CS 292F Elliptic Curve Cryptography
Winter Term 2017

Homework Assignment 04:

Consider the Koblitz curve $y^2 + xy = x^3 + x^2 + 1$ over GF(2^5). The field GF(2^5) is generated using the irreducible trinomial $p(\alpha) = \alpha^5 + \alpha^2 + 1$. The normal basis element is given as $\beta = \alpha^3 + \alpha$.

1. Compute the curve order.
2. Show that the point $P = (\alpha^2 + \alpha, \alpha^4)$ is on the curve.
3. Compute the normal representation of P.
4. Find the τ-adic expansion of 15.
5. Compute $[15]P$ in normal basis using τ-adic method.
6. Compute $[15]P$ in normal basis using standard point multiplication.

Due 5pm Tuesday March 7
Either, upload an electronic copy to the Dropbox link or bring a paper copy to the class. Electronic copy of your homework can be in Text or PDF. You could also scan/pdf your handwritten work; however, do not send low-resolution or small phone-camera images.