CS 70	Discrete Mathematics and Probability Theory	
Spring 2015	Vazirani	Discussion 6W

1. CRT Decomposition

In this problem we use the Chinese Remainder Theorem to compute 3^{302} mod 385.

(a) Write 385 as a product of prime numbers in the form $385 = p_1 \times p_2 \times p_3$.

Answer: $385 = 5 \times 7 \times 11$.

(b) Use Fermat's Little Theorem to find 3^{302} mod p_1, 3^{302} mod p_2, and 3^{302} mod p_3.

Answer: Since $3^4 \equiv 1 \pmod 5$, $3^{302} \equiv 3^{4\times 75} \cdot 3^2 \equiv 4 \pmod 5$.
Since $3^6 \equiv 1 \pmod 7$, $3^{302} \equiv 3^{6\times 50} \cdot 3^2 \equiv 2 \pmod 7$.
Since $3^{10} \equiv 1 \pmod{11}$, $3^{302} \equiv 3^{10\times 30} \cdot 3^2 \equiv 9 \pmod{11}$.

(c) Let $x = 3^{302}$. Use part (b) to express the problem as a system of congruences. Argue that there is a unique solution mod 385, and find it. What is the final answer 3^{302} mod 385?

Answer: The system of congruences is:

$$\begin{aligned} x &\equiv 4 \pmod 5 \\ x &\equiv 2 \pmod 7 \\ x &\equiv 9 \pmod{11} \end{aligned}$$

By the CRT, we know there is a unique solution $x \pmod{385}$. By inspection, we see that $x \equiv 9 \pmod{385}$ satisfies the system of congruences above, hence it must be the unique solution. So $3^{302} \equiv 9 \pmod{385}$.

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 $p(x) \cdot q(x) = 0$?

Answer: 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 $a^2 = 4b$.

Answer: 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?

Answer: 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. Roots: The Next Generations

Which of the facts from Problem 2 stay true when $\mathbb{R}$ is replaced by $GF(p)$ (i.e., if you are working modulo a prime number p)? Which change, and how?

Answer: 2(a) and 2(b) continue to hold in any field, but 2(c) is different: Even degree polynomials can still have 0 roots, for example $x^2+1 \pmod 3$. However, we lose the guarantee that every odd degree polynomial must have a root (though we are still assured of this at degree 1, i.e., linear polynomials). For example, $x^3+x+1 \pmod 5$ has no roots.

4. Interpolation Practice

(a) Find a linear polynomial $p(x)$ over $\mathbb{R}$ such that $p(1)=1$ and $p(3)=4$.

Answer: We can find $p(x)=a_1x+a_0$ 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:

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

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 $q(3)\equiv 4 \pmod 5$.

Answer: 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.