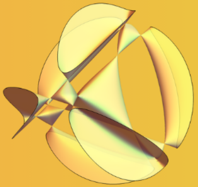
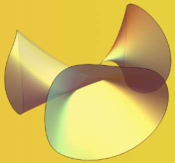
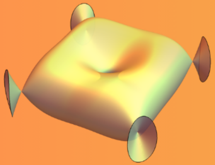
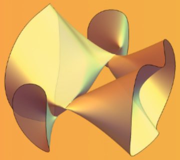
ALVARO GONZALEZ HERNANDEZ
University of Warwick





Explicit theory of Kummer surfaces in characteristic two





4TH OCTOBER 2023
LINFOOT NUMBER THEORY SEMINAR

Outline of the talk

1. Motivation

2. How to study genus 2 curves via Kummer surfaces

3. Connections with geometry

4. Problems with characteristic two

1. Motivation

Points on a curve defined over a certain field

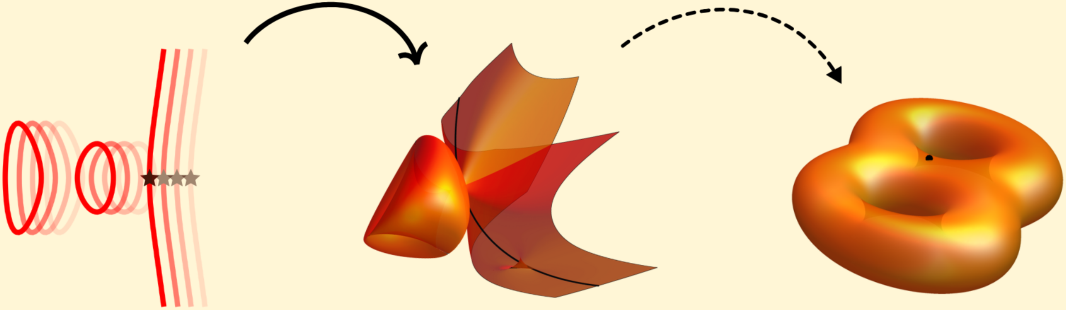
The Jacobian variety associated to the curve

Points on a curve defined over a certain field

The Jacobian variety associated to the curve

Given a hyperelliptic curve, how can we compute an explicit model of its Jacobian as a projective variety?

The idea is



$$\mathcal{C}^{(g)} = \underbrace{\mathcal{C} \times \cdots \times \mathcal{C}}_{g} \; / \; S_g$$

Jacobian variety

Hyperelliptic curves

Let

$$\mathcal{C} : y^2 + h(x)y = f(x)$$

be a hyperelliptic curve of genus $g \geq 1$ where $f(x), h(x) \in k[x]$, $\deg f(x) = 2g + 2$ and $\deg h(x) \leq g + 1$.

The curve has two different points at infinity that I will denote by ∞_+ and ∞_-.

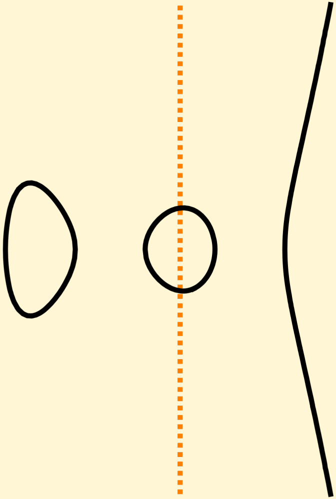
The hyperelliptic involution

The curve

$$\mathcal{C} : y^2 + h(x)y = f(x)$$

has a natural involution defined by

$$\begin{aligned} \iota_{\mathcal{C}} : \mathcal{C} &\longrightarrow \mathcal{C} \\ (x, y) &\longmapsto (x, -y - h(x)) \\ \infty_+ &\longmapsto \infty_- \\ \infty_- &\longmapsto \infty_+ \end{aligned}$$



The following:

$$\Theta_+ = \underbrace{C \times \cdots \times C}_{g-1} \times \{\infty_+\} \quad \text{and} \quad \Theta_- = \underbrace{C \times \cdots \times C}_{g-1} \times \{\infty_-\}$$

define divisors of $\mathcal{C}^{(g)}$ and an embedding of the Jacobian into projective space is given by $\mathcal{L}(2(\Theta_+ + \Theta_-))$.

