

**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.28**

**Shor's Factorization Algorithm-  
Implementation**

In the last lecture we started talking about the implementation of the factorization algorithm due to sure we will continue with our discussion and see how exactly a quantum computer will be able to implement it but let me summarize.

(Refer Slide Time: 00:32)

**Quantum Information and Computing**

## Shor's Factorization Algorithm

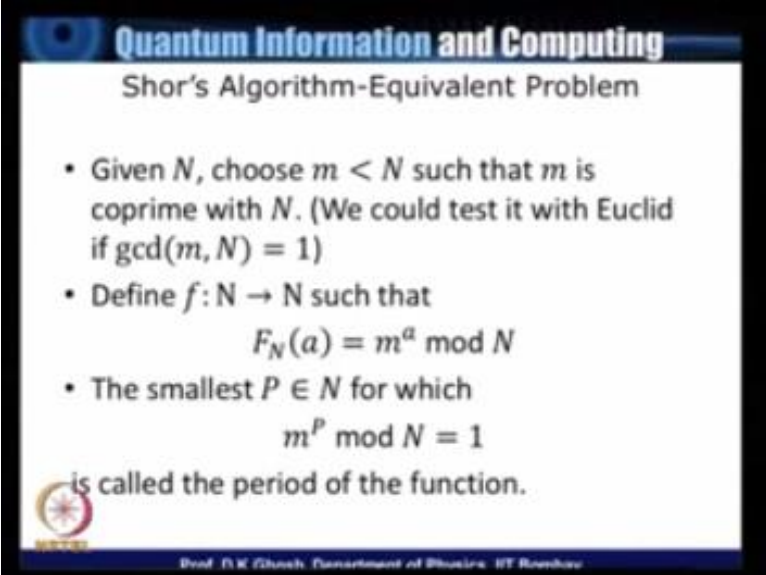
- Let  $N = pq$ , where  $p, q$  are primes. There are algorithms which compute  $p$  and  $q$  but they are not fast. Traditional Euclid algorithm takes  $\sqrt{N}$  steps.
- Fastest algorithm takes  $\exp\left((\log N)^{1/3}(\log \log N)^{2/3}\right)$  which is still very slow.

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

What we did so far we said that suppose I have a number  $N$  which = a product of two large prime numbers even though they prints in principle my algorithm is applicable to large prime numbers my illustration in this for the purpose of this course will be for relatively simple numbers because that will only enable you to appreciate what we are actually doing now we have seen that there are algorithms like Euclid algorithm or even better algorithms which can compute  $p$  and  $q$  but they are not fast enough.

The traditional Euclid algorithm takes  $\sqrt{N}$  steps in executing this the fastest possible algorithm that is known today using a traditional computer is has a complexity which is exponential of  $(\log(N))^{1/3}$  and  $(\log \log N)^{2/3}$  which is still fairly slow.

(Refer Slide Time: 01:42)



**Quantum Information and Computing**

Shor's Algorithm-Equivalent Problem

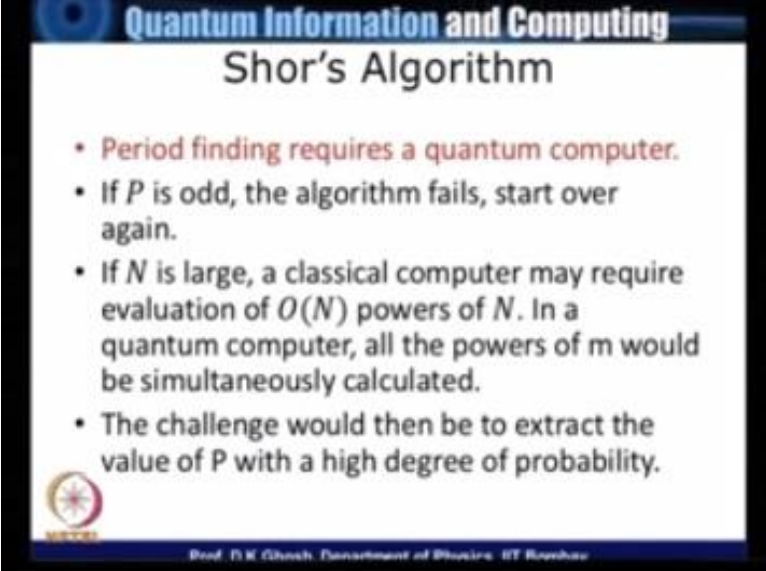
- Given  $N$ , choose  $m < N$  such that  $m$  is coprime with  $N$ . (We could test it with Euclid if  $\gcd(m, N) = 1$ )
- Define  $f: N \rightarrow N$  such that
$$F_N(a) = m^a \bmod N$$
- The smallest  $P \in N$  for which
$$m^P \bmod N = 1$$
is called the period of the function.

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

So the problem that we stated was the following that we need to solve an auxiliary problem and this auxiliary or equivalent problem is finding or having an Oracle which can compute what we call as period of a function so what we do is this we choose a random value  $M$  which is less than the  $N$  which we are required to factorize such that  $m$  is co-prime within we already had defined what is meant by a co prime that is  $m$  and  $N$  do not have a common factor having done that we defined a function  $f$  which goes from the space  $N$  to  $N$ .

And the function is  $= m^a \bmod N$  where  $a$  is some number the smallest value of  $p$  belonging to  $N$  for which  $m^p \bmod N = 1$  that is the value of  $a$  for which the  $f_N$  of  $a$  becomes  $= 1$  that is called the period of the function.

