Some Recent Progress on Diophantine Equations In Two-Variables

Minhyong Kim
University of Warwick

Rochester, May, 2021

I. Background: Arithmetic of Algebraic Curves

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: $g = 0, d = 2$

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*.

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: $g = 0$

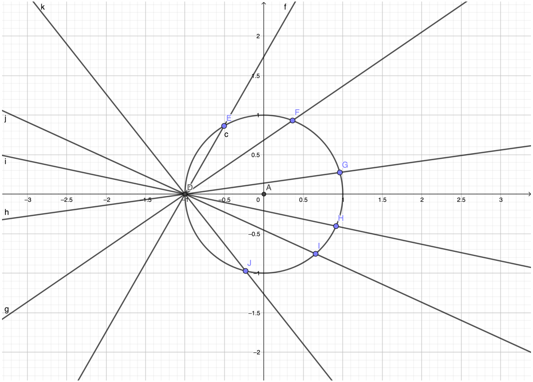


Figure: Method of sweeping lines

Sweep through the circle with all lines with rational slope going through the point $(-1, 0)$.

Arithmetic of algebraic curves: $g = 0$

A key ingredient here is a successful study of the inclusion

$$X(\mathbb{Q}) \subset \prod X(\mathbb{Q}_p)$$

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

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

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

Hasse principle fails:

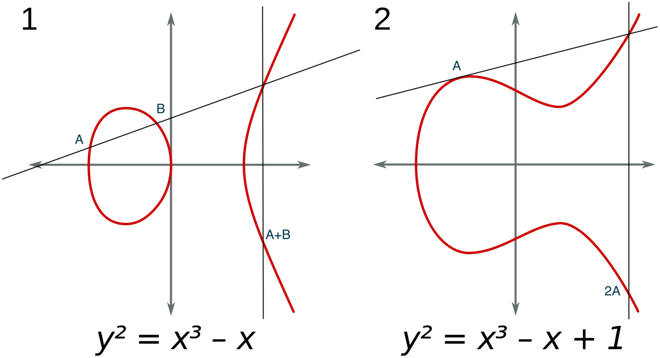
$$3x^3 + 4y^3 + 5 = 0$$

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 an abelian group via the chord-and-tangent method.

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.

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

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

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

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

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

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:

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

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.

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

Basic idea:

$$\begin{tikzcd} X(\mathbb{Q}) \arrow[r] \arrow[d] & \prod_v X(\mathbb{Q}_v) \arrow[d] \\ \mathcal{M} \arrow[r, "loc"] & \prod_v \mathcal{M}_v \end{tikzcd}$$

$$"X(\mathbb{Q}) = [\prod_v X(\mathbb{Q}_v)] \cap \mathcal{M}"$$

The spaces $\mathcal{M}$ and $\mathcal{M}_v$ are *moduli spaces of arithmetic principal bundles*.

II. Arithmetic Principal Bundles

General principle:

Bundle on $X/G \leftrightarrow G$-equivariant bundle on X

Principal Bundles

Basic case:

R group, P set with simple transitive R-action

$$P \times G \longrightarrow P$$

Thus, choice of any $z \in P$ induces a bijection

$$R \simeq P$$

$$r \mapsto zr.$$

All objects could have more structure, for example, a topology.

Principal Bundles

Could also have a family of such things over a space M:

$$f : P \longrightarrow M$$

a fibre bundle with right action of R such that locally over sufficiently small open $U \subset M$,

$$P_U = f^{-1}(U)$$

is isomorphic to $R \times U$.

That is, a choice of a section $s : U \longrightarrow P_U$ induces an isomorphism

$$R \times U \simeq P_U$$

$$(r, u) \mapsto s(u)r.$$

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 $\mathrm{Spec}(K)$.

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.

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

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.

$P(x)$ 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

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 $Z^1(G, R)$.

