University of Sydney

MATH 2988

Number Theory and Cryptography

Assignment 1

Author: Keegan Gyoery
SID: 470413467

Lecturer: Dzmitry Badziahin
Tutorial: Carslaw Tutorial Room 451
Thursday 12pm

September 7, 2017

1. (a) We are required to find $2015^{24195} \pmod{2017}$. In order to compute this, we will use the fact that 2017 is prime. The computation is thus as follows.

$$\begin{aligned}
a^{\varphi(p)} &\equiv 1 \pmod{p} \\
\therefore a^{p-1} &\equiv 1 \pmod{p} \\
\therefore 2015^{2017-1} &\equiv 1 \pmod{2017} \\
\therefore 2015^{2016} &\equiv 1 \pmod{2017} \\
24195 &= 2016 \times 12 + 3 \\
\therefore 2015^{24195} &= 2015^{2016\times 12+3} \\
&= \left(2015^{2016}\right)^{12}\left(2015^{3}\right) \\
\therefore 2015^{24195} &\equiv \left(2015^{2016}\right)^{12}\left(2015^{3}\right) \pmod{2017} \\
&\equiv \left(2015^{3}\right) \pmod{2017} \quad \text{as } 2015^{2016} \equiv 1 \pmod{2017} \\
&\equiv (-2)^3 \pmod{2017} \\
&\equiv -8 \pmod{2017} \\
&\equiv 2009 \pmod{2017} \\
\therefore 2015^{24195} &\equiv 2009 \pmod{2017}
\end{aligned}$$

(b) For the next proof, let $m,\ n \in \mathbb{Z}^+$, and $m,\ n$ be coprime, that is $\gcd(m,n) = 1$. Furthermore, $a \in \mathbb{Z}$, and $\gcd(a, mn) = 1$. Thus we have $\gcd(a,m) = 1$ and $\gcd(a,n) = 1$. We are now required to prove that the following is true.

$$a^{\operatorname{lcm}(\phi(m),\phi(n))} \equiv 1 \pmod{mn}$$

In order to complete this proof, we must first examine the result of $\operatorname{lcm}(\phi(m), \phi(n))$. The $\operatorname{lcm}(\phi(m), \phi(n))$ may be written as a multiple of either $\phi(m)$ or $\phi(n)$. Thus the following result is true.

$$\begin{aligned}
\operatorname{lcm}(\phi(m), \phi(n)) &= k_1\phi(m) \\
&= k_2\phi(n) \qquad k_1,\ k_2 \in \mathbb{Z}^+
\end{aligned}$$

Using the Euler-Fermat Theorem, the result is derived in the proof that follows.

$$\begin{aligned}
a^{\phi(m)} &\equiv 1 \pmod{m} \\
\therefore \left[a^{\phi(m)}\right]^{k_1} &\equiv 1 \pmod{m} \\
\therefore a^{k_1\phi(m)} &\equiv 1 \pmod{m} \quad \text{as } \gcd(a,m) = 1 \\
\therefore a^{\operatorname{lcm}(\phi(m),\phi(n))} &\equiv 1 \pmod{m} \ldots\ldots (1) \\
a^{\phi(n)} &\equiv 1 \pmod{n} \\
\therefore \left[a^{\phi(n)}\right]^{k_2} &\equiv 1 \pmod{n} \\
\therefore a^{k_2\phi(n)} &\equiv 1 \pmod{n} \quad \text{as } \gcd(a,n) = 1 \\
\therefore a^{\operatorname{lcm}(\phi(m),\phi(n))} &\equiv 1 \pmod{n} \ldots\ldots (2) \\
\therefore a^{\operatorname{lcm}(\phi(m),\phi(n))} &\equiv 1 \pmod{mn} \quad \text{by the CRT on equations (1) and (2)}
\end{aligned}$$

Thus the required result is proved. Note that CRT means Chinese Remainder Theorem.

We are now required to show that for any a coprime to 10, the following result holds.

$$a^{20} \equiv 1 \pmod{100}$$

Thus we shall select $m = 25$ and $n = 4$. Thus, by our selection of m and n, the $\gcd(m, n) = 1$, and thus the derivation is as follows.

$$\begin{aligned}
a^{\operatorname{lcm}(\phi(m),\phi(n))} &\equiv 1 \pmod{nm}\\
\therefore a^{\operatorname{lcm}(\phi(25),\phi(4))} &\equiv 1 \pmod{100}\\
\therefore a^{\operatorname{lcm}\left(\phi(5^2),\phi(2^2)\right)} &\equiv 1 \pmod{100}\\
\therefore a^{\operatorname{lcm}\left(5^2-5,2^2-2\right)} &\equiv 1 \pmod{100}\\
\therefore a^{\operatorname{lcm}(20,2)} &\equiv 1 \pmod{100}\\
\therefore a^{20} &\equiv 1 \pmod{100}
\end{aligned}$$

(c) We are now required to compute the last two digits of the numbers 7^{7^4} and $7^{7^{400}}$. In order to do this, we shall compute the above two numbers $\pmod{100}$. Furthermore, we have the result that, for a coprime to 10, $a^{20} \equiv 1 \pmod{100}$. As 7 is coprime to 10, the previous result holds.

