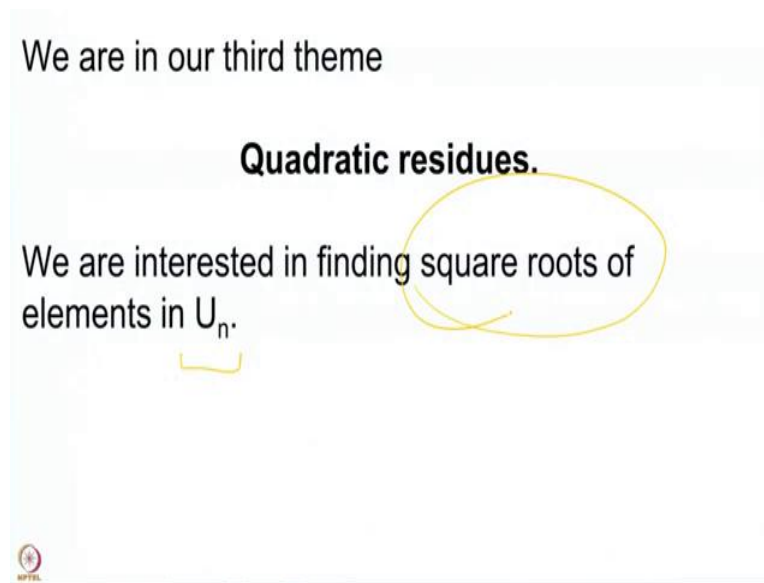


A Basic Course in Number Theory
Professor Shripad Garge
Department of Mathematics
Indian Institute of Technology, Bombay
Lecture 31
Quadratic Residues

Welcome back. We have completed almost half of our course and among the themes we have completed two major themes and we started with the third theme in the last lecture towards the end. I hope you are also as excited as I am about this theme. This is on quadratic residues.

(Refer Slide Time: 0:45)



So, this is our our third theme quadratic residues and what we are going to do in this is essentially to solve quadratic equations over \mathbb{Z}_n . But we saw that we will of course not be able to solve the quadratic equations for every coefficients, but we will need to take the 2 a to be an invertible element modulo N.

So, a if you remember from last lecture was the coefficient of x square, so that a needs to be an invertible element and moreover a 2 also needs to be an invertible element. This is what we have seen in the last lecture and then we saw that to solve such an equation, it is enough to find square roots of various elements.

So, what we are restricting ourselves at the moment is that we will look at elements which are invertible. So, these are elements in U_n . And we want to compute square roots of these elements, so this is something that I have already remarked to you that U_n is a group. We have that \mathbb{Z}_n is a ring and therefore U_n the set of all invertible elements modulo n forms a group under multiplication. And now if I want to find what elements have square roots or

what are those square roots further, the simplest thing would be to compute squares of every element.


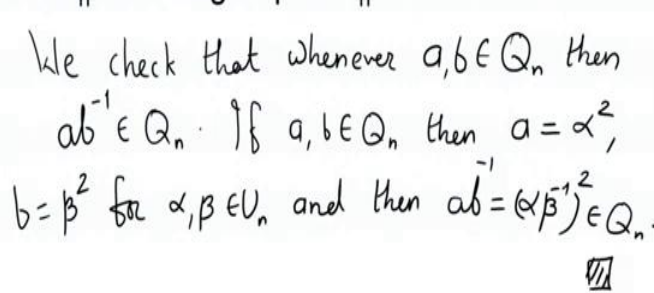
So, once you know, what are the squares and you would also know which element squared to what element and therefore in the reverse way you will know which are the square roots of your given element, whether it has a square root or not. And whenever it has what are the square roots, this is the knowledge we will have. So, we want to compute the set of all squares in U_n .

(Refer Slide Time: 2:44)

Let Q_n denote the set of quadratic residues modulo n , these are the squares of elements in U_n .

Note that Q_n is a subgroup of U_n .

We check that whenever $a, b \in Q_n$ then $ab^{-1} \in Q_n$. If $a, b \in Q_n$ then $a = \alpha^2$, $b = \beta^2$ for $\alpha, \beta \in U_n$ and then $ab^{-1} = (\alpha\beta^{-1})^2 \in Q_n$.



This is our notation for the quadratic residues modulo n and this as we have noted these are nothing but squares of elements in U_n . Now, there is one small thing which we are going to observe and this small remark is very useful in many of the computations that we are going to do later.

