The Menu

(1) Hilbert's Tenth Problem and Diophantine Stability

(2) **Logic related to Elliptic Curves and their rational points**

(3) Methods

Recalling the motivation of Matiyasevich (and how elliptic curves might enter the picture)

One first gives Diophantine definitions of ‘basic subsets’ of **Z** and systematically builds up.

For example, Lagrange’s Theorem says that any positive whole number is expressible as a sum of four squares. In Diophantine language, this means that the polynomial

$$f(t; X_1, X_2, X_3, X_4) := \quad t - \Sigma_{i=1}^{4} X_j^2$$

cuts out the set of positive integers; so the set of positive numbers is Diophantine.

Building the vocabulary

Therefore it follows, by easy steps, that these sets are too:

- the set of numbers $\geq a$ for any given $a \in \mathbf{Z}$,
- the set of numbers $\leq b$ for any given $b \in \mathbf{Z}$,
- any finite subset of $\mathbf{Z}$,
- the complement of any finite subset of $\mathbf{Z}$.

Little by little

- So, if D is Diophantine, then any set obtained from D by removing and adding finite sets is also Diophantine.

Little by little

- So, if D is Diophantine, then any set obtained from D by removing and adding finite sets is also Diophantine.

- Arithmetic progressions are Diophantine; as are the set of all squares, all cubes, all n-th powers for any given n.

Little by little

- So, if D is Diophantine, then any set obtained from D by removing and adding finite sets is also Diophantine.
- Arithmetic progressions are Diophantine; as are the set of all squares, all cubes, all n-th powers for any given n.
- Composite numbers.

Little by little

- So, if D is Diophantine, then any set obtained from D by removing and adding finite sets is also Diophantine.

- Arithmetic progressions are Diophantine; as are the set of all squares, all cubes, all n-th powers for any given n.

- Composite numbers.

- For any fixed (say, nonsquare, positive) integer d, consider the set of integers t that come in solutions of the Pell equation
$$t^2 - ds^2 = 1$$
(this being a set that grows roughly exponentially).

Factorials

There is a system of polynomials that cut out the set of factorials $1!, 2!, 3! \dots$ The fact that this set is Diophantine played a big role in the development of the subject.

To get such a polynomial one starts by finding a Diophantine way of expressing the binomial coefficients $\binom{n}{m}$ and then dealing with the—to me surprisingly unpromising—formula:

Factorials

$$m! = \lim_{n\to\infty} \frac{n^m}{\binom{n}{m}}.$$

(!!!)

Comments on the History

This work ranges from 1944 when Emil Post said that Hilbert's tenth problem

"begs for an unsolvability proof"

to 1970 when Matijasevic clinched the theorem.

A three decade range (beautifully and informatively documented)!

Focus on very roughly exponential functions

But I'll begin in 1960, when Julia Robinson, sharpening work of Martin Davis, and Hillary Putnam, showed that if there exists a *very roughly exponential function* defined in a diophantine way; i.e., a Diophantine set $\mathcal{F}$ of couples (a, b) in $\mathbf{N} \times \mathbf{N}$ with two properties:

1. If $(a, b) \in \mathcal{F}$ then $a < b^b$.
2. For each positive integer k there is an $(a, b) \in \mathcal{D}$ with $b > a^k$.

then all listable sets would be Diophantine.

Fibonacci

In 1970, Matiyasevich provides a Diophantine definition of a set $\mathcal{F}$ as required by J.R.: he took his $\mathcal{F}$ to be the collection of pairs (a, b) such that

$$b = F_{2a}$$

where F_n is the nth Fibonacci number.

Fibonacci

In 1970, Matiyasevich provides a Diophantine definition of a set $\mathcal{F}$ as required by J.R.: he took his $\mathcal{F}$ to be the collection of pairs (a, b) such that

$$b = F_{2a}$$

where F_n is the nth Fibonacci number.

He managed to define this set $\mathcal{F}$ in a diophantine way, thereby completing the proof that all listable sets are Diophantine and establishing the fact that Hilbert's tenth problem (over $\mathbf{Z}$) is unsolvable.

