Computing (Hyper)Elliptic Curves Over \( \mathbb{Q} \)

Mohammad Sadek

Sabancı Algebra Seminar

Nov 11, 2020
Diophantine Problems

What are Diophantine problems?

Barry Mazur: I don't know the answer, But I can feel my way around it.

Pythagoras: List all right-angle triangles all of whose sides are integral.

Find all integers \(a\), \(b\), \(c\) such that

\[ a^2 + b^2 = c^2. \]

Solution: \(a = 2rs\), \(b = r^2 - s^2\), \(c = r^2 + s^2\), where \(r, s \in \mathbb{Z}\).

"1955" Given a positive integer \(k\), can we write \(k\) as the sum of three cubes?

Find three integers \(a\), \(b\), \(c\) such that

\[ k = a^3 + b^3 + c^3. \]

In 2018, Andrew Booker:

\[ 33 = (8, 866, 128, 975, 287, 528)^3 + (−8, 778, 405, 442, 862, 239)^3 + (−2, 736, 111, 468, 807, 040)^3. \]

Mohammad Sadek Computing (Hyper)Elliptic Curves Over \(\mathbb{Q}\)
What are Diophantine problems?

Pythagoras: List all right-angle triangles all of whose sides are integral.

Find all integers \( a, b, c \) such that
\[
a^2 + b^2 = c^2.
\]

Solution:
\[
a = 2rs,\quad b = r^2 - s^2,\quad c = r^2 + s^2,
\]
where \( r, s \in \mathbb{Z} \).

Given a positive integer \( k \), can we write \( k \) as the sum of three cubes?

In 2018, Andrew Booker:
\[
33 = (8, 866, 128, 975, 287, 528)^3 + (-8, 778, 405, 442, 862, 239)^3 + (-2, 736, 111, 468, 807, 040)^3.
\]
What are Diophantine problems?

Barry Mazur:

Pythagoras: List all right-angle triangles all of whose sides are integral. Find all integers $a$, $b$, $c$ such that $a^2 + b^2 = c^2$.

Solution: $a = 2rs$, $b = r^2 - s^2$, $c = r^2 + s^2$, where $r, s \in \mathbb{Z}$.

Given a positive integer $k$, can we write $k$ as the sum of three cubes? Find three integers $a$, $b$, $c$ such that $k = a^3 + b^3 + c^3$.

In 2018, Andrew Booker: $33 = (8, 866, 128, 975, 287)^3 + (-8, 778, 405, 442, 862)^3 + (-2, 736, 111, 468, 807, 040)^3$. 

Mohammad Sadek Computing (Hyper)Elliptic Curves Over $\mathbb{Q}$
What are Diophantine problems?

**Barry Mazur:** I don’t know the answer

---

Find all integers $a, b, c$ such that

\[ a^2 + b^2 = c^2. \]

Solution:

\[ a = 2rs, \quad b = r^2 - s^2, \quad c = r^2 + s^2, \]

where $r, s \in \mathbb{Z}$.

---

Given a positive integer $k$, can we write $k$ as the sum of three cubes?

Find three integers $a, b, c$ such that

\[ k = a^3 + b^3 + c^3. \]

In 2018, Andrew Booker:

\[
33 = (8, 866, 128, 975, 287, 528)^3 + (-8, 778, 405, 442, 862, 239)^3 + (-2, 736, 111, 468, 807, 040)^3.
\]
What are Diophantine problems?

Barry Mazur: I don’t know the answer, But I can feel my way around it.

Pythagoras: List all right-angle triangles all of whose sides are integral.

Find all integers \( a, b, c \) such that

\[
\begin{align*}
  a^2 + b^2 &= c^2
\end{align*}
\]

Solution:

\[
\begin{align*}
  a &= 2rs, \\
  b &= r^2 - s^2, \\
  c &= r^2 + s^2
\end{align*}
\]

where \( r, s \in \mathbb{Z} \).

Given a positive integer \( k \), can we write \( k \) as the sum of three cubes?

Find three integers \( a, b, c \) such that

\[
\begin{align*}
  k &= a^3 + b^3 + c^3
\end{align*}
\]

In 2018, Andrew Booker:

\[
\begin{align*}
  33 &= (8, 866, 128, 975, 287, 528)^3 + (-8, 778, 405, 442, 862, 239)^3 + (-2, 736, 111, 468, 807, 040)^3
\end{align*}
\]
What are Diophantine problems?

Barry Mazur: I don’t know the answer, But I can feel my way around it.

Pythagoras: List all right-angle triangles all of whose sides are integral.

“1955”

Given a positive integer $k$, can we write $k$ as the sum of three cubes?

Solution:

Find three integers $a, b, c$ such that $k = a^3 + b^3 + c^3$.

In 2018, Andrew Booker:

$33 = (8, 866, 128, 975, 287, 528)^3 + (-8, 778, 405, 442, 862, 239)^3 + (-2, 736, 111, 468, 807, 040)^3$. 

Mohammad Sadek

Computing (Hyper)Elliptic Curves Over $\mathbb{Q}$
What are Diophantine problems?

Barry Mazur: I don’t know the answer, But I can feel my way around it.

Pythagoras: List all right-angle triangles all of whose sides are integral.

Find all integers \( a, b, c \) such that \( a^2 + b^2 = c^2 \)

Solution:

\[
a = 2rs, \\
b = r^2 - s^2, \\
c = r^2 + s^2.
\]

Given a positive integer \( k \), can we write \( k \) as the sum of three cubes?

In 2018, Andrew Booker: \( 33 = (8, 866, 128, 975, 287, 528)^3 + (-8, 778, 405, 442, 862, 239)^3 + (-2, 736, 111, 468, 807, 040)^3 \).
Diophantine Problems

- What are Diophantine problems?
- **Barry Mazur:** I don’t know the answer, But I can feel my way around it.
- **Pythagoras:** List all right-angle triangles all of whose sides are integral.

Find all integers $a, b, c$ such that $a^2 + b^2 = c^2$

Solution: $a = 2rs$, $b = r^2 - s^2$, $c = r^2 + s^2$, where $r, s \in \mathbb{Z}$.
What are Diophantine problems?

Barry Mazur: I don’t know the answer, But I can feel my way around it.

Pythagoras: List all right-angle triangles all of whose sides are integral.

Find all integers \( a, b, c \) such that \( a^2 + b^2 = c^2 \)

Solution: \( a = 2rs, \ b = r^2 - s^2, \ c = r^2 + s^2 \), where \( r, s \in \mathbb{Z} \).

”1955” Given a positive integer \( k \), can we write \( k \) as the sum of three cubes?
What are Diophantine problems?

Barry Mazur: I don’t know the answer, But I can feel my way around it.

Pythagoras: List all right-angle triangles all of whose sides are integral.

Find all integers $a, b, c$ such that $a^2 + b^2 = c^2$

Solution: $a = 2rs$, $b = r^2 - s^2$, $c = r^2 + s^2$, where $r, s \in \mathbb{Z}$.

”1955” Given a positive integer $k$, can we write $k$ as the sum of three cubes?

Find three integers $a, b, c$ such that $k = a^3 + b^3 + c^3$
What are Diophantine problems?

Barry Mazur: I don’t know the answer, But I can feel my way around it.

Pythagoras: List all right-angle triangles all of whose sides are integral.

Find all integers \( a, b, c \) such that \( a^2 + b^2 = c^2 \)

Solution: \( a = 2rs, b = r^2 - s^2, c = r^2 + s^2 \), where \( r, s \in \mathbb{Z} \).

”1955” Given a positive integer \( k \), can we write \( k \) as the sum of three cubes?

Find three integers \( a, b, c \) such that \( k = a^3 + b^3 + c^3 \)

In 2018, Andrew Booker:

\[ 33 = (8, 866, 128, 975, 287, 528)^3 + (-8, 778, 405, 442, 862, 239)^3 + (-2, 736, 111, 468, 807, 040)^3. \]
Diophantine Problems

- What are Diophantine problems?
- **Barry Mazur**: I don’t know the answer, But I can feel my way around it.
- **Pythagoras**: List all right-angle triangles all of whose sides are integral.

Find all integers \( a, b, c \) such that \( a^2 + b^2 = c^2 \)

Solution: \( a = 2rs, \ b = r^2 - s^2, \ c = r^2 + s^2, \) where \( r, s \in \mathbb{Z} \).

- ”1955” Given a positive integer \( k \), can we write \( k \) as the sum of three cubes?

Find three integers \( a, b, c \) such that \( k = a^3 + b^3 + c^3 \)

In 2018, Andrew Booker:

\[ 33 = \]

Mohammad Sadek
Computing (Hyper)Elliptic Curves Over \( \mathbb{Q} \)
Diophantine Problems

- What are Diophantine problems?
- **Barry Mazur**: I don’t know the answer, But I can feel my way around it.
- **Pythagoras**: List all right-angle triangles all of whose sides are integral.

Find all integers \(a, b, c\) such that \(a^2 + b^2 = c^2\)

Solution: \(a = 2rs, b = r^2 - s^2, c = r^2 + s^2\), where \(r, s \in \mathbb{Z}\).

”1955” Given a positive integer \(k\), can we write \(k\) as the sum of three cubes?

Find three integers \(a, b, c\) such that \(k = a^3 + b^3 + c^3\)

In 2018, Andrew Booker:

\[
33 = (8, 866, 128, 975, 287, 528)^3 + (-8, 778, 405, 442, 862, 239)^3
\]
\[
+ (-2, 736, 111, 468, 807, 040)^3
\]
Diophantine Equations

Studying zeros of multivariate polynomials with integer coefficients, we will only consider polynomials \( F(x, y) \) \( \in \mathbb{Z}[x, y] \) in two variables, then we ask questions about the set \( V_F = \{ (x, y) \in \mathbb{Q} \times \mathbb{Q} : F(x, y) = 0 \} \).

François Viète: "the proud problem of problems is to leave no problem unsolved"
Diophantine Problems

Francois Viete: "the proud problem of problems is to leave no problem unsolved"

Mohammad Sadek: Computing (Hyper)Elliptic Curves Over $\mathbb{Q}$
Studying zeros of multivariate polynomials with integer coefficients, Diophantine Equations will only consider polynomials \( F(x, y) \in \mathbb{Z}[x, y] \) in two variables, then we ask questions about the set \( V_F = \{ (x, y) \in \mathbb{Q} \times \mathbb{Q} : F(x, y) = 0 \} \).

Francois Viete: "the proud problem of problems is to leave no problem unsolved".

