Curves and Jacobians

Nicolas Mascot

LIBPARI25
25 Jun 2025

Question

Let C be the plane curve over $\mathbb{Q}$ defined by $F(x, y) = 0$, where

$$F(x,y) = 27y^8 + (16x^{15} - 96x^{14} - 384x^{13} + 3232x^{12} - 5424x^{11} + 960x^{10} + 960x^8 + 5424x^7 + 3232x^6 + 384x^5 - 96x^4 - 16x^3)y^6$$
$$+(-288x^{28} + 3456x^{27} - 14400x^{26} + 14976x^{25} + 56160x^{24} - 142848x^{23} - 52992x^{22} + 400896x^{21} - 55872x^{20} - 624384x^{19}$$
$$+134784x^{18} + 624384x^{17} - 55872x^{16} - 400896x^{15} - 52992x^{14} + 142848x^{13} + 56160x^{12} - 14976x^{11} - 14400x^{10} - 3456x^9 - 288x^8)y^4$$
$$-256x^{56} + 6144x^{55} - 62464x^{54} + 333824x^{53} - 859648x^{52} - 120832x^{51} + 7252992x^{50} - 16046080x^{49} - 9891072x^{48} + 90136576x^{47}$$
$$-73076736x^{46} - 237805568x^{45} + 420485120x^{44} + 341843968x^{43} - 1165840384x^{42} - 192667648x^{41} + 2178936320x^{40} - 238563328x^{39}$$
$$-3063240704x^{38} + 639488000x^{37} + 3412593664x^{36} - 639488000x^{35} - 3063240704x^{34} + 238563328x^{33} + 2178936320x^{32}$$
$$+192667648x^{31} - 1165840384x^{30} - 341843968x^{29} + 420485120x^{28} + 237805568x^{27} - 73076736x^{26} - 90136576x^{25} - 9891072x^{24}$$
$$+16046080x^{23} + 7252992x^{22} + 120832x^{21} - 859648x^{20} - 333824x^{19} - 62464x^{18} - 6144x^{17} - 256x^{16}.$$

What is the genus of C?

Goals

Fix a field K (think $K = \mathbb{Q}$).

Consider a curve

$$C : F(x, y) = 0$$

where $F(x, y) \in K[x, y]$ irreducible over $\overline{K}$.

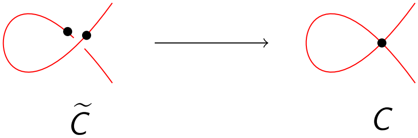
We would like to

- Determine the genus of C,
- Compute Riemann-Roch spaces on C,
- Construct the Jacobian of C,
- ...

Goals

- Determine the genus of C,
- Compute Riemann-Roch spaces on C,
- Construct the Jacobian of C,
- ...

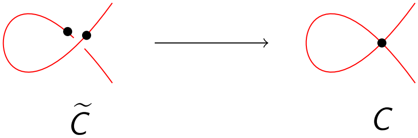
All this actually refers to the desingularisation $\widetilde{C} \to C$ of C.



Goals

- Determine the genus of C,
- Compute Riemann-Roch spaces on C,
- Construct the Jacobian of C,
- $\dots$

All this actually refers to the desingularisation $\widetilde{C} \to C$ of C.



Main idea: represent "difficult" points of $\widetilde{C}$ by formal parametrisations $x(t), y(t) \in \overline{K}((t))$.
These series can be found by a desingularisation process based on Puiseux series (factorisation of $F(x,y)$ in $K((x))[y]$).

Handling field extensions

$$K \subset L \subset M$$

Suppose we have a field extension $L = K[a]/A(a)$ of the ground field K, and let $P(x) \in L[x]$.

Handling field extensions

$$K \subset L \subset M$$

Suppose we have a field extension $L = K[a]/A(a)$ of the ground field K, and let $P(x) \in L[x]$.

Want to factor $P(x) = \prod_i P_i(x)$ over L. Furthermore, for each i, want to represent

$$M_i = L[x]/P_i(x)$$

as $M_i = K[b]/B_i(b)$ along with an expression $a = a(b) \in K[b]$ so as to understand $L \subset M_i$.

Handling field extensions

$$K \subset L \subset M$$

Suppose we have a field extension $L = K[a]/A(a)$ of the ground field K, and let $P(x) \in L[x]$.

Want to factor $P(x) = \prod_i P_i(x)$ over L. Furthermore, for each i, want to represent

$$M_i = L[x]/P_i(x)$$

as $M_i = K[b]/B_i(b)$ along with an expression $a = a(b) \in K[b]$ so as to understand $L \subset M_i$.

Implemented for $K = \mathbb{Q}$ and $\mathbb{Q}(\alpha)$ (with `polred`), $\mathbb{F}_p$, $\mathbb{F}_q$; should also work for general K of characteristic 0, as long as `factor` accepts inputs in $K[x]$.

