15-251 : Great Theoretical Ideas In Computer Science

Fall 2013

Assignment 11

Due: Friday, Dec. 6, 2013 11:59 PM

Name: ______________________________

Andrew ID: ______________________________

Question:	1	2	3	4	5	Total
Points:	35	20	10	35	10	110
Score:						

1. Don't Phear the Phi Phunction

Recall from lecture that $\phi(n)$ is the number of positive integers less than or equal to n which are relatively prime to n.

(15) (a) Show that if $gcd(a, b) = 1$, then $\phi(ab) = \phi(a)\phi(b)$

Solution:

(5) (b) Use the above formula and $\phi(p^k) = p^k - p^{k-1}$, p is prime, to evaluate $3^{1201} + 7^{2402} + 11^{3603}$ mod 1000

Solution:

(15) (c) Use induction to show $\Sigma_{d|n}\phi(d) = n$ for any positive integer n.

Solution:

2. Le Petit Fermat

Solve the following problems using Fermat's Little Theorem

(5) (a) Prove that if 5 does not divide n, then $5|n^4 - 1$

Solution:

(5) (b) Prove $12|n^2 - 1$ if the $GCD(n, 6) = 1$

Solution:

(10) (c) Prove that if 5 does not divide $n - 1$, n, or $n + 1$, then $5|(n^2 + 1)$

Solution:

3. You be the Menace

(5) (a) Show that if n is prime, then $(n-1)! = -1 \mod n$.

Solution:

(5) (b) Show that if n is not prime, then $(n-1)! \neq -1 \mod n$.

Solution:

4. Groups

(10) (a) Show that if every element of a group has order 2 except the identity (which always has order 1), then the group is abelian.

Solution:

(10) (b) Show if a and b are elements of an abelian group and a and b have finite order, then ab has finite order.

Solution:

(15) (c) Show that every subgroup of a cyclic group is cyclic.

Solution:

5. Extra Credit

(10) (a) Prove that the language *treg* encoding the set of Turing machines that accept regular languages is undecidable.
[HINT: Show that if there existed a Turing machine T that decided *treg*, then you could use it to solve the Halting problem. For this, on every input (P, ω) of the Halting problem, you must pass an appropriate Turing machine as an input to T.]

Solution: