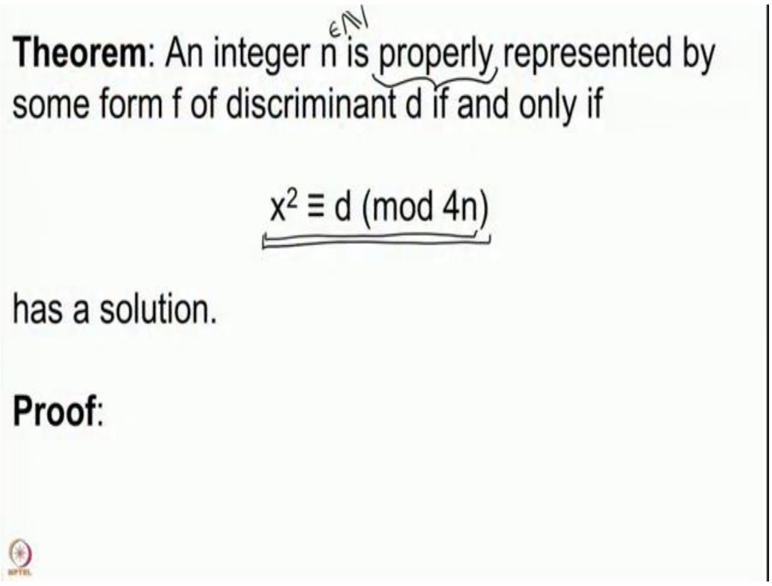
A Basic Course in Number Theory
Professor Shripad Garge
Department of Mathematics
Indian Institute of Technology, Bombay
Lecture-45
Sums of Squares - I

Welcome back, we have proved this theorem in the last lecture, it took the whole of our lecture, that if you have 2 reduced forms which are equivalent, then those 2 reduced forms have to be one and the same. and I also told you that while proving that we actually computed the set of all possible transformations, which will take one reduced form to itself depending on, of course, the conditions that you have on the coefficients a, b and c. We are now going towards proving the, we are now going towards determining the set of integers which is sums of two squares and for that, we will require a small criterion of a number represented by some form in the terms of the discriminant of the form.

(Refer Slide Time: 1:16)



Theorem: An integer $\overset{\in\mathbb{N}}{n}$ is $\underbrace{\text{properly}}$ represented by some form f of discriminant d if and only if

$$\underline{x^2 \equiv d \pmod{4n}}$$

has a solution.

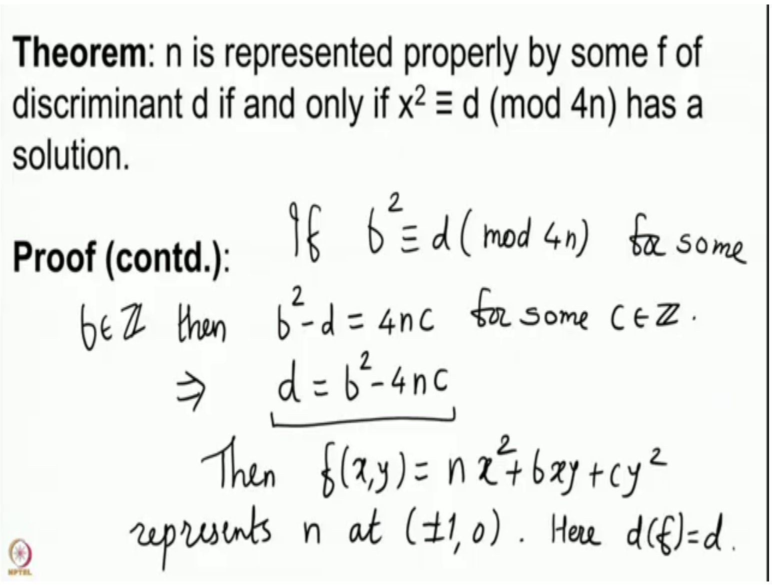
Proof:

So, the statement is here in front of you, that an integer n, so of course, this is in natural numbers, it is properly represented by some form f of discriminant d if and only if we have that x square congruent to d mod 4 n has a solution. Let us make sure that we understand the statement clearly. There is one condition which says that d is a square modulo 4 n, this is something that we understand quite well by now, we have understood the theory of congruences very well, we also know how to compute square modulo of given integer using chinese remainder theorem and then using the quadratic reciprocity laws.

