Homotopy theory and Diophantine geometry

Minhyong Kim

British Mathematical Colloquium, April, 2011

Some examples of Diophantine equations in two variables

Some examples of Diophantine equations in two variables

$$x^2 + y^2 = 1 \tag{0}$$

Some examples of Diophantine equations in two variables

$$x^2 + y^2 = 1 \tag{0}$$

$$y^2 = x^3 - 2 \tag{1}$$

Some examples of Diophantine equations in two variables

$$x^2 + y^2 = 1 \tag{0}$$

$$y^2 = x^3 - 2 \tag{1}$$

For $a, b, c \in \mathbb{Z}$, positive and $n \geq 4$:

$$ax^n + by^n = c \tag{2}$$

Some rational solutions

Some rational solutions

(0)

$$\left(\frac{-238740}{238741}\right)^2 + \left(\frac{691}{238741}\right)^2 = 1$$

Some rational solutions

(0)

$$(\frac{-238740}{238741})^2 + (\frac{691}{238741})^2 = 1$$

(1)

$$(\frac{113259286337279}{449455096000})^2 = (\frac{2340922881}{58675600})^3 - 2$$

Some rational solutions

(0)

$$(\frac{-238740}{238741})^2 + (\frac{691}{238741})^2 = 1$$

(1)

$$(\frac{1132592863372791}{449455096000})^2 = (\frac{2340922881}{58675600})^3 - 2$$

There are *geometric methods* for producing and organizing such solutions:

the method of sweeping lines

and

the chord-tangent method

Rational points on real algebraic curves

We think of solutions as *points* on real algebraic curves.

Rational points on real algebraic curves

We think of solutions as *points* on real algebraic curves.
That is, visualize the points

$$P = (\frac{-238740}{238741}, \frac{691}{238741})$$

and

$$Q = (\frac{2340922881}{58675600}, \frac{113259286337279}{449455096000})$$

on the real algebraic curves $x^2 + y^2 = 1$ and $y^2 = x^3 - 2$.

Rational points on real algebraic curves

The real picture allows us to organize points on (0) and (1) using elementary geometry of the ambient space.

Rational points on real algebraic curves

The real picture allows us to organize points on (0) and (1) using elementary geometry of the ambient space.

However, real picture is not very useful for equation (2).

Rational points on real algebraic curves

The real picture allows us to organize points on (0) and (1) using elementary geometry of the ambient space.

However, real picture is not very useful for equation (2).

The difficulty is due in part to the *topology of the complex solution set*.

Topology of complex curves

That is, for a polynomial f, if we are interested in

$$X_f(\mathbb{Z}) := \{(a, b) \in \mathbb{Z}^2 : f(a, b) = 0\}$$

Topology of complex curves

That is, for a polynomial f, if we are interested in

$$X_f(\mathbb{Z}) := \{(a, b) \in \mathbb{Z}^2 : f(a, b) = 0\}$$

or

$$X_f(\mathbb{Q}) := \{(s, t) \in \mathbb{Q}^2 : f(s, t) = 0\},$$

Topology of complex curves

That is, for a polynomial f, if we are interested in

$$X_f(\mathbb{Z}) := \{(a,b) \in \mathbb{Z}^2 : f(a,b) = 0\}$$

or

$$X_f(\mathbb{Q}) := \{(s,t) \in \mathbb{Q}^2 : f(s,t) = 0\},$$

we are obliged to examine the topology of

$$X_f(\mathbb{C}) := \{(z,w) \in \mathbb{C}^2 : f(z,w) = 0\}$$

and its closure

$$\overline{X_f(\mathbb{C})}$$

in projective space $\mathbb{P}^2(\mathbb{C})$.

Topology of complex curves

In general, when we remove a few singular points from $\overline{X_f(\mathbb{C})}$ (say, points where $\nabla f = 0$), we get an orientable two-manifold.

Topology of complex curves

In general, when we remove a few singular points from $\overline{X_f(\mathbb{C})}$ (say, points where $\nabla f = 0$), we get an orientable two-manifold.

We use this to speak of the *genus* of the equation f.

