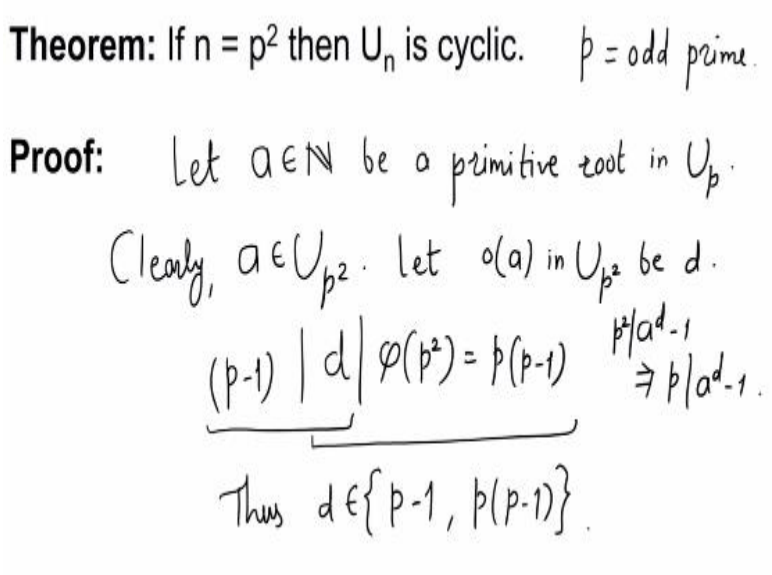
A Basic Course in Number Theory
Professor Shripad Garge
Department of Mathematics
Indian Institute of Technology, Bombay
Lecture 27
Primitive Roots - III

Welcome back. We are proving that Un is cyclic whenever n is power of n odd prime p. This is what we are proving, but to begin with our baby step is to show that Up square is cyclic. We proved that Up is cyclic for all primes p and using that we want to show that whenever p is an odd prime then Up square is cyclic.

(Refer Slide Time: 00:47)



So, we have the statement here on the slide for you. Remember that we are always taking p to be an odd prime. This is something that will remain in force now for this lecture and perhaps also for the next lecture and I have told you the plan of this proof. So, let me just quickly go through that once. What we observed in the last lecture was that if you wanted to find a primitive element in Up square.

Then by going modulo p that element should better be a primitive element in Up. So, I am looking for a primitive element mod p square modulo p this will have to be a primitive root modulo p in Up and so when I am looking for primitive root modulo is p square, I should be looking in the residue classes of the primitive roots modulo p. So, what I do is that I choose a primitive root a modulo p.

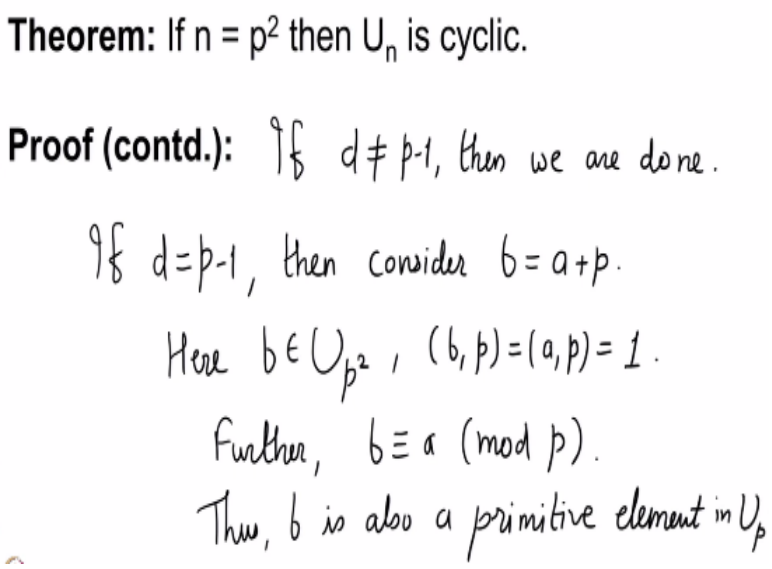
And I check whether that is also primitive root mod p square and if it is not then we will do a slight modification and get a primitive root mod p square that is the plan. So, let a in the

natural number be a primitive root in Up so modulo p this element a is a primitive root. So, clearly first of all a is an element in Up square. This is because if a is a primitive root in Up then a is an element in Up so a is coprime to p.