(Refer Slide Time: 03:13)



The slide is titled "Quantum Information and Computing" and "Shor's Algorithm". It contains four bullet points:

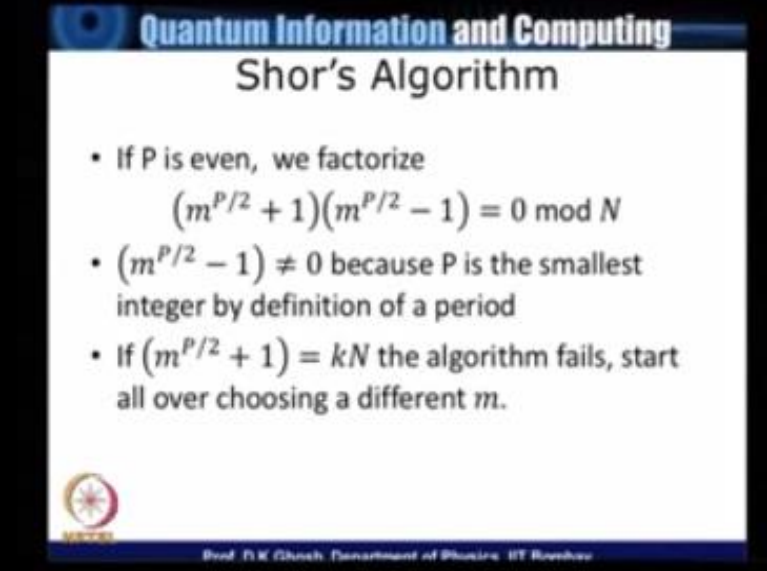
- Period finding requires a quantum computer.
- If  $P$  is odd, the algorithm fails, start over again.
- If  $N$  is large, a classical computer may require evaluation of  $O(N)$  powers of  $N$ . In a quantum computer, all the powers of  $m$  would be simultaneously calculated.
- The challenge would then be to extract the value of  $P$  with a high degree of probability.

At the bottom of the slide, there is a small logo on the left and the text "Prof. D.K. Ghosh, Department of Physics, IIT Bombay" on the right.

The quantum computers can do this step then effectively now let us see how this does it so we take at an arbitrary value of  $m$  complete its various parts till we find  $m^{2^k} \equiv 1 \pmod{N}$  now if  $p$  happens to be odd the algorithm will fail because as we have seen in our last lecture that this algorithm is based on the fact that if I have an equation  $x^2 \equiv 1 \pmod{N}$  then if  $N$  is a prime number then I will have only the trivial solution which means  $x = +$  or  $- 1$  but if  $N$  is a composite number then we have seen that it will have non-trivial solutions but the original equation based on which it was done was  $x^2 \equiv 1$ .


So therefore if I have an equation of the type  $x^2 \equiv 1 \pmod{N}$  then only my algorithm will be successful they if  $N$  is large the classical computer may require evaluation of the order of powers of  $m$  in a quantum computer as we have seen all the powers of  $m$  will be simultaneously calculated and stored of course we have been pointing out time and again that in order to extract  $p$  I need to go through certain exercise because if I simply do a measurement after the Oracle has evaluated it I would simply get a value of the power with an arbitrary probability.

(Refer Slide Time: 05:19)



**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

Now suppose  $p$  is even so that we can use this algorithm then we factorize that  $m^p - 1 = 0$  to  $(m^{p/2} + 1)(m^{p/2} - 1) = 0$  ( $m^{p/2} - 1) = 0$  is not a possible solution of this equation because we have seen that  $p$  is the smallest integer for which  $m^p = 1$  since  $p/2$  is smaller than  $p$  this is 1 that leaves us with  $m^{p/2} + 1 = 0 \pmod{N}$  if that happens again the algorithm fails the algorithm becomes useful if  $m^{p/2} + 1$  is not equal to  $0 \pmod{N}$  now if this condition is also satisfied then the solution of this equation  $m^{p/2} + 1 \times m^{p/2} - 1 = 0 \pmod{N}$  we have the relevant factors of  $N$  and this is basically the algorithm.

(Refer Slide Time: 06:39)

**Quantum Information and Computing**  
**Implementation**

- Choose  $l$  such that  $N^2 < 2^l < 2N^2$ . Let  $Q = 2^l$ . Choosing  $Q$  as a power of 2 enables us to perform QFT smoothly.
- Initialize two  $l$ -qubit registers to null state.  
 $|\psi_0\rangle = |0\rangle \otimes |0\rangle$
- Apply QFT on first register (H gates) to get a uniform linear combination of basis states

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

Now the question is how do you execute this the first step is to choose the size of the register what we do is we take an  $l$  qubit register and  $l$  is chosen such that  $2^l$  lies between  $N^2$  and  $2N^2$  some books would suggest that you take even a wider there that is choose  $L$  such that  $2^l$  lies between  $2N^2$  of  $3N^2$  but that is a matter of choice let us call  $Q = 2^l$  the reason why we will choose  $Q$  to be a power of 2 is because it will enable us to perform quantum Fourier, Fourier transform process smoothly.

The first task is to initialize I take two registers of this size that I have mentioned and I first initialize both of the registers to the null state having done that I apply a quantum Fourier transform on the first register this is something which you have been doing time and again because since these are simply null state the process is nothing other than passing all the 0 qubits states through Hadamard gates and then we will get a uniform linear combination of the basis.

(Refer Slide Time: 08:21)

**Quantum Information and Computing**

### Shor's Algorithm-Implementation

$$|\psi_1\rangle = \frac{1}{\sqrt{Q}} \sum_{x=0}^{Q-1} |x\rangle|0\rangle$$

- Choose a random number  $m < N$
- Apply the oracle to compute  $m^a \bmod N$  and store the result in the second register.

