Fundamental groups and Diophantine geometry

Minhyong Kim

6 March, 2007

Exeter pure mathematics seminar

Diophantine equation:

$$f(\underline{x}) = 0$$

for

$$f(x_1, x_2, \ldots, x_n) \in \mathbb{Z}[x_1, x_2, \ldots, x_n]$$

can be considered in any number of different environments such as

$$\mathbb{Z},\ \mathbb{Z}[1/62],\ \mathbb{Q},\ \mathbb{Z}[i],\ \mathbb{Q}[i], \ldots,\ \mathbb{Q}[i,\pi], \ldots,\ \mathbb{R},\ \mathbb{C},\ \mathbb{Q}_p,\ \mathbb{C}_p, \ldots$$

The designation of the equation as Diophantine is not a reference to any particular property of the equation itself, but rather calls attention to our primary focus on contexts closer to the beginning of the list.

Notation X for the equation thought of as a geometric object in various ways. $X(R)$ for set of solutions in ring R.

Famous results:

(1)

$$x^n + y^n = z^n$$

has only the obvious solutions in $\mathbb{Z}$ as long as $n \geq 3$.

(2)

$$f(x, y) = 0$$

for a generic f of degree at least 4 has only finitely many solutions in $\mathbb{Q}(i, \pi, e)$.

Diophantine geometry has it origins in the use of elementary coordinate geometry for describing solution sets, or at least for generating solutions.

Quadratic equation in two variables:

$$x^2 + y^2 = 1.$$

Real solution set is a circle. Leads to idea of considering the intersections with all lines that pass through the specific point $(-1, 0)$. Equations

$$y = m(x + 1)$$

for various m

Substitution leads to the constraint

$$x^2 + (m(x + 1))^2 = 1$$

or

$$(1 + m^2)x^2 + 2m^2x + m^2 - 1 = 0.$$

One solution $x = -1$ is already rational.

Slope m is rational $\Rightarrow$ other solution is also rational.

Varying m, we can generate thereby *all* the other rational solutions to the equation, e.g.,

$$(-99/101, 20/101)$$

corresponding to $m = 10$.

[$\leftrightarrow$ Pythogorean triple $99^2 + 20^2 = 101^2$]

An example of degree 3:

$$x^3 + y^3 = 1729.$$

$(9, 10)$ is a solution (Ramanujan).

Lines through it?

Unfortunately, the previous argument for the rationality of intersection points fails.

Can obtain *one* other solution, using the tangent line to the real curve at the point $(9, 10)$.

Equation of the tangent line,

$$81(x - 9) + 100(y - 10) = 0$$

or

$$y = (-81/100)x + 1729/100,$$

and substitute to obtain the equation

$$x^3 + ((-81/100)x + 1729/100)^3 = 1729.$$

We have arranged for $x = 9$ to be a double root, and hence, the remaining root is forced to be rational.

Even by hand, you can (tediously) work out the resulting rational point to be

$$(-42465969/468559, 24580/271).$$

Can continue to obtain infinitely many rational solutions. Key point is a natural *group structure* on the set of points, determined by the condition (in suitable coordinates) that

$$P + Q + R = 0$$

exactly when they lie on a line.

Geometric techniques of the same general flavor can be made considerably more sophisticated.

Compact smooth curve X, defined by equation

$$F(z_0, z_1, z_2) = 0$$

in projective space.

Can try to generalize the previous discussion in a somewhat formal way by defining

$$Pic_X = \mathbb{Z}[X]/(\text{geometric equivalence relation } R)$$

$R: \quad \Sigma_i P_i = \Sigma_i Q_i \Leftrightarrow \{P_i\}$ and $\{Q_i\}$ are both co-linear sets in some projective embedding of X.

This relation is quite complicated in general. For degree three equations, reduces to relation between three points on the curve. Accounted for by the topology of a torus:

$$X(\mathbb{C}) = \mathbb{C}/\Lambda$$

where $\Lambda \subset \mathbb{C}$ is a lattice.

For higher degree equations, sum of two points will no longer be on the curve. No group law:

$X(\mathbb{C})$: Riemann surface of higher genus.

Henceforward, assume X is a curve of genus ≥ 2.

