HANU
HANOI UNIVERSITY

FACULTY OF INFORMATION TECHNOLOGY
DEPARTMENT OF COMPUTER SCIENCE

Fall, 2024

DISCRETE MATHEMATIC LEC-06:

Polynomials

Polynomial

$$P(x) = a_d x^d + a_{d-1} x^{d-1} + \ldots + a_1 x + a_0$$

Degree: d

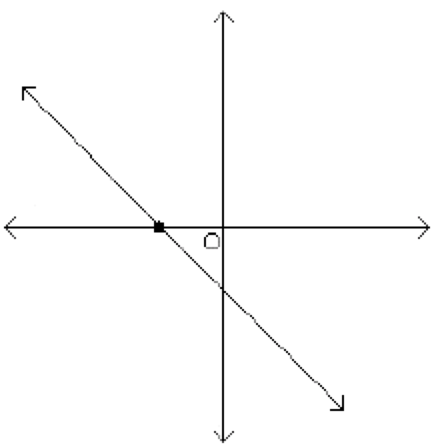
Coefficients are real numbers (a_i)

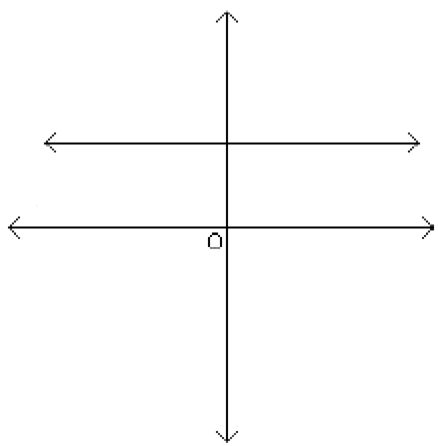
a is a root if $P(a) = 0$

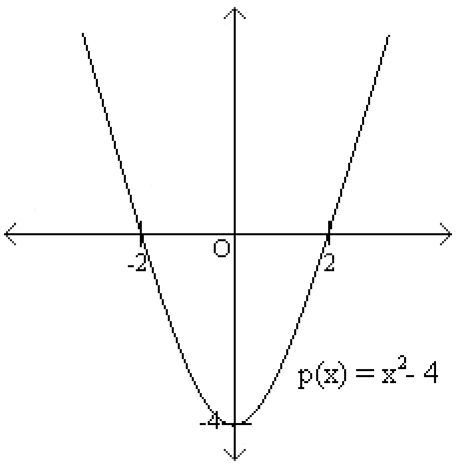
Property 1

A non-zero polynomial of degree *d* has at most *d* roots.

d = 1: linear function
d = 2: quadratic function







Proof

a is a root of $p(x)$ iff $(x\text{-}a)$ divides $p(x)$

Assume that a_1, a_2, …, a_{d+1} are d+1 distinct roots of $p(x)$ (degree d)

$\Rightarrow p(x) = c(x - a_1)\ldots(x - a_{d+1})$

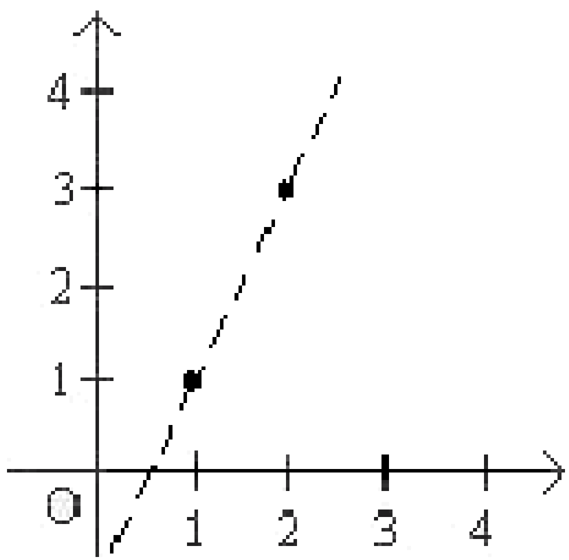
$\Rightarrow$ *P(x) has degree >= d + 1. Constradiction.*

