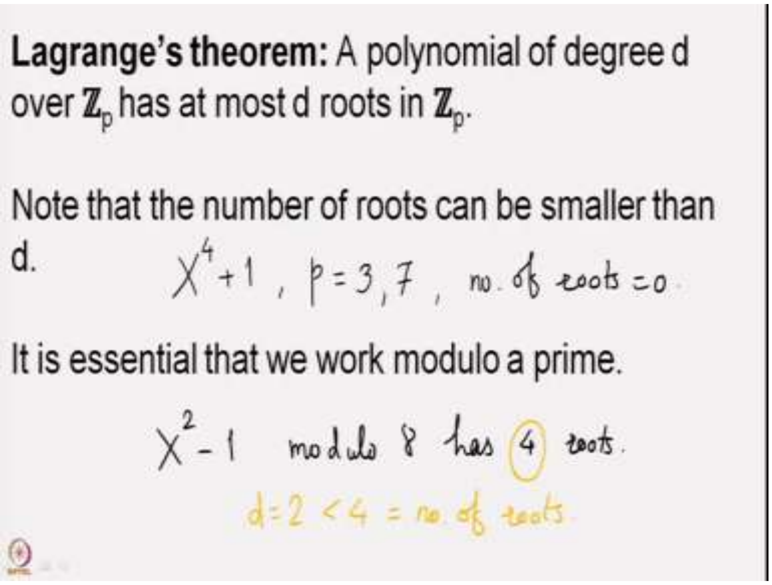
A Basic Course in Number Theory
Professor Shripad Garge
Department of Mathematics
Indian Institute of Technology, Bombay
Lecture 22
Roots of Polynomials over Zp

Welcome back, we are looking at the theorem of Lagrange that if you take Z by pZ and take a polynomial of degree d with coefficients coming from Z by pZ then there are at most d roots, this is result that we have looked just towards the end of the last lecture.

(Refer Slide Time: 00:41)



Lagrange's theorem: A polynomial of degree d over $\mathbb{Z}_p$ has at most d roots in $\mathbb{Z}_p$.

Note that the number of roots can be smaller than d.

X^4+1 , $p=3,7$, no. of roots $=0$.

It is essential that we work modulo a prime.

X^2-1 modulo 8 has $\boxed{4}$ roots.

$d=2<4=$ no. of roots.

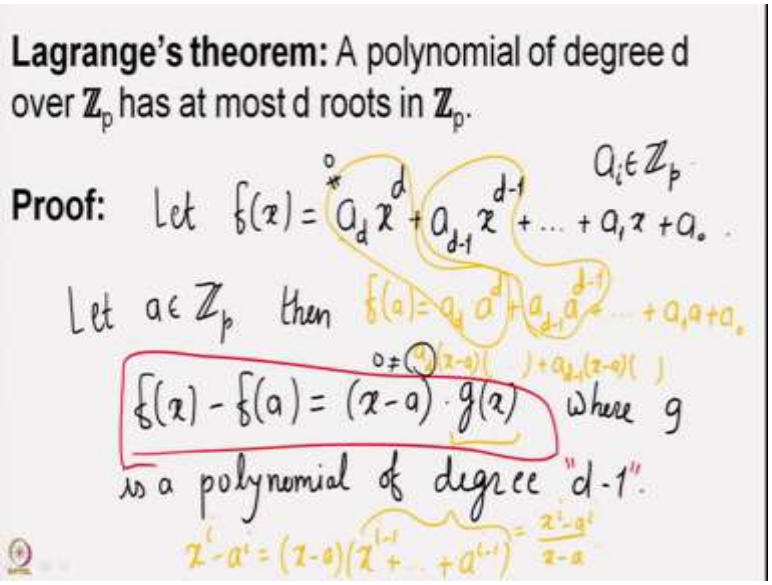
So, here is the result a polynomial of degree d over Zp has at most d roots in Zp. And we have also noticed these 2 remarks that the number of roots can of course be smaller than d and it is also essential then that we work modulo a prime.

