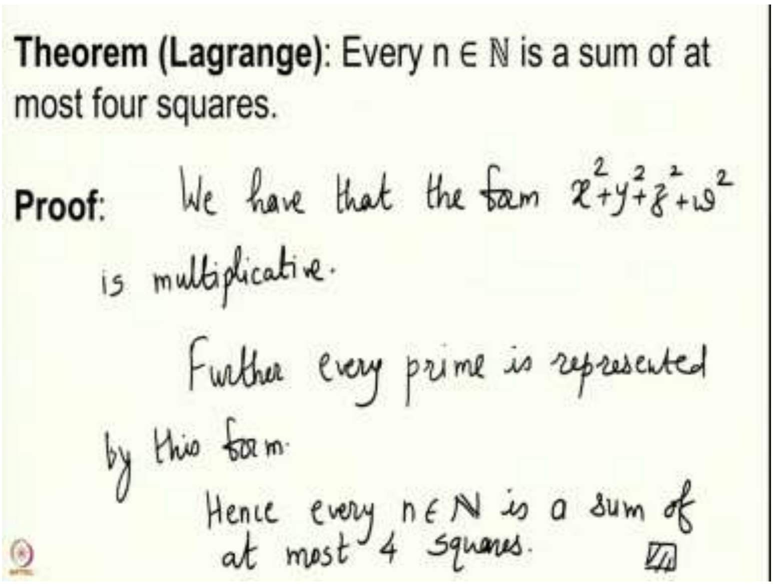
A Basic Course in Number Theory
Professor Shripad Garge
Department of Mathematics,
Indian Institute of Technology, Bombay
Lecture 48
Beyond sums of squares I

Welcome back, we have almost proved Lagrange's theorem which says that every natural number is a sum of at most four squares, we have the statement in front of you in this slide and now we are really going to prove this result.

(Refer Slide Time: 00:40)



So, we have that the form x square plus y square plus z square plus w square is multiplicative, let me recall it for you that we have given two proofs of this, we actually proved that x square plus y square plus x square plus w square is determinant of a special type of matrix and further if you take any two such matrices and take their product, then the product is again a matrix of the same form and therefore, the numbers which are represented by these two, these forms have the multiplicative identity property.

Because if you have x square plus y square plus z square plus w square into a square plus b square plus c square plus d square, you will write both of them as determinant of some matrices of that form, then you will take the product of the matrices and determinant of a product is product of the determinant. So, determinant of that product of those two matrices will give you the required form.

This is one way of proving which was a somewhat advanced prove, because we use the concept of a matrix its determinant and so on. But, in the last lecture, actually, I had written down the whole expression for you, if we had x square plus y square plus x square plus w square into x prime square plus y prime square plus z prime square plus w prime square then I actually wrote down the whole four numbers whose squares add up to the product of these two numbers. So, that's a second proof. So, therefore, we have that this form is multiplicative. Further, every prime whether it is 2 or not, is represented by this form and hence every natural number is a sum of at most four squares.

Remember also that our proof is somewhat constructive. For 2 we have constructed the numbers whose sum of squares give you 2 and similarly, for every prime the method that we have given will also tell you how to construct the expression for P as sum of four squares and once you have it for every prime, then for every integer you write it as product of primes and then for each prime factor, you have the expression, so you have the expression for n.

