CS 70   Discrete Mathematics and Probability Theory

Fall 2020   Dis 05A

1 Polynomial Practice

(a) If f and g are non-zero real polynomials, how many roots do the following polynomials have at least? How many can they have at most? (Your answer may depend on the degrees of f and g.)

$$\sum_{i=0}^{d} a_i x^i$$

(i) $f + g$

(ii) $f \cdot g$

(iii) f/g, assuming that f/g is a polynomial

Handwritten annotations:

$$x^5 \cdot x^2 = x^{5+2}$$
$$x^5 / x^2 = x^{5-2}$$

	max	min
(i)	$\max(d_{gf}, d_{gg})$	0
(ii)	$(\deg f + \deg g)$	0 #roots f + #roots g
(iii)	$(\deg f - \deg g)$	0

$$\frac{(x-1)(x^2+1)}{(x-1)}$$

(b) Now let f and g be polynomials over GF(p). $\mathbb{F}_p$ mod p

   (i) We say a polynomial $f = 0$ if $\forall x, f(x) = 0$. If $f \cdot g = 0$, is it true that either $f = 0$ or $g = 0$?

   (ii) How many f of degree *exactly* $d < p$ are there such that $f(0) = a$ for some fixed $a \in \{0, 1, \ldots, p-1\}$? $d = 3$

Handwritten annotations:

$$x^{p-1} - 1 \quad > \quad x$$

$$x(x^{p-1} - 1) \equiv x^p - x \pmod{p}$$

$$\begin{array}{c} x^3 + x^2 \\ 3x^3 - x \\ x^2 - 1 \end{array}$$

$$\underset{\neq 0}{a_d} x^d + \underbrace{a_{d-1} x^{d-1} + \cdots + a_1 x^1}_{d-1 \text{ terms}} + \underset{=\,a}{a_0}$$

p choices

$$(p-1) p^{d-1} \cdot 1$$
$$p^d \cdot 1$$

(c) Find a polynomial f over GF(5) that satisfies $f(0) = 1, f(2) = 2, f(4) = 0$. How many such polynomials are there?

Handwritten annotations:

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

$$\Delta_0(x) = (x-2)(x-4)/(0-2)(0-4)$$
$$= -\tfrac{1}{3}(x-2)(x-4)$$
$$= 2(x-2)(x-4)$$

