

A Basic Course in Number Theory
Professor Shripad Garge
Department of Mathematics
Indian Institute of Technology, Bombay
Lecture – 26
Primitive Roots - II

Welcome back. In the last lecture we proved that U_p has primitive roots. So what are U_n in general let us have a very quick recall.

(Refer Slide Time: 00:33)

The groups \mathbb{Z}_n^\times , the unit groups of \mathbb{Z}_n , are denoted by U_n .

An element $a \in U_n$ is called a primitive root if the order of a in U_n is equal to $\varphi(n)$.

$$|U_n| = \# U_n = \varphi(n)$$

So, these are the groups U_n denotes the groups \mathbb{Z}_n^\times these are the groups that we are studying and these are denoted by U_n where n is a natural number and we want to study when exactly these groups are cyclic. So, there is one thing which we should have noticed which is that cardinality of U_n which is also denoted by this symbol sometimes. This is nothing, but the Euler phi function evaluated on n . So, to say that this group is cyclic means to say that there is an element whose order is exactly equal to the order of the group.

(Refer Slide Time: 01:27)

Theorem: The groups U_p have primitive elements.

So, when we show in the next slide that the group U_p have primitive elements that means we will actually produce one element of order $p - 1$ and if you remember this proof what we proved was that whenever there was any element of order m one such element will generate a cyclic group of order m . Further, all these elements will have property that they are equal to 1 when you raise them to the power m and $x^m - 1$ over \mathbb{Z}_p cannot have more than m solutions.

So, once you have one or element of element m you have a subgroup of order m generated by these. These will contain exactly $\phi(m)$ many elements of order m . If there was anything outside of this which is also of order m . In other words, if you had any elements of order m more than these $\phi(m)$ elements then we get a contradiction. So, for each m you will have only $\phi(m)$ elements of order m or perhaps you will have no elements.

But when you take summation of $\phi(d)$ d divides $p - 1$ it should give you $p - 1$. Therefore, by counting orders of all elements in the group U_p we see that for every divisor of $p - 1$ there has to be at least one element of that order and in particular there is an element of order $p - 1$. This is the proof that we had to show that U_p is cyclic for every prime p or in other words that U_p have primitive elements. We now study the U_n slightly more in detail where n is a composite number. Let us compute these things for some small values of n .

(Refer Slide Time: 03:35)

Let us study some U_n where n is composite.

$$U_6: U_6 = \{1, 5\}.$$

$$U_6 \cong C_2, \text{ cyclic group of order 2.}$$

So, first of all we look at U_6 , 6 is the smallest number which is divisible by two different primes. So, we consider U_6 has elements which are coprime to 6 which are coprime to 2 and 3 so you get only two elements here. U_6 has exactly two elements and we know that every group of order 2 is isomorphic to the cyclic group of order 2. So U_6 is isomorphic to C_2 this is the complete information about the group U_6 . U_7 is a cyclic group because 7 is a prime number.

(Refer Slide Time: 04:30)

Let us study some U_n where n is composite.

$$U_8: U_8 = \{1, 3, 5, 7\}, \text{ further,}$$

$$3^2 = 5^2 = 7^2 = 1 \text{ in } U_8.$$

$$U_8 = C_2 \times C_2 = \{1, 3\} \times \{1, 5\}.$$

$$5 \times 3 = 7 \text{ in } U_8.$$

U_8 so we see that U_8 has only the odd elements because all the even elements are not going to be congruent to 8 they will have the GCD equal to 2 at least. So, these are all the elements

further we notice that the squares of all the non trivial elements are equal to 1 modulo 8. Thus, although you have a group of order 4 the all three non trivial elements are of order 2 and so U_8 is C_2 cross C_2 .

You actually have 1 C_2 which is 1, 3 this is the subgroup and another C_2 which is 1, 5 and note that 5 into 3 is equal to 7 in U_8 . So, there is a natural map from the product of these two subgroups to the whole group U_8 which gives you that U_8 is an internal direct product of these two subgroups. So U_8 is C_2 cross C_2 . U_9 we of course forgot one composite number 4, but that is something that we will be looking at later.

