# Parity of ranks of hyperelliptic curves

Holly Green

University College London

March 2nd, 2021

# Goal

- What can we already say about ranks of curves?
- A new method for extracting rank information for hyperelliptic curves
- The consequences this has to the Parity Conjecture

Disclaimer: will assume $\#\text{Ш}$ is finite throughout.

The rational points on *abelian varieties* have a particularly nice structure.

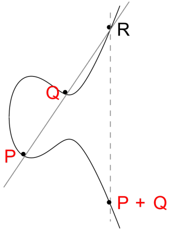
**Theorem (Mordell-Weil)**

*Let $A$ be an abelian variety over $\mathbb{Q}$. Then*

$$A(\mathbb{Q}) \cong \mathbb{Z}^{\mathrm{rank}(A/\mathbb{Q})} \times A(\mathbb{Q})_{\mathrm{tors}},$$

*for some* $\mathrm{rank}(A/\mathbb{Q}) \in \mathbb{N}$ *and* $A(\mathbb{Q})_{\mathrm{tors}}$ *a finite subgroup.*

- The 1-dimensional abelian varieties are elliptic curves.
- The 2-dimensional abelian varieties arise from hyperelliptic curves.



A hyperelliptic curve $X/\mathbb{Q}$ of genus $g$ is given by an equation

$$X : y^2 = f(x)$$

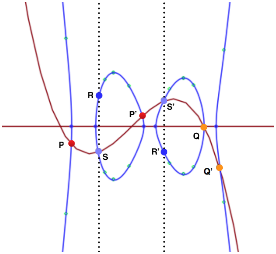
where $f(x) \in \mathbb{Q}[x]$ has degree $2g+1$ or $2g+2$ and $\Delta_X \neq 0$.

By Faltings theorem, $X(\mathbb{Q})$ is finite when $g \geq 2$. Instead we look at the *Jacobian* of the curve.

When $g = 2$, the Jacobian looks like pairs of points with

$$[P, P'] + [Q, Q'] = [R, R'].$$

We know very little about the rank of $\operatorname{Jac} X$ in general.



# The Jacobian

More formally:

- A *divisor* on $X/\mathbb{Q}$ is a finite sum $\sum_{P \in X(\overline{\mathbb{Q}})} n_P[P]$, where $n_P \in \mathbb{Z}$. This has degree $\sum_{P \in X(\overline{\mathbb{Q}})} n_P$.
- A *principal divisor* is $\sum_{P \in X(\overline{\mathbb{Q}})} \mathrm{ord}_P(f)[P]$ for $f \in \overline{\mathbb{Q}}(X)^\times$.

**Definition**

The Jacobian is $\mathrm{Jac}\, X(\overline{\mathbb{Q}}) := \{\text{divisors of degree } 0\}/\{\text{principal divisors}\}$. Moreover, a point in $\mathrm{Jac}\, X(\mathbb{Q})$ is a divisor class fixed by $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$.

If $X$ is a curve of genus $g$, then $\mathrm{Jac}\, X$ is an abelian variety of dimension $g$.

We will be interested in Jacobians of hyperelliptic curves. In particular, their ranks.

# Determining the rank of hyperelliptic curves

## Conjecture (Birch and Swinnerton-Dyer, Tate)

*Let $X/\mathbb{Q}$ be a smooth curve. Assuming $L(\mathrm{Jac}\, X/\mathbb{Q}, s)$ has an analytic continuation to $\mathbb{C}$,*

- $\mathrm{rank}(\mathrm{Jac}\, X/\mathbb{Q}) = \mathrm{ord}_{s=1} L(\mathrm{Jac}\, X/\mathbb{Q}, s)$,
- *the leading term in the Taylor expansion of $L(\mathrm{Jac}\, X/\mathbb{Q}, s)$ at $s = 1$ is*

$$\mathrm{BSD}(\mathrm{Jac}\, X/\mathbb{Q}) = \frac{\#\text{Ш}(\mathrm{Jac}\, X)\Omega(\mathrm{Jac}\, X)\mathrm{Reg}(\mathrm{Jac}\, X)C(\mathrm{Jac}\, X)}{\#\mathrm{Jac}\, X(\mathbb{Q})^2_{\mathrm{tors}}}.$$

