y-coordinates of elliptic curves

Dong Hwa Shin

Department of Mathematical Sciences
KAIST

January 11, 2010

Outline

1. Introduction
   - Elliptic integrals
   - What does E look like?
2. Elliptic curves
   - Projective plane curves
   - Elliptic functions
   - Elliptic curves
3. Modular curves
   - Modular curve of level N
   - Compactification
4. Elliptic curves and modular forms
   - Modular forms
   - Modular functions from generic elliptic curve
5. Application to number theory
   - Solving Diophantine equations
   - Construction of class fields

Outline

1. Introduction
   - Elliptic integrals
   - What does E look like?
2. Elliptic curves
   - Projective plane curves
   - Elliptic functions
   - Elliptic curves
3. Modular curves
   - Modular curve of level N
   - Compactification
4. Elliptic curves and modular forms
   - Modular forms
   - Modular functions from generic elliptic curve
5. Application to number theory
   - Solving Diophantine equations
   - Construction of class fields

Projective spaces

Denote

$$\mathbb{P}^2(\mathbb{C}) = \text{projective plane} = \left\{ [X : Y : Z] \ : \ X,\ Y,\ Z \in \mathbb{C} \text{ not all zero} \right\}$$

with the homogeneous coordinates $X,\ Y,\ Z$ and affine coordinates

$$x = \frac{X}{Z} \quad \text{and} \quad y = \frac{Y}{Z}.$$

Furthermore, let

$$\mathbb{P}^1(\mathbb{C}) = \text{projective line} = \left\{ [X : Y] \ : \ X,\ Y \in \mathbb{C} \text{ not all zero} \right\}$$

which can be identified with a Riemann sphere

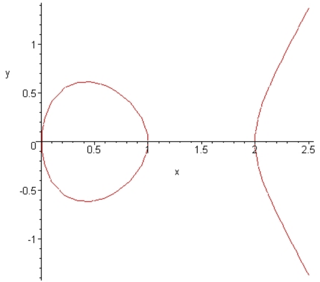
$$\widehat{\mathbb{C}} = \mathbb{C} \cup \{\infty\}.$$

Loci in $\mathbb{P}^2(\mathbb{C})$

Let E be a locus in $\mathbb{P}^2(\mathbb{C})$ defined by

$$E \; : \; y^2 = x(x-1)(x-\lambda) \quad \text{for } \lambda \neq 0, \; 1$$

with the extra point $O = [0:1:0]$. For example,



$E \; : \; y^2 = x(x-1)(x-2)$ in $\mathbb{R}^2$

Elliptic integrals

The differential form

$$\omega = \frac{dx}{y}$$

is holomorphic on E. Suppose that we try to define a map

$$\begin{array}{ccc} E & \xrightarrow{?} & \mathbb{C} \\ P & \mapsto & \displaystyle\int_O^P \omega \end{array}$$

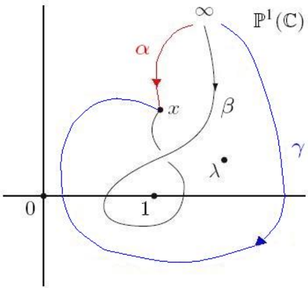
where the integral is along some path connecting O and P.

Namely, we are attempting to compute the (complex) line integral

$$\int_\infty^x \frac{dt}{\sqrt{t(t-1)(t-\lambda)}}$$

which is called an elliptic integral.

Because the square-root is not single valued, the integral is not path-independent. For example,

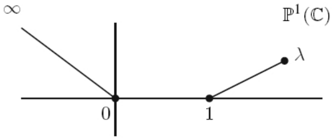


Three paths in $\mathbb{P}^1(\mathbb{C})$

three integrals $\int_\alpha \omega$, $\int_\beta \omega$, $\int_\gamma \omega$ are not equal.

Branch cuts

In order to make the integral well-defined, it is necessary to make branch cuts as follows:



Branch cuts in $\mathbb{P}^1(\mathbb{C})$

Then, then integrals will be path-independent on the complement of the branch cuts.

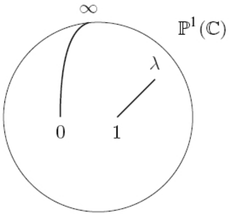
Outline

1. Introduction
   - Elliptic integrals
   - What does E look like?
2. Elliptic curves
   - Projective plane curves
   - Elliptic functions
   - Elliptic curves
3. Modular curves
   - Modular curve of level N
   - Compactification
4. Elliptic curves and modular forms
   - Modular forms
   - Modular functions from generic elliptic curve
5. Application to number theory
   - Solving Diophantine equations
   - Construction of class fields

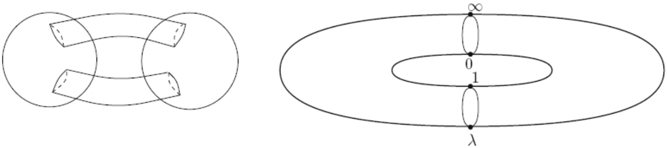
More generally, ((1) $\sim$ (10))

(1) Take two copies of $\mathbb{P}^1(\mathbb{C})$.

(2) Make the indicated branch cuts:



(3) Glue them together along the branch cuts to form a Riemann surface (or, a torus) as follows:



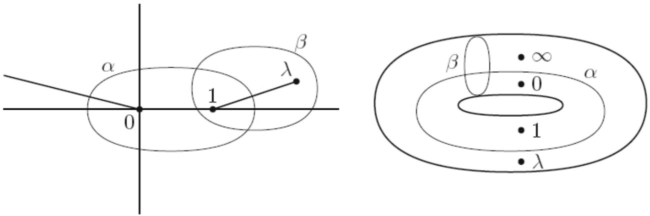
(4) On this torus, one should study the integral $\int dt/\sqrt{t(t-1)(t-\lambda)}$.

(5) In fact, elliptic curves first arose when people began to study such "elliptic integrals" which is related to the arc-length of an ellipse.

(6) The indeterminacy comes from integrating around non-contractible loops on the torus.

(7) So we introduce two complex numbers, which are called periods of E,

$$\omega_1 = \int_\alpha \omega \quad \text{and} \quad \omega_2 = \int_\beta \omega.$$



Paths on $\mathbb{P}^1(\mathbb{C})$ and on the torus

(8) Now the integral

$$\int_O^P \omega$$

is well-defined up to addition of a number of the form $n_1\omega_1 + n_2\omega_2$ for $n_1,\ n_2 \in \mathbb{Z}$.

