**Classical Question:** Given a polynomial equation, what are the rational solutions?
Classical Question: Given a polynomial equation, what are the rational solutions?

\[ y^2 = x^3 + Ax + B, \text{ with } A, B \in \mathbb{Q} \]
**Classical Question:** Given a polynomial equation, what are the rational solutions?

\[ y^2 = x^3 + Ax + B, \text{ with } A, B \in \mathbb{Q} \]

\[ E = \text{elliptic curve} / \mathbb{Q} \]
Classical Question: Given a polynomial equation, what are the rational solutions?

\[ y^2 = x^3 + Ax + B, \text{ with } A, B \in \mathbb{Q} \]

\[ E = \text{elliptic curve} / \mathbb{Q} \]

Theorem (Mordell)

\[ E(\mathbb{Q}) \text{ is a finitely generated abelian group.} \]

\[ E(\mathbb{Q}) \cong E(\mathbb{Q})[\text{tors}] \times \mathbb{Z}^r \]
Question: Which finite groups arise?
Question: Which finite groups arise?

Theorem (Mazur, 1977)

For $E/\mathbb{Q}$, $E(\mathbb{Q})[\text{tors}]$ is isomorphic to

$$\mathbb{Z}/m\mathbb{Z} \quad 1 \leq m \leq 10 \text{ or } m = 12$$

$$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2m\mathbb{Z} \quad 1 \leq m \leq 4$$
Question: Which finite groups arise?

<table>
<thead>
<tr>
<th>Theorem (Mazur, 1977)</th>
</tr>
</thead>
<tbody>
<tr>
<td>For $E / \mathbb{Q}$, $E(\mathbb{Q})[\text{tors}]$ is isomorphic to</td>
</tr>
<tr>
<td>$\mathbb{Z}/m\mathbb{Z}$</td>
</tr>
<tr>
<td>$1 \leq m \leq 10$ or $m = 12$</td>
</tr>
<tr>
<td>$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2m\mathbb{Z}$</td>
</tr>
<tr>
<td>$1 \leq m \leq 4$</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Theorem (Kamienny-Kenku-Momose)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Let $F$ be a quadratic field. For $E/F$ the group $E(F)[\text{tors}]$ is isomorphic to</td>
</tr>
<tr>
<td>$\mathbb{Z}/m\mathbb{Z}$</td>
</tr>
<tr>
<td>$1 \leq m \leq 18$, $m \neq 17$</td>
</tr>
<tr>
<td>$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2m\mathbb{Z}$</td>
</tr>
<tr>
<td>$1 \leq m \leq 6$</td>
</tr>
<tr>
<td>$\mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/3m\mathbb{Z}$</td>
</tr>
<tr>
<td>$1 \leq m \leq 2$</td>
</tr>
<tr>
<td>$\mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z}$</td>
</tr>
</tbody>
</table>
Consider all number fields $F$ of degree $d$ and all $E/F$. What $E(F)[\text{tors}]$ arise?
Consider all number fields $F$ of degree $d$ and all $E/F$. What $E(F)[\text{tors}]$ arise?

**Theorem (Merel, 1996)**

*If $E$ is an elliptic curve defined over a number field $F$ of degree $d$, then*

$$
\#E(F)[\text{tors}] \leq C(d).
$$
Consider all number fields $F$ of degree $d$ and all $E/F$. What $E(F)[\text{tors}]$ arise?

**Theorem (Merel, 1996)**

If $E$ is an elliptic curve defined over a number field $F$ of degree $d$,

$$\#E(F)[\text{tors}] \leq C(d).$$

$[F : \mathbb{Q}] = d$: Only finitely many groups arise.
For most elliptic curves, $\text{End}_\mathbb{F}(E) \cong \mathbb{Z}$.

- Usual endomorphisms: $P \mapsto [n]P$, $n \in \mathbb{Z}$. 
For most elliptic curves, $\text{End}_{\overline{F}}(E) \cong \mathbb{Z}$.

- Usual endomorphisms: $P \mapsto [n]P$, $n \in \mathbb{Z}$.

