

NPTEL

**NATIONAL PROGRAMME ON
TECHNOLOGY ENHANCED LEARNING**

IIT BOMBAY

**CDEEP
IIT BOMBAY**

**Quantum Information and
Computing**

**Prof. D.K.Ghosh
Department of Physics IIT Bombay**

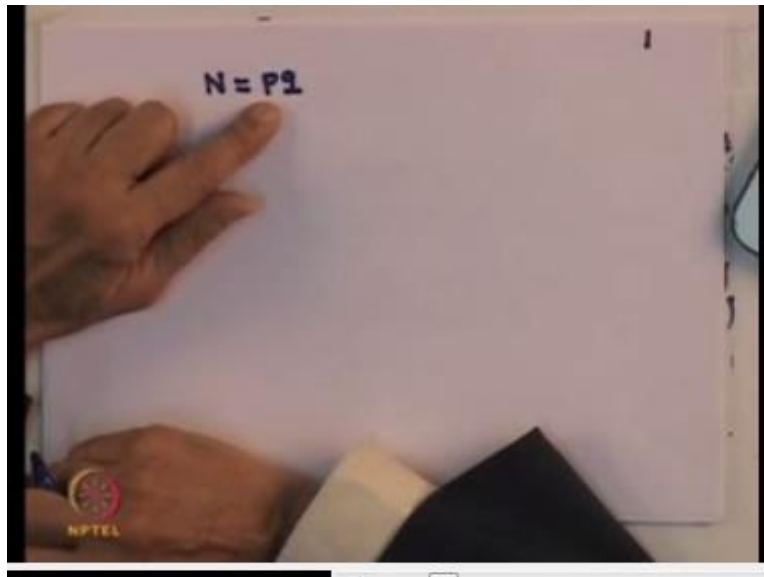
Modul No.05

Lecture No.27

Shor's Factorization Algorithm

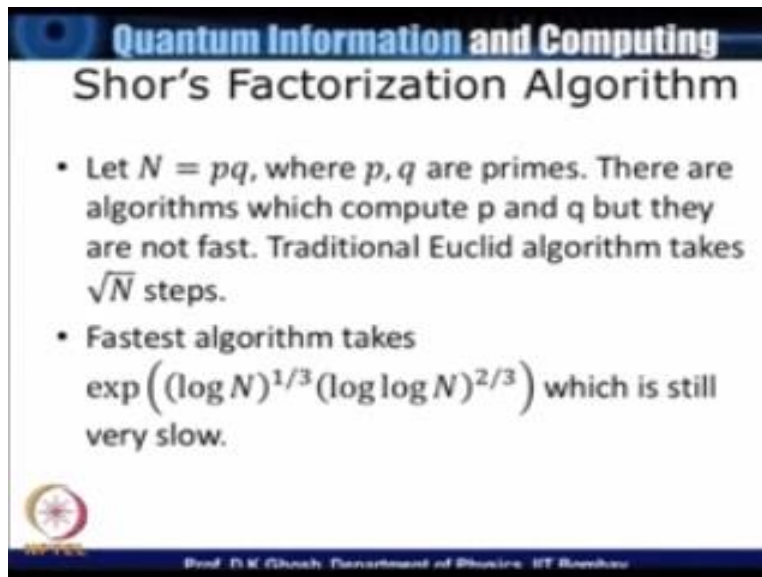
In the last lecture we had talked about the implementation of quantum Fourier transform we discussed in detail what happens to one, two and three qubit cases and then pointed out in principle one could extend it to n qubits. These were components that we require for implementing what is known as Shor's factorizing algorithm. But before I go to Shor's factorization algorithm, let me point out a few things regarding the factorization and its status with respect to classical algorithm.

(Refer Slide Time: 01:03)




So I am going to be concentrating on a situation in which I have a number n which is product of two large primes, of course in this lecture for the purpose of illustration I will not be able to take P and Q very large I will necessarily take small values but that is only to illustrate the principle they power of quantum computation lies in the fact that the algorithm that I will be discussing is applicable for large p and q . Now there are in principle algorithms which can compute the factors of a large composite number or of a composite number.

(Refer Slide Time: 01:53)



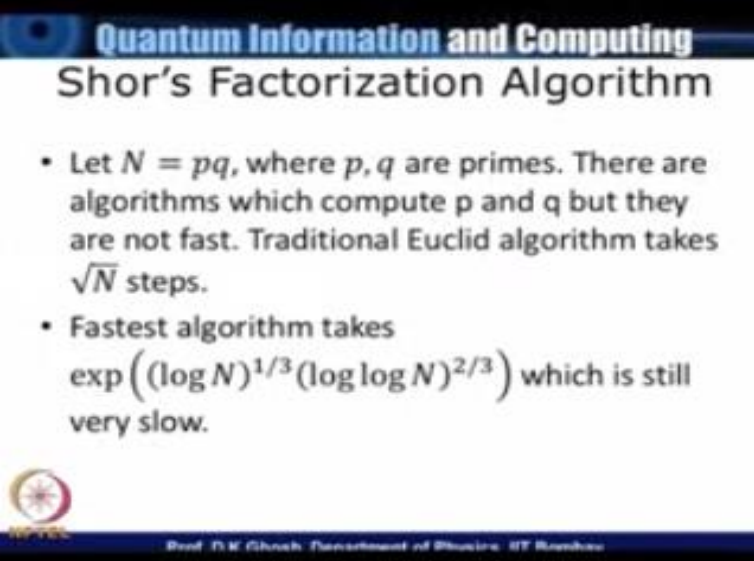
Quantum Information and Computing
Shor's Factorization Algorithm

- Let $N = pq$, where p, q are primes. There are algorithms which compute p and q but they are not fast. Traditional Euclid algorithm takes \sqrt{N} steps.
- Fastest algorithm takes $\exp\left((\log N)^{1/3}(\log \log N)^{2/3}\right)$ which is still very slow.


Prof. D.K. Ghosh, Department of Electrical Engineering, IIT Bombay


One of the algorithms is the Euclid algorithm basically it takes about \sqrt{N} steps and you can see why because if you are given a number of which there is a factor that factor has to remain less than \sqrt{N} one factor below \sqrt{N} and the other factor above \sqrt{N} is the simplest way of understanding it. The, there are many other algorithm Euclid is not particularly suitable for large numbers. So there are better algorithms much faster algorithms but if you look at.

(Refer Slide Time: 02:37)



Quantum Information and Computing
Shor's Factorization Algorithm

- Let $N = pq$, where p, q are primes. There are algorithms which compute p and q but they are not fast. Traditional Euclid algorithm takes \sqrt{N} steps.
- Fastest algorithm takes $\exp\left((\log N)^{1/3}(\log \log N)^{2/3}\right)$ which is still very slow.



Prof. D.K. Ghosh, Department of Physics, IIT Bombay

The fastest algorithm that is there you find that it takes this complicated expression that I have given on the slide exponential of $((\log N)^{1/3} (\log \log N)^{1/3})$ not important how it came but this is still very slow. The point to realize is that multiplication is a fast program.