Therefore, a is coprime to p square and so a is an invertible element modulo p square. So, a is our element in Up square. Let the order of a in Up square be d. We want to check whether d is equal to phi p square, phi p square is p into p minus 1. So, we of course have that d will need to divide phi p square which is p into p minus 1, but p minus 1 will also divide d. The reason being that a power d minus 1 is divisible by p square would imply that p also divides a power d minus 1.

And since we have started with a primitive root in Up the order of a in Up is p minus 1. So, p minus 1 will therefore have to divide d and d needs to divide p into p minus 1. So, the possibilities for d are p minus 1 and p into p minus 1. There are no other elements which are multiples of p minus 1 and which are also divisors of p into p minus 1. This is where we are using that p is a prime. If you show that the order of this element d cannot be p minus 1 then we are done.

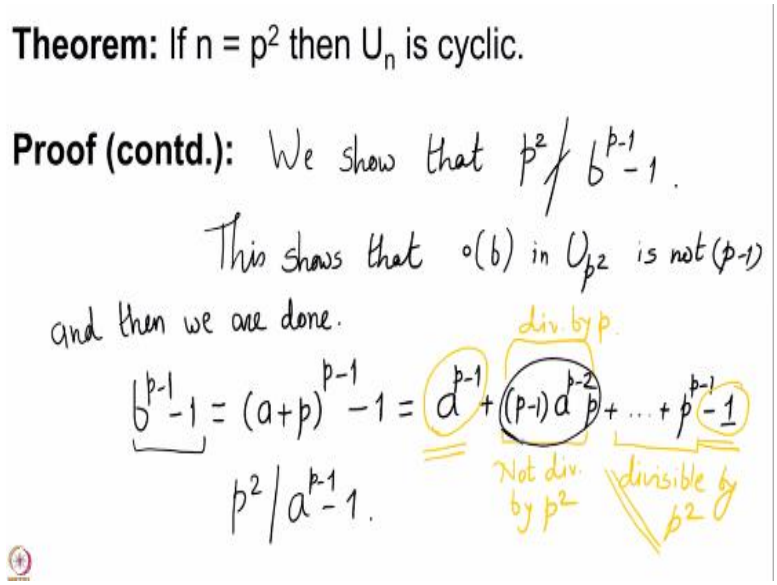
(Refer Slide Time: 04:37)



If d is not equal to p minus 1 then we are done, but this may not happen. You may have d equal to p minus 1 if the order of the element a in p square is also p minus 1 then consider a new element b which is a plus p. So, first of all here b is also an invertible element modulo p square because the GCD of b with p is also 1 and so GCD of b with p square is also going ot be 1.

So, b is an invertible element further modulo p we have that b is same as a. Therefore, b is also a primitive root modulo p. So, all the discussion that we have done with a holds for the element b also which is that order of b modulo p square can be p minus 1 or p into p minus 1 and if you can now show that the order of b modulo p square is not p minus 1 then you have got a primitive root for p square.

(Refer Slide Time: 06:56)