Firstly we shall find the result of $7^{7^4} \pmod{100}$. The computation is as follows.

$$\begin{aligned}
7^4 &= 2401\\
&= 20 \times 120 + 1\\
\therefore 7^4 &= 20 \times 120 + 1\\
\therefore 7^{7^4} &= 7^{20\times120+1}\\
&= \left[7^{20\times120}\right]7\\
&= \left[\left(7^{20}\right)^{120}\right]7\\
\therefore \left[\left(7^{20}\right)^{120}\right]7 &\equiv 7 \pmod{100} \quad \text{as } 7^{20} \equiv 1 \pmod{100}\\
\therefore 7^{7^4} &\equiv 7 \pmod{100}
\end{aligned}$$

As a result the last two digits of 7^{7^4} are 07.

Finally, we shall find the result of $7^{7^{400}} \pmod{100}$. The computation is as follows.

$$\begin{aligned}
\therefore 7^{400} &= 7^{20^{20}}\\
\therefore 7^{20^{20}} &\equiv 1 \pmod{100} \quad \text{as } 7^{20} \equiv 1 \pmod{100}\\
\therefore 7^{400} &= 100q + 1 \quad \text{for some } q \in \mathbb{Z}^+\\
\therefore 7^{7^{400}} &= 7^{100q+1}\\
&= \left[7^{100q}\right]7\\
&= \left[7^{20\times5q}\right]7\\
&= \left[\left(7^{20}\right)^{5q}\right]7\\
\therefore \left[\left(7^{20}\right)^{5q}\right]7 &\equiv 7 \pmod{100} \quad \text{as } 7^{20} \equiv 1 \pmod{100}\\
\therefore 7^{7^{400}} &\equiv 7 \pmod{100}
\end{aligned}$$

As a result the last two digits of $7^{7^{400}}$ are 07.

2. (a) For the following proof we are given that $p = 737279$ is prime, and that the following result holds.

$$2^{2p+1} \equiv 2 \pmod{2p+1}$$

As a result of the $\gcd(2, 2p+1) = 1$, we have the following result.

$$\begin{aligned} 2^{2p+1} &\equiv 2 \pmod{2p+1} \\ \therefore 2^{2p} &\equiv 1 \pmod{2p+1} \end{aligned}$$

Thus, $\operatorname{ord}_{2p+1} 2$ must divide $2p$. Thus, as p is prime, $\operatorname{ord}_{2p+1} 2$ can equal 1, 2, p, $2p$. The first two options for the $\operatorname{ord}_{2p+1} 2$ yeild the following results.

$$\begin{aligned} 2^1 &\equiv 2 \pmod{2p+1} \\ 2^2 &\equiv 4 \pmod{2p+1} \end{aligned}$$

Thus, $\operatorname{ord}_{2p+1} 2$ can only equal p or $2p$. Furthermore, we have the known result that $\operatorname{ord}_{2p+1} 2 \mid \phi(2p+1)$. Thus, as $0 < \phi(2p+1) < 2p+1$, and $\operatorname{ord}_{2p+1} 2 \mid \phi(2p+1)$, $\phi(2p+1)$ can either equal p or $2p$. Assume that $\phi(2p+1) = p$. Thus, $\phi(2p+1)$ must be odd as p is prime.

Proposition. For $n > 2$, $\phi(n)$ must be even.

Proof. By the definition of Euler's Phi Function, $\phi(n)$ is the size of the reduced set of residues modulo n. The reduced set of residues modulo n is defined by $\{a \in \mathbb{Z} \mid 0 \leq a < n\ ,\ \gcd(a, n) = 1\}$. Let $n \in \mathbb{Z}^+$ and set $n > 2$. Thus n can be decomposed into its prime factors, which will contain either at least one odd prime factor, or be a power of 2.

