Due date: March 14 (in the beginning of the class period)

It is ok to discuss solutions with other students but make sure to think about it first yourself. If you do discuss solutions, include a list of collaborators on your answer sheet. The writeup of the homework should be fully your own.

1. Find a primitive root of the prime 19. Find a number between 1 and 18 that is not a primitive root of 19

2. Find Let $p$ and $q$ be two distinct prime numbers. Find a formula for $\Phi(pq)$, where $\Phi$ is Euler’s $\Phi$-function ($\Phi(n)$ is the number of positive integers smaller than $n$ and coprime with $n$). Justify your answer.

3. Compute $563^{13532} \pmod{93}$. Show your work.

4. Compute $142^{2068} \pmod{77}$. Show your work.

5. Let $p$ be a prime and $g$ be a primitive root of $\mathbb{Z}_p$ (integers modulo $p$). Suppose that $x = a$ and $x = b$ are both integer solutions to the congruence $g^x \equiv h \pmod{p}$. Prove that $a \equiv b \pmod{p-1}$.

6. Let $p$ be a prime and $g$ be a primitive root of $\mathbb{Z}_p$. For $h$ such that $1 \leq h \leq (p-1)$, let $\log_g(h)$ denote the unique integer between 1 and $p-1$ such that $g^{\log_g(h)} \equiv h \pmod{p}$. (This is the discrete log of $h$ with respect to the primitive root $g$). Prove that for that for all $h_1, h_2$ such that $1 \leq h_1, h_2 \leq p-1$, 

$$\log_g(h_1h_2) \equiv \log_g(h_1) + \log_g(h_2) \pmod{p-1}$$