Mohammad Sadek: Computing (Hyper)Elliptic Curves Over \( \mathbb{Q} \).
Diophantine Problems ≈ Studying zeros of multivariate polynomials with integer coefficients, *Diophantine Equations*
Diophantine Problems $\approx$ Studying zeros of multivariate polynomials with integer coefficients, *Diophantine Equations*

*We will only consider polynomials $F(x, y) \in \mathbb{Z}[x, y]$ in two variables,*
Diophantine Equations

- Diophantine Problems ≈ Studying zeros of multivariate polynomials with integer coefficients, *Diophantine Equations*
- *We will only consider polynomials* $F(x, y) \in \mathbb{Z}[x, y]$ *in two variables, then we ask questions about the set*

$$V_F = \{(x, y) \in \mathbb{Q} \times \mathbb{Q} : F(x, y) = 0\}$$
Diophantine Problems ≈ Studying zeros of multivariate polynomials with integer coefficients, *Diophantine Equations*

*We will only consider polynomials $F(x, y) \in \mathbb{Z}[x, y]$ in two variables, then we ask questions about the set*

$$V_F = \{ (x, y) \in \mathbb{Q} \times \mathbb{Q} : F(x, y) = 0 \}$$

*François Viète:*
Diophantine Problems ≈ Studying zeros of multivariate polynomials with integer coefficients, *Diophantine Equations*

*We will only consider polynomials* \( F(x, y) \in \mathbb{Z}[x, y] \) *in two variables, then we ask questions about the set*

\[
V_F = \{(x, y) \in \mathbb{Q} \times \mathbb{Q} : F(x, y) = 0\}
\]

*François Viète:*

"the proud problem of problems is to leave no problem unsolved"

Mohammad Sadek
Computing (Hyper)Elliptic Curves Over \( \mathbb{Q} \)
Diophantine Equations

Given $F(x, y) \in \mathbb{Z}[x, y]$ with $V_F = \{(x, y) \in \mathbb{Q} \times \mathbb{Q} : F(x, y) = 0\}$

Is it possible to devise a process according to which it can be determined by a finite number of steps whether $V_F \neq \emptyset$?

Mohammad Sadek
Computing (Hyper)Elliptic Curves Over $\mathbb{Q}$
Diophantine Equations

Given $F(x, y) \in \mathbb{Z}[x, y]$ with $V_F = \{(x, y) \in \mathbb{Q} \times \mathbb{Q} : F(x, y) = 0\}$
Given $F(x, y) \in \mathbb{Z}[x, y]$ with $V_F = \{(x, y) \in \mathbb{Q} \times \mathbb{Q} : F(x, y) = 0\}$

Is it possible to devise a process according to which it can be determined by a finite number of steps whether $V_F \neq \emptyset$?
Diophantine Equations

We organize Diophantine equations by degrees.

degree 1.

\[ F(x, y) = ax + by - c, \quad a, b, c \in \mathbb{Z} \]

Then there is a pair \((x_0, y_0) \in V_F \cap \mathbb{Z}^2\) if and only if \(g := \gcd(a, b) \mid c\).

In the latter case \(V_F \cap \mathbb{Z}^2 = \{(x_0 + bk/g, y_0 - ak/g), k \in \mathbb{Z}\}\).

degree 2.

\[ F(x, y) = a_1x^2 + a_2xy + a_3y^2 + a_4x + a_5y + a_6, \quad a_i \in \mathbb{Z} \]

\(V_F \neq \emptyset\) if and only if \(|V_F| = \infty\).

There are effective algorithms to find whether \(V_F = \emptyset\).

We know how to describe every point in \(V_F\) explicitly.

Example: For \(F(x, y) = x^2 + y^2 - 1\), \(V_F = \{(2rs, r^2 - s^2) \mid r, s \in \mathbb{Z}\}\).
Diophantine Equations

We organize Diophantine equations by degrees.

- **degree 1.**

\[ F(x, y) = ax + by - c, \quad a, b, c \in \mathbb{Z}. \]

Then there is a pair \((x_0, y_0) \in V_F \cap \mathbb{Z}^2\) if and only if \(g := \gcd(a, b) | c\).

In the latter case \(V_F \cap \mathbb{Z}^2 = \{(x_0 + bk/g, y_0 - ak/g) \mid k \in \mathbb{Z}\}\).

- **degree 2.**

\[ F(x, y) = a_1 x^2 + a_2 xy + a_3 y^2 + a_4 x + a_5 y + a_6, \quad a_i \in \mathbb{Z}. \]

\(V_F \neq \emptyset\) if and only if \(|V_F| = \infty\).

There are effective algorithms to find whether \(V_F = \emptyset\).

We know how to describe every point in \(V_F\) explicitly.

**Example:** For \(F(x, y) = x^2 + y^2 - 1\), \(V_F = \{(2rsr^2 + s^2, r^2 - s^2r^2 + s^2) \mid r, s \in \mathbb{Z}\}\).\{0,0\}
Diophantine Equations

We organize Diophantine equations by degrees.

- **degree 1.** $F(x, y) = ax + by - c$, $a, b, c \in \mathbb{Z}$.
We organize Diophantine equations by degrees.

- **Degree 1.** \( F(x, y) = ax + by - c, \ a, b, c \in \mathbb{Z} \). Then there is a pair \((x_0, y_0) \in V_F \cap \mathbb{Z}^2\) if and only if \( g := \gcd(a, b) | c \).
We organize Diophantine equations by degrees.

- **degree 1.** \( F(x, y) = ax + by - c, \ a, b, c \in \mathbb{Z}. \)

Then there is a pair \((x_0, y_0) \in V_F \cap \mathbb{Z}^2\) if and only if 
\( g := \gcd(a, b) | c. \) In the latter case

\[
V_F \cap \mathbb{Z}^2 = \{(x_0 + bk/g, y_0 - ak/g), \ k \in \mathbb{Z}\}.
\]
Diophantine Equations

We organize Diophantine equations by degrees.

- **degree 1.** \( F(x, y) = ax + by - c, \ a, b, c \in \mathbb{Z}. \)
  Then there is a pair \((x_0, y_0) \in V_F \cap \mathbb{Z}^2\) if and only if \(g := \gcd(a, b)|c\). In the latter case
  \[
  V_F \cap \mathbb{Z}^2 = \{(x_0 + bk/g, y_0 - ak/g), \ k \in \mathbb{Z}\}.
  \]

- **degree 2.**

Mohammad Sadek

Computing (Hyper)Elliptic Curves Over \(\mathbb{Q}\)
We organize Diophantine equations by degrees.

- **degree 1.** \( F(x, y) = ax + by - c, \ a, b, c \in \mathbb{Z} \). 
  Then there is a pair \((x_0, y_0) \in V_F \cap \mathbb{Z}^2\) if and only if \( g := \gcd(a, b) | c \). In the latter case

\[
V_F \cap \mathbb{Z}^2 = \{(x_0 + bk/g, y_0 - ak/g), \ k \in \mathbb{Z}\}.
\]

- **degree 2.** \( F(x, y) = a_1x^2 + a_2xy + a_3y^2 + a_4x + a_5y + a_6, \ a_i \in \mathbb{Z} \).
Diophantine Equations

We organize Diophantine equations by degrees.

- **degree 1.** $F(x, y) = ax + by - c, \ a, b, c \in \mathbb{Z}$. Then there is a pair $(x_0, y_0) \in V_F \cap \mathbb{Z}^2$ if and only if $g := \gcd(a, b)|c$. In the latter case

$$V_F \cap \mathbb{Z}^2 = \{(x_0 + bk/g, y_0 - ak/g), \ k \in \mathbb{Z}\}.$$

- **degree 2.** $F(x, y) = a_1x^2 + a_2xy + a_3y^2 + a_4x + a_5y + a_6, \ a_i \in \mathbb{Z}$.

$$V_F \neq \emptyset \text{ if and only if } |V_F| = \infty.$$
Diophantine Equations

We organize Diophantine equations by degrees.

- **degree 1.** $F(x, y) = ax + by - c$, $a, b, c \in \mathbb{Z}$.
  Then there is a pair $(x_0, y_0) \in V_F \cap \mathbb{Z}^2$ if and only if $g := \gcd(a, b) | c$. In the latter case

  $$V_F \cap \mathbb{Z}^2 = \{(x_0 + bk/g, y_0 - ak/g), \ k \in \mathbb{Z}\}.$$

- **degree 2.** $F(x, y) = a_1x^2 + a_2xy + a_3y^2 + a_4x + a_5y + a_6$, $a_i \in \mathbb{Z}$.
  $V_F \neq \emptyset$ if and only if $|V_F| = \infty$.
  There are effective algorithms to find whether $V_F = \emptyset$. 

Mohammad Sadek
Computing (Hyper)Elliptic Curves Over $\mathbb{Q}$
Diophantine Equations

We organize Diophantine equations by degrees.

- **degree 1.** $F(x, y) = ax + by - c$, $a, b, c \in \mathbb{Z}$.
  Then there is a pair $(x_0, y_0) \in V_F \cap \mathbb{Z}^2$ if and only if $g := \gcd(a, b)|c$. In the latter case
  \[ V_F \cap \mathbb{Z}^2 = \{(x_0 + bk/g, y_0 - ak/g), \ k \in \mathbb{Z}\}. \]

- **degree 2.** $F(x, y) = a_1x^2 + a_2xy + a_3y^2 + a_4x + a_5y + a_6$, $a_i \in \mathbb{Z}$.
  \[ V_F \neq \emptyset \text{ if and only if } |V_F| = \infty. \]
  There are effective algorithms to find whether $V_F = \emptyset$. We know how to describe every point in $V_F$ explicitly.
Diophantine Equations

We organize Diophantine equations by degrees.

- **degree 1.** $F(x, y) = ax + by - c$, $a, b, c \in \mathbb{Z}$.

  Then there is a pair $(x_0, y_0) \in V_F \cap \mathbb{Z}^2$ if and only if $g := \gcd(a, b) | c$. In the latter case

  $$V_F \cap \mathbb{Z}^2 = \{(x_0 + bk/g, y_0 - ak/g), k \in \mathbb{Z}\}.$$

- **degree 2.** $F(x, y) = a_1x^2 + a_2xy + a_3y^2 + a_4x + a_5y + a_6$, $a_i \in \mathbb{Z}$.

  $$V_F \neq \emptyset$$ if and only if $|V_F| = \infty$.

  There are effective algorithms to find whether $V_F = \emptyset$. We know how to describe every point in $V_F$ explicitly.

  Example: For $F(x, y) = x^2 + y^2 - 1$,

  $$V_F = \left\{ \left( \frac{2rs}{r^2 + s^2}, \frac{r^2 - s^2}{r^2 + s^2} \right), r, s \in \mathbb{Z} \right\} \setminus \{(0, 0)\}.$$
Diophantine Equations

A Diophantine equation is a polynomial equation with integer coefficients that is to be solved in integers. For a degree 3 equation,

\[ F(x, y) = a_1 x^3 + a_2 x^2 y + a_3 x^2 + a_4 xy^2 + a_5 x + a_6 xy + a_7 y^3 + a_8 y^2 + a_9 y + a_{10} , \]

where \( a_i \in \mathbb{Z} \).

