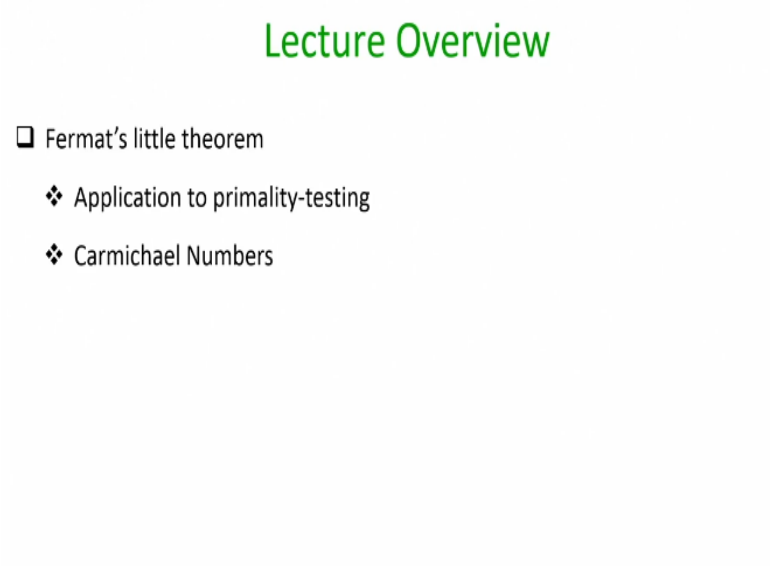
Discrete Mathematics
Prof. Ashish Choudhry
International Institute of Information Technology - Bangalore

Lecture - 60
Fermat's Little Theorem, Primality Carmichael Numbers

(Refer Slide Time: 00:23)

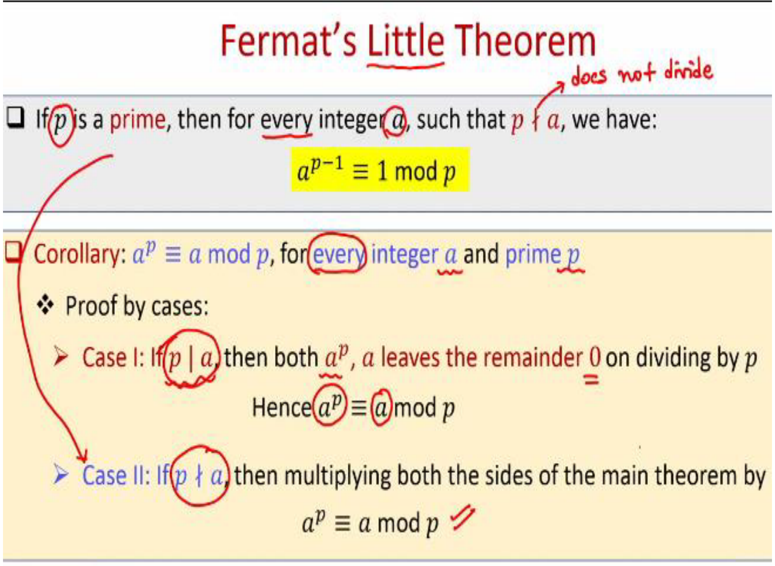


Lecture Overview

- ❑ Fermat's little theorem
  - ❖ Application to primality-testing
  - ❖ Carmichael Numbers

Hello everyone, welcome to this lecture, so the plan for this lecture is as follows: in this lecture, we will discuss about Fermat's little theorem, and we will see its application to primality testing, and we will also discuss about Carmichael numbers.

(Refer Slide Time: 00:35)



Fermat's Little Theorem

does not divide

❑ If p is a prime, then for every integer a, such that $p \nmid a$, we have:

$$a^{p-1} \equiv 1 \bmod p$$

❑ Corollary: $a^p \equiv a \bmod p$, for every integer a and prime p

❖ Proof by cases:

➢ Case I: If $p \mid a$ then both a^p, a leaves the remainder 0 on dividing by p

Hence $a^p \equiv a \bmod p$

➢ Case II: If $p \nmid a$ then multiplying both the sides of the main theorem by

$a^p \equiv a \bmod p$ ✓

So let us begin with Fermat's little theorem so, the theorem says that, if p is a prime number and if a is an integer such that p does not divide a. So, this notation means does not divide : ∤, in other words, a is co-prime to p, then the theorem says that $a^{p-1} \equiv 1$ modulo p. And this is true for every integer a, which is co-prime to p. So, that is the Fermat's little theorem attributed to Fermat.

