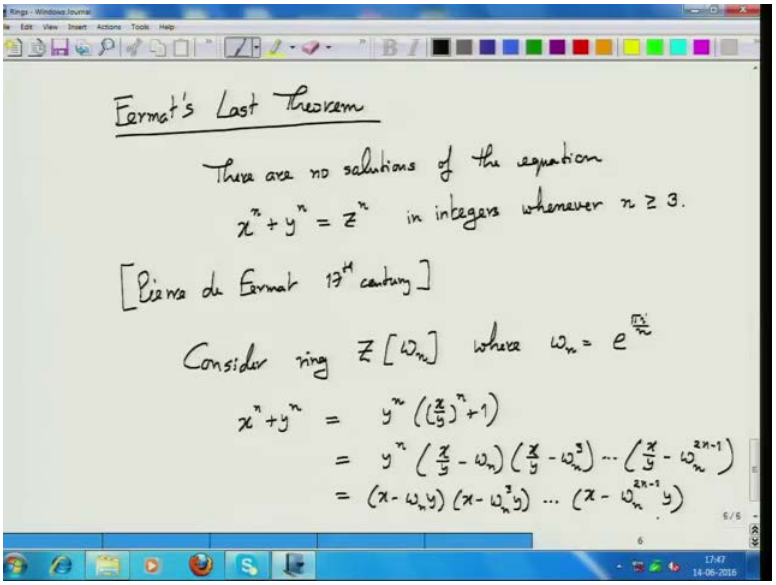
Modern Algebra
Prof. Manindra Agrawal
Department of Computer Science and Engineering
Indian Institute of Technology, Kanpur

Lecture - 08
Rings: Failure of Unique Factorization

Let us start today with bit over history, which is also the story of exactly how and why these kind of rings that I described yesterday; we have studied and, that factorization of numbers into primes and the problems they are on was found. So, this is related to Fermat's Last Theorem.

(Refer Slide Time: 00:51)



Now, how many of you have heard about this Fermat's Last Theorem? Anyone?

Student: (Refer Time: 01:02).

What?

Student: (Refer Time: 01:04).

You have heard of it. It states that, there are no solution of the equation in integers whenever n is greater than equal to 3. So, this was (Refer Time: 01:48) when that was for a hypothesis, which was made by Pierre de Fermat, who was a mathematician in seventeenth century. This is a very interesting statement, because when n equals 2, then x

square plus y square is equal to z square has lots of solutions; 3 square plus 4 square is equal to 5 square, being one of them; where, as soon as n becomes 3 or higher number, there are no solutions; that is a claim by this.

And, to such a nice and simple statement and. so (Refer Time: 02:37) a lot of attention. In fact, Fermat is – while he was studying a book by Euclid and in the margin of that book, he wrote this statement and also wrote that I have found a very ingenious proof of this statement, but this margin is too small to write that proof down; and, soon after he died. So, he could never write down his proof. And, this became a big mystery to all other mathematicians, exactly what was that proof of Fermat that he could not write down.

And, over the centuries, number of mathematicians tried to find the proof were elusive proofs; but, none of them succeeded. This theorem was finally proved after more than 300 years in 1995 about 20 years ago using some very advanced mathematics. But, that is not really what I am talking about today. I am talking about a proof that was also other (Refer Time: 03:47) proof that was found of this long time ago around nineteenth century. And, that proof end like this. Let us consider ring – So, you take this complex number and then just like we did last time that, introduce or add this into the set of integers and look at all the numbers we can form with this. These are going to be a subset of complex numbers.

Now, If you look at this x to the n plus y to the n – the left hand side of this equation, I can write it as; here I can just take y to the n out in common – x by y to the n plus 1. And, this number a raised to the n plus 1; this will factor in this way, very nice way. What is the property of omega n? Omega n is e to the pi i by n. Then, omega n to the n is e to the pi i. And, what is e to the pi i? Minus 1, so omega to the n is minus 1. And, omega to the 2 n is plus 1 (Refer Time: 05:54). So, this will factor as this being exactly the one of the values of x by y would be omega n. But, there will be many values. In fact omega n q also will satisfy this property, that is, n-th power is minus 1.

So, in fact, you can see omega n, omega n cube, omega n to the 5, essentially all odd powers of omega n, will satisfy this, that is, n-th power is minus 1. All even powers will satisfy that their n-th power is plus 1. So, I can factor this as – and therefore, equal to x minus omega n y, x minus omega n cube y. And, each one of these is in number in this.

