Descent on Elliptic Curves

an honours seminar by

Martin Leslie

Supervisor: Dr Victor Scharaschkin
We call a positive integer $n$ a *congruent number* if there exists a right angled triangle with sides of rational length and area $n$. 

### Congruent numbers

We call a positive integer $n$ a *congruent number* if there exists a right angled triangle with sides of rational length and area $n$. 

### Congruent numbers
Congruent numbers

- We call a positive integer \( n \) a *congruent number* if there exists a right angled triangle with sides of rational length and area \( n \).
- For example the 3-4-5 triangle has area 6 so 6 is a congruent number. What about 5?
We call a positive integer $n$ a **congruent number** if there exists a right angled triangle with sides of rational length and area $n$.

For example the 3-4-5 triangle has area 6 so 6 is a congruent number. What about 5?

We require $a, b, c \in \mathbb{Q}$ such that $a^2 + b^2 = c^2$ and $n = ab/2$. Make the change of variables $x = (c/2)^2$ and $y = (b^2 - a^2)c/8$. We can easily check that

$$y^2 = x^3 - n^2x.$$
We call a positive integer $n$ a *congruent number* if there exists a right angled triangle with sides of rational length and area $n$.

For example the 3-4-5 triangle has area 6 so 6 is a congruent number. What about 5?

We require $a, b, c \in \mathbb{Q}$ such that $a^2 + b^2 = c^2$ and $n = ab/2$. Make the change of variables $x = (c/2)^2$ and $y = (b^2 - a^2)c/8$. We can easily check that

$$y^2 = x^3 - n^2 x.$$ 

So we have converted our problem into finding rational points on a curve – as we will see this is actually an elliptic curve.
Elliptic Curves

An elliptic curve is the set of points on a curve
\[ y^2 = x^3 + ax + b \]
together with a ‘point at infinity’, \( O \).
Elliptic Curves

- An elliptic curve is the set of points on a curve $y^2 = x^3 + ax + b$ together with a ‘point at infinity’, $O$.
- We also require the curve to be non-singular – to have no cusps or self intersections. This is equivalent to requiring that $x^3 + ax + b$ has no repeated roots.
The Group Law

- Given two points on an elliptic curve draw the line from $P$ to $Q$ until you hit the curve again.
The Group Law

Given two points on an elliptic curve draw the line from \( P \) to \( Q \) until you hit the curve again.

Next draw a line from the point at infinity to this point. The point \( P + Q \) is where this line intersects the elliptic curve again.
Under this definition of the group law the (possibly complex) points on the elliptic curve form an abelian group (with identity $\mathcal{O}$) that we will denote $E$. 
Under this definition of the group law the (possibly complex) points on the elliptic curve form an abelian group (with identity $\mathcal{O}$) that we will denote $E$.

There is a subgroup made up of the points on the elliptic curve that have rational coordinates, denoted $E(\mathbb{Q})$. 
Under this definition of the group law the (possibly complex) points on the elliptic curve form an abelian group (with identity $\mathcal{O}$) that we will denote $E$.

There is a subgroup made up of the points on the elliptic curve that have rational coordinates, denoted $E(\mathbb{Q})$.

As we are doing number theory we are interested in finding this group.
Why We Study Elliptic Curves

Applications:
- Elliptic curve cryptography.
- Elliptic curve integer factorisation.
- Proving Fermat’s Last Theorem.
Why We Study Elliptic Curves

Applications:
- Elliptic curve cryptography.
- Elliptic curve integer factorisation.
- Proving Fermat’s Last Theorem.

Elliptic curves are projective curves of genus one with a specified basepoint. Curves of genus zero are conics and are well understood – if they have one rational point then they have infinitely many.
Why We Study Elliptic Curves

Applications:
- Elliptic curve cryptography.
- Elliptic curve integer factorisation.
- Proving Fermat’s Last Theorem.

Elliptic curves are projective curves of genus one with a specified basepoint. Curves of genus zero are conics and are well understood – if they have one rational point then they have infinitely many.

Curves of genus greater than one have only finitely many rational points by a deep theorem of Falting. Thus elliptic curves are an interesting boundary case that have provided much of the motivation for modern algebraic geometry and arithmetic geometry.
The Mordell–Weil Theorem

We present our major theorem.

