Hilbert's Tenth Problem: Undecidability of Polynomial Equations

Alexandra Shlapentokh

East Carolina University,
Greenville, North Carolina, USA

October, 2006

Table of Contents

Hilbert's Question about Polynomial Equations

Is there an algorithm which can determine whether or not an arbitrary polynomial equation in several variables has solutions in integers?

Using modern terms one can ask if there exists a program taking coefficients of a polynomial equation as input and producing "yes" or "no" answer to the question "Are there integer solutions?".

This problem became known as Hilbert's Tenth Problem

The Answer

This question was answered negatively (with the final piece in place in 1970) in the work of Martin Davis, Hilary Putnam, Julia Robinson and Yuri Matiyasevich. Actually a much stronger result was proved. It was shown that the recursively enumerable subsets of $\mathbb{Z}$ are the same as the Diophantine subsets of $\mathbb{Z}$.

Recursive and Recursively Enumerable Subsets of $\mathbb{Z}$

Recursive Sets

A set $A \subseteq \mathbb{Z}^m$ is called recursive or decidable if there is an algorithm (or a computer program) to determine the membership in the set.

Recursively Enumerable Sets

A set $A \subseteq \mathbb{Z}^m$ is called recursively enumerable if there is an algorithm (or a computer program) to list the set.

Theorem

There exist recursively enumerable sets which are not recursive.

Diophantine Sets

A subset $A \subset \mathbb{Z}^m$ is called Diophantine over $\mathbb{Z}$ if there exists a polynomial $p(T_1, \ldots T_m, X_1, \ldots, X_k)$ with rational integer coefficients such that for any element $(t_1, \ldots, t_m) \in \mathbb{Z}^m$ we have that

$$\exists x_1, \ldots, x_k \in \mathbb{Z} : p(t_1, \ldots, t_m, x_1, \ldots, x_k) = 0$$

$$\Updownarrow$$

$$(t_1, \ldots, t_m) \in A.$$

In this case we call $p(T_1, \ldots, T_m, X_1, \ldots, X_k)$ a Diophantine definition of A over $\mathbb{Z}$.

Corollary

There are undecidable Diophantine subsets of $\mathbb{Z}$.

Existence of Undecidable Diophantine Sets Implies No Algorithm

Suppose $A \subset \mathbb{Z}$ is an undecidable Diophantine set with a Diophantine definition $P(T, X_1, \ldots, X_k)$. Assume also that we have an algorithm to determine existence of integer solutions for polynomials. Now, let $a \in \mathbb{Z}_{>0}$ and observe that $a \in A$ iff $P(a, X_1, \ldots, X_K) = 0$ has solutions in $\mathbb{Z}^k$. So if can answer Hilbert's question effectively, we can determine the membership in A effectively.

Diophantine Sets Are Recursively Enumerable

It is not hard to see that Diophantine sets are recursively enumerable. Given a polynomial $p(T, \bar{X})$ we can effectively list all $t \in \mathbb{Z}$ such that $p(T, \bar{X}) = 0$ has a solution $\bar{x} \in \mathbb{Z}^k$ in the following fashion. Using a recursive listing of $\mathbb{Z}^{k+1}$, we can plug each $(k+1)$-tuple into $p(T, \bar{X})$ to see if the value is 0. Each time we get a zero we add the first element of the $(k+1)$-tuple to the t-list.

A Simple Example of a Diophantine Set over $\mathbb{Z}$

The set of even integers

$$\{t \in \mathbb{Z} | \exists w \in \mathbb{Z} : t = 2w\}$$

To construct more complicated examples we need to establish some properties of Diophantine sets.

Intersections and Unions of Diophantine Sets

Lemma

Intersections and unions of Diophantine sets are Diophantine.

Proof.

