Selmer Schemes I

Minhyong Kim

Tucson, March, 2020

Disclaimer

These lecture slides come with a bibliography at the end. However, there has been no attempt at accurate attribution of mathematical results. Rather, the list mostly contains works the lecturer has consulted during preparation, which he hopes will be helpful for users.

I. Background: Arithmetic of Algebraic Curves

Arithmetic of algebraic curves

X: a smooth algebraic curve of genus g defined over $\mathbb{Q}$.

Arithmetic of algebraic curves

X: a smooth algebraic curve of genus g defined over $\mathbb{Q}$.

For example, given by a polynomial equation

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

of degree d with rational coefficients, where

$$g = (d - 1)(d - 2)/2.$$

Arithmetic of algebraic curves

X: a smooth algebraic curve of genus g defined over $\mathbb{Q}$.

For example, given by a polynomial equation

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

of degree d with rational coefficients, where

$$g = (d-1)(d-2)/2.$$

Diophantine geometry studies the set $X(\mathbb{Q})$ of rational solutions from a geometric point of view.

Arithmetic of algebraic curves

X: a smooth algebraic curve of genus g defined over $\mathbb{Q}$.

For example, given by a polynomial equation

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

of degree d with rational coefficients, where

$$g = (d-1)(d-2)/2.$$

Diophantine geometry studies the set $X(\mathbb{Q})$ of rational solutions from a geometric point of view.

Structure is quite different in the three cases:

$g = 0$, spherical geometry (positive curvature);
$g = 1$, flat geometry (zero curvature);
$g \geq 2$, hyperbolic geometry (negative curvature).

Arithmetic of algebraic curves: $g = 0, d \leq 2$

Arithmetic of algebraic curves: $g = 0, d \leq 2$

Even now (after millennia of studying these problems), $g = 0$ is the only case that is completely understood.

Arithmetic of algebraic curves: $g = 0, d \leq 2$

Even now (after millennia of studying these problems), $g = 0$ is the only case that is completely understood.

For $g = 0$, techniques reduce to class field theory and algebraic geometry: **local-to-global methods**, generation of solutions via sweeping lines, etc.

Arithmetic of algebraic curves: $g = 0, d \leq 2$

Even now (after millennia of studying these problems), $g = 0$ is the only case that is completely understood.

For $g = 0$, techniques reduce to class field theory and algebraic geometry: **local-to-global methods**, generation of solutions via sweeping lines, etc.

Idea is to study $\mathbb{Q}$-solutions by considering the geometry of solutions in various completions, the local fields

$$\mathbb{R}, \mathbb{Q}_2, \mathbb{Q}_3, \ldots, \mathbb{Q}_{691}, \ \ldots,$$

Local-to-global methods

$$\begin{tikzcd}
\mathbb{Q}_2 & \mathbb{R} & \mathbb{Q}_3 \\
\mathbb{Q}_{37} & \mathbb{Q} \arrow[ul, hook] \arrow[u, hook] \arrow[ur, hook] \arrow[l, hook] \arrow[r, hook] \arrow[dl, hook] \arrow[d, hook] \arrow[dr, hook] & \cdots \\
\mathbb{Q}_{691} & \mathbb{Q}_{65537} & \mathbb{Q}_{2^{82,589,933}-1}
\end{tikzcd}$$

Arithmetic of algebraic curves: $g = 0$

Local-to-global methods sometimes allow us to 'globalise'. For example,

$$37x^2 + 59y^2 - 67 = 0$$

has a $\mathbb{Q}$-solution if and only if it has a solution in each of $\mathbb{R}, \mathbb{Q}_2, \mathbb{Q}_{37}, \mathbb{Q}_{59}, \mathbb{Q}_{67}$, a criterion that can be effectively implemented. This is called the *Hasse principle*.

Arithmetic of algebraic curves: $g = 0$

Local-to-global methods sometimes allow us to 'globalise'. For example,

$$37x^2 + 59y^2 - 67 = 0$$

has a $\mathbb{Q}$-solution if and only if it has a solution in each of $\mathbb{R}, \mathbb{Q}_2, \mathbb{Q}_{37}, \mathbb{Q}_{59}, \mathbb{Q}_{67}$, a criterion that can be effectively implemented. This is called the *Hasse principle*.

If the existence of a solution is guaranteed, it can be found by an exhaustive search. From one solution, there is a method for parametrising all others: for example, from $(0, -1)$, generate solutions

$$\left(\frac{t^2-1}{t^2+1}, \frac{2t}{t^2+1}\right)$$

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

Arithmetic of algebraic curves: $g = 0$

In other words, there is a successful study of the inclusion

$$X(\mathbb{Q}) \subset X(\mathbb{A}_{\mathbb{Q}}) = \prod' X(\mathbb{Q}_p)$$

coming from **reciprocity laws** (class field theory).

Arithmetic of algebraic curves: $g = 1$ ($d = 3$)

Arithmetic of algebraic curves: $g = 1$ ($d = 3$)

$X(\mathbb{Q}) = \phi$, non-empty finite, infinite, all are possible.

Arithmetic of algebraic curves: $g = 1$ ($d = 3$)

$X(\mathbb{Q}) = \phi$, non-empty finite, infinite, all are possible.

Hasse principle fails:

$$3x^3 + 4y^3 + 5 = 0$$

has points in $\mathbb{Q}_v$ for all v, but no rational points.

Arithmetic of algebraic curves: $g = 1$ ($d = 3$)

$X(\mathbb{Q}) = \phi$, non-empty finite, infinite, all are possible.

Hasse principle fails:

$$3x^3 + 4y^3 + 5 = 0$$

has points in $\mathbb{Q}_v$ for all v, but no rational points.

Even when $X(\mathbb{Q}) \neq \phi$, difficult to describe the full set.

Arithmetic of algebraic curves: $g = 1$ ($d = 3$)

$X(\mathbb{Q}) = \phi$, non-empty finite, infinite, all are possible.

Hasse principle fails:

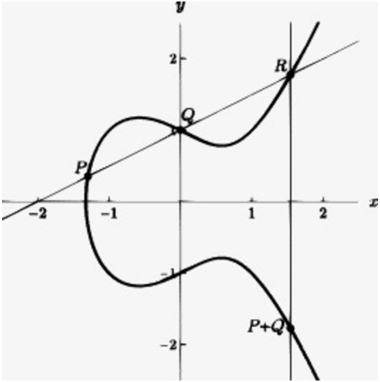
$$3x^3 + 4y^3 + 5 = 0$$

has points in $\mathbb{Q}_v$ for all v, but no rational points.

