

# HTP over Algebraic Extensions of $\mathbb{Q}$ : Normforms vs. Elliptic Curves

Alexandra Shlapentokh

East Carolina University



Number Theory and Computability, ICMS, June 2007

# A Talk in Two Rounds

## Round II: Elliptic Curves

Today

# Table of Contents

- 1 Diophantine Sets, Definitions and Models**
- 2 Constructing Diophantine Definitions Using Elliptic Curves**
  - The Weak Vertical Method Revisited
  - Some Properties of Elliptic Curves
  - Wish List
- 3 Diophantine Models of Integers over Very Big Rings**
  - A Diophantine Model for a Very Big Subring of  $\mathbb{Q}$
  - A Diophantine Model for a Big Subring of a Number Field
  - Very Big Rings in Infinite Extensions
  - The Final Score

# Diophantine Sets

## Diophantine Sets

Let  $R$  be an integral domain. Then a subset  $A \subset R^m$  is called Diophantine over  $R$  if there exists a polynomial  $p(T_1, \dots, T_m, X_1, \dots, X_k)$  with coefficients in  $R$  such that for any  $m$ -tuple  $(t_1, \dots, t_m) \in R^m$  we have that

$$\exists x_1, \dots, x_k \in R : p(t_1, \dots, t_m, x_1, \dots, x_k) = 0$$



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

In this case we call  $p(T_1, \dots, T_m, X_1, \dots, X_k)$  a **Diophantine definition** of  $A$  over  $R$ .

# Diophantine Sets

## Other Descriptions

Diophantine sets can also be described as **projections of algebraic sets** or sets **existentially definable** in the language of rings.

# Diophantine Subsets of $\mathbb{Z}$

## MDRP Theorem

The recursively enumerable subsets of  $\mathbb{Z}$  are the same as the Diophantine subsets of  $\mathbb{Z}$ .

## Corollary

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

# Diophantine Models

## Definition

Let  $R_1, R_2$  be two recursive rings and let  $\phi : R_1 \longrightarrow R_2^m, m \in \mathbb{Z}_{>0}$  be an injective recursive map sending Diophantine sets of  $R_1^k, k \in \mathbb{Z}_{>0}$  to Diophantine sets of  $R_2^{k+m}$ . Then  $\phi$  is called a **Diophantine model** of  $R_1$  over  $R_2$ .

## Remark

If  $R_1 \subset R_2$  and  $\phi$  is the inclusion map, then  $R_1$  has a Diophantine definition over  $R_2$ . Conversely, if  $R_1$  has a Diophantine definition over  $R_2$ , then  $R_2$  has a Diophantine model of  $R_1$  with  $\phi$  being the inclusion map.

# Diophantine Models and Diophantine Undecidability

## Proposition

*Suppose  $R_1$  has undecidable Diophantine sets and  $R_2$  has a Diophantine model of  $R_1$ . Then  $R_2$  also has undecidable Diophantine sets.*

## Corollary

*If  $R$  is a countable ring with a Diophantine model of  $\mathbb{Z}$ , then  $R$  has undecidable Diophantine sets and therefore HTP is unsolvable over  $R$ .*

## Remark

*Most of the known Diophantine undecidability results over algebraic extensions of  $\mathbb{Q}$  are obtained by constructing a Diophantine definition of  $\mathbb{Z}$ . However, there are notable exceptions to this pattern, where a Diophantine model which is not a Diophantine definition is constructed.*

# The Weak Vertical Method

## The Main Idea

If an *element above* is equivalent to an *element below* modulo sufficiently *large element below*, then the *element above* is really *below*.

