How often does a polynomial hit a square?

Mohammad Sadek

Sabancı University

April 11, 2019
Algebraic Geometry

Studying zeros of multivariate polynomials using abstract algebraic techniques mainly from commutative algebra. Algebraic Varieties (solutions of systems of polynomial equations). Algebraic varieties include plane curves.

Questions: singular points, topology of the variety, how large the variety is. Complex points of the algebraic varieties; more generally, solutions with coordinates in an algebraically closed field.

Mohammad Sadek

How often does a polynomial hit a square?
Studying zeros of multivariate polynomials using abstract algebraic techniques mainly from commutative algebra.
Studying zeros of multivariate polynomials using abstract algebraic techniques mainly from commutative algebra.

*Algebraic Varieties* (solutions of systems of polynomial equations).

- Complex points of the algebraic varieties; more generally, solutions with coordinates in an algebraically closed field.
Studying zeros of multivariate polynomials using abstract algebraic techniques mainly from commutative algebra.

*Algebraic Varieties* (solutions of systems of polynomial equations).

Algebraic varieties include *plane curves*.
Studying zeros of multivariate polynomials using abstract algebraic techniques mainly from commutative algebra.

**Algebraic Varieties** (solutions of systems of polynomial equations).

Algebraic varieties include *plane curves*.

**Questions**: singular points, topology of the variety, how large the variety is.
Algebraic Geometry

- Studying zeros of multivariate polynomials using abstract algebraic techniques mainly from commutative algebra.
- *Algebraic Varieties* (solutions of systems of polynomial equations).
- Algebraic varieties include *plane curves*.
- **Questions**: singular points, topology of the variety, how large the variety is.
- Complex points of the algebraic varieties; more generally, solutions with coordinates in an algebraically closed field.
The study of the points of an algebraic variety with coordinates in \( \mathbb{Q} \), a number field \( K \); in \( \mathbb{Z} \), a ring of integers of \( K \); or a finite field. Intersection between Algebraic Geometry and Number Theory.

How often does a polynomial hit a square?
The study of the points of an algebraic variety with coordinates in $\mathbb{Q}$, a number field $K$; in $\mathbb{Z}$, a ring of integers of $K$; or a finite field.
The study of the points of an algebraic variety with coordinates in $\mathbb{Q}$, a number field $K$; in $\mathbb{Z}$, a ring of integers of $K$; or a finite field.

Intersection between Algebraic Geometry and Number Theory.
Let $f(x)$ be a polynomial with integer coefficients $f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0$, $a_n \neq 0$, $n \geq 2$.

How often does $f(x)$ take square values in $\mathbb{Q}$?
Let $f(x)$ be a polynomial with integer coefficients

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0, \quad a_n \neq 0, \quad n \geq 2.$$
Let $f(x)$ be a polynomial with integer coefficients

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0, \quad a_n \neq 0, \quad n \geq 2.$$

How often does $f(x)$ take square values in $\mathbb{Q}$?
Example.

Take \( f(x) = x^2 + 1 \). What are the values for \( x \in \mathbb{Q} \) such that \( x^2 + 1 \) is a square in \( \mathbb{Q} \)?

In other words, find the pairs \((x, y) \in \mathbb{Q} \times \mathbb{Q}\) such that \( y^2 = x^2 + 1 \).

What if I want such pairs in \( \mathbb{Z} \times \mathbb{Z} \)?

Trivial! \((x, y) = (0, \pm 1)\).

The equation \( y^2 = x^2 + 1 \) describes an algebraic variety.

If you feel more comfortable with integers, then think of

\[ Y^2 = X^2 + Z^2. \]

Pythagorean Triples!

How often does a polynomial hit a square?
Example. Take $f(x) = x^2 + 1$. What are the values for $x \in \mathbb{Q}$ such that $x^2 + 1$ is a square in $\mathbb{Q}$?
Example. Take $f(x) = x^2 + 1$. What are the values for $x \in \mathbb{Q}$ such that $x^2 + 1$ is a square in $\mathbb{Q}$? In other words, find the pairs $(x, y) \in \mathbb{Q} \times \mathbb{Q}$ such that $y^2 = x^2 + 1$. 

What if I want such pairs in $\mathbb{Z} \times \mathbb{Z}$? Trivial! $(x, y) = (0, \pm 1)$.
Example. Take $f(x) = x^2 + 1$. What are the values for $x \in \mathbb{Q}$ such that $x^2 + 1$ is a square in $\mathbb{Q}$? In other words, find the pairs $(x, y) \in \mathbb{Q} \times \mathbb{Q}$ such that $y^2 = x^2 + 1$.

What if I want such pairs in $\mathbb{Z} \times \mathbb{Z}$?
Example. Take \( f(x) = x^2 + 1 \). What are the values for \( x \in \mathbb{Q} \) such that \( x^2 + 1 \) is a square in \( \mathbb{Q} \)? In other words, find the pairs \( (x, y) \in \mathbb{Q} \times \mathbb{Q} \) such that \( y^2 = x^2 + 1 \).

What if I want such pairs in \( \mathbb{Z} \times \mathbb{Z} \)? Trivial! \( (x, y) = (0, \pm 1) \).
Example. Take \( f(x) = x^2 + 1 \). What are the values for \( x \in \mathbb{Q} \) such that \( x^2 + 1 \) is a square in \( \mathbb{Q} \)? In other words, find the pairs \((x, y) \in \mathbb{Q} \times \mathbb{Q}\) such that \( y^2 = x^2 + 1 \).

What if I want such pairs in \( \mathbb{Z} \times \mathbb{Z} \)? Trivial! \((x, y) = (0, \pm 1)\). The equation \( y^2 = x^2 + 1 \) describes an algebraic variety.
**Example.** Take \( f(x) = x^2 + 1 \). What are the values for \( x \in \mathbb{Q} \) such that \( x^2 + 1 \) is a square in \( \mathbb{Q} \)? In other words, find the pairs \( (x, y) \in \mathbb{Q} \times \mathbb{Q} \) such that \( y^2 = x^2 + 1 \).

What if I want such pairs in \( \mathbb{Z} \times \mathbb{Z} \)? Trivial! \( (x, y) = (0, \pm 1) \). The equation \( y^2 = x^2 + 1 \) describes an algebraic variety.

If you feel more comfortable with integers, then think of \( Y^2 = X^2 + Z^2 \).
Example. Take \( f(x) = x^2 + 1 \). What are the values for \( x \in \mathbb{Q} \) such that \( x^2 + 1 \) is a square in \( \mathbb{Q} \)? In other words, find the pairs \( (x, y) \in \mathbb{Q} \times \mathbb{Q} \) such that \( y^2 = x^2 + 1 \).

What if I want such pairs in \( \mathbb{Z} \times \mathbb{Z} \)? Trivial! \( (x, y) = (0, \pm 1) \). The equation \( y^2 = x^2 + 1 \) describes an algebraic variety.

If you feel more comfortable with integers, then think of \( Y^2 = X^2 + Z^2 \). Pythagorean Triples!
We need to find the set of zeros of $Y^2 = X^2 + Z^2$. 

Are they finite? Are they infinite? Why?

Any solution to $X^2 + Z^2 = Y^2$ is given by $(X, Y, Z) = (s^2 - t^2, 2st, s^2 + t^2)$, $s, t \in \mathbb{Z}$. 

Mohammad Sadek
How often does a polynomial hit a square?
Square values taken by $x^2 + 1$

- We need to find the set of zeros of $Y^2 = X^2 + Z^2$.
- This is a list of such zeros:

  $$(3, 4, 5) \quad (9, 40, 41) \quad (36, 77, 85) \quad (65, 72, 97)$$

Mohammad Sadek

How often does a polynomial hit a square?
We need to find the set of zeros of \( Y^2 = X^2 + Z^2 \).

This is a list of such zeros:

\[
(3, 4, 5) \quad (9, 40, 41) \quad (36, 77, 85) \quad (65, 72, 97) \\
(51, 140, 149) \quad (84, 187, 205) \quad (105, 208, 233) \quad (68, 285, 293)
\]
We need to find the set of zeros of $Y^2 = X^2 + Z^2$.

This is a list of such zeros:

$(3, 4, 5) \quad (9, 40, 41) \quad (36, 77, 85) \quad (65, 72, 97)$
$(51, 140, 149) \quad (84, 187, 205) \quad (105, 208, 233) \quad (68, 285, 293)$
$(12709, 13500, 18541)$
Square values taken by $x^2 + 1$

- We need to find the set of zeros of $Y^2 = X^2 + Z^2$.
- This is a list of such zeros:
  - $(3, 4, 5)$
  - $(9, 40, 41)$
  - $(36, 77, 85)$
  - $(65, 72, 97)$
  - $(51, 140, 149)$
  - $(84, 187, 205)$
  - $(105, 208, 233)$
  - $(68, 285, 293)$
  - $(12709, 13500, 18541)$

- Are they finite?
We need to find the set of zeros of $Y^2 = X^2 + Z^2$.

This is a list of such zeros:

$(3, 4, 5) \quad (9, 40, 41) \quad (36, 77, 85) \quad (65, 72, 97)\)
$(51, 140, 149) \quad (84, 187, 205) \quad (105, 208, 233) \quad (68, 285, 293)\)
$(12709, 13500, 18541)\)

Are they finite? Are they infinite?
We need to find the set of zeros of $Y^2 = X^2 + Z^2$.

