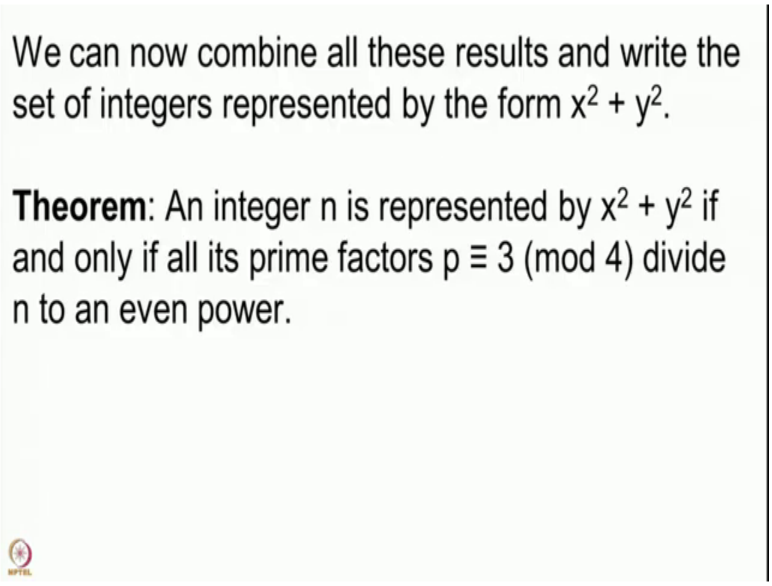
A Basic Course In Number Theory
Professor Shripad Garge
Department of Mathematics
Indian Institute of Technology, Bombay
Lecture - 46
Sums of squares - II

Welcome back, I hope you are all anticipating the result that we are going to describe, all integers which can be written as sums of two squares. And indeed, we are going to do that, let me recall the result that we have proved so far in that direction. We first of all proved that the form x square plus y square is multiplicative, which means that if I take 2 integers which are represented by the numbers, by the form x square plus y square then their product is again represented by the same form.

Further we proved that 2 is represented by the form x square plus y square, p congruent to 1 modulo 4 is represented by the form. So, product of all these integers 2 power alpha into p 1 power alpha 1, p 2 power alpha 2, so on up to pr power alpha r, where pi are congruent to 1 mod 4 will definitely be represented by x square plus y square. Moreover, we can multiply any such number by a square, a single square is always represented by x square plus y square.

And now, we tell that p congruent to 3 mod 4 if it divides x square plus y square then its square should divide x square plus y square. So, all these results are going to enable us to prove the following result. So, we can now combine all these results and write the set of integers represented by the form x square plus y square in the following result.

(Refer Slide Time: 1:53)

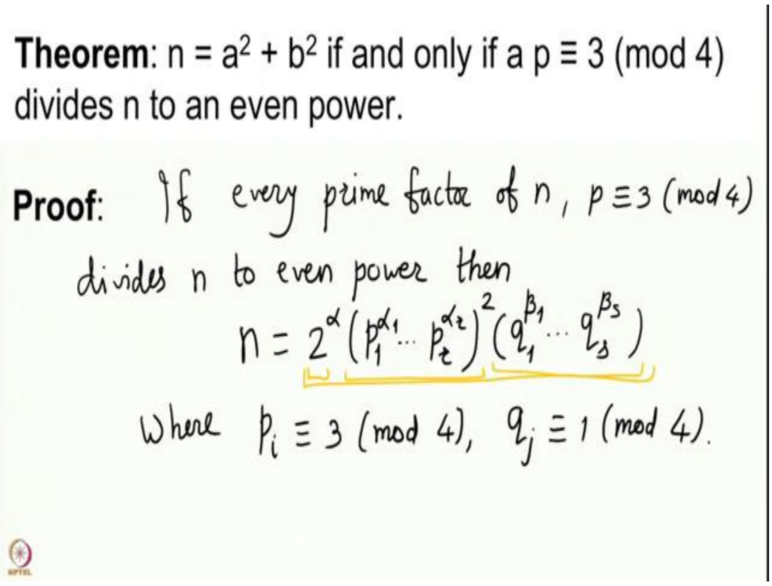


We can now combine all these results and write the set of integers represented by the form $x^2 + y^2$.

Theorem: An integer n is represented by $x^2 + y^2$ if and only if all its prime factors $p \equiv 3 \pmod 4$ divide n to an even power.

An integer n is represented by x square plus y square if and only if all its prime factors p congruent to 3 mod 4 divide n to an even power. The only condition is on the factors of n which are congruent to 3 mod 4, that these factors, these prime factors should come with an even power this is the only condition. Clearly there is no condition on the powers of 2 that may appear, there is no condition on the powers of the other set of primes, those which are congruent to 1 modulo 4 on them also we have no condition.

(Refer Slide Time: 2:37)



Theorem: n = $a^2 + b^2$ if and only if a $p \equiv 3 \pmod 4$ divides n to an even power.