Topology of complex curves

In general, when we remove a few singular points from $\overline{X_f(\mathbb{C})}$ (say, points where $\nabla f = 0$), we get an orientable two-manifold.

We use this to speak of the *genus* of the equation f.

In the previous examples,
equation (0) has genus 0;
equation (1) has genus 1;
equation (2) has genus 2.

Topology of complex curves and the theorem of Faltings

Theorem (Faltings)

Whenever f has genus ≥ 2, $X_f(\mathbb{Q})$ is finite.

Topology of complex curves and the theorem of Faltings

Theorem (Faltings)

Whenever f has genus ≥ 2, $X_f(\mathbb{Q})$ is finite.

Most equations of degree ≥ 4, e.g.,

$$ax^n + by^n = c \qquad (n \geq 4),$$

have genus ≥ 2.

The effective Mordell problem

Find a method for computing the set

$$X_f(\mathbb{Q})$$

for f of genus ≥ 2.

The effective Mordell problem

Find a method for computing the set

$$X_f(\mathbb{Q})$$

for f of genus ≥ 2.

Many years of experience indicates that the real picture is not very useful for this problem.

Non-abelian fundamental groups

Key fact:

The fundamental group $\pi_1(\overline{X_f(\mathbb{C})}, b)$ is non-abelian when f has genus ≥ 2.

Non-abelian fundamental groups

Key fact:

The fundamental group $\pi_1(\overline{X_f(\mathbb{C})}, b)$ is non-abelian when f has genus ≥ 2.

This non-abelian nature is strongly linked to the difficulty of the rational solution set, but may provide a natural arena for resolving the effective Mordell problem.

Non-abelian fundamental groups

Key fact:

The fundamental group $\pi_1(\overline{X_f(\mathbb{C})}, b)$ is non-abelian when f has genus ≥ 2.

This non-abelian nature is strongly linked to the difficulty of the rational solution set, but may provide a natural arena for resolving the effective Mordell problem.

Naturally linked to a *p-adic embedding* that can be used to analyze the arithmetic structure.

Interlude: *L*-functions and elliptic curves

The zero set of an equation of genus one is called an *elliptic curve*, usually written in the (Weierstrass minimal) form

$$E: \quad y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6.$$

Interlude: L-functions and elliptic curves

The zero set of an equation of genus one is called an *elliptic curve*, usually written in the (Weierstrass minimal) form

$$E: \quad y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6.$$

Still many unresolved problems in this direction, but a *conjectural picture* is relatively complete. In particular, we can always compute $E(\mathbb{Q})$ in practice, given enough time.

Interlude: L-functions and elliptic curves

It is a theorem of Wiles (and Taylor and Breuil, Conrad, Diamond, Taylor) that there is an arithmetic uniformization

$$\pi : \mathbb{H} \longrightarrow E(\mathbb{C}),$$

where $\mathbb{H}$ is the complex upper-half plane:

$$\mathbb{H} = \{z \in \mathbb{C} : Im(z) > 0\}.$$

Interlude: L-functions and elliptic curves

It is a theorem of Wiles (and Taylor and Breuil, Conrad, Diamond, Taylor) that there is an arithmetic uniformization

$$\pi : \mathbb{H} \longrightarrow E(\mathbb{C}),$$

where $\mathbb{H}$ is the complex upper-half plane:

$$\mathbb{H} = \{z \in \mathbb{C} : Im(z) > 0\}.$$

'Arithmetic' here refers to the fact that the fibers of π should contain the orbits of a congruence subgroup

$$\Gamma_0(N) := \{\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z}) : c \equiv 0 \mod N\}$$

of $SL_2(\mathbb{Z})$.

Interlude: *L*-functions and elliptic curves

The *L-function* of E is the entire function

$$L(E,s) := \frac{1}{\Gamma(s)} \int_0^\infty \pi^*(\alpha)(iy)^s \frac{dy}{y},$$

where α is given by the formula:

$$\alpha := \frac{dx}{2y + a_1 x + a_3}.$$

Interlude: The Coates-Wiles theorem

Consider the family

$$E_d : \quad y^2 = x^3 - d$$

$(d \in \mathbb{Z} \setminus \{0\})$.

