Invariants of Artin-Schreier curves

Juanita Duque Rosero
Boston University

Joint work with Heidi Goodson, Elisa Lorenzo García, Beth Malmskog, and Renate Scheidler

Recognize the Colombian bird species

Credit: Rodrigo Duque López

Recognize the Colombian bird species

(Up to isomorphism)

Credit: Rodrigo Duque López

Recognize the Colombian bird species

(Up to isomorphism)

$\simeq$

The j-invariant

Given an **elliptic curve** over a field K,

$$E\colon\ y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6,$$

its j-invariant is

$$\begin{aligned} j(E) \;=\; & \big(a_1^{12} + 24a_1^{10}a_2 - 72a_1^9a_3 + 240a_1^8a_2^2 - 144a_1^8a_4 - 1152a_1^7a_2a_3 + 1280a_1^6a_2^3 - 2304a_1^6a_2a_4 + 1728a_1^6a_3^2 \\ & -6912a_1^5a_2^2a_3 + 6912a_1^5a_3a_4 + 3840a_1^4a_2^4 - 13824a_1^4a_2^2a_4 + 13824a_1^4a_2a_3^2 + 6912a_1^4a_4^2 - 18432a_1^3a_2^3a_3 \\ & +55296a_1^3a_2a_3a_4 - 13824a_1^3a_3^3 + 6144a_1^2a_2^5 - 36864a_1^2a_2^3a_4 + 27648a_1^2a_2^2a_3^2 + 55296a_1^2a_2a_4^2 - 82944a_1^2a_3^2a_4 \\ & -18432a_1a_2^4a_3 + 110592a_1a_2^2a_3a_4 - 165888a_1a_3a_4^2 + 4096a_2^6 - 36864a_2^4a_4 + 110592a_2^2a_4^2 - 110592a_4^3\big) \\ & \big(- a_1^6a_6 + a_1^5a_3a_4 - a_1^4a_2a_3^2 - 12a_1^4a_2a_6 + a_1^4a_4^2 + 8a_1^3a_2a_3a_4 + 9a_1^3a_3^4 - 8a_1^3a_3^3 + 36a_1^3a_3a_6 - 8a_1^2a_2^2a_3^2 \\ & -48a_1^2a_2^2a_6 + 8a_1^2a_2a_4^2 + 18a_1^2a_3^3a_4 - 48a_1^2a_3^2a_4 + 72a_1^2a_4a_6 + 16a_1a_2^2a_3a_4 + 36a_1a_2a_3^4 + 144a_1a_2a_3a_6 \\ & -96a_1a_3a_4^2 - 16a_2^3a_3^2 - 64a_2^3a_6 + 16a_2^2a_4^2 + 72a_2a_3^3a_4 + 288a_2a_4a_6 - 27a_3^6 - 216a_3^3a_6 - 64a_4^3 - 432a_6^2\big)^{-1} \end{aligned}$$