So just to recall it for you, I will make it clear that here you can take the example of x to the 4 plus 1. And you can take this example where p is 3. So, here there is a polynomial of degree 4, and in Z3, there are no roots at all or you may also take p equal to 7; even in 7, Z modulo 7 Z, we have no root at all for x to the 4 plus 1. This is like saying that minus 1 is a fourth power.

If you had any solution to this polynomial, any root of this polynomial would give you a raise to 4 is minus 1 modulo 7, minus 1 is 6 modulo 7. So this would say that 6 is a 4 power modulo 7, but 1 sees by a computing squares that 6 is not even a square. So we do not get any root here and therefore the number of roots is indeed less than degree which is that 0.

Whereas if you do not work modulo a prime and then we have seen that x to the 2, which is x square minus 1 modulo 8 has 4 roots. So this number is bigger than the number of degree. This is your number of roots and the d here is 2 which is less than 4 which is the number of roots. So to have Lagrange's theorem, it is essential that you work modulo a prime and not modulo a composite number. So let us go about proving this result.

(Refer Slide Time: 03:00)



Lagrange's theorem: A polynomial of degree d over $\mathbb{Z}_p$ has at most d roots in $\mathbb{Z}_p$.

Proof: Let $f(x) = \overset{0}{\overset{*}{a_d}} x^d + a_{d-1} x^{d-1} + \dots + a_1 x + a_0$. $a_i \in \mathbb{Z}_p$

Let $a \in \mathbb{Z}_p$ then $f(a) = a_d a^d + a_{d-1} a^{d-1} + \dots + a_1 a + a_0$

$0 \neq a_d (x-a)(\quad) + a_{d-1}(x-a)(\quad)$

$\boxed{f(x) - f(a) = (x-a) \cdot g(x)}$ where g is a polynomial of degree "d-1".

$x^i - a^i = (x-a)(\overbrace{x^{i-1} + \dots + a^{i-1}}) = \frac{x^i - a^i}{x-a}$

The proof is not very difficult, it is quite easy, but before we prove this, let me just remark one thing. So, suppose I start with a polynomial f of degree d so what we have is we have it to be x ad x to the d plus a d minus 1 x raise to d minus 1 plus dot, dot, dot a1 x plus a0 this is a polynomial that we have and assume that we have some element in Zp then fx minus fa is x minus a into g x where g is a polynomial of degree d minus 1.

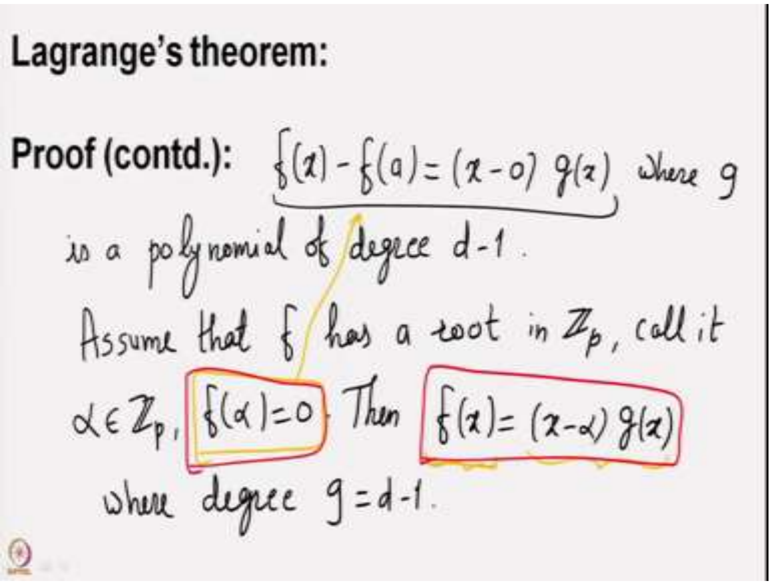
This is something which holds in general, this is because what we have is that we have fx which is given by this formula and then fa would be also given similarly, you will have ad, a power d plus a d minus 1 a power d minus 1 plus dot, dot, dot plus a1 a plus a naught. So, recall here that these ai are taken as coefficients, they are elements in Zp there is no relation between ai and a. That is something that we should not forget about.