I find this quotation of Matiyasevich illuminating:

"The idea was as follows. A universal computer science tool for representing information uses words rather than numbers. However, there are many ways to represent words by numbers. One such method is naturally related to Diophantine equations. Namely, it is not difficult to show that every 2×2 matrix

$$\begin{pmatrix} m_{11} & m_{12} \\ m_{21} & m_{22} \end{pmatrix}$$

with the m's being non-negative integers and the determinant

$$m_{11}m_{22} - m_{12}m_{21}$$

equal to 1 can be represented, in a unique way, as a product of matrices:

$$M_0 := \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$$

and

$$M_1 := \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}.$$

It is evident that any product of such matrices has non-negative integer elements and the determinant equals 1. This implies that we can uniquely represent a word in the two-letter alphabet M_0, M_1 by the four-tuple

$$(m_{11}, m_{12}, m_{21}, m_{22})$$

such that the numbers evidently satisfy the Diophantine equation

$$m_{11}m_{22} - m_{12}m_{21} \ = \ 1.$$

Representing words in a diophantine way

Under this representation of words by matrices, the operation of concatenation-of-words corresponds to matrix multiplication and thus can be easily expressed as a system of Diophantine equations,

opening up a way of transforming an arbitrary system of word equations into “equivalent” Diophantine equations.

Many decision problems about words had been shown undecidable, so it was quite natural to try to attack Hilbert's tenth problem by proving the undecidability of systems of word equations.”

Pell's Equation versus Elliptic curves with infinitely many rational points

Pell's Equation:

$$Y^2 - DX^2$$

or the Norm equation giving units in real quadratic fields was, in effect, what Matiyasevich used rather than matrices.

—The Fibonacci numbers come as the coefficients of the group of units

$$(\frac{1+\sqrt{5}}{2})^n.$$

The Bootstrap Method: Find a 'definable model' of a subring $A \hookrightarrow B$ in the vocabulary of B

If you can construct a *definable set-theoretic injection*

$$A \hookrightarrow B^N$$

that has the property that the image of 1, and the graphs of *addition* and *multiplication* are all definable, then one says that

The ring B 'has' a definable model of A

If a ring B has a definable model of A we get the following "Bootstrap" transport of undecidability:

undecidability of A $\quad\Longrightarrow\quad$ **undecidability of** B**.**

Recall from the first lecture: Diophantine versus First-Order undecidability

Decidability of B: There is an algorithm to determine a yes or no answer for the truth of 'sentences in the language of B.'

- *Diophantine decidability:* The naive notion: we get an answer for any sentence asserting that some diophantine equation (or finite collection of them) has a (simultaneous) solution.
- *First-order decidability:* The sentences may include

$$\exists\forall\exists\ldots$$

Again: if B has a definable model of A:

Decidability of B $\Longrightarrow$ **Decidability of A.**

The Bootstrap Method, Elliptic curves, and Diophantine stability

The problem with Pell's Equation for the 'Bootstrap method' to pass from a ring A to a larger ring B—i.e., when you consider equations of the form

$$Y^2 - DX^2 = \pm 1,$$

is that you often get *more rational solutions* in B and hence the *set of rational solutions over* B has, in a sense, forgotten about the subring A.

Bootstrapping a definition of $\mathbf{Z}$ to the ring of integers, $\mathcal{O}_K$, of a number field

Theorems of
Cornelissen-Pheidas-Zahidi, Poonen, Shlapentokh

1. Find some elliptic curve E over $\mathbf{Q}$ that has

   (a) infinitely many rational points over $\mathbf{Q}$

   and

   (b) the diophantine-stability property: $E(\mathbf{Q}) = E(K)$.

Then the set of rational integers is diophantine over $\mathcal{O}_K$.

Climbing number field extensions L/K

(B. Poonen, A. Shlapentokh) Let $K \subset L$ be number fields. If there exists an elliptic curve E over K having **(a)** infinitely many rational points over K

and

(b) the diophantine-stability property for the extension L/K:

$$E(K) = E(L),$$

Climbing number field extensions L/K

(B. Poonen, A. Shlapentokh) Let $K \subset L$ be number fields. If there exists an elliptic curve E over K having **(a)** infinitely many rational points over K

and

(b) the diophantine-stability property for the extension L/K:

$$E(K) = E(L),$$

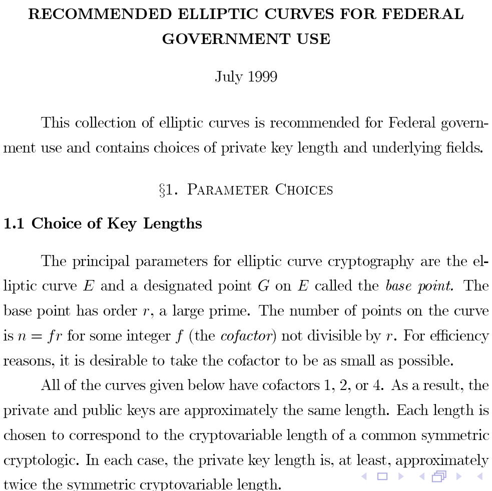
then there exists a a diophantine definition of $\mathcal{O}_K$ in $\mathcal{O}_L$.

