Hilbert 10 via additive combinatorics I

Peter Koymans
Utrecht University

Utrecht University

Number Theory Web Seminar

15 May 2025

History

At the 1900 mathematical conference in Paris, Hilbert introduced his famous list of 23 problems.

History

At the 1900 mathematical conference in Paris, Hilbert introduced his famous list of 23 problems.

Question (Hilbert's tenth problem)

Given a Diophantine equation with any number of unknown quantities and with rational integral numerical coefficients: To devise a process according to which it can be determined in a finite number of operations whether the equation is solvable in rational integers.

History

At the 1900 mathematical conference in Paris, Hilbert introduced his famous list of 23 problems.

Question (Hilbert's tenth problem)

Given a Diophantine equation with any number of unknown quantities and with rational integral numerical coefficients: To devise a process according to which it can be determined in a finite number of operations whether the equation is solvable in rational integers.

In modern terms: does there exist an algorithm such that:
Input: a polynomial $p \in \mathbb{Z}[x_1, \ldots, x_n]$.
Output: "YES" if there is an integer solution $(a_1, \ldots, a_n) \in \mathbb{Z}^n$ with $p(a_1, \ldots, a_n) = 0$, "NO" otherwise.

Diophantine and listable sets

Definition (Diophantine set)

We say that a subset $S \subseteq \mathbb{Z}^n$ is Diophantine if there exists a polynomial $p(x_1, \ldots, x_n, y_1, \ldots, y_m) \in \mathbb{Z}[\mathbf{x}, \mathbf{y}]$ such that

$$S = \{\mathbf{x} \in \mathbb{Z}^n : \exists \mathbf{y} \in \mathbb{Z}^m \text{ such that } p(\mathbf{x}, \mathbf{y}) = 0\}.$$

Diophantine and listable sets

Definition (Diophantine set)

We say that a subset $S \subseteq \mathbb{Z}^n$ is Diophantine if there exists a polynomial $p(x_1, \ldots, x_n, y_1, \ldots, y_m) \in \mathbb{Z}[\mathbf{x}, \mathbf{y}]$ such that

$$S = \{\mathbf{x} \in \mathbb{Z}^n : \exists \mathbf{y} \in \mathbb{Z}^m \text{ such that } p(\mathbf{x}, \mathbf{y}) = 0\}.$$

Definition (Listable set)

We say that a subset $S \subseteq \mathbb{Z}^n$ is listable (or recursively enumerable) if there is an algorithm that enumerates S when left running forever.

Diophantine and listable sets

Definition (Diophantine set)

We say that a subset $S \subseteq \mathbb{Z}^n$ is Diophantine if there exists a polynomial $p(x_1, \ldots, x_n, y_1, \ldots, y_m) \in \mathbb{Z}[\mathbf{x}, \mathbf{y}]$ such that

$$S = \{\mathbf{x} \in \mathbb{Z}^n : \exists \mathbf{y} \in \mathbb{Z}^m \text{ such that } p(\mathbf{x}, \mathbf{y}) = 0\}.$$

Definition (Listable set)

We say that a subset $S \subseteq \mathbb{Z}^n$ is listable (or recursively enumerable) if there is an algorithm that enumerates S when left running forever.

Theorem (MRDP, 1970)

A subset $S \subseteq \mathbb{Z}^n$ is Diophantine if and only if it is listable.

Diophantine and listable sets

Definition (Diophantine set)

We say that a subset $S \subseteq \mathbb{Z}^n$ is Diophantine if there exists a polynomial $p(x_1, \ldots, x_n, y_1, \ldots, y_m) \in \mathbb{Z}[\mathbf{x}, \mathbf{y}]$ such that

$$S = \{\mathbf{x} \in \mathbb{Z}^n : \exists \mathbf{y} \in \mathbb{Z}^m \text{ such that } p(\mathbf{x}, \mathbf{y}) = 0\}.$$

Definition (Listable set)

We say that a subset $S \subseteq \mathbb{Z}^n$ is listable (or recursively enumerable) if there is an algorithm that enumerates S when left running forever.

Theorem (MRDP, 1970)

A subset $S \subseteq \mathbb{Z}^n$ is Diophantine if and only if it is listable.

Corollary (Hilbert's tenth problem)

Hilbert's tenth problem is undecidable, i.e. there is no algorithm that can decide whether a polynomial $p \in \mathbb{Z}[x_1, \ldots, x_n]$ has a zero or not.

The MRDP theorem

The MRDP theorem is historically proven by three major results:

The MRDP theorem

The MRDP theorem is historically proven by three major results:

- In 1950, Julia Robinson proves that "J.R." implies that exponentiation is Diophantine, i.e.

$$\{(a, b, c) \in \mathbb{Z}^3 : a = b^c\}$$

  is Diophantine. Pell's equation is a key ingredient.

The MRDP theorem

The MRDP theorem is historically proven by three major results:

- In 1950, Julia Robinson proves that "J.R." implies that exponentiation is Diophantine, i.e.

$$\{(a, b, c) \in \mathbb{Z}^3 : a = b^c\}$$

  is Diophantine. Pell's equation is a key ingredient.
- In 1961, Davis–Putnam–Robinson prove that exponential Diophantine sets are precisely the listable sets.

The MRDP theorem

The MRDP theorem is historically proven by three major results:

- In 1950, Julia Robinson proves that "J.R." implies that exponentiation is Diophantine, i.e.

$$\{(a, b, c) \in \mathbb{Z}^3 : a = b^c\}$$

  is Diophantine. Pell's equation is a key ingredient.
- In 1961, Davis–Putnam–Robinson prove that exponential Diophantine sets are precisely the listable sets.

  In particular, "J.R." implies that a set is Diophantine if and only if it is listable, and Hilbert's tenth problem is undecidable.

The MRDP theorem

The MRDP theorem is historically proven by three major results:

- In 1950, Julia Robinson proves that "J.R." implies that exponentiation is Diophantine, i.e.

$$\{(a, b, c) \in \mathbb{Z}^3 : a = b^c\}$$

  is Diophantine. Pell's equation is a key ingredient.
- In 1961, Davis–Putnam–Robinson prove that exponential Diophantine sets are precisely the listable sets.

  In particular, "J.R." implies that a set is Diophantine if and only if it is listable, and Hilbert's tenth problem is undecidable.
- In 1970, Matiyasevich proves "J.R.", thus settling Hilbert's tenth problem. Pell's equation is a key ingredient in this step as well.