Considering the first case, where n contains an odd factor, we can decompose $n = q \cdot p^k$, for some prime factor $p \in \mathbb{Z}^+$, and $q,\ k \in \mathbb{Z}^+$. Then,

$$\begin{aligned} \phi(n) &= \phi\left(q \cdot p^k\right) \\ &= \phi(q)\phi(p^k) \\ &= \left(p^k - p^{k-1}\right)\phi(q) \\ &= (p-1)\left(p^{k-1}\right)\phi(q) \end{aligned}$$

As p is odd, the factor $(p-1)$ is even, thus making $\phi(n)$ even.

Considering the second and final case, where n is a power of 2, and thus contains no odd prime factors, we can write $n = 2^r$, for some $r \in \mathbb{Z}^+$. Then,

$$\begin{aligned} \phi(n) &= \phi\left(2^r\right) \\ &= 2^r - 2^{r-1} \\ &= (2-1)\left(2^{r-1}\right) \\ &= 2^{r-1} \end{aligned}$$

Obviously, $\phi(n)$ contains a factor of 2, thus making $\phi(n)$ even.

Thus Euler's Phi Function, $\phi(n)$ is even $\forall n \in \mathbb{Z}^+$ and $n > 2$.

As a result of this proof, we have contradicted our choice of $\phi(2p+1) = p$, as $\phi(2p+1)$ must be even, and p is clearly odd. Thus, $\phi(2p+1) = 2p$. This result of Euler's Phi Function holding a value, $2p$, that is one less than the given value, $2p+1$, is a result that only holds when the given value is prime. Thus, $2p+1$ is clearly prime.

(b) For the following proof, let $n = 2^{131} - 1$. We are now required to show that the following result is true.

$$2^{n-1} \equiv 1 \pmod{n}$$

Using the following proof, and the fact that 131 is prime, we will derive the required result.

$$\begin{aligned}
2^{130} &\equiv 1 \pmod{131} \quad \text{as 131 prime} \\
\therefore 2^{130} - 1 &\equiv 0 \pmod{131} \\
\therefore 2\left[2^{130} - 1\right] &\equiv 0 \pmod{131} \\
\therefore 2^{131} - 2 &\equiv 0 \pmod{131} \\
\therefore n - 1 &\equiv 0 \pmod{131} \\
\therefore 131 &\mid n - 1 \\
\therefore n - 1 &= 131k \quad \text{for some } k \in \mathbb{Z}^+ \\
2^{131} - 1 &\equiv 0 \pmod{2^{131} - 1} \\
\therefore 2^{131} &\equiv 1 \pmod{2^{131} - 1} \\
\therefore \left[2^{131}\right]^k &\equiv 1 \pmod{2^{131} - 1} \\
\therefore 2^{131k} &\equiv 1 \pmod{2^{131} - 1} \\
\therefore 2^{n-1} &\equiv 1 \pmod{n}
\end{aligned}$$

Thus the required result is achieved.

(c) We are now required to show that 263 divides $n = 2^{131} - 1$, meaning that n is not in fact prime. In order to achieve the final result, we shall start with the following known fact.

$$131 = 2^7 + 2^1 + 2^0$$

Using this result and the summing of squares, we are able to compute the following results.

$$\begin{aligned}
131 &= 2^7 + 2^1 + 2^0 \\
2^{131} &= 2^{\left[2^7 + 2^1 + 2^0\right]} \\
\therefore 2^{131} &= 2^{2^7} 2^{2^1} 2^{2^0} \\
\therefore 2^{131} &\equiv 2^{2^7} 2^{2^1} 2^{2^0} \pmod{263}
\end{aligned}$$

In order to compute the congruence of the RHS of the above congruence relation, we must compute the congruence of each of the terms in the RHS. To do so, we will use a table to easily compute the results. Furthermore, using the relation that $a_{n+1} = {a_n}^2$, to compute the congruences $\pmod{263}$. The computations are fairly simple and straightforward.

n	0	1	2	3	4	5	6	7
2^{2^n}	2	4	16	-7	49	34	104	33

Thus, using the above table for the successive squares congruences, we get the following results.

$$\begin{aligned}
\therefore 2^{131} &\equiv 2^{2^7} 2^{2^1} 2^{2^0} \pmod{263} \\
&\equiv 33 \cdot 4 \cdot 2 \pmod{263} \\
&\equiv 264 \pmod{263} \\
&\equiv 1 \pmod{263} \\
\therefore 2^{131} &\equiv 1 \pmod{263} \\
\therefore 2^{131} - 1 &\equiv 0 \pmod{263} \\
\therefore 263 &\mid 2^{131} - 1
\end{aligned}$$

Thus 263 divides $n = 2^{131} - 1$, and thus n is not prime.