Computing the genus

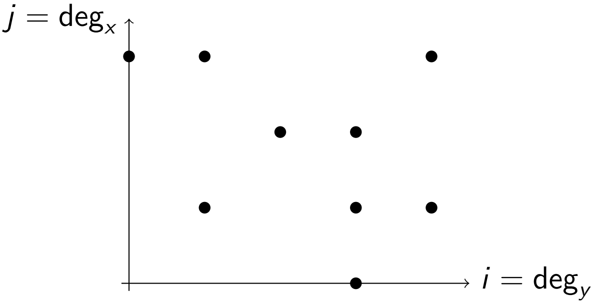
Theorem

For (i, j) strictly in the convex hull of the support of $F(x, y)$, the differential $\omega_{i,j} = \frac{x^{j-1}y^{i-1}}{\partial F/\partial y}\,\mathrm{d}x$ is regular everywhere on $F(x, y) = 0$, except maybe at singular points.
Any regular differential is a linear combination of these.

Computing the genus

Theorem

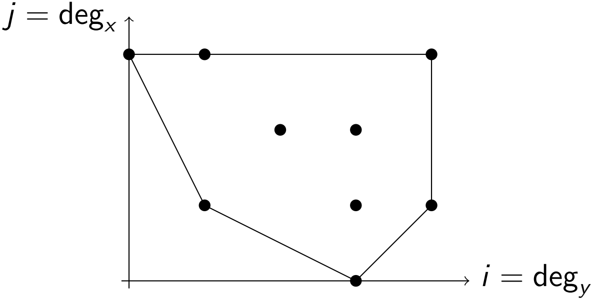
For (i, j) strictly in the convex hull of the support of $F(x, y)$, the differential $\omega_{i,j} = \frac{x^{j-1}y^{i-1}}{\partial F / \partial y} \mathrm{d}x$ is regular everywhere on $F(x, y) = 0$, except maybe at singular points.
Any regular differential is a linear combination of these.



Computing the genus

Theorem

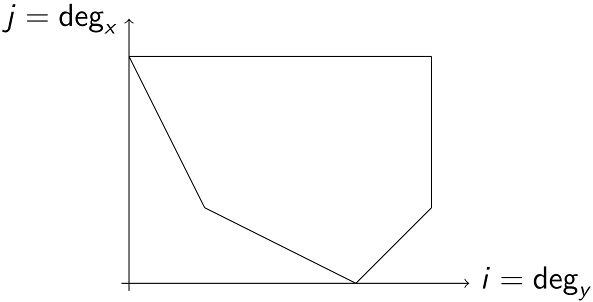
For (i, j) strictly in the convex hull of the support of $F(x, y)$, the differential $\omega_{i,j} = \frac{x^{j-1}y^{i-1}}{\partial F/\partial y}\,\mathrm{d}x$ is regular everywhere on $F(x, y) = 0$, except maybe at singular points.
Any regular differential is a linear combination of these.



Computing the genus

Theorem

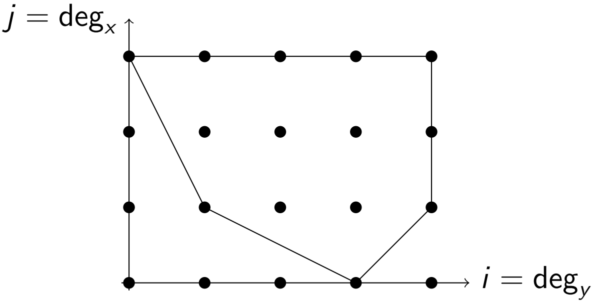
For (i,j) strictly in the convex hull of the support of $F(x,y)$, the differential $\omega_{i,j} = \frac{x^{j-1}y^{i-1}}{\partial F/\partial y}\,\mathrm{d}x$ is regular everywhere on $F(x,y)=0$, except maybe at singular points.
Any regular differential is a linear combination of these.



Computing the genus

Theorem

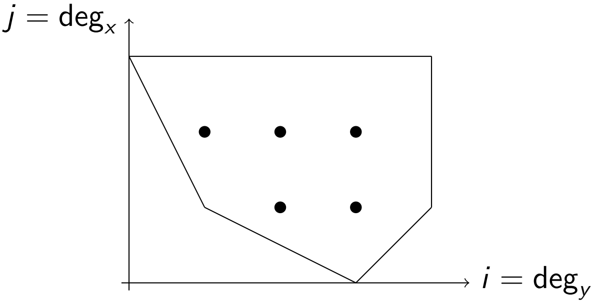
For (i, j) strictly in the convex hull of the support of $F(x, y)$, the differential $\omega_{i,j} = \frac{x^{j-1}y^{i-1}}{\partial F/\partial y}\,\mathrm{d}x$ is regular everywhere on $F(x, y) = 0$, except maybe at singular points. Any regular differential is a linear combination of these.