(Refer Slide Time: 03:07)

Quantum Information and Computing

Euclid Algorithm

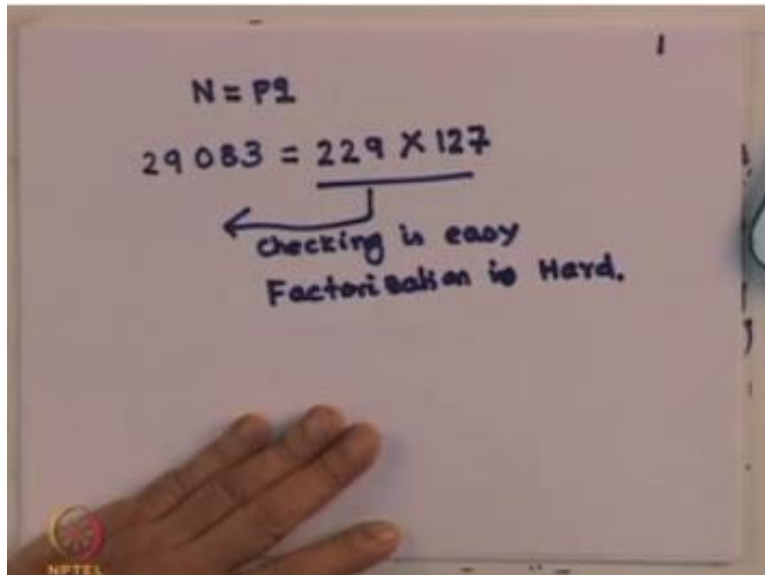
- Let $a = bq - r$. Find c such that c divides a and b . Let $a = mc$ $b = nc$.
- $r = a - bq = (m - nq)c$ so that c divides r

$$q_1 = \left\lfloor \frac{a}{b} \right\rfloor \quad r_1 = a - bq_1$$
$$q_2 = \left\lfloor \frac{b}{r_1} \right\rfloor \quad r_2 = b - q_2r_1$$
$$q_3 = \left\lfloor \frac{r_1}{r_2} \right\rfloor \quad r_3 = r_1 - q_3r_2$$

Prof. D.K. Ghosh, Department of Physics, IIT Bombay

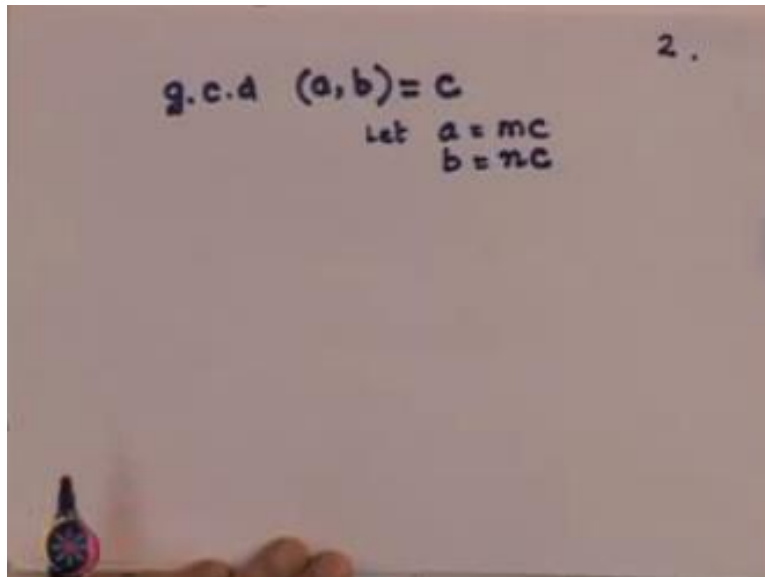
So just to give you an idea that supposing I ask you find the factors of a number like 29083 you can use Euclid or any other algorithm that you want and you will take about a couple of hours if you are using some of these things using current consider at least you will take of your hours.

(Refer Slide Time: 04:06)



However if I tell you that this number is essentially 229×127 back checking it checking is easy factorization is hard. So before I bring in Shor's algorithm let me tell you how this Euclid algorithm works. So basically what we will do in case of a Euclid algorithm is the following, suppose I have two numbers A and B and I am supposed to find.

(Refer Slide Time: 04:32)



The greatest common divisor of A and B and let it be equal to some number c, by definition then c divides both A and B. So let a be written as mc and B be written as nc, where m and n are integers. Now notice one thing that suppose I divide a/b now if I divide a/b unless be happens to be a factor of a, a long division will leave a remainder.

(Refer Slide Time: 05:16)

Handwritten mathematical derivation on a whiteboard:

$$\begin{aligned} \text{g.c.d } (a, b) &= c && 2. \\ \text{let } a &= mc && b < a. \\ & && b = nc \\ r &= a - bq && : c \text{ divides } r \\ &= (m - nq)c \end{aligned}$$

So let me say that this remainder is $a - bq$ smaller one of the 2, so $b < a$. Now one can easily show that c divides r this is the remainder. The reason is very simple see you can write this as $mc - nq$ multiplied this, so c divides r , so what is done in Euclid algorithm is the following. You start with a long division of a / b .

(Refer Slide Time: 06:08)

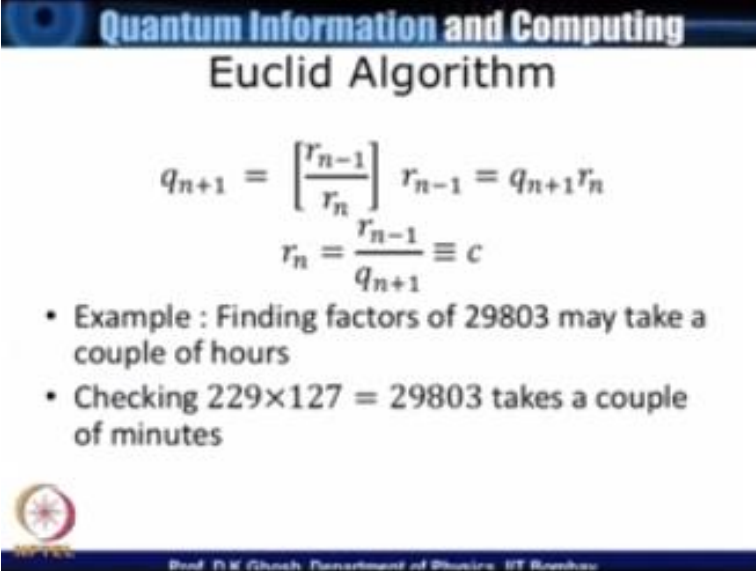
$$\begin{array}{l}
 \text{g.c.d } (a, b) = c \\
 \text{let } a = mc \quad b < a \\
 \quad \quad \quad b = nc \\
 r = a - bq \quad : \quad c \text{ divides } r \\
 \quad \quad \quad = (m - nq)c \\
 \begin{array}{l}
 q_1 = \left[\frac{a}{b} \right] \\
 q_2 = \left[\frac{b}{r_1} \right] \\
 q_3 = \left[\frac{r_1}{r_2} \right]
 \end{array}
 \quad
 \begin{array}{l}
 r_1 = a - bq_1 \\
 r_2 = b - q_2 r_1 \\
 r_3 : \quad q_{n+1} = \frac{r_{n-1}}{r_n} \\
 \quad \quad r_n = c
 \end{array}
 \end{array}$$

$$\begin{array}{r}
 24 \overline{) 75} \\
 \underline{72} \\
 3 \\
 \underline{24} \\
 3 \\
 \underline{24} \\
 0
 \end{array}$$

Let it be equal to q_1 and let there be a remainder which is $a - bq$, let me just simply take the following. Supposing I have a number which let us say is 75 and let me say $b=24$, so what I have done actually is this, this of course will complete in essentially one or two steps. So this is my q so that is 72 and I am left with 3 as the remainder. At that stage what I do is i divide b by your remainder of the first part this was my remainder and this will have a remainder which is $b - q_2 r_1$ so now I what is I do this division is now carried as this remainder as the divisor and the previous divisor as the dividend.

