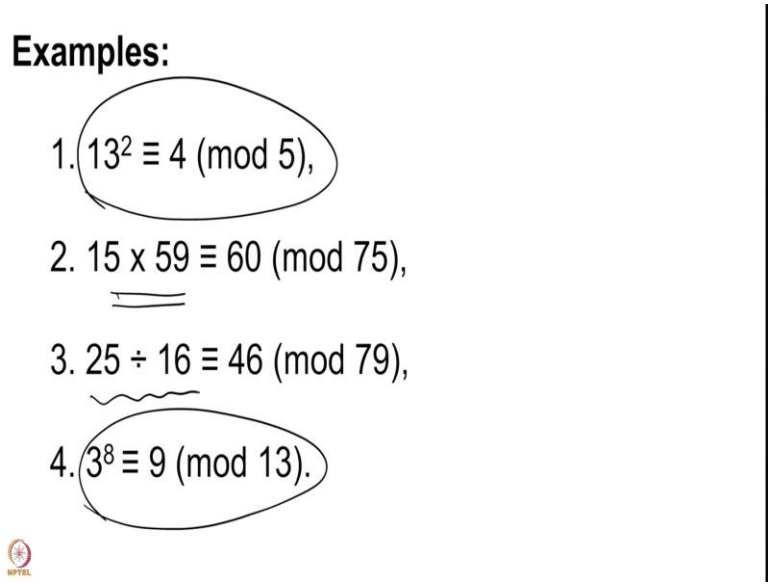
A Basic Course in Number Theory
Professor Shripad Garge
Department of Mathematics
Indian Institute of Technology, Bombay
Lecture number 12
Arithmetic modulo n, more examples

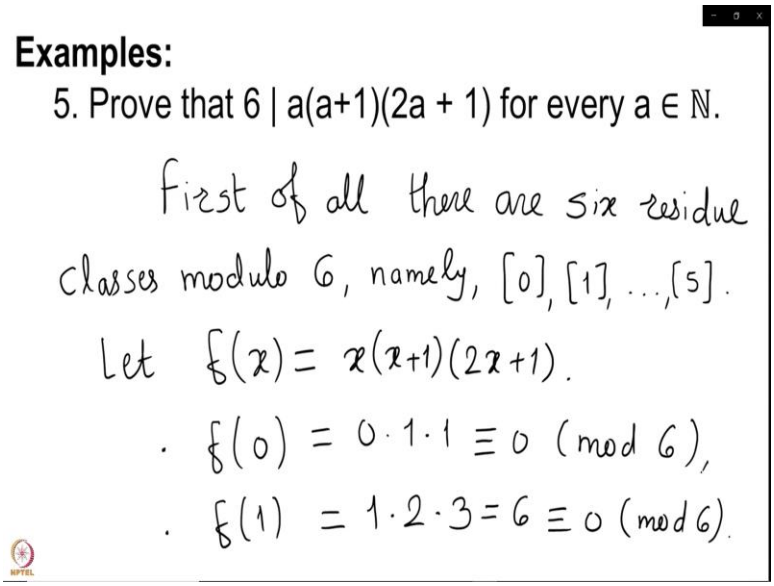
Ok, welcome back. We are doing some computations which is really getting our hands dirty with all these numbers and multiplications, additions and so on, but nothing like a good warm up to do the heavy theory that follows.

(Refer Slide Time: 0:38)



So, we have been doing these four problems in the last lecture. We will continue with this. Remember we computed some powers here, so, we computed powers of 13 and power of 3 modulo various numbers. We computed a product and we also looked at a division. After this, these are all basic operations that we have defined. So, these four are done.

(Refer Slide Time: 1:11)