Elliptic curves and Logic

Aside: *Mention the strong(er) Lang conjecture*

Elliptic curves seem to be in close contact with a surprising number of different fields of mathematics, and physics and applied areas.
For example, in their essential role in cryptography, elliptic curves have a certain predominance that warrants publications such as this 1999 government memo:

Elliptic curves and cryptography



RECOMMENDED ELLIPTIC CURVES FOR FEDERAL GOVERNMENT USE

July 1999

This collection of elliptic curves is recommended for Federal government use and contains choices of private key length and underlying fields.

§1. Parameter Choices

1.1 Choice of Key Lengths

The principal parameters for elliptic curve cryptography are the elliptic curve E and a designated point G on E called the *base point.* The base point has order r, a large prime. The number of points on the curve is $n = fr$ for some integer f (the *cofactor*) not divisible by r. For efficiency reasons, it is desirable to take the cofactor to be as small as possible.

All of the curves given below have cofactors 1, 2, or 4. As a result, the private and public keys are approximately the same length. Each length is chosen to correspond to the cryptovariable length of a common symmetric cryptologic. In each case, the private key length is, at least, approximately twice the symmetric cryptovariable length.

Discrete Logarithm Problem

The first page of that memorandum already gets down to the business of discussing the discrete logarithm problem when posed in terms of the near-cyclic group of rational points of those *preferred* elliptic curves, and specifically, the *difficulty* of computing such logs, which—in this game—is a virtue.

Elliptic curves as algebraic curves

Elliptic curves can be represented as smooth plane cubic curves with one point at infinity, and therefore by adroit linear change of variables can be given by an affine equation of the form

$$y^2 = g(x) := x^3 + cx + d,$$

for c, d constants, where the cubic polynomial $g(x)$ has no multiple roots.

Rational points

Such curves then are algebraic objects, and can be defined over any field k, by taking the constants $c, d \in k$.

The "elliptic curve" E itself then is the projective model of this affine curve, and its points rational over the field k is usually denoted $E(k)$ which consists of the single point at infinity –usually called, perversely, 0 or the origin—and all affine points

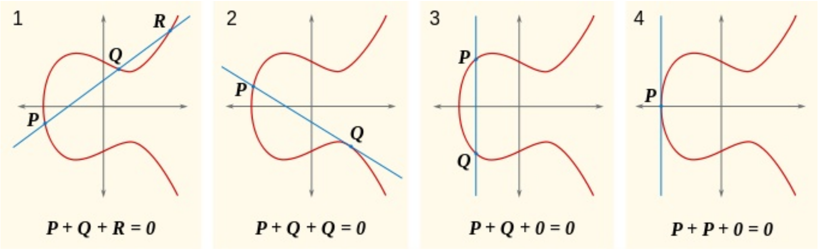
$$(\alpha, \beta)$$

each entry in k, satisfying the equation

$$\beta^2 = \alpha^3 + c \cdot \alpha + d.$$

Chord-and Tangent

Some readers of Diophantus seem to already find in his treatise hints of what later came to be called the "chord-and-tangent process" for making new points on this curve E (rational over k) from pairs of points in $E(k)$:



$P + Q + R = 0$ $\quad$ $P + Q + Q = 0$ $\quad$ $P + Q + 0 = 0$ $\quad$ $P + P + 0 = 0$

Interesting similar structure for cubic hypersurfaces of any dimension, but . . .

This “chord-and-tangent process” banks on the fact that our curve is a cubic hypersurface and would work in any dimension.

But when E is an elliptic curve, defining an addition law of $E(k)$ by stipulating that any 'three' collinear points sum to zero, gives $E(k)$, as it turns out, an abelian group structure:

$$E(k) \times E(k) \longrightarrow E(k)$$

In the era of Mordell,

the arithmetic of elliptic curves was already in full swing, and any number of a host of questions Mordell himself asked, such as

> *What products of two consecutive integers are equal to a product of three consecutive integers?*

provide very interesting questions about elliptic curves.