Computing the genus

Theorem

For (i,j) strictly in the convex hull of the support of $F(x,y)$, the differential $\omega_{i,j} = \frac{x^{j-1}y^{i-1}}{\partial F/\partial y}\,\mathrm{d}x$ is regular everywhere on $F(x,y)=0$, except maybe at singular points.
Any regular differential is a linear combination of these.



Computing the genus

Theorem

For (i,j) strictly in the convex hull of the support of $F(x,y)$, the differential $\omega_{i,j} = \frac{x^{j-1}y^{i-1}}{\partial F/\partial y}\,\mathrm{d}x$ is regular everywhere on $F(x,y)=0$, except maybe at singular points.
Any regular differential is a linear combination of these.

$\rightsquigarrow$ Strategy: Compute local parametrisations at all the singular points . Plug them into the $\omega_{i,j}$, and use linear algebra over K to find the combinations whose polar parts vanish.

$\rightsquigarrow$ Get K-basis of the space $\Omega(C)$ of holomorphic differentials. The genus of the curve is its dimension.

Application: Hyperelliptic curves

Suppose we find C has genus 2 $\rightsquigarrow$ has Weierstrass model

$$H : w^2 = f(u).$$

$\Omega^1(H) = \langle \frac{\mathrm{d}u}{w}, \frac{u\,\mathrm{d}u}{w} \rangle \rightsquigarrow$ our basis of $\Omega^1(C)$ is $\frac{(au+b)\,\mathrm{d}u}{w}$, $\frac{(cu+d)\,\mathrm{d}u}{w}$
$\rightsquigarrow$ Their quotient is $\frac{au+b}{cu+d}$.

Application: Hyperelliptic curves

Suppose we find C has genus 2 $\rightsquigarrow$ has Weierstrass model

$$H : w^2 = f(u).$$

$\Omega^1(H) = \langle \frac{du}{w}, \frac{u\,du}{w} \rangle \rightsquigarrow$ our basis of $\Omega^1(C)$ is $\frac{(au+b)\,du}{w}$, $\frac{(cu+d)\,du}{w}$
$\rightsquigarrow$ Their quotient is $\frac{au+b}{cu+d}$.

Theorem (van Hoeij)

More generally, let $\Omega(C) = \langle \omega_1, \cdots, \omega_g \rangle$, and let d be the dimension of the span of the $\omega_i \omega_j$.

- *If C is hyperelliptic, then there exist $u, w \in K(C)$ such that $[K(C) : K(u)] = 2$ and*

$$\Omega(C) = \left\langle \frac{u^i du}{w} \,\middle|\, 0 \leqslant i \leqslant g-1 \right\rangle,$$

  so $d = 2g - 1$.
- *If C is not hyperelliptic, then $d > 2g - 1$.*

Application: Canonical projections

Let $\Omega(C) = \langle \omega_1, \cdots, \omega_g \rangle$. The canonical embedding is

$$C \xrightarrow{(\omega_1 : \cdots : \omega_g)} \mathbb{P}^{g-1}.$$

- If C is not hyperelliptic, this is really an embedding.
- If C is hyperelliptic, then this is $2:1$ with image a conic.

When C is not hyperelliptic, we can project onto a plane $\rightsquigarrow$ nicer equations for C.

Example

By this method, we find a much nicer model for our horrible curve of genus 7:
$(3y^5 - 6y^3 + 3y)x^4 + (2y^8 - 8y^7 + 4y^6 + 12y^5 + 12y^3 - 4y^2 - 8y - 2)x^2$
$+(9y^9 - 36y^8 - 36y^7 + 36y^6 + 18y^5 - 36y^4 - 36y^3 + 36y^2 + 9y) = 0.$

Riemann-Roch

Let $D = \sum n_{\widetilde{P}} \widetilde{P}$ formal $\mathbb{Z}$-linear combination of points of $\widetilde{C}$.
The attached Riemann-Roch space is

$$\mathcal{L}(D) = \{f \in K(C) \mid \operatorname{ord}_{\widetilde{P}} h \geqslant -n_{\widetilde{P}} \text{ for all } \widetilde{P} \in \widetilde{C}\}.$$

This is a finite-dimensional K-vector space. We want a basis.

Represent points $\widetilde{P} \in \widetilde{C}$ either as nonsingular points $P \in C$, or as local parametrisations.

Strategy:

- Precompute the integral closure $\mathcal{O}_C$ of $K[x]$ in the function field $K(C) = K(x)[y]/F(x,y)$ of C.
- Find common denominator $d(x) \in K[x]$ such that $f(x,y) \in \mathcal{L}(D) \Longrightarrow d(x)h(x,y) \in \mathcal{O}_C$.
- Use local parametrisations to find combinations vanishing at appropriate order at relevant points.