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

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

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

We will endow (refinements of) $H^1(G_K, R)$ geometric structures that have applications to Diophantine geometry.

Remark for number theorists:

When R is (the set of $\mathbb{Q}_p$ points of) a reductive group with 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

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

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

Diophantine principal bundles

The main principal bundles of interest are

$$\pi_1(M, b)$$

$$\pi_1(M; b, x)$$

M is a topological space and where $\pi_1(M, b)$ acts on P_{top} via

$$(p, g) \mapsto pg,$$

precomposing paths with loops.

In usual topology, somewhat pedantic to distinguish R and P.

Diophantine principal bundles

More structure enters when we replace fundamental groups by $\mathbb{Q}_p$-unipotent completions:

$$U(\pi_1(M,b)) = \text{''}\pi_1(M,b) \otimes \mathbb{Q}_p\text{''}$$

$$P(\pi_1(M;b,x)) = [\pi_1(M;b,x) \times U(\pi_1(M,b))]/\pi_1(M,b).$$

$U(\pi_1(M,b))$ is the universal $\mathbb{Q}_p$-pro-algebraic group together with a map

$$\pi_1(M,b) \longrightarrow U.$$

Diophantine principal bundles

$U(\Gamma)$ can be defined for any group Γ.

Examples:

$$U(\mathbb{Z}) = \mathbb{Z} \otimes \mathbb{Q}_p = \mathbb{Q}_p.$$

If Γ is a two-step nilpotent group, then $U(\Gamma)$ is a 'Heisenberg' group that fits into an exact sequence

$$0 \longrightarrow [\Gamma, \Gamma] \otimes \mathbb{Q}_p \longrightarrow U(\Gamma) \longrightarrow \Gamma^{ab} \otimes \mathbb{Q}_p \longrightarrow 0.$$

Diophantine principal bundles

Fundamental fact of arithmetic homotopy:

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

$$U(X,b) = U(\pi_1(X,b)), \quad P(X;b,x) = P(\pi_1(X;b,x))$$

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

The triples

$$(G_{\mathbb{Q}}, U(X,b), P(X;b,x))$$

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

We get thereby moduli spaces of principal bundles:

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

that are limits of algebraic varieties.

Diophantine principal bundles

Using these constructions, we also get a map

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

given by

$$x \mapsto [P(X; b, x)]$$

For each prime v, have local versions

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

given by

$$x \mapsto [P(X; b, x)]$$

which turn out to be computable. These are *period maps* and involved non-Archimedean iterated integrals. Put $per := \prod_v j_v$.

Diophantine principal bundles

Localization diagram:

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

The lower row of this diagram is an algebraic map. In particular, the image

$$loc(H^1(\mathbb{Q}, U(X,b))) \subset \prod_v H^1(\mathbb{Q}_v, U(X,b))$$

is computable in principle.

Diophantine principal bundles

$$X(\mathbb{Q}) \subset per^{-1}(loc[H^1(\mathbb{Q}, U(X,b))]) \subset \prod_v X(\mathbb{Q}_v).$$

We focus then on the p-adic component:

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

Non-Archimedean effective Mordell Conjecture:

I. $\boxed{pr_p[per^{-1}(loc[H^1(\mathbb{Q}, U(X,b))])] = X(\mathbb{Q})}$

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

Diophantine principal bundles

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

$$H^1(\mathbb{Q}, U(X,b)) \longrightarrow \prod_v H^1(\mathbb{Q}_v, U(X,b)) \xrightarrow{\alpha} \mathbb{Q}_p$$

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

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

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

This turns out to be an intersection of zero sets of p-adic iterated integrals.

IV. Computing Rational Points

Computing rational points

For $X = \mathbb{P}^1 \setminus \{0, 1, \infty\}$. This is equivalent to the study of *unit equations*, i.e., solutions to

$$a + b = 1$$

where a and b are both invertible elements in a ring like $\mathbb{Z}[1/N]$.