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

So therefore at this stage my state of the system which I will call a  $\Psi_1$  is given by  $\frac{1}{\sqrt{Q}} \sum_{x=0}^{Q-1} |x\rangle|0\rangle$  state  $x$  and of course the second register is still in state 0 I will now choose a random number  $m$  which as we have seen must be co-prime with capital  $N$  and then I will have a quantum Oracle to compute the various powers of this  $m$  modulus  $n$  and I would like to store these in the second register so this is clean and it does not require much of an.


(Refer Slide Time: 09:14)

**Quantum Information and Computing**

## Shor's Algorithm - Implementation

- In our example we choose  $m=13$ , which has a period of  $P=20$

$13^1=13$	$13^2=43$	$13^3=28$	$13^4=8$	$13^5=18$
$13^6=4$	$13^7=9$	$13^8=34$	$13^9=49$	$13^{10}=14$
$13^{11}=52$	$13^{12}=7$	$13^{13}=2$	$13^{14}=32$	$13^{15}=17$
$13^{16}=16$	$13^{17}=26$	$13^{18}=26$	$13^{19}=31$	$13^{20}=1$

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

Effort now let me illustrate this with an example I will take.




(Refer Slide Time: 09:21)

**Quantum Information and Computing**

### Shor's Algorithm-Implementation

$$|\psi_1\rangle = \frac{1}{\sqrt{Q}} \sum_{x=0}^{Q-1} |x\rangle|0\rangle$$

- Choose a random number  $m < N$
- Apply the oracle to compute  $m^a \bmod N$  and store the result in the second register.



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


(Refer Slide Time: 09:22)

**Quantum Information and Computing**

## Shor's Algorithm - Implementation

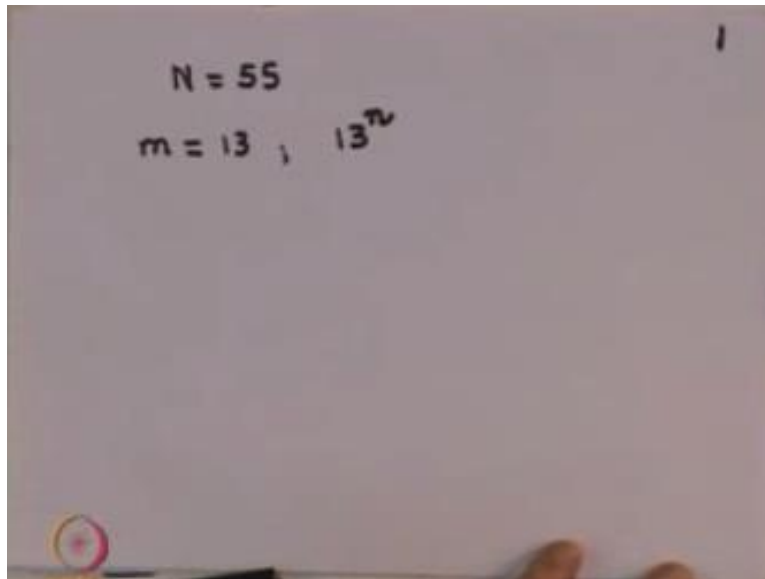
- In our example we choose  $m=13$ , which has a period of  $P=20$

$13^1=13$	$13^2=43$	$13^3=28$	$13^4=8$	$13^5=18$
$13^6=4$	$13^7=9$	$13^8=34$	$13^9=49$	$13^{10}=14$
$13^{11}=52$	$13^{12}=7$	$13^{13}=2$	$13^{14}=32$	$13^{15}=17$
$13^{16}=16$	$13^{17}=26$	$13^{18}=26$	$13^{19}=31$	$13^{20}=1$

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

Number N to be 55 now you would say.

(Refer Slide Time: 09:28)


$$N = 55$$
$$m = 13, 13^2$$

That you are using a quantum computer to factorize such a small number as I have told you time and again I would like the principle to be illustrated by small numbers which I can execute on the desktop now if  $n$  is equal to 55 which of course I know I have factors 11 and 5 let me choose  $m$  now in principle I could choose  $m$  anything other than a number which has either 5 or 11 as a factor but let me just randomly choose the number 13.

So my job now will be to calculate various powers of 13, so  $13^n$  now this I have shown it on my slide.


(Refer Slide Time: 10:24)

**Quantum Information and Computing**

## Shor's Algorithm - Implementation

- In our example we choose  $m=13$ , which has a period of  $P=20$

$13^0=13$	$13^1=43$	$13^2=28$	$13^3=8$	$13^4=18$
$13^5=4$	$13^6=9$	$13^7=34$	$13^8=49$	$13^9=14$
$13^{10}=52$	$13^{11}=7$	$13^{12}=2$	$13^{13}=32$	$13^{14}=17$
$13^{15}=16$	$13^{16}=26$	$13^{17}=25$	$13^{18}=31$	$13^{19}=1$

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

Various powers but let me try to work it out on the paper as well. So the thing is this that.

(Refer Slide Time: 10:34)

$N = 55$   
 $m = 13 ; 13^n$   
 $13^1 = 13$   
 $13^2 = 169 = 4 \pmod{55}$   
 $13^3 = 52$   
 $13^4 = 16$   
 $13^5 = 43$   
...  
 $13^{15} = 32$   
...  
 $13^{20} = 1$   
Period of  $m = 13$  is  
 $P = 20$

You can see  $13^1$  is of course 13, remember these are discrete arithmetic, now because of the discrete arithmetic we have certain advantages which you I should use, now  $13^2$  is 169 which is nothing  $4 + 165$ , 165 is nothing but  $3 \times 55$  so this is equal to 4, I will not write it always but let me remind you this is mod 55. How do I calculate  $13^3$  do I calculate  $13^3$  and proceed the answer is no, because  $13^3$  is nothing but  $13^2 \times 13^1$  so it is  $4 \times 13 = 52$  the attractive thing about modular arithmetic.