So, we will understand this thing quite well when a certain d is a square modulo 4 n, this is equivalent to some form of discriminant d representing n properly. So, we have some pair of integers m comma n which are co prime or since you have taken n already, we will take some pair of integers p comma r which are co prime and f of p comma r is equal to n. This is the statement that we have, that this integer n is properly represented by some form.

We will begin with some form f of discriminant d representing n and we will show that x square congruent to d mod 4 n has a solution and in the other direction, we will assume that x square congruent to d mod 4 n has a solution and we will construct some form, the form is not fixed. The statement therefore is very liberal, we are allowed to choose any form of a given discriminant which represents the number n properly. So let us assume first of all that x square congruent to d mod 4 n has a solution.

(Refer Slide Time: 3:32)



Theorem: n is represented properly by some f of discriminant d if and only if $x^2 \equiv d \pmod{4n}$ has a solution.

Proof (contd.): If $b^2 \equiv d \pmod{4n}$ for some $b \in \mathbb{Z}$ then $b^2 - d = 4nc$ for some $c \in \mathbb{Z}$.

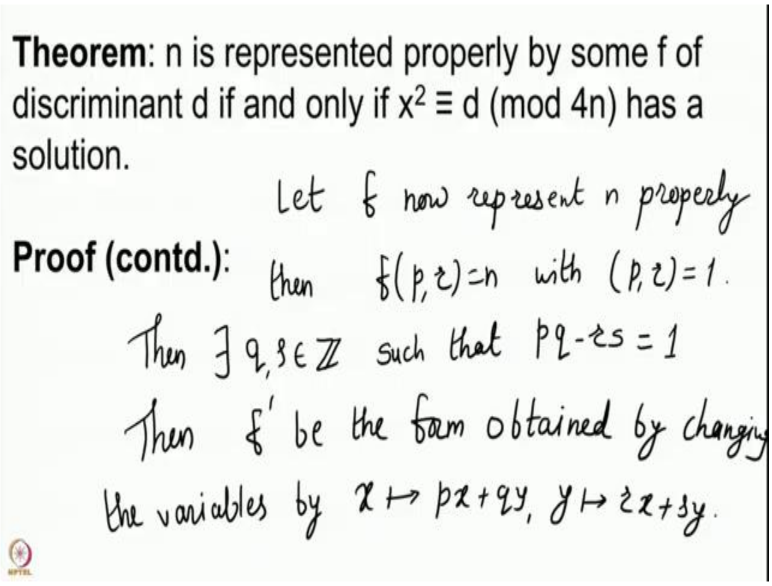
$$\Rightarrow \underbrace{d = b^2 - 4nc}$$

Then $f(x,y) = nx^2 + bxy + cy^2$ represents n at $(\pm 1, 0)$. Here $d(f) = d$.

If b square is congruent to d modulo 4 n for some b in integers, then b square minus d is 4 n c once again for some c in integers or this also implies that d is b square minus 4 n c, which reads something like our formula of the discriminant b square minus 4 ac, n is taking the role of a. Then the form where I will just put n instead of a, n x square plus b x y plus c y square represents n at plus minus 1 comma 0.

Of course, plus minus 1 comma 0 is a co prime pair of integers and therefore, we have that n is properly represented by some form f of discriminant equal to d. This is the form formula for the discriminant. So we have proved one way of this statement. We started with assuming that x square congruent to d mod 4 n has a solution and we have constructed a form which has discriminant d and it represents n properly. Now, we will prove the other direction which is where we will start with assuming that f represents n properly and we will need to prove that the discriminant f which is d has to be a square modulo 4 n.

(Refer Slide Time: 5:58)



Theorem: n is represented properly by some f of discriminant d if and only if $x^2 \equiv d$ (mod 4n) has a solution.

