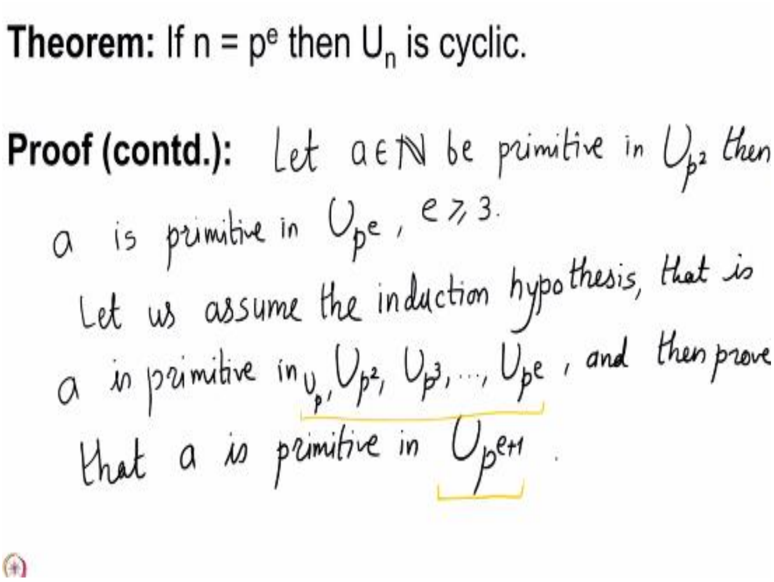
A Basic Course in Number Theory
Professor. Shripad Garge
Department of Mathematics
Indian Institute of Technology, Bombay
Lecture 28
Primitive Roots - IV

Welcome back. We are in the middle of the proof actually we are proving that Un is cyclic whenever n is power of an odd prime. We have proved the case Up square being cyclic in a separate result and then we started this proof of Un being cyclic when n is p power e where p is odd and we have just proved that Up cube is cyclic that was to give you a glimpse of the general proof. I told you that the general proof is by induction and now we have the proof.

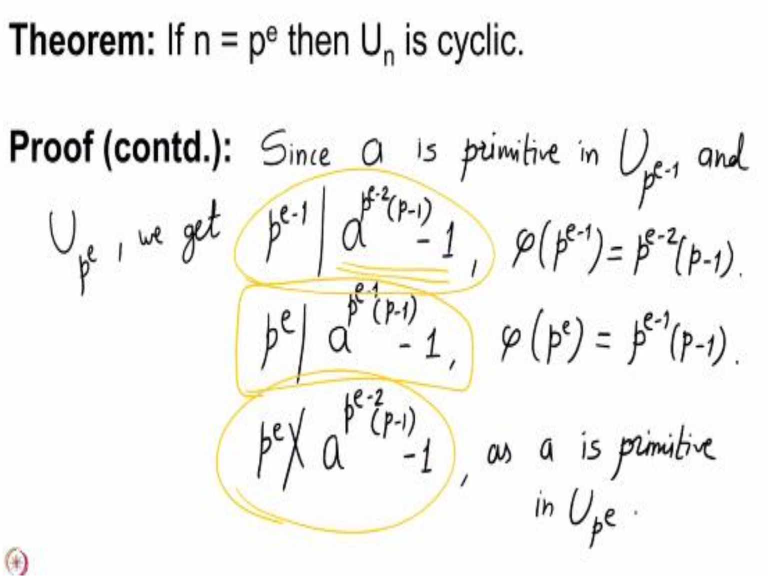
(Refer Slide Time: 00:59)



So, we begin with the assumption that so the assumption is as follows. Let a in N be primitive in Up square and we show that a is primitive in Up cube Up power e for we proved that it is actually primitive in p power 3, but we will show that it remains primitive in all the higher p power Up power is. So, let us assume the induction hypothesis that is a is primitive in Up square, Up cube so on.

In fact it will remain primitive in Up also up to p power e and then prove that a is primitive in Up power e plus 1. This is our plan we will start with the induction as hypothesis that our element remains primitive for all these groups and we will prove that it remains primitive in the next group as well.