So, when you take the differences you will look at ad x power d minus ad a power d and this can be written as ad x minus a into a polynomial if any degree d minus 1. Similarly, you will have this the difference of a d minus 1 x minus a into a polynomial of degree d minus 2.

So, what we are really looking at this at this point is that x to the i minus a to the i is x minus a, x raise to i minus 1 and then you have some terms here and finally, you will have a power i minus 1 this is the polynomial that we will look at this is the polynomial which is x power i minus a power i upon x minus a. So, combining all these polynomials for different degrees will give you the polynomial g x this is what we get.

So the most important thing for us from this point is this point that fx minus fa is actually our x minus a into g x where g has to be a polynomial of degree d minus 1 because if f is your polynomial of degree d minus 1, then that will tell you that a sub d has to be non-zero. This is not equal to 0, and it is the same coefficient that you are going to get here when you look at the d minus 1 coefficient, it is the same coefficient that you had. So g is also a polynomial of degree d minus 1. This is the most important thing that we need to remember.

(Refer Slide Time: 06:47)



Lagrange's theorem:

Proof (contd.): $\underbrace{f(x) - f(a) = (x-a)\, g(x)}$ where g is a polynomial of degree $d-1$.

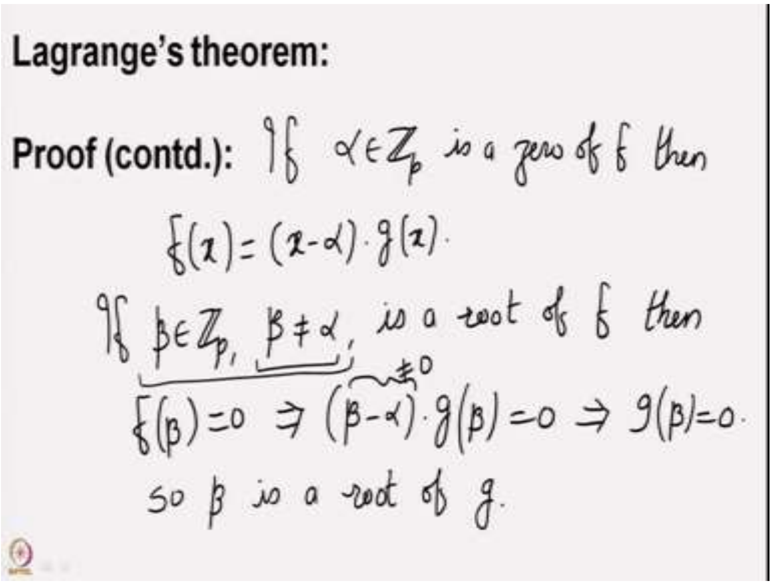
Assume that f has a root in $\mathbb{Z}_p$, call it $\alpha \in \mathbb{Z}_p$, $\boxed{f(\alpha)=0}$. Then $\boxed{f(x) = (x-\alpha)\, g(x)}$ where degree $g = d-1$.

So fx minus fa is x minus a into a polynomial gx where g is a polynomial of degree d minus 1. So, we have 1 less degree for g than the degree of f. Now, so assume that f has a root in Zp, call it alpha. So we have an element alpha in Zp with the property that f alpha is 0 and then by applying this reserved where you put a equal to alpha, what we get is fx equal to x minus a into some polynomial of gx where degree g is d minus 1. This is because instead of fa, we will get 0 there so this f alpha equal to 0.

This is the thing which we put here and so on this side we get only fx, we do not get fx minus some constant, that constant is 0. So on the left hand side we would simply get fx. So this is only fx and on the right hand side we have x minus alpha into gx. So what this tells us is that whenever we have a root for the polynomial f, then x minus alpha divides the polynomial f.

You can actually write fx as x minus alpha into another polynomial of smaller degree, okay. This is the thing that we need to take ahead from this second slide that fx is now x minus alpha into gx where you have f alpha to be 0.

(Refer Slide Time: 09:27)



Lagrange's theorem:

Proof (contd.): If $\alpha \in \mathbb{Z}_p$ is a zero of f then

$$f(x) = (x-\alpha)\cdot g(x).$$

If $\underbrace{\beta \in \mathbb{Z}_p, \underbrace{\beta \neq \alpha}}$, is a root of f then

$$f(\beta) = 0 \Rightarrow (\overset{\neq 0}{\beta - \alpha})\cdot g(\beta) = 0 \Rightarrow g(\beta) = 0.$$

so β is a root of g.

