Math 42-Number Theory
Problem Set #5
Due Thursday, March 17, 2011

7. Prove that if u_1 and u_2 are elements of U_m with orders n_1 and n_2 respectively and $(n_1, n_2) = 1$, then the order of $u_1 u_2$ is $n_1 n_2$.

Solution: Suppose $(u_1u_2)^k \equiv 1 \mod m$. Then consider $((u_1u_2)^k)^{n_1} = u_1^{kn_1} u_2^{kn_1} \equiv 1^{n_1} \equiv 1 \mod m$. Since n_1 is the order of u_1, in particular $u_1^{kn_1} \equiv 1 \mod m$, so we really have

$$u_2^{kn_1} \equiv 1 \mod m.$$

We showed in class that if $u^\ell \equiv 1 \mod m$, then the order of u divides ℓ. Thus, $n_2 \mid kn_1$. But since $(n_1, n_2) = 1$, by the fundamental theorem of arithmetic, $n_2 \mid k$. By similar logic (considering $((u_1u_2)^k)^{n_2}$ now), we get that $n_1 \mid k$ also. But since $(n_1, n_2) = 1$, we have by the problem on the midterm that $(n_1 n_2) \mid k$. Thus, the smallest natural number k such that $(u_1u_2)^k \equiv 1 \mod m$ is $n_1 n_2$ itself, and the order of $u_1 u_2$ is $n_1 n_2$.

9. Prove that if u has order n in U_m and $d \mid n$, then there is an element of U_m with order d.

Solution: We claim that u^ℓ, where $\ell = \frac{n}{d}$ has order d. Suppose $(u^\ell)^k \equiv 1 \mod m$. then $n \mid \ell k$, or in other words, $n = \ell k t$ for some integer t. But $n = d\ell$, so in fact, $d = kt$, and $k \mid d$. Thus, the smallest natural number k such that $(u^\ell)^k \equiv 1 \mod m$ is $k = d$, and the order of u^ℓ is d.

10. Problems 8 and 10 together show that if on the quest for a generator, we encounter u_1 and u_2 with orders n_1 and n_2 respectively where the LCM of n_1 and n_2 is $\varphi(m)$, we can find a generator quickly. Let $(n_1, n_2) = d$. Describe a method to find a generator and give an example.

Solution: We'll start with a simpler example, then move to the general case. Suppose $n_1 = dk_1$ and $n_2 = dk_2$, where $(k_1, d) = 1$. Note that $(k_1, k_2) = 1$ since d is the GCD of n_1 and n_2. Then k_1 and dk_2 are relatively prime, and their product is $\varphi(m)$, since their product is just the LCM of n_1 and n_2. Luckily, we have elements of orders k_1 and dk_2: from problem 9, u_1^d has order k_1, and u_2 had order dk_2 by assumption. Then by problem 7, $u_1^d u_2$ has order $\varphi(m)$ and is a generator.

Now what if $(k_1, d) \neq 1$ and $(k_2, d) \neq 1$? We need to be slightly trickier. Let d factor $d = d_1 d_2$ where $(d_2, k_1) = 1$ and $(d_1, k_2) = 1$ and $(d_1, d_2) = 1$. We can do this because $(k_1, k_2) = 1$ (essentially, we're splitting up the factors that d shares with k_1 and k_2 respectively). Now we will find elements of order $d_1 k_1$ and $d_2 k_2$ using problem 9. But $d_1 k_1$ and $d_2 k_2$ are relatively prime by construction, so we can use problem 7 to get a generator. Namely, our generator in this case is $u_1^{d_2} u_1^{d_1}$.

For example, suppose u_1 has order $n_1 = 50$ and u_2 has order $n_2 = 20$ in U_{101}. Then the LCM of the order is 100, as desired. In this case, $d = 10$ and $k_1 = 5$, $k_2 = 2$. Then we make $d_1 = 5$ and $d_2 = 2$, and find elements of order 25 and 4 respectively. In particular, u_1^2 has order 25, and u_2^5 has order 4. Their product then has order 100 and is thus a generator.