Functions, Reciprocity, and the Obstruction to Divisors on Curves

Samir Siksek

15th July 2005

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 $q|Y$, $q \neq 2$ is a prime then $\left(\frac{17}{q}\right) = 1 \Rightarrow \left(\frac{q}{17}\right) = 1$ (also $\left(\frac{2}{17}\right) = 1$)
$\therefore Y \equiv Y_0^2 \mod 17 \quad \therefore 2Y_0^4 \equiv X^4 \mod 17$. 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 homogenous of *even* 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. There exists a λ such that $(\lambda X, \lambda Z) \equiv (\alpha, \beta) \mod (\beta X - \alpha Z)$

$$\therefore \gamma\delta^2 \equiv F(\alpha, \beta) \equiv F(\lambda X, \lambda Z) \equiv \lambda^{2r} F(X, Z) \equiv (\lambda^r Y)^2 \mod (\beta X - \alpha Z)$$

$\therefore \gamma$ is a quadratic residue mod $(\beta X - \alpha Z)$. $\therefore$ Get congruences for $\beta X - \alpha Z$. Repeat with several pairs α, β until we get a contradiction.

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

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

ELS but has no rational points.

Proof. WLOG $X, Y, Z \in \mathbb{Z}$, $\gcd(X, Z) = 1$, $Z > 0$. 2-adic solvability $\Rightarrow$ $Z = Z_0$ or $Z = 2Z_0$ where $2 \nmid Z_0$. If $q|Z_0$ then $\left(\frac{-1}{q}\right) = 1 \quad \therefore q \equiv 1 \mod 4$
$\therefore Z_0 \equiv 1 \mod 4$

$$\therefore\ Z \equiv 1 \mod 4 \qquad \text{or} \qquad Z \equiv 2 \mod 8.$$

Also $F(-53,16) = -2^2$. Get $|16X + 53Z| \equiv 1 \mod 4$ or $2 \mod 8$ Real solubility $\Rightarrow 16X + 53Z < 0 \quad \therefore 16X + 53Z \equiv 3 \mod 4$ or $6 \mod 8$.

$$\therefore\ Z \equiv 3 \mod 4 \qquad \text{or} \qquad Z \equiv 6 \mod 8.$$

Contradiction.

Part II: Functions and Divisors

Let C/K smooth projective curve, $f \in K(C) \setminus K$, $S \subseteq C(\bar{K})$ support of f. Define $\mathrm{Div}(\bar{C}) = \{\sum_{P \in C(\bar{K})} n_P P : n_P \in \mathbb{Z}, \text{ almost all } = 0\}$, $\mathrm{Div}(C) = (\mathrm{Div}\,\bar{C})^{\mathrm{Gal}(\bar{K}/K)}$, $(\mathrm{Div}\,C)_S$ divisors that *avoid* S.

Extend $f : (\mathrm{Div}\,C)_S \to K^*$, $f(\sum n_P P) = \prod f(P)^{n_P}$. Suppose $g \in K(C) \setminus K$ such that $\mathrm{support}(g) \cap S = \emptyset$. Then by Weil's reciprocity $f(\mathrm{div}(g)) = g(\mathrm{div}(f)) = \prod_{P \in S} g(P)^{\mathrm{ord}_P(f)} = \prod_{P \in S'} (\mathrm{Norm}(g(P)))^{\mathrm{ord}_P(f)}$ where $S' = \mathrm{Gal}(\bar{K}/K) \setminus S$.

