**4400-001 - SPRING 2022 - WEEK 14 (4/19, 4/21)**
**ELLIPTIC CURVES (BONUS)**

*Some of these exercises can be found in Savin - Chapter 9.*

**Exercise 1 (required for bonus assignment).**
Consider the equation $E : y^2 = x^3 + 8$.

(1) For $P = (x_1, y_1)$ and $Q = (x_2, y_2)$, assuming $x_1 \neq x_2$, give a formula for $P + Q$.

(2) Compute $(-2, 0) +_E (1, 3)$

(3) For $P = (x, y)$, give a formula for $2P$.

(4) Compute $2P$ and $4P$ for $P = (1, 3)$.

(5) Solve the equation $2P = \infty$ on $E$.

**Exercise 2.**

(1) Compute all of the points on $E : y^2 = x^3 + 8$ over $\mathbb{F}_5$.

(2) Find a partner and use ECC with this curve over $\mathbb{F}_5$ to establish a shared secret.

**Exercise 3.**

(1) For small values of $p$, compute all of the solutions to $y^2 = x^3 + x$ in $\mathbb{F}_p$. Notice any patterns? Can you prove them?

(2) Explain why if $\alpha$ is a Gaussian integer and $P = (x, y)$ is a solution in $\mathbb{C}^2$ to $y^2 = x^3 + x$, it makes sense to write $\alpha \cdot P$ (generalizing $nP$ for $n \in \mathbb{Z}$).

(3) Questions (1) and (2) are related. How?