Fundamental groups and Diophantine geometry

Minhyong Kim

7 November, 2008

Lille 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 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 E of points, determined by the condition (in suitable coordinates) that

$$P + Q + R = 0$$

exactly when they lie on a line.

In fact, fixing any point $O \in E$ determines a bijection

$$E \simeq \mathbb{Z}[E]_0/R$$

$$P \mapsto [P] - [O],$$

where

-$\mathbb{Z}[E]$ is the free abelian group generated by the points of E;

-$\mathbb{Z}[E]_0 \subset \mathbb{Z}[E]$ is the subgroup of degree zero elements;

- and R is the subgroup of relations

$$[P] + [Q] + [R] - 3[O].$$

Some aspects of this construction can be generalized.

Compact smooth curve X, defined by equation

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

in projective space.

Define the Jacobian of X as

$$J_X = \mathbb{Z}[X]_0/(\text{geometric equivalence relation } R)$$

$R: \quad \Sigma_i P_i = \Sigma_i Q_i \Leftrightarrow \{P_i\}$ 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. For example,

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

Many other descriptions and constructions.

Difference is that $X \neq J_X$ for X of higher genus. Nevertheless, many applications of J_X in complex and arithmetic geometry.

For applications to Diophantine geometry, 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 $\mathbb{Q}$.

If $b \in X(\mathbb{Q})$, 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 between the group law on J_X and complicated topology of X. Weil had attempted in his thesis to implement this idea directly to prove Mordell's conjecture (without success).

Difficult to extricate $X(\mathbb{Q})$ from the surrounding $J_X(\mathbb{Q})$.

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 $X(\mathbb{C})$.

So Weil considered the natural non-abelianization

Line bundles $\rightarrow$ vector bundles.

But considered the fundamental group to be somehow relevant!

Weil's work led eventually to 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 start from a consideration of π_1 and then 'algebraize' it in some fashion. Thereby end up with 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.

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* for $\pi_1(X,b)$.

There is 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

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

$$l\mapsto p\circ l$$

Of course, $\pi_1(X;b,x)$ is a torsor 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

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

correspond to ring-homomorphisms

$$A \rightarrow B$$

Provides an *intrinsic geometry* to Diophantine problems.

Associate to the polynomial

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

the ring

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

This leads to a natural correspondence between solutions

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

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

$$A \rightarrow K$$

That is, an *arbitrary* n-tuple

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

determines a ring homomorphism $\mathbb{Q}[\underline{x}] \rightarrow X$ 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 $X(K)$ in K comes into bijection with the set of maps

$$\mathrm{Spec}(K) \rightarrow X := \mathrm{Spec}(A).$$

Also an obvious ‘structure map’

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

corresponding to the inclusion

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

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

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

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

of the fibration.

Note that $\mathrm{Spec}(\mathbb{Q})$ 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($\mathbb{Q}$) are endowed now with very non-trivial topologies that go beyond scheme theory. Open covering is a map

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

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

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 $\mathrm{Spec}(B)$ over $\mathrm{Spec}(A)$,

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

$$k = A/m$$

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

Cohomology of sheaves in this topology has many well-known applications.

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

M: manifold. $b \in M$.

The fundamental group $\pi_1(M,b)$ of M with base-point b can be defined in several different ways avoiding direct reference to topological loops.

Fiber functor approach:

A loop l acts naturally on the fiber over b of any covering space $N \to M$ of M using the monodromy of a lifting $\tilde{l}$ of l to N:

$$l_N : N_b \simeq N_b$$

Compatible with composition of loops and with maps between covering spaces. That is, $(l_1 l_2)_N = (l_1)_N \circ (l_2)_N$, and if $f : N \to P$ is a map of covering spaces, then

$$f \circ l_N = l_P \circ f$$

as maps from N_b to P_b.

Minor surprise: loops give the only way to specify such a compatible collection of automorphisms.

Concise formulation via the functor

$$F_b : \mathrm{Cov}(M) \to \mathrm{Sets}$$

that associates to each covering N its fiber N_b over b. Then

$$\pi_1(M, b) \simeq \mathrm{Aut}(F_b)$$

with the Aut understood in the sense of invertible natural transformations of a functor. Similarly,

$$\pi_1(M; b, x) \simeq \mathrm{Isom}(F_b, F_x).$$

Given a variety V, we can use this approach to *define* the pro-finite étale fundamental group simply by changing the category of coverings.

$\mathrm{Cov}^{et}(V)$: the finite étale covers of V.

For any point $b \in V$, have F_b^{et} that takes $W \to V$ to the fiber W_b. Then

$$\pi_1^{et}(V, b) := \mathrm{Aut}(F_b^{et})$$

Similarly,

$$\pi_1^{et}(V; b, x) := \mathrm{Isom}(F_b^{et}, F_x^{et}).$$

Constructions of this nature have now become commonplace in mathematics, the best known being associated to the notion of a linear Tannakian category, whereby the automorphisms of suitable functors defined on agreeable categories give rise to group schemes.

