of 2 divides the denominator of the third side.

For example, when $n = 31$, the point $(41^2/7^2, 29520/7^3)$ on the curve $y^2 = x^3 - n^2 x$ doesn't come from a triangle.

Proposition 13 *For (x, y) a point with rational coordinates on the curve $y^2 = x^3 - n^2x$. Suppose x satisfies:*

(1) x is the square of a rational number

(2) the denominator of x is even.

(3) the numerator has no common factor with n

Then there exists a right triangle with rational sides and area n which corresponds to x under the correspondence $x \mapsto X = \sqrt{x+n} - \sqrt{x-n}, Y = \sqrt{x+n} + \sqrt{x-n}, Z = 2\sqrt{x}$.

3.3 Elliptic curves

For K field that does not has characteristic 2, f cubic polynomial that has distinct root. Then the solution of

$$y^2 = f(x)$$

where x, y are in some extension K' of K are called the $K'-$points of the elliptic curve defined by $y^2 = f(x)$.

Note that $y^2 = x^3 - n^2x$ satisfies the condition if the characteristic p does not divides $2n$.

In general, if $x_0, y_0 \in K'$ are the coordinates of a point on a curve C defined by $F(x, y) = 0$, we say that C is "smooth" at (x_0, y_0) if $\partial F/\partial x$, $\partial F/\partial y$ are both not zero. This make sence regardless of the ground field for the partial derivative of polynomials is defined by usual formula.

By this way, we obtain the new definition of Elliptic curves. From now on, we have got out of the fields of analysis and comes to algebra.

Now, given L the lattice of $\mathbb{C}$, denote E_L the elliptic function w.r.t. L, then as is proved in Theorem 9, $E_L = \mathbb{C}(p, p')$.

We have already defined the addition group structure of points in $\mathbb{C}P^2$ on the elliptic curve $y^2 = f(x)$. We have (x, y) has finite order iff $Nz \in L$, that is, z is a rational combination of ω_1, ω_2.

Under the isomorphism from $\mathbb{R}/\mathbb{Z} \times \mathbb{R}/\mathbb{Z}$ to the elliptic curve given by $(a, b) \mapsto P_{a\omega_1 + b\omega_2}$, it is the image of $\mathbb{Q}/\mathbb{Z} \times \mathbb{Q}/\mathbb{Z}$ which is the torsion subgroup of the elliptic curve.

Now, for N a fixed integer, f a cubic polynomial with coeff. in K with distinct roots. For $N > 2$, we say P is a nontrivial point of order N is to say $P \neq 0, NP = 0$

for N odd, and $2P \neq 0, NP = 0$.

Proposition 14 *Let K' be any field extension of K (not necessarily algebraic), and let $\sigma : K \to \sigma K$ be any field isomorphism which leaves fixed all elements of K. Let $P \in \mathbb{C}P^2_K$ be a point of exact order N on the elliptic curve $y^2 = f(x)$, where $f(x) \in K[x]$. Then σP has exact order N.*

Trivial.

Proposition 15 *Let $K_N \subset \mathbb{C}$ the field obtained by adjoining to K the x and y coordinates of all points of order N. Let K_N^+ denote the field obtained by adjoining just their x coordinates. Then both K_N and K_N^+ are finite Galois extensions of K*

Noticing that $\sigma(P)$ is also of order N finish the proof.

As an example, $K_2 = K_2^+$ is the splitting field of $f(x)$ over K.

We have $Gal(K_N/K)$ is isomorphic to a subgroup of $GL_2(\mathbb{Z}/N\mathbb{Z})$.

You may compare this to the dim 1 case, for $\mathbb{Q}_N = \mathbb{Q}(\zeta_N)$, we have $Gal(\mathbb{Q}_N/\mathbb{Q}) \simeq (\mathbb{Z}/N\mathbb{Z})^* = GL_1(\mathbb{Z}/N\mathbb{Z})$.

Now, for $K \subset \mathbb{C}$, $K = \mathbb{Q}(g_2, g_3)$, where $y^2 = f(x) = 4x^2 - g_2x - g_3$, we shall use the $p-$function to determine the polynomial whose roots are the $x-$coordinates of the points of order N i.e. K_N^+ will be the splitting field of such a polynomial.

we first construct $f_N(z)$ whose zeros are precisely the nonzero values of z s.t. P_z is a point of order N. For N odd, define

$$f_N(z) = N \prod (p(z) - p(u))$$

where u taken from each pair $u, -u$ s.t. $Nu \in L$. For $f_N(z) = F_N(p(z))$, F_N is a polynomial of degree $(N^2-1)/2$. Then f_N has N^2-1 simple zeros and a single pole at 0 of order N^2-1 with leading term N/z^{N^2-1}.

For N even, we may let the upper u range over nontrivial u s.t. $Nu \in L$. For $\tilde{f}_N(z)$ the product, $\tilde{f}_N(z) = F_N(p(z))$. F_N a polynomial of degree $(N^2-4)/2$, $\tilde{f}_N$ has has N^2-4 simple zeros and a single pole at 0 of order N^2-4 with leading term N/z^{N^2-4}.

Then, in this case, we may define $f_N = -\frac{1}{2}p'\tilde{f}_N$

In each case, we can check that

$$f_N(z)^2 = N^2 \prod_{0 \neq u \in \mathbb{C}/L, Nu \in L} (p(z) - p(u))$$

We see $(x, y) = (p(z), p'(z))$ has odd order N iff $F_N(x) = 0$, and has even order

N iff $F_N(x) = 0$ or $y = 0$.

We know that all automorphism of $\mathbb{C}$ fixing $K = \mathbb{Q}(g_2, g_3)$ permutes roots of F_N. Hence the coeff. of F_N are in K.

Remark 7 If we do not start form the Weierstrass form, with $y^2 = f(x)$ an elliptic curve over any field K of characteristic not equals to 2, we could also show by some discussion that there are at most N^2 points or order N over any extension K' of K.

Now, let's pay attention to the finite field: For $\mathbb{F}_q$, there are only $q^2 + q + 1$ points in $\mathbb{F}_q P^2 := \mathbb{P}^2_{\mathbb{F}_q}$, there are only finitely many $\mathbb{F}_q-$points on an elliptic curve $y^2 = f(x)$, where $f(x) \in \mathbb{F}_q[x]$. So the group of $\mathbb{F}_q-$points is a finite abelian group.

We all know about the structure of abelian group, that it can be decomposed into cyclic group with order p^{α_p}. Then by Remark 6, we have each prime p there are at most two $p-$power components.

Proposition 16 *Let $q = p^f$, $p \nmid 2n$. Suppose that $q \equiv 3[4]$, then there are $q + 1$ $\mathbb{F}_q-$points on the elliptic curve $y^2 = x^3 - n^2 x$.*

There are 4 points of order 2: infinity, $(0,0)$, $(\pm n, 0)$. Devide those $q - 3$ x in pairs $(x, -x)$, by simple discussion of number theory, we get there is only one x s.t. $\sqrt{f(x)}$ make sence in $\mathbb{F}_q$.

As an example, for $q = 7^3$, there are $344 = 2^3 \times 43$ points. Since there are four points of order 2, the type of the group of $\mathbb{F}_343$-points on $y^2 = x^3 - n^2 x$ must be $(2, 2^2, 43)$.

Another example is $q = p = 107$, we have $108 = 2^2 \times 3^3$. So the type is either $(2, 2, 3, 9)$ or $(2, 2, 27)$. To determine those case, we must determine the number of order 3 points.

We have the equation of points of order 3 is $-3x^4 + 6n^2x^2 + n^4 = 0$. That is, $\pm n\sqrt{1 \pm 2\sqrt{3}/3}$. However, if (x, y) is in $\mathbb{F}_{107}$, then so is for $\left(-x, \sqrt{-1}y\right)$. However, $\sqrt{-1}$ is not in $\mathbb{F}_{107}$. So there are only 3 points of order 3, the type of this group is $(2, 2, 3^3)$.

For K is of characteristic 3, there is no nontrivial point of order 3 for $-3x^4 + 6n^2x^2 + n^4 = n^4 \neq 0$. In fact, the same is true for any $p \equiv 3[4]$.

Now, let's look back to the elliptic curve: Denote the elliptic curve $y^2 = x^3 - n^2 x$ over $\mathbb{Q}$ by E_n.

E_n defined over $\mathbb{F}_p$ is called the "reduction" modulo p, and the reduction is called "good" if $p \nmid 2n$. The point is we can use reduction to determine the torsion subgroup of $E_n(\mathbb{Q})$.

Mordell stated that the group $E(\mathbb{Q})$ is a finitely generated abelian group. This means that the torsion group is finite an $E(\mathbb{Q}) \simeq E(\mathbb{Q})_{tors} \oplus \mathbb{Z}^r$ with r nonnegative and finite. It is greater than 0 iff $E(\mathbb{Q})$ finite. By the way, as is proved by Andre Weil, this is also true while replacing $\mathbb{Q}$ by other number field. The story will be talked in next section. Now, we just admit it.

