CSE 311: Foundations of Computing I

Homework 5 (due November 5th 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. It's Feedback Time (0 points)

Approximately how much time (in minutes) did you spend on each problem of this homework? Were any problems especially difficult or especially interesting?

2. A Wink and a Mod (12 points)

Compute each of the following using Euclid's Algorithm. Show your intermediate results, both as a sequence of recursive calls and in tableau form (showing just the divisions performed, as shown in lecture).

(a) $\gcd(344, 124)$

(b) $\gcd(56, 252)$

(c) $\gcd(2^{32} - 1, 2^1 - 1)$

3. The Mod Couple (24 points)

(a) [10 Points] Compute the multiplicative inverse of 15 modulo 101 using the Extended Euclidean Algorithm. Your answer should be a number between 0 and 100. Show your work in tableau form (the divisions performed, the equations for the remainders, and the sequence of substitutions).

(b) [6 Points] Find all integer solutions $x \in \mathbb{Z}$ to the equation

$$15x \equiv_{101} 4$$

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

(c) [4 Points] Prove that there are no integer solutions to the equation

$$7x \equiv_{21} 16$$

Note: this does not follow from (just) the fact that 7 does not have a multiplicative inverse modulo 21. That argument, if true, would apply to the equation $7x \equiv_{21} 14$, which actually does have solutions (e.g., $x = 2$)! 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) [4 Points] Prove that all solutions to the equation in part (b) are also solutions to

$$50x + 8 \equiv_{101} 5x + 20$$

4. Mod Squad (12 points)

We say an integer is *palindromic* if its digits, when written in decimal (with no leading zeros), form a palindrome. Show that every palindromic integer with an even number of digits is divisible by 11. (Do not use induction.)

Hint: $10 \equiv_{11} -1$

5. Modding Off (12 points)

(a) [10 Points] Compute $3^{298} \bmod 100$ using the efficient modular exponentiation algorithm. Show all intermediate results.

(b) [1 Point] How many multiplications does the algorithm use for this computation? (Assume that we do not need to perform a multiplication to calculate $3^1 = 3$ since we know that $x^1 = x$ for any x.)

(c) [1 Point] The integer 3^{298} has 143 digits, so calculating $3^{298} \bmod 100$ by first calculating 3^{298} and then reducing it modulo 100 would require storing a 143-digit number.

If we calculate $3^{298} \bmod 100$ as in part (a), with each of the modular multiplications $(a \times b) \bmod 100$ performed by calculating the integer $a \times b$ and then reducing it modulo 100, what is the largest number of digits that could appear in any number?

6. Induction Worker (20 points)

Prove, by induction, that $n^3 + 2n$ is divisible by 3 for any positive integer n.

7. Alien Induction (20 points)

Prove that for all integers n with $n \geq 1$, we have $n \cdot 4^n \leq (n+8)!$, where $k!$ is defined for any $k \geq 1$ to be the product $k \cdot (k-1) \cdot \ldots \cdot 2 \cdot 1$. (For example, $5! = 5 \cdot 4 \cdot 3 \cdot 2 \cdot 1 = 120$.) Note that $(k+1)! = (k+1) \cdot k!$.

8. Extra Credit: Walk Like an Encryption (0 points)

We know that we can reduce the *base* of an exponent modulo m : $a^k \equiv_m (a \bmod m)^k$. But the same is not true of the exponent! That is, we cannot write $a^k \equiv_m a^{k \bmod m}$. 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 $a^{\phi(m)} \equiv_m 1$, where $\phi(m) = |R|$.

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

(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.