TEST #2

MAT 4/521 (NUMBER THEORY)

Directions: Solve *five* of the following *eight* problems: three in Part I, two in Part II. Each is worth 10 points. If you find yourself struggling; I can "sell" you a hint if it helps earn more points in return. (One percent penalty per hint.) I have sometimes used small numbers to save time. *Do not* abuse this by resorting to brute force by, for instance, listing all possible solutions and eliminating the ones that do not work: That will earn no points.

Part 1. Solve three problems. These problems are primarily computational.

1. Solve each system of simultaneous congruences *without* using brute force. Is there more than one solution? If so, is there a modulus with only one?
   (a) $x \equiv 4 \pmod 5$ and $x \equiv 5 \pmod 7$
   (b) $x \equiv 5 \pmod{10}$ and $x \equiv 6 \pmod{14}$

2. Solve the following congruences. If no solution is possible, indicate the reason.
   (a) $x^5 \equiv 7 \pmod 9$
   (b) $x^5 \equiv 6 \pmod 9$

3. (a) Why must every prime number be congruent modulo 8 to 1, 3, 5, or 7?
   (b) Show that there are infinitely many primes that are congruent to 3 modulo 8, *without* using Dirichlet's Theorem.

4. Consider the following card trick: (continues on back/next page)

   (1) Have the audience pick one of 12 cards.
   (2) Lay the cards in 3 columns, and ask the audience to indicate the column that contains their card. Let a be that number.
   (3) *Preserving the order of the cards,* lay the cards in 4 columns and ask the audience to indicate the column that contains their card. Let b be that number.
   (4) Let $c = 4a - 3b$. Add 12 to c if need be to make it positive. Count c cards; this is the audience's card.

   (a) Explain how this problem is related to the Chinese Remainder Theorem.
   (b) Show that the formula for c is correct.
   (c) Suppose we wanted to work with 21 cards, instead. Explain why the trick should still work, as long as we change c appropriately. Indicate how the game would change: would the number of columns change in any step? what would the formula for c be? would we still add 12, or a different number?

Date: Summer 2015.

Part 2. Solve two problems. The solution to these problems must include a *thorough* explanation or a proof for your answer. It is a good idea to do an example or two (or ten) with concrete numbers, but doing that alone will net you relatively little credit.

5. Show that a number of the form $3^i 5^j 7^k$ cannot be perfect.

6. This problem is related to Mersenne primes.
   (a) Show that $3^n - 1$ is never prime if $n \geq 2$.
   (b) Show that if n is even, then $3^n-1/2$ is not prime.
   (c) Find a value of n for which $3^n-1/2$ is prime.

7. Do *only one* of the following. The encoding of a message (transformation from characters to numbers) is the same as the one used in homework: $0 \mapsto 0$, $1 \mapsto 1$, …, $9 \mapsto 9$, space$\mapsto 10$, A$\mapsto 11$, B$\mapsto 12$, …, Z$\mapsto 36$.
   (a) The following message was encrypted using RSA with the public key $m = 39$ (modulus) and $k = 5$ (exponent). Find your private key and decrypt the message below.

   24, 25, 25, 18, 25, 25

   (b) The following message was encrypted using El Gamal with the public key $m = 37$ (modulus) and $\alpha^a = 7$ (multiplier). Your private key is $b = 2$. Decrypt the message below.

   19, 4, 4, 20, 9, 18, 4, 33

8. (a) Show that if $1 \leq a < m$ and $\gcd(m,a) = 1$ then $\gcd(m-a,a) = 1$.
   (b) Let $a_1, a_2, \ldots, a_{\phi(m)}$ be the numbers between 1 and m relatively prime to m. Consider the quantity
   $$\frac{A_m}{B_m} = \frac{1}{a_1} + \frac{1}{a_2} + \cdots + \frac{1}{a_{\phi(m)}}.$$
   Show that the unreduced $A_m \equiv 0 \pmod{m}$. Then explain why this remains true even if we reduce A_m/B_m to lowest terms.
   Hint: The answer to part (a) would be *really* helpful.