So it is 3×8 is 24 and you carry on this task till situation of this type this is r_1 by r_2 extra, extra you go you have a r_3 there which I will not write down and finally you say $q_{n+1} = r_{n-1} / r_n$ and let us suppose this completes the division that is there are no remainders left. And so then my r_n becomes equal to C and this is the way Euclid's algorithm works. It is a decent algorithm to work with reasonably small numbers, but is no good if you take up very, very large numbers. So let us look at how do we handle the situation here.


(Refer Slide Time: 08:31)



Quantum Information and Computing
Euclid Algorithm

$$q_{n+1} = \left[\frac{r_{n-1}}{r_n} \right] \quad r_{n-1} = q_{n+1}r_n$$
$$r_n = \frac{r_{n-1}}{q_{n+1}} \equiv c$$

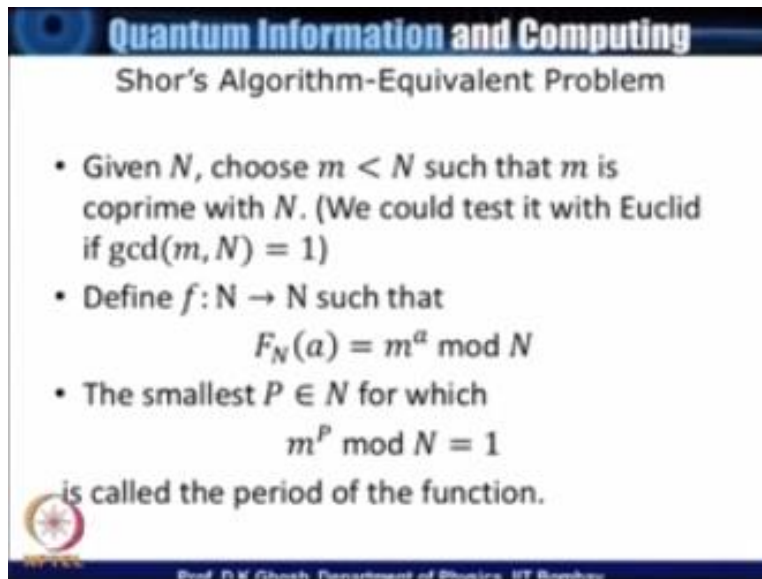
- Example : Finding factors of 29803 may take a couple of hours
- Checking $229 \times 127 = 29803$ takes a couple of minutes



Prof. D.K. Ghosh, Department of Physics, IIT Bombay

So I gave you that 29803 as an example which is what is listed in this thing.


(Refer Slide Time: 08:40)



Quantum Information and Computing

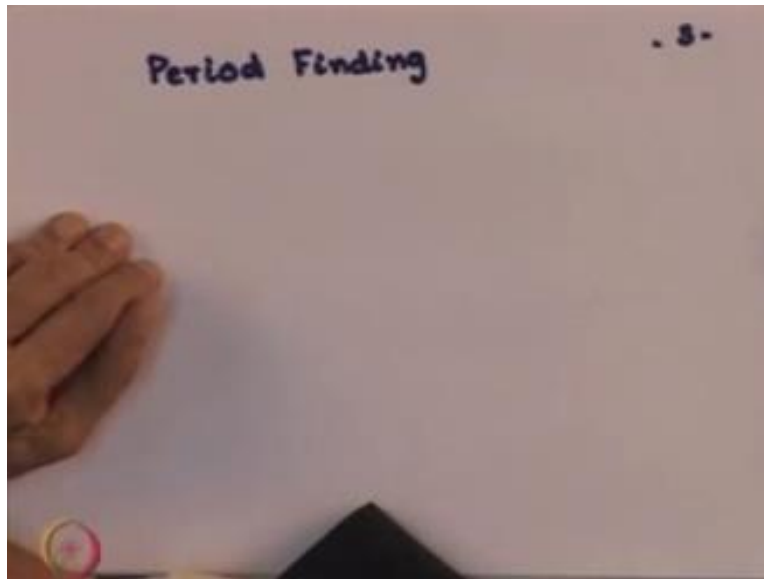
Shor's Algorithm-Equivalent Problem

- Given N , choose $m < N$ such that m is coprime with N . (We could test it with Euclid if $\gcd(m, N) = 1$)
- Define $f: \mathbb{N} \rightarrow \mathbb{N}$ such that
$$F_N(a) = m^a \bmod N$$
- The smallest $P \in \mathbb{N}$ for which
$$m^P \bmod N = 1$$
is called the period of the function.

 Prof. D.K. Ghosh, Department of Physics, IIT Bombay

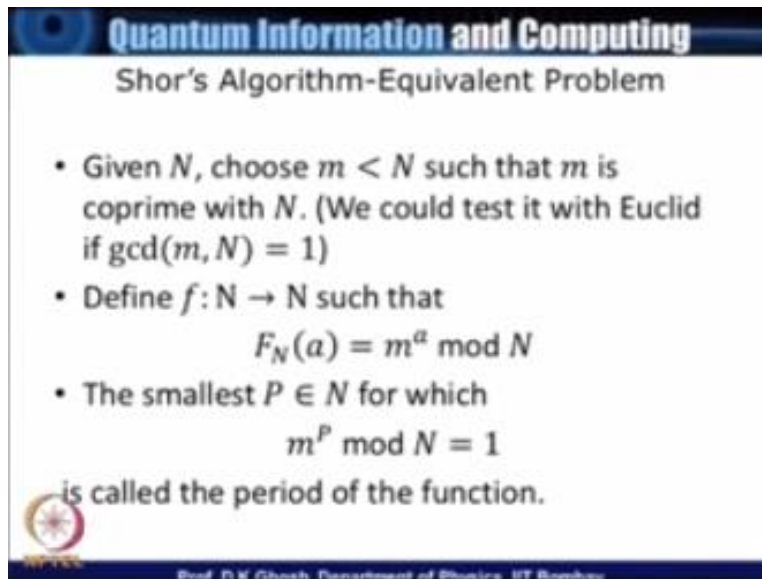
In order to use this algorithm Shor's suggested that you solve an equivalent problem, and this equivalent problem is called period finding.

(Refer Slide Time: 08:59)



You might recollect that we have mentioned about finding periods and its connection with the Fourier transform.