But there is another geometric structure underlying this construction.

$$Pic_X = J_X \times \mathbb{Z}$$

where

$$J_X = \mathbb{Z}[X]_0/R$$

$$\mathbb{Z}[X]_0 = \{\Sigma n_P[P] \mid \Sigma n_P = 0\}$$

and

$$J_X(\mathbb{C}) = H^0(X(\mathbb{C}), \Omega_{X(\mathbb{C})})^*/H_1(X(\mathbb{C}), \mathbb{Z})$$

Many other descriptions and constructions.

Weil gave a purely *algebraic* construction of J_X as a projective variety:

$$J_X \sim Sym^g(X)$$

In particular,

X defined over $\mathbb{Q} \Rightarrow J_X$ defined over $\mathbb{Q}$. Finally, if $b \in X(\mathbb{C})$, then get a map

$$i_b : X \hookrightarrow J_X$$

defined over $\mathbb{Q}$ that sends any other point x to $[x] - [b]$. *Albanese map.*

In particular,

$$X(\mathbb{Q}) \hookrightarrow J_X(\mathbb{Q})$$

and one might attempt to study the structure of $X(\mathbb{Q})$ *using* $J_X(\mathbb{Q})$. Weil's main motivation for algebraic construction.

In fact, $J_X(\mathbb{Q})$ is a finitely-generated abelian group. Frequently infinite, again because of group structure. But points of J_X are usually not points of X. Cannot be used to generate points on X.

Mordell's conjecture: X has at most finitely many rational points.

Proved in 80's by Faltings.

From our perspective, an arithmetic manifestation of incompatibility of group law on J_X with complicated topology of X. Weil had attempted in his thesis to implement this idea directly to prove Mordell's conjecture (without success).

Remark: Problem is the intrinsically abelian nature of the category of motives reflecting the properties of *homology*. So, even in the best of possible worlds (i.e., where all conjectures are theorems), the category of motives misses out on fundamental objects of arithmetic, i.e., sets

$$X(\mathbb{Q}).$$

Might attempt to replace J_X by a more complicate object.

Weil 1938: ‘Generalization of abelian functions’.

‘A paper about geometry disguised as a paper about analysis whose motivation is arithmetic’ (Serre).

Stresses importance of developing ‘non-abelian mathematics with a key role for non-abelian fundamental groups.

Clearly motivated by the Mordell conjecture.

In this paper, established first theorems relating fundamental groups and vector bundles on curves.

In addition to previous descriptions, recall that J_X over $\mathbb{C}$ can also be thought of as

-the space of unitary characters (S^1-valued) of $\pi_1(X(\mathbb{C}))$;

-space of line bundles of degree zero on $X(\mathbb{C})$.

Weil's generalized this to vector bundles, leading eventually to work Narasimhan-Seshadri, Donaldson, Simpson, etc., referred to as *non-abelian Hodge theory*.

For example, the theorem of N-S says that there is an equivalence between moduli of irreducible unitary representations of π_1 and that of stable vector bundles of degree zero on $X(\mathbb{C})$.

From view of arithmetic, the point of such theorems is to 'algebraize' data of π_1, thereby leading to an arithmetic object defined over $\mathbb{Q}$, with potential for arithmetic applications. That is, theory of vector bundles is a kind of theory of fundamental groups over $\mathbb{Q}$.

However loss of Albanese map:

$$x \mapsto \mathcal{O}_X((x) - (b))$$

No way to associate a vector bundle to a point.

However, one needn't algebraize directly. *Arithmetic topology* gives another way to 'define fundamental groups over $\mathbb{Q}$:' Grothendieck's theory.

Yet another view of Jacobian and AJ map: motivic interpretation.

$$J_X(\mathbb{C}) = \mathrm{Ext}^1_{MHS}(\mathbb{Z}, H_1(X(\mathbb{C}), \mathbb{Z}))$$

and

$$i_b(x)$$

$$= [0 \to H_1(X(\mathbb{C}), \mathbb{Z}) \to H_1(X(\mathbb{C}), \{b, x\}; \mathbb{Z}) \to \mathbb{Z} \to 0]$$

Several advantages of this view:

-Replaces the need for algebraically constructed Jacobian with that of some *homology* preserving arithmetic information.

-Suggests the possibility of direct use of π_1 as well as a 'non-abelian' AJ map.

