HOMEWORK ASSIGNMENT #7, DUE MONDAY, 11/15/2010

Notice that this assignment is due on Monday instead of Friday, because of the second midterm. You can use a calculator to calculate products mod n.

(1) Consider the group $(\mathbb{Z}/n\mathbb{Z}, +)$.
   (a) Show that the order of $a \mod n$ in this group is equal to $n/\gcd(a, n)$.
   (b) Let d be a positive integer which divides n. Find the number of elements of $(\mathbb{Z}/n\mathbb{Z}, +)$ with order d.

(2) Suppose m, n are positive integers which are not coprime. Show that $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ is not isomorphic to $\mathbb{Z}/nm\mathbb{Z}$. (In particular this shows that $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ is not cyclic.)

(3) Suppose m, n are positive integers which are coprime. Show that $U_n \times U_m$ is isomorphic to U_{mn}.

(4) (a) Show that 5 is a primitive root mod 18.
   (b) Which powers of $5 \mod 18$ are also primitive roots mod 18?

(5) $p = 229$ is a prime. How many elements of U_{229} are
   (a) squares in U_{229}?
   (b) cubes in U_{229}?
   (c) eighth powers in U_{229}?

(6) Show that 112 is a primitive root mod 11, but not a primitive root mod 121. Find a primitive root mod 121.

(7) (a) True or false: suppose p, q are odd primes. If g is a primitive root mod p and mod q, then g is a primitive root mod pq.
   (b) True or false: suppose p is an odd prime, $e \geq 1$. If g is a primitive root mod 2 and mod p^e, then g is a primitive root mod $2p^e$.