# CS 70 Discrete Mathematics and Probability Theory
# Spring 2015 Vazirani Discussion 7M

**1. Sanity Check!**

1. What's the minimum number of roots of a degree 4 real polynomial?

2. What's the minimum number of roots of a degree 5 real polynomial?

3. What's the minimum number of roots of a degree 5 polynomial in GF(7)?

4. How many degree at most 3 polynomials are there in GF(7)?

**2. Lagrange Interpolation**

Find a unique real polynomial $p(x)$ of degree at most 3 that passes through points $(-1,3)$, $(0,1)$, $(1,2)$, and $(2,0)$ using Lagrange interpolation.

1. Find $\Delta_{-1}(x)$ where $\Delta_{-1}(0) = \Delta_{-1}(1) = \Delta_{-1}(2) = 0$ and $\Delta_{-1}(-1) = 1$.

2. Find $\Delta_0(x)$ where $\Delta_0(-1) = \Delta_0(1) = \Delta_0(2) = 0$ and $\Delta_0(0) = 1$.

3. Find $\Delta_1(x)$ where $\Delta_1(-1) = \Delta_1(0) = \Delta_1(2) = 0$ and $\Delta_1(1) = 1$.

4. Find $\Delta_2(x)$ where $\Delta_2(-1) = \Delta_2(0) = \Delta_2(1) = 0$ and $\Delta_2(2) = 1$.

5. Construct $p(x)$ using a linear combination of $\Delta_{-1}(x)$, $\Delta_0(x)$, $\Delta_1(x)$ and $\Delta_2(x)$.

## 3. Secret Sharing

Umesh wants to share a secret among 4 TAs and 14 readers, such that a subset of them can reconstruct the secret iff it contains either (i) at least 2 TAs, or (ii) at least 1 TA and at least 2 readers, or (iii) at least 4 readers. Explain how this can be accomplished.

## 4. Polynomial Intersections

Find (and prove) an upper-bound on the number of times two distinct degree $d$ polynomials can intersect. What if the polynomials' degrees differ?