Let $G_f = \prod_{P \in S'} (\mathrm{Norm}_{K(P)/K}(K(P)^*))^{\mathrm{ord}_P(f)}$, $\quad \therefore f(\mathrm{Princ}(C)_S) \subseteq G_f$, $\therefore f$ induces

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

But $\mathrm{Pic}\,C := \mathrm{Div}\,C/\mathrm{Princ}(C) = (\mathrm{Div}\,C)_S/\mathrm{Princ}(C)_S$, $\quad \therefore f \in K(C) \setminus K$ induces

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

PartII.V Class Field Theory

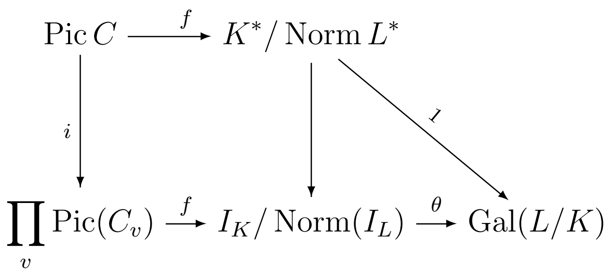
Let K number field, L/K finite abelian extension, I_K ideles $[I_K = \{(a_v)_v : a_v \in K_v^* \ldots\}]$.
Suppose v is a prime of K, $w|v$ prime of L.
Local Artin Map $\theta_v : K_v^*/\mathrm{Norm}(L_w^*) \to \mathrm{Gal}(L/K)$.
Artin Map $\theta : I_K/\mathrm{Norm}(I_L) \to \mathrm{Gal}(L/K)$ given by $\theta = \prod \theta_v$.
Artin Reciprocity. The sequence $K^* \to I_K/\mathrm{Norm}(I_L) \xrightarrow{\theta} \mathrm{Gal}(L/K)$ is exact.

Example. $K = \mathbb{Q}$, $L = \mathbb{Q}(i)$. Identify $\mathrm{Gal}(L/K) = \mu_2 = \{1, -1\}$. Local Artin map $\theta_p : \mathbb{Q}_p^* \to \{1,-1\}$, $\theta_p(\alpha) = \begin{cases} 1 & \text{if } \alpha = x^2 + y^2 \text{ with } x, y \in \mathbb{Q}_p \\ -1 & \text{otherwise.} \end{cases}$

III Reciprocity Joint with Martin Bright

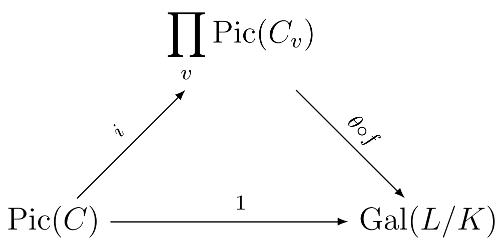
Let K number field, C/K curve, L/K finite abelian extension. Suppose $\mathrm{div}(f) = \sum_{\sigma \in \mathrm{Gal}(L/K)} D^\sigma$ where $\mathrm{supp}(D) \subseteq C(L)$. Then we get $G_f \subseteq$

$\operatorname{Norm}(L^*)$. So f induces

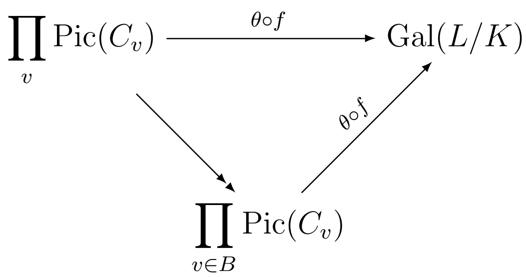


where θ is the Artin map.

Get

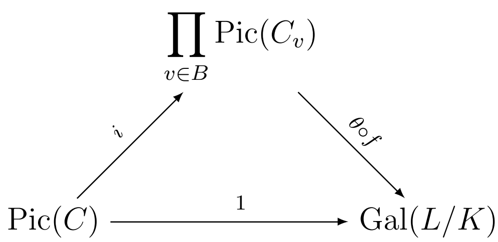


Lemma. $\exists$ a finite computable set B such that

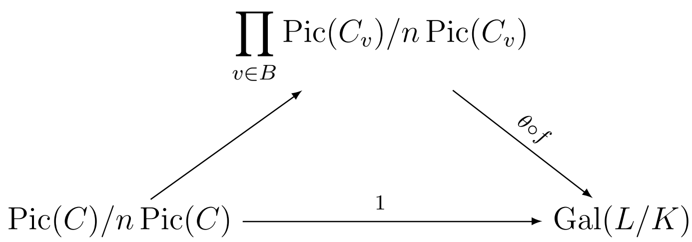


commutes.