If \( \nabla F = (0, 0) \) and \( V_F \neq \emptyset \), then

\[ F(x, y) = y^2 - x^3 - Ax - B, \quad A, B \in \mathbb{Z} \]

describes an elliptic curve. An elliptic curve is an algebraic variety which possesses a group structure. The group law can be described using geometry, algebra, or analysis.

Elliptic curves are ubiquitous. They appear in number theory, complex analysis, cryptography, and mathematical physics.
Diophantine Equations

- degree 3.

\[ F(x, y) = a_1 x^3 + a_2 x^2 y + a_3 x^2 + a_4 xy^2 + a_5 x + a_6 xy + a_7 y^3 + a_8 y^2 + a_9 y + a_{10}, \]

\[ a_i \in \mathbb{Z}. \]

If \( (\frac{\partial F}{\partial x}, \frac{\partial F}{\partial y}) \neq (0, 0) \), and \( V_F \neq \emptyset \), then

\[ F(x, y) = y^2 - x^3 - Ax - B, \]

\[ A, B \in \mathbb{Z} \]

\[ y^2 = x^3 + Ax + b \]

describes an elliptic curve.

An elliptic curve is an algebraic variety which possesses a group structure.

The group law can be described using geometry, algebra, or analysis.

Elliptic curves are ubiquitous. They appear in number theory, complex analysis, cryptography, and mathematical physics.
Diophantine Equations

- degree 3. 😞

An elliptic curve is an algebraic variety which possesses a group structure. The group law can be described using geometry, algebra, or analysis. Elliptic curves are ubiquitous. They appear in number theory, complex analysis, cryptography, and mathematical physics.
**Diophantine Equations**

- **degree 3. 🙁**
  
  \[ F(x, y) = a_1 x^3 + a_2 x^2 y + a_3 x^2 + a_4 xy^2 + a_5 x + a_6 xy + a_7 y^3 + a_8 y^2 + a_9 y + a_{10}, \]
  
  \[ a_i \in \mathbb{Z}. \]
Diophantine Equations

- **degree 3.** 😞
  \[ F(x, y) = \]
  \[ a_1x^3 + a_2x^2y + a_3x^2 + a_4xy^2 + a_5x + a_6xy + a_7y^3 + a_8y^2 + a_9y + a_{10}, \]
  \[ a_i \in \mathbb{Z}. \]

If \( (\frac{\partial F}{\partial x}, \frac{\partial F}{\partial y}) \neq (0, 0) \), and \( V_F \neq \emptyset \),
Diophantine Equations

- degree 3.

\[ F(x, y) = \]
\[ a_1 x^3 + a_2 x^2 y + a_3 x^2 + a_4 xy^2 + a_5 x + a_6 xy + a_7 y^3 + a_8 y^2 + a_9 y + a_{10}, \]
\[ a_i \in \mathbb{Z}. \]

If \( (\frac{\partial F}{\partial x}, \frac{\partial F}{\partial y}) \neq (0, 0), \) and \( V_F \neq \emptyset, \) then

\[ F(x, y) = y^2 - x^3 - Ax - B, \quad A, B \in \mathbb{Z} \]
Diophantine Equations

- **degree 3.**

  \[ F(x, y) = a_1 x^3 + a_2 x^2 y + a_3 x^2 + a_4 x y^2 + a_5 x + a_6 x y + a_7 y^3 + a_8 y^2 + a_9 y + a_{10}, \]
  \[ a_i \in \mathbb{Z}. \]

  If \((\partial F / \partial x, \partial F / \partial y) \neq (0, 0)\), and \(V_F \neq \emptyset\), then

  \[ F(x, y) = y^2 - x^3 - A x - B, \quad A, B \in \mathbb{Z} \]

- \( y^2 = x^3 + A x + b \) describes an

Mohammad Sadek  |  Computing (Hyper)Elliptic Curves Over \( \mathbb{Q} \)
Diophantine Equations

- **degree 3. 😞**

  \[ F(x, y) = \]
  \[ a_1 x^3 + a_2 x^2 y + a_3 x^2 + a_4 xy^2 + a_5 x + a_6 xy + a_7 y^3 + a_8 y^2 + a_9 y + a_{10}, \]
  \[ a_i \in \mathbb{Z}. \]

  If \( \left( \frac{\partial F}{\partial x}, \frac{\partial F}{\partial y} \right) \neq (0, 0) \), and \( V_F \neq \emptyset \), then

  \[ F(x, y) = y^2 - x^3 - Ax - B, \quad A, B \in \mathbb{Z} \]

- \( y^2 = x^3 + Ax + b \) describes an **elliptic curve**
Diophantine Equations

- **degree 3.**

\[ F(x, y) = a_1x^3 + a_2x^2y + a_3x^2 + a_4xy^2 + a_5x + a_6xy + a_7y^3 + a_8y^2 + a_9y + a_{10}, \]

\[ a_i \in \mathbb{Z}. \]

If \( (\frac{\partial F}{\partial x}, \frac{\partial F}{\partial y}) \neq (0, 0), \) and \( V_F \neq \emptyset, \) then

\[ F(x, y) = y^2 - x^3 - Ax - B, \quad A, B \in \mathbb{Z} \]

- \( y^2 = x^3 + Ax + b \) describes an **elliptic curve**

- An elliptic curve is an algebraic variety which possesses a group structure.
Diophantine Equations

- **degree 3.**
  
  \[ F(x, y) = a_1 x^3 + a_2 x^2 y + a_3 x^2 + a_4 xy^2 + a_5 x + a_6 xy + a_7 y^3 + a_8 y^2 + a_9 y + a_{10}, \]
  \[ a_i \in \mathbb{Z}. \]

  If \( \left( \frac{\partial F}{\partial x}, \frac{\partial F}{\partial y} \right) \neq (0, 0), \) and \( V_F \neq \emptyset, \) then

  \[ F(x, y) = y^2 - x^3 - Ax - B, \quad A, B \in \mathbb{Z} \]

- \( y^2 = x^3 + Ax + b \) describes an **elliptic curve**

- An elliptic curve is an algebraic variety which possesses a group structure.

- The group law can be described using geometry, algebra, or analysis.
Diophantine Equations

- **degree 3.**

  \[ F(x, y) = a_1 x^3 + a_2 x^2 y + a_3 x^2 + a_4 xy^2 + a_5 x + a_6 xy + a_7 y^3 + a_8 y^2 + a_9 y + a_{10}, \]
  \[ a_i \in \mathbb{Z}. \]

  If \((\frac{\partial F}{\partial x}, \frac{\partial F}{\partial y}) \neq (0, 0), \text{ and } V_F \neq \emptyset\), then

  \[ F(x, y) = y^2 - x^3 - Ax - B, \quad A, B \in \mathbb{Z} \]

- \(y^2 = x^3 + Ax + b\) describes an **elliptic curve**

- An elliptic curve is an algebraic variety which possesses a group structure.

- The group law can be described using geometry, algebra, or analysis.

- Elliptic curves are ubiquitous. They appear in number theory, complex analysis, cryptography, and mathematical physics.
Elliptic Curves

An elliptic curve $E$ over the rationals is a curve described by

$$y^2 = x^3 + Ax + B, \quad A, B \in \mathbb{Z}$$

where $\Delta(E) = -16(4A^3 + 27B^2) \neq 0$ is called the discriminant of $E$. 

Mohammad Sadek
Computing (Hyper)Elliptic Curves Over $\mathbb{Q}$
An elliptic curve $E$ over the rationals is a curve described by

$$y^2 = x^3 + Ax + B, \quad A, B \in \mathbb{Z}$$

where $\Delta(E) = -16(4A^3 + 27B^2) \neq 0$ is called the \textit{discriminant} of $E$. 
Elliptic curves

\[ y^2 = x^3 + Ax + B, \quad A, B \in \mathbb{Z} \]
Elliptic curves

$y^2 = x^3 + Ax + B, \quad A, B \in \mathbb{Z}$
Elliptic curves

\[ y^2 = x^3 + Ax + B, \quad A, B \in \mathbb{Z} \]
An Example

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

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

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

Mohammad Sadek
Computing (Hyper)Elliptic Curves Over \( \mathbb{Q} \)
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 \( P = (3, 6) \in E \)
- \( 2P = \left( -\frac{23}{144}, \frac{2827}{1728} \right) \)
- \( 3P = \left( -\frac{193101}{207025}, -\frac{53536482}{94196375} \right) \)
An Example

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

- The point \( P = (3, 6) \in E \)
- \( 2P = (-23/144, 2827/1728) \)
- \( 3P = (-193101/207025, -53536482/94196375) \)
- \( 4P = (3324592417/4603351104, -685780509326543/312328165704192) \)
Two elliptic curves described over $\mathbb{Q}$ by

$$
\begin{align*}
y^2 &= x^3 + Ax + B \\
y^2 &= x^3 + A'x + B'
\end{align*}
$$

are isomorphic if

$$(x, y) \mapsto (u^2x, u^3y) \quad \text{for some } u \in \mathbb{Q} \setminus \{0\}.$$ 

Then $A' = u^4 A$ and $B' = u^6 B$ and $\Delta' = u^{12} \Delta$. 

Mohammad Sadek

Computing (Hyper)Elliptic Curves Over $\mathbb{Q}$
Let $E$ be an elliptic curve over $\mathbb{Q}$ defined by $y^2 = x^3 + Ax + B$.

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

$E(\mathbb{Q})$ is a subgroup of $E$. Once you describe $E(\mathbb{Q})$, you solve a Diophantine equation.

The following celebrated theorem is due to Mordell.

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

$E(\mathbb{Q})$ is a subgroup of $E$. Once you describe $E(\mathbb{Q})$, you solve a Diophantine equation.

The following celebrated theorem is due to Mordell.

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

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

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

Let $E$ be an elliptic curve over $\mathbb{Q}$ defined by $y^2 = x^3 + Ax + B$.

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

$E(\mathbb{Q})$ is a subgroup of $E$. Once you describe $E(\mathbb{Q})$, you solve a Diophantine equation.
Let $E$ be an elliptic curve over $\mathbb{Q}$ defined by $y^2 = x^3 + Ax + B$.

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

$E(\mathbb{Q})$ is a subgroup of $E$. Once you describe $E(\mathbb{Q})$, you solve a Diophantine equation. The following celebrated theorem is due to Mordell.
Let $E$ be an elliptic curve over $\mathbb{Q}$ defined by $y^2 = x^3 + Ax + B$.

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

$E(\mathbb{Q})$ is a subgroup of $E$. Once you describe $E(\mathbb{Q})$, you solve a Diophantine equation. The following celebrated theorem is due to Mordell.