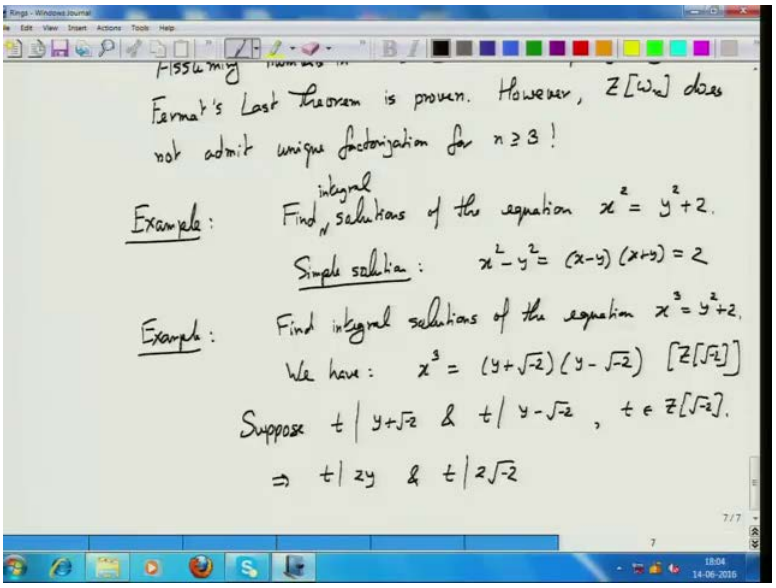
And now, since I have this being equal to z to the n, this would mean that this product equals z multiplied – z is an integer, which is multiplied to itself n times. These are also numbers. So, z is an integer in this ring and these are also in numbers from this ring. So, the same number is being written as a product in two different phases now.

If unique factorization holds in this ring; then, the only way it is possible is that, the numbers further get factored out. Each of this number gets further factored into other numbers. Similarly, the z here also gets factored into other numbers. And, all of them when their two sides essentially the primes and this, when you write z to the n in terms of product of primes and this, this also in terms of product of primes and this, it comes out to be same.

And then, it was shown, then that is not the case. That factorizes these numbers – factor into primes, which are of a kind different; then, this integer z factoring into primes in this ring. And, this would hold whenever n was 3 or more. Now, what does that mean? That means this equation cannot be satisfied. There is no x, y, z, which satisfies this equation, because if it did exist, then we will have these two distinct factorizations of the same number in this ring. And, that is not possible.

So, mathematician of 19th century implicitly assume that, in this ring, there will be unique factorization. And, based on this assumption, this was a short proof that Fermat's Last Theorem is true. And, many actually thought that, this is the proof that Fermat also formed. The only problem was, in fact, when this was published, everybody were very happy and then suddenly somebody found, rather observed that, this ring has a problem; that is, a number can be factorized in this ring in two different ways just like we had that, z square root of minus 5; two different ways of factorizing. And suddenly, the whole proof broke down that, of course, one - if you can factorize number in two completely different ways, then this argument does not.(Refer Time: 10:32).

(Refer Slide Time: 10:35)



So, in summary, there is no unique factorization for n greater than or equal to 3. So, this brought to the notice of the community that, there are rings of numbers, which rings of integer of a more general kind, where the unique factorization into primes does not work. This was a ver, very unusual situation. It made a lot people very uncomfortable that how can this be and these – what are these? These are certainly are numbers, but numbers must have this nice property of unique factorization and they do not have. So, a lot of effort was made trying to restore this unique factorization property. And, the mathematician, who was finally able to do, was Martin Kummer I believe, who introduced what are called ideal numbers in these rings of numbers, using which he restored the unique factorization property.

Now, ideal numbers, which I will describe shortly, got more nicely captured as or shortened as ideals. And, ideals have since then come to acquire a very, very important place in the theory of rings. So, that is a story. And, that is how this (Refer Time: 13:25) General ring of numbers was initially considered and this structure of this ring needs to be understood rather than because we would like to see exactly how these rings behave. As you can see that, this ring is intimately connected to a very nice question about integers, in order to resolve this question about integers; we have naturally introduced this ring.

