

Finite descent obstructions for integral points on curves

Felipe Voloch

University of Texas at Austin

Talk at Torsors conference ICMS, Jan 2011

Abstract

We will discuss various conjectures about finite descent obstructions for integral points on curves and their interrelations. We will also discuss an approach (via modularity) that leads to results on modular curves over the rational and can perhaps be extended to many other situations.

Introduction

Let $f(x, y) \in \mathbb{Z}[x, y]$. The equation $f = 0$ defines an algebraic curve and the integral points are the solutions to this equation with integer coordinates.

Obvious remark. If there exists a solution to $f = 0$ in integer coordinates then, for any integer $m > 2$, there are solutions to the congruence $f(x, y) \equiv 0 \pmod{m}$.

The converse does not hold, except in very simple situations, but it seems to be possible to determine the existence of integer solutions to $f = 0$ using congruences.

Basic definitions

K - number field (e.g. $K = \mathbb{Q}$)

S - finite set of primes of K

\mathcal{O}_S - S -integers of K (e.g. if $S = \{2\}$ and $K = \mathbb{Q}$, \mathcal{O}_S is the ring of rational numbers whose denominator is a power of 2.)

X is a (smooth, irreducible affine) algebraic curve over K .

$X(\mathcal{O}_S)$ - Set of S -integral points of X , i.e. the set of points of X with coordinates in \mathcal{O}_S (for some fixed choice of coordinate system).

Example to keep in mind: $x + y = 1, xu = 1, yv = 1$ in 4-space.

Solutions in \mathcal{O}_S are units $x, y \in \mathcal{O}_S$, with $x + y = 1$.

Local points

We denote by \mathcal{O}_v the completion of \mathcal{O}_S for a prime v of K not in S .

The set $X(\mathcal{O}_v)$ is the set of points of X with coordinates in \mathcal{O}_v . We will look at $\prod_{v \notin S} X(\mathcal{O}_v)$ as a proxy for looking at $f \equiv 0 \pmod{m}$ for all m .

An example

The equation $x^2 + 23y^2 = 41$ has no solutions in integers (easy) but it has solutions modulo m for all m . Note it has rational solutions (e.g. $(1/3, 4/3), (9/4, 5/4)$). The first provides solutions modulo m if $(m, 3) = 1$ and the second if $(m, 2) = 1$, so there are solutions modulo every m .

Covers and twists

A cover $\pi : Y \rightarrow X$ is a map of curves such that $\pi : Y(\mathbb{C}) \rightarrow X(\mathbb{C})$ is Galois and unramified.

A twist of a cover π is a map $\pi' : Y' \rightarrow X$ such that it is isomorphic over \bar{K} to $\pi : Y \rightarrow X$ as a cover. The set of isomorphism classes of twists of π will be denoted $Tw(\pi)$.

Chevalley-Weil Theorem

$X(\mathcal{O}_S) = \cup_{\pi' \in Tw_0(\pi)} \pi'(Y'(\mathcal{O}_S)), Tw_0(\pi) \subset Tw(\pi)$ finite.

In fact, $Tw_0(\pi)$ can be taken to be the set of π' such that

$$\prod_{v \notin S} Y'(\mathcal{O}_v) \neq \emptyset.$$

In the example $x + y = 1, xu = 1, yv = 1$ in 4-space. We can consider covers $z^n = x, w^n = y$. The twists are $z^n = ax, w^n = by$. For a such twist to have local points $a, b \in \mathcal{O}_S^*/(\mathcal{O}_S^*)^n$, which is finite.

Another viewpoint

For $P \in X(F)$, F a field, $\pi^{-1}(P)$ is a G_F -torsor, (G_F absolute galois group of F).

View $\pi^{-1}(P) \in H^1(G_F, G)$. For $(P_v) \in \prod_{v \notin S} X(\mathcal{O}_v)$ get class in $\prod H^1(G_{K_v}, G)$ and look at set of (P_v) for which the corresponding class is global.

Main Conjecture

Motivated by the Chevalley-Weil Theorem, consider X^{f-cov} the subset of $(P_v) \in \prod_{v \notin S} X(\mathcal{O}_v)$, such that for all covers π of X there exists a twist π' of it and a point (Q_v) in the corresponding $\prod_{v \notin S} Y'(\mathcal{O}_v)$ with $\pi'(Q_v) = P_v, \forall v$.

Main Conjecture: $X^{f-cov} = X(\mathcal{O}_S)$.

Similar statement previously made for rational points by Stoll.

Integral points considered in a paper of Harari and V. where we looked mostly at abelian covers .

Abelian covers equivalent to Brauer-Manin for curves.

Consequences

Main conjecture implies there is an algorithm to decide if $X(\mathcal{O}_S) = \emptyset$.

Also implies an old conjecture of Skolem. Exponential diophantine equations in unknowns $x_i, y_i \in \mathbb{Z}$,

$$a \prod d_i^{x_i} + b \prod d_i^{y_i} = c$$

has solutions iff corresponding congruences modulo m have solutions for all m .

Elliptic curves minus a point

Main conjecture needs non-abelian covers (Harari and V.)

E/\mathbb{Q} elliptic curve, $X = E - \{0\}$. $E(\mathbb{Q})$ can be infinite while $X(\mathcal{O}_S)$ is finite. $\pi_1(E) \neq \pi_1(X)$ but they have the same abelianization.



Modularity I

Main conjecture is true for twists of modular curves over \mathbb{Q} (Helm and V.).

Y_N moduli space of (E, P, C) , E elliptic curve, $P \in E$ order N , C cyclic subgroup of E of order N . $Y_N \rightarrow Y_M$ if $M|N$.

Twists of Y_N over F , correspond to $\rho : G_F \rightarrow \mathrm{GL}_2(\mathbb{Z}/N)$ with $\det \rho$ cyclotomic character.

Modularity II

Fix a twist of some Y_N corresponding to ρ . Assume that $X^{f-cov} \neq \emptyset$. Then we get elliptic curves E_v/K_v with good reduction at v , $\forall v \notin S$. Also, $\forall \ell$ primes we get Galois representations $\rho_\ell : G_K \rightarrow GL_2(\mathbb{Z}_\ell)$, whose determinant is the cyclotomic character and compatible with ρ , such that ρ_ℓ restricted to a decomposition group at v is (as a Galois module) the Tate module $T_\ell E_v$.

Modularity III

Over \mathbb{Q} , Serre's conjecture (proved by Khare and Winterberger) implies that such ρ_ℓ come from an elliptic curve over \mathbb{Q} and so $X(\mathcal{O}_S) \neq \emptyset$.

Over an arbitrary number field, the Fontaine-Mazur conjecture (still open) implies similar conclusion (even for higher dim'l abelian varieties!).

Note: Fontaine-Mazur needs only one ℓ and, apart from good reduction, only requires existence of E_v if $v|\ell$. Reminiscent of section conjecture, where just existence of section (= gal. rep) is enough to get point.

THANK YOU

Papers available at

<http://www.ma.utexas.edu/users/voloch/>