Suppose that we are in case (3) in the definition of $P+Q$, and let $y = \alpha x+\beta$ be the equation of the line through P and Q (which is not a vertical line in case (3)). Then $\alpha = (y_2 - y_1)/(x_2 - x_1)$, and $\beta = y_1 - \alpha x_1$. A point on ℓ, i.e., a point $(x, \alpha x + \beta)$, lies on the elliptic curve if and only if $(\alpha x + \beta)^2 = x^3 + ax + b$. Thus, there is one intersection point for each root of the cubic equation $x^3 - (\alpha x + \beta)^2 + ax + b$. We already know that there are the two roots x_1 and x_2, because $(x_1, \alpha x_1 + \beta)$, $(x_2, \alpha x_2 + \beta)$ are the points P, Q on the curve. Since the sum of the roots of a monic polynomial is equal to minus the coefficient of the second-to-highest power, we conclude that the third root in this case is $x_3 = \alpha^2 - x_1 - x_2$. This leads to an expression for x_3, and hence $P + Q = (x_3, -(\alpha x_3 + \beta))$, in terms of x_1, x_2, y_1, y_2:

$$\begin{aligned} x_3 &= \left(\frac{y_2 - y_1}{x_2 - x_1}\right)^2 - x_1 - x_2; \\ y_3 &= -y_1 + \left(\frac{y_2 - y_1}{x_2 - x_1}\right)(x_1 - x_3). \end{aligned} \tag{4}$$

The case (5) when $P = Q$ is similar, except that α is now the derivative dy/dx at P. Implicit differentiation of Equation (1) leads to the formula $\alpha = (3x_1^2 + a)/2y_1$, and so we obtain the following formulas for the coordinates of twice P:

$$\begin{aligned} x_3 &= \left(\frac{3x_1^2 + a}{2y_1}\right)^2 - 2x_1; \\ y_3 &= -y_1 + \left(\frac{3x_1^2 + a}{2y_1}\right)(x_1 - x_3). \end{aligned} \tag{5}$$

Example 2. On the elliptic curve $y^2 = x^3 - 36x$ let $P = (-3, 9)$ and $Q = (-2, 8)$. Find $P + Q$ and $2P$.

Solution. Substituting $x_1 = -3$, $y_1 = 9$, $x_2 = -2$, $y_2 = 8$ in the first equation in (4) gives $x_3 = 6$; then the second equation in (4) gives $y_3 = 0$. Next, substituting $x_1 = -3$, $y_1 = 9$, $a = -36$ in the first equation in (5) gives $25/4$ for the x-coordinate of $2P$; then the second equation in (5) gives $-35/8$ for its y-coordinate.

There are several ways of proving that the above definition of $P + Q$ makes the points on an elliptic curve into an abelian group. One can use an argument from projective geometry, a complex analytic argument with doubly periodic functions, or an algebraic argument involving divisors on curves. See the references at the end of the section for proofs of each type.

As in any abelian group, we use the notation nP to denote P added to itself n times if n is positive, and otherwise $-P$ added to itself $|n|$ times.

We have not yet said much about the "point of infinity" O. By definition, it is the identity of the group law. In the diagram above, it should be visualized as sitting infinitely far up the y-axis, in the limiting direction of the ever-steeper tangents to the curve. It is the "third point of intersection" of any vertical line with the curve; that is, such a line has points of intersection of the form (x_1, y_1), $(x_1, -y_1)$ and O. A more natural way to introduce the point O is as follows.