

104B Problem Set 2

Rino Sanchez

January 27, 2003

1. Calculate $\lambda(30)$ and find all the elements with this order modulo 30.

We would like to find the smallest positive k such that $a^k \equiv 1 \pmod{30}$ for all integers a such that $(a, 30) = 1$, the definition of $\lambda(30)$. The equation $a^k \equiv 1 \pmod{30}$ is equivalent to the equations $a^k \equiv 1 \pmod{2}$, $a^k \equiv 1 \pmod{3}$, and $a^k \equiv 1 \pmod{5}$ because of the prime factorization of 30. Since $\lambda(2) = 1$, $\lambda(3) = 2$, and $\lambda(5) = 4$, we know that $\lambda(30) = [1, 2, 4] = 4$. First we need is to find the primitive roots modulo 5, namely 2 and 3. Then we find all the integers a from 1 to 30 such that $(a, 30) = 1$ and $a \equiv 2, 3 \pmod{5}$. If we go through the list the possibilities are 7, 13, 17, and 23. These are all the elements of order 4 modulo 30.

2. Calculate $\lambda(4000)$ and find an element with this order modulo 4000.

Since $4000 = 2^5 \cdot 5^3$, we know that $\lambda(4000) = [\lambda(2^5), \lambda(5^3)] = [8, 100] = 200$. Now we find an element of maximal order modulo 2^5 , and from a previous exercise we know that $\text{ord}_{2^5}(3) = 2^3$. Now we need to find a primitive root modulo 5^3 , which we've done before, so we know 2 is a primitive root modulo 5^3 . Now we need to find an integer a such that $a \equiv 3 \pmod{2^5}$ and $a \equiv 2 \pmod{5^3}$, so we need the Chinese remainder theorem. Mathematica tells me the smallest possible number is 2627 (I don't need to practice my Chinese Remainder Theorem like some people).

7.2, # 9, 16

9. Let p be an odd prime. Prove that there are exactly $\phi(p-1)$ primitive roots of p that are incongruent modulo p^2 and that are not primitive roots of p^2 .

We know that there are $\phi(\phi(p)) = \phi(p-1)$ primitive roots modulo p , and there are $\phi(\phi(p^2)) = \phi(p(p-1)) = \phi(p)\phi(p-1) = (p-1)\phi(p-1)$ primitive roots (the second equal follows because $(p, p-1) = 1$). Let $N = \phi(p-1)$ and g_1, \dots, g_N be different primitive roots modulo p . Consider the integers $g_1, g_1 + p, g_1 + 2p, \dots, g_1 + p(p-1)$. They are all congruent to g_1 modulo p but are inequivalent modulo p^2 . If we do this for each g_i and compile a set of these integers, we have a set S of $pN = p\phi(p-1)$ integers, all primitive roots modulo p and inequivalent modulo p^2 . If we subtract the number of primitive roots modulo p^2 from the number of elements of S , we get $\phi(p-1)$, our desired number (coincidence?).

Some of the integers in S are also primitive roots modulo p^2 . We will prove that all the primitive roots modulo are in S . More precisely, any primitive root modulo p^2 is congruent to exactly one element of S modulo p^2 . This is accomplished by proving that any primitive root modulo p^2 is a primitive root modulo p .

Let g be a primitive root modulo p^2 . Let $k = \text{ord}_p(g)$. Then $g^k \equiv 1 \pmod{p}$ so that $g^k = 1 + mp$ for some integer m . If we raise that equation to the p -th power, we can use Claim I from the notes of Lecture 5 and we find that $g^{kp} \equiv 1 \pmod{p^2}$. Since $\text{ord}_{p^2}(g) = p(p-1)$, we know that $p(p-1)$ divides kp by Proposition 7.1.3, so $p-1$ divides k . Hence g is a primitive root modulo p .

Now S contains all the congruence classes modulo p^2 of primitive roots modulo p , and it contains all the primitive roots modulo p^2 . We want to count the number of primitive roots modulo p that are not primitive roots modulo p^2 , so we subtract $p\phi(p-1) - (p-1)\phi(p-1) = \phi(p-1)$ and confirm that we have the right number.

16. Suppose p is an odd prime, $p \equiv 1 \pmod{4}$. Show that there exists an element x of order 4. What is $x^2 \pmod{p}$? Does $x^2 \equiv -1 \pmod{p}$ have a solution for $p \equiv 3 \pmod{4}$.

Let g be a primitive root modulo p , so that $g^{p-1} \equiv 1 \pmod{p}$. Since $p \equiv 1 \pmod{4}$, we can take $x = g^{(p-1)/4}$ which has order 4. Then x^2 has order 2, and the only elements of order 2 modulo p are ± 1 . Since $x^2 \not\equiv 1 \pmod{p}$ (or g cannot be a primitive root), we must have $x^2 \equiv -1 \pmod{p}$.

Can $x^2 \equiv 1 \pmod{p}$ have a solution for $p \equiv 3 \pmod{4}$? Well, say we had a solution x . Then x would clearly have order 4, and 4 would divide $\phi(p) = p - 1$ making $p \equiv 1 \pmod{4}$, which is a contradiction, so the answer to the question is no.