The MRDP theorem

The MRDP theorem is historically proven by three major results:

- In 1950, Julia Robinson proves that "J.R." implies that exponentiation is Diophantine, i.e.

$$\{(a, b, c) \in \mathbb{Z}^3 : a = b^c\}$$

  is Diophantine. Pell's equation is a key ingredient.
- In 1961, Davis–Putnam–Robinson prove that exponential Diophantine sets are precisely the listable sets.

  In particular, "J.R." implies that a set is Diophantine if and only if it is listable, and Hilbert's tenth problem is undecidable.
- In 1970, Matiyasevich proves "J.R.", thus settling Hilbert's tenth problem. Pell's equation is a key ingredient in this step as well.

Matiyasevich asks in the 1970s: what about other rings?

Finitely generated rings

Definition

For a finitely generated ring R, we have natural analogues of "Hilbert's tenth problem", "Diophantine set" and "listable set" by replacing all occurrences of $\mathbb{Z}$ by R.

Finitely generated rings

Definition

For a finitely generated ring R, we have natural analogues of "Hilbert's tenth problem", "Diophantine set" and "listable set" by replacing all occurrences of $\mathbb{Z}$ by R.

Theorem (Mazur–Rubin, 2009)

Assume BSD. Let R be a finitely generated ring with $|R| = \infty$. Then Hilbert's tenth problem is undecidable over R.

Finitely generated rings

Definition

For a finitely generated ring R, we have natural analogues of "Hilbert's tenth problem", "Diophantine set" and "listable set" by replacing all occurrences of $\mathbb{Z}$ by R.

Theorem (Mazur–Rubin, 2009)

Assume BSD. Let R be a finitely generated ring with $|R| = \infty$. Then Hilbert's tenth problem is undecidable over R.

Theorem (K.–Pagano, 2024)

Let R be a finitely generated ring with $|R| = \infty$. Then Hilbert's tenth problem is undecidable over R.

Finitely generated rings

Definition

For a finitely generated ring R, we have natural analogues of "Hilbert's tenth problem", "Diophantine set" and "listable set" by replacing all occurrences of $\mathbb{Z}$ by R.

Theorem (Mazur–Rubin, 2009)

Assume BSD. Let R be a finitely generated ring with $|R| = \infty$. Then Hilbert's tenth problem is undecidable over R.

Theorem (K.–Pagano, 2024)

Let R be a finitely generated ring with $|R| = \infty$. Then Hilbert's tenth problem is undecidable over R.

We do this by proving the following conjecture of Denef–Lipshitz (1978).

Finitely generated rings

Definition

For a finitely generated ring R, we have natural analogues of "Hilbert's tenth problem", "Diophantine set" and "listable set" by replacing all occurrences of $\mathbb{Z}$ by R.

Theorem (Mazur–Rubin, 2009)

Assume BSD. Let R be a finitely generated ring with $|R| = \infty$. Then Hilbert's tenth problem is undecidable over R.

Theorem (K.–Pagano, 2024)

Let R be a finitely generated ring with $|R| = \infty$. Then Hilbert's tenth problem is undecidable over R.

We do this by proving the following conjecture of Denef–Lipshitz (1978).

Theorem (K.–Pagano, 2024)

Let K be a number field. Then $\mathbb{Z}$ is Diophantine over O_K.

Finitely generated rings

Definition

For a finitely generated ring R, we have natural analogues of "Hilbert's tenth problem", "Diophantine set" and "listable set" by replacing all occurrences of $\mathbb{Z}$ by R.

Theorem (Mazur–Rubin, 2009)

Assume BSD. Let R be a finitely generated ring with $|R| = \infty$. Then Hilbert's tenth problem is undecidable over R.

Theorem (K.–Pagano, 2024)

Let R be a finitely generated ring with $|R| = \infty$. Then Hilbert's tenth problem is undecidable over R.

We do this by proving the following conjecture of Denef–Lipshitz (1978).

Theorem (K.–Pagano, 2024)

Let K be a number field. Then $\mathbb{Z}$ is Diophantine over O_K.

This implies the previous theorem by work of Eisenträger.

Elliptic curves

Recall that Pell's equation plays an important role in the MRDP theorem.

Elliptic curves

Recall that Pell's equation plays an important role in the MRDP theorem.

The theory of Pell's equation works well over totally real number fields. Denef (1980) suggested to use other algebraic groups of rank 1 for number fields that are not totally real.

Elliptic curves

Recall that Pell's equation plays an important role in the MRDP theorem.

The theory of Pell's equation works well over totally real number fields. Denef (1980) suggested to use other algebraic groups of rank 1 for number fields that are not totally real.

The next result builds on work of Poonen and Cornelissen–Pheidas–Zahidi.

Elliptic curves

Recall that Pell's equation plays an important role in the MRDP theorem.

The theory of Pell's equation works well over totally real number fields. Denef (1980) suggested to use other algebraic groups of rank 1 for number fields that are not totally real.

The next result builds on work of Poonen and Cornelissen–Pheidas–Zahidi.

Theorem (Shlapentokh (2008))

Let L/K be an extension of number fields. Suppose that there exists an elliptic curve E/K such that $\operatorname{rk} E(L) = \operatorname{rk} E(K) > 0$. Then O_K is Diophantine over O_L.

Elliptic curves

Recall that Pell's equation plays an important role in the MRDP theorem.

The theory of Pell's equation works well over totally real number fields. Denef (1980) suggested to use other algebraic groups of rank 1 for number fields that are not totally real.

The next result builds on work of Poonen and Cornelissen–Pheidas–Zahidi.

Theorem (Shlapentokh (2008))

Let L/K be an extension of number fields. Suppose that there exists an elliptic curve E/K such that $\operatorname{rk} E(L) = \operatorname{rk} E(K) > 0$. Then O_K is Diophantine over O_L.