Basic idea:

$$i_b^{na}(x) := [\pi_1(X; b, x)]$$

where the image runs over a classifying space (similar to classifying space of mixed Hodge structures). In fact, previous abelian Albanese map can be viewed as

$$x \mapsto [\pi_1(X; b, x)/\pi_1(X; b)^{(3)}]$$

(quotient modulo a level of the descending central series).

$\pi_1(X; b, x)$ is a *torsor* or a principal bundle for $\pi_1(X, b)$. Have an action by composition

$$\pi_1(X; b, x) \times \pi_1(X; b) \rightarrow \pi_1(X; b, x)$$

and the choice of an path $p \in \pi_1(X; b, x)$ determines a bijection

$$\pi_1(X; b) \simeq \pi_1(X; b, x)$$

$$l \mapsto p \circ l$$

Recall the universal covering space

$$(\tilde{X}(\mathbb{C}), \tilde{b}) \rightarrow (X(\mathbb{C}), b)$$

which is a principal $\pi_1(X; b)$-bundle over $X(\mathbb{C})$. This specializes to the $\pi_1(X; b, x)$:

$$\tilde{X}_b \simeq \pi_1(X; b)$$

and

$$\tilde{X}_x \simeq \pi_1(X; b, x)$$

via lifting of paths.

Of course, $\pi_1(X; b, x)$, in contrast to $\tilde{X}$, is a principal bundle over a point, and hence, trivial.

Grothendieck's theories allow us to enrich points in various ways.

I. Schemes (function-theoretic enrichment).

Given (commutative unital) ring R, view it as ring of functions on a space

$$\mathrm{Spec}(R)$$

Set-theoretically, the prime ideals of R.

Maps

$$\mathrm{Spec}(B) \to \mathrm{Spec}(A)$$

correspond to ring-homomorphisms

$$A \to B$$

Provides an *intrinsic geometry* to Diophantine problems.

Associate to the polynomial

$$f(\underline{x}) \in \mathbb{Z}[\underline{x}]$$

the ring

$$A := \mathbb{Z}[\underline{x}]/(f(\underline{x})).$$

This leads to a natural correspondence between solutions

$$(r_1, \ldots, r_n)$$

of $f(\underline{x}) = 0$ in a ring R, and ring homomorphisms

$$A \rightarrow R$$

That is, an *arbitrary* n-tuple

$$\underline{r} = (r_1, \ldots, r_n)$$

determines a ring homomorphism $\mathbb{Z}[\underline{x}] \rightarrow R$ that sends x_i to r_i, which factors through the quotient ring A exactly when $\underline{r}$ is a zero of $f(\underline{x})$.

Thus, the set of solutions $X(R)$ in R come into bijection with the set of maps

$$\mathrm{Spec}(R) \to X := \mathrm{Spec}(A).$$

Also an obvious ‘structure map’

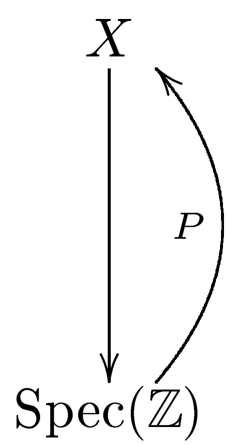
$$\begin{array}{c} X \\ \downarrow \\ \mathrm{Spec}(\mathbb{Z}) \end{array}$$

corresponding to the inclusion

$$\mathbb{Z} \rightarrow A = \mathbb{Z}[\underline{x}]/(f(\underline{x})),$$

using which we think of X as a fibration over $\mathrm{Spec}(\mathbb{Z})$.

Then the solutions in $\mathbb{Z}$, the elements of $X(\mathbb{Z})$, are precisely the *sections*



of the fibration.

The inclusion

$$\mathrm{Spec}(\mathbb{Q}) \hookrightarrow \mathrm{Spec}(\mathbb{Z})$$

can be used to pull-back the fibration:

$$\begin{array}{ccc} X_{\mathbb{Q}} & \hookrightarrow & X \\ \downarrow & & \downarrow \\ \mathrm{Spec}(\mathbb{Q}) & \hookrightarrow & \mathrm{Spec}(\mathbb{Z}) \end{array}$$

and rational solutions will correspond to sections

$$\begin{array}{c} X_{\mathbb{Q}} \\ \downarrow \uparrow P \\ \mathrm{Spec}(\mathbb{Q}) \end{array}$$

Note that Spec($\mathbb{Q}$) is just a point, but scheme theory endows it with the sophisticated ring $\mathbb{Q}$ of functions. Space is trivial, but ring of functions is not. Thus, fields like $\mathbb{Q}$ provide an enrichment of a point.