(9) Let

$$\Lambda = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2.$$

Thus we have shown that there is a well-defined map

$$\begin{array}{ccc} E & \longrightarrow & \mathbb{C}/\Lambda \\ P & \mapsto & \displaystyle\int_O^P \omega \pmod{\Lambda}. \end{array}$$

(10) If Λ is a lattice in $\mathbb{C}$, then the quotient space $\mathbb{C}/\Lambda$ will be a Riemann surface.
Then by using the translation invariance of ω,
one can verify that the above map is a complex analytic isomorphism.

Outline

1. Introduction
   - Elliptic integrals
   - What does E look like?
2. Elliptic curves
   - Projective plane curves
   - Elliptic functions
   - Elliptic curves
3. Modular curves
   - Modular curve of level N
   - Compactification
4. Elliptic curves and modular forms
   - Modular forms
   - Modular functions from generic elliptic curve
5. Application to number theory
   - Solving Diophantine equations
   - Construction of class fields

Outline

1. Introduction
   - Elliptic integrals
   - What does E look like?
2. Elliptic curves
   - Projective plane curves
   - Elliptic functions
   - Elliptic curves
3. Modular curves
   - Modular curve of level N
   - Compactification
4. Elliptic curves and modular forms
   - Modular forms
   - Modular functions from generic elliptic curve
5. Application to number theory
   - Solving Diophantine equations
   - Construction of class fields

Covers of $\mathbb{P}^2(\mathbb{C})$

The projective plane

$$\mathbb{P}^2(\mathbb{C}) = (\mathbb{C}^3 - \{0\})/\mathbb{C}^*$$

is a Hausdorff compact space which can be covered by the three open sets

$$\begin{aligned} U_0 &= \Big\{[X:Y:Z] \ : \ X \neq 0\Big\} \\ U_1 &= \Big\{[X:Y:Z] \ : \ Y \neq 0\Big\} \\ U_2 &= \Big\{[X:Y:Z] \ : \ Z \neq 0\Big\}. \end{aligned}$$

Each U_i is homeomorphic to $\mathbb{C}^2$, for example

$$\begin{array}{ccc} U_2 & \xrightarrow{\approx} & \mathbb{C}^2 \\ [X:Y:Z] & \mapsto & (x,\ y) = (X/Z,\ Y/Z). \end{array}$$

Projective plane curve V

For a (nonconstant) homogeneous polynomial $F(X, Y, Z)$, consider its locus

$$V = \left\{ [X : Y : Z] \in \mathbb{P}^2(\mathbb{C}) \ : \ F(X, Y, Z) = 0 \right\}.$$

The intersection

$$V_i = V \cap U_i \qquad (i = 0,\ 1,\ 2)$$

is exactly an affine plane curve when transported to $\mathbb{C}^2$.

For example, V_2 is homeomorphic to the affine plane curve described by the equation

$$f(x,\ y) = F(x,\ y,\ 1) = 0.$$

Nonsingular F defines a compact Riemann surface

$F(X,Y,Z)$ is said to be nonsingular if there are no common solutions (in $\mathbb{P}^2(\mathbb{C})$) to the system of equations

$$F = \frac{\partial F}{\partial X} = \frac{\partial F}{\partial Y} = \frac{\partial F}{\partial Z} = 0.$$

Then one can obtain

$$F \text{ is nonsingular} \iff \text{each } V_i \text{ is a smooth affine plane curve (in } \mathbb{C}^2\text{)}.$$

If $F(X,Y,Z)$ is a nonsingular (irreducible) polynomial defining the projective plane curve V, then

(1) each V_i ($i = 0,\ 1,\ 2$) is a smooth (irreducible) affine plane curve, and hence is a Riemann surface;

(2) at each point of V_i we take a ratio of the homogeneous coordinates as a local coordinate;

(3) then V becomes a compact Riemann surface as a closed subset of compact $\mathbb{P}^2(\mathbb{C})$.

Outline

1. Introduction
   - Elliptic integrals
   - What does E look like?
2. Elliptic curves
   - Projective plane curves
   - Elliptic functions
   - Elliptic curves
3. Modular curves
   - Modular curve of level N
   - Compactification
4. Elliptic curves and modular forms
   - Modular forms
   - Modular functions from generic elliptic curve
5. Application to number theory
   - Solving Diophantine equations
   - Construction of class fields

Elliptic functions

Let Λ be a lattice in $\mathbb{C}$, that is,

$$\Lambda = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2 \quad \text{for some } \mathbb{R}\text{-basis } \{\omega_1,\ \omega_2\} \text{ of } \mathbb{C}.$$

We often write $\Lambda = [\omega_1,\ \omega_2]$.

An elliptic function (relative to Λ) is a meromorphic functions $f(z)$ on $\mathbb{C}$ which satisfies

$$f(z+\omega) = f(z) \quad \text{for all } \omega \in \Lambda,\ z \in \mathbb{C}.$$

(1) We can view elliptic functions as meromorphic functions on the torus $\mathbb{C}/\Lambda$.

(2) Hence an elliptic function with no poles is constant.

(3) The field of all such functions is denoted $\mathbb{C}(\Lambda)$.

Weierstrass functions

The Weierstrass $\wp$-function (relative to Λ) is defined by the series

$$\wp(z;\ \Lambda) = \frac{1}{z^2} + \sum_{\omega \in \Lambda - \{0\}} \left(\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2} \right) \qquad (z \in \mathbb{C}).$$

Clearly, $\wp(z;\ \Lambda) = \wp(-z;\ \Lambda)$ (that is, $\wp(z;\ \Lambda)$ is an even function).

By termwise differentiation (w.r.t. z) we get

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

which is obviously an elliptic function.

$\wp(z;\ \Lambda)$ is an elliptic function

(1) Let $\omega \in \Lambda$. Integrating

$$\wp'(z+\omega;\ \Lambda) = \wp'(z;\ \Lambda) \qquad (z \in \mathbb{C} - \Lambda)$$

yields

$$\wp(z+\omega;\ \Lambda) = \wp(z;\ \Lambda) + c(\omega) \quad \text{for some } c(\omega) \text{ independent of } z.$$

(2) Letting $z = -\omega/2$ we get that

$$\begin{aligned} \wp(\omega/2;\ \Lambda) &= \wp(-\omega/2;\ \Lambda) + c(\omega) \\ &= \wp(\omega/2;\ \Lambda) + c(\omega) \quad \text{because } \wp \text{ is even,} \end{aligned}$$

which shows $c(\omega) = 0$.