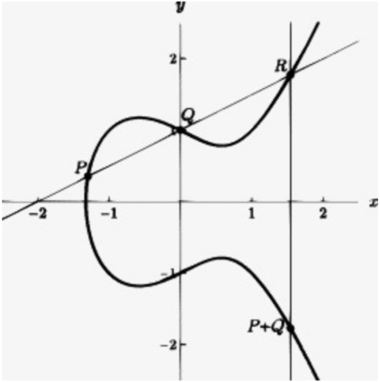
Even when $X(\mathbb{Q}) \neq \phi$, difficult to describe the full set.

But fixing an origin $O \in X(\mathbb{Q})$ gives $X(\mathbb{Q})$ the structure of a finitely-generated abelian group via the chord-and-tangent method.

Arithmetic of algebraic curves: $g = 1$ ($d = 3$)



Arithmetic of algebraic curves: $g = 1$ ($d = 3$)



(Mordell)

$$X(\mathbb{Q}) \simeq X(\mathbb{Q})_{tor} \times \mathbb{Z}^r.$$

Here, r is called the rank of the curve and $X(\mathbb{Q})_{tor}$ is a finite effectively computable abelian group.

Arithmetic of algebraic curves: $g = 1$

To compute $X(\mathbb{Q})_{tor}$, write

$$X := \{y^2 = x^3 + ax + b\} \cup \{\infty\}$$

$(a, b \in \mathbb{Z})$.

Then $(x, y) \in X(\mathbb{Q})_{tor} \Rightarrow x, y$ are integral and

$$y^2 | (4a^3 + 27b^2).$$

Arithmetic of algebraic curves: $g = 1$

However, the algorithmic computation of the rank and a full set of generators for $X(\mathbb{Q})$ is very difficult, and is the subject of the conjecture of Birch and Swinnerton-Dyer.

Arithmetic of algebraic curves: $g = 1$

However, the algorithmic computation of the rank and a full set of generators for $X(\mathbb{Q})$ is very difficult, and is the subject of the conjecture of Birch and Swinnerton-Dyer.

In practice, it is often possible to compute these. For example, for

$$y^2 = x^3 - 2,$$

Sage will give you $r = 1$ and the point $(3, 5)$ as generator.

Arithmetic of algebraic curves: $g = 1$

However, the algorithmic computation of the rank and a full set of generators for $X(\mathbb{Q})$ is very difficult, and is the subject of the conjecture of Birch and Swinnerton-Dyer.

In practice, it is often possible to compute these. For example, for

$$y^2 = x^3 - 2,$$

Sage will give you $r = 1$ and the point $(3, 5)$ as generator.

The algorithm *uses* the BSD conjecture.

Arithmetic of algebraic curves: $g = 1$

Note that

$$2(3,5) = (129/100, -383/1000)$$

$$3(3,5) = (164323/29241, -66234835/5000211)$$

$$4(3,5) = (2340922881/58675600, 113259286337279/449455096000)$$

Arithmetic of algebraic curves: $g = 1$

Note that

$$2(3,5) = (129/100, -383/1000)$$

$$3(3,5) = (164323/29241, -66234835/5000211)$$

$$4(3,5) = (2340922881/58675600, 1132592863337279/449455096000)$$

Figure: Denominators of $N(3,5)$

Arithmetic of algebraic curves: $g \geq 2$ ($d \geq 4$)

Arithmetic of algebraic curves: $g \geq 2$ ($d \geq 4$)

$X(\mathbb{Q})$ is always finite (Mordell conjecture as proved by Faltings)

Arithmetic of algebraic curves: $g \geq 2$ ($d \geq 4$)

$X(\mathbb{Q})$ is always finite (Mordell conjecture as proved by Faltings)

However, *very* difficult to compute: consider

$$x^n + y^n = 1$$

for $n \geq 4$.

Arithmetic of algebraic curves: $g \geq 2$ ($d \geq 4$)

$X(\mathbb{Q})$ is always finite (Mordell conjecture as proved by Faltings)

However, *very* difficult to compute: consider

$$x^n + y^n = 1$$

for $n \geq 4$.

Sometime easy, such as

$$x^4 + y^4 = -1.$$

Arithmetic of algebraic curves: $g \geq 2$ ($d \geq 4$)

$X(\mathbb{Q})$ is always finite (Mordell conjecture as proved by Faltings)

However, *very* difficult to compute: consider

$$x^n + y^n = 1$$

for $n \geq 4$.

Sometime easy, such as

$$x^4 + y^4 = -1.$$

However, when there isn't an obvious reason for non-existence, e.g., there already is one solution, then it's hard to know when you have the full list.

Arithmetic of algebraic curves: $g \geq 2$ ($d \geq 4$)

$X(\mathbb{Q})$ is always finite (Mordell conjecture as proved by Faltings)

However, *very* difficult to compute: consider

$$x^n + y^n = 1$$

for $n \geq 4$.

Sometime easy, such as

$$x^4 + y^4 = -1.$$

However, when there isn't an obvious reason for non-existence, e.g., there already is one solution, then it's hard to know when you have the full list. For example,

$$y^3 = x^6 + 23x^5 + 37x^4 + 691x^3 - 631204x^2 + 5169373941$$

obviously has the solution $(1, 1729)$, but are there any others?

Arithmetic of algebraic curves: $g \geq 2$ ($d \geq 4$)

Effective Mordell problem:

$$\boxed{\textbf{Find a terminating algorithm: } X \mapsto X(\mathbb{Q})}$$

Arithmetic of algebraic curves: $g \geq 2$ ($d \geq 4$)

Effective Mordell problem:

$$\boxed{\textbf{Find a terminating algorithm: } X \mapsto X(\mathbb{Q})}$$

The **Effective Mordell conjecture** (Szpiro, Vojta, ABC, ...) makes this precise using (archimedean) height inequalities. That is, it proposes that you can give a priori bounds on the size of numerators and denominators of solutions.

Arithmetic of algebraic curves: $g \geq 2$ ($d \geq 4$)

Effective Mordell problem:

$$\boxed{\textbf{Find a terminating algorithm: } X \mapsto X(\mathbb{Q})}$$

The **Effective Mordell conjecture** (Szpiro, Vojta, ABC, ...) makes this precise using (archimedean) height inequalities. That is, it proposes that you can give a priori bounds on the size of numerators and denominators of solutions.

Will describe today an approach to this problem using the (non-archimedean) arithmetic geometry of principal bundles.

II. Arithmetic Principal Bundles

Arithmetic principal bundles: (G_K, R, P)

Arithmetic principal bundles: (G_K, R, P)

K: field of characteristic zero.
$G_K = \mathrm{Gal}(\bar{K}/K)$: absolute Galois group of K. Topological group with open subgroups given by $\mathrm{Gal}(\bar{K}/L)$ for finite field extensions L/K in $\bar{K}$.

