CS280, Spring 2008: Prelim

The test is out of 50; the points for each question are marked. Don't forget to put your name and student number on each blue book that you use. You can answer the questions in any order, but mark your work clearly. Don't forget to show all your work. Give us a chance to give you partial credit! You have 90 minutes. Good luck!

1. [4 points] Suppose $f : A \to A$ is defined by $f(x) = 3x - 5$. Is f a 1-1 and onto (i.e., injective and surjective) if $A = Z$? What about if $A = Q$ (the rational numbers)? (If you think f is injective or surjective, explain why. If you don't, give a counterexample.)

2. [5 points]

   (a) [1 point] What is an *equivalence relation* on S. (It's enough to just list the three properties of an equivalence relation; you don't have to explain what they are.)

   (b) [4 points] Recall that the *reverse* of a relation R is $\{(b, a) : (a, b) \in R\}$. Let R^r be the reverse of R. Prove that, for any relation R, $R \cup R^r$ is symmetric.

3. [5 points] Consider the following algorithm:

   Input m $\quad [m \in N]$
   $k \leftarrow m$
   $n \leftarrow 0$
   while $k \neq 0$ **do**
   $\quad n \leftarrow n + m$
   $\quad k \leftarrow k - 1$
   end
   return n

   (a) What does this algorithm compute on input m?

   (b) Prove your claim in (a) by using an appropriate loop invariant and induction. (Note that you also have to prove that the algorithm terminates.)

4. [3 points] Explain carefully what the bug is in the following argument:

   > We prove by strong induction that all orders of fish for at least 10 pounds of fish can be filled using only 5-pound fish. Let $P(n)$ be the statement that an order of fish for n pounds of fish can be filled using only 5-pound fish. We prove $P(n)$ for $n \geq 10$. Clearly $P(10)$ is true: an order for 10 pounds of fish can be proved using two 5-pound fish. Suppose that $P(10), \ldots, P(n)$ are all true. We prove $P(n + 1)$. We want to show that

we can fill an order for $n+1$ pounds of fish using 5-pound fish, if $n \geq 10$. By the induction hypothesis, we can fill an order for $n-4$ pounds of fish using 5-pound fish. Add one more 5-pound fish, and we've filled the order for $n+1$ pounds. This completes the induction argument.

5. Suppose the sets $P_0, P_1, P_2, \ldots$ of bit strings (that is, strings of 0s and 1s) are defined inductively by taking $P_0 = \{\lambda\}$ (where λ denotes the empty string, which is taken to have length 0) and $P_{n+1} = P_n \cup \{x11, x01, x10, x11 : x \in P_n\}$. Let $P = \cup_{k=0}^{\infty} P_k$.

   Let Q be the smallest set such that

   - $\lambda \in Q$;
   - if $x \in Q$, then $x00, x01, x10, x11 \in Q$.

   (a) [5 points] Prove that P_n consists of all even strings of length at most $2n$.

   (b) [6 points] Prove that $P = Q$.

6. [4 points] Bob and Alice want to choose a secret key that they can use for cryptography, but all that they have is a bugged phone line, so an eavesdropper can listen to all their messages. Bob proposes that they each choose a secret number. Call Alice's number a and Bob's number b. They also choose, over the telephone number, a prime p and another number q. (Don't worry about exactly how they choose a, b, p, and q. All that matters is that they discuss p and q over the telephone line, so that someone bugging the line will hear what they are.) Bob will then send Alice $bq \bmod p$, and Alice will send Bob $aq \bmod p$. Their key (which they will keep secret) is then $abq \bmod p$. Note that they can both compute $abq \bmod p$. Alice hears $bq \bmod p$ from Bob, and knows a (that's her secret) so she can compute $abq \bmod p$. Similarly, Bob knows b and $aq \bmod p$, so can compute $abq \bmod p$. As Bob explains, their wiretapper will know p, q, $aq \bmod p$, and $bq \bmod p$, but will not know a or b, so their key will be safe (that is, despite hearing all their telephone discussions, an eavesdropper will not be able to figure out $abq \bmod p$.

   Is Bob right? Explain why or why not.

7. [5 points] Use the Extended Euclid's algorithm to find s and t such that $42s + 47t = 1$. (You *must* show the steps of the algorithm. It is not enough to just write down s and t.)

8. [4 points] Show that if n is a composite and $\gcd(n, b) > 1$ then $b^k \not\equiv 1 \pmod{n}$ if $k \geq 1$. Hint: what can you say if $b^k \equiv 1 \pmod{n}$?

9. [4 points] Recall that the ISBN number for a book is given by 10 numbers $a_1, \ldots, a_{10}$ where $a_1, \ldots, a_9$ are in the range 0–9 (inclusive) and a_{10} is in the range 0-10 (in practice, "10" is represented by an x) such that

$$(1 \times a_1) + (2 \times a_2) + \cdots (9 \times a_9) + (10 \times a_{10}) \equiv 0 \pmod{11}. \quad (1)$$

Show that ISBN numbers can detect errors in single digits. More precisely, suppose that the ISBN number of a book is supposed to be $a_1, \ldots, a_{10}$ (so that these numbers satisfy Equation (1)), and a_3 is mistyped as a_3'. Show that a_1, a_2, a_3', a_4, $\ldots$, a_{10} can't be a valid ISBN number. That is, show that it cannot satisfy Equation (1). (The same argument works if any other digit is mistyped, of course.)

10. [5 points] Use the Chinese Remainder Theorem to find *all* integers x that satisfy the following system of congruences:

$$x \equiv 2 \pmod{3}$$
$$x \equiv 1 \pmod{4}$$
$$x \equiv 2 \pmod{7}$$