Interlude: The Coates-Wiles theorem

Consider the family

$$E_d : \quad y^2 = x^3 - d$$

($d \in \mathbb{Z} \setminus \{0\}$).

Theorem (Coates-Wiles)

If $L(E_d, 1) \neq 0$, then $E(\mathbb{Q})$ is finite

For example, for E_2, $L(E_2, 1) = 0$.

Remarks: The Coates-Wiles theorem

Remarks: The Coates-Wiles theorem

- Special case of a theorem on *elliptic curves with complex multiplication*.

Remarks: The Coates-Wiles theorem

- Special case of a theorem on *elliptic curves with complex multiplication*.
- Has been generalized to non-CM elliptic curves over $\mathbb{Q}$ by Kolyvagin, Rubin, and Kato.

Remarks: The Coates-Wiles theorem

- Special case of a theorem on *elliptic curves with complex multiplication*.
- Has been generalized to non-CM elliptic curves over $\mathbb{Q}$ by Kolyvagin, Rubin, and Kato.
- The theorem relies on a study of the *homology* of the elliptic curve.

Remarks: The Coates-Wiles theorem

- Special case of a theorem on *elliptic curves with complex multiplication*.
- Has been generalized to non-CM elliptic curves over $\mathbb{Q}$ by Kolyvagin, Rubin, and Kato.
- The theorem relies on a study of the *homology* of the elliptic curve.
- Would like to generalize the ideas to other varieties, for example, curves of higher genus using *homotopy theory*.

Homotopy theory: Points and principal bundles

Homotopy theory: Points and principal bundles

Given an equation

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

with $f \in \mathbb{Q}[x, y]$, write $X(\mathbb{C})$ for the projective compactification of the complex solutions.

Homotopy theory: Points and principal bundles

Given an equation

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

with $f \in \mathbb{Q}[x, y]$, write $X(\mathbb{C})$ for the projective compactification of the complex solutions.

The *fundamental groupoid* is made up of the path spaces

$$\pi_1(X(\mathbb{C}); a, b)$$

as the two points a and b vary over $X(\mathbb{C})$, together with the composition

$$\pi_1(X(\mathbb{C}); b, c) \times \pi_1(X(\mathbb{C}); a, b) \to \pi_1(X(\mathbb{C}); a, c)$$

obtained by concatenating paths.

Homotopy theory: Points and principal bundles

The portion that originates at a fixed base-point b is comprised of the fundamental group

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

and the homotopy classes of paths

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

for any other point $x \in X(\mathbb{C})$.

Homotopy theory: Points and principal bundles

The portion that originates at a fixed base-point b is comprised of the fundamental group

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

and the homotopy classes of paths

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

for any other point $x \in X(\mathbb{C})$.

We will focus mostly on the category of *principal bundles* for the group $\pi_1(X(\mathbb{C}), b)$ made up by the path spaces $\pi_1(X(\mathbb{C}); b, x)$.

Homotopy theory: Points and principal bundles

This means that there is a group action

$$\pi_1(X(\mathbb{C}); b, x) \times \pi_1(X(\mathbb{C}), b) \longrightarrow \pi_1(X(\mathbb{C}); b, x)$$

that is simply transitive.

Homotopy theory: Points and principal bundles

This means that there is a group action

$$\pi_1(X(\mathbb{C}); b, x) \times \pi_1(X(\mathbb{C}), b) \longrightarrow \pi_1(X(\mathbb{C}); b, x)$$

that is simply transitive.

Alternatively, any choice of a path $p \in \pi_1(X(\mathbb{C}); b, x)$ determines a bijection

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

$$\gamma \mapsto p \circ \gamma.$$

Homotopy theory: Points and principal bundles

This means that there is a group action

$$\pi_1(X(\mathbb{C}); b, x) \times \pi_1(X(\mathbb{C}), b) \longrightarrow \pi_1(X(\mathbb{C}); b, x)$$

that is simply transitive.