**Theorem** (Mordell 1922). Let $E$ be an elliptic curve defined over $\mathbb{Q}$. Then $E(\mathbb{Q})$ is finitely generated.
The Mordell–Weil Theorem

We present our major theorem.

**Theorem** (Mordell 1922). Let $E$ be an elliptic curve defined over $\mathbb{Q}$. Then $E(\mathbb{Q})$ is finitely generated.

By the fundamental theorem of finitely generated abelian groups this means that

$$E(\mathbb{Q}) \cong E_{\text{tors}}(\mathbb{Q}) \oplus \mathbb{Z}^r.$$
Finding the rank

It is fairly easy to find the points of finite order, $E_{\text{tors}}(\mathbb{Q})$, but there is no effective method to find $r$, the rank.
Finding the rank

- It is fairly easy to find the points of finite order, $E_{\text{tors}}(\mathbb{Q})$, but there is no effective method to find $r$, the rank.

- Since we are looking for rational points you might think we can just search for them. However relatively simple curves can have very complicated points.
Finding the rank

- It is fairly easy to find the points of finite order, $E_{\text{tors}}(\mathbb{Q})$, but there is no effective method to find $r$, the rank.
- Since we are looking for rational points you might think we can just search for them. However relatively simple curves can have very complicated points.
- For example the curve $y^2 = x^3 + 877x$ has rank one and the $x$–coordinate of a generator is given by

$$
\left( \frac{612776083187947368101}{7884153586063900210} \right)^2.
$$
The Congruent number problem

We have the following solution (if we can find ranks effectively) to our congruent number problem

**Theorem.** A positive integer $n$ is a congruent number if and only if the elliptic curve $y^2 = x^3 - n^2 x$ has rank greater than zero.
The Congruent number problem

- We have the following solution (if we can find ranks effectively) to our congruent number problem

**Theorem.** A positive integer $n$ is a congruent number if and only if the elliptic curve $y^2 = x^3 - n^2 x$ has rank greater than zero.

- The congruent numbers less than 100 are

5, 6, 7, 13, 14, 15, 20, 21, 22, 23, 24, 28, 29, 30, 31, 34, 37, 38, 39, 41, 45, 46, 47, 52, 53, 54, 55, 56, 60, 61, 62, 63, 65, 69, 70, 71, 77, 78, 79, 80, 84, 85, 86, 87, 88, 92, 93, 94, 95, 96
The Congruent number problem

- We have the following solution (if we can find ranks effectively) to our congruent number problem

**Theorem.** A positive integer $n$ is a congruent number if and only if the elliptic curve $y^2 = x^3 - n^2x$ has rank greater than zero.

- The congruent numbers less than 100 are

5, 6, 7, 13, 14, 15, 20, 21, 22, 23, 24, 28, 29, 30, 31, 34, 37, 38, 39, 41, 45, 46, 47, 52, 53, 54, 55, 56, 60, 61, 62, 63, 65, 69, 70, 71, 77, 78, 79, 80, 84, 85, 86, 87, 88, 92, 93, 94, 95, 96

- Tunnel (1983) gave an effective procedure for determining if $n$ is a congruent number assuming the Birch–Swinnerton-Dyer conjecture.
It is conjectured that there are curves of arbitrarily high rank (although most elliptic curves are of very small rank).
Rank

- It is conjectured that there are curves of arbitrarily high rank (although most elliptic curves are of very small rank).

- As of 2006 the curve of highest known rank is of rank at least 28. It is given by

\[ y^2 + xy + y = x^3 - x^2 - 2006776241557552658503^{3208209338542750930230312178956502}x + 34481611795030556467032985690390720374855944359319180^{361266008296291939448732243429}. \]
The Weak Mordell–Weil Theorem

In our proof of the Mordell–Weil Theorem we use the following

**Theorem.** Let $E$ be an elliptic curve defined over $\mathbb{Q}$. Then $E(\mathbb{Q})/2E(\mathbb{Q})$ is finite.
The Weak Mordell–Weil Theorem