For elliptic curves with complex multiplication (CM), $\text{End}_{\overline{F}}(E) \cong \mathcal{O} = \mathbb{Z} + f\mathcal{O}_K$. 

The elliptic curve $y^2 = x^3 + 1$ has CM by the maximal order in $\mathbb{Q}(\sqrt{-3})$. 

Extra endomorphism: $(x, y) \mapsto (-1 + \sqrt{-3}/2 \cdot x, y)$. 


CM Elliptic Curves

For most elliptic curves, \( \text{End}_\mathbb{𝔽}(E) \cong \mathbb{ℤ} \).

- Usual endomorphisms: \( P \mapsto [n]P, \ n \in \mathbb{ℤ} \).

For elliptic curves with complex multiplication (CM), \( \text{End}_\mathbb{𝔽}(E) \cong \mathcal{O} = \mathbb{ℤ} + f \mathcal{O}_K \).

- The elliptic curve \( y^2 = x^3 + 1 \) has CM by the maximal order in \( \mathbb{ℚ}(\sqrt{-3}) \).
- Extra endomorphism:

\[
(x, y) \mapsto \left( \frac{-1 + \sqrt{-3}}{2} x, y \right)
\]
Theorem (Olson, 1974)

Let $E/\mathbb{Q}$ be a CM elliptic curve. Then $E(\mathbb{Q})[\text{tors}]$ is isomorphic to one of the following 6 groups:

$$\{\cdot\}, \mathbb{Z}/2\mathbb{Z}, \mathbb{Z}/3\mathbb{Z}, \mathbb{Z}/4\mathbb{Z}, \mathbb{Z}/6\mathbb{Z}, \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$$
Theorem (Olson, 1974)

Let \( E/\mathbb{Q} \) be a CM elliptic curve. Then \( E(\mathbb{Q})[\text{tors}] \) is isomorphic to one of the following 6 groups:

\[
\{\cdot\}, \quad \mathbb{Z}/2\mathbb{Z}, \quad \mathbb{Z}/3\mathbb{Z}, \quad \mathbb{Z}/4\mathbb{Z}, \quad \mathbb{Z}/6\mathbb{Z}, \quad \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}
\]

- \([F : \mathbb{Q}] \leq 13\): Clark, Corn, Rice, Stankewicz, 2014.
Theorem (Olson, 1974)

Let $E/\mathbb{Q}$ be a CM elliptic curve. Then $E(\mathbb{Q})[\text{tors}]$ is isomorphic to one of the following 6 groups:

\[
\{\cdot\}, \quad \mathbb{Z}/2\mathbb{Z}, \quad \mathbb{Z}/3\mathbb{Z}, \quad \mathbb{Z}/4\mathbb{Z}, \quad \mathbb{Z}/6\mathbb{Z}, \quad \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}
\]

- $[F : \mathbb{Q}] \leq 13$: Clark, Corn, Rice, Stankewicz, 2014.
- $[F : \mathbb{Q}] = p$ or $p^2$: Bourdon, Clark, Stankewicz, 2015.
Theorem (Olson, 1974)

Let $E/\mathbb{Q}$ be a CM elliptic curve. Then $E(\mathbb{Q})[\text{tors}]$ is isomorphic to one of the following 6 groups:

\[ \{\cdot\}, \mathbb{Z}/2\mathbb{Z}, \mathbb{Z}/3\mathbb{Z}, \mathbb{Z}/4\mathbb{Z}, \mathbb{Z}/6\mathbb{Z}, \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} \]

- $[F : \mathbb{Q}] \leq 13$: Clark, Corn, Rice, Stankewicz, 2014.
- $[F : \mathbb{Q}] = p$ or $p^2$: Bourdon, Clark, Stankewicz, 2015.
- $[F : \mathbb{Q}]$ odd: Bourdon, Pollack, 2017.
What happens when $E$ is defined over a number field of degree 14?