Alternatively, any choice of a path $p \in \pi_1(X(\mathbb{C}); b, x)$ determines a bijection

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

$$\gamma \mapsto p \circ \gamma.$$

The proposal of arithmetic homotopy is to encode solutions to the equation, i.e., points on X, into the structures $\pi_1(X(\mathbb{C}); b, x)$.

Arithmetic homotopy and Diophantine geometry

To distinguish rational solutions $X(\mathbb{Q})$ from arbitrary complex ones, one passes to a non-archimedean *linearization*.

Arithmetic homotopy and Diophantine geometry

To distinguish rational solutions $X(\mathbb{Q})$ from arbitrary complex ones, one passes to a non-archimedean *linearization*.

Standard linearization: the group ring

$$\mathbb{Q}_p[\pi_1(X(\mathbb{C}), b)].$$

Obtain thereby, a number of additional structures.

Arithmetic homotopy and Diophantine geometry

The group ring is a Hopf algebra with comultiplication

$$\Delta : \mathbb{Q}_p[\pi_1(X(\mathbb{C}), b)] \rightarrow \mathbb{Q}_p[\pi_1(X(\mathbb{C}), b)] \otimes \mathbb{Q}_p[\pi_1(X(\mathbb{C}), b)]$$

determined by the formula

$$\Delta(g) = g \otimes g$$

for $g \in \pi_1(X(\mathbb{C}), b)$.

Arithmetic homotopy and Diophantine geometry

The group ring is a Hopf algebra with comultiplication

$$\Delta : \mathbb{Q}_p[\pi_1(X(\mathbb{C}), b)] \rightarrow \mathbb{Q}_p[\pi_1(X(\mathbb{C}), b)] \otimes \mathbb{Q}_p[\pi_1(X(\mathbb{C}), b)]$$

determined by the formula

$$\Delta(g) = g \otimes g$$

for $g \in \pi_1(X(\mathbb{C}), b)$.
Inside the group ring there is the augmentation ideal

$$J \subset \mathbb{Q}_p[\pi_1(X(\mathbb{C}), b)]$$

generated by elements of the form $g - 1$.

Arithmetic homotopy and Diophantine geometry

Completion:

$$A = \mathbb{Q}_p[[\pi_1(X(\mathbb{C}), b)]] := \varprojlim_n \mathbb{Q}_p[\pi_1(X(\mathbb{C}), b)]/J^n,$$

whose elements can be thought of as non-commuative formal power series in elements $g - 1$, $g \in \pi_1$.

Arithmetic homotopy and Diophantine geometry

Completion:

$$A = \mathbb{Q}_p[[\pi_1(X(\mathbb{C}), b)]] := \varprojlim_n \mathbb{Q}_p[\pi_1(X(\mathbb{C}), b)]/J^n,$$

whose elements can be thought of as non-commuative formal power series in elements $g - 1$, $g \in \pi_1$.

The previous co-product carries over to an algebra homomorphism

$$\Delta : A \longrightarrow A \hat{\otimes} A := \varprojlim A/J^n \otimes A/J^m,$$

turning A into a *complete Hopf algebra*.
Study of such structures originates in *rational homotopy theory*, with which we are actually concerned from a motivic point of view.

Arithmetic homotopy and Diophantine geometry

One defines the 'group-like elements' in the complete Hopf algebra:

$$U = \{g \in A \mid \Delta(g) = g \otimes g\}.$$

The elements of the discrete fundamental group give rise to elements of U, but there are many more. For example, given $g \in \pi_1$, one can obtain elements of U using $\mathbb{Q}_p$-powers of g:

$$g^{\lambda} := \exp(\lambda \log(g)).$$

Arithmetic homotopy and Diophantine geometry

One defines the 'group-like elements' in the complete Hopf algebra:

$$U = \{g \in A \mid \Delta(g) = g \otimes g\}.$$

The elements of the discrete fundamental group give rise to elements of U, but there are many more. For example, given $g \in \pi_1$, one can obtain elements of U using $\mathbb{Q}_p$-powers of g:

$$g^\lambda := \exp(\lambda \log(g)).$$

U can be thought of as a group generated by such $\mathbb{Q}_p$-powers.