So, if alpha in the Zp is 0 of f then fx equal to x minus alpha into gx. Now, suppose that there is 1 more root beta. So, if beta in the Zp beta not equal to alpha is a root of f then f beta is 0 which implies that alpha minus beta or actually you will have beta minus alpha into g beta equal to 0.

But since you have that beta is not equal to alpha that tells you that this is non-zero. And if this is non-zero what we should get is g beta equal to 0. What is happening here is that we are looking at elements in Zp, Z by pZ and once you put these values in the polynomial the g beta or beta minus alpha, these are all elements in Z by pZ and these are all represented by natural numbers.

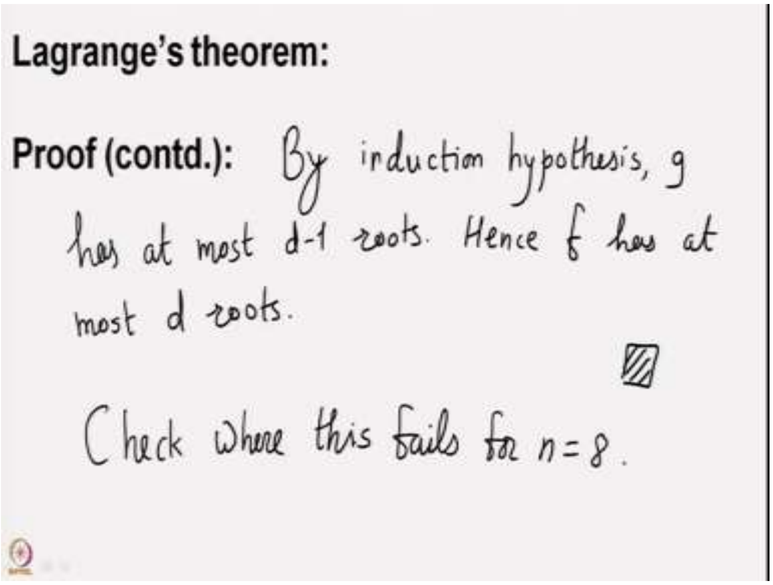
So actually these are looking, these are some natural numbers and we are simply going modulo the prime p that is what we are doing, okay. So, when we say that some product is 0 then it tells us that p divides the product, because something is 0 in Z modulo pZ only means that when you divide by p, the remainder is 0. That means p divides that natural number, but p being a prime has the property that when p divides a product of 2 numbers, p has to divide 1 of the 2.

And therefore, if 1 of them is not 0 modulo p, so here beta minus alpha is not 0 in Zp that means p does not divide beta minus alpha, but p divides the product of beta minus alpha into g beta. So p has to divide the other thing which is g beta and therefore, g beta has to be 0. So, we get that if you have any such other root then beta is a root of g. Now g is of degree d minus 1 and we apply induction hypothesis we will start our induction with polynomials of degree 1 which are linear polynomials.

And those we have already observed that a linear polynomial where the coefficient of x is not 0 gives you a unique root. So, the result is true for degree equal to 1 and then we apply induction hypothesis to the polynomial g, g has degree d minus 1 and the polynomial and degree d minus 1 can have at most d minus 1 roots together with the root alpha, which might also be a root of g. In that case, we will not have to count alpha separately.

But even if alpha is not a root of g, you may have to just add that single root. So whenever you are counting the distinct roots of the polynomial f, you are looking at the distinct roots of the polynomial g once you have taken one root alpha out and then you add this single root alpha to the list of the roots of g, okay.

(Refer Slide Time: 13:31)



Lagrange's theorem:

Proof (contd.): By induction hypothesis, g has at most $d-1$ roots. Hence f has at most d roots.