(Refer Slide Time: 06:06)

Let us study some U_n where n is composite.

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

$$2, 2^2=4, 2^3=8, 2^4=16=7, 2^5=14=5,$$

$$2^6=10=1, \text{ thus } 2, 2^2, 2^3, 2^4, 2^5, 2^6=1,$$

are all distinct elements. In other words,

$$o(2)=6, \text{ so } U_9 \cong C_6.$$

So, this is the next composite number U_9 when we write U_9 we will have to be careful that no multiple of 3 should come. These are all the elements in U_9 . Let us try to find orders of elements in the group U_9 . So, suppose we start with 2 square is 4, 2 cube is 8, 2 raise to 4 is 16, but your modulo 9 so this is 7, 2 raise to 5 is now 14 because it is 7 into 2, but modulo 9, 14 is 5.

And then we get 2 raise to 6 which is 10 this is also 1. So, 2 square, 2 cube, 2 raise to 4, 2 raise to 5 and 2 raise to 6 are all distinct elements. In other words the order of 2 in this group is 6. So, U_9 is actually a cyclic group of order 6 so we have that U_8 was C_2 cross C_2 , U_6 was cyclic, U_7 was cyclic and U_9 is also cyclic.

(Refer Slide Time: 08:21)

Let us study some U_n where n is composite.

$$U_{10}: U_{10} = \{1, 3, 7, 9\}. \text{ Note } \#U_{10} = \#U_8 = 4.$$

$\varphi(10) = \varphi(8)$

$$3, 3^2=9, 3^3=27=7, 3^4=7 \times 3=21=1.$$

$$o(3) = 4, \text{ so } U_{10} \cong C_4.$$

$$U_{10} \not\cong U_8.$$

Let us go one step ahead and look at U_{10} . So, in U_{10} we should not because 2 divide 10 so we should not write the even elements, but we should also make sure that 5 does not come so the only elements you have are 1, 3, 7 and 9. So, note first of all that cardinality of U_{10} is equal to the cardinality of U_8 which is 4. This is one small observation because of course we have that $\varphi(10)$ is equal to $\varphi(8)$ which is equal to 4.

And here now let us try to compute orders of 3. So, 3 square is 9, 3 cube is 27 which is 7 because we are working modulo 10 and then 3 raise to 4 is 7 into 3 this is 21 and therefore this is 1. So, order of 3 in this group is 4 and so we get that U_{10} is isomorphic to C_4 . So, this is one major thing because U_8 has exactly as many elements as there are in U_{10} if you were looking at just the number of elements.

You would have no way to distinguish U_8 and U_{10} and what we find here is that U_8 is isomorphic to C_2 cross C_2 , but U_{10} is cyclic it is isomorphic to C_4 and as a small corollary we get that U_{10} is not isomorphic to the group U_8 . This is why we are looking at the group structure on this sets. If you were looking at only the orders of these sets then we would have that U_{10} and U_8 have the same number of elements. However, as groups these two are distinct.

(Refer Slide Time: 10:52)

Let us study some U_n where n is composite.

$$U_{12}: U_{12} = \{1, 5, 7, 11\} \left. \begin{array}{l} 5, 5^2 = 1, \\ 7, 7^2 = 1, \\ 11, 11^2 = 1, \end{array} \right\} U_{12} \cong C_2 \times C_2$$

$$U_{10} \not\cong U_{12} \text{ but } U_{12} \cong U_8 \\ \cong C_2 \times C_2.$$

Just as a curiosity let us look at U_{12} . U_{12} has number of elements 1, 2 will not come, 3 will not come, 4 will not come, but 5 comes, 6 will not come and then 7 comes, 8, 9, 10 these three will not come. So, next one is 11 and of course 12 will not come. So, if I now want to compute the orders of this elements let us again look at the order of 5 so you have 5 and you have 5 square which is 25, but 25 is 1 modulo 12.