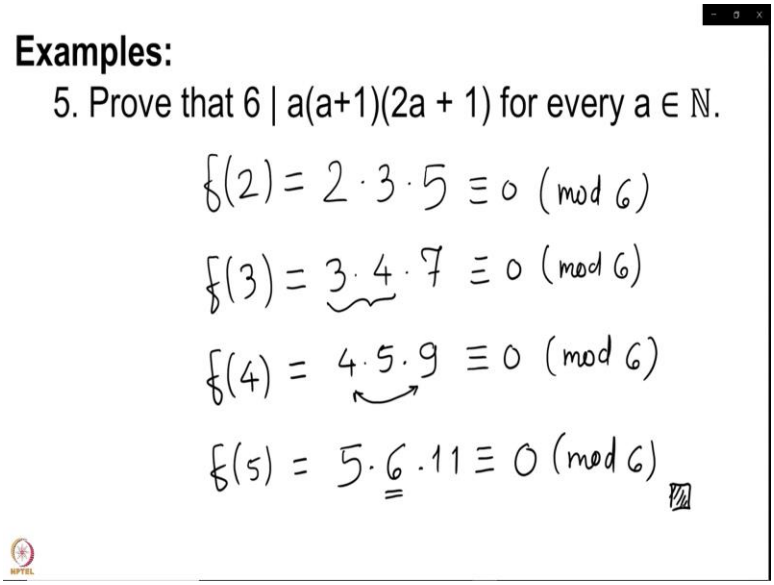
After this, I want you to think about this problem- Prove that 6 divides a, a plus 1 into 2a plus 1, for ever a in n. So, if you take the product on the right hand side, then this product for any natural number a is always a multiple of 6. This is the problem that we should think about now. So, I will give you 2 ways to do this.

First of all, there are 6 residue classes, modulo 6, namely, the class of 0, 1, 2, 3, 4 and 5. And we let a polynomial effects to be this polynomial x into x plus 1 into 2x plus 1. What we have to check is that for every class a modulo 6, f of a is congruent to 0 mod 6. This is what we want to check. So, we simply put various values, so we check that f of 0 is, of course, 0 into 1 into 1. This is 0 mod 6, that is good?

Let us look at f of 1. This is 1 into 1 plus 1 is 2 and 2 plus 1 is 3, which is 6 and 6 is, of course, 0 mod 6. So, for the class 0 and for the class 1, we do indeed, have that the polynomial effects which x, x plus 1 into 2x plus 1 evaluated at these two classes gives you 0. So, already you have proved the result for one-third of the natural numbers.

Any natural number which is congruent to 0 mod 6 has the property that 6 divides that natural number into that natural number plus 1 into twice of that natural number plus 1. So, whenever a is 0 mod 6, we are done. Whenever a is 1 mod 6, we are done. Now, we are left with 4 residue classes. So, l look at those as well.

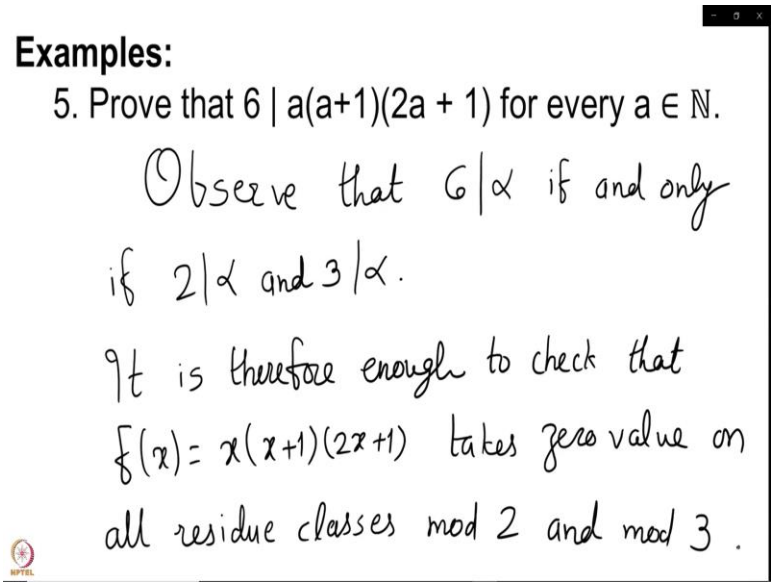
(Refer Slide Time: 4:35)



So, we will check. 0 is done, 1 is done. So, I need to check what happens when we put the value of 2. So, this is going to give you 2 into 3 into 5, which is 30 and of course, this is also 0 mod 6. Class of 3, this gives you 3 into 4 into 7. Since, here, already, we have 12, which 0 mod 6, we get that this is 0 mod 6. Then, we take the class of 4, which gives us 4 into 5 into this quantity will give us 9.