(3) Hence $\wp(z;\ \Lambda)$ is an elliptic function, too.

(4) As is well-known

$$\mathbb{C}(\Lambda) = \mathbb{C}\Big(\wp(z;\ \Lambda),\ \wp'(z;\ \Lambda)\Big).$$

Laurent serious for $\wp(z;\ \Lambda)$

(1) For a lattice Λ in $\mathbb{C}$, the Eisenstein series of weight $2k$ (relative to Λ) is the series

$$G_{2k}(\Lambda) = \sum_{\omega \in \Lambda - \{0\}} \frac{1}{\omega^{2k}}.$$

Then for all integer $k > 1$, $G_{2k}(\Lambda)$ is absolutely convergent.

(2) Let $z \in \mathbb{C}$ and $\omega \in \Lambda$. If $|z| < |\omega|$, then

$$\begin{aligned} \frac{1}{(z-\omega)^2} - \frac{1}{\omega^2} &= \frac{1}{\omega^2}\left(\frac{1}{(1-z/w)^2} - 1\right) \\ &= \sum_{n=1}^{\infty}(n+1)\frac{z^n}{\omega^{n+2}}. \end{aligned}$$

(3) Hence the Laurent series for $\wp(z;\ \Lambda)$ about $z = 0$ is given by

$$\wp(z;\ \Lambda) = \frac{1}{z^2} + \sum_{\omega \in \Lambda - \{0\}} \left(\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2}\right) = \frac{1}{z^2} + \sum_{k=1}^{\infty}(2k+1)G_{2k+2}(\Lambda)z^{2k}.$$

Relation between $\wp(z;\ \Lambda)$ and $\wp'(z;\ \Lambda)$

(1) Write out the first few terms in various Laurent expansions:

$$\begin{aligned} \wp'(z;\ \Lambda)^2 &= \frac{4}{z^6} - 24G_4(\Lambda)\frac{1}{z^2} - 80G_6(\Lambda) + \cdots \\ \wp(z;\ \Lambda)^3 &= \frac{1}{z^6} + 9G_4(\Lambda)\frac{1}{z^2} + 15G_6(\Lambda) + \cdots \\ \wp(z;\ \Lambda) &= \frac{1}{z^2} + 3G_4(\Lambda)z^2 + \cdots . \end{aligned}$$

(2) Comparing these, we see that the function

$$f(z) = \wp'(z;\ \Lambda)^2 - 4\wp(z;\ \Lambda)^3 + 60G_4(\Lambda)\wp(z;\ \Lambda) + 140G_6(\Lambda)$$

is holomorphic around $z = 0$ and vanishes at $z = 0$.

(3) Since $\wp(z;\ \Lambda)$ and $\wp'(z;\ \Lambda)$ are holomorphic away from Λ, so does $f(z)$.

(4) Hence $f(z)$ is a holomorphic functions on $\mathbb{C}/\Lambda$, from which we conclude that $f(z)$ is identically zero.

Parametrization of a projective curve E

It is standard to set

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

$$\Delta(\Lambda) = g_2(\Lambda)^3 - 27g_3(\Lambda)^2, \qquad j(\Lambda) = \frac{g_2(\Lambda)^3}{\Delta(\Lambda)}.$$

Let E be the (projective) curve defined by the (affine) equation

$$E \ : \ y^2 = 4x^3 - g_2(\Lambda)x - g_3(\Lambda).$$

Then the map

$$\begin{array}{rccl} \varphi \ : \ \mathbb{C}/\Lambda & \longrightarrow & E \subset \mathbb{P}^2(\mathbb{C}) & \\ z \pmod{\Lambda} & \mapsto & \begin{cases} [\wp(z;\ \Lambda) : \wp'(z;\ \Lambda) : 1] & \text{if } z \notin \Lambda \\ [0 : 1 : 0] & \text{if } z \in \Lambda \end{cases} \end{array}$$

becomes an isomorphism between compact Riemann surfaces.

Outline

1 Introduction
- Elliptic integrals
- What does E look like?

2 Elliptic curves
- Projective plane curves
- Elliptic functions
- Elliptic curves

3 Modular curves
- Modular curve of level N
- Compactification

4 Elliptic curves and modular forms
- Modular forms
- Modular functions from generic elliptic curve

5 Application to number theory
- Solving Diophantine equations
- Construction of class fields

Elliptic curve E as a projective plane curve

An elliptic curve E (over $\mathbb{C}$) is a projective plane curve defined by the (affine) equation

$$E \ : \ y^2 = 4x^3 - g_2 x - g_3$$

with extra point $O = [0 : 1 : 0]$ where

$$g_2, \ g_3 \in \mathbb{C} \quad \text{with } \Delta = g_2^3 - 27g_2^2 \neq 0.$$

The above equation is called a Weierstrass equation for E.

The fact $\Delta \neq 0$ implies that E is smooth.

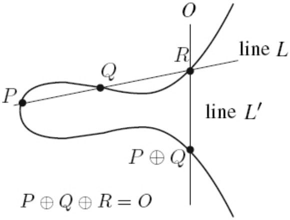
Group structure on E

For an elliptic curve E, let P and $Q \in E$.

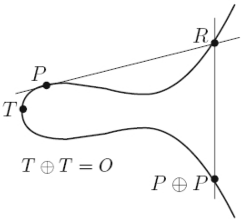
(1) Let L be the line connecting P and Q, and R be the third point of intersection of L with the curve E.

(2) Let L' be the line connecting O and R.

(3) Then $P \oplus Q$ is the point s.t. L' intersects E at O, R and $P \oplus Q$.



Addition of distinct points



Adding a point to itself

Then E becomes an abelian group with identity O, and hence it is a complex Lie group.

