Elliptic curves of rank one

Peter Koymans
Utrecht University

ANTS XVII

8 July 2026

What numbers are ranks?

Theorem (Mordell–Weil)

Let $E/\mathbb{Q}$ be an elliptic curve. Then we have

$$E(\mathbb{Q}) = \mathbb{Z}^r \oplus F,$$

where F is a finite abelian group.

What numbers are ranks?

Theorem (Mordell–Weil)

Let $E/\mathbb{Q}$ be an elliptic curve. Then we have

$$E(\mathbb{Q}) = \mathbb{Z}^r \oplus F,$$

where F is a finite abelian group.

We call r the rank of E, written $\mathrm{rk}\, E$.

What numbers are ranks?

Theorem (Mordell–Weil)

Let $E/\mathbb{Q}$ be an elliptic curve. Then we have

$$E(\mathbb{Q}) = \mathbb{Z}^r \oplus F,$$

where F is a finite abelian group.

We call r the rank of E, written $\operatorname{rk} E$.

The sets

$$\begin{aligned}\mathcal{R}_\infty &:= \{r : \text{there exist inf. many non-iso. } E/\mathbb{Q} \text{ with } r = \operatorname{rk} E\}\\ \mathcal{R} &:= \{r : \text{there exists } E/\mathbb{Q} \text{ with } r = \operatorname{rk} E\}\end{aligned}$$

have been the subject of much debate.

What numbers are ranks?

Theorem (Mordell–Weil)

Let $E/\mathbb{Q}$ be an elliptic curve. Then we have

$$E(\mathbb{Q}) = \mathbb{Z}^r \oplus F,$$

where F is a finite abelian group.

We call r the rank of E, written $\operatorname{rk} E$.

The sets

$$\begin{aligned}\mathcal{R}_\infty &:= \{r : \text{there exist inf. many non-iso. } E/\mathbb{Q} \text{ with } r = \operatorname{rk} E\}\\ \mathcal{R} &:= \{r : \text{there exists } E/\mathbb{Q} \text{ with } r = \operatorname{rk} E\}\end{aligned}$$

have been the subject of much debate.

For instance, ranks are bounded if and only if $\#\mathcal{R} < \infty$.

What numbers are ranks?

Theorem (Mordell–Weil)

Let $E/\mathbb{Q}$ be an elliptic curve. Then we have

$$E(\mathbb{Q}) = \mathbb{Z}^r \oplus F,$$

where F is a finite abelian group.

We call r the rank of E, written $\operatorname{rk} E$.

The sets

$$\begin{aligned}\mathcal{R}_\infty &:= \{r : \text{there exist inf. many non-iso. } E/\mathbb{Q} \text{ with } r = \operatorname{rk} E\}\\ \mathcal{R} &:= \{r : \text{there exists } E/\mathbb{Q} \text{ with } r = \operatorname{rk} E\}\end{aligned}$$

have been the subject of much debate.

For instance, ranks are bounded if and only if $\#\mathcal{R} < \infty$.

Until recently, the only integers provably in $\mathcal{R}$ are 0 and 1.

Number fields

The Mordell–Weil theorem is also true for number fields. Thus we can define for each number field K

$$\mathcal{R}_\infty(K) := \{r : \text{there exist inf. many non-iso. } E/K \text{ with } r = \operatorname{rk} E\}.$$

Number fields

The Mordell–Weil theorem is also true for number fields. Thus we can define for each number field K

$$\mathcal{R}_\infty(K) := \{r : \text{there exist inf. many non-iso. } E/K \text{ with } r = \operatorname{rk} E\}.$$

Theorem (Mazur–Rubin (2009))

Let K be a number field. Then $0 \in \mathcal{R}_\infty(K)$.

Number fields

The Mordell–Weil theorem is also true for number fields. Thus we can define for each number field K

$$\mathcal{R}_\infty(K) := \{r : \text{there exist inf. many non-iso. } E/K \text{ with } r = \operatorname{rk} E\}.$$

Theorem (Mazur–Rubin (2009))

Let K be a number field. Then $0 \in \mathcal{R}_\infty(K)$. Furthermore, assuming that $Ш(E/K)[2^\infty]$ is finite for all E/K, then $1 \in \mathcal{R}_\infty(K)$.