In our proof of the Mordell–Weil Theorem we use the following

**Theorem.** Let $E$ be an elliptic curve defined over $\mathbb{Q}$. Then $E(\mathbb{Q})/2E(\mathbb{Q})$ is finite.

In fact it can be shown that if we can find generators for $E(\mathbb{Q})/2E(\mathbb{Q})$ then we have an effective procedure to find generators for $E(\mathbb{Q})$. 
The Weak Mordell–Weil Theorem

In our proof of the Mordell–Weil Theorem we use the following

**Theorem.** Let $E$ be an elliptic curve defined over $\mathbb{Q}$. Then $E(\mathbb{Q})/2E(\mathbb{Q})$ is finite.

In fact it can be shown that if we can find generators for $E(\mathbb{Q})/2E(\mathbb{Q})$ then we have an effective procedure to find generators for $E(\mathbb{Q})$.

Thus from now on we are only concerned with finding $E(\mathbb{Q})/2E(\mathbb{Q})$. 
$p$–adic numbers

When looking for integer solutions to equations (‘Diophantine equations’) it is often useful to consider the equation modulo a prime $p$. The $p$–adic numbers generalise this idea by considering the equation modulo $p^n$ for all $n$ at once.
\( p \)-adic numbers

- When looking for integer solutions to equations (‘Diophantine equations’) it is often useful to consider the equation modulo a prime \( p \). The \( p \)-adic numbers generalise this idea by considering the equation modulo \( p^n \) for all \( n \) at once.

- Define the \( p \)-adic integers, \( \mathbb{Z}_p \), to be the set of sequences

\[
x = (\ldots, x_n, \ldots, x_2, x_1)
\]

where \( x_n \equiv x_{n-1} \pmod{p^{n-1}} \).
$p$–adic numbers

When looking for integer solutions to equations (‘Diophantine equations’) it is often useful to consider the equation modulo a prime $p$. The $p$–adic numbers generalise this idea by considering the equation modulo $p^n$ for all $n$ at once.

Define the $p$–adic integers, $\mathbb{Z}_p$, to be the set of sequences

$$x = (\ldots, x_n, \ldots, x_2, x_1)$$

where $x_n \equiv x_{n-1} \pmod{p^{n-1}}$.

Thus $(\ldots, 23, 5, 2)$ is in $\mathbb{Z}_3$ but $(\ldots, 22, 5, 2)$ isn’t since $22 \not\equiv 5 \pmod{9}$.
Then let the $p$–adic numbers, $\mathbb{Q}_p$, be the field of fractions of the $p$–adic integers (exactly how the rational numbers are constructed from the integers).
Then let the $p$–adic numbers, $\mathbb{Q}_p$, be the field of fractions of the $p$–adic integers (exactly how the rational numbers are constructed from the integers).

The $p$–adic numbers contain $\mathbb{Q}$ and are a field of characteristic zero.
Then let the $p$–adic numbers, $\mathbb{Q}_p$, be the field of fractions of the $p$–adic integers (exactly how the rational numbers are constructed from the integers).

The $p$–adic numbers contain $\mathbb{Q}$ and are a field of characteristic zero.

It can be shown that the only possible completions of the rationals are the $p$–adic numbers for each $p$ and the reals. For this reason we denote $\mathbb{R}$ by $\mathbb{Q}_\infty$. 

Descent on Elliptic Curves – p. 13/2
The Local-Global principle

A quadratic polynomial in two variables with rational coefficients has a rational solution if and only if it has a solution in $\mathbb{Q}_p$ for every prime $p \leq \infty$. 
The Local-Global principle

- A quadratic polynomial in two variables with rational coefficients has a rational solution if and only if it has a solution in $\mathbb{Q}_p$ for every prime $p \leq \infty$.

- Thus to find ‘global’ solutions over $\mathbb{Q}$ only need to consider the equation ‘locally’ at each prime $p$. 
The Local-Global principle

- A quadratic polynomial in two variables with rational coefficients has a rational solution if and only if it has a solution in $\mathbb{Q}_p$ for every prime $p \leq \infty$.

- Thus to find ‘global’ solutions over $\mathbb{Q}$ only need to consider the equation ‘locally’ at each prime $p$.