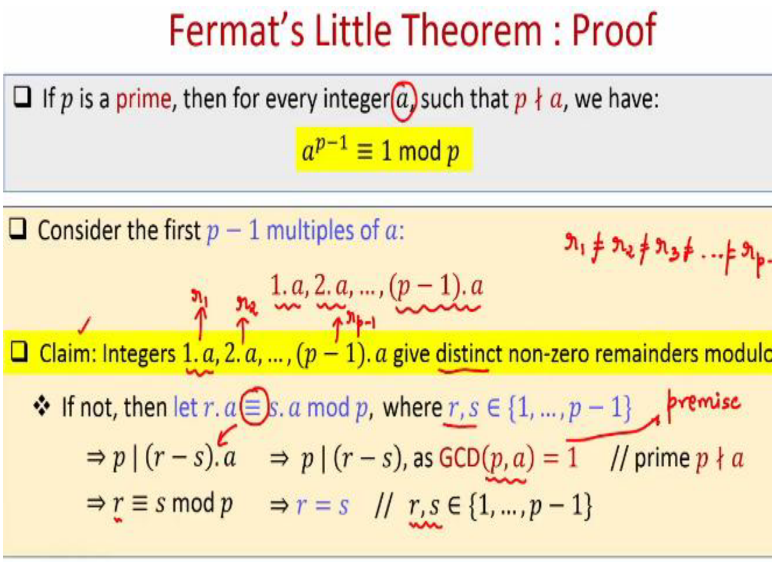
Why it is called little theorem because we want to distinguish this theorem from another interesting theorem attributed to Fermat's, which is also called as Fermat's last theorem. And this theorem also forms the basis for an interesting primality testing that we will see later on. So, this is the theorem statement but before going into the proof of the theorem statement, let us see an interesting corollary of this theorem statement.

So assume for the moment that this theorem statement is true, let us see an interesting corollary. So, the corollary is $a^p \equiv a$ modulo p for every integer a and prime p. And we can divide the proof into cases so, the corollary is for every integer it is not only for those integers a which are co-prime to p, whereas the Fermat's little theorem is strictly for those integers a which are co-prime to p. So, let us see the proof of the corollary first, so, we have 2 cases depending upon whether $p \mid a$ or not.

So, the first case is when $p \mid a$ so, if you have an integer a such that $p \mid a$, then since a is divisible by p any multiple of a is also divisible by p. So hence, a^p is completely divisible by p. And that means I can say that a^p gives you the same remainder, which a gives you on getting divided by p namely the remainder 0 because both a as well as a^p will be completely divisible by p if a is divisible by p. So that proves that the corollary is true for case 1.

Whereas if $p \nmid a$, then we can apply the Fermat's little theorem so if $p \nmid a$ then that means the premise of the Fermat's little theorem is satisfied. That means I can say that $a^{p-1} \equiv 1$ modulo p. And if that is the case, then if I multiply both sides by a, I get the conclusion that $a^p \equiv a$ modulo p so that proves that the corollary is true even for the case when a is not divisible by p.

(Refer Slide Time: 03:58)



Fermat’s Little Theorem : Proof

❑ If p is a prime, then for every integer a, such that $p \nmid a$, we have:

$$a^{p-1} \equiv 1 \bmod p$$

❑ Consider the first $p-1$ multiples of a:

$r_1 \neq r_2 \neq r_3 \neq \dots \neq r_{p-1}$

$$\underset{\uparrow r_1}{1.a}, \underset{\uparrow r_2}{2.a}, \dots, \underset{\uparrow r_{p-1}}{(p-1).a}$$

✓ ❑ Claim: Integers $1.a, 2.a, \dots, (p-1).a$ give distinct non-zero remainders modulc

❖ If not, then let $r.a \equiv s.a \bmod p$, where $r, s \in \{1, \dots, p-1\}$ premise

$\Rightarrow p \mid (r-s).a$ $\Rightarrow p \mid (r-s)$, as $\mathrm{GCD}(p, a) = 1$ // prime $p \nmid a$

$\Rightarrow r \equiv s \bmod p$ $\Rightarrow r = s$ // $r, s \in \{1, \dots, p-1\}$

So now let us come back to Fermat's little theorem and we prove it. So, we want to prove that you take any integer a, which is co-prime to p, then $a^{p-1} \equiv 1$ modulo p that is what we want to prove. So the proof is as follows: so, you consider the first p - 1 multiples of a, namely, 1 times a, 2 times a, 3 times a like that p - 1 times a, all these are different multiples of a. The claim is that all these multiples of a namely 1 times a, 2 times a, 3 times a, p - 1 times a when getting divided by p will give you distinct, non 0 remainders.

That means whatever is the remainder that you will obtain, by dividing 1 time a by p call that remainder is r_1 whatever remainder you obtained by dividing 2 times a by p call that remainder as r_2 and like that whatever remainder you obtain by dividing p - 1 times a by p called that remainder as r_{p-1}, the claim is that none of these remainders are same and of course, all of them are non 0. So, the proof will be by contradiction, we will now prove this claim by contradiction.

So, imagine you have 2 different multiples of a say r times and s times a where r and s belongs to the set 1 to p - 1 such that the remainder which you obtain by dividing r times a on dividing by p and the remainder that you obtain upon dividing s times a by p are same. The claim says that is not the case, but assume on contrary that you have 2 such different multiples, which gives you the same remainder.

Now, if r times a and s times a are congruent modulo p, then as per the definition of congruence, I can say that r times a - s times a is completely divisible by p: $(p \mid (ra - sa))$. That means p divides r - s times a: $(p \mid a(r - s))$; that implies that p has to divide r – s : $(p \mid$