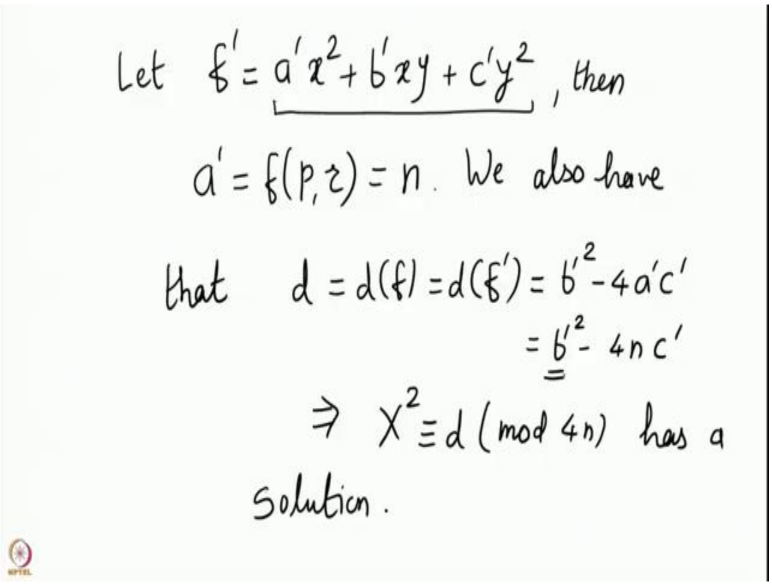
Proof (contd.): Let f now represent n properly then $f(p,r)=n$ with $(p,r)=1$.

Then $\exists\, q,s \in \mathbb{Z}$ such that $pq-rs=1$

Then f' be the form obtained by changing the variables by $x \mapsto px+qy$, $y \mapsto rx+sy$.

Let f now represent n properly then f p comma r is n, with the GCD of p and r is 1. but whenever we have GCD to be 1, remember that the GCD is a linear combination of your integer, your 2 integers with integer coefficients. So then there are these q and s coming from integers such that p q minus r s is equal to the GCD which is 1. Then f prime be the form obtained by changing the variables by x going to be x plus 2 y, y going to r x plus s y.

(Refer Slide Time: 7:53)



Let $f' = \underbrace{a'x^2+b'xy+c'y^2}$, then

$a' = f(p,r) = n$. We also have

that $d = d(f) = d(f') = b'^2 - 4a'c'$

$= \underline{\underline{b'}}^2 - 4nc'$

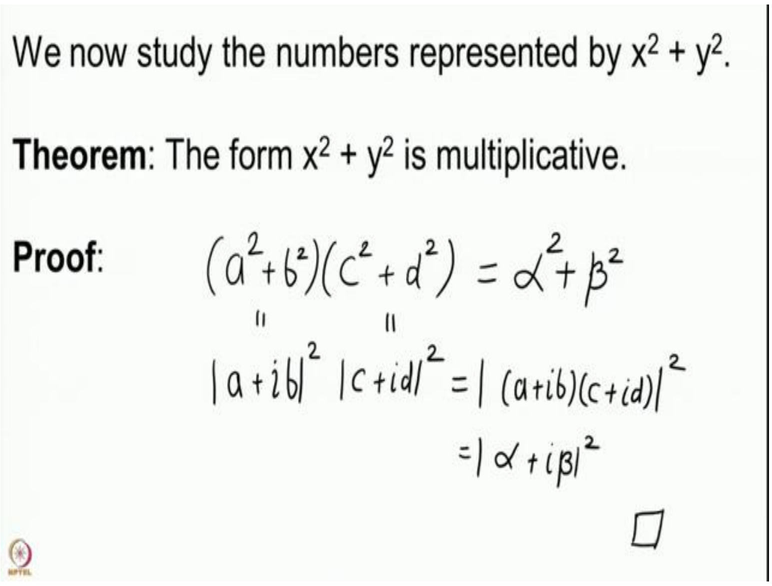
$\Rightarrow X^2 \equiv d \pmod{4n}$ has a solution.

