Counting Rational Points on Curves and Surfaces

Noah Braeger
Utah State University

Result

Theorem: The counting function (of rational points) on the three-parameter family of generalized mirror K3 surfaces can be computed explicitly (it is a multivariate generalization of the Gauss hypergeometric function).

Overview

1. Elliptic Curves
2. Counting Rational Points on Elliptic Curves
3. Elliptic Integrals
4. K3 Surfaces
5. Counting Rational Point on K3 Surfaces

Elliptic Curves

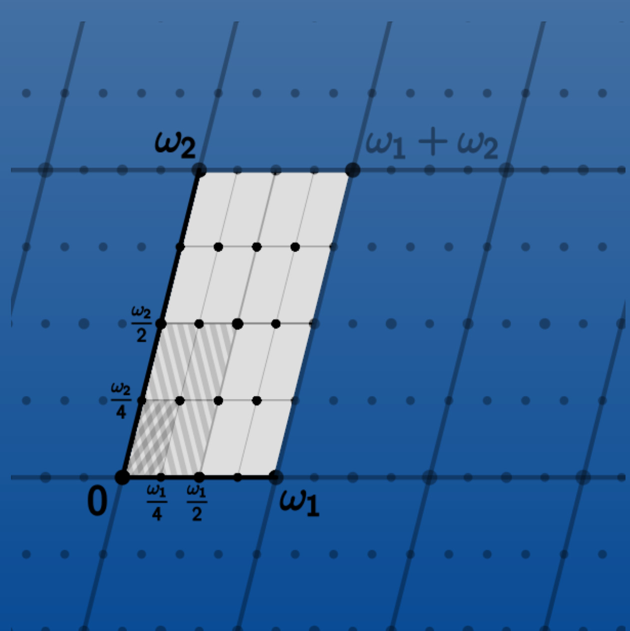
- For periods $\omega_1 = 1$ and $\omega_2 = \tau$ we consider the lattice of points given by:

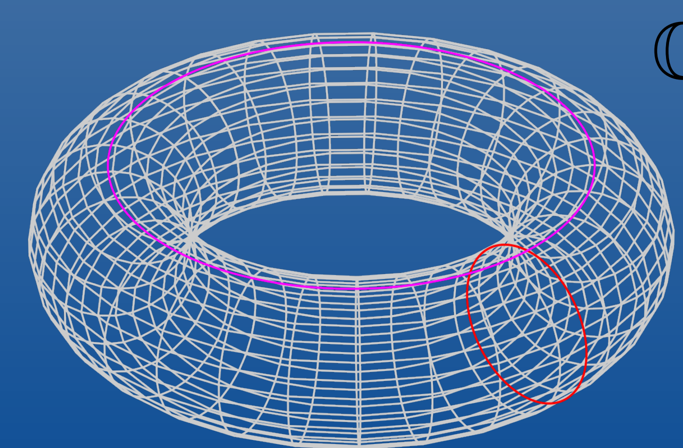
$$\Lambda = \{n + m\tau : n, m \in \mathbb{Z}\}$$

- We obtain the complex torus through defining congruence modulo our lattice.

$$z = w + n + m\tau$$

$$z \sim w$$





$\mathbb{C}/\Lambda$

Elliptic Functions

- A non-constant doubly periodic meromorphic function is called an elliptic function.

- The Weierstrass $\wp$ function is a doubly periodic meromorphic function with double poles at the lattice points

$$\wp(z) = \frac{1}{z^2} + \sum_{(n,m)\neq(0,0)} \left[\frac{1}{(z+n+m\tau)^2} - \frac{1}{(n+m\tau)^2}\right]$$

The Weierstrass $\wp$ Function

Elliptic Curves

$(\wp')^2$ is a cubic polynomial in $\wp$

An elliptic curve over C is a nonsingular cubic curve over C together with an abelian group structure.