Proposition 17 $\#E_n(\mathbb{Q})_{tors} = 4$.

Proof: First of all, we may notice that $(0,0), (\pm n, 0)$ and the infinity is in $E_n(\mathbb{Q})_{tors}$.

The idea is to construct a homomorphism from $E_n(\mathbb{Q})_{tors}$ to $E_n(\mathbb{F}_p)$ which is injective for most p. That will imply that the order of $E_n(\mathbb{Q})_{tors}$ divides the order of $E_n(\mathbb{F}_p)$ for such p. But all number greater than 4 can divide all $\#E_n(\mathbb{F}_p)$ for it has $p+1$ element for $p \equiv 3[4]$.

Consider the map from $\mathbb{P}^2_{\mathbb{Q}}$ to $\mathbb{P}^2_{\mathbb{F}_p}$. We shall choose (x,y,z) s.t. (x,y,z) integer with no common factor. This is unique up to multiplication by ± 1.

It is easy to see that for $P = (x,y,z)$ in $E_n(\mathbb{Q})$, then $\bar{P}$ is in $E_n(\mathbb{F}_p)$. Moreover, the image of $P_1 + P_2$ is $\bar{P}_1 + \bar{P}_2$. Hence this is a homomorphism from $E_n(\mathbb{Q})_{tors}$ to $E_n(\mathbb{F}_p)$ when p does not dividing $2n$.

Now, we should determine when this map is not injective.

Lemma 18 *$\bar{P}_1 = \bar{P}_2$ iff p divides $x_1z_2 - x_2z_1$, $y_1z_2 - y_2z_1$, $x_1y_2 - y_1z_2$.*

This lemma is not hard.

Now, suppose $E_n(\mathbb{Q})$ contains a point of finite order greater than 2, then either it contains an element of odd number of the group of points of order 4 contains at least 8 elements. We then have a subgroup $S = \{P_1, \cdots P_m\}$ where $m = \#S$ is either 8 or an odd number.

For $P_i = (x_i, y_i, z_i)$, we have $N > 0$ s.t. $\forall p > N$ prime, for all the cross product $(y_iz_j - y_jz_i, \cdots)$, p does not divide them. That is, if the proposition does not hold, there are only finite many number of primes of the form $\begin{cases} 8k+3 & m = 8 \\ 4mk+3 & m\ odd, 3 \nmid m \\ 12k+7 & m\ odd, 3|m \end{cases}$

In each case, it is contradict to the Dirichlet Theorem. □

Now, we have the corollary

Corollary 19 *n is a congruent number if and only if $E_n(\mathbb{Q})$ has nonzero rank r.*

Proof: The "only if" side is trivial: we have then attains a nontrivial point on $E_n(\mathbb{Q})$. And it is not $(\pm n, 0), (0,0)$ and infinity, then it hold by Proposition 15.

Conversely, suppose that P is a point of infinite order, the x coordinate of $2P$ is a square of a rational number having even denominator. Then it hold by Proposition 11. □

Proposition 20 *Let E be the elliptic curve $y^2 = (x - e_1)(x - e_2)(x - e_3)$ with $e_i \in \mathbb{Q}$. Let $P = (x_0, y_0) \in E(\mathbb{Q}) - 0$, then $P \in 2E(\mathbb{Q}) - 0$ iff $x_0 - e_1, x_0 - e_2, x_0 - e_3$ are all squares of rational numbers.*

Proof: WLOG, we may assume $x_0 = 0$.

Then, if $2Q = P$, then there are exactly 4 points Q, Q_1, Q_2, Q_3 s.t. $2Q_i = P$, where Q_i is added by $(e_i, 0)$.

For $Q = (x, y)$ s.t. $2Q = P = (0, y_0)$. That is, the tangent line to the curve at Q pass through $-P = (0, -y_0)$.

We have (x, y) are rational iff the slope of the line from $-P$ to Q is rational. And then, $m \in \mathbb{C}$ the clope of a line from $-P$ is a tangent to E iff the following eqn has a double root:

$$(mx - y_0)^2 = (x - e_1)(x - e_2)(x - e_3) = x^3 + ax^2 + bx + c$$

with

$$a = -e_1 - e_2 - e_3, b = e_1e_2 + e_2e_3 + e_1e_3, c = -e_1e_2e_3 = y_0^2$$

Now, we simplify the condition, it becomes that

$$x^2 + \left(a - m^2\right)x + (b + 2my_0) = 0$$

has a double root. That is,

$$\left(a - m^2\right)^2 - 4(b + 2my_0) = 0$$

We need to find when one (and hence four) m are rational. Noticed that y_0 is the symmetric polynomial in the $\sqrt{e_i}$, let $f_i^2 = -e_i$, we have $y_0 = f_1f_2f_3$.

Now, let $s_1 = f_1 + f_2 + f_3$, $s_2 = f_1f_2 + f_2f_3 + f_1f_3$, then

$$a = s_1^2 - 2s_2, b = s_2^2 - 2s_1s_3, y_0 = s_3$$

Thus, the equation becomes

$$0 = \left(m^2 - s_1^2\right)^2 + 4s_2\left(m^2 - s_1^2\right) - 8s_3(m - s_1)$$

We have $m = s_1 = f_1 + f_2 + f_3$ is a root. Since the choice only need to $f_1 f_2 f_3 = y_0$ hold, all the solutions are:

$$m_1 = f_1 - f_2 - f_3, m_2 = -f_1 + f_2 - f_3, m_3 = -f_1 - f_2 + f_3, m_4 = f_1 + f_2 + f_3$$

We have m_i are rational, then f_1, f_2, f_3 are rational. □

REMARK 8 The proof of Proposition 18 also hold when replace $\mathbb{Q}$ by any field K that does not has characteristic 2.

4 Elliptic curve-The Hasse-Weil L-Function

At last subsection, we determine the torsion group of $E_n : y^2 = x^3 - n^2 x$. To determine the torsion-free part is hard. Here, we are going to introduce the technique of Hasse-Weil $L-$function.

One may know much about the Riemann $\zeta-$function,

and the Dirichlet $L-$function in the Algebraic Number Theory. (Please forgive me for breaking this sentence into two rows. LaTeX draw blue line when the two components get in 1 row and I don't know why, that make me ANGRY.)

In 1955, Hasse introduced the $\zeta-$function associated with a curve. Today, it is called the Hasse-Weil zeta function. For the Fermat curve $x^m + y^m = 1$ he obtained an expression for his $\zeta-$function in terms of $L-$function in terms of $L-$functions with a Hecke character.(See [8])

However, this is not the topic I'm going to talk about. To get near the Theorem of Tunnell, we still have a long way to go. So let's take a glimpse about the Hasse-Weil $\zeta-$function of the elliptic curve.

4.1 zeta-function

For a sequence N_r, we may define the $\zeta-$function By

$$Z(T) = \exp\left(\sum_{r=1}^{\infty} N_r \frac{T^r}{r}\right)$$

Now, let V be an affine or projective variety defined over $\mathbb{F}_q$, we let $V(K)$ denote the set of $K-$points of V. We may define that $N_r = \#V(\mathbb{F}_{q^r})$, then we define

$$Z(V/\mathbb{F}_q; T) = \exp\left(\sum_r \#V(\mathbb{F}_{q^r} T^r)/r\right)$$

The point is the cingruence zeta-function of any elliptic elliptic curve defined over $\mathbb{F}_q$ has the form

$$Z\left(E/\mathbb{F}_q;T\right)=\frac{1-2a_ET+qT^2}{\left(1-T\right)\left(1-qT\right)}$$

where only the integer $2a_E$ depends on E. We may soon prove this for $E_n: y^2 = x^3-n^2x$. Now, consider α one reciprocal root of the numerator, then $1-2a_ET+qT^2 = \left(1-\alpha T\right)\left(1-\frac{q}{\alpha}T\right)$. Take the logarithmic derivative, we get

$$N_r = q^r+1-\alpha^r-\left(q/\alpha\right)^r$$

Specially, $N_1 = q+1-2a_E$. Thus, if we determine N_1, then we can determine $Z\left(E/\mathbb{F}_q;T\right)$, thus N_r.

Also, there are $|\alpha| = \sqrt{q}$. In the case of $y^2 = x^3-n^2x$, α is a square root of $-q$ if $q\equiv 3[4]$, and is of the form $a+bi$ s.t. $a^2+b^2 = q$ for $q\equiv 1[4]$.

This result is a special case of a much more general fact concerning smoothe projective algebraic varieties over finite fields, which is conjectured by Andre Weil in [weil]. And the most difficult part was proved by Pierre Deligne in 1973. That is:

(i) $Z\left(V/\mathbb{F}_q;T\right)$ is a rational function of T which for a smooth curve has the form $P\left(T\right)/\left(1-T\right)\left(1-qT\right)$. Here the $P\left(T\right)$ has coefficients in $\mathbb{Z}$ and constant term 1.