So, this remark is that Q_n is a subgroup of U_n . So, perhaps we can also see a proof of this quickly. There are several ways to check when some subset is a subgroup. The essential thing is that you should check that it is closed under taking multiplication, 1 is there and further inverse of every element is also there. Or all these things can be combined in the following statements.

So, we check that whenever a and b are elements in Q_n then ab^{-1} is also in Q_n . This one statement will capture all the properties that you want to have. So, how do we have this statement? If you have a and b in Q_n then a is square of some α , b is the square of some β for α, β in U_n . And then it is a simple matter to check that ab^{-1} is the square

of alpha, beta inverse square. So, ab inverse is the square of alpha beta inverse and therefore this is also in Q_n . So, we have that Q_n is actually a subgroup of the group U_n of all invertible elements. And this one thing helps us quite a lot as we will see in the coming slides, but we also did some computations of Q_n for some small integers n . Let me recall that for you.

(Refer Slide Time: 05:38)

Let Q_n denote the set of quadratic residues modulo n , these are the squares of elements in U_n .

Note that Q_n is a subgroup of U_n .

Examples:

1. Compute $Q_7: \{1, 4, 2\} \subseteq U_7 = \{1, 2, \dots, 6\}$
2. Compute $Q_8: \{1\} \subseteq U_8 = \{1, 3, 5, 7\}$

We have we computed Q_7 which was 1, 2 and 4. This is sitting in U_7 , which you remember is 1, 2 all the way up to 6. And Q_8 , it is simply 1, this is sitting in U_8 which is the set of all odd elements up to 8. So, here we had only four elements in U_8 . And surprisingly there is only one element in Q_n . Only the identity element is the square in Q_8 . In U_8 , that is the only square so there is only one element in Q_8 .

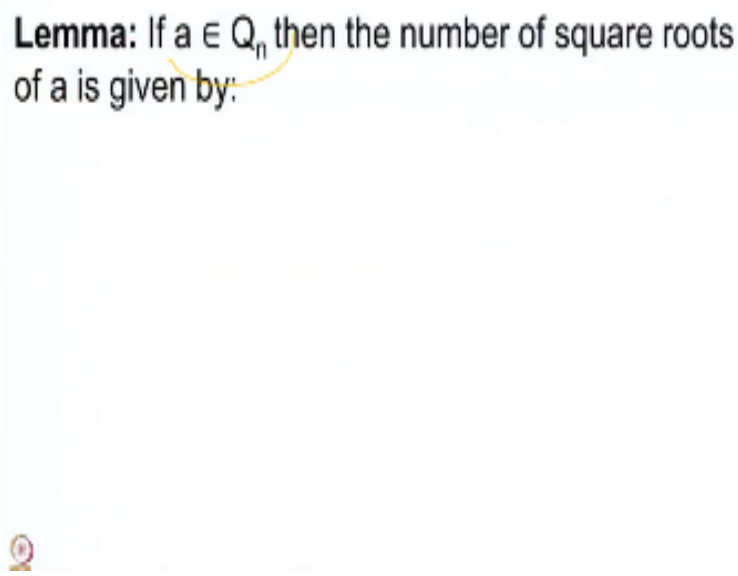
Whereas here in U_7 , we had six elements and their squares gave us a set of three elements. So, this is something which we see is a different behaviour because our 7 is a prime number and 8 is a power of 2. So, 7 corresponds to something which is an odd prime and 8 corresponds to the oddest of the primes as we have started calling it, the even prime too.

So, this is the behaviour that we are going to see. We will also see later that in most of the discussions we will off course be taking the n , to be odd. So, we will not look at the number 2 or in fact any even number right now, we will only look odd numbers and so whenever we will also talk about primes we will only concentrate on odd primes.

You know, as far as squares are concerned when you look at \mathbb{Z} by $2\mathbb{Z}$, everything is the square. \mathbb{Z} by $2\mathbb{Z}$ is 0 and 1, 0 square is 0 and 1 square is 1. So, everything is a square only when we go beyond 2 then, we get some non square elements and so things get more interesting as you go beyond 2.

So, that is the reason that among the primes we will not look at the prime P equal to 2, but we will look at odd primes and as we have seen at the beginning of the discussion of this theme that when you take the quadratic polynomial $ax^2 + bx + c$, you are going to have to divide by $2a$. So, $2a$, has to be invertible which says that a has to be invertible and 2 has to be invertible and so n will have to be an odd natural number.

(Refer Slide Time: 08:27)



Lemma: If $a \in \mathbb{Q}_n$ then the number of square roots of a is given by:

This is our beginning statement that you start with a in \mathbb{Q}_n , then the number of square roots of a , so we are assuming already that a is in \mathbb{Q}_n that is something that we already assumed. So, a is already a square, then the number of square roots of a is given by the following formula.

(Refer Slide Time: 08:57)

Lemma: If $a \in \mathbb{Q}_n$ then the number of square roots of a is given by:

$$\begin{cases} 2^{k-1} & \text{if } n \equiv 2 \pmod{4}, \quad n \neq 2 \\ 2^{k+1} & \text{if } n \equiv 0 \pmod{8}, \\ 2^k & \text{otherwise.} \end{cases} \left. \begin{array}{l} n \text{ is odd} \\ n=4m, m \text{ is odd} \end{array} \right\}$$

where k = number of distinct prime factors of n .

This formula is $2^k - 1$. Where, n is congruent to $2 \pmod{4}$. Remember that here we are not taking n equal to 2 because that is a case that we are not looking at. So, here we will start with 6 onwards. And so, therefore you are at least going to have k to be more than 1. So, k will be 2 or above and therefore $2^k - 1$ does make sense. If you are looking at n equal to 2 then k is 1. And then you have only 2^0 which is 1 so that is also correct. But at the moment we are not looking at the case n equal to 2.

Here whenever 8 divides n we have the number to be $2^k + 1$ which is 1 more than the number of primes and in all the other cases. So, here the other cases are where n is odd or n equal to $4m$ where m is odd. These are the remaining cases. So, in all these cases we have that the number of prime factors if that is k then, the square roots of any given element in \mathbb{Q}_n is a fixed number that depends only on n and that is given by this formula.

You will realize that this was the same formula we had for computing the number of square roots of 1. When we computed the solutions to the equation $x^2 \equiv 1 \pmod{n}$ we got exactly the same formula and that is the same formula and the reason will become very clear to you. Once you recall that \mathbb{Q}_n is a subgroup of \mathbb{U}_n .

(Refer Slide Time: 11:04)

Proof: Consider a group hom. $\varphi: U_n \rightarrow U_n$
 $a \mapsto a^2$.

Since U_n is abelian φ is a group homomorphism.

By definition $Q_n = \varphi(U_n) = \{a^2 : a \in U_n\}$.

The number given above, in the statement,
is $|\ker \varphi| = N$.

So, let us quickly prove this formula. The formula can be proved in the following way. So, we consider a group homomorphism call it phi from U_n to U_n . And this is defined by sending an a to its square. So, this is clearly a group homomorphism because our group is abelian. So, since U_n is abelian, phi is a group homomorphism. And now by definition Q_n is the image of the group U_n under phi. Because we are looking at Q_n to be the set of all squares in U_n . So, these are precisely the image, this is precisely the image of the homomorphism phi.

So, this is nothing but a square where a belongs to U_n . This is what we have and we can also determine the kernel. So, the number given above and by above I mean in the statement of the result, is the cardinality of the kernel of phi. So, we have a cardinality of this kernel of phi.

What is kernel in the language of group theory? Kernel is the set of all elements in U_n which under the map phi go to the trivial element. But our map phi is defined by taking an element to its square. So, kernel is precisely those elements whose square is 1. And therefore, kernel is precisely the set of square roots of 1. These are precisely the elements satisfying $x^2 - 1 = 0$ in $\mathbb{Z}/n\mathbb{Z}$.

So, kernel has some quantity. So, the cardinality of this kernel is capital N which is defined in the previous slide given by 2^{k-1} , 2^k or 2^{k+1} depending on how 2 divides the number n and the number of prime factors of n . We

have the number so that capital N will depend only on small n. And that is exactly the cardinality of the kernel.