So, that is kind of another example of what I claimed earlier right in the beginning of this

course that, these abstractions – once you did it and once you study them, will help us in proving things about – no, things of real live off there are of real interest to us. Problems about integers are course interesting. So, one would like to prove them and this is one way to (Refer Time: 14:37).

Let us take another example: of another type of Ring. Let us say, we want to answer the question find solutions of the equation x square equals y square plus 2. So, essentially, you want to know the pair and this is solutions over integers. This answers the question of or addresses the question of whether two squares are separated by number 2 and value 2. And, you want to find the solutions of this. How would you go about finding a solution? You have a strategy in mind? Yes?

Student: We can factorize x square minus y square.

Factorize x square minus y square, so x minus y and x plus y, OK?

Student: (Refer Time: 15:56).

So, then you have a very; good, excellent. So, you factorize simple solution. You have x minus y square, which is x minus y x plus y, which is 2. So, there are two integers, product is 2. So, one of them has to be 1 and other has to be 2, and then you just write down all these solutions (Refer Time: 16:25) Next example: This made x square to x cube. This is asking the question, if a cube and square is deferred by 2. Now, that factorization trick would not work; x cube minus y square you cannot factorize. So, what can one do? Why here, why not factorize the right-hand side – y square plus 2?

Student: y plus y root two (Refer Time: 18:04).

That is right, y plus i root 2 of (Refer Time: 18:07).

Student: (Refer Time: 18:09).

See, we want to (Refer Time: 18:13) We measure a number, is not allowed to have a value of x and y. That is correct; we have to find integers values. Now, we want to find a way to derive these solutions. So, in order to find that way, there is no restrictions, we can use any which way. So, since this idea that, once if you can factorize both sides, then and then you can equate the side as the factors; that is the idea, which was used here in x

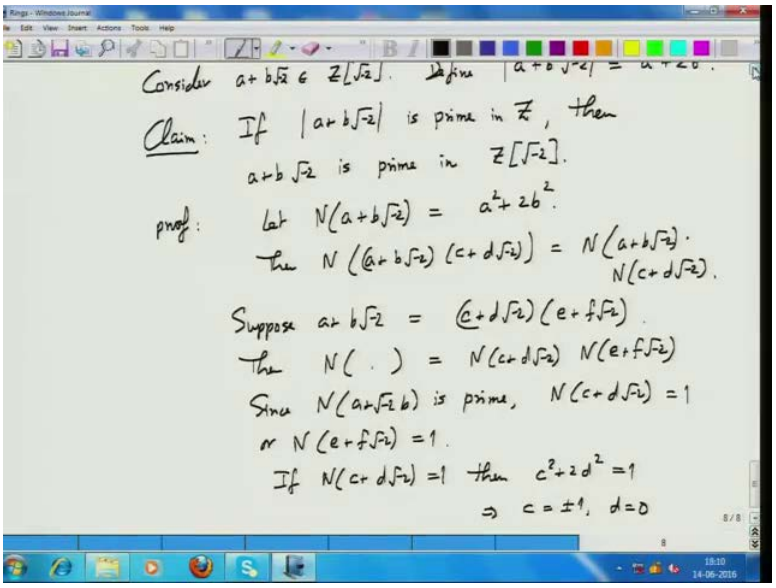
square – x minus y times x plus y equals 2. That is very simple factorization got it as a result very quickly; here I am trying to use the same idea.

The only difference here is that, now, I have moved from the domain of integers to a larger ring of integers. This is the ring – z square root of minus 2. That is a ring that had occurred last time also. Of course, we again come to this issue of unique factorization being there and can this be factorized, can there be unique factorization in this ring. It turns out that, in this ring, the unique factorization holds. It requires certain effort to prove, and I will not make that effort; you have to just believe me. It is not very difficult to prove, but it just requires some calculations to show. Then, unique factorization does work in this ring.

The whole point being that, the knowledge or extensions to these bigger rings will help or does help us in answering questions about integers. The questions are the kind we are interested in. So, this shows and gives us a reason why we would like to study this larger rings of numbers in general rings. So, let us continue a bit more or towards this. So, since unique factorization holds, we will have x cube equals these two products. Now, of course, we have to see and it is possible that, these numbers further factor into something. That is always possible. Then, that will depend on the value y, which is what we need to find out.