(ii) If V was obtained by reducting modulo p a variety $\tilde{V}$ defined over $\mathbb{Q}$, then $\deg P = 2g$, g the genus of the complex analytic manifold $\tilde{V}$.

(iii) If α a reciprocal root for the numerator, then so is $\frac{q}{\alpha}$.

(iv) All α reciprocal roots have complex absolute value $\sqrt{q}$.

Now, we come back to the theorem

Theorem 21 *Let E_n be the elliptic curve $y^2 = x^3-n^2x$ defined over $\mathbb{F}_p$ with $p \not| 2n$, then*

$$Z\left(E_n/\mathbb{F}_p;T\right)=\frac{1-aT+pT^2}{\left(1-T\right)\left(1-pT\right)}=\frac{\left(1-\alpha T\right)\left(1-\bar{\alpha}T\right)}{\left(1-T\right)\left(1-pT\right)}$$

Where $a = Re\ \alpha$, $\alpha = i\sqrt{p}$ if $p\equiv 3[4]$, and if $p\equiv 1[4]$, then α is an element of $\mathbb{Z}[i]$ of norm p which is congruent to $\left(\frac{n}{p}\right)$ modulo $2+2i$.

We may firstly find that for E_n, consider $E_n' : u^2 = v^4+4n^2$. Let $p\nmid 2n$, we can easily find the correspondence: for $(x,y)\in E_n$ with $x\neq 0$, $(u,v) = (2x-y^2/x^2, y/x)\in E_n'$, and for $(u,v)\in E_n'$, $(x,y) = \left(\frac{1}{2}\left(u+v^2\right), \frac{1}{2}v\left(u+v^2\right)\right)\in E_n$. Hence above all, $N_1 = N'+2$. We only need to compute N'.

Now, let's consider the tools come from traditional number theory: Gauss sum and

Jacobi sum. For $\psi : \mathbb{F}_q \to \mathbb{C}^*$ nontrivial additive character defined by $\psi(x) = \zeta^{\mathrm{Tr}\, x}$, where $\zeta = e^{2\pi i/p}$, $Tr : \mathbb{F}_q \to \mathbb{F}_p$ nontrivial, $\chi : \mathbb{F}_q^* \to \mathbb{C}^*$ multiplicative character. Assume ψ fixed, define the Gauss sum

$$g(\chi) = \sum_{x \in \mathbb{F}_q} \chi(x)\, \psi(x)$$

(where we can define $\chi(0) = 0$).

And the Jacobi sum

$$J(\chi_1, \chi_2) = \sum_{x \in \mathbb{F}_q} \chi_1(x)\, \chi_2(1 - x)$$

They have the following properties

(1) $g(\chi_{triv}) = -1$; $J(\chi_{triv}, \chi_{triv})$; $J(\chi_{triv}, \chi) = -1$;

$J(\chi, \bar{\chi}) = -\chi(-1)$; $J(\chi_1, \chi_2) = J(\chi_2, \chi_1)$

(2) $g(\chi)\, g(\bar{\chi}) = \chi(-1)\, q$; $|g(\chi)| = \sqrt{q}$

(3) $J(\chi_1, \chi_2) = \frac{g(\chi_1) g(\chi_2)}{g(\chi_1 \chi_2)}$ is $\chi_2 \neq \chi_1$

Now, for all m dividing $q - 1$, notice that the number of solutions $x \in \mathbb{F}_q$ to $x^m = a$ is given by

$$\#\{x^m = a\} = \sum_{\chi^m = 1} \chi(a)\, (*)$$

Both sides equals to m if a is an $m-$th power of in $\mathbb{F}_q$ and 0 otherwise.

We know that $N_1 = q + 1$ for $q \equiv 3[4]$. Now, we may suppose $q \equiv 1[4]$.

$$N' = \#\left\{u | u^2 = 4n^2\right\} + \#\left\{v | 0 = v^4 + 4n^2\right\} + \#\left\{u, v | u^2 = v^4 + 4n^2\right\}$$

The first term is 2, the second terms equals to $2 + 2\chi_4\left(-4n^2\right)$ by $(*)$. We have the thrid term equals to

$$\sum_{a,b,a=b+4n^2} \#\left\{u^2 = a\right\} \cdot \#\left\{v^4 = b\right\} = \sum_{a \in \mathbb{F}^*, a - 4n^2 \neq 0}\ \sum_{j=1,2,3,4;k=1,2} \chi_2^k(a)\, \chi_4^j\left(a - 4n^2\right)$$

Take $x = \frac{a}{4n^2}$, RHS becomes

$$\sum_{j=1,2,3,4;k=1,2} \chi_4^j\left(-4n^2\right) \sum_{x \in \mathbb{F}_q^*} \chi_2^k(x)\, \chi_4^j(1 - x) = \sum_{j=1,2,3,4;k=1,2} \chi_4^j\left(-4n^2\right) J\left(\chi_2^k, \chi_4^j\right)$$

Add up those, we have

$$N' = 4 + 2\chi_4\left(-4n^2\right) + \sum_{j=1,3} \chi_4^j\left(-4n^2\right) J\left(\chi_2, \chi_4^j\right) + q - 2 - 3 + 2\chi_4\left(-4n^2\right)(-1)$$

$$= q - 1 + \chi_4\left(-4n^2\right)\left(J(\chi_2, \chi_4) + J(\chi_2, \chi_4)\right)$$

Since there are $\chi_4(-4) = 1$, $\chi_4\left(-4n^2\right) = \chi_2(n)$. Set $\alpha = -\chi_2(n)\, J(\chi_2, \chi_4)$, $N_1 =$

$q+1-\alpha-\bar{\alpha}$.

According to the property relating Jacobi to Gauss sum,

$$\alpha=-\chi_2(n)\,g(\chi_2)\,g(\chi_4)/g(\bar{\chi_4})$$

Hence by property (2), $|\alpha|^2=q$.

Lemma 22 *Let $q\equiv 1[4]$, χ_2,χ_4 be characters of $\mathbb{F}_q^*$ of exact order 2 or 4, then $1+J(\chi_2,\chi_4)$ is divisible by $2+2i$ in $\mathbb{Z}[i]$*

Proof: There are $J(\chi_2,\chi_4)=J(\chi_4,\chi_4)\,g(\chi_2)^2/g(\chi_4)\,g(\bar{\chi_4})=\chi_4(-1)\,J(\chi_4,\chi_4)$. And,

$$J(\chi_4,\chi_4)=\sum\chi_4(x)\,\chi_4(1-x)=\chi_4^2\left(\frac{p+1}{2}\right)+2{\sum}'\chi_4(x)\,\chi_4(1-x)$$

where $\sum'$ is a sum over $(q-3)/2$ elements. Noticed that $\chi_4(x)\equiv 1[1+i]$, then $2\chi_4(x)\,\chi_4(1-x)\equiv 2[2+2i]$. Then, $J(\chi_4,\chi_4)\equiv q-3+\chi_4^2\left(\frac{p+1}{2}\right)\equiv 2+\chi_4(4)$. Then

$$1+J(\chi_2,\chi_4)=1+\chi_4(-1)\,J(\chi_4,\chi_4)\equiv 1+\chi_4(-4)+2\chi_4(-1)\,[2+2i]$$

Then, $1+J$ is divisible by $2+2i$. □

Now, let's look back to the theorem.

Theorem 23 *Let E_n be the elliptic curve $y^2=x^3-n^2x$ defined over $\mathbb{F}_p$ with $p\not|2n$, then*

$$Z(E_n/\mathbb{F}_p;T)=\frac{1-aT+pT^2}{(1-T)(1-pT)}=\frac{(1-\alpha T)(1-\bar{\alpha}T)}{(1-T)(1-pT)}$$

Where $a=Re\ \alpha$, $\alpha=i\sqrt{p}$ if $p\equiv 3[4]$, and if $p\equiv 1[4]$, then α is an element of $\mathbb{Z}[i]$ of norm p which is congruent to $\left(\frac{n}{p}\right)$ modulo $2+2i$.

Proof: Here, we must let p vary, and determine $N_r=\#E_n(\mathbb{F}_{p^r})$ for $p\equiv 1[4]$, and N_{2r} for $p\equiv 3[4]$.

Fix $q=p$ for the first case and $q=p^2$ for the second case, we need find a formula for $\#E_n(\mathbb{F}_q)$, $q\equiv 1[4]$.