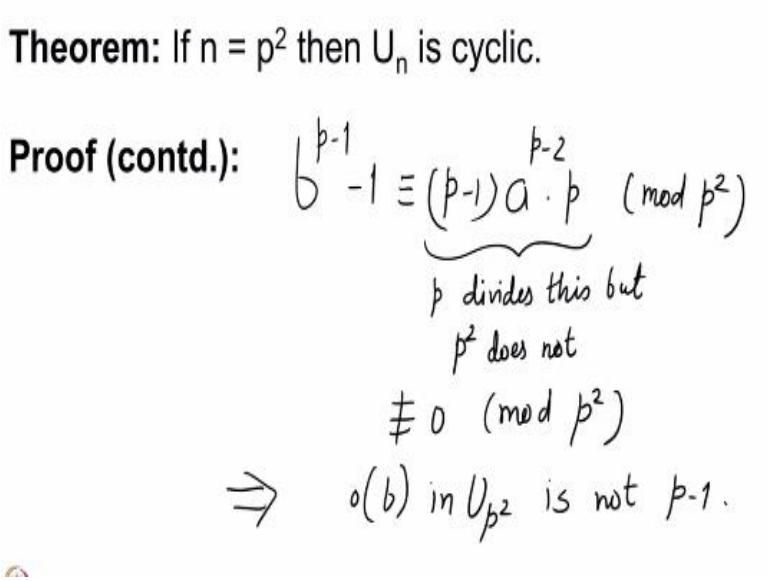


We show that p square does not divide b power p minus 1 minus 1. This will tell that order of b in Up square is not p minus 1 and then we are done. So, we now need to only compute this b power p minus 1 minus 1. Remember b is a plus p and now we apply the binomial theorem which will give us a power p minus 1 plus p minus 1 into a power p minus 2 into p plus dot, dot, dot the last term will be p power p minus 1 and finally we have 1.

So, in this binomial expansion we notice that the elements from here onwards are divisible by p square of course we do not have 1 divisible by p square. What we mean to say is that from this up to p power p minus 1 these are all divisible by p. This is not divisible by p square, but it is divisible by p and finally we have a to the p minus 1 minus 1, a to the p minus 1 minus 1 this is divisible by p square.

This is because the order of a modulo p square was p minus 1. So, we have among the right-hand side the elements which are divisible by p square so this is divisible by p square together with minus 1 and these things are divisible by p square.

(Refer Slide Time: 09:55)

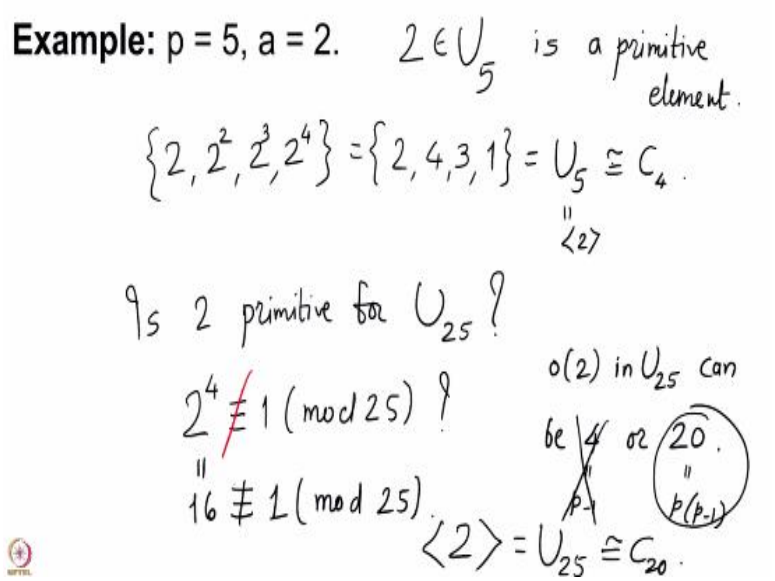


So, when you look at this modulo p square the b power p minus 1 is exactly this p minus 1 a raise to p minus 2 into p. And here you have p divides it, but p square does not. So, we get it to be not congruent to 0 mod p square and therefore the order of b in Up square is not p minus 1 that is it then this b will have to be a primitive root modulo p square by the discussion that we have seen earlier. So, once again what we did was that we observed first of all that Up is cyclic so Up has to have a primitive element.

Secondly, a primitive element in Up square has to be a primitive element for Up when you go further modulo p. So, we will start with the primitive elements modulo p and checks its order mod p square. We observed that there are only two possibilities p minus 1 or p into p minus 1. So, it is almost a primitive root modulo p square or it is only a primitive root modulo p and not modulo p square.

If it is not you simply add p to it and then we see that by adding p to the element a that you started with we do get a primitive root modulo p square. So, what we now intend to do is to do this as an example for this very particular case.