Then you will look at 7 and 7 square is 49 which is also 1 modulo 12 and of course 11 square is going to be 1 because 11 is minus 1 modulo 12. So, these three tell you that U_{12} is isomorphic to C_2 cross C_2 . Therefore, we have this nice result that U_{10} is also not isomorphic to U_{12} , but we do have that as groups U_{12} and U_8 are isomorphic both being isomorphic to C_2 cross C_2 .

In general, what we would want to do is to find the structure of all U_n we want to understand all U_n for every natural number n . We have made a step we have began the study of these structures of U_n by looking at U_p where p is a prime. Our experience has been that U_p are much more tractable the prime numbers things related to prime numbers are more tractable than things related to natural numbers. So, we would want to see whether the same thing holds in general.

(Refer Slide Time: 13:07)

If we expect a U_n to be a cyclic group then it should have at most 2 square roots of unity.

If C_n has a cyclic subgroup of order l
then it is the unique such subgroup.

$\#U_n = \varphi(n)$ and
each $\varphi(n)$, $n > 2$, is even!

However, when you are looking at a group U_n and you wonder whether that is a cyclic group we notice that in a cyclic group there are unique subgroups of any order which divides the order of the group. So, what I mean is that if C_n has a cyclic group of order l then it is the unique such subgroup meaning if I take a cyclic group of order n here that was C_n then first of all for every divisor of n there is a cyclic subgroup of that order.

But suppose we have a cyclic subgroup of C_n of order l then there is only one such subgroup you cannot have more than one such subgroups. Therefore, when we are looking at U_n for n higher up. So, we have looked at 2, 4 and the primes and so on then we noticed that whenever n is not equal to 2 then 2 has to divide $\varphi(n)$. So, there are two things that we have to notice here first of all the cardinality of each U_n is $\varphi(n)$ and each $\varphi(n)$ for n bigger than 2 is even. So, 2 is going to divide the cardinality of U_n and you may ask how many elements are there which have order 2. Is there a single such subgroup.

(Refer Slide Time: 15:23)

If we expect a U_n to be a cyclic group then it should have at most 2 square roots of unity.

Thus, whenever the number of square roots of 1 is more than 2, the group U_n cannot be a cyclic group.

So, whenever the number of square roots of 1 is more than 2 then the group U_n cannot be a cyclic group. So, what we are going to do is that we will look at all U_n we will take away the U_n which are never going to be cyclic because we have computed the number of square roots of 1 in all \mathbb{Z} by $n\mathbb{Z}$. We have their exact number depending on the number of prime factors and whether 2 divides it, 4 divides it, 8 divides it we have the exact description of the number of square roots of 1.

So, using that we will be able to tell exactly when these groups cannot be cyclic. So, the groups which can be cyclic that number is those groups are among the remaining ones and we will study them one by one that is our plan. So, now let us look at the U_n which cannot be cyclic and therefore we will have to recall the number of square roots of 1 that we have already computed.

(Refer Slide Time: 16:42)

Recall our calculation of the number of square roots of 1 in \mathbb{Z}_n :

$$2 < \begin{cases} 2^{k-1} & \text{sometimes} \\ 2^{k+1} & \text{always} \\ 2^k & \text{if } k \geq 2 \end{cases} \begin{cases} \text{if } n \equiv 2 \pmod{4}, \\ \text{if } n \equiv 0 \pmod{8}, \\ \text{otherwise.} \end{cases}$$

where $k =$ number of distinct prime factors of n .

So, these are the number of square roots of 1 in \mathbb{Z}_n and if you remember this was the exact description. So, whenever we had k distinct prime factors, we had the numbers to be these three numbers. Now, whenever these numbers are more than 2 then our U_n cannot be a cyclic group. So, here we want to look at these to be more than 2 that is the thing that we have to find.