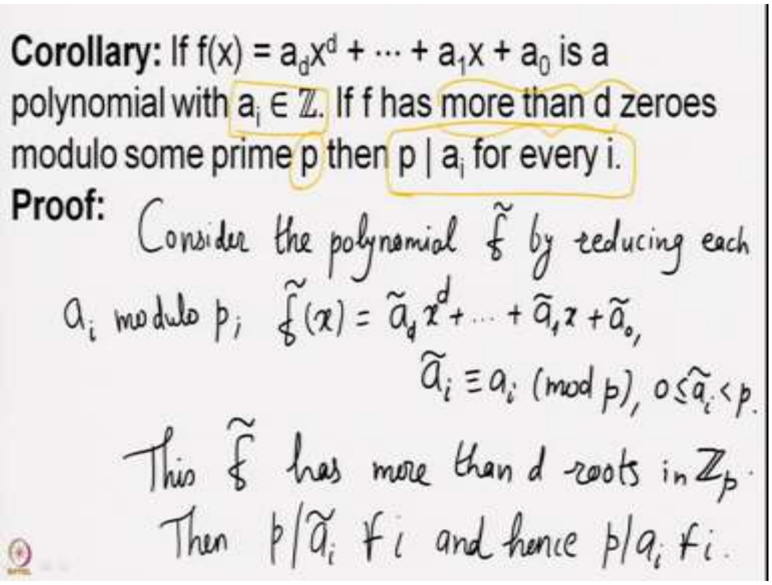
▨

Check where this fails for $n=8$.

So by induction hypothesis g has at most d minus 1 roots and hence f has at most d roots that completes the proof. So, you may wonder where does this proof fail when you have modulus which is not a prime when you have a composite modulus and the point is exactly that you may have 8 for instance where we had 4 roots for it. 8 divides product of 2 but when it 8 does not divide 1, it does not imply that a divides the other one. So, check this as a basic exercise check where this fails for n equal to 8, okay.

So, we have Lagrange's theorem, which says that whenever you have a polynomial of degree d over the Z by a pZ then such a polynomial can have at most d roots and when we are saying at most d roots, we are counting the roots distinctly. If the roots come with multiplicity, then of course, this number will further go down, but let us not worry about that. There is one very nice corollary of this result. So, let us see this corollary.

(Refer Slide Time: 15:33)



Corollary: If $f(x) = a_dx^d + \cdots + a_1x + a_0$ is a polynomial with $a_i \in \mathbb{Z}$. If f has more than d zeroes modulo some prime p then $p \mid a_i$ for every i.

Proof: Consider the polynomial $\tilde{f}$ by reducing each a_i modulo p; $\tilde{f}(x) = \tilde{a}_d x^d + \cdots + \tilde{a}_1 x + \tilde{a}_0$,

$\tilde{a}_i \equiv a_i \pmod{p}$, $0 \leq \tilde{a}_i < p$.

This $\tilde{f}$ has more than d roots in $\mathbb{Z}_p$.

Then $p/\tilde{a}_i \ \forall i$ and hence $p/a_i \ \forall i$.

The corollary says, that if you have a polynomial in degree d with coefficients coming from integers and suppose modulo some prime, you have the number of 0s to be more than d, then p must divide ai for every i. So, first of all, we are starting with a polynomial which is defined over integers or you may also take a polynomial or natural numbers, but integers is more desirable.

And then we look at modulo some prime p, so p is a prime and suppose that the number of zeros is more than D, then what we should get is that p divides the coefficients for all i. This is the basic statement which we would now like to prove. So consider the polynomial f tilde by reducing each ai modulo p.

So, we will have a polynomial f tilde x which is given by ad x power d plus dot, dot, dot plus a 1 x plus a 0, but we are looking at not necessarily the ai, but ai tilde where the ai tilde are congruent to ai mod p and you may assume that your ai tilde are between 0 to p. So, we now have a polynomial over Zp, we have a polynomial over the set Z by pZ.

And here by our assumption we have more than d roots. This is what we have seen that there are more than d0. So, this f tilde has more than d roots in Zp. So what is going wrong Lagrange's theorem told us that whenever you have a polynomial of degree d, it can have at most d roots. It seems that here we have a polynomial of degree d, we have this polynomial ad tilde x power d plus the next coefficient will be ad minus 1 to x power d minus 1 plus dot, dot, dot plus a 1 x a1 tilde x plus a0 tilde.