Our main new technical result is (rank growth theorem):

Theorem (K.–Pagano, 2024)

Let K be a number field with at least 32 real embeddings. Then there exists an elliptic curve E/K such that

$$\operatorname{rk} E(K) = \operatorname{rk} E(K(i)) > 0.$$

Reduction to the rank growth theorem

Lemma (Denef, Denef–Lipshitz)

Let $K \subseteq L$ be number fields. Then:

(i) *If $D_1, D_2 \subseteq O_K$ are Diophantine over O_K, so is $D_1 \cap D_2$.*

Reduction to the rank growth theorem

Lemma (Denef, Denef–Lipshitz)

Let $K \subseteq L$ be number fields. Then:

(i) *If $D_1, D_2 \subseteq O_K$ are Diophantine over O_K, so is $D_1 \cap D_2$.*

(ii) *If $D \subseteq O_K$ is Diophantine over O_K and if O_K is Diophantine over O_L, then D is Diophantine over O_L.*

Reduction to the rank growth theorem

Lemma (Denef, Denef–Lipshitz)

Let $K \subseteq L$ be number fields. Then:

(i) *If $D_1, D_2 \subseteq O_K$ are Diophantine over O_K, so is $D_1 \cap D_2$.*

(ii) *If $D \subseteq O_K$ is Diophantine over O_K and if O_K is Diophantine over O_L, then D is Diophantine over O_L.*

(iii) *If $\mathbb{Z}$ is Diophantine over O_L, then $\mathbb{Z}$ is Diophantine over O_K.*

Reduction to the rank growth theorem

Lemma (Denef, Denef–Lipshitz)

Let $K \subseteq L$ be number fields. Then:

(i) *If $D_1, D_2 \subseteq O_K$ are Diophantine over O_K, so is $D_1 \cap D_2$.*

(ii) *If $D \subseteq O_K$ is Diophantine over O_K and if O_K is Diophantine over O_L, then D is Diophantine over O_L.*

(iii) *If $\mathbb{Z}$ is Diophantine over O_L, then $\mathbb{Z}$ is Diophantine over O_K.*

(iv) *If K is totally real, then $\mathbb{Z}$ is Diophantine over O_K.*

Reduction to the rank growth theorem

Lemma (Denef, Denef–Lipshitz)

Let $K \subseteq L$ be number fields. Then:

(i) *If $D_1, D_2 \subseteq O_K$ are Diophantine over O_K, so is $D_1 \cap D_2$.*

(ii) *If $D \subseteq O_K$ is Diophantine over O_K and if O_K is Diophantine over O_L, then D is Diophantine over O_L.*

(iii) *If $\mathbb{Z}$ is Diophantine over O_L, then $\mathbb{Z}$ is Diophantine over O_K.*

(iv) *If K is totally real, then $\mathbb{Z}$ is Diophantine over O_K.*

Rank growth implies that $\mathbb{Z}$ is Diophantine over O_K.

Let K be a number field: we will show that $\mathbb{Z}$ is Dio over O_K. Define M to be the Galois closure of $K(i, \sqrt{3}, \sqrt{5}, \sqrt{7}, \sqrt{11}, \sqrt{13}, \sqrt{17})$, so suffices to show that $\mathbb{Z}$ is Dio over O_M by (*iii*).

Reduction to the rank growth theorem

Lemma (Denef, Denef–Lipshitz)

Let $K \subseteq L$ be number fields. Then:

(i) *If $D_1, D_2 \subseteq O_K$ are Diophantine over O_K, so is $D_1 \cap D_2$.*

(ii) *If $D \subseteq O_K$ is Diophantine over O_K and if O_K is Diophantine over O_L, then D is Diophantine over O_L.*

(iii) *If $\mathbb{Z}$ is Diophantine over O_L, then $\mathbb{Z}$ is Diophantine over O_K.*

(iv) *If K is totally real, then $\mathbb{Z}$ is Diophantine over O_K.*

Rank growth implies that $\mathbb{Z}$ is Diophantine over O_K.

Let K be a number field: we will show that $\mathbb{Z}$ is Dio over O_K. Define M to be the Galois closure of $K(i, \sqrt{3}, \sqrt{5}, \sqrt{7}, \sqrt{11}, \sqrt{13}, \sqrt{17})$, so suffices to show that $\mathbb{Z}$ is Dio over O_M by (*iii*). Let $D \subseteq \mathrm{Gal}(M/\mathbb{Q})$ be a decomposition group at infinity, so $i \notin M^D =: L$ and $M = L(i)$.

Reduction to the rank growth theorem

Lemma (Denef, Denef–Lipshitz)

Let $K \subseteq L$ be number fields. Then:

(i) *If $D_1, D_2 \subseteq O_K$ are Diophantine over O_K, so is $D_1 \cap D_2$.*

(ii) *If $D \subseteq O_K$ is Diophantine over O_K and if O_K is Diophantine over O_L, then D is Diophantine over O_L.*

(iii) *If $\mathbb{Z}$ is Diophantine over O_L, then $\mathbb{Z}$ is Diophantine over O_K.*

(iv) *If K is totally real, then $\mathbb{Z}$ is Diophantine over O_K.*

Rank growth implies that $\mathbb{Z}$ is Diophantine over O_K.

Let K be a number field: we will show that $\mathbb{Z}$ is Dio over O_K. Define M to be the Galois closure of $K(i, \sqrt{3}, \sqrt{5}, \sqrt{7}, \sqrt{11}, \sqrt{13}, \sqrt{17})$, so suffices to show that $\mathbb{Z}$ is Dio over O_M by (*iii*). Let $D \subseteq \mathrm{Gal}(M/\mathbb{Q})$ be a decomposition group at infinity, so $i \notin M^D =: L$ and $M = L(i)$. Hence rank growth and Shlapentokh's theorem show that O_{M^D} is Dio over O_M.

Reduction to the rank growth theorem

Lemma (Denef, Denef–Lipshitz)

Let $K \subseteq L$ be number fields. Then:

(i) *If $D_1, D_2 \subseteq O_K$ are Diophantine over O_K, so is $D_1 \cap D_2$.*

(ii) *If $D \subseteq O_K$ is Diophantine over O_K and if O_K is Diophantine over O_L, then D is Diophantine over O_L.*

(iii) *If $\mathbb{Z}$ is Diophantine over O_L, then $\mathbb{Z}$ is Diophantine over O_K.*

(iv) *If K is totally real, then $\mathbb{Z}$ is Diophantine over O_K.*

Rank growth implies that $\mathbb{Z}$ is Diophantine over O_K.

Let K be a number field: we will show that $\mathbb{Z}$ is Dio over O_K. Define M to be the Galois closure of $K(i, \sqrt{3}, \sqrt{5}, \sqrt{7}, \sqrt{11}, \sqrt{13}, \sqrt{17})$, so suffices to show that $\mathbb{Z}$ is Dio over O_M by (iii). Let $D \subseteq \mathrm{Gal}(M/\mathbb{Q})$ be a decomposition group at infinity, so $i \notin M^D =: L$ and $M = L(i)$. Hence rank growth and Shlapentokh's theorem show that O_{M^D} is Dio over O_M. By (i), we get that O_F is Dio over O_M, where F is the intersection of all the M^D (with D a decomposition group at infinity).