The group U is in fact very large, with the structure of an infinite-dimensional pro-algebraic group over $\mathbb{Q}_p$, the $\mathbb{Q}_p$-*pro-unipotent completion* of $\pi_1(X(\mathbb{C}), b)$:

$$\pi_1(X(\mathbb{C}), b) \longrightarrow U.$$

Arithmetic homotopy and Diophantine geometry

The group U is in fact very large, with the structure of an infinite-dimensional pro-algebraic group over $\mathbb{Q}_p$, the $\mathbb{Q}_p$-*pro-unipotent completion* of $\pi_1(X(\mathbb{C}), b)$:

$$\pi_1(X(\mathbb{C}), b) \longrightarrow U.$$

The principal bundles of paths can be completed as well, to give

$$P(x) := \pi_1(X(\mathbb{C}), b)\backslash[\pi_1(X(\mathbb{C}); b, c) \times U],$$

which are principal bundles for U.

Arithmetic homotopy and Diophantine geometry

Now, when b and x are both rational points both U and $P(x)$ admit a very large group of hidden symmetries, a continuous action of

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

The symmetry arises from a reinterpretation of these constructions in terms of the étale topology of the scheme X.

Now, when b and x are both rational points both U and $P(x)$ admit a very large group of hidden symmetries, a continuous action of

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

The symmetry arises from a reinterpretation of these constructions in terms of the étale topology of the scheme X.

The principal bundles $P(x)$ themselves are non-trivial for the *étale topology* of $\mathrm{Spec}(\mathbb{Q})$.

Arithmetic homotopy and Diophantine geometry

Two important facts:

Arithmetic homotopy and Diophantine geometry

Two important facts:
-If p is chosen large enough and the fundamental group is non-abelian, then the structure $P(x)$ completely determines the point x. That is, if

$$P(x) \simeq P(x')$$

as U-bundle with G-action, then $x = x'$.

Arithmetic homotopy and Diophantine geometry

Two important facts:
-If p is chosen large enough and the fundamental group is non-abelian, then the structure $P(x)$ completely determines the point x. That is, if

$$P(x) \simeq P(x')$$

as U-bundle with G-action, then $x = x'$.

-Can classify such structures, using a pro-algebraic moduli space

$$H^1_f(G, U),$$

of principal bundles described using non-abelian continuous group cohomology: The $\mathbb{Q}_p$-*Selmer scheme* of X.

Arithmetic homotopy and Diophantine geometry

Arithmetic homotopy and Diophantine geometry

Each $P(x)$ determines an element of this space.

$$X(\mathbb{Q}) \longrightarrow H^1_f(G, U);$$

$$x \mapsto [P(x)];$$

defining an embedding of the rational points of X into a *moduli space of principal bundles.*

Thereby, the $\mathbb{Q}$-points $X(\mathbb{Q})$ become embedded in a canonical algebraic family.

Arithmetic homotopy and Diophantine geometry

Localization:

$$\begin{array}{ccc} X(\mathbb{Q}) & \longrightarrow & X(\mathbb{Q}_p) \\ \downarrow & & \downarrow \\ H^1_f(G, U) & \xrightarrow{\mathrm{loc}_p} & H^1_f(G_p, U) \end{array}$$

Here $G_p = \mathrm{Gal}(\bar{\mathbb{Q}}_p/\mathbb{Q}_p) \subset G$.