Proof: If every prime factor of n, $p \equiv 3 \pmod 4$ divides n to even power then

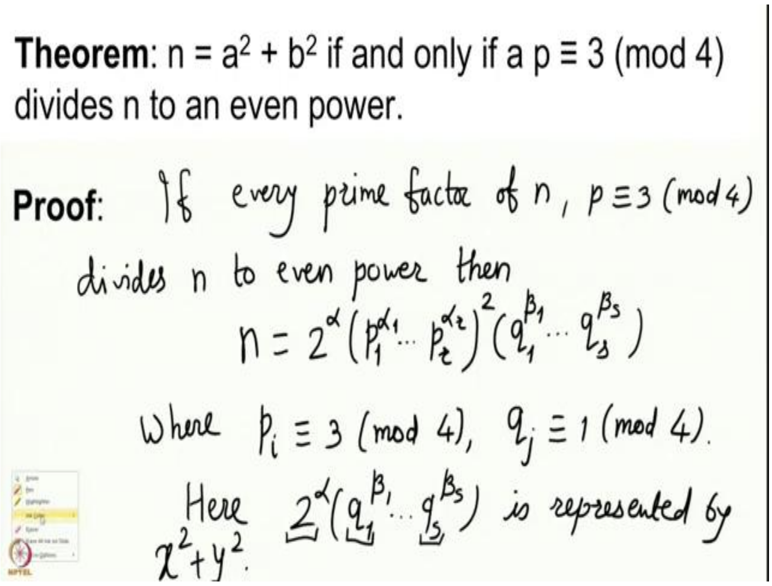
$$n = \underbrace{\underbrace{2^{\alpha}}\underbrace{(p_1^{\alpha_1}\cdots p_t^{\alpha_t})^2}\underbrace{(q_1^{\beta_1}\cdots q_s^{\beta_s})}}$$

where $p_i \equiv 3 \pmod 4$, $q_j \equiv 1 \pmod 4$.

So, let us go and prove this result, we first prove that the condition is sufficient. So, if every prime factor of n, p congruent to 3 mod 4 divides n to an even power then n is 2 power alpha p 1 power alpha 1 dot dot dot p r power alpha r square, q 1 power beta 1 dot dot dot q s power beta s where pi are congruent to 3 mod 4, qj's are congruent to 1 modulo 4.

We are starting with the decomposition of our n into all its prime factors. The prime factors may be 2, they may be 1 mod 4 or they may be 3 mod 4. The prime factors which are 3 mod 4 have to come we can even power, therefore we have the following description.

(Refer Slide Time: 4:45)



Theorem: $n = a^2 + b^2$ if and only if a $p \equiv 3 \pmod 4$ divides n to an even power.

Proof: If every prime factor of n, $p \equiv 3 \pmod 4$ divides n to even power then

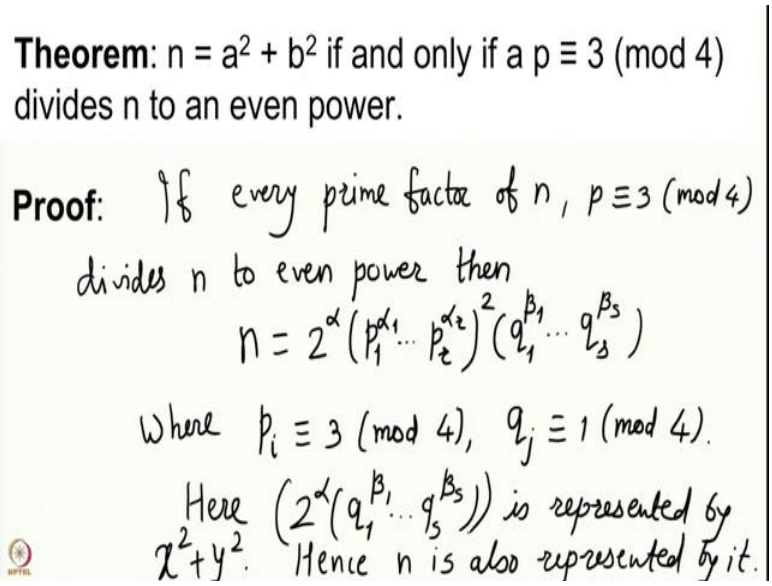
$$n = 2^{\alpha}(p_1^{\alpha_1} \cdots p_t^{\alpha_t})^2 (q_1^{\beta_1} \cdots q_s^{\beta_s})$$

where $p_i \equiv 3 \pmod 4$, $q_j \equiv 1 \pmod 4$.

Here $\underline{2}^{\alpha}(\underline{q_1}^{\beta_1} \cdots \underline{q_s}^{\beta_s})$ is represented by x^2+y^2.

Here 2 power alpha into q1 power beta 1 dot dot dot q s power beta s is represented by the form x square plus y square. Remember our form is multiplicative and each of these 2 q 1, so on up to q s, each of these is represented by the given form.