So, the product of these two is 36, which is 0 mod 6. Therefore, the whole thing is 0 mod 6. And finally, we compute the value of the polynomial at 5. So that, we have as 5 into 6, there is already a 6 coming here. So, because of this, we get it 0 mod 6. That is it. We have a problem to be checked for all natural numbers and by doing the arithmetic modulo 6, it has been reduced to ring the problem for only 6 classes. Some of you may have some more ideas of doing these problems.

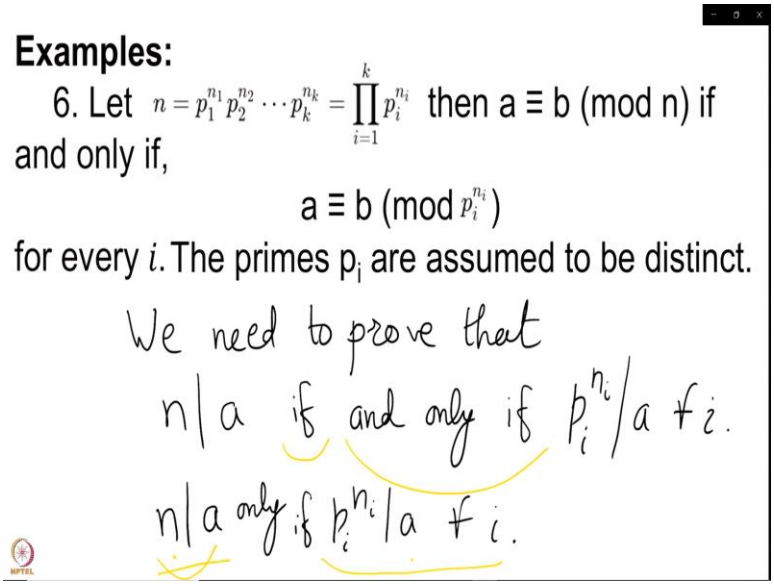
(Refer Slide Time: 6:31)



So, let me tell you one more thing. So, observe that 6 divides sum integer alpha if any only if 2 divides alpha and 3 divides alpha. So, it would be enough to check. So, it is, therefore, enough to check that f x, which we have define to be x. x plus 1, 2x plus 1, takes 0 value on all residue classes mod 2 and mod 3. So, earlier we have observed that we had to do only 6 checks, because we were working modulo 6, but this observation tells you that all you need to check is modulo 2 and modulo 3.

Modulo 2, there are 2 checks. You will put the value 0, and you will put the value 1. Modulo 3, there are 3 checks, you will put the value 0, you will put the value 1, you will put the value 2 and since x divides the polynomial f x, for 0 you are always going to get 0. So, actually, you have to check only 3 cases, 1 modulo 2, 1 modulo and 2 modulo 3. So, the whole problem of checking over all natural numbers is now reduced to checking some very simple equation. So, this also tells you something that I would like to encode in the next problem.

(Refer Slide Time: 8:52)



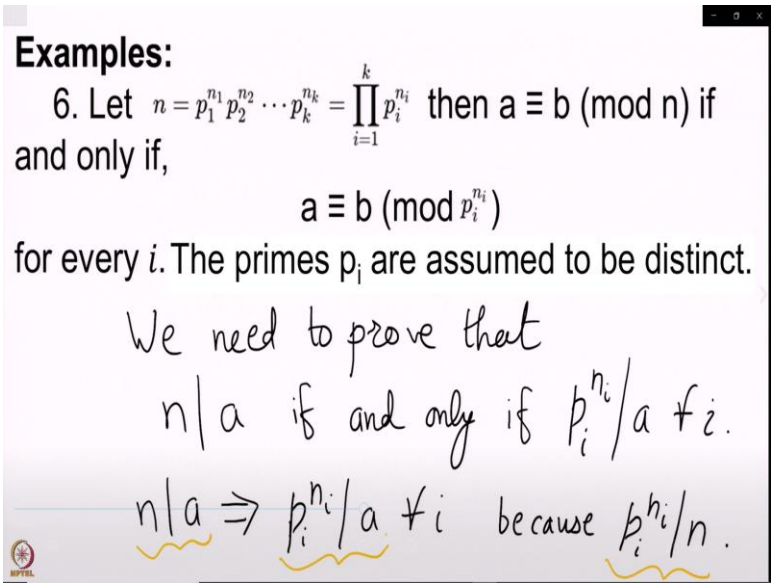
Suppose we have the following prime factorization for n. So, n is b1 power n1 into b2 power n2 dot dot dot, bk power nk, which we write as product of bi power ni, where i goes from 1 to k. Then, a and b modulo n are equal if and only if a and b are equal modulo pi power ni for every i. So, this proof is actually similar to what we have done in the previous case. So, we need to prove that n divides sum number a if and only if pi power ni divides a for every i. This is the thing that we have to prove.