**Theorem**

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

There exists a nonnegative integer $r$ such that

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

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

In other words, there exist finitely many $P_1, \ldots, P_s \in E(\mathbb{Q})$, $s \geq r$, such that any point $P \in E(\mathbb{Q})$ can be written as

$$P = n_1P_1 + n_2P_2 + \ldots + n_sP_s, \quad n_i \in \mathbb{Z}.$$
E(\mathbb{Q}) \sim \mathbb{Z}^r \times \mathbb{T}

The following theorem is due to Mazur.
The following theorem is due to Mazur.

**Theorem**

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

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

**Theorem**

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

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

In particular, \( |\mathbb{T}| \leq 16 \).
Finding solutions for a polynomial equation over a finite field is easier than finding solutions in \( \mathbb{Q} \).

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

In particular, if \( p \geq 5 \), then \( \Delta(E) = -16(4A^3 + 27B^2) \not\equiv 0 \mod p \).

\( E(\mathbb{F}_p) \) is either cyclic or \( E(\mathbb{F}_p) \sim \mathbb{Z}/M\mathbb{Z} \times \mathbb{Z}/L\mathbb{Z} \) with \( L | M \).
Finding solutions for a polynomial equation over a finite field is easier than finding solutions in \( \mathbb{Q} \).
Finding solutions for a polynomial equation over a finite field is easier than finding solutions in $\mathbb{Q}$.

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

$E(\mathbb{F}_p) = \{(x, y) : x, y \in \mathbb{F}_p, y^2 = x^3 + Ax + B\}$ is either cyclic or $E(\mathbb{F}_p) \cong \mathbb{Z}/M\mathbb{Z} \times \mathbb{Z}/L\mathbb{Z}$ with $L | M$. 

Mohammad Sadek
Computing (Hyper)Elliptic Curves Over $\mathbb{Q}$
Finding solutions for a polynomial equation over a finite field is easier than finding solutions in $\mathbb{Q}$.

Let $E$ be an elliptic curve defined by $y^2 = x^3 + Ax + B$, $A, B \in \mathbb{F}_p$. In particular, if $p \geq 5$, then

$$\Delta(E) = -16(4A^3 + 27B^2) \not\equiv 0 \pmod{p}.$$
Finding solutions for a polynomial equation over a finite field is easier than finding solutions in \( \mathbb{Q} \).

Let \( E \) be an elliptic curve defined by \( y^2 = x^3 + Ax + B \), \( A, B \in \mathbb{F}_p \). In particular, if \( p \geq 5 \), then

\[
\Delta(E) = -16(4A^3 + 27B^2) \not\equiv 0 \mod p.
\]

\[E(\mathbb{F}_p) = \{(x, y) : x, y \in \mathbb{F}_p, \, y^2 = x^3 + Ax + B\}\]
Finding solutions for a polynomial equation over a finite field is easier than finding solutions in $\mathbb{Q}$.

Let $E$ be an elliptic curve defined by $y^2 = x^3 + Ax + B$, $A, B \in \mathbb{F}_p$. In particular, if $p \geq 5$, then

$$\Delta(E) = -16(4A^3 + 27B^2) \not\equiv 0 \mod p.$$  

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

$E(\mathbb{F}_p)$ is either **cyclic** or $E(\mathbb{F}_p) \cong \mathbb{Z}/M\mathbb{Z} \times \mathbb{Z}/L\mathbb{Z}$ with $L|M$. 
Let \( E : y^2 = x^3 + Ax + B, \) \( A, B \in \mathbb{Z} \) and \( p \geq 5 \) a prime.
Let $E : y^2 = x^3 + Ax + B$, $A, B \in \mathbb{Z}$ and $p \geq 5$ a prime

The above Weierstrass equation is called $p$-minimal if $\nu_p(\Delta)$ is the smallest among all elliptic curves isomorphic to $E$.
Let $E : y^2 = x^3 + Ax + B$, $A, B \in \mathbb{Z}$ and $p \geq 5$ a prime.

The above Weierstrass equation is called \textit{p-minimal} if $\nu_p(\Delta)$ is the smallest among all elliptic curves isomorphic to $E$.

Every elliptic curve over $\mathbb{Q}$ has a globally minimal Weierstrass equation ($p$-minimal at every prime $p$).
Let $E : y^2 = x^3 + Ax + B$, $A, B \in \mathbb{Z}$ and $p \geq 5$ a prime.

The above Weierstrass equation is called $p$-minimal if $\nu_p(\Delta)$ is the smallest among all elliptic curves isomorphic to $E$.

Every elliptic curve over $\mathbb{Q}$ has a globally minimal Weierstrass equation ($p$-minimal at every prime $p$).

We set $E_p : y^2 = x^3 + A_p x + B_p$ where

$$A_p \equiv A \mod p, \quad B_p \equiv B \mod p.$$
Let $E : y^2 = x^3 + Ax + B$, $A, B \in \mathbb{Z}$ and $p \geq 5$ a prime

The above Weierstrass equation is called \textit{$p$-minimal} if $\nu_p(\Delta)$ is the smallest among all elliptic curves isomorphic to $E$

Every elliptic curve over $\mathbb{Q}$ has a globally minimal Weierstrass equation (\textit{$p$-minimal} at every prime $p$).

We set $E_p : y^2 = x^3 + A_p x + B_p$ where

$$A_p \equiv A \mod p, \quad B_p \equiv B \mod p.$$ 

Is $E_p$ still an elliptic curve over $\mathbb{F}_p$?
Reduction of elliptic curves

\[ \frac{E}{\mathbb{Q}} \]
\[ y^2 = x^3 + Ax + B \]
\[ \Delta \neq 0 \]

\[ E \downarrow \begin{array}{c}
\text{reduction} \\
\text{mod } p
\end{array} \]
\[ E_p \]

\[ \frac{E_p}{\mathbb{F}_p} \]
\[ y^2 = x^3 + ax + b \]

\[ p = 2 \quad \Delta(E_2) \equiv 0 \text{ mod } 2 \]
\[ p = 3 \quad \Delta(E_3) \equiv 0 \text{ mod } 3 \]
\[ p = 5 \quad \Delta(E_5) \equiv 0 \text{ mod } 5 \]
\[ p = 7 \quad \Delta(E_7) \equiv 0 \text{ mod } 7 \]
\[ p = 11 \quad \Delta(E_{11}) \equiv 0 \text{ mod } 11 \]
\[ p = 13 \quad \Delta(E_{13}) \equiv 0 \text{ mod } 13 \]
Reduction of elliptic curves

Let $E : y^2 = x^3 + Ax + B$, $A, B \in \mathbb{Z}$, be an elliptic curve with minimal discriminant $\Delta$. 

$E_p : y^2 = x^3 + A_p x + B_p$ is an elliptic curve if $\nu_p(\Delta) = 0$.

$E$ is said to have good reduction at $p$.

$E_p$ is a singular curve if $\nu_p(\Delta) > 0$.

$E$ is said to have bad reduction at $p$.

If moreover $\nu_p(A) = 0$ ($\nu_p(A) > 0$), then $E$ is said to have multiplicative (additive) reduction at $p$.

The reason is: $E_p(F_p) \sim = F \times_p E_p(F_p) \sim = F + p(E_p(F_p))$. 

Mohammad Sadek
Computing (Hyper)Elliptic Curves Over $\mathbb{Q}$
• Let $E : y^2 = x^3 + Ax + B$, $A, B \in \mathbb{Z}$, be an elliptic curve with minimal discriminant $\Delta$.

• $E_p : y^2 = x^3 + A_p x + B_p$ is an elliptic curve if $\nu_p(\Delta) = 0$.

Mohammad Sadek Computing (Hyper)Elliptic Curves Over $\mathbb{Q}$
Reduction of elliptic curves

Let \( E : y^2 = x^3 + Ax + B, \ A, B \in \mathbb{Z}, \) be an elliptic curve with minimal discriminant \( \Delta. \)

\( E_p : y^2 = x^3 + A_p x + B_p \) is an elliptic curve if \( \nu_p(\Delta) = 0. \) \( E \) is said to have good reduction at \( p. \)
Let $E : y^2 = x^3 + Ax + B$, $A, B \in \mathbb{Z}$, be an elliptic curve with minimal discriminant $\Delta$.

$E_p : y^2 = x^3 + A_p x + B_p$ is an elliptic curve if $\nu_p(\Delta) = 0$. $E$ is said to have good reduction at $p$.

$E_p$ is a singular curve if $\nu_p(\Delta) > 0$. 
Let $E : y^2 = x^3 + Ax + B$, $A, B \in \mathbb{Z}$, be an elliptic curve with minimal discriminant $\Delta$.

- $E_p : y^2 = x^3 + A_p x + B_p$ is an elliptic curve if $\nu_p(\Delta) = 0$. $E$ is said to have \textit{good reduction} at $p$.
- $E_p$ is a singular curve if $\nu_p(\Delta) > 0$. $E$ is said to have \textit{bad reduction} at $p$. 

Mohammad Sadek

Computing (Hyper)Elliptic Curves Over $\mathbb{Q}$
Let $E : y^2 = x^3 + Ax + B$, $A, B \in \mathbb{Z}$, be an elliptic curve with minimal discriminant $\Delta$.

$E_p : y^2 = x^3 + A_p x + B_p$ is an elliptic curve if $\nu_p(\Delta) = 0$. $E$ is said to have good reduction at $p$.

$E_p$ is a singular curve if $\nu_p(\Delta) > 0$. $E$ is said to have bad reduction at $p$. If moreover $\nu_p(A) = 0$ ($\nu_p(A) > 0$), then $E$ is said to have multiplicative (additive) reduction at $p$. 
Let $E : y^2 = x^3 + Ax + B$, $A, B \in \mathbb{Z}$, be an elliptic curve with minimal discriminant $\Delta$.

$E_p : y^2 = x^3 + A_p x + B_p$ is an elliptic curve if $\nu_p(\Delta) = 0$. $E$ is said to have *good reduction* at $p$.

$E_p$ is a singular curve if $\nu_p(\Delta) > 0$. $E$ is said to have *bad reduction* at $p$. If moreover $\nu_p(A) = 0$ ($\nu_p(A) > 0$), then $E$ is said to have multiplicative (additive) reduction at $p$.

The reason is: $E_p(\overline{\mathbb{F}}_p) \cong \overline{\mathbb{F}}_p^\times$ ($E_p(\overline{\mathbb{F}}_p) \cong \overline{\mathbb{F}}_p^+$).
Reduction of elliptic curves

The (globally) minimal Weierstrass equation describing \( E \) defines a scheme over \( \mathbb{Z} \) for every prime \( p \).

The resulting scheme may not be regular if \( \nu_p(\Delta) \neq 0 \).

