Local-Global principles for integral points on curves

Felipe Voloch

University of Texas at Austin

Talk at University of North Texas, September 2012

Abstract

Abstract: In this talk we discuss a conjectural local-global principle to decide existence of integral points on algebraic curves and present some partial results and evidence towards this conjecture.

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 $f(x, y) \equiv 0 \mod m$.

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 together with places at ∞.

$\mathcal{O}_S$ - 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. It is a ring that should be thought of as having the information of all congruences modulo powers of v. In the case of $\mathbb{Q}$ we get the p-adic integers

$$\mathbb{Z}_p = \{\sum_{n=0}^{\infty} a_n p^n \mid 0 \leq a_n \leq p-1\}$$

(base p expansions that stretch to infinity)

The set $X(\mathcal{O}_v)$ is the set of points of X with coordinates in $\mathcal{O}_v$. We will look at $\prod_{v \notin S} X(\mathcal{O}_v) \times \prod_{v \in S} X(K_v)$ as a proxy for looking at $f \equiv 0 \mod m$ 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 $\gcd(m, 3) = 1$ and the second does if $\gcd(m, 2) = 1$. So get solutions for all m.

Covers and twists

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

A twist of a cover π is a map $\pi' : Y' \to X$ such that it is isomorphic over $\bar{K}$ to $\pi : Y \to X$ 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

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

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.

Main Conjecture

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

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.

Consequences

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

So it cannot work in arbitrary dimension!

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 correspoding congruences modulo m have solutions for all m.

Results

Function fields: (Harari and V.) Main conjecture is true for varieties of arbitrary dimension. Proof uses Artin-Schreier covers which don't exist in char. zero.

Modular curves: Main conjecture is true for twists of modular curves over $\mathbb{Q}$ (Helm and V.) Proof uses "modularity".

But it doesn't extend to number fields.

Elliptic curves minus a point

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.

A counterexample in dim. two

According to Colliot-Thélène and Wittenberg, the equation $2x^2 + 3y^2 + 4z^2 = 1$ has local solutions everywhere, no global solutions, and no Brauer-Manin obstructions. It pointed out by J. Park that the surface is also simply-connected, so has no covers.

THANK YOU

Papers available at

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