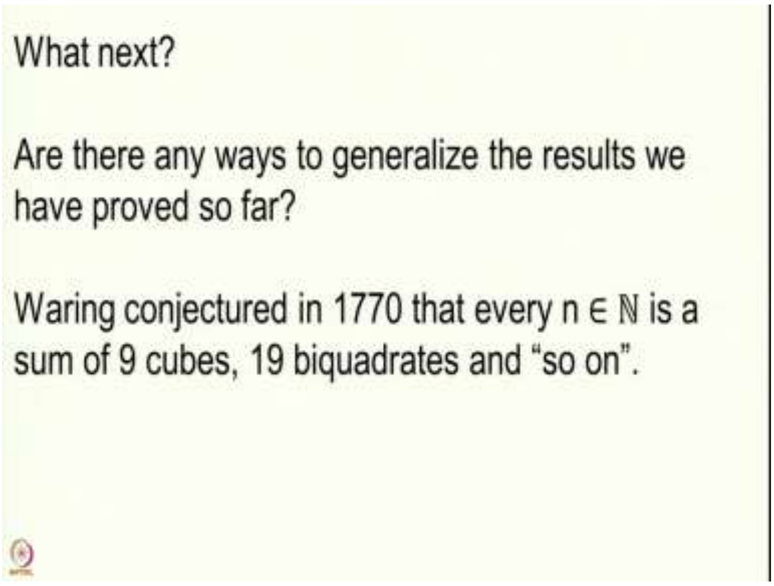
This is something which is very important, because if you wanted to write from the scratch, for an element n, for a number n as a sum of four squares, then the standard algorithms in computers may not work. For instance, there is this greedy algorithm, which would say that for every n, you take this largest square before that and then you have a smaller number you write that number as sum of squares and so on, but this thing may not always work.

For instance, if you happen to choose your number to be 32, 32 has the property that it is between two squares 25 and 36 and therefore, greedy algorithm will say that you write 32 as 25 plus 7 and once you have written it as 25 plus 7, 25 is a square 7 is a much smaller number, you should be able to write 7 as a sum of squares, but we have already observed that 7 needs four squares, you cannot write 7 as a sum of three squares.

So, in all for 32 you have used five squares 25 plus 4 plus 1 plus 1 plus 1 whereas, actually 32 is just 16 plus 16. So, writing the number as sum of squares can be done in an effective way if you use the prime factorization, the greedy algorithm will not always give you the solution. So, once having proved Lagrange's theorem, then next thing we can ask is what next?

So, after having proved Lagrange's theorem which is a very beautiful theorem proved by Lagrange in 1770, I must say remark here that another mathematician by the name Bachet had stated this as a possibility in 1621 and about 150 years later Lagrange proved this in 1770 and surely, any result of such nice property any such beautiful result must inspire more research in mathematics.

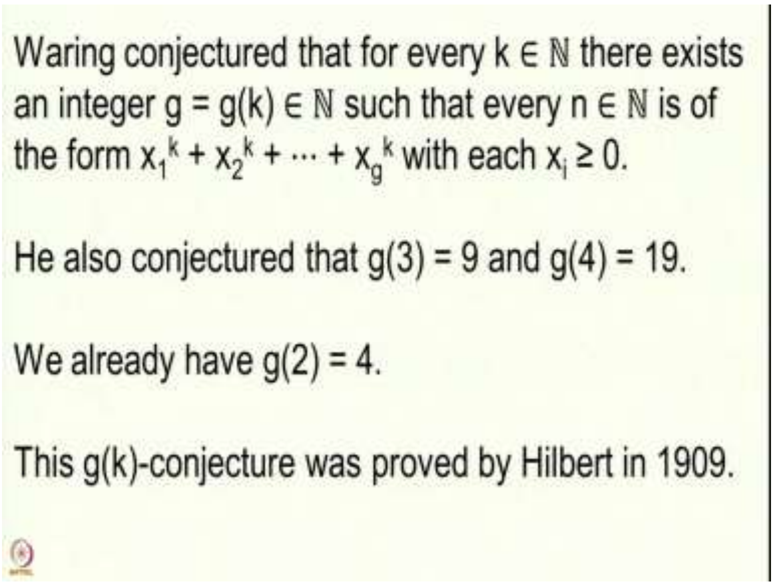
(Refer Slide Time: 06:19)



So, one would ask what next? Does it lead to anything in the further directions and there are indeed many directions. So, one can ask are there any ways to generalize the results that we have proved so far. Especially, Lagrange's theorem is there a way to generalize Lagrange's theorem to some other concept. So, Waring conjectured in 1770 immediately as Lagrange proved the result wearing said that wow this is good, if you require four squares to write every number it should be possible to write every number using only 9 cubes, 19 biquadrates, biquadrates means fourth powers and so on.