Reduction to the rank growth theorem

Lemma (Denef, Denef–Lipshitz)

Let $K \subseteq L$ be number fields. Then:

(i) *If $D_1, D_2 \subseteq O_K$ are Diophantine over O_K, so is $D_1 \cap D_2$.*

(ii) *If $D \subseteq O_K$ is Diophantine over O_K and if O_K is Diophantine over O_L, then D is Diophantine over O_L.*

(iii) *If $\mathbb{Z}$ is Diophantine over O_L, then $\mathbb{Z}$ is Diophantine over O_K.*

(iv) *If K is totally real, then $\mathbb{Z}$ is Diophantine over O_K.*

Rank growth implies that $\mathbb{Z}$ is Diophantine over O_K.

Let K be a number field: we will show that $\mathbb{Z}$ is Dio over O_K. Define M to be the Galois closure of $K(i, \sqrt{3}, \sqrt{5}, \sqrt{7}, \sqrt{11}, \sqrt{13}, \sqrt{17})$, so suffices to show that $\mathbb{Z}$ is Dio over O_M by (iii). Let $D \subseteq \mathrm{Gal}(M/\mathbb{Q})$ be a decomposition group at infinity, so $i \notin M^D =: L$ and $M = L(i)$. Hence rank growth and Shlapentokh's theorem show that O_{M^D} is Dio over O_M. By (i), we get that O_F is Dio over O_M, where F is the intersection of all the M^D (with D a decomposition group at infinity). But F is totally real, so $\mathbb{Z}$ is Dio over O_F by (iv), and therefore over O_M by (ii). □

Rank growth

We recall:

Theorem (K.–Pagano, 2024)

Let K be a number field with at least 32 real embeddings. Then there exists an elliptic curve E/K such that

$$\operatorname{rk} E(K) = \operatorname{rk} E(K(i)) > 0.$$

Rank growth

We recall:

Theorem (K.–Pagano, 2024)

Let K be a number field with at least 32 real embeddings. Then there exists an elliptic curve E/K such that

$$\operatorname{rk} E(K) = \operatorname{rk} E(K(i)) > 0.$$

What is the challenge?

Rank growth

We recall:

Theorem (K.–Pagano, 2024)

Let K be a number field with at least 32 real embeddings. Then there exists an elliptic curve E/K such that

$$\operatorname{rk} E(K) = \operatorname{rk} E(K(i)) > 0.$$

What is the challenge?

- It is easy to construct elliptic curves E/K with $\operatorname{rk} E(K) > 0$.

Rank growth

We recall:

Theorem (K.–Pagano, 2024)

Let K be a number field with at least 32 real embeddings. Then there exists an elliptic curve E/K such that

$$\operatorname{rk} E(K) = \operatorname{rk} E(K(i)) > 0.$$

What is the challenge?

- It is easy to construct elliptic curves E/K with $\operatorname{rk} E(K) > 0$.
- It is also easy to use 2-descent to upper bound the rank of E/K.

Rank growth

We recall:

Theorem (K.–Pagano, 2024)

Let K be a number field with at least 32 real embeddings. Then there exists an elliptic curve E/K such that

$$\operatorname{rk} E(K) = \operatorname{rk} E(K(i)) > 0.$$

What is the challenge?

- It is easy to construct elliptic curves E/K with $\operatorname{rk} E(K) > 0$.
- It is also easy to use 2-descent to upper bound the rank of E/K.

However, it is not at all clear how to combine this.

The 2-Selmer group

Consider the short exact sequence of $G_K := \mathrm{Gal}(\overline{K}/K)$-modules

$$0 \to E[2] \to E \xrightarrow{\cdot 2} E \to 0.$$

The 2-Selmer group

Consider the short exact sequence of $G_K := \mathrm{Gal}(\overline{K}/K)$-modules

$$0 \to E[2] \to E \xrightarrow{\cdot 2} E \to 0.$$

Taking Galois cohomology gives

$$0 \to E(K)[2] \to E(K) \xrightarrow{\cdot 2} E(K) \xrightarrow{\delta} H^1(G_K, E[2]),$$

so $E(K)/2E(K) \xhookrightarrow{\delta} H^1(G_K, E[2])$.

The 2-Selmer group

Consider the short exact sequence of $G_K := \mathrm{Gal}(\overline{K}/K)$-modules

$$0 \to E[2] \to E \xrightarrow{\cdot 2} E \to 0.$$

Taking Galois cohomology gives

$$0 \to E(K)[2] \to E(K) \xrightarrow{\cdot 2} E(K) \xrightarrow{\delta} H^1(G_K, E[2]),$$

so $E(K)/2E(K) \xhookrightarrow{\delta} H^1(G_K, E[2])$. However, $\dim_{\mathbb{F}_2} H^1(G_K, E[2]) = \infty$ so this is not too informative.

The 2-Selmer group

Consider the short exact sequence of $G_K := \mathrm{Gal}(\overline{K}/K)$-modules

$$0 \to E[2] \to E \xrightarrow{\cdot 2} E \to 0.$$

Taking Galois cohomology gives

$$0 \to E(K)[2] \to E(K) \xrightarrow{\cdot 2} E(K) \xrightarrow{\delta} H^1(G_K, E[2]),$$

so $E(K)/2E(K) \xhookrightarrow{\delta} H^1(G_K, E[2])$. However, $\dim_{\mathbb{F}_2} H^1(G_K, E[2]) = \infty$ so this is not too informative. But, for each place v of K we have

$$\begin{array}{ccccccccc}
0 & \longrightarrow & E(K)[2] & \longrightarrow & E(K) & \xrightarrow{\cdot 2} & E(K) & \xrightarrow{\delta} & H^1(G_K, E[2]) \\
 & & \downarrow & & \downarrow & & \downarrow & & \downarrow{\scriptstyle \mathrm{res}_v} \\
0 & \longrightarrow & E(K_v)[2] & \longrightarrow & E(K_v) & \xrightarrow{\cdot 2} & E(K_v) & \xrightarrow{\delta_v} & H^1(G_{K_v}, E[2]).
\end{array}$$