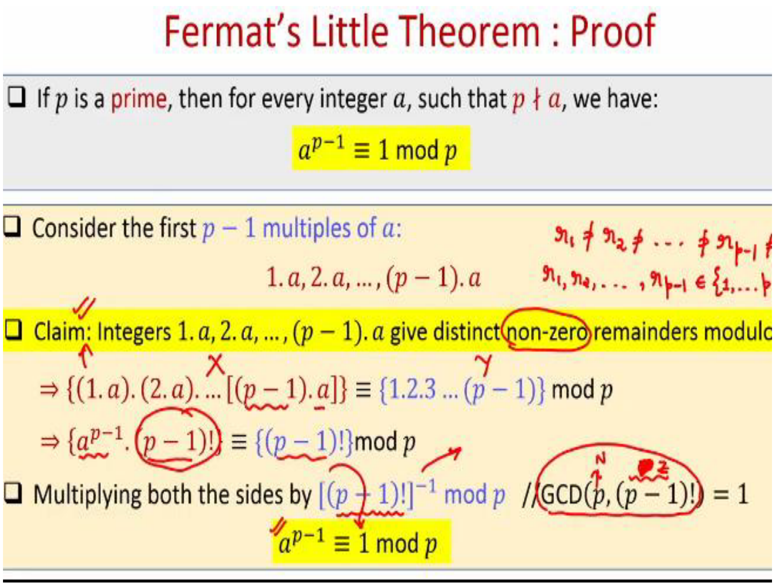
(r – s)), because as per the premise of my theorem statement GCD(p, a) is 1 as a is co-prime to p. So, this is the premise of my theorem statement you have a number p which is prime and p does not divide a that means the GCD (p, a) = 1.

So now, you can recall one of the properties of divisibility that we had discussed in earlier lecture. If p is a prime, which divides the product of 2 numbers and one of the numbers in a product is not divisible by the prime that means the other number has to be definitely divisible by the prime. So you have 2 numbers, A B, so you can imagine r - s as A and a as B. So, we have p divides the product of A and B, but p does not divide B. So that is possible only if p divides A, A is r - s.

So, we get the conclusion that p has to divide r - s or in other words, r and s are congruent modulo p. But if r and s are congruent modulo p and since both r and s are strictly less than p, then the only way it is possible that r is congruent to s modulo p is that r is exactly equal to s. Of course, if r and s would have been outside the range 1 to p - 1 then it might be possible that even though the value of r and value of s are different, but still they are congruent modulo p.

But remember that r and s are strictly less than p and if they are congruent modulo p, then that is possible only when r = s. So, we arrive at a contradiction because we assumed that r and s were different. So, r times a and s times a were different multiples and that means r was different from s that was our assumption, but we come to the conclusion that r = s. So, that means, whatever contrary statement we assumed is incorrect that means this claim is true so, we have proved this claim.

(Refer Slide Time: 08:58)



Fermat's Little Theorem : Proof

❑ If p is a prime, then for every integer a, such that $p \nmid a$, we have:

$$a^{p-1} \equiv 1 \bmod p$$

❑ Consider the first $p - 1$ multiples of a:

$$1.a, 2.a, \dots, (p-1).a$$

$r_1 \neq r_2 \neq \dots \neq r_{p-1} \neq$

$r_1, r_2, \dots, r_{p-1} \in \{1, \dots p$

❑ Claim: Integers $1.a, 2.a, \dots, (p-1).a$ give distinct non-zero remainders modulo

$$\Rightarrow \overset{X}{\{(1.a).(2.a)\dots[(p-1).a]\}} \equiv \overset{Y}{\{1.2.3\dots(p-1)\}} \bmod p$$

$$\Rightarrow \{a^{p-1}.(p-1)!\} \equiv \{(p-1)!\} \bmod p$$

❑ Multiplying both the sides by $[(p-1)!]^{-1} \bmod p$ // $\mathrm{GCD}(\overset{N}{p}, \overset{Z}{(p-1)!}) = 1$

$$a^{p-1} \equiv 1 \bmod p$$

Now, my claim is that if you multiply these p - 1 multiples of a, so, you have 1 time a, 2 times a, 3 times a, p - 1 times a if you multiply them you will get one number. If you divide that number by p you will get the same remainder which you will obtain if you multiply the numbers 1, 2, 3 up to p - 1 and then divide the resultant value by p. That means call the value on your left hand side as X, call the value on your right hand side is Y I am saying here that X ≡ Y.

And this follows from your claim that we had just proved this is because as per claim the various remainders which you obtained by dividing these p - 1 distinct multiples of a, call them as r_1, r_2, r_{p-1}, we have proved that all these remainders are non 0 and they are distinct. That is what the claim we have just proved and all these remainders r_1, r_2, r_{p-1} they are the remainders obtained by dividing a value by p.

So, the possible remainders that you can obtain could be 0 to p - 1. But 0 is not a possible remainder as per the claim statement we are not going to get a 0 remainder. That means the only remainders that I can obtain are 1 to p - 1 and at the same time, they are distinct. So that means definitely, out of this p - 1 remainders, one of the remainders is definitely 1, out of this p - 1 remainders that we are getting one of the remainders is definitely 2, out of this p - 1 remainders that we are getting one of the remainders is definitely p - 1.

So, that means, remember, the law of modular arithmetic says that if you want to multiply many numbers and then want to take modulo, you want to compute the remainder, then that is equivalent to saying that you reduce each of the numbers first modulo the same modulus and then multiply them. So I can say that the value of X modulo p will be the same as multiplying the remainders r_1, r_2, r_{p-1} and then taking modulo p.

