CSE 311: Foundations of Computing I

Homework 5 (due November 1st 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. A Modding Acquaintance (10 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) $\gcd(44, 180)$

(b) $\gcd(340, 178)$

(c) $\gcd(2^{32} - 1, 2^0 - 1)$.

2. Mod Squad (22 points)

(a) [5 Points] Compute the multiplicative inverse of 15 modulo 103 using the Extended Euclidean Algorithm. Your answer should be a number between 0 and 102. Show your work in tableau form (the divisions performed, the equations for the remainders, and the sequence of substitutions).

(b) [8 Points] Find all integer solutions $x \in \mathbb{Z}$ to the equation

$$15x \equiv 11 \pmod{103}$$

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

(c) [6 Points] Prove that there are no integer solutions to the equation

$$10x \equiv 3 \pmod{15}$$

Note: this does not follow from (just) the fact that 10 does not have a multiplicative inverse modulo 15. That argument, if true, would apply to the equation $10x \equiv 10 \pmod{15}$, 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) [3 Points] Prove that all solutions to the equation in part (b) are also solutions to

$$34x + 3 \equiv 4x + 25 \pmod{103}.$$

3. Two Peas In a Mod (10 points)

(a) [7 Points] Compute $3^{338} \bmod 100$ 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^{338}. How many decimal digits does it have?

4. Weekend At Cape Mod (18 points)

Let m and n be positive integers.

(a) [6 Points] Prove that, if $a \equiv b \pmod{m}$ and $a \equiv c \pmod{n}$, then $b \equiv c \pmod{d}$, where $d = \gcd(m, n)$.

(b) [10 Points] Prove that, if $b \equiv c \pmod{d}$, with $d = \gcd(m, n)$, then there exists some $a \in \mathbb{Z}$ such that $a \equiv b \pmod{m}$ and $a \equiv c \pmod{n}$.

Hint: Start by applying Bézout's theorem to m and n. Then, use the assumption to find a number of the form $c + (\dots)n$ that is also of the form $b + (\dots)m$.

(c) [2 Points] Explain why the pair of congruences, $a \equiv b \pmod{m}$ and $a \equiv c \pmod{n}$, has a solution if and only if $b \equiv c \pmod{d}$, where $d = \gcd(m, n)$.

5. Master of Induction (20 points)

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

6. Super Colliding Super Inductor (20 points)

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

7. RSA [Extra credit] (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 $R = \{n \in \mathbb{Z} : 1 \leq n \leq m-1 \wedge \gcd(n, m) = 1\}$. 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 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.