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 $\overline{E}_5$.

(a) $\overline{E}_5 = \{(0, 2), (0, 3), (1, 0), (3, 1), (3, 4), \infty\}$.
(b) $\overline{E}_5$ is a group with 6 elements. By Lagrange's Theorem, the order of an element divides the order of the group.
(c) To compute $2P$, we find the tangent line through P. By implicit differentiation, we get $[2]y\frac{dy}{dx} = [3]x^2$, so the slope of the tangent line at P is $\frac{[3]\cdot[3]^2}{[2]\cdot[1]} = \frac{[27]}{[2]} = \frac{[2]}{[2]} = [1]$. The tangent line is then $y = x + [3]$. Plugging this into the original equation and solving (or just testing the other points in E) we get that the other point of intersection is $([0], [3])$, so $2P = ([0], [-3]) = ([0], [2])$. To compute $3P$,we take the line between P and $2P$. The slope is $\frac{[1]-[2]}{[3]-[0]} = \frac{[4]}{[3]} = [4][2] = [3]$, so the line is $y = [3]x + [2]$. The third point of intersection (by substitution or trial and error) is $([1], [0])$, which is its own inverse, so $3P = ([1], [0])$.
(d) Since we ruled out 2 and 3, we know that P has order exactly 6. Then $3(2P) = \infty$ but $2(2P) \neq \infty$, so $2P$ has order 3, and $3P$ has order 2. The remaining points are $([0], [3]) = (2P)^\vee = 4P$ which has order 3 and $([3], [4]) = P^\vee = 5P$ which has order 6.

(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 $8P = \infty$.

(a) $\overline{E}_5 = \{(0, 1), (0, 4), (1, 1), (1, 4), (3, 0), (4, 1), (4, 4), \infty\}$.
(b) The order of $\overline{E}_5$ is 8, so by Lagrange, every element has order dividing 8, which implies even (whenever the order isn't 1).
(c) If the order of P is d and $d|8$, write $8 = de$; then $8P = deP = e(dP) = e\infty = \infty$.