The j-invariant

Given an **elliptic curve** over a field K,

$$E\colon\ y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6,$$

its j-invariant is

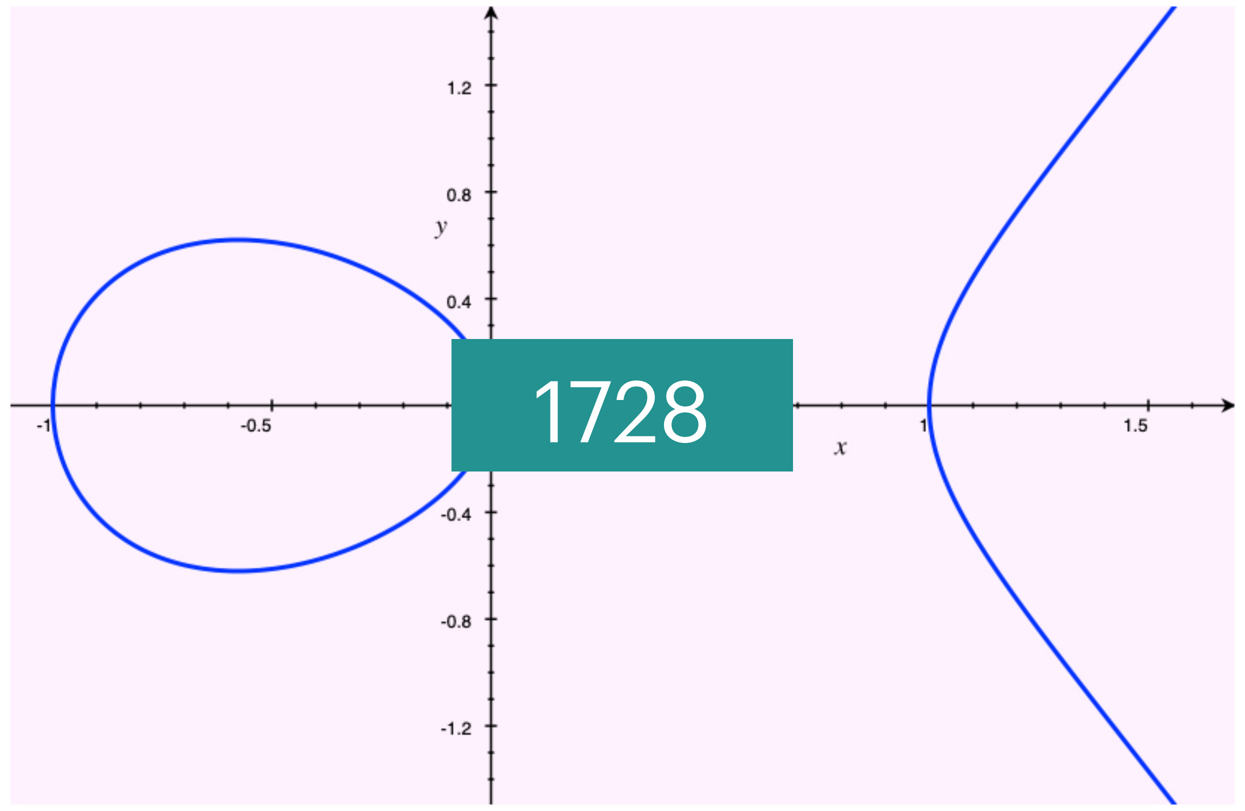
$$\begin{aligned} j(E) \;=\; & \big(a_1^{12} + 24a_1^{10}a_2 - 72a_1^9a_3 + 240a_1^8a_2^2 - 144a_1^8a_4 - 1152a_1^7a_2a_3 + 1280a_1^6a_2^3 - 2304a_1^6a_2a_4 + 1728a_1^6a_3^2 \\ & -6912a_1^5a_2^2a_3 + 6912a_1^5a_3a_4 + 3840a_1^4a_2^4 - 13824a_1^4a_2^2a_4 + 13824a_1^4a_2a_3^2 + 6912a_1^4a_4^2 - 18432a_1^3a_2^3a_3 \\ & +55296a_1^3a_2a_3a_4 - 13824a_1^3a_3^3 + 6144a_1^2a_2^5 - 36864a_1^2a_2^3a_4 + 27648a_1^2a_2^2a_3^2 + 55296a_1^2a_2a_4^2 - 82944a_1^2a_3^2a_4 \\ & -18432a_1a_2^4a_3 + 110592a_1a_2^2a_3a_4 - 165888a_1a_3a_4^2 + 4096a_2^6 - 36864a_2^4a_4 + 110592a_2^2a_4^2 - 110592a_4^3\big) \\ & \big(-a_1^6a_6 + a_1^5a_3a_4 - a_1^4a_2a_3^2 - 12a_1^4a_2a_6 + a_1^4a_4^2 + 8a_1^3a_2a_3a_4 + 9a_1^3a_3^4 - 8a_1^3a_3^3 + 36a_1^3a_3a_6 - 8a_1^2a_2^2a_3^2 \\ & -48a_1^2a_2^2a_6 + 8a_1^2a_2a_4^2 + 18a_1^2a_3^3a_4 - 48a_1^2a_3^2a_4 + 72a_1^2a_4a_6 + 16a_1a_2^2a_3a_4 + 36a_1a_2a_3^4 + 144a_1a_2a_3a_6 \\ & -96a_1a_3a_4^2 - 16a_2^3a_3^2 - 64a_2^3a_6 + 16a_2^2a_4^2 + 72a_2a_3^3a_4 + 288a_2a_4a_6 - 27a_3^6 - 216a_3^3a_6 - 64a_4^3 - 432a_6^2\big)^{-1} \end{aligned}$$

Theorem. Two elliptic curves E_1 and E_2 are isomorphic over $\overline{K}$ if and only if $j(E_1) = j(E_2)$.

