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

(16) $P = (2, 7)$ $q = 2$ $b = 3$

doublings		halvings	Accu.	Answer
P	$(2,7)$	19	P	odd add P
$2P$	$(14,15)$	9	$P+2P$	odd, add $2P$
$4P$	$(15,5)$	4	$P+2P$	even, don't add
$8P$	$(8,15)$	2	$P+2P$	even, don't add
$16P$	$(3,6)$	1	$P+2P+16P$	odd, add $16P$

$P = (2, 7)$

$2P = P + P$ $\lambda = \frac{3x_P^2 + a}{2y_P} = \frac{3 \cdot 2^2 + 2}{2 \cdot 7} = \frac{14}{14} = 1$

In $\mathbb{Z}_{12}$ $\frac{1}{14} = 11$ since $14 \cdot 11 = 154 = 153 + 1 = 1$

So $\lambda = 11 \cdot 1 = 11$

$x_R = \lambda^2 - x_P - x_P = 11^2 - 2 - 2 = 121 - 2 - 2 - 3 = 14$

$y_R = y_P + \lambda(x_R - x_P) = 7 + 11(14 - 2) = 7 + 132 = 139 = 2$

since $2P = -R$, $2P = (14, 15)$

$4P = 2(14, 15)$

$\lambda = \frac{3 \cdot 14^2 + 2}{2(15)} = \frac{12}{13}$ $\mathbb{Z}_{13}$ $\frac{1}{13} = 4 \cdot 13 = 51 + 1 = 1$

$\lambda = 12 \cdot 1 = 14$

$x_R = 14^2 - 14 - 14 = 15$

$y_R = 15 + 14(15 - 14) = 12$ $4P = (15, 5)$

$2P = -R \quad -12 = 5$

$P = (2, 7)$

$a = 2, \quad b = 3$

$8P = 2(15, 5)$

$\lambda = \frac{3(15^2) + 2}{2(5)} \quad \frac{14}{10}$

$Z_{17}\ \frac{1}{10} = 12 \cdot 10 = 179 \cdot 11 = 120 = 1$

$\lambda = 15$

$12 \cdot 11 = 15$

$x_R = 15^2 - 15 - 15 = 4 - 15 - 15 = 8$

$y_R = y_P + \lambda(x_R - x_P) = 5 + 15(8 - 15) = 2$

$2P = -R \qquad 17 - 2 = 15$

$8P = (8, 15)$

$16P = 2(8, 15)$

$\lambda = \frac{3(8^{\overset{13}{2}}) + 2}{2(15)} = \frac{7}{13} \qquad Z_{17}\ \frac{1}{13} = 4$

$\lambda = 4 \cdot 7 = 11$

$x_R = 11^2 - 8 - 8 = 3$

$y_R = 15 + 11(3 - 8) = 11$

$2P = -R \qquad 17 - 11 = 6$

$16P = (3, 6)$

$16P + 2P = \underset{P}{(3,6)} + \underset{Q}{(14,15)} = 18P = 1 \quad (15, 12)$

$\lambda = \frac{15 - 6}{14 - 3} = \frac{9}{11} \qquad Z_{17}\ \frac{1}{11} = 14 \cdot 9 = 7$

$x_R = 7^2 - 3 - 14 = 15 \qquad y_R = 6 + 7(15 - 3) = 5$

$16P + P = 19P = (15, 12) + (2, 7)$

(P, Q)

$\lambda = \frac{7 - 12}{2 - 15} = \frac{12}{4}$

$\frac{1}{4} = 13 - 12 = 3$

$\lambda = 3$

$x_R = 3^2 - 15 - 2 = 9$

$y_R = 12 + 3(9 - 15) = 11$

$17 - 11 = 6$

$19P = (9, 6)$