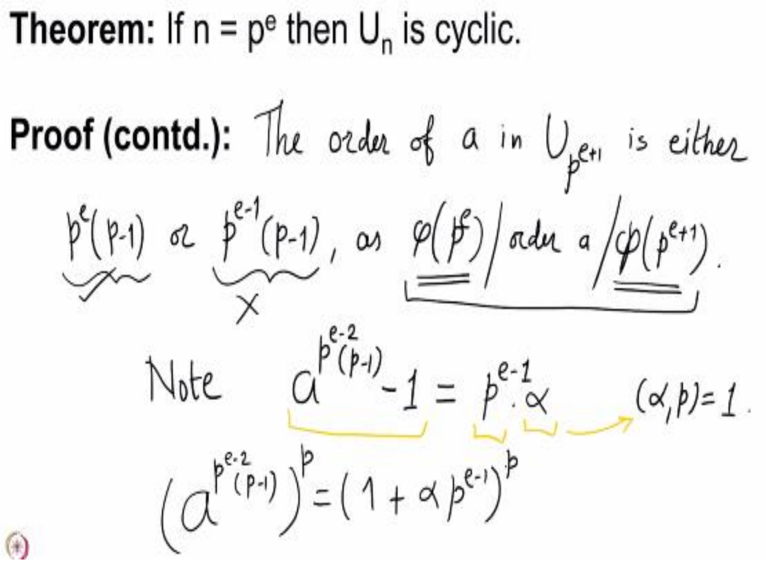
(Refer Slide Time: 03:15)



So, since a is primitive in Up power e minus 1 and Up power e we get the following statements. First of all you will have that p power e minus 1 we will divide a power p power e minus 2 into p minus 1 minus 1. Here the Euler phi function of p power e minus 1 is 1 less power of p into p minus 1 and similarly we will have that p power e divides a power p power e minus 1 into p minus 1.

This is because the Euler phi function of p power e is p power e minus 1 into p minus 1. Moreover, we have that p power e does not divide the earlier thing as a is primitive in Up power e. These are the three things that we are going to need so we have these three things that p power e divides this quantity p power e minus we will divide it, but p power e will not divide. You will check that these two are the same a power p power e minus 2 p minus 1 and a power p power e minus 2 into p minus 1.

(Refer Slide Time: 05:25)

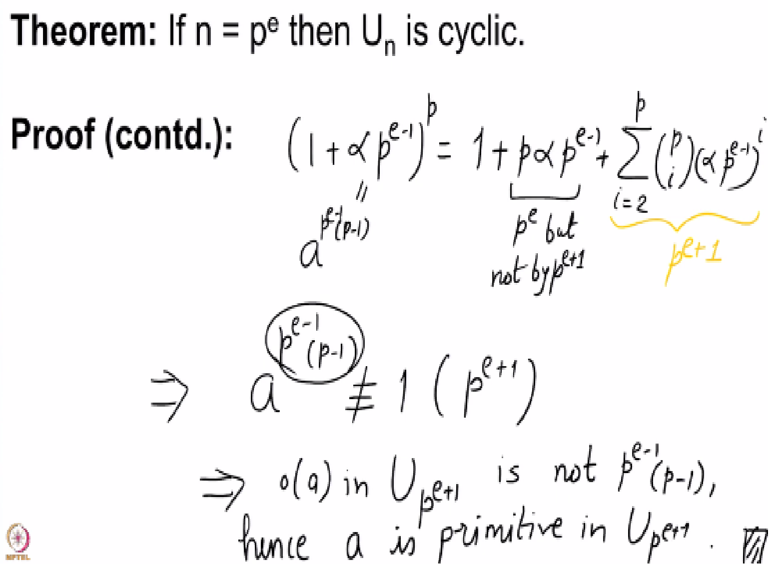


Further, when we look at the group Up power e plus 1 the order of a in Up power e plus 1 is either p power e into p minus 1 or p power e minus 1 into p minus 1 as the Euler phi function of p power e should divide the order a and further order a should divide the Euler phi function of p power e plus 1. So, we have these possibilities and the difference the ratio of phi of p power e plus 1 upon phi of p power e is p.

