CS 70 Spring 2008 — Discrete Mathematics for CS — David Wagner — HW 6

Due Thursday, March 6th

1. (10 pts.) Break the generator, become a poker champion
A *pseudorandom number generator* is a way of generating a large quantity of random-looking numbers, if all we have is a little bit of randomness (known as the *seed*). One simple scheme is the *linear congruential generator*, where we let x_0 denote the seed and define

$$x_{t+1} = (ax_t + b) \bmod m$$

for some modulus m and some constants a, b. (Notice that $0 \leq x_t < m$ holds for every t.)

You've discovered that a popular web site uses a linear congruential generator to generate poker hands for its players. For instance, it uses x_0 to pseudo-randomly pick the first card to go into your hand, x_1 to pseudo-randomly pick the second card to go into your hand, and so on. For extra security, the poker site has kept the parameters a and b secret, but you do know that the modulus is $m = 2^{31} - 1$ (which is prime).

Suppose that you can observe the values x_0, x_1, x_2, x_3, and x_4 from the information available to you, and that the values $x_5, \ldots, x_9$ will be used to pseudo-randomly pick the cards for the next person's hand. Describe how to efficiently predict the values $x_5, \ldots, x_9$, given the values known to you.

2. (5 pts.) Interpolation practice
Find a polynomial $h(x) = ax^2 + bx + c$ of degree at most 2 such that $h(0) \equiv 3 \pmod 7$, $h(1) \equiv 6 \pmod 7$, and $h(2) \equiv 6 \pmod 7$.

Hint: You could write a system of linear equations in the unknowns a, b, c, or use Question 4 below.

3. (10 pts.) Rational interpolation
Find a non-zero polynomial $g(x) = ax^2 + bx + c$ of degree at most 2 and a non-zero polynomial $h(x) = dx + e$ of degree at most 1 such that $g(0) \equiv 3 \cdot h(0) \pmod 7$, $g(1) \equiv 3 \cdot h(1) \pmod 7$, $g(2) \equiv 2 \cdot h(2) \pmod 7$, and $g(3) \equiv 4 \cdot h(3) \pmod 7$.

Hint: You might try setting up a system of linear equations and solving it.

Important note: The solution $a \equiv b \equiv c \equiv d \equiv e \equiv 0 \pmod 7$ doesn't count. Find any other solution. (Revised 3/2/2008 to add this requirement.)

4. (25 pts.) Polynomial interpolation
In this problem, you will develop an algorithm for polynomial interpolation: given a prime p and n values $a_0, a_1, \ldots, a_n \pmod p$ (where $n < p$), you will show how to construct a polynomial $h(x)$ of degree at most n such that $h(i) \equiv a_i \pmod p$ for $i = 0, \ldots, n$.

(a) Prove the following: If p is a prime and $y_1, \ldots, y_n \in \mathbb{N}$ are all different from 0 modulo p, then $y_1 \times \cdots \times y_n$ is also different from 0 modulo p.

(b) Prove the following: Given a prime p and two integers a, b, it is always possible to find a polynomial $f(x)$ of degree at most 1 such that $f(0) \equiv a \pmod p$ and $f(1) \equiv b \pmod p$.

(c) You are given a prime p and a positive number $n < p$. Show how to find a polynomial $f(x)$ of degree at most n satisfying $f(0) \equiv f(1) \equiv \cdots \equiv f(n-1) \equiv 0 \pmod{p}$ and $f(n) \equiv 1 \pmod{p}$. In other words, the polynomial f should be congruent to zero at the points $x = 0, \ldots, n-1$; at $x = n$ the polynomial should be 1 mod p.

Hint: Consider $F(x) = (x-0)(x-1)(x-2)\cdots(x-(n-1))$; what can you say about it?

(d) You are given p and n as before, but now you are also given an index j with $0 \le j \le n$. Show how to find a polynomial $g_j(x)$ of degree at most n satisfying

$$g_j(i) \equiv \begin{cases} 0 & \text{if } i \neq j \\ 1 & \text{if } i = j \end{cases} \pmod{p} \qquad \text{for each } i = 0, 1, \ldots, n.$$

In other words, the polynomial g_j should be congruent to zero at the points $x = 0, \ldots, n$, except that at $x = j$ it should be congruent to 1 mod p.

(e) You are given a prime p, a number n with $0 < n < p$, and a sequence of values $a_0, a_1, \ldots, a_n \pmod{p}$. Describe an efficient algorithm to find a polynomial $h(x)$ of degree at most n satisfying $h(0) \equiv a_0 \pmod{p}$, $h(1) \equiv a_1 \pmod{p}$, $\ldots$, $h(n) \equiv a_n \pmod{p}$.

Hint: What can you say about the polynomial $3g_0(x) + 7g_1(x)$, where $g_0(x), g_1(x)$ are as defined in part (d)? Does this give you any ideas?