Arithmetic principal bundles: (G_K, R, P)

K: field of characteristic zero.
$G_K = \mathrm{Gal}(\bar{K}/K)$: absolute Galois group of K. Topological group with open subgroups given by $\mathrm{Gal}(\bar{K}/L)$ for finite field extensions L/K in $\bar{K}$.

A *group over K* is a topological group R with a continuous action of G_K by group automorphisms:

$$G_K \times R \longrightarrow R.$$

Arithmetic principal bundles: (G_K, R, P)

K: field of characteristic zero.
$G_K = \mathrm{Gal}(\bar{K}/K)$: absolute Galois group of K. Topological group with open subgroups given by $\mathrm{Gal}(\bar{K}/L)$ for finite field extensions L/K in $\bar{K}$.

A *group over* K is a topological group R with a continuous action of G_K by group automorphisms:

$$G_K \times R \longrightarrow R.$$

In an abstract framework, one can view R as a family of groups

over the space $\mathrm{Spec}(K)$.

Arithmetic principal bundles: (G_K, R, P)

K: field of characteristic zero.
$G_K = \mathrm{Gal}(\bar{K}/K)$: absolute Galois group of K. Topological group with open subgroups given by $\mathrm{Gal}(\bar{K}/L)$ for finite field extensions L/K in $\bar{K}$.

A *group over K* is a topological group R with a continuous action of G_K by group automorphisms:

$$G_K \times R \longrightarrow R.$$

In an abstract framework, one can view R as a family of groups

over the space $\mathrm{Spec}(K)$.

Example:

$$R = A(\bar{K}),$$

where A is an algebraic group defined over K, e.g., GL_n or an abelian variety. Here, R has the discrete topology.

Arithmetic principal bundles

Example:

$$R = \mathbb{Z}_p(1) := \varprojlim \mu_{p^n},$$

where $\mu_{p^n} \subset \bar{K}$ is the group of p^n-th roots of 1.

Arithmetic principal bundles

Example:

$$R = \mathbb{Z}_p(1) := \varprojlim \mu_{p^n},$$

where $\mu_{p^n} \subset \bar{K}$ is the group of p^n-th roots of 1.

Thus,

$$\mathbb{Z}_p(1) = \{(\zeta_n)_n\},$$

where

$$\zeta_n^{p^n} = 1; \quad \zeta_{nm}^{p^m} = \zeta_n.$$

As a group,

$$\mathbb{Z}_p(1) \simeq \mathbb{Z}_p = \varprojlim_n \mathbb{Z}/p^n,$$

but there is a continuous action of G_K.

Arithmetic principal bundles: (G_K, R, P)

A principal R-bundle over K is a topological space P with compatible continuous actions of G_K (left) and R (right, simply transitive):

$$P \times R \longrightarrow P;$$

$$G_K \times P \longrightarrow P;$$

$$g(zr) = g(z)g(r)$$

for $g \in G_K$, $z \in P$, $r \in R$.

Arithmetic principal bundles: (G_K, R, P)

A principal R-bundle over K is a topological space P with compatible continuous actions of G_K (left) and R (right, simply transitive):

$$P \times R \longrightarrow P;$$

$$G_K \times P \longrightarrow P;$$

$$g(zr) = g(z)g(r)$$

for $g \in G_K$, $z \in P$, $r \in R$.

Note that P is *trivial*, i.e., $\cong R$, exactly when there is a fixed point $z \in P^{G_K}$:

$$R \cong z \times R \cong P.$$

Arithmetic principal bundles

Example:

Given any $x \in K^*$, get principal $\mathbb{Z}_p(1)$-bundle

$$P(x) := \{(y_n)_n \mid y_n^{p^n} = x,\ y_{nm}^{p^m} = y_n.\}$$

over K.

Arithmetic principal bundles

Example:

Given any $x \in K^*$, get principal $\mathbb{Z}_p(1)$-bundle

$$P(x) := \{(y_n)_n \mid y_n^{p^n} = x,\ y_{nm}^{p^m} = y_n.\}$$

over K.

$P(x)$ is trivial iff x admits a p^n-th root in K for all n.

Arithmetic principal bundles

Example:

Given any $x \in K^*$, get principal $\mathbb{Z}_p(1)$-bundle

$$P(x) := \{(y_n)_n \mid y_n^{p^n} = x,\ y_{nm}^{p^m} = y_n.\}$$

over K.

$P(x)$ is trivial iff x admits a p^n-th root in K for all n.

For example, when $K = \mathbb{C}$, $P(x)$ is always trivial.

Arithmetic principal bundles

Example:

Given any $x \in K^*$, get principal $\mathbb{Z}_p(1)$-bundle

$$P(x) := \{(y_n)_n \mid y_n^{p^n} = x, \ y_{nm}^{p^m} = y_n.\}$$

over K.

$P(x)$ is trivial iff x admits a p^n-th root in K for all n.

For example, when $K = \mathbb{C}$, $P(x)$ is always trivial.

When $K = \mathbb{Q}$, $P(x)$ is trivial iff $x = 1$ or p is odd and $x = -1$.

Arithmetic principal bundles

Example:

Given any $x \in K^*$, get principal $\mathbb{Z}_p(1)$-bundle

$$P(x) := \{(y_n)_n \mid y_n^{p^n} = x, \; y_{nm}^{p^m} = y_n.\}$$

over K.

$P(x)$ is trivial iff x admits a p^n-th root in K for all n.

For example, when $K = \mathbb{C}$, $P(x)$ is always trivial.

When $K = \mathbb{Q}$, $P(x)$ is trivial iff $x = 1$ or p is odd and $x = -1$.

For $K = \mathbb{R}$, and p odd, $P(x)$ is trivial for all x.

Arithmetic principal bundles

Example:

Given any $x \in K^*$, get principal $\mathbb{Z}_p(1)$-bundle

$$P(x) := \{(y_n)_n \mid y_n^{p^n} = x,\ y_{nm}^{p^m} = y_n.\}$$

over K.

$P(x)$ is trivial iff x admits a p^n-th root in K for all n.

For example, when $K = \mathbb{C}$, $P(x)$ is always trivial.

When $K = \mathbb{Q}$, $P(x)$ is trivial iff $x = 1$ or p is odd and $x = -1$.

For $K = \mathbb{R}$, and p odd, $P(x)$ is trivial for all x.

For $K = \mathbb{R}$ and $p = 2$, $P(x)$ is trivial iff $x > 0$.