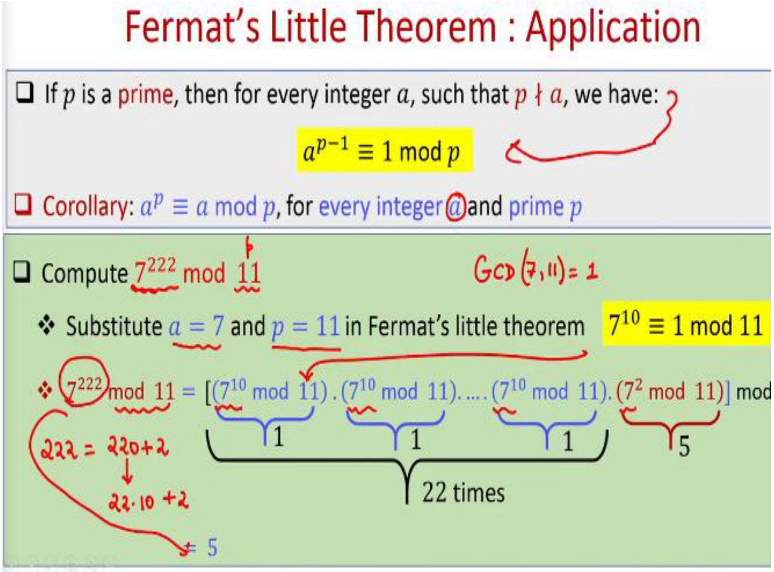
And I know that r_1, r_2, r_{p-1} are the values 1 to p - 1 in some order; r_1 may not be exactly 1, r_2 may not be exactly 2, r_{p-1} may not be exactly p - 1. But I know that the remainders 1 to p - 1 occurs exactly once among these p - 1 remainders. So that is why I can say that the product of these p - 1 remainders is congruent to the product of 1, 2, 3 up to p - 1 modulo p, which is Y.

So that means now I can say the following, so if you see the expression X the value a is appearing p - 1 times, so I can take out a^{p-1} outside. And then if I collect the product of 1, 2, up to p - 1, that will be (p – 1)!. Whereas in my right hand side, namely Y, I have (p – 1)!, because that is a product of 1, 2 up to p - 1. So that means I can say that a^{p-1} times (p – 1)! ≡ (p – 1)! modulo p.

Now, what I will do is the following, let me multiply both sides of this equation by the multiplicative inverse of (p – 1)! modulo p. Now, you might be wondering, what is the guarantee that the multiplicative inverse of (p – 1)! modulo p exists. So recall we discussed in one of our earlier lectures, that multiplicative inverse of a value modulo some modulus N exists if and only if that value is co-prime to the modulus. So that means (p – 1)! multiplicative inverse will exist only if this condition is true.

Because your modulus is p, and this is the value X, whose inverse you want to find out; let us not call it X, because I have already used X for something else so call this value as Z. So my claim is that this is the value Z which is (p – 1)! is indeed co-prime to n. And it is very simple to prove that I am not going to prove that for you I leave that as exercise for you. So, since the multiplicative inverse of (p – 1)! exist, if I multiply both sides by the multiplicative inverse of (p – 1)!, then this (p – 1)!, when multiplied by its multiplicative inverse will give me 1 and 1 multiplied by a^{p-1} will give me a^{p-1} in the left hand side whereas in the right hand side, when I multiply (p – 1)! with its multiplicative inverse, I get 1. So I get the conclusion that $a^{p-1} \equiv 1$ modulo p, which proves my Fermat's little theorem.

(Refer Slide Time: 14:50)



Fermat's Little Theorem : Application

❑ If p is a prime, then for every integer a, such that $p \nmid a$, we have:

$a^{p-1} \equiv 1 \bmod p$

❑ Corollary: $a^p \equiv a \bmod p$, for every integer a and prime p

❑ Compute $7^{222} \bmod \overset{p}{11}$ GCD(7, 11) = 1

❖ Substitute $a = 7$ and $p = 11$ in Fermat's little theorem $7^{10} \equiv 1 \bmod 11$

❖ $7^{222} \bmod 11 = [\underbrace{\underbrace{(7^{10} \bmod 11)}_{1} . \underbrace{(7^{10} \bmod 11)}_{1} \dots . \underbrace{(7^{10} \bmod 11)}_{1}}_{22 \text{ times}} . \underbrace{(7^2 \bmod 11)}_{5}] \bmod$

$222 = 220 + 2$

$\downarrow$

$22 \cdot 10 + 2$

$= 5$

So this is the Fermat's little theorem, which says that every integer a which is co-prime to p satisfies the condition that $a^{p - 1} \equiv 1$ modulo p. And I have a corollary of this theorem that you take any integer a which need not be co-prime to a, it satisfies the property that $a^p \equiv a$ modulo p. So, now let us see some of the applications of this theorem it has this Fermat's little theorem has got tremendous applications.

So let us see how exactly we can use this theorem to compute the value of some expressions modulo some modulus which is a prime number. So, your modulo modulus p here is prime and say I want to compute the value of 7^{222} modulo 11 of course, you can write down a computer program and compute the value of 7^{222} modulo 11. But I want to do it very quickly using my paper and pen and using Fermat's little theorem.

