Homework 4

Michael Pham

Spring 2023

Contents

0 Sundry

I worked alone on this homework.

1 Fermat's Little Theorem

Problem 1.1. Without using induction, prove that for all natural numbers m, $m^{13}-m$ is divisible by 130.

Solution. The problem is asking us to show that $m^{13}-m \equiv 0 \pmod{130}$.

Now, we observe that by Fermat's Little Theorem, we have that $m^{13} \equiv m \pmod{13}$. In other words, $m^{13}-m \equiv 0 \pmod{13}$.

Next, we see that $m^{13}-m = m(m^{12}-1)$. Now, we observe that there are two cases:

1. m is coprime to 2.
2. m is not coprime to 2.

In the first case, by Fermat's Little Theorem, we see that $m^{12}-1 = (m^1)^{12}-1 \equiv 0 \pmod{2}$. Then, we see that $m^{13}-m = m(m^{12}-1) \equiv 0 \pmod{2}$.

In the second case, since m is not coprime to 2, then it must mean that $m \equiv 0 \pmod{2}$, which then implies that $m^{13}-m = m(m^{12}-1) \equiv 0 \pmod{2}$.

Then, we see that in both cases, $m^{13}-m \equiv 0 \pmod{2}$.

Finally, observe that we can rewrite $m^{12}-1$ as $(m^4)^3-1$. Once again, we consider two cases:

1. m is coprime to 5.
2. m is not coprime to 5.

In the first case, by Fermat's Little Theorem, we have that $m^{13}-m = m((m^4)^3-1) \equiv 0 \pmod{5}$.

In the second case, we see that since m is not coprime to 5, then $m \equiv 0 \pmod{5}$. Therefore, $m^{13}-m = m\left((m^4)^3-1\right) \equiv 0 \pmod{5}$.

In both cases, we see that $m^{13}-m \equiv 0 \pmod{5}$.

Now, since we have that $m^{13}-m \equiv 0 \pmod{13}$, $m^{13}-m \equiv 0 \pmod{5}$, and $m^{13}-m \equiv 0 \pmod{2}$, then we can conclude that $m^{13}-m \equiv 0 \pmod{130}$. ■

2 Euler's Totient Function

Euler's Totient Function is defined as follows:

$$\phi(n) = |\{i : 1 \leq i \leq n, \gcd(n, i) = 1\}|$$

In other words, $\phi(n)$ is the total number of positive integers less than or equal to n which are relatively prime to it. We develop a general formula to compute $\phi(n)$.

Problem 2.1. Let p be a prime number. What is $\phi(p)$?

Solution. We see that $\phi(p) = |\{1, \ldots, p\} \setminus \{p\}| = p - 1$ if p is a prime number. ■

Problem 2.2. Let p be a prime number and k some positive integer. What is $\phi(p^k)$?

Solution. We observe that $\phi(p^k) = |\{1, \ldots, p^k\} \setminus \{m : m \leq p^k, m \equiv 0 \pmod{p}\}| = p^k - p^{k-1}$. This can then be rewritten as $p^k(1 - p^{-1}) = p^k(\frac{p-1}{p})$. ■

Problem 2.3. Show that if $\gcd(a, b) = 1$, then $\phi(ab) = \phi(a)\phi(b)$.

Solution. To begin with, let us define the following sets:

- $S_{ab} = \{i : 1 \leq i \leq ab, \gcd(ab, i) = 1\}$
- $S_a = \{i : 1 \leq i \leq a, \gcd(a, i) = 1\}$
- $S_b = \{i : 1 \leq i \leq b, \gcd(b, i) = 1\}$

Now, we observe that $|S_{ab}| = \phi(ab)$, and $|S_a \times S_b| = \phi(a)\phi(b)$. Our goal now is to show that the cardinality of S_{ab} is equal to $S_a \times S_b$. To do this, we will construct a bijection between the two sets.

To do this, let us define a function $f : S_{ab} \to S_a \times S_a$, where $f(x) = (x \pmod{a}, x \pmod{b})$.