So, Waring said that every integer every positive integer is a sum of at most nine cubes, it is a sum up at most 19 fourth powers and so on. So, this so on is very peculiar, what is so on; what is the meaning of so on? So, let me explain the meaning of so on to you in this slide.

(Refer Slide Time: 07:38)



Waring made this explicit conjecture, he said that take any natural number k which is bigger than 1, then he proved that there is an integer g which is g of k, because it depends on the integer k. So, Waring conjectured that there is a g with the property that every natural number is a sum of at most g kth powers. I told you that you could actually have obtained every number as the sum of squares using the greedy algorithm which would tell you that every number is a sum of squares.

Ofcourse, we know that one is a square, so it is not difficult to prove that every integer is a sum of squares. It is not difficult to prove that every integer is a sum of kth powers because 1 is a kth power, but we do not want to write 20-20 as 1 plus 1 plus 1 plus 1, 20-20 times. We would like to have a finite number we would like to know that there is a number g depending on k such that my 20-20 is a sum of at most g many kth powers.

This was stated in 1770 by Waring and again about 130 years later, this was proved. Waring also conjectured that the number g3 is 9. So he said that you need 9 cubes. So, g3 is 9 has two statements in it. It means that for every n, 9 cubes are sufficient and moreover, that there is a number which requires 9 cubes.

For instance, Lagrange’s theorem said that every integer is a sum of 4 squares, at most 4 squares and we noted that 7 actually needs 4 squares. You cannot write every integer as sum of 3 squares because 7 is not a sum of 3 squares. So, you need to have four of them. The squares need to come four of them, you cannot just have three squares and they will give you they will sum to every natural number that is not true.

So g of 2 is 4 and Waring conjectured that g of 3 is 9 and further that g of 4 is 19. So, he noted that 9 and 19 are needed. But he also conjectured that these are enough, what is a conjecture? Conjecture is a statement which a mathematician really, really believes to be true, but he or she does not have time to prove it or perhaps he or she thinks that it is very difficult will perhaps require some techniques which are yet to be developed and so on.

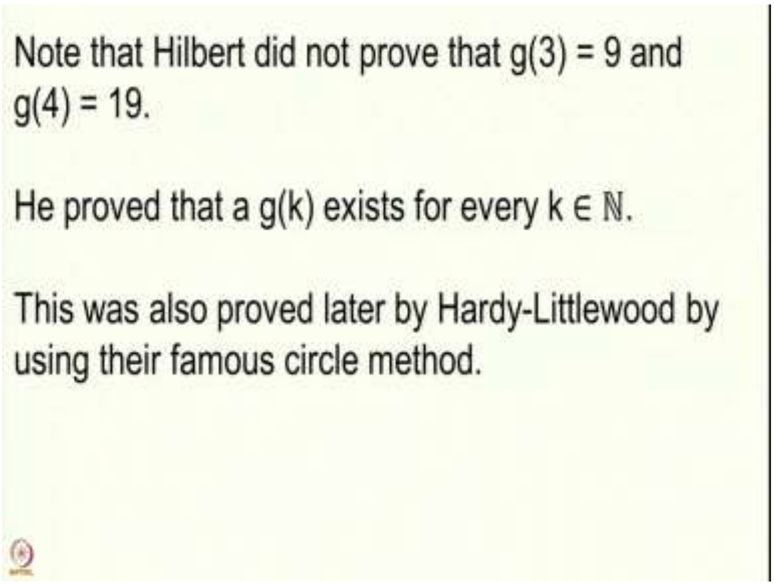
So, mathematician calls such a statement to be a conjecture and it is ofcourse, a non-trivial thing to call something as a conjecture, you are putting your reputation at stake, when you call something as a conjecture. But there are mathematicians who have feeling about math, various mathematical areas and so they really believe that some statement has to be true and so, they make conjectures.

So Waring conjecture this that for every k, there is a fixed number called that g depending on k such that every natural number is at most, g is a sum of kth powers, but at most g many of them and further he proved that the g of 3 is 9 and g of 4 is 19 and as I have remarked, we already have that g of 2 is 4 by a Lagrange.