And if and only if means that we will able to break this statement into two parts. So, what are those 2 parts? Let me explain it to you with this. So, first of all, there are 2 parts. There is this and then there is this. So, when we talk about a statement being true if and only if some other statement is true, you should be able to read it in the following way. We read it as 'n divides a if pi power ni divides a for all i. This would be 1 part of the statement. What it means to say is that…

So, let me write this statement down, n divides a if pi power ni divide a for all i. So, we will, then have to prove whenever this condition holds, for all i, pi power ni divides a, then n must divide a. So, we will assume this part and we will prove this part. This would be 1 part of proving this if and only if statement. But then there is the other part which is the only if part.

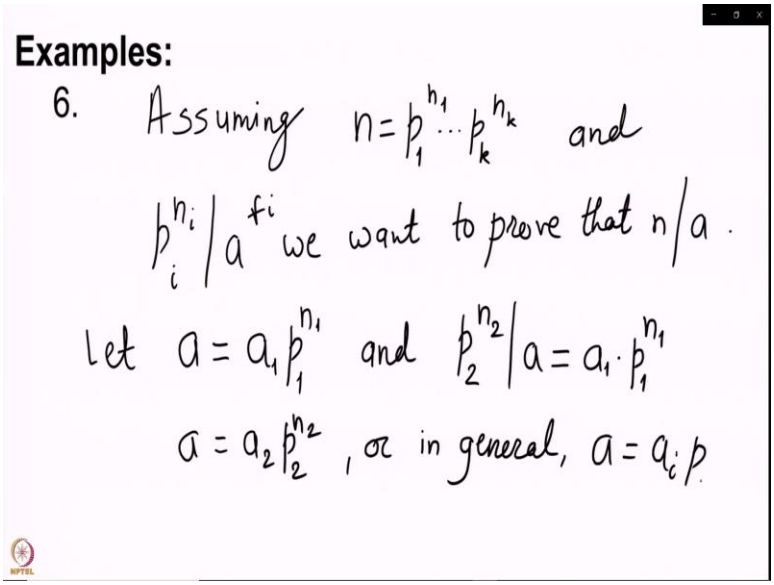
So, how do we read the only if part? That would mean that n divides a, can happen only when this happens. If this does not happen, then this does not happen. So, whenever this happens, we should be able to prove that this happens. So, there are 2 parts to proving a statement of the part which has if and only if. And we will here, be proving both the parts.

(Refer Slide Time: 12:08)



So, the simpler part is that whenever n divides a, the pi power ni divides a. We will prove this statement. But this is quite easy. This holds because pi power ni that itself, divides n. So, we have here, that you have this division, pi power ni divides n and n divides a, then of course, you should have that pi power ni should divide a. The non-trivial proof, although, it is also not very difficult, is to show that the other implication holds, which is to say that when we have pi power ni divide a, for every i, we will have to prove than n divides a.

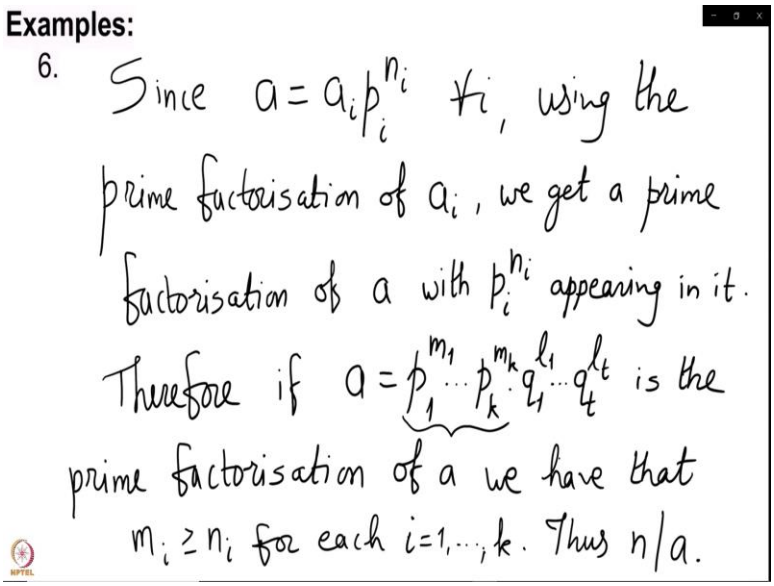
(Refer Slide Time: 13:14)