- However a similar theorem doesn’t hold for cubic polynomials so local information doesn’t give the full picture for elliptic curves.
The Local-Global principle

- A quadratic polynomial in two variables with rational coefficients has a rational solution if and only if it has a solution in $\mathbb{Q}_p$ for every prime $p \leq \infty$.

- Thus to find ‘global’ solutions over $\mathbb{Q}$ only need to consider the equation ‘locally’ at each prime $p$.

- However a similar theorem doesn’t hold for cubic polynomials so local information doesn’t give the full picture for elliptic curves.

- We are still interested in local methods but now we need to keep track of when they fail.
The algebraic closure of $\mathbb{Q}$, denoted $\overline{\mathbb{Q}}$, is the set of all solutions of polynomials with rational coefficients. The Galois group $G = \text{Gal}(\overline{\mathbb{Q}}, \mathbb{Q})$ is the set of isomorphisms from $\overline{\mathbb{Q}}$ to $\overline{\mathbb{Q}}$ that fix $\mathbb{Q}$. 
Some Galois Cohomology

The algebraic closure of \( \mathbb{Q} \), denoted \( \overline{\mathbb{Q}} \), is the set of all solutions of polynomials with rational coefficients. The Galois group \( G = \text{Gal}(\overline{\mathbb{Q}}, \mathbb{Q}) \) is the set of isomorphisms from \( \overline{\mathbb{Q}} \) to \( \overline{\mathbb{Q}} \) that fix \( \mathbb{Q} \).

Define a \( G \)-module to be an abelian group \( M \) with an action of \( G \) (\( \sigma \in G \) acts on \( m \in M \) by sending \( m \mapsto m^\sigma \)) such that

- \( m^1 = m \)
- \( (m + m')^\sigma = m^\sigma + m'^\sigma \)
- \( (m^\sigma)^\tau = m^{\sigma \tau} \).
Some Galois Cohomology

- The algebraic closure of $\mathbb{Q}$, denoted $\overline{\mathbb{Q}}$, is the set of all solutions of polynomials with rational coefficients. The Galois group $G = \text{Gal}(\overline{\mathbb{Q}}, \mathbb{Q})$ is the set of isomorphisms from $\overline{\mathbb{Q}}$ to $\overline{\mathbb{Q}}$ that fix $\mathbb{Q}$.

- Define a $G$–module to be an abelian group $M$ with an action of $G$ ($\sigma \in G$ acts on $m \in M$ by sending $m \mapsto m^\sigma$) such that
  - $m^1 = m$
  - $(m + m')^\sigma = m^\sigma + m'^\sigma$
  - $(m^\sigma)^\tau = m^{\sigma\tau}$.

- Examples of $G$–modules are $\overline{\mathbb{Q}}$ and $E$. 
We define two cohomology groups so that later we can do some algebraic trickery. For a $G$–module $M$ define:
We define two cohomology groups so that later we can do some algebraic trickery. For a $G$–module $M$ define:

$$H^0(G, M) = M^G = \{ m \in M \mid m^\sigma = m \text{ for all } \sigma \in G \}.$$
We define two cohomology groups so that later we can do some algebraic trickery. For a $G$–module $M$ define:

1. $H^0(G, M) = M^G = \{ m \in M \mid m^\sigma = m \text{ for all } \sigma \in G \}$.

2. $H^1(G, M) = Z^1(G, M)/B^1(G, M)$ where $Z^1(G, M)$ is the group of maps $\xi: G \to M$ satisfying the cocycle condition

$$\xi(\sigma \tau) = \xi(\sigma)^\tau + \xi(\tau)$$

and $B^1(G, M)$, is the group of maps $\xi: G \to M$ where there exists an $m \in M$ such that, for all $\sigma \in G$

$$\xi(\sigma) = m^\sigma - m.$$

$H^0$ and $H^1$
A commutative diagram is a diagram such that it doesn’t matter what path we take. For example the next diagram is commutative if and only if $g \circ f = k \circ h$.

\[
\begin{array}{ccc}
A & \rightarrow & B \\
\downarrow h & & \downarrow g \\
C & \rightarrow & D \\
\end{array}
\]
Diagrams and Exact Sequences

A commutative diagram is a diagram such that it doesn’t matter what path we take. For example the next diagram is commutative if and only if $g \circ f = k \circ h$.