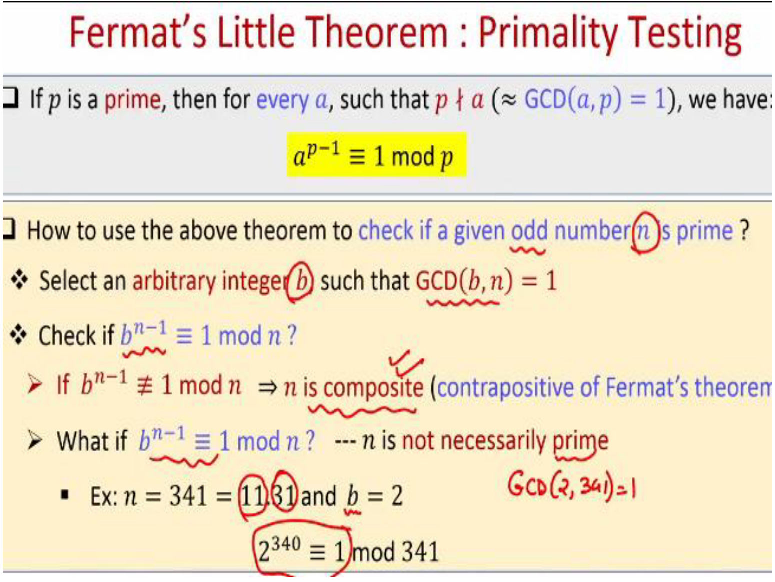
So what I can do here is the following, if I substitute a = 7 and p = 11 in Fermat's little theorem, then I see that the condition of the Fermat's little theorem is satisfied because indeed GCD(7, 11) is 1, namely 7 is co-prime to 11 because the GCD(7, 11) is 1 and hence, I can say that $7^{10} \equiv 1$ modulo 11 that means, if you divide 7^{10} by 11, you will get a remainder 1.

Now I can rewrite 7^{222} as follows, I can treat it as 7^{10} modulo 11 multiplied by 7^{10} modulo 11 multiplied by 7^{10} modulo 11 and then finally 7^2 modulo 11 and then everything modulo 11. So, basically what I am doing here is that 222 can be rewritten as 220 + 2 and now, this 220 can be written as 22 times 10 and then you have 2 anyhow, so this 7^{222} I have splitted it into many blocks of 7^{10}, 7^{10}, 7^{10} namely 22 blocks and then finally I will be left with 7^2.

And then since I have to do or I have to compute everything modulo 11 I can take modulo 11 with each block of 7^{10}. Again this comes from your rules of modular arithmetic. Now, I know that 7^{10} modulo 11 will give me 1 so, each block of 7^{10} modulo 11 will give me 1, 1, 1, 1, 1 that means I will get 1 multiplied with itself 22 times which will be giving me again 1 and then that will be multiplied with 7^2 modulo 11 and 7^2 modulo 11 is 5 and then I can say that 1 into 5 is 5, 5 modulo 11 is 5.

So, you can now see that I do not need to write any complicated program or I do not need to do any sophisticated computation I can simply apply the Fermat's little theorem and so conveniently I can compute the value of 7^{222} modulo 11.

(Refer Slide Time: 18:32)



Fermat's Little Theorem : Primality Testing

❑ If p is a prime, then for every a, such that $p \nmid a$ ($\approx \text{GCD}(a,p) = 1$), we have

$$a^{p-1} \equiv 1 \bmod p$$

❑ How to use the above theorem to check if a given odd number n is prime ?

❖ Select an arbitrary integer b such that $\text{GCD}(b,n) = 1$

❖ Check if $b^{n-1} \equiv 1 \bmod n$?

➢ If $b^{n-1} \not\equiv 1 \bmod n \Rightarrow n$ is composite ✓ (contrapositive of Fermat's theore

➢ What if $b^{n-1} \equiv 1 \bmod n$? --- n is not necessarily prime

▪ Ex: $n = 341 = 11 \cdot 31$ and $b = 2$ GCD(2, 341)=1

$2^{340} \equiv 1 \bmod 341$

Now, as I said at the beginning of the lecture Fermat's little theorem also forms the basis of very interesting primality testing algorithm. We would not be seeing the full primality testing algorithm, but we will see a part of it. So, this is the statement of the Fermat's little theorem, which says that if you have a number p which is prime and an integer a; if you have an integer a which is co-prime to p, then for every such integer a, the value of $a^{p - 1} \equiv 1$ modulo p.

So now the question is can I use the theorems statement to check whether a given number n is prime or not, of course, the number n has to be odd, because if I give you n = 2 you can easily verify, you can easily conclude that it is a prime number because that is the only even prime number. But other than that if at all n is a prime number it has to be odd. So now, you are given an odd prime number, it might be an arbitrary large prime number and you want to utilize Fermat's little theorem to verify whether the given number is prime or not.

So the idea here will be that I will pick some arbitrary integer b such that b is co-prime to n and then I will check whether $b^{n-1} \equiv 1$ modulo n or not, I do not know whether n is prime or composite, I have to check. So what I am saying is to verify whether the given n is prime, pick some random integer b, which is co-prime to n. And then check whether for the B that you have chosen $b^{n-1} \equiv 1$ modulo the given n. Now, you will get either the answer yes or no.