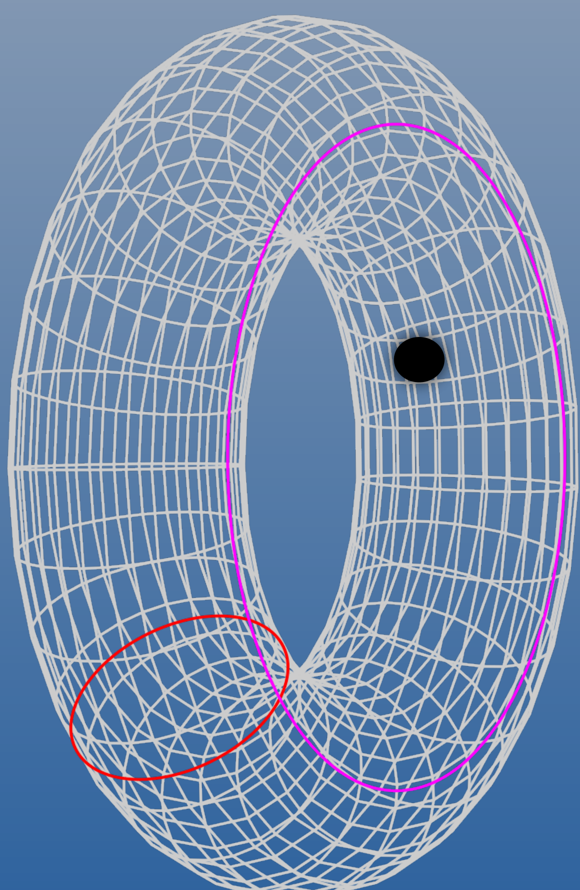
$$(\wp')^2 = 4\wp^3 - g_2\wp - g_3$$

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

We obtain the following isomorphism between the complex torus and the complex points on our elliptic curve