Arithmetic principal bundles: moduli spaces

Arithmetic principal bundles: moduli spaces

Given a principal R-bundle P over K, choose $z \in P$. This determines a continuous function $c_P : G_K \longrightarrow R$ via

$$g(z) = zc_P(g).$$

It satisfies the 'cocycle' condition

$$c_P(g_1g_2) = c_P(g_1)g_1(c_P(g_2)),$$

defining the set $Z^1(G, R)$.

Arithmetic principal bundles: moduli spaces

Given a principal R-bundle P over K, choose $z \in P$. This determines a continuous function $c_P : G_K \longrightarrow R$ via

$$g(z) = zc_P(g).$$

It satisfies the 'cocycle' condition

$$c_P(g_1 g_2) = c_P(g_1) g_1(c_P(g_2)),$$

defining the set $Z^1(G, R)$.

We get a well-defined class in non-abelian cohomology

$$[c_P] \in R\backslash Z^1(G_K, R) =: H^1(G_K, R) = H^1(K, R),$$

where the R-action is defined by

$$c^r(g) = rc(g)g(r^{-1}).$$

Arithmetic principal bundles: moduli spaces

This induces a bijection

$$\{\text{Isomorphism classes of principal } R\text{-bundles over K}\} \cong H^1(G_K, R).$$

Arithmetic principal bundles: moduli spaces

This induces a bijection

$$\{\text{Isomorphism classes of principal } R\text{-bundles over K}\} \cong H^1(G_K, R).$$

Our main concern is the geometry of non-abelian cohomology spaces in various forms.

Arithmetic principal bundles: moduli spaces

This induces a bijection

$$\{\text{Isomorphism classes of principal } R\text{-bundles over K}\} \cong H^1(G_K, R).$$

Our main concern is the geometry of non-abelian cohomology spaces in various forms.

For these lectures, R will mostly be a unipotent fundamental group of an algebraic curve with a very complicated K-structure.

Two more classes of important examples:

–R is the holonomy group of a specific local system on a curve. (Lawrence and Venkatesh)

–R is a reductive group with a trivial K-structure:

$$H^1(G_K, R) = R\backslash \mathrm{Hom}(G_K, R).$$

These are analytic moduli spaces of Galois representations.

Arithmetic principal bundles: moduli spaces

When $K = \mathbb{Q}$, there are completions $\mathbb{Q}_v$ and injections

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

Arithmetic principal bundles: moduli spaces

When $K = \mathbb{Q}$, there are completions $\mathbb{Q}_v$ and injections

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

giving rise to the localisation map

$$loc : H^1(\mathbb{Q}, R) \longrightarrow \prod_v H^1(\mathbb{Q}_v, R).$$

and an associated local-to-global problem.

Arithmetic principal bundles: moduli spaces

When $K = \mathbb{Q}$, there are completions $\mathbb{Q}_v$ and injections

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

giving rise to the localisation map

$$loc : H^1(\mathbb{Q}, R) \longrightarrow \prod_v H^1(\mathbb{Q}_v, R).$$

and an associated local-to-global problem.

In fact, a wide range of problems in number theory rely on the study of its image. The general principle is that the local-to-global problem is easier to study for principal bundles than for points.

III. Diophantine principal bundles: elliptic curves

Diophantine principal bundles: elliptic curves

Diophantine principal bundles: elliptic curves

E: elliptic curve over $\mathbb{Q}$.

Diophantine principal bundles: elliptic curves

E: elliptic curve over $\mathbb{Q}$.

We let $G = \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ act on the exact sequence

$$0 \longrightarrow E[p](\bar{\mathbb{Q}}) \longrightarrow E(\bar{\mathbb{Q}}) \xrightarrow{p} E(\bar{\mathbb{Q}}) \longrightarrow 0$$

Diophantine principal bundles: elliptic curves

E: elliptic curve over $\mathbb{Q}$.

We let $G = \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ act on the exact sequence

$$0 \longrightarrow E[p](\bar{\mathbb{Q}}) \longrightarrow E(\bar{\mathbb{Q}}) \xrightarrow{p} E(\bar{\mathbb{Q}}) \longrightarrow 0$$

to generate the long exact sequence

$$0 \longrightarrow E(\mathbb{Q})[p] \longrightarrow E(\mathbb{Q}) \xrightarrow{p} E(\mathbb{Q})$$

$$\longrightarrow H^1(\mathbb{Q}, E[p]) \longrightarrow H^1(\mathbb{Q}, E) \xrightarrow{p} H^1(\mathbb{Q}, E),$$

from which we get the inclusion (Kummer map)

$$0 \longrightarrow E(\mathbb{Q})/pE(\mathbb{Q}) \hookrightarrow H^1(\mathbb{Q}, E[p])$$

Diophantine principal bundles: elliptic curves

The central problem in the theory of elliptic curves is the identification of the image

$$Im(E(\mathbb{Q})/pE(\mathbb{Q})) \subset H^1(\mathbb{Q}, E[p]).$$

We remark that computing a set of generators for $E(\mathbb{Q})/pE(\mathbb{Q})$ leads easily to a set of generators for $E(\mathbb{Q})$ itself.

Diophantine principal bundles: elliptic curves

The central problem in the theory of elliptic curves is the identification of the image

$$Im(E(\mathbb{Q})/pE(\mathbb{Q})) \subset H^1(\mathbb{Q}, E[p]).$$

We remark that computing a set of generators for $E(\mathbb{Q})/pE(\mathbb{Q})$ leads easily to a set of generators for $E(\mathbb{Q})$ itself.

An essential restriction comes from the p-Selmer group

$$Sel(\mathbb{Q}, E[p]) \subset H^1(\mathbb{Q}, E[p])$$

defined to be the classes in $H^1(\mathbb{Q}, E[p])$ that locally come from points.

Diophantine principal bundles: elliptic curves

The central problem in the theory of elliptic curves is the identification of the image

$$Im(E(\mathbb{Q})/pE(\mathbb{Q})) \subset H^1(\mathbb{Q}, E[p]).$$

We remark that computing a set of generators for $E(\mathbb{Q})/pE(\mathbb{Q})$ leads easily to a set of generators for $E(\mathbb{Q})$ itself.

An essential restriction comes from the p-Selmer group

$$Sel(\mathbb{Q}, E[p]) \subset H^1(\mathbb{Q}, E[p])$$

defined to be the classes in $H^1(\mathbb{Q}, E[p])$ that locally come from points.
This is useful because the local version of this problem can be solved.