Number fields

The Mordell–Weil theorem is also true for number fields. Thus we can define for each number field K

$$\mathcal{R}_\infty(K) := \{r : \text{there exist inf. many non-iso. } E/K \text{ with } r = \operatorname{rk} E\}.$$

Theorem (Mazur–Rubin (2009))

Let K be a number field. Then $0 \in \mathcal{R}_\infty(K)$. Furthermore, assuming that $Ш(E/K)[2^\infty]$ is finite for all E/K, then $1 \in \mathcal{R}_\infty(K)$.

Theorem (K.–Pagano (2025))

Let K be a number field. Then $1 \in \mathcal{R}_\infty(K)$.

Number fields

The Mordell–Weil theorem is also true for number fields. Thus we can define for each number field K

$$\mathcal{R}_\infty(K) := \{r : \text{there exist inf. many non-iso. } E/K \text{ with } r = \operatorname{rk} E\}.$$

Theorem (Mazur–Rubin (2009))

Let K be a number field. Then $0 \in \mathcal{R}_\infty(K)$. Furthermore, assuming that $Ш(E/K)[2^\infty]$ is finite for all E/K, then $1 \in \mathcal{R}_\infty(K)$.

Theorem (K.–Pagano (2025))

Let K be a number field. Then $1 \in \mathcal{R}_\infty(K)$.

The latter result was proven independently by Zywina (2025).

Connections to logic

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

Connections to logic

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.

Connections to logic

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 an integral solution or not.

The MRDP theorem

The MRDP theorem rests on three major results:

The MRDP theorem

The MRDP theorem rests on 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 rests on 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 rests on 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 rests on 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 rests on 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.

In the 1970s, Matiyasevich asked: 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 finiteness of $Ш$. 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 finiteness of $Ш$. 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.

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.

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

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

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.

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

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

Our rank one result builds on ideas developed in the above theorem.

Applications of rank one elliptic curves to logic

Theorem (Cornelissen–Shlapentokh (2008))

Let K be a number field. Assume that there exists E/K with rank one.

Then there is a sequence of sets of primes S_n in K with densities converging to 1, as n goes to infinity, with the property that $\mathbb{Z}$ can be defined over $O_K[S_n^{-1}]$ using at most two universal quantifiers.

Applications of rank one elliptic curves to logic

Theorem (Cornelissen–Shlapentokh (2008))

Let K be a number field. Assume that there exists E/K with rank one.

Then there is a sequence of sets of primes S_n in K with densities converging to 1, as n goes to infinity, with the property that $\mathbb{Z}$ can be defined over $O_K[S_n^{-1}]$ using at most two universal quantifiers.

Theorem (Eisenträger–Everest–Shlapentokh (2011))

Let K be a number field. Assume that there exists E/K with rank one.

For any decomposition $\delta_1 + \cdots + \delta_t = 1$ with $t > 1$ and $\delta_1, \ldots, \delta_t$ computable positive real numbers, there is a partition $S_1, \ldots, S_t$ of the finite places of K, where each S_i has natural density equal to δ_i and such that $\mathbb{Z}$ admits a Diophantine model over $O_K[S_i^{-1}]$.

Rank one

We recall:

Theorem (K.–Pagano (2024))

Let K be a number field. Then $1 \in \mathcal{R}_\infty(K)$.

Rank one

We recall:

Theorem (K.–Pagano (2024))

Let K be a number field. Then $1 \in \mathcal{R}_\infty(K)$.

Where is the difficulty?

Rank one

We recall:

Theorem (K.–Pagano (2024))

Let K be a number field. Then $1 \in \mathcal{R}_\infty(K)$.

Where is the difficulty?

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

Rank one

We recall:

Theorem (K.–Pagano (2024))

Let K be a number field. Then $1 \in \mathcal{R}_\infty(K)$.

Where is the difficulty?

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

Rank one

We recall:

Theorem (K.–Pagano (2024))

Let K be a number field. Then $1 \in \mathcal{R}_\infty(K)$.

Where is the difficulty?

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

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

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:

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:

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

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.

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

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

(2) The group $\mathrm{Sel}^2(E/K)$ is computable and finite dimensional.

(3) The group $\mathrm{Sel}^2(E/K)$ can be computed using "Legendre symbols" between primes dividing Δ_E.

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 $t := (n - a_1)(n - a_2)(n - a_3)$.

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 ranks in this family.

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 ranks in this family. Instead, we consider E_1^t with $t := m(n - a_1 m)(n - a_2 m)(n - a_3 m)$.

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 ranks 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 $\mathrm{rk}\, E_1^t(K) > 0$.