What about  $13^4$   $13^2$  is 4, so therefore  $13^4$  is  $4 \times 4 = 16$  like this you can carry on the various numbers so let me just repeat a few of them,  $13^5$  is 43 you can try out various results,  $13^{15}$  happens to be 32 and finally as you go along you will find  $13^{20}$  happens to be equal to 1. Now this is not very difficult to work out, because we have seen this is what actually we would do in order to compute these numbers.

So therefore period of  $m=13$  is 20, so most of my effort today will be to use this example and carry you through the general process that I have introduced. Now Owe have said that we must choose.

(Refer Slide Time: 13:01)

- 2 -

$$XN^2 < 2^2 < 2N^2.$$
$$N^2 = 3025 \quad 2N^2 = 4050 \quad 6050$$
$$\boxed{Q = 2^{12} = 4096}$$
$$|\psi_1\rangle =$$

The size of the register to be an 12 qubit register which lies between  $2N^2$  sorry  $N^2$  and  $2N^2$  a simple calculator will tell you that  $N^2$  is 3025 and  $2N^2$  is 4050, sorry 6050. So I can find out what is the 12 value which satisfies this inequality, and you can then see that the possibility is  $Q=2^{12} = 4096$ . So therefore, I take a 12 qubit register, at that stage my value of  $|\psi_1\rangle$  which we have seen is obtained by passing the null state of the first register, so Hadamard gate and this is then.

(Refer Slide Time: 14:17)

$$\begin{aligned}
 & \sqrt{N^2} < 2^L < 2N^2. & -2- \\
 & N^2 = 3025 & 2N^2 = \overset{6050}{\cancel{4050}} \\
 & \boxed{Q = 2^{12} = 4096} \\
 & |\Psi_1\rangle = \frac{1}{\sqrt{4096}} [ |0,0\rangle + |1,0\rangle + \dots + |4095,0\rangle ] \\
 & |\Psi_2\rangle = \frac{1}{\sqrt{4096}} [ |0,1\rangle + |1,13\rangle + |2,13^2 \equiv 4 \pmod{55}\rangle \\
 & \quad + \dots + |20,13^{20} \equiv 1 \pmod{55}\rangle + \\
 & \quad + |4095,13^{4095} \equiv 31\rangle ].
 \end{aligned}$$

$1/\sqrt{4096}$  we just happens to be  $1/64$ ,  $[|0,0\rangle + |1,0\rangle$  remember the second register continues to be in the  $|0\rangle$  state last one will be  $4095, 0$ . Now what do I do for the second step, in the next case I compute the various powers of  $m$  which has been chosen to be equal to  $13$ , and then store my result in the second register, the second register had  $0$  so the oracle will automatically give me the value of the function itself, and at that stage I do not disturb the first register at all.

So cycle will then be  $\sqrt{4096}$  this is  $64$  now I need  $13^0$  which is equal to  $1$ , then  $|1$ , and  $13^1$  so that is nothing but  $13$ , I have actually made that table so it should not be very difficult to work out, but on the other hand let us write one or two terms so  $2, 13^2, 13^2$  as we have seen is  $169$  whose, which is equal to  $5 \pmod{55}$ , sorry this is  $4 \pmod{55}$ . And like this I can go till I reach  $20$ , then I say the second register is  $13^{20}$  which we have seen equal to  $1 \pmod{55}$  and then my entire series from here starts again.

And finally I will get to the last state which is  $4095, 13^{4095}$  and this will work out to I think  $31$  but you can check it. Now at this stage suppose I were to measure the second register then what I would get would be a random value from  $1$  to the last value that I calculated for  $13$  various powers, and let me go back to my table there.

(Refer Slide Time: 17:28)

**Quantum Information and Computing**  
**Shor's Algorithm - Implementation**

- In our example we choose  $m=13$ , which has a period of  $P=20$

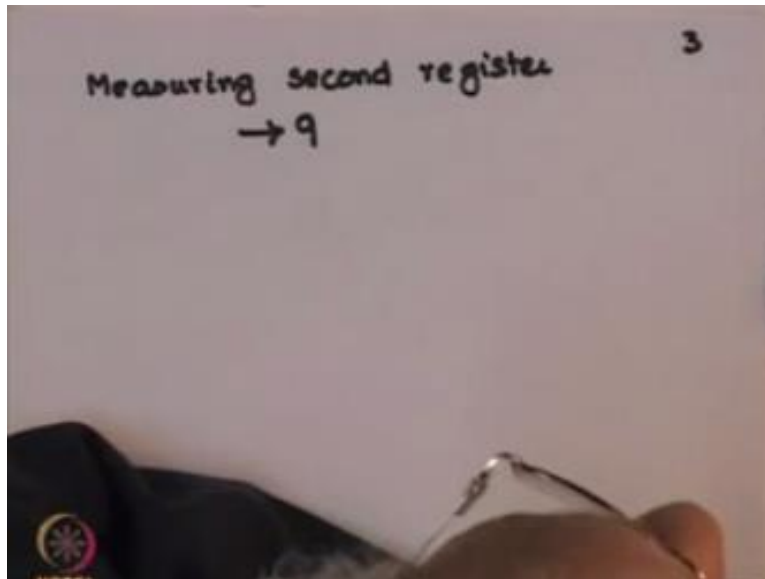
$13^0=13$	$13^1=41$	$13^2=28$	$13^3=8$	$13^4=18$
$13^5=4$	$13^6=9$	$13^7=34$	$13^8=49$	$13^9=14$
$13^{10}=52$	$13^1=7$	$13^{11}=2$	$13^{12}=32$	$13^{13}=17$
$13^{14}=16$	$13^{15}=26$	$13^{16}=26$	$13^{17}=31$	$13^{18}=1$

Prof. P. K. Choudhary, Department of Physics, IIT Bombay

You can see these were my various values and so if I measure the second register I would get 13 for 50 to 16 like this and a measurement of the second register and through in any result and you can use anyone of the members on this table to do your calculation. But let me say measuring second register give me.