$$\Delta_2(x) = x(x-4)/((2-0)(2-4))$$
$$= x(x-4)$$

$$\Delta_4(x) = x(x-2)/((4-0)(4-2))$$
$$= 2x(x-2)$$

$1\Delta_0 + 2\Delta_2 + 0\Delta_4$

$2(x-2)(x-4) + 2x(x-4)$

$-2 \cdot 0 - 4 = 8 \equiv 3$

$2^{-1} \bmod 5$

$3^{-1} \equiv 2 \bmod 5$

$2 \cdot 0 - 2 \equiv 1 \quad -4 \equiv 1 \bmod 5$
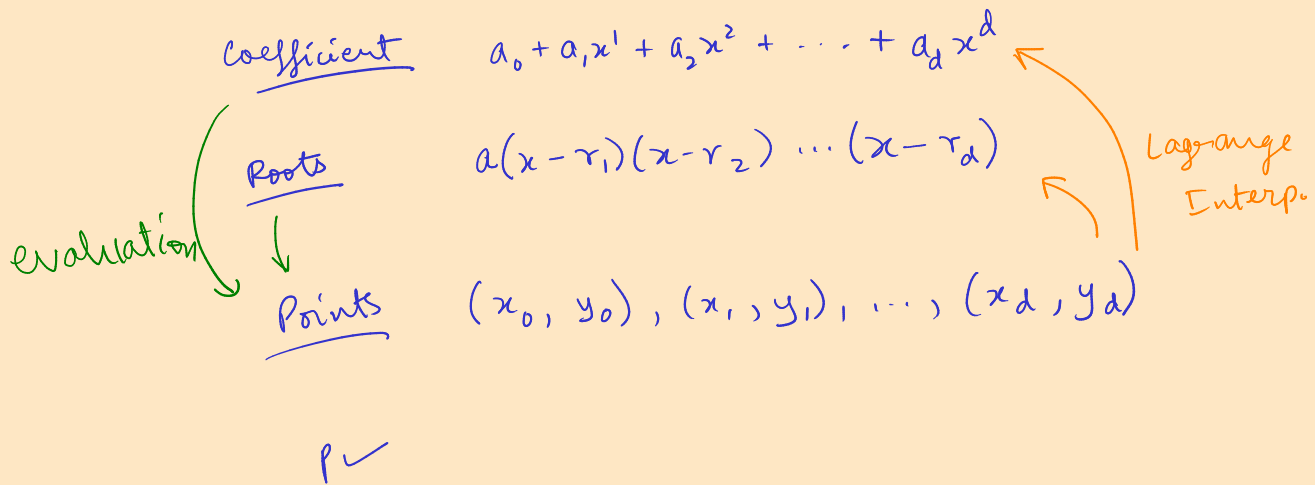
$4 \cdot 2 = 8 \equiv 3 \bmod 5$

$3^{-1} \equiv 2 \bmod 5$

$$x^P \equiv x \mod p \qquad \forall x \in \{0, 1, \ldots, p-1\}$$

$$x^{P-1} \equiv 1 \mod p$$

$$x^7 \equiv (x^5) x^2 \equiv x \cdot x^2 \equiv x^3 \pmod 5$$

Coefficient $\qquad a_0 + a_1 x^1 + a_2 x^2 + \cdots + a_d x^d$

Roots $\qquad a(x - r_1)(x - r_2) \cdots (x - r_d)$

Lagrange Interp.

evaluation

Points $\qquad (x_0, y_0), (x_1, y_1), \ldots, (x_d, y_d)$

$p \checkmark$

$$x^2 + 1 \qquad \mod 3$$

$$a_0 = 1, \ a_1 = 0, \ a_2 = 1$$

$$x_0 = 0, \ x_1 = 1, \ x_2 = 2$$
$$y_0 = 1 \qquad y_1 = 2 \quad y_2 = 2$$

$$(0, 1), (1, 2), (2, 2)$$

2 Rational Root Theorem

The rational root theorem states that for a polynomial

$$P(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_0,$$

$a_0, \cdots, a_n \in \mathbb{Z}$, if $a_0, a_n \neq 0$, then for each rational solution $\frac{p}{q}$ such that $\gcd(p,q) = 1$, $p | a_0$ and $q | a_n$. Prove the rational root theorem.

3 Secret Sharing Practice

Consider the following secret sharing schemes and solve for asked variables.

(a) Suppose there is a bag of candy locked with a passcode between 0 and an integer n. Create a scheme for 5 trick-or-treaters such that they can only open the bag of candy if 3 of them agree to open it.

(b) Create a scheme for the following situation: There are 4 cats and 3 dogs in the neighborhood, and you want them to only be able to get the treats if the majority of the animals of each type are hungry. The treats are locked by a passcode between 0 and an integer n.

4 Old Secrets, New Secrets

In order to share a secret number s, Alice distributed the values $(1, p(1)), (2, p(2)), \ldots, (n+1, p(n+1))$ of a degree n polynomial p with her friends $\text{Bob}_1, \ldots, \text{Bob}_{n+1}$. As usual, she chose p such that $p(0) = s$. Bob_1 through Bob_{n+1} now gather to jointly discover the secret. Suppose that for some reason Bob_1 already knows s, and wants to play a joke on $\text{Bob}_2, \ldots, \text{Bob}_{n+1}$, making them believe

that the secret is in fact some fixed $s' \neq s$. How could he achieve this? In other words, what value should he report in order to make the others believe that the secret is s'?