So, this was stated in 1770 and about 140 years later, Hilbert proved it in the last century 20th century, Hilbert proved this statement and he proved the gk conjecture, which is that for every k, he proved that there is such a finite number g with the property that every natural number is a sum of at most g kth powers.

This is the statement that he proved, he did not prove that g 3 is 9, neither did he proved that g four is equal to 19. He proved that such a Gk exists for every k in n for every natural number n ofcourse bigger than 1, he proved that a G k exists and this is a very important theorem.

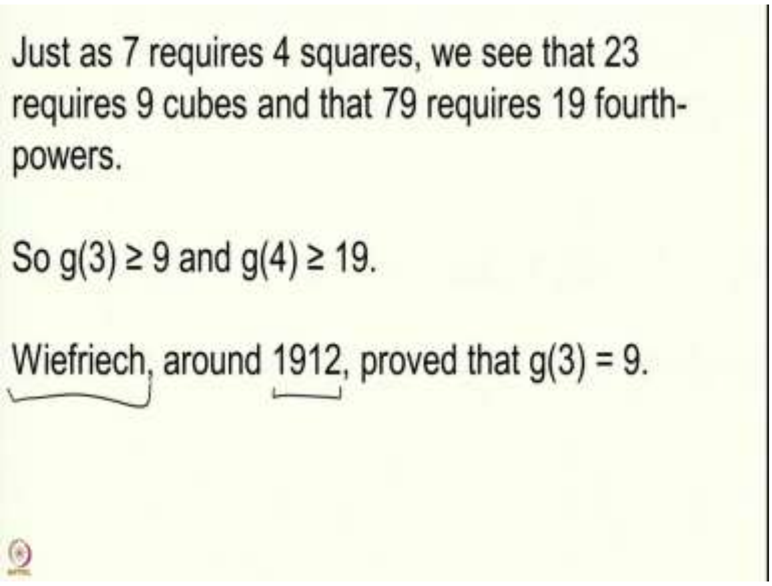
(Refer Slide Time: 12:48)



And therefore, there was another proof of this theorem given by these famous mathematicians Hardy and Littlewood and they proved this result using what is called the circle method. So, this is a method which was developed by Ramanujan essentially while dealing with the partition function and asymptotic of this function, but this was developed later by Hardy and Littlewood so it is called Hardy-Littlewood circle method and using this method as an application they gave a proof of Hilbert's theorem of Waring's conjecture.

So, they proved the way conjecture made by Waring once again, that such a gk exists. Once you prove that such a gk exists. Now, you would want to know what are the gk's for every k? What are the numbers g 3? What is g 4? What is g5? What is g 6? And so on, these are the things one would know want to know and mathematicians started working on this.

(Refer Slide Time: 13:58)



Further, let me just recall this for you that 7 does require 4 squares, you cannot write seven as a sum of 3 squares. Similarly, 23 will require 9 cubes. So, 23 is a number which does require 9 cubes, you cannot write it as a sum of 8 cubes and you also have that 79 will require 94 powers.

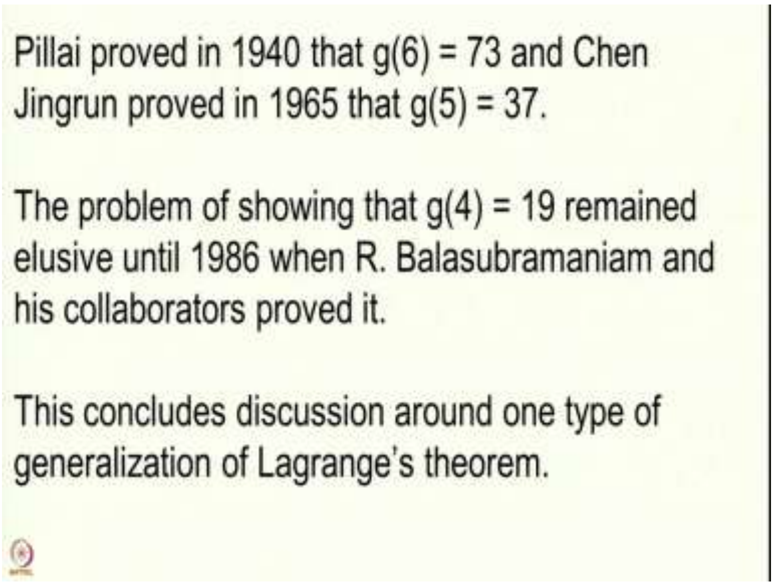
In fact, it is easy to give what number, so 9 and 19 these are the lower bounds for g 3 and g 4 and in fact, it is easy to get these lower bounds. What you have to notice is that there are some integers such that the only kth powers less than or equal to those integers is 1. So, if you start from 1 power k, which is 1 and go all the way up to 2 power k then, until you reach 2 power k, the only integer the only case power that you have is 1.