Additive combinatorics

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

$$\dim_{\mathbb{F}_2} \mathrm{Sel}^2(E_1^t/K) = 3,$$

as this implies $0 < \mathrm{rk}\, E_1^t(K) \leq 3 - 2$, so $\mathrm{rk}\, E_1^t(K) = 1$, and we take $E := E_1^t$.

Additive combinatorics

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

$$\dim_{\mathbb{F}_2} \mathrm{Sel}^2(E_1^t/K) = 3,$$

as this implies $0 < \mathrm{rk}\, E_1^t(K) \leq 3 - 2$, so $\mathrm{rk}\, E_1^t(K) = 1$, and we take $E := E_1^t$.

Note that for some constant c depending only on E_1

$$\Delta_{E_1^t} = cm(n - a_1 m)(n - a_2 m)(n - a_3 m).$$

Additive combinatorics

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

$$\dim_{\mathbb{F}_2} \mathrm{Sel}^2(E_1^t/K) = 3,$$

as this implies $0 < \mathrm{rk}\, E_1^t(K) \leq 3 - 2$, so $\mathrm{rk}\, E_1^t(K) = 1$, and we take $E := E_1^t$.

Note that for some constant c depending only on E_1

$$\Delta_{E_1^t} = cm(n - a_1 m)(n - a_2 m)(n - a_3 m).$$

Recall that $\mathrm{Sel}^2(E_1^t/K)$ can be computed from the Legendre symbols between the prime divisors of $\Delta_{E_1^t}$.

Additive combinatorics

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

$$\dim_{\mathbb{F}_2} \mathrm{Sel}^2(E_1^t/K) = 3,$$

as this implies $0 < \mathrm{rk}\, E_1^t(K) \leq 3 - 2$, so $\mathrm{rk}\, E_1^t(K) = 1$, and we take $E := E_1^t$.

Note that for some constant c depending only on E_1

$$\Delta_{E_1^t} = cm(n - a_1 m)(n - a_2 m)(n - a_3 m).$$

Recall that $\mathrm{Sel}^2(E_1^t/K)$ can be computed from the Legendre symbols between the prime divisors of $\Delta_{E_1^t}$.

Our key new insight is to apply additive combinatorics to the problem.

Additive combinatorics

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

$$\dim_{\mathbb{F}_2} \mathrm{Sel}^2(E_1^t/K) = 3,$$

as this implies $0 < \mathrm{rk}\, E_1^t(K) \leq 3 - 2$, so $\mathrm{rk}\, E_1^t(K) = 1$, and we take $E := E_1^t$.

Note that for some constant c depending only on E_1

$$\Delta_{E_1^t} = cm(n - a_1 m)(n - a_2 m)(n - a_3 m).$$

Recall that $\mathrm{Sel}^2(E_1^t/K)$ can be computed from the Legendre symbols between the prime divisors of $\Delta_{E_1^t}$.

Our key new insight is to apply additive combinatorics to the problem. 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

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

$$\dim_{\mathbb{F}_2} \mathrm{Sel}^2(E_1^t/K) = 3,$$

as this implies $0 < \mathrm{rk}\, E_1^t(K) \leq 3 - 2$, so $\mathrm{rk}\, E_1^t(K) = 1$, and we take $E := E_1^t$.

Note that for some constant c depending only on E_1

$$\Delta_{E_1^t} = cm(n - a_1 m)(n - a_2 m)(n - a_3 m).$$

Recall that $\mathrm{Sel}^2(E_1^t/K)$ can be computed from the Legendre symbols between the prime divisors of $\Delta_{E_1^t}$.

Our key new insight is to apply additive combinatorics to the problem. 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 (generalized to number fields by Kai).

Final hurdles

The strategy is then:

Final hurdles

The strategy is then:

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

Final hurdles

The strategy is then:

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

(2) Then twist by $n - a_1 m = P_1, n - a_2 m = P_2, n - a_3 m = P_3, m = \kappa P_4$ in a controlled way, and take

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

Final hurdles

The strategy is then:

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

(2) Then twist by $n - a_1 m = P_1, n - a_2 m = P_2, n - a_3 m = P_3, m = \kappa P_4$ in a controlled way, and take

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

A direct strategy is to take an assignment of Legendre symbols with $\dim_{\mathbb{F}_2} \mathrm{Sel}^2(E_1^t/K) = 3$ (which exists by Heath-Brown/Kane/Smith), and then mimic this assignment with $\kappa, P_1, P_2, P_3, P_4$.

