Functions, Reciprocity & the Obstruction to Divisors on Curves

~~**Objective** Understand counterexamples to the Hasse principle using some high-brow theory.~~

Objective Develope a practical method which can show that a curve having no rational points does indeed have no rational points (for certain classes of curves).

Example (Lind) $2Y^2 = X^4 - 17Z^4$ is a counterexample to Hasse principle.

Proof By contradiction. WLOG $X, Y, Z \in \mathbb{Z}$, $\gcd(X, Z) = 1$, $Y > 0$.

If $q \mid Y$, $q \neq 2$ is prime then

$$\left(\frac{17}{q}\right) = 1 \Rightarrow \left(\frac{q}{17}\right) = 1 \qquad \left(\text{also } \left(\frac{2}{17}\right) = 1\right)$$

$\therefore$ $Y \equiv Y_0^2 \mod 17$ $\therefore$ $2Y_0^4 \equiv X^4 \ (17)$

But $2 \notin (\mathbb{F}_{17}^*)^4$ Contradiction

Question Can Lind's strategy be applied to other curves?

Answer For hyperelliptic curves, yes.

Suppose $F(X,Z) \in \mathbb{Z}[X,Z]$ is homogeneous of <u>even</u> degree $2r$.

Suppose we want to show that $Y^2 = F(X,Z)$ has no points.

Argue by contradiction:

Suppose we have a solution with $X, Y, Z \in \mathbb{Z}$, $\gcd(X,Z) = 1$, $Z > 0$

Choose $\alpha, \beta \in \mathbb{Z}$ $\gcd(\alpha,\beta) = 1$ and let $F(\alpha,\beta) = \gamma\delta^2$ γ squarefree.

$\exists \lambda$ s.t. $(\lambda X, \lambda Z) \equiv (\alpha, \beta) \bmod (\beta X - \alpha Z)$

$$
\begin{aligned}
\therefore \gamma\delta^2 &\equiv F(\alpha,\beta) \\
&\equiv F(\lambda X, \lambda Z) \\
&\equiv \lambda^{2r} F(X,Z) \\
&\equiv (\lambda^r Y)^2 \quad \bmod (\beta X - \alpha Z)
\end{aligned}
$$

$\therefore \gamma$ is a quadratic res. $\bmod (\beta X - \alpha Z)$.

$\therefore$ Get congruences for $\beta X - \alpha Z$.

Repeat with several pairs α, β until we get contradiction.

Example First $|\text{Ш}| > 1$ is 571A for which $|\text{Ш}| = 4$. Take 2-covering

$$Y^2 = -4X^4 + 4X^3Z + 92X^2Z^2 - 104XZ^3 - 727Z^4$$

ELS but has no rational points.

Proof WLOG $X, Y, Z \in \mathbb{Z}$ $\gcd(X,Z) = 1$ $Z > 0$.

2-adic solvability $\Longrightarrow$ $Z = Z_0$ or $Z = 2Z_0$ where $2 \nmid Z_0$.

If $q \mid Z_0$ then $\left(\frac{-1}{q}\right) = 1$

$\therefore$ $q \equiv 1 \pmod 4$ $\therefore$ $Z_0 \equiv 1 \pmod 4$

$$\boxed{\therefore \quad Z \equiv 1 \pmod 4 \quad \text{or} \quad Z \equiv 2 \pmod 8}$$

Also $F(\underset{\alpha}{-53}, \underset{\beta}{16}) = -2^2$. Get

$$|16X + 53Z| \equiv 1 \pmod 4 \quad \text{or} \quad 2 \pmod 8$$

Real solubility $\Rightarrow$ $16X + 53Z < 0$

$\therefore$ $16X + 53Z \equiv 3 \pmod 4$ or $6 \pmod 8$

$$\boxed{\therefore \quad Z \equiv 3 \pmod 4 \quad \text{or} \quad Z \equiv 6 \pmod 8}$$

Contradiction.

Part II : Functions & Divisors

Let C/K smooth projective curve (K perfect)

$f \in K(C) \setminus K$

$S \subseteq C(\bar{K})$ support of f

Define $\operatorname{Div} \bar{C} = \left\{ \sum_{P \in C(\bar{K})} n_P P \; : \; \begin{array}{c} n_P \in \mathbb{Z} \\ \text{almost all} \\ = 0 \end{array} \right\}$

$\operatorname{Div} C = (\operatorname{Div} \bar{C})^{\operatorname{Gal}(\bar{K}/K)}$

$(\operatorname{Div} C)_S$ divisors that avoid S.

Extend $f : (\operatorname{Div} C)_S \longrightarrow K^*$

$$f\left(\sum n_P P\right) = \prod f(P)^{n_P}$$

Suppose $g \in K(C) \setminus K$ such that

$\operatorname{support}(g) \cap S = \phi$. Then

$f(\operatorname{div}(g)) = g(\operatorname{div}(f))$ Weil's Reciprocity

$$= \prod_{P \in S} g(P)^{\operatorname{ord}_P(f)}$$

$$= \prod_{P \in S'} \left(\operatorname{Norm}(g(P))\right)^{\operatorname{ord}_P(f)}$$

where $S' = {}_{\mathrm{Gal}(\overline{K}/K)} \backslash S$.

