

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 $y^2 = x^3 + 5x + 1$ 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) $(4, 3)^8$.

2. **This problem moved to HW12.** We will cover the necessary material on Wednesday Apr 13.

Alice and Bob wish to share a secret using Elliptic Curve-based Diffie–Hellman. They agree on the curve E given by $y^2 = x^3 + 14x + 2$ over \mathbb{F}_{31} and the base element $g = (12, 10)$.

- (a) Bob picks $b = 10$ as his private exponent. What should Bob send to Alice?
- (b) Alice sends $A = (18, 17)$ to Bob. Compute Alice and Bob's shared secret.
- (c) **[Challenge (optional)]** Find Alice's private exponent a . In other words, find a such that $g^a = A$. This is an instance of the Elliptic Curve Discrete Logarithm Problem (ECDLP).