(Refer Slide Time: 17:53)




Supposing it gives me 9, now if it gives you 9 refer back to the slide again you find that I have here.

(Refer Slide Time: 18:16)

**Quantum Information and Computing**  
**Shor's Algorithm - Implementation**

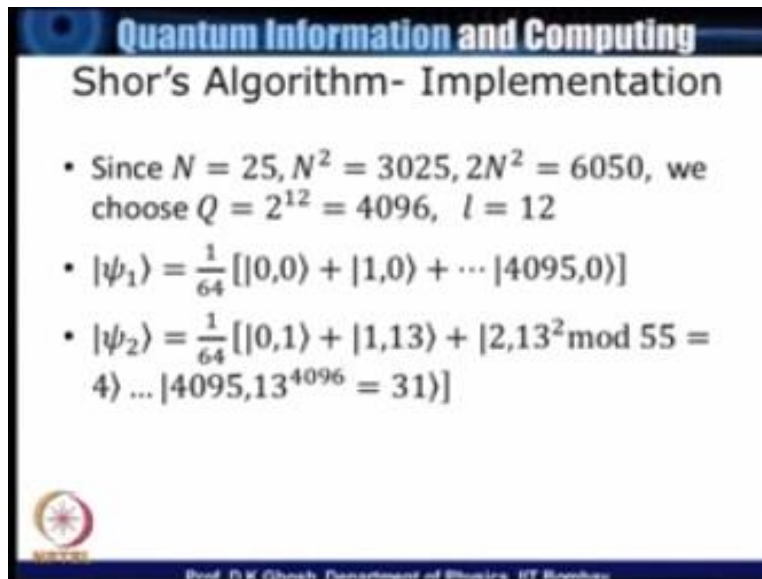
- In our example we choose  $m=13$ , which has a period of  $P=20$

$13^1=13$	$13^2=41$	$13^3=28$	$13^4=8$	$13^5=18$
$13^6=9$	$13^7=9$	$13^8=34$	$13^9=49$	$13^{10}=14$
$13^{11}=52$	$13^{12}=7$	$13^{13}=2$	$13^{14}=32$	$13^{15}=17$
$13^{16}=16$	$13^{17}=26$	$13^{18}=26$	$13^{19}=31$	$13^{20}=1$

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

$13^6=9$  so I will, if I have measured 9 then at that time my first register might have been in any stage like 6, 26 another 20, 46 extra, extra, extra.


(Refer Slide Time: 18:40)



**Quantum Information and Computing**

### Shor's Algorithm- Implementation

- Since  $N = 25$ ,  $N^2 = 3025$ ,  $2N^2 = 6050$ , we choose  $Q = 2^{12} = 4096$ ,  $l = 12$
- $|\psi_1\rangle = \frac{1}{64} [ |0,0\rangle + |1,0\rangle + \dots + |4095,0\rangle ]$
- $|\psi_2\rangle = \frac{1}{64} [ |0,1\rangle + |1,13\rangle + |2,13^2 \bmod 55 = 4\rangle \dots + |4095, 13^{4096} \bmod 55 = 31\rangle ]$

  
Prof. P. K. Ghosh, Department of Physics, IIT Kharagpur

So the result that I get is the following  $|\psi_3\rangle$ .

(Refer Slide Time: 18:48)

Measuring second register 3  
→ 9 : 205 values in  
1st Register .

$|45\rangle =$

$204 \times 20 = 4080$

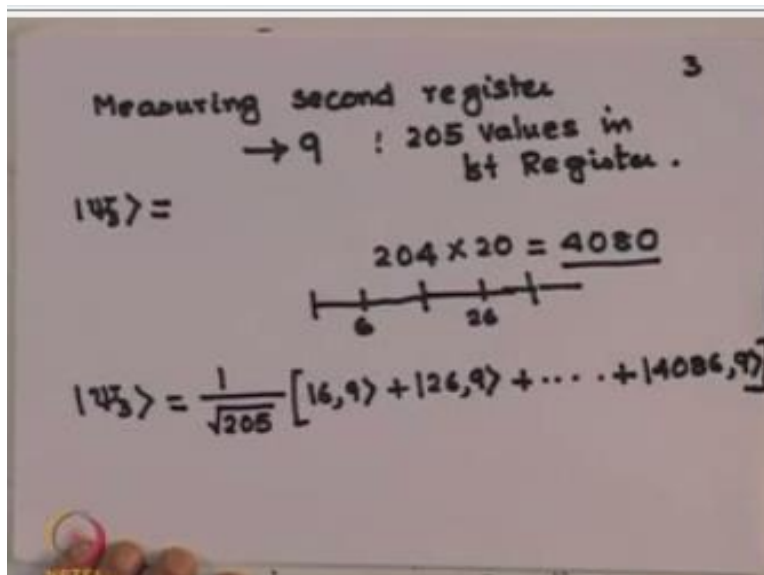
$|45\rangle = \frac{1}{\sqrt{205}} [ |6,9\rangle + |26,9\rangle + \dots + |4086,9\rangle ]$

The diagram shows a horizontal line with tick marks. Below the first tick mark is the number '6', and below the second tick mark is the number '26'. Above the line, the calculation '204 x 20 = 4080' is written, with a horizontal line under '4080'.