$0, 6,$ and 210

The answer to this question, known to Mordell half a century ago, is that the only such products are $0, 6,$ and 210.

The equation whose integral solutions "solves" Mordell's Question is

$$\mathcal{E}: \quad y^2 + y = x^3 - x$$

and this is an affine model, over $\mathbf{Z}$, of an elliptic curve over $\mathbf{Q}$ which we'll call

Mordell's Elliptic Curve

Integral solutions

Mordell's original question is about integral solutions.

Now, for any equation that equates a quadratic expression of the variable y to a cubic expression of x (with no multiple roots)

there is an algorithm allowing one to finitely determine all its integral solutions.

Algorithm for integral solutions

(A. Baker): if the maximum height of the coefficients of this equation is H , then all solutions of the satisfy

$$\max(|x|, |y|) < \exp\{(10^6 H)^{10^6}\}.$$

This success is in contrast to the general problem of integral solutions as posed by Hilbert's Tenth Problem solved negatively by Matyasevich. And in contrast to the problem of rational solutions.

Rational solutions

So let's return to Mordell's equation and determine its *rational* rather than only integral solutions. We get quite a different, and striking, answer: there are infinitely many rational solutions, and all of them are 'generated' out of the simplest of its solutions: $(x, y) = (0, 0)$.

$$0^2 + 0 = 0^3 - 0$$

Denominators of the *x*-coordinates

1
1
1
1
4
1
9
25
49
16
529
841
3481
16641
98596
4225
2337841
13608721
67387681
264517696
6941055969
12925188721
384768368209
5677664356225
61935294530404
49020596163841
16063784753682169
158432514799144041
2846153597907293521
62586636021357187216
2237394491744632911601
1870098771536627436025
126208279317419543003841
41998153797159031581158401
1063198259901027900600665796

$P_1 = [0, 0]$

$P_2 = [1, 0]$

$P_3 = [-1, -1]$

$P_4 = [2, -3]$

$P_5 = [1/4, -5/8]$

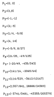
$P_6 = [6, 14]$

$P_7 = [-5/9, 8/27]$

$P_8 = [21/25, -69/125]$

$P_9 = [-20/49, -435/343]$

Notice the growth of the numerators and denominators of these solutions!



P_1=[0, 0]

P_2=[1,0]

P_3=[-1,-1]

P_4=[2,-3]

P_5=[1/4, -5/8]

P_6=[6, 14]

P_7=[-5/9, 8/27]

P_8=[21/25, -69/125]

P_9= (-20/49, -435/343)

P_{10}=[161/16, -2065/64]

P_{11}=[116/529, -3612/12167]

P_{12}=[1357/841, 28888/24389]

P_{13}=[-3741/3481, -43355/205379]

They trace out the shadow of a parabola.

The equation of the 'limit' parabola is itself an important arithmetic invariant of the elliptic curve (if you normalize for the size of typefont)—determined by the *regulator* of this elliptic curve.

Can you make use of the set of denominators of the x-coordinates of the rational points Mordell's elliptic curve,

$$1, 9, 25, 49, 16, 529, 841, \ldots$$

just as Matiyasevich used the Fibonacci numbers to construct a model of the rational integers?

Work of Cornelissen, Pheidas, Zahidi and independently Poonen showed how to do that (in a more general context).

Work of Cornelissen, Pheidas, Zahidi and independently Poonen showed how to do that (in a more general context).

AND if Mordell's elliptic curve is diophantine-stable for the extension $L/\mathbf{Q}$, you can use those denominators to give a diophantine construction of the ring of rational integers in the ring of integers of L.

Discuss!

Classical pillars of the arithmetic of elliptic curves

Modular curves play two somewhat disjoint roles in the foundations of the theory of elliptic curves. As algebraic geometric objects they enter the scene as 'classifiers.'

Their (noncuspidal) points determined (and classify all) elliptic curves with some extra interesting arithmetic structure, such as

Pairs (E, P), where E is an elliptic curve and P a point of order $N \geq 3$ on it.

The completed moduli space that classifies this particular problem is a curve usually denoted

$$X_1(N) := \mathcal{H}/\Gamma_1(N) \cup cusps,$$

and its K-rational (noncuspidal) points give K-rational pairs (E, P).

Classical pillars of the arithmetic of elliptic curves

The other role modular curves play is via the famous *modularity theorem*.