Therefore, these are the only two possibilities if we show that this is not the order of the element a in Up power e plus 1 then we are done then this will have to be the order of a in Up power e plus 1. So, for that we go one step back and notice that a raise to p raise to e minus 2 p minus 1 minus 1 because of what we have observed here is p power e minus 2 into some element alpha which is coprime to p.

This is because the thing on the left-hand side is divisible by p power e power 2, but not by p power e minus 1. So, therefore we got that one second we have to make a correction here that this 2 is 1. So, we see that this left-hand side is divisible by p power e minus 1, but not by p power e therefore alpha is coprime to p and now we just raise both sides to the power p. So, we look at a power p power e minus 2 into p minus 1 to the power p. This is 1 plus alpha p power e minus 1 to the power p and then apply the binomial theorem.

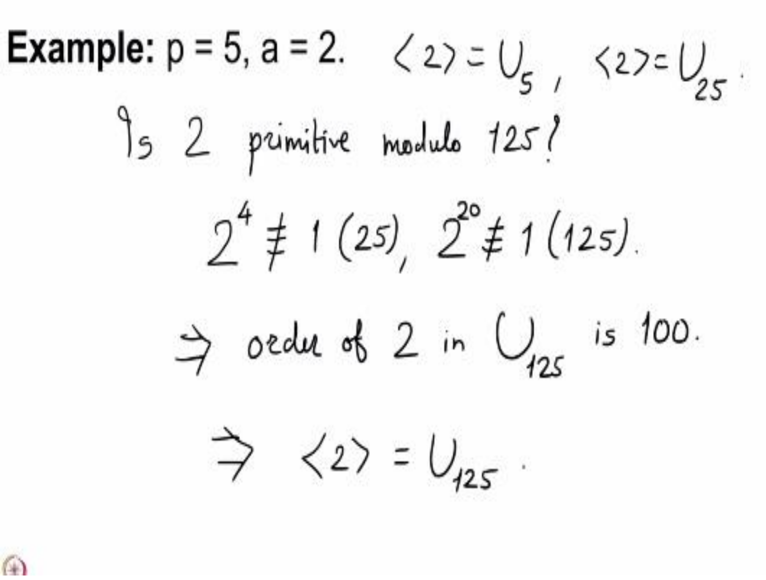
(Refer Slide Time: 08:31)



So, 1 plus alpha p power e minus 1 to the power p will give you 1 plus p alpha p power e minus 1 plus summation i from 2 to p, p chose i 1 will remain as it is and we will have alpha p power e minus 1 to the power i. Now depending on what our p power e is we will see this quite easily that these terms are all divisible by p power e plus 1 and moreover on the left hand side we have this to be a power p power e minus 1 into p minus 1.

And what we have is that this quantity is divisible by p power e, but not by p power e plus 1. So, it tells us that a power p power e minus 1 into p minus 1 is not congruent to 1 modulo p power e plus 1 which is to say that the order of a in Up e plus 1 is not this quantity which is p power e minus 1 into p minus 1. Hence a is primitive in Up e plus 1 this completes our long proof which has been going on over several last lectures. So, this proves that when p is in odd prime the group of units modulo n is a cyclic group and the only remaining case now is where n is 2 times p power e.

(Refer Slide Time: 11:07)



But before that let us look at this particular example where we have p equal to 5 and a equal to 2. I hope you will remember that 2 is not just a generator for U5, but it is also a generator for U25 and now we have to only check or verify that the order of 2 modulo the next prime power next power of 5 which is 125 is correct number or not. So, is 2 primitive modulo 125 this is the question.

So, we observe that 2 power 4 is not congruent to 1 modulo 25 and this by the proof that we have done we will tell you that 2 power 20 is not going to be congruent to 1 modulo 125 and therefore the order of 2 in U125 is equal to 100. Remember that the order of 2 in U125 could have been 20 or 5 into 20 which is 100 and therefore what we have is that 2 also generates U125.