So, k because you will have at least 1 prime factor so whenever you have 2 or more factors then this will tell you if there are 2 or more odd factors let us say because the even factors are divided in two cases here. So, whenever you have two or more odd prime factors then the number of square roots of 1 is going to be 2 power k which is bigger than 2. So, this is bigger than 2 if this number k is bigger equal to 2.

So, whenever you have two or more odd prime factors the group U_n cannot be cyclic. So, for instance if you were looking at 3 into 5 and therefore you would look at U_{15} then U_{15} is never going to be a cyclic group that is because the number of square roots of 1 in U_{15} or in \mathbb{Z}_{15} which is the same thing is equal to 4. There are 2 coming from 3 and 2 coming from 5.

So, once you have more than or equal to 2 odd prime factors then U_n cannot be cyclic. Let us now look at the possibility where one of the factors can be 2. So, if 2 is the only prime power of 2 which divides the group and no higher prime power divide then you are in this situation. So, 2 divides but 4 does not divide that is the situation that we are looking at and here once again we have 2 power k minus 1 among the k minus 1, k is already equal to 2.

One of the primes that you have is already equal to 2 so you are looking at all other odd primes and therefore if you have k minus 1 odd prime factors together with 2 where that k minus 1 is 2 or more which means to say that k is 3 or more the total number of prime factors including 2 is 3 or more and 4 does not divide the number than you cannot have the group U_n to be cyclic.

And finally, if you have n congruent to 0 mod 8 whatever number of prime factors you have 2 power k plus n is always going to be bigger than or equal to 2. So, here you always have this to be bigger equal to this is something that you have to study later so we will say sometimes. So, these are the three major observations which we write down here.

(Refer Slide Time: 20:09)

If n has two or more odd ^{prime} factors, then U_n is not cyclic.
 2^k square roots of 1.



If n has two or more odd prime factors then U_n is not cyclic. This is once again recalling that the number of prime factors being k will give you that there are 2 power k square roots of 1 and therefore once k is bigger equal to 2 than U_n cannot be cyclic. So, whenever you have two or more odd prime factors this has to be prime then U_n cannot be cyclic.

(Refer Slide Time: 20:48)

If n has two or more odd ^{prime} factors, then U_n is not cyclic.

If $n \equiv 0 \pmod{8}$, then U_n is not cyclic. $2^{k+1} > 2$ as $k \geq 1$.



If n has two or more odd ^{prime} factors, then U_n is not cyclic.

If $n \equiv 0 \pmod{8}$, then U_n is not cyclic.

If $n = 4m$, where m is odd, ^{$m \geq 1$} then again U_n is not cyclic.

$$U_2 = \{1\} \cong C_1, \quad U_4 = \{1, 3\} \cong C_2.$$

We know that U_2 and U_4 are cyclic.



So, we next come to 2 dividing the number n and assume that 8 divide. So, we will look at the cases where 2 divides, but 4 does not divide, 4 divides but 8 does not divide and 8 divides. These are the three cases so whenever you have an congruent to 0 mod 8 then U_n is not cyclic so here the number of square roots of 1 was 2 power k plus 1 which is always bigger than 2 because you have at least one prime which is 2 dividing it. So k is bigger than or equal to 1.

So, this group is also not a cyclic group. So now the cases are as follows. You will have that 4 divides your number n and then there can be one more odd factor. If there are two or more odd factors then we will refer to the first statement and U_n cannot be cyclic. So, now we are

going to deal with the cases where n is p power e where p is odd 2 into p power e where p is odd or 4 into p power e where p is odd those are the cases that we have to deal with.

So, this is the last case $4n$ is $4m$ where m is odd then again U_n is not cyclic. This is because in this case if you were looking at the square roots modulo n . There is a square root modulo 4 namely 3 the square root of 1 and m being odd will give you at least one more square root and together with the element 1 you have more than 2 square roots of 1 and so U_n is not going to be cyclic.

(Refer Slide Time: 22:44)


If n has two or more odd ^{prime} factors, then U_n is not cyclic.