So, assuming n equal to p1 n1, pk, nk and pi power ni divides a, we want to prove that n divides a. This is the thing that we want to prove. So, this is of course, we have, for all i. So, whenever pi power ni divides a for every i, we want to prove that n itself, divides a. So, let a be equal to ai into pi power ni. Or we begin, let us say, with the first among the primes. So, we have a equal to a1 into p1 power n1. Alright?

So, we also have that p2 power n2 divides a. Since we have this for every i, we have also, that p2 power n2 divides a, but a can be written as a1 into p1 power n1. Now, what we observe here is the following thing. Since p2 power n2 divides a, we also have a2p, a2 into p2 power n2. Or in general, we have that a is ai into pi power ni.

(Refer Slide Time: 15:12)



So, since, a is ai into pi power ni for every i, using the prime factorization of ai, we get a prime factorization of a with pi power ni appearing in it. So, therefore, if a equal to p1 power m1, pk power mk, q1 power l1, qt power lt is the prime factorization of a. So, what we are doing here is that we are considering the prime factorization of a into prod, so, we are factoring a into product of primes and collecting all primes which are same together.

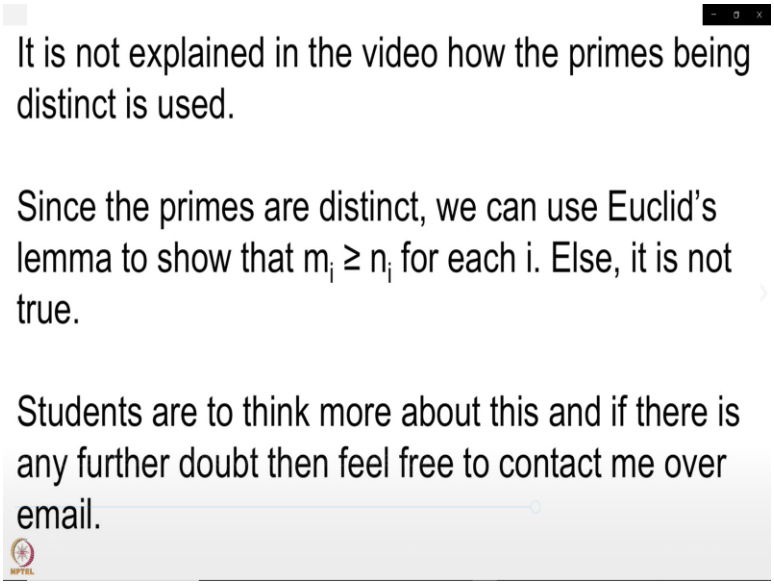
And so, we can put them in the power of p1. So, these p1 p2 pk power m1 m2 mk, these mi can be 0 to begin with. We will assume. If some pi does not appear in the prime factorization of a, let that be 0. But because we have that this pi power ni appears in some factorization of a and further we also know by fundamental theorem of arithmetic, that the factorization is unique.