However, there is one thing we can do, which is to look at these two factors and ask the question – do they have a nontrivial GCD? So, suppose a number t divides y plus square root of minus 2 and t divides y minus square root of minus 2; they have a common factor. Remember t is in this ring, because this is the ring over which we are now operating. Then what? Then, it follows that, this implies that, t divides 2y and t divides their difference, which is 2 square root of minus 2. So, this limits the possibilities of t. So, t can only be. Now, of course, I have to see what are the primes in this ring. So, let me give you a trick to find out a number whether a number is prime in a ring like this. And, that trick involves using norms.

(Refer Slide Time: 22:39)



So, let us just consider this following: a plus b square root 2 – square root of minus 2. Define norm of this to be a square plus 2 b square. And now, the claim is if norm of a plus b square root of minus 2 is prime in z; then, that number is prime in z square root minus 2. This is a very simple proof. Let us see if we can discover it. Suppose norm is prime and further suppose this is not prime; then, it factors – I should give you a (Refer Time: 24:04) cannot expect you to prove it immediately, because there is one more fact that we must know that, if you have a number; so, let us denote by n of the number to be represent the norm; then, norm happens to be multiplicative.

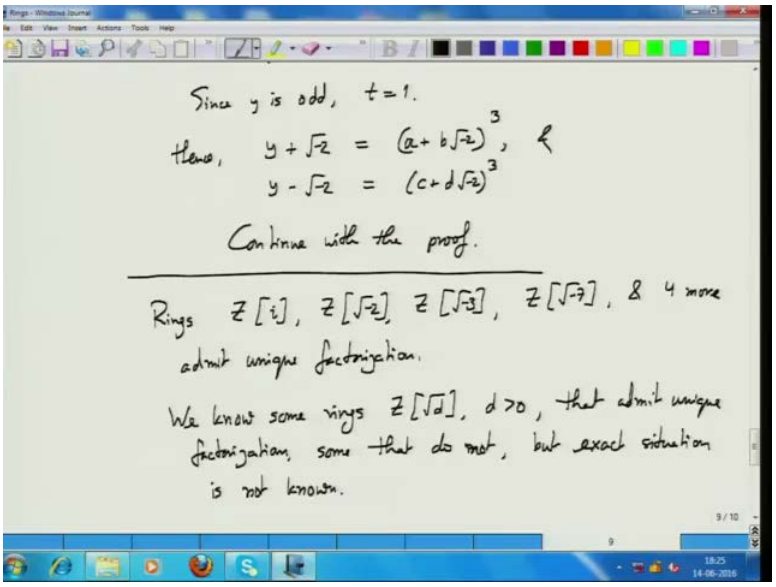
This can be verified very simply. You just multiply this out; compute the norm on both side and see that is as simple as that. It will turn out that, it is actually multiplicative, which is a very nice property particularly with respect to finding if a number is prime in this ring, because if now suppose that, a plus b square root 2 is not a prime; it factors as this. Then, norms of this equals product of norms of this; norm of this is a prime. So, since this is a prime over integers, these two are also integers. So, product of these two integers is a prime; that means one of these two integers must be equal to that prime and the other must be equal to 1; whichever it is.

Now, let us see suppose N norm of c plus d square root minus 2 is 1. By definition, norm is 2 d square is 1. Now, c, d is integers. And, this is everything is positive here. So, what would this mean? This means d is 0; d cannot be anything other than 0. And, c is plus

minus 1; which means that, the other factor - one of the two factors is simply plus minus 1; which shows that, this number a plus b square root of minus 2 is a prime in that larger ring.

So, this is the trick, which is very commonly used to establish if a number is prime in the larger rings (Refer Time: 27:49) Now, let us get back to our proof here t divides 2 y and t divides 2 square root of minus 2. So, what can t be? See t divides 2 square root of minus 2; and, 2 is square root of minus 2 whole squared minus of that; right?

(Refer Slide Time: 28:18)



Since t divides 2 square root of minus 2 and this happens to be equal to minus square root of minus 2 whole cube; which means that, t is basically some power of square root of minus 2; square root of minus 2 is square root of minus 2 whole square is square root of minus 2 whole cube. These are three possibilities for t; all right? And, t divided 2 y as well. So, that implies that, if t were equal to t, was 2; then of course, this is perfectly fine. t is a square root minus 2; that is also fine. It divides this t.

If t was square root of minus 2 whole cube; then, it would imply that, y itself is a multiple of square root of minus 2. So, y is an integer; so, y must be even. So, that is what we have to write basically. Either if t is 2 or square root of minus 2; then, it is fine; it is not, and then it is going to be now, y is going to be even. And then, you go back to this. And, I think I am just going to leave this proof at some point, but let us continue until we have time.

