CSE 20, Discrete Mathematics, Fall 1995
Functions, the Pigeon-hole Principle and Partial Orders
Homework 4, Due Wednesday November 29
Answer Key

Full Proofs (12 pts. each):

Palindromes Call a binary string $w = w_1..w_k \in \{0,1\}^k$ a *palindrome* if $w_1..w_k = w_k..w_1$. Prove that there are exactly 2^k palindromes of length $2k$. (Examples: 01110, 1001, 01010, 011110 are all palindromes (because they stay the same if you reverse them; 0111 ,1010, 00001, 0010 are not palindromes. Over the Roman alphabet, madaminedenimadam and ablewasiereisawelba are famous palidromes.) (Hint: there are exactly 2^k words in $\{0,1\}^k$. Give a one-to-one, onto correspondence between the words of length k and the palindromes of length $2k$.)

Let $A = \{0,1\}^k$ be the set of binary words of length k, and let $P = \{p \in \{0,1\}^{2k} | p \text{ is a palindrome}\}$ be the set of palindromes of length $2k$. We want to show $|P| = |A| = 2^k$. We do this by showing two functions that are mutual inverses between the two sets. Let $f(w_1...w_k) = w_1...w_k w_k..w_1$. Then $f(w)$ is always a palindrome of length $2k$, since the $2k - i$'th symbol is equal to the $i+1$'st symbol. So $f : A \rightarrow P$. Let $g : P \rightarrow A$ be defined by $g(p_1, ..p_{2k}) = p_1...p_k$. Then we claim f and g are mutual inverses.

First for any $w_1..w_k \in A$, $g(f(w_1, ..w_k)) = g(w_1..w_k w_k..w_1) = w_1..w_k$.

Secondly, let $p_1...p_{2k} \in P$. Then by the definition of palindrome $p_1..p_{2k} = p_{2k}..p_1$, so $p_1 = p_{2k} p_2 = p_{2k-1}, ..p_{i+1} = p_{2k-i}, ..p_k = p_{k+1}$. Then $f(g(p_1, ..p_{2k}) = f(p_1, .p_k) = p_1..p_k p_k..p_1 = p_1...p_k p_{k+1} p_{k+2}...p_{2k}$. Thus f and g are inverses. So both functions are 1-1 and onto. So $|P| = |A| = 2^k$.

Prove that for any 3 integers, there must be two whose sum is even.

By the pigeonhole principle (where we think of the three numbers as the 3 pigeons and "even" and "odd" as the two pigeonholes) either two of the numbers are even or two are odd. Since the sum of two even numbers is even and the sum of two odd numbers is even, in either case, the sum of these two numbers is even.

Prove that for any number N, there is a number divisible by N whose decimal representation contains only 3's and 0's. (Hint: look at $3 mod N$, $33 mod N$, $333 mod N$, etc.)

Let N be any positive integer. Prove that there is a positive integer n so that $N|n$ and the decimal representation of n has only 3 and 0's as digits. Look at the sequence $3 mod N$, $33 mod N$,... $33333...3 mod N$, where the last in the sequence has $N+1$ digits. Then by the pigeonhole principle, since this is a sequence of $N+1$ numbers between 0 and $N-1$, two must be identical. Then there are $i > j$ so that $333..3(itimes) mod N = 333..3(jtimes) mod N$. Then their difference is evenly divisible by N and in decimal is 33..3 (i-j times) $0..0(jtimes)$. So there is a number n whose digits are all either 3 or 0 where $N|n$.

Say that a program P has l lines. Prove that if P goes for more than l steps without changing the value of a variable, then P is in an infinite loop, i.e., P will never halt. Assume that P never increases the value of any of its variables, all of which are input variables. Describe how to modify P to get an equivalent program P' that always eventually halts on every input; if P halts, P' should have the same output, if P does not halt, P' should output an error message.

(Proofs for this problem can be slightly informal, but still be precise.)

