CS 70 Discrete Mathematics and Probability Theory
Spring 2011 Demmel HW5

Due Feb 25, 8:00am

You may work in groups of up to 3 people (no larger!). Please read the group collaboration policies on bSpace or `www.cs.berkeley.edu/~demmel/cs70_Spr11` before beginning group work. You *must* write up the solution set entirely on your own. You must never look at any other students' solutions (from any semester, not even a draft), nor share your own solutions (not even a draft).

Please begin your answer to each question on a new sheet of paper, and make sure that each sheet is labeled with your name, GSI name, the assignment number, the question number, and "CS70-Spring 2011".

Turn in each question in a different box in 283 Soda Hall: Question 1 in the box labeled "CS70 - 1", Question 2 in the box labeled "CS70 - 2", etc. Reason: Different problems will be graded in parallel by different readers.

Warning: You risk receiving no credit, or losing points, for any homework that does not conform to the above regulations! Please take the time to write clear and concise solutions; we will not grade messy or unreadable submissions. No late homeworks will be accepted. We will drop the lowest two homework scores.

1. (15 pts.)
Let $\pi(n)$ be the number of primes less than or equal to n. The Prime Number Theorem says that $\lim_{n\to\infty} \frac{\pi(n)}{(n/\ln n)} = 1$, where $\ln n$ is the natural logarithm of n (logarithm base e).

(a) Let n and d be integers, and $x = n \cdot 10^d$. Use the Prime Number Theorem to prove $\lim_{d\to\infty} \frac{\pi\left((n+1)\cdot 10^d\right)}{\pi\left(n\cdot 10^d\right)} = \frac{n+1}{n}$.

(b) Use part (a) to show that given any arbitrary string of decimal digits (representing the integer n), then for all sufficiently large M, there is always a prime p such that (1) p has an M-digit decimal expansion, and (2) p's decimal expansion starts with the given string (representing n). For example, there are infinitely many primes that start with the digits 31415926535.

(c) Repeat part (b) for n a string of bits starting the prime, instead of a decimal string. In other words, show that given any bit string, there are infinitely many primes whose binary expansions start with that bit string.

2. (10 pts.)
Show that if p is prime, then $(p-1)! \equiv -1 \bmod p$. Hint: Every number x in the range from 1 to $p-1$ has a unique multiplicative inverse y in the range 1 to $p-1$. When are x and y different? Try some examples for small primes p to see if you see a pattern.

3. (10 pts.)
Let $p(x) = \sum_{i=0}^{n} a_i x^i$ be a polynomial with nonnegative integer coefficients. Suppose you only have a subroutine that can evaluate $p(x)$ for any integer x, but you are not given the coefficients a_i.

(1) Suppose you knew some upper bound $M \geq \max_i a_i$ on the value of all coefficients. Show that there is a single integer value z where you can

(a) evaluate $p(z)$

(b) determine all the coefficients a_i, knowing just the value of $p(z)$.

(2) How can you compute M, if you are only allowed to evaluate $p(x)$ at one more point?

4. (15 pts.)
a) Prove the following theorem (all variables are positive integers): if m is a prime then for all x, y

$$(x^2 + y^2 \equiv 2 \cdot x \cdot y \bmod m) \text{ if and only if } (x \equiv y \bmod m)$$

b) Is the result still true if m is a product of one or more distinct primes? Justify your answer (with a proof if it is true, or a counterexample if it is not).

c) Is the result true for any $m > 1$? Justify your answer (with a proof if it is true, or a counterexample if it is not).

5. (6 pts.)
You are sent an encoded message $(c_1, c_2, c_3, c_4, c_5, c_6)$ where $c_i = \sum_{j=0}^{3} m_j \cdot i^j \bmod 7$, and the m_j are integers mod 7. You actually receive $(5, X, 2, 5, X, 6)$, where X means "missing". Reconstruct the original message (m_0, m_1, m_2, m_3). Justify your answer.

6. (10 pts.) (Unlucky) ISBN checksums
An ISBN is a 10-digit number that serves as a serial number for books. The last digit is a checksum, which can be helpful for detecting data entry errors when typing in an ISBN. If the first nine digits are given by $x_1, \ldots, x_9$ (where $0 \le x_i \le 9$), the checksum digit x_{10} is given by

$$x_{10} = \bmod(x_1 + 2x_2 + \cdots + 8x_8 + 9x_9, 13).$$

(The checksum "digit" is in the range $0 \le x_{10} \le 12$, with X, Y and Z used to represent 10, 11 and 12. ISBN checksums are actually computed $\pmod{11}$, with X representing 10, but suppose today is Friday the 13th). An equivalent way to describe the ISBN algorithm is like this: the checksum digit x_{10} is chosen so that the following equation is true:

$$12x_1 + 11x_2 + \cdots + 5x_8 + 4x_9 + x_{10} \equiv 0 \pmod{13}.$$

For instance, a sample ISBN is 0201896831; this has a valid checksum, since

$$12 \cdot 0 + 11 \cdot 2 + 10 \cdot 0 + 9 \cdot 1 + 8 \cdot 8 + 7 \cdot 9 + 6 \cdot 6 + 5 \cdot 8 + 4 \cdot 3 + 1 \cdot 1 = 247 \equiv 0 \pmod{13}.$$

For each of the following claims about this checksum algorithm, say whether the claim is true or false. Justify your answer.

1. The ISBN checksum detects all single-digit errors (i.e., all errors where a single digit is entered incorrectly).
2. The ISBN checksum detects all two-digit errors (i.e., all errors where a pair of digits, not necessarily adjacent, are entered incorrectly).
3. The ISBN checksum detects all errors where a pair of adjacent digits are transposed (e.g., where we enter 0021896831 instead of 0201896831).