\[
\begin{array}{ccc}
A & \xrightarrow{f} & B \\
| & \downarrow{h} & | \\
C & \xrightarrow{k} & D
\end{array}
\]

An exact sequence is a set of $G$–modules with homomorphisms between them

\[
\cdots \longrightarrow A_{i-1} \xrightarrow{f_{j-1}} A_i \xrightarrow{f_j} A_{i+1} \longrightarrow \cdots
\]

such that $\text{Im } f_{j-1} = \text{Ker } f_j$ for all $j$. 
A short exact sequence is an exact sequence of the form

\[ 0 \rightarrow A \xrightarrow{f} B \xrightarrow{g} C \rightarrow 0 . \]

Note that in a short exact sequence \( f \) is injective, \( g \) is surjective and \( \text{Im} \ f = \text{Ker} \ g \).
A short exact sequence is an exact sequence of the form

\[ 0 \longrightarrow A \stackrel{f}{\longrightarrow} B \stackrel{g}{\longrightarrow} C \longrightarrow 0. \]

Note that in a short exact sequence \( f \) is injective, \( g \) is surjective and \( \text{Im} f = \text{Ker} g \).

Short exact sequences give us lots of information. We can see that every element of \( B \) either is an element of an isomorphic copy of \( A \) or maps nontrivially into \( C \).
For an abelian group $A$ we denote the 2–torsion by $A[2] = \{a \in A \mid 2a = 0\}$. Set $G_p = \text{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)$. Using Galois cohomology and a generalisation of Hilbert Theorem 90 we can find a commutative diagram with exact rows (all products are over $p = 2, 3, 5, \ldots, \infty$).

\[
\begin{array}{ccccccccc}
0 & \rightarrow & E(\mathbb{Q})/2E(\mathbb{Q}) & \rightarrow & H^1(G, E[2]) & \rightarrow & H^1(G, E)[2] & \rightarrow & 0 \\
& & \downarrow & & \downarrow & & \downarrow \lambda & & \downarrow \theta \\
0 & \rightarrow & \prod E(\mathbb{Q}_p)/2E(\mathbb{Q}_p) & \rightarrow & \prod H^1(G_p, E[2]) & \rightarrow & \prod H^1(G_p, E)[2] & \rightarrow & 0
\end{array}
\]
2-Descent

For an abelian group $A$ we denote the 2–torsion by $A[2] = \{a \in A \mid 2a = 0\}$. Set $G_p = \text{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)$. Using Galois cohomology and a generalisation of Hilbert Theorem 90 we can find a commutative diagram with exact rows (all products are over $p = 2, 3, 5, \ldots, \infty$).

$$
\begin{array}{cccccc}
0 & \rightarrow & E(\mathbb{Q})/2E(\mathbb{Q}) & \rightarrow & H^1(G, E[2]) & \rightarrow & H^1(G, E)[2] & \rightarrow & 0 \\
\downarrow & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \rightarrow & \prod E(\mathbb{Q}_p)/2E(\mathbb{Q}_p) & \rightarrow & \prod H^1(G_p, E[2]) & \rightarrow & \prod H^1(G_p, E)[2] & \rightarrow & 0
\end{array}
$$

We are interested in finding $E(\mathbb{Q})/2E(\mathbb{Q})$ but to do this we use local information – Hensel’s lemma tells us that calculating the bottom row can be reduced to a finite amount of computation.
Define the *Tate–Shafarevich group* \( \text{III}[2] = \ker \lambda \) and the *Selmer group* \( S^{(2)} = \ker \theta \).
Define the *Tate–Shafarevich group* $\Sha[2] = \ker \lambda$ and the *Selmer group* $S^{(2)} = \ker \theta$.

From previous diagram we can find the *descent sequence*

$$
0 \longrightarrow E(\mathbb{Q})/2E(\mathbb{Q}) \longrightarrow S^{(2)} \longrightarrow \Sha[2] \longrightarrow 0.
$$
Define the *Tate–Shafarevich group* $\Sha[2] = \ker \lambda$ and the *Selmer group* $S^{(2)} = \ker \theta$.