If $n \equiv 0 \pmod{8}$, then U_n is not cyclic.

If $n = 4m$, where m is odd, then again U_n is not cyclic.

$$U_2 = \{1\} \cong C_1, \quad U_4 = \{1, 3\} \cong C_2.$$

We know that U_2 and U_4 are cyclic.



And the final thing that we have to now notice is where 2 is the only factor or you have that n is equal to 4 because when you are looking at here n is $4m$ m is odd and we are going to take m to be strictly bigger than 1. This is the case when U_n is not cyclic. And so the final thing is where we have U_2 and U_4 these are cyclic, this is something that we can easily see. So U_2 for instance is the trivial group.

And therefore, it is isomorphic to C_1 and U_4 has only two elements 1, 3 and therefore it is isomorphic to C_2 . So, both U_2 and U_4 are cyclic. So, the only remaining cases now are where you have 2 divides the number n no higher power of 2 divides n and the only other factor the only other prime factor is a single odd prime.

(Refer Slide Time: 24:06)

Thus, the only remaining cases are $n = p^e$ or $2p^e$ where p is an odd prime.

We will prove that in these cases the group U_n is cyclic.

This is proved by producing a primitive element in each of these U_n .

So, the only remaining cases are n equal to p power e or 2 times p power e and what we are now going to show is that in both these cases the groups U_n are cyclic and this is going to be done by producing a primitive element in each of these U_n . So, primitive element just to recall is an element whose order is exactly equal to $\phi(n)$. This is what we are going to do, we will produce a primitive element in each of these U_n . So, the very first stage we actually have to look at p power e and $2 p$ power e .

(Refer Slide Time: 24:51)

Theorem: If $n = p^2$ then U_n is cyclic. ($p = \text{odd}$)

Proof: " $\exists a \in \mathbb{N}$ is a primitive root modulo p^2 then a is also a primitive root modulo p

$$o(a) = d \text{ in } U_{p^2} \text{ is } p(p-1).$$

$$\Rightarrow o(a) = d_1 \text{ in } U_p \text{ is } (p-1).$$

$$p \mid a^{d_1} - 1 \text{ then } p^2 \mid a^{d_1 p} - 1.$$

But we will start with the case where n is p square and remember this is something that I will not repeat that p is always an odd prime. So, we are going to prove that whenever n is p

square than U_n is a cyclic group. So, one basic statement here that we are going to use is the following. If $a \in \mathbb{N}$ the natural numbers a is a primitive root modulo p^2 then a is also a primitive root modulo p .

This is a basic statement. So, what we observe here is that when we are starting with $a \in \mathbb{N}$ being a primitive root modulo p^2 , we will start with the assumption that the order of a which is d modulo p^2 so in U_{p^2} is $p-1$. This is the order we are starting with the statement this implies that the order of a which we can call d_1 in U_p is $p-1$.

So, what we will have to show in this case is that if you have some d_1 so p divides $d_1 - 1$ then p^2 divides $d_1 - 1$. This is something that we will have to show. So, this will imply that if you had any smaller d_1 inside the group $\mathbb{Z}/p\mathbb{Z}$ as your order of the element a in U_p then the order of a in U_{p^2} will have to be smaller than $p-1$.

So, with this exercise we have this observation that a primitive root modulo p^2 is also a primitive root modulo p . Here, we will want to show that U_n is cyclic U_{p^2} is cyclic so we will need to produce a primitive root modulo p^2 and when you look at it modulo p that should already be a primitive root modulo p . We know that there are primitive roots modulo p .

So, we will pick one of those we will see whether that is already a primitive root modulo p^2 and if not then we will add a suitable multiple of p to get a primitive root modulo p^2 keeping the same modulo p , the same residue plus modulo p . Since this proof is going to involve few more slides and sore more time. I think we should begin this proof in our next lecture. Please remember what we have done and the plan of the proof is also something that I have told you just now. So, we will start with this proof in our next lecture. Thank you.