ECC, problem 01.**08

Roman

November 25, 2023

Problem

Prove that three points on an elliptic curve E over the set of rational numbers $\mathbb{Q}$ are collinear iff they add to the identity element $\mathcal{O}$. To simplify the proof, you may assume that the three points are distinct.

Solution

Proof.

Sufficient condition.

Let P, Q, R be three points on E such that $P + Q + R = \mathcal{O}$. We want to show that P, Q, R are collinear, i.e.

$$P + Q + R = \mathcal{O} \implies P, Q, R \text{ are collinear}$$

The x-coordinates of $P + Q + R$ is (from the explicit formula for the addition law on E)

$$x_{P+Q+R} = \frac{(y_{P+Q} - y_R)^2}{(x_{P+Q} - x_R)^2} - x_{P+Q} - x_R$$

As $P + Q + R = \mathcal{O}$, we have $x_{P+Q} = x_R$. From that, using the explicit formula for the addition law on E for the second time,

$$x_{P+Q} = x_R = \frac{(y_P - y_Q)^2}{(x_P - x_Q)^2} - x_P - x_Q$$

or

$$\frac{(y_P - y_Q)^2}{(x_P - x_Q)^2} = x_P + x_Q + x_R$$

The group law on E is commutative and associative, so from $P + Q + R = \mathcal{O}$ with choosing another order of summation one gets:

$$\frac{(y_P - y_Q)^2}{(x_P - x_Q)^2} = \frac{(y_P - y_R)^2}{(x_P - x_R)^2} = \frac{(y_Q - y_R)^2}{(x_Q - x_R)^2}$$

which states that the slopes of the lines PQ, PR, QR are equal. Therefore, P, Q, R are collinear.

Necessary condition.

Let P, Q, R be three points on E such that P, Q, R are collinear. We want to show that $P + Q + R = \mathcal{O}$, i.e.

$$P + Q + R = \mathcal{O} \impliedby P, Q, R \text{ are collinear}$$

From the associative property of the group law on E, we have

$$(P + Q) + R = P + (Q + R)$$

For the x-coordinates of the both sides of the equation above, we have

$$x_{(P+Q)+R} = \frac{(y_{P+Q} - y_R)^2}{(x_{P+Q} - x_R)^2} - x_{P+Q} - x_R$$

and

$$x_{P+(Q+R)} = \frac{(y_P - y_{Q+R})^2}{(x_P - x_{Q+R})^2} - x_P - x_{Q+R}$$

which combined together give

$$\frac{(y_{P+Q} - y_R)^2}{(x_{P+Q} - x_R)^2} - x_{P+Q} - x_R = \frac{(y_P - y_{Q+R})^2}{(x_P - x_{Q+R})^2} - x_P - x_{Q+R}$$

Using the explicit formula for the addition law on E, we have for the x-coordinates of $P+Q$ and $Q+R$:

$$x_{P+Q} = \frac{(y_P - y_Q)^2}{(x_P - x_Q)^2} - x_P - x_Q$$

and

$$x_{Q+R} = \frac{(y_Q - y_R)^2}{(x_Q - x_R)^2} - x_Q - x_R$$

Substituting these into the equation above, it folows that the following equation holds for any three collinear points P, Q, R:

$$\frac{(y_{P+Q} - y_R)^2}{(x_{P+Q} - x_R)^2} - \frac{(y_P - y_{Q+R})^2}{(x_P - x_{Q+R})^2} = 0$$

as the slopes of the lines PQ and QR are equal. This equation can be rewritten as

$$\frac{(y_{P+Q} - y_R)^2}{(x_{P+Q} - x_R)^2} = \frac{(y_P - y_{Q+R})^2}{(x_P - x_{Q+R})^2}$$

For that to hold for any three collinear points P, Q, R, the following equation must hold for any two points P, Q:

$$x_{P+Q} - x_R = x_P - x_{Q+R} = 0$$

That proves that $P + Q + R = \mathcal{O}$.

Conclusion.

We have shown that three points on an elliptic curve E over the set of rational numbers $\mathbb{Q}$ are collinear iff they add to the identity element $\mathcal{O}$:

$$\boxed{P + Q + R = \mathcal{O} \iff P, Q, R \text{ are collinear}}$$

$\square$