So, let f prime be given by a prime x square plus b prime x y plus c prime y square, then we know that f a prime has to be the value of the original form taken at t comma r, but we had assumed this to be equal to n, we had assumed that f of p comma r is n. So, the new a prime is equal to n, we also have that the d remains the same, that means the discriminant of f and the discriminant of f prime are the same. And from this formula, we can compute the value for the discriminant of f prime which is b prime square minus 4 a prime c prime which is b prime square minus 4 n c prime.

And it shows that x square congruent to d modulo 4 n has a solution, our b prime is going to give you that solution. So, we prove that whenever our form f represents an integer n properly then modulo 4 n the discriminant of the form f has to be a square. This is a very important and very useful criterion. Note that here we do not have a control on the form f, but we can we have that the there is some form of discriminant d which is going to represent our integer n and by using the equivalence we can show that there is a reduced form of the given discriminant d which represents n.

Now, if you happen to have that h of d is 1, then there would be a unique form, unique reduced form of the given discriminant. And that would mean that any form of the discriminant d represents n properly. We will soon see an application of this result, but before that, we have to think about the form x square plus y square. We are going to study all integers represented by x square plus y square, but this form in particular x square plus y square has a very peculiar condition, it has a very nice property. And we are going to see this property in the next slide.

(Refer Slide Time: 10:48)



We now study the numbers represented by $x^2 + y^2$.

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

Proof:

$$\underset{\|}{(a^2+b^2)}\underset{\|}{(c^2+d^2)} = \alpha^2+\beta^2$$

$$|a+ib|^2\,|c+id|^2 = |(a+ib)(c+id)|^2$$

$$= |\alpha+i\beta|^2$$

□

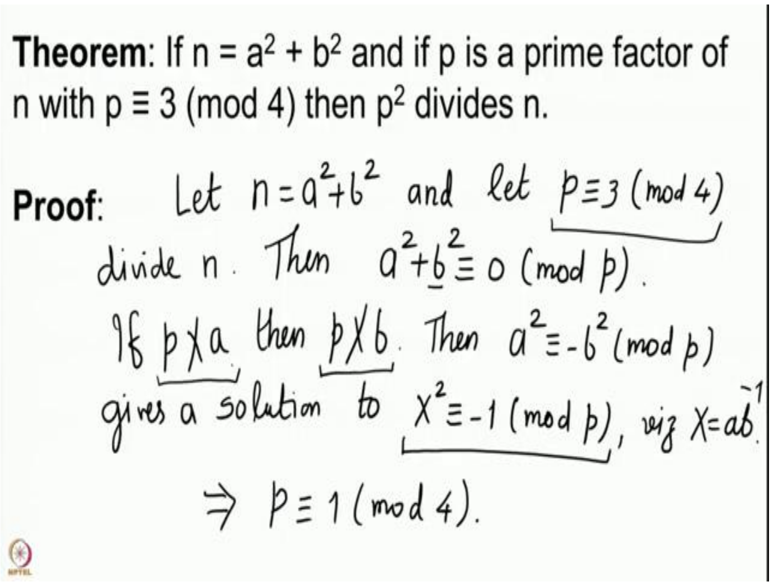
That the form x square plus y square is multiplicative. What do I mean by this? I mean that if I take a square plus b square and multiply to that by c square plus d square, then this is again a sum of 2 squares. This is a very remarkable property, it says that the form is multiplicative. That means, if I take 2 numbers which are represented by the form, take the product of those 2 numbers, that product is also represented by the form. This cannot be true for all forms, but for this form this is true.

And the proof is very simple, all you have to do is observe that this is nothing but a plus i b modulus square, a and b are integers, you construct the complex number a plus ib. I said in the beginning of the lectures course, that I am not going to use any advanced techniques, but I believe that the notion of complex numbers is a very basic concept and therefore, everyone would know that. I will assume this and we also have that c square plus d square is mod c plus id whole square.