(Refer Slide Time: 14:17)

Proof (contd.): Further, if $a \in Q_n$, $a = \alpha^2$
 then there is a bijection

$$A = \{ \beta \in U_n : \beta^2 = a \} \xleftrightarrow{\theta} \{ \gamma \in U_n : \gamma^2 = 1 \} = \ker \varphi$$

$\beta \mapsto \beta \alpha^{-1}$ $(\beta \alpha^{-1})^2 = \beta^2 \alpha^{-2} = 1$
 $\theta : A \rightarrow \ker \varphi, \beta \mapsto \beta \alpha^{-1}$

$\exists \gamma \in \ker \varphi$, we take $\beta = \gamma \alpha$. (Onto)
 $\exists \beta_1 \alpha^{-1} = \beta_2 \alpha^{-1} \Rightarrow \beta_1 = \beta_2$

Further we have this very basic statement coming from group theory. Further, if a is in Q_n so a is alpha square then, there is a bijection so then there is a bijection between two sets. All the beta's in U_n , where beta square is a, with all the gamma in U_n , with gamma square equal to 1. And once you start with a beta here we will send the beta to beta alpha inverse.

So, let us check that this is indeed a bijection. We will check it by using a different ink. So, to show that this is a bijection clearly we have to show that whenever you start with a beta here, its image beta in alpha inverse belongs to this set. But that is clear because beta alpha inverse square is beta square alpha raise to minus 2. You have fixed your alpha with the property that alpha square is a. And you also have that beta square is a, so this is equal to 1.

So, have fixed beta, we have fixed an alpha and then for every beta in this set, call it capital A and this is our set kernel phi. Then we have this natural map and we will show that it is a bijection. It is a natural map only once you have fixed this element alpha. Alright, so what we have shown is that the map, let me call this map by theta. So, there is this map theta from a to kernel phi, this map is well-defined now. It is obtained by sending the element beta to beta alpha inverse.

We want to show that this is a bijection so we should show that it is a one-to-one onto map. So, if there is a gamma in kernel phi. We take beta to be, we have to take a beta such that beta

alpha inverse is gamma. We are now starting with an element in kernel phi, and we are now trying to define an element in capital A which under the map theta gets sent to gamma. So, we should construct a beta such that beta alpha inverse is gamma. But this beta should be gamma into alpha so that when you cancel out alpha you get gamma.

This is quite clear. So, this beta now so this gives onto nis. And now we need to show one to one property. But if you have beta 1 alpha inverse equal to beta 2 alpha inverse that would imply that beta 1 is beta 2, because alpha is after all an element in Un. You can multiply by alpha to the both the sides of this equality beta 1 alpha inverse equal to beta 2 alpha inverse. So, you are cancelling the alpha inverse to get that beta 1 is beta 2.

So, this says that the map is also 1 to 1. So, what we have now proved is that there is a bijection from the set capital A to the kernel of the map phi. And once we have this bijection we are now able to get our result. So, we would want to show that the cardinality of the set a is exactly the same as the cardinality of kernel phi and that will follow once we have that there is this bijection.

(Refer Slide Time: 19:10)

Proof (contd.): Further, if $a \in Q_n$, $a = \alpha^2$

then there is a bijection

$$A = \{ \beta \in U_n : \beta^2 = a \} \xleftrightarrow{\text{bij}} \{ \gamma \in U_n : \gamma^2 = 1 \}$$

(coset of α) $\beta \mapsto \beta \alpha^{-1}$

$$|A| = |\ker \varphi| = \begin{cases} 2^{k-1} & n \equiv 2(4), \\ 2^{k+1} & n \equiv 0(8), \\ 2^k & \text{else.} \end{cases}$$

□

So, this bijection, will tell us that cardinality of the set A is equal to cardinality of the set kernel phi which is the numbers that we had earlier 2 power k minus 1, 2 power k plus 1 and 2 power k. And if you remember this was n congruent to 2 mod 4, this was the case n congruent to 0 mod 8. And this is the remaining case. So, this completes our proof, whenever there is an element in Qn, then the number of all square roots of the number A, the element A is given by the cardinality of the kernel of the map phi.

So, you see that once we have used that Q_n is a subgroup. We know that it can be seen as image of this square map. And therefore, we are able to compute the cardinality of the kernel. And after all if you also remember some of the group theory you will see that the inverse image of every other element will give you a certain coset. And each coset will have the cardinality equal to the cardinality of the kernel. We see that here this A is nothing but the coset of the element α , this is what we have.

So, the cosets will all have the cardinality equal to coset of the trivial element which is your sub Group by which you are going modulo. So, in this case it is the kernel. So, this is one very nice calculation. It will tell you that once you have some element to be in Q_n it is going to have a large number of square roots and so we can somehow hope to compute the number of elements in Q_n from this.