Denote $\mathbb{N}_r:\mathbb{F}_{q^r}\to\mathbb{F}_q$ by $g\mapsto g^{1+q+\cdots+q^{r-1}}$, we denote $\chi_{4,r}=\chi_4\circ\mathbb{N}_r$, $\chi_{2,r}=\chi_2\circ\mathbb{N}_r$

Then, one can write

$$\#E_n(\mathbb{F}_{q^r})=q^r+1-\alpha_{n,q^r}-\bar{\alpha}_{n,q^r}$$

where $\alpha_{n,q^r}=-\chi_{2,r}(n)\,\frac{g(\chi_{2,r})g(\chi_{4,r})}{g(\bar{\chi_{4}},_r)}$ Now, we should notice the fact of Gauss sum that

$$-g(\chi\circ\mathbb{N}_r)=(-g(\chi))^r$$

Noticed that $\chi_{2,r}(n) = \chi_2(n^r) = \chi_2(n)^r$, we conclude that

$$\alpha_{n,q^r} = \alpha_{n,q}^r$$

Hence

$$N_r = p^r + 1 - \alpha^r - \bar{\alpha}^r$$

That we have proven the case for $p \equiv 1[4]$

Now, for $p \equiv 3[4]$, $q = p^2$, then $\chi_2(n) = 1$. Then $\alpha_{n,q}$ is a Gaussian integer of norm q which is congruent to 1 mod $2+2i$. For $i^j p, j = 0,1,2,3$, only $-p$ satisfies this property. Then, we have for even r

$$N_r = \# E_n\left(\mathbb{F}_{q^{r/2}}\right) = p^r + 1 - (-p)^{r/2} - (-p)^{r/2}$$

Hence, for all r, we have

$$N_r = p^r + 1 - (i\sqrt{p})^r - (-i\sqrt{p})^r$$

This finishes the proof of the theorem. □

4.2 Riemann zeta-function

After these section of all this section, all proofs are omitted due to the limitation of space. More about this is in [7].

Proposition 24

$$(1-T)(1-pT)\,Z(E_n/\mathbb{F}_p;T) = \prod_{P|(p)}\left(1 - (\alpha_P T)^{deg\ P}\right)$$

where the product is over the (one or two) prime ideals of $\mathbb{Z}[i]$ dividing (p), and where $\alpha_P = i\sqrt{p}$ if $P = (p)$ and $\alpha_P = a + bi$ if P splits. We take $\alpha_P = 0$ if $P|2n$

Now, define $\chi_n'(x) = 0$ if x has no common factor with $2n$. For $n = 1$, define $\chi_1'(x) = i^j$ if $i^j x \equiv 1[2i+2]$. For higher n, define $\chi_n'(x) = \chi_1'(x)\left(\frac{n}{\mathbb{N}x}\right)$, where $\mathbb{N}x = x \cdot \bar{x}$ a positive odd integer. Now, define $\tilde{\chi}_n(x) = x\chi_n'(x)$.

Proposition 25 *$\tilde{\chi}_n$ is the unique multiplicative map on $\mathbb{Z}[i]$ which coincides with $\alpha_P^{\deg P}$ on any generator of a prime ideal P. And it is a primitive multiplicative character modulo $(2+2i)\,n$ for odd n and modulo $2n$ for even n.*

Now, we may choose $n' = \begin{cases} (2+2i)\,n & n\ odd \\ 2n & n\ even \end{cases}$, define our additive character on

$\mathbb{Z}[i]/n'$ by:

$$\psi\left(x\right)=e^{2\pi i\,\mathrm{Re}(x/n')}$$

It is easy to check that ψ is a nontrivial additive character of $\mathbb{Z}[i]/n'$ which is also nontrivial on the multiples of any proper divisor of n'.

Proposition 26

$$g\left(\chi_n'\right):=\sum_{x\in\mathbb{Z}[i]/n'}\chi_n'\left(x\right)e^{2\pi i\,\mathrm{Re}(x/n')}=\begin{cases}\left(\frac{-2}{n}\right)n', & n\ odd\\ \left(\frac{-1}{n_0}\right)in' & n=2n_0\ even\end{cases}$$

One may compare the result to the Gauss sum in the Algebraic number theory. Now, define

$$\begin{aligned}L\left(E_n,s\right)&:=\frac{\zeta\left(s\right)\zeta\left(s-1\right)}{\prod_p Z\left(E_n/\mathbb{F}_p;p^{-s}\right)}\\&=\prod_{p\nmid 2n}\frac{1}{1-2a_{E_n,p}p^{-s}+p^{1-2s}}\\&=\prod_{P\nmid 2n}\frac{1}{1-\alpha_P^{\deg P}\left(\mathbb{N}P\right)^{-s}}\end{aligned}$$

This is called that Hasse-Weil $L-$function. With the restriction $\mathrm{Re}\,s\geqslant\frac{3}{2}$ on $s\in\mathbb{C}$ we can ensure the product converge. We can expand it into the Dirichlet series i.e.

$$L\left(E_n,s\right)=\sum_m b_{m,n}m^{-s}$$

For example,

$$\begin{aligned}L\left(E_1,s\right)&=\frac{1}{1+3\cdot 9^{-s}}\cdot\frac{1}{1+2\cdot 5^{-s}+5\cdot 25^{-s}}\cdot\frac{1}{1+7\cdot 49^{-s}}\cdot\cdots\\&=1-2\cdot 5^{-s}-3\cdot 9^{-s}+6\cdot 13^{-s}+2\cdot 17^{-s}+\cdots\end{aligned}$$

There are

$$L\left(E_n,s\right)=\prod_{P\nmid 2n}\left(1-\frac{\tilde{\chi}_n\left(P\right)}{\left(\mathbb{N}P\right)^s}\right)^{-1}$$

Noticed that both $\tilde{\chi}_n$ and $\mathbb{N}$ are multiplicative, we obtain:

$$L\left(E_n,s\right)=\sum_I\tilde{\chi}_n\left(I\right)\left(\mathbb{N}I\right)^{-s}$$

the sum is over all nonzero ideals of $\mathbb{Z}[i]$. As is learned in the course of Algebraic Number Theory, a series of this form is called a "Hecke $L-$series", and the $\tilde{\chi}_n$ is called the "Hecke character". Then, one may work it with Dirichlet $L-$series and discuss the analytic continuation and functional equation.

Then, we obtain that $b_{m,n} = \sum_{I,\mathbb{N}_i=m} \tilde{\chi}_n\left(I\right)$. Noticed that $\tilde{\chi}_n\left(I\right) = \tilde{\chi}_1\left(I\right)\left(\frac{n}{\mathbb{N}I}\right)$, we have

$$b_{m,n} = \left(\frac{n}{m}\right) \sum_{I,\mathbb{N}I=m} \tilde{\chi}_1\left(I\right) = \left(\frac{n}{m}\right) b_m$$

Denote $\chi_n : m \mapsto \left(\frac{n}{m}\right)$, there are $L\left(E_n, s\right) = \sum \chi_n\left(m\right) b_m m^{-s}$. One can say that $L\left(E_n, s\right)$ is a "twisting" of $L\left(E_1, s\right)$ by χ_n. The conductor of χ_n is n when $n \equiv 1[4]$ and equals to $4n$ when $n \equiv 2, 3[4]$. Since $\mathbb{Z}[i]$ is PID,

$$b_{m,n} = \frac{1}{4} \sum_{a+bi, a^2+b^2=m} \tilde{\chi}_n\left(a+bi\right)$$

and

$$L\left(E_n, s\right) = \frac{1}{4} \sum_{a+bi} \frac{\left(a+bi\right)\chi'_n\left(a+bi\right)}{\left(a^2+b^2\right)^s}$$

Theorem 27 *The Hasse-Weil $L-$function $L\left(E_n, s\right)$ for the elliptic curve $E_n : y^2 = x^3 - n^2 x$ defined on the whole $\operatorname{Re} s > \frac{3}{2}$ extends analytically to an entire function on the whole complex s-plane. In addition, Let*

$$N = 4|n'|^2 = \begin{cases} 32n^2 & n \text{ odd} \\ 16n^2 & n \text{ even} \end{cases}$$

And

$$\Lambda\left(s\right) := \left(\frac{\sqrt{N}}{2\pi}\right)^s \Gamma\left(s\right) L\left(E_n, s\right)$$

Then $L\left(E_n, s\right)$ satisfies the functional equation

$$\Lambda\left(s\right) = \pm\Lambda\left(2-s\right)$$

where the "root number" ± 1 is equals to 1 if $n \equiv 1, 2, 3[8]$ and is equals to -1 in $n \equiv 5, 6, 7[8]$

The proof of this theorem use the tools of Fourier Analysis. One student in Qiuzhen College should have learnt the outline of the proof since he finishes the study of Stein and Real Analysis.

4.3 Critical value: The key to solve the problem

Conjecture 28 *(B. J. Birch and H. P. F. Swinnerton-Dyer)*

$L(E,1)=0$ *if and only if* E *has infinitely many rational points.*

In this conjecture E is any elliptic curve defined over $\mathbb{Q}$. We shall call the above conjecture the "weak Birch-Swinnerton-Dyer conjecture", because Birch and Swinnerton-Dyer made a much more detailed conjecture about the behavior of $L(E,s)$ at $s=1$ in the 1960s.