So, since we have a polynomial of degree d should have at most d roots, but our assumption says that we are getting more than d roots. So, what must be happening is that Lagrange's, the hypothesis in Lagrange's his theorem must not be satisfied. So, there are many, the hypothesis has many parts let us go from the last part. The last part was that we are working modulo a prime that is certainly true here, we are looking at the prime p and we are working modulo p. So that is alright.

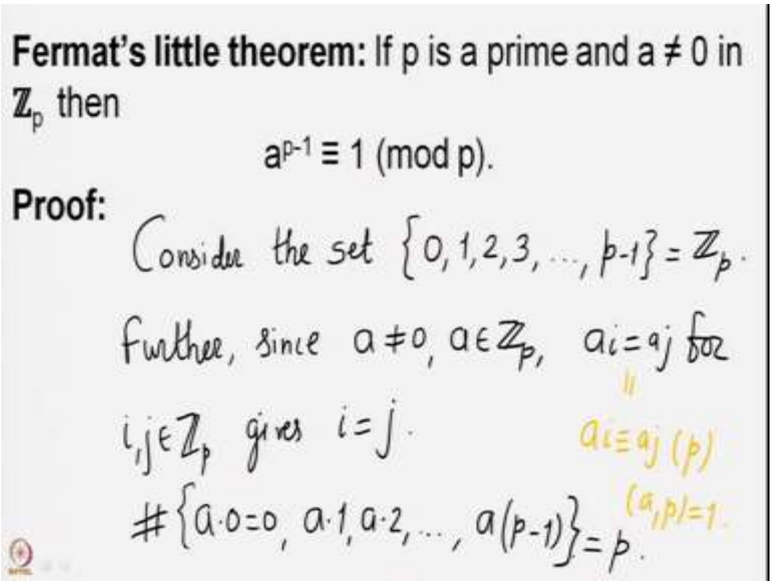
Then we go further and we see that the hypothesis says that you have a polynomial of degree d, somehow this must not be true, but clearly we have something of the type ad tilde x power d plus dot, dot, dot. How does a polynomial of degree d look if not like this? So, if you are saying that this is not a polynomial of degree d, then what must happen is that the coefficient of x power d must not be a non-zero element because if that is a non-zero element, then it is a polynomial of degree d and then we get a contradiction somehow.

So, the ad tilde should not be 0, should not be non-zero ad tilde should be 0 which means that p will divide ad tilde, but ad tilde is congruent to ad modulo p. So p will divide ad. Once you have that ad tilde becomes 0 modulo p, the degree of the polynomial has reduced and if any ai tilde had been non-zero modulo p you would get a polynomial of degree smaller than d and again the fact that the number of roots is more than p, d would give you a contradiction.

So, what must happen therefore is that every coefficient must be divisible by p. So, then p divides ai tilde for each i and hence, B divides ai for each i. The only way a polynomial which is defined over natural numbers has more than d roots over a prime p will be where the polynomial when reduced to Z by pZ gives you a 0 polynomial. And that would happen exactly when the prime p divides all the coefficients of the polynomial and that is what we have.

So, the corollary says that if you have a polynomial of some degree d and modulo some prime you have more than p roots d roots, then the prime p should divide the all the coefficients of the polynomial, f. We will, this is a very pretty corollary there are many nice applications of this we will see some of these applications when we go to assignments.

(Refer Slide Time: 21:57)



