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

1. Find a generator for U_{29}. Use it to make a table of logarithms. Use your table of logarithms from problem 1 to solve $13x^3 = 21 \mod 29$.

2. Use your table of logarithms to solve $x^4 = 7 \mod 29$.

3. Use your table of logarithms to solve $x^7 = 18 \mod 29$.

4. Given that 5 is a generator for U_{97}, list all the other generators of U_{97}. Do not make a full power table.

5. What is the order of 28 in U_{29}? Of 16 in U_{29}? Of $28 \cdot 16$ in U_{29}? (Note: Using a generator of U_{29} and problem 8 of pset 4 may make this easier.)

6. In U_{71}, what is the order of 7, of 2, of $7 \cdot 2$, of 51, of 54, of $51 \cdot 54$? (Note: Using that 7 is a generator of U_{71} and problem 8 of pset 4 may make this easier.)

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 $n_1 n_2$.

8. Give an example showing that the statement in problem 8 is false if we remove the condition that $(n_1, n_2) = 1$.

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.

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.