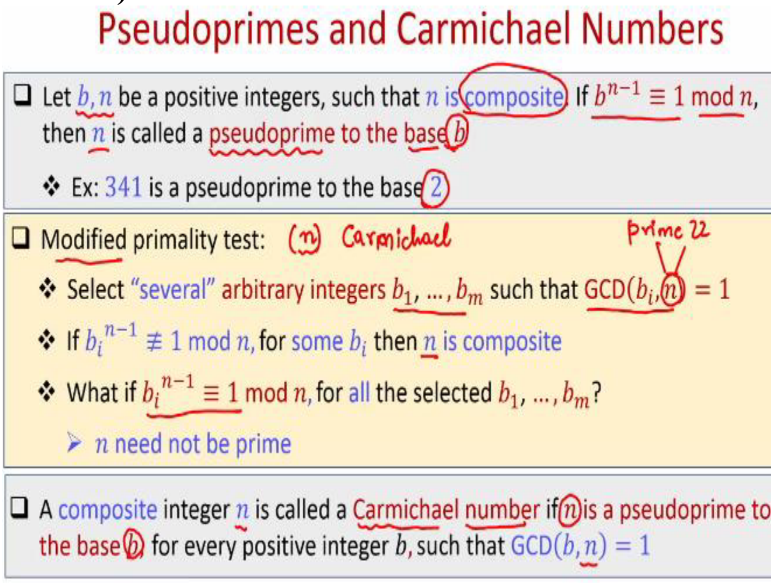
If you see that $b^{n-1} \not\equiv 1$ modulo and then you can simply declare that the given number n is composite, because that comes from the contrapositive of your Fermat's theorem. So the Fermat's theorem states that if you have a number a which is co-prime to p. And if p would have been prime, and a^{p-1} will give you 1 modulo p, so the contrapositive of that will be if you have a number a which is co-prime to p, and if $a^{p-1} \not\equiv 1$ modulo p, then that implies that p is not prime, even though a is co-prime to p, that is the contrapositive. And that is what precisely we are using here. But what if $b^{n-1} \equiv 1$ modulo n can I declare my n to be a prime number, that is the problem with this primality testing. Even if $b^{n-1} \equiv 1$ modulo the given n, you cannot necessarily declare your number n to be a prime number.

So here is a counter example, so imagine you are given n is 341, which is an odd number, and which is not a prime, it is a composite number because the number 341 has factors 11, 31. Now suppose when you run this primality testing algorithm, for n = 341, you pick your b to be 2. So indeed, GCD of 2 and 341 is 1. And it also turns out that for the given b that you have chosen arbitrarily, $b^{n-1} \equiv 1$ modulo the same n.

So even though this condition is true, the condition of Fermat's little theorem is true, you cannot declare your n to be prime because the value n = 341 is indeed composite. So that is why this primality testing algorithm is not a robust algorithm; robust in the sense, you cannot trust the answer. If the answer is composite yes you can trust it. But you cannot trust answer that n is prime. It may be the case that even though your value n is not a prime number, the condition for Fermat's little theorem is satisfied.

So now, you might be wondering that why cannot I do the following? It might be possible that I have chosen a bad b with respect to my given composite number n what if I choose a good b, which is coprime to n, and for which the Fermat's little theorem condition fails. In that case, I can declare that my n is not a prime number why cannot I do that.

(Refer Slide Time: 23:33)



Pseudoprimes and Carmichael Numbers

❑ Let b, n be a positive integers, such that n is composite. If $b^{n-1} \equiv 1 \bmod n$, then n is called a pseudoprime to the base b

❖ Ex: 341 is a pseudoprime to the base 2

❑ Modified primality test: (n) Carmichael

❖ Select "several" arbitrary integers $b_1, \dots, b_m$ such that $\mathrm{GCD}(b_i, \overset{\text{prime 22}}{n}) = 1$

❖ If $b_i^{n-1} \not\equiv 1 \bmod n$, for some b_i then n is composite

❖ What if $b_i^{n-1} \equiv 1 \bmod n$, for all the selected $b_1, \dots, b_m$?

➢ n need not be prime

❑ A composite integer n is called a Carmichael number if n is a pseudoprime to the base b for every positive integer b, such that $\mathrm{GCD}(b, n) = 1$

However, it turns out that even if you do so, your primality testing algorithm will fail because there are some very interesting numbers which are called as pseudo primes and Carmichael numbers, which will cause your primality testing algorithm to fail for the case when your n is composite, but you are not able to detect that. So let us first define pseudo primes and then we will use it to define Carmichael numbers. So, imagine you are given positive integers b and n and say your n is composite.

Now, if it turns out that $b^{n-1} \equiv 1$ modulo n, then I will call my n to be a pseudo prime to the base b. Why I am calling it pseudo prime, because it is a false prime. In the sense even though my n is composite, it satisfies the condition of Fermat's little theorem with respect to the integer b. That is why I am calling it base b because b is appearing in the base and n - 1 is appearing in the exponent.

So for instance, the counter example that we just saw in the previous slide shows us that a value n = 341 is a pseudo prime it is a false prime because it is actually a composite number, but still it satisfies the condition of your Fermat's little theorem with respect to your base b = 2. So, now as I said earlier, you might try to run the primality testing algorithm with respect to several bases for a given number n with a hope that indeed if your value n is composite you hit upon some base for which the condition or the conclusion of Fermat's little theorem is not satisfied. So, what we are doing here is we are now proposing a modified primality testing algorithm where instead of picking 1 base b, which we had done earlier. We are now randomly picking many bases say m number of bases b_1 to b_m each of which is co-prime to your given number n you want to check whether the number n is prime or composite.

And now, you check whether the condition of Fermat's little theorem holds for each of the b_i, and given n namely you check whether $b_1^{n-1} \equiv 1$ or not $b_2^{n-1} \equiv 1$ or not and $b_m^{n-1} \equiv 1$ or not. Even if for one of the basis b_i, the condition of the Fermat's little theorem does not hold, you can very confidently declare that your number n is composite.

