CSE 311: Foundations of Computing I

Homework 5 (due May 10th 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. However, you may use results from lecture, the theorems handout, and previous homeworks without proof.*

1. down: Gnawing Carrots Delightedly (10 points)

(a) [1 Point] Compute $\gcd(8234742112, 0)$.

(b) [3 Points] Compute $\gcd(180, 36)$ using Euclid's Algorithm. Show your intermediate results.

(c) [6 Points] Compute $\gcd(170, 332)$ using Euclid's Algorithm. Show your intermediate results.

2. across: Because I Was (20 points)

(a) [5 Points] Compute the multiplicative inverse of 11 modulo 103 using the Extended Euclidean Algorithm. Your answer should be a number between 0 and 102. Show your work.

(b) [5 Points] Find all solutions x to the equation:

$$11x \equiv 4 \pmod{103}$$

It is not sufficient just to state the answer. You need to *prove* that your answer is correct.

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

$$8x \equiv 5 \pmod{20}$$

Note: this does not follow from (just) the fact that 8 does not have a multiplicative inverse modulo 20. That argument, if true, would apply to the equation $8x \equiv 8 \pmod{20}$, which actually does have solutions (e.g., $x = 1$)! Hence, a different argument is required to show that this equation has no integer solutions.

Hint: By De Morgan, there does not exist a solution if and only if every $x \in \mathbb{Z}$ is not a solution. Hence, one way to prove this is to assume that x satisfies the above equation and establish that this is a contradiction. That would show that the assumption (that x was a solution) is false.

(d) [5 Points] Find **all** solutions to the equation

$$55x \equiv 20 \pmod{515}.$$

Use the property that you proved in Problem 5 of Homework 4 ("Weekend At Cape Mod").

3. down: Rabbit Population Model (10 points)

(a) [7 Points] Compute $3^{273} \bmod 100$ using the efficient modular exponentiation algorithm. Show all intermediate results.

(b) [1 Point] How many multiplications does the algorithm use for this computation?

(c) [1 Point] For the multiplications performed by the algorithm, what is the maximum number of decimal digits in the result?

(d) [1 Point] Suppose that we instead computed the integer 3^{273}. How many decimal digits does it have?

4. across: A Man, A Plan, A Canal (20 points)

We say an integer is *palindromic* if the digits read the same when written forward or backward. Show that every palindromic integer with an even number of digits is divisible by 11. (No induction proofs.)

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

5. across: Edgar Martinez, 2019 (20 points)

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

$$6 \cdot \sum_{k=1}^{n} k^2 = n(2n^2 + 3n + 1)$$

6. across: Alligator Eats The Bigger One (20 points)

Prove that for all integers n with $n \geq 1$, we have $n \cdot 4^n \leq (n+8)!$.

7. across: Rabbit-Safe Asparagus [Extra credit] (0 points)

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 $a^{\phi(m)} \equiv 1 \pmod{m}$, where $\phi(m) = |R|$.

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

(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 primes a and b with $a \neq b$, we have $\phi(ab) = \phi(a)\phi(b)$. (Or slightly more challenging: show this second claim for *all positive integers* a and b with $\gcd(a, b) = 1$.)

The second fact of part (d) implies 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.

Answer Sheet (Optional)