The j-invariant

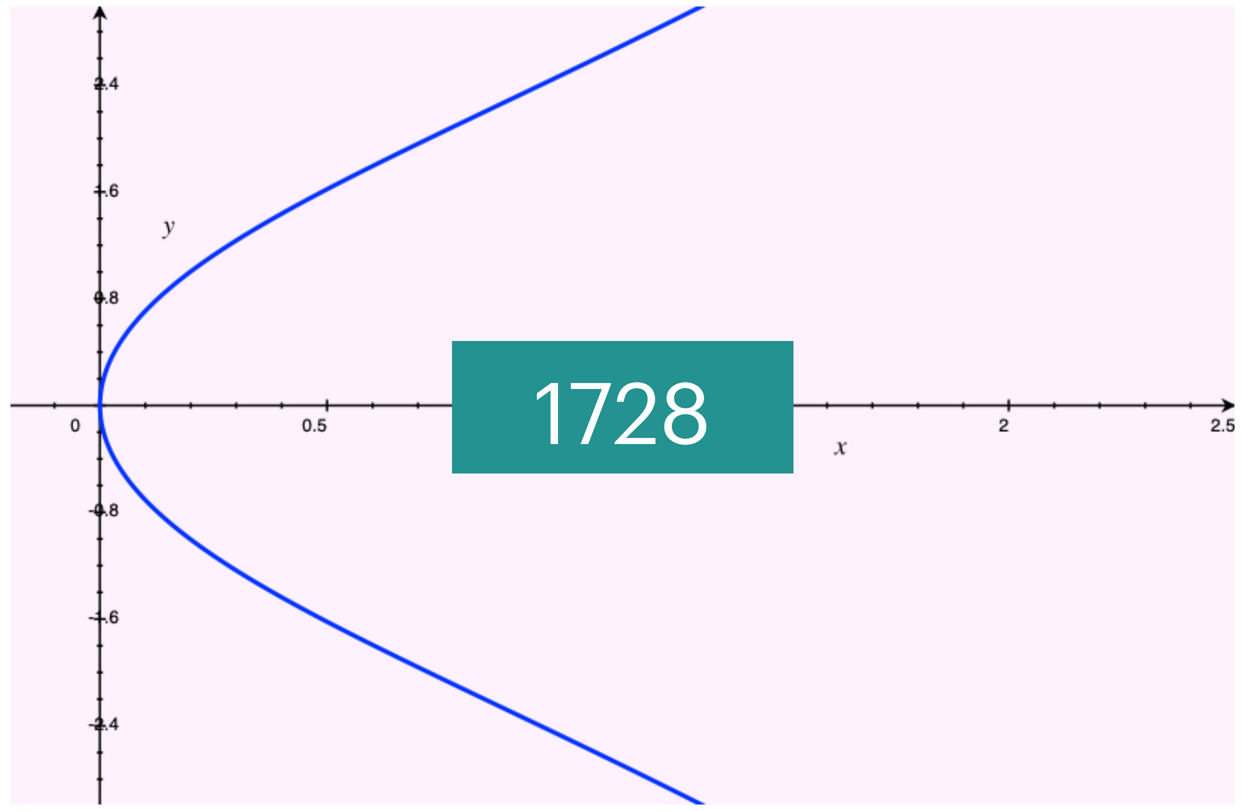
The value $j(E)$ is a **reconstructing invariant**: for all $j(E) \in \overline{\mathbb{Q}}$, there is an elliptic curve with this j-invariant.

Example. For $j(E) = 1728$, we can pick



$$a_1 = a_2 = a_3 = a_6 = 0 \text{ and } a_4 = -1$$
$$y^2 = x^3 - x$$

$$\simeq$$



$$a_1 = a_2 = a_3 = a_6 = 0 \text{ and } a_4 = 5$$
$$y^2 = x^3 + 5x$$

Invariants for curves

- Elliptic curves (genus 1): j-invariant.
- Genus 2 curves over $\mathbb{Q}$: Igusa-Clebsch invariants [Igusa '60].
- Genus 3 non-hyperelliptic curves [Ohno '07].
- Genus 3 hyperelliptic curves [Shioda '67, Lercier-Ritzenthaler '12].