Diophantine principal bundles: elliptic curves

$$\begin{tikzcd}
0 \arrow[r] & E(\mathbb{Q})/pE(\mathbb{Q}) \arrow[r, hook] \arrow[d, "loc_v"'] & H^1(\mathbb{Q}, E[p]) \arrow[d, "loc_v"'] \\
0 \arrow[r] & E(\mathbb{Q}_v)/pE(\mathbb{Q}_v) \arrow[r, hook] & H^1(\mathbb{Q}_v, E[p])
\end{tikzcd}$$

Diophantine principal bundles: elliptic curves

$$\begin{tikzcd}
0 \arrow[r] & E(\mathbb{Q})/pE(\mathbb{Q}) \arrow[r, hook] \arrow[d, "loc_v"'] & H^1(\mathbb{Q}, E[p]) \arrow[d, "loc_v"'] \\
0 \arrow[r] & E(\mathbb{Q}_v)/pE(\mathbb{Q}_v) \arrow[r, hook] & H^1(\mathbb{Q}_v, E[p])
\end{tikzcd}$$

Then

$$Sel(\mathbb{Q}, E[p]) := \cap_v \mathrm{loc}_v^{-1}(Im(E(\mathbb{Q}_v)/pE(\mathbb{Q}_v))).$$

Diophantine principal bundles: elliptic curves

The key point is that **the p-Selmer group is a finite-dimensional $\mathbb{F}_p$-vector space that is effectively computable** and this already gives us a bound on the Mordell-Weil group of E:

$$E(\mathbb{Q})/pE(\mathbb{Q}) \subset Sel(\mathbb{Q}, E[p]).$$

Diophantine principal bundles: elliptic curves

The key point is that **the p-Selmer group is a finite-dimensional $\mathbb{F}_p$-vector space that is effectively computable** and this already gives us a bound on the Mordell-Weil group of E:

$$E(\mathbb{Q})/pE(\mathbb{Q}) \subset Sel(\mathbb{Q}, E[p]).$$

This is then refined by way of the diagram

$$\begin{tikzcd}
0 \arrow[r] & E(\mathbb{Q})/p^nE(\mathbb{Q}) \arrow[r] \arrow[d] & Sel(\mathbb{Q}, E[p^n]) \arrow[d] \\
0 \arrow[r] & E(\mathbb{Q})/pE(\mathbb{Q}) \arrow[r] & Sel(\mathbb{Q}, E[p])
\end{tikzcd}$$

for increasing values of n.

Diophantine principal bundles: elliptic curves

Conjecture: (BSD, Tate-Shafarevich)

$$Im(E(\mathbb{Q})/pE(\mathbb{Q})) = \cap_{n=1}^{\infty} Im[Sel(\mathbb{Q}, E[p^n]] \subset Sel(\mathbb{Q}, E[p]).$$

Diophantine principal bundles: elliptic curves

Conjecture: (BSD, Tate-Shafarevich)

$$Im(E(\mathbb{Q})/pE(\mathbb{Q})) = \cap_{n=1}^{\infty} Im[Sel(\mathbb{Q}, E[p^n]] \subset Sel(\mathbb{Q}, E[p]).$$

Of course this implies that

$$Im(E(\mathbb{Q})/pE(\mathbb{Q})) = Im[Sel(\mathbb{Q}, E[p^N]] \subset Sel(\mathbb{Q}, E[p])$$

at some finite level p^N.

Diophantine principal bundles: elliptic curves

Conjecture: (BSD, Tate-Shafarevich)

$$Im(E(\mathbb{Q})/pE(\mathbb{Q})) = \cap_{n=1}^{\infty} Im[Sel(\mathbb{Q}, E[p^n]] \subset Sel(\mathbb{Q}, E[p]).$$

Of course this implies that

$$Im(E(\mathbb{Q})/pE(\mathbb{Q})) = Im[Sel(\mathbb{Q}, E[p^N]] \subset Sel(\mathbb{Q}, E[p])$$

at some finite level p^N. There is a conditional algorithm for verifying this:

$$\cdots \subset E(\mathbb{Q})_{\leq n}/pE(\mathbb{Q}) \subset E(\mathbb{Q})_{\leq n+1}/pE(\mathbb{Q}) \subset \cdots \subset E(\mathbb{Q})/pE(\mathbb{Q})$$

$$\cdots \subset Im[Sel(\mathbb{Q}, E[p^{n+1}]] \subset Im[Sel(\mathbb{Q}, E[p^n]] \subset \cdots \subset Sel(\mathbb{Q}, E[p])$$

A main goal of BSD is to remove the conditional aspect.

IV. Diophantine principal bundles II: The non-abelian case

Diophantine principal bundles II: The non-abelian case

To generalise, focus on the sequence of maps

$$\cdots \longrightarrow E[p^3] \xrightarrow{p} E[p^2] \xrightarrow{p} E[p]$$

of which we take the inverse limit to get the p-adic Tate module of E:

$$T_pE := \varprojlim E[p^n].$$

This is a free $\mathbb{Z}_p$-module of rank 2. (Each $E[p^n] \simeq (\mathbb{Z}/p^n)^2$ as groups.)

Diophantine principal bundles II: The non-abelian case

To generalise, focus on the sequence of maps

$$\cdots \longrightarrow E[p^3] \xrightarrow{p} E[p^2] \xrightarrow{p} E[p]$$

of which we take the inverse limit to get the p-adic Tate module of E:

$$T_pE := \varprojlim E[p^n].$$

This is a free $\mathbb{Z}_p$-module of rank 2. (Each $E[p^n] \simeq (\mathbb{Z}/p^n)^2$ as groups.)

The previous finite boundary maps can be packaged into

$$j : E(\mathbb{Q}) \longrightarrow \varprojlim H^1(\mathbb{Q}, E[p^n]) = H^1(\mathbb{Q}, T_pE).$$

Diophantine principal bundles II: The non-abelian case

The key point is that

$$T_pE \simeq \pi_1^p(\bar{E}, O),$$

where $\pi_1^p(\bar{X}, b)$ refers to the pro-p completion of the fundamental group $\pi_1(X(\mathbb{C}), b)$ of a variety X.

The map j can be thought of as

$$x \mapsto \pi^p(\bar{E}; O, x).$$

Diophantine principal bundles II: The non-abelian case

Fundamental fact of arithmetic homotopy:

If X is a variety defined over $\mathbb{Q}$ and $b, x \in X(\mathbb{Q})$, then

$$\pi_1^p(\bar{X}, b), \quad \pi_1^p(\bar{X}; b, x)$$

admit compatible actions of $G = \mathbf{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$.