And we know that if I take 2 complex numbers, take their modulus and take their product, this is same as taking the complex numbers taking their product and then taking the modulus. So this is nothing but a plus i b into c plus id mod square. And I will write this inside complex number as the complex number alpha plus i beta whole square and then we are done. So any 2 numbers which are represented by x square plus y square, their product is also represented by x square plus y square.

This is a very useful fact, because, if we could determine all the primes which are represented by x square plus y square then we are essentially done it will tell us a big set of numbers which are represented by x square plus y square.

(Refer Slide Time: 13:30)



Theorem: If $n = a^2 + b^2$ and if p is a prime factor of n with $p \equiv 3 \pmod 4$ then p^2 divides n.

Proof: Let $n = a^2+b^2$ and let $\underbrace{p \equiv 3 \pmod 4}$ divide n. Then $a^2+\underline{b}^2 \equiv 0 \pmod p$.

If $\underbrace{p \nmid a}$ then $\underbrace{p \nmid b}$. Then $a^2 \equiv -b^2 \pmod p$ gives a solution to $\underbrace{x^2 \equiv -1 \pmod p}$, viz $x = ab^{-1}$.

$\Rightarrow p \equiv 1 \pmod 4$.

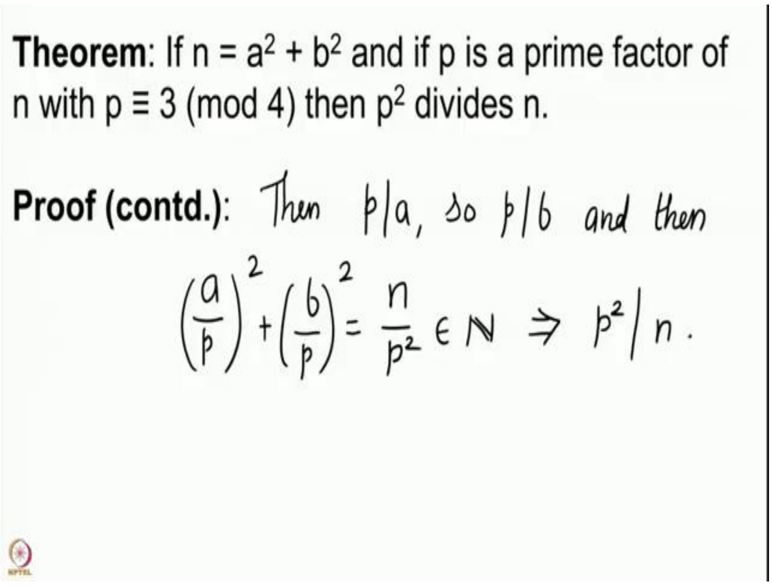
And before going to do that, we will also need this important result that if you have n which is a square plus b square and p is a prime factor of n with p congruent to 3 mod 4, then p square should divide n. In the introduction I had listed out some primes which are not sums of 2 squares and I had listed them out as 3, 7, 11 and so on, these are all the primes which are congruent to 3 mod 4. And if you should have so assuming this result we see that whenever n prime congruent to 3 mod 4 divides a sum of 2 squares, then the square of that number should divide.

It would then follow that such a prime p congruent or 3 mod 4 cannot be a sum of 2 squares. Let us go on and try to prove this result. So let n be a square plus b square and let be congruent to 3 mod 4 divide n, then a square plus b square is congruent to 0 modulo p, because p divides n, p divides a square plus b square. So a squared plus b squared is 0 mod p. If p does not divide a, then p does not divide b.

That is quite clear because if p divides b, then a square plus b square is 0 mod p, therefore b square is 0 mod p would tell you that a square is 0 mod p and therefore p will have to divide a. So whenever p does not divide any of the a's a and b it will divide none of them, then a square congruent to minus b square mod p gives a solution to x square congruent to minus 1 mod p. This is because, since b is not divisible by p you can simply cancel out b square and write this, namely x equal to a b inverse, the b inverse being computed modulo p.