Suppose $P_1(T, \bar{X}), P_2(T, \bar{Y})$ are Diophantine definitions of subsets A_1 and A_2 of $\mathbb{Z}$ respectively over $\mathbb{Z}$. Then

$$P_1(T, \bar{X})P_2(T, \bar{Y})$$

is a Diophantine definition of $A_1 \cup A_2$, and

$$P_1^2(T, \bar{X}) + P_2^2(T, \bar{Y})$$

is a Diophantine definition of $A_1 \cap A_2$. □

One vs. Infinitely Many

Replacing Finitely Many by One

- We can let Diophantine definitions consist of several equations without changing the nature of the relation.
- Any finite system of equations over $\mathbb{Z}$ can be effectively replaced by a single polynomial equation over $\mathbb{Z}$ with the identical $\mathbb{Z}$-solution set.
- The statements above remain valid if we replace $\mathbb{Z}$ by any recursive integral domain R whose fraction field is not algebraically closed.

More Complicated Diophantine Definitions

The set of non-zero integers has the following Diophantine definition:

$$\{t \in \mathbb{Z} | \exists x, u, v \in \mathbb{Z} : (2u-1)(3v-1) = tx\}$$

Proof.

If $t = 0$, then either $2u - 1 = 0$ or $3v - 1 = 0$ has a solution in $\mathbb{Z}$, which is impossible.
Suppose now $t \neq 0$. Write $t = t_2 t_3$, where t_2 is odd and $t_3 \not\equiv 0 \mod 3$. Then since $(t_2, 2) = 1$ and $(t_3, 3) = 1$, there exist $u, v, x_2, x_3 \in \mathbb{Z}$ such that $2u - 1 = t_2 x_2 \wedge 2v - 1 = t_3 x_3$. □

The set of non-negative integers

From Lagrange's Theorem we get the following representation of non-negative integers:

$$\{t \in \mathbb{Z} | \exists x_1, x_2, x_3, x_4 : t = x_1^2 + x_2^2 + x_3^2 + x_4^2\}$$

A General Question

A Question about an Arbitrary Recursive Ring R

Is there an algorithm, which if given an arbitrary polynomial equation in several variables with coefficients in R, can determine whether this equation has solutions in R?

The most prominent open questions are probably the decidability of HTP for $R = \mathbb{Q}$ and R equal to the ring of integers of an arbitrary number field.

Undecidability of HTP over $\mathbb{Q}$ Implies Undecidability of HTP for $\mathbb{Z}$

Indeed, suppose we knew how to determine whether solutions exist over $\mathbb{Z}$. Let $Q(x_1, \ldots, x_k)$ be a polynomial with rational coefficients. Then

$$\exists x_1, \ldots, x_k \in \mathbb{Q} : Q(x_1, \ldots, x_k) = 0$$

$$\Updownarrow$$

$$\exists y_1, \ldots, y_k, z_1, \ldots, z_k \in \mathbb{Z} : Q(\frac{y_1}{z_1}, \ldots, \frac{y_k}{z_k}) = 0 \wedge z_1 \ldots z_k \neq 0.$$

So decidability of HTP over $\mathbb{Z}$ would imply the decidability of HTP over $\mathbb{Q}$.

Using Diophantine Definitions to Solve the Problem

Lemma

Let R be a recursive ring of characteristic 0 such that $\mathbb{Z}$ has a Diophantine definition $p(T, \bar{X})$ over R. Then HTP is not decidable over R.

Proof.

Let $h(T_1, \ldots, T_l)$ be a polynomial with rational integer coefficients and consider the following system of equations.

$$\begin{cases} h(T_1, \ldots, T_l) = 0 \\ p(T_1, \bar{X}_1) = 0 \\ \ldots \\ p(T_l, \bar{X}_l) = 0 \end{cases} \tag{1}$$

It is easy to see that $h(T_1, \ldots, T_l) = 0$ has solutions in $\mathbb{Z}$ iff (1) has solutions in R. Thus if HTP is decidable over R, it is decidable over $\mathbb{Z}$. □

The Plan

So to show that HTP is undecidable over $\mathbb{Q}$ we just need to construct a Diophantine definition of $\mathbb{Z}$ over $\mathbb{Q}$!!!

