Fundamental groups, principal bundles, and Diophantine geometry

Minhyong Kim

14 March, 2007

Kings colloquium

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* 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 as follows: Fix one point $0 \in X(\mathbb{Q})$ as the origin. For any P, Q, there exists a rational function f with zeros exactly at P and Q and one pole at 0. $P + Q$ is defined to be the other pole.

Can add or simply double old solutions to get new ones.

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 formal way by defining

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

$R: \quad \Sigma_i P_i = \Sigma_i Q_i \Leftrightarrow$ there exists a rational function whose zeros are exactly the $\{P_i\}$ and whose poles are the $\{Q_i\}$.

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.

Reason for emphasizing non-abelian π_1: Classical construction of J_X is homological.

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 geometrically.

Arithmetic topology

gives another way to define fundamental groups over $\mathbb{Q}$:

In fact, Grothendieck's theory of the *étale fundamental group* leads to a theory of *non-abelian Albanese maps*.

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

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

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

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

$$l \mapsto p \circ l$$

$\pi_1(X;b,x)$ is a principal bundle over a point, and hence, trivial.

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

Example:

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

Function-theoretic enrichment of a point.

Topological 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: proper finite-to-one maps with surjective tangent map.

On $\mathbb{C}^*$

$$z \mapsto z^2$$

is étale.

scheme-theoretically,

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

corresponding to

$$\mathbb{C}[t,t^{-1}] \leftarrow \mathbb{C}[t,t^{-1}]$$

$$t^2 \leftarrow t$$

Same for

$$\mathrm{Spec}(\mathbb{Q}[t,t^{-1}])\to\mathrm{Spec}(\mathbb{Q}[t,t^{-1}])$$

Main point, in fact, is that we can refer to such covering maps for spaces with very sparse collections of points.

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

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

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

Pro-finite sheaves on $\mathrm{Spec}(\mathbb{Q})$ canonically identified with pro-finite sets carrying continuous action of

$$G = \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}))$$

For 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, with numerous applications: Weil conjectures, Faltings' theorem, Wiles theorem, etc.

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

X variety defined over $\mathbb{Q}$ and $b \in X(\mathbb{Q})$.

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.

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

can be *approximated* by finite covers

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

Example:

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

is approximated by

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

Note that the approximating system is *defined over* $\mathbb{Q}$.

Even in general, there is a system

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

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

(Warning: In this assertion, we are using the rationality of the base-point.)

The fiber $\tilde{X}_b^{et}$ 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 $x \in X(\mathbb{Q})$,

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

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

The group and principal bundle carry compatible Galois actions reflecting the fact that there are sheaves

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

and

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

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

[Recall:

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

]

Thus we get an arithmetic Albanese map

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

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

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

For curves of genus ≥ 1, this map is injective!

In this form, a bit difficult to study, because geometry has been entirely removed. Only profinite topology remains.

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

Geometry of the space vs. geometry of coefficients

is an important theme in arithmetic geometry.

Γ finitely-generated discrete group. $\mathbb{C}[\Gamma]$ group algebra.

$$\Delta : \mathbb{C}[\Gamma] \rightarrow \mathbb{C}[\Gamma] \otimes \mathbb{C}[\Gamma]$$

induced by

$$\gamma \mapsto \gamma \otimes \gamma$$

for $\gamma \in \Gamma$. Then, in fact,

$$\Gamma = \{f \in \mathbb{C}[\Gamma] : \Delta(f) = f \otimes f\}$$

i.e., Γ is the set of ‘group-like elements’ in the Hopf algebra $\mathbb{C}[\Gamma]$.

But can consider the formally completed group algebra

$$\mathbb{C}[[\Gamma]] := \varprojlim \mathbb{C}[\Gamma]/I^n$$

where $I \subset \mathbb{C}[\Gamma]$ is the augmentation ideal.

Then we get more group-like elements, e.g.,

$$\exp(\lambda \log(\gamma))$$

for $\gamma \in \Gamma$ and $\lambda \in \mathbb{C}$.

The unipotent completion Γ^u of Γ is the set of group-like elements in $\mathbb{C}[[\Gamma]]$.

Thereby arrive at a more structured object:

Γ^u is a pro-algebraic group.

$\Gamma^u_n := \Gamma^u/(\Gamma^u)^{(n)}$ is an algebraic group for each n.

Can do this to the fundamental group:

$$\pi_1(X(\mathbb{C}), b) \to \pi_1^u(X(\mathbb{C}), b)$$

getting the group generated by the holonomy of all unipotent connections on $X(\mathbb{C})$.

Also have ‘unipotent principal bundle of paths’

$$\pi_1^u(X(\mathbb{C}); b, x)$$

Can carry out same construction for the étale fundamental group and the completed group ring

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

to arrive at the $\mathbb{Q}_p$-pro-unipotent étale fundamental group:

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

The previous classifying space gets replaced by

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

which then has the structure of a pro-algebraic variety (being a moduli space of principal bundles for a pro-algebraic group).

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.

They fit into a tower:

$$\begin{tikzcd}
 & & \vdots \\
 & \vdots & H^1_f(G, [\pi_1^{u,\mathbb{Q}_p}(\bar{X}, b)]_4) \arrow[d] \\
 & & H^1_f(G, [\pi_1^{u,\mathbb{Q}_p}(\bar{X}, b)]_3) \arrow[d] \\
 & & H^1_f(G, [\pi_1^{u,\mathbb{Q}_p}(\bar{X}, b)]_2) \arrow[d] \\
X(\mathbb{Q}) \arrow[rr] \arrow[urr] \arrow[uurr] \arrow[uuurr] & & H^1_f(G, [\pi_1^{u,\mathbb{Q}_p}(\bar{X}, b)]_1)
\end{tikzcd}$$

refining the map at the bottom (which has a classical interpretation in Kummer theory).

End up with a diagram:

$$\begin{tikzcd}
X(\mathbb{Q}) \arrow[r] \arrow[d] & X(\mathbb{Q}_p) \arrow[d] \\
H^1_f(\Gamma, [\pi_1^{u,\mathbb{Q}_p}(\bar{X}, b)]_n) \arrow[r] & H^1_f(\Gamma_p, [\pi_1^{u,\mathbb{Q}_p}(\bar{X}, b)]_n)
\end{tikzcd}$$

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 principal bundles.

The local classifying space

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

has the structure of a p-adic symmetric space, and the map

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

is obtained by solving p-adic differential equations (for parallel transport).

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

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

Idea of proof: (1)

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

is finite-to-one: a purely analytic fact;

(2)

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

is a dense analytic curve: Fact about p-adic transcendental functions;

(3)

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

lies inside a proper closed subvariety.

(2) and (3) imply that

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

is finite.

Together with (1), get finiteness of $X(\mathbb{Q})$.

Can use the theorem 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.

In fact,

Finiteness of zeros of p-adic L-function $\Rightarrow$ finiteness of integral points

in the case of CM elliptic curves.