

Due: Saturday, 2/25, 4:00 PM
Grace period until Saturday, 2/25, 6:00 PM

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.)

1 Equivalent Polynomials

Note 7
Note 8
This problem is about polynomials with coefficients in $\text{GF}(p)$ for some prime $p \in \mathbb{N}$. We say that two such polynomials f and g are *equivalent* if $f(x) = g(x)$ for every $x \in \text{GF}(p)$.

- Use Fermat's Little Theorem to find a polynomial with degree strictly less than 5 that is equivalent to $f(x) = x^5$ over $\text{GF}(5)$; then find a polynomial with degree strictly less than 11 that is equivalent to $g(x) = 4x^{70} + 9x^{11} + 70$ over $\text{GF}(11)$.
- In $\text{GF}(p)$, prove that whenever $f(x)$ has degree $\geq p$, it is equivalent to some polynomial $\tilde{f}(x)$ with degree $< p$.

2 One Point Interpolation

Note 8
Suppose we have a polynomial $f(x) = x^k + c_{k-1}x^{k-1} + \dots + c_2x^2 + c_1x + c_0$.

- Can we determine $f(x)$ with k points? If so, provide a set of inputs x_0, x_1, \dots, x_{k-1} such that knowing points $(x_0, f(x_0)), (x_1, f(x_1)), \dots, (x_{k-1}, f(x_{k-1}))$ allows us to uniquely determine $f(x)$, and show how $f(x)$ can be determined from such points. If not, provide a proof of why this is not possible.
- Now, assume each coefficient is an integer satisfying $0 \leq c_i < 100 \quad \forall i \in [0, k-1]$. Can we determine $f(x)$ with one point? If so, provide an input x_* such that knowing the point $(x_*, f(x_*))$ allows us to uniquely determine $f(x)$, and show how $f(x)$ can be determined from this point. If not, provide a proof of why this is not possible.

3 The CRT and Lagrange Interpolation

Note 6
Note 8

Let n_1, \dots, n_k be pairwise co-prime, i.e. n_i and n_j are co-prime for all $i \neq j$. The Chinese Remainder Theorem (CRT) tells us that there exist solutions to the following system of congruences:

$$x \equiv a_1 \pmod{n_1} \tag{1}$$

$$x \equiv a_2 \pmod{n_2} \tag{2}$$

$$\vdots \tag{i}$$

$$x \equiv a_k \pmod{n_k} \tag{k}$$

and all solutions are equivalent $\pmod{n_1 n_2 \cdots n_k}$. For this problem, parts (a)-(c) will walk us through a proof of the Chinese Remainder Theorem. We will then use the CRT to revisit Lagrange interpolation.

- (a) We start by proving the $k = 2$ case: Prove that we can always find an integer x_1 that solves (1) and (2) with $a_1 = 1, a_2 = 0$. Similarly, prove that we can always find an integer x_2 that solves (1) and (2) with $a_1 = 0, a_2 = 1$.
- (b) Use part (a) to prove that we can always find at least one solution to (1) and (2) for any a_1, a_2 . Furthermore, prove that all possible solutions are equivalent $\pmod{n_1 n_2}$.
- (c) Now we can tackle the case of arbitrary k : Use part (b) to prove that there exists a solution x to (1)-(k) and that this solution is unique $\pmod{n_1 n_2 \cdots n_k}$.
- (d) For polynomials $p_1(x), p_2(x)$ and $q(x)$ we say that $p_1(x) \equiv p_2(x) \pmod{q(x)}$ if $p_1(x) - p_2(x)$ is of the form $q(x) \times m(x)$ for some polynomial $m(x)$.

