Assignment 3

Policy: You may discuss problems with others, but all written work submitted must be your own. *You may not copy nor solicit solutions, complete or partial, from any source.*

1. (a) Find all the elements of $\mathbb{Z}_{22}^*$.

   (b) Find the permutation (reordering) of the elements of $\mathbb{Z}_{22}^*$ resulting from the function $x \to x^3 \mod 22$.

2. Consider the group Z_{23}^*, and its subgroup $G_{11} = \{x^2 \mod p : x \in Z_{23}^*\}$. Any non-identity element, such as $g = 4(= 2^2)$, is a generator of this group. Show this is the case for $g = 4$ by finding $4^1, 4^2, 4^3, \ldots, 4^{11} \mod 23$ in that order.

3. Describe a polynomial-time procedure that finds a "safe" prime (aka Sophie Germain prime) $p \in \tilde{\Pi}_n$ that fails with negligible probability. Use the assumption that there is a constant C such that for all n, $\tilde{\Pi}_n \geq \frac{2^n}{Cn^2}$.

4. Suppose we know that $x^{13} \equiv 3 \mod 77$.

   (a) Find $\Phi(77)$.

   (b) Use the Euclidean algorithm to find $d = 13^{-1} \mod \Phi(77)$.

   (c) Use d and the fast exponentiation procedure to find $x \mod 77$. Feel free to use computation to help with the multiplications/divisions, but otherwise show your work.

5. Let $N = pq$ where p and q are distinct primes.

   (a) Show how to solve for p and q with the knowledge of N and $\phi(N)$.

   (b) Use this method to factor $N = 477709$ with the knowledge that $\phi(N) = 476316$.

6. Prove Theorem 57.2 in the text.