(Refer Slide Time: 12:40)

Example: p = 5, a = $\cancel{2}$. 7

$\langle 7 \rangle = U_5$, $\langle 7 \rangle \neq U_{25}$.

7 is not primitive in U_{125}.

The next example that we had seen in our last lecture was where our a was 7 and we observed that 7 is a generator it is a primitive element for U5, but we saw that it is not a primitive element for U25 and clearly 7 is not going to be primitive in U125. This is because to have something primitive modulo 125 we should have the element to be primitive modulo 25 to begin with. Now, the only case remaining is U 2 into p power e where p is an odd prime and I have promised you that we will show that this group is also a cyclic group.

(Refer Slide Time: 13:37)

Theorem: If n = 2p^e then U$_n$ is cyclic. p = odd prime.

Proof: If p is odd then $\varphi(2p^e) = \varphi(p^e)$.

Let p=3, e=2, n = 18, $\frac{n}{2}=9$

$U_{18} = \{1, 5, 7, 11, 13, 17\}$, $\varphi(18) = \varphi(9) = 6$.

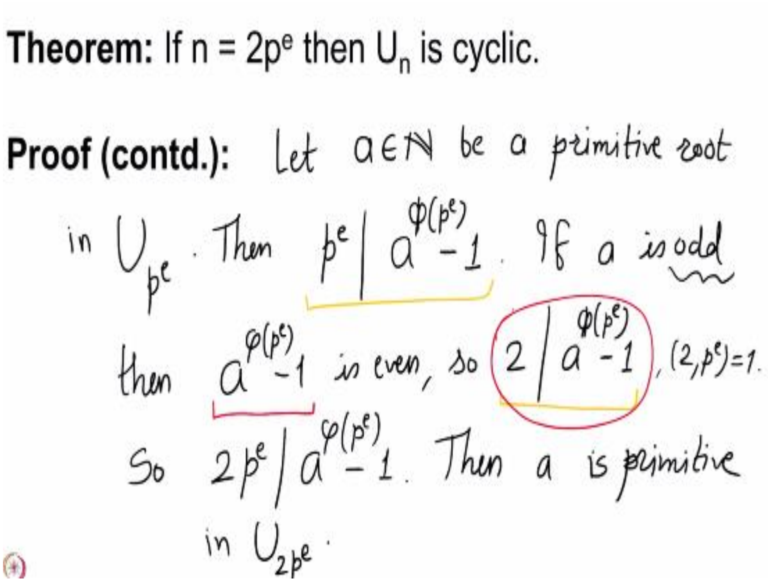
$U_9 = \{1, 2, 4, 5, 7, 8\}$

So, let me remark here again that p remains an odd prime so observe if p is odd then the Euler phi function of 2 times p power e is the Euler phi function of p power e. So, the number of elements in Un where n is 2 times p power e is same as the number of elements in Un by 2, but that does not mean that the numbers are the elements themselves are same because to belong to Un where n is 2 into p power e each number will have to be an odd number which is not the case when you were looking at U p power e.

So, let me do one basic example where p power e is 3 square which is 9. So, let p be equal to 3 and e be equal to 2 so you have n to be 18 and n by 2 is 9. Let us observe that U18 has elements 1. 2 will not come because 2 is even so we should look at the next odd numbers only 3 will not come, but 5 will come 7 comes, 9 does not come, but 11 and 13 come, 15 does not come, but 17 will come.

So, U18 has exactly 6 elements because phi 18 is phi 9 which is 6. U9 has also 6 elements and these are the elements 1, 2, 4, 5 and 7, 8. So, note that for every even element here there is an element which is just obtained by adding 1 times 9 to it to get the next element. So, 8 plus 9 is actually 17 and this is how we get this number. So, 1, 5 and 7 these are the elements which remained as they were. And for all the even elements in U9 we simply had to add 9 once to get the next element. So, this is how we see that the orders of these two groups are same and in fact we will prove that both the groups are actually isomorphic.