Uniformization theorem

The uniformization theorem asserts that for $g_2,\ g_3 \in \mathbb{C}$ with

$$g_2^3 - 27g_3^2 \neq 0,$$

there exists a unique lattice Λ in $\mathbb{C}$ such that

$$g_2 = g_2(\Lambda) \text{ and } g_3 = g_3(\Lambda).$$

Hence one can show that the isomorphism

$$\begin{array}{rcl} \varphi\ :\ \mathbb{C}/\Lambda & \xrightarrow{\sim} & E\ :\ y^2 = 4x^3 - g_2x - g_3 \\ z & \mapsto & [\wp(z;\ \Lambda) : \wp'(z;\ \Lambda) : 1] \end{array}$$

between compact Riemann surfaces is also a group homomorphism (by using some properties of divisors on E).
That is, φ is a complex analytic isomorphism between complex Lie groups.

Complex multiplication

Let E be an elliptic curve parametrized by using a lattice $\Lambda = [\omega_1,\ \omega_2]$ in $\mathbb{C}$.

(1) The complex analytic endomorphisms of E correspond to the multiplication maps of $\mathbb{C}/\Lambda$ onto itself.

(2) Let $\alpha \in \mathbb{C}$. Note that

$$\text{the multiplication by } \alpha : \mathbb{C}/\Lambda \to \mathbb{C}/\Lambda \text{ is well-defined} \iff \alpha\Lambda \subset \Lambda.$$

(3) Such α's form a ring, which contains $\mathbb{Z}$.
If the ring is strictly larger than $\mathbb{Z}$, E is said to have complex multiplication.

(4) It is well-known that

$$E \text{ has complex multiplication} \iff \omega_1/\omega_2 \text{ is imaginary quadratic}.$$

Outline

1. Introduction
   - Elliptic integrals
   - What does E look like?
2. Elliptic curves
   - Projective plane curves
   - Elliptic functions
   - Elliptic curves
3. Modular curves
   - Modular curve of level N
   - Compactification
4. Elliptic curves and modular forms
   - Modular forms
   - Modular functions from generic elliptic curve
5. Application to number theory
   - Solving Diophantine equations
   - Construction of class fields

Outline

1 Introduction
- Elliptic integrals
- What does E look like?

2 Elliptic curves
- Projective plane curves
- Elliptic functions
- Elliptic curves

3 Modular curves
- Modular curve of level N
- Compactification

4 Elliptic curves and modular forms
- Modular forms
- Modular functions from generic elliptic curve

5 Application to number theory
- Solving Diophantine equations
- Construction of class fields

Action of $SL_2(\mathbb{Z})$ on $\mathfrak{H}$

Let

$$\mathfrak{H} = \text{complex upper half-plane} = \left\{\tau \in \mathbb{C} : \mathrm{Im}(\tau) > 0\right\}$$

which inherits the Euclidean topology as a subspace of $\mathbb{R}^2$. Then

$$SL_2(\mathbb{Z}) = \text{modular group} = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \ : \ a,\ b,\ c,\ d \in \mathbb{Z},\ ad - bc = 1 \right\}$$

acts on $\mathfrak{H}$ by linear fractional transformation, namely

$$\begin{array}{rccc} \gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} : & \mathfrak{H} & \longrightarrow & \mathfrak{H} \\ & \tau & \mapsto & \gamma(\tau) = \dfrac{a\tau + b}{c\tau + d}. \end{array}$$

Note that

$$\gamma_1,\ \gamma_2 \in SL_2(\mathbb{Z}) \text{ give rise to the same action on } \mathfrak{H} \iff \gamma_1 = \pm \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right) \gamma_2.$$

Orbit space $Y(N)$

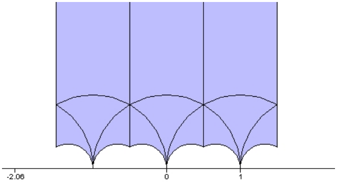
For a positive integer N, let

$$\Gamma(N) = \text{(principal) congruence subgroup of level } N = \left\{\gamma \in \mathrm{SL}_2(\mathbb{Z}) \;:\; \gamma \equiv \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \pmod N\right\}.$$

For simplicity, write $\Gamma = \Gamma(N)$. The natural projection

$$\begin{aligned} \pi \;:\; \mathfrak{H} &\longrightarrow Y(N) = \Gamma\backslash\mathfrak{H} = \left\{\Gamma\tau \;:\; \tau \in \mathfrak{H}\right\} \\ \tau &\longmapsto \Gamma\tau \end{aligned}$$

gives $Y(N)$ the quotient topology so that π is an open mapping.



Fundamental domain of $Y(3)$

Isotropy subgroup Γ_z

For each point $z \in \mathfrak{H}$, we denote

$$\Gamma_z = \text{isotropy subgroup of } z = \{\gamma \in \Gamma \ : \ \gamma(z) = z\}.$$

In particular, if $|\pm\Gamma_z/\{\pm 1_2\}| > 1$, then z is called an elliptic point (for Γ).

Since Γ is discrete, we can take a neighborhood U of z s.t.

$$\left\{\gamma \in \Gamma : \gamma(U) \cap U \neq \emptyset\right\} = \Gamma_z.$$

Such a neighborhood U has no elliptic points except possibly z.

Local coordinate φ

W define a map

$$\begin{array}{rcl} \psi : U & \longrightarrow & \mathbb{C} \\ \tau & \mapsto & \left(\dfrac{\tau - z}{\tau - \bar{z}}\right)^{|\pm\Gamma_z/\{\pm 1_2\}|} \end{array}.$$

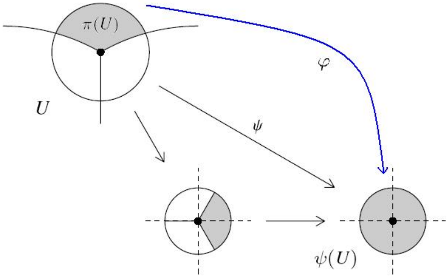
Its image $\psi(U)$ is an open subset of $\mathbb{C}$ by the open mapping theorem, and there exists a natural bijection $\varphi : \pi(U) \to \psi(U)$ s.t.

$$\begin{tikzcd} & U \arrow[dl, "\pi"'] \arrow[dr, "\psi"] & \\ \pi(U) \arrow[rr, "\varphi"] & & \psi(U) \end{tikzcd}$$

The map φ becomes a local coordinate, that is,

(1) the coordinate neighborhood about $\pi(z)$ in $Y(N)$ is $\pi(U)$;

(2) the map $\varphi : \pi(U) \to \psi(U)$ is a homeomorphism.



Local coordinate at an ellpitic point

Since the transition maps between these coordinate charts are holomorphic, $Y(N)$ can be viewed as a Riemann surface, which is called the modular curve of level N.

