Math373 **Homework 12** **Due Wed, Apr 19, 2023**

Directions: Solve the following problems. All written work must be your own. See the course syllabus for detailed rules.

1. Let E be the elliptic curve given by $y^2 = x^3 + 17$ over the real numbers. Let $P = (-1, 4)$ and $Q = (2, 5)$.

   (a) Compute PQ and $\frac{P}{Q}$. Hint: What does it mean to divide by a point in an elliptic curve group?

   (b) Compute P^2 and Q^2.

2. Let E be the elliptic curve given by $y^2 = x^3 + 5x + 1$ over $\mathbb{F}_{19}$. Compute the following.

   (a) $(4, 3)\mathcal{O}$.

   (b) $(4, 3)^{-1}$.

   (c) $(4, 3)(10, -5)$.

   (d) $(4, 3)^2$.

   (e) $(4, 3)^4$.

   (f) $(4, 3)^8$.

3. Let E be the elliptic curve given by $y^2 = x^3 + 5x + 1$ over $\mathbb{F}_{19}$ and let $g = (4, 3)$. Find the following.

   (a) $\log_g(\mathcal{O})$

   (b) $\log_g((4, -3))$

   (c) $\log_g((11, 0))$