So the singular point on the special fiber may be a singular point of the scheme.

By resolving the singularity, one obtains the minimal proper regular model of \( E \), whose generic fiber is isomorphic to \( E \), and whose special fiber is a union of curves.

The classification of such models is due to Néron-Kodaira.

The possibilities for such a model are denoted by a Kodaira symbol:

- Good Reduction: \( I^0 \)
- Multiplicative Reduction: \( I^n \), \( n \geq 1 \)
- Additive Reduction: \( II, III, IV, I^*n, II^*, III^*, IV^* \)

Mohammad Sadek Computing (Hyper)Elliptic Curves Over \( \mathbb{Q} \)
The (globally) minimal Weierstrass equation describing $E$ defines a scheme over $\mathbb{Z}_p$ for every prime $p$. The resulting scheme may not be regular if $\nu_p(\Delta) \neq 0$. So the singular point on the special fiber may be a singular point of the scheme. By resolving the singularity, one obtains the minimal proper regular model of $E$, whose generic fiber is isomorphic to $E$, and whose special fiber is a union of curves. The classification of such models is due to Néron-Kodaira. The possibilities for such a model are denoted by a Kodaira symbol:

- **Good Reduction**: $I^0$
- **Multiplicative Reduction**: $I^n$, $n \geq 1$
- **Additive Reduction**: $II$, $III$, $IV$, $I^*n$, $n \geq 0$, $IV^*$, $III^*$, $II^*$
The (globally) minimal Weierstrass equation describing $E$ defines a scheme over $\mathbb{Z}_p$ for every prime $p$. The resulting scheme may not be regular if $\nu_p(\Delta) \neq 0$. 
The (globally) minimal Weierstrass equation describing $E$ defines a scheme over $\mathbb{Z}_p$ for every prime $p$. The resulting scheme may not be regular if $\nu_p(\Delta) \neq 0$. So the singular point on the special fiber may be a singular point of the scheme.
The (globally) minimal Weierstrass equation describing $E$ defines a scheme over $\mathbb{Z}_p$ for every prime $p$. The resulting scheme may not be regular if $\nu_p(\Delta) \neq 0$. So the singular point on the special fiber may be a singular point of the scheme. By resolving the singularity, one obtains the minimal proper regular model of $E$, whose generic fiber is isomorphic to $E$, and whose special fiber is a union of curves.
The (globally) minimal Weierstrass equation describing $E$ defines a scheme over $\mathbb{Z}_p$ for every prime $p$. The resulting scheme may not be regular if $\nu_p(\Delta) \neq 0$. So the singular point on the special fiber may be a singular point of the scheme. By resolving the singularity, one obtains the minimal proper regular model of $E$, whose generic fiber is isomorphic to $E$, and whose special fiber is a union of curves.

The classification of such models is due to Néron-Kodaira.
The (globally) minimal Weierstrass equation describing $E$ defines a scheme over $\mathbb{Z}_p$ for every prime $p$. The resulting scheme may not be regular if $\nu_p(\Delta) \neq 0$. So the singular point on the special fiber may be a singular point of the scheme. By resolving the singularity, one obtains the minimal proper regular model of $E$, whose generic fiber is isomorphic to $E$, and whose special fiber is a union of curves.

The classification of such models is due to Néron-Kodaira. The possibilities for such a model are denoted by a Kodaira symbol:

- **Good Reduction**: $I_0$,
- **Multiplicative Reduction**: $I_n, n \geq 1$,
- **Additive Reduction**: $II, III, IV, I_n^*, n \geq 0, IV^*, III^*, II^*$
Tate’s algorithm produces the model of a given elliptic curve.
Tate’s algorithm produces the model of a given elliptic curve. The algorithm analyses the $p$-valuations of the coefficients in the minimal Weierstrass equation together with the discriminant.
Tate’s algorithm produces the model of a given elliptic curve. The algorithm analyses the $p$-valuations of the coefficients in the minimal Weierstrass equation together with the discriminant.

**Example.**

- The elliptic curve $E : y^2 = x^3 - 7x + 6$ has minimal discriminant $\Delta_E = 2^8 \times 5^2$. 
Tate’s algorithm produces the model of a given elliptic curve. The algorithm analyses the $p$-valuations of the coefficients in the minimal Weierstrass equation together with the discriminant.

**Example.**

- The elliptic curve $E : y^2 = x^3 - 7x + 6$ has minimal discriminant $\Delta_E = 2^8 \times 5^2$.
- $E$ has good reduction at any prime $p \neq 2, 5$. 
Tate’s algorithm produces the model of a given elliptic curve. The algorithm analyses the $p$-valuations of the coefficients in the minimal Weierstrass equation together with the discriminant.

**Example.**

- The elliptic curve $E : y^2 = x^3 - 7x + 6$ has minimal discriminant $\Delta_E = 2^8 \times 5^2$.
- $E$ has good reduction at any prime $p \neq 2, 5$.
- $E$ has additive reduction at 2, of type $I_0^*$. 
Tate’s algorithm produces the model of a given elliptic curve. The algorithm analyses the $p$-valuations of the coefficients in the minimal Weierstrass equation together with the discriminant.

Example.

- The elliptic curve $E : y^2 = x^3 - 7x + 6$ has minimal discriminant $\Delta_E = 2^8 \times 5^2$.
- $E$ has good reduction at any prime $p \neq 2, 5$.
- $E$ has additive reduction at 2, of type $I_0^*$.
- $E$ has multiplicative reduction at 5, of type $I_2$. 
The Discriminant

The minimal discriminant $\Delta_E$ of $E$ carries information about the elliptic curve $E$, e.g., how many primes $p$ are there such that $E_p$ is not an elliptic curve over $\mathbb{F}_p$? how hard it is to get rid of the singularity of $E_p$?

Mohammad Sadek
Computing (Hyper)Elliptic Curves Over $\mathbb{Q}$
The minimal discriminant $\Delta_E$ of $E$ carries information about the elliptic curve $E$, e.g., how many primes $p$ are there such that $E_p$ is not an elliptic curve over $\mathbb{F}_p$? how hard it is to get rid of the singularity of $E_p$?
Elliptic curves with a prescribed discriminant

Given a nonzero integer $D$, how many elliptic curves $E$ are there such that $\Delta_E = D$?

There is no elliptic curve over $\mathbb{Q}$ whose minimal discriminant is $\pm 1$.

Shafarevich's Theorem. Up to isomorphisms over $\mathbb{Q}$, there are only finitely many elliptic curves $E$ over $\mathbb{Q}$ such that $\Delta_E = D$.

How finite? Is there a way we can list all such isomorphism classes of elliptic curves?
Question. Given a nonzero integer $D$, how many elliptic curves $E$ are there such that $\Delta_E = D$?
Question. Given a nonzero integer $D$, how many elliptic curves $E$ are there such that $\Delta_E = D$?

There is no elliptic curve over $\mathbb{Q}$ whose minimal discriminant is $\pm 1$. 
Question. Given a nonzero integer $D$, how many elliptic curves $E$ are there such that $\Delta_E = D$?

There is no elliptic curve over $\mathbb{Q}$ whose minimal discriminant is $\pm 1$.

Shafarevich’s Theorem. Up to isomorphisms over $\mathbb{Q}$, there are only finitely many elliptic curves $E$ over $\mathbb{Q}$ such that $\Delta_E = D$. 
Question. Given a nonzero integer $D$, how many elliptic curves $E$ are there such that $\Delta_E = D$?

There is no elliptic curve over $\mathbb{Q}$ whose minimal discriminant is $\pm 1$.

Shafarevich’s Theorem. Up to isomorphisms over $\mathbb{Q}$, there are only finitely many elliptic curves $E$ over $\mathbb{Q}$ such that $\Delta_E = D$.

How finite?
Question. Given a nonzero integer $D$, how many elliptic curves $E$ are there such that $\Delta_E = D$?

There is no elliptic curve over $\mathbb{Q}$ whose minimal discriminant is $\pm 1$.

Shafarevich's Theorem. Up to isomorphisms over $\mathbb{Q}$, there are only finitely many elliptic curves $E$ over $\mathbb{Q}$ such that $\Delta_E = D$.

How finite? Is there a way we can list all such isomorphism classes of elliptic curves?
Elliptic curves with a prescribed discriminant

Why is the question hard?
Elliptic curves with a prescribed discriminant

Why is the question hard?

- Let $E$ be an elliptic curve over $\mathbb{Q}$. 

A globally minimal Weierstrass equation describing $E$ is of the form

$$y^2 + a_1 xy + a_3 y = x^3 + a_2 x^2 + a_4 x + a_6,$$

where $a_i \in \mathbb{Z}$.

$$b_2 = a_2^2 + 4a_2,$$

$$b_4 = 2a_4 + a_1 a_3,$$

$$b_6 = a_2^3 + 4a_6,$$

$$\Delta_E = -b_2^2 b_8 - 8b_3^4 - 27b_2^6 + 9b_2 b_4 b_6.$$

To find elliptic curves with prime power discriminant $\pm p^\alpha$, we solve the Diophantine equation

$$-b_2^2 b_8 - 8b_3^4 - 27b_2^6 + 9b_2 b_4 b_6 = \pm p^\alpha$$

in $b_2, b_4, b_6, b_8, p, \alpha$. 
Elliptic curves with a prescribed discriminant

Why is the question hard?

- Let $E$ be an elliptic curve over $\mathbb{Q}$.
- A globally minimal Weierstrass equation describing $E$ is of the form
  \[ y^2 + a_1 xy + a_3 y = x^3 + a_2 x^2 + a_4 x + a_6, \quad a_i \in \mathbb{Z}. \]

To find elliptic curves with prime power discriminant $\pm p^\alpha$, we solve the Diophantine equation
\[ -b_2^2 b_8 - 8 b_3^4 - 27 b_2^6 + 9 b_2 b_4 b_6 = \pm p^\alpha \]
in $b_2, b_4, b_6, b_8, p, \alpha$.  

Mohammad Sadek  
Computing (Hyper)Elliptic Curves Over $\mathbb{Q}$
Elliptic curves with a prescribed discriminant

Why is the question hard?

- Let $E$ be an elliptic curve over $\mathbb{Q}$.
- A globally minimal Weierstrass equation describing $E$ is of the form $y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$, $a_i \in \mathbb{Z}$.

\[
\begin{align*}
  b_2 &= a_1^2 + 4a_2 \\
  b_4 &= 2a_4 + a_1a_3 \\
  b_6 &= a_3^2 + 4a_6 \\
  b_8 &= a_1^2a_6 + 4a_2a_6 - a_1a_3a_4 + a_2a_3^2 - a_4^2 \\
  \Delta_E &= -b_2^2b_8 - 8b_4^3 - 27b_6^2 + 9b_2b_4b_6
\end{align*}
\]
Elliptic curves with a prescribed discriminant

Why is the question hard?

