ELLIPTIC CURVES OVER FINITE FIELDS

DEFINITION: Let $p \geq 5$ be a prime. An **elliptic curve** over $\mathbb{Z}_p$ is the solution set E_p in $\mathbb{Z}_p \times \mathbb{Z}_p$ to an equation of the form $y^2 = x^3 + [a]x + [b]$ for real constants $[a], [b] \in \mathbb{Z}_p$ that satisfy the technical assumption that $[4][a]^3 + [27][b]^2 \neq 0$. For an elliptic curve E_p we define $\overline{E}_p = E_p \cup \{\infty\}$, where ∞ is a formal symbol.

THEOREM: There is a group structure on $\overline{E}_p$ with operation $\star$, identity element ∞, and inverse $-^\vee$ given by the same geometric rules as in the real case.

(1) Consider the elliptic curve $\overline{E}_5 : y^2 = x^3 - [1]$ over $\mathbb{Z}_5$.
   (a) Use trial and error to compute all of the points in $\overline{E}_5$.
   (b) Without any computation, explain why each element of E_5 (not including ∞) has order $2, 3$, or 6.
   (c) For $P = ([3], [1])$, compute $2P$ and $3P$.
   (d) Without any further computation of $\star$ with lines and whatnot, determine the order of each point in $\overline{E}_5$.

(2) Consider the elliptic curve $\overline{E}_5 : y^2 = x^3 - x + [1]$ over $\mathbb{Z}_5$.
   (a) Use trial and error to compute all of the points in $\overline{E}_5$.
   (b) Explain why there are no points in E_5 (not including ∞) with odd order.
   (c) Explain why every point $P \in \overline{E}_5$ has $8P = \infty$.