Introduction to rational points

Bjorn Poonen

University of California at Berkeley

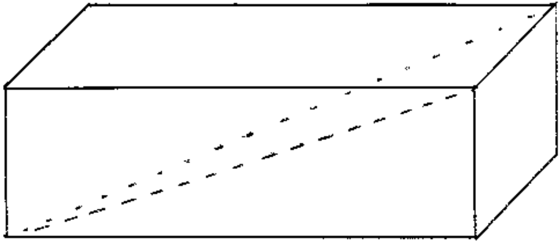
MSRI Introductory Workshop on Rational and Integral Points on Higher-dimensional Varieties

(organized by Jean-Louis Colliot-Thélène, Roger Heath-Brown, János Kollár, Bjorn Poonen, Alice Silverberg, Yuri Tschinkel)

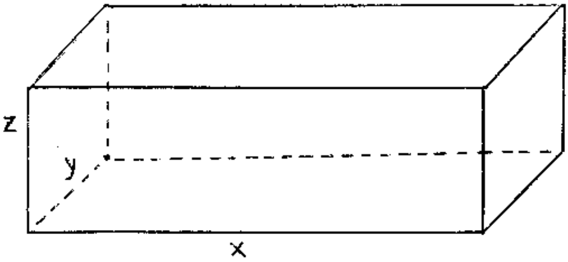
January 17, 2006

An open problem

Is there a rectangular box such that the lengths of the edges, face diagonals, and long diagonals are all rational numbers?



No one knows.



Equivalently, are there rational points (x, y, z, p, q, r, s) with positive coordinates on the variety defined by

$$x^2 + y^2 = p^2$$
$$y^2 + z^2 = q^2$$
$$z^2 + x^2 = r^2$$
$$x^2 + y^2 + z^2 = s^2 \ ?$$

One of the hopes of arithmetic geometry is that geometric methods will give insight regarding the rational points.

Affine varieties

- Affine space $\mathbb{A}^n$ is such that $\mathbb{A}^n(L) = L^n$ for any field L.
- An affine variety X over a field k is given by a system of multivariable polynomial equations with coefficients in k

$$\begin{aligned} f_1(x_1, \ldots, x_n) &= 0 \\ &\vdots \\ f_m(x_1, \ldots, x_n) &= 0. \end{aligned}$$

For any extension $L \supseteq k$, the set of L-rational points (also called L-points) on X is

$$X(L) := \{\vec{a} \in L^n : f_1(\vec{a}) = \cdots = f_m(\vec{a}) = 0\}.$$

Projective varieties

If L is a field, the multiplicative group $L^\times$ acts on $L^{n+1} - \{\vec{0}\}$ by scalar multiplication, and we may take the set of orbits.

- Projective space $\mathbb{P}^n$ is such that

$$\mathbb{P}^n(L) = \frac{L^{n+1} - \{\vec{0}\}}{L^\times}$$

  for every field L. Write $(a_0 : \cdots : a_n) \in \mathbb{P}^n(L)$ for the orbit of $(a_0, \ldots, a_n) \in L^{n+1} - \{\vec{0}\}$.

- A projective variety X over k is defined by a polynomial system $\vec{f} = 0$ where $\vec{f} = (f_1, \ldots, f_m)$ and the $f_i \in k[x_0, \ldots, x_n]$ are *homogeneous*.
  For any field extension $L \supseteq k$, define

$$X(L) := \{(a_0 : \cdots : a_n) \in \mathbb{P}^n(L) : \vec{f}(\vec{a}) = 0\}.$$

Guiding problems of arithmetic geometry

Given a variety X over $\mathbb{Q}$, can we

1. decide if X has a $\mathbb{Q}$-point?
2. describe the set $X(\mathbb{Q})$?

- The first problem is well-defined. Tomorrow's lecture on Hilbert's tenth problem will discuss weak evidence to suggest that it is undecidable.
- The second problem is more vague. If $X(\mathbb{Q})$ is finite, then we can ask for a list of its points. But if $X(\mathbb{Q})$ is infinite, then it is not always clear what constitutes a description of it.

The same questions can be asked over other fields, such as

- number fields (finite extensions of $\mathbb{Q}$), or
- function fields (such as $\mathbb{F}_p(t)$ or $\mathbb{C}(t)$).

Dimension, smoothness, irreducibility

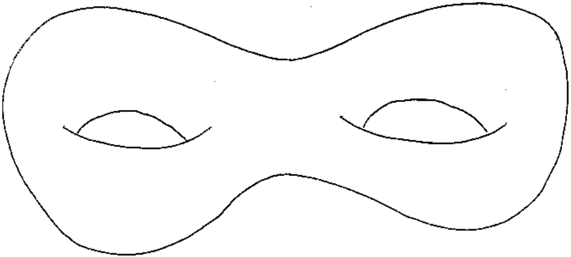
- Let X be a variety over a subfield of $\mathbb{C}$. Its dimension $d = \dim X$ can be thought of as the complex dimension of the complex space $X(\mathbb{C})$.
- If there are no singularities, $X(\mathbb{C})$ is a d-dimensional complex manifold, and X is called smooth in this case.
- Call X geometrically irreducible if X is not a union of two strictly smaller closed subvarieties, even when considered over $\mathbb{C}$. ("Geometric" refers to behavior over $\mathbb{C}$ or some other algebraically closed field.)
  Example: The affine variety $x^2 - 2y^2 = 0$ over $\mathbb{Q}$ is not geometrically irreducible.
- *From now on, varieties will be assumed smooth, projective, and geometrically irreducible.*

Much is known about the guiding problems in the case of curves ($d = 1$). We will discuss this next, because it helps motivate the conjectures in the higher-dimensional case.