Fermat's little theorem: If p is a prime and a ≠ 0 in $\mathbb{Z}_p$ then

$$a^{p-1} \equiv 1 \pmod p.$$

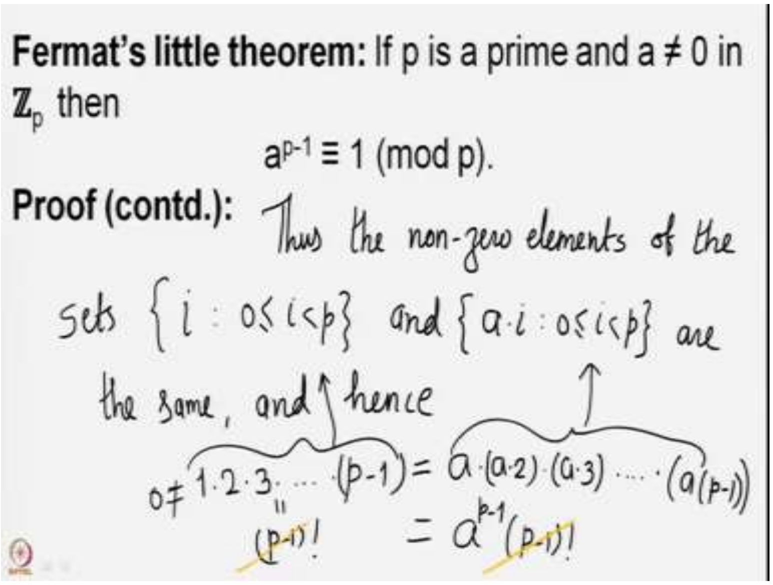
Proof: Consider the set $\{0, 1, 2, 3, \ldots, p-1\} = \mathbb{Z}_p$.

Further, since $a \neq 0$, $a \in \mathbb{Z}_p$, $ai = aj$ for $i, j \in \mathbb{Z}_p$ gives $i = j$.

$\shortparallel$

$ai \equiv aj\ (p)$

$\#\{a\cdot 0 = 0, a\cdot 1, a\cdot 2, \ldots, a(p-1)\} = p.$ $(a,p)=1.$



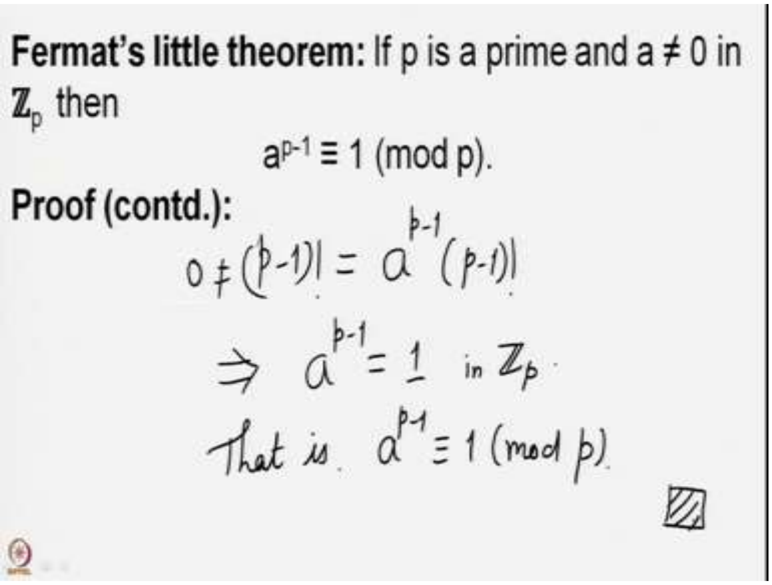
Fermat's little theorem: If p is a prime and a ≠ 0 in $\mathbb{Z}_p$ then

$$a^{p-1} \equiv 1 \pmod p.$$

Proof (contd.): Thus the non-zero elements of the sets $\{i : 0 \leq i < p\}$ and $\{a\cdot i : 0 \leq i < p\}$ are the same, and hence

$$0 \neq \underset{\cancel{(p-1)!}}{\underset{\shortparallel}{\overbrace{1\cdot 2\cdot 3\cdot \cdots \cdot (p-1)}}} = \overbrace{a\cdot(a\cdot 2)\cdot(a\cdot 3)\cdot \cdots \cdot(a(p-1))}$$

$$= a^{p-1}\cancel{(p-1)!}$$



Fermat's little theorem: If p is a prime and $a \neq 0$ in $\mathbb{Z}_p$ then

$$a^{p-1} \equiv 1 \pmod{p}.$$

Proof (contd.):

$$0 \neq (p-1)! = a^{p-1}(p-1)!$$

$$\Rightarrow a^{p-1} = \underline{1} \text{ in } \mathbb{Z}_p.$$

That is. $a^{p-1} \equiv 1 \pmod{p}$. ▨

But right now, I will go ahead and prove one small result which is called Fermat's Last, Fermat's Little Theorem. This is also pronounced as FLT this is also short form as FLT. But this is not that famous FLT, which was the Fermat's Last Theorem. This is the Fermat's little theorem. What does this theorem say? The theorem says that if you have any non-zero element in Zp, then raising that element to the power p minus 1 will give you 1. That is very remarkable.

