01204211 Discrete Mathematics
Lecture 10a: Polynomials (2)[1]

Jittat Fakcharoenphol

October 18, 2022

[1] This section is from Berkeley CS70 lecture notes.

Fun fact: Check digit for Thai National ID

1 2 3 4 5 6 7 8 9 0 1 2 $\boxed{7}$

check digit.

$$(1 * 13 + 2 * 12 + \boxed{3 \times 11} + \cdots) \bmod 11$$

Review: Polynomials

A **single-variable polynomial** is a function $p(x)$ of the form

$$p(x) = a_d x^d + a_{d-1} x^{d-1} + \cdots + a_1 x + a_0.$$

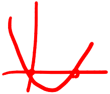
We call a_i's *coefficients*. Usually, variable x and coefficients a_i's are real numbers. The **degree** of a polynomial is the largest exponent of the terms with non-zero coefficients.

$\boxed{\text{จะ "ไม่เกิน" } d}$

degree 3 $\quad x^3 + 2x$

$\boxed{20x^2 + x}$

Review: Basic facts



Definition

a is a **root** of polynomial $f(x)$ if $f(a) = 0$.

Properties

Property 1: A non-zero polynomial of degree d has at most d roots.

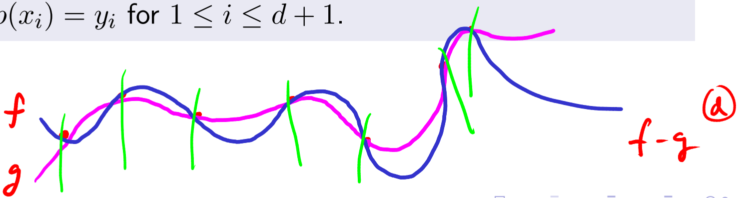
Property 2: Given $d+1$ pairs $(x_1, y_1), \dots, (x_{d+1}, y_{d+1})$ with distinct x_i's, there is a *unique* polynomial $p(x)$ of degree at most d such that $p(x_i) = y_i$ for $1 \le i \le d+1$.

$\exists$

Unique

$\Uparrow$

Prop 1



Polynomial division

degree f − degree g

$$x^2 - 8x$$

$$g(x) = x^3 + 9x^2 + 10 \;\big)\; x^5 + x^4 + 2x^3 + 4x^2 + 4x = f(x)$$

$$x^5 + 9x^4 + 10x^2$$

$$-8x^4 + 2x^3 - 6x^2 + 4x$$

$$-8x^4$$

$r(x)$

degree < deg g

Polynomial division

$$x^2+2x+1 = \underline{(x+1)}(x+1)$$

$$x^2-1 = (x-1)(x+1)$$

If you have a polynomial $p(x)$ of degree d, you can divide it with a polynomial $q(x)$ of degree $\leq d$. You have that there exists a pair of polynomial $q'(x)$ and $r(x)$ such that

$$p(x) = q'(x)q(x) + r(x),$$

and $r(x)$ is of degree **less** than $q(x)$'s degree.

→ หารสัมประสิทธิ์ได้ **

Lemma 1

If a is a root of polynomial $p(x)$ with degree $d \geq 1$, then $p(x) = (x-a)q(x)$ for some polynomial $q(x)$ with degree at most $d-1$

Proof.

• หาร $p(x)$ ด้วย $\underbrace{(x-a)}$

$\Rightarrow$ มี $q(x)$ & $r(x)$ ที่

degree $< 1 = 0$

c

$$p(x) = q(x)(x-a) + \underbrace{\cancel{r(x)}}$$

Lemma 1

If a is a root of polynomial $p(x)$ with degree $d \geq 1$, then $p(x) = (x - a)q(x)$ for some polynomial $q(x)$ with degree at most $d - 1$

Proof.

Dividing $p(x)$ with $(x - a)$, we get that

$$p(x) = q'(x)(x - a) + r(x),$$

where $r(x)$ is of degree at most $1 - 1 = 0$, i.e., $r(x)$ must be a constant; thus, we assume that $r(x) = c$. Let's evaluate $p(a)$; note that $p(a) = c$, since

$$p(a) = q'(a)(a - a) + c = 0 + c = c.$$

However we know that a is a root of $p(x)$, i.e., $p(a) = 0$. Therefore $c = 0$, or $r(x) = 0$. Thus, the lemma follows. □

Lemma 2

If $p(x)$ is a polynomial of degree d with d distinct roots $a_1, a_2, \ldots, a_d$, $p(x)$ can be written as $c(x - a_1)(x - a_2) \cdots (x - a_d)$.