(*These are functions in the function field of* $\mathcal{C}^{(g)}$ *that at worst can only possibly have poles in* $2(\Theta_+ + \Theta_-)$ *of the "right" multiplicity.*)

What happens, for instance, when $g = 2$?

For $g = 2$, let's consider two copies of a curve $\mathcal{C}$

$$y_1^2 + h(x_1)y_1 = f(x_1) \qquad y_2^2 + h(x_2)y_2 = f(x_2)$$

Then, some independent functions of $\mathcal{L}(2(\Theta_+ + \Theta_-))$ are

$$1, x_1 + x_2, x_1x_2, (x_1 + x_2)^2, \tfrac{(2y_1+h(x_1))-(2y_2+h(x_2))}{x_1-x_2}, \ldots$$

In this case $|\mathcal{L}(2(\Theta_+ + \Theta_-))| = 16$.

What happens, for instance, when $g = 2$

The embedding would be obtained by considering the closure of

$$[1 : x_1 + x_2 : x_1 x_2 : (x_1 + x_2)^2 : \tfrac{(2y_1 + h(x_1)) - (2y_2 + h(x_2))}{x_1 - x_2}, \ldots] \hookrightarrow \mathbb{P}^{15}$$

where $(x_1, y_1), (x_2, y_2) \in \mathcal{C}$.

Given a point of the Jacobian as a projective variety over a field k, we can also identify it as a degree 0 divisor modulo linear equivalence.

But there is a drawback...

The embedding by $\mathcal{L}(2(\Theta_+ + \Theta_-))$ is given by the intersection of **many** conics:

Genus	1	2	3	$\cdots$	g
$\mathbb{P}^n$ in which it embeds	3	15	63	$\cdots$	$4^g - 1$
Number of conics	2	72	1568	$\cdots$	$2^{2g-1}(2^g - 1)^2$

Simplifying models at the cost of losing information

$\iota_{\mathcal{C}}$ extends to an involution on $\mathcal{C}^{(g)}$, such that $\iota_{\mathcal{C}}$ acts linearly on the elements of $\mathcal{L}(2(\Theta_+ + \Theta_-))$. If the field of definition has characteristic different than 2, we can "diagonalise" this action to obtain a decomposition:

$$\mathcal{L}(2(\Theta_+ + \Theta_-)) = \{\text{even functions}\} \oplus \{\text{odd functions}\}$$

where

$$\iota_{\mathcal{C}}(\text{even}) = \text{even} \qquad \iota_{\mathcal{C}}(\text{odd}) = -\text{odd}$$

Going back to our example when $g = 2$

The functions

$$\{1, x_1 + x_2, x_1 x_2, (x_1 + x_2)^2, \dots\}$$

are even and $\#\{\text{even functions}\} = 10.$

The functions

$$\left\{\frac{(2y_1+h(x_1))-(2y_2+h(x_2))}{x_1-x_2}, \frac{(2y_1+h(x_1))x_2-(2y_2+h(x_2))x_1}{x_1-x_2}, \dots\right\}$$

are odd and $\#\{\text{odd functions}\} = 6.$

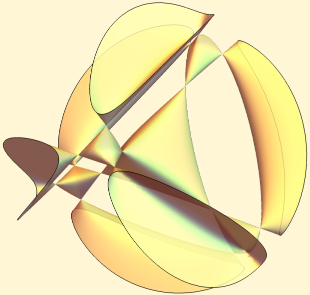
Kummer variety

Let $\mathcal{A}$ be an Abelian variety (e.g. the Jacobian of a hyperelliptic curve) and let ι be the involution in $\mathcal{A}$ that sends an element to its inverse. Then, the **Kummer variety** associated to $\mathcal{A}$, $\mathrm{Kum}(\mathcal{A})$ is the quotient variety $\mathcal{A}/\iota$.

Fact

For $g > 1$, $\mathcal{A}[2]$ is the set of all fixed points under the action of ι and these points are singular points of $\mathrm{Kum}(\mathcal{A})$.