Example: Creation, divisors, Riemann-Roch

```
C=crvinit(x^11+y^7-2*x*y^5,t,a);
crvprint(C)

P=[1,1]
D=[P,-3;1,2;2,-1]
crvdivprint(C,D);

L=crvRR(C,D)
crvfndiv(C,L[1],1);
crvfndiv(C,L[2],1);
```

Example: Rational curves

```
f=x^5+y^7+Mod(b,b^2-2)*x^3*y^3;
C=crvinit(f,t,a);
crvprint(C)

[T,param]=crvrat(C,1,3)

lift(param)
substvec(f,[x,y],param)

lift(T)
crvfndiv(C,T,1);

crvrat(C)
```

Example: Hyperelliptic / elliptic curves

```
C=crvinit(x^5+y^6+x^3*y,t,a);
crvprint(C)
crvishyperell(C)
crvhyperell(C)
```

```
C1=crvinit(x^5+y^7+x^3*y^4,t,a);
crvprint(C1)
crvell(C1,[1,-1,0])
```

Application 1: Jacobians and mod ℓ Galois representations

The Jacobian; Makdisi's algorithms

The Jacobian of $\widetilde{C}$ is an Abelian variety $J = \mathrm{Pic}^0(\widetilde{C})$.

The Jacobian; Makdisi's algorithms

The Jacobian of $\widetilde{C}$ is an Abelian variety $J = \operatorname{Pic}^0(\widetilde{C})$.

Fix an effective divisor D_0 on $\widetilde{C}$ of degree $d_0 \gg g$, and compute $V = \mathcal{L}(2D_0)$.
Also fix sufficiently many points $P_1, P_2, \cdots \in C$ to faithfully represent $v \in V$ as $(v(P_1), v(P_2), \cdots)$.

Each $x \in J = \operatorname{Pic}^0(\widetilde{C})$ is of the form $x = [D - D_0]$ for some effective D of degree d_0. Represent it by the matrix

$$\begin{pmatrix} v_1(P_1) & v_2(P_1) & \cdots \\ v_1(P_2) & v_2(P_2) & \cdots \\ \vdots & \vdots & \ddots \end{pmatrix}$$

where $v_1, v_2, \cdots$ is a basis of $\mathcal{L}(2D_0 - D) \subset \mathcal{L}(2D_0)$.

The Jacobian; Makdisi's algorithms

Fix an effective divisor D_0 on $\widetilde{C}$ of degree $d_0 \gg g$, and compute $V = \mathcal{L}(2D_0)$.

Each $x \in J = \operatorname{Pic}^0(\widetilde{C})$ is of the form $x = [D - D_0]$ for some effective D of degree d_0. Represent it by $\mathcal{L}(2D_0 - D) \subset V$.

Algorithm (Group law in J)

Given $x_1 = [D_1 - D_0]$ and $x_2 = [D_2 - D_0] \in J$, let's compute $x_3 = [D_3 - D_0] \in J$: $x_1 + x_2 + x_3 = 0$.

1. $\mathcal{L}(4D_0 - D_1 - D_2) = \mathcal{L}(2D_0 - D_1) \cdot \mathcal{L}(2D_0 - D_2)$,
2. $\mathcal{L}(3D_0 - D_1 - D_2) =$
$$\{s \in \mathcal{L}(3D_0) \mid s \cdot \mathcal{L}(D_0) \subset \mathcal{L}(4D_0 - D_1 - D_2)\},$$
3. Pick $0 \neq f \in \mathcal{L}(3D_0 - D_1 - D_2)$; then $(f) = -3D_0 + D_1 + D_2 + D_3 \rightsquigarrow x_3 = [D_3 - D_0]$,
4. $\mathcal{L}(2D_0 - D_3) =$
$$\{s \in \mathcal{L}(2D_0) \mid s \cdot \mathcal{L}(3D_0 - D_1 - D_2) \subset f\mathcal{L}(2D_0)\}.$$

Division polynomials, Galois representations

Suppose $K = \mathbb{Q}$. Let $\ell \in \mathbb{N}$ prime, suppose we want to understand the Galois action on $J[\ell]$.

1. Fix $p \neq \ell$ of good reduction. Find $q = p^a$ such that $J[\ell]$ defined over $\mathbb{F}_q$.
2. Generate $\mathbb{F}_q$-points of $J[\ell]$ until we get an $\mathbb{F}_\ell$-basis.
3. Hensel-lift these points from $J(\mathbb{F}_q)$ to $J(\mathbb{Z}_q/p^e)$, $e \gg 1$.
4. Use Makdisi to recover all of $J(\mathbb{Z}_q/p^e)[\ell]$.
5. Pick $\alpha \in \mathbb{Q}(J)$. Evaluate $\psi_\ell(x) = \prod_{t \in T} \left(x - \alpha(t)\right)$.
6. Identify $\psi_\ell(x) \in \mathbb{Q}[x]$.

And now, surfaces!