We may see that why the conjecture "looks true". Let's pretend that the Euler product for it is convergent for $s=1$, in that case, we have:

$$L(E,1)=\prod_p \frac{1}{1-2a_{E,p}p^{-s}+p^{1-2s}}=\prod_p \frac{p}{N_p}$$

Roughly, $N_p \approx p \pm \sqrt{p}$. If N_p lies on the both sides with "same possibility", one may think that it converges to a nonzero number. If it tends to lie on the large side, then it should be 0.

If there's infinitely many rational points, one may expect that by reduction modulo p, we could obtain a large guaranteed contribution to N_p for all p, they tend to have $N_p \approx p+\sqrt{p}$. Otherwise, if there are finitely many rational points, N_p will have randomly $N_p \approx p \pm \sqrt{p}$.

Now, come out of the dream, we have the theorem

Theorem 29 *(J. Coates and A. Wiles) Let* E *be an elliptic curve defined over* $\mathbb{Q}$ *and having complex multiplication. If* E *has infinitely many* $\mathbb{Q}-$*points, then* $L(E,1)=0$

The proof is hard. One can refer to [2].

Proposition 30 *If* $n \equiv 5,6,7[8]$*, and if the weak B-S-D conjecture holds for* E_n*, then* n *is a congurent number.*

Proof: We have by the functional equation, $\Lambda(s)=-\Lambda(2-s)$, hence $\Lambda(1)=0$. But $\Lambda(1)$ differs from $L(E_n,1)$ by a nonzero factor. Thus $L=0$, and then there's infinitely many rational points on E_n, and then n is a congruent number. □

Proposition 31 *The critical value of the Hasse-Weil* $L-$*function of the elliptic curve* $E_n: y^2=x^3-n^2x$ *for squarefree* $n\equiv 1,2,3[8]$ *is given by:*

$$L(E_n,1)=2\sum_{m=1}^{\infty}\frac{b_{m,n}}{m}e^{-\pi m/\sqrt{N'}}$$

where

$$\sqrt{N'} = \begin{cases} 2n\sqrt{2} & n \text{ odd} \\ 2n & n \text{ even} \end{cases}$$

Here, the coefficients $b_{m,n}$ are the Dirichlet series coefficients obtained by expanding

$$L\left(E_n, s\right) = \prod_{p \nmid 2n} \left(1 - 2a_{E_n,p}p^{-s} + p^{1-2s}\right)^{-1} = \sum_{m=1}^{\infty} b_{m,n}m^{-s}$$

In addition, the absolute value of the coefficient $b_{m,n}$ is bounded by $\sigma_0\left(m\right)\sqrt{m}$, where $\sigma_0\left(m\right)$ denotes the number of divisors of m

Proof: Everything new for us is the bound of $b_{m,n}$. If we write the Euler factor in the form $\left(1 - \alpha_p p^{-s}\right)^{-1}\left(1 - \bar{\alpha_p} p^{-s}\right)^{-1}$, the coefficient of p^{-es} is $\alpha_p^e + \alpha_p^{e-1}\bar{\alpha_p} + \cdots + \bar{\alpha_p}^e$. Then, $b_{m,n} = \prod_p \left(\alpha_p^e + \alpha_p^{e-1}\bar{\alpha_p} + \cdots + \bar{\alpha_p}^e\right) \leqslant \sigma_0\left(m\right)\sqrt{m}$. □

Then, we have

$$L_1\left(E_1, 1\right) =$$

$$2\left(e^{-\pi/2\sqrt{2}} - \frac{2}{5}e^{-5\pi/2\sqrt{2}} - \frac{1}{3}e^{-9\pi/2\sqrt{2}} + \frac{6}{13}e^{-13\pi/2\sqrt{2}} + \frac{2}{17}e^{-17\pi/2\sqrt{2}} + \cdots\right)$$

$$= 0.6555143\cdots + R_{25}$$

Denoted by $R_M = 2\sum_{m \geqslant M} \frac{b_m}{m} e^{-\pi M/2\sqrt{2}}$, by the upper bound

$$\left|R_M\right| \leqslant 4\sum_{m \geqslant M} e^{-\pi m/2\sqrt{2}} = \frac{4}{1 - e^{-\pi/2\sqrt{2}}}e^{-\pi M/2\sqrt{2}}$$

So, $L\left(E_1, 1\right) = 0.65\cdots + R_5$, with $\left|R_5\right| \leqslant 0.023$. Hence, by the Coates-Wiles theorem, 1 is not congruent.

5 Modular forms

The history of the development of modular form is divided into 4 periods:

1. In connection with the theory of elliptic functions in the earlt nineteenth century

2. By Felix Klein and others towards the end of the nineteenth century as the automorphic form concept became understood (for one variable)

3. By Erich Hecke from about 1925

4. In the 1960s, as the needs of number theory and the formulation of the modularity theorem in particular made it clear that modular forms are deeply implicated.

In 2001, all elliptic curves were proven to be modular over rational numbers. In 2013 elliptic curves were proven to be modular over real quadratic fields. In 2023 elliptic curves were proven to be modular over about half of imaginary quadratic fields, including fields formed by combining the rational numbers with the square root of integers down to -5. [11]

The famous story is in 1994, Andrew Wiles used modular forms and elliptic curves to prove the Fermat's Last Theorem. The story is morelessly like the story that we will talk: to use these tool to solve the problem in number theory.

5.1 The simplest case–$SL_2\left(\mathbb{Z}\right)$

We can define the action of $SL_2\left(\mathbb{R}\right)$ on $\tilde{\mathbb{C}} = \mathbb{C} \cup \{\infty\}$ by

$$gz = \frac{az+b}{cz+b}$$

Noticed that $\pm I$ the only matrix acts trivially on $\tilde{\mathbb{C}}$, we may consider the quotient group $PSL_2\left(\mathbb{R}\right)$.

We can easily verify that

$$\operatorname{Im}\left(gz\right) = |cz+d|^{-2} \operatorname{Im} z$$

then, it acts on the upper half plane $\mathcal{H}$.

Now, we may consider $\Gamma = SL_2\left(\mathbb{Z}\right)$, we define

$$\Gamma\left(N\right) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} | a \equiv d \equiv 1[N], b \equiv c \equiv 0[N] \right\}$$

$\Gamma\left(N\right)$ is called the "principal congruence subgroup of level N". We can samely define $\bar{\Gamma} = \Gamma / \pm I$ and prove that $\bar{\Gamma}\left(N\right) = \Gamma\left(N\right)$. A subgroup of Γ(or of $\bar{\Gamma}$) is called a "congruence subgroup of level N". The most important cases are

$$\Gamma\left(N\right) = \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} [N] \right\}$$

$$\Gamma_1\left(N\right) = \left\{ \begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix} [N] \right\}$$

$$\Gamma_0(N) = \left\{ \begin{pmatrix} * & * \\ 0 & * \end{pmatrix} [N] \right\}$$

For G, we say z_1, z_2 is $G-$equivalent, if they lies on the same orbits. We say F a closed region in $\mathcal{H}$ a fundamental domain if every $z \in H$ is equivalent to a point in F, but no two distinct points are equivalent in F.

Proposition 32

$$F := \left\{ z \in \mathcal{H} | -\frac{1}{2} \leqslant \operatorname{Re} z \leqslant \frac{1}{2}, |z| \geqslant 1 \right\}$$

is a fundamental domain of Γ*. Moreover, two distinct point* z_1, z_2 *on the boundary are equivalent if and only if* $\operatorname{Re} z_1 = \pm\frac{1}{2}$ *and* $z_2 = z_1 \mp 1$*, or* z_1 *on the unit circle and* $z_1 z_2 = -1$*.*

Proposition 33

$$T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$$

$$S = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$$

Then for $z \in F$*,* Γ_z *are in the following 4 cases*

(1)$\pm \{I, S\}$ *for* $z = i$

(2)$\pm \left\{I, ST, (ST)^2\right\}$ *for* $z = \omega = \frac{-1+\sqrt{-3}}{2}$

(3)$\pm \left\{I, TS, (TS)^2\right\}$ *for* $z = -\bar{\omega} = \frac{1+\sqrt{-3}}{2}$

(4)$\pm \{I\}$ *otherwise*

Proposition 34 $\bar{\Gamma}$ *is generated by* S *and* T*.*

Refer to [9].

Now, let $\bar{H} = H \cup \{\infty\} \cup \mathbb{Q}$, the topology on the boundary is given by $N_C = \{z | \operatorname{Im} z > C\} \cup \{\infty\}$, and gN_C for $z = \frac{a}{c}$, $g = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$

In section 3, we define the function maps $\mathbb{C}/L$ to $\mathbb{P}^2_{\mathbb{C}}$ by the $\wp-$function. Now, we will define a certain function maps $\bar{F} = \Gamma \backslash \bar{H}$ to the projective line $\mathbb{P}^1_{\mathbb{C}}$.