(Refer Slide Time: 09:10)



Quantum Information and Computing

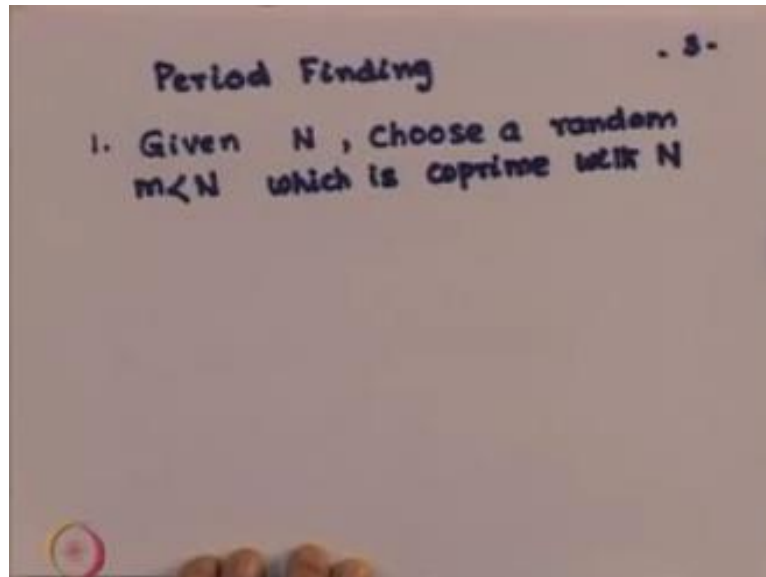
Shor's Algorithm-Equivalent Problem

- Given N , choose $m < N$ such that m is coprime with N . (We could test it with Euclid if $\gcd(m, N) = 1$)
- Define $f: \mathbb{N} \rightarrow \mathbb{N}$ such that
$$F_N(a) = m^a \bmod N$$
- The smallest $P \in \mathbb{N}$ for which
$$m^P \bmod N = 1$$
is called the period of the function.

 Prof. D.K. Ghosh, Department of Physics, IIT Bombay

So what we will do is this the first step in Shor's algorithm.

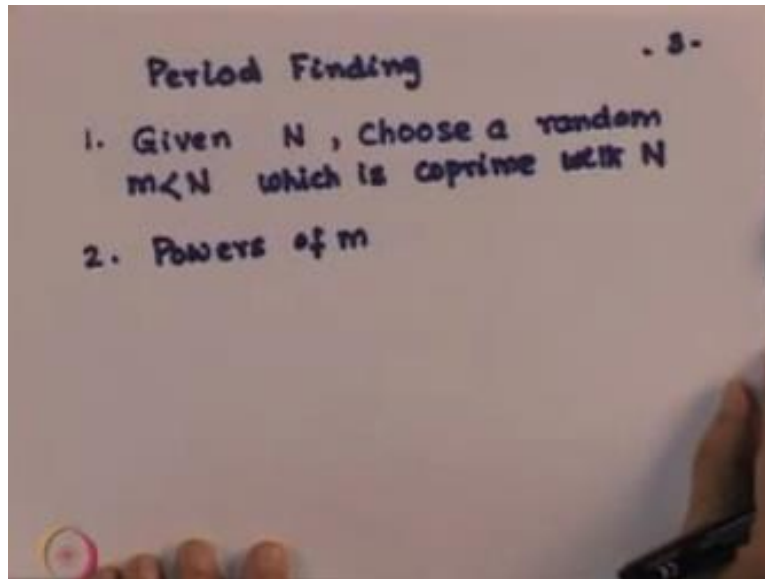
(Refer Slide Time: 09:18)



Is given a N choose a random number m which is less than N which is coprime with N , let me explain what is meant by that, pure numbers are said to be coprimes if they have no common factor among themselves and you are simply choosing a random number and it is they are very easy using you click type of algorithm to find out whether the m that you have chosen is a factor of N or not.

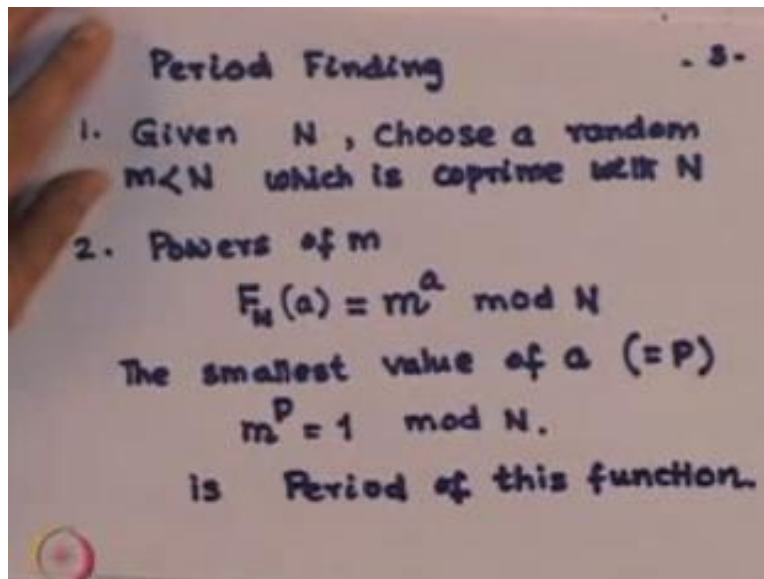
So if there is if they have a common factor that is, that is very easy because it is a matter of checking. Now what you do is that corresponding to this m .

(Refer Slide Time: 10:28)



We will try to find out the various powers of N , let me define a function with reference to the slide.

(Refer Slide Time: 10:46)




So I define a function $f_N(a)$ this is that $m^a \pmod{N}$ m is that random number that I chose which was coprime with N modulus N these are all discrete mathematics so you, we are talking about modular explanation session. Now the smallest p , the smallest value of a , let us call it P for which $m^P = 1 \pmod{N}$ this is called period of this function that I have defined. I just give you numerical example of how it works.

(Refer Slide Time: 12:06)

Quantum Information and Computing

Shor's Algorithm-Equivalent Problem

- Given N , choose $m < N$ such that m is coprime with N . (We could test it with Euclid if $\gcd(m, N) = 1$)
- Define $f: \mathbb{N} \rightarrow \mathbb{N}$ such that
$$F_N(a) = m^a \bmod N$$
- The smallest $P \in \mathbb{N}$ for which
$$m^P \bmod N = 1$$
is called the period of the function.