Let

$$G_f = \prod_{P \in S'} \left(\mathrm{Norm}_{K(P)/K} \left(K(P)^* \right) \right)^{\mathrm{ord}_P f}$$

$$\therefore \quad f\left(\mathrm{Princ}(C)_S \right) \subseteq G_f$$

$\therefore$ f induces

$$f : (\mathrm{Div}\, C)_S / \mathrm{Princ}(C)_S \longrightarrow K^* / G_f$$

But $\mathrm{Pic}\, C := \mathrm{Div}\, C / \mathrm{Princ}(C) = (\mathrm{Div}\, C)_S / \mathrm{Princ}(C)_S$

$\therefore$ $f \in K(C) \setminus K$ induces

$$f : \mathrm{Pic}\, C \longrightarrow K^* / G_f$$

Part II.V Class Field Theory

Let K number field

L/K finite abelian extention

I_K idèles

$\left[I_K = \{ (a_v)_v : a_v \in K_v^* \text{ ....} \} \right]$

Suppose v is a prime of K
$w | v$ prime of L

Local Artin Map $\theta_v : K_v^* / \mathrm{Norm}(L_w^*) \longrightarrow \mathrm{Gal}(L/K)$

Artin Map $\theta :$ $I_K / \mathrm{Norm}(I_L) \longrightarrow \mathrm{Gal}(L/K)$

given by $\theta = \prod \theta_v$.

Artin Reciprocity The sequence

$$K^* \longrightarrow I_K / \mathrm{Norm}(I_L) \xrightarrow{\theta} \mathrm{Gal}(L/K)$$

is exact.

Example $K = \mathbb{Q}$

$L = \mathbb{Q}(i)$

Identify $\mathrm{Gal}(L/K) = \mu_2 = \{1, -1\}$.

Local Artin map $\theta_p : \mathbb{Q}_p^* \longrightarrow \{1, -1\}$

$$\theta_p(\alpha) = \begin{cases} 1 & \text{if } \alpha = x^2 + y^2 \text{ with } x, y \in \mathbb{Q}_p \\ -1 & \text{otherwise.} \end{cases}$$

III Reciprocity

Joint with Martin Bright

Let K number field

C/K curve

L/K finite abelian extn

Suppose $\mathrm{div}(f) = \sum_{\sigma \in \mathrm{Gal}(L/K)} D^\sigma$

where $\mathrm{supp}(D) \subseteq C(L)$.

Then we get $G_f \subseteq \mathrm{Norm}(L^*)$.

So f induces

$$\begin{tikzcd}
\mathrm{Pic}\, C \arrow[r, "f"] \arrow[d, "i"] & K^*/\mathrm{Norm}\, L^* \arrow[d] \arrow[dr, "1"] & \\
\prod_v \mathrm{Pic}(C_v) \arrow[r, "f"] & I_K/\mathrm{Norm}(I_L) \arrow[r, "\theta", "\text{Artin map}"'] & \mathrm{Gal}(L/K)
\end{tikzcd}$$

Get

$$\begin{tikzcd}
\mathrm{Pic}(C) \arrow[r, "i"] \arrow[rr, bend right, "1"'] & \prod_v \mathrm{Pic}(C_v) \arrow[r, "\theta\circ f"] & \mathrm{Gal}(L/K)
\end{tikzcd}$$

9 **Lemma** $\exists$ a finite computable set B such that

$$\begin{tikzcd}
\prod_{v} \mathrm{Pic}(C_v) \arrow[rr, "\theta \circ f"] \arrow[dr] & & \mathrm{Gal}(L/K) \\
& \prod_{v \in B} \mathrm{Pic}(C_v) \arrow[ur, "\theta \circ f"] &
\end{tikzcd}$$

commutes

Get

$$\begin{tikzcd}
\mathrm{Pic}(C) \arrow[r, "i"] \arrow[rr, bend right, "1"'] & \prod_{v \in B} \mathrm{Pic}(C_v) \arrow[r, "\theta \circ f"] & \mathrm{Gal}(L/K)
\end{tikzcd}$$

Let $n = \# \mathrm{Gal}(L/K)$ then

$$\begin{tikzcd}
\mathrm{Pic}(C)/n\mathrm{Pic}(C) \arrow[r] \arrow[rr, bend right, "1"'] & \prod_{v \in B} \mathrm{Pic}(C_v)/n\mathrm{Pic}(C_v) \arrow[r] & \mathrm{Gal}(L/K)
\end{tikzcd}$$

finite and computable.