Proposition 35 *For* $\Gamma' \subset \Gamma$*,* $[\Gamma : \Gamma'] = n < \infty$*, then for* $\Gamma = \sqcup \alpha_i \Gamma$*,* $F' = \cup \alpha_i^{-1} F$ *is a fondamental domain of* Γ'

Now, we may define the modular forms for $SL_2(\mathbb{Z})$.

For f meromorphic function on $\mathcal{H}$ and k an integer. Suppose f satisfies the relation

$$f(gz) = (cz+d)^k f(z), \forall g = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z})$$

which is equals to that $f(z+1) = f(z), f(-1/z) = (-z)^k f(z)$.

Further more, we may suppose that f is "meromorphic at infinity" i.e. for $f(z) = \sum_{n\in\mathbb{Z}} a_n q^n$ where $q = e^{2i\pi z}$ has at most finitely many nonzero a_n with $n < 0$. Then f is called a "modular function of weight k for Γ". In addition, if f is holomorphic on $\mathcal{H}$ and at infinity, then it is called a modular form. The set for modular form of weight k for Γ is denoted $M_k(\Gamma)$.

If we furthermore assume that $a_0 = 0$, then $f(z)$ is called a "cusp-form of weight k for Γ". The set for cusp-form of weight k for Γ is denoted $S_k(\Gamma)$. Here, the S comes from the German "Spitzenform". And the cusp-form is also called "parabolic forms".

For example, let k be an even integer greater than 2, we can define

$$G_k(z) := \sum_{m,n}{}' \frac{1}{(mz+n)^k}$$

Remark 9 For k even,

$$\lim_{z\to i\infty} G_k(z) = 2\zeta(k)$$

Since we can easily prove that $M_k = 0$ for k odd, we may assume that k even. It is easy to check that $G(z) = G(z+1)$, $z^{-k}G_k\left(-\frac{1}{z}\right) = G_k(z)$. Hence $G_k \in M_k(\Gamma)$.

Proposition 36 *Let k be an even integer greater than 2, and let $z \in \mathcal{H}$. Then G_k has the following $q-$expansion*

$$G_k(z) = 2\zeta(k)\left(1 - \frac{2k}{B_k}\sum_{n=1}^{\infty} \sigma_{k-1}(n) q^n\right)$$

where $q = e^{2\pi iz}$ and the Bernoulli number B_k are defined by setting

$$\frac{x}{e^x - 1} = \sum_{k=0}^{\infty} B_k \frac{x^k}{k!}$$

By this proposition, we may define

$$E_k = \frac{1}{2\zeta(k)} G_k = 1 - \frac{2k}{B_k}\sum_n \sigma_{k-1}(n) q^n$$

Then, $\Delta(z) = \frac{(2\pi)^{12}}{1728}(E_4^3 - E_6^2)$, is a cusp form with weight 12.

Now, by drawing a proper contour around the fundamental domain F and integrate $\frac{f'}{f}$, we obtain the following proposition

Proposition 37 *Let $f(z)$ be a nonzero modular function of weight k for Γ. Let $v_p(f)$ denote the order of zero of $f(z)$ at point P. Then*

$$v_\infty + \frac{1}{2}v_i + \frac{1}{3}v_\omega + \sum_{P \in \Gamma\backslash\mathcal{H}, P \neq i,\omega} v_P = \frac{k}{12}$$

And thus the following proposition

Proposition 38 *Let k be an even integer, $\Gamma = SL_2(\mathbb{Z})$.*

(a) The only modular forms of weight 0 is constant. $M_0 = \mathbb{C}$.

(b) $M_k(\Gamma) = 0$ if k negative or $k = 2$.

(c) M_k is dim-1 and generated by E_k if $k = 4, 6, 8, 10, 14$.

(d) $S_k(\Gamma) = 0$ if $k < 12$ or $k = 14$. And $S_{12}(\Gamma) = \mathbb{C}\Delta$. For $k > 14$, $S_k = \Delta M_{k-12}$.

(e) $M_k(\Gamma) = S_k(\Gamma) \oplus \mathbb{C}E_k$.

Then,

Proposition 39 *Any $f \in M_k(\Gamma)$ can be written in the form*

$$f(z) = \sum_{4i+6j=k} c_{i,j} E_4^i E_6^j$$

Now, consider $j(z) = 1728\frac{E_4^3}{E_4^3 - E_6^2}$

Proposition 40 *j gives a bijection from $\Gamma\backslash\bar{H}$ to the Riemann sphere $\mathbb{P}^1_{\mathbb{C}} = \mathbb{C} \cup \{\infty\}$.*

The key is, $1728E_4^3 - C(E_4^3 - E_6^2)$, by prop 37, must vanish at exactly one point in $\mathcal{H}$.

Proposition 41 *The modular function of weight zero for Γ are precisely the rational functions of j.*

The proof is morelessly like Theorem 11. By this proposition, we can prove the former question we asked at:

Proposition 42 *For any $A, B \in \mathbb{C}$, $A^3 \neq 27B^2$, there exists $L = \lambda L_z = \{m\lambda z + n\lambda\}$*

s.t.

$$g_2(L) := \frac{4}{3}\pi^4 E_4(z) = A, g_3(L) := \frac{8}{27}\pi^6 E_6(z) = B$$

And, by the way, we recall that

Proposition 43

$$(2\pi)^{-12}\Delta(z) = q\prod_{n=1}^{\infty}(1-q^n)^{24}, q = e^{2\pi iz}$$

5.2 For congruence subgroup

In this section, we only list the properties of the modular forms for the congruence group.

Denote $f(z)\,|[\gamma]_k = (\det\gamma)^{k/2}(cz+d)^{-k} f(\gamma z)$ for $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in GL_2^+(\mathbb{Q})$.

Definition 4 Let $f(z)$ a meromorphic function on $\mathcal{H}$, and let $\Gamma' \subset \Gamma$ a congruence subgroup of level N, i.e. $\Gamma' \supset \Gamma(N)$. Let $k \in \mathbb{Z}$, we call $f(z)$ a modular function of weight k for Γ' if

$$f|[\gamma]_k = f, \forall\gamma \in \Gamma'$$

and if $\forall\gamma_0 \in \Gamma$, $f(z)\,|[\gamma_0]_k$ has the form $\sum a_n q_N^n$ with $a_n = 0$ for $n << 0(*)$. We call such an $f(z)$ a modular form of weight k for Γ' if it is holomorphic on $\mathcal{H}$ and if for all $\gamma_0 \in \Gamma$ we have $a_n = 0$ for all $n < 0$. We call a modular form a cusp form if in addition $a_0 = 0$ for all $\gamma_0 \in \Gamma$.

Proposition 44 *The condition $(*)$ only depends on the $\Gamma'-$equivalence class of $s = \gamma_0\infty$. Moreover, if $\gamma_1\infty = \gamma'\gamma_2\infty$ for some $\gamma' \in \Gamma'$, then the smallest power of q_N that occurs in the Fourier expansion of $f|[\gamma_1]_k$ and $f|[\gamma_2]_k$ are the same. Moreover, if the smallest term is the constant term, then the value at $q_N = 0$ is the same for $f(z)\,|[\gamma_1]_k$ and $f(z)\,|[\gamma_2]_k$ for k even, and may change the sign for k odd.*

Then, we have the proposition, denote the subspace of $M_k(\Gamma_1(N))$ f which $f|[\gamma]_k = \chi(d)\,f$ whenever $\gamma \in \Gamma_0(N)$ by $M_k(N,\chi)$, we have

Proposition 45 *(a) Let's Γ' be a congruence subgroup of Γ, let $\alpha \in GL_2^+(\mathbb{Q})$, and set $\Gamma'' = \alpha^{-1}\Gamma'\alpha \cap \Gamma$. Then Γ'' is a congruence subgroup of Γ, and the map $f \mapsto f|[\alpha]_k$ takes $M_k(\Gamma')$ to $M_k(\Gamma'')$, and takes $S_k(\Gamma')$ to $S_k(\Gamma'')$. In particular, if $f \in M_k(\Gamma)$*

and $g(z) = f(Nz)$, then $g \in M_k(\Gamma_0(N))$ and one has $g(\infty) = f(\infty), g(0) = N^{-k} f(0)$.

(b) Let χ be a Dirichlet character modulo M, and let χ_1 be a primitive Dirichlet character modulo N.

If $f(z) = \sum_{n=0}^{\infty} a_n q^n \in M_k(M, \chi)$ and $f_{\chi_1}(z) = \sum_{n=0}^{\infty} a_n \chi_1(n) q^n$, then $f_{\chi_1} \in M_k(MN^2, \chi\chi_1^2)$. If f is a cusp form, then so is f_{χ_1}. In particular, if $f \in M_k(\Gamma_0(M))$ and χ_1 is quadratic, then $f_{\chi_1} \in M_k(\Gamma_0(MN^2))$.