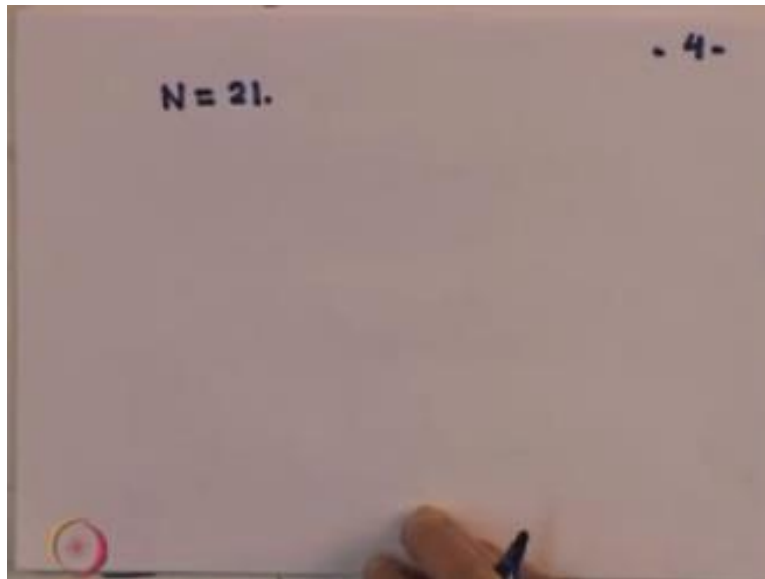
Prof. D.K. Ghosh, Department of Physics, IIT Bombay

(Refer Slide Time: 12:10)



Let me take a very simple number as I said many of my illustrations will be trivial illustrations but that helps in establishing the principle that I am talking about. So we will do let me take $N=21$.

(Refer Slide Time: 12:29)



If we take $N=21$ of course you will say that I know it is 3×7 , but then I am not going to be using a quantum computer to find out the factors of 21,55 extra. But this is to illustrate it, now let me choose.

(Refer Slide Time: 12:50)

The image shows a whiteboard with handwritten mathematical work. At the top right, there is a small number '- 4 -'. Below it, the text reads 'N = 21.' followed by 'Choose m = 2'. The next line shows a sequence of powers of 2: '2, 2^2 = 4, 2^3 = 8, 2^4 = 16, 2^5 = 32 = 11 mod 21'. The following line shows '2^6 = 64 = 1 mod 21'. An arrow points from this line down to the word 'Period.' and the equation 'P = 6'.

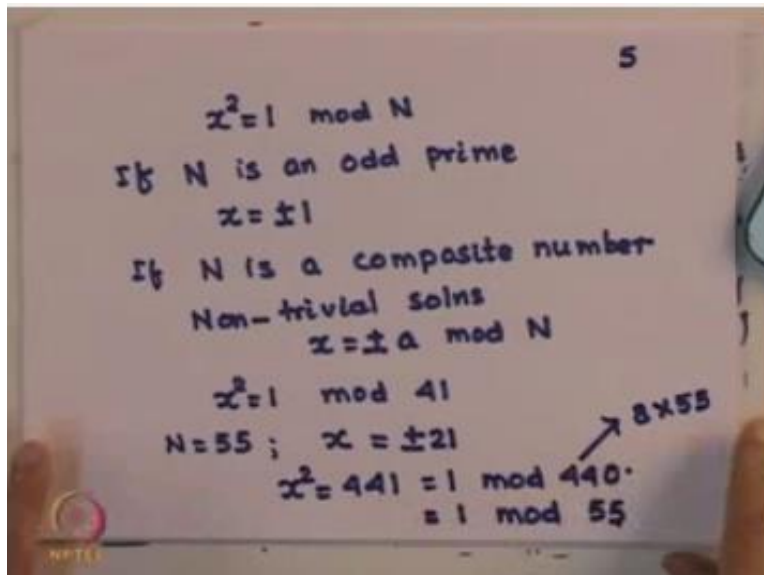
A random m as I said, but let me choose $m=2$ how do I go ahead and find the period, so I find various powers of 2 so I get to 2, 2^2 which is equal to 4, 2^3 which is 8, 2^4 is 16, 2^5 is already exceeded 21, 32 but that is equal to $11 \pmod{21}$, 2^6 is 64 which is $1 \pmod{21}$, because 64 is $63+1$ so therefore, this defines my period. So choosing $m=2$, for $N=21$ I find the period P to be equal to 6. What is one thing any of these numbers for example I have chosen 2.

(Refer Slide Time: 14:06)

$N = 21.$
Choose $m = 2$
 $2, 2^2 = 4, 2^3 = 8, 2^4 = 16, 2^5 = 32 =$
 $2^6 = 64 = 1 \pmod{21}$
↙ Period. $P = 6$
 $m \in \{2, 4, 8, 8, 10, 11, 13, 16, 17,$

m could belong to anyone of these sets i could choose 4 5 6 i cannot because it has a common factor 7 i cannot because 7×3 is 21 8 10 11 13 16 17 19 and 20 you could choose any one of these and calculate the powers now what is the relationship of this power calculation with factor now in order to be that I will need some elementary result from discrete algebra i will not be proving all of them but the groups are available in any standard textbook but i will be sort of illustrating now consider a quadratic equation for instance.

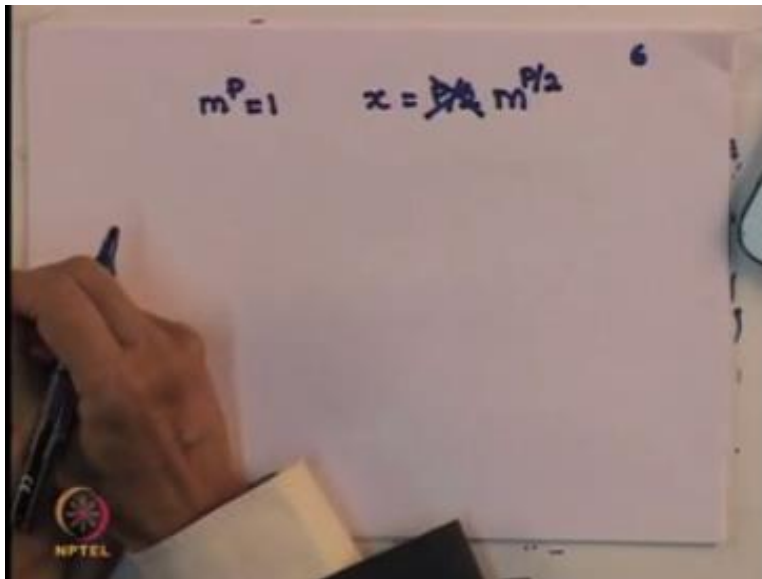
(Refer Slide Time: 15:16)



$x^2 = 1 \pmod{N}$ now if N is a prime I should more appropriately say if m is an odd prime then one can show that this equation has only trivial solutions that is $x = +$ or $- 1$ on the other hand if n happens to be a composite number then in addition to the trivial solutions there are also non-trivial solutions of the problem pair of non-trivial solutions for instance x could be some $+$ or $- a$ remember these are modular arithmetic so when I say something is $+$ or $- a$ it means it is that quantity $+ a$ times number n to illustrate what I mean by this statement let us consider the following consider the solution.