(Refer Slide Time: 11:56)

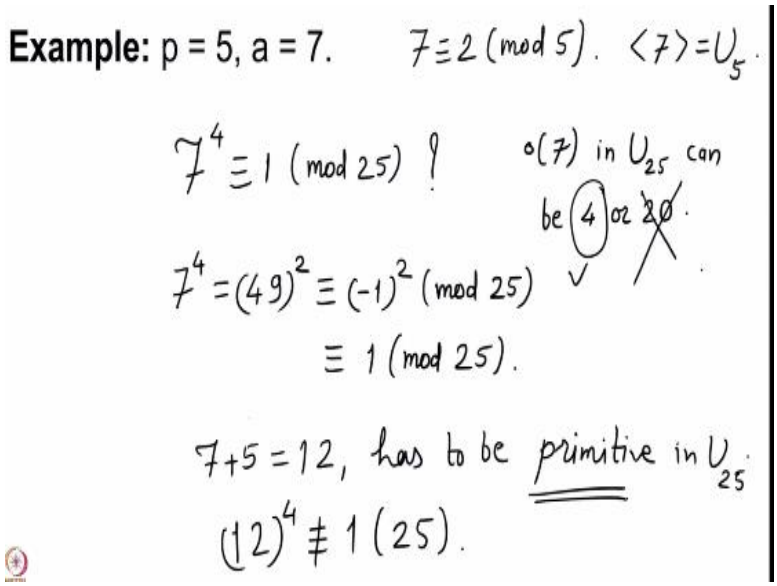


P is 5 a is 2 so 2 in U5 is a primitive root or what is also called as primitive element. This is because 2, 2 square, 2 cube and 2 power 4 these are all distinct elements you get as a collection because there can be repetitions, we have 4 then we get 3 and then we get 1 so this is exactly U5. So, we have that U5 is isomorphic to C4 and it is generated by the element 2. Now, the question is 2 primitives for U25?

This is the question, but so for this we need to check whether 2 power 4 is congruent to 1 modulo 25. So, we know that the order of 2 in U25 can be 4 or 20 this is your p minus 1 and this is your p into p minus 1. These are the only possibilities for the order of 4 modulo 25. Is this true? So, 2 power 4 is actually 16, but 16 is not congruent to 1 mod 25. Therefore, the order of 2 mod 25 will have to be then 20 because this is not possible.

And hence 2 also generates the group U25 which is isomorphic to C20. So, if we were lucky and we had chosen the generator for 5 to be 2 then we will get that 2 is going to further generate the element the group U25, but you may make a small mistake and instead of 2 you may take a to be 7.

(Refer Slide Time: 14:37)



So, observe that modulo 5 7 is congruent to 2 and therefore 7 also generates the group U5 this is something that we already have, but is it true that 7 power 4 is congruent to 1 modulo 25 because we know that order of 7 in U25 it can be 4 or 20. If it is 4 then it is not a primitive root modulo 25. If it is not 4 then it is a primitive root modulo 25 so 7 power 4 is 49 square and therefore when you go modulo 25 49 is actually minus 1.

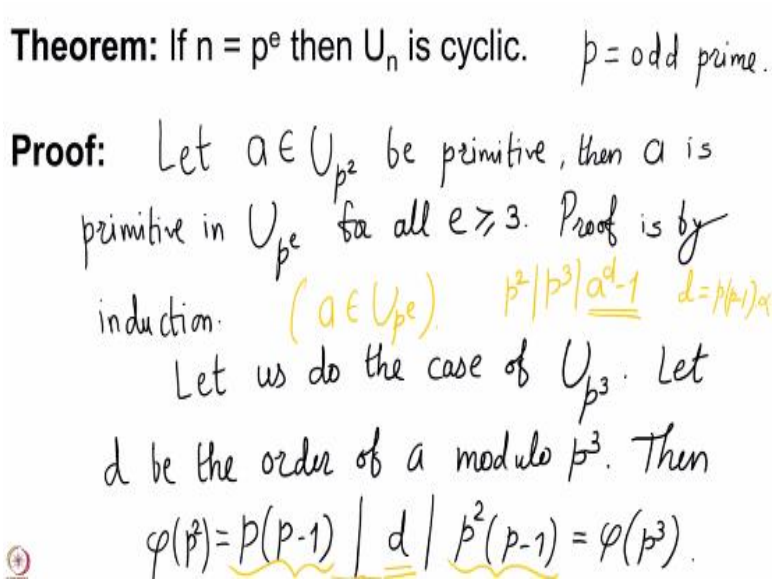
Because 50 minus 1 is 49 and so this is 1 modulo 25. So, this tells you that the order of 7 in U25 is actually 4 and so it cannot be this and then by the method of proof we would look at 7 plus 5 which is 12 this has to be a primitive element in U25. This is something that you should check so what you should check is that 12 power 4 is not congruent to 1 modulo 25. Now, once you check this then this will be proved.

