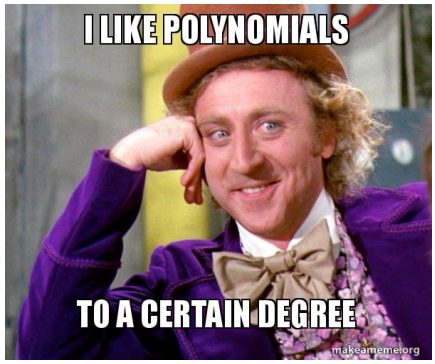
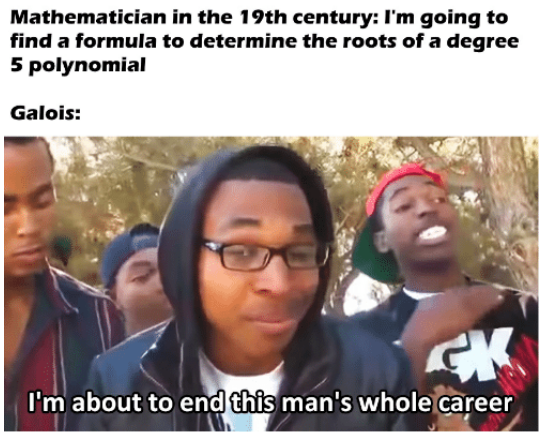
DIS 05A: Polynomials, Secret-Sharing

- Midterm 1 in two weeks (10/13 at 8PM)
- join the disc + add to our playlist





Things to know

- How do I uniquely determine a degree d polynomial? (2 ways)
  1) coeff's, i.e. $a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0$
  2) roots.
- Working over GF(p)
  - Counting polynomials
- Secret Sharing (Shamir's)
- Lagrange Interpolation

QOTD: what's one thing we need more $ in the world?

1 Polynomial Practice

$f = x^3 + 2$

$g = x^6 + x^3$.

(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.)

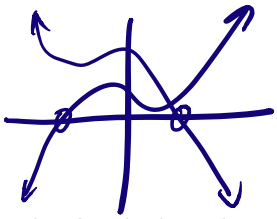
(i) $f+g$

(ii) $f \cdot g$

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

	at least	at most
$f+g$	0 //	$\max(\deg f, \deg g)$
$f \cdot g$	0 //	$\deg f + \deg g$.
f/g	0 //	$\deg f - \deg g$.

↑ even ↑ odd.



(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) False, take $f(x) = x^{p-1} - 1$ & $g(x) = x$. $\Rightarrow x^p - x = 0$

0 at everything but 0 (FLT) 0 at $x = 0$.

$\Rightarrow \boxed{x^p \equiv x \pmod p}$

(ii) $\deg f = d$ need $d+1$ points, have one determined, d choices left

$f(0) = a$.

$\Rightarrow \boxed{p^d}$

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

$\boxed{(p-1)\, p^{d-1}}$

$(p-1) \times p \times \cdots \times p \times 1 = a$

(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?

$\boxed{f(x) = 4x^2 + 1}$

$\deg f \le 2$.

$\Delta_0(x) \to \Delta_0(0) = 1, \Delta_0(2) = 0, \Delta_0(4) = 0$.

$\Delta_2(x) \to \Delta_2(0) = 0, \Delta_2(2) = 1, \Delta_2(4) = 0$

$\Delta_4(x) \to \Delta_4(0) = 0, \Delta_4(2) = 0, \Delta_4(4) = 1$.

$f(x) = 1 \cdot \Delta_0(x) + 2 \cdot \Delta_2(x) + 0 \cdot \Delta_4(x)$.