(Refer Slide Time: 5:15)



Theorem: $n = a^2 + b^2$ if and only if a $p \equiv 3 \pmod 4$ divides n to an even power.

Proof: If every prime factor of n, $p \equiv 3 \pmod 4$ divides n to even power then

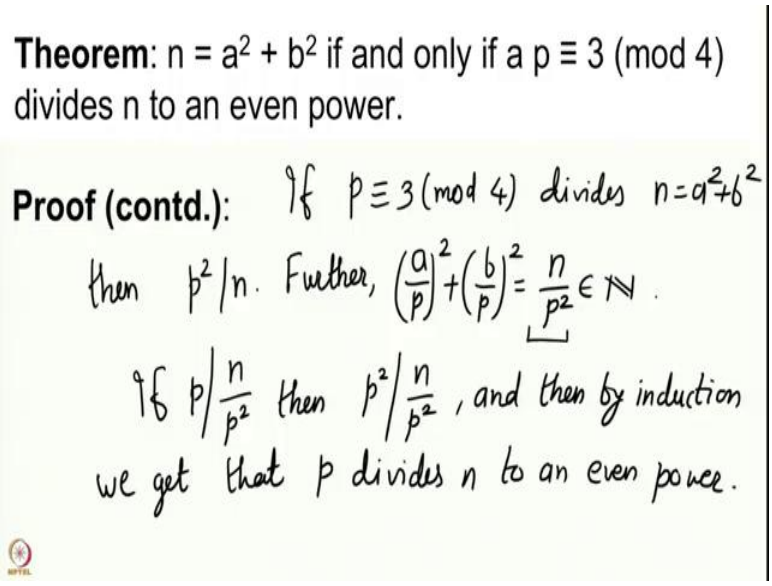
$$n = 2^{\alpha}(p_1^{\alpha_1} \cdots p_t^{\alpha_t})^2 (q_1^{\beta_1} \cdots q_s^{\beta_s})$$

where $p_i \equiv 3 \pmod 4$, $q_j \equiv 1 \pmod 4$.

Here $(2^{\alpha}(q_1^{\beta_1} \cdots q_s^{\beta_s}))$ is represented by x^2+y^2. Hence n is also represented by it.

So, their product in any way you take is going to be represented by the form. Hence n is also represented by, represented by it. So, because n is nothing but a square into this quantity, so n is also going to be represented by the form x square plus y square. So, we have proved that whenever p congruent to 3 mod 4 type of primes divide n to an even power, then n is always a sum of 2 squares. Now, we prove it in the other direction that when n is the sum of 2 squares, and p congruent to 3 mod 4 divides n it should divide it with an even power.

(Refer Slide Time: 6:20)



Theorem: $n = a^2 + b^2$ if and only if a $p \equiv 3 \pmod 4$ divides n to an even power.

Proof (contd.): If $p \equiv 3 \pmod 4$ divides $n = a^2+b^2$ then p^2 / n. Further, $\left(\frac{a}{p}\right)^2 + \left(\frac{b}{p}\right)^2 = \underbrace{\frac{n}{p^2}}_{} \in \mathbb{N}$.

If $p / \frac{n}{p^2}$ then $p^2 / \frac{n}{p^2}$, and then by induction we get that p divides n to an even power.

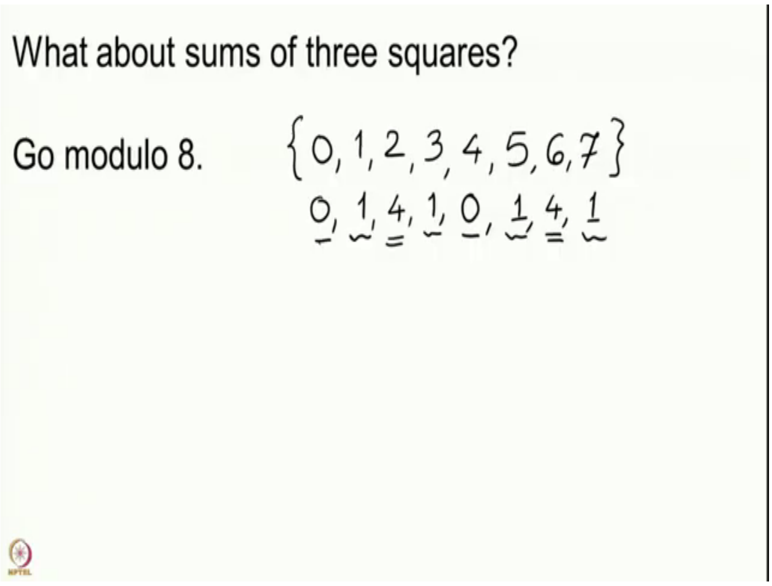
This is very easy, if p congruent to 3 mod 4 divides n which is sum of 2 squares, then we have proved that p square should divide n, this is something that we have already proved. And we have also proved that p should divide a and p should divide b. So, further we get that a by p square plus b by p squares divides, it gives you n by p square, n by p square is a natural number. So, now, we consider this number n by p square, if p again divides it, then we have if p divides n by p square, then its square should divide n by p square.