Classical pillars of the arithmetic of elliptic curves

The Mordell-Weil Theorem for any elliptic curve E over any number field K is simply fundamental for the arithmetic theory.

It asserts that:

the group $E(K)$, of K-rational points is a *finitely generated* abelian group.

So $E(K)$ is characterized up to isomorphism by its two invariants:

Rank and Torsion

I.e.,

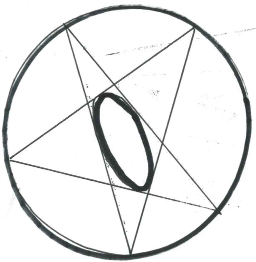
$$E(K) \;\simeq\; \boxed{\text{T(E,K)}} \;\bigoplus\; \mathbf{Z}^{\boxed{\text{r(E,K)}}}.$$

This launches two (surprisingly differently) mathematical projects:

- Study the behavior of torsion $(E, K) \;\mapsto\; \boxed{\text{T(E,K)}}$,
- Study the behavior of rank $(E, K) \;\mapsto\; \boxed{\text{r(E,K)}}$.

Torsion

Torsion in elliptic curves have, as one of their many neat realizations, periodic arrays in the classical *Poncelet Billiard game*



Torsion over $\mathbf{Q}$

We have a complete classification of torsion, rational over Q for elliptic curves defined over Q. It could be stated this "minimalist" way...

Torsion over $\mathbf{Q}$

Theorem

The isomorphy type of a finite group T occurs as the rational torsion group $T(E, \mathbf{Q})$ of some elliptic curves over $\mathbf{Q}$ only when it is forced to occur, by algebraic geometry.

Torsion over $\mathbf{Q}$

Theorem

The isomorphy type of a finite group T occurs as the rational torsion group $T(E, \mathbf{Q})$ of some elliptic curves over $\mathbf{Q}$ only when it is forced to occur, by algebraic geometry.

Namely, only when the modular curve classifying pairs consisting of elliptic curves together with a specified finite subgroup isomorphic to T is isomorphic to the projective line over $\mathbf{Q}$.

Torsion over $\mathbf{Q}$

Theorem

The isomorphy type of a finite group T occurs as the rational torsion group $T(E, \mathbf{Q})$ of some elliptic curves over $\mathbf{Q}$ only when it is forced to occur, by algebraic geometry.

Namely, only when the modular curve classifying pairs consisting of elliptic curves together with a specified finite subgroup isomorphic to T is isomorphic to the projective line over $\mathbf{Q}$.

In such a case, there is an infinite rationally parametrized family of elliptic curves over $\mathbf{Q}$ possess T as rational torsion group.

Torsion over Number Fields

Fix a positive integer d and let $P(d)$ be:

the *largest* prime number p such that there exists an elliptic curve (no CM) defined over some number field of degree $\leq d$ over $\mathbf{Q}$ and for which there is a point of order p on that elliptic curve, rational over that field.

Bounds for prime torsion

A result of Merel, Oesterlé, Parent :

$$d^{1/2} << P(d) << 3^d.$$

It is tempting to conjecture:

$$P(d) \quad <<_\epsilon \quad d^{1/2+\epsilon} \quad (?)$$

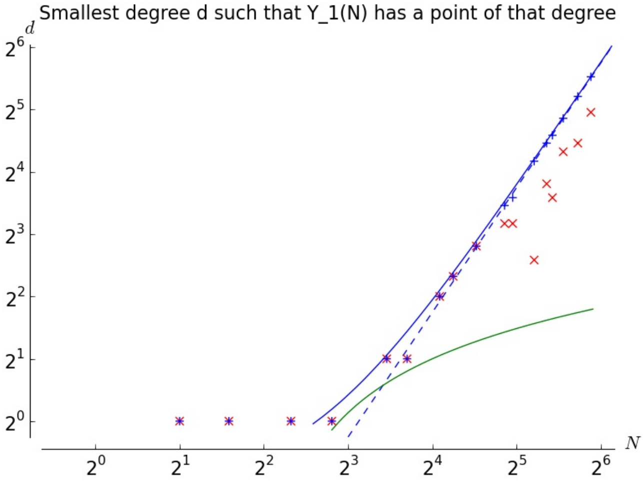
Data

Thanks to Maarten Derickx and Mark van Hoej:
Here is a log-log plot where the axes are

$$(x, y) = (\log p, \log d),$$

the data points recording examples of 'lowest' degree d for the corresponding p occurs as prime torsion over a field of degree d (in a non-CM elliptic curve).