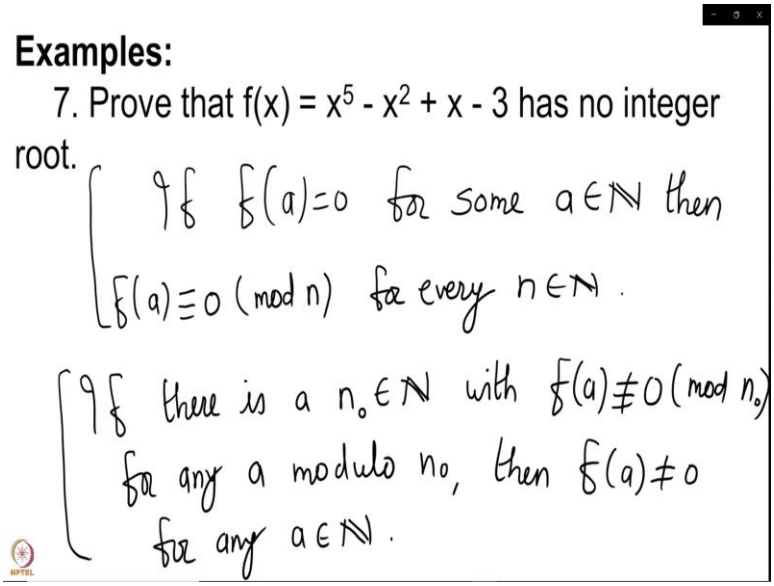
So, it will tell you that pi power ni should occur. So, we have that mi is bigger than or equal to ni. You may have p1 appearing with some more powers in the factorization of a. But what we do know is that p1 should appear with the multiplicity n1 or more. So, you have that for each i from 1 to k. The prime pi comes with multiplicity at least ni or perhaps, more.

So, this is thus, n should divide a. Because we have that the p1 power m1 up to pk power nk will have p1 power n1, p2 power n2, pk power nk appearing there in the prime factorization of a and that then tells us that n should appear as a factor of a and therefore, we have that n divides a. So, if we were to go back, we have that whenever n divided a, we proved that pi power ni divides a.

And then, we assumed that pi power ni divides a and we proved that actually, we have that n must divide a.

(Refer Slide Time: 19:11)



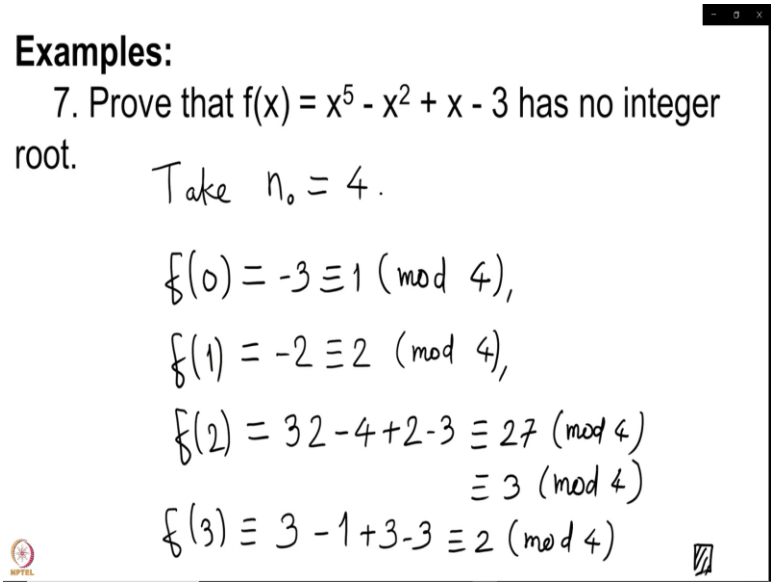


So, now, I will go to the next problem, which is to look for solution of a polynomial among the set of natural numbers and here, we have this problem. Prove that f of x which is x to the five minus x square plus x minus 3 has no integer root. So, we want to prove that there is no integer a such that f a is 0 for this polynomial f. So, if you had that there was a solution to this, if f a was 0 for sum a in n then, f a should be congruent to 0 mod n for every natural number n.

Therefore, if you could show, so if there is some n naught in n, with fa naught being congruent to 0 mod n naught for any a modulo n naught. Then, fa is never 0. We have just twisted this statement and put it in this way. If you have a statement that fa is 0 for sum a in n, then for that particular a, fa will give you 0 congruence class modulo n for every n.

And therefore, if you can find an n naught such that there is no 0 for the polynomial f modulo n naught, then, the polynomial f cannot have a 0 in n. So, for us to show that this given polynomial x to the 5 minus x square plus x minus 3 has no integer root, we need to only show that there is some n naught for which we get no root and we will take that n naught very cleverly.

