Theorem: Given E, an elliptic curve defined in a field F, and given $P = (x_p, y_p)$ and $Q = (x_q, y_q)$ defined in the same field F, that lie somewhere on the curve E (such that either $P \neq Q$ and $x_p \neq x_q$, or $P = Q$ and the line is therefore tangent to the curve E), a straight line L, through P and Q, intersects the curve E at a third point, $R = (x_r, y_r)$, which is also in F. Furthermore, these are the only points at which L will intersect E in F

Note: Any elliptic curve, defined on a field with characteristic other than 2 or 3, can be converted into the Weierstrass form $y^2 = x^3 + ax + b$. This will not be proved here, but explored elsewhere, and taken here, as given.

This proof only applies to elliptic curves in the Weierstrass form of the elliptic curve. It therefore only applies to elliptic curves defined in a field with characteristic other than 2 or 3.

Proof:

Let F be a field

Let $E : y^2 = x^3 + a_E x + b_E$ be an elliptic curve, defined on F in the Weierstrass form, for some a_E, $b_E \in \mathbb{R}$

Let $P = (x_p, y_p)$ and $Q = (x_q, y_q)$ be points on the elliptic curve E

Let $L : y = m_L x + b_L$ be the straight line through P and Q, for some m_L, $b_L \in \mathbb{R}$

NOTE: in this form, the line L has a gradient of m. It should be noted that we are not considering the case where the line L is vertical, that is, $m \neq \infty$

So, $y^2 = m_L^2 x^2 + 2m_L b_L x + b_L^2$

And, the points at which L intersects with E are given by:

$m_L^2 x^2 + 2m_L b_L x + b_L^2 = x^3 + a_E x + b_E$

$x^3 - m_L^2 x^2 - 2m_L b_L x + a_E x + b_E - b_L^2 = 0$

$x^3 - m_L^2 x^2 + (a_E - 2m_L b_L)x + (b_E - b_L^2) = 0$

Which defines a cubic.

Let $C : y = x^3 - m_L^2 x^2 + (a_E - 2m_L b_L)x + (b_E - b_L^2)$ be the cubic whose roots are equivalent to the x values when L intersects with E

We know that 2 solutions to this cubic C are $x = x_p$ and $x = x_q$

We also know that there is a maximum of 3 solutions to the cubic equation C, which means there must be a maximum of 3 points at which the line L intersects with the elliptic curve E.

The case where $P = Q = R$:

When $P = Q = R$, the line L only intersects the curve E at one point. In this case, $x_p = x_q = x_r$ and the conditions of our proof are met - i.e. $P = Q = R = (x_p, y_p) = (x_r, y_r) \in F$

The case where $P \neq Q$:

When $P \neq Q$, the line L intersects the curve E at a minimum of 2 distinct points, those being $P = (x_p, y_p)$ and $Q = (x_q, y_q)$

So, $C : y = (x - x_p)(x - x_q)(x - x_r)$ where x_r is some value, the third root of C

We can expand C in the above form, and we get $y = x^3 - (x_p + x_q + x_r)x^2$... (the other coefficients don't matter)

Thus: $(x_p + x_q + x_r) = m_L^2$ (because, from above $C : y = x^3 - m_L^2 x^2 + (a_E - 2m_L b_L)x + (b_E - b_L^2)$ - the coefficient of x^2 is $-m_L^2$)

$x_r = m_L^2 - x_p - x_q$, which exists in the field F in which P and Q are defined (strictly, when $m_L \neq \infty$ - the line L is not vertical).

Therefore, if P and Q, $P \neq Q$, exist in field F, then R exists in F as well.

The case where $P = Q$:

When $P = Q = (x_p, y_p)$, the line L is tangent to the curve E at 1 point, that being $P = Q = (x_p, y_p)$

So, $C : y = (x - x_p)^2(x - x_r)$ where x_r is some value, the third root of C

If we expand C in the above form, we get $y = x^3 - (2x_p + x_r)x^2$... (the other coefficients don't matter)

And thus: $(2x_p + x_r) = m_L^2$ (because, from above $C : y = x^3 - m_L^2 x^2 + (a_E - 2m_L b_L)x + (b_E - b_L^2)$ - the coefficient of x_2 is $-m_L^2$)

$x_r = m^2 - 2x_p$, which exists in the Field in which P and Q defined (strictly, when $m_L \neq \infty$ - the line L is not vertical).

Therefore, if P and Q, $P = Q$, exist in field F, then R exists in F as well.

Furthermore, as there are only 3 possible solutions to the cubic C, P, Q and R are the only points at which L intersects with E.