(Refer Slide Time: 16:54)

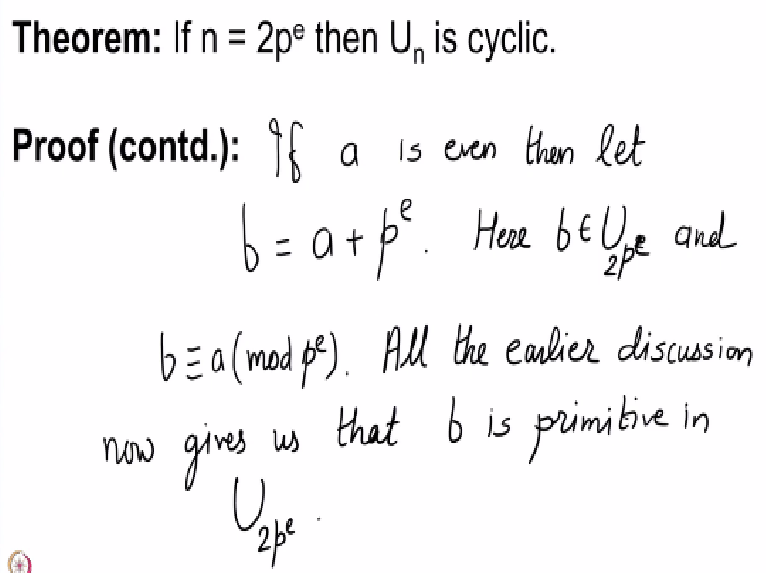


So, the proof would be as follows let a in N be a primitive root in Up power e because whenever we have a divisor of n which is 2 times p power e and we are looking for primitive roots modulo n it should remain a primitive root modulo Up power e as well. So, what it says is that p power e is going to divide the element a raise to the correct order which is phi of p power e minus 1.

Now, if a is an odd number then a raise to 5 p power e minus 1 is even so 2 divides this quantity. You have that 2 divides one particular number you have that p power e also divides the same number and 2, p power e these are coprime because p is odd. So, 2 times p power e will have to divide this number a to the power phi p power e minus 1 and then we are done because then a is primitive in U 2 times p power e as well.

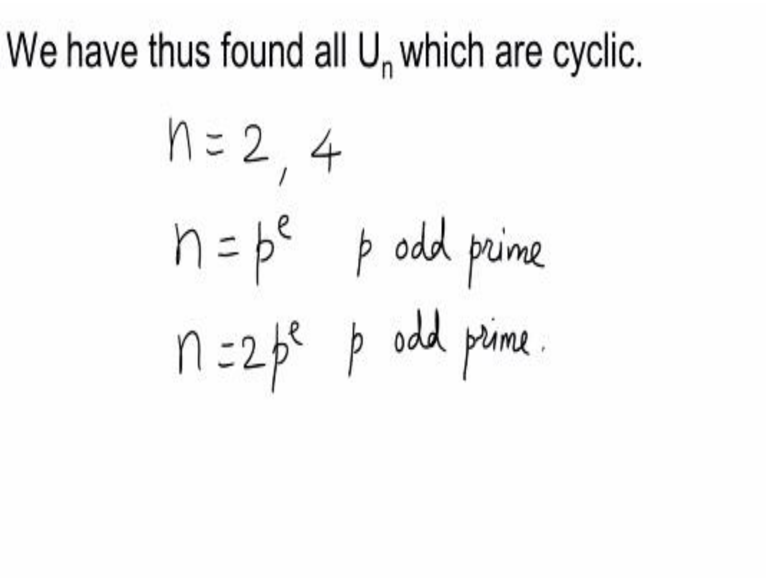
So, the only situation where we will not get a to be a primitive root would be when a is not odd if a is even then this number that we get here will not be even this will actually be odd and you will not have to dividing a raise to phi p power e minus 1.