From previous diagram we can find the *descent sequence*

\[
0 \longrightarrow E(\mathbb{Q})/2E(\mathbb{Q}) \longrightarrow S^{(2)} \longrightarrow \Sha[2] \longrightarrow 0.
\]

The group $S^{(2)}$ is finite and computable (this means that $E(\mathbb{Q})/2E(\mathbb{Q})$ is finite: the weak Mordell–Weil theorem). Figuring out whether a point in $S^{(2)}$ comes from $E(\mathbb{Q})/2E(\mathbb{Q})$ or maps nontrivially into $\Sha[2]$ is hard.
Homogenous spaces

We have an exact correspondence between elements of $H^1(G, E)$ and equivalence classes of curves that we call ‘homogenous spaces’.
Homogenous spaces

- We have an exact correspondence between elements of $H^1(G, E)$ and equivalence classes of curves that we call ‘homogenous spaces’.

- We can think of $\mathbb{III}$ as the group of homogenous spaces which have a $\mathbb{Q}_p$–rational point for every prime $p$. If a curve has $\mathbb{Q}_p$–rational points for every $p$ but no $\mathbb{Q}$–rational point then it is a non-trivial element of $\mathbb{III}$. 
Homogenous spaces

- We have an exact correspondence between elements of $H^1(G, E)$ and equivalence classes of curves that we call ‘homogenous spaces’.

- We can think of $\mathbb{III}$ as the group of homogenous spaces which have a $\mathbb{Q}_p$–rational point for every prime $p$. If a curve has $\mathbb{Q}_p$–rational points for every $p$ but no $\mathbb{Q}$–rational point then it is a non-trivial element of $\mathbb{III}$.

- Thus $\mathbb{III}$ measures the failure of the local–global principle.
Calculating the rank

If $\mathcal{M}[2] = 0$ then $\frac{E(\mathbb{Q})}{2E(\mathbb{Q})} \cong S^{(2)}$ is able to be calculated. If $\mathcal{M}[2]$ is nontrivial then we only get a bound on the rank.
Calculating the rank

- If $\exists[2] = 0$ then $E(\mathbb{Q})/2E(\mathbb{Q}) \cong S^{(2)}$ is able to be calculated. If $\exists[2]$ is nontrivial then we only get a bound on the rank.

- Programs like mwrank can calculate ranks quite well practically but there is no algorithm that always works.
Calculating the rank

- If $\mathcal{W}[2] = 0$ then $E(\mathbb{Q})/2E(\mathbb{Q}) \cong S^{(2)}$ is able to be calculated. If $\mathcal{W}[2]$ is nontrivial then we only get a bound on the rank.

- Programs like mwrank can calculate ranks quite well practically but there is no algorithm that always works.

- Going back to our motivating problem consider the question of the congruent number problem for $n = 5$. By running mwrank we can see that the curve $y^2 = x^3 - 25x$ has rank one. In fact with a little more work we can find a point $(1681/144, 62279/1728)$ on our curve. This corresponds to a triangle $(a, b, c) = (3/2, 20/3, 41/6)$. 
Future Work

What I’m doing: looking at an idea of Flynn. He carries out descent without using homogenous spaces.
Future Work

- What I’m doing: looking at an idea of Flynn. He carries out descent without using homogenous spaces.
- What other people are doing: Higher descent – 3-descent, second 2-descent, 5 descent,...
Future Work

• What I’m doing: looking at an idea of Flynn. He carries out descent without using homogenous spaces.

• What other people are doing: Higher descent – 3-descent, second 2-descent, 5 descent,...

• Trying to win a million dollars: The Clay Institute is offering one million dollars for a proof of the Birch–Swinnerton-Dyer conjecture. Associated to an elliptic curve \( E \) is an \( L \)-series \( L_E(s) \). The BSD conjecture is that

\[
L_E(s) \text{ has a zero at } s = 1 \text{ of order equal to the rank of } E(\mathbb{Q}); \text{ and}
\]

\[
\lim_{s \to 1} \frac{L_E(s)}{(s - 1)^r} = \frac{\Omega_R|\Sha| \prod\Delta c_p}{|E_{tors}(\mathbb{Q})|^2}.
\]
The End

Any questions?