So we can compute $\mathrm{H}^1_{\text{ét}}(\text{Curve}, \mathbb{Z}/\ell\mathbb{Z})$.

What about $\mathrm{H}^2_{\text{ét}}(\text{Surface}, \mathbb{Z}/\ell\mathbb{Z})$?

And now, surfaces!

So we can compute $\mathrm{H}^1_{\text{ét}}(\text{Curve}, \mathbb{Z}/\ell\mathbb{Z})$.

What about $\mathrm{H}^2_{\text{ét}}(\text{Surface}, \mathbb{Z}/\ell\mathbb{Z})$?

Solution: *dévissage* by Leray's spectral sequence

$$\text{“}\,\mathrm{H}^p(\mathrm{H}^q) \Rightarrow \mathrm{H}^{p+q}\,\text{”}.$$

And now, surfaces!

So we can compute $\mathrm{H}^1_{\text{ét}}(\text{Curve}, \mathbb{Z}/\ell\mathbb{Z})$.

What about $\mathrm{H}^2_{\text{ét}}(\text{Surface}, \mathbb{Z}/\ell\mathbb{Z})$?

Solution: *dévissage* by Leray's spectral sequence

$$\text{“}\mathrm{H}^p(\mathrm{H}^q) \Rightarrow \mathrm{H}^{p+q}\text{”}.$$

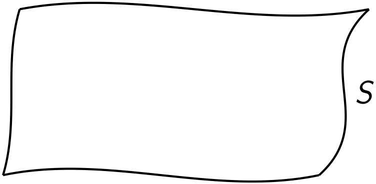
Theorem (M., 2019))

Let $S/\mathbb{Q}$ be a regular surface. For every ℓ, one can construct a curve $C/\mathbb{Q}$ such that $\mathrm{H}^2(S, \mathbb{Z}/\ell\mathbb{Z}) \subset \mathrm{Jac}(C)[\ell]$ (as Galois-modules, up to twist by the cyclotomic character and uninteresting bits).

And now, surfaces!

Theorem (M., 2019))

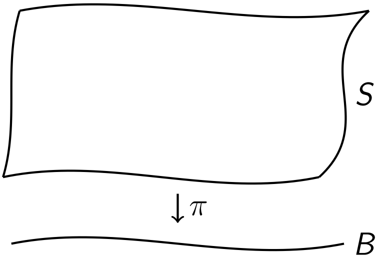
Let $S/\mathbb{Q}$ be a regular surface. For every ℓ, one can construct a curve $C/\mathbb{Q}$ such that $\mathrm{H}^2(S, \mathbb{Z}/\ell\mathbb{Z}) \subset \mathrm{Jac}(C)[\ell]$.



And now, surfaces!

Theorem (M., 2019))

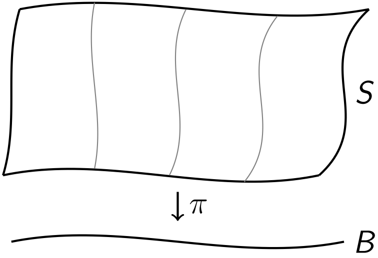
Let $S/\mathbb{Q}$ be a regular surface. For every ℓ, one can construct a curve $C/\mathbb{Q}$ such that $\mathrm{H}^2(S, \mathbb{Z}/\ell\mathbb{Z}) \subset \mathrm{Jac}(C)[\ell]$.



And now, surfaces!

Theorem (M., 2019))

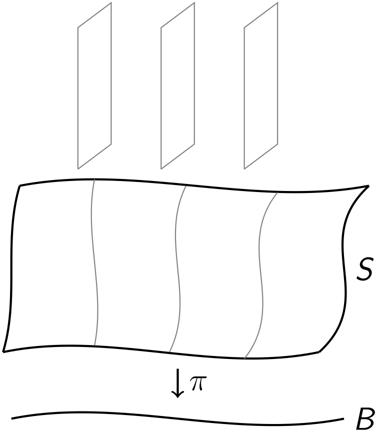
Let $S/\mathbb{Q}$ be a regular surface. For every ℓ, one can construct a curve $C/\mathbb{Q}$ such that $\mathrm{H}^2(S, \mathbb{Z}/\ell\mathbb{Z}) \subset \mathrm{Jac}(C)[\ell]$.



And now, surfaces!

Theorem (M., 2019))

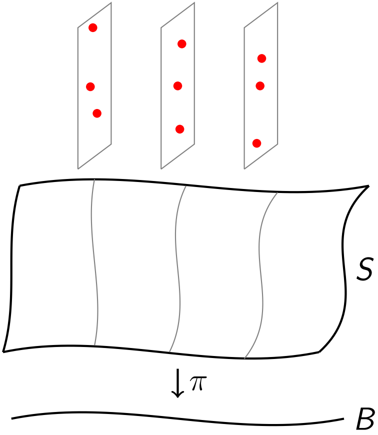
Let $S/\mathbb{Q}$ be a regular surface. For every ℓ, one can construct a curve $C/\mathbb{Q}$ such that $\mathrm{H}^2(S, \mathbb{Z}/\ell\mathbb{Z}) \subset \mathrm{Jac}(C)[\ell]$.