Arithmetic homotopy and Diophantine geometry

The local moduli space and the classifying map can be computed using non-abelian p-adic Hodge theory.

$$H^1_f(G_p, U) \simeq \mathbb{Q}_p^\infty$$

and the map

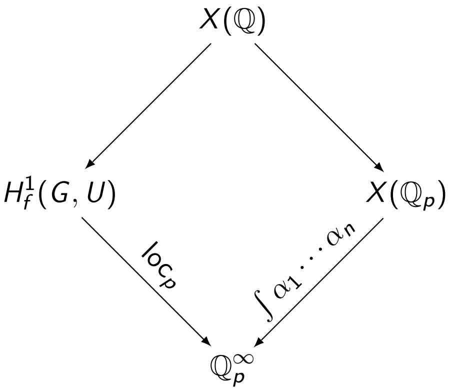
$$X(\mathbb{Q}_p) \longrightarrow H^1_f(G_p, U)$$

has coordinates that are p-adic iterated integrals:

$$z \mapsto (\cdots, \int_b^z \alpha_1\alpha_2\cdots\alpha_n, \cdots).$$

Arithmetic homotopy and Diophantine finiteness

These constructions are captured by the following diagram:



Arithmetic homotopy and Diophantine finiteness

so that

$$Im(H^1_f(G,U)) \subset \mathbb{Q}_p^\infty$$

is an algebraic subspace such that

$$X(\mathbb{Q}) \subset Im(H^1_f(G,U)) \cap X(\mathbb{Q}_p) \subset \mathbb{Q}_p^\infty$$

Arithmetic homotopy and Diophantine finiteness

For the equation

$$ax^n + by^n = c$$

($n \geq 4$), one can show (joint work with John Coates) that

$$Im(H^1_f(G, U)) \cap X(\mathbb{Q}_p) \subset \mathbb{Q}_p^\infty$$

is finite, and deduce from this the finiteness of points.

Arithmetic homotopy and Diophantine finiteness

An important technical ingredient is *multi-variable Iwasawa theory* , whereby one shows the sparseness of zeros for an

algebraic p-adic L-function.

Arithmetic homotopy and Diophantine finiteness

An important technical ingredient is *multi-variable Iwasawa theory* , whereby one shows the sparseness of zeros for an

algebraic p-adic L-function.

This sparseness in turn implies that the closure of

$$Im(H^1_f(G,U)) \subset \mathbb{Q}_p^\infty$$

is a proper algebraic subspace.

Arithmetic homotopy and Diophantine finiteness

An important technical ingredient is *multi-variable Iwasawa theory* , whereby one shows the sparseness of zeros for an

algebraic p-adic L-function.

This sparseness in turn implies that the closure of

$$Im(H^1_f(G, U)) \subset \mathbb{Q}_p^{\infty}$$

is a proper algebraic subspace.
The finiteness of the intersection follows then from the analytic fact that

$$Im(X(\mathbb{Q}_p)) \subset \mathbb{Q}_p^{\infty}$$

is a *space-filling curve*, which therefore must meet a proper subspace in a discrete set of points.

Arithmetic homotopy and Diophantine finiteness

But it is further plausible that

$$Im(H^1_f(G, U)) \cap X(\mathbb{Q}_p) \subset \mathbb{Q}_p^\infty$$

is *computable*, since

$$X(\mathbb{Q}_p) \subset \mathbb{Q}_p^\infty$$

is computable and the map

$$H^1_f(G, U) \longrightarrow \mathbb{Q}_p^\infty$$

is algebraic.

Arithmetic homotopy and Diophantine finiteness

But it is further plausible that

$$Im(H^1_f(G,U)) \cap X(\mathbb{Q}_p) \subset \mathbb{Q}_p^\infty$$

is *computable*, since

$$X(\mathbb{Q}_p) \subset \mathbb{Q}_p^\infty$$

is computable and the map

$$H^1_f(G,U) \longrightarrow \mathbb{Q}_p^\infty$$

is algebraic.

The intersection might be regarded as a 'computable approximation' to $X(\mathbb{Q})$.

The effective Mordell problem

A tool for the effective Mordell problem:

$$? \quad X(\mathbb{Q}) \subset Im(H^1_f(G, U)) \cap X(\mathbb{Q}_p) \subset \mathbb{Q}_p^{\infty} \quad ?$$

The effective Mordell problem

A tool for the effective Mordell problem:

$$? \quad X(\mathbb{Q}) \subset Im(H^1_f(G, U)) \cap X(\mathbb{Q}_p) \subset \mathbb{Q}_p^\infty \quad ?$$

Appears to require further input from Grothendieck's *anabelian geometry*.