# Dis 3C: Polynomials & Secret Sharing

Wednesday, 8 July 2020 10:00 PM

*2 Representations of polynomials:*

A) value $(x_1, y_1), (x_2, y_2), \ldots, (x_n, y_n)$

B) coefficient $a_n x^n + \cdots + a_1 x + a_0$

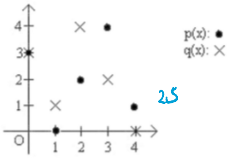
via Lagrange Interpolation

d+1 pts ⇒ deg d poly.

*Useful facts:*

1. 2 pts uniquely determine a line (degree 1 polynomial)
2. A degree d polynomial has at most d roots

Working over a Galois field GF(m) GF(5) mod 5




25

## 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 $g$.)

(i) $f+g$

(ii) $f \cdot g$

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

i) 0 $f(x) = x$, $g(x) = -x+1$

∞ $f(x) = x$, $g(x) = -x$

ii) $\deg(f) + \deg(g)$

0 $(x^2+1)(1) =$

iii) $\deg(f) - \deg(g)$, 0

2 roots 2 roots

$f = x^2+1$, $g = 1$

(b) Now let $f$ and $g$ be polynomials over 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 $a \in \{0, 1, \ldots, p-1\}$?

i) F. $f = 0$ for $x \in \{0, 1, 2, \ldots, k-1\}$

$g = 0$ for $x \in \{k, k+1, \ldots p-1\}$ ⇒ $fg(x) = 0$

ii) $f(x) = a_d x^d + a_{d-1} x^{d-1} + \cdots + a_1 x^1 + a_0$, where $a_d \neq 0$

⇒ $a_0 = a$

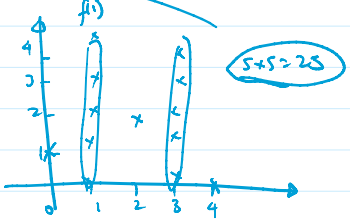
$p^{d-1}$ $p$ → $a_j$ . $j \in \{1, 2, \ldots, d-1\}$

$p-1$ $a_d$ ⇒ $(p-1)\,p^{d-1}$

(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?

$\deg(f) \leq 4$

$f(1)$




5+5 = 25

## 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

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.

poly .... if i) / ii) isn't satisfied no one has enough info

① get a poly $f(x)$, where $f(0) = s$, GF($p$), $p \Rightarrow n$

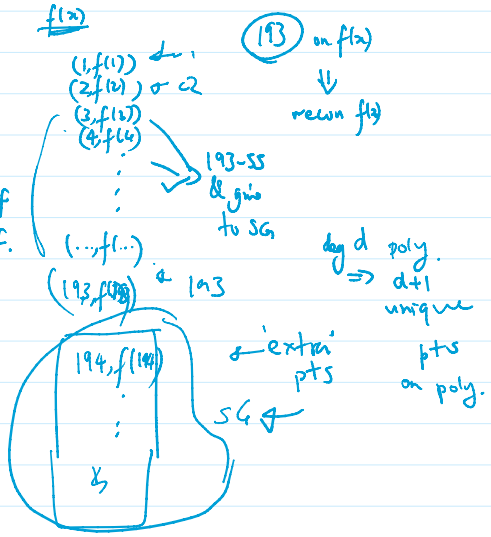
② show it works

$f$ = deg (192) each country gets a pt on $f(x)$

$f$ as deg 192 poly

i) 193 pt $\Rightarrow$ 193 must agree to reconstruct $f$

ii) give SG 193 − 55 pts on $f$. recon. $f$.




(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.

## 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 $p(0) = s$. $\text{Bob}_1$ through $\text{Bob}_{n+1}$ now gather to jointly discover the secret. Suppose that for some reason $\text{Bob}_1$ 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 $s'$?

Lagrange

val. repr ↔ coeff of poly.

$d$ pts → $(d-1)$ degr. poly.

$(x_1, y_1), \ldots, (x_d, y_d)$ ← crosses all these pt.

$p(x) = y_1 \Delta_1(x) + \cdots + y_d \Delta_d(x)$

$\Delta_1(x) = \frac{(x - x_2)\cdots(x - x_d)}{(x_1 - x_2)\cdots(x_1 - x_d)}$ ← by construction

$p(x_1) = y_1 \Delta_1(x_1) + \cdots = y_1 \cdot \frac{(x_1 - x_2)\cdots(x_1 - x_d)}{(x_1 - x_2)\cdots(x_1 - x_d)} + \cdots$

$p(x_1) = y_1 + \cdots + y_2 \Delta_2(x_1) + \cdots + y_d \Delta_d(x_1)$

$\Delta_i(x) = \frac{(x - x_1)(x - x_2)\cdots(x - x_{i-1})(x - x_{i+1})\cdots(x - x_d)}{(x_i - x_1)(x_i - x_2)\cdots(x_i - x_d)}$

$\Delta_i(x_1) =$ top is 0

want to find set of cons. #s

name: $a, a+1, a+2, a+3, \ldots, a+k-1$

want none to be prime pwrs

$\Rightarrow$ want written as product of $\geq 2$ distinct primes

$p_1 p_{k+1} \mid a$

$a = p_1 p_{k+1}$

$a+1 = p_2 p_{k+2}$

$\vdots$

$a+k-1 = p_k p_{2k}$

$p_2 p_{k+2} \mid a+1$

want an $a$ s.t.