You see after all what we have is that Q_n being the image is also actually a subgroup of U_n because you have this square map from U_n and to U_n , sending every element to its square. So, Q_n is the image on the right hand side a subgroup and therefore its cardinality will have to divide the cardinality of the whole group, which is $\phi(n)$. But because the kernel has cardinality N , then we know exactly how many elements there can be in Q_n .

(Refer Slide Time: 21:58)

Corollary: The number of elements in Q_n is $\frac{\phi(n)}{N}$ where $N \in \{2^{k-1}, 2^k, 2^{k+1}\}$ as in the previous lemma. *ϕ is the Euler ϕ function*

Proof: This follows from the earlier proof with $|Q_n| = |\varphi(U_n)| = \frac{|U_n|}{|\ker \varphi} = \frac{\phi(n)}{N}$

So, this follows from the earlier proof with cardinality of $\phi(U_n)$ equal to cardinality of U_n upon cardinality of kernel ϕ . So, this is actually cardinality of our subgroup Q_n and here we have this to be cardinality U_n is the Euler ϕ function, so I should not have used the same

symbol phi here. So, let me write the Euler phi function in a different ink, upon N where N is this number. So, this phi is the Euler phi function.

So, this corollary follows quite easily and we also have one more small result, which says that whenever the group U_n has a primitive root. So, whenever the group U_n is cyclic, then Q_n will have exactly $\phi(N)/2$ elements. So, the second statement here follows quite nicely because our N is going to be 2 when U_n is cyclic.

This is because whenever your U_n is cyclic, we know that the number of square roots of 1 is going to give you a subgroup and so you cannot have more than 1 cyclic subgroup of any given order inside a cyclic group. So, the number of square roots of 1, if there were more than 2 square roots, then you will have multiple copies of cyclic groups of order 2 sitting in U_n . This is something that we have remarked earlier as well.

(Refer Slide Time: 24:40)

Corollary: For $n > 2$, if U_n has a primitive root, g , then " Q_n is a cyclic subgroup of U_n generated by g^2 " and hence has $\phi(n)/2$ elements.

Proof: " $N=2$ when U_n is cyclic"

$$Q_n = \{a^2 : a \in U_n\} = \{(g^i)^2 : i \in \mathbb{N}\}$$

$$= \{(g^2)^i : i \in \mathbb{N}\} = \langle g^2 \rangle.$$

$|Q_n| = \phi(n)/2$. Here ϕ is the Euler ϕ function.

But even here we can see that statement quite easily because it will follow from the above statement that Q_n is a cyclic subgroup of U_n generated by g square. Once we prove this then it will follow quite easily that the cardinality of Q_n is exactly 1 by 2 of the cardinality of U_n and so it will have $\phi(n)/2$ elements.

And this statement is also quite easy to see because Q_n is after all the squares of every element in U_n . But every element in U_n is some power of g . Because g is your primitive root, you have fixed a primitive root g . And then you are going to take the square. So, this is for i let us say in capital N. And therefore, this is nothing but a group which is generated by g

squares. And so we get that Q_n is the subgroup of U_n which is generated by g^2 . So, here we have proved that every element of Q_n is a power of g^2 and that already tells you that the cyclic subgroup Q_n of U_n is generated by g^2 .

So, you will have that there are exactly half the elements in Q_n as they were in U_n . And so the cardinality of Q_n then happens to be $\phi(n)/2$. Where this ϕ is the Euler phi function. So, here there is one small thing where I would like to draw your attention to which is that we are taking n to be bigger than 2, if your n is equal to 2, of course that is the case that we are avoiding everywhere. But if you were taking n to be equal to 2 then U_2 has only 1 element.

And although g which is a primitive root for U_2 which is 1 is itself a square. So, Q_2 also has 1 element and therefore this statement will not be quite true. So, that is one small rework for which we have to take n to be bigger than 2 because then we know that $\phi(n)$ is going to be an even number for every n bigger than 2 the Euler phi function is always an even number. Once we have this then the rest of the things follow quite nicely.

So, what we are now going to do is to look very closely to the squares in general for the squares in U_n . Try to devise a way to compute these squares and get some nice formulae about it. The punch lines that are going to come are the quadratic reciprocity laws. These are some very important laws and they have very interesting generalizations in higher dimension.

Where instead of quadratic you have a cubic reciprocity law; a quadratic reciprocity law and so on and finally there is the pinnacle of algebraic number theory, which is Artin's reciprocity law, but to go to that we must first learn the quadratic reciprocity law. We will go towards that in our next lecture. I hope to see you until then. Thank you.