Data of p-torsion in elliptic curves over Number Fields of degree d



Rationally parametrized families of p-torsion

Let p be a prime number, and $d \geq 1$. If there is a $\mathbf{Q}$-rational map

$$f : X_1(p) \to \mathbf{P}^1$$

of degree d of the modular curve $X_1(p)$, you get a "rationally parametrized family" of elliptic curves defined over fields of degree d possessing rational p-torsion over those fields by systematically taking the inverse image of the $\mathbf{Q}$-rational points of $\mathbf{P}^1$.

Sporadic Torsion

Say that a point of order p on an elliptic curve over a number field of degree d is d-**sporadic** if it doesn't occur as a member of such a family.

There are NO d-sporadic points (of prime order) for $d = 1, 2$ or 4.

Interesting possibilities for some experimentation here. . .

Rank

Let K be a fixed number field and consider the collection of all elliptic curves defined over K. The most natural 'first question' that is somewhat of a statistical nature that you might ask about Mordell-Weil rank is:

> *Does $r(E; K)$ admit a finite upper bound (for fixed K and all elliptic curves over K)?*

Here, far from actually knowing the answer, we don't even seem to enjoy a uniform consensus about guesses for what the truth is here, even for the field $\mathbf{Q}$.

Recent newsbreaking heuristics of J. Park, B. Poonen, J.Voight, and M. M. Wood

Rank, so far

rank ≥	year	Author(s)
3	1938	*Billing*
4	1945	*Wiman*
6, 7	1974, 75	*Penney − Pomerance*
8	1977	*Grunewald − Zimmert*
9	1977	*Brumer − Kramer*
12, 14, 15	1982, 86, 92	*Mestre*
17	1992	*Nagao*
19	1992	*Fermigier*
20	1993	*Nagao*
21	1994	*Nagao − Kouya*
22	1997	*Fermigier*
23, 24	1998, 2000	*Martin − McMillen*
28	2006	*Elkies*

Elkies' elliptic curve

To see what's involved in the last entry (Elkies elliptic curve) of this table:

$$\mathcal{E}: \quad Y^2 + XY + Y \;=\; X^3 - X^2 -$$

$$2006776241557552658503320820$$

$$933854275093023031217895650 2X$$

$$+$$

$$34481611795030556467032985690390720374855$$

$$944359319180361266008296291939448732243429$$

What can knowledge of Mordell-Weil ranks of elliptic curves over large fields of algebraic numbers get you?

Let L be a (large) subfield of $\mathbf{Q}^{\mathrm{alg}}$, and E an elliptic curve over L.

As Sasha Shlapentokh explained to me:

IF $\exists$ an elliptic curve E over L such that: $E(L)$ is finitely generated and of positive rank,

1. then there is a first-order model of Z in the ring of integers of L (and in all its subrings).

   So we get first-order undecidability for these.

First-order definability of $\mathbf{Z}$

Theorem (with Karl Rubin): Let E be an elliptic curve over $\mathbf{Q}$ (for example). Let p be any prime number (or ∞).

There are uncountably many subfields K of the field of algebraic numbers in $\mathbf{Q}_p$ for which $E(K)$ is finitely generated.

For these fields, $\mathbf{Z}$ *is first order definable over* K,

The first-order theory for any subfield of such fields K—and for its ring of integers—is undecidable.

Friday's lecture on diophantine stability

In the next lecture we'll describe the methods we use to get our diophantine-stability theorems. These theorems are very far, though, from the following conjectures:

A Conjecture: Let E be an elliptic curve over a number field K and

$$\ell \gg_{X,K} 0.$$

Then for 100% of the cyclic extensions L/K of degree ℓ over K we have $E(L) = E(K)$.**(??)**

More generally:

Diophantine stability for curves

A Conjecture: Let X be an irreducible curve of positive genus over a number field K and

$$\ell \gg_{X,K} 0.$$

Then for 100% of the cyclic extensions L/K of degree ℓ over K we have $X(L) = X(K)$. **(??)**

A Question

Is it possible that we have the following dichotomy for any projective variety V over a number field K and any large enough prime number

$$\ell \gg_{V,K} 0:$$

1. V contains the image of the projective line defined over K, or
2. For 100% of the cyclic extensions L/K of degree ℓ over K we have diophantine stability: $V(L) = V(K)$.**(??)**