Kummer varieties according to the genus



Suppose that the field of definition is algebraically closed and has characteristic different than 2.

- If the dimension of $\mathcal{A}$ is 2, $\mathrm{Kum}(\mathcal{A})$ is a surface described by a quartic in $\mathbb{P}^3$ with 16 nodal singularities.
- Generally, if the dimension of $\mathcal{A}$ is g, $\mathrm{Kum}(\mathcal{A})$ can be found as an intersection in $\mathbb{P}^{2^g-1}$.

Why are Kummer varieties relevant?

WARWICK
THE UNIVERSITY OF WARWICK

- Their models are considerably easier.
- They are **not** Abelian varieties, so they do not have a group law. However, they inherit a *pseudo-group law* that helps to makes computations in the Jacobian (this is strongly used in cryptography).
- For a hyperelliptic curve $\mathcal{C}$, the projective embedding of the Kummer variety associated to the Jacobian of $\mathcal{C}$ is given by $\mathcal{L}(\Theta_+ + \Theta_-)$.

2. How to study genus 2 curves via Kummer surfaces

Let's illustrate this with an example

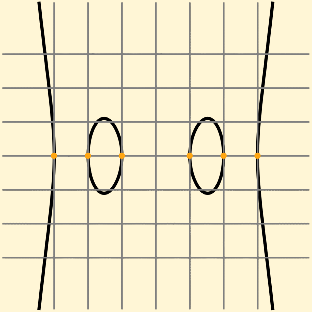
Let $\mathcal{C}$ be the following genus 2 curve defined over $\mathbb{F}_7$

$$\mathcal{C} : y^2 = (x-1)(x+1)(x-2)(x+2)(x-3)(x+3) = x^6 - 1$$

We want to study $\mathcal{C}(\mathbb{F}_7)$ and $\mathrm{Jac}(\mathcal{C})(\mathbb{F}_7)$.

Because we are working over a finite field, it is easy to check that

$$\mathcal{C}(\mathbb{F}_7) = \{\infty_\pm\} \cup \{(n,0) \mid n \in \{-3,-2,-1,1,2,3\}\}$$



Let's illustrate this with an example

WARWICK
THE UNIVERSITY OF WARWICK

As for $\mathrm{Jac}(\mathcal{C})(\mathbb{F}_7)$, we can write a basis of $\mathcal{L}(2(\Theta_+ + \Theta_-))$

$$\mathcal{L}(2(\Theta_+ + \Theta_-)) = \left\{1, x_1 + x_2, x_1 x_2, (x_1 + x_2)^2, \frac{y_1 - y_2}{x_1 - x_2}, \frac{x_2 y_1 - x_1 y_2}{x_1 - x_2}, \ldots\right\}$$

and the 72 equations that define. With even more brute force, we could count the points of $\mathrm{Jac}(\mathcal{C})(\mathbb{F}_7)$, and deduce that

$$\mathrm{Jac}(\mathcal{C})(\mathbb{F}_7) \cong (\mathbb{Z}/2\mathbb{Z})^4 \times \mathbb{Z}/3\mathbb{Z}$$

Why is this a bad idea?

Essentially, the problem is that $\mathrm{Jac}(\mathcal{C})$ is defined by a very complicated intersection in a large projective space, so the points of $\mathrm{Jac}(\mathcal{C})(\mathbb{F}_7)$ are really sparse in $\mathbb{P}^{15}(\mathbb{F}_7)$

$$\#\mathbb{P}^{15}(\mathbb{F}_7) \approx 5.54 \times 10^{12} \qquad \#\mathrm{Jac}(\mathcal{C})(\mathbb{F}_7) = 48$$

For this example, it works, but there is no hope that we can replicate this for bigger finite fields and definitely not for global fields.

Here is where Kummer surfaces offer a solution!

