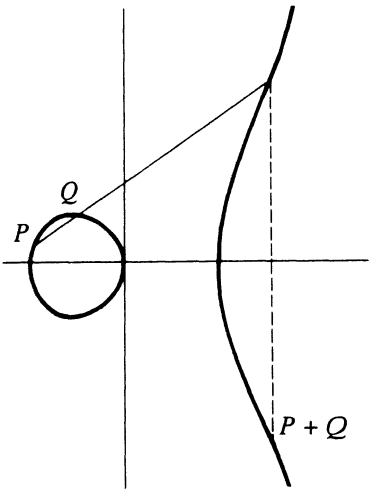
1. If P is the point at infinity O, then we define $-P$ to be O and $P+Q$ to be Q; that is, O serves as the additive identity ("zero element") of the group of points. In what follows, we shall suppose that neither P nor Q is the point at infinity.
2. The negative $-P$ is the point with the same x-coordinate but negative the y-coordinate of P, i.e., $-(x,y) = (x,-y)$. It is obvious from (1) that $(x,-y)$ is on the curve whenever (x,y) is.
3. If P and Q have different x-coordinates, then it is not hard to see that the line $\ell = \overline{PQ}$ intersects the curve in exactly one more point R (unless that line is tangent to the curve at P, in which case we take $R = P$, or at Q, in which case we take $R = Q$). Then define $P+Q$ to be $-R$, i.e., the mirror image (with respect to the x-axis) of the third point of intersection. The geometrical construction that gives $P+Q$ is illustrated in Example 1 below.
4. If $Q=-P$ (i.e., Q has the same x-coordinate but minus the y-coordinate), then we define $P+Q = O$ (the point at infinity). (This is forced on us by (2).)
5. The final possibility is $P = Q$. Then let ℓ be the tangent line to the curve at P, let R be the only other point of intersection of ℓ with the curve, and define $P+Q = -R$. (R is taken to be P if the tangent line has a "double tangency" at P, i.e., if P is a point of inflection.)

Example 1. The elliptic curve $y^2 = x^3 - x$ in the xy-plane is sketched to the right. The diagram also shows a typical case of adding points P and Q. To find $P+Q$ one draws a chord through P and Q, and takes $P+Q$ to be the point symmetric (with respect to the x-axis) to the third point where the line through P and Q intersects the curve. If P and Q were the same point, i.e., if we wanted to find $2P$, we would use the tangent line to the curve at P; then $2P$ is the point symmetric to the third point where that tangent line intersects the curve.



We now show why there is exactly one more point where the line ℓ through P and Q intersects the curve; at the same time we will derive a formula for the coordinates of this third point, and hence for the coordinates of $P+Q$.

Let (x_1, y_1), (x_2, y_2) and (x_3, y_3) denote the coordinates of P, Q, and $P+Q$, respectively. We want to express x_3 and y_3 in terms of x_1, y_1, x_2, y_2.