Since I have made the measurement of the second register, I have to actually count how many times 9 appears there. Now this is what too difficult see what we have our 4096 states starting from 0 to 4095, now in that case I get the 6th one that 26th one, so since I know the period to be 20 I can immediately count that there are total 204 states in the first period. Because I have, once I have a 6 there in the first period I will have a 26 in the second period, 46 in the third period extra, extra.

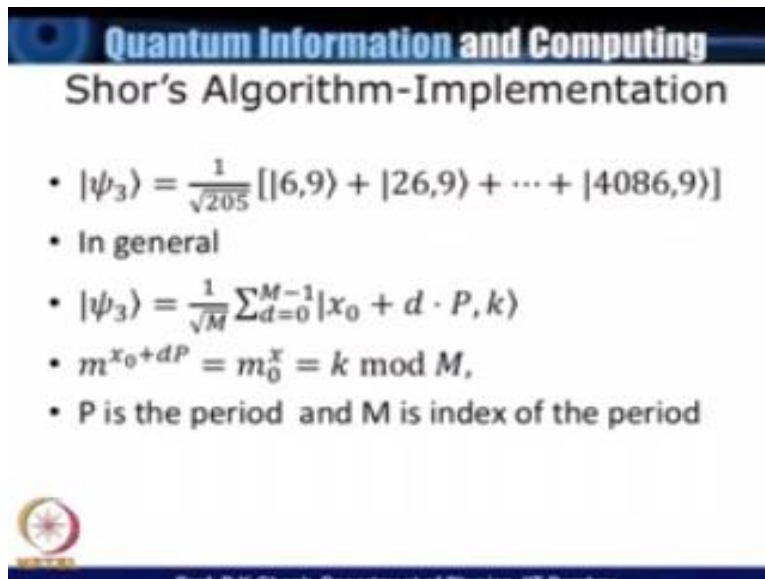
But then  $204 \times 20$  is 4080 so remaining 16 of them where 9 comes also will appear once more so in another words I will have 205 values of in first register corresponding to the second register having a value line and once I have normalized that state I will have  $\psi_3 = 1/\sqrt{205} [6, 9, 26, 9]$  etcetera and you can check it should be equal to 4080 was the end of a period so therefore last one would be 4086, 9.

(Refer Slide Time: 20:50)




In general structure of this.

(Refer Slide Time: 20:59)



**Quantum Information and Computing**  
**Shor's Algorithm-Implementation**

- $|\psi_3\rangle = \frac{1}{\sqrt{205}} [ |6,9\rangle + |26,9\rangle + \dots + |4086,9\rangle ]$
- In general
- $|\psi_3\rangle = \frac{1}{\sqrt{M}} \sum_{d=0}^{M-1} |x_0 + d \cdot P, k\rangle$
- $m^{x_0+dP} = m_0^x = k \pmod{M}$ ,
- P is the period and M is index of the period



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

Would be given by what is shown in the slide as  $1/\sqrt{M}$ , M is the number corresponding to this number which is the number of states in the first register corresponding to a given value in the second register and this is the combined state supposing my measurement in the second register it is k then the first register will have  $X_0$  which is a starting point plus the position in the period is it in the first period which may call  $d = 0$  second period third period etc. So d is the running index on that times period, so this is exactly what is written down.

(Refer Slide Time: 22:01)

. 4 .

QFT on 1st Register.

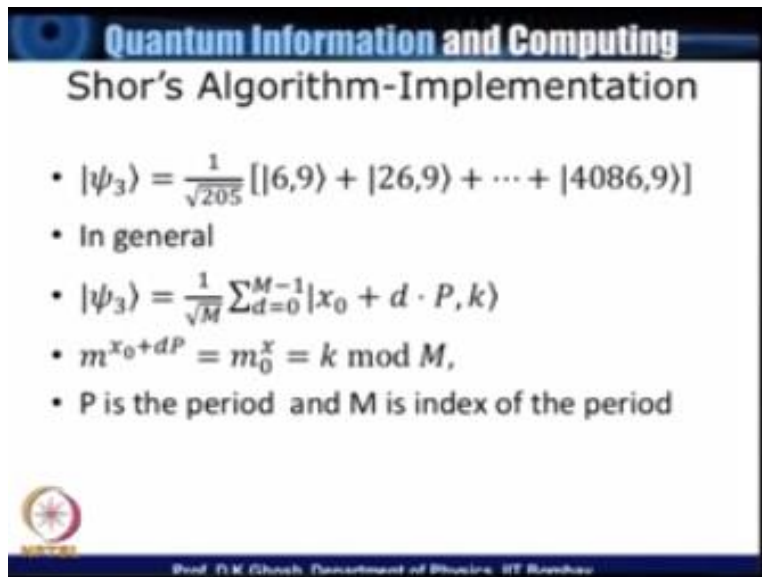
$$\begin{aligned}
 |\psi_3\rangle &= \frac{1}{\sqrt{M}} \sum_{d=0}^{M-1} |x_0 + dp, k\rangle \\
 |\psi_4\rangle &= \frac{1}{\sqrt{QM}} \sum_{y=0}^{Q-1} \sum_{d=0}^{M-1} \exp[2\pi i y(x_0 + dp)/Q] |y, k\rangle \\
 &= \frac{1}{\sqrt{QM}} \sum_{y=0}^{Q-1} e^{2\pi i y x_0 / Q} \sum_d e^{2\pi i y dp / Q} |y, k\rangle \\
 &= \frac{1}{\sqrt{QM}} \sum_{y=0}^{Q-1} e^{2\pi i y x_0 / Q} \left( \sum_d z^d \right) |y, k\rangle \\
 &\quad z = e^{2\pi i y p / Q} .
 \end{aligned}$$

