Compute $19P$ using the elliptic curve $y^2 = x^3 + 2x + 3$ over Z_{17}, and base point $P = (2,7)$

$a = 2, x_P = 2, y_P = 7$

Note: Inverse values (i.e. $\frac{1}{10} = 10^{-1}$) can be found in the Z_{17} chart (i.e. where $10 = 1$)

Calculate $2P = P + P$ using tangent line equation to calculate λ, mod 17 all the way.

$P = (2,7)$

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

$x_R = \lambda^2 - x_P - x_P = 1^2 - 2 - 2 = -3$

$y_R = y_P + \lambda(x_R - x_P) = 7 + 1(-3 - 2) = 2$

$R = (x_R, y_R) = (-3,2), 2P = -R = (-3,-2) = (-3 + 17, -2 + 17) \rightarrow \boldsymbol{2P} = (\mathbf{14}, \mathbf{15})$

Calculate $3P = P + 2P$ using secant line equation to calculate λ, mod 17 all the way.

$P = (2,7), Q = 2P = (14,15)$

$\lambda = \frac{y_P - y_Q}{x_P - x_Q} = \frac{7-15}{2-14} = \frac{-8+17}{-12+17} = \frac{9}{5} = 9 \cdot \frac{1}{5} = 9 \cdot 5^{-1} = 9 \cdot 7 = 63\, mod\, 17 = 12$

$x_R = \lambda^2 = x_P - x_Q = 12^2 - 2 - 14 = 128\, mod\, 17 = 9$

$y_R = y_P + \lambda(x_R - x_P) = 7 + 12(9 - 2) = 91\, mod\, 17 = 6$

$R = (x_R, y_R) = (9,6), 3P = -R = (9,-6) = (9, -6 + 17) \rightarrow \boldsymbol{3P} = (\mathbf{9}, \mathbf{11})$

Continue doubling from $2P$ to $16P$ (using tangent equation), then calculate $19P = 16P + 3P$

Calculate $4P = 2P + 2P$

$2P = (14,15)$

$\lambda = \frac{3x_P^2+a}{2y_P} = \frac{3(14^2)+2}{2(15)} = \frac{590}{30} = 59 \cdot \frac{1}{3} = 59\, mod\, 17 \cdot 3^{-1} = 8 \cdot 6 = 48\, mod\, 17 = 14$

$x_R = \lambda^2 = x_P - x_P = 14^2 - 14 - 14 = 168\, mod\, 17 = 15$

$y_R = y_P + \lambda(x_R - x_P) = 15 + 14(15 - 14) = 29\, mod\, 17 = 12$

$R = (x_R, y_R) = (15,12), 4P = -R = (15,-12) = (15, -12 + 17) \rightarrow \boldsymbol{4P} = (\mathbf{15}, \mathbf{5})$

Calculate $8P = 4P + 4P$

$4P = (15,5)$

$\lambda = \frac{3x_P^2+a}{2y_P} = \frac{3(15^2)+2}{2(5)} = \frac{677}{10} = 677 \cdot \frac{1}{10} = 677\, mod\ 17 \cdot 10^{-1} = 14 \cdot 12 = 168\, mod\ 17 = 15$

$x_R = \lambda^2 = x_P - x_P = 15^2 - 15 - 15 = 195\, mod\ 17 = 8$

$y_R = y_P + \lambda(x_R - x_P) = 5 + 15(8 - 15) = -100\, mod\ 17 = -15$

$R = (x_R, y_R) = (8, -15), 8P = -R = (8,15) \rightarrow \mathbf{8P = (8, 15)}$

Calculate $16P = 8P + 8P$

$8P = (8,15)$

$\lambda = \frac{3x_P^2+a}{2y_P} = \frac{3(8^2)+2}{2(15)} = \frac{194}{30} = 194 \cdot \frac{1}{30} = 194\, mod\ 17 \cdot (30\, mod\ 17)^{-1} = 7 \cdot 13^{-1} = 7 \cdot 4 =$
$28\, mod\ 17 = 11$

$x_R = \lambda^2 = x_P - x_P = 11^2 - 8 - 8 = 105\, mod\ 17 = 3$

$y_R = y_P + \lambda(x_R - x_P) = 15 + 11(3 - 8) = -40\, mod\ 17 = -6$

$R = (x_R, y_R) = (3, -6), 16P = -R = (3,6) \rightarrow \mathbf{16P = (3, 6)}$

Calculate $19P = 16P + 3P$ using secant line equation to calculate λ, mod 17 all the way.

$P = 19P = (3,6), Q = 3P = (9,11)$

$\lambda = \frac{y_P - y_Q}{x_P - x_Q} = \frac{11-6}{9-3} = \frac{5}{6} = 5 \cdot \frac{1}{6} = 5 \cdot 6^{-1} = 5 \cdot 3 = 15$

$x_R = \lambda^2 = x_P - x_Q = 15 - 3 - 9 = 213\, mod\ 17 = 9$

$y_R = y_P + \lambda(x_R - x_P) = 6 + 15(9 - 3) = 96\, mod\ 17 = 11$

$R = (x_R, y_R) = (9,11), 3P = -R = (9, -11) = (9, -11 + 17) \rightarrow \mathbf{19P = (9, 6)}$