A Conjecture of Barry Mazur

The Conjecture on the Topology of Rational Points

Let V be any variety over $\mathbb{Q}$. Then the topological closure of $V(\mathbb{Q})$ in $V(\mathbb{R})$ possesses at most a finite number of connected components.

A Nasty Consequence

There is no Diophantine definition of $\mathbb{Z}$ over $\mathbb{Q}$.

Actually if the conjecture is true, no infinite and discrete (in the archimedean topology) set has a Diophantine definition over $\mathbb{Q}$.

Another Plan: Diophantine Models

What is a Diophantine Model of $\mathbb{Z}$?

Let R be a recursive ring whose fraction field is not algebraically closed and let $\phi : \mathbb{Z} \longrightarrow R$ be a recursive injection mapping Diophantine sets of $\mathbb{Z}$ to Diophantine sets of R. Then ϕ is called a Diophantine model of $\mathbb{Z}$ over R.

Sending Diophantine Sets to Diophantine Sets Makes the Map Recursive

Actually the recursiveness of the map will follow from the fact that the ϕ-image of the graph of addition is Diophantine. Indeed, if the ϕ-image of the graph of addition is Diophantine, it is recursively enumerable. So we have an effective listing of the set

$$D_+ = \{(\phi(m), \phi(n), \phi(m+n)), m, n \in \mathbb{Z}\}.$$

Assume we have computed $\phi(k-1)$. Now start listing D_+ until we come across a triple whose first two entries are $\phi(k-1)$ and $\phi(1)$. Then third element of the triple must be $\phi(k)$.

Making Addition and Multiplication Diophantine is Enough

It is enough to require that the ϕ-images of the graphs of $\mathbb{Z}$-addition and $\mathbb{Z}$-multiplication are Diophantine over R. For example, consider the ϕ image of a set

$$D = \{t \in \mathbb{Z} | \exists x \in \mathbb{Z} : t = x^2 + x\}$$

Let $D_\times$ be the graph of multiplication and let D_+ be the graph of addition. Then by assumption $\phi(D_\times)$ and $\phi(D_+)$ are Diophantine sets with R-Diophantine definitions $F_+(A, B, C, \bar{Y})$ and $F_x(A, B, C, \bar{Z})$ respectively. Thus, we have that $T \in \phi(D)$ iff $\exists W, X \in R$ such that $(W, X, T) \in \phi(D_+)$ and $(X, X, W) \in \phi(D_\times)$. Using Diophantine definitions we can rephrase this in the following manner: $T \in \phi(D)$ iff there exist $W, X, \bar{Y}, \bar{Z}$ in R such that

$$\begin{cases} F_+(W, X, T, \bar{Y}) = 0 \\ F_\times(X, X, W, \bar{Z}) = 0 \end{cases}$$

Diophantine Model of $\mathbb{Z}$ Implies Undecidability

If R has a Diophantine model of $\mathbb{Z}$, then R has undecidable Diophantine sets. Indeed, let $A \subset \mathbb{Z}$ be an undecidable Diophantine set. Suppose we want to determine whether an integer $n \in A$. Instead of answering this question directly we can ask whether $\phi(n) \in \phi(A)$. By assumption $\phi(n)$ is algorithmically computable. So if $\phi(A)$ is a computable subset of R, we have a contradiction.

So all we need is a Diophantine model of $\mathbb{Z}$ over $\mathbb{Q}$!!!!

A Theorem of Cornelissen and Zahidi

Theorem

If Mazur's conjecture on topology of rational points holds, then there is no Diophantine model of $\mathbb{Z}$ over $\mathbb{Q}$.

The Rings between $\mathbb{Z}$ and $\mathbb{Q}$

A Ring in between

Let $\mathcal{S}$ be a set of (non-archimedean) primes of $\mathbb{Q}$. Let $O_{\mathbb{Q},\mathcal{S}}$ be the following subring of $\mathbb{Q}$.

$$\left\{ \frac{m}{n} : m, n \in \mathbb{Z}, n \neq 0, n \text{ is divisible by primes of } \mathcal{S} \text{ only} \right\}$$

If $\mathcal{S} = \emptyset$, then $O_{\mathbb{Q},\mathcal{S}} = \mathbb{Z}$. If $\mathcal{S}$ contains all the primes of $\mathbb{Q}$, then $O_{\mathbb{Q},\mathcal{S}} = \mathbb{Q}$. If $\mathcal{S}$ is finite, we call the ring small. If $\mathcal{S}$ is infinite, we call the ring large.