Define the polynomials $x - a$ and $x - b$ to be co-prime if they have no common divisor of degree 1. Assuming that the CRT still holds when replacing x, a_i and n_i with polynomials (using the definition of co-prime polynomials just given), show that the system of congruences

$$p(x) \equiv y_1 \pmod{(x - x_1)} \tag{1'}$$

$$p(x) \equiv y_2 \pmod{(x - x_2)} \tag{2'}$$

$$\vdots \tag{i'}$$

$$p(x) \equiv y_k \pmod{(x - x_k)} \tag{k'}$$

has a unique solution $\pmod{(x - x_1) \cdots (x - x_k)}$ whenever the x_i are pairwise distinct. What is the connection to Lagrange interpolation?

Hint: To show that a unique solution exists, you may use the fact that the CRT has a unique solution when certain properties are satisfied.

4 Trust No One

Note 8

Gandalf has assembled a fellowship of nine peoples to transport the One Ring to the fires of Mount Doom: five humans, two hobbits, 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.

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 five humans, two hobbits, an elf, and a dwarf, and a secret message that must remain unknown to everyone if not enough members of the party agree.
- A group of people consisting of at least two people from different people classes and at least one people class that is fully represented (i.e., has all members present) can unlock the secret of the ring.

A few examples: only five humans agreeing to use the ring is not enough to know the instructions. One hobbit and four humans is not enough. However, all five humans and one hobbit agreeing is enough. Both hobbits and the dwarf agreeing is enough.

5 Secret Sharing with Spies

Note 8
Note 9

An officer stored an important letter in her safe. In case she becomes unreachable in battle, she decides to share the password (which is a number) with her troops. However, everyone knows that there are 3 spies among the troops, but no one knows who they are except for the three spies themselves. The 3 spies can coordinate with each other and they will either lie and make people not able to open the safe, or will open the safe themselves if they can. Therefore, the officer would like a scheme to share the password that satisfies the following conditions:

- When N of them get together, they are guaranteed to be able to open the safe even if they have spies among them.
- The 3 spies must not be able to open the safe all by themselves.

Please help the officer to design a scheme to share her password. What is the scheme? What is the smallest N ? Show your work and argue why your scheme works and any smaller N couldn't work. (The troops only have one chance to open the safe; if they fail the safe will self-destruct.)

6 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.

7 Alice and Bob

Note 8
Note 9

- (a) Alice decides that instead of encoding her message as the values of a polynomial, she will encode her message as the coefficients of a degree 2 polynomial $P(x)$. For her message $[m_1, m_2, m_3]$, she creates the polynomial $P(x) = m_1x^2 + m_2x + m_3$ and sends the five packets $(0, P(0))$, $(1, P(1))$, $(2, P(2))$, $(3, P(3))$, and $(4, P(4))$ to Bob. However, one of the packet y -values is changed by Eve before it reaches Bob. If Bob receives

$$(0, 1), (1, 3), (2, 0), (3, 1), (4, 0)$$

and knows Alice's encoding scheme and that Eve changed one of the packets, can he recover the original message? If so, find it as well as the x -value of the packet that Eve changed. If he can't, explain why. Work in mod 7.

- (b) Bob gets tired of decoding degree 2 polynomials. He convinces Alice to encode her messages on a degree 1 polynomial. Alice, just to be safe, continues to send 5 points on her polynomial even though it is only degree 1. She makes sure to choose her message so that it can be encoded on a degree 1 polynomial. However, Eve changes two of the packets. Bob receives $(0, 5)$, $(1, 7)$, $(2, x)$, $(3, 5)$, $(4, 0)$. If Alice sent $(0, 5)$, $(1, 7)$, $(2, 9)$, $(3, -2)$, $(4, 0)$, for what values of x will Bob not uniquely be able to determine Alice's message? Assume that Bob knows Eve changed two packets. Work in mod 13.
- (c) Alice wants to send a length 9 message to Bob. There are two communication channels available to her: Channel X and Channel Y. When n packets are fed through Channel X, only 6 packets, picked arbitrarily, are delivered. Similarly, Channel Y will only deliver 6 packets, picked arbitrarily, but it will also corrupt (change the value) of one of the delivered packets. Each channel will only work if at least 10 packets are sent through it. Using each of the two channels once, provide a way for Alice to send her message to Bob so that he can always reconstruct it.