$$z \mapsto (x, y) = (\wp(z), \wp'(z)) \text{ where } \mathbb{C}/\Lambda$$

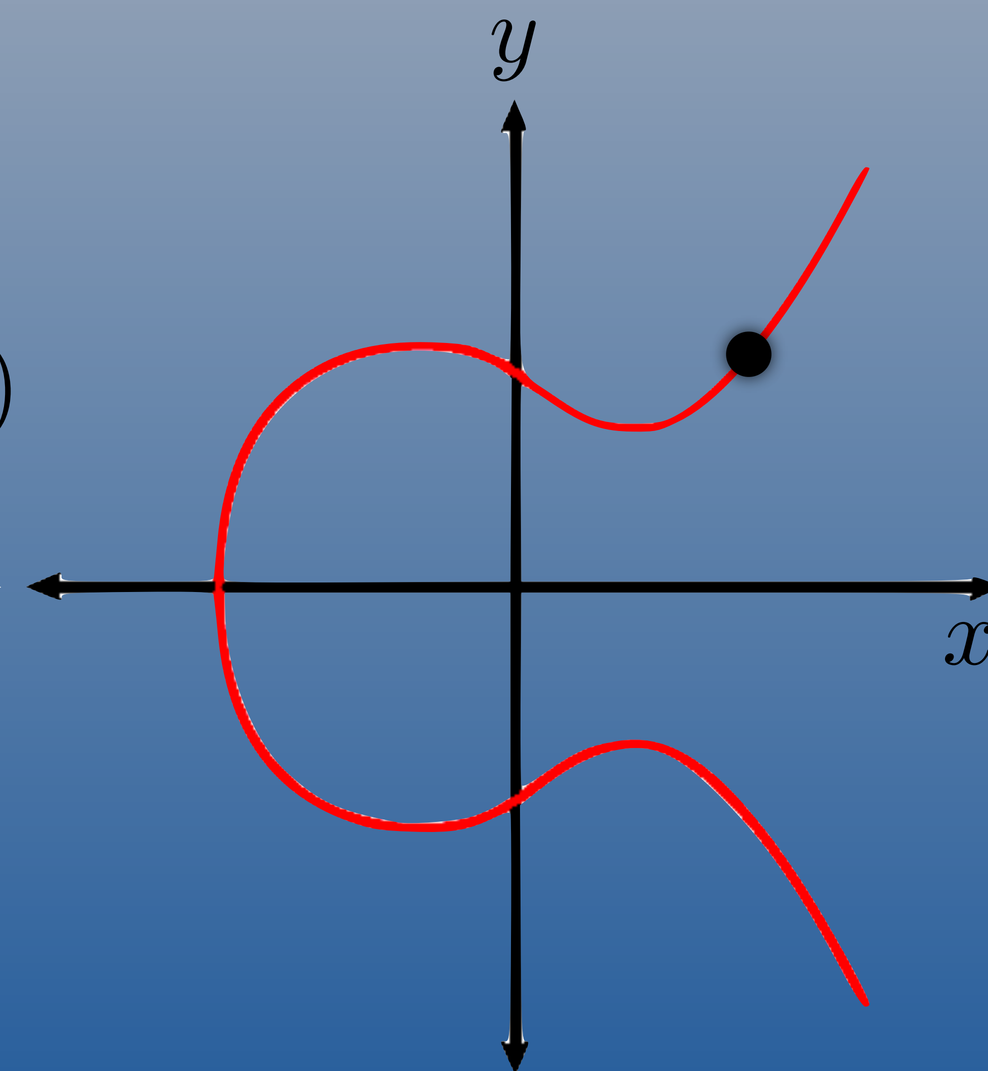
Elliptic Curves



$$z \mapsto (x, y) = (\wp(z), \wp'(z))$$

$$\tau \longrightarrow g_2,\ g_3$$

$$z \longrightarrow (x, y)$$



Counting Rational Points on Elliptic Curves

$$y^2 = 4x^3 - g_2 x - g_3 \longrightarrow y^2 = x(x-1)(x-\lambda)$$

Family of Elliptic Curves:

$$X_\lambda = \{y^2 = x(x-1)(x-\lambda)\}, \text{ where } \lambda \in \mathbb{C} - \{0,1\}$$

Now, let's count the number of rational points in this family modulo p.

Fermat's Little Theorem:

$$\text{If p is a prime, } a \in \mathbb{Z}, \text{ and p } \not| a \text{ then } a^{p-1} \equiv 1 \pmod{p}$$

Let $a \neq 0 \in \mathbb{F}_p$ Then,

$$a^{\frac{p-1}{2}} = \begin{cases} 1 & \text{, there exists } y \in \mathbb{F}_p \text{ such that } a = y^2 \\ -1 & \text{, otherwise} \end{cases}$$

Counting Rational Points on Elliptic Curves

Let $a \neq 0 \in \mathbb{F}_p$ Then,

$$a^{\frac{p-1}{2}} = \begin{cases} 1 & \text{, there exists } y \in \mathbb{F}_p \text{ such that } a = y^2 \\ -1 & \text{, otherwise} \end{cases}$$

Let $a = x(x-1)(x-\lambda) = y^2$

Consider pairs of rational numbers (x,y)

If $a^{\frac{p-1}{2}} \equiv 1$ then there are two rational points, (x,y) and (x,-y)

If a = 0, namely $x = 0, 1, \lambda$ then there is one rational point (x,0)

If $a^{\frac{p-1}{2}} \equiv -1$ there is no rational point.

Counting Rational Points on Elliptic Curves

Overall, the number of rational points for X_λ modulo p is

$$|X_\lambda| \equiv \sum_{x \in \mathbb{F}_p} (1 + (x(x-1)(x-\lambda))^{\frac{p-1}{2}}) \text{ mod p}$$

Further expanding this sum gives

$$|X_\lambda| = -(-1)^{\frac{p-1}{2}} \sum_{r=0}^{\frac{p-1}{2}} \binom{-\frac{1}{2}}{r}^2 \lambda^r \text{ mod p}$$

$$= -(-1)^{\frac{p-1}{2}} (1 + \frac{1}{4}\lambda + \frac{9}{64}\lambda^2 + \frac{25}{256}\lambda^3 + \dots)_{trunc} \text{ mod p}$$

$$= -(-1)^{\frac{p-1}{2}} {}_2F_1\left(\frac{1}{2}, \frac{1}{2}, 1, ; \lambda\right)_{trunc} \text{ mod p}$$

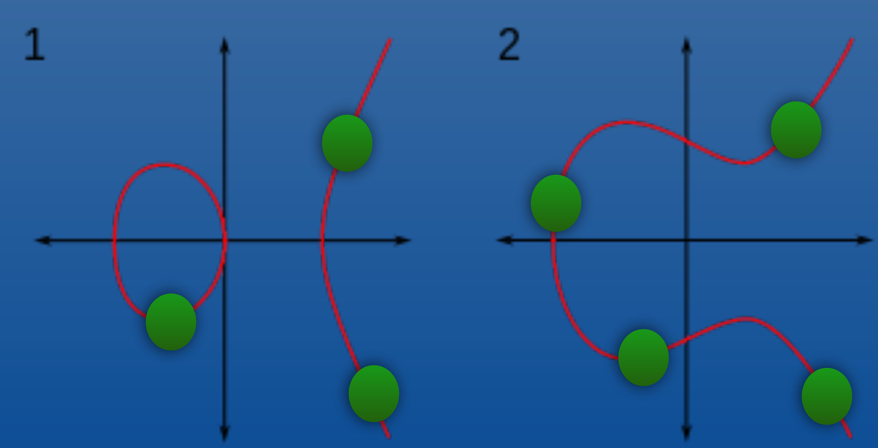
Counting Rational Points on Elliptic Curves