And now, surfaces!

Theorem (M., 2019))

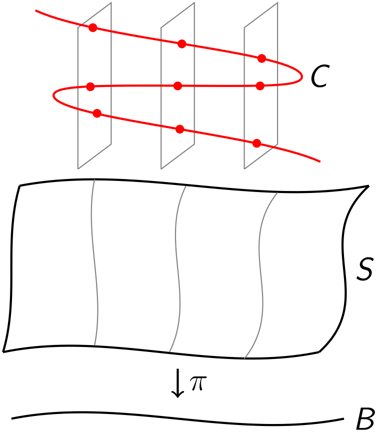
Let $S/\mathbb{Q}$ be a regular surface. For every ℓ, one can construct a curve $C/\mathbb{Q}$ such that $\mathrm{H}^2(S, \mathbb{Z}/\ell\mathbb{Z}) \subset \mathrm{Jac}(C)[\ell]$.



And now, surfaces!

Theorem (M., 2019))

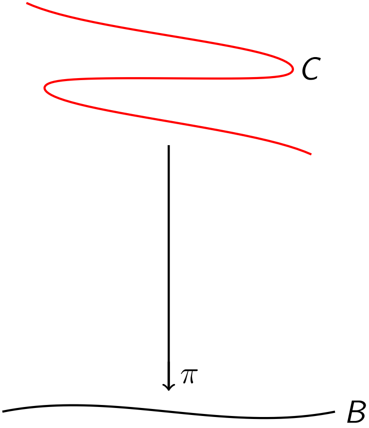
Let $S/\mathbb{Q}$ be a regular surface. For every ℓ, one can construct a curve $C/\mathbb{Q}$ such that $\mathrm{H}^2(S, \mathbb{Z}/\ell\mathbb{Z}) \subset \mathrm{Jac}(C)[\ell]$.



And now, surfaces!

Theorem (M., 2019))

Let $S/\mathbb{Q}$ be a regular surface. For every ℓ, one can construct a curve $C/\mathbb{Q}$ such that $\mathrm{H}^2(S, \mathbb{Z}/\ell\mathbb{Z}) \subset \mathrm{Jac}(C)[\ell]$.



Application 2: Integration of algebraic functions

Integrating algebraic functions

Let $f(x, y)$ be an algebraic function.
This means f lies in the function field
$K(C) = K(x)[y]/\big(F(x, y)\big)$ of a curve $C : F(x, y) = 0$.

Is $\displaystyle\int f(x, y)\,\mathrm{d}x$ elementary?

Integrating algebraic functions

Let $f(x,y)$ be an algebraic function.
This means f lies in the function field
$K(C) = K(x)[y]/\big(F(x,y)\big)$ of a curve $C : F(x,y) = 0$.

Is $\displaystyle\int f(x,y)\,\mathrm{d}x$ elementary?

Usually not!

Example

$$\int \frac{x\,\mathrm{d}x}{\sqrt{x^4+10x^2-96x-m}}$$

is not elementary for most values of $m \in \mathbb{Q}$... but

$$\int \frac{x\,\mathrm{d}x}{\sqrt{x^4+10x^2-96x-71}}$$

is elementary!

Integrating algebraic functions

Example

$$\int \frac{x\,\mathrm{d}x}{\sqrt{x^4+10x^2-96x-m}}$$

is not elementary for most values of $m \in \mathbb{Q}$... but

$$\int \frac{x\,\mathrm{d}x}{\sqrt{x^4+10x^2-96x-71}}$$

is elementary!

Liouville's criterion shows that $\int f(x,y)\,\mathrm{d}x$ elementary "iff." some divisors are torsion in $\operatorname{Pic}^0(C)$.

Example

On $C_m : y^2 = x^4+10x^2-96x-m$, $\omega = x\,\mathrm{d}x/y$ has simple poles at ∞_+ and ∞_- with $\operatorname{Res}_{\infty_\pm}\omega = \pm 1$, and $[\infty_+ - \infty_-]$ is 8-torsion for $m=71$, but non-torsion for most m.

Testing for torsion

- Let C curve over a number field K, and $T = \mathrm{Pic}^0(C)_{\mathrm{tors}}$. If $\mathfrak{p}$ is a prime of K above $p \in \mathbb{N}$ such that C has good reduction at $\mathfrak{p}$, then

  Reduction mod $\mathfrak{p}$ is injective on the prime-to-p part of T.