## Conjecture (The Parity Conjecture)

*Let $X/\mathbb{Q}$ be a smooth curve. Then*

$$(-1)^{\mathrm{rank}(\mathrm{Jac}\, X/\mathbb{Q})} = w(\mathrm{Jac}\, X/\mathbb{Q}) := \prod_{v=p,\infty} w_v(\mathrm{Jac}\, X/\mathbb{Q}).$$

# Example: Parity Conjecture for elliptic curves

**Theorem (Rohrlich)**

*For $E/\mathbb{Q}$ and elliptic curve, $w_\infty(E/\mathbb{Q}) = -1$ and*

$$w_p(E/\mathbb{Q}) = \begin{cases} +1 & E/\mathbb{Q}_p \textit{ has good reduction} \\ -1 & E/\mathbb{Q}_p \textit{ has split multiplicative reduction} \\ +1 & E/\mathbb{Q}_p \textit{ has non-split multiplicative reduction} \end{cases}$$

Take $E : y^2 = x^3 + 4x^2 - 80x + 400$ (715.b1), then $\Delta_E = -5^3 \cdot 11 \cdot 13$

- When $p = 5$ or 13, reduction is split multiplicative
- When $p = 11$, reduction is non-split multiplicative

$$\omega(E/\mathbb{Q}) = (-1)^3 = -1 \Rightarrow \text{rank}(E/\mathbb{Q}) \text{ is odd.}$$

# A new method for extracting rank information

Define a hyperelliptic curve $C/\mathbb{Q}$ by $C : y^2 = f_1(x)f_2(x),\ f_1, f_2 \in \mathbb{Q}[x]$.

We want to be able to say something about $\text{rank}(\text{Jac}\, C/\mathbb{Q})$.

Consider the following diagram of curves

$$\begin{tikzcd}[column sep=small]
 & B : \{y^2 = f_1(x),\ z^2 = f_2(x)\} \arrow[dl, dash] \arrow[d, dash] \arrow[dr, dash] & \\
C_1 : y^2 = f_1(x) \arrow[dr, dash] & C : y^2 = f_1(x)f_2(x) \arrow[d, dash] & C_2 : y^2 = f_2(x) \arrow[dl, dash] \\
 & \mathbb{P}^1 &
\end{tikzcd}$$

## Theorem (G.)

*Let $C_1$, $C_2$, $C$, $B$ be as above. Then,*

- *there's an isogeny* $\varphi : \text{Jac}\, C_1 \times \text{Jac}\, C_2 \times \text{Jac}\, C \to \text{Jac}\, B$,
- $\text{BSD}(\text{Jac}\, C_1)\text{BSD}(\text{Jac}\, C_2)\text{BSD}(\text{Jac}\, C) = \text{BSD}(\text{Jac}\, B)$.

# A new method for extracting rank information

Recall that

$$\mathrm{BSD}(\mathrm{Jac}\,X) = \frac{\#\text{Ш}(\mathrm{Jac}\,X)\Omega(\mathrm{Jac}\,X)\mathrm{Reg}(\mathrm{Jac}\,X)C(\mathrm{Jac}\,X)}{\#\mathrm{Jac}\,X(\mathbb{Q})^2_{\mathrm{tors}}}.$$

The following quotient of regulators can be shown to contains rank information:

$$\square \cdot 2^{\mathrm{rank}(\mathrm{Jac}\,C_1/\mathbb{Q})+\mathrm{rank}(\mathrm{Jac}\,C_2/\mathbb{Q})+\mathrm{rank}(\mathrm{Jac}\,C/\mathbb{Q})} = \frac{\mathrm{Reg}(\mathrm{Jac}\,B)}{\mathrm{Reg}(\mathrm{Jac}\,C_1)\mathrm{Reg}(\mathrm{Jac}\,C_2)\mathrm{Reg}(\mathrm{Jac}\,C)}$$

Using our previous observation:

$$= \frac{\#\text{Ш}(\mathrm{Jac}\,C_1)\#\text{Ш}(\mathrm{Jac}\,C_2)\#\text{Ш}(\mathrm{Jac}\,C)}{\#\text{Ш}(\mathrm{Jac}\,B)} \frac{\Omega(\mathrm{Jac}\,C_1)\Omega(\mathrm{Jac}\,C_2)\Omega(\mathrm{Jac}\,C)}{\Omega(\mathrm{Jac}\,B)} \prod_p \frac{c_p(\mathrm{Jac}\,C_1)c_p(\mathrm{Jac}\,C_2)c_p(\mathrm{Jac}\,C)}{c_p(\mathrm{Jac}\,B)}.$$

This is *almost* an expression of local data. What can we say about $\#\text{Ш}$?

