Worksheet 22

Recall that an elliptic curve is an equation of the form $y^2 = x^3 + ax + b$ with special conditions on a and b so that the curve is nice. One reason elliptic curves are special is that there is a notion of *addition* of rational points. Here's how the proceedure goes: Start with two distinct points P and Q on your elliptic curve E. The line through P and Q generally intersects E in a third point, called R. We define $P + Q = -R$, where $-R$ is defined to be the reflection of R around the x-axis.

1. Let E be the elliptic curve $y^2 = x^3 + 17$, and let $P = (-2, 3)$ and $Q = (2, 5)$.
   (a) Sketch a picture of E along with the points P, Q, R and $P + Q$.
   (b) On your graph, label $-P$. How would you try and define $P + -P$? *(How do you want addition to work?)*
   (c) Find as many different rational points on E as your heart desires!

2. The procedure above assumed that P and Q were distinct points. However, we should still have a way of adding a point to itself, otherwise we don't have a very good definition of addition!
   (a) Try and come up with a way of defining $P + P$, which we will call $2P$. *(What should it mean for a line to intersect twice at P?)*
   (b) Let E be the elliptic curve $y^2 = x^3 - 3x + 7$ and let $P = (2, 3)$. Compute the coordinates of $2P$.
   (c) Let E be the elliptic curve $y^2 = x^3 - x$ and let $P = (-1, 0)$. Sketch a picture of E along with the point P. How would you try and define $2P$ in this case?
   (d) Let E be the elliptic curve $y^3 = x^3 + 4$ and let $P = (0, 2)$. Sketch a picture of E along with the point P. How would you try and define $2P$ in this case?

   The above problems should give you a very basic idea of how addition of points on elliptic curves work. As you can see, there's many different things to consider!

3. Here's a very famous example of how elliptic curves naturally arise in number theory. A positive integer n is called a *congruent number* if there exists a right triangle whose sides are rational numbers and whose area equals n. For example, 6 is a congruent number because the right triangle with sides $(3, 4, 5)$ has area 6.
   (a) Let $C_n = \{(a, b, c) \in \mathbb{Z}^3 : a^2 + b^2 = c^2, \frac{ab}{2} = n\}$ and $E_n = \{(x, y) \in \mathbb{Q}^2 : y^3 = x^3 - n^2 x, y \neq 0\}$. Prove that the maps $(a, b, c) \mapsto (\frac{nb}{c-a}, \frac{2n^2}{c-a})$ and $(x, y) \mapsto (\frac{x^2-n^2}{y}, \frac{2nx}{y}, \frac{x^2+n^2}{y})$ define functions from C_n to E_n and E_n to C_n respectively, and show that these functions are inverses of each other. This says the problem of determining if n is a congruent number is the same as determining if a certain elliptic curve has integer points.
   (b) The point $(3, 4, 5) \in C_6$ corresponds to the point $P = (12, 36)$ on the elliptic curve $y^2 = x^3 - 36x$. Compute $2P$ and use this to find another right triangle that works for $n = 6$.