Outline

1 Introduction
- Elliptic integrals
- What does E look like?

2 Elliptic curves
- Projective plane curves
- Elliptic functions
- Elliptic curves

3 Modular curves
- Modular curve of level N
- Compactification

4 Elliptic curves and modular forms
- Modular forms
- Modular functions from generic elliptic curve

5 Application to number theory
- Solving Diophantine equations
- Construction of class fields

Extended space $\mathfrak{H}^*$

Consider the extended upper half-plane

$$\mathfrak{H}^* = \mathfrak{H} \cup \underbrace{\mathbb{Q} \cup \{\infty\}}_{\text{cusps}}.$$

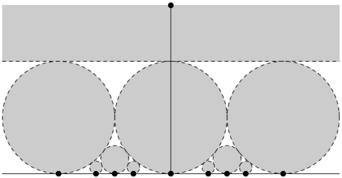
For any $M > 0$ let

$$\mathcal{N}_M = \left\{ \tau \in \mathfrak{H} \ : \ \operatorname{Im}(\tau) > M \right\}.$$

Adjoin the sets

$$\gamma(\mathcal{N}_M \cup \{\infty\}) \text{ for all } M > 0 \text{ and } \gamma \in \mathrm{SL}_2(\mathbb{Z})$$

to the usual open sets of $\mathfrak{H}$ to serve as a basis of neighborhoods of the cusps, and take the resulting topology on $\mathfrak{H}^*$.



Neighborhoods of cusps

Compactification of $Y(N)$

Now consider the extended quotient

$$X(N) = \Gamma \backslash \mathfrak{H}^* = Y(N) \cup \Gamma \backslash (\mathbb{Q} \cup \{\infty\}),$$

which is Hausdorff, connected and compact.
Give $X(N)$ the quotient topology and extend the natural projection to $\pi : \mathfrak{H}^* \to X(N)$.

To make $X(N)$ a compact Riemann surface we have to give it complex charts.

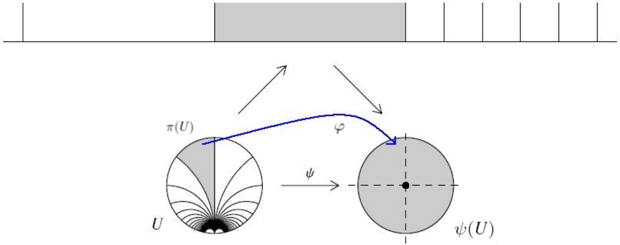
(1) For $z \in \mathfrak{H}$ we just retain the complex chart of $Y(N)$.

(2) For a cusp $s \in \mathbb{Q} \cup \{\infty\}$ take a matrix $\gamma \in \mathrm{SL}_2(\mathbb{Z})$ s.t. $\gamma(s) = \infty$, and define a map

$$\begin{array}{rcl} \psi \ : \ U = \gamma^{-1}(\mathcal{N}_2 \cup \{\infty\}) & \longrightarrow & \mathbb{C} \\ \tau & \mapsto & e^{2\pi i \gamma(\tau)/|\mathrm{SL}_2(\mathbb{Z})_\infty / \pm\Gamma_\infty|}. \end{array}$$

The image $\psi(U)$ is an open subset of $\mathbb{C}$, and
there exists a homeomorphism $\varphi : \pi(U) \to \psi(U)$ s.t.

$$\begin{tikzcd}
 & U \arrow[dl, "\pi"'] \arrow[dr, "\psi"] & \\
\pi(U) \arrow[rr, "\varphi"] & & \psi(U)
\end{tikzcd}$$



Complex chart at a cusp

It is routine to check that the transition maps between charts of $X(N)$ are holomorphic.
Therefore $X(N)$ is now a compact Riemann surface, also called the modular curve of level N.

Outline

1. Introduction
   - Elliptic integrals
   - What does E look like?
2. Elliptic curves
   - Projective plane curves
   - Elliptic functions
   - Elliptic curves
3. Modular curves
   - Modular curve of level N
   - Compactification
4. Elliptic curves and modular forms
   - Modular forms
   - Modular functions from generic elliptic curve
5. Application to number theory
   - Solving Diophantine equations
   - Construction of class fields

Outline

1. Introduction
   - Elliptic integrals
   - What does E look like?
2. Elliptic curves
   - Projective plane curves
   - Elliptic functions
   - Elliptic curves
3. Modular curves
   - Modular curve of level N
   - Compactification
4. Elliptic curves and modular forms
   - Modular forms
   - Modular functions from generic elliptic curve
5. Application to number theory
   - Solving Diophantine equations
   - Construction of class fields

Modular forms of level N and weight k

For $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z})$ and $k \in \mathbb{Z}$,
we define the weight-k operator $\cdot|[\gamma]_k$ on functions $f : \mathfrak{H} \to \widehat{\mathbb{C}}$ as

$$f(\tau)|[\gamma]_k = (c\tau + d)^{-k} f\big(\gamma(\tau)\big) \qquad (\tau \in \mathfrak{H}).$$

Then it is easily verified that for $\gamma_1,\ \gamma_2 \in \mathrm{SL}_2(\mathbb{Z})$

$$f|[\gamma_1\gamma_2]_k = \Big(f|[\gamma_1]_k\Big)|[\gamma_2]_k.$$

A function $f : \mathfrak{H} \to \widehat{\mathbb{C}}$ is a modular form of level $N(\geq 1)$ and weight k if

(1) f is meromorphic on $\mathfrak{H}$;

(2) f is invariant under $\cdot|[\gamma]_k$ for all $\gamma \in \Gamma(N)$;

(3) $f|[\alpha]_k$ is meromorphic at ∞ for all $\alpha \in \mathrm{SL}_2(\mathbb{Z})$.

Meromorphicity at ∞

(1) To discuss meromorphicity of $f|[\alpha]_k$ at ∞ we note that

- $\Gamma(N)$ is a normal subgroup of $\mathrm{SL}_2(\mathbb{Z})$;
- $\left(\begin{smallmatrix} 1 & N \\ 0 & 1 \end{smallmatrix}\right) \in \Gamma(N)$.