This is a list of such zeros:

$(3, 4, 5)$ $(9, 40, 41)$ $(36, 77, 85)$ $(65, 72, 97)$
$(51, 140, 149)$ $(84, 187, 205)$ $(105, 208, 233)$ $(68, 285, 293)$
$(12709, 13500, 18541)$

Are they finite? Are they infinite? Why?
Square values taken by $x^2 + 1$

- We need to find the set of zeros of $Y^2 = X^2 + Z^2$.
- This is a list of such zeros:

  
  \[
  (3, 4, 5) \quad (9, 40, 41) \quad (36, 77, 85) \quad (65, 72, 97) \\
  (51, 140, 149) \quad (84, 187, 205) \quad (105, 208, 233) \quad (68, 285, 293) \\
  (12709, 13500, 18541)
  \]

- Are they finite? Are they infinite? Why?
- Any solution to $X^2 + Z^2 = Y^2$ is given by

  \[
  (X, Y, Z) = (s^2 - t^2, 2st, s^2 + t^2), \quad s, t \in \mathbb{Z}.
  \]
Squares represented by sums of multiples of squares

Theorem

Let $C$ be the conic described by $ax^2 + by^2 + c = 0$, where $a, b, c$ are square free coprime integers. The set of rational points is the set

$$C(\mathbb{Q}) = \{(x, y) : ax^2 + by^2 + c = 0, x, y \in \mathbb{Q}\}.$$

Then

1) Either $C(\mathbb{Q}) = \emptyset$, or
2) $C(\mathbb{Q}) \neq \emptyset$, hence infinite.

This means that once we have a rational point on $C$, there exists infinitely many!

But how would I find a rational point in the first place?

Mohammad Sadek
How often does a polynomial hit a square?
Theorem

Let $C$ be the conic described by $ax^2 + by^2 + c = 0$, where $a, b, c$ are square free coprime integers. The set of \textbf{rational points} is the set

$$C(\mathbb{Q}) = \{(x, y) : ax^2 + by^2 + c = 0, x, y \in \mathbb{Q}\}.$$ 

Then

1) Either $C(\mathbb{Q}) = \emptyset$, or
Theorem

Let $C$ be the conic described by $ax^2 + by^2 + c = 0$, where $a, b, c$ are square free coprime integers. The set of rational points is the set

$$C(\mathbb{Q}) = \{(x, y) : ax^2 + by^2 + c = 0, x, y \in \mathbb{Q}\}.$$  

Then

1) Either $C(\mathbb{Q}) = \emptyset$, or

2) $C(\mathbb{Q}) \neq \emptyset$, 

But how would I find a rational point in the first place?
Squares represented by sums of multiples of squares

Theorem

Let $C$ be the conic described by $ax^2 + by^2 + c = 0$, where $a, b, c$ are square free coprime integers. The set of rational points is the set

$$C(\mathbb{Q}) = \{(x, y) : ax^2 + by^2 + c = 0, x, y \in \mathbb{Q}\}.$$ 

Then

1) Either $C(\mathbb{Q}) = \emptyset$, or
2) $C(\mathbb{Q}) \neq \emptyset$, hence infinite.
Squares represented by sums of multiples of squares

Theorem

Let $C$ be the conic described by $ax^2 + by^2 + c = 0$, where $a, b, c$ are square free coprime integers. The set of rational points is the set

$$C(\mathbb{Q}) = \{(x, y) : ax^2 + by^2 + c = 0, x, y \in \mathbb{Q}\}.$$  

Then

1) Either $C(\mathbb{Q}) = \emptyset$, or
2) $C(\mathbb{Q}) \neq \emptyset$, hence infinite.

This means that once we have a rational point on $C$, there exists infinitely many!
Theorem

Let \( C \) be the conic described by \( ax^2 + by^2 + c = 0 \), where \( a, b, c \) are square free coprime integers. The set of rational points is the set

\[
C(\mathbb{Q}) = \{(x, y) : ax^2 + by^2 + c = 0, x, y \in \mathbb{Q}\}.
\]

Then

1) Either \( C(\mathbb{Q}) = \emptyset \), or
2) \( C(\mathbb{Q}) \neq \emptyset \), hence infinite.

This means that once we have a rational point on \( C \), there exists infinitely many! But how would I find a rational point in the first place?
Theorem (Legendre)

The curve \( C : ax^2 + by^2 + c = 0 \), where \( a, b, c \) are square free coprime integers, has a rational point if and only if

1) \( a, b, c \) do not all have the same sign, and
2) the congruences
   \[
   \begin{align*}
   &ax^2 + b \equiv 0 \pmod{c} \\
   &by^2 + c \equiv 0 \pmod{a} \\
   &cx^2 + a \equiv 0 \pmod{b}
   \end{align*}
   \]
   have solutions \( s, t, u \in \mathbb{Z} \).
Theorem (Legendre)

The curve $C : ax^2 + by^2 + c = 0$, where $a, b, c$ are square free coprime integers, has a rational point if and only if

1) $a, b, c$ do not all have the same sign, and
Theorem (Legendre)

The curve $C : ax^2 + by^2 + c = 0$, where $a, b, c$ are square free coprime integers, has a rational point if and only if

1) $a, b, c$ do not all have the same sign, and

2) the congruences

\[ as^2 + b \equiv 0 \pmod{c} \]
\[ bt^2 + c \equiv 0 \pmod{a} \]
\[ cu^2 + a \equiv 0 \pmod{b} \]

have solutions $s, t, u \in \mathbb{Z}$.
What if I have linear terms in $x$ or $y$?

Given a conic $C$ described by a homogeneous polynomial of degree 2 with rational coefficients, $C$ is isomorphic to a conic of the form $aX^2 + bY^2 + cZ^2 = 0$ where $a, b, c \in \mathbb{Z}$ are coprime and square free.

Complete Squares!

The picture is complete here!
What if I have linear terms in $x$ or $y$?

Given a conic $C$ described by a homogeneous polynomial of degree 2 with rational coefficient, $C$ is isomorphic to a conic of the form $aX^2 + bY^2 + cZ^2 = 0$ where $a, b, c \in \mathbb{Z}$ are coprime and square free.
What if I have linear terms in $x$ or $y$?

Given a conic $C$ described by a homogeneous polynomial of degree 2 with rational coefficient, $C$ is isomorphic to a conic of the form $aX^2 + bY^2 + cZ^2 = 0$ where $a, b, c \in \mathbb{Z}$ are coprime and square free. Complete Squares!
Polynomials of degree 2

- What if I have linear terms in $x$ or $y$?

- Given a conic $C$ described by a homogeneous polynomial of degree 2 with rational coefficient, $C$ is isomorphic to a conic of the form $aX^2 + bY^2 + cZ^2 = 0$ where $a, b, c \in \mathbb{Z}$ are coprime and square free. Complete Squares!

- The picture is complete here!
The problem.

Let \( f(x) = a_n x^n + a_{n-1} x^{n-1} + \ldots + a_0 \in \mathbb{Z}[x] \). When does \( f(x) \) take a square value?
The problem.

- Let $f(x) = a_nx^n + a_{n-1}x^{n-1} + \ldots + a_0 \in \mathbb{Z}[x]$. When does $f(x)$ take a square value?
- In other words, when does the curve $C$ described by $y^2 = f(x)$ has a rational point?
The problem.

- Let \( f(x) = a_n x^n + a_{n-1} x^{n-1} + \ldots + a_0 \in \mathbb{Z}[x] \). When does \( f(x) \) take a square value?

- In other words, when does the curve \( C \) described by \( y^2 = f(x) \) has a rational point?

- Is \( C(\mathbb{Q}) = \{ (x, y) : y^2 = f(x), \ x, y \in \mathbb{Q} \} \neq \emptyset \)?
The problem.

- Let \( f(x) = a_n x^n + a_{n-1} x^{n-1} + \ldots + a_0 \in \mathbb{Z}[x]. \) When does \( f(x) \) take a square value?
- In other words, when does the curve \( C \) described by \( y^2 = f(x) \) has a rational point?
- Is \( C(\mathbb{Q}) = \{(x, y) : y^2 = f(x), \ x, y \in \mathbb{Q}\} \neq \emptyset? \)
- If so, then how large \( C(\mathbb{Q}) \) is?
The problem.

- Let $f(x) = a_n x^n + a_{n-1} x^{n-1} + \ldots + a_0 \in \mathbb{Z}[x]$. When does $f(x)$ take a square value?
- In other words, when does the curve $C$ described by $y^2 = f(x)$ have a rational point?
- Is $C(\mathbb{Q}) = \{(x, y) : y^2 = f(x), x, y \in \mathbb{Q}\} \neq \emptyset$?
- If so, then how large $C(\mathbb{Q})$ is? Finite (how finite?).
The problem.

Let \( f(x) = a_n x^n + a_{n-1} x^{n-1} + \ldots + a_0 \in \mathbb{Z}[x] \). When does \( f(x) \) take a square value?

In other words, when does the curve \( C \) described by \( y^2 = f(x) \) has a rational point?

Is \( C(\mathbb{Q}) = \{(x, y) : y^2 = f(x), x, y \in \mathbb{Q}\} \neq \emptyset \)?

If so, then how large \( C(\mathbb{Q}) \) is? Finite (how finite?). Infinite (how infinite?)
The problem.

- Let $f(x) = a_n x^n + a_{n-1} x^{n-1} + \ldots + a_0 \in \mathbb{Z}[x]$. When does $f(x)$ take a square value?
- In other words, when does the curve $C$ described by $y^2 = f(x)$ have a rational point?
- Is $C(\mathbb{Q}) = \{(x, y) : y^2 = f(x), x, y \in \mathbb{Q}\} \neq \emptyset$?
- If so, then how large is $C(\mathbb{Q})$? Finite (how finite?). Infinite (how infinite?)
- The answer is beautiful! It depends on the graph of $C$ in $\mathbb{C}^2$. 

Mohammad Sadek

How often does a polynomial hit a square?
Topology and rational points

Curves given by $y^2 = f(x)$, $\deg f \geq 3$, are one family of curves called (hyper)elliptic curves. They form one subfamily out of the family of algebraic curves described by $h(x, y) = 0$. The topology of a curve $C$ defined by $h(x, y) = 0$ but thought of as a surface in $C_2$ provides us with an answer to our previous question.

How often does a polynomial hit a square?
Curves given by $y^2 = f(x)$, $\deg f \geq 3$, are one family of curves called \textit{(hyper)elliptic curves}.
Curves given by $y^2 = f(x)$, $\deg f \geq 3$, are one family of curves called (hyper)elliptic curves.