So, you will need to use 1 1 1 1 1 to write any number from 1 to 2 power k minus 1 as a sum of kth powers and if you then go further until 3 power k, then the only numbers at your disposal are 2 power k and 1 power k. So, what one notices is that between these numbers 1 to 3 power k minus 1, there is one particular number which is called 2 power k plus integral part of 3 by 2 power k minus 1.

So, this number is the one which requires only 2 power k which has only 2 power ks and 1 power ks to write it and there is only one effective way to write this number as a sum of kth powers that would give you a lower bound on gk. So, similar things can be done by us for the particular cases where k is 3 and k is 4 and then we see that 23 is the number which requires 9 cubes and 79 requires 19 biquadrates or 19 fourth powers.

So, these are the lower bounds we wanted to now prove the upper bounds, which is a more difficult thing we wanted to prove that every n can be written as sum of 9 cubes, every n can be written as sum of 19 biquadrates that is very difficult and there are other problems g5 g6 and so on. So, around 1912 I told you that Hilbert proved the existence of gk in 1909. From 1909 to 1912 in a series of papers Wiefriech proved that g 3 is 9.

(Refer Slide Time: 17:09)

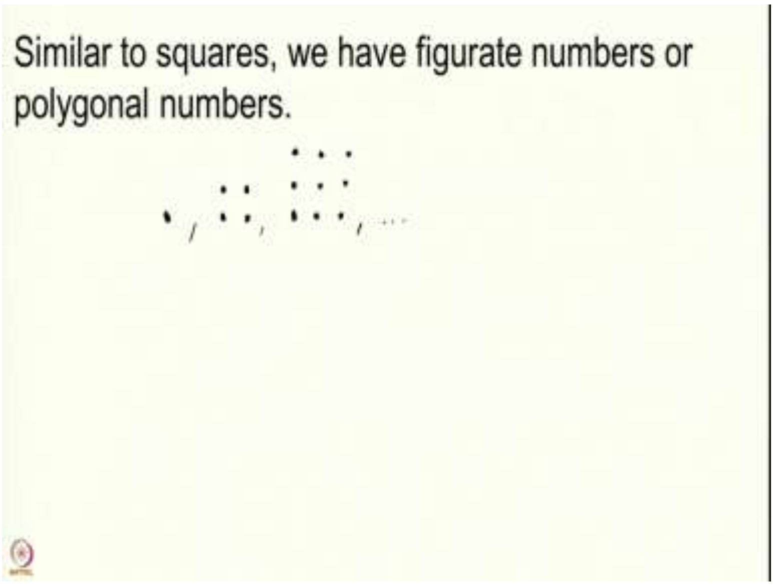


Then (Sarwad) S. S. Pillai, this is an Indian mathematician once again contemporary to Ramanujan. He proved that g 6 is 73. Remember, we are looking at g 3 and g 4, g 3 is 9 g 4 is 19. There are g 5 also in between, but Pillai proved that g 6 is 73 and in about 25 years this mathematician by name Jigrun he proved that g 5 is 37.

So, g 3 was computed, g 5 was computed and g 6 was computed, the problem of finding g 4 remained elusive until 1986. So almost till 20 more years this problem was not solved until 1986 when an Indian mathematician by the name R. Balasubramaniam and his collaborators solved it. So, this was a remarkable result and this result put India once again on the world map as far as number theory is concerned, it was such a remarkable result.

