CS 70 - HW05

Sunday

della.lee@berkeley.edu

CSUO@berkeley.edu

1] Equivalent Polynomials

a) Find: polynomial w/ degree ≤ 5 equivalent to:

$f(x) = x^5$ over GF(5)

↳ $f(x) = x^5$ FLT ⟶ $a^{p-1} \equiv 1 \pmod{n}$

↳ $x^4 \equiv 1 \pmod{5}$

↳ $x(x^4) = x^5$

⟶ $x(1) \equiv x \pmod{5}$

↳ this shows us that the function w/ degree ≤ 5 equivalent to $f(x) = x^5$ over GF(5) is just $y = x \pmod{5}$

Find: polynomial w/ degree 11 equivalent to

$q(x) = 4x^{20} + 9x^{11} + 20$ over GF(11)

$4x^{20} + 9x^{11} + 20$; FLT

↳ $x^{11} = x \bmod 11$ → $9x \bmod 11$

$x^{10} = 1 \bmod 11$

↳ $4x^{20} \rightarrow (4x^2)^{10} \rightarrow 4$

↳ $9x + 20 + 4 \bmod 11$

↳ $9x + 7 \bmod 11$

b) Use FLT

For any integer where gcd(a, p) = 1

$$a^{p-1} = a^{p-2}\, a \equiv a^{p-2}\, a \bmod p$$

$$\downarrow \quad a^{p} \equiv a \bmod p$$

$$a^{p-2+1} \bmod p$$

↓ This tells us that x^p is equivalent to a polynomial we already know where $a^{p-2+1} \bmod p$. Essentially we need to subtract p by 1, x^2 would be $x^{2-2(p-1)}$ which further proves our argument.

21 One point Interpolation

polynomial: $f(x) = x^{k} + c_{k-1}x^{k-1} + \dots + c_2 x^2 + c_1 x + c_0$

a) Yes, we can determine $f(x)$ with k points

we can do this through Lagrange Interpolation:

La Grange Interpolation

Given: $k+1$ points $(x_0, f(x_0)), (x_1, f(x_1)), \dots, (x_{k-1}, f(x_{k-1}))$

Goal: Find degree k polynomial that passes through all of these points

method:

$$\Delta_i(x) = \frac{\prod_{j \neq i} (x - x_j)}{\prod_{j \neq i} (x_i - x_j)} \quad \text{for } k+1 \text{ points}$$

↳ The Lagrange interpolation will output a polynomial that passes all the given requirements

b) coefficient integer C_i ; $0 \leq c_i \leq 100$

$\forall i \in [0, 15-1]$

↳ Find: $f(x)$ with 1 point

Result: Impossible

-> Because the Lagrange Interpolation requires 2 points on a graph in order to interpret, either we were given a limitation on how the potential other point can lie that isn't known limitations to accurately depict a graph via Lagrange Interpolation

3) CRT and Lagrange Interpolation

a) $k = 2$ Part 1 / Part 2

→ $x \equiv a_1 \bmod n_1$ → $x \equiv 1 \bmod m$

$x \equiv a_2 \bmod n_2$ $x \equiv 0 \bmod n_2$

Step 1 - prove GCD of $n_1, n_2 = 1$

↳ $\gcd(n_1, n_2)$ given = 1

→ This tells me that the values for n_1 and n_2 for the $\gcd = 1$ or $(2_1, 2_2)$ form the following:

↳ $2_1 k_1 + 2_2 k_2 = 1$

We can find both parts of the equation by plugging in the values we have)

$x_1 = -2_2 n_2 + 1$ or $x_2 = -2_1 n_1 + 1$

b) continuing of proof

when proof is easier: $a_1x_1 + a_2x_2 \pmod{n_1 n_2}$

♫ always a solution

$\rightarrow a_1x_1 + a_2x_2 \equiv a_1 \cdot 1 + a_2 \cdot 0 \equiv a_1 \bmod n_1$

$\rightarrow a_1x_1 + a_2x_2 \equiv a_1 \cdot 0 + a_2 \cdot 1 \equiv a_2 \bmod n_2$

$\rightarrow$ this implies we that we would have at

least 2 unique solutions which were

supposed with equations $a_1 \bmod n_1$ and

$a_2 \bmod n_2$. this also suggests that

the 2 unique solutions are dividing

by n_1 and n_2. this is to the high

proves that all the results are unique

to $\bmod n_1 n_2$

C) prove CRT with induction

BC: $(n=1)$ proved in part a

IH: for $k \leq l$, $k+1$ will produce a unique solution $c \pmod{n_1 \dots n_k}$.

IS: $x \equiv a_{l+1} \pmod{n_{l+1}}$

$(k=l+1)$

by we were given that $n_1, n_2 \dots n_k$ are coprime. this fulfills one of our conditions, both proves that there will be at least a unique solution c'. this will fully use that c' is the unique solution for this problem

2) Connection to Lagrange Interpolation

Need to prove that $q_1(x) = (x - x_1)$ and
$q_2(x) = (x - x_2)$

are coprime so that the $\gcd(q_1, q_2) \neq 1$

If the divisor $= q_1(x)$, then our theorem would fail but since the degree of $q_1(x)$ is 1, we know that for some other solution polynomial that its degree is 0. This means it's a constant divisor of $q_1(x)$. And with the given knowledge, we find that (1') - (4') constructs all the polynomial $p(x)$ such that $p(x_1) = y_1$.