And then by induction we get that p divides n to an even power. We are reducing the numbers that are represented by a square plus b square in each step, if p divides n we have p square dividing n, so we will look at n by p square. If p divides this number then p square should divide this number. So, we will look at n by p power 4, these numbers are slowly reducing and ultimately p will stop dividing these numbers and therefore, we will have that p power 2 r divides n.

This is done for every prime p congruent to 3 mod 4. And therefore, we have that whenever n is a sum of 2 squares, then a prime p congruent to 3 mod 4 will divide n only with an even power. This gives a complete description as we have written in the last slide, we have that n equal to a square plus b square are of the form where 2 is allowed to come with any power primes which are congruent to 1 mod 4, they are allowed to come with any power, the primes which are congruent to 3 mod 4, they should come with an even power.

This is the only condition which will now determine the whole set of integers which are sums of 2 squares for us completely. This gives the complete answer of forms which are represented by the numbers which are represented by the form x square plus y square.

(Refer Slide Time: 9:26)



What about sums of three squares?

Go modulo 8. $\{0, 1, 2, 3, 4, 5, 6, 7\}$

$\underline{0}, \underset{\sim}{1}, \underline{\underline{4}}, \underline{1}, \underline{0}, \underset{\sim}{1}, \underline{\underline{4}}, \underset{\sim}{1}$

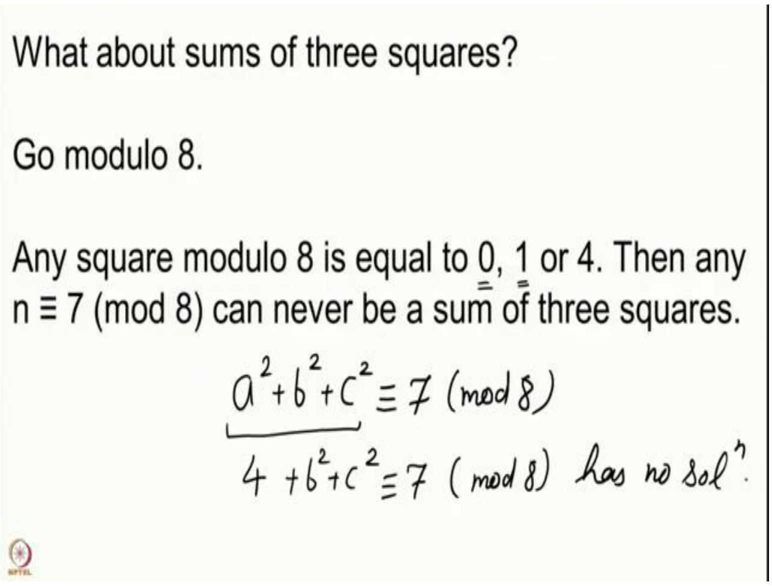
Once we are done with sum of 2 squares, the next natural question is, what about sums of 3 squares. So, when we were looking at sums of 2 squares, it was useful to study the numbers modulo 4, because modulo 4 we know that the numbers, the squares are congruent to 0 or 1 modulo 4 the numbers are 0, 1, 2 and 3. When we take the squares, 1 and 3 will give you the square to be 1, 2 and 0 will give you the square to be 0. So, you will have 0 comma 1, these are the only possible squares modulo 4.

And therefore, if you had a number which is 3 mod 4, that will never be a sum of 2 squares because you go modulo 4, now possibilities modulo 4 for squares are 0 and 1. So, sums of 2 squares will be 0 plus 1, 1 plus 1 or 1 plus 0 and of course 0 plus 0. So, all these will give you the possibilities to be 0 mod 4, 1 mod 4 or 2 mod 4, 3 mod 4 is not a possibility. And indeed, I leave this as an exercise to you, that any number which is 3 mod 4 has to have a prime factor, which is congruent to 3 mod 4 with an odd power.

And therefore clearly, such a number will not be a sum of 2 squares. But what about 3 squares? Something which is congruent to 3 mod 4 can be a sum of 3 squares. You may have 1 square plus 1 square plus 1 square, three odd numbers, their squares is congruent to 3 mod 4 when summed up. So, going modulo 4 is not enough, we go modulo 8. It is useful to go modulo 8 when we are looking at some of 3 squares, the squares modulo 8, now the numbers modulo 8, let us do this computation.

So, numbers modulo 8 are 0, 1, 2, 3, 4, 5, 6, and 7, let us compute their squares. 0 square is 0, 1 Square is 1, 2 square is 4, 3 square is 9 which is again 1, 4 squared is 16, which is 0, 5 square is 25 which is 1, 6 squared is 36 which is 4 modulo 8, and 7 square is 1. So, what it tells us that there are only these 3 numbers which are congruent to squares modulo 8.