Genus of a curve

Let X be a curve over $\mathbb{C}$. The genus $g \in \{0, 1, 2, \ldots\}$ of X is a geometric invariant that can be defined in many ways:

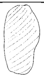
- The compact Riemann surface $X(\mathbb{C})$ is a g-holed torus (topological genus).



- g is the dimension of the space $H^0(X, \Omega^1)$ of holomorphic 1-forms on X (geometric genus).
- g is the dimension of the sheaf cohomology group $H^1(X, \mathcal{O}_X)$ (arithmetic genus).

Classification of curves over $\mathbb{C}$: moduli spaces

Curves of genus g over $\mathbb{C}$ are in bijection with the complex points of an irreducible variety $\mathcal{M}_g$, called the moduli space of genus-g curves.

g		moduli space $\mathcal{M}_g$
≥ 2		variety of dimension $3g-3$
1	$\longleftrightarrow$	$\mathbb{A}^1$ (parameterizing elliptic curves by j-invariant)
0	$\bullet$	point (representing $\mathbb{P}^1$)

Classification of curves over $\mathbb{C}$: the trichotomy

- The value of g influences many geometric properties of X:

g	curvature	canonical bundle	Kodaira dim
≥ 2	negative	$\deg K > 0$ (K ample)	$\kappa = 1$ (general type)
1	zero	$K = 0$	$\kappa = 0$
0	positive	$\deg K < 0$ (anti-ample, Fano)	$\kappa = -\infty$

- Surprisingly, if X is over a number field k, then g influences also the set of rational points. Roughly, the higher g is in this trichotomy, the fewer rational points there are.
- Generalizations to higher-dimensional varieties will appear in Caporaso's lectures.

Genus ≥ 2

Theorem (Faltings 1983, second proof by Vojta 1989)

Let X be a curve of genus ≥ 2 over a number field k. Then $X(k)$ is finite (maybe empty).

- Both proofs give, in principle, an upper bound on $\#X(k)$ computable in terms of X and k. But they are ineffective in that they cannot list the points of $X(k)$, even in principle.
- The question of *how* the upper bound depends on X and k will be discussed in Caporaso's lecture on uniformity of rational points today.
- There exist a few methods (not based on the proofs of Faltings and Vojta) that in combination often succeed in determining $X(k)$ for individual curves of genus ≥ 2:
  1. the p-adic method of Chabauty and Coleman.
  2. the Brauer-Manin obstruction, which for curves can be understood as a "Mordell-Weil sieve".
  3. descent, to replace the problem with the analogous problem for a finite collection of finite étale covers of X.

Genus 1

Let X be a curve of genus 1 over a number field k.

- It may happen that $X(k)$ is empty.
- If $X(k)$ is nonempty, then X is an elliptic curve, and the Mordell-Weil theorem states that $X(k)$ has the structure of a finitely generated abelian group. This will be discussed further in Rubin's lectures.
- In any case, there will exist a finite extension $L \supseteq k$ such that $X(L)$ is infinite. (A generalization of this property to higher-dimensional varieties will appear in Hassett's lecture on potential density.)
- But even when $X(L)$ is infinite, it is "sparse" in a sense to be made precise later, when we discuss counting points of bounded height.

Genus 0: existence of rational points

Let X be a curve of genus 0 over a number field k.

- There is a simple test to decide whether X has a k-point.
- For example, if $k = \mathbb{Q}$, one has

$$X(\mathbb{Q}) \neq \emptyset \iff \begin{array}{c} X(\mathbb{R}) \neq \emptyset, \text{ and} \\ X(\mathbb{Q}_p) \neq \emptyset \text{ for all primes } p. \end{array}$$

  (This is an instance of the Hasse principle, to be discussed further in the lectures by Wooley and Harari.)
- The conditions about $\mathbb{Q}_p$-points mean concretely that there are no obstructions to rational points arising from considering equations modulo various integers. We will make this even more concrete on the next slide.

Genus 0: existence of rational points (continued)

Every genus-0 curve over $\mathbb{Q}$ is isomorphic to a conic in $\mathbb{P}^2$ given by an equation

$$ax^2 + by^2 + cz^2 = 0$$

where $a, b, c \in \mathbb{Z}$ are squarefree and pairwise relatively prime.