So we get

$$\begin{pmatrix} 1 & N \\ 0 & 1 \end{pmatrix} = \alpha^{-1}\gamma\alpha \quad \text{for some } \gamma \in \Gamma(N).$$

(2) Observe that

$$\begin{aligned} \Big(f|[\alpha]_k\Big)(\tau+N) &= \Big(f|[\alpha]_k\Big)|[\left(\begin{smallmatrix} 1 & N \\ 0 & 1 \end{smallmatrix}\right)]_k \\ &= \Big(f|[\alpha]_k\Big)|[\alpha^{-1}\gamma\alpha]_k \\ &= f|[\alpha\alpha^{-1}\gamma\alpha]_k = f|[\alpha]_k, \end{aligned}$$

which shows that $f|[\alpha]_k$ has period N.

(4) Let

$$q = e^{2\pi i\tau} \qquad (\tau \in \mathfrak{H}).$$

Then $f|[\alpha]_k$ is a function w.r.t. $q^{\frac{1}{N}}$ on some punctured disc about $q = 0$. If the function has a Laurent series w.r.t. $q^{\frac{1}{N}}$, namely

$$f|[\alpha]_k = \sum_{n \geq m}^{\infty} c_n \left(q^{\frac{1}{N}}\right)^n \qquad (c_n \in \mathbb{C})$$

for some integer m, then $f|[\alpha]_k$ is said to be meromorphic at ∞.

(5) The above series is conventionally called the Fourier expansion of $f|[\alpha]_k$ at ∞ (or, f at $\alpha(\infty)$) with Fourier coefficients c_n.

(6) Modular forms of level N and weight 0 are called modular functions of level N. They are exactly meromorphic functions defined on the modular curve $X(N)$ and vice versa.

Example

(1) Let

$$\Lambda = [\tau,\ 1] \quad \text{with } \tau \in \mathfrak{H}$$

be a lattice. Recall the constants (relative to Λ)

$$\begin{aligned}
g_2(\Lambda) &= 60 \sum_{(m,\,n)\in\mathbb{Z}^2-\{(0,\,0)\}} \frac{1}{(m\tau+n)^4} \\
g_3(\Lambda) &= 140 \sum_{(m,\,n)\in\mathbb{Z}^2-\{(0,\,0)\}} \frac{1}{(m\tau+n)^6} \\
\Delta(\Lambda) &= g_2(\Lambda)^3 - 27g_3(\Lambda)^2 \\
j(\Lambda) &= \frac{g_2(\Lambda)^3}{\Delta(\Lambda)}.
\end{aligned}$$

(2) Regard τ as a variable on $\mathfrak{H}$, and let

$$\begin{aligned} g_2(\tau) &= g_2([\tau,\ 1]) \\ g_3(\tau) &= g_3([\tau,\ 1]) \\ \Delta(\tau) &= \Delta([\tau,\ 1]) \\ j(\tau) &= j([\tau,\ 1]). \end{aligned}$$

Directly from the definitions, for $\gamma \in \mathrm{SL}_2(\mathbb{Z})$ we have

$$\begin{aligned} g_2(\tau)|[\gamma]_4 &= g_2(\tau) \\ g_3(\tau)|[\gamma]_6 &= g_3(\tau) \\ \Delta(\tau)|[\gamma]_{12} &= \Delta(\tau) \\ j(\tau)|[\gamma]_0 &= j(\tau). \end{aligned}$$

(3) We have the product formula

$$\sin \pi\tau = \pi\tau \prod_{n=1}^{\infty} \left(1 - \frac{\tau}{n}\right)\left(1 + \frac{\tau}{n}\right).$$

Taking the logarithmic derivative yields

$$\pi \frac{\cos \pi\tau}{\sin \pi\tau} = \frac{1}{\tau} + \sum_{n=1}^{\infty} \left(\frac{1}{\tau - n} + \frac{1}{\tau + n}\right).$$

On the other hand, since

$$\cos \pi\tau = \frac{1}{2} q^{-\frac{1}{2}}(q+1) \quad \text{and} \quad \sin \pi\tau = \frac{1}{2i} q^{-\frac{1}{2}}(q-1),$$

we get

$$\pi \frac{\cos \pi\tau}{\sin \pi\tau} = \pi i \frac{q+1}{q-1} = \pi i - 2\pi i \sum_{\nu=0}^{\infty} q^{\nu}.$$

(4) Differentiating two expressions for $\pi \frac{\cos \pi\tau}{\sin \pi\tau}$ repeatedly yields

$$(-1)^{k-1}(k-1)! \sum_{n=-\infty}^{\infty} \frac{1}{(\tau-n)^k} = -\sum_{\nu=1}^{\infty} (2\pi i)^k \nu^{k-1} q^{\nu}.$$

We obtain from the above relation that

$$\begin{aligned}
g_2(\tau) &= (2\pi)^4 \frac{1}{12}\left(1 + 240 \sum_{n=1}^{\infty} (\sum_{d|n} d^3) q^n\right) \\
g_3(\tau) &= (2\pi)^6 \frac{1}{216}\left(1 - 504 \sum_{n=1}^{\infty} (\sum_{d|n} d^5) q^n\right) \\
\Delta(\tau) &= (2\pi)^{12} q \left(1 + \sum_{n=1}^{\infty} c_n q^n\right) \qquad (d_n \in \mathbb{Z}) \\
j(\tau) &= \frac{1}{q} + 744 + 196884q + 21493760q^2 + 864299970q^3 + 20245856256q^4 \\
&\quad +333202640600q^5 + 4252023300096q^6 + 44656994071935q^7 + \cdots .
\end{aligned}$$

(5) Hence all the $g_2(\tau)$, $g_3(\tau)$, $\Delta(\tau)$ and $j(\tau)$ are meromorphic at the cusp ∞ (which is the unique inequivalent cusp for $\mathrm{SL}_2(\mathbb{Z})$).
Therefore

$$\begin{array}{rcl} g_2(\tau) & = & \text{a modular form of level 1 and weight 4} \\ g_3(\tau) & = & \text{a modular form of level 1 and weight 6} \\ \Delta(\tau) & = & \text{a modular form of level 1 and weight 12} \\ j(\tau) & = & \text{a modular function of level 1.} \end{array}$$

(6) Note that $j(\tau)$ is holomorphic on $\mathfrak{H}$ and has simple pole at ∞.
Hence the map

$$\begin{array}{rcl} X(1) & \longrightarrow & \mathbb{P}^1(\mathbb{C}) \\ \tau & \mapsto & [j(\tau) : 1] \end{array}$$

is an isomorphism between two Riemann spheres. Therefore

$$\text{the field of all meromorphic functions on } X(1) = \mathbb{C}\Big(j(\tau)\Big).$$