Family of Elliptic Curves:

$$X_\lambda = \{y^2 = x(x-1)(x-\lambda)\}, \text{ where } \lambda \in \mathbb{C} - \{0, 1\}$$

Counting Function for Family of Elliptic Curves:

$$|X_\lambda| = -(-1)^{\frac{p-1}{2}} {}_2F_1\left(\frac{1}{2}, \frac{1}{2}, 1, ; \lambda\right)_{trunc} \text{ mod p}$$



Elliptic Integrals

In introductory Calculus, we dealt with integrals of the type:

$$\int_0^1 \frac{1}{\sqrt{1+\lambda^2 x^2}}\,dx$$

$$= \frac{arcsinh(\lambda)}{\lambda} = 1 - \frac{1}{6}c^2 + \frac{3}{40}c^4 + \dots$$

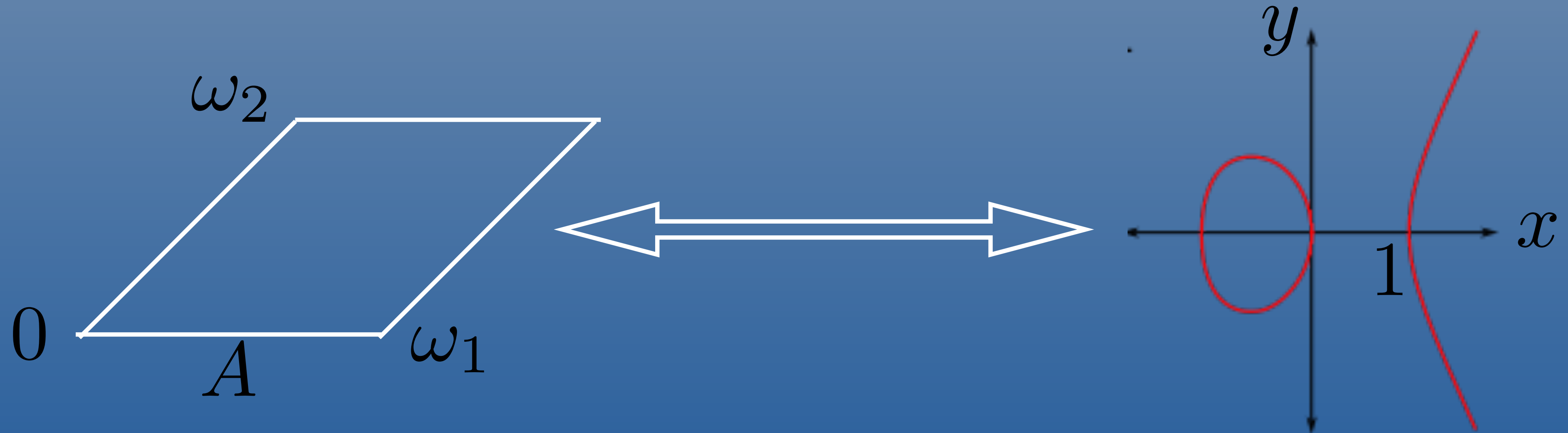
Elliptic Integral:

$$\int_1^\infty \frac{dx}{\sqrt{x(x-1)(x-\lambda)}} = 1 + \frac{1}{4}\lambda + \frac{9}{64}\lambda^2 + \frac{25}{256}\lambda^3 + \cdots = {}_2F_1\left(\frac{1}{2}, \frac{1}{2}, 1; \lambda\right)$$

Geometric Intuition of Elliptic Integrals

Elliptic Integrals can be seen as giving the length of the one-dimensional cycles of a torus.