So, this is a very simple example which tells how we can compute the primitive roots. Once you know the primitive root modulo p you have a primitive root modulo p square which is congruent to the primitive root that you started with modulo p. You may ask how many primitive roots modulo p square can I get in this way. So, the question that you may ask is suppose I fix one primitive root modulo p we know by our method of the proof.

That there has to be a primitive root mod p square which is congruent to the primitive root mod p that you have fixed, but among all those different p elements which are congruent to the same element modulo p. How many are going to give you the primitive roots modulo p square. This is a very interesting question it is so interesting that I am going to ask you this

question in the tutorial, but think about this question and we will see the answer in the tutorial.

(Refer Slide Time: 17:49)



We now go to our next result which shows that if you have n to be p power e then Un is cyclic and I will remind you once again because we are stating the theorem here for the first time that our p is an odd prime once again our beginning step will be the same step which we had for n equal to p square which is that we observe that to get a primitive root modulo p square we needed to start with a primitive root modulo p.

Here if we are taking e to be bigger than or equal to 3 because for Up and Up square we are done then we have to start with a primitive root modulo p square and work with that in Up power e. We will show in fact a more stronger result then we had in the case where n was p square. Let a in Up square be primitive then a is primitive in Up power e for all e bigger than or equal to 3 this is the fantastic result.

It tells you that once you start with a primitive root modulo p square that element will continue to remain primitive modulo all the higher powers that is a great result because now, we do not have to work with cases. When we looked at the case of Up square and we started with a primitive root modulo p we had to deal with the possibility that the element will not remain primitive mod p square there is no more such possibility.

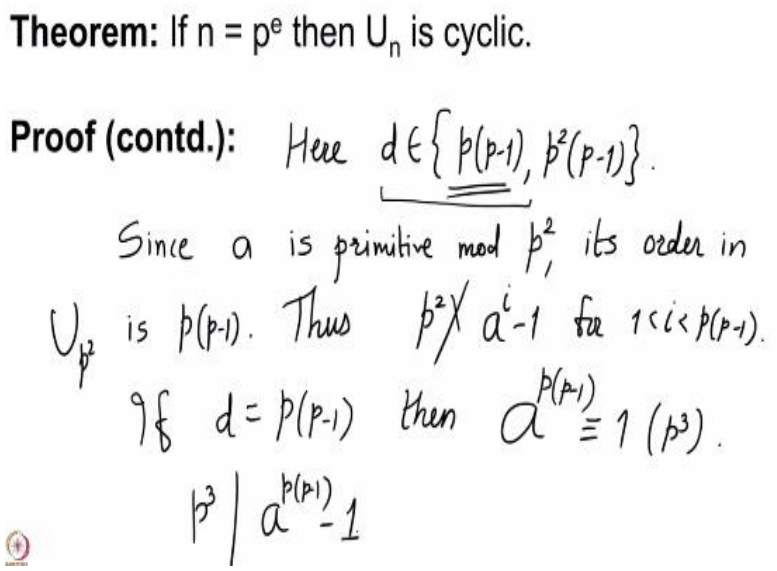
Any a which is primitive mod p square is going to remain primitive mod p power e for e bigger than or equal to 3 and the proof is using induction proof uses induction. To understand

the proof clearly let us deal with the case p cube first. Here I am going to observe and will not repeat this observation that a is always coprime to the prime p it is relatively prime with p and therefore it is an element in Up power e that is something that we are going to use.

So, let us do the case of Up cube let d be the order of a modulo p cube then once again as we have observed in the previous proof p into p minus 1 which is phi of p square will have to divide the order d and it will also divide p square into p minus 1 which is phi p cube. It will be a multiple of this because whenever you have p cube dividing a to the d minus 1 you have p square also divides p cube.