They form one subfamily out of the family of algebraic curves described by $h(x, y) = 0$. 

Mohammad Sadek

How often does a polynomial hit a square?
Topology and rational points

Curves given by $y^2 = f(x)$, $\deg f \geq 3$, are one family of curves called (hyper)elliptic curves.

They form one subfamily out of the family of algebraic curves described by $h(x, y) = 0$.

The topology of a curve $C$ defined by $h(x, y) = 0$ but thought of as a surface in $\mathbb{C}^2$ provides us with an answer to our previous question.
Recall

\[ C(\mathbb{Q}) = \{(x, y) : h(x, y) = 0, \quad x, y \in \mathbb{Q}\}. \]

**Theorem**

*Let* \( C \) *be an algebraic curve defined by* \( h(x, y) = 0 \) *where* \( h(x, y) \) *has integer coefficients.*

1. If \( g = 0 \), then \( C(\mathbb{Q}) \) *is either empty or infinite.*
2. If \( g = 1 \), then \( C(\mathbb{Q}) \) *is either finite or infinite.*
3. If \( g \geq 2 \), then \( C(\mathbb{Q}) \) *is finite.*

*(Mordell's Conjecture, Faltings' Theorem 1983)*
Recall

\[ C(\mathbb{Q}) = \{(x, y) : h(x, y) = 0, \quad x, y \in \mathbb{Q}\}. \]

**Theorem**

Let \( C \) be an algebraic curve defined by \( h(x, y) = 0 \) where \( h(x, y) \) has integer coefficients. Let \( g \) be the genus of the surface given by \( h(x, y) = 0 \) in \( \mathbb{C}^2 \).

1. If \( g = 0 \), then \( C(\mathbb{Q}) \) is either empty or infinite.
2. If \( g = 1 \), then \( C(\mathbb{Q}) \) is either finite or infinite.
3. If \( g \geq 2 \), then \( C(\mathbb{Q}) \) is finite.
Recall

\[ C(\mathbb{Q}) = \{(x, y) : h(x, y) = 0, \quad x, y \in \mathbb{Q}\}. \]

**Theorem**

Let \( C \) be an algebraic curve defined by \( h(x, y) = 0 \) where \( h(x, y) \) has integer coefficients. Let \( g \) be the genus of the surface given by \( h(x, y) = 0 \) in \( \mathbb{C}^2 \).

1) If \( g = 0 \), then \( C(\mathbb{Q}) \) is either **empty** or **infinite**.
Recall

\[ C(\mathbb{Q}) = \{(x, y) : h(x, y) = 0, \quad x, y \in \mathbb{Q}\}. \]

**Theorem**

Let \( C \) be an algebraic curve defined by \( h(x, y) = 0 \) where \( h(x, y) \) has integer coefficients. Let \( g \) be the genus of the surface given by \( h(x, y) = 0 \) in \( \mathbb{C}^2 \).

1) If \( g = 0 \), then \( C(\mathbb{Q}) \) is either **empty** or **infinite**.
2) If \( g = 1 \), then \( C(\mathbb{Q}) \) is either **finite** or **infinite**.
Recall

\[ C(\mathbb{Q}) = \{(x, y) : h(x, y) = 0, \quad x, y \in \mathbb{Q}\}. \]

**Theorem**

Let \( C \) be an algebraic curve defined by \( h(x, y) = 0 \) where \( h(x, y) \) has integer coefficients. Let \( g \) be the genus of the surface given by \( h(x, y) = 0 \) in \( \mathbb{C}^2 \).

1) If \( g = 0 \), then \( C(\mathbb{Q}) \) is either **empty** or **infinite**.

2) If \( g = 1 \), then \( C(\mathbb{Q}) \) is either **finite** or **infinite**.

3) If \( g \geq 2 \), then \( C(\mathbb{Q}) \) is finite.

(Mordell's Conjecture, Faltings' Theorem 1983)
Recall

\[ C(\mathbb{Q}) = \{(x, y) : h(x, y) = 0, \quad x, y \in \mathbb{Q}\}. \]

**Theorem**

Let \( C \) be an algebraic curve defined by \( h(x, y) = 0 \) where \( h(x, y) \) has integer coefficients. Let \( g \) be the genus of the surface given by \( h(x, y) = 0 \) in \( \mathbb{C}^2 \).

1) If \( g = 0 \), then \( C(\mathbb{Q}) \) is either **empty** or **infinite**.
2) If \( g = 1 \), then \( C(\mathbb{Q}) \) is either **finite** or **infinite**.
3) If \( g \geq 2 \), then \( C(\mathbb{Q}) \) is finite. (Mordell’s Conjecture, Faltings’ Theorem 1983)
Degree and rational points

Let $C$ be described by $y^2 = f(x)$ where $\deg f(x) = n$ and $f(x)$ has no double roots.
Degree and rational points

Let $C$ be described by $y^2 = f(x)$ where $\deg f(x) = n$ and $f(x)$ has no double roots. $f(x)$ has no double roots to ensure smoothness.
Degree and rational points

Let $C$ be described by $y^2 = f(x)$ where $\text{deg } f(x) = n$ and $f(x)$ has no double roots. $f(x)$ has no double roots to ensure smoothness. The genus of the surface defined by the latter equation in $\mathbb{C}^2$ is

$$g = \left\lfloor \frac{n - 1}{2} \right\rfloor.$$
Degree and rational points

Let $C$ be described by $y^2 = f(x)$ where $\deg f(x) = n$ and $f(x)$ has no double roots. $f(x)$ has no double roots to ensure smoothness. The genus of the surface defined by the latter equation in $\mathbb{C}^2$ is

$$g = \left\lfloor \frac{n - 1}{2} \right\rfloor.$$

**Theorem**

*Let $C$ be a curve defined by the equation $y^2 = f(x)$ where $f(x)$ is a polynomial whose coefficients are integers and has no double roots.*

1) If $\deg f(x) = 1$ or $2$, then either $C(\mathbb{Q})$ is empty or infinite. Effective!

2) If $\deg f(x) = 3$ or $4$, then either $C(\mathbb{Q})$ is finite or infinite. Ineffective!

3) If $\deg f(x) \geq 5$, then $C(\mathbb{Q})$ is finite. Ineffective!
Degree and rational points

Let $C$ be described by $y^2 = f(x)$ where $\deg f(x) = n$ and $f(x)$ has no double roots. $f(x)$ has no double roots to ensure smoothness. The genus of the surface defined by the latter equation in $\mathbb{C}^2$ is

$$g = \left\lfloor \frac{n - 1}{2} \right\rfloor.$$

Theorem

Let $C$ be a curve defined by the equation $y^2 = f(x)$ where $f(x)$ is a polynomial whose coefficients are integers and has no double roots.

1) If $\deg f(x) = 1$ or 2, then either $C(\mathbb{Q})$ is empty or infinite.
Let $C$ be described by $y^2 = f(x)$ where $\deg f(x) = n$ and $f(x)$ has no double roots. $f(x)$ has no double roots to ensure smoothness. The genus of the surface defined by the latter equation in $\mathbb{C}^2$ is

$$g = \left\lfloor \frac{n - 1}{2} \right\rfloor.$$

**Theorem**

Let $C$ be a curve defined by the equation $y^2 = f(x)$ where $f(x)$ is a polynomial whose coefficients are integers and has no double roots.

1) If $\deg f(x) = 1$ or 2, then either $C(\mathbb{Q})$ is empty or infinite. Effective!
Degree and rational points

Let $C$ be described by $y^2 = f(x)$ where $\deg f(x) = n$ and $f(x)$ has no double roots. $f(x)$ has no double roots to ensure smoothness. The genus of the surface defined by the latter equation in $\mathbb{C}^2$ is

$$g = \left\lfloor \frac{n - 1}{2} \right\rfloor.$$

Theorem

Let $C$ be a curve defined by the equation $y^2 = f(x)$ where $f(x)$ is a polynomial whose coefficients are integers and has no double roots.

1) If $\deg f(x) = 1$ or 2, then either $C(\mathbb{Q})$ is empty or infinite. Effective!

2) If $\deg f(x) = 3$ or 4, then either $C(\mathbb{Q})$ is finite or infinite.
Let $C$ be described by $y^2 = f(x)$ where $\deg f(x) = n$ and $f(x)$ has no double roots. $f(x)$ has no double roots to ensure smoothness. The genus of the surface defined by the latter equation in $\mathbb{C}^2$ is

$$g = \left\lfloor \frac{n - 1}{2} \right\rfloor.$$ 

**Theorem**

Let $C$ be a curve defined by the equation $y^2 = f(x)$ where $f(x)$ is a polynomial whose coefficients are integers and has no double roots.

1) If $\deg f(x) = 1$ or $2$, then either $C(\mathbb{Q})$ is empty or infinite. Effective!

2) If $\deg f(x) = 3$ or $4$, then either $C(\mathbb{Q})$ is finite or infinite. Ineffective!
Degree and rational points

Let $C$ be described by $y^2 = f(x)$ where $\deg f(x) = n$ and $f(x)$ has no double roots. $f(x)$ has no double roots to ensure smoothness. The genus of the surface defined by the latter equation in $\mathbb{C}^2$ is

$$g = \left\lfloor \frac{n-1}{2} \right\rfloor.$$ 

**Theorem**

Let $C$ be a curve defined by the equation $y^2 = f(x)$ where $f(x)$ is a polynomial whose coefficients are integers and has no double roots.

1) If $\deg f(x) = 1$ or 2, then either $C(\mathbb{Q})$ is empty or infinite. Effective!

2) If $\deg f(x) = 3$ or 4, then either $C(\mathbb{Q})$ is finite or infinite. Ineffective!