Now at that stage we will apply QFT on the first register. this requires a bit of an algebra but let us look at what am I getting. So we had in principle  $\psi_3$  let me write it down  $1/\sqrt{M} \sum_{d=0}^{M-1}$  which is just the running index of which period it is in  $X_0$  is the starting point of that first register for which the value in the second register was  $k$  plus  $d$  times  $p$ ,  $k$  which is the result of the second register which in my example I told you as 9.

Now if I now introduce a q f t on the first register I will get  $\psi_4$  so this now QFT is being done on the first register which has  $q$  number of elements so therefore this is  $1/\sqrt{QM} \sum_{y=0}^{Q-1} \sum_{d=0}^{M-1}$  exponential of  $2\pi i y x_0 + dp/Q$  and  $y, k$  this is standard definition of the Fourier transform. Now let us write it in a particular way so this is equal to  $1/\sqrt{QM} \sum_{y=0}^{Q-1} e^{2\pi i y x_0}$  the first term by  $Q$  multiplied with some over  $D$  because  $D$  is only appearing in the second term  $e^{2\pi i y dp/Q}$  and then of course  $y, k$ .

Now let me write it this  $\sum_d$  notice that this is only there in this term so this is equal to  $1/\sqrt{QM} \sum_{y=0}^{Q-1} e^{2\pi i y x_0 / Q} \sum_d$  we put it in bracket let us call this  $Z^d$  and of course  $YK$  where we have defined  $Z$  to be given by  $e^{2\pi i y p / Q}$  let us look at.


(Refer Slide Time: 25:19)



**Quantum Information and Computing**

### Shor's Algorithm-Implementation

- $|\psi_3\rangle = \frac{1}{\sqrt{205}} [|6,9\rangle + |26,9\rangle + \dots + |4086,9\rangle]$
- In general
- $|\psi_3\rangle = \frac{1}{\sqrt{M}} \sum_{d=0}^{M-1} |x_0 + d \cdot P, k\rangle$
- $m^{x_0+dP} = m_0^x = k \pmod{M}$ ,
- P is the period and M is index of the period

  
Prof. P.K. Ghosh, Department of Physics, IIT Roorkee

What this quantity gives me because once I have this now supposing either to measure the first register.



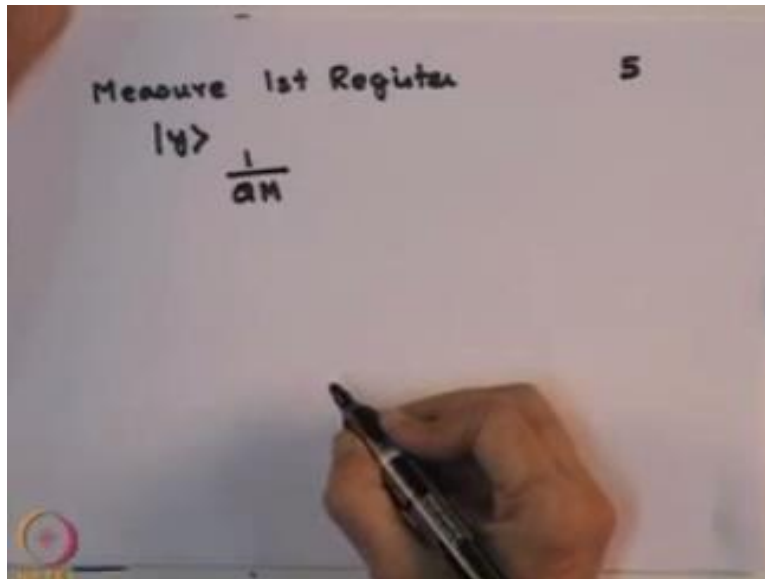
(Refer Slide Time: 25:30)

QFT on 1st Register. . 4 .

$$\begin{aligned} |\psi\rangle &= \frac{1}{\sqrt{M}} \sum_{d=0}^{M-1} |x_0 + dP, k\rangle \\ |\psi\rangle &= \frac{1}{\sqrt{QM}} \sum_{y=0}^{Q-1} \sum_{d=0}^{M-1} \exp[2\pi i y(x_0 + dP)/Q] |y, k\rangle \\ &= \frac{1}{\sqrt{QM}} \sum_{y=0}^{Q-1} e^{2\pi i y x_0 / Q} \sum_d e^{2\pi i y d P / Q} |y, k\rangle \\ &= \frac{1}{\sqrt{QM}} \sum_{y=0}^{Q-1} e^{2\pi i y x_0 / Q} \left( \sum_d z^d \right) |y, k\rangle \\ & \quad z = e^{2\pi i y P / Q} \end{aligned}$$

If I have to measure the first register what will I get I will get a particular value of  $y$ .

(Refer Slide Time: 25:37)



I will get a particular value of  $y$  with the probability  $1 / \sqrt{M}$  because there was a  $1/\sqrt{M}$  there.

(Refer Slide Time: 25:59)

. 4 .