Final hurdles

The strategy is then:

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

(2) Then twist by $n - a_1 m = P_1, n - a_2 m = P_2, n - a_3 m = P_3, m = \kappa P_4$ in a controlled way, and take

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

A direct strategy is to take an assignment of Legendre symbols with $\dim_{\mathbb{F}_2} \mathrm{Sel}^2(E_1^t/K) = 3$ (which exists by Heath-Brown/Kane/Smith), and then mimic this assignment with $\kappa, P_1, P_2, P_3, P_4$.

However, since $P_i = n - a_i m$ and $P_4 \mid m$, there are constraints between (P_i/P_j), and also $(P_1 P_2/r) = (P_1 P_3/r) = (P_2 P_3/r) = +1$ with $r \mid \kappa$.

Final hurdles

The strategy is then:

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

(2) Then twist by $n - a_1 m = P_1, n - a_2 m = P_2, n - a_3 m = P_3, m = \kappa P_4$ in a controlled way, and take

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

A direct strategy is to take an assignment of Legendre symbols with $\dim_{\mathbb{F}_2} \mathrm{Sel}^2(E_1^t/K) = 3$ (which exists by Heath-Brown/Kane/Smith), and then mimic this assignment with $\kappa, P_1, P_2, P_3, P_4$.

However, since $P_i = n - a_i m$ and $P_4 \mid m$, there are constraints between (P_i/P_j), and also $(P_1 P_2/r) = (P_1 P_3/r) = (P_2 P_3/r) = +1$ with $r \mid \kappa$.

The Green–Tao does not provide control over the Legendre symbol (P_i/P_j).

Final hurdles

The strategy is then:

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

(2) Then twist by $n - a_1 m = P_1, n - a_2 m = P_2, n - a_3 m = P_3, m = \kappa P_4$ in a controlled way, and take

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

A direct strategy is to take an assignment of Legendre symbols with $\dim_{\mathbb{F}_2} \mathrm{Sel}^2(E_1^t/K) = 3$ (which exists by Heath-Brown/Kane/Smith), and then mimic this assignment with $\kappa, P_1, P_2, P_3, P_4$.

However, since $P_i = n - a_i m$ and $P_4 \mid m$, there are constraints between (P_i/P_j), and also $(P_1P_2/r) = (P_1P_3/r) = (P_2P_3/r) = +1$ with $r \mid \kappa$.

The Green–Tao does not provide 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).

Even more recent work

There has been a lot of recent work combining additive combinatorics with 2-descent.

Even more recent work

There has been a lot of recent work combining additive combinatorics with 2-descent.

Theorem (Zywina (2025))

We have $2 \in \mathcal{R}_\infty$.

Even more recent work

There has been a lot of recent work combining additive combinatorics with 2-descent.

Theorem (Zywina (2025))

We have $2 \in \mathcal{R}_\infty$.

Theorem (Zywina (2026))

For every number field K*, we have* $\{0, 1, 2, 3, 4\} \subseteq \mathcal{R}_\infty(K)$.

Even more recent work

There has been a lot of recent work combining additive combinatorics with 2-descent.

Theorem (Zywina (2025))

We have $2 \in \mathcal{R}_\infty$.

Theorem (Zywina (2026))

For every number field K*, we have* $\{0, 1, 2, 3, 4\} \subseteq \mathcal{R}_\infty(K)$.

Theorem (K.–Morgan (2025))

For every integer $g \geq 1$ *and every number field* K*, there exists a hyperelliptic curve* C/K *of genus* g *such that* $\operatorname{rk} \operatorname{Jac}(C) = 1$.

Summary

We prove that for every number field K, there is an elliptic curve E of rank one. This has several applications to logic.

Summary

We prove that for every number field K, there is an elliptic curve E of rank one. This has several applications to logic.

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

Summary

We prove that for every number field K, there is an elliptic curve E of rank one. This has several applications to logic.

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

We construct a (quadratic) family with elevated rank in order to guarantee positive rank.

Summary

We prove that for every number field K, there is an elliptic curve E of rank one. This has several applications to logic.

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

We construct a (quadratic) family with elevated rank in order to guarantee positive rank.

By finding a prime specialization with additive combinatorics, 2-descent then shows that $\mathrm{rk}\, E(K) = 1$.

Summary

We prove that for every number field K, there is an elliptic curve E of rank one. This has several applications to logic.

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

We construct a (quadratic) family with elevated rank in order to guarantee positive rank.

By finding a prime specialization with additive combinatorics, 2-descent then shows that $\mathrm{rk}\, E(K) = 1$.

Thank you for your attention!