Now, t is a – let us say t is 2. There are three possibilities of t we identified: square roots of minus 2 – 2 or square root of minus 2 whole cube. Suppose t is 2; that divide y plus square root of minus 2 as well as this. So, what would that imply? So, that would mean that, should have gone right up here. Look at this equation.

And, let me ask the question can y be even? Suppose y is even; then, right-hand side is even; which means left-hand side must also be even; which means x is even. If x is even; then, x cube is a multiple of 4 actually multiple of 8, but it is certainly a multiple of 4. So, left-hand side is a multiple of 4; which means right-hand side must also be a multiple of 4. Since y is even, y square is a multiple of 4; then, 2 should also be a multiple of 4; which it is not. Therefore, y must be odd. And, since y is odd; now, let us come to this. We know now that y is odd. y is odd and t divides y plus square root of 2.

Look at the norms. So, y plus square root of 2 can be written as t times something else. Take the norms. What is the norm of y plus square root of 2? It is y square plus 2. So, that means y square plus 2 can be written as norm of t times something else. So, what is norm of t? t is only possibilities are for t are square root of minus 2 some power of square root minus 2.

In whatever power it is, the norm of t must be even; whereas, y square plus 2 is an odd number. So, that is also not possible. So, the only possibility for t therefore is that, t is 1. That is the only thing possible. And, the fact that, t is 1 implies going back that, these two: y plus square root of minus 2 and y minus square root of minus 2 are – do not have a common divisor. They do not have a common divisor, yet their product is a cube. What does it mean? It means that, individually they must be cubes; otherwise, it is not possible.

And now, we can carry this. So, this is already a – in fact, not just this, there is y minus square root of minus 2; that is also a cube. Both factors must be cubes (Refer Time: 34:46) And then, we can carry this argument further and derive from this the possible values of y; I am not going to give you the complete details, but this is the type of argument one employs when finding out integral solutions of equations. And, as you see, it very naturally lends to this larger rings. And, those larger rings actually help finding the solution like this property for example that we have just derived, we could not have found without going into these larger rings. I will just leave it at this point.

Now, let us work it out. It requires a little bit more work. In fact, we can quickly see that, c must be equal to a and d must be equal to minus b, because there is product of these 2 is x cube, which is x; and, x is an integer. So, that means, product of these two must be an integer. So, that is the only way it is an integer, which is this that, it is equal to a square plus – I mean while you multiply this and this, you must get a square plus 2 b square.

And, that will give us a (Refer Time: 36:28) It will also imply that, x is equal to a square plus 2 b square and y plus square root 2 is equal to this. So, we have now got expressions of both x and y in terms of a and b. And then, we can further argue; find out what values of a and b are possible. So, this example also illustrates the same point that, these rings are extremely useful in solving the problems that we encounter over integers. One of the key things, which I use without proving in this ring, admits unique factorization; otherwise, this whole argument breaks down. So, ring admitting unique factorization is very important.

So, the next question is which of these rings admit unique factorization? And, a lot of work has actually gone into that. And, we now know lot about it, but not the complete picture. So, let me give you what we know about this. Then, I think we have 7 and 4 more. There are 4 other numbers, which are larger and I do not recall them now. But, in the square root of a negative number, now, there are 8 rings, which admit unique factorization. All other square root of negative numbers do not admit unique factorization. In fact, last time we saw an example of z of square root of minus 5; that did not admit unique factorization.

What about the positive side? The positive side we know much less. We know some rings that admit unique factorization. Some that do not, but exact situation is not known. That exactly which of these rings that of square root of d; where, d is positive admits unique factorization, which one does not (Refer Time: 40:17) So, that is the state of current knowledge. And, that already shows that, there are number of interesting problems, which are still a challenge to mathematicians to address.

For this course, we will not get into those challenges. We will stay with what is very well-known. And so, coming back to these rings, we have seen examples of how and why these rings are useful. We also have seen why these rings having a unique

factorization, is important. And, we have also seen why some rings do have a unique factorization, some rings do not.

Now, the next step is to like I said, come up with a notion, which allows unique factorization in all these rings. And, that is where either it mentioned already is - that is given by the theory of ideals. And, that is something we will start in the next lecture.