3) If $\deg f(x) \geq 5$, then $C(\mathbb{Q})$ is finite.
Degree and rational points

Let $C$ be described by $y^2 = f(x)$ where $\deg f(x) = n$ and $f(x)$ has no double roots. $f(x)$ has no double roots to ensure smoothness. The genus of the surface defined by the latter equation in $\mathbb{C}^2$ is

$$g = \left\lfloor \frac{n - 1}{2} \right\rfloor.$$

**Theorem**

Let $C$ be a curve defined by the equation $y^2 = f(x)$ where $f(x)$ is a polynomial whose coefficients are integers and has no double roots.

1) If $\deg f(x) = 1$ or $2$, then either $C(\mathbb{Q})$ is empty or infinite. **Effective!**

2) If $\deg f(x) = 3$ or $4$, then either $C(\mathbb{Q})$ is finite or infinite. **Ineffective!**

3) If $\deg f(x) \geq 5$, then $C(\mathbb{Q})$ is finite. **Ineffective!**
Genus 1 curves

\[ y^2 = f(x) \]

When deg \( f(x) \) = 3 or 4, this is the first case where we do not understand in general what is happening. We do not know how to decide whether \( C(\mathbb{Q}) \) is finite or infinite. In fact the situation is even worse. We do not know how to decide whether a nontrivial rational point exists on \( C \) or not. Let alone finding an algorithm which lists all the rational points in \( C(\mathbb{Q}) \).
Genus 1 curves

\[ y^2 = f(x) \]

- When \( \text{deg } f(x) = 3 \) or 4, this is the first case where we do not understand in general what is happening.
Genus 1 curves

\[ y^2 = f(x) \]

- When \( \deg f(x) = 3 \) or \( 4 \), this is the first case where we do not understand in general what is happening.
- We do not know how to decide whether \( C(\mathbb{Q}) \) is finite or infinite.

Mohammad Sadek

How often does a polynomial hit a square?
When \( \text{deg } f(x) = 3 \) or 4, this is the first case where we do not understand in general what is happening.

We do not know how to decide whether \( C(\mathbb{Q}) \) is finite or infinite.

In fact the situation is even worse. We do not know how to decide whether a nontrivial rational point exists on \( C \) or not.
When $\deg f(x) = 3$ or 4, this is the first case where we do not understand in general what is happening.

We do not know how to decide whether $C(\mathbb{Q})$ is finite or infinite.

In fact the situation is even worse. We do not know how to decide whether a nontrivial rational point exists on $C$ or not. Let alone finding an algorithm which lists all the rational points in $C(\mathbb{Q})$. 

$y^2 = f(x)$
Number Theory

If \( \deg f(x) = 3 \), how often does \( f(x) \) attain a square rational value over the rational numbers?

Geometry.

Let \( E \) be the curve described by the equation \( y^2 = f(x) \).

What is the structure of the set of rational points \( E(\mathbb{Q}) = \{ (x, y) : y^2 = f(x), x, y \in \mathbb{Q} \} \).

From now on the curve \( E \) is called an elliptic curve.

A simple transformation allows us to assume that \( f(x) = x^3 + ax + b \), \( a, b \in \mathbb{Q} \).

Algebra.

A group structure!
Number Theory If \( \deg f(x) = 3 \), how often does \( f(x) \) attain a square rational value over the rational numbers?
Number Theory If $\deg f(x) = 3$, how often does $f(x)$ attain a square rational value over the rational numbers?

Geometry.
- **Number Theory** If $\deg f(x) = 3$, how often does $f(x)$ attain a square rational value over the rational numbers?
- **Geometry.** Let $E$ be the curve described by the equation $y^2 = f(x)$.

A simple transformation allows us to assume that $f(x) = x^3 + ax + b$, $a, b \in \mathbb{Q}$. 

Algebra. A group structure!
**Number Theory** If $\deg f(x) = 3$, how often does $f(x)$ attain a square rational value over the rational numbers?

**Geometry.** Let $E$ be the curve described by the equation $y^2 = f(x)$. What is the structure of the set of rational points $E(\mathbb{Q}) = \{(x, y) : y^2 = f(x), \ x, y \in \mathbb{Q}\}$. From now on the curve $E$ is called an elliptic curve. A simple transformation allows us to assume that $f(x) = x^3 + ax + b$, $a, b \in \mathbb{Q}$. **Algebra.** A group structure!
**Number Theory** If \( \text{deg } f(x) = 3 \), how often does \( f(x) \) attain a square rational value over the rational numbers?

**Geometry.** Let \( E \) be the curve described by the equation \( y^2 = f(x) \). What is the structure of the set of rational points

\[
E(\mathbb{Q}) = \{(x, y) : y^2 = f(x), \quad x, y \in \mathbb{Q}\}.
\]

From now on the curve \( E \) is called an **elliptic curve**.
• **Number Theory** If \( \deg f(x) = 3 \), how often does \( f(x) \) attain a square rational value over the rational numbers?

• **Geometry.** Let \( E \) be the curve described by the equation \( y^2 = f(x) \). What is the structure of the set of rational points

\[
E(\mathbb{Q}) = \{(x, y) : y^2 = f(x), \quad x, y \in \mathbb{Q}\}.
\]

• From now on the curve \( E \) is called an **elliptic curve**.

• A simple transformation allows us to assume that

\[
f(x) = x^3 + ax + b, \quad a, b \in \mathbb{Q}.
\]
- **Number Theory** If $\deg f(x) = 3$, how often does $f(x)$ attain a square rational value over the rational numbers?

- **Geometry.** Let $E$ be the curve described by the equation $y^2 = f(x)$. What is the structure of the set of rational points

  
  $E(\mathbb{Q}) = \{(x, y) : y^2 = f(x), \ x, y \in \mathbb{Q}\}$.

- From now on the curve $E$ is called an **elliptic curve**.

- A simple transformation allows us to assume that $f(x) = x^3 + ax + b$, $a, b \in \mathbb{Q}$.

- **Algebra.**
Number Theory If \( \deg f(x) = 3 \), how often does \( f(x) \) attain a square rational value over the rational numbers?

Geometry. Let \( E \) be the curve described by the equation \( y^2 = f(x) \). What is the structure of the set of rational points

\[
E(\mathbb{Q}) = \{(x, y) : y^2 = f(x), \ x, y \in \mathbb{Q}\}.
\]

From now on the curve \( E \) is called an **elliptic curve**.

A simple transformation allows us to assume that

\[ f(x) = x^3 + ax + b, \ a, b \in \mathbb{Q}. \]

Algebra. A group structure!
Elliptic curves

\[ y^2 = x^3 + ax + b, \quad a, b \in \mathbb{Q} \]
Elliptic curves

Elliptic curves are defined by the equation:

\[ y^2 = x^3 + ax + b, \quad a, b \in \mathbb{Q} \]
Elliptic curves

The equation of an elliptic curve is:

$$y^2 = x^3 + ax + b, \quad a, b \in \mathbb{Q}$$
Suppose $P_1 = (x_1, y_1)$ and $P_2 = (x_2, y_2)$ are points on the elliptic curve $E : y^2 = x^3 + Ax + B$. 

Mohammad Sadek

How often does a polynomial hit a square?
Suppose $P_1 = (x_1, y_1)$ and $P_2 = (x_2, y_2)$ are points on the elliptic curve $E : y^2 = x^3 + Ax + B$. We assume $P_1 \neq P_2$. Let 

$$\lambda = \frac{y_2 - y_1}{x_2 - x_1}.$$
Suppose $P_1 = (x_1, y_1)$ and $P_2 = (x_2, y_2)$ are points on the elliptic curve $E : y^2 = x^3 + Ax + B$. We assume $P_1 \neq P_2$. Let
\[\lambda = \frac{y_2 - y_1}{x_2 - x_1}.
\]
One has
\[P_1 + P_2 = (\lambda^2 - x_1 - x_2, -\lambda^3 + 2\lambda x_1 + \lambda x_2 - y_1).\]
An Example

\[ E : y^2 = x^3 + 2x + 3 \]
An Example

\[ E : y^2 = x^3 + 2x + 3 \]

The point \( P = (3, 6) \in E \)
An Example

\[ E : y^2 = x^3 + 2x + 3 \]

- The point \( P = (3, 6) \in E \)
- \( 2P = (-23/144, 2827/1728) \)
An Example

$E : y^2 = x^3 + 2x + 3$

- The point $P = (3, 6) \in E$
- $2P = (-23/144, 2827/1728)$
- $3P = (-193101/207025, -53536482/94196375)$
An Example

$E : y^2 = x^3 + 2x + 3$

- The point $P = (3, 6) \in E$
- $2P = (-23/144, 2827/1728)$
- $3P = (-193101/207025, -53536482/94196375)$
- $4P = $(3324592417/4603351104, 685780509326543/312328165704192)
Subgroups of $E$

Let $K$ be a field. Let $E$ be an elliptic curve defined by $y^2 = x^3 + Ax + B$ with $A, B \in K$.

Then $E(K)$ is a subgroup of $E$.

Mohammad Sadek
How often does a polynomial hit a square?
Let $K$ be a field. Let $E$ be an elliptic curve defined by

$$y^2 = x^3 + Ax + B \text{ with } A, B \in K.$$
Let $K$ be a field. Let $E$ be an elliptic curve defined by

$$y^2 = x^3 + Ax + B$$
with $A, B \in K$.

Let

$$E(K) = \{(x, y) \in E : x, y \in K\} \cup \{O_E\}.$$ 

Then $E(K)$ is a subgroup of $E$. 

Mohammad Sadek

How often does a polynomial hit a square?
History: how did they originate?

Recall that the arc length of the upper half of $x^2 + y^2 = a^2$ is given by
\[
\int_{-a}^{a} \sqrt{a^2 - x^2} \, dx.
\]
The arc length of the upper half of $\frac{x^2}{a^2} + \frac{y^2}{b^2} = 1$, $b < a$, is given by
\[
\int_{-a}^{a} \sqrt{a^2 - \left(1 - \frac{b^2}{a^2}\right)x^2} \, dx.
\]
Mohammad Sadek

How often does a polynomial hit a square?
History: how did they originate?

