Elliptic curves and the group law

- An elliptic curve over a field F (without characteristic 2 or 3) is an algebraic curve of the form

$$y^2 = x^3 + bx + c.$$

  where b and c are in your field and the polynomial on the right has no multiple roots.
- The points on the elliptic curve are the elements of the group together with a formal 0 which is the identity.
- 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 $P + Q$.

Elliptic curves and the group law, cont'd

- 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 $P + P = 0$.

Example from Thursday

- An elliptic curve over a field F (without characteristic 2 or 3) is an algebraic curve of the form

$$y^2 = x^3 + bx + c.$$

  where b and c are in F and the polynomial on the right has no multiple roots.
- If $P = (x_1, y_1)$ and $Q = (x_2, y_2)$ and $x_1 \neq x_2$ then the slope of the line through PQ is

$$m = \frac{y_2 - y_1}{x_2 - x_1}.$$

  Then the line through PQ is $y = mx + a$ where $a = y_1 - mx_1$. All of these calculations are happening in F.

Example from Thursday, cont'd

- Substituting the line into the equation for the curve, we get

  $(mx+a)^2 = x^3+bx+c$ and so $x^3-mx^2+(b-2ma)x+c-a^2 = 0$.

- Two roots of the last equation are $x = x_1$ and $x = x_2$ so if we call the third root x_3 then we have

  $$x^3 - m^2x^2 + (b-2ma)x + c - a^2 = (x-x_1)(x-x_2)(x-x_3).$$

  Looking at the x^2 term we see $-m^2 = -(x_1 + x_2 + x_3)$.
- So $x_3 = m^2 - (x_1 + x_2)$ and $y_3 = mx_3 + a = m(x_3 - x_1) + y_1$.
- Finally
  $P + Q = (x_3, -y_3) = (m^2 - (x_1 + x_2), m(x_1 - x_3) - y_1)$.

Example from Thursday, cont'd

- Now if $x_1 = x_2$ then there are two cases:
- If $y_1 = -y_2$ then P and Q are reflected images of each other in the x-axis and so $P + Q = 0$.
- If $y_1 = y_2$ then $P = Q$ and we need to compute the tangent line to the curve through P. This is done formally by implicit differentiation; from the equation for the curve we get

$$2yy' = 3x^2 + b \text{ and so } y' = \frac{3x^2 + b}{2y}.$$

  One sees here why we want the characteristic of F not to be 2 or 3.
- So if $y_1 \neq 0$ then the slope of the tangent line is $m = \frac{3x_1^2+b}{2y_1}$ and the rest of the calculation is as above so

$$P + P = (x_3, -y_3) = (m^2 - 2x_1), m(x_1 - x_3) - y_1).$$

- Finally, if $y_1 = 0$ then the tangent line is vertical and we get $P + P = 0$.