EECS 70 Discrete Mathematics and Probability Theory
Fall 2015 Satish Rao

Discussion 6A

1. RSA Reasoning

In RSA, if Alice wants to send a confidential message to Bob, she uses Bob's public key to encode it. Then Bob uses his private key to decode the message. Suppose that Bob chose $N = 77$. And then Bob chose $e = 3$ so his public key is $(3,77)$.And then Bob chose $d = 26$ so his private key is $(26,77)$.

Will this work for encoding and decoding messages? If not, where did Bob first go wrong in the above sequence of steps and what is the consequence of that error? If it does work, then show that it works.

Solution: e should be co-prime to $(p-1)(q-1)$.
$e = 3$ is not co-prime to $(7-1)(11-1) = 60$, so this is incorrect, since therefore e does not have an inverse mod 60.

2. Roots

Let's make sure you're comfortable with roots of polynomials in the familiar real numbers $\mathbb{R}$. Recall that a polynomial of degree d has at most d roots. In this problem, assume we are working with polynomials over $\mathbb{R}$.

(a) Suppose $p(x)$ and $q(x)$ are two different nonzero polynomials with degrees d_1 and d_2 respectively. What can you say about the number of solutions of $p(x) = q(x)$? How about $p(x) \cdot q(x) = 0$?

Solution: A solution of $p(x) = q(x)$ is a root of the polynomial $p(x) - q(x)$, which has degree at most $\max(d_1, d_2)$. Therefore, the number of solutions is also at most $\max(d_1, d_2)$.

A solution of $p(x) \cdot q(x) = 0$ is a root of the polynomial $p(x) \cdot q(x)$, which has degree $d_1 + d_2$. Therefore, the number of solutions is at most $d_1 + d_2$.

(b) Consider the degree 2 polynomial $f(x) = x^2 + ax + b$. Show that, if f has exactly one root, then $a^2 = 4b$.

Solution: If there is a root c, then the polynomial is divisible by $x - c$. Therefore it can be written as $f(x) = (x-c)g(x)$. But $g(x)$ is a degree one polynomial and by looking at coefficients it is obvious that its leading coefficient is 1. Therefore $g(x) = x - d$ for some d. But then d is also a root, which means that $d = c$. So $f(x) = (x-c)^2$ which means that $a = -2c$ and $b = c^2$, so $a^2 = 4b$.

(c) What is the *minimal* number of real roots that a nonzero polynomial of degree d can have? How does the answer depend on d?

Solution: If d is even, the polynomial can have 0 roots (e.g., consider $x^d + 1$, which is always positive for all $x \in \mathbb{R}$). If d is odd, the polynomial must have at least 1 root (a polynomial of odd degree takes on arbitrarily large positive and negative values, and thus must pass through 0 inbetween them at least once).

3. 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 $\Delta_{-1}(-1) = 1$.

   Solution: $\Delta_{-1}(x) = \frac{x(x-1)(x-2)}{-6}$

2. Find $\Delta_0(x)$ where $\Delta_0(-1) = \Delta_0(1) = \Delta_0(2) = 0$ and $\Delta_0(0) = 1$.
   Solution: $\Delta_0(x) = \frac{(x+1)(x-1)(x-2)}{2}$
3. Find $\Delta_1(x)$ where $\Delta_1(-1) = \Delta_1(0) = \Delta_1(2) = 0$ and $\Delta_1(1) = 1$.
   Solution: $\Delta_1(x) = \frac{(x+1)(x)(x-2)}{-2}$.
4. Find $\Delta_2(x)$ where $\Delta_2(-1) = \Delta_2(0) = \Delta_2(1) = 0$ and $\Delta_2(2) = 1$.
   Solution: $\Delta_2(x) = \frac{(x+1)(x)(x-1)}{6}$.
5. Construct $p(x)$ using a linear combination of $\Delta_{-1}(x)$, $\Delta_0(x)$, $\Delta_1(x)$ and $\Delta_2(x)$.
   Solution: We don't need $\Delta_2(x)$.
   $p(x) = 3 \cdot \Delta_{-1}(x) + 1 \cdot \Delta_0(x) + 2 \cdot \Delta_1(x) + 0 \cdot \Delta_2(x)$.

