Alice AG

Bob 9G

Curva $y^2 = x^3 + x - 1$, $p = 7$

$G = (1, 1)$

$2G = x_3 = \left(\frac{3+1}{2}\right)^2 - 1 - 1 = (2)^2 - 2 = 2$

$y_3 = 2(1-2) - 1 = 2(-1) - 1 = -3$

$2G : (2, -3)$

$4G = 2G \oplus 2G$

$x_3 = \left(\frac{3(2)^2+1}{2(-3)}\right)^2 - 4 = \left(\frac{3(4)+1}{-6}\right)^2 - 4$

$= \left(\frac{13}{-6}\right)^2 - 4 = \left(\frac{6}{-6}\right)^2 - 4 = -3$

$= 4$

$y_3 = -1(2+3) + 3 = -5 + 3 = -2$

$= 5$

$4G : (4, 5)$

$8G :$

$x_3 = \left(\frac{3(4)^2+1}{2(5)}\right)^2 - 8 = \left(\frac{3(16)+1}{10}\right)^2 - 8$

$= \left(\frac{3(2)+1}{3}\right)^2 + 6 = \left(\frac{7}{3}\right)^2 + 6$

$= 0 + 6 = 6$

$y_3 = 0(4-6) - 5 = 2$

$8G : (6,2) \quad G : (1,1)$

$$x_3 = \left(\frac{1-2}{1-6}\right)^2 - 1 - 6 = \left(\frac{-1}{-5}\right)^2 - 7$$

$$= \left(\frac{1}{5}\right)^2 - 7 = (3)^2 - 0 = 2$$

$$y_3 = 3(6-2) - 2 = 3(4) - 2 = 12 - 2 = 10$$

$$= 3$$

$$9G = (2,3)$$

$\alpha = 4 \quad \beta = 9$

$4G = (4,5) \qquad 9G = (2,3)$

$9G \cdot 4$

$(2,3) \oplus (2,3)$

$$x_3 = \left(\frac{3(2)^2+1}{2(3)}\right)^2 - 4 = \left(\frac{3(4)+1}{6}\right)^2 - 4 = \left(\frac{13}{6}\right)^2 - 4$$

$$1 - 4 = 4$$

$$y_3 = 1(2-4) - 3 = 1(-2) - 3 = -5 = 2$$

$2(9G) : (4,2)$

$$x_3 = \left(\frac{3(4)^2+1}{2(2)}\right)^2 - 8 = \left(\frac{3(2)+1}{4}\right)^2 + 6 = 0 + 6 = 6$$

$$y_3 = 0(4-6) - 2 = -2 = 5$$

$4(9G) : (6,5)$

+300*