CSE 311: Foundations of Computing I

Homework 5 (due Feb 12, 2020 at 11:00 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. Read the CSE 311 grading guidelines from the course webpage for more details and for permitted resources and collaboration.*

1. GCDs are easier than factoring (10 points)

(a) [1 Point] Compute $\gcd(0, 1275965)$.

(b) [3 Points] Compute $\gcd(217, 69)$ using Euclid's Algorithm.

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

2. Inverted Sugar (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. 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. (No induction proofs.)

Hint 1: $10 \equiv -1 (\text{mod } 11)$.
Hint 2: Write the number in terms of its $2n$ decimal digits as $d_0 + d_1 \cdot 10 + d_2 \cdot 10^2 + \cdots d_{2n-1} \cdot 10^{2n-1}$

4. The Prime Generation (10 points)

Prove or disprove: For every integer $x > 0$, $x^2 + x + 41$ is a prime number.

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: Exponential Fun (0 points)

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

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

a) Let $R = \{n \in \mathbb{Z} : 1 \leq n \leq m-1 \wedge \gcd(n,m) = 1\}$. Define the set $aR = \{ax \bmod m : x \in R\}$. 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 $a^{\varphi(m)} \equiv 1 \pmod m$, where $\varphi(m) = |R|$.

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

d) Now suppose that $y = x^e \bmod m$ for some x with $\gcd(x,m) = 1$ and integer $e \geq 0$ such that $\gcd(e, \varphi(m)) = 1$. Let $d = e^{-1} \bmod \varphi(m)$. Prove that $y^d \equiv x \pmod m$.

e) Prove the following two facts about the function φ: 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 $\varphi(ab) = \varphi(a)\varphi(b)$.

These facts together form the basis for the most widely used public key encryption system. One chooses $m = pq$ for large primes p and q, and chooses a nice value of e. To send a message x one computes $y = x^e \bmod m$ and sends the encryption y. To decrypt, one computes $y^d \bmod m$. Its security relies on it being hard to compute d from just e and m. What are some things that could go wrong with this scheme?