cs70, fall 2001
midterm 2 solutions
professor wagner

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

(a) C(n,i)/2^n

(b) 0.3 <= Pr[E union F] <= 0.5. 0.3 occurs if E is a subset of F, and 0.5 occurs if E and F are disjoint.

(c) 2002, since each such string is of the form [k]1[2000-k]0 (where the quantity in brackets indicates the number of times to repeat) for some k in {0, 1, ..., 2001}, and there are 2002 such k.

(d) All of them, since 2z = n+1 = 1 (mod n), so z-inverse = 2 (mod n). (Alternate explanation: gcd((n+1)/2,n) = gcd((n+1)/2,(n-1)/2) = gcd(1,(n-1)/2)=1 by Euclidean algorithm, so gcd(z,n) = 1, so z has an inverse mod n.)

Problem #2 (12 pts.) Digit sums

Consider an arbitrary natural number n.

Write n in decimal: n = Ak*10^k + ... + A1*10 + A0

Then

```
f(n) = Ak^3 + ... + A1^3 + A0^3          [by defn of f]
     = Ak   + ... + A1   + A0
     = Ak*10^k + ... + A1+10 + A0        [since 10^j = 1 (mod 3) for all j]
     = n (mod 3)
```

n was arbitrary, so this must hold for all natural numbers.

Problem #3 (12 pts.) Computing with polynomials

(a) O(d^2(lg p)^2) There are O(d^2) cross-terms, and each requires O((lg p)^2) work to do a modular multiplication and addition.

(b) O(d(lg p)^2) Computing the sequence 1, u, u^2, ..., u^d mod p takes d multiplications, then multiplying by Ai mod p takes d+1 multiplications, plus d more additions.

(c) 1. Let v = f(u) mod p using part (b).
2. Return v^2 mod p
Takes O(d(lg p)^2 + (lg p)^2) = O(d(lg p)^2) time.

Note that computing f(x)^2 first (using part (c)) then evaluating at u gives a slower algorithm.

Problem #4 (8 pts.) Mystical polynomials

(a) No. f(6) = 57, which is divisible by 3 and hence not prime. (But note that f(3) = 3, which is prime, so f(3) is not a counterexample to f being mystical.)

(b)

> which means that 3 is a divisor of f(3). **Consequently, f(3) cannot be prime**, which implies that f is not mystical.

The bold statement is wrong. The case f(3) = 3 is compatible with 3 dividing f(3), and yet 3 is prime. Hence the underlined statement does not follow, and in fact the polynomial in part (a) gives an example where the reasoning breaks down. Worse still, the "theorem" is wrong: f(x) = 3 is a counterexample (it is mystical).