(Refer Slide Time: 12:12)



What about sums of three squares?

Go modulo 8.

Any square modulo 8 is equal to $\underline{\underline{0}}$, $\underline{\underline{1}}$ or 4. Then any n ≡ 7 (mod 8) can never be a sum of three squares.

$$\underbrace{a^2+b^2+}c^2 \equiv 7 \ (\text{mod } 8)$$

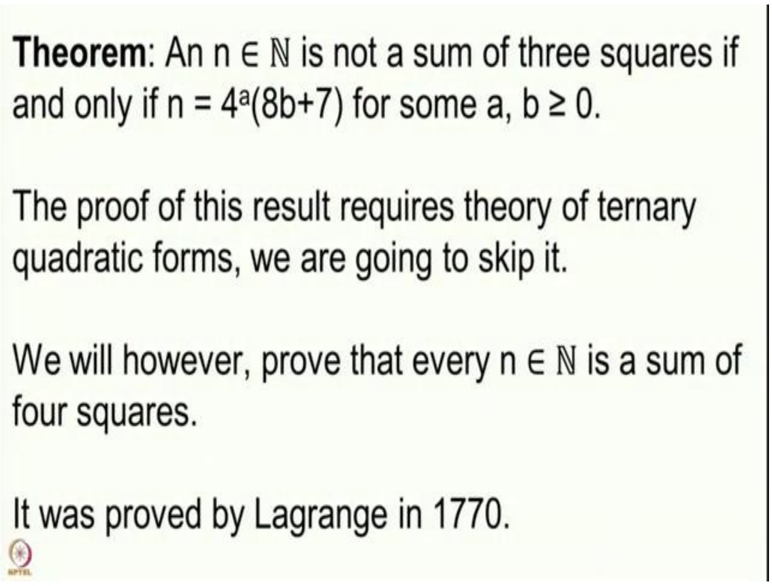
$$4 + b^2 + c^2 \equiv 7 \ (\text{mod } 8) \text{ has no sol}^n.$$

Any square modulo 8 is equivalent to equal to 0, 1 or 4. And therefore, any n which is 7 mod 8, can never be a sum of 3 squares. Anything else will appear as a sum of 3 squares, possibly, but 7 mod 8 will never come as a sum of 3 squares. Indeed, if you had 3 squares, if you had a square plus b square plus c square, congruent to 7 mod 8, clearly all these a, b, c, their squares cannot come alone from 0 and 1, because then you do not reach 7. If a square and b square and c square come only from 0, 1, you do not reach 7, you will maximum reach 3.

So, at least one of them has to be equal to 4. If you take one of them to be 4, now there are only 2 possibilities left. If you take 0 0, you are stuck at 4, if you take 1 0 or 0 1, you are stuck at 5. And if you take 1 1, you are stuck at 6, there is no way that you are going to get 7. So, 4 plus b square plus c square congruent to 7 mod 8 has no solution. So, if you have a number which is congruent to 7 mod 8, that is never going to be sum of 3 squares.

Just like we had that a number which is 3 mod 4 is not a sum of 2 squares. This is a result in one direction. It says that if your number is of this form, it is not a sum of 3 squares. But it would be interesting to have a precise result, just like we had for 2 squares, where we described the set of all integers, which are sums of 2 squares. We would like to know what are all integers, which can be written as sums of 3 squares, the more precise result is as follows.

(Refer Slide Time: 14:23)



Theorem: An $n \in \mathbb{N}$ is not a sum of three squares if and only if $n = 4^a(8b+7)$ for some $a, b \geq 0$.

The proof of this result requires theory of ternary quadratic forms, we are going to skip it.

We will however, prove that every $n \in \mathbb{N}$ is a sum of four squares.

It was proved by Lagrange in 1770.

That any natural number which is not a sum of three squares, such a number will have to be of the form 4 power a into 8 b plus 7 for some a, b non negative. So, that means if you assume this number to not have the factor 2, then such a number has to be congruent to 7 modulo 8. This is an if and only if statement, you start with an n a natural number, assume that it is not a sum of 3 squares, then it has to be of this form. Which means that if you take an integer which is not of this form, then it has to be a sum of 3 squares.

It would have been very interesting to see the proof of this result, but just like sum of 2 squares needed the theory of binary forms, we have used almost everything that we did for binary forms in proving this single theorem. In fact, one may say that we developed this whole theory because we wanted to prove this theorem.

