CS 292F Elliptic Curve Cryptography
Winter Term 2017

Homework Assignment 01:

1. Compute $19^{-1} \pmod{58}$ using the EEA.
2. Compute $25^{-1} \pmod{113}$ using the Fermat's method.
3. Compute $\phi(248)$ using the properties of Euler Phi Function.
4. Compute $23^{-1} \pmod{248}$ using the Euler's method.
5. Compute $23^{24} \pmod{31}$ by hand using binary exponentiation method.
6. Compute X using the Chinese remainder algorithm, such that X has the remainders $(1, 2, 3, 4)$ with respect to the moduli $(11, 13, 15, 17)$.
7. Find all primitive elements in the group $G = (Z_{23}^*, * \bmod 23)$.
8. Consider the field GF(2^6) with the irreducible polynomial $p(x) = x^6 + x + 1$. Perform the following operations:

$$\begin{aligned} (x^5 + x^2) &+ (x^4 + x^2 + x) \\ (x^5 + x^2) &\times (x^4 + x^2 + x) \end{aligned}$$

9. Show that an irreducible binomial of degree 4 over GF(2) does not exist by trying all possible candidates.
10. Solve for x in $x^2 = 239 \pmod{323}$, and find all square roots. Note that $323 = 17 \times 19$.

Due 5pm Thursday January 26
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.