Next, we see that, by definition, for $x \in S_{ab}$, $\gcd(x, ab) = 1$, as S_{ab} is the set of positive coprime integers less than or equal to n. Now, as $\gcd(x, ab) = 1$, then it follows that $\gcd(x, a) = 1 = \gcd(x, b)$. This then also implies that $\gcd(x \pmod{a}, a) = 1 = \gcd(x \pmod{b}, b)$.

With this, we see that our function f gives us an ordered pair whose first element x_1 is coprime to a and the second element x_2 is coprime to b, along with the fact that $1 \leq x_1 \leq a$ and $1 \leq x_2 \leq b$. In other words, our function yields us an ordered pair in the set $S_a \times S_b$.

From here, we observe that since $\gcd(a, b) = 1$, then for some m where $0 \leq m < a$ and $\gcd(m, a) = 1$, along with some n where $0 \leq n < b$ and $\gcd(n, b) = 1$, the following system

$$\begin{aligned} x &\equiv m \pmod{a} \\ x &\equiv n \pmod{b} \end{aligned}$$

has a solution x' which is unique $\pmod{ab}$ by the Chinese Remainder Theorem. In other words, we see that for every $m : \gcd(m, a) = 1$ and $n : \gcd(n, b) = 1$ (meaning they are within the set $S_a \times S_b$), there exists a unique x which is in the set S_{ab} which maps to it.

This then means that there is a bijection between S_{ab} and $S_a \times S_b$. In other words, the size of the two sets must be the same, and thus $\phi(ab) = \phi(a)\phi(b)$. ■

Problem 2.4. Argue that if the prime factorisation of $n = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$, then

$$\phi(n) = n \prod_{i=1}^{k} \frac{p_i - 1}{p_i}$$

Solution. We observe that since $\phi(ab) = \phi(a)\phi(b)$, then we can rewrite $\phi(n)$ as

$$\begin{aligned}
\phi(n) &= \phi(p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}) \\
&= \phi(p_1^{e_1})\phi(p_2^{e_2}) \cdots \phi(p_k^{e_k}) \\
&= p_1^{e_1}\left(\frac{p_1 - 1}{p_1}\right) p_2^{e_2}\left(\frac{p_2 - 1}{p_2}\right) \cdots p_k^{e_k}\left(\frac{p_k - 1}{p_k}\right) \\
&= (p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k})\left(\frac{p_1 - 1}{p_1}\right)\left(\frac{p_2 - 1}{p_2}\right) \cdots \left(\frac{p_k - 1}{p_k}\right) \\
&= n \prod_{i=1}^{k} \frac{p_i - 1}{p_i}
\end{aligned}$$

■

3 Euler's Totient Theorem

Euler's Totient Theorem states that if n and a are coprime, then

$$a^{\phi(n)} \equiv 1 \pmod{n}$$

where $\phi(n)$ is the number of positive integers less than or equal to n which are coprime to n (including 1).

Problem 3.1. Let the numbers less than n which are coprime to n be $m_1, m_2, \ldots, m_{\phi(n)}$. Argue that the set

$$\{am_1, am_2, \ldots, am_{\phi(n)}\}$$

is a permutation of the set

$$\{m_1, m_2, \ldots, m_{\phi(n)}\}.$$

In other words, prove that

$$f : \{m_1, m_2, \ldots, m_{\phi(n)}\} \to \{m_1, m_2, \ldots, m_{\phi(n)}\}$$

is a bijection, where $f(x) := ax \pmod{n}$.

Solution. We shall proceed by contradiction.

Suppose that we have a function $f : \{m_1, m_2, \ldots, m_{\phi(n)}\} \to \{m_1, m_2, \ldots, m_{\phi(n)}\}$, where $f(x) := ax \pmod{n}$. Also, observe that a is coprime to n.