Theorem (C., 2019)

Let $F$ be a number field of degree 14. Let $E/F$ be a CM elliptic curve. For $E/F$ the group $E(F)\,[\text{tors}]$ is isomorphic to one of the following:

- $\mathbb{Z}/m\mathbb{Z}$ with $1 \leq m \leq 4$
- $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/m\mathbb{Z}$ with $1 \leq m \leq 3$
- $\mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/m\mathbb{Z}$

The groups that did not arise in degree 2 are $\mathbb{Z}/29\mathbb{Z}$, $\mathbb{Z}/43\mathbb{Z}$, $\mathbb{Z}/49\mathbb{Z}$, $\mathbb{Z}/53\mathbb{Z}$, $\ldots$. 
What happens when E is defined over a number field of degree 14?

Theorem (C., 2019)

Let $F$ be a number field of degree 14. Let $E/F$ be a CM elliptic curve. For $E/F$ the group $E(F)[\text{tors}]$ is isomorphic to one of the following:

- $\mathbb{Z}/m\mathbb{Z}$ for $1 \leq m \leq 4$ or $m = 6, 7, 10, 29, 43, 49, 53$
- $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2m\mathbb{Z}$ for $1 \leq m \leq 3$
- $\mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z}$
What happens when $E$ is defined over a number field of degree 14?

**Theorem (C., 2019)**

Let $F$ be a number field of degree 14. Let $E/F$ be a CM elliptic curve. For $E/F$ the group $E(F)[\text{tors}]$ is isomorphic to one of the following:

- $\mathbb{Z}/m\mathbb{Z}$ for $1 \leq m \leq 4$ or $m = 6, 7, 10, 29, 43, 49, 53$
- $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2m\mathbb{Z}$ for $1 \leq m \leq 3$
- $\mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z}$

The groups that did not arise in degree 2 are

$\mathbb{Z}/29\mathbb{Z}, \mathbb{Z}/43\mathbb{Z}, \mathbb{Z}/49\mathbb{Z}, \mathbb{Z}/58\mathbb{Z}$.
Theorem (Bourdon, Clark, 2018)

If a CM elliptic curve $E$ defined over a number field $F$ of degree 14 has a point of order $N$, then

$$\frac{\varphi(N)}{\#O^x} \mid 14.$$
Lemma (C., 2019)

Let $\mathcal{O}$ be the order of discriminant $\Delta$ and let $\ell_1^{a_1} \cdots \ell_n^{a_n}$ denote the prime power decomposition of $N \geq 4$. If $\frac{\varphi(N)}{\omega} = d$, then, in order to have a point of order $N$ occur in degree $d$, we must have $(\frac{\Delta}{\ell}) = 0$ for every odd prime $\ell | N$. Furthermore, if the largest power of two dividing $N$ is 2, then two may be split but otherwise 2 must also be ramified.
Lemma (C., 2019)

Let $O$ be the order of discriminant $\Delta$ and let $\ell_1^{a_1} \cdots \ell_n^{a_n}$ denote the prime power decomposition of $N \geq 4$. If $\frac{\varphi(N)}{\omega} = d$, then, in order to have a point of order $N$ occur in degree $d$, we must have $(\frac{\Delta}{\ell}) = 0$ for every odd prime $\ell \mid N$. Furthermore, if the largest power of two dividing $N$ is 2, then two may be split but otherwise 2 must also be ramified.

- Bourdon, Clark, 2019.
But wait! There’s more!

**Theorem (C., 2019)**

Let $F$ be a number field of degree $2p$. Let $E/F$ be a CM elliptic curve. Then $E(F)[tors]$ is isomorphic to one of the groups arising over quadratic fields or to one of the following groups:

<table>
<thead>
<tr>
<th>degree</th>
<th>group</th>
</tr>
</thead>
<tbody>
<tr>
<td>22</td>
<td></td>
</tr>
</tbody>
</table>
Theorem (C., 2019)

Let $F$ be a number field of degree $2p$. Let $E/F$ be a CM elliptic curve. Then $E(F)[\text{tors}]$ is isomorphic to one of the groups arising over quadratic fields or to one of the following groups:

