

# The Parity Conjecture for hyperelliptic curves

Holly Green

University College London

June 3rd, 2021

Want to be able to prove the Parity Conjecture for hyperelliptic curves over  $\mathbb{Q}$  given by  $y^2 = f(x)g(x)$ .

## Conjecture (The Parity Conjecture)

*Let  $C/\mathbb{Q}$  be an algebraic curve. Then  $(-1)^{\text{rank}(\text{Jac } C)} = w(\text{Jac } C)$ .*

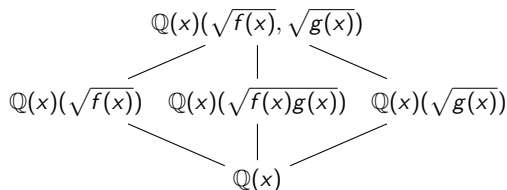
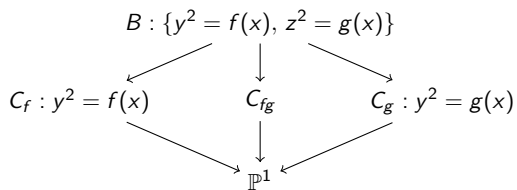
To do this, we need an understanding of the main ingredients, i.e:

- $w(\text{Jac } C) = w_\infty(\text{Jac } C) \prod_p w_p(\text{Jac } C)$ ,
- $\text{rank}(\text{Jac } C)$ .

Disclaimer: we will assume  $\#\text{III}$  is finite.

# Extracting parity information from an isogeny

To understand the rank of  $C_{fg} : y^2 = f(x)g(x)$ , we will use an isogeny.



## Theorem (G.)

- 1  $\text{Jac } C_f \times \text{Jac } C_g \times \text{Jac } C_{fg} \rightarrow \text{Jac } B$
- 2  $\text{BSD}(\text{Jac } C_f)\text{BSD}(\text{Jac } C_g)\text{BSD}(\text{Jac } C_{fg}) = \text{BSD}(\text{Jac } B)$
- 3  $\text{rank}(\text{Jac } C_f) + \text{rank}(\text{Jac } C_g) + \text{rank}(\text{Jac } C_{fg}) \equiv \lambda_\infty + \sum_p \lambda_p \pmod{2}$ .

# Extracting parity information from an isogeny

## Example

When  $f(x) = x^2 + ax + b$  and  $g(x) = x$  then

$$C_{fg} : y^2 = x^3 + ax^2 + bx, \quad B : y^2 = x^4 + ax^2 + b$$

and  $\text{rank}(C_{fg}) \equiv \lambda_\infty + \sum_p \lambda_p \pmod{2}$  where  $\lambda_\infty = \text{ord}_2 \left( \frac{\Omega(C_{fg})}{\Omega(\text{Jac } B)} \right)$  and  $\lambda_p = \text{ord}_2 \left( \frac{c_p(C_{fg})}{c_p(\text{Jac } B)} \right)$ .

More generally,

$$\lambda_v = \text{ord}_2 \left( \frac{c_v(\text{Jac } C_f) c_v(\text{Jac } C_g) c_v(\text{Jac } C_{fg}) d_v(C_f) d_v(C_g) d_v(C_{fg})}{c_v(\text{Jac } B) d_v(B)} \right).$$

## Question

How does this construction compare to BSD? BSD predicts

$$(-1)^{\text{rank}(C_f) + \text{rank}(C_g) + \text{rank}(C_{fg})} = w_\infty(C_f) w_\infty(C_g) w_\infty(C_{fg}) \prod_p w_p(C_f) w_p(C_g) w_p(C_{fg}).$$

# Proving the Parity Conjecture

At a place  $v$  of  $\mathbb{Q}$  define a *discrepancy factor*  $\mu_v = (-1)^{\lambda_v} w_v(\text{Jac } C_f) w_v(\text{Jac } C_g) w_v(\text{Jac } C_{fg})$ .

$$\begin{aligned} \prod_{v=p,\infty} \mu_v &= (-1)^{\lambda_\infty + \sum \lambda_p} w(\text{Jac } C_f) w(\text{Jac } C_g) w(\text{Jac } C_{fg}) \\ &= (-1)^{\text{rank}(\text{Jac } C_f) + \text{rank}(\text{Jac } C_g) + \text{rank}(\text{Jac } C_{fg})} w(\text{Jac } C_f) w(\text{Jac } C_g) w(\text{Jac } C_{fg}). \end{aligned}$$

If the Parity Conjecture holds for  $C_f$  and  $C_g$ , then

$$\prod_{v=p,\infty} \mu_v = (-1)^{\text{rank}(\text{Jac } C_{fg})} w(\text{Jac } C_{fg}).$$

Let  $(\cdot, \cdot)_v$  denote the Hilbert symbol. If  $A, B \in \mathbb{Q}$ , then  $\prod_{v=p,\infty} (A, B)_v = +1$ .

