Homework 4 : Due Wednesday, February 24

Problem 1: Let p be an odd prime.
a. Let $k \geq 1$. Show that if g is primitive root modulo p^k, then g is a primitive root modulo p.
b. Show that g is a primitive root modulo p if and only if

$$g^{(p-1)/q} \not\equiv_p 1$$

for all prime divisors q of $p-1$.

Problem 2:
a. Show that 2 is primitive root modulo 29.
b. We know by applying the theorem from class on Friday that there are seven solutions to $x^7 \equiv_{29} 1$. Use part a to find these solutions. Explain your method.
c. Solve the congruence $1 + x + x^2 + \cdots + x^6 \equiv_{29} 0$.

Problem 3: Let p be an odd prime. Show how to use the existence of a primitive root modulo p to prove Wilson's Theorem that $(p-1)! \equiv_p -1$.

Problem 4: Suppose that $p > 3$ is prime.
a. How many primitive roots modulo p are there in the set $\{1, 2, \ldots, p-1\}$? Explain.
b. Show the product of these primitive roots gives 1 modulo p.

Problem 5: Let p be an odd prime, let $k \geq 1$, and suppose that $p \nmid a$. If $x^2 \equiv a \pmod{p^k}$ has a solution, then certainly $x^2 \equiv a \pmod{p}$ has a solution because $p \mid p^k$. Show the converse. That is, show that if $x^2 \equiv a \pmod{p}$ has a solution, then $x^2 \equiv a \pmod{p^k}$ also has a solution. Moreover, show that in this case, there are exactly two solutions modulo p^k.

Problem 6: Let p be an odd prime. Show that $x^4 \equiv_p -1$ has a solution if and only if $p \equiv_8 1$.