# Deficiency

**Definition**

Let $X/\mathbb{Q}$ be a curve of genus $g$. We say that $X$ is *deficient* at a place $v$ of $\mathbb{Q}$ if it has no $\mathbb{Q}_v$-rational divisor of degree $g-1$.

**Example**

Is $x^2 + y^2 = -1$ deficient at $\infty$? Is there a degree $-1$ divisor fixed by complex conjugation? No $\Rightarrow$ this is deficient.

**Example**

Is $y^2 = (x^2 - 6)(x^4 + 1)$ deficient at 5? Is there a degree 1 divisor fixed by $G_{\mathbb{Q}_5}$? Yes as 6 is a square in $\mathbb{Q}_5$ $\Rightarrow$ this is not deficient.

# Controlling $\#Ш$

Let $X/\mathbb{Q}$ be a curve of genus $g$. For a place $v$ of $\mathbb{Q}$, define

$$d_v(X) := \begin{cases} 2 & X \text{ is deficient at } v \\ 1 & \text{otherwise.} \end{cases}$$

## Theorem (B. Poonen & M. Stoll)

*For $X/\mathbb{Q}$ a curve,* $\#Ш(\mathrm{Jac}\,X) = \square \cdot d_\infty(X) \prod_p d_p(X)$.

So, $\square \cdot 2^{\mathrm{rank}(\mathrm{Jac}\,C_1/\mathbb{Q}) + \mathrm{rank}(\mathrm{Jac}\,C_2/\mathbb{Q}) + \mathrm{rank}(\mathrm{Jac}\,C/\mathbb{Q})}$

$$= \frac{\Omega(\mathrm{Jac}\,C_1)\Omega(\mathrm{Jac}\,C_2)\Omega(\mathrm{Jac}\,C)}{\Omega(\mathrm{Jac}\,B)} \prod_{v=p,\infty} \frac{d_v(C_1)d_v(C_2)d_v(C)}{d_v(B)} \prod_p \frac{c_p(\mathrm{Jac}\,C_1)c_p(\mathrm{Jac}\,C_2)c_p(\mathrm{Jac}\,C)}{c_p(\mathrm{Jac}\,B)}.$$

## Theorem (G.)

$$\mathrm{rank}(\mathrm{Jac}\,C_1/\mathbb{Q}) + \mathrm{rank}(\mathrm{Jac}\,C_2/\mathbb{Q}) + \mathrm{rank}(\mathrm{Jac}\,C/\mathbb{Q}) \equiv \lambda_\infty + \sum_p \lambda_p \mod 2.$$

# Example: elliptic curves

Let $f_1(x) = x^2 + x - 1$ and $f_2(x) = x$.

First observe that $C_1(\mathbb{Q}), C_2(\mathbb{Q}), C(\mathbb{Q}), B(\mathbb{Q}) \neq 0$ so $d_v = 1$.

- $\mathrm{Jac}\, C_1 = \mathrm{Jac}\, C_2 = 0$
- $\mathrm{Jac}\, C = C$ is the elliptic curve 20.a3, $\Delta_{\mathrm{Jac}\, C} = 2^4 \cdot 5$
- $B : y^2 = z^4 + z^2 - 1$ so $\mathrm{Jac}\, B : y^2 = x^3 + x^2 + 4x + 4$ is the elliptic curve 20.a4, $\Delta_{\mathrm{Jac}\, B} = -2^8 \cdot 5^2$

We obtain the following data:

$$
\begin{aligned}
c_2(\mathrm{Jac}\, C) &= 3 & \qquad c_2(\mathrm{Jac}\, B) &= 3 \\
c_5(\mathrm{Jac}\, C) &= 1 & \qquad c_5(\mathrm{Jac}\, B) &= 2 \\
\Omega(\mathrm{Jac}\, C) &= 5.64875\ldots & \qquad \Omega(\mathrm{Jac}\, B) &= 2.824375\ldots
\end{aligned}
$$

Therefore,

$$
2^{\mathrm{rank}(\mathrm{Jac}\, C/\mathbb{Q})} \equiv \frac{3}{3} \times \frac{1}{2} \times \frac{5.64875\ldots}{2.824375\ldots} = 1 \Rightarrow \mathrm{rank}(\mathrm{Jac}\, C/\mathbb{Q}) \text{ is even.}
$$

# Example: genus 2 hyperelliptic curves

Let $f_1(x) = x^2 - 2x - 3$ and $f_2(x) = x^4 - 2x^3 - x^2 - 2x - 3$.

