Uniform boundedness of rational points

Bjorn Poonen

MIT

CNTA XII, Lethbridge
June 21, 2012

PART 1: RATIONAL POINTS

Example

The equation

$$y^2 = x^6 + 8x^5 + 22x^4 + 22x^3 + 5x^2 + 6x + 1$$

has 4 rational solutions.

Example

The equation

$$y^2 = -x^6 - x^5 - x^4 - x^3 - x^2 - x - 1$$

has 0 rational solutions.

Example

The equation

$$y^2 = x^6 + 2x^5 + 5x^4 + 10x^3 + 10x^2 + 4x + 1$$

has 4 rational solutions.

Example

The equation

$$y^2 = x^6 + 2x^5 + x^4 + 2x^3 + 6x^2 + 4x + 1$$

has 4 rational solutions.

Example

The equation

$$y^2 = x^6 - 2x^4 + 2x^3 + 5x^2 + 2x + 1$$

has 6 rational solutions.

Example (Stoll, found by searching in a family constructed by Elkies)

The equation

$$y^2 = 82342800x^6 - 470135160x^5 + 52485681x^4 + 2396040466x^3 \\ + 567207969x^2 - 985905640x + 247747600$$

has at least 642 rational solutions.

Finiteness and uniform boundedness

Theorem (special case of Faltings 1983)

If $f(x) \in \mathbb{Q}[x]$ is squarefree of degree 6, then the number of rational solutions to $y^2 = f(x)$ is finite.

Question (special case of Caporaso, Harris, and Mazur 1997)

Is there a number B such that for any squarefree $f(x) \in \mathbb{Q}[x]$ of degree 6, the number of rational solutions to $y^2 = f(x)$ is at most B?

$$\left\{ \begin{array}{c} \text{(smooth projective models of)} \\ \text{the curves } y^2 = f(x)\text{:} \\ f(x) \in \mathbb{Q}[x] \text{ squarefree} \\ \deg f = 6 \end{array} \right\} = \left\{ \begin{array}{c} \text{genus 2 curves} \\ \text{over } \mathbb{Q} \end{array} \right\}$$

Theorem (Faltings 1983)

~~*If $f(x) \in \mathbb{Q}[x]$ is squarefree of degree 6,*~~
~~*then the number of rational solutions to $y^2 = f(x)$ is finite.*~~
If X is a curve of genus ≥ 2 over a number field k,
then $X(k)$ is finite.

Question (Caporaso, Harris, and Mazur 1997)

~~*Is there a number B such that*~~
~~*for each squarefree $f(x) \in \mathbb{Q}[x]$ of degree 6,*~~
~~*the number of rational solutions to $y^2 = f(x)$ is at most B?*~~
Given $g \geq 2$ and a number field k,
is there $B_{g,k}$ such that for each curve X of genus g over k,
$\#X(k) \leq B_{g,k}$?

Question (Caporaso, Harris, and Mazur 1997, again)

Given $g \geq 2$ and a number field k,
is there $B_{g,k}$ such that for each curve X of genus g over k,
$\#X(k) \leq B_{g,k}$?

Example

- $B_{2,\mathbb{Q}} \geq 642$ (Stoll, building on work of Elkies).
- $B_{g,\mathbb{Q}} \geq 8g + 16$ (Mestre).

- Caporaso, Harris, and Mazur showed that a conjecture of Lang would imply a positive answer to their question.
- Pacelli showed that Lang's conjecture would imply also that $B_{g,k}$ could be chosen to depend only on g and $[k : \mathbb{Q}]$.
- Abramovich and Voloch generalized to higher-dimensional varieties for which all subvarieties are of general type ("Lang implies uniform Lang").

Uniform boundedness for arbitrary families

Is it true that in *any* algebraic family of varieties, the number of rational points of the varieties is uniformly bounded after discarding the varieties with infinitely many rational points? More precisely:

Main Question

k: number field
$\pi\colon X \to S$ a morphism of finite-type k-schemes
For $s \in X(k)$, let X_s be the fiber $\pi^{-1}(s)$.
Must $\{\#X_s(k) : s \in S(k)\}$ be finite?

Example

Let X be $y^2 = x^3 + ax + b$ in $\mathbb{A}^4 = \operatorname{Spec} \mathbb{Q}[x, y, a, b]$ mapping to $S = \mathbb{A}^2 = \operatorname{Spec} \mathbb{Q}[a, b]$ by projection onto the (a, b)-coordinates. For most $s = (a_0, b_0) \in S(\mathbb{Q})$, the fiber X_s is an elliptic curve over $\mathbb{Q}$ (minus the point at infinity). By Mazur's theorem,

$$\{\#X_s(\mathbb{Q}) : s \in S(\mathbb{Q})\} \;=\; \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 11, 15, \aleph_0\},$$

which is a finite set.

Main Question

k: number field
$\pi\colon X \to S$ a morphism of finite-type k-schemes
Must $\{\#X_s(k) : s \in S(k)\}$ be finite?