Invariants for curves

- Elliptic curves (genus 1): j-invariant.
- Genus 2 curves over $\mathbb{Q}$: Igusa-Clebsch invariants [Igusa '60].
- Genus 3 non-hyperelliptic curves [Ohno '07].
- Genus 3 hyperelliptic curves [Shioda '67, Lercier-Ritzenthaler '12].

Today: Invariants for Artin-Schreier curves.

Artin-Schreier curves

Fix a prime p. An **Artin-Schreier curve** over $\overline{\mathbb{F}}_p$ is a curve of the form

$$C_f\colon\ y^p - y = f(x),$$

where $f(x) \in \overline{\mathbb{F}}_p(x)$ and $f(x) \neq z^p - z$ for any $z \in \overline{\mathbb{F}}_p(x)$.

Artin-Schreier curves

Fix a prime p. An **Artin-Schreier curve** over $\overline{\mathbb{F}}_p$ is a curve of the form

$$C_f\colon\ y^p - y = f(x),$$

where $f(x) \in \overline{\mathbb{F}}_p(x)$ and $f(x) \neq z^p - z$ for any $z \in \overline{\mathbb{F}}_p(x)$.

The genus of C_f is $\dfrac{p-1}{2}\sum (d_i + 1)$, where the order of the poles of $f(x)$ is d_i.

Artin-Schreier curves

Fix a prime p. An **Artin-Schreier curve** over $\overline{\mathbb{F}}_p$ is a curve of the form

$$C_f\colon\ y^p - y = f(x),$$

where $f(x) \in \overline{\mathbb{F}}_p(x)$ and $f(x) \neq z^p - z$ for any $z \in \overline{\mathbb{F}}_p(x)$.

The genus of C_f is $\dfrac{p-1}{2}\sum (d_i + 1)$, where the order of the poles of $f(x)$ is d_i.

Applications to coding theory. van der Geer and van der Vlugt, for example, study codes coming from the curves $y^p - y = ax + 1/x$ and construct curves with many points using Artin-Schreier curves.

Describing the moduli space

- Given $g \geq 0$, we study $\mathscr{AS}_g$, the moduli space of Artin-Schreier $\overline{\mathbb{F}}_p$-curves of genus g.
- Let $\mathscr{AS}_{g,s}$ be the locus of $\mathscr{AS}_g$ corresponding to the curves with p-rank exactly s.
- **Theorem [Pries-Zhu '12].** The set of irreducible components of $\mathscr{AS}_{g,s}$ is in bijection with the set of partitions of $\big((2g)(p-1)^{-1}+2\big)$ into $\big(s(p-1)^{-1}+1\big)$ positive integers that are not equal to 1 modulo p.
- **Example.** For $p = 3$,

$$\mathscr{AS}_{11,8} = \mathscr{AS}_{[5,2,2,2,2]} + \mathscr{AS}_{[3,3,3,2,2]}\,.$$

Artin-Schreier curves

Theorem [D.-Goodson-Lorenzo García-Malmskog-Scheidler '24]. There is an explicit set of reconstructing invariants for all Artin-Schreier curves of genus 3 and 4 in odd characteristic.

Artin-Schreier curves

Theorem [D.-Goodson-Lorenzo García-Malmskog-Scheidler '24]. There is an explicit set of reconstructing invariants for all Artin-Schreier curves of genus 3 and 4 in odd characteristic.

Theorem [D.-Lorenzo García-Malmskog-Scheidler *(in progress)*]. There is an algorithm to find the set of reconstructing invariants for $\mathscr{AS}_{g,s}$ in odd characteristic.

Artin-Schreier curves

Theorem [D.-Goodson-Lorenzo García-Malmskog-Scheidler '24]. There is an explicit set of reconstructing invariants for all Artin-Schreier curves of genus 3 and 4 in odd characteristic.

Theorem [D.-Lorenzo García-Malmskog-Scheidler *(in progress)*]. There is an algorithm to find the set of reconstructing invariants for $\mathcal{AS}_{g,s}$ in odd characteristic.