Diophantine principal bundles II: The non-abelian case

Fundamental fact of arithmetic homotopy:

If X is a variety defined over $\mathbb{Q}$ and $b, x \in X(\mathbb{Q})$, then

$$\pi_1^p(\bar{X}, b), \quad \pi_1^p(\bar{X}; b, x)$$

admit compatible actions of $G = \mathbf{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$.

The triples

$$(G_{\mathbb{Q}}, \pi_1^p(\bar{X}, b), \pi_1^p(\bar{X}; b, x))$$

are important concrete examples of (G_K, R, P) from the general definitions.

Diophantine principal bundles II: The non-abelian case

Diophantine principal bundles II: The non-abelian case

This formulation then extends to general X, whereby we get a map

$$j : X(\mathbb{Q}) \longrightarrow H^1(\mathbb{Q}, \pi_1^p(\bar{X}, b))$$

given by

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

Diophantine principal bundles II: The non-abelian case

This formulation then extends to general X, whereby we get a map

$$j : X(\mathbb{Q}) \longrightarrow H^1(\mathbb{Q}, \pi_1^p(\bar{X}, b))$$

given by

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

For each prime v, have local versions

$$j_v : X(\mathbb{Q}_v) \longrightarrow H^1(\mathbb{Q}_v, \pi_1^p(\bar{X}, b))$$

given by

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

which turn out to be far more computable than the global map.

Diophantine principal bundles II: The non-abelian case

Localization diagram:

$$\begin{tikzcd}
X(\mathbb{Q}) \arrow[r] \arrow[d, "j"'] & \prod_v X(\mathbb{Q}_v) \arrow[d, "\prod_v j_v"] \\
H^1(\mathbb{Q}, \pi_1^p(\bar{X}, b)) \arrow[r, "loc"] & \prod_v H^1(\mathbb{Q}_v, \pi_1^p(\bar{X}, b))
\end{tikzcd}$$

Diophantine principal bundles II: The non-abelian case

Localization diagram:

$$\begin{tikzcd} X(\mathbb{Q}) \arrow[r] \arrow[d, "j"'] & \prod_v X(\mathbb{Q}_v) \arrow[d, "\prod_v j_v"'] \\ H^1(\mathbb{Q}, \pi_1^p(\bar{X}, b)) \arrow[r, "loc"] & \prod_v H^1(\mathbb{Q}_v, \pi_1^p(\bar{X}, b)) \end{tikzcd}$$

As in the elliptic curve case, our interest is in the interaction between the images of *loc* and $\prod_v j_v$.

Diophantine principal bundles II: The non-abelian case

Actual applications use

$$\begin{tikzcd}
X(\mathbb{Q}) \arrow[r] \arrow[d, "j"'] & \prod_v X(\mathbb{Q}_v) \arrow[d, "\prod_v j_v"'] \\
H^1(\mathbb{Q}, U(\bar{X}, b)) \arrow[r] & \prod_v H^1(\mathbb{Q}_v, U(\bar{X}, b))
\end{tikzcd}$$

where

$$U(\bar{X}, b) = `\pi_1^p(X, b) \otimes \mathbb{Q}_p`$$

is the $\mathbb{Q}_p$-pro-unipotent completion of $\pi_1^p(\bar{X}, b)$.

Diophantine principal bundles II: The non-abelian case

Actual applications use

$$\begin{tikzcd} X(\mathbb{Q}) \arrow[rr] \arrow[d, "j"'] & & \prod_v X(\mathbb{Q}_v) \arrow[d, "\prod_v j_v"'] \\ H^1(\mathbb{Q}, U(\bar{X}, b)) \arrow[r] & \prod_v H^1(\mathbb{Q}_v, U(\bar{X}, b)) & \end{tikzcd}$$

where

$$U(\bar{X}, b) = \text{`}\pi_1^p(X, b) \otimes \mathbb{Q}_p\text{'}$$

is the $\mathbb{Q}_p$-pro-unipotent completion of $\pi_1^p(\bar{X}, b)$.

The effect is that the moduli spaces become pro-algebraic schemes over $\mathbb{Q}_p$ and the lower row of this diagram an algebraic map.

Diophantine principal bundles II: The non-abelian case

That is, the key object of study is

$$H^1_f(\mathbb{Q}, U(\bar{X}, b))$$

the **Selmer scheme** of X, defined to be the subfunctor of $H^1(\mathbb{Q}, U(\bar{X}, b))$ satisfying local conditions at all (or most) v.

These are conditions like ‘unramified at most primes’, ‘crystalline at p’, and often a few extra conditions.

Diophantine principal bundles II: The non-abelian case

$$\begin{tikzcd}
X(\mathbb{Q}) \arrow[r] \arrow[d, "j"'] & \prod_v X(\mathbb{Q}_v) \arrow[d, "\prod_v j_v"'] & \\
H^1_f(\mathbb{Q}, U(\bar{X}, b)) \arrow[r] & \prod_v H^1_f(\mathbb{Q}_v, U(\bar{X}, b)) \arrow[r, "\alpha"] & \mathbb{Q}_p
\end{tikzcd}$$

If α is an algebraic function vanishing on the image, then

$$\alpha \circ \prod_v j_v$$

gives a defining equation for $X(\mathbb{Q})$ inside $\prod_v X(\mathbb{Q}_v)$.

Diophantine principal bundles II: The non-abelian case

To make this concretely computable, we take the projection

$$pr_p : \prod_v X(\mathbb{Q}_v) \longrightarrow X(\mathbb{Q}_p)$$

and try to compute

$$\cap_\alpha pr_p(Z(\alpha \circ \prod_v j_v)) \subset X(\mathbb{Q}_p).$$

Diophantine principal bundles II: The non-abelian case

To make this concretely computable, we take the projection

$$pr_p : \prod_v X(\mathbb{Q}_v) \longrightarrow X(\mathbb{Q}_p)$$

and try to compute

$$\cap_\alpha pr_p(Z(\alpha \circ \prod_v j_v)) \subset X(\mathbb{Q}_p).$$

Non-Archimedean effective Mordell Conjecture:

I. $\boxed{\cap_\alpha pr_p(Z(\alpha \circ \prod_v j_v)) = X(\mathbb{Q})}$

Diophantine principal bundles II: The non-abelian case

To make this concretely computable, we take the projection

$$pr_p : \prod_v X(\mathbb{Q}_v) \longrightarrow X(\mathbb{Q}_p)$$

and try to compute

$$\cap_\alpha pr_p(Z(\alpha \circ \prod_v j_v)) \subset X(\mathbb{Q}_p).$$

Non-Archimedean effective Mordell Conjecture:

I. $\boxed{\cap_\alpha pr_p(Z(\alpha \circ \prod_v j_v)) = X(\mathbb{Q})}$

II. $\boxed{\text{This set is effectively computable.}}$

Diophantine principal bundles II: The non-abelian case

Remarks:

1. As soon as there is one α with α_p non-trivial, $pr_p(Z(\alpha \circ \prod_v j_v))$ is finite.

2. There is a (highly reliable) conjectural mechanism for producing infinitely many algebraically independent α.

3. This conjecture is essentially implied by Grothendieck's *section conjecture*: Rather, it does give an effective method of computing $X(\mathbb{Q})$ via the main diagram.