So, this is one way Waring's problem is one way by which we can generalize the theorem of Lagrange, which is that since you are writing every number as a sum of squares, you can ask how many cubes are needed, how many fourth powers are needed and so on and this is intimately related to many other things in mathematics like circle method and so on as, well as the techniques which are developed by R. Balasubramaniam and so on. So, this is one way the theorem can be generalised, there are another ways.

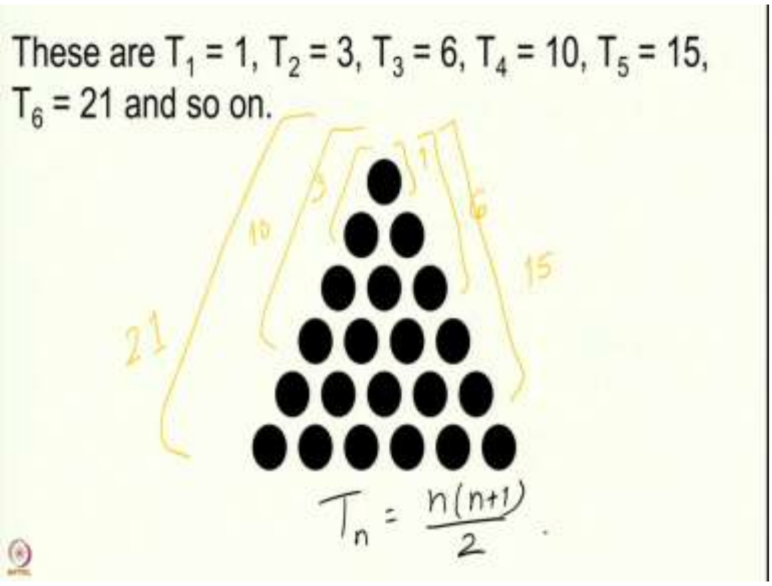
(Refer Slide Time: 19:04)



Similar to squares, we have figurate numbers or what are also known as polygonal numbers. So, squares are the numbers which can be written in a grid of squares. This is 1, 2 and then you have a grid of squares to write 9 and so on. So, we have actually a square number is called a square because you can put that number in a square grid where each side is represented by the square root of that number.

So, 16 is the number of elements which are put in a square grid consisting of 4 rows and 4 columns. So, square is a geometrical figure, we can look at other geometrical figures, let us start with triangles, we start with triangles.

(Refer Slide Time: 20:11)

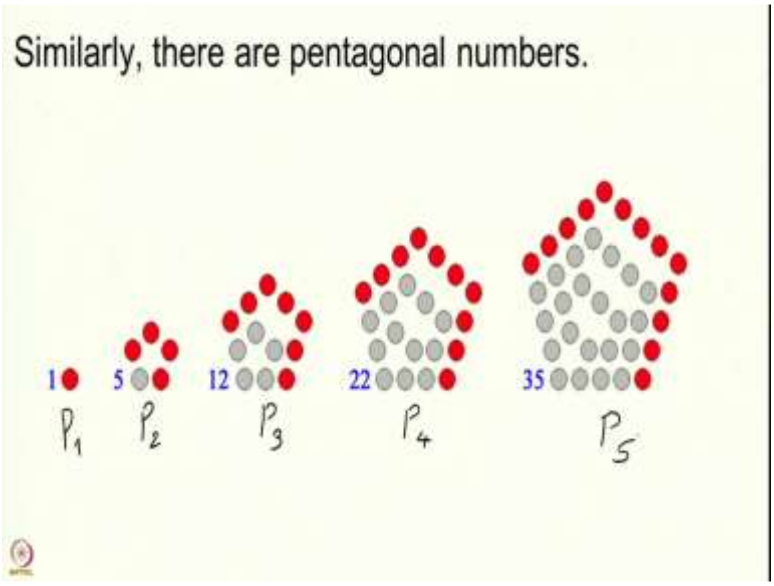


So, we have triangular numbers, these are T1 which is 1, T2 which is 3, T3 is 6, T4 is 10, T5 is 15, T6 is 21 and so on and let me give you a figure to represent the triangular numbers, here we see that this number is 1, if you just consider only 1 dot consisting of a single triangle of only the side is equal to 1.