$f(0) = 1 \cdot \Delta_0(0) + 2 \cdot \Delta_2(0) + 0 \cdot \Delta_4(0)$

$\Delta_0(x) = a(x-2)(x-4)$

$1 = \Delta_0(0) = a(-2)(-4) = 8a$

$a = 1/8 \equiv 3^{-1} \equiv 2$

$\Delta_2(x) = b(x-0)(x-4)$

$2 = \Delta_2(2) = b \cdot (-4)$

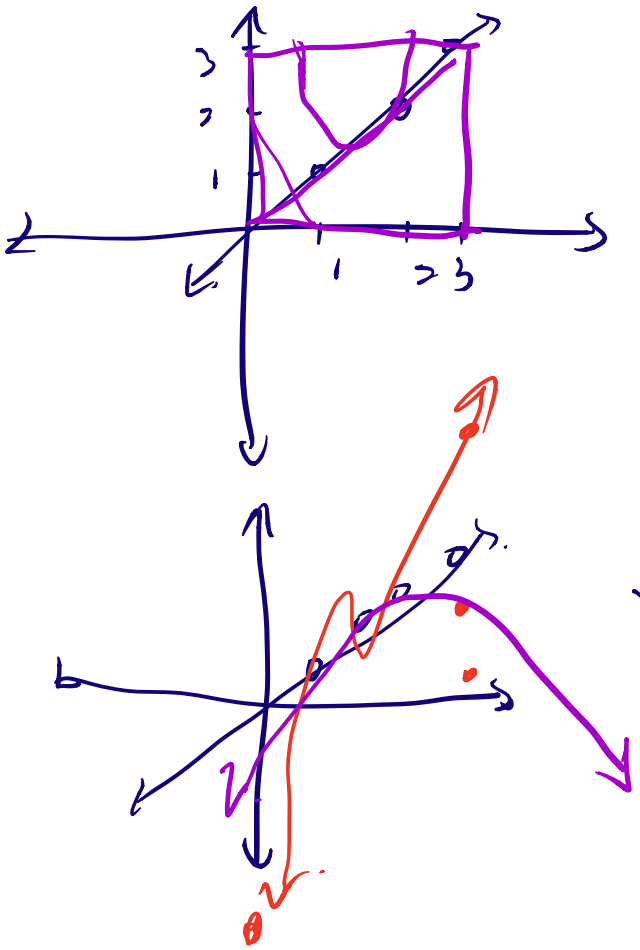
$b = -1/2 \equiv -1 \cdot 2^{-1} \equiv -3 \equiv 2$.

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.



deg ≤ 2 (x-2)(x-3).

coeff's are (mod p)

GF(p) → values are (mod p)

4 pts. ≤ 3,

} w/ 3 pts, still other possibilities

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.

$P(x) = s_0 + a_1 x + a_2 x^2 + \dots$

$s_0 = P(0)$

k $P(1), P(2), \dots P(k)$

reveal $P(x) \Rightarrow P(0)$.

poly needs to be deg ≤ 2.

give each person a point $P(i)$ for $1 \leq i \leq 5$.

$P(1) = 1$ $P(2) = 2$ $P(3) = 3$

$P(x) = x$

(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.

over $GF(n)$.

main $\Rightarrow s_0$

cats: if ≥ 3 cats agree, c_0.

dogs: if ≥ 2 dogs agree, d_0

cat poly is $c(x)$, deg ≤ 2

secret @ $c(0)$, pass out $c(1), c(2), c(3), \dots c(k)$.

dogs poly is $d(x)$, deg ≤ 1.

secret @ $d(0)$. pass out $d(1) \dots$

main: poly is $p(x)$, $p(1) = c_0$ $p(2) = d_0$.

deg ≤ 1. $p(0) = s_0$.

4 Old Secrets, New Secrets

In order to share a secret number s, Alice distributed the values $(1, p(1)), (2, p(2)), \dots, (n+1, p(n+1))$ of a degree n polynomial p with her friends $\text{Bob}_1, \dots, \text{Bob}_{n+1}$. 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 $\text{Bob}_2, \dots, \text{Bob}_{n+1}$, 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'?