V. Computing Rational Points

Computing rational points

[Dan-Cohen, Wewers]

For $X = \mathbb{P}^1 \setminus \{0, 1, \infty\}$,

$$X(\mathbb{Z}[1/2]) = \{2, -1, 1/2\} \subset \{D_2(z) = 0\} \cap \{D_4(z) = 0\},$$

Computing rational points

[Dan-Cohen, Wewers]

For $X = \mathbb{P}^1 \setminus \{0, 1, \infty\}$,

$$X(\mathbb{Z}[1/2]) = \{2, -1, 1/2\} \subset \{D_2(z) = 0\} \cap \{D_4(z) = 0\},$$

where

$$D_2(z) = \ell_2(z) + (1/2)\log(z)\log(1-z),$$

$$D_4(z) = \zeta(3)\ell_4(z) + (8/7)[\log^3 2/24 + \ell_4(1/2)/\log 2]\log(z)\ell_3(z)$$

$$+[(4/21)(\log^3 2/24 + \ell_4(1/2)/\log 2) + \zeta(3)/24]\log^3(z)\log(1-z),$$

and

$$\ell_k(z) = \sum_{n=1}^{\infty} \frac{z^n}{n^k}.$$

Computing rational points

[Dan-Cohen, Wewers]

For $X = \mathbb{P}^1 \setminus \{0, 1, \infty\}$,

$$X(\mathbb{Z}[1/2]) = \{2, -1, 1/2\} \subset \{D_2(z) = 0\} \cap \{D_4(z) = 0\},$$

where

$$D_2(z) = \ell_2(z) + (1/2)\log(z)\log(1-z),$$

$$D_4(z) = \zeta(3)\ell_4(z) + (8/7)[\log^3 2/24 + \ell_4(1/2)/\log 2]\log(z)\ell_3(z)$$
$$+[(4/21)(\log^3 2/24 + \ell_4(1/2)/\log 2) + \zeta(3)/24]\log^3(z)\log(1-z),$$

and

$$\ell_k(z) = \sum_{n=1}^{\infty} \frac{z^n}{n^k}.$$

Numerically, the inclusion appears to be an equality.

Computing rational points

Some qualitative results:

[Coates and Kim]

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

for $n \geq 4$ has only finitely many rational points.

Computing rational points

Some qualitative results:

[Coates and Kim]

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

for $n \geq 4$ has only finitely many rational points.

Standard structural conjectures on mixed motives (generalised BSD)
$\Rightarrow$ There exist many non-zero α as above.

Computing rational points

Some qualitative results:

[Coates and Kim]

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

for $n \geq 4$ has only finitely many rational points.

Standard structural conjectures on mixed motives (generalised BSD)
$\Rightarrow$ There exist many non-zero α as above.

($\Rightarrow$ Faltings's theorem.)

Computing rational points

A recent result on modular curves by Balakrishnan, Dogra, Mueller, Tuitmann, Vonk. [Explicit Chabauty-Kim for the split Cartan modular curve of level 13. Annals of Math. 189]

Computing rational points

A recent result on modular curves by Balakrishnan, Dogra, Mueller, Tuitmann, Vonk. [Explicit Chabauty-Kim for the split Cartan modular curve of level 13. Annals of Math. 189]

$$X_s^+(N) = X(N)/C_s^+(N),$$

where $X(N)$ the the compactification of the moduli space of pairs

$$(E, \phi : E[N] \simeq (\mathbb{Z}/N)^2),$$

and $C_s^+(N) \subset GL_2(\mathbb{Z}/N)$ is the normaliser of a split Cartan subgroup.

Computing rational points

A recent result on modular curves by Balakrishnan, Dogra, Mueller, Tuitmann, Vonk. [Explicit Chabauty-Kim for the split Cartan modular curve of level 13. Annals of Math. 189]

$$X_s^+(N) = X(N)/C_s^+(N),$$

where $X(N)$ the the compactification of the moduli space of pairs

$$(E, \phi : E[N] \simeq (\mathbb{Z}/N)^2),$$

and $C_s^+(N) \subset GL_2(\mathbb{Z}/N)$ is the normaliser of a split Cartan subgroup.

Bilu-Parent-Rebolledo had shown that $X_s^+(p)(\mathbb{Q})$ consists entirely of cusps and CM points for all primes $p > 7$, $p \neq 13$. They called $p = 13$ the 'cursed level'.

Computing rational points

Theorem (BDMTV)

The modular curve

$$X_s^+(13)$$

has exactly 7 rational points, consisting of the cusp and 6 CM points.

Computing rational points

Theorem (BDMTV)

The modular curve

$$X_s^+(13)$$

has exactly 7 rational points, consisting of the cusp and 6 CM points.

This concludes an important chapter of a conjecture of Serre from the 1970s:

There is an absolute constant A such that

$$G_{\mathbb{Q}} \longrightarrow \mathrm{Aut}(E[p])$$

is surjective for all non-CM elliptic curves $E/\mathbb{Q}$ and primes $p > A$.

Computing rational points

[Burcu Baran]

$$y^4 + 5x^4 - 6x^2y^2 + 6x^3z + 26x^2yz + 10xy^2z - 10y^3z$$
$$-32x^2z^2 - 40xyz^2 + 24y^2z^2 + 32xz^3 - 16yz^3 = 0$$

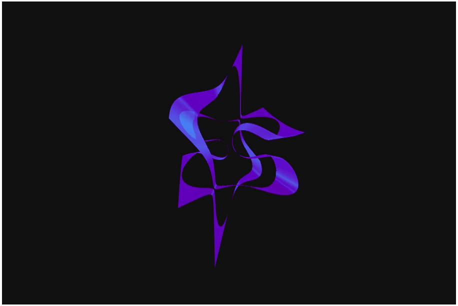


Figure: The cursed curve

{(1:1:1), (1:1:2), (0:0:1), (-3:3:2), (1:1:0), (0,2:1), (-1:1:0) }

VI. Some speculations on rational points and critical points

Some speculations on rational points and critical points

Would like to think of

$$H^1(G, U(\bar{X}, b)) \longrightarrow \prod_v H^1(G_v, U(\bar{X}, b))$$

as being like

$$\mathbb{S}(M, G) \subset \mathcal{A}(M, G)$$

the space of solutions to a set of Euler-Lagrange equations on a space of connections.