# A Generic Application Instance of WVM

## Proposition

Let  $K/F$  be a number field extension with a basis  $\Lambda = \{1, \alpha, \dots, \alpha^{m-1}\} \subset \mathcal{O}_K$ . Let  $x \in \mathcal{O}_K, w, y \in \mathcal{O}_F$ . Assume that  $y$  is not zero and is not an integral unit. Let  $c \in \mathbb{Z}_{>0}$  be fixed, let  $n = [K : \mathbb{Q}]$ . Suppose that the following equalities and inequalities hold.

$$x = \sum_{i=0}^{m-1} a_i \alpha^i, a_i \in F, \quad (1)$$

$$|\mathbf{N}_{K/\mathbb{Q}}(Da_i)| \leq |\mathbf{N}_{K/\mathbb{Q}}(y)^c|, i = 1, \dots, m-1 \quad (2)$$

where  $D$  is the discriminant of  $\Lambda$ , and

$$x \equiv w \pmod{y^{2c}}. \quad (3)$$

Then  $x \in \mathcal{O}_F$ .

# A Generic Application of WVM

## Proof.

From (1) and (3), we conclude that

$$x - w = (a_0 - w) + a_1\alpha + \dots + a_{n-1}\alpha^{m-1} \equiv 0 \pmod{y^{2c}}.$$

Thus,

$$\frac{x - w}{y^{2c}} = \frac{a_0 - w}{y^{2c}} + \frac{a_1}{y^{2c}}\alpha + \dots + \frac{a_{m-1}}{y^{2c}}\alpha^{m-1} \in O_K.$$

We have that  $\frac{Da_i}{y^{2c}} \in O_F$ , and therefore  $|\mathbf{N}_{K/\mathbb{Q}}(Da_i)| \geq \mathbf{N}_{K/\mathbb{Q}}(y^{2c})$  or  $|\mathbf{N}_{K/\mathbb{Q}}(a_i)| = 0$ . At the same time from (2) we conclude that

$$|\mathbf{N}_{K/\mathbb{Q}}(Da_i)| \leq |\mathbf{N}_{K/\mathbb{Q}}(y)|^c < \mathbf{N}_{K/\mathbb{Q}}(y)^{2c},$$

since  $y$  is not an integral unit. Hence, for  $i = 1, \dots, m$ , we have that  $|\mathbf{N}_{K/\mathbb{Q}}(a_i)| = 0$ , and therefore  $a_i = 0$ , for  $i = 1, \dots, m - 1$ . Consequently,  $x \in O_F$ . □

# Divisors of Number Field Elements

## Definition

Let  $K$  be a number field and let  $x \in K$ . Let  $\mathcal{P}(K)$  be the set of all non-archimedean primes of  $K$  (ideals of  $O_K$  or non-archimedean valuations of  $K$ ). Then the divisor of  $x$  is

$$\prod_{\mathfrak{p} \in \mathcal{P}(K)} \mathfrak{p}^{\text{ord}_{\mathfrak{p}} x}.$$

Let

$$n(x) = \prod_{\mathfrak{p} \in \mathcal{P}(K), \text{ord}_{\mathfrak{p}} x > 0} \mathfrak{p}^{\text{ord}_{\mathfrak{p}} x},$$

$$d(x) = \prod_{\mathfrak{p} \in \mathcal{P}(K), \text{ord}_{\mathfrak{p}} x < 0} \mathfrak{p}^{-\text{ord}_{\mathfrak{p}} x}.$$

# Integral Divisors

## Definition

Let  $K$  be a number field, let  $\mathcal{A}$  be a finite collection of primes of  $K$ . Let

$$\mathfrak{I} = \prod_{\mathfrak{p} \in \mathcal{A}} \mathfrak{p}^{a(\mathfrak{p})},$$

where  $a(\mathfrak{p}) \geq 0$ . Then  $\mathfrak{I}$  is called an **integral divisor**. Further for  $\mathfrak{p} \in \mathcal{A}$  let  $\text{ord}_{\mathfrak{p}} \mathfrak{I} = a(\mathfrak{p})$ . If  $\mathfrak{p} \notin \mathcal{A}$  then let  $\text{ord}_{\mathfrak{p}} \mathfrak{I} = 0$ . If  $\mathfrak{J}$  is another integral divisor such that for every  $\mathfrak{p} \in \mathcal{P}(K)$  we have that

$$\text{ord}_{\mathfrak{p}} \mathfrak{I} \geq \text{ord}_{\mathfrak{p}} \mathfrak{J},$$

then we will say that  **$\mathfrak{I}$  divides  $\mathfrak{J}$** .