(Refer Slide Time: 19:26)



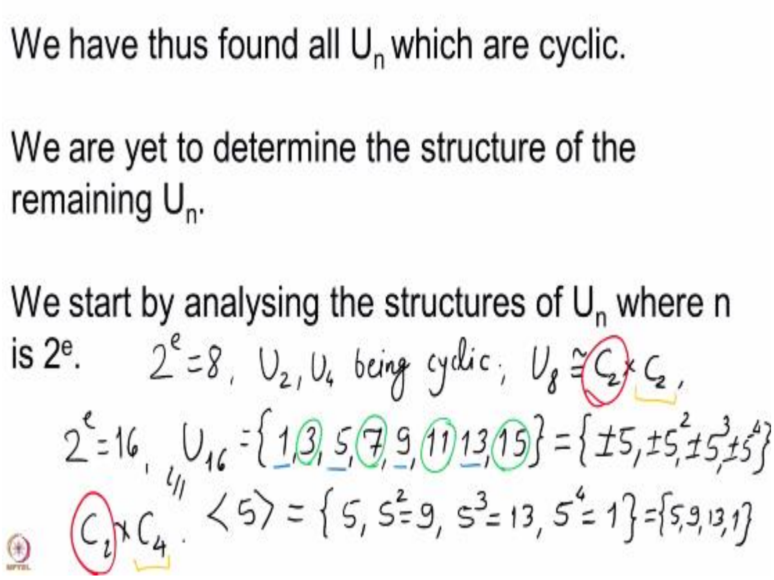
So, if a is even then we have to get a separate proof then let b be a plus p power e. Here b is an element in U 2 times p power e and b is congruent to a mod p power e. So, all the earlier discussion now holds for b a is even and you have added an odd prime power to it so b is odd. So, all the earlier discussion now gives us that b is primitive in U 2 times p power e and so whenever n is 2 times power of an odd prime then Un is a cyclic group. So, we have computed all Un which are cyclic groups.

(Refer Slide Time: 21:05)



And just to recall this for you these are where n is 2, n is 4, n is power of an odd prime or n is 2 times p power e where p is an odd prime. These are all the cases where our groups Un are cyclic and in all the remaining cases we have seen that the groups Un cannot be cyclic. So, as far as getting the cyclic group structure on Un is concerned we have solved the problem. However we cannot say that we have understood all Un. Because we do not understand the structure of the other Un which are not yet cyclic. So that is something that we would want to do.

(Refer Slide Time: 22:03)



We are yet to determine the structure of the remaining Un which are not cyclic if you remember these were the n for which n had two or more prime factors or n was of the form 4 into m where m is odd or it was of the form 8 into anything. So, 8 divided n or 4 divided n and the factor is an odd element bigger than 1 of course and the other third possibility was that n is product of two or more distinct prime powers.

So, it has two or more distinct prime factors. These were the cases where the groups Un are not cyclic and we want to understand the structure of these groups. So, once again we will begin by looking at the groups of the form Un where n is a power of 2. The very basic such case would be where we would look at U8. So, we consider the case 2 power e equal to 8. If you remember U2 and U4 are already cyclic and we also saw that U8 is isomorphic to C2 cross C2.

So, the next case we should look at is 16 U16 has 8 elements all the elements which are odd numbers up to 16 and here I will give you one particular subgroup. The subgroup generated by 5 is 5 square which is 9 modulo 16 5 cube is 45 and so modulo 16 this is 13 and then 5 raise to 4 which is 13 into 5 which is 65 so that is 1 modulo 16. So, we get this group to be 5, 9, 13 and 1 and we observe that this therefore is plus minus 5.

Because we have these elements so 5, 9, 13 and 1 these are already there and their negatives are these elements. So, negative 5 is 11 negative 9 is 7, negative 13 is 3 and negative 1 is 15. So, we get that our group is actually plus minus 5 plus minus 5 square plus minus 5 cube and plus minus 5 raise to 4. Thus, U16 is C2 cross C4. So, the structure of the group U2 power e where 2 power e is 8 or above is that it will have a direct factor which is C2 in both these cases 8 as well as 16 we got a direct factor which is C2.

And then there is one more cyclic subgroup which together with C2 gives us the U2 power e completely. So, this is the way we are going to prove our result finally that the group Un where n is 2 power e bigger than or equal to 8 then Un is product of two cyclic groups. One of them being of order 2. So, I hope to see you in the next lecture to study this. Thank you.