Some speculations on rational points and critical points

Would like to think of

$$H^1(G, U(\bar{X}, b)) \longrightarrow \prod_v H^1(G_v, U(\bar{X}, b))$$

as being like

$$\mathbb{S}(M, G) \subset \mathcal{A}(M, G)$$

the space of solutions to a set of Euler-Lagrange equations on a space of connections.

In particular, functions cutting out the image of localisation should be thought of as 'classical equations of motion' for gauge fields.

Some speculations on rational points and critical points

When X is smooth and projective, $X(\mathbb{Q}) = X(\mathbb{Z})$, and we are actually interested in

$$Im(H^1(G_S, U)) \cap \prod_{v \in S} H^1_f(G_v, U) \subset \prod_{v \in S} H^1(G_v, U),$$

where

$$H^1_f(G_v, U) \subset H^1(G_v, U)$$

is a subvariety defined by some integral or Hodge-theoretic conditions.

Some speculations on rational points and critical points

When X is smooth and projective, $X(\mathbb{Q}) = X(\mathbb{Z})$, and we are actually interested in

$$Im(H^1(G_S, U)) \cap \prod_{v \in S} H^1_f(G_v, U) \subset \prod_{v \in S} H^1(G_v, U),$$

where

$$H^1_f(G_v, U) \subset H^1(G_v, U)$$

is a subvariety defined by some integral or Hodge-theoretic conditions.

In order to apply symplectic techniques, replace U by

$$T^*(1)U := (LieU)^*(1) \rtimes U.$$

Some speculations on rational points and critical points

Then

$$\prod_{v \in S} H^1(G_v, T^*(1)U)$$

is a symplectic variety and

$$Im(H^1(G_S, T^*(1)U)), \qquad \prod_{v \in S} H^1_f(G_v, T^*(1)U)$$

are Lagrangian subvarieties.

Some speculations on rational points and critical points

Then

$$\prod_{v\in S} H^1(G_v, T^*(1)U)$$

is a symplectic variety and

$$Im(H^1(G_S, T^*(1)U)), \qquad \prod_{v\in S} H^1_f(G_v, T^*(1)U)$$

are Lagrangian subvarieties.

Thus, the (derived) intersection

$$\mathcal{D}_S(X) := Im(H^1(G_S, T^*(1)U)) \cap \prod_{v\in S} H^1_f(G_v, T^*(1)U)$$

has a $[-1]$-shifted symplectic structure.

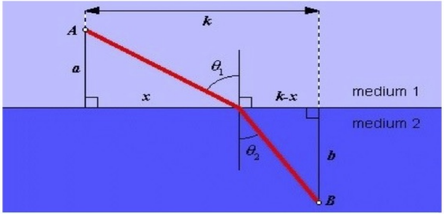
Zariski-locally the critical set of a function. (Brav, Bussi, Joyce)

Some speculations on rational points and critical points

$$\begin{tikzcd}
X(\mathbb{Z}) \arrow[r] \arrow[d, "j^g"'] & j_S^{-1}(\mathcal{D}_S(X)) \arrow[r, hook] \arrow[d, "j_S"'] & \prod_{v\in S} X(\mathbb{Q}_v) \arrow[d, "j_S"'] \\
H^1_f(G_S, T^*(1)U) \arrow[r, "loc_S"] & \mathcal{D}_S(X) \arrow[r, hook] & \prod_{v\in S} H^1(G_v, T^*(1)U_n)
\end{tikzcd}$$

From this view, the global points can be obtained by pulling back 'Euler-Lagrange equations' via a period map.

Some speculations on rational points and critical points



For integers $n > 2$ the equation

$$a^n + b^n = c^n$$

cannot be solved with positive integers a, b, c.

Figure: Pierre de Fermat (1607-1665)

Bibliography

- J. Balakrishnan, N. Dogra, S. Müller, J. Tuitman, J. Vonk Explicit Chabauty-Kim for the split Cartan modular curve of level 13. Annals of Math. 189 (2019), Issue 3, pp. 888-944
- Betts, L. Alexander, Dogra, Netan The local theory of unipotent Kummer maps and refined Selmer schemes. arXiv:1909.05734
- Bilu, Yuri; Parent, Pierre Serre's uniformity problem in the split Cartan case. Ann. of Math. (2) 173 (2011), no. 1, 569–584.
- Bilu, Yuri; Parent, Pierre; Rebolledo, Marusia Rational points on $X_0^+(p^r)$. Ann. Inst. Fourier (Grenoble) 63 (2013), no. 3, 957–984.
- Brav, Christopher; Bussi, Vittoria; Joyce, Dominic A 'Darboux theorem' for derived schemes with shifted symplectic structure. arXiv:1305.6302v3

Bibliography

- Chenevier, Gaëtan The p-adic analytic space of pseudocharacters of a profinite group and pseudorepresentations over arbitrary rings. Automorphic forms and Galois representations. Vol. 1, 221–285, London Math. Soc. Lecture Note Ser., 414, Cambridge Univ. Press, Cambridge, 2014.
- Coates, John; Kim, Minhyong Selmer varieties for curves with CM Jacobians. Kyoto J. Math. 50 (2010), no. 4, 827–852.
- Dan-Cohen, Ishai; Wewers, Stefan Mixed Tate motives and the unit equation. https://arxiv.org/abs/1311.7008
- Dan-Cohen, Ishai; Wewers, Stefan Mixed Tate motives and the unit equation II. https://arxiv.org/abs/1510.01362

Bibliography

- Deligne, Pierre Le groupe fondamental de la droite projective moins trois points. Galois groups over $\mathbb{Q}$ (Berkeley, CA, 1987), 79–297, Math. Sci. Res. Inst. Publ., 16, Springer, New York, 1989.
- Faltings, G. Endlichkeitssätze für abelsche Varietäten über Zahlkörpern. Invent. Math. 73 (1983), no. 3, 349-366.
- Fontaine, Jean-Marc (ed.) *Périodes p-adiques*. Astérisque, 223, Paris: Société Mathématique de France (1994)
- Lawrence, Brian, Venkatesh, Akshay Diophantine problems and p-adic period mappings
- Serre, J.-P. A course in arithmetic. Graduate Texts in Mathematics, No. 7. Springer-Verlag, New York-Heidelberg, 1973.
- Silverman, Joseph H. The arithmetic of elliptic curves. Second edition. Graduate Texts in Mathematics, 106. Springer, Dordrecht, 2009.