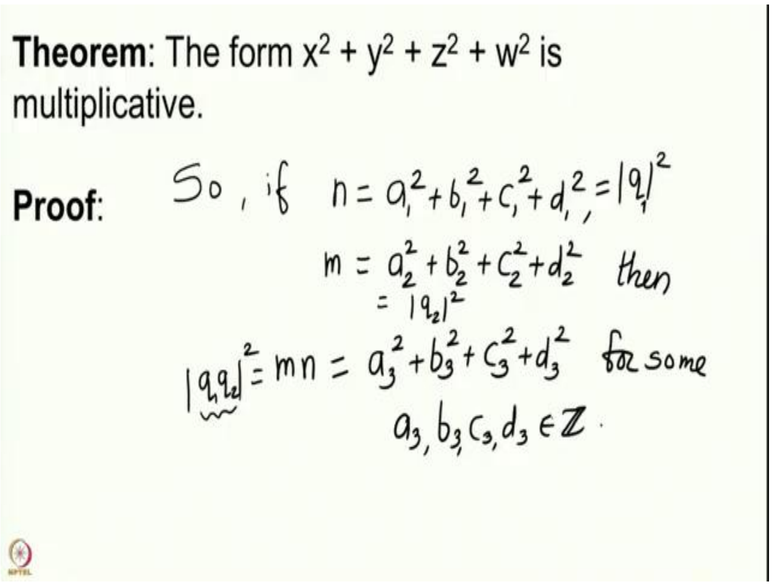
We use the equivalence, we use the theory of reduced forms, we use the theory that h d is 1 for d is equal to minus 4, we proved that, use that there are only, there is only one reduced form up to equivalence, we have used all these things when we studied the numbers which are represented by sums of 2 squares. So, similarly, this result, the proof of this result requires theory of ternary quadratic forms. Some people also call them tertiary quadratic forms.

Of course, we are going to skip it, because we do not have time to spend some more lectures on the theory of ternary quadratic forms, which is a very interesting theory by the way, and it would tell us this result, it would give us this result, giving us an explicit description of the numbers which are represented by sum of 3 squares. I should tell you that one important component in the representation for numbers of the form x square plus y square, was that the form x square plus y square was multiplicative.

That is no longer true, you may have 3 numbers, you may have 2 numbers, which are both sums of 3 squares and you may wonder whether the product is also a sum of 3 squares. That may follow from the description that we have here. But, otherwise, just by looking at the forms, we do not have that result. That means, it is not necessary that 2 numbers which are sums of 3 squares have the property that their product is also a sum of 3 squares. So, we are not going to study this.

On the other hand, we are going to study the theorem which is one step further, which is Lagrange's theorem. We will however, prove that every natural number is a sum of 4 squares. This interesting result was proved by Lagrange in 1770. It was stated earlier by other mathematicians but Lagrange seems to be the one who gave the proof for the first time. And so we know it as Lagrange's theorem, which says that every natural number n is a sum of 4 squares.

(Refer Slide Time: 18:27)



Theorem: The form $x^2 + y^2 + z^2 + w^2$ is multiplicative.

Proof: So, if $n = a_1^2+b_1^2+c_1^2+d_1^2 = |q_1|^2$

$m = a_2^2+b_2^2+c_2^2+d_2^2$ then

$= |q_2|^2$

$|\underset{\sim}{q_1q_2}|^2 = mn = a_3^2+b_3^2+c_3^2+d_3^2$ for some

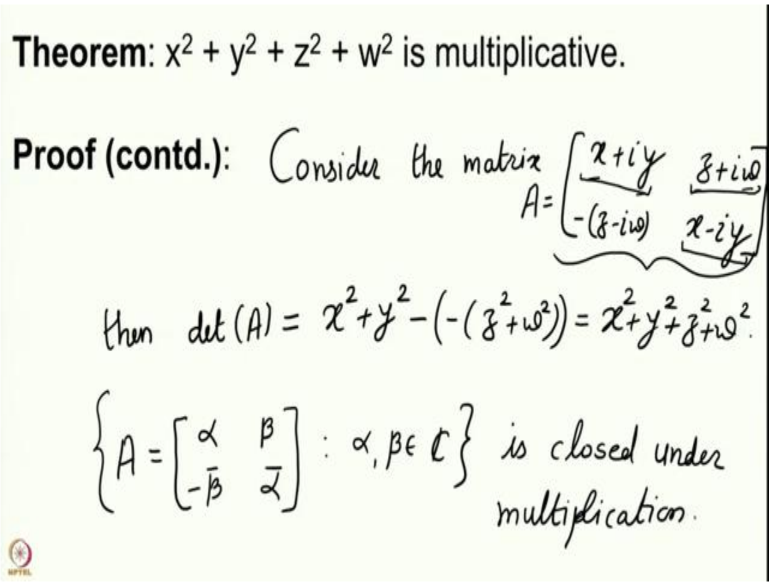
$a_3, b_3, c_3, d_3 \in \mathbb{Z}$.

And just as we proved that the form x square plus y square is multiplicative, while determining the set of integers which are sums of 2 squares, here also we have the property that this for x square plus y square plus z square plus w square is multiplicative. By this I mean that if we have, so if n is a 1 square plus b 1 square plus c 1 square plus d 1 square, m is a 2 square plus b 2 square plus c 2 square plus d 2 square then m n equal to a 3 square plus b 3 square plus c 3 square plus d 3 square for some a 3, b 3, c 3, d 3 in integers.