Proof.

Lemma 1

If a is a root of polynomial $p(x)$ with degree $d \geq 1$, then $p(x) = (x - a)q(x)$ for some polynomial $q(x)$ with degree at most $d - 1$

Lemma 2

If $p(x)$ is a polynomial of degree d with d distinct roots $a_1, a_2, \ldots, a_d$, $p(x)$ can be written as $c(x - a_1)(x - a_2) \cdots (x - a_d)$.

Proof.

We prove by induction on d.

Lemma 2

If $p(x)$ is a polynomial of degree d with d distinct roots $a_1, a_2, \ldots, a_d$, $p(x)$ can be written as $c(x-a_1)(x-a_2)\cdots(x-a_d)$.

Proof.

We prove by induction on d.

Base case: พิจารณา $d=0$. polynomial degree 0

เขียนอยู่ในรูป $p(x)=c$ ได้เลย.

Lemma 2

If $p(x)$ is a polynomial of degree d with d distinct roots $a_1, a_2, \ldots, a_d$, $p(x)$ can be written as $c(x - a_1)(x - a_2) \cdots (x - a_d)$.

Proof.

We prove by induction on d.

Base case:

Inductive step:

Lemma 2

If $p(x)$ is a polynomial of degree d with d distinct roots $a_1, a_2, \ldots, a_d$, $p(x)$ can be written as $c(x - a_1)(x - a_2) \cdots (x - a_d)$.

Proof.

We prove by induction on d.

Base case:

Inductive step: Assume that $p(x)$ is a polynomial of degree $d + 1$ with distinct roots $a_1, \ldots, a_d, a_{d+1}$.

Lemma 2

If $p(x)$ is a polynomial of degree d with d distinct roots $a_1, a_2, \ldots, a_d$, $p(x)$ can be written as $c(x - a_1)(x - a_2)\cdots(x - a_d)$.

Proof.

We prove by induction on d.
Base case:
Inductive step: Assume that $p(x)$ is a polynomial of degree $d + 1$ with distinct roots $a_1, \ldots, a_d, a_{d+1}$. Since a_{d+1} is $p(x)$'s root, we can divide on (lemma 1)
$p(x)$ with $(x - a_{d+1})$ and get that

$$p(x) = (x - a_{d+1})q(x),$$

where

Lemma 2

If $p(x)$ is a polynomial of degree d with d distinct roots $a_1, a_2, \dots, a_d$, $p(x)$ can be written as $c(x-a_1)(x-a_2)\cdots(x-a_d)$.

Proof.

We prove by induction on d.

Base case:

Inductive step: Assume that $p(x)$ is a polynomial of degree $\underline{d+1}$ with distinct roots $a_1, \dots, a_d, a_{d+1}$. Since a_{d+1} is $p(x)$'s root, we can divide $p(x)$ with $(x - a_{d+1})$ and get that

$$p(x) = \underline{(x - a_{d+1})}\,\underline{q(x)}, \qquad (*)$$

where $q(x)$ is a polynomial of degree $\underline{d}$ with d distinct roots $\underbrace{a_1, \dots, a_d}$. □

By induction hypothesis, ได้ว่า เขียน $q(x)$ ในรูป :

$$q(x) = c(x-a_1)(x-a_2)\cdots(x-a_d)$$

แทนค่าใน (*) ได้ว่า $p(x) = c(x-a_1)\cdots(x-a_d)(x-a_{d+1})$ ตามต้องการ

Property 1: A non-zero polynomial $p(x)$ of degree d has at most d roots

Proof: by contradiction. Assume $p(x)$ มี $d+1$ roots: $a_1, a_2, \ldots, a_{d+1}$

จาก lemma 2 เนื่องจาก $p(x)$ degree d และมี $a_1, a_2, \ldots, a_d$ เป็น roots ที่แตกต่างกัน

เราสามารถเขียน $p(x)$ ได้ในรูป $c(x-a_1)(x-a_2)\cdots(x-a_d)$

เนื่องจาก $p(x)$ ไม่เป็น 0, $c \neq 0$.