You take any prime, just compute p minus 1 and then for any non 0 number for 0, ofcourse, you raise it to any power and you are going to get 0 you will not get 1, but if you raise any non-zero number to the power p minus 1, then you will get only one, you are not going to get any other answer. So let us see one basic proof. There are several proofs of this.

If you happen to know group theory, then there is a quick proof which would come. The proof if I can just tell you orally would be this, that the integers co-prime to p form a group under multiplication. Because when you have a and b in Zp and both a and b are non-zero then the product is also non-zero. Written in other way, whenever a b is 0, then a 0 or b is 0 modulo p. So if you are taking both a and b to be non-zero, the product is going to be non-zero.

Therefore, the set of the natural numbers from 1 to p minus 1 is closed under the product taken modulo p. Whenever you take product of any two, you get it to be a non-zero element. So, it is again an element from 1 to p minus 1. And this is a group because every element has an inverse. And then the order of this group is p minus 1 and this is the basic fact from group theory that any element 2 raised to the order of the group will give you 1.

So, that tells that a power p minus 1 is 1 modulo p, but since we are doing number theory, there are some nice number theoretic proofs. So, consider the set 0, 1, 2, 3 dot, dot, dot up to p minus 1, you will immediately recognize that this is nothing with Zp with respect to addition and product modulo p, this is the set Zp that I have listed further. Since a is not 0 and it is an element in Zp what we get is that ai is equal to aj for i, j in Zp gives i equal to j.

You can cancel a from both the sides. So this tells you that ai is congruent to aj modulo p. But since a and p are co-prime, you can simply cancel a from both the sides and that will give you that i is j. And therefore, if I write the elements a into 0, which is actually 0, a into 1, a into 2 dot, dot, dot all the way up to a into p minus 1, then I am going to get once again, p elements.

The cardinality of this set is equal to p we are going to get different p elements. So thus the non-zero elements of the sets 1 or you may just consider you will have these sets i, where you have 0 less than or equal to i less than p and a into i. The non-zero elements in both the sets are the same and hence when I take the product of all these numbers, so I have 1 into 2 into 3 and I take the product up to p minus 1, I am going to get a into 1 into a into 2 into a into 3 dot, dot, dot a into p minus 1.

On both the sides, we should get the same number because these are all the non-zero elements coming from these 2 different sets. So when I have 2 sets, and I am taking the non-zero elements in those 2 sets and take the product, if this numbers themselves are same perhaps they will be permuted, when I multiply by a, but the set the numbers as a set are same, then the product should give me the same value.

So here we know this is congruent to minus 1 modulo p. So this is in particular, not 0. And here I can take a common from each term I will get it to be p minus 1. And I once again, remember this is p minus 1 factorial and here I am getting the same number. So by canceling the number p minus 1 factorial which is a non-zero number, we get that 1 has to be equal to. So we get that p minus 1 factorial is equal to a raise to p minus 1 into p minus 1 factorial.

But since this is equal to minus 1 which is not a 0 quantity, we simply cancel it out to get that a raise to p minus 1 is 1 in Zp which is to say that a raise to p minus 1 is congruent to 1 modulo p. So it is a very beautiful small fact and this such a fact actually tells you whether a number can be prime or not. Because if you take some number 8, for instance and you raise some element to seventh power and you do not get the congruent to be 1 modulo 8, then ofcourse your 8 cannot be prime.

So for big numbers, this is quite a useful test of primality that you take a number from 1 to n minus 1 and raise that number to the power n minus 1 if the result modulo n is not 1 modulo n, then your number n cannot be a prime. However, as fate would have it, there are some knotty composite numbers and which satisfy Fermat's little theorem. We will have to treat with them separately that is not part of our course.

We will perhaps talk about them in the next lecture, but only to give you information about it. So I hope to see you in our next lecture. Thank you.