# A variation

## Proposition

Let  $K/F$  be a number field extension with a basis  $\Lambda = \{1, \alpha, \dots, \alpha^{m-1}\} \subset O_K$ . Let  $x \in O_K, y \in O_F, w \in F$ . Assume that  $y$  is not zero and is not an integral unit. Let  $c \in \mathbb{Z}_{>0}$  be fixed, let  $n = [K : \mathbb{Q}]$ . Suppose that the following equalities and inequalities hold.

$$x = \sum_{i=0}^{m-1} a_i \alpha^i, a_i \in F, \quad (4)$$

$$|\mathbf{N}_{K/\mathbb{Q}}(Da_i)| \leq |\mathbf{N}_{K/\mathbb{Q}}(y)^c|, i = 1, \dots, m-1 \quad (5)$$

where  $D$  is the discriminant of  $\Lambda$ , and

$$\mathfrak{n}(y^{2c}) \text{ divides } \mathfrak{n}(x - w). \quad (6)$$

Then  $x \in O_F$ .

## A variation

### Proof.

Let  $\mathcal{A}$  be the set of all primes of  $K$  occurring in  $\mathfrak{n}(y)$ . Observe that for each  $\mathfrak{p} \in \mathcal{A}$  we have that  $\text{ord}_{\mathfrak{p}}(x - w) > 0$ . Thus, by the Strong Approximation Theorem there exists  $v \in O_F$  such that for all  $\mathfrak{p} \in \mathcal{A}$  we have that

$$\text{ord}_{\mathfrak{p}}(w - v) > \text{ord}_{\mathfrak{p}}(w - x).$$

Now observe that

$$\text{ord}_{\mathfrak{p}}(v - x) = \min(\text{ord}_{\mathfrak{p}}(v - w), \text{ord}_{\mathfrak{p}}(w - x)) = \text{ord}_{\mathfrak{p}}(w - x).$$

Thus,  $\mathfrak{n}(y^{2c})$  divides  $\mathfrak{n}(v - x)$  or in other words,

$$x \equiv v \pmod{\mathfrak{n}(y^{2c})}.$$

# How Do You Write Down Divisibility of Numerators and Denominators

Let  $M/K$  be a number field extension. Let  $z \in O_M$ ,  $u, w \in K$  and assume  $\mathfrak{d}(w)$  divides  $\mathfrak{n}(z - u)$ . We need to rewrite this divisibility condition as a Diophantine equation over  $M$ .

First of all, observe that  $\mathfrak{d}(w)$  and  $\mathfrak{d}(u)$  are relatively prime integral divisors. Otherwise for some  $\mathfrak{p}$  occurring in  $\mathfrak{d}(w)$  we have  $\text{ord}_{\mathfrak{p}}(z - u) < 0$ . Therefore, by the Strong Approximation Theorem, we can write  $u = \frac{u_1}{u_2}$ ,  $w = \frac{w_1}{w_2}$ , where  $u_1, u_2, w_1, w_2 \in O_M$ ,  $\mathfrak{d}(w)$  divides  $\mathfrak{n}(w_2)$ , and  $\mathfrak{n}(u_2)$  is relatively prime to  $\mathfrak{n}(w_2)$ . Now consider the following equations:

$$w_1(u_2z - u_1) = w_2v,$$

$$Au_2 + Bw_2 = 1$$

where  $A, B, v \in O_M$ . We claim that these two equations are equivalent to our divisibility condition.