จึงพบว่า $p(a_{d+1}) \neq 0$, เราได้ contradiction

เนื่องจาก a_{d+1} เป็นรากของ $p(x)$

Polynomials over a finite field $GF(p)$

- polynomial division — หารกันของ สัมประสิทธิ์

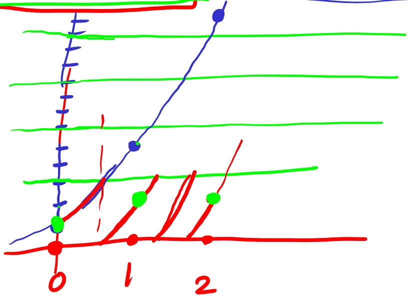
$\mathbb{R}$,

$GF(p)$

$p = 3$

$5x^2 + 2x + 1 \equiv 2x^2 + 2x + 1 \boxed{(\bmod 3)}$

เมื่อ p เป็น จน.เฉพาะ



Examples - evaluation

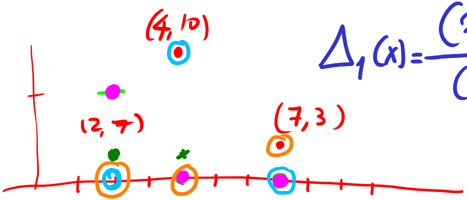
0 – 10

Suppose that we work over $GF(m)$ where $m = 11$. Let $p(x) = 4 \cdot x^2 + 5 \cdot x + 3$. We have

x	$p(x)$	$p(x) \bmod m$
0	3	3
1	12	1
2	29	7
3	54	10
4	87	10
5	128	7
6	177	1
7	234	3
8	299	2
9	372	9
10	453	2
11	542	3

Examples - interpolation

Let $m = 11$. Suppose that $p(x)$ is a polynomial over $GF(m)$ of degree 2 passing through $(2,7)$, $(4,10)$, and $(7,3)$. Find $p(x)$.



$$\Delta_1(x) = \frac{(x-4)(x-7)}{(2-4)(2-7)} = \frac{(x-4)(x-7)}{10} = 10(x-4)(x-7)$$

$$\Delta_2(x) = \frac{(x-2)(x-7)}{(4-2)(4-7)} = \frac{(x-2)(x-7)}{-6} = \frac{(x-2)(x-7)}{5}$$

Examples - interpolation

Let $m = 11$. Suppose that $p(x)$ is a polynomial over $GF(m)$ of degree 2 passing through $(2, 7), (4, 10)$, and $(7, 3)$. Find $p(x)$.
Let

Examples - interpolation

Let $m = 11$. Suppose that $p(x)$ is a polynomial over $GF(m)$ of degree 2 passing through $(2, 7), (4, 10)$, and $(7, 3)$. Find $p(x)$.
Let

- $\Delta_1(x) = \frac{(x-4)(x-7)}{(2-4)(2-7)} = \frac{x^2-11x+28}{(-2)\cdot(-5)} = \frac{x^2+6}{10} = 10x^2 + 5$

Examples - interpolation

Let $m = 11$. Suppose that $p(x)$ is a polynomial over $GF(m)$ of degree 2 passing through $(2,7),(4,10)$, and $(7,3)$. Find $p(x)$.
Let

- $\Delta_1(x) = \frac{(x-4)(x-7)}{(2-4)(2-7)} = \frac{x^2-11x+28}{(-2)\cdot(-5)} = \frac{x^2+6}{10} = 10x^2+5$
- $\Delta_2(x) = \frac{(x-2)(x-7)}{(4-2)(4-7)} = \frac{x^2-9x+14}{2\cdot(-3)} = \frac{x^2+2x+3}{5} = 9x^2+7x+5$

Examples - interpolation

Let $m = 11$. Suppose that $p(x)$ is a polynomial over $GF(m)$ of degree 2 passing through $(2,7), (4,10)$, and $(7,3)$. Find $p(x)$.
Let

- $\Delta_1(x) = \frac{(x-4)(x-7)}{(2-4)(2-7)} = \frac{x^2-11x+28}{(-2)\cdot(-5)} = \frac{x^2+6}{10} = 10x^2+5$
- $\Delta_2(x) = \frac{(x-2)(x-7)}{(4-2)(4-7)} = \frac{x^2-9x+14}{2\cdot(-3)} = \frac{x^2+2x+3}{5} = 9x^2+7x+5$
- $\Delta_2(x) = \frac{(x-2)(x-4)}{(7-2)(7-4)} = \frac{x^2-6x+8}{5\cdot 3} = \frac{x^2+5x+8}{4} = 3x^2+4x+2$

Thus,

$$\begin{aligned} p(x) &= 7\Delta_1(x) + 10\Delta_2(x) + 3\Delta_3(x) \\ &= (70x^2+35) + (90x^2+70x+50) + (9x^2+12x+6) \\ &= \underline{4x^2+5x+3} \end{aligned}$$

Practice

$64000\,01\underbrace{234}_{a_2,\,a_1,\,a_0}$

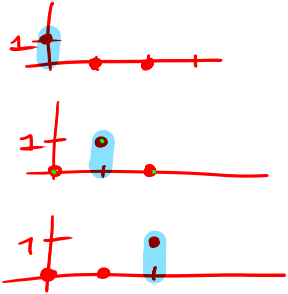
Let's work modulo 11.