Theorem (Legendre)

This curve has a rational point if and only if

1. *a, b, c do not all have the same sign, and*
2. *the congruences*

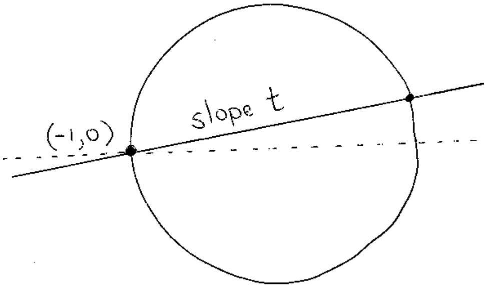
$$as^2 + b \equiv 0 \pmod{c}$$
$$bt^2 + c \equiv 0 \pmod{a}$$
$$cu^2 + a \equiv 0 \pmod{b}$$

have solutions $s, t, u \in \mathbb{Z}$.

Genus 0: parameterization of rational points

- If $X(k)$ is nonempty, then $X \simeq \mathbb{P}^1$ over k. In other words, $X(k)$ can be parameterized by rational functions.
- For example, suppose X is the affine curve $x^2 + y^2 = 1$ over $\mathbb{Q}$. Drawing a line of variable rational slope t through $(-1, 0)$ and computing its second intersection point with X leads to

$$X(\mathbb{Q}) = \left\{ \left(\frac{1-t^2}{1+t^2}, \frac{2t}{1+t^2} \right) : t \in \mathbb{Q} \right\} \cup \{(-1,0)\}.$$



Counting rational points of bounded height

How do we measure $X(\mathbb{Q})$ when it is infinite?

- If X is affine, we can count for each $B > 0$ the (finite) number of points in $X(\mathbb{Q})$ whose coordinates have numerator and denominator bounded by B in absolute value, and see how this count grows as $B \to \infty$.
- Similarly, if $X \subseteq \mathbb{P}^n$ is projective, we define

$$N_X(B) := \#\{(a_0 : \cdots : a_n) \in X(\mathbb{Q}) : a_i \in \mathbb{Z}, \max |a_i| \leq B\}$$

  and ask about the asymptotic growth of $N_X(B)$ as $B \to \infty$. The measure $\max |a_i|$ of a point $(a_0 : \cdots : a_n)$ with $a_i \in \mathbb{Z}$ is the first example of height, which will be developed further in the lectures by Silverman.

Counting points on curves

Let X be a genus-g curve over $\mathbb{Q}$ with at least one $\mathbb{Q}$-point.

g	$N_X(B)$ up to a factor $(c+o(1))$ for some $c>0$	
≥ 2	1	(eventually constant, by Faltings)
1	$(\log B)^{r/2}$	where $r := \operatorname{rank} X(\mathbb{Q})$
0	B^a	where $a>0$ depends on how X is embedded in projective space.

Example:
For the genus-0 curve $X=\mathbb{P}^1$ (embedded in itself),

$$N_X(B) \approx \frac{12}{\pi^2} B^2.$$

One method for bounding $N_X(B)$ for a higher-dimensional variety X is to view X as a family of curves $\{Y_t\}$. For this one wants a bound on $N_{Y_t}(B)$ that is uniform in t (work of Bombieri, Pila, Heath-Brown, Ellenberg, Venkatesh, Salberger, Browning).

Counting points on hypersurfaces

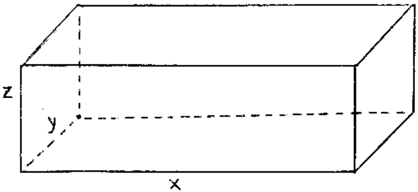
Let X be a degree-d hypersurface $f(x_0, \ldots, x_n) = 0$ in $\mathbb{P}^n$ over $\mathbb{Q}$.

- The number of $(a_0 : \cdots , a_n) \in \mathbb{P}^n(\mathbb{Q})$ with $a_i \in \mathbb{Z}$ and $\max |a_i| \le B$ is of order B^{n+1}. For each such $\vec{a} = (a_0, \ldots, a_{n+1})$, the value $f(\vec{a})$ is of size $O(B^d)$. If we use the heuristic that a number of size $O(B^d)$ is 0 with probability $1/B^d$, we predict that

$$N_X(B) \sim B^{n+1-d}.$$

- Warning: this conclusion is sometimes false!.
- Interestingly, the sign of $n + 1 - d$ determines also whether the canonical bundle of X is ample.
- The circle method, to be discussed in Wooley's lectures, *proves* results along these lines when $n \gg d$.
- In the "Fano" case $n + 1 - d > 0$ (i.e., $-K$ ample), these heuristics lead to examples of the Manin conjecture, to be discussed in Heath-Brown's lectures.

Back to the box



- The system

$$x^2 + y^2 = p^2$$
$$y^2 + z^2 = q^2$$
$$z^2 + x^2 = r^2$$
$$x^2 + y^2 + z^2 = s^2$$

  defines a surface of general type in $\mathbb{P}^6$ (van Luijk).
- Various heuristics suggest that there are no rational points with positive coordinates.
- But techniques to *prove* such a claim have not yet been developed.