CS280, Spring 2004: Prelim Solutions

1. [3 points] What is the transitive closure of the relation

$$\{(1,2),(2,3),(3,1),(3,4)\}?$$

Solution: It is $\{(1,2),(2,3),(3,1),(3,4),(1,1),(2,2),(3,3),(1,3),(1,4),(2,4),(2,1),(3,2)\}$.

Grading: You lost two points if the transitive closure did not include the original relation. You lost one point for the first missing element (of additional element) in the transitive closure, and .5 for each additional missing/extra element.

2. [4 points] If f is a function from A to B, and S and T are subsets of B, prove that $f^{-1}(S \cap T) = f^{-1}(S) \cap f^{-1}(T)$.

Solution: Recall that if f is a function from A to B, then f^{-1} maps B to 2^A. If $S \subseteq B$, then $f^{-1}(B) = \{x : f(x) \in B\}$.

We need to show that (a) $f^{-1}(S \cap T) \subseteq f^{-1}(S) \cap f^{-1}(T)$ and (b) $f^{-1}(S \cap T) \subseteq f^{-1}(S) \cap f^{-1}(T)$. For (a), suppose that $x \in f^{-1}(S \cap T)$. Let $y = f(x)$. Then $y \in S \cap T$. Since $y \in S$, $x \in f^{-1}(S)$; similarly $x \in f^{-1}(T)$. Thus, $x \in f^{-1}(S \cap T)$. That proves (a). For (b), suppose that $x \in f^{-1}(S) \cap f^{-1}(T)$. Let $y = f(x)$. We must have $y \in S$, since $x \in f^{-1}(S)$, and $y \in T$, since $x \in f^{-1}(T)$. Thus, $y \in S \cap T$, and $x \in f^{-1}(S \cap T)$.

Grading: Two points for each half of the argument (that is, two points for proving $\subseteq$ and two points for proving $\supseteq$).

3. [6 points] Suppose that R_1 and R_2 are both relations on N, the natural numbers. True or false:

   (a) if R_1 and R_2 are transitive relations, then so is $R_1 \cup R_2$.

   (b) if R_1 and R_2 are reflexive relations, then so is $R_1 \cup R_2$.

   In each case, if you think it's true, prove it. If not, give a counterexample.

Solution: (a) is false. Here is one of many possible counterexamples: Suppose $R_1 = \{(1,2)\}$ and $R_2 = \{(2,3)\}$. Each of R_1 and R_2 is transitive, $R_1 \cup R_2 = I\{(1,2),(2,3)\}$ is not transitive.

(b) is true (no matter what the domain of R_1 and R_2 are). Recall that a relation is a set of ordered pairs, and a relation R is reflexive if, for every element n in R's domain, the pair $(n,n) \in R$. It's OK if the relation has pairs not of the form (n,n). Now on to the proof: If n is in the domain of $R_1 \cup R_2$, then it is in the domain of R_1 or in the domain of R_2, If it is in the domain of R_1, then $(n,n) \in R_1$ (since R_1 is reflexive); if it is in the domain of R_2, then $(n,n) \in R_2$ (since R_2 is reflexive.

Thus, $(n, n) \in R_1 \cup R_2$. Since $(n, n) \in R_1 \cup R_2$ for all n in the domain of $R_1 \cup R_2$, it follows that $R_1 \cup R_2$ is reflexive.

Grading: One point in each case for the right answer. Two points for the counterexample in part (a); two points for the proof in part (b).

4. [8 points] 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) and $P_{n+1} = P_n \cup \{x11, x01, x10, x11 : x \in P_n\}$. Let $P = \cup_{k=1}^{\infty} P_k$.

   Let Q be the smallest set such that

   (a) $\lambda \in Q$;

   (b) if $x \in Q$, then $x00, x01, x10, x11 \in Q$.

   Prove that $P = Q$.

   Solution: We need to show that $P \subseteq Q$ and $Q \subseteq P$. Since Q is the smallest set with properties (a) and (b), to show that $Q \subseteq P$, it suffices to show that P has properties (a) and (b). Clearly it has property (a), since $\lambda \in P_0 \subseteq P$. It also has property (b), since if $x \in P$, then $x \in P_n$ for some n. Then, by definition, $x00, x01, x10, x11 \in P_{n+1} \subseteq P$.

