# 01204211 Discrete Mathematics Lecture 10a: Polynomials (1)<sup>1</sup>

Jittat Fakcharoenphol

October 19, 2023

<sup>&</sup>lt;sup>1</sup>This section is from Berkeley CS70 lecture notes.

## Quick exercise

For any integer  $a \neq 1$ ,  $a - 1|a^2 - 1$ .

For any integer  $a \neq 1$  and  $n \geq 1$ ,  $a - 1|a^n - 1$ .

## **Polynomials**

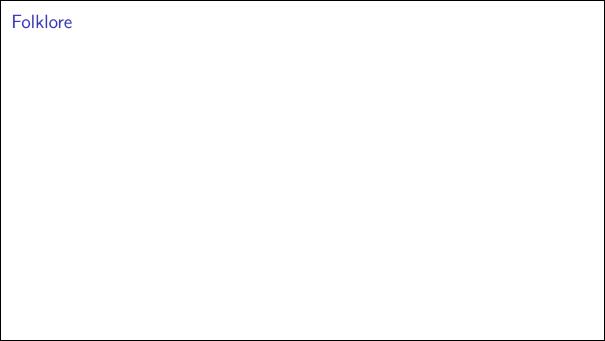
A single-variable polynomial is a function p(x) of the form

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

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.

#### **Examples**

- $x^3 3x + 1$
- x + 10
- ▶ 10
- **•** 0



# **Applications**

- Secret sharing
- ► Error-correcting codes

### 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  $(x_1,y_1),\ldots,(x_{d+1},y_{d+1})$  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  $1\leq i\leq d+1$ .

#### Lemma 1

If two polynomials f(x) and g(x) of degree at most d that share d+1 points  $(x_1,y_1),\ldots,(x_{d+1},y_{d+1})$ , where all  $x_i$ 's are distinct, i.e.,  $f(x_i)=g(x_i)=y_i$ , then f(x)=g(x).

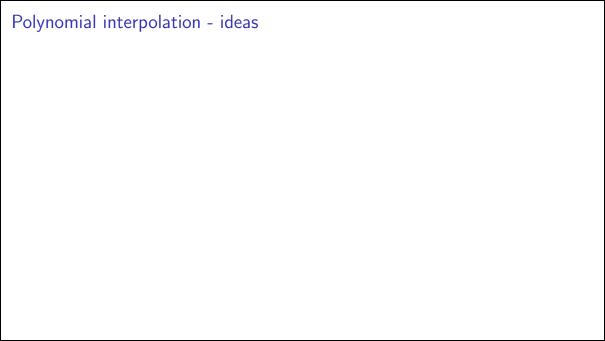
#### Proof.

Suppose that  $f(x) = a_d x^d + a_{d-1} x^{d-1} + \cdots + a_0$  and  $g(x) = b_d x^d + b_{d-1} x^{d-1} + \cdots + b_0$ . Let h(x) = f(x) - g(x), i.e., let  $h(x) = c_d x^d + c_{d-1} x^{d-1} + \cdots + c_0$ , where  $c_i = a_i - b_i$ . Note that h(x) is also a polynomial of degree (at most) d. We claim that h(x) has d+1 roots. Note that since  $f(x_i) = g(x_i) = y_i$ , we have that

$$h(x_i) = f(x_i) - g(x_i) = y_i - y_i = 0,$$

i.e., every  $x_i$  is a root of h(x).

From **Property 1**, if h(x) is non-zero it has at most d roots; therefore, h(x) must be zero, i.e., f(x) - g(x) = 0 or f(x) = g(x) as required.



# Lagrange polynomial

For 
$$d+1$$
 points  $(x_1,y_1),(x_2,y_2),\ldots,(x_{d+1},y_{d+1})$  where all  $x_i$ 's are distinct, let 
$$\Delta_i(x)=\frac{(x-x_1)(x-x_2)\cdots(x-x_{i-1})(x-x_{i+1})\cdots(x-x_{d+1})}{(x_i-x_1)(x_i-x_2)\cdots(x_i-x_{i-1})(x_i-x_{i+1})\cdots(x_i-x_{d+1})}.$$

Note that  $\Delta_i(x)$  is a polynomial of degree d. Also we have that

- ightharpoonup For  $i \neq i$ ,  $\Delta_i(x_i) = 0$ , and
- $\Delta_i(x_i) = 1.$

We can use  $\Delta_i(x)$  to construct a degree-d polynomial

$$p(x) = y_1 \cdot \Delta_1(x) + y_2 \cdot \Delta_2(x) + \cdots + y_{d+1} \cdot \Delta_{d+1}(x).$$

What can you say about  $p(x_i)$ ?

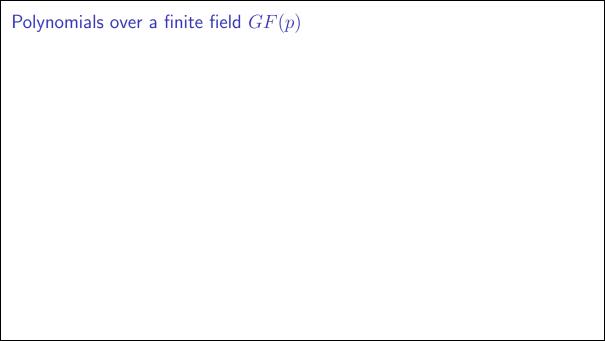
### Property 2

Given d+1 pairs  $(x_1,y_1),\ldots,(x_{d+1},y_{d+1})$  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  $1 \le i \le d+1$ .

#### Proof of Property 2.

Using Lagrange interpolation, we know that there exists a polynomial p(x) of degree d such that  $p(x_i) = y_i$  for all  $1 \le i \le d+1$ .

For uniqueness, assume that there exists another polynomial g(x) of degree d also satifying the condition. Since p(x) and g(x) agrees on more than d points, p(x) and g(x) must be equal from Lemma 1.



### Examples - evaluation

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). Let

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

Thus,

$$p(x) = 7\Delta_1(x) + 10\Delta_2(x) + 3\Delta_3(x)$$
  
=  $(70x^2 + 35) + (90x^2 + 70x + 50) + (9x^2 + 12x + 6)$   
=  $4x^2 + 5x + 3$ 

# Secret sharing scheme - settings

- ▶ 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

- ightharpoonup 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  $1 \le i \le n$ .
- ightharpoonup Correctness: for any set of k people,
- ightharpoonup Correctness: for any set of k-1 people, how many possible candidate secrets compatible with the information these people have?