The 2-Selmer group II

Recall:

$$\begin{array}{ccc} E(K)/2E(K) & \xhookrightarrow{\delta} & H^1(G_K, E[2]) \\ \downarrow & & \downarrow \mathrm{res}_v \\ E(K_v)/2E(K_v) & \xhookrightarrow{\delta_v} & H^1(G_{K_v}, E[2]) \end{array}$$

The 2-Selmer group II

Recall:

$$\begin{array}{ccc} E(K)/2E(K) & \xhookrightarrow{\delta} & H^1(G_K, E[2]) \\ \downarrow & & \downarrow \mathrm{res}_v \\ E(K_v)/2E(K_v) & \xhookrightarrow{\delta_v} & H^1(G_{K_v}, E[2]) \end{array}$$

We define

$$\mathrm{Sel}^2(E/K) := \ker\left(H^1(G_K, E[2]) \xrightarrow{\prod_v \mathrm{res}_v} \prod_v \frac{H^1(G_{K_v}, E[2])}{\mathrm{im}(\delta_v)} \right).$$

The 2-Selmer group II

Recall:

$$\begin{array}{ccc} E(K)/2E(K) & \xhookrightarrow{\delta} & H^1(G_K, E[2]) \\ \downarrow & & \downarrow \mathrm{res}_v \\ E(K_v)/2E(K_v) & \xhookrightarrow{\delta_v} & H^1(G_{K_v}, E[2]) \end{array}$$

We define

$$\mathrm{Sel}^2(E/K) := \ker\left(H^1(G_K, E[2]) \xrightarrow{\prod_v \mathrm{res}_v} \prod_v \frac{H^1(G_{K_v}, E[2])}{\mathrm{im}(\delta_v)} \right).$$

Key facts:

(1) We have $\mathrm{im}(\delta) \subseteq \mathrm{Sel}^2(E/K)$,

The 2-Selmer group II

Recall:

$$\begin{array}{ccc} E(K)/2E(K) & \xhookrightarrow{\delta} & H^1(G_K, E[2]) \\ \downarrow & & \downarrow \mathrm{res}_v \\ E(K_v)/2E(K_v) & \xhookrightarrow{\delta_v} & H^1(G_{K_v}, E[2]) \end{array}$$

We define

$$\mathrm{Sel}^2(E/K) := \ker\left(H^1(G_K, E[2]) \xrightarrow{\prod_v \mathrm{res}_v} \prod_v \frac{H^1(G_{K_v}, E[2])}{\mathrm{im}(\delta_v)} \right).$$

Key facts:

(1) We have $\mathrm{im}(\delta) \subseteq \mathrm{Sel}^2(E/K)$, and hence

$$\mathrm{rk}\, E(K) + \dim_{\mathbb{F}_2} E(K)[2] = \dim_{\mathbb{F}_2} E(K)/2E(K) \leq \dim_{\mathbb{F}_2} \mathrm{Sel}^2(E/K).$$

The 2-Selmer group II

Recall:

$$\begin{array}{ccc} E(K)/2E(K) & \xhookrightarrow{\delta} & H^1(G_K, E[2]) \\ \downarrow & & \downarrow{\scriptstyle \mathrm{res}_v} \\ E(K_v)/2E(K_v) & \xhookrightarrow{\delta_v} & H^1(G_{K_v}, E[2]) \end{array}$$

We define

$$\mathrm{Sel}^2(E/K) := \ker\left(H^1(G_K, E[2]) \xrightarrow{\prod_v \mathrm{res}_v} \prod_v \frac{H^1(G_{K_v}, E[2])}{\mathrm{im}(\delta_v)} \right).$$

Key facts:

(1) We have $\mathrm{im}(\delta) \subseteq \mathrm{Sel}^2(E/K)$, and hence

$$\mathrm{rk}\, E(K) + \dim_{\mathbb{F}_2} E(K)[2] = \dim_{\mathbb{F}_2} E(K)/2E(K) \leq \dim_{\mathbb{F}_2} \mathrm{Sel}^2(E/K).$$

(2) The group $\mathrm{Sel}^2(E/K)$ is computable and finite dimensional (note that rank is not known to be computable!).

Forcing positive rank

Take some E_1 with $E_1(K)[2] \cong \mathbb{F}_2^2$, i.e.

$$E_1 : y^2 = (x - a_1)(x - a_2)(x - a_3) \qquad a_1, a_2, a_3 \in K \text{ distinct.}$$

Forcing positive rank

Take some E_1 with $E_1(K)[2] \cong \mathbb{F}_2^2$, i.e.

$$E_1 : y^2 = (x - a_1)(x - a_2)(x - a_3) \qquad a_1, a_2, a_3 \in K \text{ distinct.}$$

Consider the quadratic twist E_1^t with $t := (n - a_1)(n - a_2)(n - a_3)$. Then

$$E_1^t : (n - a_1)(n - a_2)(n - a_3)y^2 = (x - a_1)(x - a_2)(x - a_3)$$

has the rational point $(x, y) = (n, 1)$.

Forcing positive rank

Take some E_1 with $E_1(K)[2] \cong \mathbb{F}_2^2$, i.e.

$$E_1 : y^2 = (x - a_1)(x - a_2)(x - a_3) \qquad a_1, a_2, a_3 \in K \text{ distinct.}$$

Consider the quadratic twist E_1^t with $t := (n - a_1)(n - a_2)(n - a_3)$. Then

$$E_1^t : (n - a_1)(n - a_2)(n - a_3)y^2 = (x - a_1)(x - a_2)(x - a_3)$$

has the rational point $(x, y) = (n, 1)$. It is not hard to show that this point is almost never torsion (Northcott's theorem + height bounds).

Forcing positive rank

Take some E_1 with $E_1(K)[2] \cong \mathbb{F}_2^2$, i.e.

$$E_1 : y^2 = (x - a_1)(x - a_2)(x - a_3) \qquad a_1, a_2, a_3 \in K \text{ distinct.}$$

Consider the quadratic twist E_1^t with $t := (n - a_1)(n - a_2)(n - a_3)$. Then

$$E_1^t : (n - a_1)(n - a_2)(n - a_3)y^2 = (x - a_1)(x - a_2)(x - a_3)$$

has the rational point $(x, y) = (n, 1)$. It is not hard to show that this point is almost never torsion (Northcott's theorem + height bounds).