- Let $E$ be an elliptic curve over $\mathbb{Q}$.
- A globally minimal Weierstrass equation describing $E$ is of the form $y^2 + a_1 xy + a_3 y = x^3 + a_2 x^2 + a_4 x + a_6$, $a_i \in \mathbb{Z}$.

\[
\begin{align*}
    b_2 &= a_1^2 + 4a_2 \\
    b_4 &= 2a_4 + a_1 a_3 \\
    b_6 &= a_3^2 + 4a_6 \\
    b_8 &= a_1^2 a_6 + 4a_2 a_6 - a_1 a_3 a_4 + a_2 a_3^2 - a_4^2 \\
    \Delta_E &= -b_2^2 b_8 - 8b_4^3 - 27b_6^2 + 9b_2 b_4 b_6
\end{align*}
\]

- To find elliptic curves with prime power discriminant $\pm p^\alpha$, we solve the Diophantine equation

\[-b_2^2 b_8 - 8b_4^3 - 27b_6^2 + 9b_2 b_4 b_6 = \pm p^\alpha\]

in $b_2, b_4, b_6, b_8, p, \alpha$. 
Elliptic curves with a prescribed discriminant

Given a specified number field and a finite set of primes $S$, there is an algorithm that gives a complete set of elliptic curves over $K$ with good reduction outside $S$, Cremona-Lingham.

Example. If $K = \mathbb{Q}$ and $S = \{2, 3\}$, then there are 6120 elliptic curves over $\mathbb{Q}$, up to $\mathbb{Q}$-isomorphism, with discriminant $2^a \times 3^b$ ($a \leq 8$, $b \leq 5$). This list was given earlier by Ogg and Hadano.
Given a specified number field and a finite set of primes $S$, there is an algorithm that gives a complete set of elliptic curves over $K$ with good reduction outside $S$, Cremona-Lingham.
Elliptic curves with a prescribed discriminant

- Given a specified number field and a finite set of primes $S$, there is an algorithm that gives a complete set of elliptic curves over $K$ with good reduction outside $S$, Cremona-Lingham.

- **Example.** If $K = \mathbb{Q}$ and $S = \{2, 3\}$, then there are 6120 elliptic curves over $\mathbb{Q}$, up to $\mathbb{Q}$-isomorphism, with discriminant $2^a \times 3^b$ ($a \leq 8$, $b \leq 5$).
Given a specified number field and a finite set of primes $S$, there is an algorithm that gives a complete set of elliptic curves over $K$ with good reduction outside $S$, Cremona-Lingham.

**Example.** If $K = \mathbb{Q}$ and $S = \{2, 3\}$, then there are 6120 elliptic curves over $\mathbb{Q}$, up to $\mathbb{Q}$-isomorphism, with discriminant $2^a \times 3^b$ ($a \leq 8, b \leq 5$). This list was given earlier by Ogg and Hadano.
Elliptic curves with a prescribed discriminant

Can we list all elliptic curves over \( \mathbb{Q} \) whose minimal discriminant is a prime power, \( p^\alpha, \alpha \geq 1 \)?

Either \( |\Delta_E| = p \) or \( p^2 \), or else \( p = 11 \) and \( \Delta_E = 11^5 \), or \( p = 17 \) and \( \Delta_E = 17^4 \), or \( p = 19 \) and \( \Delta_E = 19^3 \), or \( p = 37 \) and \( \Delta_E = 37^3 \) (Serre, Mestre, Frey, Mazur, Oesterlé, Edixhoven, De Groot, J. Top).

It is conjectured that there are infinitely many elliptic curves with prime discriminant!

Can we classify all elliptic curves over \( \mathbb{Q} \) whose minimal discriminant is a product of two prime powers?

Mohammad Sadek

Computing (Hyper)Elliptic Curves Over \( \mathbb{Q} \)
Can we list all elliptic curves over $\mathbb{Q}$ whose minimal
discriminant is a prime power, $p^\alpha$, $\alpha \geq 1$?
Can we list all elliptic curves over $\mathbb{Q}$ whose minimal discriminant is a prime power, $p^\alpha$, $\alpha \geq 1$?

Either $|\Delta_E| = p$ or $p^2$, or else $p = 11$ and $\Delta_E = 11^5$, or $p = 17$ and $\Delta_E = 17^4$, or $p = 19$ and $\Delta_E = 19^3$, or $p = 37$ and $\Delta_E = 37^3$ (Serre, Mestre, Frey, Mazur, Oesterlé, Edixhoven, De Groot, J. Top).
Can we list all elliptic curves over $\mathbb{Q}$ whose minimal discriminant is a prime power, $p^\alpha$, $\alpha \geq 1$?

Either $|\Delta_E| = p$ or $p^2$, or else $p = 11$ and $\Delta_E = 11^5$, or $p = 17$ and $\Delta_E = 17^4$, or $p = 19$ and $\Delta_E = 19^3$, or $p = 37$ and $\Delta_E = 37^3$ (Serre, Mestre, Frey, Mazur, Oesterlé, Edixhoven, De Groot, J. Top).

It is conjectured that there are infinitely many elliptic curves with prime discriminant!
Can we list all elliptic curves over $\mathbb{Q}$ whose minimal discriminant is a prime power, $p^\alpha$, $\alpha \geq 1$?

Either $|\Delta_E| = p$ or $p^2$, or else $p = 11$ and $\Delta_E = 11^5$, or $p = 17$ and $\Delta_E = 17^4$, or $p = 19$ and $\Delta_E = 19^3$, or $p = 37$ and $\Delta_E = 37^3$ (Serre, Mestre, Frey, Mazur, Oesterlé, Edixhoven, De Groot, J. Top).

It is conjectured that there are infinitely many elliptic curves with prime discriminant!

Can we classify all elliptic curves over $\mathbb{Q}$ whose minimal discriminant is a product of two prime powers?
Elliptic curves with a prescribed discriminant

History.
History.

- The list of all elliptic curves with 2-torsion and with minimal discriminant $2^k p^m$ was given by Ogg, Hadano, and Ivorra.

It is an open problem to classify elliptic curves over $\mathbb{Q}$ with a rational 3-torsion point and good reduction outside the set $\{p, q\}$, with $p$ and $q$ different primes $\geq 5$.

It is an open problem to classify elliptic curves over $\mathbb{Q}$ with trivial rational torsion and good reduction outside the set $\{p, q\}$, with $p$ and $q$ different primes.
History.

- The list of all elliptic curves with 2-torsion and with minimal discriminant $2^k p^m$ was given by Ogg, Hadano, and Ivorra.
- The list of elliptic curves with $n$-torsion, $n \geq 4$, and with minimal discriminant $p^m q^n$, where $p$ and $q$ are distinct primes was given by Bennett-Vatsal-Yazdani, Sadek, Dąbrowski-Jędrzejak.
History.

- The list of all elliptic curves with 2-torsion and with minimal discriminant $2^k p^m$ was given by Ogg, Hadano, and Ivorra.
- The list of elliptic curves with $n$-torsion, $n \geq 4$, and with minimal discriminant $p^m q^n$, where $p$ and $q$ are distinct primes was given by Bennett-Vatsal-Yazdani, Sadek, Dąbrowski-Jędrzejak.
- It is an open problem to classify elliptic curves over $\mathbb{Q}$ with a rational 3-torsion point and good reduction outside the set $\{p, q\}$, with $p$ and $q$ different primes $\geq 5$. 
History.

- The list of all elliptic curves with 2-torsion and with minimal discriminant $2^k p^m$ was given by Ogg, Hadano, and Ivorra.
- The list of elliptic curves with $n$-torsion, $n \geq 4$, and with minimal discriminant $p^m q^n$, where $p$ and $q$ are distinct primes was given by Bennett-Vatsal-Yazdani, Sadek, Dąbrowski-Jędrzejak.
- It is an open problem to classify elliptic curves over $\mathbb{Q}$ with a rational 3-torsion point and good reduction outside the set $\{p, q\}$, with $p$ and $q$ different primes $\geq 5$.
- It is an open problem to classify elliptic curves over $\mathbb{Q}$ with trivial rational torsion and good reduction outside the set $\{p, q\}$, with $p$ and $q$ different primes.
Goal:

Given an integer $p^aq^b$, where $q \neq p$ are primes and $a, b > 0$, provide a recipe to find all elliptic curves with a non-trivial torsion point and minimal discriminant $\Delta = \pm p^aq^b$. 
The Tate normal form of an elliptic curve $E$ with torsion point $P = (0, 0) \in E(\mathbb{Q})[m], m \neq 2, 3$, is:

$$y^2 + (1 - c)xy - by = x^3 - bx^2$$
The Tate normal form of an elliptic curve $E$ with torsion point $P = (0, 0) \in E(\mathbb{Q})[m]$, $m \neq 2, 3$, is:

$$y^2 + (1 - c)xy - by = x^3 - bx^2$$

The discriminant:

$$\Delta_E = b^3(16b^2 - b(8c^2 + 20c - 1) - c(1 - c)^3)$$
The Tate normal form of an elliptic curve $E$ with torsion point $P = (0, 0) \in E(\mathbb{Q})[m], \ m \neq 2, 3,$ is:

$$y^2 + (1 - c)xy - by = x^3 - bx^2$$

The discriminant:

$$\Delta_E = b^3(16b^2 - b(8c^2 + 20c - 1) - c(1 - c)^3)$$

**Strategy.** Solve the Diophantine equation:

$$\Delta_E = \pm p^aq^b$$

We solve the problem when the order of the torsion point is $m \geq 4$, and $p, q \geq 5$. 
when \( E(\mathbb{Q})[5] \neq \{0\} \), we solve the Diophantine equation:

\[
5st + 5(5s^2 - 11st - t^2) = \pm 5^a q^b
\]

for \( p \neq q \) primes, and \( a, b > 0 \).

Theorem (Sadek, 2014)

Let \( E/\mathbb{Q} \) be an elliptic curve such that \( E(\mathbb{Q})[5] \neq \{0\} \) and \( \Delta_E = \pm 5^a q^b \) for distinct prime \( p \) and \( q \). It follows that \( \Delta_E \) is given as follows:

\[
\begin{align*}
25 \times 5^2, \\
215 \times 5^2, \\
35 \times 5^2, \\
13 \times 5^2, \\
37 \times 31^2, \\
7 \times 5^3, \\
p^k q^k
\end{align*}
\]

Similar lists when \( E(\mathbb{Q})[m] \neq \{0\} \), \( m \geq 4 \).

