1. What is a curve?

We started by considering the idea of a curve. This is just the set of points in the plane which satisfy a polynomial equation. For example, a circle, a line, a parabola, an ellipse... these are all curves.

2. Rational points on curves

A rational point on a curve \( f(x, y) = 0 \) (where \( f \) is a polynomial, with rational coefficients, say) is a point \((x_0, y_0)\) such that \( f(x_0, y_0) = 0 \) and both \( x_0 \) and \( y_0 \) are in the set \( \mathbb{Q} \) of rational numbers.

We proved that if you have two lines with rational slopes, say \( \ell_1 \) and \( \ell_2 \), and if \( \ell_i \) passes through a rational point \( p_i \), then the intersection point \( q \) of \( \ell_1 \) and \( \ell_2 \) is rational. This was just a geometry problem which we solved by using the slopes of the lines (rational numbers \( m_1 \) and \( m_2 \), say) to compute the intersection point \( q \) in terms of \( p_1, p_2, m_1, m_2 \) explicitly.

Next, we used this theorem to write down all the rational points on the circle \( x^2 + y^2 = 1 \).

It turns out that we can pick a line \( \ell \) with rational slope, for example \( x = 1 \), and a rational point \( q_{\infty} \), such as \((-1,0)\), and then proceed as follows. For any point \( p_t = (1, t) \) on \( \ell \), where \( t \) is rational, consider the line \( \overline{q_{\infty}p_t} \). This will intersect the circle \( x^2 + y^2 = 1 \) at a unique rational point \( q_t \). On the other hand, for any rational point \( q \) on the circle, we form the line \( \overline{q_{\infty}q} \) and consider the point \( p \) where this line meets \( \ell \). This point will have to be rational. So there is a one-to-one correspondence between rational points on \( \ell \) and rational points on the circle (except for the fixed point \( q_{\infty} \) we started with). If we pretend that “\( \infty \)” is a rational number we can consider the “point” \( p_{\infty} \) infinitely far up the line \( \ell \). Then the “line” \( \overline{p_{\infty}q_{\infty}} \) only meets \( \ell \) infinitely far away: they are parallel. This parallel line passes through the circle at the unique point \( q_{\infty} \), where it is tangent to the circle. So if we use an “expanded” notion of rational numbers \( \mathbb{Q} \cup \{\infty\} \) we can parametrize all the rational points on \( x^2 + y^2 = 1 \) by the rational points \((1, t)\) on \( \ell \) for \( t \in \mathbb{Q} \cup \{\infty\} \).

For homework, I asked you to think about the rational points on \( x^2 + y^2 = 3 \). By clearing denominators, these were the same as sets \((A, B, C)\) of integers satisfying \( A^2 + B^2 = 3C^2 \). Taking this equation \( \pmod{3} \), we saw that there were \emph{no} such sets \((A, B, C)\): we know that \( 0^2 = 0, 1^2 = 1, 2^2 = -1 \) when we think about the integers \( \pmod{3} \). So no combination of two squares can give \( 0 \) \( \pmod{3} \) unless both \( A \) and \( B \) are already \( 0 \) \( \pmod{3} \). But this means that if \( A^2 + B^2 = 3C^2 \) then we can write \( A = 3a, B = 3b \). So \( 9a^2 + 9b^2 = 3C^2 \). Or \( 3a^2 + 3b^2 = C^2 \). The lefthand side is divisible by 3, so \( C^2 \) and hence \( C \) must therefore be divisible by 3. So write \( C = 3c \). Then \( 9a^2 + 9b^2 = 27c^2 \), which means \( a^2 + b^2 = 3c^2 \). Hence we started with a
solution
\[ (A, B, C) \]
and got a new solution
\[ (a, b, c) = \left( \frac{A}{3}, \frac{B}{3}, \frac{C}{3} \right). \]
But now we can do the same thing all over again! So we must get an infinite sequence of solutions which always get smaller and smaller. And of course this is impossible since there is a smallest positive integer, namely 1.