Testing for torsion

- Let C curve over a number field K, and $T = \operatorname{Pic}^0(C)_{\text{tors}}$. If $\mathfrak{p}$ is a prime of K above $p \in \mathbb{N}$ such that C has good reduction at $\mathfrak{p}$, then

  $\boxed{\text{Reduction mod } \mathfrak{p} \text{ is injective on the prime-to-}p \text{ part of } T.}$

- Let $\overline{C}/\mathbb{F}_q$ have genus g.Its Zeta function is

$$Z(\overline{C}/\mathbb{F}_q, t) = \exp \sum_{d=1}^{+\infty} \frac{\#\overline{C}(\mathbb{F}_{q^d})}{d} t^d = \frac{L(t)}{(1-t)(1-qt)}$$

where $L(t) \in \mathbb{Z}[t]$ determined by $\#\overline{C}(\mathbb{F}_{q^d})$ for $d \leqslant g$.

Furthermore, $\boxed{\#\operatorname{Pic}^0(\overline{C}) = L(t=1).}$

Testing for torsion

- Let C curve over a number field K, and $T = \operatorname{Pic}^0(C)_{\text{tors}}$. If $\mathfrak{p}$ is a prime of K above $p \in \mathbb{N}$ such that C has good reduction at $\mathfrak{p}$, then

  $\boxed{\text{Reduction mod } \mathfrak{p} \text{ is injective on the prime-to-} p \text{ part of } T.}$

- Let $\overline{C}/\mathbb{F}_q$ have genus g.Its Zeta function is

$$Z(\overline{C}/\mathbb{F}_q, t) = \exp \sum_{d=1}^{+\infty} \frac{\#\overline{C}(\mathbb{F}_{q^d})}{d} t^d = \frac{L(t)}{(1-t)(1-qt)}$$

  where $L(t) \in \mathbb{Z}[t]$ determined by $\#\overline{C}(\mathbb{F}_{q^d})$ for $d \leqslant g$.

  Furthermore, $\boxed{\# \operatorname{Pic}^0(\overline{C}) = L(t=1).}$

$\rightsquigarrow$ With $\mathfrak{p}_1, \mathfrak{p}_2$ such that $p_1 \neq p_2$, can find $m \in \mathbb{N}$: $\#T \mid m$.

Testing for torsion

$\rightsquigarrow$ With $\mathfrak{p}_1, \mathfrak{p}_2$ such that $p_1 \neq p_2$, can find $m \in \mathbb{N}$: $\#T \mid m$.

Let $D \in \mathrm{Div}^0(C)$. If m is small, we compute $\mathcal{L}(dD)$ for $d \mid m$. If m is large, we check the order of D in $\mathrm{Pic}^0(\overline{C}_{\mathfrak{p}_i})$ by using Makdisi's algorithms.

Testing for torsion

$\rightsquigarrow$ With $\mathfrak{p}_1, \mathfrak{p}_2$ such that $p_1 \neq p_2$, can find $m \in \mathbb{N}$: $\#T \mid m$.

```
C=crvinit(x^9-y^5+2*x^4*y^2,t,b); crvprint(C);

L=crvzeta(C,11)
factor(subst(L,x,1))

crvboundtorsion(C)

D1=[[-1,1],1;1,-1]; crvdivprint(C,D1);
crvdivistorsion(C,D1)

D2=[2,1;3,-1]; crvdivprint(C,D2);
crvdivistorsion(C,D2)
crvfndiv(C,%[2],1);
```

An example with 91-torsion

Let $f(x) = x^8 - 2x^7 + 7x^6 - 6x^5 - x^4 + 10x^3 - 6x^2 + 1$.

Then $\displaystyle\int \frac{2x^3 + 22x^2 + 47x - 91}{x\sqrt{f(x)}}\,\mathrm{d}x$

