CS70 - Lecture 10 Notes

Name: Felix Su SID: 25794773

Spring 2016 GSI: Gerald Zhang

Polynomials

- **Fact**: Any $d+1$ points specifies a distinct degree d polynomial
- **Modular Fact**: Any $d+1$ points specifies a distinct degree d polynomial in mod p space when p is prime
- **Uniqueness Fact**: At most one degree d polynomial hits $d+1$ points

Uniqueness.

Uniqueness Fact. At most one degree d polynomial hits $d+1$ points.

Proof:

Roots fact: Any degree d polynomial has at most d roots.

Assume two different polynomials $Q(x)$ and $P(x)$ hit the points.

$R(x) = Q(x) - P(x)$ has $d+1$ roots and is degree d.
Contradiction.

- **Roots Fact**: Any degree d polynomial has at most d roots

Only d roots.

Lemma 1: $P(x)$ has root a iff $P(x)/(x-a)$ has remainder 0:
$P(x) = (x-a)Q(x)$.

Proof: $P(x) = (x-a)Q(x) + r$.
Plugin a: $P(a) = r$.
It is a root if and only if $r = 0$.
$\square$

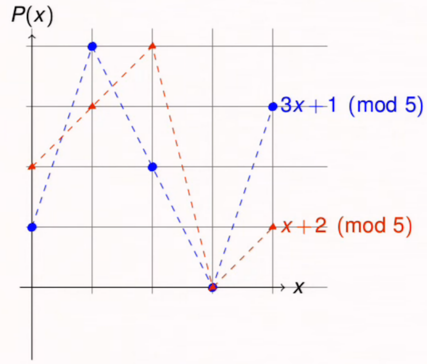
Lemma 2: $P(x)$ has d roots; $r_1, \ldots, r_d$ then
$P(x) = c(x-r_1)(x-r_2)\cdots(x-r_d)$.
Proof Sketch: By induction.

Induction Step: $P(x) = (x-r_1)Q(x)$ by Lemma 1. $Q(x)$ has smaller degree so use the induction hypothesis. $\square$

$d+1$ roots implies degree is at least $d+1$.

Roots fact: Any degree d polynomial has at most d roots.

Polynomial: $P(x) = a_d x^4 + \cdots + a_0 \pmod{p}$



Finding an intersection.
$x+2 \equiv 3x+1 \pmod 5$
$\implies 2x \equiv 1 \pmod 5 \implies x \equiv 3 \pmod 5$
3 is multiplicative inverse of 2 modulo 5.
Good when modulus is prime!!

- Polynomials only map to f(x) at integer values of x
- f(x) is contained in the mod space
- Use delta functions to create meaningful polynomials in mod space

Shamir's k out of n scheme:
Secret $s \in \{0, ..., p-1\}$
Set $a_0 = s$, randomly assign $a_1, ..., a_{k-1}$
Let $P(x) = a_{k-1}x^{k-1} + a_{k-2}x^{k-2} + ... + a0$ with $P(0) = a_0 = s$
Share $(i, P(i) \bmod p)$ with i-th person
k shares gives secret (degree $= d = k-1$, Modular fact, $d+1 = k$ shares gives the polynomial which reveals $P(0) = s$
Solve for polynomial given $d+1$ coordinates

In general..

Given points: $(x_1, y_1); (x_2, y_2) \cdots (x_k, y_k)$.

Solve...

$$
\begin{aligned}
a_{k-1}x_1^{k-1} + \cdots + a_0 &\equiv y_1 \pmod p \\
a_{k-1}x_2^{k-1} + \cdots + a_0 &\equiv y_2 \pmod p \\
&\cdot \\
&\cdot \\
a_{k-1}x_k^{k-1} + \cdots + a_0 &\equiv y_k \pmod p
\end{aligned}
$$

Will this always work?

As long as solution **exists** and it is **unique!** And...

Modular Arithmetic Fact: Exactly 1 degree $\leq d$ polynomial with arithmetic modulo prime p contains $d+1$ pts.

- $d = k-1, d+1 = k$
- Solve system of linear equations to get a_0

Lagrange Interpolation

Delta Function

$$\Delta_i(x) = \begin{cases} 1, & x = x_i \\ 0, & x = x_j \text{ for } j \neq i \\ \text{doesn't matter}, & x = \text{anything else} \end{cases}$$

- 1 at one point (x-value), 0 everywhere else
- valid for a set of x values $x_1, ..., x_{d+1}$
- $y_i \Delta_i(x) = y_i$ because $\Delta_i(x)$ is 1 at x_i and 0 everywhere else
  - ⋆ $P(x) = y_1\Delta_1(x) + y_2\Delta_2(x) + ... + y_{d+1}\Delta_{d+1}(x)$ because at x_i you only get y_i (Δx_i is 0 at anything except x_i)

Formation of Delta Function:
Given points: $(x_1, y_1); (x_2, y_2); ...(x_{d+1}, y_{d+1})$

$$\Delta_i(x) = \frac{\prod_{j \neq i}(x - x_j)}{\prod_{j \neq i}(x_i - x_j)} \tag{1}$$