Consider the Fundamental Parallelogram in our Lattice:



We can integrate around one of these cycles. Since $x = \wp(z)$ and $y = \wp'(z)$

$$\omega_1 = \int_A dz = \int_1^\infty \frac{dx}{y}$$

Counting Rational Points on Elliptic Curves and Elliptic Integrals

$$\text{On } X_\lambda : \; y^2 = x(x-1)(x-\lambda)$$

ω_λ is called the holomorphic one-form of the torus

$$\omega_\lambda = \frac{dx}{y} = \frac{dx}{(x(x-1)(x-\lambda))^{\frac{1}{2}}}$$

Elliptic Integrals:

$$\omega_1 = \int_1^\infty \frac{dx}{\sqrt{x(x-1)(x-\lambda)}} = 1 + \frac{1}{4}\lambda + \frac{9}{64}\lambda^2 + \frac{25}{256}\lambda^3 + \cdots = {}_2F_1\left(\frac{1}{2}, \frac{1}{2}, 1; \lambda\right)$$

Counting Rational Points on Elliptic Curves

Family of Elliptic Curves (tori):

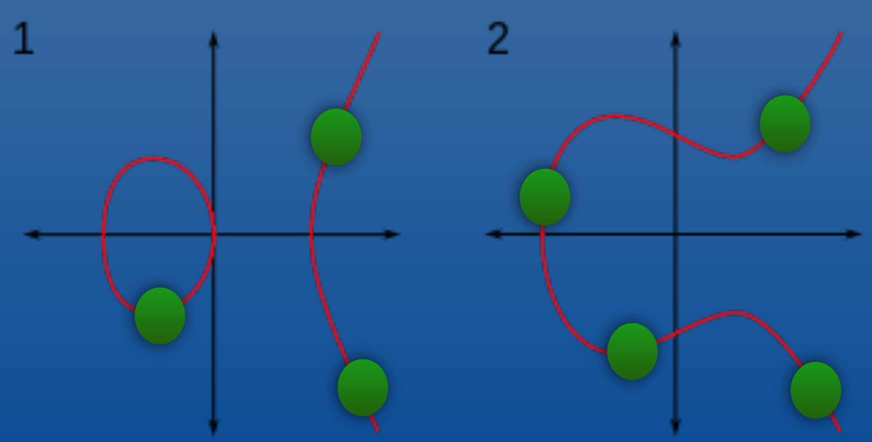
$$X_\lambda = \{y^2 = x(x-1)(x-\lambda)\}, \text{ where } \lambda \in \mathbb{C} - \{0,1\}$$

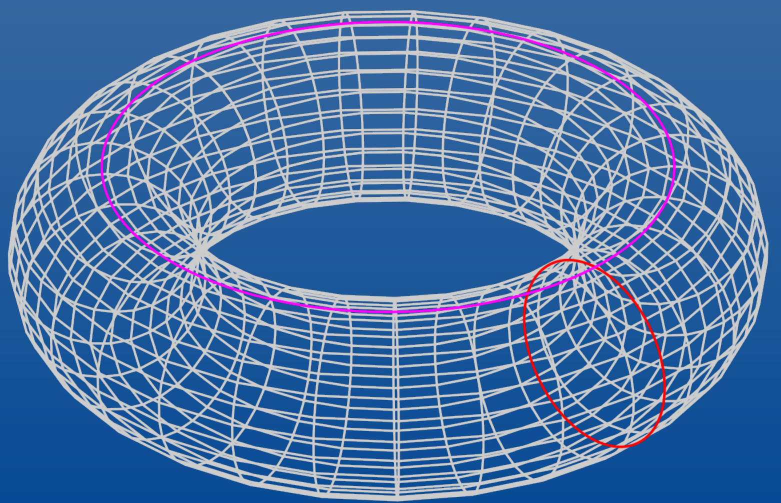
Elliptic Integrals (from geometry):

$$\omega_1 = \int_1^\infty \frac{dx}{\sqrt{x(x-1)(x-\lambda)}} = 1 + \frac{1}{4}\lambda + \frac{9}{64}\lambda^2 + \frac{25}{256}\lambda^3 + \cdots = {}_2F_1\left(\frac{1}{2}, \frac{1}{2}, 1; \lambda\right)$$