4. Interpolation Practice

(a) Find a linear polynomial $p(x)$ over $\mathbb{R}$ such that $p(1) = 1$ and $p(3) = 4$.
Solution: We can find $p(x) = a_1 x + a_0$ by solving the system of linear equations

$$\begin{aligned} p(1) &= a_1 + a_0 &= 1 \\ p(3) &= 3a_1 + a_0 &= 4 \end{aligned}$$

However, let us use Lagrange interpolation to illustrate the difference with part (b).
We know the polynomial passes through $(x_1, y_1) = (1, 1)$ and $(x_2, y_2) = (3, 4)$. We form the following Delta functions:

$$\begin{aligned} \Delta_1(x) &= \frac{x - x_2}{x_1 - x_2} = \frac{x-3}{1-3} = -\frac{1}{2}x + \frac{3}{2} && \text{(note that } \Delta_1(x_1) = 1,\ \Delta_1(x_2) = 0) \\ \Delta_2(x) &= \frac{x - x_1}{x_2 - x_1} = \frac{x-1}{3-1} = \frac{1}{2}x - \frac{1}{2} && \text{(note that } \Delta_2(x_1) = 0,\ \Delta_2(x_2) = 1) \end{aligned}$$

Then the polynomial p is given by

$$p(x) = y_1 \Delta_1(x) + y_2 \Delta_2(x) = 1 \cdot \left(-\frac{1}{2}x + \frac{3}{2}\right) + 4 \cdot \left(\frac{1}{2}x - \frac{1}{2}\right) = \frac{3}{2}x - \frac{1}{2}.$$

Note that $p(1) = 1$ and $p(3) = 4$, as desired.

(b) Find a linear polynomial $q(x)$ over $GF(5)$ such that $q(1) \equiv 1 \pmod 5$ and $q(3) \equiv 4 \pmod 5$.
Solution: We use Lagrange interpolation. The Delta functions are:

$$\begin{aligned} \Delta_1(x) &= \frac{x - x_2}{x_1 - x_2} = \frac{x-3}{1-3} \equiv -2^{-1}(x-3) \equiv -3(x-3) \equiv 2x + 4 \pmod 5, \\ \Delta_2(x) &= \frac{x - x_1}{x_2 - x_1} = \frac{x-1}{3-1} \equiv 2^{-1}(x-1) \equiv 3(x-1) \equiv 3x + 2 \pmod 5 \end{aligned}$$

In the calculation above we have used the fact that dividing by 2 is equivalent to multiplying by $2^{-1} \equiv 3 \pmod 5$. Then the polynomial q is given by

$$q(x) = y_1 \Delta_1(x) + y_2 \Delta_2(x) \equiv 1 \cdot (2x+4) + 4 \cdot (3x+2) \equiv 14x + 12 \equiv 4x + 2 \pmod 5.$$

Note that $q(1) \equiv 6 \equiv 1 \pmod 5$ and $q(3) \equiv 14 \equiv 4 \pmod 5$, as desired. Also note that unlike in part (a), here the polynomials Δ_1, Δ_2, and q all have integer coefficients.

Solver.

1. Prepare: comfortable position, pencil, paper, etc.
2. Read hints, suggestions, discuss with partner.
3. Read the problem aloud.
4. Solve on own. You speak, you solve, parter listens.
5. Speak! No need to choose words.
6. Go back over problem; “I’m stuck. I better start over.” “No that won’t work”, “Let’s see...hmmm”
7. Try to solve even trivial problems!

Listener.

1. Listener not a critic. “Please elaborate.” “What are you thinking now?” “Can you check that?”
2. Role: (a) demand that PS keep talking but don’t interrupt. (b) make sure that PS foillows the strategy adn doesn’t skip any of the steps. (c) help PS improve his/her accuracy. (d) help reflect the mental process PS is following. (e) make sure you understnad each step.
3. Do not turn away from PS and start to work on problem!!!!!
4. Do not let PS continue if:
   (a) you don’t understand. “I don’t understand” or “I don’t follow that.”
   (b) when there is a mistake. “Maybe check that”, “Does that sound right”
5. No hints! Point out errors, but no correction.