(Refer Slide Time: 22:32)



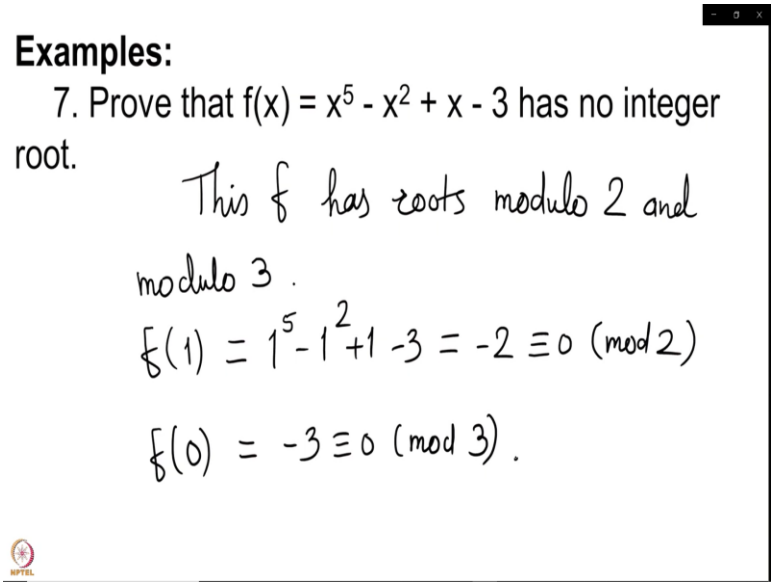
So we say that take n naught to be 4. Let us do the calculation for every residue class modulo 4. So, what do we do? F of 0 is 0 minus 0 plus 0 minus 3 which is congruent to 1 mod 4, doesn't give you 0. F1, 1 minus 1 plus 1 minus 3, so 1 minus 1 get cancelled, but 1 minus 3 will give you minus 2 which is 2, modulo 4. Do not get a 0. F of 2, 2 to the 5, what is 2 to the 5? 2 square is 4, 2 cube is 8, 2 raised to 4 is 16 and 2 to the 5 is 32.

So, we have 32 minus 2 square which gives you 4 plus x which is 2 minus 3. So, 34 minus 4 which is 30 minus 3, 30 minus 3 is 27, which is equal to 27, but we can as well put in congruent sign modulo 4, you do not get a 0. This is actually congruent to 3 mod 4. And finally, when you compute f of 3, you get 3 to the 5, so, 3 square, we are looking at it modulo 4. 3 square is 9,

which is 1 modulo 4. So, when you want to compute 3 power 5, this is 3 square into 3 square into 3. So, you get 1 into 1 into 3.

So, the ultimate answer is only 3 minus 3 square which is 1 plus x which is 3 minus 3. So, you get 3 minus 1 which is 2 plus 0. So, you get this to be 2 modulo 4. So, we are not getting 0 mod 4 for any of the residue class mod 4 and therefore, here, we have no solution modulo 4. You may wonder why I took n naught to be 4 and why not 2 or 3. So, it turns out that modulo 2 and 3, there are actually solutions for this polynomial.

(Refer Slide Time: 25:11)



This f has roots modulo 2 and modulo 3. How do we check that? So, if you are considering modulo 2, let us look at f of 1, this is 1 power 5 minus 1 square, plus 1 minus 3 which gives you minus 2, which is 0 mod 2. So, 1 is a root for the polynomial f modulo 2 and if you are looking at modulo 3, then consider f of 0, which is simply minus 3 which is 0 mod 3. And, of course, if you were to look at n equal to 1, everything has its root modulo 1.

Every polynomial with integer coefficients will give you the value to be an integer and any integer is divisible by 1. So, you will always have roots modulo 1. So, what we have observed here is that the cases n equal to 2 and n equal to 3 would not work for us. You do get a root for the polynomial f, modulo 2 as well as modulo 3. So, we have to go to the n equal to 4 to check

that there is no root. Sometimes, you may have to go very far to prove that some polynomial does not have a root, you will have to take a very large n, to show that there is no root.

So, whenever you get a root to an integer coefficient polynomial over some residue classes modulo n do not assume that there is a root always, do not assume that there is a root in integers. There can be polynomials, which have roots modulo every n. But there is no integer root. We will see one such example in the next lecture. But proving that will require some higher theory. However, I will just tell you that example, and then we will go to some more discussions. Thank you.