However, it is very difficult to control rank in this family. Instead, we consider E_1^t with $t := m(n - a_1 m)(n - a_2 m)(n - a_3 m)$. Then

$$E_1^t : m(n - a_1 m)(n - a_2 m)(n - a_3 m)y^2 = (x - a_1)(x - a_2)(x - a_3)$$

has the rational point $(x, y) = (n/m, 1/m^2)$ and hence $\operatorname{rk} E_1^t(K) > 0$.

Forcing positive rank II

Because $i \notin K$ (since K has 32 real places), we get

$$\operatorname{rk} E_1^t(K(i)) = \operatorname{rk} E_1^t(K) + \operatorname{rk} E_1^{-t}(K).$$

Forcing positive rank II

Because $i \notin K$ (since K has 32 real places), we get

$$\operatorname{rk} E_1^t(K(i)) = \operatorname{rk} E_1^t(K) + \operatorname{rk} E_1^{-t}(K).$$

Hence it suffices to find $t := m(n - a_1 m)(n - a_2 m)(n - a_3 m)$ with

$$\operatorname{rk} E_1^{-t}(K) = 0,$$

as then $E := E_1^t$ satisfies $\operatorname{rk} E(K(i)) = \operatorname{rk} E(K) > 0$ as desired.

Forcing positive rank II

Because $i \notin K$ (since K has 32 real places), we get

$$\operatorname{rk} E_1^t(K(i)) = \operatorname{rk} E_1^t(K) + \operatorname{rk} E_1^{-t}(K).$$

Hence it suffices to find $t := m(n - a_1 m)(n - a_2 m)(n - a_3 m)$ with

$$\operatorname{rk} E_1^{-t}(K) = 0,$$

as then $E := E_1^t$ satisfies $\operatorname{rk} E(K(i)) = \operatorname{rk} E(K) > 0$ as desired.

Because E_1 has full rational 2-torsion (and therefore all of its quadratic twists do), it suffices to find $t := m(n - a_1 m)(n - a_2 m)(n - a_3 m)$ with

$$\dim_{\mathbb{F}_2} \operatorname{Sel}^2(E_1^{-t}/K) = 2,$$

as this implies $\operatorname{rk} E_1^{-t}(K) = 0$.

Computing 2-Selmer

We now restrict to $K = \mathbb{Q}$ for simplicity.

Computing 2-Selmer

We now restrict to $K = \mathbb{Q}$ for simplicity.

Because $E(\mathbb{Q})[2] \cong \mathbb{F}_2^2$, we get

$$\begin{aligned}\mathrm{Sel}^2(E/\mathbb{Q}) \subseteq H^1(G_{\mathbb{Q}}, E[2]) \cong H^1(G_{\mathbb{Q}}, \mathbb{F}_2^2) &\cong (\mathbb{Q}^*/\mathbb{Q}^{*2})^2 \\ &= \{(x_1, x_2) : x_1, x_2 \text{ squarefree}\}.\end{aligned}$$

Computing 2-Selmer

We now restrict to $K = \mathbb{Q}$ for simplicity.

Because $E(\mathbb{Q})[2] \cong \mathbb{F}_2^2$, we get

$$\begin{aligned}\mathrm{Sel}^2(E/\mathbb{Q}) \subseteq H^1(G_{\mathbb{Q}}, E[2]) \cong H^1(G_{\mathbb{Q}}, \mathbb{F}_2^2) &\cong (\mathbb{Q}^*/\mathbb{Q}^{*2})^2 \\ &= \{(x_1, x_2) : x_1, x_2 \text{ squarefree}\}.\end{aligned}$$

The local conditions $\mathrm{im}(\delta_v)$ are hard to describe for $v \mid \Delta_{E_1}$. But for E_1^d (with d squarefree and $\gcd(d, \Delta_{E_1}) = 1$), we have the explicit description

$$\mathrm{im}(\delta_v) = \begin{cases} \langle (\alpha\beta, d\alpha), (-d\alpha, -\alpha\gamma) \rangle & \text{if } v \mid d \\ H^1_{\mathrm{ur}}(G_{\mathbb{Q}_v}, \mathbb{F}_2^2) & \text{if } v \nmid d\Delta_{E_1} \end{cases}$$

with $\alpha = a_1 - a_2$, $\beta = a_1 - a_3$ and $\gamma = a_2 - a_3$.

Computing 2-Selmer

We now restrict to $K = \mathbb{Q}$ for simplicity.

Because $E(\mathbb{Q})[2] \cong \mathbb{F}_2^2$, we get

$$\begin{aligned}\mathrm{Sel}^2(E/\mathbb{Q}) \subseteq H^1(G_\mathbb{Q}, E[2]) \cong H^1(G_\mathbb{Q}, \mathbb{F}_2^2) &\cong (\mathbb{Q}^*/\mathbb{Q}^{*2})^2 \\ &= \{(x_1, x_2) : x_1, x_2 \text{ squarefree}\}.\end{aligned}$$

The local conditions $\mathrm{im}(\delta_v)$ are hard to describe for $v \mid \Delta_{E_1}$. But for E_1^d (with d squarefree and $\gcd(d, \Delta_{E_1}) = 1$), we have the explicit description

$$\mathrm{im}(\delta_v) = \begin{cases} \langle (\alpha\beta, d\alpha), (-d\alpha, -\alpha\gamma) \rangle & \text{if } v \mid d \\ H^1_{\mathrm{ur}}(G_{\mathbb{Q}_v}, \mathbb{F}_2^2) & \text{if } v \nmid d\Delta_{E_1} \end{cases}$$

with $\alpha = a_1 - a_2$, $\beta = a_1 - a_3$ and $\gamma = a_2 - a_3$.

In particular, if $(x_1, x_2) \in \mathrm{Sel}^2(E_1^d/\mathbb{Q})$, then x_1, x_2 are only divisible by primes dividing $d\Delta_E$.