Get



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



and $\prod_{v \in B} \operatorname{Pic}(C_v)/n \operatorname{Pic}(C_v)$ is finite and computable.

If $P_v \in C(K_v)$ then $\operatorname{Pic}(C_v)/n \operatorname{Pic}(C_v) = (\mathbb{Z}/n\mathbb{Z})P_v \oplus J(K_v)/nJ(K_v)$.

Lemma. Suppose $0 < r < n$. Let $(\operatorname{Pic}(C_v)/n \operatorname{Pic}(C_v))_r$ = subset of elements with degree $r \mod n$.

Suppose that the "kernel" of $\prod_{v \in B} (\operatorname{Pic}(C_v)/n \operatorname{Pic}(C_v))_r \xrightarrow{\theta \circ f} \operatorname{Gal}(L/K)$ is *empty*, then $\operatorname{Pic}^r(C) = \operatorname{Pic}^{r+n}(C) = \operatorname{Pic}^{r+2n}(C) = \ldots = \emptyset$.

Hyperelliptic Curves

$C : y^2 = g(x)$, $g(x) \in \mathbb{Z}[x]$, $K = \mathbb{Q}$.

How to construct a suitable f?

Suppose $x_1, x_2 \in \mathbb{Q}$ such that $g(x_1) = dy_1^2$, $g(x_2) = dy_2^2$ for some $d \in \mathbb{Z} \setminus \{0\}$, d square-free, $y_1, y_2 \in \mathbb{Q}^*$. Let $f = \frac{x - x_1}{x - x_2}$. Then

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

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

Example. $C : y^2 = \underbrace{-727x^4 - 104x^3 + 92x^2 + 4x - 4}_{g(x)}$

$g(0) = -1 \cdot 2^2$, $g(\frac{-16}{53}) = \frac{-1 \cdot 2^2}{53^4}$, $f = \frac{1}{x}(x + \frac{16}{53})$, $L = \mathbb{Q}(i)$.

$B = \{\infty, 2\}$

Primes	Basis for $\operatorname{Pic}(C_p)/2\operatorname{Pic}(C_p)$	$f(P)$	$(\theta_p \circ f)(P)$
$p = \infty$	$P_0 = (-0.3\ldots, 0.0003\ldots)$	-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 $(\prod_p \operatorname{Pic}(C_p)/2\operatorname{Pic}(C_p))_1 \to \{1, -1\}$ is *empty*. $\therefore C(\mathbb{Q}) = \emptyset$.

Generalization

C curve $/K$ number field. $f \in K(C) \setminus K$, $S = \operatorname{supp}(f)$.

Suppose $\exists P \in \operatorname{supp}(f)$ such that $\operatorname{ord}_P(f) = \pm 1$.

Define $Cl_K = I_K/K^*$ idèle class group. Then by class field theory $\exists$ abelian extension L/K such that $\operatorname{Norm}(Cl_L) = \prod \operatorname{Norm}(Cl_{K(P)})^{\operatorname{ord}_P(f)}$. Can extend f to $\operatorname{Pic}(C) \to K^*/\operatorname{Norm}(L^*)$. We call f *anti-Hasse* if L/K is 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 $\operatorname{Pic}(C) \to K^*/G_f$?

Example. (S. S. and A. Skorobogatov)

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

Theorem. 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 $X \to Y$ where $Y : v^2 = -(3u^2 + 12u + 13)(u^2 + 12u + 39)$.

References

[1] S. Siksek, Sieving for rational points on hyperelliptic curves, *M. Corp.* 2001.

[2] S. Siksek, Descent on Picard groups using functions on curves, *Bull. Austral. Math. Soc.* 2002.

[3] S. Siksek, and A. Skorobogatov, On a Shimura curve that is a counterexample to the Hasse principle, *Bull. London. Math. Soc.* 2003.

[4] S. Siksek, and 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

The diagrams were drawn with Paul Taylor's commutative diagrams package.