Now, suppose for contradiction that there exists distinct x and x' in $\{m_1, m_2, \ldots, m_{\phi(n)}\}$ such that $ax \equiv ax' \pmod{n}$.

Since a and n are coprime to each other, we know that there must exist a multiplicative inverse a^{-1} such that $a(a^{-1}) \equiv 1 \pmod{n}$.

With this in mind, by multiplying both sides by a^{-1}, we get $x \equiv x' \pmod{n}$. However, this is a contradiction as this means that x and x' are not distinct. Therefore, we can conclude that f must be a bijection. ■

Problem 3.2. Prove Euler's Totient Theorem.

Solution. We now want to prove that $a^{\phi(n)} \equiv 1 \pmod{n}$.

Suppose we take the product of all the numbers in the set $S = \{am_1, am_2, \ldots, am_{\phi(n)}\}$, yielding us $am_1 \times am_2 \times \cdots \times am_{\phi(n)} \equiv a^{\phi(n)}m \pmod{n}$, where $m = am_1(am_2)\cdots(am_{\phi(n)})$.

Then, take the product of all the numbers in $S' = \{m_1, m_2, \ldots, m_{\phi(n)}\}$, yielding us $m \pmod{n}$.

Now, from Problem 3.1, we know that since S is a permutation of S', then it follows that $a^{\phi(n)}m \equiv m \pmod{n}$. Now, since m is the product of all the numbers less than n which are coprime to it, then we know that $\gcd(m, n) = 1$, meaning that there exists a multiplicative inverse m^{-1} such that $m(m^{-1}) \equiv 1 \pmod{n}$. Then, by multiplying both sides by m^{-1}, we get the following:

$$a^{\phi(n)} \equiv 1 \pmod{n}$$

Therefore, we can conclude that Euler's Totient Theorem is true. ■

4 Sparsity of Primes

Problem 4.1. A prime power is a number that can be written as p^i for some prime p and some positive integer i. So, $9 = 3^2$ is a prime power, and so is $8 = 2^3$. $42 = 2 \cdot 3 \cdot 7$ is not a prime power.

Prove that for any positive integer k, there exists k consecutive positive integers such that none of them are prime powers.

Solution. The problem is essentially asking us to find some n such that $n+1, n+2, \ldots, n+k$ are all not powers of primes. In other words, each of them are divisible by two different primes.

Now, since there are an infinite number of primes then, from this observation, we consider the first $2k$ primes p_i for $i = 1, \ldots, 2k$, which are all distinct from each other, pairing them up such that we get the following:

$$\begin{aligned} n+1 &\equiv 0 \pmod{p_1 p_2} \\ n+2 &\equiv 0 \pmod{p_3 p_4} \\ &\vdots \\ n+k &\equiv 0 \pmod{p_{2k-1} q_{2k}} \end{aligned}$$

This then implies the following:

$$\begin{aligned} n &\equiv -1 \pmod{p_1 p_2} \\ n &\equiv -2 \pmod{p_3 q_4} \\ &\vdots \\ n &\equiv -k \pmod{p_{2k-1} q_{2k}} \end{aligned}$$

Then, from here, we observe that $p_1 p_2, p_3 p_4, \ldots, p_{2k-1} p_{2k}$ are all co-prime to each other as they share no common factors. Then, by the Chinese Remainder Theorem, it is guaranteed for there to be some n which satisfies the system of k congruence equations, meaning that for any positive integer k, there exists k consecutive positive integers such that none of them are prime powers. ■

5 RSA Practice

Consider the following RSA schemes and solve for asked variables.

> **Problem 5.1.** Assume for an RSA scheme we pick 2 primes, $p = 5$ and $q = 11$ with encryption key $e = 9$. Calculate the exact value of the decryption key d.

Solution. The decryption key d is the inverse multiplicative of $e \pmod{(p-1)(q-1)}$.

First, we want to find $(p-1)(q-1)$, which is $(5-1)(11-1) = (4)(10) = 40$.