Use the last 3 digits of your student ID. Suppose that they are a_2, a_1, a_0. Find a polynomial $p(x)$ of degree 2 such that $p(i) = a_i$ for $i = 0, 1, 2$.

$\Delta_1(x)$

$\Delta_2(x)$

$\Delta_3(x)$

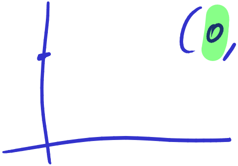


$$\frac{(x-1)(x-2)}{(0-1)(0-2)} = \frac{(x-1)(x-2)}{2}$$

$$= 6(x-1)(x-2)$$

$$= 6x^2+4x+1$$

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

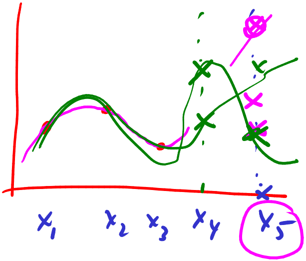


How many?

พิจารณา polynomial degree $\boxed{d}$ $\boxed{\text{mod } m}$

จุด	# poly
$d+1$	1
d	m
$d-1$	m^2
$\vdots$	$\vdots$
1	m^d
0	m^{d+1}

$d = 4$



$P(x_5)$

Two ways of specifying a polynomial $p(x)$ of degree d:

- Specify its coefficients $a_0, a_1, \ldots, a_d$, i.e., the polynomial is

$$p(x) = a_d x^d + \ldots a_1 x + a_0.$$

Two ways of specifying a polynomial $p(x)$ of degree d:

- Specify its coefficients $a_0, a_1, \ldots, a_d$, i.e., the polynomial is

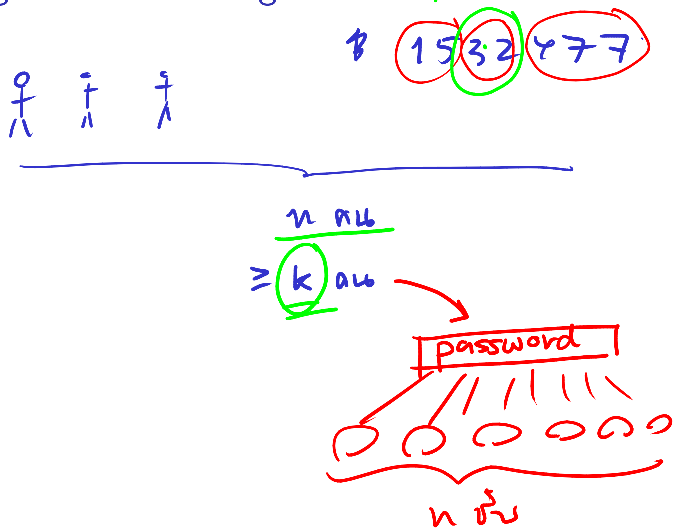
$$p(x) = a_d x^d + \ldots a_1 x + a_0.$$

- Specify $d+1$ points, i.e., $(x_1, y_1), (x_2, y_2), \ldots, (x_{d+1}, y_{d+1})$, where all x_i are distinct. There is a *unique* polynomial $p(x)$ of degree at most d that passes through these points (from Property 2).

For polynomials of degree at most d over $GF(m)$, if you specify q points, there are:

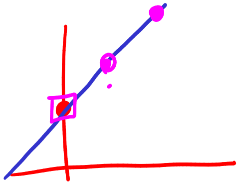
q	numbers of polynomials
$d+1$	1
d	m
$d-1$	m^2
$d-2$	m^3
$\vdots$	$\vdots$
1	m^d
0	m^{d+1}

