

## The group law made explicit.

Let  $k$  be a field of characteristic not equal to 2. Then the equation

$$y^2 = x^3 + Ax + B$$

with  $A, B \in k$ , defines an elliptic curve if  $4A^3 + 27B^2 \neq 0$ , that is, if the roots of the cubic (in an algebraically closed field containing  $k$ ) are distinct. Let's assume that this is the case. Say  $P = (x_0, y_0)$  is a point on the curve. We have seen in lectures that  $-P = (x_0, -y_0)$ . Let's work out  $2P$ .

### The doubling formula.

To double  $P = (x_0, y_0)$  we must draw the tangent to the cubic at  $P$ . One easy case is if  $y_0 = 0$ ; then  $2P$  is the point at infinity, the identity for the group law. If however  $y_0 \neq 0$  then the gradient of the cubic at  $P$  is  $m := (3x_0^2 + A)/(2y_0)$  by standard calculus, so the tangent line through  $P$  is  $y = mx + c$  for some  $c$ , and subbing in gives

$$(mx + c)^2 = x^3 + Ax + B.$$

The three roots of this cubic will be  $x = x_0$  twice, and  $x = x_d$ , where  $2P = (x_d, y_d)$  ( $d$  for double). But the sum of the roots is minus the coefficient of  $x^2$ , and hence

$$x_d = m^2 - 2x_0 = \frac{(3x_0^2 + A)^2 - 8x_0y_0^2}{4y_0^2}$$

and because  $P$  is on the cubic we see that  $y_0^2 = x_0^3 + Ax_0 + B$  and hence

$$x_d = \frac{x_0^4 - 2Ax_0^2 - 8Bx_0 + A^2}{4(x_0^3 + Ax_0 + B)}.$$

Finding the constant  $c$  explicitly is easy but messy, and then substituting in the linear equation gives  $-y_d = mx_d + c$  (the minus sign because line intersects the cubic at  $P$ ,  $P$  and  $-2P$ ).

### Adding two distinct points.

Addition of two distinct points  $P = (x_1, y_1)$  and  $Q = (x_2, y_2)$  is just as easy. If  $x_1 = x_2$  then either  $Q = P$  (a case we have done already) or  $Q = -P$  (in which case the answer is the point at infinity). So we can assume  $x_1 \neq x_2$ . Now the line through  $P$  and  $Q$  is

$$y = mx + c$$

with  $m = (y_1 - y_2)/(x_1 - x_2)$ . Arguing as in the doubling case, we see that  $P + Q = (x_3, y_3)$  with  $-y_3 = mx_3 + c$  and

$$x_1 + x_2 + x_3 = m^2,$$

that is,

$$\begin{aligned} (x_1 - x_2)^2 x_3 &= (y_1 - y_2)^2 - (x_1 - x_2)^2 (x_1 + x_2) \\ &= -2y_1 y_2 + (x_1 + x_2)(x_1 x_2 + A) + 2B \end{aligned}$$

so

$$x_3 = \frac{-2y_1 y_2 + (x_1 + x_2)(x_1 x_2 + A) + 2B}{(x_1 - x_2)^2},$$

and substituting into the linear equation gives  $y_3$ , although the general formula is quite messy to write down (note however that if we are given values for  $A$  and  $B$  then things are a lot easier to work out explicitly).