Example of a Small Ring not Equal to $\mathbb{Z}$

$$\{ \frac{m}{3^a 5^b} : m \in \mathbb{Z}, a, b \in \mathbb{Z}_{>0} \}$$

Small Subrings of Number Fields

Theorem

Let K be a number field. Let $\mathfrak{p}$ be a non-archimedean prime of K. Then the set of elements of K integral at $\mathfrak{p}$ is Diophantine over K. (Julia Robinson and others)

Theorem

Let K be a number field. Let $\mathcal{S}$ be any set of non-archimedean primes of K. Then the set of non-zero elements of $O_{K,\mathcal{S}}$ is Diophantine over $O_{K,\mathcal{S}}$. (Denef, Lipshitz)

Corollary

- *$\mathbb{Z}$ has a Diophantine definition over the small subrings of $\mathbb{Q}$.*
- *HTP is undecidable over the small subrings of $\mathbb{Q}$.*

Large Subrings of Number Fields

Theorem

Let K be a totally real number field or an extension of degree 2 of a totally real number field, and let $\varepsilon > 0$ be given. Then there exists a set $\mathcal{S}$ of non-archimedean primes of K such that

- *The natural density of $\mathcal{S}$ is greater $1 - \frac{1}{[K:\mathbb{Q}]} - \varepsilon$.*
- *$\mathbb{Z}$ is a Diophantine subset of $O_{K,\mathcal{S}}$.*
- *HTP is undecidable over $O_{K,\mathcal{S}}$.*

Note that this result says nothing about large subrings of $\mathbb{Q}$.

Ring Version of Mazur's Conjecture

An Easier Question?

Let K be a number field and let $\mathcal{W}$ be a set of non-archimedean primes of K. Let V be any affine algebraic set defined over K. Let $\overline{V(O_{K,\mathcal{W}})}$ be the topological closure of $V(O_{K,\mathcal{W}})$ in $\mathbb{R}$ if $K \subset \mathbb{R}$ or in $\mathbb{C}$, otherwise. Then how many connected components does $\overline{V(O_{K,\mathcal{W}})}$ have?

The ring version of Mazur's conjecture has the same implication for Diophantine definability and models as its field counterpart. In other words if a ring conjecture holds over a ring R, then no infinite discrete in archimedean topology set has a Diophantine definition over R and $\mathbb{Z}$ has no Diophantine model over R.

Some Remarks Concerning the Ring Version of Mazur's Conjecture

What Happens over Small Rings?

Let $\mathcal{S}$ be a finite set of rational primes. Then we can define integers over $O_{\mathbb{Q},\mathcal{S}}$. In other words there exists a polynomial $P(T, \bar{X})$ such that for $t \in O_{\mathbb{Q},\mathcal{S}}$ we have that $P(t, \bar{X}) = 0$ has a solution $\bar{x}$ in the small ring $O_{\mathbb{Q},\mathcal{S}}$ if and only if $t \in \mathbb{Z}$. Let V be the algebraic set corresponding to the polynomial $P(T, \bar{X})$. Then clearly $\overline{V(O_{\mathbb{Q},\mathcal{S}})}$ has infinitely many connected components because the first coordinate is running through integers.

Remarks Concerning the Ring Version of Mazur's Conjecture, continued

What Happens Near $\mathbb{Q}$?