Let's utilise the power of Kummer surfaces

In order to compute $\mathrm{Kum}(\mathcal{C})$, we first find a basis for $\mathcal{L}(\Theta_+ + \Theta_-)$

$$\mathcal{L}(\Theta_+ + \Theta_-) = \left\{1, x_1 + x_2, x_1x_2, \frac{-1 + x_1^3x_2^3 - y_1y_2}{(x_1 - x_2)^2}\right\}$$

where $(x_1, x_2) \in \mathcal{C}$. Then,

$$[k_1 : k_2 : k_3 : k_4] = \left[1 : x_1 + x_2 : x_1x_2 : \frac{-1 + x_1^3x_2^3 - y_1y_2}{(x_1 - x_2)^2}\right] \hookrightarrow \mathbb{P}^3$$

defines an embedding of $\mathrm{Kum}(\mathcal{C}) \subset \mathbb{P}^3$ given by

$$(3k_1k_3 - k_2^2)k_4^2 - 3(k_1^3 - k_3^3)k_4 - 3(k_1k_3 - k_2^2)^2 = 0$$

Let's utilise the power of Kummer surfaces

$$\mathrm{Kum}(\mathcal{C}) : (3k_1k_3 - k_2^2)k_4^2 - 3(k_1^3 - k_3^3)k_4 - 3(k_1k_3 - k_2^2)^2 = 0$$

We can start by computing all the points of the Kummer over $\mathbb{F}_7$.

$$\#\,\mathrm{Kum}(\mathcal{C})(\mathbb{F}_7) = 48$$

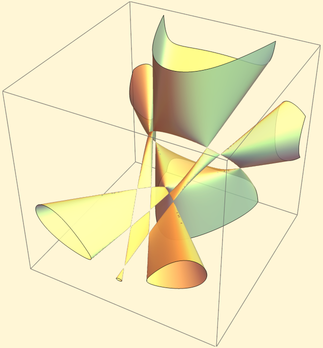
Let's utilise the power of Kummer surfaces

$$\mathrm{Kum}(\mathcal{C}) : (3k_1k_3 - k_2^2)k_4^2 - 3(k_1^3 - k_3^3)k_4 - 3(k_1k_3 - k_2^2)^2 = 0$$

We can start by computing all the points of the Kummer over $\mathbb{F}_7$.

$$\#\,\mathrm{Kum}(\mathcal{C})(\mathbb{F}_7) = 48$$

Out of this 48 points, 16 are **singular points** of the Kummer and the other 32 are **smooth points**.



Let's utilise the power of Kummer surfaces

Proposition

The inclusion $\mathcal{L}(\Theta_+ + \Theta_-) \subset \mathcal{L}(2(\Theta_+ + \Theta_-))$ induces a quotient morphism

$$\mathrm{Jac}(\mathcal{C}) \xrightarrow{\pi} \mathrm{Kum}(\mathcal{C})$$

such that for any field k,

$$\mathrm{Jac}(\mathcal{C})(k) \subseteq \pi^{-1}(\mathrm{Kum}(\mathcal{C})(k))$$
$$\mathrm{Jac}(\mathcal{C})[2](k) = \pi^{-1}(\mathrm{Sing}(\mathrm{Kum}(\mathcal{C})(k)))$$

From the previous theorem...

We deduce that

$$16 \leq \mathrm{Jac}(\mathcal{C})(\mathbb{F}_7) \leq 80$$

and that, in order to know what is $\mathrm{Jac}(\mathcal{C})(\mathbb{F}_7)$, we only need to understand if the preimages with respect to π of the smooth points of $\mathrm{Kum}(\mathcal{C})(\mathbb{F}_7)$ lie in $\mathrm{Jac}(\mathcal{C})(\mathbb{F}_7)$.

Going back to the start of the talk...

Considering the involution of $\mathcal{C}$

$$\begin{aligned} \iota_{\mathcal{C}} : \mathcal{C} &\longrightarrow \mathcal{C} \\ (x, y) &\longmapsto (x, -y) \end{aligned}$$

we obtain

$$\mathcal{L}(2(\Theta_+ + \Theta_-)) = \{\text{even functions}\} \oplus \{\text{odd functions}\}$$

$$\#\{\text{even functions}\} = 10 \qquad \#\{\text{odd functions}\} = 6$$

where

$$\iota_{\mathcal{C}}(\text{even}) = \text{even} \qquad \iota_{\mathcal{C}}(\text{odd}) = -\text{odd}$$