By reducing to the case where X and S are affine, one gets:

Main Question (equivalent version)

k: number field
$f_1, \ldots, f_m \in k[s_1, \ldots, s_r, x_1, \ldots, x_n]$
For $\vec{a} \in k^r$, let $N_{\vec{a}}$ = number of solutions to $\vec{f}(\vec{a}, \vec{x}) = 0$ in k^n.
Is there a bound $B = B(k, \vec{f})$ such that
$$N_{\vec{a}} \leq B \qquad \text{for all } \vec{a} \text{ for which } N_{\vec{a}} \text{ is finite?}$$

The case $k = \mathbb{Q}$ is equivalent to the case of a general number field.
Why?

Restriction of scalars

The case $k = \mathbb{Q}$ is equivalent to the case of a general number field. Why?

Any polynomial equation over a number field can be converted to a system of polynomial equations over $\mathbb{Q}$.

Example (copied from Filip Najman's talk)

The solutions to

$$y^2 = x^3 + i$$

in $\mathbb{Q}(i)$ are in bijection with the solutions to

$$(y_0 + y_1 i)^2 = (x_0 + x_1 i)^3 + i$$

in $\mathbb{Q}$, and the latter can be expanded into real and imaginary parts

$$\begin{aligned} y_0^2 - y_1^2 &= x_0^3 - 3x_0x_1^2 \\ 2y_0y_1 &= 3x_0^2x_1 - x_1^3 + 1. \end{aligned}$$

"Restriction of scalars" lets one show also that it is no more general if one asks for uniform boundedness as L ranges over extensions of k of bounded degree:

Main Question (equivalent version)

k: number field
$\pi \colon X \to S$ a morphism of finite-type k-schemes
$d \geq 1$
Must $\{\#X_s(L) : [L : k] \leq d,\ s \in S(L)\}$ be finite?

(Introduce the coefficients of the equation defining L/k as additional parameters, and consider the giant family consisting of all restrictions of scalars obtained.)

Combining many equations into one of degree 4 (Skolem's trick)

Example

The equation $y^2 = x^5 + 7$ over $\mathbb{Q}$ is equivalent to the system

$$u = x^2, \qquad v = u^2, \qquad y^2 = xv + 7$$

of equations of degree 2, which is equivalent to the equation

$$(u - x^2)^2 + (v - u^2)^2 + (y^2 - xv - 7)^2 = 0$$

of degree 4.

Main Question (equivalent version)

For each $n \geq 1$, is there a number B_n such that for every $f \in \mathbb{Q}[x_1, \ldots, x_n]$ of total degree 4 such that $f(\vec{x}) = 0$ has finitely many rational solutions, the number of solutions is $\leq B_n$?

Other fields

Main Question for the field k

$\pi\colon X \to S$ a morphism of finite-type k-schemes.
Must $\{\#X_s(k) : s \in S(k)\}$ be finite?

- If $k = \mathbb{F}_p(t)$ for some $p > 2$, the answer is NO:
  The curve
  $$X_a\colon x - ax^p = y^p$$
  has finitely many k-points for each $a \in k - k^p$,
  but $\#X_a(k)$ is unbounded as a varies in this set
  (Abramovich and Voloch 1996).
- If k is a finitely generated extension of $\mathbb{Q}$,
  the answer might still be YES.
- For $\mathbb{C}$, $\mathbb{R}$, $\mathbb{Q}_p$, the answer is YES.
- There exists an (artificial) field of characteristic 0
  for which the answer is NO.

Stronger variant 1: Zariski closures

Question

k: number field (or finitely generated extension of $\mathbb{Q}$)
$\pi\colon X \to S$ a morphism of finite-type k-schemes
For $s \in S(k)$, let z_s be the number of irreducible components of the Zariski closure of $X_s(k)$ in X_s.
Must $\{z_s : s \in S(k)\}$ be bounded?

This is at least as strong as the Main Question.

Stronger variant 2: Topology of rational points

X: finite-type $\mathbb{Q}$-scheme
Define

$$\overline{X(\mathbb{Q})} := \text{closure of } X(\mathbb{Q}) \text{ in } X(\mathbb{R}) \text{ in Euclidean topology.}$$

Conjecture (Mazur 1992)

$\overline{X(\mathbb{Q})}$ has at most finitely many connected components.

Question

$\pi \colon X \to S$ a morphism of finite-type $\mathbb{Q}$-schemes
For $s \in S(\mathbb{Q})$, let c_s be the number of connected components of $\overline{X_s(\mathbb{Q})}$. Must $\{c_s : s \in S(\mathbb{Q})\}$ be finite?

This is at least as strong as the Main Question.

Example

For families of curves over $\mathbb{Q}$, this new question is equivalent to the Caporaso-Harris-Mazur question. (Use boundedness of $E(\mathbb{Q})_{\mathrm{tors}}$ to handle families of genus 1 curves.)

PART 2: PREPERIODIC POINTS

Definition

Given $f\colon X \to X$ and $x \in X(k)$,

$$\begin{aligned} x \text{ is preperiodic } &\iff \text{its forward trajectory is finite} \\ &\iff f^n(x) = f^m(x) \text{ for some } m > n. \end{aligned}$$

Let $\mathrm{PrePer}(f, k)$ be the set of such points.