# How Do You Write Down Divisibility of Numerators and Denominators

Suppose these equations are satisfied. Then since  $v \in O_M$  and  $(u_2, w_2) = 1$  we conclude that

$$n\left(\frac{w_2}{w_1}\right) \text{ divides } n\left(z - \frac{u_1}{u_2}\right).$$

Since  $n\left(\frac{w_2}{w_1}\right) = \mathfrak{d}(w)$ , this implies the original divisibility condition. Conversely, let  $u_1, u_2, w_1, w_2$  as described above. We can decompose  $n(w_2)$  into two parts:  $\mathfrak{d}(w)$  and  $\mathfrak{A}$ , the part common with  $n(w_1)$ . Since  $\mathfrak{d}(w)$  divides  $n(u_2z - u_1)$  and  $\mathfrak{A}$  divides  $n(w_1)$  we can conclude that  $n(w_2)$  divides  $n(w_1(u_2z - u_1))$ . Thus the divisor of  $v = \frac{w_1(u_2z - u_1)}{w_2}$  is an integral divisor and therefore this element is in  $O_M$ .

# How to Establish Bounds

## Lemma

Let  $K$  be a number field of degree  $n$ . Let  $x, y \in O_K$ , assume  $y$  is not a unit and  $x(x + \ell_1) \dots (x + \ell_n)$  divides  $y$  in  $O_K$  for some distinct integers  $\ell_1, \dots, \ell_n$ . Then for some positive constant  $c$ , depending on  $K$  and  $\ell_1, \dots, \ell_n$  only, for every  $\sigma$ , embedding of  $K$  into its algebraic closure,  $|\sigma(x)| < |\mathbf{N}_{K/\mathbb{Q}}(y)|^c$ .

## Proof.

Linear Algebra □

## Corollary

Let  $K, x, y$  be as above. Let  $K/F$  be a finite extension and let  $\Lambda = \{1, \alpha, \dots, \alpha^{m-1}\}$  be a basis of  $K$  over  $F$ . Let  $x = \sum_{i=0}^{m-1} a_i \alpha^i$ ,  $a_i \in F$ . Then for some positive constant  $c'$  depending on  $K, \ell_1, \dots, \ell_n$  and  $\Lambda$  only, we have that

$$\mathbf{N}_{K/\mathbb{Q}}(Da_i) < \mathbf{N}_{K/\mathbb{Q}}(y^{c'})$$

## Proof.

More Linear Algebra □

# The Main Ingredient

Let  $M/K$  be a number field extension. We need an elliptic curve  $E$  defined over  $K$  such that  $\text{rank } E(M) = \text{rank } E(K) > 0$ . A Weierstrass equation of this elliptic curve will be the equation whose solutions above are really below. To simplify the discussion we can assume that  $E(K) = E(M)$ .

# Points of Infinite Order

## Notation

- Let  $E$  be an elliptic curve defined over a number field  $K$  and of positive rank over  $K$ .
- Let  $y^2 = x^3 + ax + b$ ,  $a, b \in O_K$  be a fixed Weierstrass equation for this curve.
- Let  $P \in E(K)$  be a point of infinite order.
- Let  $(x_n, y_n)$  be the affine coordinates of  $[n]P$  derived from our fixed Weierstrass equation.
- For  $n \neq 0$  let  $\mathcal{S}_n$  (support of  $[n]P$ ) consist of all  $K$ -primes  $\mathfrak{p}$  such that  $\text{ord}_{\mathfrak{p}} \mathfrak{v}(x_n) > 0$ .
- We will also call a  $K$ -prime “bad” if it ramifies in  $K/\mathbb{Q}$ , or if the reduction of the chosen Weierstrass equation is singular (this includes all primes above 2), or if the coordinates of  $P$  are not integral at the prime.

