CS 70 Discrete Mathematics for CS
Spring 2006 Vazirani

HW 6

Due Friday March 10

1. (25 pts.) Chinese remainder theorem

Solve the following equations for x modulo the indicated modulus, or show that no solution exists.

(a) Suppose $x \equiv 3 \pmod 5$, $x \equiv 4 \pmod 7$. Find x mod 35.

(b) Suppose $x \equiv 3 \pmod 6$, $x \equiv 6 \pmod 7$, $x \equiv 2 \pmod 8$. Find x mod 504.

(c) Suppose $x \equiv 1 \pmod p$, $x \equiv 0 \pmod q$, and $\gcd(p,q) = 1$. Describe an efficient algorithm $\text{UNIT}(p,q)$ to compute x mod pq given p and q as input.

2. (20 pts.) Secure fingerprinting

(a) We showed in class how to compute a fast fingerprint on a n-bit message x: pick a random prime $p < n^3$, and use $F_p(x) = x \bmod p$ as our fingerprint.

An antivirus company proposes that we use this idea to protect files on our hard disk against attack from viruses. We'll pick a single random prime p, and store p secretly in a safe place. Then, for all of the files $x_1, \ldots, x_k$ on our hard disk, we'll store their fingerprints $F_p(x_1), \ldots, F_p(x_k)$ on the hard disk as well. When the computer boots up, the first thing it will do is check the files on the hard disk against their stored fingerprints using its secret prime p.

Assume a virus can examine and modify everything stored on the hard disk. Assume that the secret prime p is stored in a safe place where no virus can learn it (e.g., on a smartcard). The evil virus writer would like try to inject specially constructed 'errors' into our files, with the hope of avoiding detection. The antivirus company hopes the fingerprinting scheme will be secure against this sort of attack.

What do you think of the antivirus company's proposal?

(b) Describe a better scheme to allow us to verify that stored files have not been modified, under the above assumptions.

3. (15 pts.) Roots

Recall that we showed the following basic fact about the roots of polynomials over a finite field:

Theorem: Let p be prime, and $f(X)$ be a non-zero polynomial of degree d. Then the equation $f(x) \equiv 0 \pmod p$ has at most d solutions for x mod p.

With that background, do the following two problems:

(a) Let p be prime. Argue that every value z has at most 2 square roots modulo p.

(b) If n is a product of k distinct primes and z is relatively prime to n, how many different square roots can z have modulo n (at most)? Explain why.

4. Polynomials

(a) List all the degree 3 polynomials $P(x)$ over GF_3 such that $P(0) = 1$ and $P(2) = 2$.

(b) Use the polynomial interpolation formula to find a polynomial of degree 2, $P(x)$, over the finite field GF_5, such that $P(0) = 4$, $P(1) = 3$ and $P(2) = 2$.

5. Secret Sharing Suppose that the teaching staff of a course involves two professors and three TAs. University regulations require that changes to the database for recording student grades must be carried out either by both professors or one professor and two of the TAs. Suggest a secret-sharing scheme that achieves this. (*Hint:* Try weights.)

6. 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, consisting of $n = 3$ numbers, each modulo 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.