Math 42-Number Theory
Problem Set #4
Due Tuesday, March 8, 2011

8. Prove that if g is a generator for U_p, then g^k has order $\frac{p-1}{d}$, where $d = (p-1, k)$. Here, p is prime.

Solution: Suppose $(g^k)^x \equiv 1 \mod p$. Then in fact $g^{kx} \equiv 1 \mod p$, and by something we proved in class, it must be the case that $(p-1) \mid kx$ since $p-1$ is the order of g. Then, letting $d = (p-1, k)$ and $p-1 = dm$, $k = dn$, we get

$$(p-1)\ell = dm\ell = kx = dnx$$

for some $\ell \in \mathbb{Z}$. Thus, because $d \neq 0$, $m\ell = nx$ and in fact $m \mid nx$. But since d was the GCD of $p-1$ and k, m and n must be relatively prime. Thus, by the fundamental theorem of arithmetic, $m \mid x$. So we've shown that whenever $(g^k)^x \equiv 1 \mod p$, that $m \mid x$. Thus, the smallest natural number x satisfying $(g^k)^x \equiv 1 \mod p$ is $m = \frac{p-1}{d}$. In other words, the order of g^k is $\frac{p-1}{d}$, where $d = (p-1, k)$.

9. Fill in the blank: U_p has _____ generators when p is prime. (You may assume that U_p has at least one generator.)

Solution: U_p has $\varphi(p-1)$ generators.

10. Prove your statement from problem 9.

Solution: If g is a generator of U_p, then the powers of g run through all elements of U_p. We need to know: for which powers g^k do we get a generator again? From problem 8, we know the order of g^k is $\frac{p-1}{(p-1,k)}$. Thus, g^k has order $p-1$ if $(p-1, k) = 1$ (and of course, g^k is a generator if and only if it has order $p-1$). Therefore, to count generators, we need only count exponents k such that $1 \leq k \leq p-1$ and $(k, p-1) = 1$. The number of such exponents is $\varphi(p-1)$ by definition, so the number of generators is also $\varphi(p-1)$.