# How to capture Integers and Establish Divisibility

## Lemma

*There exists  $r \in \mathbb{Z}_{>0}$  such that for all  $k, m \in \mathbb{Z}_{>0}$  we have that  $\mathfrak{d}(x_{rm})$  divides  $n\left(\frac{x_{rm}}{x_{rmk}} - k^2\right)^2$*

## Lemma

*For any integral divisor  $\mathfrak{J}$ , there exists  $r \in \mathbb{Z}_{>0}$  such that for any  $m \in \mathbb{Z}_{>0}$ , it is the case that  $\mathfrak{J}$  divides  $\mathfrak{d}(x_{rm})$ .*

# Setting Up the Equations

## Lemma

Let  $M/K$  be a number field extension. Let  $E$  be an elliptic curve defined over  $K$  and such that  $E(K) = E(M)$  with  $\text{rank } E(K) > 0$ . Let  $y^2 = x^3 + ax + b$  be a fixed Weierstrass equation for  $E$  with  $a, b \in O_K$ . Let  $X = \{x \in K : \exists y \in K, y^2 = x^3 + ax + b\}$ . Let  $z \in O_M$  and assume that the following conditions hold.

$$\left\{ \begin{array}{l} u_1, u_2, u_3 \in X \\ n(z(z + \ell_1) \dots (z + \ell_n)) \text{ divides } \mathfrak{d}(u_1) \\ \mathfrak{d}(u_1^{2^c}) \text{ divides } \mathfrak{d}(u_2) \\ \mathfrak{d}(u_2) \text{ divides } n\left(\frac{u_3}{u_2} - z\right)^2 \end{array} \right. \quad (7)$$

Then  $z \in O_K$ . Conversely, if  $z$  is a square of an integer, the conditions above can be satisfied.

## Remark

*This elliptic curve method can be modified to work for big rings and infinite extensions but the issue of bounds becomes more complicated, especially in the case of infinite extensions, forcing us not to move too far away from totally real extensions.*

# SPR Conjectures

## Theorem

*Let  $M/K$  be a number field extension with  $\text{rank } E(M) = \text{rank } E(K) > 0$ . Then  $O_K$  has a Diophantine definition over  $O_M$ .*

## Conjecture

*Let  $M/K$  be any number field extension. Then there exists an elliptic curve  $E$  defined over  $K$  such that  $\text{rank } E(M) = \text{rank } E(K) > 0$ .*

Note that replacing  $K$  by  $\mathbb{Q}$  results in an equivalent statement.

# SPR Conjectures

## Conjecture

*Let  $M/K$  be any cyclic number field extension. Then there exists an elliptic curve  $E$  defined over  $K$  such that  $\text{rank } E(M) = \text{rank } E(K) > 0$ .*

## Conjecture

*Let  $M/K$  be any Kummer number field extension. Then there exists an elliptic curve  $E$  defined over  $K$  such that  $\text{rank } E(M) = \text{rank } E(K) > 0$ .*

The truth of either of these two conjectures is enough to get a Diophantine definition of  $\mathbb{Z}$  over the ring of integers of any number field.

# SPR Conjectures

First of all it would be enough to show that for any Galois extension  $M$  of  $\mathbb{Q}$  we have a Diophantine definition of  $\mathbb{Z}$  over  $M$ . Secondly, let  $E_1, \dots, E_k$  be all the cyclic subextensions of  $M$ . Observe that  $\bigcap E_i = \mathbb{Q}$  and if we could define existentially all  $O_{E_i}$  over  $O_M$ , we could define also their intersection over  $O_M$ . Finally let  $m = [M : \mathbb{Q}]!$ . Let  $\xi_m$  be a primitive  $m$ -th root of unity and consider defining  $O_{\mathbb{Q}(\xi_m)}$  over  $O_{M(\xi_m)}$ . By an analogous argument we just need to look at cyclic subextensions of  $M(\xi_m)$  containing  $\mathbb{Q}(\xi_m)$ . But given the presence of the relevant root of unity, all of the cyclic extensions will be generated by radicals.