From here, we want to find the inverse multiplicative of $9 \pmod{40}$. Using the Extended Euclidean Algorithm, we get the following:

$$\begin{array}{rl}
40 = 4(9) + 4 & p_0 = 0 \\
9 = 2(4) + 1 & p_1 = 1 \\
4 = 4(1) + 0 & p_2 = 0 - 1(2) \pmod{40} = -2 \pmod{4} \equiv 38 \pmod{40} \\
 & p_3 = 1 - 38(4) \pmod{40} = -151 \pmod{40} \equiv 9 \pmod{40}
\end{array}$$

Then, we see that $d = 9$. To confirm, we observe that $9(9) \pmod{40} = 81 \pmod{40} \equiv 1 \pmod{40}$. Thus, $d = 9$ is indeed the multiplicative inverse of $e \pmod{(p-1)(q-1)} = 9 \pmod{40}$. ■

> **Problem 5.2.** If the receiver gets 4, what was the original message?

Solution. In order to find the original message x which the receiver gets, we compute the following:

$$\begin{aligned}
x &\equiv 4^9 \pmod{55} \\
&\equiv (4^3)^3 \pmod{55} \\
&\equiv 64^3 \pmod{55} \\
&\equiv 9^3 \pmod{55} \\
&\equiv 9(9^2) \pmod{55} \\
&\equiv 9(81) \pmod{55} \\
&\equiv 9(26) \pmod{55} \\
&\equiv 9(13)(2) \pmod{55} \\
&\equiv 117(2) \pmod{55} \\
&\equiv 7(2) \pmod{55} \\
&\equiv 14 \pmod{55}
\end{aligned}$$

Thus, the original message x is 14. ■

Problem 5.3. Encode your answer from Problem 5.2 to check its correctness.

Solution. The encoded message is:

$$\begin{aligned}
14^9 &\equiv 14(14^2)(14^2)(14^2)(14^2) \pmod{55} \\
&\equiv 14(196)(196)(196)(196) \pmod{55} \\
&\equiv 7(2)(31)(31)(31)(31) \pmod{55} \\
&\equiv 7(62)(31)(31)(31) \pmod{55} \\
&\equiv 7(7)(31)(31)(31) \pmod{55} \\
&\equiv 217(217)(31) \pmod{55} \\
&\equiv 52(52)(31) \pmod{55} \\
&\equiv 2(2)(13)(52)(31) \pmod{55} \\
&\equiv 2(13)(104)(31) \pmod{55} \\
&\equiv 2(13)(49)(31) \pmod{55} \\
&\equiv 13(98)(31) \pmod{55} \\
&\equiv 13(43)(31) \pmod{55} \\
&\equiv (430+129)(31) \pmod{55} \\
&\equiv (45+19)(31) \pmod{55} \\
&\equiv 9(31) \pmod{55} \\
&\equiv 3(3)(31) \pmod{55} \\
&\equiv 3(93) \pmod{55} \\
&\equiv 3(38) \pmod{55} \\
&\equiv 114 \pmod{55} \\
&\equiv 4 \pmod{55}
\end{aligned}$$

And from here, we see that the message becomes encoded to 4, which is precisely the message which was received in Problem 5.2. ■

6 Tweaking RSA

You are trying to send a message to your friend, and as usual, Eve is trying to decipher what the message is. However, you get lazy, so you use $N = p$, and p is prime. Similar to the original method, for any message $x \in \{0, 1, \ldots, N-1\}$, $E(x) \equiv x^e \pmod{N}$, and $D(y) \equiv y^d \pmod{N}$.

Problem 6.1. Show how you choose e and d in the encryption and decryption function, respectively. Prove that the message x is recovered after it goes through your new encryption and decryption functions, $E(x)$ and $D(y)$.

Solution. We choose e to be some number which is relatively prime to $p-1$, and d to be the inverse multiplicative of $e \pmod{p-1}$.

Now, we want to prove that x is recovered it goes through our new encryption and decryption functions. That is, $D(E(x)) = (x^e)^d \equiv x \pmod{p}$.