So we have that x square congruent to minus 1 mod p has a solution, but this would imply that p is then congruent to 1 modulo 4, we have completed precisely when minus 1 is a square modulo p, it would then imply that p is congruent to 1 modulo 4 which is contradiction, because we have started with p congruent to 3 mod 4. So this contradiction says that something that we have assumed on the way has to be false. And the thing that we have assumed is this, that p does not divide a. This was the assumption that we started with, it then said that p does not divide b and then it gave us a non trivial, a solution to x square congruent to minus 1 mod p.

(Refer Slide Time: 17:26)



Theorem: If n = $a^2 + b^2$ and if p is a prime factor of n with $p \equiv 3 \pmod 4$ then p^2 divides n.

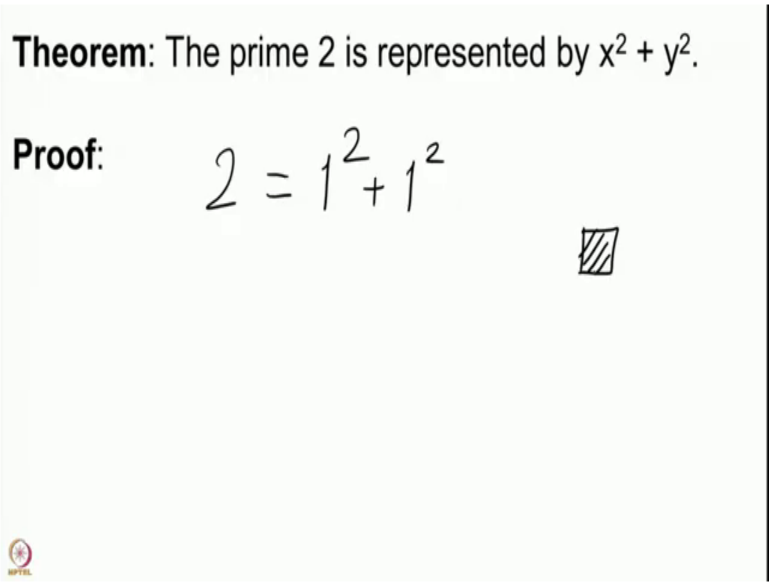
Proof (contd.): Then $p|a$, so $p|b$ and then

$$\left(\frac{a}{p}\right)^2 + \left(\frac{b}{p}\right)^2 = \frac{n}{p^2} \in \mathbb{N} \Rightarrow p^2 | n.$$

So, this assumption has to be false, which would mean that p divides a so p divides b and then we have a by p which is an integer its square plus b by p square is n by p square, this is an integer and clearly a natural number which implies that p square divides n. We had that a square plus b square is n and we proved that if p divides n then p should divide a and p should divide b. So a by p is an integer, a by p square plus b by p square is a square plus b square upon p square, but a square plus b square is n.

So, you get that n upon p square is an integer has to be a natural number, then p square divides n. So what we have proved is that whenever we had a prime p congruent to 3 mod 4 dividing a sum of 2 squares, then square of that prime should divide the integer n.

(Refer Slide Time: 18:59)

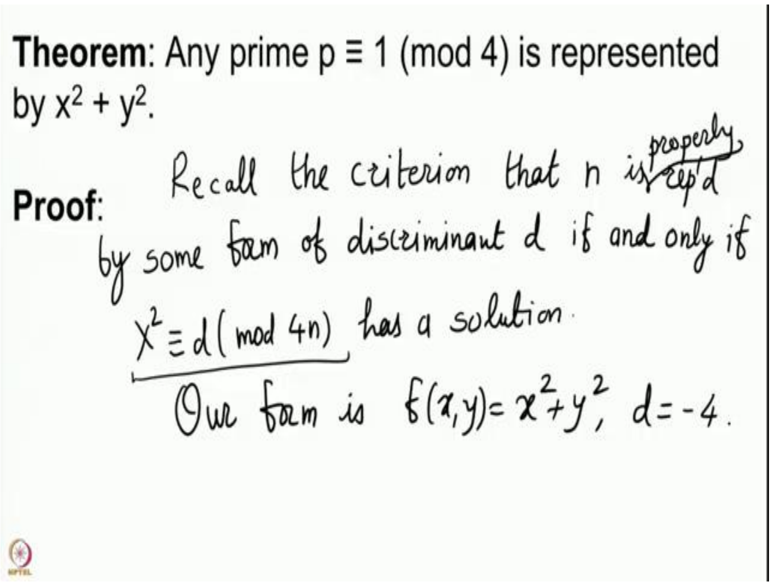


Theorem: The prime 2 is represented by $x^2 + y^2$.