# 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  $S$  of rational primes containing  $\mathcal{T}_1$  and avoiding  $\mathcal{T}_2$ , the following hold:*

- $\mathbb{Z}$  has a Diophantine model over  $O_{\mathbb{Q},S}$ .
- Hilbert's Tenth Problem is undecidable over  $O_{\mathbb{Q},S}$ .

# Diophantine Models of $\mathbb{Z}$

## Definition

Let  $R$  be a recursive ring and let  $\phi : \mathbb{Z} \longrightarrow R$  be a recursive map sending Diophantine sets of  $\mathbb{Z}$  to Diophantine sets of  $R$ . Then  $\phi$  is called a **Diophantine model** of  $\mathbb{Z}$  over  $R$ .

## Remark

*It is enough to map the graphs of addition and multiplication to Diophantine sets. This will automatically insure that all the Diophantine sets are mapped to Diophantine sets and the map is recursive. The last assertion follows from the fact that Diophantine sets are r.e. and from the graph of addition we can recover the map.*

# 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

$$y^2 = x^3 + ax + b.$$

- 1 Show that there exists a computable sequence of rational primes  $\ell_1 < \dots < \ell_n < \dots$  such that  $[\ell_j]P = (x_{\ell_j}, y_{\ell_j})$ , 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 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

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

$$D_+ = \{(y_{l_i}, y_{l_j}, y_{l_k}) \in D^3 : k = i + j, k, i, j \in \mathbb{Z}_{>0}\}$$

and

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

(Note that if  $D_+$  and  $D_2$  are Diophantine, then

$D_\times = \{(y_{l_i}, y_{l_j}, y_{l_k}) \in D^3 : k = ij, k, i, j \in \mathbb{Z}_{>0}\}$  is also Diophantine since  $xy = \frac{1}{2}((x + y)^2 - x^2 - y^2)$ .)

# Constructing a Model of $\mathbb{Z}_{>0}$ Using $y_{\ell_j}$ 's

## 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  $\{\varepsilon_j\} \subset \mathbb{R}_{>0}$ , 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. Then the natural density of the set of primes*

$$\{l \in \mathcal{P}(\mathbb{Q}) : (l\alpha \pmod{1}) \in J\}$$

*is equal to the length of  $J$ .*

# Arranging to Get Close to Positive Integers

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  $\{I \in \mathcal{P}(\mathbb{Q}) \mid y([I]P) \in J\}$  has positive natural density.*

# Getting Rid of Undesirable Points

## 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 properties of elliptic curves.

- If  $m, n \in \mathbb{Z}_{>0}$ , are sufficiently large and  $m|n$ , then  $\mathfrak{d}(x_m)$  divides  $\mathfrak{d}(x_n)$ .
- Let  $\mathcal{S}_n = \{p : \text{ord}_p(\mathfrak{d}(x_m)) > 0\}$ . Then for all sufficiently large  $m$  we have that  $\mathcal{S}_m \subset \mathcal{S}_n$  implies that  $m|n$ .
- If  $m, n \in \mathbb{Z}_{>0}$  are large enough with  $n > m$ , then there exists a prime  $q$  such that  $\text{ord}_q \mathfrak{d}(x_n) > 0$  and  $\text{ord}_q \mathfrak{d}(x_m) = 0$ .
- If  $(m, n) = 1$  then  $\text{GCD}(\mathfrak{d}(x_m), \mathfrak{d}(x_n))$  depends only on  $P$  and not on  $m$  and  $n$ .

# Getting Rid of Undesirable Points

For each sufficiently large prime  $\ell$  let  $p_\ell$  be the largest prime occurring in  $\mathfrak{d}(x_\ell)$  but not in any  $\mathfrak{d}(x_q)$  for  $q < \ell$ . If we remove  $p_\ell$  from  $\mathcal{S}$ , the set of primes allowed in the denominator, then not only  $[\ell]P$  but also all multiples of  $[\ell]P$  will disappear from  $E(O_{\mathbb{Q},\mathcal{S}})$ . At the same time all points of the form  $[m]P$ ,  $(m, \ell) = 1$  will not be affected.