For example, there exists no elliptic curve \( E/\mathbb{Q} \) with \( E(\mathbb{Q})[10] \neq \{0\} \) and \( |\Delta_E| = 5^a q^b \), where \( p \neq q \) are primes, and \( a, b > 0 \).
when $E(\mathbb{Q})[5] \neq \{O\}$, we solve the Diophantine equation:

$$s^5 t^5 (s^2 - 11st - t^2) = \pm p^aq^b$$

for $p \neq q$ primes, and $a, b > 0$
• when $E(\mathbb{Q})[5] \neq \{O\}$, we solve the Diophantine equation:

$$s^5t^5(s^2 - 11st - t^2) = \pm p^aq^b$$

for $p \neq q$ primes, and $a, b > 0$

**Theorem (Sadek, 2014)**

Let $E/\mathbb{Q}$ be an elliptic curve such that $E(\mathbb{Q})[5] \neq \{0\}$ and $\Delta_E = \pm p^aq^b$ for distinct prime $p$ and $q$. It follows that $\Delta_E$ is given as follows:

$$2^5 \times 5^2, 2^{15} \times 5^2, 3^5 \times 5^2, 13^5 \times 5^2, 37^5 \times 31^2, 7^5 \times 5^3, p^kq$$
when \( E(\mathbb{Q})[5] \neq \{O\} \), we solve the Diophantine equation:

\[
s^5t^5(s^2 - 11st - t^2) = \pm p^aq^b
\]

for \( p \neq q \) primes, and \( a, b > 0 \)

**Theorem (Sadek, 2014)**

\( E/\mathbb{Q} \) be an elliptic curve such that \( E(\mathbb{Q})[5] \neq \{0\} \) and \( \Delta_E = \pm p^aq^b \) for distinct prime \( p \) and \( q \). It follows that \( \Delta_E \) is given as follows:

\[
2^5 \times 5^2, \ 2^{15} \times 5^2, \ 3^5 \times 5^2, \ 13^5 \times 5^2, \ 37^5 \times 31^2, \ 7^5 \times 5^3, \ p^{5k}q
\]

Similar lists when \( E(\mathbb{Q})[m] \neq \{0\}, m \geq 4 \).
When \( E(\mathbb{Q})[5] \neq \{O\} \), we solve the Diophantine equation:

\[
s^5 t^5 (s^2 - 11st - t^2) = \pm p^a q^b
\]

for \( p \neq q \) primes, and \( a, b > 0 \)

**Theorem (Sadek, 2014)**

Let \( E/\mathbb{Q} \) be an elliptic curve such that \( E(\mathbb{Q})[5] \neq \{0\} \) and \( \Delta_E = \pm p^a q^b \) for distinct prime \( p \) and \( q \). It follows that \( \Delta_E \) is given as follows:

\[
2^5 \times 5^2, 2^{15} \times 5^2, 3^5 \times 5^2, 13^5 \times 5^2, 37^5 \times 31^2, 7^5 \times 5^3, p^{5k} q
\]

Similar lists when \( E(\mathbb{Q})[m] \neq \{0\}, m \geq 4 \).

For example, There exists no elliptic curve \( E/\mathbb{Q} \) with \( E(\mathbb{Q})[10] \neq \{0\} \) and \( |\Delta_E| = p^a q^b \), where \( p \neq q \) are primes, and \( a, b > 0 \).
Let

\[ f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_0, \quad a_i \in K, \quad a_n \neq 0 \]

where \( n \geq 5 \) and \( f(x) \) has no double roots.
Let
\[ f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_0, \quad a_i \in K, \quad a_n \neq 0 \]

where \( n \geq 5 \) and \( f(x) \) has no double roots.

The curve \( C : y^2 = f(x) \), is a **hyperelliptic curve**.
Let
\[ f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_0, \quad a_i \in K, \quad a_n \neq 0 \]
where \( n \geq 5 \) and \( f(x) \) has no double roots.

The curve \( C : y^2 = f(x) \), is a **hyperelliptic curve**.

The genus of the curve \( C \) is \( \left\lfloor \frac{n-1}{2} \right\rfloor \geq 2 \).
Let

\[ f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_0, \quad a_i \in K, \quad a_n \neq 0 \]

where \( n \geq 5 \) and \( f(x) \) has no double roots. The curve \( C : y^2 = f(x) \), is a \textbf{hyperelliptic curve}.

The genus of the curve \( C \) is \( \left\lfloor \frac{n - 1}{2} \right\rfloor \geq 2 \).

Recall that

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

\[ f(x) = a_nx^n + a_{n-1}x^{n-1} + \cdots + a_0, \quad a_i \in K, \quad a_n \neq 0 \]

where \( n \geq 5 \) and \( f(x) \) has no double roots.

The curve \( C : y^2 = f(x) \), is a **hyperelliptic curve**.

The genus of the curve \( C \) is \( \left\lfloor \frac{n-1}{2} \right\rfloor \geq 2 \).

Recall that

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

**Theorem (Faltings’ Theorem)**

\( C(\mathbb{Q}) \) is finite.
The curve $C : y^2 = f(x)$, $\deg f(x) \geq 5$, and $g(C) = \left\lfloor \frac{n-1}{2} \right\rfloor$.

$C(\mathbb{F}_p) = \{(x, y) : x, y \in \mathbb{F}_p, y^2 = f(x)\}$. 
The curve $C : y^2 = f(x)$, $\deg f(x) \geq 5$, and $g(C) = \left\lfloor \frac{n-1}{2} \right\rfloor$.

$$C(\mathbb{F}_p) = \{(x, y) : x, y \in \mathbb{F}_p, y^2 = f(x)\}.$$
Let $C$ be a hyperelliptic curve defined by $y^2 = f(x)$, where $f(x) \in \mathbb{Z}[x]$ and $\deg f(x)$ is either 5 or 6, over $\mathbb{Q}$.
Let $C$ be a hyperelliptic curve defined by $y^2 = f(x)$, where $f(x) \in \mathbb{Z}[x]$ and deg $f(x)$ is either 5 or 6, over $\mathbb{Q}$.

Let $C_p$ be the curve defined by $y^2 = f_p(x)$, where $f_p(x)$ is the reduction of $f(x) \mod p$. 
Let $C$ be a hyperelliptic curve defined by $y^2 = f(x)$, where $f(x) \in \mathbb{Z}[x]$ and $\deg f(x)$ is either 5 or 6, over $\mathbb{Q}$.

Let $C_p$ be the curve defined by $y^2 = f_p(x)$, where $f_p(x)$ is the reduction of $f(x) \mod p$. When $g = 1$, there were 3 possibilities,
Let $C$ be a hyperelliptic curve defined by $y^2 = f(x)$, where $f(x) \in \mathbb{Z}[x]$ and $\deg f(x)$ is either 5 or 6, over $\mathbb{Q}$.

Let $C_p$ be the curve defined by $y^2 = f_p(x)$, where $f_p(x)$ is the reduction of $f(x)$ mod $p$. When $g = 1$, there were 3 possibilities, when $g = 2$, there are 8 possibilities for $C_p$. 

There is a globally minimal discriminant $\Delta_C$ of $C$ over $\mathbb{Q}$, (Lockhart, Liu). $C_p$ is singular if and only if $\nu_p(\Delta_C) > 0$. 

Mohammad Sadek
Computing (Hyper)Elliptic Curves Over $\mathbb{Q}$
Let $C$ be a hyperelliptic curve defined by $y^2 = f(x)$, where $f(x) \in \mathbb{Z}[x]$ and $\deg f(x)$ is either 5 or 6, over $\mathbb{Q}$.

Let $C_p$ be the curve defined by $y^2 = f_p(x)$, where $f_p(x)$ is the reduction of $f(x)$ mod $p$. When $g = 1$, there were 3 possibilities, when $g = 2$, there are 8 possibilities for $C_p$.

One may define the discriminant of $C$. 
Let $C$ be a hyperelliptic curve defined by $y^2 = f(x)$, where $f(x) \in \mathbb{Z}[x]$ and $\deg f(x)$ is either 5 or 6, over $\mathbb{Q}$.

Let $C_p$ be the curve defined by $y^2 = f_p(x)$, where $f_p(x)$ is the reduction of $f(x)$ mod $p$. When $g = 1$, there were 3 possibilities, when $g = 2$, there are 8 possibilities for $C_p$.

One may define the discriminant of $C$. There is a globally minimal discriminant $\Delta_C$ of $C$ over $\mathbb{Q}$, (Lockhart, Liu).
Let $C$ be a hyperelliptic curve defined by $y^2 = f(x)$, where $f(x) \in \mathbb{Z}[x]$ and $\deg f(x)$ is either 5 or 6, over $\mathbb{Q}$.

Let $C_p$ be the curve defined by $y^2 = f_p(x)$, where $f_p(x)$ is the reduction of $f(x) \bmod p$. When $g = 1$, there were 3 possibilities, when $g = 2$, there are 8 possibilities for $C_p$.

One may define the discriminant of $C$. There is a globally minimal discriminant $\Delta_C$ of $C$ over $\mathbb{Q}$, (Lockhart, Liu).

$C_p$ is singular if and only if $\nu_p(\Delta_C) > 0$. 

Let \( C \) be a hyperelliptic curve defined by \( y^2 = f(x) \), where \( f(x) \in \mathbb{Z}[x] \) and \( \deg f(x) \) is either 5 or 6, over \( \mathbb{Q} \).
Let $C$ be a hyperelliptic curve defined by $y^2 = f(x)$, where $f(x) \in \mathbb{Z}[x]$ and $\deg f(x)$ is either 5 or 6, over $\mathbb{Q}$.

There is a minimal regular model for $C$ over $\mathbb{Z}_p$ for every prime $p$, (Ueno-Namikawa, Liu).
Let $C$ be a hyperelliptic curve defined by $y^2 = f(x)$, where $f(x) \in \mathbb{Z}[x]$ and $\deg f(x)$ is either 5 or 6, over $\mathbb{Q}$.

There is a minimal regular model for $C$ over $\mathbb{Z}_p$ for every prime $p$, (Ueno-Namikawa, Liu).

There are 120 possibilities for these minimal proper regular models.
Let \( C \) be a hyperelliptic curve defined by \( y^2 = f(x) \), where \( f(x) \in \mathbb{Z}[x] \) and \( \deg f(x) \) is either 5 or 6, over \( \mathbb{Q} \).

There is a minimal regular model for \( C \) over \( \mathbb{Z}_p \) for every prime \( p \), (Ueno-Namikawa, Liu).

There are 120 possibilities for these minimal proper regular models.

Given a hyperelliptic curve \( C : y^2 = f(x) \), \( \deg f(x) = 5, 6 \), an algorithm due to Liu gives the minimal proper regular model of \( C \).
Question. Given a nonzero integer $D$, list all genus 2 curves with minimal discriminant $D$. Up to isomorphisms over $\mathbb{Q}$, there are only finitely many hyperelliptic curves $C$ over $\mathbb{Q}$ with genus 2 such that $\Delta_C = D$, (Shafarevich, Merriman, Oort, Parˇsin, Faltings).
Hyperelliptic curves with a prescribed discriminant

**Question.** Given a nonzero integer $D$, list all genus 2 curves with minimal discriminant $D$. 
Question. Given a nonzero integer $D$, list all genus 2 curves with minimal discriminant $D$.

