2.1 The group law: the chord-and-tangent rule

We now turn to describing the elliptic curve group law, and it is here that viewing pictures of elliptic curves over $\mathbb{R}$ is especially instructive. We start with a less formal description until we define the role of the point at infinity $\mathcal{O}$. The group law exploits the fact that, over any field, a line (a degree one equation in x and y) intersects a cubic curve (a degree three equation in x and y) in three places (this is a special case of a more general theorem due to Bezout [Har77, I.7.8]). Namely, if we run a line $\ell : y = \lambda x + \nu$ between two points $P = (x_P, y_P)$ and $Q = (x_Q, y_Q)$ on E, then substituting this line into $E : y^2 = x^3 + ax + b$ will give a cubic polynomial in x, the roots of which are the x-coordinates of the three points of intersection between ℓ and E. Knowing the two roots (x_P and x_Q) allows us to determine a unique third root that corresponds to the third and only other point in the affine intersection $\ell \cap E$, which we denote by $\ominus R$ (the reason will become clear in a moment). The point $\ominus R$ is then "flipped" over the x-axis to the point R. In general, the elliptic curve composition law $\oplus$ is defined by this process, namely $R = P \oplus Q$. When computing $R = P \oplus P$, the line ℓ is computed as the tangent to E at P. That is, the derivatives of ℓ and E are matched at P, so (counting multiplicities) ℓ intersects E "twice" at P. Figures 2.5 and 2.6 illustrate why this process is aptly named the *chord-and-tangent* rule.

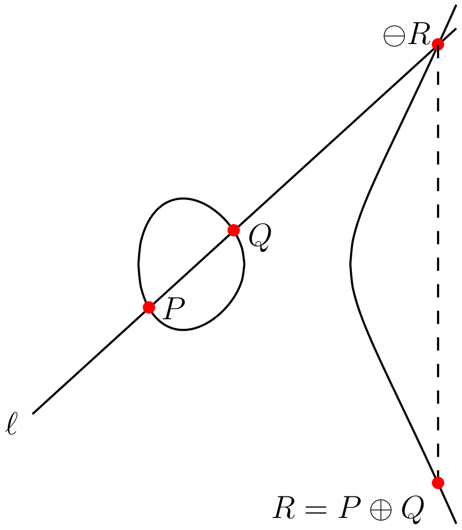

Figure 2.5: Elliptic curve addition.

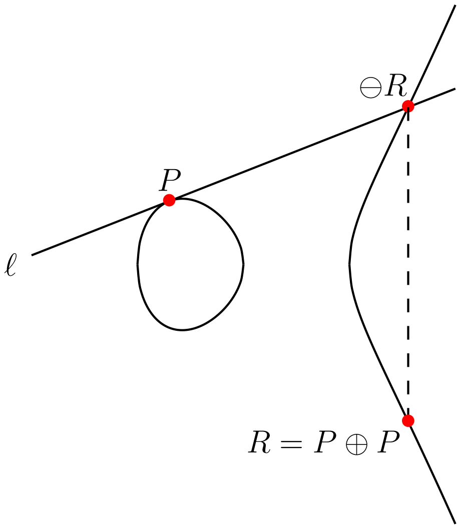

Figure 2.6: Elliptic curve doubling.

Having loosely defined the general group operation, we can now (also loosely) define the role of the point at infinity $\mathcal{O}$. To try and place it somewhere in the above diagrams, one can think of $\mathcal{O}$ as being a point that simultaneously sits infinitely high and infinitely low in the y direction. This allows us to informally conceptualise two properties of elliptic curve groups: firstly, that the point at infinity $\mathcal{O}$ plays the role of the *identity* of the group; and secondly, that the unique inverse of a point is its reflected image over the x-axis (e.g. the $\ominus R$'s in Figures 2.5 and 2.6 are the respective inverses of the R's, and vice versa). If we apply the process in the previous paragraph to compute $R \oplus (\ominus R)$, we start by finding the vertical line that connects them (the dashed lines in Figures 2.5 and 2.6). This line also intersects E (twice) at the point at infinity $\mathcal{O}$, which is then reflected back onto itself, giving $R \oplus (\ominus R) = \mathcal{O}$. Thus, if we define the identity of the group to be $\mathcal{O}$, then the inverse of any element $R = (x_R, y_R)$ is taken as $\ominus R = (x_R, -y_R)$.

Example 2.1.1 (Magma script). $E/\mathbb{R} : y^2 = x^3 - 2x$ is an elliptic curve. The points $(-1,-1)$, $(0,0)$ and $(2,2)$ are all on E, and are also on the line $\ell : y = x$. Applying the technique described above to compute some example group law operations via the line ℓ, we have $(-1,-1) \oplus (0,0) = (2,-2)$, $(2,2) \oplus (0,0) = (-1,1)$, and $(-1,-1) \oplus (2,2) = (0,0)$. All but four points come in pairs with their inverse (i.e. (x', y') and $(x', -y')$); the exceptions being $(0,0)$, $(\sqrt{2}, 0)$, $(-\sqrt{2}, 0)$ (notice the vertical tangents when $y = 0$ in these cases), and $\mathcal{O}$, which are all their own inverse, e.g. $(0,0) = \ominus(0,0)$, so $(0,0) \oplus (0,0) = \mathcal{O}$ on E. The tangent line ℓ' to E at $(-1,-1)$ is $\ell' : y = -\frac{1}{2}x - \frac{3}{2}$, and it intersects E once more at $(\frac{9}{4}, -\frac{21}{8})$, which gives $(-1,-1) \oplus (-1,-1) = [2](-1,-1) = (\frac{9}{4}, \frac{21}{8})$.

Example 2.1.2 (Magma script). In this example we consider the same curve equation as the last example, but this time over a small finite field, namely $E/\mathbb{F}_{11} : y^2 = x^3 - 2x$. Rational points are injected naturally across to the finite field case (as long as there is no conflict with the characteristic), so we can immediately find the points $(0,0)$, $(2,2)$ and $(-1,-1) = (10,10)$ (and their inverses) in Figure 2.9. In this case, consider performing the group law operation between the (blue) points $(5,7)$ and $(8,10)$. The line ℓ that joins them is $y = x + 2$, which intersects E once more at $(10,1)$. Negating the y-coordinate finds the other point on the dashed line, and gives $(5,7) \oplus (8,10) = (10,10)$.

Example 2.1.2 is also intended to justify why, although (in cryptography) we only ever use elliptic curves over finite fields, we often opt to illustrate the group law by drawing the continuous pictures of curves over $\mathbb{R}$.