Computing 2-Selmer II

Theorem

Let $E_1/\mathbb{Q}$ be an elliptic curve with $E_1[2] \cong \mathbb{F}_2^2$. Let $d_1 = p_1 \cdots p_r$ be squarefree and let $d_2 = q_1 \cdots q_r$ be squarefree. Assume that:

Computing 2-Selmer II

Theorem

Let $E_1/\mathbb{Q}$ be an elliptic curve with $E_1[2] \cong \mathbb{F}_2^2$. Let $d_1 = p_1 \cdots p_r$ be squarefree and let $d_2 = q_1 \cdots q_r$ be squarefree. Assume that:

- *the primes p_i, q_i do not divide Δ_{E_1},*

Computing 2-Selmer II

Theorem

Let $E_1/\mathbb{Q}$ be an elliptic curve with $E_1[2] \cong \mathbb{F}_2^2$. Let $d_1 = p_1 \cdots p_r$ be squarefree and let $d_2 = q_1 \cdots q_r$ be squarefree. Assume that:

- *the primes p_i, q_i do not divide Δ_{E_1},*
- *we have $(p_i/r) = (q_i/r)$ for all odd $r \mid \Delta_{E_1}$ and $p_i \equiv q_i \bmod 8$,*

Computing 2-Selmer II

Theorem

Let $E_1/\mathbb{Q}$ be an elliptic curve with $E_1[2] \cong \mathbb{F}_2^2$. Let $d_1 = p_1 \cdots p_r$ be squarefree and let $d_2 = q_1 \cdots q_r$ be squarefree. Assume that:

- *the primes p_i, q_i do not divide Δ_{E_1},*
- *we have $(p_i/r) = (q_i/r)$ for all odd $r \mid \Delta_{E_1}$ and $p_i \equiv q_i \bmod 8$,*
- *we have $(p_i/p_j) = (q_i/q_j)$ for all $1 \leq i < j \leq r$.*

Computing 2-Selmer II

Theorem

Let $E_1/\mathbb{Q}$ be an elliptic curve with $E_1[2] \cong \mathbb{F}_2^2$. Let $d_1 = p_1 \cdots p_r$ be squarefree and let $d_2 = q_1 \cdots q_r$ be squarefree. Assume that:

- *the primes p_i, q_i do not divide Δ_{E_1},*
- *we have $(p_i/r) = (q_i/r)$ for all odd $r \mid \Delta_{E_1}$ and $p_i \equiv q_i \bmod 8$,*
- *we have $(p_i/p_j) = (q_i/q_j)$ for all $1 \leq i < j \leq r$.*

Then we have $\mathrm{Sel}^2(E_1^{d_1}/\mathbb{Q}) \cong \mathrm{Sel}^2(E_1^{d_2}/\mathbb{Q})$.

Computing 2-Selmer II

Theorem

Let $E_1/\mathbb{Q}$ be an elliptic curve with $E_1[2] \cong \mathbb{F}_2^2$. Let $d_1 = p_1 \cdots p_r$ be squarefree and let $d_2 = q_1 \cdots q_r$ be squarefree. Assume that:

- *the primes p_i, q_i do not divide Δ_{E_1},*
- *we have $(p_i/r) = (q_i/r)$ for all odd $r \mid \Delta_{E_1}$ and $p_i \equiv q_i \bmod 8$,*
- *we have $(p_i/p_j) = (q_i/q_j)$ for all $1 \leq i < j \leq r$.*

Then we have $\mathrm{Sel}^2(E_1^{d_1}/\mathbb{Q}) \cong \mathrm{Sel}^2(E_1^{d_2}/\mathbb{Q})$.

In particular, fixing some d, we can compute $\mathrm{Sel}^2(E_1^{dp}/\mathbb{Q})$ from $\mathrm{Sel}^2(E_1^{d}/\mathbb{Q})$ and the congruence of p modulo $8d\Delta_E$.

Computing 2-Selmer II

Theorem

Let $E_1/\mathbb{Q}$ be an elliptic curve with $E_1[2] \cong \mathbb{F}_2^2$. Let $d_1 = p_1 \cdots p_r$ be squarefree and let $d_2 = q_1 \cdots q_r$ be squarefree. Assume that:

- *the primes p_i, q_i do not divide Δ_{E_1},*
- *we have $(p_i/r) = (q_i/r)$ for all odd $r \mid \Delta_{E_1}$ and $p_i \equiv q_i \bmod 8$,*
- *we have $(p_i/p_j) = (q_i/q_j)$ for all $1 \leq i < j \leq r$.*

Then we have $\mathrm{Sel}^2(E_1^{d_1}/\mathbb{Q}) \cong \mathrm{Sel}^2(E_1^{d_2}/\mathbb{Q})$.

In particular, fixing some d, we can compute $\mathrm{Sel}^2(E_1^{dp}/\mathbb{Q})$ from $\mathrm{Sel}^2(E_1^{d}/\mathbb{Q})$ and the congruence of p modulo $8d\Delta_E$.

Distribution of $\mathrm{Sel}^2(E_1^{d}/\mathbb{Q})$ was found by Heath-Brown, Kane and Smith.

Additive combinatorics

Our key new insight is to bring additive combinatorics into the field.

Additive combinatorics

Our key new insight is to bring additive combinatorics into the field. Take

$$t = m(n - a_1 m)(n - a_2 m)(n - a_3 m) = \kappa P_1 P_2 P_3 P_4$$

with

$$n - a_1 m = P_1, \quad n - a_2 m = P_2, \quad n - a_3 m = P_3, \quad m = \kappa P_4.$$

Additive combinatorics

Our key new insight is to bring additive combinatorics into the field. Take

$$t = m(n - a_1 m)(n - a_2 m)(n - a_3 m) = \kappa P_1 P_2 P_3 P_4$$

with

$$n - a_1 m = P_1, \quad n - a_2 m = P_2, \quad n - a_3 m = P_3, \quad m = \kappa P_4.$$

This is possible by the Green–Tao theorem (recently generalized to number fields by Kai).

Additive combinatorics

Our key new insight is to bring additive combinatorics into the field. Take

$$t = m(n - a_1 m)(n - a_2 m)(n - a_3 m) = \kappa P_1 P_2 P_3 P_4$$

with

$$n - a_1 m = P_1, \quad n - a_2 m = P_2, \quad n - a_3 m = P_3, \quad m = \kappa P_4.$$

This is possible by the Green–Tao theorem (recently generalized to number fields by Kai).

The strategy is then:

Additive combinatorics

Our key new insight is to bring additive combinatorics into the field. Take

$$t = m(n - a_1 m)(n - a_2 m)(n - a_3 m) = \kappa P_1 P_2 P_3 P_4$$

with

$$n - a_1 m = P_1, \quad n - a_2 m = P_2, \quad n - a_3 m = P_3, \quad m = \kappa P_4.$$

This is possible by the Green–Tao theorem (recently generalized to number fields by Kai).

The strategy is then:

(1) First arrange $\mathrm{Sel}^2(E_1^\kappa/\mathbb{Q})$ favorably.