Secret sharing scheme - settings



Secret sharing scheme - settings

n= 2 , k=2

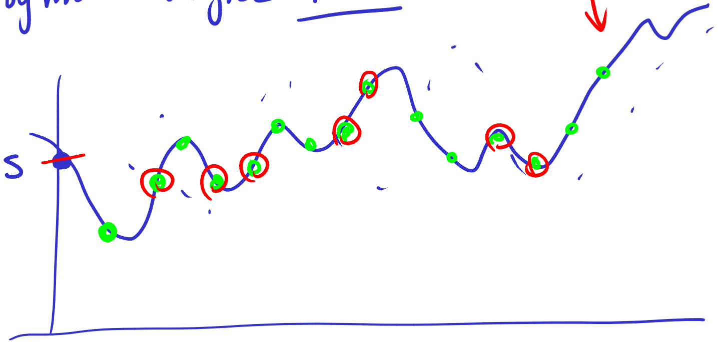


- There are n people, a secret s, and an integer k.
- We want to "distribute" the secret in such a way that any set of $k-1$ people cannot know anything about s, but any set of k people can reconstruct s.

Secret sharing scheme

polynomial degree $k-1$

poly degree $k-1$



$p(0) = s$

Secret sharing scheme

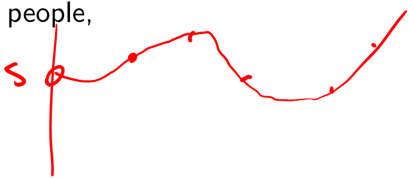
- Pick m to be larger than n and s. (Much larger than s, i.e., $m >>> s$.)
- Pick a random polynomial of degree $k-1$ such that $P(0) = s$.
- Give $P(i)$ to person i, for $1 \leq i \leq n$.
- Correctness: for any set of k people,

$a_0 = s$

$a_1 = ?$

$\vdots$

$a_{k-1} = ?$



Secret sharing scheme

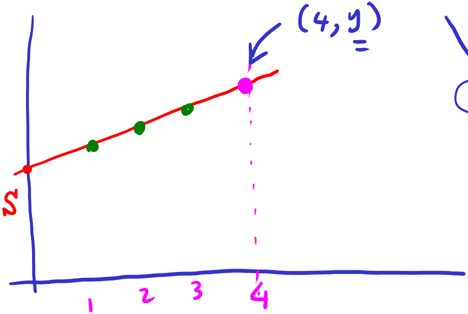
- Pick m to be larger than n and s. (Much larger than s, i.e., $m >>> s$.)
- Pick a random polynomial of degree $k-1$ such that $P(0) = s$.
- Give $P(i)$ to person i, for $1 \leq i \leq n$.
- Correctness: for any set of k people,
- Correctness: for any set of $k-1$ people, how many possible candidate secrets compatible with the information these people have?

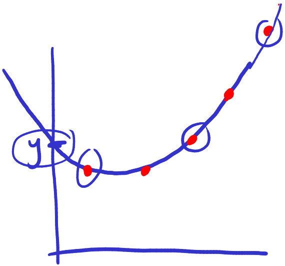
$\boxed{m \quad \text{live}}$

A more complex secret sharing scheme

S

Suppose that a company has 3 VPs and 5 senior members. You want to distribute a secret such that (1) any 2 VPs can obtain the secret or (2) a single VP with 3 senior members can also obtain the secret. How can you do that?

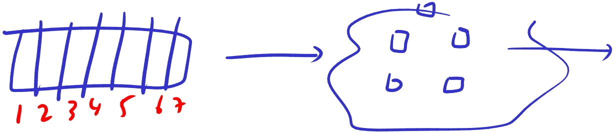




Sending a message

(1,1) (2,2) (3,1) (4,1) . . .

Suppose that you want to send a message 1,2,1,1,3,4,4,10 over the internet.



Sending a message

Suppose that you want to send a message `1,2,1,1,3,4,4,10` over the internet.
Since the internet does not maintain the ordering (if you send with UDP), you have to maintain the "ordering" youself, e.g., you can add the message indices, i.e.,

Sending a message

Suppose that you want to send a message `1,2,1,1,3,4,4,10` over the internet.
Since the internet does not maintain the ordering (if you send with UDP), you have to maintain the “ordering” youself, e.g., you can add the message indices, i.e.,
Lossy internet:

(1,1) , (2,2) ~~(1,3)~~ (1,4) ~~(3,5)~~ (4,6)

(4,7) ~~(10,8)~~

Erasure codes

Suppose that we want to send a message $m_1, m_2, \ldots, m_k$ where $m_i \leq p - 1$ for some prime p.
However, we know that our communication channel is lossy, i.e., some messages can be *dropped*. How can we send this message?