Second enrichment: The *étale topology*.

Spaces like Spec($\mathbb{Q}$) or Spec($\mathbb{Z}$) are endowed now with very non-trivial topologies that go beyond scheme theory.

In general, a Grothendieck topology on an object T allows open sets to be certain maps with range T from domains that are not necessarily subsets of T.

For example, can consider the *covering space topology* on a topological space. Leads to nothing essentially new.

In algebraic geometry, there are many maps that behave formally like local homeomorphisms without actually being so: *étale maps* between schemes.

A nice and fairly general class of examples:

$$\mathrm{Spec}(B) \to \mathrm{Spec}(A)$$

corresponding to maps of rings $A \to B$

$$B = A[x]/(f(x))$$

for a monic polynomial $f(x)$.

Étale if the fibers of Spec(B) over Spec(A),

$$\mathrm{Spec}(k[x]/(\bar{f}(x)))$$

$$k = A/m$$

have the same number of elements, indicating an absence of ramification. That is, the discriminant of f should be a unit in A.

The obvious map

$$\mathrm{Spec}(\mathbb{C}[t][x]/(x^2 - t)) \to \mathrm{Spec}(\mathbb{C}[t]),$$

is not étale, the discriminant of $x^2 - t$ being the non-unit $4t$, while

$$\mathrm{Spec}(\mathbb{C}[t, t^{-1}][x]/(x^2 - t)) \to \mathrm{Spec}(\mathbb{C}[t, t^{-1}]),$$

is étale.

The connected étale coverings of $\mathrm{Spec}(\mathbb{Q})$ are maps

$$\mathrm{Spec}(F) \rightarrow \mathrm{Spec}(\mathbb{Q}),$$

where F is a finite field extension of $\mathbb{Q}$.

For $\mathrm{Spec}(\mathbb{Z})$, one can construct an open covering using the two maps

$$\mathrm{Spec}(\mathbb{Z}[i][1/2]) \rightarrow \mathrm{Spec}(\mathbb{Z})$$

and

$$\mathrm{Spec}(\mathbb{Z}[(1+\sqrt{-7})/2][1/7]) \rightarrow \mathrm{Spec}(\mathbb{Z}).$$

Sheaf (co)homology for these theories rather well-known. Can construct Jacobians and AJ maps in arithmetic topology:

$$J_X^{et} = \mathrm{Ext}^1_{\mathbb{Q}^{et}}(\hat{\mathbb{Z}}, H_1(\bar{X}^{et}, \hat{\mathbb{Z}}))$$

and

$$i_b(x) = [0 \rightarrow H_1(\bar{X}^{et}, \hat{\mathbb{Z}}) \rightarrow H_1(\bar{X}^{et}, \{b, x\}; \hat{\mathbb{Z}}) \rightarrow \hat{\mathbb{Z}} \rightarrow 0]$$

[Here, we use a correspondence:

Sheaves on Spec($\mathbb{Q}$) $\leftrightarrow$ Sets with Gal($\bar{\mathbb{Q}}/\mathbb{Q}$)-action.]

Grothendieck's exotic topologies also lead to interesting *homotopy* groups.

One construction: $\tilde{X}(\mathbb{C})\to X(\mathbb{C})$ can be *approximated* by finite covers

$$X_i(\mathbb{C})\to X(\mathbb{C})$$

Example:

$$\exp(2\pi i(\cdot)) : \mathbb{C}\to\mathbb{C}^*$$

is approximated by

$$(\cdot)^n : \mathbb{C}^*\to\mathbb{C}^*$$

In general, the system

$$\tilde{X} = \{X_i\}$$

can be defined over $\mathbb{Q}$, and viewed as an arithmetic universal covering space.