Steps:

1. Define standard forms.
2. Find all possible isomorphisms to other curves in standard form.
3. Compute invariants of the ring.

Artin-Schreier curves

Theorem [D.-Goodson-Lorenzo García-Malmskog-Scheidler '24]. There is an explicit set of reconstructing invariants for all Artin-Schreier curves of genus 3 and 4 in odd characteristic.

Theorem [D.-Lorenzo García-Malmskog-Scheidler *(in progress)*]. There is an algorithm to find the set of reconstructing invariants for $\mathscr{AS}_{g,s}$ in odd characteristic.

Steps:

1. Define standard forms.
2. Find all possible isomorphisms to other curves in standard form. HARD!
3. Compute invariants of the ring.

Artin-Schreier curves

Theorem [D.-Goodson-Lorenzo García-Malmskog-Scheidler ’24]. There is an explicit set of reconstructing invariants for all Artin-Schreier curves of genus 3 and 4 in odd characteristic.

Theorem [D.-Lorenzo García-Malmskog-Scheidler *(in progress)*]. There is an algorithm to find the set of reconstructing invariants for $\mathscr{AS}_{g,s}$ in odd characteristic.

Steps:

1. Define standard forms.
2. Find all possible isomorphisms to other curves in standard form. HARD!
3. Compute invariants of the ring. EXPENSIVE!

Isomorphisms

Lemma. Any isomorphism between Artin-Schreier curves is given by a map of the form

$$(x, y) \mapsto \left(\frac{\alpha x + \beta}{\gamma x + \delta}, \lambda y + h(x)\right),$$

where

$$\lambda \in \mathbb{F}_p^{\times}, \qquad \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \in \mathrm{GL}_2(\overline{\mathbb{F}}_p), \qquad h(x) \in \overline{\mathbb{F}}_p(x).$$

Isomorphisms

Lemma. Any isomorphism between Artin-Schreier curves is given by a map of the form

$$(x, y) \mapsto \left(\frac{\alpha x + \beta}{\gamma x + \delta}, \lambda y + h(x) \right),$$

where

$$\lambda \in \mathbb{F}_p^{\times}, \qquad \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \in \mathrm{GL}_2(\overline{\mathbb{F}}_p), \qquad h(x) \in \overline{\mathbb{F}}_p(x).$$

Example. $y^3 - y = x^4 - x^3 - x^2 + x$ and $y^3 - y = x^4 - x^2$ are isomorphic via

$$(x, y) \mapsto (-x + 1, y - \epsilon), \text{ where } \epsilon \text{ is a root of } t^3 - t - 1 = 0.$$

Standard form

Let p be an odd prime and $C_f\colon\ y^p - y = f(x)$ be an Artin-Schreier $\overline{\mathbb{F}}_p$-curve with $f(x)$ having exactly one pole of order d. Then C_f is isomorphic to an Artin-Schreier curve

$$C\colon\ y^p - y = x^d + Q(x),$$

where $Q(x) \in \overline{\mathbb{F}}_p[x]$ is a multiple of x^2 and no monomial appearing in $Q(x)$ has an exponent that is divisible by p.

Standard form

Let p be an odd prime and $C_f\colon\ y^p - y = f(x)$ be an Artin-Schreier $\overline{\mathbb{F}}_p$-curve with $f(x)$ having exactly 3 poles of respective orders $d_1 \geq d_2 \geq d_3$. Then C_f is isomorphic to

$$C_g\colon\ y^p - y = g(x),$$

where $g(x) \in \overline{\mathbb{F}}_p(x)$ is given by

$$g(x) = F(x) + G\left(\frac{1}{x}\right) + H\left(\frac{1}{x-1}\right),$$

for $F(x), G(x), H(x) \in \overline{\mathbb{F}}_p[x]$, $\deg(F) = d_1,\ \deg(G) = d_2,\ \deg(H) = d_3$, and no monomial appearing in $F(x), G(x), H(x)$, has an exponent that is divisible by p.

Example: $\mathscr{AS}_{3,0}$

Example: $\mathscr{AS}_{3,0}$

Every Artin-Schreier $\overline{\mathbb{F}}_3$-curve with $f(x)$ having only one pole of order 4 is isomorphic to a curve of the form

$$C\colon\ y^3 - y = x^4 + ax^2$$

where $a \in \overline{\mathbb{F}}_3$.

