NUMBER THEORY MIDTERM PRACTICE

0. Solve the system of congruence:

$$\begin{aligned} 3x &\equiv 1 \mod 5 \\ 2x &\equiv 1 \mod 7 \\ 4x &\equiv 2 \mod 6 \end{aligned}$$

1. Let p be a prime.
   (1) Show that $p|\binom{p}{k}$ for $1 \leq k \leq p-1$.
   (2) Show that $(a+b)^p \equiv a+b \mod p$. (Hint: binomial theorem.)

2. Find $(189, 1239)$ by using Euclidean algorithm. Find integers x, y such that $189x + 1239y = (189, 1239)$. Find a formula for all integer solutions to the equation.

3. Show that $\phi(n)$ is even when $n > 2$.

4. Suppose we have integers x, y, z such that

$$x^3 + y^3 \equiv z^3 \mod 7$$

   (1) Show that if 7 does not divide x, then $x^3 \equiv \pm 1 \mod 7$.
   (2) Deduce that $7|xyz$.

5. Show that $\sqrt{p}$ is irrational for any prime p.

6. Let q be an integer. Suppose for any a, b, we know that $q|ab \Rightarrow$ either $q|a$ or $q|b$. Show that if $d|q$, then either $d = 1$ or $d = q$.

7. Suppose $(a, b) = d$, show that
   (1) For any positive n, $\phi(n^2) = n\phi(n)$. (Hint: show this for $n = p^k$ first. Or you can use a previous homework assignment.)
   (2) Show that $\phi(d)\phi(ab) = d\phi(a)\phi(b)$.

8. Can -1 be a quadratic residue in some congruence classes?

9. Let p be a prime.
   (1) What is the definition of the order of 2 in the congruence class mod N?
   (2) Show that if $2^k \equiv 1 \mod N$, then order of 2 divides k. (Hint: let order of 2 be d. If this is not true, then $k = dq + r$. Consider 2^{dq+r}.)
   (3) Let $N = 2^p - 1$. Show that $2^p \equiv 1 \mod N$. Deduce that order of 2 is p.
   (4) Show that $p|\phi(N)$.
   (5) Show that $p|2^p - 2$ for all primes, and conclude that $2^{N-1} \equiv 1 \mod N$, where N is defined in (3).

10. Find an upper bound for each of the functions $\phi(n), \tau(n), \sigma(n)$. That is, find numbers N_1, N_2, N_3, such that $\phi(n) \leq N_1, \tau(n) \leq N_2, \sigma(n) \leq N_3$. ($N_i$ should be expressed in terms of n.)

Date: October 17, 2020.