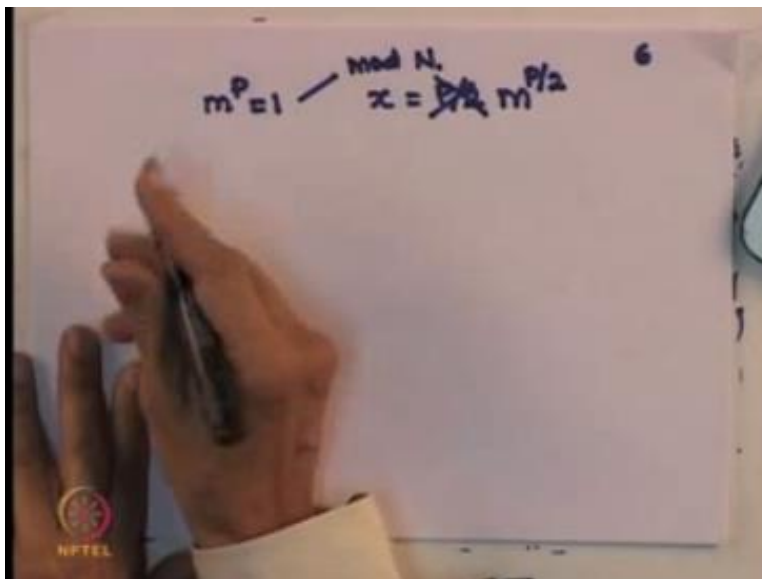
Of $x^2 = 1 \pmod{41}$ this equation only has trivial solution and the reason is that 41 is a prime number or prime number but on the other hand consider 55 let $N = 55$ then I came that because 55 is a composite number the equation $x^2 = 1 \pmod{55}$ has in addition to the trivial solution has a pair of non-trivial solutions and these you can easily calculate because I claim that x equal to $+$ or $- 21$ are solutions now you can see y because if $x = +$ or $- 21$ $x^2 = 441$, 21 square is that which is $= 1 \pmod{440}$ recall 440 is eight times 55 so therefore this is also $= 1 \pmod{55}$ what is the connection of this theorem with whatever we are doing so we said we have chosen $m^P = 1$.

(Refer Slide Time: 18:16)



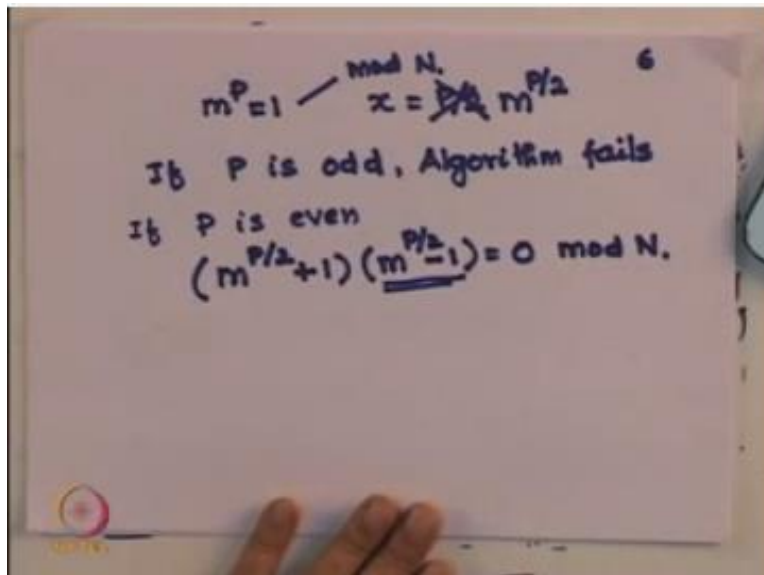
So that tells me that if I choose $x = P/2$ sorry $x = m^{p/2}$ then this equation gets converted to an $x^2 = 1$ equation mod N of course.

(Refer Slide Time: 18:45)



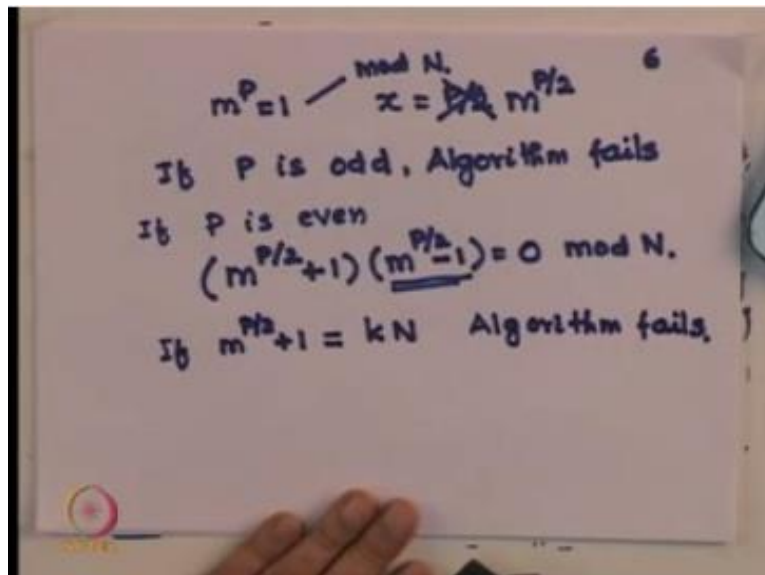
Now obviously in order that I can do that my p has to be even so one of the requirements of Shor's algorithm is P better be even.

(Refer Slide Time: 19:04)



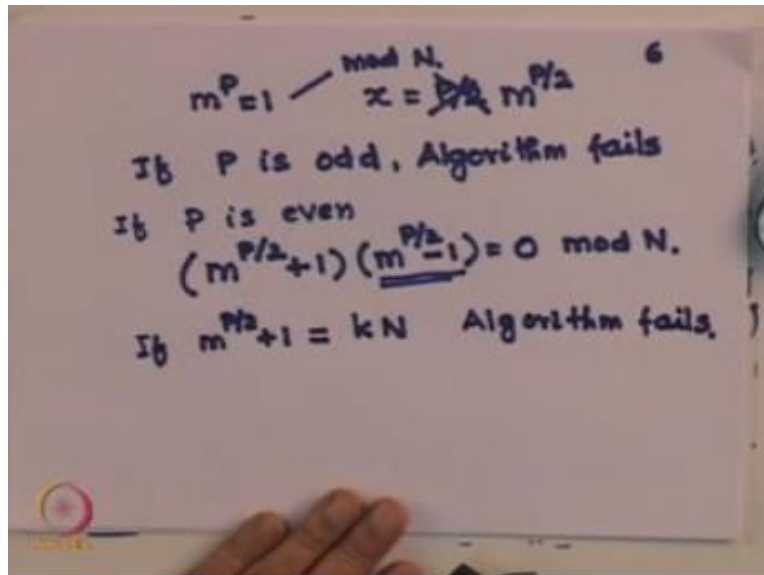
If P is odd the algorithm fails and what we do in that case just go back choose the different m and carry on again until you are successful now if P is even I write this equation as $m^{p/2} + 1$ I just factorize it $m^{p/2} + 1 \times m^{p/2} - 1 = 0 \pmod N$ he now this, this include this is $\equiv 0 \pmod N$ now remember that this is discrete mathematics so when something is $0 \pmod N$ it does not mean it is $= 0$ per se it simply means it is $0 + \text{sometimes } n$ but you see this cannot be $0 \pmod N$ that is because of our definition of the period we said period p is the smallest integer for which $m^p = 1$ so therefore i cannot have.

