Problem 4. «Elliptic curve points»

Alice is studying elliptic curve cryptography. Her task for today is in practice with basic operations on elliptic curve points. Let $\mathbb{F}_p$ be the finite field with p elements ($p > 3$ prime). Let $E/\mathbb{F}_p$ be an elliptic curve in Weierstrass form, that is a curve with equation $y^2 = x^3 + ax + b$, where $a, b \in \mathbb{F}_p$ and $4a^3 + 27b^2 \neq 0$. Recall that the affine points on E and the point $\mathcal{O}$ at infinity form an abelian group, denoted

$$E(\mathbb{F}_p) = \{(x, y) \in \mathbb{F}_p^2 \colon y^2 = x^3 + ax + b\} \cup \{\mathcal{O}\} \ .$$

Assume that $b = 0$. Let $R \in E(\mathbb{F}_p)$ be an element of odd order, $R \neq \mathcal{O}$. Consider $H = \langle R \rangle$ that is the subgroup generated by R.

Help Alice to show that if $(u, v) \in H$, then u is a quadratic residue mod p.

Remark. For the Weierstrass form, $P_1 + P_2$ for $P_1, P_2 \in E(\mathbb{F}_p)$ is calculated as follows:

- $P_1 + \mathcal{O} = P_1$.
  Next, we assume that $P_1, P_2 \neq \mathcal{O}$ and $P_1 = (x_1, y_1)$, $P_2 = (x_2, y_2)$.
- $P_1 + (-P_1) = \mathcal{O}$. Note that $-(x_1, y_1) = (x_1, -y_1)$.
  Next, we assume that $P_1 \neq -P_2$.
- $P_1 + P_1 = P_3 = (x_3, y_3)$ can be calculated in the following way:

$$x_3 = \frac{(3x_1^2 + a)^2}{(2y_1)^2} - 2x_1, \qquad y_3 = -y_1 - \frac{3x_1^2 + a}{2y_1}(x_3 - x_1).$$

  Next, we assume that $P_1 \neq P_2$.
- $P_1 + P_2 = P_3 = (x_3, y_3)$ can be calculated in the following way:

$$x_3 = \frac{(y_2 - y_1)^2}{(x_2 - x_1)^2} - x_1 - x_2, \qquad y_3 = -y_1 - \frac{y_2 - y_1}{x_2 - x_1}(x_3 - x_1).$$