Example

Fix $c \in \mathbb{Q}$ and consider

$$\begin{aligned} f\colon \mathbb{A}^1 &\to \mathbb{A}^1 \\ z &\mapsto z^2 + c. \end{aligned}$$

For $z \in \mathbb{Q}$, the heights satisfy $h(z^2 + c) = 2h(z) + O(1)$.
So if z has sufficiently large height, then $z, f(z), f(f(z)), \ldots$ will have strictly increasing height, so z will not be preperiodic.
Thus $\mathrm{PrePer}(f, \mathbb{Q})$ is of bounded height, hence finite (Northcott).

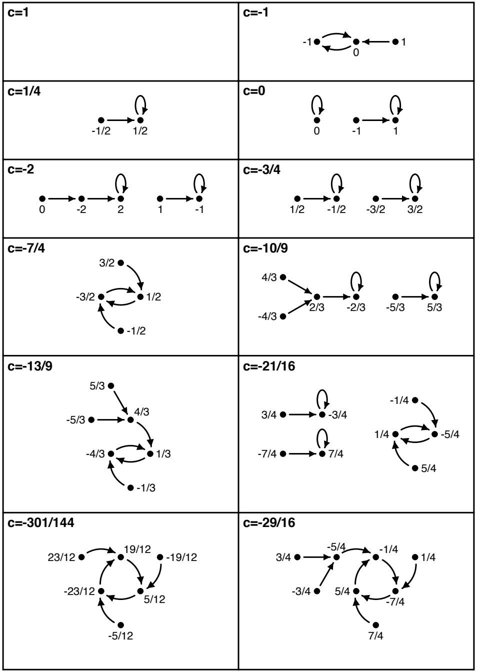

Figure 1. Finite Rational Preperiodic Points of z^2+c.

Finiteness and uniform boundedness

Theorem (Northcott 1950)

k: number field
$f : \mathbb{P}^n \to \mathbb{P}^n$ a morphism of degree $d \geq 2$ over k
Then $\operatorname{PrePer}(f, k)$ is finite.

Morton-Silverman conjecture (1994)

For k and f as above, $\# \operatorname{PrePer}(f, k)$ is bounded by a constant depending only on n, d, and $[k : \mathbb{Q}]$.

Although the Morton-Silverman conjecture is only for self-maps of $\mathbb{P}^n$, it implies boundedness for self-maps of some other varieties.

Example

A: abelian variety over a number field k

$[2]: A \to A$ the multiplication-by-2 map

Then $\mathrm{PrePer}([2], k) = A(k)_{\mathrm{tors}}$.

Fakhruddin: one can find maps i and f completing the diagram

$$\begin{tikzcd} A \arrow[r, "{[2]}"] \arrow[d, hook, "i"] & A \arrow[d, hook, "i"] \\ \mathbb{P}^n \arrow[r, "f"] & \mathbb{P}^n \end{tikzcd}$$

Corollary: The Morton-Silverman conjecture would imply the following generalization of the Mazur-Kamienny-Merel theorem:

Uniform boundedness conjecture for torsion of abelian varieties

$\#A(k)_{\mathrm{tors}}$ *is bounded by a constant depending only on* $\dim A$ *and* $[k : \mathbb{Q}]$.

Uniform boundedness for preperiodic points

k: number field (or finitely generated extension of $\mathbb{Q}$)
$\pi\colon X \to S$ a morphism of finite-type k-schemes
$f\colon X \to X$ an S-morphism

$$\begin{tikzcd} X \arrow[rr, "f"] \arrow[dr, "\pi"'] & & X \arrow[dl, "\pi"] \\ & S & \end{tikzcd}$$

The data above define a family of dynamical systems:
for each $s \in S(k)$, one gets $f_s\colon X_s \to X_s$ over k.

Main Question for preperiodic points

For k, π, f as above, must $\{\#\operatorname{PrePer}(f_s, k) : s \in S(k)\}$ be finite?

Example

If f is the identity morphism, then $\operatorname{PrePer}(f_s, k) = X_s(k)$,
so this special case is the Main Question for rational points.

Uniform boundedness for preperiodic points: variants

Main Question for preperiodic points (again)

k: number field (or finitely generated extension of $\mathbb{Q}$)
$\pi\colon X \to S$ a morphism of finite-type k-schemes
$f\colon X \to X$ an S-morphism
Must $\{\#\operatorname{PrePer}(f_s, k) : s \in S(k)\}$ be finite?

As with the Main Question for rational points,
there are stronger variants for

- preperiodic points over L with $[L : k]$ bounded
  (equivalent question, if X is quasi-projective over S)
  Taking the universal family of degree d self-maps of $\mathbb{P}^n$ yields the Morton-Silverman conjecture.
- the Zariski closure of $\operatorname{PrePer}(f_s, k)$
- the connected components of $\overline{\operatorname{PrePer}(f_s, \mathbb{Q})}$ in $X_s(\mathbb{R})$.