And the CRT we proven earlier says that $p(x)$ will be unique modulo the degree polynomial, which is the connection to Lagrange Interpolation.

4) Trust No One

Parts: humans hospitals ECE servers

5 2 1 1

Requires: 1 fully vaccinated person

1 other person

Fin7: secret sharing scheme

General threshold

→ the requirements apply for 2 conditional statements

1) all 1 vaccinated person = RaP

2) at least 2 vaccinated persons = ALR

when both need to happen

Looking at condition 1) or RaP

→ when all individuals in a vaccinated couple,

they will be given a special letter

or A. The vaccinated with only 1 vaccine will

have it automatically

Looking at condition 2? or AND

→ If 2 values are in favor, then they will be given a special letter or B.

↳ only when A and B are available can they be used to find the secret C. A and B work independently though to function.

→ Note: we can only attain degree 1 robustness at most since there isn't any redundancy in people who influence the secret.

Example: 8 humans

↳ fails since it fails A but not B, means C wouldn't be obtained

Example 8 humans + 1 CA

↳ works since A chosen and B chosen too leading to C.

S1 2 conditions

- If M properly guarantee ones
- 3 spikes countdown the scale

↳ Develop fcn for degree M−1

Notes.

- Since there are spikes, we need to account this more fcn.
- We also need to make the degree of our function M−1 in order to prevent spikes from opening, the scale or 9.
- Give 6 points to ensure in order to consolidate potential errors

↳ (t+1, f(t+1)) ... (t+6, f(t+6))

↳ This would make it so that you need at least 6 = M meaning our conditions are fulfilled.

6) Error correcting code

a) n+k packets

↳ find packets need to send at end

when $0 < \alpha < 1$ lost packets

→ If we sent "x" packets, then

the max α lost would be (αx) and

the max received would be $(1-\alpha)x$.

In order to receive at least n packets,

our formula becomes $\underline{n \geq (1-\alpha)x}$.

b) For general case

We need $k \geq \alpha x$; x = packets

number of max corrupted packets = αx

If $x = n + 2k$ then the following would hold

↳ $x \geq n + 2\alpha x$

↳ However, this isn't possible if $\alpha \geq 1/2$ for

this case because of what it is.

2) Hide and Rob

a) Lagrange Interpolation

points: (0, 1) (1, 3) (2, 0) (3, 1) (4, 0)

polynomial function

$P(x) = m_1 x^2 + m_2 x + m_3$

* one channel unclear ; mol ?

to use LI on degree 2, we need 3 points

pick: (0, 1) (1, 3) (3, 1)

$$\Delta_1(x) = \frac{(x-1)(x-3)}{(0-1)(0-3)} = \frac{x^2-4x+3}{3}$$

$$\Delta_2(x) = \frac{(x-0)(x-3)}{(1-0)(1-3)} = \frac{x^2-3x}{-2}$$

$$\Delta_3(x) = \frac{(x-0)(x-1)}{(3-1)(3-0)} = \frac{x^2-x}{6}$$

$$L_1 [\Delta_1(x) \cdot 1] + [\Delta_2(x) \cdot 3] + (\Delta_3(x) \cdot 1)$$

↓

$$\left(\frac{1}{3}x^2 - \frac{4}{3}x + 1\right) + \left(\frac{-3x^2}{2} + \frac{9x}{2}\right) + \left(\frac{x^2}{6} - \frac{x}{6}\right)$$

$$\Rightarrow x^2\left(\frac{1}{3} - \frac{3}{2} + \frac{1}{6}\right) + x\left(-\frac{4}{3} + \frac{9}{2} - \frac{1}{6}\right) + (1)$$

$\Rightarrow -x^2 + 3x + 1$ = polynomial in mod 7

Lagrange

$$\downarrow$$

$$6x^2 + 3x + 1 \pmod 7$$

$\Rightarrow$ Test other points

$$6(2)^2 + 3(2) + 1 \pmod 7$$

$$24 + 6 + 1 \pmod 7$$

$$31 \pmod 7$$

$$3 \pmod 7 \neq 0$$

$(2,0)$ incorrect point

$-16 + 12 + 1$

17

$-3 \pmod 7$

$4 \pmod 7$

$6(4n^2+3n+1 \mod 5)$

$9\theta+12+1 \mod 2)$

$(0+ \mod 2)$

$4 \mod 1)$ incorrect mode

h) The only time Bob cannot figure out Alice's message is when she sends a 2-degree polynomial that goes through 2 or 5 points.

↳ Degree 2 polynomials mean that there are 2 lines for which plotting the lines would provide a graph. We can then use that graph to find the 2 points and determine the message.

→ After plotting the points, we find that $(2, x)$ is unclear to determine what 2 points constructs a line. This means that we can't to correctly solve the line

C) Channel X will provide 6 packets of

arbitrarily. If we sent 10, then

Bob will still be able to construct

a 4 degree polynomial with

the given information. Since we

know that then will be a

general error, we can send a

message of length 4 in order to

get a degree 2. In total, this

is over 4 send a 10 packet

message, we can send a

Channels 1-6 and 6-10 for

our original to be Channel