Property 2

Given d+1 pairs (x_1,y_1), (x_2,y_2)…, (x_{d+1},y_{d+1}), there is a unique polynomial of degree (at most) d: $P(x_i)=y_i$ $(1 \le i \le d+1)$

***d* = 1: two points determine a line**

***d* = 2: three points determine a degree 2 polynomial**



Proof by Contradiction

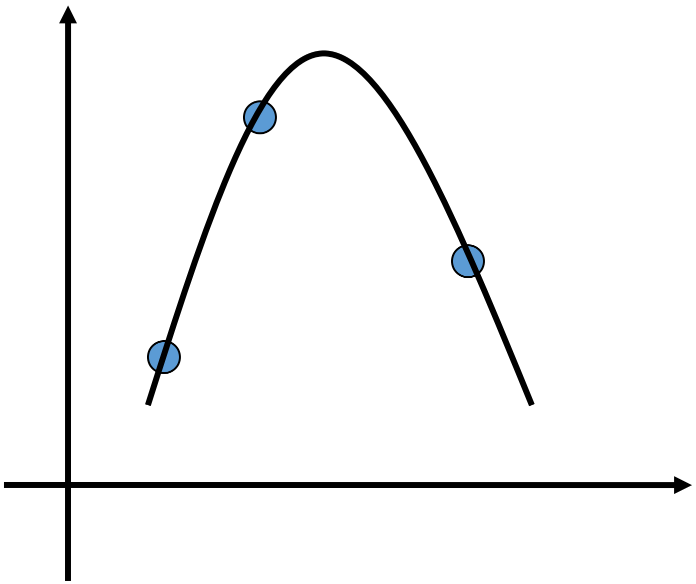
Assume there exists $P_1(x)$ and $P_2(x)$ (degree less than d) that goes through d+1 points.

Let $P(x) = P_1(x) – P_2(x)$

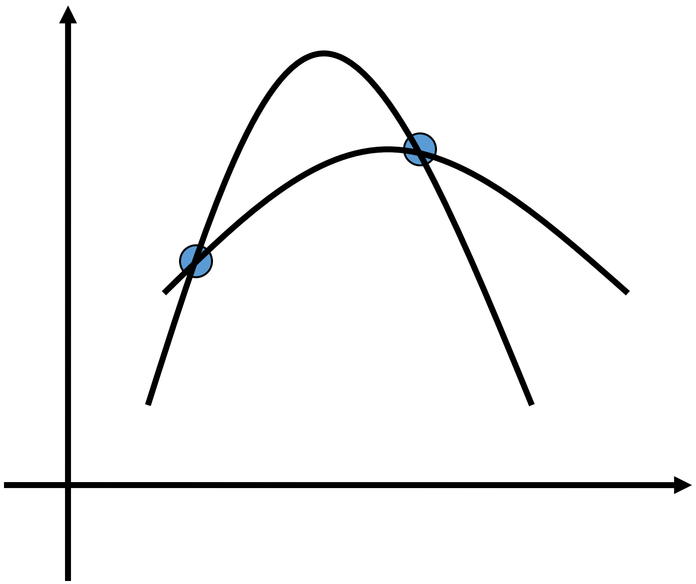
$P(x)$ has at least d+1 roots

$P(x)$ has at most degree d. Contradiction.