Additive combinatorics

Our key new insight is to bring additive combinatorics into the field. Take

$$t = m(n - a_1 m)(n - a_2 m)(n - a_3 m) = \kappa P_1 P_2 P_3 P_4$$

with

$$n - a_1 m = P_1, \quad n - a_2 m = P_2, \quad n - a_3 m = P_3, \quad m = \kappa P_4.$$

This is possible by the Green–Tao theorem (recently generalized to number fields by Kai).

The strategy is then:

(1) First arrange $\mathrm{Sel}^2(E_1^\kappa/\mathbb{Q})$ favorably.

(2) Then twist by P_1, P_2, P_3, P_4 in a controlled way.

Final hurdles

A direct strategy is to take an assignment of Legendre symbols with $\dim_{\mathbb{F}_2} \mathrm{Sel}^2(E_1^d/\mathbb{Q}) = 2$ (which exists by Heath-Brown/Kane/Smith), and then mimic this assignment with $\kappa, P_1, P_2, P_3, P_4$.

Final hurdles

A direct strategy is to take an assignment of Legendre symbols with $\dim_{\mathbb{F}_2} \mathrm{Sel}^2(E_1^d/\mathbb{Q}) = 2$ (which exists by Heath-Brown/Kane/Smith), and then mimic this assignment with $\kappa, P_1, P_2, P_3, P_4$.

However, since $P_i = n - a_i d$ and $P_4 = \kappa d$, we see that there are constraints between (P_i/P_j), and moreover $(P_i P_j/r) = +1$ with $r \mid \kappa$.

Final hurdles

A direct strategy is to take an assignment of Legendre symbols with $\dim_{\mathbb{F}_2} \mathrm{Sel}^2(E_1^d/\mathbb{Q}) = 2$ (which exists by Heath-Brown/Kane/Smith), and then mimic this assignment with $\kappa, P_1, P_2, P_3, P_4$.

However, since $P_i = n - a_i d$ and $P_4 = \kappa d$, we see that there are constraints between (P_i/P_j), and moreover $(P_i P_j/r) = +1$ with $r \mid \kappa$.

An extra complication is that Green–Tao does not give control over the Legendre symbol (P_i/P_j).

Final hurdles

A direct strategy is to take an assignment of Legendre symbols with $\dim_{\mathbb{F}_2} \mathrm{Sel}^2(E_1^d/\mathbb{Q}) = 2$ (which exists by Heath-Brown/Kane/Smith), and then mimic this assignment with $\kappa, P_1, P_2, P_3, P_4$.

However, since $P_i = n - a_i d$ and $P_4 = \kappa d$, we see that there are constraints between (P_i/P_j), and moreover $(P_i P_j/r) = +1$ with $r \mid \kappa$.

An extra complication is that Green–Tao does not give control over the Legendre symbol (P_i/P_j).

We circumvent this by carefully choosing κ and then P_1, P_2, P_3, P_4 (as an analogy: one can choose 3 entries of a 2×2-matrix so that the matrix is invertible no matter the choice of the fourth entry).

Final hurdles

A direct strategy is to take an assignment of Legendre symbols with $\dim_{\mathbb{F}_2} \mathrm{Sel}^2(E_1^d/\mathbb{Q}) = 2$ (which exists by Heath-Brown/Kane/Smith), and then mimic this assignment with $\kappa, P_1, P_2, P_3, P_4$.

However, since $P_i = n - a_i d$ and $P_4 = \kappa d$, we see that there are constraints between (P_i/P_j), and moreover $(P_i P_j/r) = +1$ with $r \mid \kappa$.

An extra complication is that Green–Tao does not give control over the Legendre symbol (P_i/P_j).

We circumvent this by carefully choosing κ and then P_1, P_2, P_3, P_4 (as an analogy: one can choose 3 entries of a 2×2-matrix so that the matrix is invertible no matter the choice of the fourth entry).

It is only here that we use the presence of the 32 real places of K to play off some symbols against each other with quadratic reciprocity.

Summary

Hilbert's tenth problem is undecidable for every finitely generated ring R with $|R| = \infty$, strengthening previous conditional work of Mazur–Rubin.

Summary

Hilbert's tenth problem is undecidable for every finitely generated ring R with $|R| = \infty$, strengthening previous conditional work of Mazur–Rubin.

The key technical result is a rank growth result: under mild hypotheses, there exists an elliptic curve E/K with $\mathrm{rk}\, E(K(i)) = \mathrm{rk}\, E(K) > 0$.

Summary

Hilbert's tenth problem is undecidable for every finitely generated ring R with $|R| = \infty$, strengthening previous conditional work of Mazur–Rubin.

The key technical result is a rank growth result: under mild hypotheses, there exists an elliptic curve E/K with $\mathrm{rk}\, E(K(i)) = \mathrm{rk}\, E(K) > 0$.

This result is proven by a combination of 2-descent and additive combinatorics.

Summary

Hilbert's tenth problem is undecidable for every finitely generated ring R with $|R| = \infty$, strengthening previous conditional work of Mazur–Rubin.

The key technical result is a rank growth result: under mild hypotheses, there exists an elliptic curve E/K with $\operatorname{rk} E(K(i)) = \operatorname{rk} E(K) > 0$.

This result is proven by a combination of 2-descent and additive combinatorics.

We consider a family with elevated rank to guarantee positive rank.

Summary

Hilbert's tenth problem is undecidable for every finitely generated ring R with $|R| = \infty$, strengthening previous conditional work of Mazur–Rubin.

The key technical result is a rank growth result: under mild hypotheses, there exists an elliptic curve E/K with $\operatorname{rk} E(K(i)) = \operatorname{rk} E(K) > 0$.

This result is proven by a combination of 2-descent and additive combinatorics.

We consider a family with elevated rank to guarantee positive rank.

By finding a prime specialization with additive combinatorics, 2-descent allows us to show that $\operatorname{rk} E^{-1}(K) = 0$.

Summary

Hilbert's tenth problem is undecidable for every finitely generated ring R with $|R| = \infty$, strengthening previous conditional work of Mazur–Rubin.

The key technical result is a rank growth result: under mild hypotheses, there exists an elliptic curve E/K with $\operatorname{rk} E(K(i)) = \operatorname{rk} E(K) > 0$.

This result is proven by a combination of 2-descent and additive combinatorics.

We consider a family with elevated rank to guarantee positive rank.

By finding a prime specialization with additive combinatorics, 2-descent allows us to show that $\operatorname{rk} E^{-1}(K) = 0$.

Thank you for your attention!