   To prove that $P \subseteq Q$, we prove by induction that $P_n \subseteq Q$. Let $P(n)$ be the statement that $P_n \subseteq Q$. The base case is immediate, since $P_0 = \{\lambda\}$, and $\lambda \in Q$. Suppose that $P_n \subseteq Q$. To see that $P_{n+1} \subseteq Q$, suppose that $x \in P_{n+1}$. Then there exists some $y \in P_n$ such that x is one of $y00, y01, y10, y11$. By the inductive hypothesis, each of $y \in Q$. By definition of Q, it must be the case that $y00$, $y01$, $y10$, and $y11$ are all in Q. Thus, $x \in P_{n+1}$.

   Grading: Four points for each half of the proof. For the second half, you got one point for realizing that you had to prove by induction that $P_n \subseteq Q$ for all n, and three points for the induction argument itself. On the whole, people did quite badly on this problem. There was a problem just like this done in class, and another that was assigned for homework.

5. [3 points] Canada has a two-dollar coin known colloquially as a "toonie". (The one-dollar coin, which has a picture of a loon on it, is called a "loonie".) What is wrong with the following argument, which purports to show that any debt of $n > 1$ Canadian dollars can be repaid (exactly) using only toonies?

   > We proceed by strong induction. Let $P(k)$ be the statement that a debt of k dollars can be repaid exactly using only toonies.
   >
   > The base case is $k = 2$. Clearly a debt of \$2 Canadidan can be repaid with one toonie.
   >
   > Assume that $P(k)$ is true for $k = 2, \ldots, n$. We now prove $P(n + 1)$. By the induction hypothesis, a debt of $n-1$ dollars can be repaid exacatly

using toonies, by the induction hypothesis. Using one more toonie, the debt of $n+1$ dollars can be repaid.

Solution: The problem with this argument is that $n-1$ is not necessarily in the range $2, \ldots, n$. In particular, this is the case if $n = 2$. That means that there will be a problem proving $P(3)$, (where $n = 2$ and $n+1 = 3$). And, indeed, $P(3)$ is false.

6. [8 points] For $n \geq 0$, let $F_n = 2^{2^n} + 1$. (Those numbers F_n which are prime are called *Fermat primes.*)

   (a) [4 points] Prove by induction that $\prod_{r=0}^{n-1} F_r = F_n - 2$ for $n \geq 1$.

   (b) [4 points] Prove that $\gcd(F_m, F_n) = 1$ for all m, n with $m \neq n$. (Hint: use part (a)—which you can use even if you haven't proved it—and some standard facts about divisibility.)

   Solution: Let $P(n)$ be the statement $\prod_{r=0}^{n-1} F_r = F_n - 2$. We prove $P(n)$ for $n \geq 1$. For the base case, note that

$$\prod_{r=0}^{0} F_r = F_0 = 2^{2^0} + 1 = 2^1 + 1 = 3 = F(1) - 2,$$

   since $F(1) = 2^{2^1} + 1 = 5$.

   Assume $P(n)$. To prove $P(n+1)$, note that

$$\begin{aligned} \textstyle\prod_{r=0}^{n} F_r &= (\textstyle\prod_{r=0}^{n-1} F_r) \times F_n \\ &= (F_n - 2)F_n \quad \text{[induction hypothesis]} \\ &= (2^{2^n} - 1)(2^{2^n} + 1) \\ &= 2^{2 \cdot 2^n} - 1 \\ &= 2^{2^{n+1}} - 1 \\ &= F_{n+1} - 2 \end{aligned}$$

   For part (b), suppose, by way of contradiction, that $\gcd(F_n, F_m) = k > 1$. Without loss of generality, suppose that $n > m$. By part (a), $F_n - 2 = \prod_{r=0}^{n-1} F_r$. Therefore, F_m is a factor of $F_n - 2$. Since $k | F_m$, it must be the case that $k | F_n - 2$. Since $k | F_n$, it also be the case that $k | F_n - (F_n - 2)$, that is, $k | 2$. That means $k = 2$. But clearly 2^{2^n} is even, so $F_n = 2^{2^n} + 1$ must be odd. That means $2 \not| F_n$. This is a contradiction.