There is an S_3-action on solutions a generated by $z \mapsto 1 - z$ and $z \mapsto 1/z$.

Computing rational points

[Dan-Cohen, Wewers]

In $\mathbb{Z}[1/2]$, only solutions a are

$$\{2, -1, 1/2\} \subset \{D_2(z) = 0\} \cap \{D_4(z) = 0\},$$

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

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

These equations all occur in the field of p-adic integers $\mathbb{Z}_p$ for some p. Numerically, the inclusion appears to be an equality.

Computing rational points

[Alex Betts]
If ℓ is a prime, then solutions in $\mathbb{Z}[1/\ell]$ are in the zero set of

$$\log(z) = 0, L_2(z) = 2$$

and S_3 permutations.

If q, ℓ are primes different from 3 then the solutions in $\mathbb{Z}[1/q\ell]$ consists of -1, at most one other point, and S_3 permutations.

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]

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

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.

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]

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

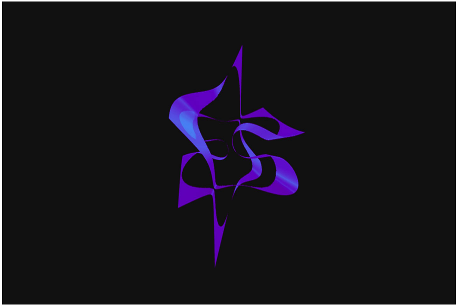


Figure: The cursed curve

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

V. Why Diophantine Equations?

Why Diophantine Equations?

In arithmetic geometry, the basic number systems are *finitely generated rings*:

$$\mathbb{Z}[1/N][\alpha_1, \alpha_2, \alpha_3, \ldots, \alpha_n].$$

The α_i could be algebraic numbers like $\sqrt{2}, \sqrt{691}, e^{2\pi i/m}$, or transcendental numbers like $\pi, e, e^{\sqrt{2}}$.

These are number systems with *intrinsic discreteness*.

Given a finitely-generated ring A, arithmetic geometers associate to it a geometric space called the *spectrum* of A:

$$\mathrm{Spec}(A).$$

An arithmetic scheme is glued out of finitely many such spectra. These are the main space of study in arithmetic geometry.

Why Diophantine Equations?

Ubiquity of arithmetic schemes:

All objects in algebraic geometry have an underlying arithmetic scheme:

$$f(x_1, x_2, \ldots, x_n) = 0 \leftrightarrow \mathrm{Spec}(R[x_1, x_2, \ldots, x_n]/(f)) =: X$$

where R is the ring generated by the coefficients of f.

So we can look for solutions in any ring $T \supset R$. Denote by $X(T)$ the solutions in T.

[In fact, Faltings's theorem implies that when X is a curve of genus at least two, $X(T)$ is finite for any finitely-generated T.]

Why Diophantine Equations?

Ubiquity of arithmetic schemes:

If M is compact manifold, then it is diffeomorphic to $X(\mathbb{R})$, where X is an arithmetic scheme. [Nash-Tognoli]

If Σ is a compact Riemann surface, then it is conformally equivalent to $X(\mathbb{C})$, where X is an arithmetic scheme.

Can consider $X(A) \subset X(\mathbb{C})$ for finitely-generated $A \subset \mathbb{C}$.

These are natural discrete subsets of world-sheets of strings.

Similarly for

$$X(A) \subset X(\mathbb{R}) = M$$

and compact manifolds.

Why Diophantine Equations?

For either $X(\mathbb{R})$ or $X(\mathbb{C})$, have a sequence of natural discrete approximations

$$X(A_1) \subset X(A_2) \subset X(A_3) \subset \cdots \subset X(\mathbb{R}) \; (X(\mathbb{C}))$$

as we run over finitely-generated number systems A_i.

Is this a 'practical' approximation?

First need to know how to compute the $X(A_i)$. If the computational problem were easy, we might consider applications more freely.