EECS 70 Discrete Mathematics and Probability Theory
Spring 2014 Anant Sahai

Discussion 6A

1. Systems of linear equations

Consider the following system of linear equations

$$\begin{cases} x+y+z=0 \\ x-y+3z=5 \\ -4x+2y+z=1 \end{cases}$$

1. Solve in the real numbers (familiar, non-modular arithmetic).
2. Solve in arithmetic modulo 7.

2. Polynomial Interpolation

Let P a polynomial of degree at most 2 such that $P(-1)=3, P(0)=1, P(1)=2$.

1. Find the coefficients of P using the Lagrange interpolation method in the real numbers.
2. Find the coefficients of P using the Lagrange interpolation method in arithmetic modulo 5.
3. Find the coefficients of P by solving a system of linear equations in the real numbers.

3. RSA with multiple keys Members of a secret society know a secret word. They transmit this secret word x between each other many times, each time encrypting it with the RSA method. Eve who is listening to all of their communications notices that in all of the public keys they use, the exponent e is the same. Therefore the public keys used look like $(e,N_1),\ldots,(e,N_k)$ where no two N_i's are the same. Assume that the message is x such that $0 \leq x < N_i$ for every i.

1. Show that if two of the N_i's have a gcd other than 1, then Eve can easily decrypt the word x.
2. Now suppose that every pair of N_i's are co-prime (i.e. they have a gcd of 1). Suppose that Eve has a machine that given the remainders of an unknown number y mod each N_i produces the remainder of y mod $N_1 \times N_2 \times \ldots N_k$. If she uses this machine on all of the encrypted messages, what does she get?
3. Eve knows how to take the t-th root of any real number (not modulo something though) for any t. Using this fact show that if $k > e$ then she can find out the secret word x.

4. Roots

1. Suppose $P(x)$ and $Q(x)$ are two different polynomials over $\mathbb{R}$ with degrees d_1 and d_2 respectively. What can you say about the number of solutions of $P(x)=Q(x)$? How about $P(x)\cdot Q(x)=0$?
2. Let p be a prime. Consider the degree-2 polynomial $f(x)=x^2+ax+b \pmod p$ over $GF(p)$. Show that, if f has exactly one root, then $a^2 = 4b \bmod p$.