Let $\mathcal{W}$ be a set of rational primes containing all but finitely many primes. Then $O_{\mathbb{Q},\mathcal{W}}$ has a Diophantine definition over $\mathbb{Q}$. Let $P(T,\bar{X}) = P(T, Y_1, \ldots, Y_m)$ such a Diophantine definition. Suppose now that Mazur's conjecture holds over $\mathbb{Q}$. Let $f(Y_1, \ldots, Y_k)$ be a polynomial over $\mathbb{Q}$ and let $A \subset \mathbb{Q}^k$ be the algebraic set defined by this polynomial. Next consider the following system of equations.

$$\begin{cases} f(Y_1, \ldots, Y_k) = 0 \\ P(Y_1, \bar{X}_1) = 0 \\ \ldots \\ P(Y_k, \bar{X}_k) = 0 \end{cases}$$

This system defines an algebraic set $B \subset \mathbb{Q}^{k+km}$ and therefore, if we assume the conjecture holds, must have finitely many components only in the closure. On the other hand the projection of B on the first k coordinates will produce exactly $A(O_{\mathbb{Q},\mathcal{W}}) = A \cap O_{\mathbb{Q},\mathcal{W}}$. Thus $\overline{A(O_{\mathbb{Q},\mathcal{W}})}$ must have finitely many components only.

A Natural Question

So if we allow finitely many primes in the denominators only, we definitely can have infinitely many components. If we allow all but finitely many primes in the denominators and the conjecture holds, then we will see finitely many components only. So can we produce an example of a ring where infinitely many primes are allowed in the denominator and where we do have an algebraic set with infinitely many components in the closure?

The First "Counterexample"

Let M be a cyclic extension of $\mathbb{Q}$ of prime degree $p > 2$. Let $\mathcal{W}$ be the set of rational primes which do not split in the extension $M/\mathbb{Q}$. Let $\omega_1, \ldots, \omega_p$ be an integral basis of M over $\mathbb{Q}$ and consider the following equation

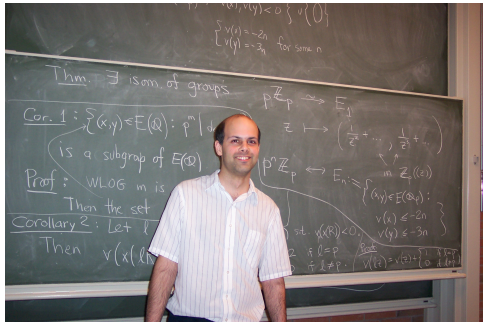
$$\prod_{j=1}^{p} \sum_{i=1}^{p} a_i \sigma_j(\omega_i) = 1,$$

where $\sigma_1 = \mathrm{id}, \ldots, \sigma_p$ are all the embeddings of M into $\mathbb{C}$ and $a_1, \ldots, a_p \in O_{\mathbb{Q},\mathcal{W}}$. Given our choice of $\mathcal{W}$, all the solutions $(a_1, \ldots, a_p)$ are actually in $\mathbb{Z}^p$ and the set of these solutions is infinite. So we have produced a Diophantine definition of a discrete infinite subset of the ring. Thus the ring version of Mazur's conjecture does not hold over this ring. Further the density of the prime set $\mathcal{W}$ is $1 - \frac{1}{p}$. So by selecting a large enough p we can get arbitrarily close to 1.
This construction can be lifted to the totally real number fields and extensions of degree 2 of the totally real number fields.

A More Difficult Question

Can we arrange the density of $\mathcal{W}$ to be 1 and still have a "counterexample" to the conjecture?

The Statement of Poonen's Theorem



Theorem

There exist recursive sets of rational primes $\mathcal{T}_1$ and $\mathcal{T}_2$, both of natural density zero and with an empty intersection, such that for any set $\mathcal{S}$ of rational primes containing $\mathcal{T}_1$ and avoiding $\mathcal{T}_2$, the following hold:

- *There exists an affine curve E defined over $\mathbb{Q}$ such that the topological closure of $E(O_{\mathbb{Q},\mathcal{S}})$ in $E(\mathbb{R})$ is an infinite discrete set. Thus the ring version of Mazur's conjecture does not hold for $O_{\mathbb{Q},\mathcal{S}}$.*
- *$\mathbb{Z}$ has a Diophantine model over $O_{\mathbb{Q},\mathcal{S}}$.*
- *Hilbert's Tenth Problem is undecidable over $O_{\mathbb{Q},\mathcal{S}}$.*

A Proof Overview

The proof of the theorem relies on the existence of an elliptic curve E defined over $\mathbb{Q}$ such that the following conditions are satisfied.