So, of course, we will be able to write this a 3, b 3, c 3, d 3 in terms of a 1, b 1, c 1, d 1 and a 2, b 2, c 2, d 2. We had used the theory of complex numbers, while studying the sums of 2 squares we saw that x square plus y square is actually the square of the modulus of the complex numbers, complex number x plus i y. Here we have a similar theory, there are numbers which are called quaternions and it turns out that x square plus y square plus z square plus w square is indeed square of a certain quaternion.

And the quaternions are closed under multiplication. So, what we would have is that this is square of one particular quaternion, let us call it q1 and this is square of some another quaternion called q2 and then it would follow that we have q1 q2 the product and their modulus square is m n, which is then further written as sum of 4 squares because the modulus square of a quaternion is a sum of 4 squares. But unless and until we know quaternions, you would, we would not be able to appreciate this. So, let us look at it from another angle.

(Refer Slide Time: 21:02)



Theorem: $x^2 + y^2 + z^2 + w^2$ is multiplicative.

Proof (contd.): Consider the matrix $A = \underbrace{\begin{bmatrix} \underline{x+iy} & \underline{z+iw} \\ -(z-iw) & \underline{x-iy} \end{bmatrix}}$

then $\det(A) = x^2+y^2-(-(z^2+w^2)) = x^2+y^2+z^2+w^2.$

$\left\{ A = \begin{bmatrix} \alpha & \beta \\ -\bar{\beta} & \bar{\alpha} \end{bmatrix} : \alpha, \beta \in \mathbb{C} \right\}$ is closed under multiplication.

Consider the matrix x plus i y and the second diagonal entry is x minus i y, so that when we take this product, we are going to get x square plus i x y minus i x y minus i square y square, which gives us x square plus y square and we have z plus w there so we will take z plus i w and minus of z minus i w. So, we have this matrix, let us call this matrix has A, then determinant of A is the diagonal entries product, which is x square plus y square minus the product in the anti diagonal entries, which is negative of z square plus w square.

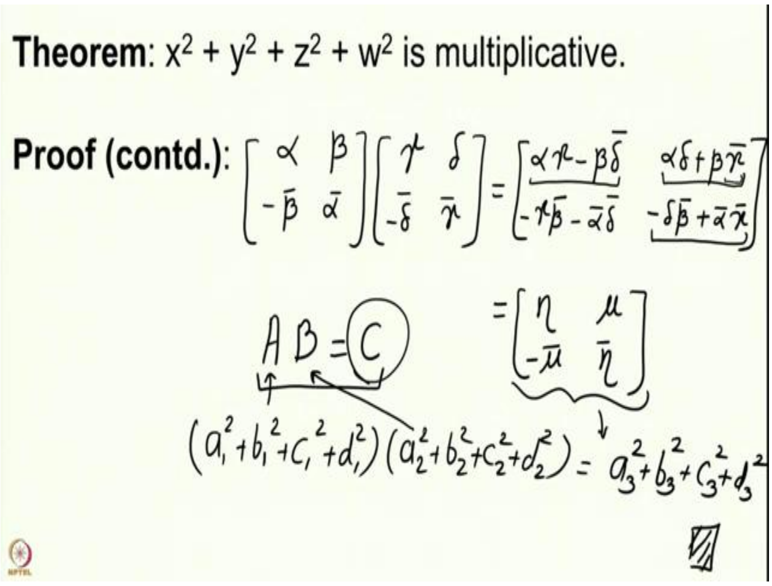
Which gives us x square plus y square plus z square plus w square. So, we have noticed that the matrix of this particular type has the property that its determinant is equal to sum of 4 squares, where those 4 entries are nothing but the real part, imaginary part, real part and imaginary part in the first row.

The only thing now that we have to understand is that whenever we take such a matrix, so let me write this matrix once again for you. So, I will call this matrix by alpha and alpha bar here, because if you have the complex number here to be alpha, this number is its complex conjugate. So, you have alpha alpha bar, here I have another complex number beta, then I have negative of beta beta bar.

So, our matrix is of the form alpha beta minus beta bar alpha bar, we are looking at the set of these matrices where alpha and beta come from complex numbers. We claim that this is closed under multiplication. So, we will prove that whenever I take any matrix A of this form and another matrix B of this form, suppose alpha beta minus beta bar alpha bar, gamma delta minus gamma, minus delta bar gamma bar, their product should again be of matrix of the same form.

If you have this property, then it will be clear that the a square plus b square plus c square plus d square, which is determinant of one such matrix into some another say x square plus y square plus z square plus w square, which is determinant of another such matrix will again be determinant of their product. Which are, which is again of the same form and so the determinant is going to be a sum of 4 squares once again. So, we have to just prove that when we take alpha beta minus beta bar alpha bar into gamma delta minus delta bar gamma bar, the product is again of the same form.