First, we shall consider the exponent, ed. We observe that, as d is the multiplicative inverse of e, then $ed \equiv 1 \pmod{p-1}$. In other words, we can express ed as $ed = 1 + k(p-1)$ for $k \in \mathbb{Z}$.

From here, we see that $x^{ed} - x = x^{1+k(p-1)} - x = x(x^{k(p-1)} - 1)$. With this in mind, we want to now show that this expression mod p is equal to zero. To do this, let us consider the two cases:

1. x is a multiple of p.
2. x is not a multiple of p.

In the first case, we observe that since x is a multiple of p, then we see that $x \equiv 0 \pmod{p}$ and $x^{ed} \equiv 0 \pmod{p}$. Therefore, the expression $x^{ed} - x \equiv 0 \pmod{p}$, as desired.

In the second case, we see that by Fermat's Little Theorem, we know that $x^{p-1} \equiv 1 \pmod{p}$, as p is a prime number. Then, we see that $x^{k(p-1)} \equiv 1^k \equiv 1 \pmod{p}$. It then follows that $x^{k(p-1)} - 1 \equiv 0 \pmod{p}$, and thus the expression is equivalent to $0 \pmod{p}$.

Therefore, we see that the message x is recovered after it goes through our new encryption and decryption functions. ■

Problem 6.2. Can Eve now compute d in the decryption function? If so, by what algorithm?

Solution. Yes, Eve can still compute d in the decryption function. This can be done using the Extended Euclidean Algorithm in order to find the inverse of $e \pmod{p-1}$. ■

Problem 6.3. Now you wonder if you can modify the RSA encryption method to work with three primes ($N = pqr$ where p, q, r are all prime). Explain how you can do so, and include a proof of correctness showing that $D(E(x)) = x$.

Solution. For $N = pqr$, where p, q, r are all primes, we can let e be some number which is relatively prime to $(p-1)(q-1)(r-1)$. Then, we let d be the multiplicative inverse of $e \pmod{(p-1)(q-1)(r-1)}$.

From here, we define our encryption function $E(x)$ as $E(x) \equiv x^e \pmod{N}$ and our decryption function $D(y)$ as $D(y) \equiv y^d \pmod{N}$.

Now, we want to show that $D(E(x)) = x$. In otherwords, $(x^e)^d \equiv x \pmod{N}$.

First, we consider the exponent ed. As d is a multiplicative inverse of e then, by definition, $ed \equiv 1 \pmod{(p-1)(q-1)(r-1)}$. Therefore, for some $k \in \mathbb{Z}$, we have that $ed = 1 + k(p-1)(q-1)(r-1)$.

Now, from here, we observe that $x^{ed} - x = x^{1+k(p-1)(q-1)(r-1)} - x = x(x^{k(p-1)(q-1)(r-1)} - 1)$.

To show that $D(E(x)) = x$, we want to show that the expression above is equal to $0 \pmod{N}$. To do this, we observe the following two cases:

1. x is a multiple of p.
2. x is not a multiple of p.

In the first case, by inspection we can see that if x is a multiple of [], then it follows that $x(x^{k(p-1)(q-1)(r-1)}) - 1) \equiv 0 \pmod{N}$, as it has a factor that's a multiple of p.

In the second case, we first observe that $x^{(p-1)} \equiv 1 \pmod{p}$ by Fermat's Little Theorem, as p is prime. It then follows that $x^{k(p-1)(q-1)(r-1)} - 1 \equiv 0 \pmod{p}$. Then, the expression will also be equivalent to $0 \pmod{p}$.

Now, by a symmetrical argument, $x(x^{k(p-1)(q-1)(r-1)})$ is also divisible by q and r. Then, we observe that since p, q, r are all primes, then the expression must be divisible by their product $N = pqr$ as well. Then, we see that the expression is equivalent to $0 \pmod{N}$, which is our claim.

Therefore, we can conclude that $D(E(x)) = x$. ■