Even and odd interactions

WARWICK
THE UNIVERSITY OF WARWICK

$$\begin{aligned}\mathcal{L}(\Theta_+ + \Theta_-) &= \{k_1, k_2, k_3, k_4\} \\ &= \left\{1, x_1 + x_2, x_1 x_2, \frac{-1 + x_1^3 x_2^3 - y_1 y_2}{(x_1 - x_2)^2}\right\} \\ &\subset \{\text{even functions of } \mathcal{L}(2(\Theta_+ + \Theta_-))\}\end{aligned}$$

In fact, the space of even functions of $\mathcal{L}(2(\Theta_+ + \Theta_-))$ is generated as a vector space by the products of every two functions of $\mathcal{L}(\Theta_+ + \Theta_-)$, i.e.

$$\{\text{even functions}\} = \{k_1^2, k_1k_2, k_1k_3, k_1k_4, k_2^2, k_2k_3, k_2k_4, k_3^2, k_3k_4, k_4^2\}$$

And here is the twist

Consider a basis for the odd functions

$$\{\text{odd functions}\} = \{b_1, b_2, b_3, b_4, b_5, b_6\}$$
$$= \left\{ \frac{y_1 - y_2}{(x_1 - x_2)}, \frac{x_2 y_1 - x_1 y_2}{(x_1 - x_2)}, \frac{x_2^2 y_1 - x_1^2 y_2}{(x_1 - x_2)}, \dots \right\}$$

The embedding of the Jacobian is given by quadratics relations between the elements of $\mathcal{L}(2(\Theta_+ + \Theta_-))$. But the fact that the product of any two odd functions is an even function, allows us to express the product of every two b_i as a homogeneous polynomial of degree 4 on the k_j.

In the example

$$\begin{cases} b_1^2 & = 4(k_2^4 - 2k_1k_2^2k_3 + k_1^2k_3^2 + k_1^3k_4) \\ b_1b_2 & = 4k_2(k_2^2k_3 - k_1k_3^2 - 3k_1^2k_4) \\ b_2^2 & = 3(k_1^4 - k_2^2k_3^2 - k_1^2k_3k_4) \\ b_1b_3 & = 4(k_2^2k_3^2 - k_1k_3^3 - 3k_1k_2^2k_4 - k_1^2k_3k_4) \\ & \vdots \end{cases}$$

We can evaluate $\{k_1, k_2, k_3, k_4\}$ at the points of $\mathrm{Kum}(\mathcal{C})(\mathbb{F}_7)$ to see if there exist $b_i \in \mathbb{F}_7$ satisfying those equations. Those points for which this is possible lift to points in $\mathrm{Jac}(\mathcal{C})(\mathbb{F}_7)$. This allows us to compute $\mathrm{Jac}(\mathcal{C})(\mathbb{F}_7)$.

Moving on to rational points

Suppose that we now want to study the points of the curve

$$\mathcal{C} : y^2 = (x-1)(x+1)(x-2)(x+2)(x-3)(x+3)$$

over the rationals. As $\mathcal{C}$ has good reduction at 7, we have that

$$\mathrm{Jac}(C)(\mathbb{Q})_{\text{torsion}} \hookrightarrow \mathrm{Jac}(C)(\mathbb{F}_7)$$

and in this case this is actually an isomorphism.
Computing the rank is **notoriously difficult**. In this case, it can be checked that the rank is zero and so

$$\mathrm{Jac}(\mathcal{C})(\mathbb{Q}) \cong (\mathbb{Z}/2\mathbb{Z})^4 \times \mathbb{Z}/3\mathbb{Z}$$

3. Connections with geometry

Redefining Kummer surfaces

WARWICK
THE UNIVERSITY OF WARWICK

Kummer surfaces

A **Kummer surface** is a quartic surface in $\mathbb{P}^3$ with 16 isolated singularities.

Every Kummer surface has 16 special conics known as **tropes** in the following configuration:

- Each trope goes through 6 singular points.
- For each singular point, there are 6 tropes going through it.