Counting Function for Family of Elliptic Curves:

$$|X_\lambda| = -(-1)^{\frac{p-1}{2}} (\omega_1)_{trunc} \text{ mod p}$$





Projective Varieties
Elliptic Curves - K3 Surfaces

Elliptic curves can more correctly be thought of as solution sets of degree-3 homogenous polynomials in 2-dimensional projective space $(\mathbb{P}^2)$

$$\text{For } (x, y, z) \in \mathbb{P}^2,\ (x, y, z) \sim (\lambda x, \lambda y, \lambda z)$$

$$y^2 = x(x-1)(x-\lambda) \longrightarrow Y^2 Z = X(X-Z)(X-\lambda Z)$$

K3 surfaces are thought of as solution sets of degree-4 homogeneous polynomials in 3-dimensional projective space $(\mathbb{P}^3)$

$$\text{For } (x, y, w, z) \in \mathbb{P}^3,\ (x, y, w, z) \sim (\lambda x, \lambda y, \lambda w, \lambda z)$$

$$X^4 + Y^4 + W^4 + Z^4 + C_1 X^3 YZW + C_2 X^3 Y Z^2 + \dots$$

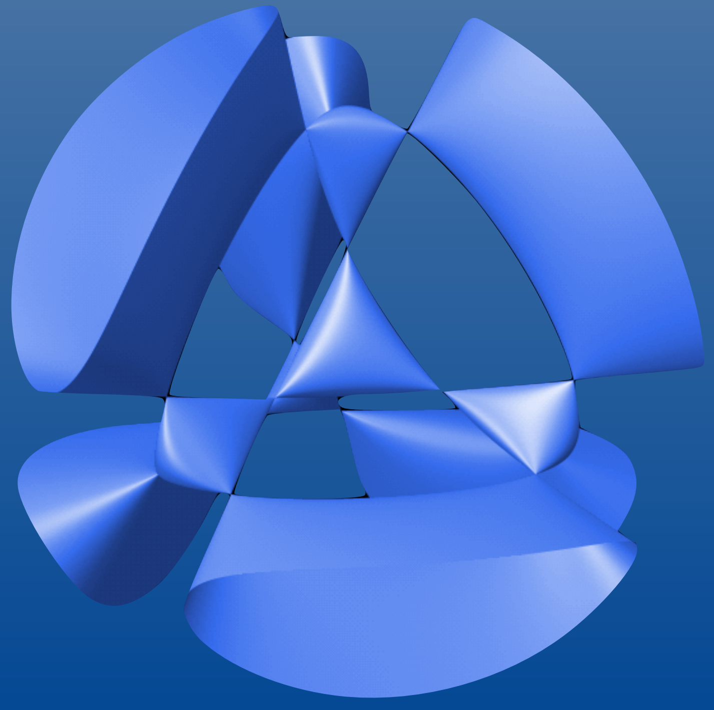
Kummer Surfaces

Consider the quartic surface in three-dimensional projective space
(special K3)

$$X^4 + Y^4 + W^4 + Z^4 + 2DXYWZ - A(X^2Z^2 + Y^2W^2) - B(X^2Y^2 + W^2Z^2) - C(X^2W^2 + Y^2Z^2) = 0$$

$$A, B, C, D \in \mathbb{C}$$

Kummer surfaces emit 16 nodal singularities. After resolving the singularities, we obtain a K3 surface.



Relating Different K3 Surfaces - Mirror Symmetry and String Theory

General Smooth K3
(symplectic manifold)
(A-Side)

Family of Complex K3 Manifolds
(B-Side)

Greene-Plesser
(divide by symmetry
group and resolve
singularities)

Quartic in $\mathbb{P}^3$
(singular K3)

$$X^4 + Y^4 + W^4 + Z^4 + 4\lambda XYWZ = 0$$

Dwork Pencil

<u>What makes these K3 surfaces mirrors?</u>

- Equivalent Hodge Structures
- "Same" Rational Point Counts

Greene-Plesser Orbifolding Mechanism

Through the Greene-Plesser orbifolding procedure, we are allowed to construct the mirror family of K3 surfaces for our Dwork pencil.

$$x_1 = \frac{Y^3}{4XWZ\lambda},\ x_2 = \frac{W^3}{4XYZ\lambda},\ x_3 = \frac{Z^3}{4XYW\lambda},\ \mu = \frac{1}{\lambda^4}$$

$$x_1x_2x_3(x_1 + x_2 + x_3 + 1) + \frac{\mu}{4^4} = 0$$

Greene-Plesser Orbifolding Mechanism

On the new family of K3 surfaces produced from the Greene-Plesser mechanism

$$x_1 x_2 x_3 (x_1 + x_2 + x_3 + 1) + \frac{\mu}{4^4} = 0$$

we can compute period integrals for this family.

$$\omega_1 = \left({}_2F_1\left(\frac{1}{8}, \frac{3}{8}, 1; \mu\right)\right)^2, \text{ holomorphic as } t \mapsto 0$$

The K3 surface itself is described by 3 periods which can be written in terms of this period.