Proof: $2 = 1^2 + 1^2$ ▨

After that we have one very small cute result, which is that the prime 2 is represented by x square plus y square. I believe that all of you can prove this, we have that 2 is nothing but 1 square plus 1 square. So we have dealt with p congruent to 3 modulo 4, we have dealt with the oddest of the primes, which is the prime 2, now the only class of the primes which remains is the prime is the set of primes p congruent to 1 modulo 4. We will prove that every such prime is a sum of 2 squares, every such prime is represented by x square plus y square.

(Refer Slide Time: 19:47)



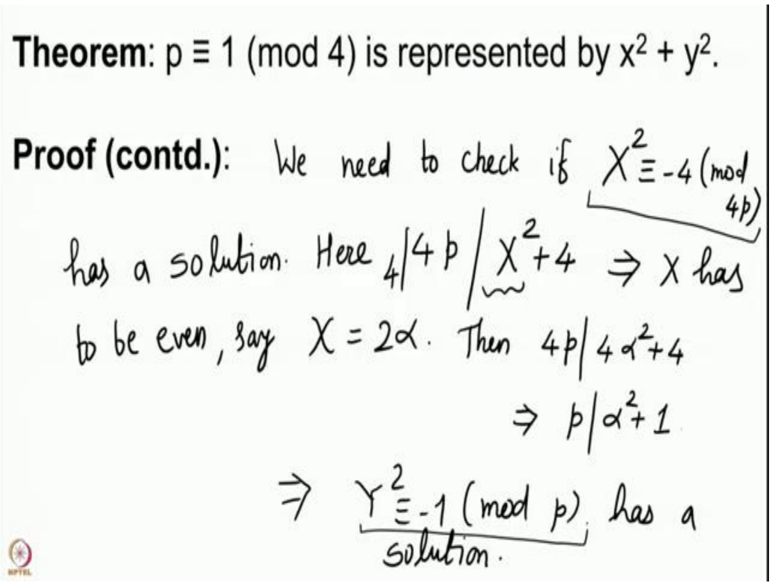
Theorem: Any prime $p \equiv 1 \pmod 4$ is represented by $x^2 + y^2$.

Proof: Recall the criterion that n is properly rep'd by some form of discriminant d if and only if $\underline{x^2 \equiv d \pmod{4n}}$ has a solution.

Our form is $f(x,y) = x^2 + y^2$, $d = -4$.

This is our next result, any prime p congruent to 1 modulo 4 is represented by x square plus y square. Recall the criterion which we did in the beginning of this lecture that n is represented by some form of discriminant b if and only if here we have the criterion for proper representation x square congruent to d mod 4 n has a solution. We are looking at the form x square plus y square, our form is and its discriminant if you remember is minus of 4. Its discriminant if you remember is minus 4. So, we want to see where we have this congruence, where n is now our prime p congruent to 1 modulo 4.

(Refer Slide Time: 21:41)



Theorem: $p \equiv 1 \pmod 4$ is represented by $x^2 + y^2$.

Proof (contd.): We need to check if $\underline{X^2 \equiv -4 \pmod{4p}}$ has a solution. Here $4 | 4p \,|\, X^2+4 \Rightarrow X$ has to be even, say $X = 2\alpha$. Then $4p | 4\alpha^2+4$