Recall that the arc length of the upper half of $x^2 + y^2 = a^2$ is given by

$$\int_{-a}^{a} \frac{a}{\sqrt{a^2 - x^2}} \, dx.$$
Recall that the arc length of the upper half of \( x^2 + y^2 = a^2 \) is given by
\[
\int_{-a}^{a} \frac{a}{\sqrt{a^2 - x^2}} \, dx.
\]

The arc length of the upper half of \( x^2/a^2 + y^2/b^2 = 1, \ b < a, \) is given by
\[
\int_{-a}^{a} \sqrt{\frac{a^2 - (1 - b^2/a^2)x^2}{a^2 - x^2}} \, dx.
\]
Set $k^2 = 1 - \frac{b^2}{a^2}$ and take the substitution $x \mapsto ax$. Then the arc length becomes
\[
a \int_{1}^{1} \sqrt{1 - k^2 x^2} \, dx.
\]
Recall that $y^2 = (1 - x^2)(1 - k^2 x^2)$ is an elliptic curve. The latter arc length is given by
\[
a \int_{1}^{1} \sqrt{(1 - x^2)(1 - k^2 x^2)} \, dx.
\]
An elliptic integral is an integral of the form
\[
\int R(x, y) \, dx,
\]
where $R(x, y)$ is a rational function of the coordinates $(x, y)$ on an elliptic curve $E$ $y^2 = f(x)$, $f(x)$ is a cubic or a quartic polynomial.
Set $k^2 = 1 - b^2/a^2$ and take the substitution $x \mapsto ax$. Then the arc length becomes

$$a \int_{-1}^{1} \sqrt{\frac{1 - k^2x^2}{1 - x^2}} \, dx$$
Set $k^2 = 1 - b^2 / a^2$ and take the substitution $x \mapsto ax$. Then the arc length becomes

$$a \int_{-1}^{1} \sqrt{\frac{1 - k^2 x^2}{1 - x^2}} \, dx = a \int_{-1}^{1} \frac{1 - k^2 x^2}{\sqrt{(1 - x^2)(1 - k^2 x^2)}} \, dx.$$
Set $k^2 = 1 - b^2/a^2$ and take the substitution $x \mapsto ax$. Then the arc length becomes

$$a \int_{-1}^{1} \sqrt{\frac{1 - k^2 x^2}{1 - x^2}} \, dx = a \int_{-1}^{1} \frac{1 - k^2 x^2}{\sqrt{(1 - x^2)(1 - k^2 x^2)}} \, dx.$$ 

Recall that $y^2 = (1 - x^2)(1 - k^2 x^2)$ is an elliptic curve.
Set $k^2 = 1 - b^2/a^2$ and take the substitution $x \mapsto ax$. Then the arc length becomes

$$a \int_{-1}^{1} \sqrt{\frac{1 - k^2 x^2}{1 - x^2}} \, dx = a \int_{-1}^{1} \frac{1 - k^2 x^2}{\sqrt{(1 - x^2)(1 - k^2 x^2)}} \, dx.$$ 

Recall that $y^2 = (1 - x^2)(1 - k^2 x^2)$ is an elliptic curve. The latter arc length is given by

$$a \int_{-1}^{1} \frac{1 - k^2 x^2}{y} \, dx.$$
Set \( k^2 = 1 - b^2/a^2 \) and take the substitution \( x \mapsto ax \). Then the arc length becomes

\[
a \int_{-1}^{1} \sqrt{1 - k^2x^2} \frac{dx}{1 - x^2} = a \int_{-1}^{1} \frac{1 - k^2x^2}{\sqrt{(1 - x^2)(1 - k^2x^2)}} \, dx.
\]

Recall that \( y^2 = (1 - x^2)(1 - k^2x^2) \) is an elliptic curve.

The latter arc length is given by

\[
a \int_{-1}^{1} \frac{1 - k^2x^2}{y} \, dx.
\]

An elliptic integral is an integral of the form \( \int R(x, y) \, dx \), where \( R(x, y) \) is a rational function of the coordinates \( (x, y) \) on an elliptic curve \( E : y^2 = f(x) \), \( f(x) \) is a cubic or a quartic polynomial.
Let $E$ be an elliptic curve over $\mathbb{Q}$ defined by $y^2 = x^3 + Ax + B$. Set $E(\mathbb{Q}) = \{(x, y) : y^2 = x^3 + Ax + B, x, y \in \mathbb{Q}\}$.

Recall that $E(\mathbb{Q})$ is a subgroup of $E$.

The following celebrated theorem is due to Mordell.

**Theorem (Mordell, 1922)** $E(\mathbb{Q})$ is a finitely generated abelian group.

**Corollary** There exists a nonnegative integer $r$ such that $E(\mathbb{Q}) \cong \mathbb{Z}^r \times T$, $|T| < \infty$. $r$ is the rank of $E(\mathbb{Q})$.

Mohammad Sadek

How often does a polynomial hit a square?
Let $E$ be an elliptic curve over $\mathbb{Q}$ defined by $y^2 = x^3 + Ax + B$. 

Recall that $E(\mathbb{Q})$ is a subgroup of $E$. 

The following celebrated theorem is due to Mordell.

**Theorem (Mordell, 1922)**

$E(\mathbb{Q})$ is a finitely generated abelian group.

**Corollary**

There exists a nonnegative integer $r$ such that $E(\mathbb{Q}) \cong \mathbb{Z}^r \times T$, $|T| < \infty$. $r$ is the rank of $E(\mathbb{Q})$. 

Mohammad Sadek

How often does a polynomial hit a square?
Let $E$ be an elliptic curve over $\mathbb{Q}$ defined by $y^2 = x^3 + Ax + B$. Set

$$E(\mathbb{Q}) = \{(x, y) : y^2 = x^3 + Ax + B, x, y \in \mathbb{Q}\}.$$

Recall that $E(\mathbb{Q})$ is a subgroup of $E$.

The following celebrated theorem is due to Mordell.

Theorem (Mordell, 1922) $E(\mathbb{Q})$ is a finitely generated abelian group.

Corollary There exists a nonnegative integer $r$ such that $E(\mathbb{Q}) \cong \mathbb{Z}^r \times T$, $|T| < \infty$.

$r$ is the rank of $E(\mathbb{Q})$. 

Mohammad Sadek How often does a polynomial hit a square?
Let $E$ be an elliptic curve over $\mathbb{Q}$ defined by $y^2 = x^3 + Ax + B$. Set

$$E(\mathbb{Q}) = \{(x, y) : y^2 = x^3 + Ax + B, x, y \in \mathbb{Q}\}.$$ 

Recall that $E(\mathbb{Q})$ is a subgroup of $E$. 

**Theorem (Mordell, 1922)**

$E(\mathbb{Q})$ is a finitely generated abelian group.

**Corollary**

There exists a nonnegative integer $r$ such that $E(\mathbb{Q}) \cong \mathbb{Z}^r \times T$, $|T| < \infty$.

$r$ is the rank of $E(\mathbb{Q})$. 

Mohammad Sadek

How often does a polynomial hit a square?
Let $E$ be an elliptic curve over $\mathbb{Q}$ defined by $y^2 = x^3 + Ax + B$. Set

$$E(\mathbb{Q}) = \{(x, y) : y^2 = x^3 + Ax + B, x, y \in \mathbb{Q}\}.$$ 

Recall that $E(\mathbb{Q})$ is a subgroup of $E$. The following celebrated theorem is due to Mordell.
Let $E$ be an elliptic curve over $\mathbb{Q}$ defined by $y^2 = x^3 + Ax + B$. Set

$$E(\mathbb{Q}) = \{(x, y) : y^2 = x^3 + Ax + B, x, y \in \mathbb{Q}\}.$$

Recall that $E(\mathbb{Q})$ is a subgroup of $E$. The following celebrated theorem is due to Mordell.

**Theorem (Mordell, 1922)**

$E(\mathbb{Q})$ is a finitely generated abelian group.
Let $E$ be an elliptic curve over $\mathbb{Q}$ defined by $y^2 = x^3 + Ax + B$. Set

$$E(\mathbb{Q}) = \{ (x, y) : y^2 = x^3 + Ax + B, x, y \in \mathbb{Q} \}.$$

Recall that $E(\mathbb{Q})$ is a subgroup of $E$. The following celebrated theorem is due to Mordell.

**Theorem (Mordell, 1922)**

$E(\mathbb{Q})$ is a finitely generated abelian group.

**Corollary**

*There exists a nonnegative integer $r$ such that*

$$E(\mathbb{Q}) \cong \mathbb{Z}^r \times T, \quad |T| < \infty.$$  

$r$ is the **rank** of $E(\mathbb{Q})$. 
In other words, there exist finitely many points $P_1, \ldots, P_s \in E(Q)$, $s \geq r$, such that any point $P \in E(Q)$ can be written as $P = n_1P_1 + n_2P_2 + \ldots + n_sP_s$, $n_i \in \mathbb{Z}$.

This means that there exist finitely many points in $E(Q)$ that I can start from using the chord & tangent process and produce every single point in $E(Q)$. How often does a polynomial hit a square?
In other words, there exist finitely many points $P_1, \ldots, P_s \in E(\mathbb{Q})$, $s \geq r$, such that any point $P \in E(\mathbb{Q})$ can be written as

$$P = n_1 P_1 + n_2 P_2 + \ldots + n_s P_s, \quad n_i \in \mathbb{Z}.$$
In other words, there exist finitely many points $P_1, \ldots, P_s \in E(\mathbb{Q})$, $s \geq r$, such that any point $P \in E(\mathbb{Q})$ can be written as

$$P = n_1 P_1 + n_2 P_2 + \ldots + n_s P_s, \quad n_i \in \mathbb{Z}.$$ 

This means that there exist finitely many points in $E(\mathbb{Q})$ that I can start from using the chord & tangent process and produce every single point in $E(\mathbb{Q})$. 

Mohammad Sadek

How often does a polynomial hit a square?
The following theorem is due to Mazur.

