Name: Solutions

Directions: Show all work. No credit for answers without work.

1. **[2 parts, 4 points each]** Let $p = 67$ and let E be the elliptic curve given by $y^2 = x^3 + 9x + 33$ over $\mathbb{F}_p$. Let $P = (42, 53)$ and $Q = (62, 8)$. Compute the following points.

   (a) P^2

$y^2 = x^3 + Ax + B, \quad 2y\frac{dy}{dx} = 3x^2 + A$

$\lambda = \frac{3x_1^2 + A}{2y_1} = \frac{3(42)^2 + 9}{2(53)} = \frac{5301}{106} = \frac{8}{39} = 8\cdot(39)^{-1} = 8\cdot(-12) = 8\cdot 55 = 38.$

EEA(67, 39):

$67 = (1)(39) + 28$
$39 = (1)(28) + 11$
$28 = (2)(11) + 6$
$11 = (1)(6) + 5$
$6 = (1)(5) + 1$

$1 = 6 + (-1)(5) = 6 + (-1)[11 + (-1)(6)]$
$= (2)(6) + (-1)(11) = (2)[28 + (-2)(11)] + (-1)(11)$
$= (2)(28) + (-5)(11) = (2)(28) + (-5)[39 + (-1)(28)]$
$= (7)(28) + (-5)(39) = 7(67 + (-1)(39)) + (-5)(39)$
$= (7)(67) + (-12)(39)$

$x_3 = \lambda^2 - x_1 - x_2$
$= (38)^2 - 42 - 42 = 1360 = 20$

$y_3 = \lambda(x_1 - x_3) - y_1 = (38)(42 - 20) - 53$
$= 38(22) - 53 = 783 = 46$

So $P^2 = \boxed{(20, 46)}$.

   (b) $\frac{P}{Q}$ and $\frac{Q}{P}$

$\frac{P}{Q} = P\cdot Q^{-1} = (42,53)\cdot(62,8)^{-1} = (42,53)\cdot(62,-8) = (42,53)\cdot(62,59).$

$\lambda = \frac{y_2 - y_1}{x_2 - x_1} = \frac{59 - 53}{62 - 42} = \frac{6}{20} = \frac{\cancel{2}\cdot 3}{\cancel{2}\cdot 10} = 3\cdot(10)^{-1} = 3\cdot(-20) = 3\cdot 47 = 7.$

EEA(67, 10):

$67 = (6)(10) + 7$
$10 = (1)(7) + 3$
$7 = (2)(3) + 1$

$1 = 7 + (-2)(3) = 7 + (-2)[10 + (-1)(7)]$
$= (3)(7) + (-2)(10) = 3(67 + (-6)(10)) + (-2)(6)$
$= (3)(67) + (-20)(10)$

$x_3 = \lambda^2 - x_1 - x_2$
$= 7^2 - 42 - 62 = -55$
$= 12$

$y_3 = \lambda(x_1 - x_3) - y_1$
$= 7(42 - 12) - 53$
$= 7(30) - 53 = 157 = 23$

So $\frac{P}{Q} = \boxed{(12, 23)}$

Also, $\frac{Q}{P} = \left(\frac{P}{Q}\right)^{-1} = \left((12,23)\right)^{-1} = (12, -23) = \boxed{(12, 44)}$

2. **[2 points]** Let $p = 11$, let $P = (1, 2)$ and $Q = (2, 3)$. Find A and B such that P and Q are both on the elliptic curve over $\mathbb{F}_p$ given by $y^2 = x^3 + Ax + B$.

$P = (1,2)$: $2^2 = 1^3 + A(1) + B$
$A + B = 3$

$Q = (2,3)$: $3^2 = 2^3 + A(2) + B$
$2A + B = 1$

$2A + B = 1$
$-(A + B = 3)$
$A = -2 = 9$

$B = 3 - A = 3 - 9 = -6 = 5$

So $\boxed{A = 9,\ B = 5}$

and E is

$\boxed{y^2 = x^3 + 9x + 5}$.