CS 70 Discrete Mathematics for CS
Fall 2004 Rao

HW 4

Due Thu, Sept. 30 at 3:29PM (283 Soda)

1. **(5 pts.) Any questions?**
What's the one thing you'd most like to see explained better in lecture or discussion sections? Are lectures too fast, too slow, or just right? Are discussion sections too fast, too slow, or just right? Any comments about what we could have done better in the past week would be appreciated.

2. **(15 pts.) Chinese remaindering**
You want to teach two kids to count up to 15. Unfortunately, they can only count up to five. Here's how you do it: You tell one of them to count up to three and go back to one when the number counted exceeds that. Tell the other to do the same thing up to five. Then you can put together the answers (say, 2 and 4) to find the unique number between 1 and 15 that has these remainders modulo 3 and 5, respectively. (In this example, the only such number is 14.)

   Here we show that this method always works.

   (a) Let $N = p_1 \cdots p_k$ be the product of k distinct primes. Now consider two integers x, y between 1 and N, and their remainders $x_i \equiv x \pmod{p_i}$, $y_i \equiv y \pmod{p_i}$. Show that, if $y_i \equiv x_i \pmod{p_i}$ for all $i = 1, \ldots, k$, then $x \equiv y \pmod{N}$. [Hint: What does $x_i \equiv y_i \pmod{p_i}$ imply for $x - y$?]

   (b) Show that there is a one-to-one correspondence between integers between 1 and N and their k-tuple of remainders modulo $p_i, i = 1, \ldots, k$. In other words, show that there is a bijective map between these two sets. [Hint: How many k-tuples are there? Then use the previous part.]

   (c) (Bonus problem) Find an efficient way of going back from the k-tuple of remainders $x_i \equiv x \pmod{p_i}$ to the unique integer between 1 and N that has these remainders.

3. **(20 pts.) RSA**
Let $p = 17$, $q = 11$ be a RSA private key and $n = pq$, $e = 3$ be the public key. Show your work. Feel free to use a computer to assist with the computations, but do show intermediate results.

   (a) What is the result of encrypting the message $m = 86$ with these keys?

   (b) What is d?

   (c) How would the encrypted message be decrypted?

4. **(20 pts.) Polynomials in one indeterminate**
We will now prove a fundamental result about polynomials: every nonzero polynomial of degree n (over a field F) has at most n roots. If you don't know what a field is, you can assume in the following that $F = \mathbb{R}$ (the real numbers).

   (a) Show that for any $\alpha \in F$, $P(x) = (x - \alpha)Q(x) + b$, where $Q(x)$ is a polynomial of degree $n - 1$ and $b \in F$.

   (b) Show that if α is a root of $P(x)$, then $P(x) = (x - \alpha)Q(x)$.

(c) Prove that any polynomial of degree 1 has at most one root. This is your base case.

(d) Now prove the inductive step: if every polynomial of degree $n-1$ has at most $n-1$ roots, then any polynomial of degree n has at most n roots.

5. (20 pts.) Secret Sharing

(a) Suppose that the teaching staff of a course involves three professors and two TAs. The solutions to the next homework are encrypted by an encryption key shared by all five. The three professors together should be able to access the solutions, or any one TA with one professor, or both TAs. Suggest a secret-sharing scheme that achieves this. (*Hint:* Try weights.)

(b) Suppose now that the class is taught by three professors, each with *her* own two TAs. Any two professors can access the data, as long as one TA from each is also present. Now what?

6. (20 pts.) Error Correction

In this question we will go through an example of error-correcting codes. Since we will do this by hand, the message we will send is going to be short, only $N = 3$ numbers, each mod 5. and the number of errors will be $k = 1$.

(a) First, construct the message Let $a_0 = 4$ and $a_1 = 3$, $a_2 = 2$; then use the polynomial interpolation formula to construct a polynomial $P(x)$ of degree 2 (remember that all arithmetic is mod 5) so that $P(0) = a_0$, $P(1) = a_1$, and $P(2) = a_2$; then extend the message to length $N+2k$ by adding $P(3)$ and $P(4)$. What is the polynomial $P(x)$ and what are $P(3)$ and $P(4)$?

(b) Suppose the message is corrupted by changing a_0 to 0. Use the Berlekamp-Welsh method to find a polynomial $g(x)$ of degree 2 that passes through 4 of the 5 points. Show all your work.