This contradiction proves that there are no rational points on the curve \( x^2 + y^2 = 3 \). This method is called Fermat’s method of infinite descent, since it works by “descending” from a bigger solution to a smaller one, and continuing infinitely in this manner. This is an idea we will return to later in the course.

3. What is an elliptic curve?

An elliptic curve is just a cubic curve
\[ y^2 = f(x) \]
where \( f(x) \) is a cubic polynomial with distinct roots. When you graph one of these, it looks smooth, with no cusps or self-intersection points. It can have either one or two components depending on what \( f \) is. We will discuss the possibilities in more detail.

Note: an ellipse is not an elliptic curve! Later in the course, hopefully, we will see what elliptic curves have to do with ellipses.

4. Why might we care about elliptic curves?

A congruent number is a number \( n \) which is the area of a Pythagorean triangle (right triangle) with rational sides. Question: Which \( n \) are congruent numbers?

Well, such an \( n \) satisfies an equation
\[ \frac{1}{2}ab = n \]
where
\[ a^2 + b^2 = c^2 \]
for some rational numbers \( a, b, c \). However, we do not have one defining polynomial in two variables which determines these conditions. Can we make a clever change of variables?

Observe that \( \left( \frac{c}{2} \right)^2 \) is the square of a rational number. This is obvious! However, this is the same as \( \frac{a^2 + b^2}{4} \). Now subtract \( n \). We get
\[ \left( \frac{c}{2} \right)^2 - n = \frac{a^2 + b^2}{4} - n = \frac{a^2 + b^2}{4} - \frac{ab}{2} = \frac{a^2 + b^2 - 2ab}{4} = \frac{(a - b)^2}{4} = \left( \frac{a - b}{2} \right)^2. \]
Similarly,
\[ \left( \frac{c}{2} \right)^2 + n = \left( \frac{a + b}{2} \right)^2. \]
So
\[
\left( \frac{c}{2} \right)^2, \left( \frac{c}{2} \right)^2 + n, \left( \frac{c}{2} \right)^2 - n
\]
are all squares of rational numbers. For shorthand write \( x = \left( \frac{c}{2} \right)^2 \). Then \( x, x + n, x - n \) are all squares. That means that
\[
x(x + n)(x - n) = x^3 - n^2 x
\]
is also a square. In particular, it is \( y^2 \) where \( y = \frac{c}{2}, \frac{a+b}{2}, \frac{a-b}{2} \). So with this change of variables, our congruent number \( n \) corresponds to a rational point \((x, y)\) on the elliptic curve
\[
y^2 = x^3 - n^2 x.
\]
Try graphing this curve in \( \mathbb{R}^2 \), the Euclidean plane, for various values of \( n \). (A computer or calculator might help.)

Moreover we know that \( y \neq 0 \) since if \( y = 0 \) then \( a = b \) (since \( a, b, c \) are positive rational numbers). But this implies that \( n = \frac{1}{2}a^2 \), or \( a^2 = 2n \). This means that \( c^2 = a^2 + a^2 = 4n \). So \( \frac{c^2}{n^2} = 2 \). But since \( a \) and \( c \) are rational, so must \( c/a \) be! And this is impossible since \( \sqrt{2} \) is irrational, as we know.

So we have a map
\[
\text{congruent number } n \mapsto \text{rational point } (x, y) \text{ on } y^2 = x^3 - n^2 x \text{ with } y \neq 0.
\]

On the other hand, if we have a rational point on this curve with \( y \neq 0 \) we can define
\[
a = \frac{x^2 - n^2}{y} \\
b = \frac{2nx}{y} \\
c = \frac{x^2 + n^2}{y}
\]
Then we can check that \( a, b, c \) are rational numbers with \( a^2 + b^2 = c^2 \) and indeed \( \frac{1}{2}ab = n \).

Try this as an exercise! So in fact our map above is a bijection: \( n \) is a congruent number if and only if there is a rational point \((x, y)\) with \( y \neq 0 \) on the elliptic curve \( y^2 = x^3 - n^2 x \).

This example shows why elliptic curves are interesting, and in particular the rational points on them.