Theorem (Mazur, 1978)

$T$ is one of the following fifteen groups:

- $\mathbb{Z}/n\mathbb{Z}$, for $1 \leq n \leq 12$, $n \neq 11$;
- $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2n\mathbb{Z}$, for $1 \leq n \leq 4$.

This implies that $|T| \leq 16$. 

Mohammad Sadek

How often does a polynomial hit a square?
The following theorem is due to Mazur.

**Theorem (Mazur, 1978)**

\( \mathbb{T} \) is one of the following fifteen groups:

\[
\begin{align*}
\mathbb{Z}/n\mathbb{Z}, & \quad 1 \leq n \leq 12, \ n \neq 11; \\
\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2n\mathbb{Z}, & \quad 1 \leq n \leq 4.
\end{align*}
\]
The following theorem is due to Mazur.

**Theorem (Mazur, 1978)**

\[ \mathbb{T} \text{ is one of the following fifteen groups:} \]

\[ \mathbb{Z}/n\mathbb{Z}, \; 1 \leq n \leq 12, \; n \neq 11; \]

\[ \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2n\mathbb{Z}, \; 1 \leq n \leq 4. \]

This implies that \(|\mathbb{T}| \leq 16.\)
What do we know about $r$?

$r$ tells us how big $E(\mathbb{Q})$ is!

But how big is $r$?

Conjecture $r$ can be arbitrarily large.

Numerical Evidence. $r = 28$ (Elkies, 2006)

What do we know about \( r \)?

- \( E(\mathbb{Q}) \cong \mathbb{Z}^r \times \mathbb{T} \)
$E(\mathbb{Q}) \simeq \mathbb{Z}^r \times \mathbb{T}$

- What do we know about $r$?
- $r$ tells us how big $E(\mathbb{Q})$ is!
$E(\mathbb{Q}) \sim \mathbb{Z}^r \times \mathbb{T}$

- What do we know about $r$?
- $r$ tells us how big $E(\mathbb{Q})$ is!
- But how big is $r$?
$E(\mathbb{Q}) \simeq \mathbb{Z}^r \times \mathbb{T}$

- What do we know about $r$?
- $r$ tells us how big $E(\mathbb{Q})$ is!
- But how big is $r$?

**Conjecture**

$r$ can be arbitrarily large.
$E(\mathbb{Q}) \simeq \mathbb{Z}^r \times \mathbb{T}$

- What do we know about $r$?
- $r$ tells us how big $E(\mathbb{Q})$ is!
- But how big is $r$?

**Conjecture**

$r$ can be arbitrarily large.

**Numerical Evidence.**
\[ E(\mathbb{Q}) \simeq \mathbb{Z}^r \times \mathbb{T} \]

- What do we know about \( r \)?
- \( r \) tells us how big \( E(\mathbb{Q}) \) is!
- But how big is \( r \)?

**Conjecture**

\( r \) can be arbitrarily large.

- **Numerical Evidence.** \( r = 28 \) (Elkies, 2006)
What do we know about $r$?
- $r$ tells us how big $E(\mathbb{Q})$ is!
- But how big is $r$?

**Conjecture**

$r$ can be arbitrarily large.

**Numerical Evidence.** $r = 28$ (Elkies, 2006)

**Warning.**
\[ E(\mathbb{Q}) \cong \mathbb{Z}^r \times \mathbb{T} \]

- What do we know about \( r \)?
- \( r \) tells us how big \( E(\mathbb{Q}) \) is!
- But how big is \( r \)?

**Conjecture**

\( r \) can be arbitrarily large.

- **Numerical Evidence.** \( r = 28 \) (Elkies, 2006)
Let $E$ be defined by $y^2 = x^3 + Ax + B$, $A, B \in \mathbb{Z}$.

Recall that $E(\mathbb{Z}) = \{(x, y) \in E : x, y \in \mathbb{Z}\}$.

$E(\mathbb{Z})$ is not a subgroup of $E$.

The following finiteness theorem is due to Siegel, 1928.

**Theorem**

$E(\mathbb{Z})$ is finite.
Let $E$ be defined by $y^2 = x^3 + Ax + B$, $A, B \in \mathbb{Z}$. 

Recall that $E(\mathbb{Z}) = \{(x, y) \in E : x, y \in \mathbb{Z}\}$. 

$E(\mathbb{Z})$ is not a subgroup of $E$. 

The following finiteness theorem is due to Siegel, 1928.

Theorem $E(\mathbb{Z})$ is finite.
Let $E$ be defined by $y^2 = x^3 + Ax + B$, $A, B \in \mathbb{Z}$. Recall that

$$E(\mathbb{Z}) = \{(x, y) \in E : x, y \in \mathbb{Z}\}.$$
Let $E$ be defined by $y^2 = x^3 + Ax + B$, $A, B \in \mathbb{Z}$. Recall that

$$E(\mathbb{Z}) = \{(x, y) \in E : x, y \in \mathbb{Z}\}.$$ 

$E(\mathbb{Z})$ is not a subgroup of $E$. 

The following finiteness theorem is due to Siegel, 1928.
Let $E$ be defined by $y^2 = x^3 + Ax + B$, $A, B \in \mathbb{Z}$. Recall that

$$E(\mathbb{Z}) = \{(x, y) \in E : x, y \in \mathbb{Z}\}.$$ 

$E(\mathbb{Z})$ is not a subgroup of $E$. The following finiteness theorem is due to Siegel, 1928.

**Theorem**

$E(\mathbb{Z})$ is finite.
$E(\mathbb{F}_p)$ and Hasse

Finding solutions for a polynomial equation over a finite field is easier than finding solutions in $\mathbb{Q}$ or $\mathbb{Z}$.

Let $E$ be an elliptic curve defined by $y^2 = x^3 + Ax + B$, $A, B \in \mathbb{F}_p$.

One expects $E(\mathbb{F}_p)$ to have approximately $p + 1$ points.

The following theorem quantifies this expectation.

Theorem (Hasse, 1922)

$|E(\mathbb{F}_p)| - (p + 1) < 2\sqrt{p}$.
Finding solutions for a polynomial equation over a finite field is easier than finding solutions in $\mathbb{Q}$ or $\mathbb{Z}$.
Finding solutions for a polynomial equation over a finite field is easier than finding solutions in $\mathbb{Q}$ or $\mathbb{Z}$. Let $E$ be an elliptic curve defined by $y^2 = x^3 + Ax + B$, $A, B \in \mathbb{F}_p$. 

Mohammad Sadek

How often does a polynomial hit a square?
Finding solutions for a polynomial equation over a finite field is easier than finding solutions in \( \mathbb{Q} \) or \( \mathbb{Z} \). Let \( E \) be an elliptic curve defined by \( y^2 = x^3 + Ax + B, \) \( A, B \in \mathbb{F}_p \). One expects \( E(\mathbb{F}_p) \) to have approximately \( p + 1 \) points.
Finding solutions for a polynomial equation over a finite field is easier than finding solutions in $\mathbb{Q}$ or $\mathbb{Z}$. Let $E$ be an elliptic curve defined by $y^2 = x^3 + Ax + B$, $A, B \in \mathbb{F}_p$. One expects $E(\mathbb{F}_p)$ to have approximately $p + 1$ points. The following theorem quantifies this expectation.
Finding solutions for a polynomial equation over a finite field is easier than finding solutions in $\mathbb{Q}$ or $\mathbb{Z}$. Let $E$ be an elliptic curve defined by $y^2 = x^3 + Ax + B$, $A, B \in \mathbb{F}_p$. One expects $E(\mathbb{F}_p)$ to have approximately $p + 1$ points. The following theorem quantifies this expectation.

**Theorem (Hasse, 1922)**

$$||E(\mathbb{F}_p)| - (p + 1)|| < 2\sqrt{p}.$$
“Thank God that number theory is unsullied by any application”
Leonard Dickson (1874-1954)

“...virtually every theorem in elementary number theory arises in a natural, motivated way in connection with the problem of making computers do high-speed numerical calculations”
Donald Knuth 1974

Rivest, Shamir, and Adleman came up with RSA, a secure algorithm for public-key cryptography, 1977!

RSA: Factorization of integers.

How often does a polynomial hit a square?
"Thank God that number theory is unsullied by any application"
Leonard Dickson (1874-1954)
"Thank God that number theory is unsullied by any application"
Leonard Dickson (1874-1954)

"...virtually every theorem in elementary number theory arises in a natural, motivated way in connection with the problem of making computers do high-speed numerical calculations”
Donald Knuth 1974
”Thank God that number theory is unsullied by any application”
Leonard Dickson (1874-1954)

”...virtually every theorem in elementary number theory arises in a natural, motivated way in connection with the problem of making computers do high-speed numerical calculations”
Donald Knuth 1974

Rivest, Shamir, and Adleman came up with RSA, a secure algorithm for public-key cryptography, 1977!
"Thank God that number theory is unsullied by any application"
Leonard Dickson (1874-1954)

"...virtually every theorem in elementary number theory arises in a natural, motivated way in connection with the problem of making computers do high-speed numerical calculations"
Donald Knuth 1974

Rivest, Shamir, and Adleman came up with RSA, a secure algorithm for public-key cryptography, 1977!

RSA: Factorization of integers.
The Discrete Logarithm Problem

Input: Let $(G, \star)$ be a group. Let $a, b \in G$ be such that $b \in \langle a \rangle$.

Output: Find $m \in \mathbb{Z}$ such that $b = a \star a \star \ldots \star a = a^m$ ($m$ times) = $a^m$ ($m = \log_a b$).

Example. Let $G = \mathbb{F}_p \times \mathbb{F}_p$ (Diffie-Hellman).
The Discrete Logarithm Problem

Discrete Logarithm Problem

Input: Let $(G, \ast)$ be a group. Let $a, b \in G$ be such that $b \in \langle a \rangle$.

Output: Find $m \in \mathbb{Z}$ such that $b = a \ast a \ast \ldots \ast a = a^m$ ($m$ times $= a^m$).