   Grading: For part (a), you got one point for the base case, and three points for the inductive step.

7. [6 points]

- [2 points] Find all solutions modulo 11 to the quadratic congruence: $x^2 \equiv 1 \pmod{11}$.
- [4 points] Find all solutions modulo p to the quadratic congruence: $x^2 \equiv 1 \pmod{p}$ when p is prime. (It's not enough to list the solutions; you must *prove* that you have found them all.)

Solution:

(a) This part is, of course, a special case of part (b) but it is simple enough to apply brute force. Here is the table of all squares mod 11:

x	0	1	2	3	4	5	6	7	8	9	10
$x^2 \bmod 11$	0	1	4	9	5	3	3	5	9	4	1

From the table, it is clear that if $x^2 \equiv 1 \pmod{11}$, then $x \equiv 1 \pmod{11}$ or $x \equiv 10 \pmod{11}$. (Note for part (b) that $10 \equiv -1 \pmod{11}$.)

(b)

$$\begin{aligned} x^2 \equiv 1 \pmod{p} &\iff p \mid x^2 - 1 \\ &\iff p \mid (x-1)(x+1) \end{aligned}$$

But p is prime so

$$\begin{aligned} p \mid (x-1)(x+1) &\iff p \mid (x-1) \text{ or } p \mid (x+1) \\ &\iff x \equiv 1 \pmod{p} \text{ or } x \equiv -1 \pmod{p}. \end{aligned}$$

Finally, note that

$$\begin{aligned} -1 \equiv 1 \pmod{p} &\iff 2 \equiv 0 \pmod{p} \\ &\iff p \mid 2 \\ &\iff p = 2. \end{aligned}$$

So for $p = 2$ the unique solution is $x \equiv 1 \pmod{2}$ while for $p > 2$ the two solutions are $x \equiv 1 \pmod{p}$ and $x \equiv -1 \equiv p - 1 \pmod{p}$.

Grading: (a) +1 point for each of the correct solutions.
(b) +1 point if you identified *both* solutions (disregarding the $p = 2$ subtlety).
+0-2 points for providing an incomplete proof that there are no other solutions. Otherwise. +3 points for a complete proof.
Solutions of the form $\sqrt{1 + kp}$ got no credit for either parts.

8. [6 points]

(a) [2 points] Define gcd and lcm.

(b) [4 points] Compute lcm(11413,12827).

Solution:

a) The gcd of $a, b \in \mathbb{Z}$ is the greatest $d \in \mathbb{N}^+$ that divides both a and b.
The lcm of $a, b \in \mathbb{Z}$ is the smallest $c \in \mathbb{N}^+$ that is an integer multiple of both a and b.

b) To find the $\text{lcm}(a, b)$ we can use the identity $ab = \gcd(a, b)\,\text{lcm}(a, b)$. The first step is to find gcd(11413,12827) using Euclid's algorithm:

$$\begin{aligned} r_i &= q_i r_i + r_{i+1} \\ 12827 &= 1 \cdot 11413 + 1414 \\ 11413 &= 8 \cdot 1414 + 101 \\ 1414 &= 14 \cdot 101. \end{aligned}$$

So, $\gcd(11413, 12827) = 101$ and

$$\text{lcm}(11413, 12827) = \frac{11413 \cdot 12827}{101} = 1449451.$$

Grading: For part (a), you got one for each definition. For (b), you got three for computing the gcd, and one more for recognizing how to use that to compute the lcm.

9. [6 points] Suppose $A = \{a_1, \ldots, a_n\}$ and $B = \{0, 1\}$.

- [3 points] Show that there are 2^n functions from A to B. (Hint: you don't need induction!)
- [3 points] Show that there are $2^n - 2$ surjective functions from A to B.

Solution: For part (a), note that a function must assign to each a_i, $i = 1, \ldots, n$ either 0 or 1. Thus, for each a_i, there are two choices. By the multiplication rule, there are 2^n such functions. For part (b), note that exactly two of the 2^n functions are *not* surjective: the function that maps each of $a_1, \ldots, a_n$ to 1, and the function that maps each of $a_1, \ldots, a_n$ to 0. The remaining $2^n - 2$ are surjective.