CS170 — Fall 2017— Homework 11 Solutions

Jonathan Sun, SID 25020651

0. Who Did You Work With?

Collaborators: Kevin Vo, Aleem Zaki, Jeremy Ou

1. True or False

For this question, I will do the first problem, which is:

Given a positive integer n, if for all $a \in \{1...n-1\}$ such that $(a, n) = 1$ we have that $a^{n-1} \equiv 1 \bmod n$ then this implies that n is a prime.

The statement above is false and I will justify this by giving a counter example. A counter example is to use a Carmichael number for n. This Carmichael number n is a composite number and a will be a number that is relatively prime to n. An example of this will be $n = 561$ and $a = 2$. $n = 561$ is a composite number because $561 = 3 \times 11 \times 17$ and $a = 2$ is relatively prime to 561 because it does not share any factors with 561 except for 1. Therefore, I will get:

$$2^{561-1} \equiv 1 \bmod 561$$
$$2^{560} \equiv 1 \bmod 561$$

Noting that $561 = 3 \times 11 \times 17$, the equation above is true because of the following:

- For 3 as the mod, $2^2 \equiv 1 \bmod 3$. So, $2^{560} = \left(2^2\right)^{280} \equiv 1^{280} \equiv 1 \bmod 3$.
- For 11 as the mod, $2^{10} \equiv 1 \bmod 11$. So, $2^{560} = \left(2^{10}\right)^{56} \equiv 1^{56} \equiv 1 \bmod 11$.
- For 17 as the mod, $2^{16} \equiv 1 \bmod 17$. So, $2^{560} = \left(2^{16}\right)^{35} \equiv 1^{35} \equiv 1 \bmod 17$.

Since $2^{560} \equiv 1 \bmod 3 \equiv 1 \bmod 11 \equiv 1 \bmod 17$, $2^{560} \equiv 1 \bmod 561$. Therefore, I have shown that $a^{n-1} \equiv 1 \bmod n$ for $a = 2$ and $n = 561$. However, the statement also says that n should also be a prime. This is not the case because $n = 561 = 3 \times 11 \times 17$. Therefore, I have shown that the statement is False.

2. Proof

Given two primes p and q and an a such that $(a, pq) = 1$, I can show that $a^{(p-1)(q-1)} \equiv 1 \bmod pq$ by letting $n = pq$ so that $a^{(p-1)(q-1)} \equiv 1 \bmod n$ such that $(a, n) = 1$.

- For p as the mod, $a^{(p-1)(q-1)} = \left(a^{p-1}\right)^{q-1}$. From Fermat's Little Theorem, we know that $a^{p-1} \equiv 1 \bmod p$ so $\left(a^{p-1}\right)^{q-1} \equiv 1^{q-1} \equiv 1 \bmod p$. Therefore, $a^{(p-1)(q-1)} \equiv 1 \bmod p$.
- For q as the mod, $a^{(p-1)(q-1)} = \left(a^{q-1}\right)^{p-1}$. From Fermat's Little Theorem, we know that $a^{q-1} \equiv 1 \bmod q$ so $\left(a^{q-1}\right)^{p-1} \equiv 1^{p-1} \equiv 1 \bmod q$. Therefore, $a^{(p-1)(q-1)} \equiv 1 \bmod q$.

So, we get that $a^{(p-1)(q-1)} \equiv 1 \bmod p$ and $a^{(p-1)(q-1)} \equiv 1 \bmod q$. Therefore, by the Chinese Remainder Theorem, there must exist an unique solution for $a^{(p-1)(q-1)} \bmod pq$ and since $a^{(p-1)(q-1)} \equiv 1 \bmod pq$ is a solution, this must also be unique. Therefore, I have shown that $a^{(p-1)(q-1)} \equiv 1 \bmod pq$.