The Parity Conjecture for hyperelliptic curves

Holly Green

University College London

June 3rd, 2021

Goal

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 $(-1)^{\mathrm{rank}(\mathrm{Jac}\, C)} = w(\mathrm{Jac}\, C)$.

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

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

Disclaimer: we will assume $\#Ш$ 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.

$$\begin{tikzcd}
 & B : \{y^2 = f(x),\, z^2 = g(x)\} \arrow[dl] \arrow[d] \arrow[dr] & \\
C_f : y^2 = f(x) \arrow[dr] & C_{fg} \arrow[d] & C_g : y^2 = g(x) \arrow[dl] \\
 & \mathbb{P}^1 &
\end{tikzcd}$$

$$\begin{tikzcd}
 & \mathbb{Q}(x)(\sqrt{f(x)}, \sqrt{g(x)}) \arrow[dl, dash] \arrow[d, dash] \arrow[dr, dash] & \\
\mathbb{Q}(x)(\sqrt{f(x)}) \arrow[dr, dash] & \mathbb{Q}(x)(\sqrt{f(x)g(x)}) \arrow[d, dash] & \mathbb{Q}(x)(\sqrt{g(x)}) \arrow[dl, dash] \\
 & \mathbb{Q}(x) &
\end{tikzcd}$$

Theorem (G.)

1. $\mathrm{Jac}\, C_f \times \mathrm{Jac}\, C_g \times \mathrm{Jac}\, C_{fg} \to \mathrm{Jac}\, B$
2. $\mathrm{BSD}(\mathrm{Jac}\, C_f)\mathrm{BSD}(\mathrm{Jac}\, C_g)\mathrm{BSD}(\mathrm{Jac}\, C_{fg}) = \mathrm{BSD}(\mathrm{Jac}\, B)$
3. $\mathrm{rank}(\mathrm{Jac}\, C_f) + \mathrm{rank}(\mathrm{Jac}\, C_g) + \mathrm{rank}(\mathrm{Jac}\, C_{fg}) \equiv \lambda_\infty + \sum_p \lambda_p \mod 2.$

Extracting parity information from an isogeny

Example

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

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

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

More generally,

$$\lambda_v = \mathrm{ord}_2\left(\frac{c_v(\mathrm{Jac}\, C_f)c_v(\mathrm{Jac}\, C_g)c_v(\mathrm{Jac}\, C_{fg})}{c_v(\mathrm{Jac}\, B)}\frac{\mathrm{d}_v(C_f)\mathrm{d}_v(C_g)\mathrm{d}_v(C_{fg})}{\mathrm{d}_v(B)}\right).$$

Question

How does this construction compare to BSD? BSD predicts

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

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

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

If the Parity Conjecture holds for C_f and C_g, then

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

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 μ_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

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

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 $(0, 1]$?

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

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.)

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

Theorem (G., A. Morgan)

Let c_i, l_i be the constant and lead terms of P_i (the ith 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

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

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

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

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 $B : y^2 = f(x^2)$.*

Proving the Parity Conjecture for a particular family

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 ith 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!