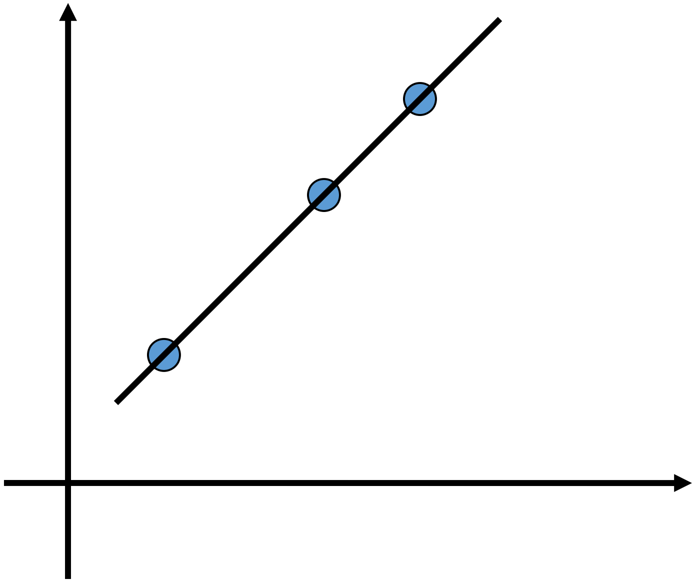
Question



Question



Question



How to find

$$\Delta_i(x) = \frac{\prod_{j \neq i}(x - x_j)}{\prod_{j \neq i}(x_i - x_j)}$$

$$\boxed{P(x) = \sum_{i=1}^{d+1} y_i \Delta_i(x)}$$

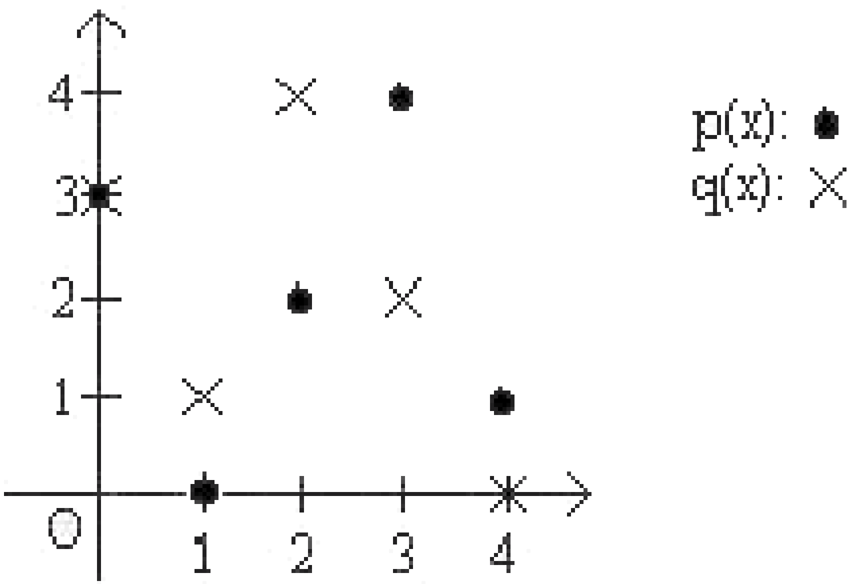
Finite Field (Galois Field)

The numbers used are limited to the range {0, 1, …, m-1}

m = 5: GF(5)

4 + 2 = 1 (mod 5)   5 divides 4 + 2 - 1
3 - 4 = 4 (mod 5)   3 - 4 – 4 is divisible by 5
3 x 4 = 2 (mod 5)   3 x 4 – 2 is divisible by 5
4 / 3 = 3 (mod 5)   2 is multiplicative inverse of 3

Finite Field GF(5)



$$p(x) = 2x + 3$$

$$q(x) = 3x - 2$$

Secret Sharing

A password is required to launch a nuclear strike.

N major officials know part of the password.

Any group of k officials can figure out the password.

No group of k-1 officials can figure out the password.

Secret Sharing

There are n officials. Group of k officials can learn the secret.

The launch code is s

Pick a random polynomial P of degree $k-1$ such that $P(0) = s$

Give $P(1)$ to the first official, $P(2)$ to the second official…

Any k officials, having the value of the polynomial at k points, can find P, and then compute $P(0)$ to learn the secret.

Example

There are 3 people. Group of 2 can learn the secret. The secret is 4.

$P(x) = x+4$

Give $P(1)=5$ to the first official, $P(2)=6$ to the second official, $P(3)=7$ to the last official.

If official 1 and 3 get together, they know $P(1)=5$ and $P(3)=7$, they can find $P(x)=x+4$.