Again observe that $C_1(\mathbb{Q}), C_2(\mathbb{Q}), C(\mathbb{Q}), B(\mathbb{Q}) \neq 0$ so $d_v = 1$.

- $\mathrm{Jac}\, C_1 = 0$
- $\mathrm{Jac}\, C_2$ is the elliptic curve 83.a1, $\Delta_{\mathrm{Jac}\, C_2} = -83$
- $C$ is the hyperelliptic curve 249.a.6723.1, $\Delta_{\mathrm{Jac}\, C} = -3^4 \cdot 83$
- $B$ is a genus 3 curve

We obtain the following data:

$$\begin{array}{lll} c_3(\mathrm{Jac}\, C_2) = 1 & c_3(\mathrm{Jac}\, C) = 4 & c_3(\mathrm{Jac}\, B) = 2 \\ c_{83}(\mathrm{Jac}\, C_2) = 1 & c_{83}(\mathrm{Jac}\, C) = 1 & c_{83}(\mathrm{Jac}\, B) = 1 \\ \Omega(\mathrm{Jac}\, C_2) = 3.37\ldots & \Omega(\mathrm{Jac}\, C) = 25.78\ldots & \Omega(\mathrm{Jac}\, B) = 348.02\ldots \end{array}$$

Therefore,

$$2^{\mathrm{rank}(\mathrm{Jac}\, C_2/\mathbb{Q}) + \mathrm{rank}(\mathrm{Jac}\, C/\mathbb{Q})} \equiv \frac{4}{2} \times \frac{1}{1} \times \frac{1}{4} = \frac{1}{2} \Rightarrow \mathrm{rank}(\mathrm{Jac}\, C/\mathbb{Q}) \text{ is even.}$$

# Proving the Parity Conjecture

We've shown that for $C_1 : y^2 = f_1(x)$, $C_2 : y^2 = f_2(x)$, $C : y^2 = f_1(x)f_2(x)$

$$\mathrm{rank}(\mathrm{Jac}\, C_1/\mathbb{Q}) + \mathrm{rank}(\mathrm{Jac}\, C_2/\mathbb{Q}) + \mathrm{rank}(\mathrm{Jac}\, C/\mathbb{Q}) \equiv \lambda_\infty + \sum_p \lambda_p \mod 2.$$

The Parity Conjecture predicts that

$$(-1)^{\mathrm{rank}(\mathrm{Jac}\, X/\mathbb{Q})} = w(\mathrm{Jac}\, X/\mathbb{Q}) = \prod_v w_v(\mathrm{Jac}\, X/\mathbb{Q}).$$

At each place $v$ of $\mathbb{Q}$ define a *discrepancy factor*

$$\mu_v = (-1)^{\lambda_v} w_v(\mathrm{Jac}\, C_1/\mathbb{Q}) w_v(\mathrm{Jac}\, C_2/\mathbb{Q}) w_v(\mathrm{Jac}\, C/\mathbb{Q}).$$

Taking the product over all $v$:

$$\prod_{v=p,\infty} \mu_v = (-1)^{\mathrm{rank}(\mathrm{Jac}\, C_1/\mathbb{Q})+\mathrm{rank}(\mathrm{Jac}\, C_2/\mathbb{Q})+\mathrm{rank}(\mathrm{Jac}\, C/\mathbb{Q})} w(\mathrm{Jac}\, C_1/\mathbb{Q}) w(\mathrm{Jac}\, C_2/\mathbb{Q}) w(\mathrm{Jac}\, C/\mathbb{Q}).$$

Assume that PC holds for Jac $C_1$ and Jac $C_2$, then proving it for Jac $C$ is equivalent to showing that $\prod_v \mu_v = +1$.

# Hilbert symbols

## Definition

The *Hilbert symbol* of $a, b \in \mathbb{Q}_v^*$ is

$$(a,b)_v = \begin{cases} +1 & z^2 - ax^2 - by^2 = 0 \text{ has a non-zero } \mathbb{Q}_v\text{-solution}, \\ -1 & \text{otherwise.} \end{cases}$$

This is a symmetric bilinear pairing satisfying a product law:

$$\prod_v (a,b)_v = +1$$

where $a, b \in \mathbb{Q}^*$ and the product is taken over all places of $\mathbb{Q}$.