If you consider this triangle, you have 3 elements. Here, there are 6 elements here there are 10 here there are 15 and finally, you have 21 elements. Many of you would have noticed that we are simply writing 1 dot followed by 2 dots followed by 3 dots and so on up to n dots, and then the nth triangular number is the sum of these numbers. So, you have n plus n minus 1 plus n minus 2 dot, dot, dot up to 1.

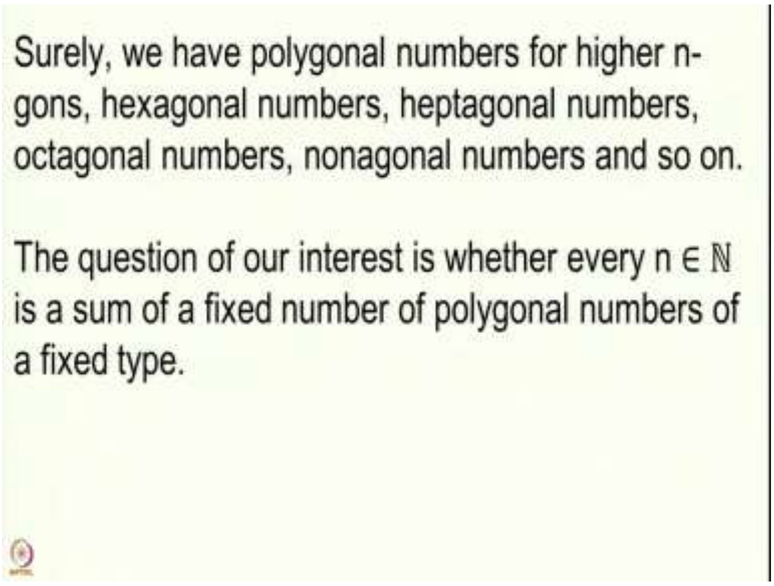
So, triangular numbers are easy to write down there is a formula for them, which is an n n plus 1 by 2, you can easily verify this formula for the triangular numbers that we have here on screen. So, these are the triangular numbers.

(Refer Slide Time: 21:48)



And now, there are also pentagonal numbers. So, you have the trivial pentagon consisting of only 1 dot and then you have the pentagon of side where each side has 2 edges, each edge has 2 vertices and so you have the number to be 5, this I have taken this picture from Wikipedia. So, we see that as you go on increasing the size, so here this is P1, P2 is 5, P3 is 12, P4 is 22, P5 is 35 and so on. So, every n for every n, we have a pentagonal number and there is a formula that one can write down for the pentagonal numbers.

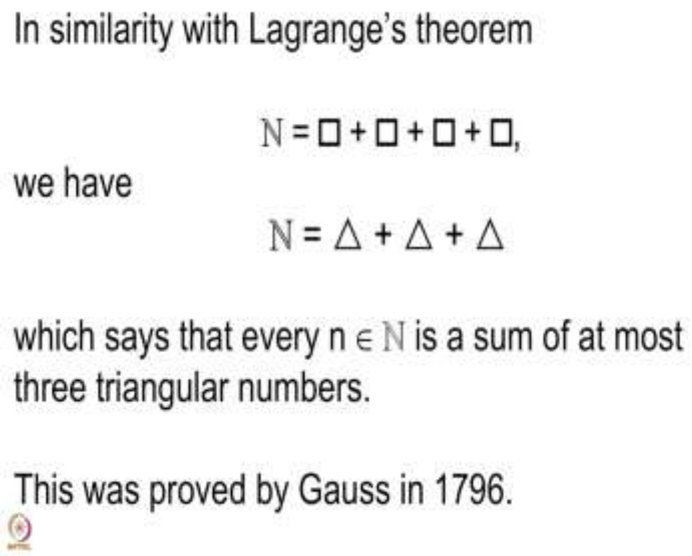
(Refer Slide Time: 22:48)



And ofcourse, we have polygonal numbers for higher n-gons, we have hexagonal numbers, these are for hexagons, we have heptagonal numbers for heptagons, octagonal numbers, nonagonal numbers, decagonal numbers and so on. So, what we would actually be interested in finding out whether every natural number is a sum of a fixed number of polygonal numbers of a fixed type.

