Homework #6

1. (a) Find a primitive root $\mod 23$
   (b) For each positive divisor d of 22, find the number of integers among 1,...,22 whose orders $\mod 23$ are d and then verify the equality
   $$\sum_{d|22} \phi(d) = 22$$
   (c) Let r be the primitive root you found in (a). Use it to express every integer from 1 to 22 as a power of r.
   (d) Use the data you obtain form (c) to decide whether the congruence $x^5 \equiv 7 \mod 23$ has a solution. If it does, find all the solutions $\mod 23$.

2. Let p be an odd prime and r be a primitive root modulo p. Recall:

   Wilson's Theorem: $(n-1)! \equiv -1 \mod n$ if and only if n is prime.

   Using Homework 5 problem 2(a) and Theorem 6.3, give an alternate proof of Wilson's Theorem.

3. Solve the congruences (i) $7x^3 \equiv 3 \mod 11$; (ii) $3x^4 \equiv 5 \mod 11$; (iii) $x^8 \equiv 10 \mod 11$.

4. On Wednesday November 14th at 2:00-2:50 in 446 College Hall there will be a seminar talk "The mathematical key to unlocking the mysteries of cryptography" by Ben Kane. Come to the talk and write down three facts (things you didn't already know abut cryptography from Math 311!) and one meaningful question.