Elliptic Fibrations and K3 Surfaces

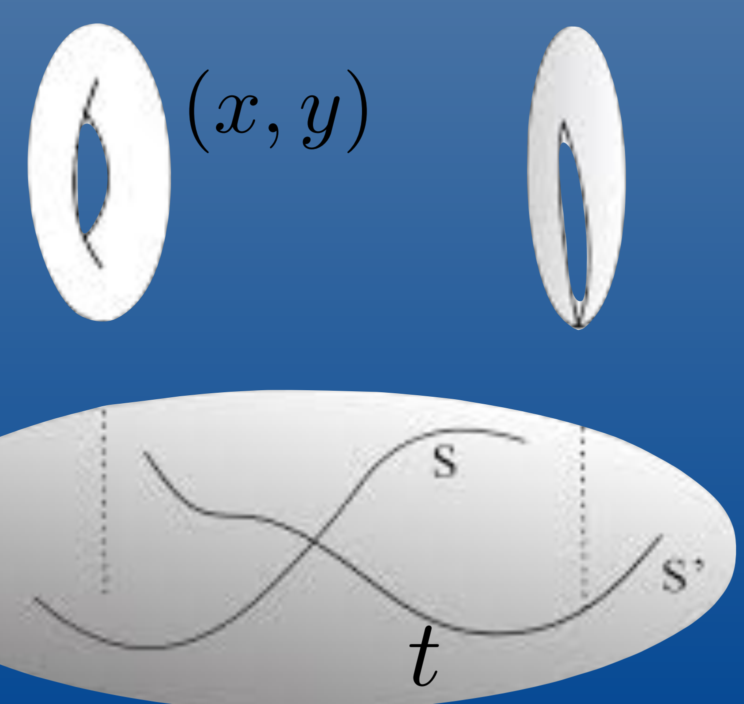
We can analyze K3 surfaces as elliptic fibrations over the Riemann sphere through brining them into Weierstrass normal form.

$$x = f_1(X, Y, W, Z) \qquad y = f_2(X, Y, W, Z) \qquad t = f_3(X, Y, W, Z)$$

$$y^2 = 4x^3 - {g_2}_{\mu}(t)x - {g_3}_{\mu}(t)$$

Elliptic K3 surfaces are thus seen to be surfaces that are constructed through attaching a torus at every point on the Riemann sphere.

$$\omega_1 = \left({}_2F_1\left(\frac{1}{8}, \frac{3}{8}, 1; \mu\right)\right)^2$$



Generalizing the Dwork Pencil

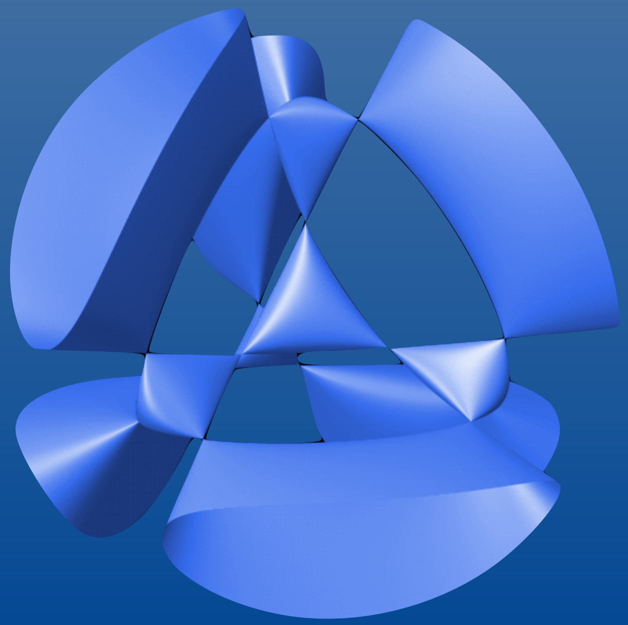
The one-parameter Dwork Pencil

$$x^4 + y^4 + w^4 + z^4 + 4\lambda xywz = 0$$

The three-parameter Kummer quartic serves as the natural generalization of the Dwork pencil, as it preserves some of the symmetry.