$\Rightarrow p | \alpha^2+1$

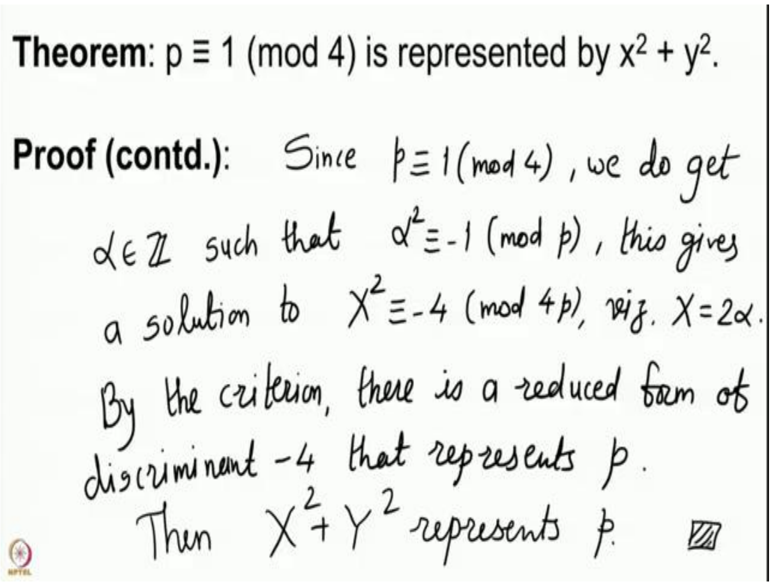
$\Rightarrow \underline{Y^2 \equiv -1 \pmod p}$ has a solution.

We need to check if x square congruent to minus 4 mod 4 p has a solution. Observe that 4 p, so then here 4 p must divide the solution x square plus 4, which implies that x has to be even, say x equal to 2 alpha. Any solution, if there is a solution, we will actually we are actually going towards constructing the solution. So we have to see what properties the possible solution should have and that will help us constructing the solution. So we observe that such an x has to be twice of an integer because 4 divides the number 4 p which divides x square plus 4 and therefore 4 divides x square.

If 4 divides a square then by unique factorization of integers, the fundamental theorem of arithmetic which gives unit factorization into prime of any integer will tell you that x also has to be an even integer. So then you have the solution to be 4 alpha and then 4 p reads for alpha square plus 4 for p divides for alpha square plus 4, which implies that p divides alpha square plus 1. Now, I hope you see the thing that we are coming to, which implies that y square congruent to minus 1 mod p has a solution.

We started with minus 4 being a square mod 4 p, and we have reached minus 1 being a square modulo p. Our p is congruent to 1 modulo 4. So, we do have such a solution, we do have that minus 1 is a square modulo p.

(Refer Slide Time: 24:18)



Theorem: $p \equiv 1 \pmod{4}$ is represented by $x^2 + y^2$.

Proof (contd.): Since $p \equiv 1 \pmod{4}$, we do get $\alpha \in \mathbb{Z}$ such that $\alpha^2 \equiv -1 \pmod{p}$, this gives a solution to $X^2 \equiv -4 \pmod{4p}$, viz. $X = 2\alpha$. By the criterion, there is a reduced form of discriminant -4 that represents p.

Then $X^2 + Y^2$ represents p. ▨

And once we have this solution, since p is congruent to 1 mod 4, we do get alpha integers such that alpha square is congruent to minus 1 mod p. This gives a solution to x square congruent to minus 4 mod for p, namely x equal to 2 alpha. So, by the criterion, there is a reduced form of discriminant minus 4 that represents p, it represents p properly, that certainly it represents p. And I would now like to recall this to you that we have computed h of minus 4, h of d for any integer d was the number of inequivalent reduced forms of discriminant d, which we also proved to be the number of reduced forms of discriminant d.

We proved that h of minus 4 was 1, there is only one form which is reduced and is of discriminant minus 4 and that form is nothing else but x square plus y square. Here we have proved that there is a reduced form of discriminant minus 1 which represents p that implies that x square plus y square represents our integer p, our prime number p.

So, let me just recall this to you once again that any p congruent to 1 mod 4 is represented by x square plus y square 2 is represented by x square plus y square p congruent to 3 mod 4 is not represented by x square plus y square, but the square of these numbers should divide the integer x square plus y square whenever p divides it. And using this in the next lecture, we are going to determine the set of all integers which can be written as sums of two squares. It is a very interesting thing to see. I will see you then thank you very much.