Math 246S: Homework 3

Due at the beginning of tutorial

Tuesday, Jan 31, 2012 at 8:10 PM sharp!

(1) Let m, n be natural numbers. Prove that if d divides both m and n then d divides the g.c.d.(m, n).

(2) The converse to Wilson's Theorem is proven in the textbook (Theorem 5.7 and Theorem 5.8). Write the proof in your own words.

(3) (a) Write the addition and multiplication tables for numbers modulo 7. Which numbers have a (mutiplicative) inverse modulo 7?
(b) Write the addition and multiplication tables for numbers modulo 8.Which numbers have a (mutiplicative) inverse modulo 8?

(4) Find the greatest common divisor of 1352 and 495 in two ways: by using the Euclidean algorithm and also by factoring each number into primes.

(5) Let p and q be distinct primes. Suppose a, b are integers satisfying $a \equiv b \ \ (\ mod\, p \ )$ and $a \equiv b \ \ (\ mod\, q \ )$. Show that $a \equiv b \ \ (\ mod\, pq \ )$.

(6) Let p and q be distinct primes and a a natural number relatively prime to pq. Prove that $a^{(p-1)(q-1)} \equiv 1 \ \ (\ mod\, pq \ )$. Hint: you can use Fermat's Little Theorem and exercise number (5) above.

(7) Find $10^{5^{101}} \ \ (\ mod\, 21 \ )$.

(8) For each of the following, find the remainder when a is divided by m:
(a) a $= 6^{229} - 4$; $m = 5$.
(b) a$=207^{321} + 689!$; $m = 7$.
(c) a=873645768765 ; m=9.
(d) a=(123)(45)(678)(910)(112) ; m=6.