# 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.

In particular it is quite a challenge 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.

# Constructing Model of a Model

## Lemma

*Let  $B = \{2^n + n^2 : n \in \mathbb{Z}_{\geq 1}\}$ . Multiplication admits a positive existential definition in the structure  $\mathcal{Z} := (\mathbb{Z}_{\geq 1}, 1, +, B)$ . (Here  $B$  is considered as a unary predicate.)*

(Y. Matijasevich and B. Poonen (independently).)

# Proof

We can define  $>$  by

$$x > y \iff (\exists z) x = y + z$$

and for fixed  $a \in \mathbb{Z}$ , we have

$$x \neq a \iff (x > a) \vee (a > x),$$

so this predicate is positive existential in  $\mathcal{Z}$ .

For fixed  $c \in \mathbb{Z}_{\geq 1}$ , the function  $x \mapsto cx$  is positive existential, since it can be obtained by repeated addition.

# Proof

Call  $x, y$  *consecutive* if there exists  $n \in \mathbb{Z}_{\geq 1}$  such that  $x = 2^n + n^2$  and  $y = 2^{n+1} + (n+1)^2$ . The set of such  $(x, y)$  is positive existential in  $\mathcal{Z}$  since it equals  $\{(x, y) \in B^2 : x < y < 3x\}$ . Next

$\{((2y-z)-(2x-y), 2x-y) : x, y \text{ are consec. and } y, z \text{ are consec.}\}$

equals the set  $T := \{(2n-1, n^2-2n-1) : n \in \mathbb{Z}_{\geq 1}\}$ . We have

$$(u = v^2) \wedge (v > 0) \iff (2v-1, u-2v-1) \in T.$$

Call this relation  $P(u, v)$ . Then

$$u = v^2 \iff P(u, v) \vee P(u, -v) \vee ((u = 0) \wedge (v = 0)),$$

$$u = vw \iff (v+w)^2 = v^2 + w^2 + 2u,$$

so we can construct a positive existential definition of multiplication.

# The Construction

Fix “good”  $K$ -primes  $\mathfrak{p}, \mathfrak{q}$  of degree 1 such that neither  $\mathfrak{p}$  nor  $\mathfrak{q}$  divides  $y_1 = y(P)$ , and such that the underlying primes  $p, q \in \mathcal{P}(\mathbb{Q})$  are distinct and odd. Let  $M = pq\#E(\mathbb{F}_{\mathfrak{p}})\#E(\mathbb{F}_{\mathfrak{q}})$ , where  $F_{\mathfrak{p}}$  and  $F_{\mathfrak{q}}$  are residue fields of  $\mathfrak{p}$  and  $\mathfrak{q}$  respectively which are under our assumptions are finite fields of size  $p$  and  $q$  respectively. We construct a sequence  $\{\ell_i\}$  of rational primes satisfying (among others) the following conditions:

- 1  $\ell_i \equiv 1 \pmod{M}$ ,
- 2 the highest power of  $p$  dividing  $(\ell_i - 1)/M$  is  $p^i$ ,
- 3  $q$  divides  $(\ell_i - 1)/M$  if and only if  $i \in B$ .

## Some Important Facts

### Proposition

- *Let  $K$  be a number field, let  $\mathfrak{p}$  be a  $K$ -prime. Then the set  $\{x \in K : \text{ord}_{\mathfrak{p}} x \geq 0\}$  is Diophantine over  $K$ . (Julia Robinson and others)*
- *Let  $K$  be a number field, let  $\mathcal{W}$  be any set of  $K$ -primes. Then the set  $\{x \in O_{K,\mathcal{W}} : x \neq 0\}$  is Diophantine over  $O_{K,\mathcal{W}}$ . (Denef, Lipshitz)*

## Lemma

If  $m \in \mathbb{Z}_{\geq 1}$ , then

$$\text{ord}_p(x_{mM+1} - x_1) = \text{ord}_p(x_{M+1} - x_1) + \text{ord}_p m.$$

## Proposition

Let  $S$  be a set of  $K$  containing the primes in  $\bigcup_{i=1}^{\infty} \mathcal{S}_{l_i}$  and omitting at least one prime from  $\mathcal{S}_\ell$  for  $\ell \notin \{l_i\}$ . Let  $A := \{x_{l_1}, x_{l_2}, \dots\}$ .