<table>
<thead>
<tr>
<th>degree</th>
<th>group</th>
</tr>
</thead>
<tbody>
<tr>
<td>22</td>
<td>$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/46\mathbb{Z}$</td>
</tr>
<tr>
<td>26</td>
<td>$\mathbb{Z}/m\mathbb{Z}$</td>
</tr>
</tbody>
</table>

$m = 21, 53, 79, 106$
Theorem (C., 2019)

Let $F$ be a number field of degree $2p$. Let $E/F$ be a CM elliptic curve. Then $E(F)[\text{tors}]$ is isomorphic to one of the groups arising over quadratic fields or to one of the following groups:

<table>
<thead>
<tr>
<th>degree</th>
<th>group</th>
</tr>
</thead>
<tbody>
<tr>
<td>22</td>
<td>$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/46\mathbb{Z}$</td>
</tr>
<tr>
<td>26</td>
<td>$\mathbb{Z}/m\mathbb{Z}$</td>
</tr>
<tr>
<td></td>
<td>$m = 21, 53, 79, 106$</td>
</tr>
<tr>
<td>34</td>
<td>$\mathbb{Z}/103\mathbb{Z}$</td>
</tr>
</tbody>
</table>
Theorem (C., 2019)

Let $F$ be a number field of degree $2p$. Let $E/F$ be a CM elliptic curve. Then $E(F)[\text{tors}]$ is isomorphic to one of the groups arising over quadratic fields or to one of the following groups:

<table>
<thead>
<tr>
<th>degree</th>
<th>group</th>
</tr>
</thead>
<tbody>
<tr>
<td>22</td>
<td>$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/46\mathbb{Z}$</td>
</tr>
<tr>
<td>26</td>
<td>$\mathbb{Z}/m\mathbb{Z}$</td>
</tr>
<tr>
<td></td>
<td>$m = 21, 53, 79, 106$</td>
</tr>
<tr>
<td>34</td>
<td>$\mathbb{Z}/103\mathbb{Z}$</td>
</tr>
<tr>
<td>38</td>
<td>NONE!</td>
</tr>
</tbody>
</table>
Theorem (C.,2019)

Let $F$ be a number field of degree $2p$ for $p > 3$ prime and $E/F$ be a CM elliptic curve. If $E(F)[\text{tors}]$ is new and $j(E) \neq 0$ or 1728, then

$$E(F)[\text{tors}] \cong \begin{cases} \mathbb{Z}/m\mathbb{Z} & m = 5, 8, 12, \text{ or } 2p + 1, \\ \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2m\mathbb{Z} & m = 2p + 1, \end{cases}$$

where $2p + 1$ is a prime greater than 3.
Theorem (C.,2019)

Let \( F \) be a number field of degree \( 2p \) for \( p > 3 \) prime and \( E/F \) be a CM elliptic curve. If \( E(F)[\text{tors}] \) is new and \( j(E) = 1728 \), then

\[
E(F)[\text{tors}] \cong \begin{cases} 
\mathbb{Z}/m\mathbb{Z} & m = 4p + 1, \\
\mathbb{Z}/2m\mathbb{Z} & m = 4p + 1, 
\end{cases}
\]

where \( 4p + 1 \) is a prime greater than \( 3 \).
Theorem (C., 2019)

Let $F$ be a number field of degree $2p$ for $p > 3$ prime and $E/F$ be a CM elliptic curve. If $E(F)[\text{tors}]$ is new, $j(E) = 0$, and

- $p \neq 7$, then

$$E(F)[\text{tors}] \cong \begin{cases} \mathbb{Z}/m\mathbb{Z} & m = 6p + 1, \\ \mathbb{Z}/m^2\mathbb{Z} & m = 7, \end{cases}$$

- $p = 7$, then

$$E(F)[\text{tors}] \cong \begin{cases} \mathbb{Z}/m\mathbb{Z} & m = 6p + 1, \\ \mathbb{Z}/m^2\mathbb{Z} & m = 7, \end{cases}$$

where $6p + 1$ is a prime greater than 3.
Thanks for listening!