Two examples:

Fix a non-archimedean completion $\mathbb{Q}_p$ of $\mathbb{Q}$.

$$\mathrm{Loc}^{et}(V, \mathbb{Q}_p)$$

category of locally constant sheaves of finite-dimensional $\mathbb{Q}_p$-vector spaces on V considered in the étale topology. There is still a fiber functor

$$F_b^{alg} : \mathrm{Loc}^{et}(V, \mathbb{Q}_p) \rightarrow \mathrm{Vect}_{\mathbb{Q}_p},$$

now taking values in $\mathbb{Q}_p$-vector spaces, that associates to each sheaf its stalk at b.

Now define

$$\pi_1^{alg,\mathbb{Q}_p}(V, b) := \mathrm{Aut}^{\otimes}(F_b^{alg}),$$

the $\mathbb{Q}_p$*-pro-algebraic completion* of $\pi_1^{et}(V, b)$.

Replace all local systems by unipotent ones, i.e., those that admit a filtration

$$L = L^0 \supset L^1 \supset \cdots L^n \supset L^{n+1} = 0$$

such that

$$L^i / L^{i+1} \simeq \mathbb{Q}_P^{r_i}$$

Get a category $\mathrm{Un}^{et}(V, \mathbb{Q}_p)$ of the right sort.

$$F_b^u : \mathrm{Un}^{et}(V, \mathbb{Q}_p) \rightarrow \mathrm{Vect}_{\mathbb{Q}_p}.$$

The $\mathbb{Q}_p$*-pro-unipotent completion* of the étale fundamental group is then defined as

$$\pi_1^{u, \mathbb{Q}_p}(V, b) := \mathrm{Aut}^{\otimes}(F_b^u)$$

In both settings, there are still torsors of paths

$$\pi_1^{alg,\mathbb{Q}_p}(V;b,x) := \mathrm{Isom}(F_b^{alg}, F_x^{alg})$$

and

$$\pi_1^{u,\mathbb{Q}_p}(V;b,x) := \mathrm{Isom}(F_b^{u}, F_x^{u})$$

In the profinite case, 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 $\pi_1^{et}(\bar{X}; b)$-torsors 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. Most tractable case at present is the unipotent completion.

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, the *Selmer variety* of (X, b).

There are quotients

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

obtained by considering quotients modulo the descending central series, which are $\mathbb{Q}_p$-algebraic varieties.

In fact, a tower of moduli spaces and maps:

$$
\begin{array}{ccc}
 & & \vdots \\
 & \vdots & H^1_f(G, [\pi_1^{u,\mathbb{Q}_p}(\bar{X}, b)]_4) \\
 & \nearrow & \downarrow \\
 & & H^1_f(G, [\pi_1^{u,\mathbb{Q}_p}(\bar{X}, b)]_3) \\
 & \nearrow & \downarrow \\
 & & H^1_f(G, [\pi_1^{u,\mathbb{Q}_p}(\bar{X}, b)]_2) \\
 & \nearrow & \downarrow \\
X(\mathbb{Q}) & \longrightarrow & H^1_f(G, [\pi_1^{u,\mathbb{Q}_p}(\bar{X}, b)]_1)
\end{array}
$$

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

End up with a diagram:

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

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*

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

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: There is a non-zero algebraic function α

$$\begin{array}{ccc} X(\mathbb{Q}) & \hookrightarrow & X(\mathbb{Q}_p) \\ \downarrow & & \downarrow \\ H^1_f(G, [\pi_1^{u,\mathbb{Q}_p}(\bar{X}, b)_n]) & \xrightarrow{\mathrm{loc}_p} & H^1_f(G_p, [\pi_1^{u,\mathbb{Q}_p}(\bar{X}, b)_n]_n) \\ & & \downarrow {\scriptstyle \exists \alpha \neq 0} \\ & & \mathbb{Q}_p \end{array}$$

vanishing on $Im[H^1_f(G, U_n)]$. Hence, $\alpha \circ \kappa^{na}_{p,n}$ vanishes on $X(\mathbb{Q})$. But this function is a non-vanishing convergent power series on each residue disk. $\square$

Can use this to prove finiteness of rational points on a compact curve of genus ≥ 2 provided its Jacobian decompose into a product of abelian varieties with complex multiplication. (Joint work with John Coates.)

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 $\Rightarrow$ control of Selmer groups $\Rightarrow$ finiteness of rational points on elliptic curves.

In the non-abelian case:

Non-vanishing of L-function $\Rightarrow$ control of Selmer varieties $\Rightarrow$ finiteness of rational points on hyperbolic curves.