CSE 311: Foundations of Computing I

Homework 5 (due May 2nd at 11:59 PM)

Directions: *Write up carefully argued solutions to the following problems. Your solution should be clear enough that it should explain to someone who does not already understand the answer why it works. You may use results from lecture, the theorems handout, and previous homeworks without proof.*

1. GCDs are easier than factoring (10 points)

(a) [1 Point] Compute $\gcd(0, 12^{75})$.

(b) [3 Points] Compute $\gcd(138, 69)$ using Euclid's Algorithm.

(c) [6 Points] Compute $\gcd(91, 434)$ using Euclid's Algorithm. Show your intermediate results.

2. Solveit (20 points)

(a) [5 Points] Compute the multiplicative inverse of 17 modulo 122 using the Extended Euclidean Algorithm. Show your work.

(b) [5 Points] Find all solutions x with $0 \leq x < 43$ to the following equation:

$$67x \equiv 3 \pmod{43}$$

Show your work.

(c) [5 Points] Prove that there are no integer solutions to the following equation:

$$51x \equiv 2 \pmod{141}$$

(d) [5 Points] Find all solutions to

$$10x \equiv 70 \pmod{135}$$

using the property that you proved in Problem 5 of Homework 4 ("Modular Numerology").

3. Modular$^{\text{Exponentiation}^{\text{Question}}}$ (10 points)

Compute $3^{70} \bmod 100$ using the efficient modular exponentation algorithm. Show your intermediate results. How many multiplications does the algorithm use for this computation?

4. Palindromes (20 points)

We say an integer is *palindromic* if the digits read the same when written forward or backward. Prove that every palindromic integer with an even number of digits is divisible by 11.

Hint 1: $10 \equiv -1 (\text{mod } 11)$.
Hint 2: Use the base-10 representation of the number as a summation.

5. An Equality (20 points)

Prove that for every positive integer n, the following equality is true:

$$1 \cdot 2^1 + 2 \cdot 2^2 + \cdots + n \cdot 2^n = (n-1)2^{n+1} + 2.$$

6. An Inequality (20 points)

Prove that for all $n \in \mathbb{N}$ and all $x \in \mathbb{R}$ with $x > -2$ the inequality $(2+x)^n \geq 2^n + n2^{n-1}x$ is true.

7. Extra credit: RSA and modular exponentiation (0 points)

We know that we can reduce the *base* of an exponent modulo $m : a^k \equiv (a \text{ mod } m)^k \pmod{m}$. But the same is not true of the exponent itself! That is, we cannot write $a^k \equiv a^{k \text{ mod } m} \pmod{m}$. This is easily seen to be false in general. Consider, for instance, that 2^{10} mod $3 = 1$ but $2^{10 \text{ mod } 3}$ mod $3 = 2^1$ mod $3 = 2$.

The correct law for the exponent is more subtle. We will prove it in steps....

a) Let $R = \{n \in \mathbb{Z} : 1 \leq n \leq m-1 \land \gcd(n,m) = 1\}$. Define the set $aR = \{ax \text{ mod } m : x \in R\}$. Prove that $aR = R$ for every integer $a > 0$ with $\gcd(a,m) = 1$.

b) Consider the product of all the elements in R modulo m and the elements in aR modulo m. By comparing those two expressions, conclude that for all $a \in R$ we have $a^{\phi(m)} \equiv 1 \pmod{m}$, where $\phi(m) = |R|$.

c) Use the last result to show that, for any $b \geq 0$ and $a \in R$, we have $a^b \equiv a^{b \text{ mod } \phi(m)} \pmod{m}$.

d) Finally, prove the following two facts about the function ϕ above. First, if p is prime, then $\phi(p) = p-1$. Second, for any positive integers a and b with $\gcd(a,b) = 1$, we have $\phi(ab) = \phi(a)\phi(b)$.

The two facts from part d imply that, if p and q are primes, then $\phi(pq) = (p-1)(q-1)$. That along with part c prove of the final claim from lecture about RSA, completing the proof of correctness of the algorithm.