(Refer Slide Time: 20:33)



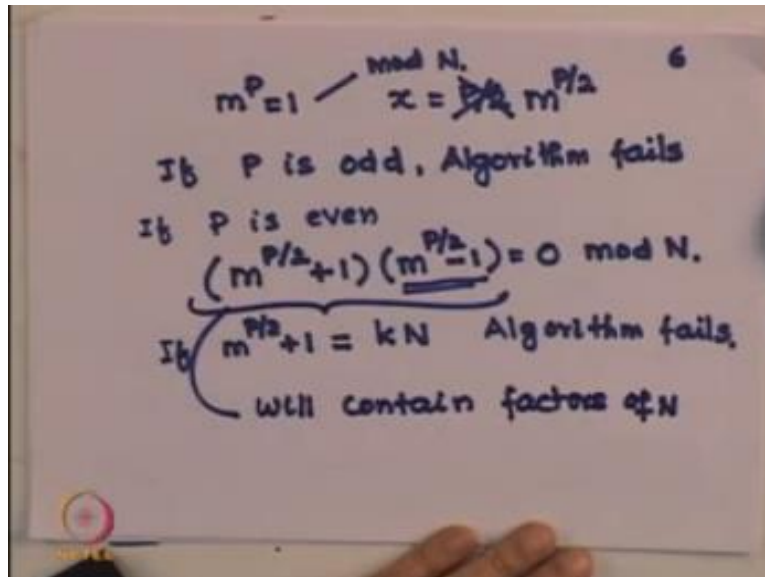
$p/2$ also satisfying this equation so this is not possible now the other possibility is $m^{p/2} + 1$ is 0 mod N which means $m^{p/2} + 1$ is some K times N now that happens also the algorithm fails so let me write it down if this happens algorithm fails. Now that happens also the algorithm fails so let me write it down if this happens algorithm fails.

(Refer Slide Time: 21:10)



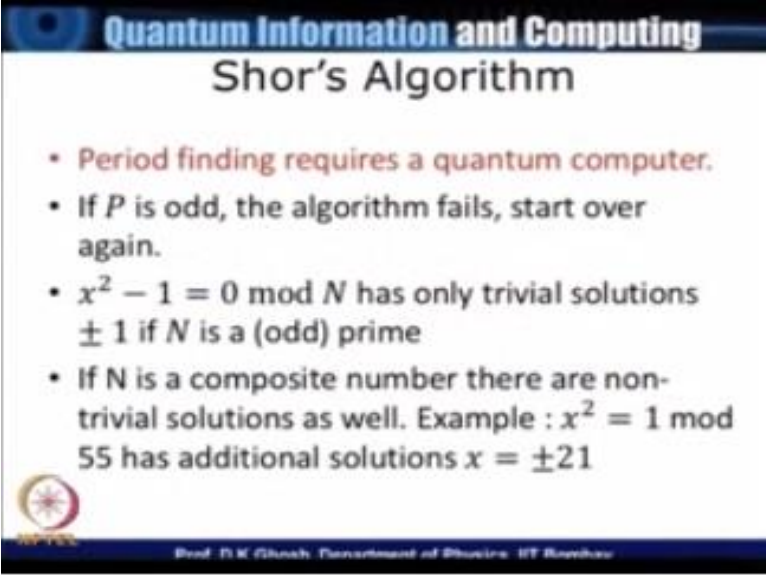
However if $M^{p/2+1}$ is not equal to 0 module then I can proceed with whatever we are doing and it has been shown that the probability of these two things that are happening what are the two things one is that the period for a random number be even and second one is that once it is even $M^{p/2+1}$ being not equal to 0 mod M has reasonably high probability for product of two prime number this can be shown to be greater than half but I will not go through the probability calculations. But suppose these two things are satisfied.

(Refer Slide Time: 22:12)




Then how can I satisfy this equation the only way I can satisfy this equation is that this and this contain factors of n . So this is where the situation lies that is if this then will contain factors of M , slide shows the summary.

(Refer Slide Time: 22:52)



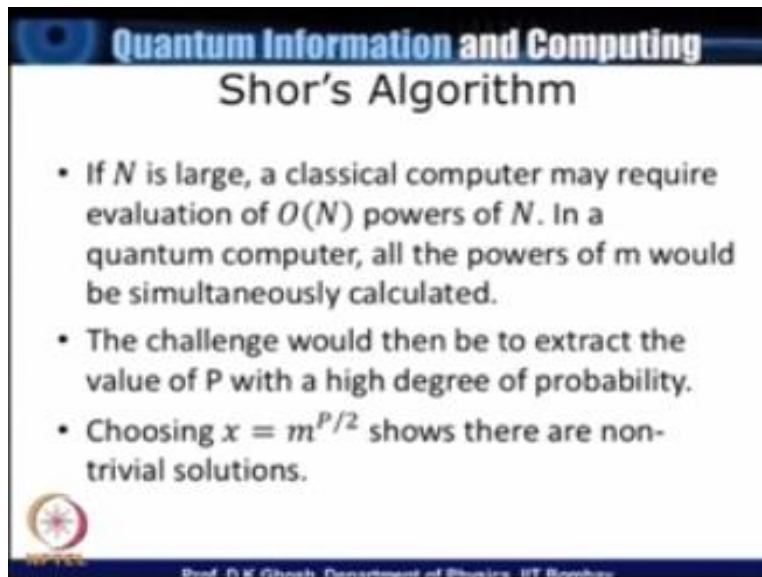
Quantum Information and Computing
Shor's Algorithm

- Period finding requires a quantum computer.
- If P is odd, the algorithm fails, start over again.
- $x^2 - 1 = 0 \pmod{N}$ has only trivial solutions ± 1 if N is a (odd) prime
- If N is a composite number there are non-trivial solutions as well. Example : $x^2 = 1 \pmod{55}$ has additional solutions $x = \pm 21$




Prof. D. K. Ghosh, Department of Business IT, IIT Bombay

(Refer Slide Time: 22:53)



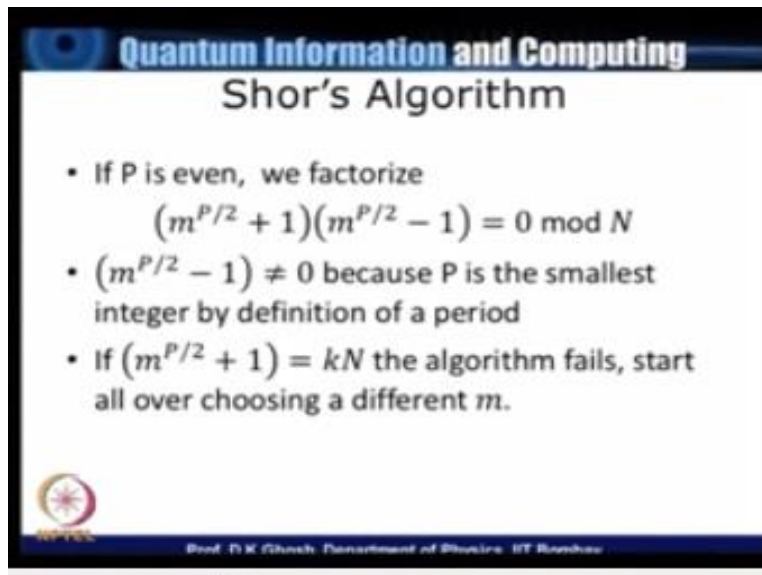
Quantum Information and Computing
Shor's Algorithm

- If N is large, a classical computer may require evaluation of $O(N)$ powers of N . In a quantum computer, all the powers of m would be simultaneously calculated.
- The challenge would then be to extract the value of P with a high degree of probability.
- Choosing $x = m^{P/2}$ shows there are non-trivial solutions.