Outline

1. Introduction
   - Elliptic integrals
   - What does E look like?
2. Elliptic curves
   - Projective plane curves
   - Elliptic functions
   - Elliptic curves
3. Modular curves
   - Modular curve of level N
   - Compactification
4. Elliptic curves and modular forms
   - Modular forms
   - Modular functions from generic elliptic curve
5. Application to number theory
   - Solving Diophantine equations
   - Construction of class fields

Change of variables

Let Λ be a lattice in $\mathbb{C}$ of the form

$$\Lambda = [\tau,\ 1] \quad \text{with } \tau \in \mathfrak{H}.$$

From the complex analytic isomorphism

$$\begin{array}{ccc} \mathbb{C}/\Lambda & \xrightarrow{\sim} & y^2 = 4x^3 - g_2(\tau)x - g_3(\tau) \\ z & \mapsto & [\wp(z;\ \Lambda) : \wp'(z;\ \Lambda) : 1], \end{array}$$

we have the relation

$$\wp'(z;\ \Lambda)^2 = 4\wp(z;\ \Lambda)^3 - g_2(\tau)\wp(z;\ \Lambda) - g_3(\tau).$$

Define

$$\eta(\tau) = \sqrt{2\pi}\zeta_8 q^{\frac{1}{24}} \prod_{n=1}^{\infty}(1 - q^n).$$

Diving both sides of the above Weierstrass equation by $\eta(\tau)^{12}$ we get

$$\left(\frac{\wp'(z;\ \Lambda)}{\eta(\tau)^6}\right)^2$$
$$= \frac{4\eta(\tau)^{60}}{g_2(\tau)^3 g_3(\tau)^3}\left(\frac{g_2(\tau)g_3(\tau)\wp(z;\ \Lambda)}{\eta(\tau)^{24}}\right)^3 - \frac{\eta(\tau)^{12}}{g_3(\tau)}\left(\frac{g_2(\tau)g_3(\tau)\wp(z;\ \Lambda)}{\eta(\tau)^{24}}\right) - \frac{g_3(\tau)}{\eta^{12}(\tau)}.$$

Write

$$z = r_1\tau + r_2 \quad \text{with } (r_1,\ r_2) \in \mathbb{R}^2 - \{(0,\ 0)\},$$

and set

$$x_{(r_1,\ r_2)}(\tau) = \frac{g_2(\tau)g_3(\tau)\wp(r_1\tau + r_2;\ \Lambda)}{\eta(\tau)^{24}} \quad \text{and} \quad y_{(r_1,\ r_2)}(\tau) = \frac{\wp'(r_1\tau + r_2;\ \Lambda)}{\eta(\tau)^6}.$$

Modular function field $\mathcal{F}_N$

For each positive integer N, let

$$\mathcal{F}_N = \text{the field of modular functions of level } N$$
$$\text{whose Fourier coefficients at } \infty \text{ belong to the } N^{\text{th}} \text{ cyclotomic field } \mathbb{Q}(e^{\frac{2\pi i}{N}}).$$

As is well-known,

(1) $\mathcal{F}_N \otimes \mathbb{C}$ is the field of meromorpic functions on $X(N)$;

(2) $\mathcal{F}_N$ is a Galois extension of $\mathcal{F}_1$;

(3) $\mathcal{F}_1 = \mathbb{Q}\Big(j(\tau)\Big)$;

(4) $\mathcal{F}_N = \mathbb{Q}\Big(e^{\frac{2\pi i}{N}},\ j(\tau),\ x_{(\frac{1}{N},\,0)}(\tau),\ x_{(0,\,\frac{1}{N})}(\tau)\Big)$ for $N > 1$.

Koo and Shin (2009) showed that

$$\mathcal{F}_N = \mathbb{Q}\left(j(\tau),\ e^{\frac{2\pi i}{N}} y_{(\frac{1}{N},\,0)}(\tau)^{\frac{4}{\gcd(4,\,N)}},\ y_{(0,\,\frac{1}{N})}(\tau)^{\frac{4}{\gcd(4,\,N)}}\right) \quad \text{for } N > 1.$$

Outline

1. Introduction
   - Elliptic integrals
   - What does E look like?
2. Elliptic curves
   - Projective plane curves
   - Elliptic functions
   - Elliptic curves
3. Modular curves
   - Modular curve of level N
   - Compactification
4. Elliptic curves and modular forms
   - Modular forms
   - Modular functions from generic elliptic curve
5. Application to number theory
   - Solving Diophantine equations
   - Construction of class fields

Outline

1. Introduction
   - Elliptic integrals
   - What does E look like?
2. Elliptic curves
   - Projective plane curves
   - Elliptic functions
   - Elliptic curves
3. Modular curves
   - Modular curve of level N
   - Compactification
4. Elliptic curves and modular forms
   - Modular forms
   - Modular functions from generic elliptic curve
5. Application to number theory
   - Solving Diophantine equations
   - Construction of class fields

History

(1) Fermat (1640 $\sim$ 1650s)

For a prime number p

$$\begin{aligned} p = x^2 + \ y^2 \text{ for } (x,\ y) \in \mathbb{Z}^2 &\iff p = 2 \text{ or } p \equiv 1 \pmod 4 \\ p = x^2 + 2y^2 \text{ for } (x,\ y) \in \mathbb{Z}^2 &\iff p = 2 \text{ or } p \equiv 1,\ 3 \pmod 8 \\ p = x^2 + 3y^2 \text{ for } (x,\ y) \in \mathbb{Z}^2 &\iff p = 3 \text{ or } p \equiv 1 \pmod 3. \end{aligned}$$

(2) Euler (1740s)

Euler conjectured for a prime number p

$$p = x^2 + 27y^2 \text{ for } (x,\ y) \in \mathbb{Z}^2 \iff \begin{cases} p \equiv 1 \pmod 3 \\ x^3 \equiv 2 \pmod p \text{ has an integer solution.} \end{cases}$$

(3) Gauss (*Disquisitiones Arithmeticae*, 1801)

$$p = x^2 + y^2 \text{ for } (x,\ y) \in \mathbb{Z}^2 \iff p = 2 \text{ or } p \text{ splits in } \mathbb{Q}(\sqrt{-1}).$$

(4) Weber (1880s)

$$\begin{aligned} & p = x^2 + (2^{\ell+1}y)^2 \ (\ell \geq 0) \text{ for } (x,\ y) \in \mathbb{Z}^2 \\ \iff \quad & p \text{ splits completely in } \mathbb{Q}(\sqrt{-1})\big(j(2^{\ell+1}\sqrt{-1})\big). \end{aligned}$$

(5) Hilbert, Deuring, Artin, Cohn, Stark (1970s)

They determined the primes p of the form $x^2 + ny^2$.

