MATH 187A - Final Reflection

1. *Cool Idea: RSA*

RSA is a system that can be used to exchange encrypted messages. Generally, these systems are explained through the perspective of 2 people, Alice and Bob, who want to securely communicate. Additionally, there may be a 3rd malicious actor named Eve.

The process starts with Bob generating and sharing a "public key", which is a pair of integer values (n, e). Bob will also have "private key", (d) that will be generated in the process that he will NOT be sharing. These values are computed with restraints in place and hold certain modular properties.

- n is a product of 2 large distinct primes (p, q)
    - $\phi(n) = (p-1)(q-1)$ can be considered a special variable for now
- d is a value "co-prime" to $\phi(n)$, i.e. whose greatest common divisor is 1 (a.k.a. not a factor of $\phi(n)$)
- e is a value generated using d which exhibits the modular property that $e \times d \equiv 1$ mod($\phi(n)$)

The "public key" is available for all to see.

Alice must "encode" her message so that it can be represented as an integer between 0 and n-1 (inclusive). Alice can then "encrypt" her encoded message using Bob's shared "public key" (e, n). The encrypted ciphertext would be generated as $c = m^e$ mod n, which Alice would send back to Bob.

Once Bob receives the ciphertext, he can decrypt the encrypted message using his "private key" (d) to obtain the original message: $m = c^d$ mod n.

Due to the constraints under which these values were generated, Alice will have an easy time generating encrypted ciphertexts and Bob will have an easy time decrypting them. Eve, however, even with knowledge of the "public key" and Alice's encrypted ciphertext, will have a HARD time decrypting. The underlying principle upon which this is built is the difficulty of prime factorizing large numbers.

I liked the RSA section because of the way it brought everything together and how it just clicked for me.

I had always:

- heard OF RSA
- generally knew that the ease of calculation relied on modular exponentiation rules
- generally knew the difficulty of "breaking" it was equated to the difficulty of prime factorizing large numbers

But I only ever heard a "pop-science" style explanation of how this stuff works with generic terms like "one-way functions" or analogies to mailboxes.

Focusing on the underlying mathematical foundations, working out exercises by hand, & writing up an implementation of RSA encryption and decryption (albeit working with very small numbers) finally pulled the veil of abstraction that had always clouded my vision of this concept.

2. *Persistance: W8DiscQ2Proof*

During Week 8's Wednesday Discussion, there was a proof question that asked us to prove the following:

Given:

- integers (a, m, x, y)
- gcd(a, m) = 1
- x = y mod $\phi(m)$

Implies:

- $a^x \equiv a^y$ mod m

At first, I wasn't completely sure what we were even being asked nor where to start. Thankfully, the TA started us off with some example problems to get a feel for statement:

Finding the last 3 digits of 7^{803} can be rephrased as finding 7^{803} mod 1000.

Since we know that 7 is co-prime to 1000 (gcd(7, 1000) = 1), we can rewrite 7^{803} as a much simpler expression using the lemma we were tasked with proving:

$$\begin{gathered} 7^{803} \qquad \text{mod } 1000 \\ a^y \equiv a^x \qquad \text{mod m} \end{gathered}$$

After getting a feel for what values are associated with each variable, we started working on simplifying the exponent "under mod $\phi(m)$"

$$\begin{aligned} \phi(1000) &= \phi(2^3 * 5^3) \\ &= \phi(2^3) * \phi(5^3) \\ &= 2^2(1) * 5^2(4) \\ &= 400 \end{aligned}$$

$$\begin{aligned} 803 &= 2(400) + 3 \\ 803 &\equiv 3 \qquad \text{mod}(400) \end{aligned}$$

So at this point I understood the lemma was asking us to prove that exponents equivalent under mod $\phi(m)$ would be equivalent when a base (co-prime to m) is raised to those exponents under mod m.

$$\begin{aligned} 7^{803} &\equiv 7^3 \qquad \text{mod } 1000 \\ &= 7^3 \qquad \text{mod } 1000 \end{aligned}$$

While the TA worked out another example (2^{1000} mod 13), I started thinking about why this might work out but nothing seemed obvious at first.

At first, I was thinking about Week 7 Tuesday's reading notes on 4.2: Euler's Phi Functions - particularly the proof exercises on how Euler's Phi Function was derived. I tried to think of ways of applying some of the techniques in those proofs to this one since that was the most recent memory of proofs that I had at that point. Needless to say, I struggled with the problem for a bit and worked on it while the TA went through the discussion for the next discussion group.

While the TA was working out the first problem for the discussion with the next section, it suddently hit me how most of the work in this secction, all the homework problems and exercises -- everything was an application of Euler's Theorem ($a^{\phi(m)} \equiv 1$ mod m).

It was then that it "clicked" for me. We were supposed to use th definition of modular congruency to show that the exponents are multiples of $\phi(m)$ away from eachother. And then we could just modular exponentiation rules to reduce the overall expression into a simpler form containing just the second ("simpler") exponent:

Step 1:

$$\begin{gathered} x \equiv y \qquad \phi(m) \\ x = y + k(\phi(m)) \end{gathered}$$

Step 2:

$$\begin{aligned} a^x &= a^{y+k\phi(m)} \\ &= a^y a^{k\phi(m)} \\ &= a^y (a^{\phi(m)})^k \\ &\equiv a^y (1)^k \qquad\qquad \text{mod m} \\ &\equiv a^y \qquad\qquad\qquad \text{mod m} \end{aligned}$$

3. *Meta-Learning: Learning Habits*

I've found that I have a tendency to "all-or-nothing". I would either take extensive notes, accompanied with python scripts to aid with exercises - or I would skip the readings all together.

I don't completely understand why. Maybe it's a need to fully understand everything before moving on? And then realizing how much of a time commitment that could take and opting to work on things with a higher priority deadline, skipping readings altogether?

"Half-assing" assignments and skimming readings is something I never really understood. Rather than distributing the time and energy to understand the breadth of a reading, I found that I would hyper-fixate on specific passages and skipping other passages either because I caught myself reading the same lines over and over, or I was behind in other coursework.

I have been able to correct this behavior when I'm actively watching out for it (specifically week 7 Tuesday's reading on 4.2: Euler's Phi Function) but I seem to revert to default settings/autopilot if I'm not paying attention. Moreover, I don't think there is a stark "right" or "wrong" way to approach learning but there definitely should be a balance between understanding and timeliness of progress. I'm not completely happy with where I am right now but I do feel like I made some decent progress in changing the ways I learn material to be more efficient.