CS/ECE/MATH 435: HOMEWORK 8, DUE NOV 9.

Consider the elliptic curve E given by the equation $y^2 = x^3 - x$ defined over the real numbers. Let $E(\mathbf{R})$ denote its set of points.

(a) Draw a picture of $E(\mathbf{R})$. If P is the point $(0, 0)$ in $E(\mathbf{R})$, what is $P + P$ (usually denoted $2P$)?

(b) For the remainder of this question, consider the elliptic curve $E : y^2 = x^3 - x$ defined over $\mathbf{Z}_p$, where p is an odd prime. If P is the point $(0, 0)$, what is $2P$? Find $3P$.

(c) Let $p = 5$. Find all points on the elliptic curve (don't forget its point at infinity). This set of points is denoted $E(\mathbf{Z}_p)$. Give its addition table.

(d) Suppose $p \pmod 4$ is 3. Assuming that $x^2 = -1 \pmod p$ has no solution (this follows since the order of x in $\mathbf{Z}_p^*$ divides the size, $p - 1$, of $\mathbf{Z}_p^*$, but you don't need to prove this), show that $E(\mathbf{Z}_p)$ contains exactly $p + 1$ points [hint: $x^3 - x$ is an odd function of x - consider what happens when you replace $x = a$ by $x = -a$. Together, how many points in $E(\mathbf{Z}_p)$ have x-coordinate a or $-a$, for a given a?].

(e) There is a powerful attack (the "MOV attack") that works best when the elliptic curve cryptosystem employs a point P whose order divides $p^k - 1$ for some k much smaller than p (it actually turns ECDLP in $E(\mathbf{Z}_p)$ into DLP in the multiplicative group of the field with p^k elements). Explain why this implies that an elliptic curve cryptosystem that uses $E : y^2 = x^3 - x$ defined over $\mathbf{Z}_p$ with $p \pmod 4 = 3$ is a poor idea.