If the program goes for $l + 1$ steps without changing a variable, then at two of these steps, the program must have been executing the same line. (By the pigeonhole principle, since each of $l + 1$ steps executes one of l lines.) If the program has the same line number and the same variable values at two times t_1 and t_2, it will continue to do the same computation that caused the cycle. Thus it will never halt.

To fix the problem, we can introduce for each variable V a new variable V' , and a counter c. Before executing any line of the old program, we save the value of V in V'. After executing the line, we compare each V and V'. If none have changed, we increment c, else we set c to 0. If c ever reaches $l + 1$, we have gone $l + 1$ steps without changing the variables, and so are in an innfinite loop. On the other hand, since P only decreases variables, if we never go $l + 1$ steps without changing a variable, the sum of the variables decreases every l steps, and so we will halt within l(Sum of variables) steps.

Primes Prove that there are exactly $p + 1/2$ quardratic residues modulo p, where $p \geq 3$ is a prime.

The idea is to use the result from the last homework showing $a^2 mod p = b^2 mod p$ if and only if $a \equiv_p b$ or $a \equiv_p p - b$. Then all the quardratic residues will be squares of numbers in the range $0, ..(p-1)/2$

Let $QR_p = \{x^2 mod p | x \in Z\}$ be the set of all quardratic residues modulo p. Let $f : \{0, ...p - 1/2\} \rightarrow QR_p$ be given by $f(x) = x^2 mod p$.

We claim f is 1-1 and onto. To see f is 1-1, assume $a, b \in \{0, 1, .(p-1)/2\}$ so that $a \neq b$ but $f(a) = f(b)$, i.e., $a^2 mod p = b^2 mod p$, Then $a^2 - b^2 mod p = (a^2 mod p - b^2 mod p) mod p = 0 mod p = 0$. In other words, p evenly divides $a^2 - b^2$. Now $a^2 - b^2 = (a - b)(a + b)$, so since if a prime number divides a product, then it divides one of the factors, either p divides $a - b$ or p divides $a + b$. But the first case is impossible, since (assuming without loss of generality that $a > b$), $1 \leq a - b \leq (p-1)/2 < p$. The second case is impossible, since $1 \leq a+b \leq 2(p-1)/2 = p-1$. Thus, since either case leads to a contradiction, the assumption that f is not $1-1$ is wrong, so f is 1-1.

To see f is onto, let $q \in QR_p$. Then $q = x^2 mod p$ for some integer x. Let $x_1 = x mod p$. Then $x_1^2 mod p = x^2 mod p = q$. If $x_1 \leq (p-1)/2$, we have found a a so that $f(a) = q$. If not, let $a = p - x_1$. Then $a^2 = p^2 - 2px_1 + x_1^2 \equiv_p x_1^2 \equiv_p q$, so $f(a) = q$. In either case, $q = f(a)$ for some $a \in 0, ..(p-1)/2$ so f is onto.

Thus, f is one-to-one and onto, so the domain and range of f have the same size. The size of the domain is $(p-1)/2 + 1 = (p+1)/2$. So this is the number of distinct quardratic residues. s On the domain $\{1, , p\}$, the above proof hints at a reason f is not 1-1. Namely, if $p|(a+b)$, then $a^2 mod p = b^2 mod p$. Thus, picking $b = p - a$ for $a \in \{1, ..(p-1)/2\}$ gives us a distinct pair whose squares have the same remainder mod p. This is the equivalent of $x^2 = (-x)^2$ over the real numbers. For example, $a = 1, b = p-1$, we have $a^2 mod p = 1 mod p = 1 = p^2 - 2p + 1 mod p = b^2 mod p$. If p is a composite number, we might have that p divides $a^2 - b^2$ without dividing $a - b$ or $a + b$. For example, $p = 15, a = 4, b = 1$, we have $a - b = 3$ and $a + b = 5$, so p divides neither, but does divide their product. So $1^2 mod 15 = 1 = 16 mod 15 = 4^2 mod 15$.