## Aim

To express  $\mu_v$  as a product of Hilbert symbols with entries in  $\mathbb{Q}$ . Then

$$\text{PC for } C_f \text{ and } C_g \Rightarrow \text{PC for } C_{fg}.$$

# Sturm's theorem

The *Sturm sequence* for  $f(x) \in \mathbb{R}[x]$  is

$$P_0 = f(x), \quad P_1 = f'(x), \quad P_{i+1} \equiv -P_{i-1} \pmod{P_i}.$$

Let  $\sigma(\alpha)$  be the number of sign changes in  $P_0(\alpha), P_1(\alpha), P_2(\alpha), \dots$

## Theorem (Sturm's theorem)

The number of  $\mathbb{R}$  roots of  $f(x)$  in the interval  $(\alpha, \beta]$  is  $\sigma(\alpha) - \sigma(\beta)$ .

## Example

Let  $f(x) = x^2 + ax + b$ . Then  $P_0 = f$ ,  $P_1 = 2x + a$ ,  $P_2 = \frac{1}{4}(a^2 - 4b) = \frac{1}{4}\Delta_f$ .

How many roots does  $x^2 + 2x - 2$  have in the interval  $(0, 1]$ ?

$$P_0(0), P_1(0), P_2(0) = -2, 2, 3; \quad P_0(1), P_1(1), P_2(1) = 1, 4, 3.$$

So  $\sigma(0) - \sigma(1) = 1 - 0 = 1$ .

# Proving the Parity Conjecture for a particular family

We will now fix  $g(x) = x$  and assume that  $f$  is monic.

## Theorem (G.)

$$\mu_\infty = \begin{cases} -1 & \#\mathbb{R}_{<0} \text{ roots of } f \equiv \deg f + (1 \text{ or } 2) \pmod{4}, \\ +1 & \text{otherwise.} \end{cases}$$

## Theorem (G., A. Morgan)

Let  $c_i, l_i$  be the constant and lead terms of  $P_i$  (the  $i$ th Sturm polynomial for  $f$ ). Then

$$\mu_\infty = \prod_{i=0}^{\deg f - 1} (-c_i, c_{i+1})_\infty (l_i, -l_{i+1})_\infty.$$

## Example

Let  $f(x) = x^2 + ax + b$ . Then  $\mu_\infty = (-b, a)(-2a, \Delta_f)$ . This expression works for  $v \neq \infty$  too.

# Proving the Parity Conjecture for a particular family

Continuing to take  $g(x) = x$  and  $f$  monic.

Theorem (G., C. Maistret)

Let  $f(x) = x^3 + ax^2 + bx + c$ . Then

$$\mu_v = (b, -c)_v (ab - 9c, -b\Delta_f)_v (-2, \Delta_f)_v.$$

$$\mu_v = (-1)^{\lambda_v} w_v(\text{Jac } C_f) w_v(\text{Jac } C_{xf})$$

$$\Rightarrow (-1)^{\text{rank}(\text{Jac } C_f) + \text{rank}(\text{Jac } C_{xf})} w(\text{Jac } C_f) w(\text{Jac } C_{xf}) = +1$$

Corollary

- 1  $PC$  holds for  $C_f : y^2 = f(x)$  iff it holds for  $C_{xf} : y^2 = xf(x)$ .
- 2 If  $E_1, E_2$  are elliptic curves with  $E_1[2] \cong E_2[2]$ , then  $PC$  holds for  $E_1$  iff it holds for  $E_2$ .
- 3  $PC$  holds for the genus 2 hyperelliptic curve  $B : y^2 = f(x^2)$ .



Continuing to take  $g(x) = x$  and  $f$  monic.

## Conjecture (G.)

Let  $c_i, l_i$  be the constant and lead terms of  $P_i$  (the  $i$ th Sturm polynomial for  $f$ ). Then

$$\mu_v = \prod_{i=0}^{\deg f - 1} (-c_i, c_{i+1})_v (l_i, -l_{i+1})_v.$$

Next step: understanding the Sturm polynomials over  $\mathbb{Q}_p$ .

Thank you for listening!