CS 70 Discrete Mathematics and Probability Theory
Summer 2025 Tate

HW 02

Due: Saturday, 7/12, 4:00 PM
Grace period until Saturday, 7/12, 6:00 PM
Remember to show your work for all problems!

Sundry

Before you start writing your final homework submission, state briefly how you worked on it. Who else did you work with? List names and email addresses. (In case of homework party, you can just describe the group.) If you used an LLM, place transcripts of your chats here.

1 Celebrate and Remember Textiles

Note 6

You've decided to knit a 70-themed baby blanket as a gift for your cousin and want to incorporate rows from three different stitch patterns with the following requirements on the row lengths of each of the stitch patterns:

- Alternating Link: Multiple of 8, plus 3
- Double Helix: Multiple of 3, plus 1
- Crossover: Multiple of 7, plus 6

You want to be able to switch between knitting these different patterns without changing the number of stitches on the needle, so you must use a number of stitches that simultaneously meets the requirements of all three patterns.

Find the *smallest number of stitches* you need to cast on in order to incorporate all three patterns in your baby blanket.

2 RSA with CRT

Note 7

Inspired by the efficiency of solving systems of modular equations with CRT, Alice decides to use CRT to speed up RSA!

She first generates the public key (e,N) and private key d as normal, keeping track of the primes $pq = N$. Recall that e is chosen to be coprime to $(p-1)(q-1)$, and d is then defined as $e^{-1} \pmod{(p-1)(q-1)}$. Next, she stores the following values:

$$d_p \equiv d \pmod{p-1}$$
$$d_q \equiv d \pmod{q-1}$$

After receiving an encrypted message $c = m^e \pmod{N}$ from Bob, Alice computes the following expressions:

$$x \equiv c^{d_p} \pmod{p}$$
$$x \equiv c^{d_q} \pmod{q}$$

The message m then calculated as the solution to the above modular system.

(a) Show that this algorithm is correct, i.e. that $x \equiv m$ is the only solution $\pmod{N}$ to the above modular system.

(b) Emboldened by her success in using CRT for RSA, Alice decides to invent a new cryptosystem. To generate her keypair, she first generates $N = pq$. Then, she chooses three numbers g, r_1, r_2 and publishes the public key $(N, g_1 = g^{r_1(p-1)} \pmod{N}, g_2 = g^{r_2(q-1)} \pmod{N})$. Her private key is (p,q).

To encrypt a message, Bob chooses two numbers s_1, s_2 and sends $c_1 = mg_1^{s_1}, c_2 = mg_2^{s_2}$.

Alice decrypts this message by solving the modular system

$$x \equiv c_1 \pmod{p}$$
$$x \equiv c_2 \pmod{q}$$

Show that this algorithm is correct, i.e. show that $x \equiv m$ is the only solution $\pmod{N}$ to the above modular system.

(c) This system is woefully insecure. Show how anyone with access to the public key can recover p, q, given that $g_1 \not\equiv 1 \pmod{q}$.

3 RSA with Just One Prime

Given the message $x \in \{0, 1, \ldots, N-1\}$ and $N = pq$, where p and q are prime numbers, conventional RSA encrypts x with $y = E(x) \equiv x^e \pmod{N}$. The decryption is done by $D(y) \equiv y^d \pmod{N}$, where d is the inverse of $e \pmod{(p-1)(q-1)}$.

Alice is trying to send a message to Bob, and as usual, Eve is trying to decipher what the message is. One day, Bob gets lazy and tells Alice that he will now use $N = p$, where p is a 1024-bit

prime number, as part of his public key. He tells Alice that it's okay, since Eve will have to try out 2^{1024} combinations to guess x. It is very likely that Eve will not find out the secret message in a reasonable amount of time! In this problem, we will see whether Bob is right or wrong. Assume that Eve has found out about this new setup and that she knows the public key.

Similar to the original method, for any message $x \in \{0, 1, \ldots, N-1\}$, $E(x) \equiv x^e \pmod{p}$, and $D(y) \equiv y^d \pmod{p}$. Choose e such that it is coprime with $p-1$, and choose $d \equiv e^{-1} \pmod{p-1}$.

(a) Prove that the message x is recovered after it goes through your new encryption and decryption functions, $E(x)$ and $D(y)$.

(b) Can Eve compute d in the decryption function? If so, by what algorithm and approximately how many iterations does it take for it to terminate?

(c) Given part (b), how would Eve recover x and what algorithm would she use? Approximately how many iterations does it take to terminate?