Suppose we want to **desingularise the Kummer surface** that we saw before:

$$\mathrm{Kum}(\mathcal{C}) : (3k_1k_3 - k_2^2)k_4^2 - 3(k_1^3 - k_3^3)k_4 - 3(k_1k_3 - k_2^2)^2 = 0$$

Consider the odd functions $\{b_1, b_2, b_3, b_4.b_5, b_6\}$. We have a **rational map**

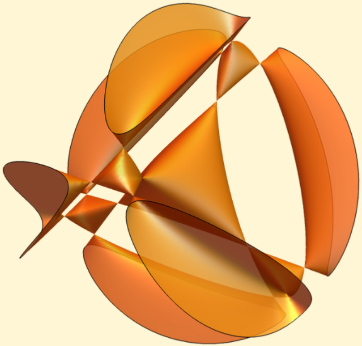
$$\mathrm{Kum}(\mathcal{C}) \xrightarrow{\phi} \mathbb{P}^5$$
$$[k_1 : k_2 : k_3 : k_4] \longmapsto [b_1 : b_2 : b_3 : b_4 : b_5 : b_6]$$

which happens to be well-defined outside of $\mathrm{Sing}(\mathrm{Kum}(\mathcal{C}))$.

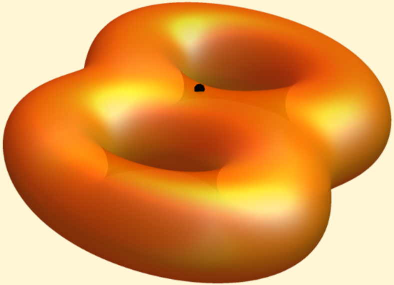
The closure of the image of this map defines a smooth surface Y in $\mathbb{P}^5$ given by the complete intersection of three quadrics.

$$\begin{cases} b_1b_2 + b_4b_5 + b_3b_6 = 0 \\ -3b_1^2 + 2b_4^2 - 3b_3b_5 + b_2b_6 = 0 \\ 2b_3b_4 - 3b_2b_5 + b_1b_6 = 0 \end{cases}$$

Actually... The map ϕ is a **birational morphism** $\mathrm{Kum}(\mathcal{C}) \dashrightarrow Y$ which turns out to be the inverse of the blow-up of the 16 singular points of $\mathrm{Kum}(\mathcal{C})$!



Desingularisation of the Kummer surface



Explicit projective models of the Jacobian of a genus 2 curve

Concerning mixed characteristic

WARWICK
THE UNIVERSITY OF WARWICK

Idea

Suppose we start with a Kummer surface defined over a number field over where all the tropes and the singular points are defined. Furthermore, assume this surface has good reduction over a prime $\mathfrak{p}$ not lying above 2.

Then, **the reduction map will preserve all the geometric and arithmetic features that we have discussed.**

Essentially the theory of Kummer surfaces is the same over characteristic zero than over characteristic $p > 2$.

4. Problems with characteristic two

1 Canonical form. We shall normally suppose that the characteristic¶ of the ground field is not 2 and consider curves $\mathcal{C}$ of genus 2 in the shape

$$\mathcal{C}: \quad Y^2 = F(X), \tag{1.1.1}$$

where

$$F(X) = f_0 + f_1 X + \ldots + f_6 X^6 \in k[X] \tag{1.1.2}$$

1. *The Jacobian variety*

We shall work with a general curve $\mathscr{C}$ of genus 2, over a ground field K of characteristic not equal to 2, 3 or 5, which may be taken to have hyperelliptic form

$$\mathscr{C} : Y^2 = F(X) = f_6 X^6 + f_5 X^5 + f_4 X^4 + f_3 X^3 + f_2 X^2 + f_1 X + f_0 \quad (1)$$

with $f_0, \ldots, f_6$ in K, $f_6 \neq 0$, and $\Delta(F) \neq 0$, where $\Delta(F)$ is the discriminant of F. In $\mathbb{F}_5$ there is, for example, the curve $Y^2 = X^5 - X$ which is not birationally equivalent to the above form.

