Why do we care about elliptic curves? The group law

- An abelian group is a set A together with a binary operation $+$ which is both commutative and associative. $+$ has an identity and inverses.
- An elliptic curve over a field F (without characteristic 2 or 3) is an algebraic curve of the form

$$y^2 = x^3 + ax + b.$$

  where a and b are in your field and the polynomial on the right has no multiple roots.
- We care about elliptic curves because they support an abelian group structure. This takes some explaining.
- The points on the elliptic curve are the elements of the group. We only need to explain how to add them.
- The easiest case is when P and Q are two different points on the curve. Draw a line between P and Q and let R be the third point of intersection with the curve. Now reflect R in the x-axis and this is $P + Q$.

Why do we care about elliptic curves? The group law

- There are a few cases not handled by the easy case. One thing we need for our group is an identity element 0; we just formally add this point to the curve (often called the point at infinity). We need 0 in the case above when the line through P and Q does not intersect the curve. In this case, we say $P + Q = 0$. Of course $P + 0 = P$ for all P.
- If $P = Q$ then we use the (formal) tangent line to the curve at P and again, if R is the other point of intersection then we reflect R in the x-axis and this is $P + P$. Finally, if the tangent line does not intersect the curve then $P + P = 0$.
- Amazingly this defines an abelian group for any elliptic curve over any field (avoiding fields with characteristic 2 or 3 for now); the truly hard thing to prove is that $+$ is associative. All the other abelian group properties are easy.