Example: $\mathscr{AS}_{3,0}$

Every Artin-Schreier $\overline{\mathbb{F}}_3$-curve with $f(x)$ having only one pole of order 4 is isomorphic to a curve of the form

$$C\colon y^3 - y = x^4 + ax^2$$

where $a \in \overline{\mathbb{F}}_3$.

To describe the space $\mathscr{AS}_{3,0}$ of Artin-Schreier $\overline{\mathbb{F}}_3$-curves with genus 3 and p-rank 0, it is enough to give $a \in \overline{\mathbb{F}}_p$!

Example: $\mathcal{AS}_{3,0}$

$$C\colon y^3 - y = x^4 + ax^2$$

Isomorphisms between curves in standard form with $a \neq 0$ are given, up to composition with powers of $\sigma\colon (x, y) \mapsto (x, y + 1)$, by

$$(x, y) \mapsto (\alpha x, \lambda y),$$

where $\lambda \in \mathbb{F}_3^\times$ and $\alpha \in \overline{\mathbb{F}}_3$ with $\alpha^4 = \lambda$.

Example: $\mathscr{AS}_{3,0}$

$$C\colon\ y^3 - y = x^4 + ax^2$$

Isomorphisms between curves in standard form with $a \neq 0$ are given, up to composition with powers of $\sigma\colon\ (x, y) \mapsto (x, y + 1)$, by

$$(x, y) \mapsto (\alpha x, \lambda y),$$

where $\lambda \in \mathbb{F}_3^\times$ and $\alpha \in \overline{\mathbb{F}}_3$ with $\alpha^4 = \lambda$.

Now we have a finite group G acting on $\overline{\mathbb{F}}_3[a]$!

Example: $\mathscr{AS}_{3,0}$

$$C\colon y^3 - y = x^4 + ax^2$$

$$(x, y) \mapsto (\alpha x, \lambda y), \quad \lambda \in \mathbb{F}_3^\times \text{ and } \alpha \in \overline{\mathbb{F}}_3 \text{ with } \alpha^4 = \lambda.$$

λ	α	$\tilde{C}$	a
1	ζ_8^2	$y^3 - y = x^4 + \zeta_8^4 ax^2$	$\zeta_8^4 a$
1	ζ_8^4	$y^3 - y = x^4 + ax^2$	$\zeta_8^8 a$
1	ζ_8^6	$y^3 - y = x^4 + \zeta_8^4 ax^2$	$\zeta_8^4 a$
1	ζ_8^8	$y^3 - y = x^4 + ax^2$	$\zeta_8^8 a$

λ	α	$\tilde{C}$	a
-1	ζ_8	$y^3 - y = x^4 - \zeta_8^2 ax^2$	$\zeta_8^6 a$
-1	ζ_8^3	$y^3 - y = x^4 - \zeta_8^6 ax^2$	$\zeta_8^2 a$
-1	ζ_8^5	$y^3 - y = x^4 - \zeta_8^2 ax^2$	$\zeta_8^6 a$
-1	ζ_8^7	$y^3 - y = x^4 - \zeta_8^6 ax^2$	$\zeta_8^2 a$

Example: $\mathscr{AS}_{3,0}$

$$C\colon\ y^3 - y = x^4 + ax^2$$

$$(x, y) \mapsto (\alpha x, \lambda y), \quad \lambda \in \mathbb{F}_3^\times \text{ and } \alpha \in \overline{\mathbb{F}}_3 \text{ with } \alpha^4 = \lambda.$$

$$\{a\}^G = \{\zeta_8^4 a,\ \zeta_8^8 a,\ \zeta_8^6 a,\ \zeta_8^2 a\}$$

Example: $\mathscr{AS}_{3,0}$

$$C\colon\ y^3 - y = x^4 + ax^2$$

$$(x, y) \mapsto (\alpha x, \lambda y), \quad \lambda \in \mathbb{F}_3^\times \text{ and } \alpha \in \overline{\mathbb{F}}_3 \text{ with } \alpha^4 = \lambda.$$

$$\{a\}^G = \{\zeta_8^4 a,\ \zeta_8^8 a,\ \zeta_8^6 a,\ \zeta_8^2 a\}$$

Corollary. The element a^4 is a reconstructing invariant and generates the ring of invariants for $\mathscr{AS}_{3,0}$.

