CS 70 Discrete Mathematics and Probability Theory
Summer 2020 Course Notes **DIS 3C**

1 Polynomial Practice

(a) If f and g are non-zero $\boxed{\text{real}}$ 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.)

(i) $f+g$ $\quad 0, 1 \;;\; \max(\deg f, \deg g)$

(ii) $f \cdot g$ $\quad a_f a_g (x-r_1)\cdots(x-r_{\deg f})\cdot(x-s_1)\cdots(x-s_{\deg g})$

$0, \underbrace{\deg f + \deg g}_{\max}$

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

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

$g(x) = x^2+2$

$f \cdot g(x) = (x^2+1)(x^2+2)$

1) $a(x-r_1)(x-r_2)\cdots(x-r_d)$

2) $a_d x^d + a_{d-1}x^{d-1} + \cdots + a_0$

3) $(x_1, f(x_1)), \ldots, (x_{d+1}, f(x_{d+1}))$

(b) Now let f and g be polynomials over $\boxed{\mathrm{GF}(p)}$.

(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 $a \in \{0, 1, \ldots, p-1\}$?

(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?

1) $p(x)$

$p(1)$ ✓

$p(5) = p(12)$ $GF(7)$

$p(3.14)$ ✗

2) Lagrange Interp.

$$f(x_1)\Delta_1(x) + f(x_2)\Delta_2(x) + \cdots + f(x_n)\Delta_n(x) = f(x)$$

$$\Delta_i(x_i) = 1$$

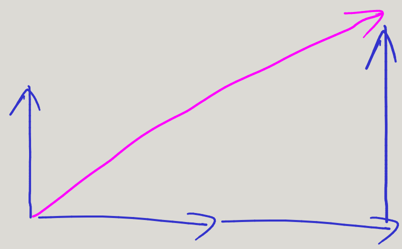
$$\Delta_i(x_j) = 0 \quad \forall j \neq i$$

$$(x_1, f(x_1)), \ldots, (x_n, f(x_n))$$

$$a_1 b_1 + a_2 b_2 + \cdots + a_n b_n = x$$

$$b_i \bmod p_i \equiv 1 \mod p_i$$

$$b_i \bmod p_j \equiv 0 \mod p_j \quad \forall j \neq i$$



3) Secret Sharing

$$(x_1, f(x_1)), \ldots, (x_n, f(x_n))$$

Alice : $(x_1, f(x_1))$

Bob : $(x_2, f(x_2))$

GF(p) Finite field

$+, -, \times, \div, 0, 1$

$\mathbb{R}$

$\mathbb{Q}$

$x + 0 = x$

$x \times 1 = x$

GF(7): $\{0, 1, 2, 3, 4, 5, 6\}$

$+, -, \times, \div, 0, 1$

$x^2 + x - 3$ GF(7)

$$f(4) \equiv 4^2 + 4 - 3 \mod 7$$
$$\equiv 16 + 1 \mod 7$$
$$\equiv 3 \mod 7$$

(i) 5 countries deg 4 poly GF($\cancel{5}$) $\geq 5+3$

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

(ii) at least 2 countries + Sec Gen

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

(1,2) (2,3)

(6,4) (7,3) (8,5)

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 Secrets in the United Nations

poly of deg $d \rightarrow d+1$ pts

A vault in the United Nations can be opened with a secret combination $s \in \mathbb{Z}$. In only two situations should this vault be opened: (i) all 193 member countries must agree, or (ii) at least 55 countries, plus the U.N. Secretary-General, must agree.

(a) Propose a scheme that gives private information to the Secretary-General and all 193 member countries so that the secret combination s can only be recovered under either one of the two specified conditions.

$P(x)$ $\underline{\deg P = 192}$ $GF(\underbrace{347}_{\geq 341})$

$\hookrightarrow$ 1 pt to each country

$\hookrightarrow$ 138 pts to Sect-Gen

$GF(p)$

$\{0, 1, \ldots, p-1\}$

(b) The General Assembly of the UN decides to add an extra level of security: each of the 193 member countries has a delegation of 12 representatives, all of whom must agree in order for that country to help open the vault. Propose a scheme that adds this new feature. The scheme should give private information to the Secretary-General and to each representative of each country.

One poly for each country

1 pt to each rep

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'?