$3 \mid 6 \Rightarrow 6 \equiv 0 \pmod 3$

$a \mid x \Rightarrow x \equiv 0 \pmod a$

$a = x + y\, p_1 p_{k+1}$

$a \equiv 0 \pmod{p_1 p_{k+1}}$

$a+1 \equiv 0 \pmod{p_2 p_{k+2}}$

$a+2 \equiv 0 \pmod{p_3 p_{k+3}}$

$\vdots$

$a+k-1 \equiv 0 \pmod{p_k p_{2k}}$

$\Rightarrow a \equiv -1 \pmod{p_2 p_{k+2}}$

$a \equiv -2 \pmod{p_3 p_{k+3}}$

$\vdots$

$x(x^{p-1}-1)$

$x(x^{p-1}-1)$

$x^{\frac{p-1}{2}}$

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

$(x^5 - x) = x(x^4-1)$

$(x\ldots)(x\ldots)(x\ldots)$

$\phi \mid x$

$q \mid x$

if $\phi = \text{prime}^2$

$pq \mid x$

$\Vert$

$(x$

$p_1^2 \mid x \mid \ldots \Rightarrow p_1^2 q_1^2 \mid x$

$p_1^2 \mid x$, $q_1^2 \mid x$ $\Rightarrow$ RHS: $p_1^2 q_1^2 \mid x$

$\gcd(p_1, q_1)$ — contradiction

$\neg$ RHS $\Rightarrow$ $p_1^2 q_1^2 \nmid x$ $\Rightarrow$ $x \equiv b \pmod{p_1^2 q_1^2}$, $b \not\equiv 0 \pmod{p_1^2 q_1^2}$

LHS $\not\Rightarrow$ $x \equiv 0 \pmod{p_1^2}$, $x \equiv 0 \pmod{q_1^2}$

$\searrow$ LHS $\Rightarrow$ $x = k_1 p_1^2 \Rightarrow$, $x = k_2 q_1^2$

$(x^e)^d \equiv x \pmod{N = pq}$, $d = e^{-1} \pmod{(p-1)(q-1)}$

$\Rightarrow de \equiv 1 \pmod{\text{"}}$

$de = 1 + k(p-1)(q-1)$

$\Leftrightarrow x^{1 + k(p-1)(q-1)} - x \equiv 0 \pmod{pq}$

$\Leftrightarrow x\left(x^{k(p-1)(q-1)} - 1\right) \equiv 0 \pmod{pq}$

$\Leftrightarrow pq \mid x\left(x^{k(p-1)(q-1)} - 1\right)$

$\Leftrightarrow p \mid x\left(x^{k(p-1)(q-1)} - 1\right)$

$q \mid \ldots$

$10 \mid 20$ $\Leftrightarrow$ $2 \mid 20$, $5 \mid 20$

$p(x) = a_n x^n + a_{n-1} x^{n-1} + \dots \pmod p$

WLOG $0 \le b \le n-1$

$ax \equiv b \pmod n$

$\gcd(a, n) = d$

$b = k_3 d$

$ax \equiv k_3 d \pmod n$

$k_1 (d) x \equiv k_3 (d) \pmod{k_2 d}$

$k_1$ |

$\gcd(n, a) = d$

$a = k_1 d$

$n = k_2 d$

$ax \equiv b \pmod n$

$k_1 d x \equiv b \pmod{k_2 d}$

$\gcd(k_1, k_2) = 1$

$k_1 x \equiv b \pmod{k_2}$

$a^{(p-1)(q-1)+1} - q \equiv 0 \pmod{pq}$

$a$

FLT + CRT

let $y = a^{(p-1)(q-1)+1}$ for conv.

by FLT:

$y \equiv a \pmod p$

$y \equiv a \pmod q$

this step

$y \equiv a_1 \pmod{m_1}$

$y \equiv a_2$ ⋮

WTS: $y \equiv a \pmod{pq}$

⇒ enter Bezout's theorem + $\gcd(p, q) = 1$

gcd

$1 = x_1 p + x_2 q$

use CRT:

$y = a(q)\left[(q^{-1})_p\right] + a(p)(p^{-1})_q \pmod{pq}$

$$y = a(q)\left[(q^{-1})_p\right] + a(p)(p^{-1})_q \pmod{pq}$$

$(q \bmod p)^{-1}$

$$\equiv a \pmod{pq}$$

$$= a q x_2 + a p x_1$$

$$= a(x_1 p + x_2 q) \pmod{pq}$$

$$= a \times 1 \pmod{pq}$$

$a^{(p-1)(q-1)+1} = y = a \pmod{pq}$