Example: $\mathscr{AS}_{3,0}$

If we start with a model

$$C\colon y^3 - y = \frac{ax^4 + bx^3 + cx^2 + dx + e}{(x-\tau)^4},$$

the reconstructing invariant can be chosen to be

$$I(C) = \frac{c^4}{(a\tau^4 + b\tau^3 + c\tau^2 + d\tau + e)^4}.$$

Example: $\mathscr{AS}_{3,0}$

If we start with a model

$$C\colon y^3 - y = \frac{ax^4 + bx^3 + cx^2 + dx + e}{(x-\tau)^4},$$

the reconstructing invariant can be chosen to be

$$I(C) = \frac{c^4}{(a\tau^4 + b\tau^3 + c\tau^2 + d\tau + e)^4}.$$

Example.

$$\begin{array}{rcll} I(y^3 - y = x^4 - x^3 - x^2 + x) & = & I(y^3 - y = x^4 - x^2) & = \quad 1 \\ y^3 - y = x^4 - x^3 - x^2 + x & \simeq & y^3 - y = x^4 - x^2 & \\ (x, y) & \mapsto & (-x + 1, y - \epsilon) & \qquad \epsilon^3 - \epsilon - 1 = 0. \end{array}$$

Theorem [D.-Goodson-Lorenzo García-Malmskog-Scheidler '24]. A system of reconstructing invariants for all Artin-Schreier curves of genus $g = 3, 4$ in characteristic $p > 2$ is:

g	p	s	Standard form	Set of Reconstructing invariants over $\overline{\mathbb{F}}_p$
3	3	0	$y^3 - y = x^4 + ax^2$	$\{a^4\}$
3	3	2	$y^3 - y = x^2 + ax + \frac{b}{x}$	$\{a^4, ab, b^4\}$
3	7	0	$y^7 - y = x^2$	$\emptyset$
4	3	0	$y^3 - y = x^5 + cx^4 + dx^2$	$\{(c^3+d)^{10}, (-cd-\epsilon^2)^5, (c^3+d)^2(-cd-\epsilon^2)\}$ where $\epsilon^3 = c$
4	3	2	$y^3 - y = x^2 + ax + \frac{b}{x} + \frac{c}{x^2}$	$\{c, ab, a^4c^2 - b^4\}$
4	3	4	$y^3 - y = x^2 + ax + \frac{b}{x} + \frac{c}{x-1}$	$\{(abc)^2, (abc)(a-b-c), ab+ac-bc\}$
4	5	0	$y^5 - y = x^3 + ax^2$	$\{a^{12}\}$
4	5	1	$y^5 - y = x + \frac{a}{x}$	$\{a^2\}$

The general algorithm

Algorithm [D.-Lorenzo García-Malmskog-Scheidler (*in progress*)].

Input: $g \geq 0$ and $s \geq 0$.

Output: A set of reconstructing invariants for $\mathcal{AS}_{g,s}$.

1. Write a general curve C in *standard form,* with variables $a_1, \ldots, a_n$.
2. Find the possible transformations of C that produce a new curve in standard form. They are compositions of the following:
    a. Swap poles that are not distinguished and have the same pole order.
    b. Pick new distinguished poles (keeping the order of the poles the same).
    c. Act with $\lambda \in \overline{\mathbb{F}}_p$ as $(x, y) \mapsto (x, \lambda y)$.
3. Collect the possible images of $a_1, \ldots, a_n$ under the transformations from step 2.
4. Compute invariants of this ring.

Thank you!

Thank you!

Theorem [D.-Goodson-Lorenzo García-Malmskog-Scheidler '24]. There is an explicit set of reconstructing invariants for all Artin-Schreier curves of genus 3 and 4 in odd characteristic.

Theorem [D.-Lorenzo García-Malmskog-Scheidler *(in progress)*]. There is an algorithm to find the set of reconstructing invariants for $\mathscr{AS}_{g,s}$ in odd characteristic.

Steps:

1. Define standard forms.
2. Find all possible isomorphisms to other curves in standard form. HARD!
3. Compute invariants of the ring. EXPENSIVE!