Example. Let $G = \mathbb{F}_p^\times$. (Diffie-Hellman)
The Discrete Logarithm Problem

### Discrete Logarithm Problem

**Input:** Let \((G,\ast)\) be a group. Let \(a, b \in G\) be such that \(b \in \langle a \rangle\).

**Output:** Find \(m \in \mathbb{Z}\) such that
\[
b = a \ast a \ast \ldots \ast a = a^m
\]

\(m\)-times
Discrete Logarithm Problem

Input: Let \((G, \ast)\) be a group. Let \(a, b \in G\) be such that \(b \in \langle a \rangle\).

Output: Find \(m \in \mathbb{Z}\) such that \(b = \underbrace{a \ast a \ast \ldots \ast a}_{m\text{-times}} = a^m\) \((m = \log_a b)\).
Discrete Logarithm Problem

**Input:** Let \((G, \cdot)\) be a group. Let \(a, b \in G\) be such that \(b \in \langle a \rangle\).

**Output:** Find \(m \in \mathbb{Z}\) such that \(b = a \cdot a \cdot \ldots \cdot a = a^m\) \((m = \log_a b)\).

**Example.** Let \(G = \mathbb{F}_p^\times\). (Diffie-Hellman)
The Discrete Logarithm Problem

Elliptic Discrete Logarithm Problem
Koblitz and Miller 1985

Input: Let $E$ be an elliptic curve defined over $\mathbb{F}_p$. Let $P, Q \in E(\mathbb{F}_p)$ be such that $Q \in \langle P \rangle$.

Output: Find $m \in \mathbb{Z}$ such that $Q = mP$ ($Q = \log_P Q$).

The best algorithms for solving the elliptic curve discrete logarithm problem (ECDLP) are much less efficient than the algorithms for solving DLP in $\mathbb{F}_p \times \mathbb{F}_p$.
Elliptic Discrete Logarithm Problem
Koblitz and Miller 1985
Elliptic Discrete Logarithm Problem
Koblitz and Miller 1985

Input: Let $E$ be an elliptic curve defined over $\mathbb{F}_p$. Let $P, Q \in E(\mathbb{F}_p)$ be such that $Q \in \langle P \rangle$. 

Output: Find $m \in \mathbb{Z}$ such that $Q = mP$ ($m = \log_P Q$).
Elliptic Discrete Logarithm Problem
Koblitz and Miller 1985

**Input:** Let $E$ be an elliptic curve defined over $\mathbb{F}_p$. Let $P, Q \in E(\mathbb{F}_p)$ be such that $Q \in \langle P \rangle$.

**Output:** Find $m \in \mathbb{Z}$ such that $Q = mP$
The Discrete Logarithm Problem

Elliptic Discrete Logarithm Problem
Koblitz and Miller 1985

**Input:** Let $E$ be an elliptic curve defined over $\mathbb{F}_p$. Let $P, Q \in E(\mathbb{F}_p)$ be such that $Q \in \langle P \rangle$.

**Output:** Find $m \in \mathbb{Z}$ such that $Q = mP$ ($m = \log_P Q$).
The best algorithms for solving the elliptic curve discrete logarithm problem (ECDLP) are much less efficient than the algorithms for solving DLP in $\mathbb{F}_p^\times$. 

Mohammad Sadek How often does a polynomial hit a square?
Question:

Fermat observed the following:

\(1 \times 3 + 1 = 2^2\),
\(1 \times 120 + 1 = 12^2\),
\(1 \times 8 + 1 = 3^2\),
\(3 \times 120 + 1 = 19^2\),
\(3 \times 8 + 1 = 5^2\),
\(8 \times 120 + 1 = 31^2\).

Definition:

A set of \(m\) positive integers (rationals) \(\{a_1, a_2, \cdots, a_m\}\) is called a \((rational) Diophantine m\)-tuple if \(a_i \times a_j + 1\) is a perfect square for all \(1 \leq i < j \leq m\).
**Question:** What is special about the set

\[ \{1, 3, 8, 120\} \]?
**Question:** What is special about the set 

\{1, 3, 8, 120\}?

Fermat observed the following

\[ 1 \times 3 + 1 = 2^2, \quad 1 \times 120 + 1 = 12^2, \quad 1 \times 8 + 1 = 3^2, \]
\[ 3 \times 120 + 1 = 19^2, \quad 3 \times 8 + 1 = 5^2, \quad 8 \times 120 + 1 = 31^2. \]
Question: What is special about the set \( \{1, 3, 8, 120\} \)?

Fermat observed the following

\[
1 \times 3 + 1 = 2^2, \quad 1 \times 120 + 1 = 12^2, \quad 1 \times 8 + 1 = 3^2, \\
3 \times 120 + 1 = 19^2, \quad 3 \times 8 + 1 = 5^2, \quad 8 \times 120 + 1 = 31^2.
\]

Definition

A set of \( m \) positive integers (rationals) \( \{a_1, a_2, \cdots, a_m\} \) is called a (rational) Diophantine \( m \)-tuple if \( a_i \times a_j + 1 \) is a perfect square for all \( 1 \leq i < j \leq m \).
Diophantine $m$-tuples

Why is this problem related to our original problem?

What is the geometry of the problem?

How large these Diophantine sets can be?

In other words, how large $m$ can be?

Mohammad Sadek

How often does a polynomial hit a square?
Why is this problem related to our original problem?
Why is this problem related to our original problem?

What is the geometry of the problem?
Diophantine $m$-tuples

- Why is this problem related to our original problem?
- What is the geometry of the problem?
- How large these Diophantine sets can be?
Why is this problem related to our original problem?
What is the geometry of the problem?
How large these Diophantine sets can be? In other words, how large $m$ can be?
Theorem (Dujella, 2004)

There does not exist a Diophantine sextuple.
Diophantine $m$-tuples, $m \geq 5$

Theorem (Dujella, 2004)

There does not exist a Diophantine sextuple.

Does there exist a Diophantine quintuple?
Diophantine $m$-tuples, $m \geq 5$

Theorem (Dujella, 2004)

There does not exist a Diophantine sextuple.

Does there exist a Diophantine quintuple?

Theorem (He, Togbé, Ziegler, 2018)

There does not exist a Diophantine quintuple.
Example.

\[ \{\frac{19}{12}, \frac{33}{4}, \frac{52}{3}, \frac{60}{2209}, -\frac{495}{24964}, \frac{595}{12}\}, \]
Example.

\{19/12, 33/4, 52/3, 60/2209, −495/24964, 595/12\},

Theorem (Dujella, Kazalicki, Mikic, Szikszai, 2017)

*There exist infinitely many rational Diophantine sextuples.*
Proof.

(1) There are infinitely many rational Diophantine triples.

(2) Consider the elliptic curve $E$: $y^2 = (ax+1)(bx+1)(cx+1)$.

(3) Observe that if $(a, b, c, d)$ is a Diophantine quadruple, then $d$ gives rise to a rational point on $E$.

(4) The trick is which rational point $(x, y) \in E(\mathbb{Q})$ gives rise to such $d$!

(5) Necessary and sufficient conditions were given so that (4) happens for three different rationals $d, e, f$, and such that $(a, b, c, d, e, f)$ is a rational Diophantine sixtuple.
Proof.

(1) There are infinitely many rational Diophantine triples.
Proof.

(1) There are infinitely many rational Diophantine triples. Pick any of these triples \((a, b, c)\).

(2) Consider the elliptic curve \(E: y^2 = (ax + 1)(bx + 1)(cx + 1)\).

(3) Observe that if \((a, b, c, d)\) is a Diophantine quadruple, then \(d\) gives rise to a rational point on \(E\).

(4) The trick is which rational point \((x, y) \in E(\mathbb{Q})\) gives rise to such \(d\!

(5) Necessary and sufficient conditions were given so that (4) happens for three different rationals \(d, e, f\), and such that \((a, b, c, d, e, f)\) is a rational Diophantine sixtuple.
Proof.

(1) There are infinitely many rational Diophantine triples. Pick any of these triples \((a, b, c)\).

(2) Consider the elliptic curve

\[ E : y^2 = (ax + 1)(bx + 1)(cx + 1) \]
Proof.

(1) There are infinitely many rational Diophantine triples. Pick any of these triples \((a, b, c)\).

(2) Consider the elliptic curve

\[
E : y^2 = (ax + 1)(bx + 1)(cx + 1)
\]

(3) Observe that if \((a, b, c, d)\) is a Diophantine quadruple, then \(d\) gives rise to a rational point on \(E\).
Proof.

(1) There are infinitely many rational Diophantine triples. Pick any of these triples \((a, b, c)\).

(2) Consider the elliptic curve

\[
E : y^2 = (ax + 1)(bx + 1)(cx + 1)
\]

(3) Observe that if \((a, b, c, d)\) is a Diophantine quadruple, then \(d\) gives rise to a rational point on \(E\).

(4) The trick is which rational point \((x, y) \in E(\mathbb{Q})\) gives rise to such \(d\)!
Proof.

(1) There are infinitely many rational Diophantine triples. Pick any of these triples \((a, b, c)\).

(2) Consider the elliptic curve

\[ E : y^2 = (ax + 1)(bx + 1)(cx + 1) \]

(3) Observe that if \((a, b, c, d)\) is a Diophantine quadruple, then \(d\) gives rise to a rational point on \(E\).

(4) The trick is which rational point \((x, y) \in E(\mathbb{Q})\) gives rise to such \(d\)!

(5) Necessary and sufficient conditions were given so that (4) happens for three different rationals \(d, e, f\), and such that \((a, b, c, d, e, f)\) is a rational Diophantine sextuple.
Rational Diophantine $m$-tuples

Conjecture

There are no rational Diophantine 9-tuples. We still do not have a single example of a rational Diophantine 7-tuple. Are they finite? Infinite? Maybe there is no such 7-tuple!
There are no rational Diophantine 9-tuples.
Rational Diophantine \( m \)-tuples

**Conjecture**

There are no rational Diophantine 9-tuples.