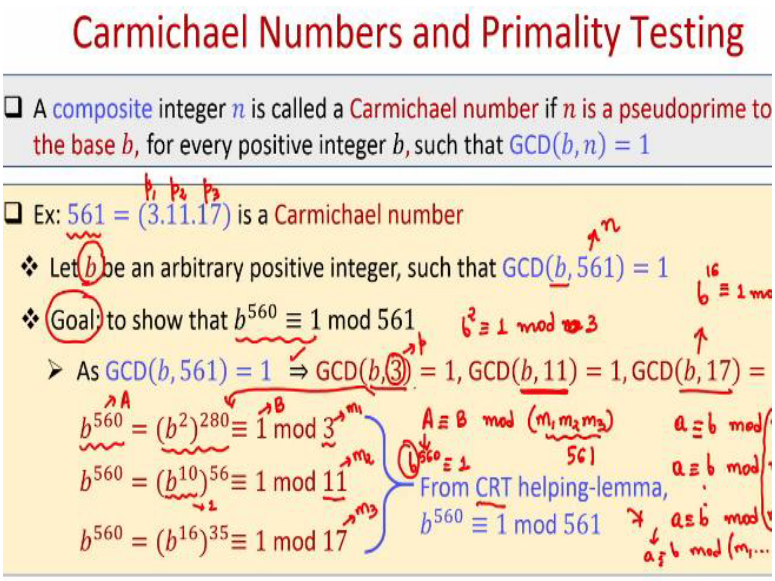
But what it so happened that for each of the m bases which you have randomly chosen, the condition of the Fermat's little theorem is satisfied, can you declare your given n to be a prime? Unfortunately, we cannot do that and there are some wonderful numbers very interesting numbers which are called as Carmichael numbers, which will actually cause your modified primality testing algorithm to fail.

So, what exactly are Carmichael numbers, so, they are composite numbers, which are pseudo primes with respect to every base that you can think of. So, you pick any base b or any integer b, which is co-prime to your number n still, the condition of Fermat's little theorem will be satisfied; that means $b^{n-1} \equiv 1$ modulo n, it does not matter whether your base b is b_1, b_2 you pick any base, that base power n - 1 will be congruent to 1 modulo n.

Namely, your n will be a pseudo prime with respect to every base that you can think of. So that tells you that if you now input a number n, which is a Carmichael number, then definitely this primality testing algorithm will fail because it does not matter how many bases you pick, each of them may be co-prime to your n fine, but still, this condition will hold. And then you will be in a dilemma whether I should safely declare n to be a prime or not.

If you declare n to be prime, then that is a false conclusion because actually your number n is composite. So that is why primality testing algorithm based on Fermat's little theorem is not a fool proof test. And we need to make additional tests in the modified primality testing algorithm to get a fool proof primality testing algorithm whose details I am not going to discuss.

(Refer Slide Time: 28:47)



Carmichael Numbers and Primality Testing

❑ A composite integer n is called a Carmichael number if n is a pseudoprime to the base b, for every positive integer b, such that $\mathrm{GCD}(b,n)=1$

❑ Ex: 561 = (3.11.17) is a Carmichael number

❖ Let b be an arbitrary positive integer, such that $\mathrm{GCD}(b,561)=1$

❖ Goal: to show that $b^{560} \equiv 1 \bmod 561$

➢ As $\mathrm{GCD}(b,561)=1 \Rightarrow \mathrm{GCD}(b,3)=1, \mathrm{GCD}(b,11)=1, \mathrm{GCD}(b,17)=$

$b^{560}=(b^{2})^{280}\equiv 1 \bmod 3$

$b^{560}=(b^{10})^{56}\equiv 1 \bmod 11$

$b^{560}=(b^{16})^{35}\equiv 1 \bmod 17$

From CRT helping-lemma, $b^{560}\equiv 1 \bmod 561$

So now, you might be wondering, do Carmichael numbers indeed exist? And if they exist, are they finite? Or are they infinite in number? So, indeed, it turns out that we have lots of Carmichael numbers. In fact, the study of Carmichael numbers itself is a very interesting research topic in number theory. So, let me give you an example of a Carmichael number. So, my claim is that 561 is a Carmichael number. So, you can see that 561 is not a prime number. Because I have written down its prime power factorization, namely, you have 3 factors p_1, p_2 and p_3 : (3, 11, 17) for the value n = 561. Now, I want to prove that the value 561 is indeed a Carmichael number for that I have to prove that it is a pseudo prime with respect to every base, you take, think of any base b, which is co-prime to your n. I will show that $b^{n-1} \equiv 1$. So that is this is my goal I am not focusing on the value of the base b, the only thing that I know is that it is co-prime to your n namely 561.

So, how do I prove that b^{560} will be indeed 1 so, since I know that the GCD of b and 561 is 1, I can imply that individually b is co-prime to each of the prime factors of my n. So, b will be co-prime to 3, b will be co-prime to 11 and b will be co-prime to 17 it is very easy to prove this implication, because, if any of these implications is false say for instance, if GCD of b and 3 is not 1 that means, there is some common factor for b as well as 3.

So, then I can come to a contradiction that GCD of b and 561 is not 1, that is as simple as that. Now, since b is co-prime to 3, b is co-prime to 11 and b is co-prime to 17 I can do the following: I can rewrite b^{560} and my goal was to show that $b^{560} \equiv 1$, so b^{560} I can rewrite as b^2 and then whole raise to power 280 and $b^{560} \equiv 1$ modulo 3 why so?