And therefore, p square divides a raise to d minus 1 and therefore d should be multiple of the phi of p square which is p into p minus 1 into some alpha for instance. So, therefore we have this so now d can be equal to this quantity or it can be equal to this.

(Refer Slide Time: 22:33)

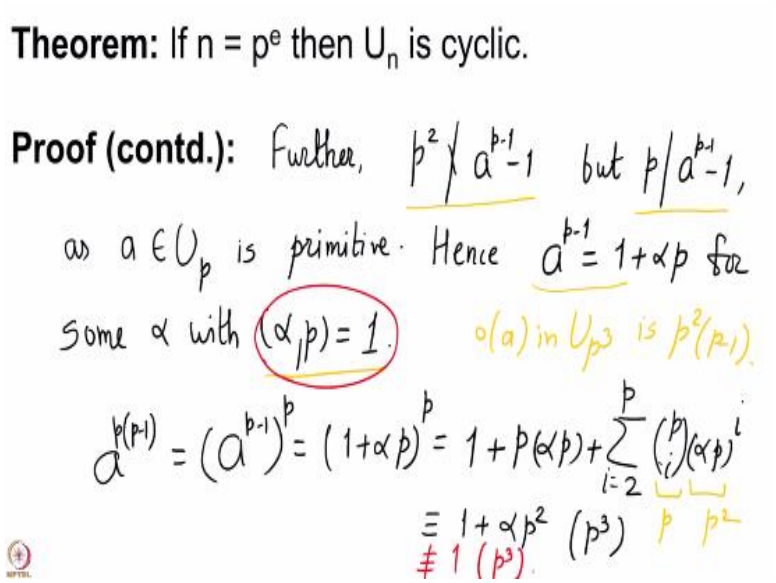


There are only two possibilities for d once again as we have noticed before in the case of Up square. So, here d will belong to the set p into p minus 1 and the set p square into p minus 1. We want to show that d cannot be this, this is the case that we want to remove. So, for that we use that since a is primitive mod p square its order in Up square is p into p minus 1. Thus, p square does not divide a power i minus 1 for 1 less than i less than p into p minus 1.

This is one simple fact that we use and now assume that if your d is p into p minus 1 then remember this is the order modulo p cube then you have that a power p into p minus 1 is

congruent to 1 modulo p cube. So, it tells you that p cube divides a power p into p minus 1 minus 1.

(Refer Slide Time: 24:25)



Further, p square does not divide a to the p minus 1 minus 1, but p divides a to the p minus 1 minus 1. This is because a in Up is primitive and then we get so this gives us that a to the p power 1 is 1 plus alpha p for some alpha with alpha being coprime to p. This is because we are starting with the difference of these being divisible by p but not by p square. So, this alpha cannot have a p in its factor.

So, therefore alpha, p has to be coprime and once we have this, we have to now raise both sides to the p th power so using binomial expansion we have that a raise to p minus 1 to the power p which is nothing but a power p into p minus 1. This gives us using the binomial expansion for this one plus alpha p to the power p that we get 1 power p which is just 1 plus p 1 power p minus 1 and alpha p plus p square.

So, we have the binomial coefficient which is p so I will just put a summation sign here because all the remaining terms will have summation p choose i 1 to the power i and alpha p to the power so alpha p power i and 1 to the power p minus I and i goes from 2 to p so these are the terms where the powers of alpha p will keep increasing and you have the coefficient to be p choose i.

So, we observe that in these coefficients you have a factor of p here actually you have a factor of p square here and you have a factor of p here. So, modulo p cube this is congruent to

1 plus alpha p square when you go modulo p cube, but remember that alpha, p is equal to 1 and therefore we have that this is not congruent to 1 mod p cube. So, the order of a modulo p cube cannot be p into p minus 1 and therefore order of a in Up cube has to be p square into p minus 1 which is what we wanted.

So, we are proving that Un where n is power of an odd prime is cyclic and what we have done is another baby step. Remember in this proof of Un being cyclic where n is a power of an odd power we did the p square case first and now we have done the p cube case. When in the beginning of the next lecture we are going to look at all the higher powers and use induction to show that such a Un is cyclic. So, I hope to see you in my next lecture. Thank you.