Then  $A$  is a Diophantine model of  $\mathcal{Z}$  over  $O_{K,S}$ , via the bijection  $\phi: \mathbb{Z}_{\geq 1} \rightarrow A$  taking  $i$  to  $x_{l_i}$ .

# Highlights of the Proof

The set  $A$  is Diophantine over  $\mathcal{O}_{K,S}$  by construction. We have

$$\begin{aligned} i \in B &\iff q \text{ divides } (\ell_i - 1)/M \\ &\iff \text{ord}_q(x_{\ell_i} - x_1) > \text{ord}_q(x_{M+1} - x_1), \end{aligned}$$

Thus the subset  $\phi(B)$  of  $A$  is Diophantine over  $\mathcal{O}_{K,S}$ .

Finally, for  $i \in \mathbb{Z}_{\geq 1}$ , we have that  $\text{ord}_p(x_{\ell_i} - x_1) = c + i$ , where the integer  $c = \text{ord}_p(x_{M+1} - x_1)$  is independent of  $i$ . Therefore, for  $i, j, k \in \mathbb{Z}_{\geq 1}$ , we have

$$i+j = k \iff \text{ord}_p(x_{\ell_i} - x_1) + \text{ord}_p(x_{\ell_j} - x_1) = \text{ord}_p(x_{\ell_k} - x_1) + c.$$

It follows that the graph of  $+$  corresponds under  $\phi$  to a subset of  $A^3$  that is Diophantine over  $\mathcal{O}_{K,S}$ .

Thus  $A$  is a Diophantine model of  $\mathcal{Z}$  over  $\mathcal{O}_{K,S}$ .

# Another Wish List

## Conjecture

*Every number field has a rank one elliptic curve.*

## Question

Let  $K$  be a number field, let  $E$  be an elliptic curve defined over  $K$ . Let  $P, Q \in E(K)$  be two independent points of infinite order. Then how does  $\mathcal{S}([n]P) \cap \mathcal{S}([m]Q)$  depend on  $m, n$ ? (Here  $\mathcal{S}([n]P)$  is the support of  $[n]P$ .)

# Rank One Elliptic Curves in Infinite Extensions

If  $K_\infty$  is an algebraic extension of  $\mathbb{Q}$  and there exists an elliptic curve  $E$  defined over  $K_\infty$  such that  $E(K_\infty)$  is of rank one and finitely generated, then the number field results lift to  $K_\infty$  provided we can define order. In other words, let  $K$  be a number field containing the coefficients of a chosen Weierstrass equation and the coordinates of the generators of  $E(K_\infty)$ . Let  $\mathfrak{p}, \mathfrak{q}$  be two primes of  $K$  as above. We need the following sets to be definable over  $K_\infty$ :

$$\{x \in K_\infty : x \text{ is integral at } \mathfrak{p}\}$$

and

$$\{x \in K_\infty : x \text{ is integral at } \mathfrak{q}\}$$

This can be done if residue fields of factors of  $\mathfrak{p}$  (resp.  $\mathfrak{q}$ ) do not become algebraically closed in  $K_\infty$  and if ramification for  $\mathfrak{p}$  (resp.  $\mathfrak{p}$ ) is bounded.

The elliptic curve method does not seem to have any built in limitations unlike the normform method, but the progress is blocked by very difficult number-theoretic conjectures.