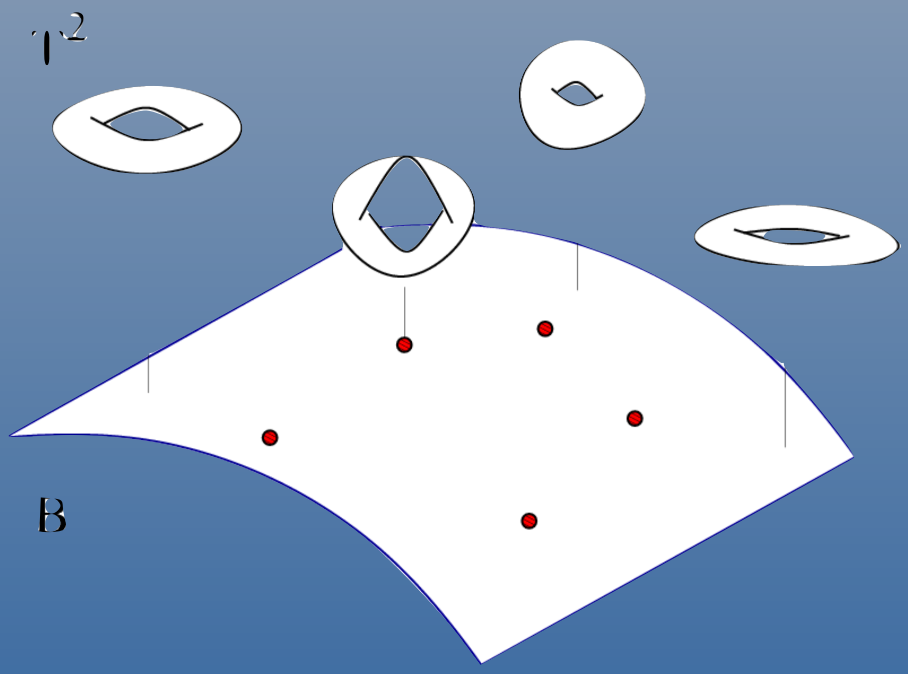
$$x^4 + y^4 + w^4 + z^4 + 2Dxywz - A(x^2z^2 + y^2w^2) - B(x^2y^2 + w^2z^2) - C(x^2w^2 + y^2z^2) = 0$$

$$A, B, C, D \in \mathbb{C}$$



Generalizing the Greene-Plesser Mechanism

We can establish elliptic fibrations both on our three-parameter Kummer quartic and the mirror of the Dwork pencil.



The elliptic fibration structure allows us to generalize the Greene-Plesser mechanism. We then obtain the three-parameter generalization of the mirror of the generalized Dwork pencil.

We can compute the fiberwise period integral. We can then express the 5 period integrals of our surface in terms of this multi-variate hypergeometric function (Aomoto-Gelfos Function).

Counting Rational Points on K3 Surfaces

We established a three-parameter family of K3 surfaces generalizing the Greene-Plesser mechanism.

$$x^4 + y^4 + w^4 + z^4 + 2Dxywz - A(x^2z^2 + y^2w^2) - B(x^2y^2 + w^2z^2) - C(x^2w^2 + y^2z^2) = 0$$

Through using the elliptic fibration on the three-parameter mirror family and relating the period integrals of different families, we show that

$$|X_{A,B,C}| = \left(\text{Special K3 Period}\right)_{trunc} \text{ mod p}$$

Results

Theorem: The counting function (of rational points) on the three-parameter family of generalized mirror K3 surfaces can be computed explicitly (it is a multivariate generalization of the Gauss hypergeometric function).

$$|X_p| \equiv (-1)^{\frac{p-1}{2}} \sum_{\ell=0}^{\frac{p-1}{2}} (-1)^{\ell} (C_{\ell}^{\frac{p-1}{2}})^2 \sum_{i+j+k=\ell} C_i^{\frac{p-1}{2}} C_j^{\frac{p-1}{2}} C_k^{\frac{p-1}{2}} a^i b^j c^k$$

The equation of the surface is:

$$y^2 = x(x-1)(x-t)(t-a)(t-b)(t-c)$$

Thank You!

Acknowledgements: Dr. Malmendier, Dr. Sung
USU URCO (Undergraduate Research and Creative Opportunities) Grant Program
USU Mini Grant Program.