(d) Based on the previous parts, can Eve recover the original message in a reasonable amount of time? Explain.

4 Equivalent Polynomials

Note 7
Note 8

This problem is about polynomials with coefficients in GF(p) for some prime $p \in \mathbb{N}$. We say that two such polynomials f and g are *equivalent* if $f(x) \equiv g(x) \pmod{p}$ for every $x \in \text{GF}(p)$.

(a) Show that $f(x) = x^{p-1}$ and $g(x) = 1$ are **not** equivalent polynomials under GF(p).

(b) Use Fermat's Little Theorem to find a polynomial with degree strictly less than 13 that is equivalent to $f(x) = x^{13}$ over GF(13); then find a polynomial with degree strictly less than 7 that is equivalent to $g(x) = 2x^{74} + 6x^7 + 3$ over GF(7).

(c) In GF(p), prove that whenever $f(x)$ has degree $\geq p$, it is equivalent to some polynomial $\tilde{f}(x)$ with degree $< p$.

5 Lagrange? More like Lamegrange.

Note 8

In this problem, we walk you through an alternative to Lagrange interpolation.

(a) Let's say we wanted to interpolate a polynomial through a single point, (x_0, y_0). What would be the polynomial that we would get? (This is not a trick question. A degree 0 polynomial is fine.)

(b) Call the polynomial from the previous part $f_0(x)$. Now say we wanted to define the polynomial $f_1(x)$ that passes through the points (x_0, y_0) and (x_1, y_1). If we write $f_1(x) = f_0(x) + a_1(x - x_0)$, what value of a_1 causes $f_1(x)$ to pass through the desired points?

(c) Now say we want a polynomial $f_2(x)$ that passes through (x_0, y_0), (x_1, y_1), and (x_2, y_2). If we write $f_2(x) = f_1(x) + a_2(x - x_0)(x - x_1)$, what value of a_2 gives us the desired polynomial?

(d) Suppose we have a polynomial $f_i(x)$ that passes through the points (x_0, y_0), ..., (x_i, y_i) and we want to find a polynomial $f_{i+1}(x)$ that passes through all those points and also (x_{i+1}, y_{i+1}). If we define $f_{i+1}(x) = f_i(x) + a_{i+1}\prod_{j=0}^{i}(x - x_j)$, what value must a_{i+1} take on?

6 Trust No One

Gandalf has assembled a fellowship of eight peoples to transport the One Ring to the fires of Mount Doom: four hobbits, two humans, one elf, and one dwarf. The ring has great power that may be of use to the fellowship during their long and dangerous journey. Unfortunately, the use of its immense power will eventually corrupt the user, so it must not be used except in the most dire of circumstances. To safeguard against this possibility, Gandalf wishes to keep the instructions a secret from members of the fellowship. The secret must only be revealed if enough members of the fellowship are present and agree to use it.

Requiring all eight members to agree is certainly a sufficient condition to know the instructions, but it seems excessive. However, we also know that the separate peoples (hobbits, humans, elf, and dwarf) do not completely trust each other so instead we decide to require members from at least two different peoples in order to use the ring. In particular, we will require a unanimous decision by all members of one group in addition to at least one member from a different group. That is, if only the four hobbits want to use the ring, then they alone should not have sufficient information to figure out the instructions. Same goes for the two humans, the elf, and the dwarf.

More explicitly, only four hobbits agreeing to use the ring is not enough to know the instructions. Only two humans agreeing is not enough. Only the elf agreeing is not enough. Only the dwarf agreeing is not enough. However, all four hobbits and a man agreeing is enough. Both humans and a dwarf agreeing is enough. Both the elf and the dwarf agreeing is enough.

Gandalf has hired your services to help him come up with a secret sharing scheme that accomplishes this task, summarized by the following points:

- There is a party of four hobbits, two humans, an elf, and a dwarf.
- There is a secret message that needs to be known if enough members of the party agree.
- The message must remain unknown to everyone if not enough members of the party agree.
- If only the members of one people agree, the message remains a secret.
- If all the members of one people agree plus at least one additional person, the message can be determined.

7 Error-Correcting Codes

Note 9

(a) Recall from class the error-correcting code for erasure errors, which protects against up to k lost packets by sending a total of $n + k$ packets (where n is the number of packets in the original message). Often the number of packets lost is not some fixed number k, but rather a *fraction* of the number of packets sent. Suppose we wish to protect against a fraction α of

lost packets (where $0 < \alpha < 1$). At least how many packets do we need to send (as a function of n and α)?

(b) Repeat part (a) for the case of general errors.