Up to isomorphisms over $\mathbb{Q}$, there are only finitely many hyperelliptic curves $C$ over $\mathbb{Q}$ with genus 2 such that $\Delta_C = D$, (Shafarevich, Merriman, Oort, Paršin, Faltings).
Hyperelliptic curves with a prescribed discriminant

Genus 2 Curve Search Results give all genus 2 curves with absolute discriminant up to $10^6$ together with much additional information (Cremona).

The complete list of genus 2 curves over $\mathbb{Q}$ with good reduction outside 2, up to isomorphism over $\mathbb{Q}$, is produced. There are 428 of them, (Smart, 1996).

Can we produce the list of genus 2 curves with good reduction away from a prime $p \neq 2$, i.e., $\Delta_C = p^a$, $a \geq 1$, for some prime $p \neq 2$?
Genus 2 Curve Search Results give all genus 2 curves with absolute discriminant up to $10^6$ together with much additional information (Cremona)
Genus 2 Curve Search Results give all genus 2 curves with absolute discriminant up to $10^6$ together with much additional information (Cremona).

The complete list of genus 2 curves over $\mathbb{Q}$ with good reduction outside 2, up to isomorphism over $\mathbb{Q}$, is produced. There are 428 of them, (Smart, 1996).
Hyperelliptic curves with a prescribed discriminant

- Genus 2 Curve Search Results give all genus 2 curves with absolute discriminant up to $10^6$ together with much additional information (Cremona).
- The complete list of genus 2 curves over $\mathbb{Q}$ with good reduction outside 2, up to isomorphism over $\mathbb{Q}$, is produced. There are 428 of them, (Smart, 1996).
- Can we produce the list of genus 2 curves with good reduction away from a prime $p \neq 2$, i.e., $\Delta_C = p^a$, $a \geq 1$, for some prime $p \neq 2$?
Hyperelliptic curves with a prescribed discriminant

Why is the question harder?
Why is the question harder?

- Let $C$ be a smooth genus two curve over $\mathbb{Q}$.
Why is the question harder?

- Let $C$ be a smooth genus two curve over $\mathbb{Q}$.
- A globally minimal equation describing $C$ is of the form

\[ y^2 + (a_0 x^2 + a_1 x + a_2)y = b_0 x^6 + b_1 x^5 + b_2 x^4 + b_3 x^3 + b_4 x^2 + b_5 x + b_6, \quad a_i, b_i \in \mathbb{Z}; \]
Why is the question harder?

Let $C$ be a smooth genus two curve over $\mathbb{Q}$.

A globally minimal equation describing $C$ is of the form

$$y^2 + (a_0 x^2 + a_1 x + a_2)y = b_0 x^6 + b_1 x^5 + b_2 x^4 + b_3 x^3 + b_4 x^2 + b_5 x + b_6, \quad a_i, b_i \in \mathbb{Z};$$

$$\Delta_C \in \mathbb{Z}[a_0, a_1, a_2, b_0, \ldots, b_6]$$

is homogeneous of degree 10.
Why is the question harder?

- Let $C$ be a smooth genus two curve over $\mathbb{Q}$.
- A globally minimal equation describing $C$ is of the form
  \[ y^2 + (a_0 x^2 + a_1 x + a_2)y = b_0 x^6 + b_1 x^5 + b_2 x^4 + b_3 x^3 + b_4 x^2 + b_5 x + b_6, \ a_i, b_i \in \mathbb{Z}; \]

  \[ \Delta_C \in \mathbb{Z}[a_0, a_1, a_2, b_0, \ldots, b_6] \]

  is homogeneous of degree 10.

- To find all genus 2 curves with minimal discriminant $\pm p^\alpha$, we solve the Diophantine equation

  \[ \Delta_C = \pm p^\alpha \]

  in $a_0, a_1, a_2, b_0, b_1, b_2, b_3, b_4, b_5, b_6, p, \alpha$. 

Mohammad Sadek  Computing (Hyper)Elliptic Curves Over $\mathbb{Q}$
Joint with A. Dąbrowski, 2020

- We assume the existence of at least two rational Weierstrass points on $C$. 

$y^2 = x^5 + a_1x^4 + a_2x^3 + a_3x^2 + a_4x + a_5,$ 
$a_i \in \mathbb{Z} = (x - A)g(x), A \in \mathbb{Z}, g(x) \in \mathbb{Z}[x]$ is monic.

Under this assumption, we find those genus 2 curves with minimal discriminant $\Delta = \pm p$, and $p$ is an odd prime.
Joint with **A. Dąbrowski**, 2020

- We assume the existence of at least two rational Weierstrass points on $C$. In particular, $C$ may be described by

$$y^2 = x^5 + a_1 x^4 + a_2 x^3 + a_3 x^2 + a_4 x + a_5, \quad a_i \in \mathbb{Z}$$
Joint with **A. Dąbrowski**, 2020

- We assume the existence of at least two rational Weierstrass points on $C$. In particular, $C$ may be described by

$$y^2 = x^5 + a_1 x^4 + a_2 x^3 + a_3 x^2 + a_4 x + a_5, \quad a_i \in \mathbb{Z}$$

$$= (x - A)g(x), \quad A \in \mathbb{Z}, \ g(x) \in \mathbb{Z}[x] \text{ is monic.}$$
Joint with A. Dąbrowski, 2020

- We assume the existence of at least two rational Weierstrass points on $C$. In particular, $C$ may be described by

$$y^2 = x^5 + a_1 x^4 + a_2 x^3 + a_3 x^2 + a_4 x + a_5, \quad a_i \in \mathbb{Z}$$

$$= (x - A)g(x), \quad A \in \mathbb{Z}, \ g(x) \in \mathbb{Z}[x] \text{ is monic.}$$

- Under this assumption, we find those genus 2 curves with minimal discriminant $\Delta = \pm p$, and $p$ is an odd prime.
Theorem (Dąbrowski-Sadek, 2020)

Let $C$ be a genus 2 curve with minimal discriminant of the form $2^a p^b$, where $p$ is an odd prime, $a \geq 0$, $b \geq 1$. If $C$ has six rational Weierstrass points, then $C$ is isomorphic to one of the following curves described by the following Weierstrass equations:

$$y^2 = x(x - 1)(x + 1)(x - 2)(x + 2), \quad \Delta_{E_0} = 2^{18} \cdot 3^4,$$
$$y^2 = x(x - 3)(x + 3)(x - 6)(x + 6), \quad \Delta_{E_1} = 2^{18} \cdot 3^{14}.$$
If we consider genus two curves with exactly three $\mathbb{Q}$-rational Weierstrass points.

**Theorem (Dąbrowski-Sadek, 2020)**

Let $C$ be a smooth projective curve of genus 2 defined over $\mathbb{Q}$ with good reduction at the prime 2. Assume that $C$ has exactly three $\mathbb{Q}$-rational Weierstrass points. If the minimal discriminant of $C$ is a square-free odd integer, then $C$ is described by one of the following globally minimal Weierstrass equations

\[
y^2 - x^2y = x^5 + 16t x^4 + (16 + 8t) x^3 + (8 + t) x^2 + xy^2 + (-x^2 - x)y = x^5 + (-1 + t) x^4 + (-2 - 2t) x^3 + (2 + t) x^2 - xy
\]

for some $t \in \mathbb{Z}$.

By Bounyakovsky' Conjecture, there are infinitely many genus 2 curves with prime discriminant.
If we consider genus two curves with exactly three $\mathbb{Q}$-rational Weierstrass points.

**Theorem (Dąbrowski-Sadek, 2020)**

Let $C$ be a smooth projective curve of genus 2 defined over $\mathbb{Q}$ with good reduction at the prime 2. Assume that $C$ has exactly three $\mathbb{Q}$-rational Weierstrass points. If the minimal discriminant of $C$ is a square-free odd integer, then $C$ is described by one of the following globally minimal Weierstrass equations

\[
\begin{align*}
  y^2 - x^2 y &= x^5 + 16t x^4 + (16 + 8t) x^3 + (8 + t) x^2 + x \\
  y^2 + (-x^2 - x) y &= x^5 + (-1 + t) x^4 + (-2 - 2t) x^3 + (2 + t) x^2 - x
\end{align*}
\]

for some $t \in \mathbb{Z}$. 

By Bounyakovsky' Conjecture, there are infinitely many genus 2 curves with prime discriminant.
If we consider genus two curves with exactly three $\mathbb{Q}$-rational Weierstrass points.

**Theorem (Dąbrowski-Sadek, 2020)**

Let $C$ be a smooth projective curve of genus 2 defined over $\mathbb{Q}$ with good reduction at the prime 2. Assume that $C$ has exactly three $\mathbb{Q}$-rational Weierstrass points. If the minimal discriminant of $C$ is a square-free odd integer, then $C$ is described by one of the following globally minimal Weierstrass equations

\[
\begin{align*}
y^2 - x^2 y &= x^5 + 16t x^4 + (16 + 8t) x^3 + (8 + t) x^2 + x \\
y^2 + (-x^2 - x)y &= x^5 + (-1 + t) x^4 + (-2 - 2t) x^3 + (2 + t) x^2 - x
\end{align*}
\]

for some $t \in \mathbb{Z}$.

$|\Delta| = p$ if a certain irreducible quartic polynomial in $\mathbb{Z}[x]$ takes the value $p$. 
If we consider genus two curves with exactly three \( \mathbb{Q} \)-rational Weierstrass points.

**Theorem (Dąbrowski-Sadek, 2020)**

Let \( C \) be a smooth projective curve of genus 2 defined over \( \mathbb{Q} \) with good reduction at the prime 2. Assume that \( C \) has exactly three \( \mathbb{Q} \)-rational Weierstrass points. If the minimal discriminant of \( C \) is a square-free odd integer, then \( C \) is described by one of the following globally minimal Weierstrass equations

\[
\begin{align*}
    y^2 - x^2 y &= x^5 + 16t x^4 + (16 + 8t) x^3 + (8 + t) x^2 + x \\
    y^2 + (-x^2 - x) y &= x^5 + (-1 + t) x^4 + (-2 - 2t) x^3 + (2 + t) x^2 - x
\end{align*}
\]

for some \( t \in \mathbb{Z} \).

\( |\Delta| = p \) if a certain irreducible quartic polynomial in \( \mathbb{Z}[x] \) takes the value \( p \). By Bounyakovsky’ Conjecture, there are infinitely many genus 2 curves with prime discriminant.
Thank you for your attention!