(Refer Slide Time: 24:55)



Theorem: $x^2 + y^2 + z^2 + w^2$ is multiplicative.

Proof (contd.): $\begin{bmatrix}\alpha & \beta \\ -\bar{\beta} & \bar{\alpha}\end{bmatrix}\begin{bmatrix}\gamma & \delta \\ -\bar{\delta} & \bar{\gamma}\end{bmatrix} = \begin{bmatrix}\underbrace{\alpha\gamma-\beta\bar{\delta}} & \underbrace{\alpha\delta+\beta\bar{\gamma}} \\ -\gamma\bar{\beta}-\bar{\alpha}\bar{\delta} & \underbrace{-\delta\bar{\beta}+\bar{\alpha}\bar{\gamma}}\end{bmatrix}$

$$AB = C \qquad = \underbrace{\begin{bmatrix}\eta & \mu \\ -\bar{\mu} & \bar{\eta}\end{bmatrix}}$$

$$(a_1^2+b_1^2+c_1^2+d_1^2)(a_2^2+b_2^2+c_2^2+d_2^2) = a_3^2+b_3^2+c_3^2+d_3^2$$

▨

We will simply compute this product of matrices, we get it to be alpha gamma minus beta delta bar, minus gamma beta bar minus alpha bar delta bar, alpha delta plus beta gamma bar and minus delta beta bar plus alpha bar gamma bar. So, we observe that this is again of the form eta, mu, minus mu bar, eta bar by observing that the complex conjugate of this number is this number. We had delta bar and here a delta is the only number which does not have a bar.

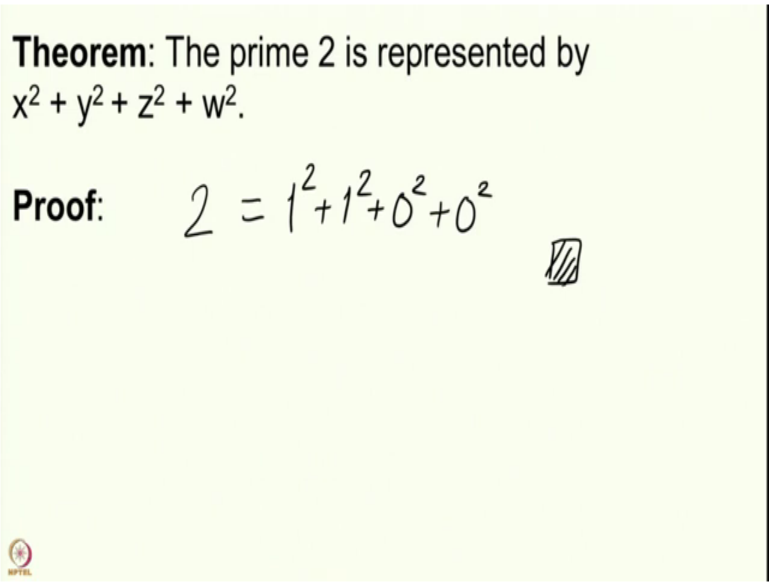
Here gamma is the only thing which has a bar and here gamma is the only thing which does not have a bar, we will take the bar which will give us alpha bar delta bar plus beta bar gamma and then we multiply by negative 1, because we want to get this as minus of mu bar, where mu is equal to this quantity.

So, we have therefore, proved that whenever I take any 2 such matrices, their product is again of the same form and this proves that if I have a 1 square plus b 1 square plus c 1 square plus d 1 square, I will write it as determinant of the matrix A, to that I multiply by the number a 2 square plus b 2 square plus c 2 square plus d 2 square, which I write as the determinant of the matrix B. I will then compute the matrix C, which is again of the same form which we have proved here, write its determinant here, which gives us a 3 square plus b 3 square plus c 3 square plus d 3 square.

So, the form x square plus y square plus z square plus w square is multiplicative. We have not developed the theory of the quaternary quadratic form so we are not going to use any theory but Lagrange's theorem is a beautiful theorem, it uses one method called the method of descent, our proof uses the method called method of descent. Where we will prove that once you start with a prime, which is represented by which, we want to be proved to be represented by this form, then a multiple of the prime is represented by this form.

And we will reduce that multiple slowly so that that multiple becomes 1. Once again, because the form is multiplicative, all you have to prove is that all primes are represented by this form, it is easy to see that 2 is represented by this form. The prime 2 is represented by this form, and that is a very simple proof.

(Refer Slide Time: 28:27)



Theorem: The prime 2 is represented by $x^2 + y^2 + z^2 + w^2$.

Proof: $2 = 1^2+1^2+0^2+0^2$ ▨

We have that 2 is 1 square plus 1 square plus 0 square plus 0 square. That is it. So, 2 is represented by this form. And now the only thing we need to do is to show that every odd prime is represented by this form, which is x square plus y square plus z square plus w square. We will prove this in the next lecture. So, see you until then. Thank you very much.