Prof. P. K. Dutta, Department of Electrical and Electronic Engineering, Indian Institute of Technology Bombay


Now it is this order finding part that needs to be done by a quantum computer and the reason is that if your N is large then all powers of N will have to be calculated and that becomes a daunting task in a classical computer. But in the quantum computer you realize all powers of m will be simultaneously calculated, but you have always pointed out that there is a challenge because you have to extract that value of P which is the relevant to our problem with a high degree of probability, because there are large number of such calculations there.

(Refer Slide Time: 23:41)



Quantum Information and Computing
Shor's Algorithm

- If P is even, we factorize
$$(m^{P/2} + 1)(m^{P/2} - 1) = 0 \pmod{N}$$
- $(m^{P/2} - 1) \neq 0$ because P is the smallest integer by definition of a period
- If $(m^{P/2} + 1) = kN$ the algorithm fails, start all over choosing a different m .


Prof. D. K. Ghosh, Department of Physics, IIT Bombay

So this is the summary of what we have talked about so far. Now let me sort of illustrate that how this works.

(Refer Slide Time: 24:00)

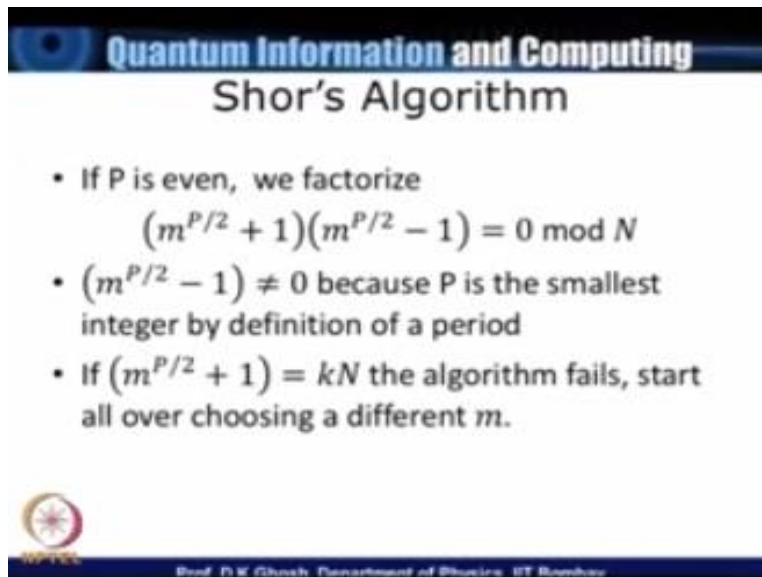
7

$$N = 21 ; m = 2, P = 6.$$
$$(m^{P/2+1})(m^{P/2-1}) = 0 \pmod{N}$$
$$\underbrace{(2^3+1)}_{\downarrow 9} \underbrace{(2^3-1)}_{\uparrow 7}$$
$$N = 35 ; \quad \underline{m = 13}$$
$$13^2 = 169$$
$$13^4 = 28561 = 35 \times 816 + 1$$
$$\underline{P = 4}$$

So let me go back to couple of examples take for example a simple number $N = 21$ we have seen that I know that the if I choose $M = 2$, P turns out to be equal to 6 by factorization then told me that I must have $M^{P/2+1} \times M^{P/2-1}$ that must be equal to 0 mod N and what are these number this is 2^3 because $6/2 + 1 \times 2^3 - 1$.


And we claim that d is them contain the factors that we are talking about, you can see that this is nothing but 9 which contains the factor 3 and this is just 7 which is one of the factors of this. As a further example let us take $n = 35$ and let me take a little more different number little different number let $M = 13$ which is co-prime to 35 because 13, 35 have no common factors. Now check 13^2 is 169, 13^3 I do not need to calculate because if it were one mod 35 then of course my algorithm will fail in this case it does not 13^4 you can take a calculator and so that it is equal to 28561 which is nothing but 35×816 a trivial calculation is what I require. So therefore my $P = 4$ in this case.

(Refer Slide Time: 25:53)



Quantum Information and Computing
Shor's Algorithm

- If P is even, we factorize
$$(m^{P/2} + 1)(m^{P/2} - 1) = 0 \pmod{N}$$
- $(m^{P/2} - 1) \neq 0$ because P is the smallest integer by definition of a period
- If $(m^{P/2} + 1) = kN$ the algorithm fails, start all over choosing a different m .



Prof. Dr. Ghosh, Department of Physics, IIT Bombay

(Refer Slide Time: 26:02)

$$\begin{aligned} & (13^2 + 1)(13^2 - 1) \\ &= 170 \times 168 \\ & \quad \uparrow \quad \quad \uparrow \\ & \text{Factor 5} \quad \text{Factor 7} \end{aligned}$$

So what do I have I since $P = 4$ I get $13^2 + 1 \times 13^2 - 1$ that contains the factors of 35 and you can check since 13 square is 169 this is 170 and this is 168 this obviously have the factor 5 and this number can be checked to be divisible by 7. Now that explains how this is carried out. Now what I have to do now is this to get these into implementation, so let us quickly summarize what we have done today.

We have given an algorithm which is actually the most important part of the algorithm which has to be done in a quantum computer and this requires calculation of a period of a discrete function we defined a discrete function which is raising the power of a random number which is co-prime to the given n for which you want to find out the factors.

And this random number raised to certain power should be equal to 1. So this step requires calculation of various powers of this random number and that part can be done very efficiently by a quantum computer. If this period of the function which is the minimum value of the power for which $M^P = 1 \pmod n$ then by a theorem of discrete algebra we find that it has nontrivial solution when my capital N is a composite number.

And then we factorized this $M^p = 1$ or rather $M^p - 0 \times M^{p/2} + 1 \times M^{p/2} - 1$ and we showed that each one of these now contains a factor of the original number what we are going to do next is to find out or is to decide, discuss how does a computer quantum computer actually implemented.

**NATIONAL PROGRAMME ON TECHNOLOGY
ENHANCED LEARNING
(NPTEL)**

**NPTEL
Principal Investigator
IIT Bombay**

Prof. R.K. Shevgaonkar

Head CDEEP

Prof. V.M. Gadre

Producer

Arun kalwankar

**Online Editor
& Digital Video Editor**

Tushar Deshpande

**Digital Video Cameraman
& Graphic Designer**

Amin B Shaikh

Jr. Technical Assistant

Vijay Kedare

Teaching Assistants

Pratik Sathe
Bhargav Sri Venkatesh M.

Sr. Web Designer

Bharati Sakpal

Research Assistant

Riya Surange

Sr. Web Designer

Bharati M. Sarang

Web Designer

Nisha Thakur

Project Attendant

Ravi Paswan
Vinayak Raut

**NATIONAL PROGRAMME ON TECHNOLOGY
ENHANCED LEARNING
(NPTEL)**

Copyright NPTEL CDEEP IIT Bombay