- We still do not have a single example of a rational Diophantine 7-tuple.
Rational Diophantine $m$-tuples

**Conjecture**

There are no rational Diophantine 9-tuples.

- We still do not have a single example of a rational Diophantine 7-tuple.
- Are they finite?
Conjecture

There are no rational Diophantine 9-tuples.

- We still do not have a single example of a rational Diophantine 7-tuple.
- Are they finite? infinite?
Rational Diophantine $m$-tuples

Conjecture

There are no rational Diophantine 9-tuples.

- We still do not have a single example of a rational Diophantine 7-tuple.
- Are they finite? infinite? Maybe there is no such 7-tuple!
Geometry of the Problem

\[ S = \{1, 3, 8, 120\} \]

\[
\begin{align*}
1 \times 3 + 1 &= 2^2, \\
1 \times 120 + 1 &= 12^2, \\
1 \times 8 + 1 &= 3^2, \\
3 \times 120 + 1 &= 19^2, \\
3 \times 8 + 1 &= 5^2, \\
8 \times 120 + 1 &= 31^2.
\end{align*}
\]
Geometry of the Problem

\[ S = \{1, 3, 8, 120\} \]

\[ 1 \times 3 + 1 = 2^2, \quad 1 \times 120 + 1 = 12^2, \quad 1 \times 8 + 1 = 3^2, \]
\[ 3 \times 120 + 1 = 19^2, \quad 3 \times 8 + 1 = 5^2, \quad 8 \times 120 + 1 = 31^2. \]

Algebraic variety \( C \) defined by the intersection of 6 quadratics in \( \mathbb{P}^1 \mathcal{Q} \).
Geometry of the Problem

\[ S = \{1, 3, 8, 120\} \]

\[ 1 \times 3 + 1 = 2^2, \quad 1 \times 120 + 1 = 12^2, \quad 1 \times 8 + 1 = 3^2, \]
\[ 3 \times 120 + 1 = 19^2, \quad 3 \times 8 + 1 = 5^2, \quad 8 \times 120 + 1 = 31^2. \]

Algebraic variety \( C \) defined by the intersection of 6 quadratics in \( \mathbb{P}^Q \)

\[ x_1 x_2 + 1 = y_1^2, \quad x_1 x_3 + 1 = y_2^2, \quad x_1 x_4 + 1 = y_3^2, \]
\[ x_2 x_3 + 1 = y_4^2, \quad x_2 x_4 + 1 = y_5^2, \quad x_3 x_4 + 1 = y_6^2. \]
Geometry of the Problem

\[ S = \{1, 3, 8, 120\} \]

\[
egin{align*}
1 \times 3 + 1 &= 2^2, & 1 \times 120 + 1 &= 12^2, & 1 \times 8 + 1 &= 3^2, \\
3 \times 120 + 1 &= 19^2, & 3 \times 8 + 1 &= 5^2, & 8 \times 120 + 1 &= 31^2.
\end{align*}
\]

Algebraic variety \( C \) defined by the intersection of 6 quadratics in \( \mathbb{P}^\mathbb{Q}^{10} \):

\[
\begin{align*}
x_1x_2 + 1 &= y_1^2, & x_1x_3 + 1 &= y_2^2, & x_1x_4 + 1 &= y_3^2, \\
x_2x_3 + 1 &= y_4^2, & x_2x_4 + 1 &= y_5^2, & x_3x_4 + 1 &= y_6^2.
\end{align*}
\]

Then we investigate \( C(\mathbb{Q}) \).
Why is this problem related to our question?

\[ S = \{1, 3, 8, 120\} \]

\[
\begin{align*}
1 \times 3 + 1 &= 2^2, & 1 \times 120 + 1 &= 12^2, & 1 \times 8 + 1 &= 3^2, \\
3 \times 120 + 1 &= 19^2, & 3 \times 8 + 1 &= 5^2, & 8 \times 120 + 1 &= 31^2.
\end{align*}
\]
Why is this problem related to our question?

$S = \{1, 3, 8, 120\}$

\[
\begin{align*}
1 \times 3 + 1 &= 2^2, & 1 \times 120 + 1 &= 12^2, & 1 \times 8 + 1 &= 3^2, \\
3 \times 120 + 1 &= 19^2, & 3 \times 8 + 1 &= 5^2, & 8 \times 120 + 1 &= 31^2.
\end{align*}
\]

$F(x, y) = xy + 1$
Why is this problem related to our question?

\[ S = \{1, 3, 8, 120\} \]

\[
\begin{align*}
1 \times 3 + 1 &= 2^2, \\
1 \times 120 + 1 &= 12^2, \\
1 \times 8 + 1 &= 3^2, \\
3 \times 120 + 1 &= 19^2, \\
3 \times 8 + 1 &= 5^2, \\
8 \times 120 + 1 &= 31^2.
\end{align*}
\]

\[ F(x, y) = xy + 1 \]

\[ F(s_i, s_j) = \Box_{ij} \quad \text{for all } s_i, s_j \in S, \ s_i \neq s_j. \]
Definition

Let $F \in \mathbb{Z}[x, y]$. A set $A \subseteq \mathbb{Z}$ is called an $F$-Diophantine set if $F(a, b)$ is a perfect square for any $a, b \in A$ with $a \neq b$. 

So Diophantine tuples are $F$-Diophantine sets for $F(x, y) = xy + 1$. 
**Definition**

Let $F \in \mathbb{Z}[x, y]$. A set $A \subseteq \mathbb{Z}$ is called an \textbf{$F$-Diophantine set} if $F(a, b)$ is a perfect square for any $a, b \in A$ with $a \neq b$.

So Diophantine tuples are $F$-Diophantine sets for $F(x, y) = xy + 1$. 
when $F = xy + 1$, the largest Diophantine set is of size 4. For different polynomials $F$, how large an $F$-Diophantine set can be? Can we find a polynomial $F$ such that there are infinite $F$-Diophantine sets?
when $F = xy + 1$, the largest Diophantine set is of size 4.
• when \( F = xy + 1 \), the largest Diophantine set is of size 4.
• For different polynomials \( F \), how large an \( F \)-Diophantine set can be?
when $F = xy + 1$, the largest Diophantine set is of size 4.

- For different polynomials $F$, how large an $F$-Diophantine set can be?
- Can we find a polynomial $F$ such that there are infinite $F$-Diophantine sets?
Can we find a polynomial $F$ such that there are infinitely many $F$-Diophantine sets?
Can we find a polynomial $F$ such that there are infinite $F$-Diophantine sets?

Think of $F(x, y) = xy$. 

Bérczes, Dujella, Hajdu and Tengely, 2017, gave a complete classification of all such polynomials $F$. For certain families of polynomials $F$, they found upper bounds on the size of $F$-Diophantine sets.
Can we find a polynomial $F$ such that there are \textbf{infinite} $F$-Diophantine sets?

Think of $F(x, y) = xy$.

Bérczes, Dujella, Hajdu and Tengely, 2017, gave a complete classification of all such polynomials $F$.
Can we find a polynomial $F$ such that there are infinite $F$-Diophantine sets?

Think of $F(x, y) = xy$.

Bérczes, Dujella, Hajdu and Tengely, 2017, gave a complete classification of all such polynomials $F$.

For certain families of polynomials $F$, they found upper bounds on the size of $F$-Diophantine sets.
More Questions

Given a set of distinct integers

\[ S = \{x_1, \cdots, x_n\} \subset \mathbb{Z} \]
Given a set of distinct integers

\[ S = \{x_1, \cdots, x_n\} \subset \mathbb{Z} \]

are there polynomials \( F \in \mathbb{Z}[x, y] \) such that \( S \) is an \( F \)-Diophantine set?
Given a set of distinct integers

\[ S = \{x_1, \cdots, x_n\} \subset \mathbb{Z} \]

- are there polynomials \( F \in \mathbb{Z}[x, y] \) such that \( S \) is an \( F \)-Diophantine set?
- if such polynomials exist, how many are they?
Given a set of distinct integers

\[ S = \{x_1, \ldots, x_n\} \subset \mathbb{Z} \]

- are there polynomials \( F \in \mathbb{Z}[x, y] \) such that \( S \) is an \( F \)-Diophantine set?
- if such polynomials exist, how many are they?
- what is the smallest possible degree of such polynomial?
Theorem (2018)

Given $S = \{x_1, \cdots, x_k\} \subset \mathbb{Z}$ where $x_i \neq x_j$ if $i \neq j$, there are infinitely many polynomials $F \in \mathbb{Z}[x, y]$ with $\deg F = 2(k - 2)$ such that the set $S$ is an $F$-Diophantine set.
Theorem (2018)

Given $S = \{x_1, \cdots, x_k\} \subset \mathbb{Z}$ where $x_i \neq x_j$ if $i \neq j$, there are infinitely many polynomials $F \in \mathbb{Z}[x, y]$ with $\deg F = 2(k - 2)$ such that the set $S$ is an $F$-Diophantine set.

Proof.

Studying Determinantal varieties that we may associate to $F$-diophantine sets.
Theorem (2018)

Given $S = \{x_1, \cdots , x_k\} \subset \mathbb{Z}$ where $x_i \neq x_j$ if $i \neq j$, there are infinitely many polynomials $F \in \mathbb{Z}[x, y]$ with $\deg F = 2(\lfloor k/3 \rfloor)$ such that the set $S$ is an $F$-Diophantine set.
Open questions

Mohammad Sadek

How often does a polynomial hit a square?
Open questions

- \((F, m)\)-Diophantine sets, \(m \geq 3\).
Open questions

- $(F, m)$-Diophantine sets, $m \geq 3$.
- *Strong* $F$-Diophantine sets.
Open questions

- \((F, m)\)-Diophantine sets, \(m \geq 3\).
- Strong \(F\)-Diophantine sets. \(F(x_i, x_i) = \square\).
Thank you!