- $E(\mathbb{Q})$ is of rank 1. (For the purposes of our discussion we will assume the torsion group is trivial.)
- $E(\mathbb{R}) \cong \mathbb{R}/\mathbb{Z}$ as topological groups.
- E does not have complex multiplication.

Proof Steps

Fix an affine Weierstrass equation for E of the form

$$y^2 = x^3 + a_2x^2 + a_4x + a_6.$$

1. Let P be any point of infinite order. Show that there exists a computable sequence of rational primes $\ell_1 < \ldots < \ell_n < \ldots$ such that $[l_j]P = (x_{\ell_j}, y_{\ell_j})$, and for all $j \in \mathbb{Z}_{>0}$, we have that $|y_{\ell_j} - j| < 10^{-j}$.
2. Prove the existence of infinite sets $\mathcal{T}_1$ and $\mathcal{T}_2$, as described in the statement of the theorem, such that for any set $\mathcal{S}$ of rational primes containing $\mathcal{T}_1$ and disjoint from $\mathcal{T}_2$, we have that
$$E(O_{\mathbb{Q},\mathcal{S}}) = \{[\pm\ell_j]P\} \cup \{ \text{ finite set } \}.$$
3. Note that $\{y_{\ell_j}\}$ is an infinite discrete Diophantine set over the ring in question, and thus is a counterexample to Mazur's conjecture for the ring $O_{\mathbb{Q},\mathcal{S}}$.
4. Show that $\{y_{\ell_j}\}$ is a Diophantine model of $\mathbb{Z}_{>0}$ over $\mathbb{Q}$.

Constructing a Model of $\mathbb{Z}_{>0}$ using y_{l_j}'s, I

We claim that $\phi : j \longrightarrow y_{\ell_j}$ is a Diophantine model of $\mathbb{Z}_{>0}$. In other words we claim that ϕ is a recursive injection and the following sets are Diophantine:

$$D+ = \{(y_{\ell_i}, y_{\ell_j}, y_{\ell_k}) \in D^3 : k = i + j, k, i, j \in \mathbb{Z}_{>0}\}$$

and

$$D_2 = \{(y_{\ell_i}, y_{\ell_k}) \in D^2 : k = i^2, i \in \mathbb{Z}_{>0}\}.$$

(Note that if $D+$ and D_2 are Diophantine, then $D_\times = \{(y_{\ell_i}, y_{\ell_j}, y_{\ell_k}) \in D^3 : k = ij, k, i, j \in \mathbb{Z}_{>0}\}$ is also Diophantine since $xy = \frac{1}{2}((x + y)^2 - x^2 - y^2.)$

Constructing a Model of $\mathbb{Z}_{>0}$ Using y_{ℓ_j}'s, II

Theorem

The set positive numbers is Diophantine over $\mathbb{Q}$. (Lagrange)

Sums and Squares Are Diophantine

It is easy to show that

$$k = i + j \Leftrightarrow |y_{\ell_i} + y_{\ell_j} - y_{\ell_k}| < 1/3.$$

and with the help of Lagrange this makes D_+ Diophantine. Similarly we have that

$$k = i^2 \Leftrightarrow |y_{\ell_i}^2 - y_{\ell_k}| < 2/5,$$

implying that D_2 is Diophantine.

Arranging to Get Close to Positive Integers

The fact that for any sequence $\{\varepsilon_j\} \subset \mathbb{R}_{>0}$, we can construct a prime sequence $\{\ell_j\}$ with $|y_{\ell_j} - j| < \varepsilon_j$ follows from a result of Vinogradov.

Theorem

Let $\alpha \in \mathbb{R} \setminus \mathbb{Q}$. Let $J \subseteq [0,1]$ be an interval. Let $\mathcal{P}(\mathbb{Q})$ be the set of all rational primes of $\mathbb{Q}$. Then the natural density of the set of primes

$$\{\ell \in \mathcal{P}(\mathbb{Q}) : (\ell\alpha \mod 1) \in J\}$$

is equal to the length of J.

