cs70, fall 2001
midterm 2
professor wagner

Problem #1 (18 pts.) Short-answer questions

In each of the following, no justification is required. However, if you give a brief explanation of your answer, we may assign partial credit based on your explanation (if your answer is incorrect), and we reserve the right to deduce points for an incorrect explanation (even if your answer is correct).

(a) [4 pts.] Alice flips a fair coin n times in a row. What is the probability that she receives exactly i heads?

(b) [4 pts.] E and F are events. Also, Pr[E] = 0.2 and Pr[F] = 0.3. What is the smallest value that Pr[E union F] could possibly be? What is the largest it could be?

(c) [5 pts.] How many 2001-bit strings are there that do not contain 01 anywhere as a substring?

(d) [5 pts.] Let n range over the positive integers such that n = 11 (mod 12), and define z = (n+1)/2. For which n is z invertible modulo n?

Problem #2 (12 pts.) Digit sums

Consider the following transformation applied to a natural number n: we write n in decimal, cube each of the digits of n, add them up, and call the results f(n). This defines a function f: **N** --> **N**. For instance, f(13) = 1^3 + 3^3 = 1 + 27 = 28, and f(215) = 2^3 + 1^3 + 5^3 = 8 + 1 + 125 = 134.

Prove that f(n) = n (mod 3) holds for all n (in the natural numbers).

Problem #3 (12 pts.) Computing with polynomials

Let f(x) = Ad*x^d + ... + A1*x + A0 be a polynomial of degree d >= 0 with integer coefficients A0, ..., Ad. Let p be a prime.

When asked to provide running times, give the asymptotic worst-case running time. You may always ignore constant factors. Feel free to use big-O notation if you like.

No proofs are necessary in any part of this question.

(a) [3 pts.] Suppose we compute g(x) = f(x)^2 (mod p) from f(x) using the standard algorithm for polynomial multiplication. Extimate the running time as a function of d and p. You may assume that the coefficients of f have already been reduced modulo p.

(The standard algorithm for multiplying h(x) * h'(x) is just what you learned in high school algebra: multiply each term of h(x) against each term of h'(x), sum them up, and collect terms. For example, (ax+b) * (cx+d) = ax*cx + ax*d + b*cx + b*d = acx^2 + (ad+bc)x + bd.)

(b) [3 pts.] Suppose you are given an integer value u and asked to compute f(u) mod p, i.e., to evaluate f(x) at u modulo p. Estimate the running time as a function of d and p. You may assume that u and the coefficients of f have already been reduced modulo p.

(c) [4 pts.] Suppose you are given an integer value u and asked to compute f(u)^2 mod p, i.e., to evaluate f(x)^2 at u modulo p. How would you do it? Describe a simple approach, and estimate the running time of your approach as a function of d and p. Try to avoid making your approach unnecessarily inefficient. You may assume that u and the coefficients of f have already been reduced modulo p.

Problem #4 (8 pts.) Mystical polynomials

Recall that an integer p is *prime* just if its only divistors are 1, -1, p, and -p, with the exception that 0, 1 and -1 are not considered prime.

A polynomial with integer coefficients is a function f(x) = An*x^n + ... + A1*x + A0, for some integers n>=0 and A0, ..., An. Let's call such a polynomial *mysical* if f(k) is prime for all natural numbers k>=1.

For instance, f(x) = x^2 + 2x + 1 is not mystical, since f(1) = 4 is not prime.

(a) [2 pts.] Is f(x) = x^3 - 6x^2 + 9x + 3 mystical? Justify your answer.

(b) [6 pts.] Professor Green shows you the following result he has prepared on mysical polynomials.

> **Theorem 1** *Let f(x) be a polynomial with integer coefficients satisfying f(0) = 3. Then f(x) is not mystical.*
>
> **Proof:** Consider f(3). Note that f(3) is an integer, since f has integer coefficients. Since f is a polynomial, we may write it as f(x) = An*x^n + ... + A1*x + A0. Then f(0) = An*0^n + ... + A1*0 + A0, so if f(0) = 3, we must have A0 = 3. Moreover, we may calculate
>
> $$f(3) = An*3^n + ... + A1*3 + 3 = An*0^n + ... + A1*0 + 0 = 0 + ... + 0 = 0 \pmod 3$$
>
> which means that 3 is a divisor of f(3). Consequently, f(3) cannot be prime, which implies that f is not mystical.

What's wrong with Professor Green's work? Be specific.

Solutions!