$= \log\left(A(x)\sqrt{f(x)} + B(x)\right) - 91\log(x)$, where $A(x) =$

$2541597392873x^{87} - 50843222146612x^{86} + 503225277935158x^{85} - 3200657096642275x^{84} + 14214462728604033x^{83} - 44579238719215767x^{82} + 90673772383763063x^{81} - 66130213758033706x^{80} - 273013962842426459x^{79} + 1133193576266076957x^{78} - 1828008617851129838x^{77} - 1325040205279907992x^{76} + 7070565814431437671x^{75} - 13820814098546580816x^{74} + 3057501416590971447x^{73} + 35452028969548856825x^{72} - 62530951562265159025x^{71} - 23621968960057272O8x^{70} + 149015656444634579168x^{69} - 167038416607981325445x^{68} - 122694173188447754583x^{67} + 429854211757535766713x^{66} - 169097783352406328449x^{65} - 555714282810473603258x^{64} + 674362321557037184728x^{63} + 312058060938121586273x^{62} - 1092460331914324201172x^{61} + 270596774739557247583x^{60} + 1120954182135661195118x^{59} - 880939983432258469781x^{58} - 730812820491441338716x^{57} + 1190924815315016075703x^{56} + 170419784195319443610x^{55} - 1106709092024065627293x^{54} + 266886129712577113986x^{53} + 775632662462383198827x^{52} - 447168828060446122800x^{51} - 414122686014061544643x^{50} + 415264647807791401896x^{49} + 156832329655217616311x^{48} - 289726675815819589903x^{47} - 26171689103841804545x^{46} + 164791091923265170230x^{45} - 17516989634058353270x^{44} - 79259644357109747485x^{43} + 20976219234985836422x^{42} + 32932548858101510407x^{41} - 13416187404910977913x^{40} - 12006472749426198850x^{39} + 6554509942630071562x^{38} + 3896330393014647662x^{37} - 2667133429777231104x^{36} - 1144094547215340652x^{35} + 936921199572723790x^{34} + 310346663095096540x^{33} - 289283382597149122x^{32} - 79724891819739155x^{31} + 79204013977345574x^{30} + 19845813628882518x^{29} - 19273182417066081x^{28} - 4834954816358415x^{27} + 4150468193299659x^{26} + 1140609211647771x^{25} - 781155386478148x^{24} - 253519603406578x^{23} + 125209807355899x^{22} + 51311674993204x^{21} - 16187503455853x^{20} - 9131100534854x^{19} + 1456557718427x^{18} + 1374884510502x^{17} - 30584589801x^{16} - 166171016046x^{15} - 18181479207x^{14} + 14582435700x^{13} + 3910302361x^{12} - 670862648x^{11} - 432933295x^{10} - 27794898x^9 + 24199247x^8 + 6635509x^7 + 89529x^6 - 311768x^5 - 83944x^4 - 11733x^3 - 982x^2 - 47x - 1$

and $B(x) \underset{\text{horror}}{\sim} A(x)$.

This is related to a rational 91-torsion point in $\mathrm{Pic}^0\left(y^2 - f(x)\right)$.
(Curve found by Steffen Müller and Berno Reitsma)

Final examples

Let $-x^5 + yx + y^4 = 0$ (genus 5).

Then $\displaystyle\int \frac{x^3}{y}\,\mathrm{d}x = \frac{4y^3}{11x} + \frac{1}{11}\log\left(\frac{y^3}{x}\right)$.

This involves spotting that some divisor is 11-torsion.

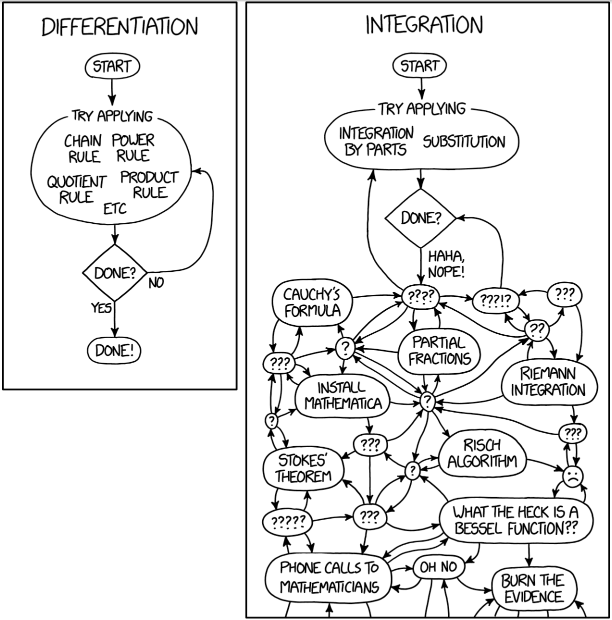
Our implementation takes 1 second; FriCAS takes 18 hours!

Same thing with

$$\int \frac{x^2 + 4y^3}{x^3}\,\mathrm{d}x = \frac{16y^3}{13x^2} + \frac{1}{13}\log\left(\frac{-x^{15} + 3yx^{10} - 3y^2x^5 + y^3}{x^{41}}\right)$$

where $-x^7 + yx^2 + y^4 = 0$ (genus 6, 13-torsion).

Conclusion



DIFFERENTIATION
START
TRY APPLYING
CHAIN RULE
POWER RULE
QUOTIENT RULE
PRODUCT RULE
ETC
DONE?
NO
YES
DONE!
INTEGRATION
START
TRY APPLYING
INTEGRATION BY PARTS
SUBSTITUTION
DONE?
HAHA, NOPE!
CAUCHY'S FORMULA
????
???!?
???
??
PARTIAL FRACTIONS
?
???
INSTALL MATHEMATICA
RIEMANN INTEGRATION
?
???
RISCH ALGORITHM
STOKES' THEOREM
???
?
?????
???
WHAT THE HECK IS A BESSEL FUNCTION??
PHONE CALLS TO MATHEMATICIANS
OH NO
BURN THE EVIDENCE

Questions?

Thank you!