An **elliptic curve** is the set of all solutions (x, y) to a Weierstrass equation which has the form:

$$y^2 = x^3 + ax + b$$

together with an extra point $\mathscr{O}(\infty, \infty)$ at infinity in the projective plane that lies on every vertical line.

Moreover, a and b must satisfy $4a^3 + 27b^2 \neq 0$.

Thus, an elliptic curve E is defined by its two parameters: a and b and obviously, a point (x, y) is on an elliptic curve E if it satisfies the Weierstrass equation associated with E.

We define the addition of points on an elliptic curve with the following algorithm:

Algorithm (Elliptic Curve addition Algorithm)**.** *Let* $E : y^2 = x^3 + ax + b$ *and* $P_1, P_2 \in E$

(a) *If* $P_1 = \mathscr{O}$*, then* $P_1 + P_2 = P_2$
(b) *else if* $P_2 = \mathscr{O}$ *then* $P_1 + P_2 = P_1$
(c) *else, write* $P_1 = (x_1, y_1)$ *and* $P_2 = (x_2, y_2)$
(d) *if* $x_1 = x_2$ *and* $y_1 = -y_2$ *then return* $P_1 + P_2 = \mathscr{O}$
(e) *Otherwise*
- *define* λ *by*
  - $\lambda = \frac{y_2 - y_1}{x_2 - x_1}$ *if* $P_1 \neq P_2$
  - $\lambda = \frac{3x_1^2 + a}{2y_1}$ *if* $P_1 = P_2$
- *Let* $x_3 = \lambda^2 - x_1 - x_2$ *and* $y_3 = \lambda(x_1 - x_3) - y_1$
- *Then return* $P_1 + P_2 = (x_3, y_3)$

Now, the addition law makes the points of an elliptic curve E into an abelian group:

Theorem. *Let* E *be an elliptic curve. Then the addition law on* E *has the following properties:*

(Identity) $P + \mathscr{O} = \mathscr{O} + P = P$, $\forall P \in E$
(Inverse) $P + (-P) = \mathscr{O}$, $\forall P \in E$
(Associative) $(P + Q) + R = P + (Q + R)$, $\forall P, Q, R \in E$
(Commutative) $P + Q = Q + P$, $\forall P, Q \in E$

Now, the identity, inverse and commutative properties are easily verifiable. However, although there are many ways to prove associativity, none of the proofs are easy and require more advanced notions on elliptic curves. However, we can approach the problem with very rudimentary means by simply using the explicit formulas described in the algorithm above and verify every case.

This approach is **very tedious.** Thus, we propose a computer-assisted approach.