Now, we may consider the Eisenstein series: For N positive integer, let $\underline{a} = (a_1, a_2)$ a pair of integers modulo N. we may consider the "level N Eisenstein series" as:

$$G_k^{\underline{a}}(z) := \sum_{\underline{m} \in \mathbb{Z}^2, \underline{m} \equiv \underline{a}[N]} \frac{1}{(m_1 z + m_2)^k}$$

we have $G_k^{\underline{0}}(z) = N^{-k} G_k(z)$.

Then we have

Proposition 46 *$G_k^{\underline{a}} \in M_k(\Gamma(N))$, and $G_k^{(0,a_2)} \in M_k(\Gamma_1(N))$.*

Now, we define $\eta(z) = e^{2\pi i z/24} \prod_n (1 - q^n)$

Proposition 47 *Let $f(z)$ be a nonzero element of $S_k(\Gamma_0(N))$, where $N = 2, 3, 5, 11$ and $k = 8, 6, 4, 2$, so that $k(N+1) = 24$, then $f(z)$ is a constant multiple of $g(z) := (\eta(z)\eta(Nz))^k$*

Note that the case of $N = 1$ is $g = C\Delta/q$.

Proposition 48 *$M_0(\Gamma') = \mathbb{C}$ for any congruence subgroup $\Gamma' \subset \Gamma$. That is, there are no non-constant modular forms of weight zero.*

Proposition 49 *For $k \geqslant 3$ let $G_k^{\underline{a}}$ be the Eisenstein series, then the q_N-expansion of $G_k^{\underline{a}}$*

$$G_k^{\underline{a}}(z) = b_{0,k}^{\underline{a}} + \sum_{n=1}^{\infty} b_{n,k}^{\underline{a}} q_N^n \, (*)$$

For $\zeta := e^{2\pi i/N}, q_N := e^{2\pi i z/N}$ can be computed as

$$b_0^{\underline{a}} = \begin{cases} 0 & a_1 \neq 0 \\ \zeta^{a_2}(k) + (-1)^k \zeta^{-a_2}(k) & a_1 = 0 \end{cases}$$

$$c_k = \frac{(-1)^{k-1} 2k\zeta(k)}{N^k B_k}$$

$$G_k^{\underline{a}} = b_0^{\underline{a}} + c_k \left(\sum_{\substack{m_1 \equiv a_1[N] \\ m_1 > 0}} \sum_{j=1}^{\infty} j^{k-1} \zeta^{ja_2} q_N^{jm_1} + (-1)^k \sum_{\substack{m_1 \equiv -a_1[N] \\ m_1 > 0}} \sum_{j=1}^{\infty} j^{k-1} \zeta^{-ja_2} q_N^{jm_1} \right)$$

Moreover, for $\underline{a} = (a_1, 0)$*, then*

$$b_{n,k}^{\underline{a}} = c_k \left(\sum_{j|n, n/j \equiv a_1[N]} j^{k-1} + (-1)^k \sum_{j|n, n/j \equiv -a_1[N]} j^{k-1} \right)$$

If $\underline{a} = (0, a_2)$*, then for* $n \geqslant 1$

$$b_{n,k^{\underline{a}}} = 0, \forall N \nmid n, b_{Nn,k}^{\underline{a}} = c_k \sum_{j|n} j^{k-1} \left(\zeta^{ja_2} + (-1)^k \zeta^{-ja_2} \right)$$

Thus, for $\underline{a} = (0, a_2)$

$$G_k^{(0,a_2)}(z) = b_{0,k}^{(0,a_2)} + c_k \sum_{n-1}^{\infty} \left(\sum_{j|n} j^{k-1} \left(\zeta^{ja_2} + (-1)^k \zeta^{-ja_2} \right) q^n \right)$$

Proposition 50 *If* $2\underline{a} \equiv (0,0)[N]$ *with* k *odd, then* $G_k^{\underline{a}} = 0$*. Otherwise,* $G_k^{(0,a_2)}$ *is nonzero at* ∞*, and* $G_k^{(a_1,0)}$ *has a zero of order* $\min(a_1, N - a_1)$*, where we are taking* a_1 *in the range* $0 < a_1 < N$*. That is, for* $\underline{a} = (a_1, 0)$*, the first power of* q_N *which occurs in* $(*)$ *with nonzero coefficient is* $q_N^{a_1}$ *or* $q_N^{N-a_1}$*.*

Then, we have

Proposition 51 *If* $2\underline{a} \not\equiv 0[N]$*, then* $G_3^{\underline{a}}(z) \neq 0$ *for* $z \in \mathcal{H}$*.*

Proposition 52 *Define*

$$h(z) = \prod_{a_2=1}^{p-1} G_3^{(0,a_2)}(z)$$

Then $h(z) \in M_{3(p-1)}(\Gamma_0(p))$*, its only zero is a* $(p^2-1)/4-$*fold zero at* 0*, and it is a constant multiple of* $(\eta^p(z)/\eta(pz))^6$

And then, for

$$f(z) = \prod_{a_2=1}^{(p-1)/2} G_3^{(0,a_2)}(z)$$

there are $h(z) = (-1)^{(p-1)/2} f(z)^2$ Hence there are

Proposition 53 *The function* $f(z)$ *is a constant multiple of* $(\eta^p(z)/\eta(pz))^3$*. More-*

over, for $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$, *then* $f|[\gamma]_{3(p-1)/2} = \left(\frac{d}{p}\right) f$, *where* $\left(\frac{d}{p}\right)$ *is the Legendre symbol.*

Remark 10 This proposition is an example of a general relationship between modular forms for $\Gamma_1(N)$ and "twisted-modular" forms for $\Gamma_0(N)$, called "modular forms with character".

Proposition 54 $M_k(\Gamma_1(N)) = \oplus M_k(N,\chi)$, *where the sum is over all Dirichlet characters modulo* N.

And thus,

Proposition 55

$$M_k(\Gamma_1(4)) = \begin{cases} M_k(4,1) & k \text{ even} \\ M_k(4,\chi) & k \text{ odd} \end{cases}$$

where 1 *denote the trivial character and* χ *the unique nontrivial character modulo* 4.

Now, look back to the theta function defined in the section 2, $\Theta^2 = \left(\sum_{n\in\mathbb{Z}} q^{n^2}\right)^2$

Proposition 56 $\Theta^2 \in M_1(\Gamma_1(4)) = M_1(4,\chi)$, *where* $\chi(d) = (-1)^{(d-1)/2}$.

Now, consider $f(z) = \sum_{n\geqslant 1} a_n q^n \in M_k(\Gamma_1(N))$. Here we have $f(\infty) = 0$. Set $g(s) := \int_0^{i\infty} f(z) z^{s-1} dz$.

There are g converges for $\operatorname{Re} s > c+1$ for $|a_n| = O(n^c)$.

$$\begin{aligned} \int_0^{i\infty} f(z) z^{s-1} dz &= \sum_{n=1}^{\infty} a_n \int_0^{i\infty} z^s e^{2\pi i n z} \frac{dz}{z} \\ &= \sum_{n=1}^{\infty} a_n \left(-\frac{1}{2\pi i n}\right)^s \int_0^{\infty} t^s e^{-t} \frac{dt}{t} \\ &= (-2\pi i)^{-s} \Gamma(s) \sum_{n=1}^{\infty} a_n n^{-s}. \end{aligned}$$

Now, define $L_f(s) = \sum_{n=1}^{\infty} a_n n^{-s}$ for $\operatorname{Re} s > c+1$, if $f(z) = \sum_{n=0}^{\infty} a_n q^n$. $g(s) = (-2\pi i)^{-s} \Gamma(s) L_f(s)$.

We may define that $\Lambda(s) = \left(-i\sqrt{N}\right)^s g(s) = \left(\sqrt{N}/2\pi\right)^s \Gamma(s) L_f(s)$. There are, $\Lambda(s) = C\Lambda(k-s)$, which one can compare this with the property of Hasse-Weil $L-$function.

Now, for $C = \pm 1$, χ of conductor m, we set

$$C_\chi = C\chi_0\left(m\right)\chi\left(-N\right)g\left(\chi\right)/g\left(\bar{\chi}\right)$$

where $g\left(\chi\right) = \sum_{j=1}^{m}\chi\left(j\right)e^{2\pi ij/N}$ the Gauss sum. Given a $q-$expansion of $f\left(z\right) = \sum_{n=0}^{\infty}a_nq^n$, $q = e^{2\pi iz}$. For $\left|a_n\right| = O\left(n^c\right)$, define the $L_f\left(s\right)$ and $\Lambda\left(s\right)$ above, and further

$$L_f\left(\chi,s\right) = \sum_{n=1}^{\infty}\chi\left(n\right)a_nn^{-s}; \Lambda\left(\chi,s\right) = \left(m\sqrt{N}/2\pi\right)^s\Gamma\left(s\right)L_f\left(\chi,s\right)$$

.