Is it true that any given natural number n is a sum of a fixed numbers? So, suppose only g many have k polygonal numbers is there a g for gk just like we had the Waring's conjecture, is there a g equal to gk for every k such that every natural number is a sum of g kth polygonal numbers, this is the question that one would want to ask.

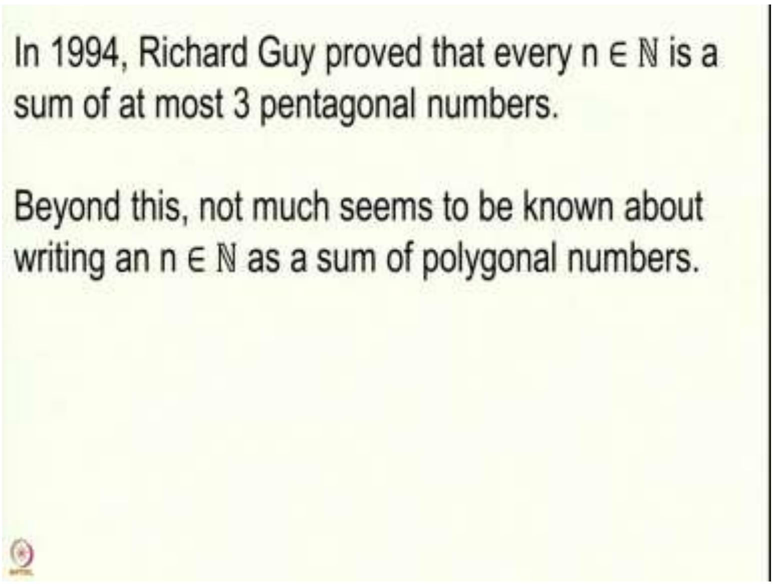
(Refer Slide Time: 23:55)



And our Lagrange's theorem says that n is sum of 4 squares. So, you have 4 squares, whose sum is every natural number. Similar to this you may have heard, this is a very famous remark by Gauss, who had written this as (())(24:11) equal to delta plus delta plus delta. So this means that every natural number n is a sum of at most 3 triangular numbers.

This was proved by Gauss. He had noted this in his diary and the date for that entry is in 1796. So, Gauss had noted this that (())(24:42) is delta plus delta plus delta you need at most 3 triangular numbers to write every natural number and we can ask what would happen for higher polygonal numbers.

(Refer Slide Time: 24:58)



So, Richard guy in 1994 proved that every natural number is a sum of at most 3 pentagonal numbers, but he generalized the earlier concept of a pentagonal number, using his slightly generalized concept, he could prove that every n is actually a sum of at most 3 pentagonal numbers. However, beyond this, not much seems to be known about this. So, this is the question of writing every natural number as a sum of polygonal numbers of a fixed type.

And so just like 4 squares, we had the polygonal numbers. Similarly, for cubes, now cube is the number of elements, which are represented in a 3-dimensional grid, just like a square was represented in a 2-dimensional grid. So, three cube is represented in a 3-dimensional grid. So, you can ask whether there are generalizations of polygonal numbers in the third dimension.

So, are there polyhedral numbers? Indeed, there are polyhedral numbers. For every dimension there are numbers and you can ask this question, whether every natural number is a sum of a fixed number of polyhedral numbers of a fixed type and nothing much seems to have been done on this ofcourse which means that it is not an easy thing to compute, but even then, I think there is quite a lot that can be done in this direction.

This concludes our discussion for the second type of generalization after Lagrange's theorem. First one was the Waring's problem where we generalize from squares to cubes, cubes to fourth powers and so on. Second was that we observed the squares represent some just certain geometrical figure and so we consider all geometrical figures. There is one more generalization and that is more interesting it refers to one of the well-known Indian origin mathematicians by name Manjul Bhargava. So, we will come to that in our next lecture. I will see you then, thank you very much.