Idea: can we express $\mu_v$ as a product of Hilbert symbols?

# Proving the Parity Conjecture for elliptic curves

Let $C$ be an elliptic curve over $\mathbb{Q}$ with a rational 2-torsion point. Then

$$C : y^2 = x(x^2 + ax + b)$$

so let $f_1(x) = x^2 + ax + b$ and $f_2(x) = x$. Assume $a \neq 0$.

Then $\mathrm{Jac}\, C_1 = \mathrm{Jac}\, C_2 = 0$.

It can be shown that for each place $v$ of $\mathbb{Q}$,

$$\mu_v := (-1)^{\lambda_v} w_v(C/\mathbb{Q}) = (a, -b)_v(-2a, a^2 - 4b)_v.$$

Taking the product over all places proves the Parity Conjecture, i.e.

$$(-1)^{\mathrm{rank}(C/\mathbb{Q})} w(C/\mathbb{Q}) = +1.$$

# Can we generalise this?

Let $f_1(x) \in \mathbb{Q}[x]$ be monic and $f_2(x) = x$. Then

$$C_1 : y^2 = f_1(x), \quad C_2 : y^2 = x, \quad C : y^2 = xf_1(x), \quad B : y^2 = f_1(x^2).$$

Recall, to calculate $\mu_\infty$ (i.e. $\lambda_\infty$ and $\omega_\infty$) we must look at these curves over $\mathbb{R}$.

**Theorem (G.)**

$$\mu_\infty = \begin{cases} -1 & \#\mathbb{R}_{<0} \textit{ roots of } f_1 \equiv \deg f_1 - (2 \textit{ or } 3) \mod 4, \\ +1 & \textit{otherwise.} \end{cases}$$

Can we find expressions to insert into Hilbert symbols which reflect this?

# Sturm's theorem

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

$$P_0 = f(x), \qquad P_1 = f'(x), \qquad P_{i+1} \equiv -P_{i-1} \mod P_i, \text{ for } i \geq 1.$$

## Example

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

For $\alpha \in \mathbb{R}$, let $V(\alpha)$ be the number of sign changes in

$$P_0(\alpha),\ P_1(\alpha),\ P_2(\alpha),\ \ldots$$

## Theorem (Sturm's theorem)

*The number of $\mathbb{R}$ roots of $f(x)$ in the interval $(s, t]$ is $V(s) - V(t)$.*

# A new conjecture

Let $l(P_i), c(P_i)$ be the lead and constant coefficients of the Sturm polynomials for $f_1(x)$.

## Conjecture (G.)

*Let $f_1(x) \in \mathbb{Q}[x]$ be monic and $f_2(x) = x$. Then*

$$\mu_v = \prod_{i=0}^{\deg f_1 - 1} \left(-c(P_i), c(P_{i+1})\right)_v \left(l(P_i), -l(P_{i+1})\right)_v .$$

- When $f_1(x) = x^2 + ax + b$,

$$\mu_v = (-b, a)_v(-2a, a^2 - 4b)_v.$$

- When $f_1(x) = x^3 + ax^2 + bx + c$, let $D = a^2 - 3b$, $L = ab - 9c$,

$$\mu_v = (b, -c)_v(-2L, \Delta)_v(L, -b)_v(D, -3\Delta)_v.$$

# Final remarks

Assuming the conjecture holds, we have the following consequences:

- When $C_1 : y^2 = f_1(x)$, $C : y^2 = xf_1(x)$, the Parity Conjecture holds for Jac $C$ if and only if it holds for Jac $C_1$:

$$1 = \prod_v \mu_v = (-1)^{\mathrm{rank}(\mathrm{Jac}\, C_1/\mathbb{Q}) + \mathrm{rank}(\mathrm{Jac}\, C/\mathbb{Q})} w(\mathrm{Jac}\, C_1/\mathbb{Q}) w(\mathrm{Jac}\, C/\mathbb{Q}).$$

- The Parity Conjecture holds for any hyperelliptic curve

$$y^2 = c \prod_{i=1}^{n} (x - \alpha_i), \quad c,\, \alpha_i \in \mathbb{Q}.$$

Thank you for listening!