Because b^{560} modulo 3 is same as b^2 whole raise to power 280 modulo 3, but I know that since b is co-prime to 3, I can apply the condition of Fermat's little theorem, so, I have I can treat 3 to be my prime p and I can treat b to be a number which is co-prime to 3. So, that gives me that $b^{3 - 1}$ namely $b^2 \equiv 1$ modulo 3. So, now if b^2 gives me the remainder 1 modulo 3, then b^{560} will give me this much remainder.

So, I have basically divided b^{560} into several blocks of b^2, b^2, b^2 namely 280 blocks and each block of b^2 gives me the remainder 1 modulo 3. So, basically, I get 1 multiplied to itself 280 times which will be 1 modulo 3. In the same way $b^{560} \equiv 1$ modulo 11 and this is again because 11 is a prime number and b is co-prime to 11.

So, I can say that from Fermat's little theorem $b^{11 - 1}$ which is $b^{10} \equiv 1$ modulo 11 and hence b^{560} can be rewritten as 56 blocks of b^{10} modulo 11 each block of b^{10} modulo 11 will give me 1 as the remainder and 1 multiplied to itself 56 times will give me the remainder 1 and in the same way $b^{560} \equiv 1$ modulo 17.

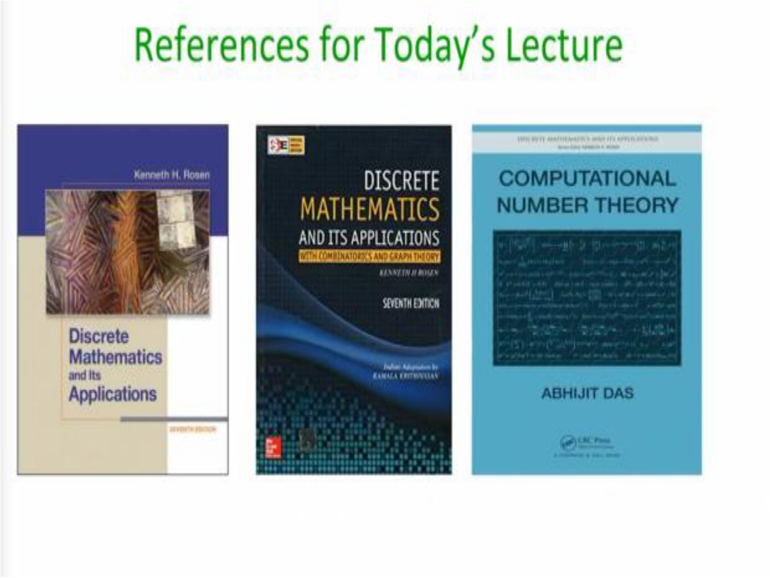
Because again I can apply the Fermat's little theorem here 17 is a prime number b is co-prime to 17. So, from Fermat's little theorem $b^{17 - 1}$ namely b^{16} will be co-prime to 1 modulo 17. So, I can rewrite b^{560} as 35 blocks of b^{16} modulo 17 each block of b^{16} modulo 17 will give me remainder 1 and hence I will get 1 multiplied to itself 35 times which will give me the remainder 17.

So that means $b^{560} \equiv 1$ modulo 3, $b^{560} \equiv 1$ modulo 11 and $b^{560} \equiv 1$ modulo 17. So recall the CRT helping lemma so let me rewrite the CRT helping lemma so there you had n modulus. Where n number of modulus, which are pairwise co-prime, and you have 2 values a and b, which are congruent to each other, with respect to all the modulus, so you have $a \equiv b$ modulo m_1, $a \equiv b$ modulo m_2 and like that, $a \equiv b$ modulo m_n.

And it is given that all these n modulus, they are pairwise co-prime, then the conclusion is that $a \equiv b$ even modulo the bigger modulus, which is the product of all the individual modulus so, that was the CRT helping lemma. So, now I can treat my A to be b^{560} I can treat my B to be 1 and I have 3 modulus here, m_1 being 3, m_2 being 11 and m_3 being 17.

So, A ≡ B modulo m_1, A ≡ B modulo m_2, A ≡ B modulo m_3 and hence, I can say that A ≡ B modulo the product of m_1, m_2, m_3. The product of m_1, m_2, m_3 is nothing but 561. A is anyhow b^{560} and B is 1. So, I have shown that b^{560} ≡ 1 modulo 561 without even knowing the value of b, so, b was an arbitrarily chosen base such that it was co-prime to your number n. So, that shows that the value 561 is indeed a Carmichael number.

(Refer Slide Time: 36:27)



References for Today's Lecture

Kenneth H. Rosen
Discrete Mathematics and Its Applications
SEVENTH EDITION
DISCRETE MATHEMATICS AND ITS APPLICATIONS
WITH COMBINATORICS AND GRAPH THEORY
KENNETH H ROSEN
SEVENTH EDITION
COMPUTATIONAL NUMBER THEORY
ABHIJIT DAS
CRC Press

So, that brings me to the end of today's lecture and with that I also finish my discussion regarding the number theory. As I said earlier, that number theory in itself is a very interesting subject and we can have a full-fledged course just on number theory. But we want to get just a flavour of number theory that is required in the context of discrete maths and computer science. Thank you.