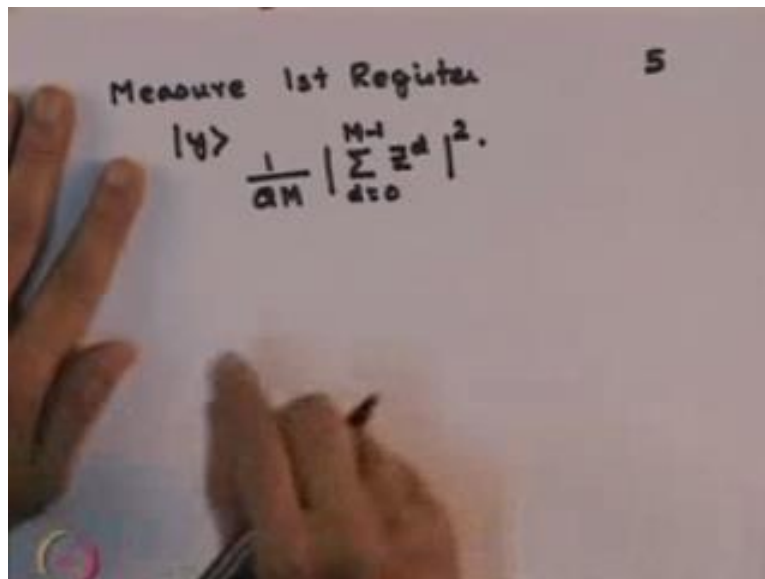
QFT on 1st Register.

$$|\psi\rangle = \frac{1}{\sqrt{M}} \sum_{d=0}^{M-1} |x_0 + dP, k\rangle$$
$$|\psi\rangle = \frac{1}{\sqrt{QM}} \sum_{y=0}^{Q-1} \sum_{d=0}^{M-1} \exp[2\pi i y(x_0 + dP)/Q] |y, k\rangle$$
$$= \frac{1}{\sqrt{QM}} \sum_{y=0}^{Q-1} e^{2\pi i y x_0 / Q} \sum_d e^{2\pi i y d P / Q} |y, k\rangle$$
$$= \frac{1}{\sqrt{QM}} \sum_{y=0}^{Q-1} e^{2\pi i y x_0 / Q} \left( \sum_d e^{2\pi i y d P / Q} \right) |y, k\rangle$$

$z = e^{2\pi i y P / Q}$

And this term is a unimodular term.

(Refer Slide Time: 26:04)



So that is one so I left with modulus of  $\sum_{d=0}^{m-1} z^d$

(Refer Slide Time: 26:23)

QFT on 1st Register.

$$|y\rangle = \frac{1}{\sqrt{M}} \sum_{d=0}^{M-1} |x_0 + dP, k\rangle$$

$$|y\rangle = \frac{1}{\sqrt{aM}} \sum_{y=0}^{a-1} \sum_{d=0}^{M-1} \exp[2\pi i y(x_0 + dP)/a] |y, k\rangle$$

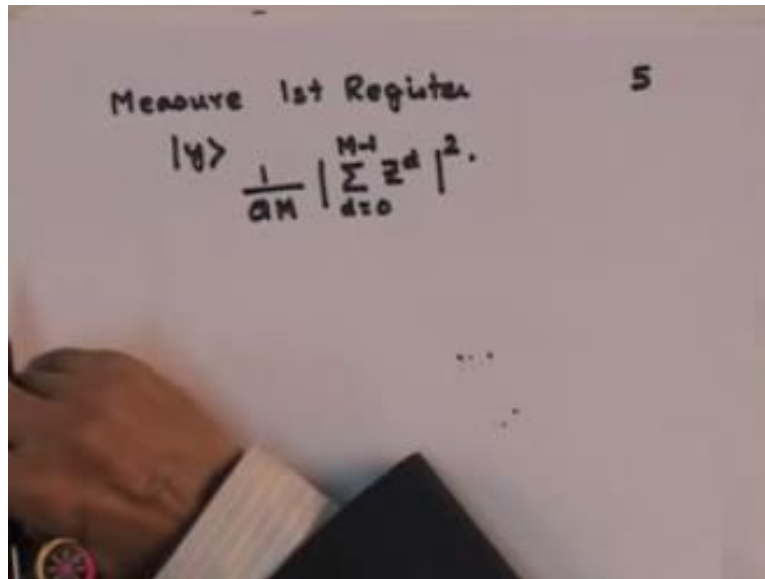
$$= \frac{1}{\sqrt{aM}} \sum_{y=0}^{a-1} e^{2\pi i y x_0 / a} \sum_d e^{2\pi i y d P / a} |y, k\rangle$$

$$= \frac{1}{\sqrt{aM}} \sum_{y=0}^{a-1} e^{2\pi i y x_0 / a} \left( \sum_d z^d \right) |y, k\rangle$$

$$z = e^{2\pi i y d P / a}$$

I have written down what is this Z here and this d the  $\sum d$  is a finite sum.

(Refer Slide Time: 26:31)



Measure 1st Register 5

$$|y\rangle \frac{1}{\sqrt{M}} \left| \sum_{d=0}^{M-1} z^d \right|^2.$$

Since the sum is the finite sum I will be able to execute the sum and find out its value. And this will give me the probability with which a particular state  $Y$  appears. We will see in the next lecture that this probability has peaks at particular value of  $y$  which enables us to determine the period  $p$ .

And so therefore by repeated measurements and certain smart manipulation of the result of such measurement will be in a position to find the period and this as we have seen is what was our biggest challenge in solving the problem of factorization. So in the next lecture I will compute this value and illustrate it for the example that I have given that is for  $N = 55$ , and then tell you what is a fast method of computing the value of the period from the result of the measurement of the first register.

**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**