The fiber $\tilde{X}_b$ now consists of systems of algebraic ($\bar{\mathbb{Q}}$) points, that are acted on by $G = \mathrm{Gal}(\bar{\mathbb{Q}}, \mathbb{Q})$. Still has the structure of a *pro-finite* group, the étale fundamental group

$$\pi_1^{et}(\bar{X}, b).$$

For any other point $x \in X(\mathbb{Q})$,

$$\pi_1^{et}(\bar{X}; b, x) := \tilde{X}_x$$

also consists of algebraic points, and is a pro-finite torsor for $\pi_1^{et}(\bar{X}, b)$.

The Galois action reflects the fact that there are sheaves

$$b^*(\tilde{X})$$

and

$$x^*(\tilde{X})$$

on Spec($\mathbb{Q}$) underlying these sets.

[Recall:

$$b, x : \mathrm{Spec}(\mathbb{Q}) \to X$$

]

Thus we get an arithmetic Albanese map

$$X(\mathbb{Q}) \rightarrow H^1(G, \pi_1^{et}(\bar{X}, b))$$

$$x \mapsto [\pi_1^{et}(\bar{X}; b, x)]$$

where the target is a classifying space for principal $\pi_1^{et}(\bar{X}; b)$-bundles on the étale topology of Spec($\mathbb{Q}$).

This map is a bit difficult to study, because algebraic geometry has been entirely removed.

Can reinsert this at the level of ‘coefficients’ for the non-abelian cohomology by replacing the fundamental groups by suitable algebraic completions.

Consider completed group ring

$$\mathbb{Q}_p[[\pi_1^{et}(\bar{X}, b)]]$$

which has the structure of a Hopf algebra with co-multiplication induced

$$\Delta(\gamma) = \gamma \otimes \gamma$$

for $\gamma \in \pi_1^{et}(\bar{X}, b)$. The group like elements for this co-multiplication form a *pro-algebraic pro-unipotent group*

$$\pi_1^{u,\mathbb{Q}_p}(\bar{X}, b)$$

Can replace the previous classifying space by

$$H^1_f(G, \pi_1^{u,\mathbb{Q}_p}(\bar{X}, b))$$

which then has the structure of a pro-algebraic variety. There are finite-dimensional quotients

$$H^1_f(G, [\pi_1^{u,\mathbb{Q}_p}(\bar{X}, b)]_n)$$

obtained by considering quotients modulo the descending central series.

End up with a diagram:

$$\begin{array}{ccc} X(\mathbb{Z}_S) & \longrightarrow & X(\mathbb{Z}_p) \\ \downarrow & & \downarrow \\ H^1_f(\Gamma, [\pi_1^{u,\mathbb{Q}_p}(\bar{X}, b)]_n) & \longrightarrow & H^1_f(\Gamma_p, [\pi_1^{u,\mathbb{Q}_p}(\bar{X}, b)]_n) \end{array}$$

involving a local version of the classifying space on the lower right hand corner, with $G_p = \mathrm{Gal}(\bar{\mathbb{Q}}_p/\mathbb{Q}_p)$.

Vertical maps are all of the form

$$x \mapsto [\pi_1^{u,\mathbb{Q}_p}(\bar{X}; b, x)]$$

obtained from the previous one by pushing out torsors.

Theorem 0.1 *Let X be a curve and suppose*

$$dim H^1_f(\Gamma, [\pi_1^{u,\mathbb{Q}_p}(\bar{X}, b)]_n) < dim H^1_f(\Gamma_p, [\pi_1^{u,\mathbb{Q}_p}(\bar{X}, b)]_n)$$

for some n. Then $X(\mathbb{Z}_S)$ is finite.

Theorem is intimately related to non-abelian nature of the fundamental groups and the corresponding non-linearity of the classifying spaces.

Can use this to prove finiteness of integral points for hyperbolic curves of genus zero and certain kinds of hyperbolic curves of genus one, e.g.,

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

The dimension hypothesis for general curves follows from 'general structure theory of mixed motives', i.e.,

Standard motivic conjectures $\Rightarrow$ Faltings' theorem.

Related to *non-abelian extensions* of the conjectures of Birch and Swinnerton-Dyer. Proofs are an extension of:

Non-vanishing of L-function $\Rightarrow$ finiteness of rational points

that occurs for elliptic curves.