From this theorem we obtain the following corollary.

Corollary

Let E be an elliptic curve defined over $\mathbb{Q}$ such that $E(\mathbb{R}) \cong \mathbb{R}/\mathbb{Z}$ as topological groups. Let P be any point of infinite order. Then for any interval $J \subset \mathbb{R}$ whose interior is non-empty, the set $\{\ell \in \mathcal{P}(\mathbb{Q}) | y([\ell]P) \in J\}$ has positive natural density.

Getting Rid of Undesirable Points I.

The Primes in the Denominator.

The next issue which needs to be considered is selecting primes for $\mathcal{S}$ so that $E(O_{\mathbb{Q},\mathcal{S}})$ essentially consists of $\{[\pm\ell_j]P, j \in \mathbb{Z}_{>0}\}$. This part depends on the following key facts.

- Let p be a rational prime outside a finite set of primes which depends on the choice of the curve and the Weierstrass equation. Then for non-zero integers m, n such that $m|n$, if p occurs in the reduced denominators of $(x_m, y_m) = [m]P$, then p occurs in the reduced denominators of $(x_n, y_n) = [n]P$.
- If m, n are as above and are large enough with $n > m$, then there exists a prime q which occurs in the reduced denomiantors of (x_n, y_n) but not in the reduced denominators of (x_m, y_m).
- If $(m, n) = 1$ then the set of primes which can occur in denominators of both pairs is finite and does not depend on m or n.

Getting Rid of Undesirable Points II.

Suppose we have constructed a sequence $\{\ell_j\}$ as above and for any $\ell \notin \{\ell_j\}$ we want to make sure that the point $[\ell]P \notin E(O_{\mathbb{Q},\mathcal{S}})$. From the previous slide we know that for all sufficiently large ℓ it is the case that (x_ℓ, y_ℓ) will have at least one prime in their reduced denominators which does not occur in the reduced denominators of (x_{ℓ_i}, y_{ℓ_i}) for any i. Call the biggest such prime p_ℓ. If p_ℓ is not in $\mathcal{S}$ then not only $[\ell]P \notin E(O_{\mathbb{Q},\mathcal{S}})$ but for any $m \equiv 0 \mod \ell$ we have that $[m]P \notin E(O_{\mathbb{Q},\mathcal{S}})$.

We also need to make sure that points $[\ell_i\ell_j]P$ and their multiples do not appear in $E(O_{\mathbb{Q},\mathcal{S}})$. Fortunately, again from the slide above, for all sufficiently ℓ_i the reduced denominators of $(x_{\ell_i\ell_j}, y_{\ell_i\ell_j})$ will have at least one prime $p_{\ell_i\ell_j}$ not occurring in the reduced denominators of any (x_{ℓ_k}, y_{ℓ_k}). Hence if we remove all primes $p_{\ell_i\ell_j}$ from $\mathcal{S}$ we will exclude almost all the points of the form $[\ell_i\ell_j]P$ and their multiples from $E(O_{\mathbb{Q},\mathcal{S}})$.

The Messy Part

The most difficult part of the proof is making sure that the sets of primes we have to remove and have to keep are of natural density 0.
For a prime ℓ let p_ℓ be the largest prime dividing the reduced denominators of $(x_\ell, y_\ell) = [\ell]P$. The challenging part here is showing that the set

$$\{p_\ell : \ell \in \mathcal{P}(\mathbb{Q})\}$$

is of natural density 0. One of the required tools is Serre's result on the action of the absolute Galois group on the torsion points of the elliptic curve.

An Advertisement

Hilbert's Tenth Problem: Diophantine Classes and Extensions to Global Fields
Series: New Mathematical Monographs (No. 7)
Alexandra Shlapentokh
East Carolina University
Hardback
(ISBN-13: 9780521833608 | ISBN-10: 0521833604)
Not yet published - available from November 2006
$99.00 (C)