Theorem 57 *(Weil) Suppose that* $f\left(z\right) = \sum_{n=0}^{\infty}a_nq^n, q = e^{2\pi iz}$ *has the property that* $\left|a_n\right| = O\left(n^c\right), c \in \mathbb{R}$. *Suppose that for* $C = 1$ *or* -1 *the function* $\Lambda\left(s\right)$ *has the property that* $\Lambda\left(s\right) + a_0\left(1/s + C/\left(k-s\right)\right)$ *extends to an entire function which is bounded in any vertical strip of the complex plane, and satisfies* $\Lambda\left(s\right) = C\Lambda\left(k-s\right)$. *Further suppose that for a "large" set of characters* χ *of conductor* m, $\Lambda\left(\chi,s\right)$ *extends to an entire function which is bounded in any vertical strip of the complex plane, and satisfies* $\Lambda\left(s\right) = C_\chi\Lambda\left(k-s\right)$.

Then, $f \in M_k\left(N,\chi_0\right)$ *and* f *satisfies that* $f|[\alpha_N]_k = Ci^{-k}f, C = 1$ *or* -1 *for* $\alpha_N = \begin{pmatrix} 0 & -1 \\ N & 0 \end{pmatrix}$. *If in addition* $L_f\left(s\right)$ *converges absolutely for* $\operatorname{Re} s > k-\epsilon$ *for some* $\epsilon > 0$, *then* f *is a cusp form.*

By this theorem, consider $L\left(E_1,s\right)$, where E_1 the elliptic curve $y^2 = x^3 - x$, we can conclude that

$$f_{E_1}\left(z\right) = q - 2q^5 - 3q^9 + 6q^{13} + 2q^{17} + \sum_{m\geqslant 25}b_mq^m$$

is a cusp form of weight two for $\Gamma_0\left(32\right)$.

And then, for $f_{E_n} = \sum\chi_n\left(m\right)b_mq^m$, $f_{E_n} \in M_2\left(\Gamma_0\left(32n^2\right)\right)$ for n odd and $f_{E_n} \in M_2\left(\Gamma_0\left(16n^2\right)\right)$ for n even.

Conjecture 58 *(Taniyaka and Weil) Every elliptic curve defined over the rational numbers has* $L-$*function which satisfies Weil's theorem for some* N.

Geometrically, the cusp forms of weight two can be regarded as holomorphic differential forms on the Riemann surface $\Gamma_0\left(N\right)\backslash\mathcal{H}$. The Taniyama-Weil conjecture then can be shown to take this form: every elliptic curve over $\mathbb{Q}$ can be obtained as a quotient of the Jacobian of some such Riemann surface.

At last, it's surprising that Gerhard Frey suggested in 1986 that the Taniyama-

Weil conjecture implies Fermat's Last Theorem. The book [7] I referred to write these part was written in 1993. In 1995 Andrew Wiles, with some help from Richard Taylor, proved the Taniyama-Shimura-Weil conjecture for all semistable elliptic curves, which he used to prove Fermat's Last Theorem, and the full Taniyama-Shimura-Weil conjecture was finally proved by Breuil, Conrad, Diamond and Taylor. Building on Wiles's work, they incrementally chipped away at the remaining cases until the full result was proved in 1999. Nowadays, it should be called "Modularity theorem" instead of "Taniyama-Weil conjecture". [12]

6 Summation: What can I say

Born from computing the perimeter of ellipse, the theory of elliptic curve come to us with dramatic background. It firstly grew in the field of analysis, helped Gauss calculate π by the Gauss AGM, and was then adapted by the doubtless talent Ramanujan. Ramanujan took up his function and his differential equations to make it known to the world of Mathematics.

Ramanujan provides us with miscellaneous result. At that time, "$\tau-$function", "P, Q, R function", "$\phi-$function" are given. The famous result $\tau\left(n\right) \equiv \sigma_{11}\left(n\right) [691]$ attracts lots of rookie like me to learn about it nowadays. However, even talents like Ramanujan can only know a small corner of the whole theory. People still don't know a lot, for example, whether $\tau \neq 0$. There is still mystery to be revealed.

Jacobi knowed the $\Theta-$function too, he derived the Jacobi Triple Identity, whose first proof was given by Ramanujan, and then a simplified one by Euler. However, a much easier one was given one centuries later. E.M. Wright give a combinatorial proof in 1965. Maybe today, a children attending the $\pi-$festival should be able to work it out by some hints, but it is intellegent to Wright to find out it first.

At the same time, one want to calculate the length of a lemniscate, in this topic, the analyzation of the classical sine functionn helped a lot. However, finally this lead to the same road where Elliptic integral goes. In this period of time, Weierstrass drewed a beautiful $\wp$: the equation $\left(\wp'\right)^2 = 4\wp^3 - g_2\wp - g_3$ begin to show the shape of the elliptic curve nowadays. By the mapping $z \to \left(z^3\wp, z^3\wp', z^3\right)$ they led elliptic function from the field of Analysis to Geometry.

In the 19th century, by the development of modular form, people saw the great potential of elliptic curve and begin to use it to solve problems in the number theory. The most famous story is the proof of Fermat Last Theorem. And in my opinion, the theorem of Tunnell on the congruent number is also a great work. From Swinnerton-Dyer conjecture to Coates-Wiles theorem, from Taniyama-Shimura-Weil conjecture to Modularity Theorem, the tools in the end of 20th century were utilized to solve the problem in the age of ancient Greece. These give people great confidence: for a long time, the Goldbach Conjecture, the Fermat Last Conjecture and some very old conjectures haven't been proved yet, they looks like a very heavy stone lies on the seedling of maths. However, by the time goes on, we are glad to see that there are some new breaches on the stone. There is hopeful to see a lot of unsolved problems solved in my lifetime.

It's such a pity that I can't finish the proof of the Tunnell Theorem due to the limitation of space and time. There are still lots of topics I want to talk about: Hecke character, the computation of $\Theta-$function, modular forms of half integer weight, how the Bridgeland Deformation Theorem help analyzing the modular space of elliptic curve, and how Professor Yanghui He use the technique of machine learning to "hear the murmuring" of elliptic curve. Maybe some these would be given in the next 50-page paper of mathematical history, but not this time.

At the end of the paper, I would like to cite a famous saying of Hilbert that:

We must know. We shall know.

7 bibliography

References

[1] Bruce C. Berndt and Ken Ono. Ramanujan's unpublished manuscript on the partition and tau functions with proofs and commentary. In Dominique Foata and Guo-Niu Han, editors, *The Andrews Festschrift*, pages 39–110, Berlin, Heidelberg, 2001. Springer Berlin Heidelberg.

[2] J. Coates and A. Wiles. On the conjecture of Birch and Swinnerton-Dyer. *Invent. Math.*, 39(3):223–251, 1977.

[3] Leonard Eugene Dickson. *History of the theory of numbers*, volume II. Carnegie Institution of Washington, 1920.

[4] Peter B. Borwein Jonathan M. Borwein. *Pi and the AGM: a study in analytic number theory and computational complexity.* Canadian Mathematical Society series of monographs and advanced texts , Monographies et etudes de la Societe mathematique du Canada. Wiley, 1998.

[5] Shaun Cooper K Venkatachaliengar. *Development of Elliptic Functions According to Ramanujan*, volume 6 of *Monographs in Number Theory.* World Scientific, 2011.

[6] Felix Klein. *Development of mathematics in the 19th century.* Lie groups 9. Math Sci Press, 1979.

[7] Neal Koblitz. *Introduction to Elliptic Curves and Modular Forms.* Graduate Texts in Mathematics. Springer New York, NY, 2 edition, 1993.

[8] LMFDB. A history of l-functions. `https://www.lmfdb.org/knowledge/show/lfunction.history`.

[9] Jean Pierre Serre. *A course in arithmetic.* Graduate Texts in Mathematics. Springer, 1973.

[10] Carl Ludwig Siegel. Elliptic functions and uniformization theory. In *Topics in Complex Function Theory*, 1969.

[11] wikipedia. Modular form. https://en.wikipedia.org/wiki/Modular_form.

[12] wikipedia. Modularity theorem. https://en.wikipedia.org/wiki/Modularity_theorem.

[13] wikipedia. Ramanujan tau function. https://en.wikipedia.org/wiki/Ramanujan_tau_function.

[14] wikipedia. Weierstrass elliptic function. https://en.wikipedia.org/wiki/Weierstrass_elliptic_function.

[15] E. M. Wright. An enumerative proof of an identity of jacobi. *Journal of the London Mathematical Society*, s1-40(1):55–57, 1965.

[16] Jinhee Yi. Theta-function identities and the explicit formulas for theta-function and their applications. *Journal of Mathematical Analysis and Applications*, 292(2):381–400, 2004.

[17] rainbow zyop Zhihu. Gauss and agm(iv-1). https://zhuanlan.zhihu.com/p/32413565/.