(6) Cox (*Primes of the Form* $x^2 + ny^2$, 1989)

Let

$$\begin{array}{rcl} n & : & \text{a positive integer} \\ K & : & \text{the imaginary quadratic field } \mathbb{Q}(\sqrt{-n}) \\ H_{\mathcal{O}} & : & \text{the ring class field of the order } \mathcal{O} = \mathbb{Z}[\sqrt{-n}] \\ \alpha & : & \text{a real algebraic integer for which } H_{\mathcal{O}} = K(\alpha). \end{array}$$

Let p be an odd prime number not dividing n. Then

$$\begin{array}{rl} & p = x^2 + ny^2 \\ \Longleftrightarrow & p \text{ splits completely in } H_{\mathcal{O}} \\ \Longleftrightarrow & \begin{cases} \left(\frac{-n}{p}\right) = 1 \text{ and} \\ \min(\alpha,\ K) \equiv 0 \pmod{p} \text{ has an integer solution.} \end{cases} \end{array}$$

Outline

1. Introduction
   - Elliptic integrals
   - What does E look like?
2. Elliptic curves
   - Projective plane curves
   - Elliptic functions
   - Elliptic curves
3. Modular curves
   - Modular curve of level N
   - Compactification
4. Elliptic curves and modular forms
   - Modular forms
   - Modular functions from generic elliptic curve
5. Application to number theory
   - Solving Diophantine equations
   - Construction of class fields

History

(1) **Kronecker-Weber** (1886, 1887)

Let L be a finite abelian extension of $\mathbb{Q}$. Then

$$L \subseteq \mathbb{Q}\big(f(\tfrac{1}{N}) \big) \text{ for some integer } N \geq 1$$

where

$$f(\tau) = e^{2\pi i \tau}.$$

(2) **Hilbert's 12th Problem** (Paris ICM, 1900) (= Kronecker's Jugendtraum)

Let

$$\begin{array}{lcl} K & : & \text{a given number field} \\ L & : & \text{arbitrary finite abelian extension of } K. \end{array}$$

Is there a transcendental function f such that

$$L = K\big(f(\alpha) \big) \text{ for some } \alpha \text{ ?}$$

Let K denote an imaginary quadratic field.

(3) **Takagi** (1920)

Takagi provided explicit generators for the maximal abelian extension K^{ab} by using special values of Jacobi functions.

(4) **Hasse** (1927)

Let

$$\theta\ (\in \mathfrak{H})\ :\ \text{a generator of the ring of integers of } K \text{ (over } \mathbb{Z}).$$

If L is a finite abelian extension of K, then

$$L \subseteq K\left(j(\theta),\ x_{(0,\ \frac{1}{N})}(\theta)\right) \text{ for some integer } N \geq 1.$$

The values $x_{(0,\ \frac{1}{N})}(\theta)$ corresponds to the x-coordinate of the N-torsion point

$$\left(x_{(0,\ \frac{1}{N})}(\theta),\ y_{(0,\ \frac{1}{N})}(\theta)\right)$$

of an elliptic curve parametrized by $\mathbb{C}/[\theta,\ 1]$ with complex multiplication.

(5) **Ramachandra** (1964)

Ramachandra showed that arbitrary finite abelian extension of K can be generated by certain elliptic unit.
But, his invariant involves too complicated products of high powers of special values of the Klein forms and Δ-function.

(6) **Cho-Koo** (2008)

They obtained a primitive generator from Hasse's two special values $j(\theta)$ and $x_{(0,\ \frac{1}{N})}(\theta)$.
But it is still hard to compute the minimal polynomial of the generator.

(7) **Koo-Shin** (2009)

If

$$\begin{array}{ccl} K & = & \mathbb{Q}(\sqrt{-n}) \quad \text{with } n \text{ square-free} \neq 1, 2, 3, 5, 6, 7, 11, 15 \\ N & : & \text{any integer} > 2, \end{array}$$

then

$$K\left(j(\theta),\ x_{(0,\ \frac{1}{N})}(\theta)\right) = K\left(y_{(0,\ \frac{1}{N})}(\theta)^{\frac{4m}{\gcd(4,\ N)}}\right) \quad \text{for any } m \neq 0$$

by using the Shimura's reciprocity law which connects the theory of modular functions and class field theory.

Example of a minimal polynomial

Let $K = \mathbb{Q}(\sqrt{-10})$ and $\theta = \sqrt{-10}$.
The minimal polynomial of the special value $y_{(0,\ \frac{1}{6})}(\theta)^{12}$ is given as follows:

$$
\begin{aligned}
&X^{16} - 5622749976591821668944491 1216X^{15}\\
&+281987387675738771039821808454272114 16X^{14}\\
&-61006294392822456973543787353433426528859172752X^{13}\\
&+2419154504055961819868557807806662102491998490989592 5564X^{12}\\
&-1457219992512158403396945180026448081831307850098282381377715440X^{11}\\
&-18752470866345884189001610098477497577054910903316185989551458784 99352X^{10}\\
&-320425805453669140355956674568263885695918616627920647592747434503845 3779344X^{9}\\
&+383798110212800409840846851392850879043779134397546083788605170327010622235878X^{8}\\
&-1154239742001591344102441518921573611681795924258535508207102881840723966924784 16X^{7}\\
&+334107284582565793933974554285013907697215168114012280251572770023994260474295208X^{6}\\
&-241306201753913238192695215039759665764921163190573494200250891932 9018160X^{5}\\
&+59471861573191065611449432210211994186104881219866586543410369 24X^{4}\\
&-5317595247800083950930014176690955051475061944750295248X^{3}\\
&+797299465586120177639706616225451835994220376X^{2}\\
&-29812156397602328057777202393119664X + 282429536481.
\end{aligned}
$$

Thank you.