1. Consider the elliptic curve \( E : y^2 = x^3 - x \) defined over \( \mathbb{R} \).
(a) Draw a picture of the curve. If \( P \) is the point \((0,0)\) in \( E(\mathbb{R}) \), what is \( P + P \) (usually denoted \( 2P \))?
(b) For the remainder of the question, consider the elliptic curve \( E : y^2 = x^3 - x \) defined over \( \mathbb{Z}_p \), 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). Give its addition table.
(d) Suppose \( p \pmod{4} = 3 \). Assuming that \( x^2 + 1 = 0 \pmod{p} \) has no solution (this follows from Lagrange’s theorem, which implies that the order of an element divides the size of the group), show that the elliptic curve group \( E(\mathbb{Z}_p) \) contains exactly \( p + 1 \) points [hint: \( x^3 - x \) is an odd function of \( x \) - consider whether neither, one, or both of \( x = a \) and \( x = -a \) can arise as the \( x \)-coordinate of a point on the curve].
(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 reduces ECDLP in \( E(\mathbb{Z}_p) \) to DLP in the multiplicative group of the field with \( p^k \) elements). Explain why an elliptic curve cryptosystem using \( E : y^2 = x^3 - x \) defined over \( \mathbb{Z}_p \) with \( p \pmod{4} = 3 \) may then be a bad idea.