1 Canonical form. We shall normally suppose that the characteristic¶ of the ground field is not 2 and consider curves $\mathcal{C}$ of genus 2 in the shape

$$\mathcal{C} : \quad Y^2 = F(X), \quad (1.1.1)$$

where

$$F(X) = f_0 + f_1 X + \ldots + f_6 X^6 \in k[X] \quad (1.1.2)$$

2. Set-up

Let k be a field of characteristic not equal to two, k^s a separable closure of k, and $f = \sum_{i=0}^{6} f_i X^i \in k[X]$ a separable polynomial with $f_6 \neq 0$. Denote by Ω the set of the six roots of f in k^s, so that $k(\Omega)$ is the splitting field of f over k in k^s. Let C be the smooth projective

But, what is so special about characteristic 2?

Fact

For $g > 1$, $\mathcal{A}[2]$ is the set of all fixed points under the action of ι and these points are singular points of $\mathrm{Kum}(\mathcal{A})$.

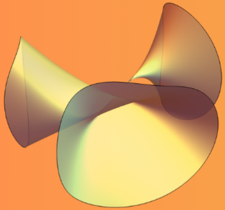
In algebraically closed fields of characteristic 2, the 2-torsion of the Jacobian of a curve $\mathcal{C}$ of genus g is

$$\mathcal{J}(\mathcal{C})[2] \cong (\mathbb{Z}/2\mathbb{Z})^r$$

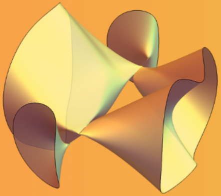
for some $0 \leq r \leq g$.

Characteristic	2			Not 2
2-rank	0	1	2	
Number of singularities	1	2	4	16
Singularity type	Elliptic	D_8	D_4	A_1

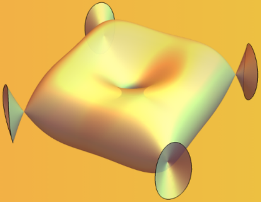
Characteristic 2



Supersingular

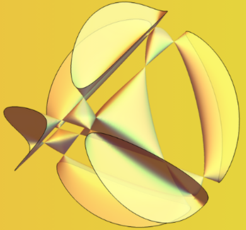


“Almost” Ordinary



Ordinary

Characteristic different than 2



But, what is so special about characteristic 2? Part II

In characteristic 2 we cannot diagonalise the action of $\iota_{\mathcal{C}}$, so it does no longer makes sense to talk about even and odd functions.

So what can be said about Kummer surfaces in characteristic two?

Kummer surfaces in characteristic 2

Arithmetic side

Geometric side

Arithmetic side

WARWICK
THE UNIVERSITY OF WARWICK

Theorem / Computation (G.)

Given a genus 2 curve $\mathcal{C}$ defined over a field k of characteristic 2, it is possible to find a basis of $\mathcal{L}(2(\Theta_+ + \Theta_-))$ that gives an explicit embedding of $\mathrm{Jac}(\mathcal{C})$ inside of $\mathbb{P}^{15}$.

$\Rightarrow$ With small modifications, we can repeat the reasoning of the previous example to study curves over fields of characteristic 2.

Geometric side

Theorem (G.)

Given a genus 2 curve $\mathcal{C}$ defined over a number field whose Jacobian has good reduction at a prime $\mathfrak{p}$ lying above 2, consider the following diagram

$$\begin{array}{ccc} \mathrm{Kum}(\mathcal{C}) & \overset{\phi^{-1}}{\dashleftarrow} & Y \\ \downarrow{\scriptstyle \mathrm{red}_{\mathfrak{p}}} & & \downarrow{\scriptstyle \mathrm{red}_{\mathfrak{p}}} \\ \mathrm{Kum}(\mathcal{C}_{\mathfrak{p}}) & \overset{\phi_{\mathfrak{p}}^{-1}}{\dashleftarrow} & Y_{\mathfrak{p}} \end{array}$$

Then, $Y_{\mathfrak{p}} \subset \mathbb{P}^5$ defines a partial desingularisation of $\mathrm{Kum}(\mathcal{C}_{\mathfrak{p}})$.

Geometric side

2-rank	0	1	2
Number of tropes	1	2	4
Singularities	$1\times$ Elliptic	$2 \times D_8$	$4 \times D_4$
Singularities after partial desingularisation	$1\times$ Simpler elliptic	$2 \times D_4 + 2 \times A_3$	$12 \times A_1$

Thank you!

Any questions?