If $P_v \in C(K_v)$ then

$$\frac{\mathrm{Pic}(C_v)}{n\mathrm{Pic}(C_v)} = (\mathbb{Z}/n\mathbb{Z}) P_v \oplus \frac{J(K_v)}{nJ(K_v)}$$

Lemma Suppose $0 < r < n$. Let

$$\left(\mathrm{Pic}(C_v) / n\,\mathrm{Pic}(C_v)\right)_r = \left\{\begin{array}{l}\text{subset of elements} \\ \text{with degree} \\ r \bmod (n)\end{array}\right\}$$

Suppose that the "kernel" of

$$\prod_{v \in B} \left(\mathrm{Pic}(C_v) / n\,\mathrm{Pic}(C_v)\right)_r \xrightarrow{\Theta \text{ of}} \mathrm{Gal}(L/K)$$

is <u>empty</u>, then

$$\mathrm{Pic}^r(C) = \mathrm{Pic}^{r+n}(C) = \mathrm{Pic}^{r+2n}(C) = \cdots = \phi.$$

Hyperelliptic Curves

$C: \; y^2 = g(x)$ $\qquad K = \mathbb{Q}$

$g(x) \in \mathbb{Z}[x]$

How to construct a suitable f ?

Suppose $x_1, x_2 \in \mathbb{Q}$ such that

$g(x_1) = d\, y_1^2 \qquad g(x_2) = d\, y_2^2$

for some $d \in \mathbb{Z} \setminus \{0\}$, d square-free, $y_1, y_2 \in \mathbb{Q}^*$.

Let $f = \dfrac{x - x_1}{x - x_2}$. Then

$$\mathrm{div}(f) = \underbrace{(x_1, y_1\sqrt{d}) - (x_2, y_2\sqrt{d})} + \text{conjugate}$$

Previous theory applies with $L = \mathbb{Q}(\sqrt{d})$.

Example

$$C: \; y^2 = \overbrace{-727x^4 - 104x^3 + 92x^2 + 4x - 4}^{g(x)}$$

$g(0) = -1 \times 2^2$ $\qquad g\left(\frac{-16}{53}\right) = \dfrac{-1 \times 2^2}{53^4}$

$f = \dfrac{1}{x}\left(x + \dfrac{16}{53}\right)$ $\qquad L = \mathbb{Q}(i)$

$\mathcal{B} = [\infty, 2]$

Primes	Basis for $\frac{Pic(C_p)}{2Pic(C_p)}$	$f(p)$	$(\theta_p \circ f)(p)$
$p=\infty$	$P_0 = (-0.3\ldots, 0.0003\ldots)$	-0.00028	-1
$p=2$	$P_0 = (2^{-1}, 2^{-2}+1+2+\cdots)$	$1+2^5+\cdots$	1
	$P_1 = (2^{-4}+\cdots, 2^{-8}+\cdots)$	$1+2^8+\cdots$	1

"Kernel" of $\left(\prod_p \frac{Pic(C_p)}{2Pic(C_p)}\right)_1 \longrightarrow \{1, -1\}$

is <u>empty</u>.

$\therefore \; C(\mathbb{Q}) = \phi.$

Generalization

C curve / K number field

$f \in K(C) \setminus K, \quad S = \text{Support}(f)$

Suppose $\exists P \in \text{Support}(f)$ s.t. $\text{ord}_P(f) = \pm 1$

Define $Cl_K = I_K / K^*$ idèle class group.

Then by class field theory $\exists$ abelian extension L/K such that

$$\text{Norm}(Cl_L) = \prod_{P \in S} \text{Norm}(Cl_{K(P)})^{\text{ord}_P(f)}.$$

Can extend f to

$$\text{Pic}(C) \longrightarrow K^* / \text{Norm}(L^*)$$

We call f anti-Hasse if L/K non-trivial.

Open Problem 1 For a given class of curves, find the anti-Hasse functions.

Open Problem 2

Can we get "arithmetic" information from the non-anti-Hasse functions using

$$\mathrm{Pic}(C) \longrightarrow K^*/G_f \quad ?$$

Example (S.S. & A. Skorobogatov)

$$X : \begin{cases} v^2 = -(3u^2+12u+13)(u^2+12u+39) \\ z^2 = 2u^2+6u+5 \end{cases}$$

Thm X does not have divisor classes of odd degree over $\mathbb{Q}(\sqrt{-13})$. (even though it is ELS).

Proof Proof uses a function f plus $X \longrightarrow Y$ where

$$Y : \quad v^2 = -(3u^2+12u+13)(u^2+12u+39)$$

References

1. "Sieving for rational points on hyperelliptic curves", M. Comp, 2001.

2. "Descent on Picard groups using functions on curves", Bull. Austral. Math. Soc. 2002

3. (S.S. & A. Skorobogatov) "On a Shimura curve that is a counterexample to the Hasse principle", Bull. London Math. Soc. 2003

4. (S.S. & M. Bright) "Functions, Reciprocity and the obstruction to divisors on curves" in preparation.

Samir Siksek
University of Warwick, UK

http://www.maths.warwick.uk/~siksek