NPTEL

NATIONAL PROGRAMME ON
TECHNOLOGY ENHANCED LEARNING

IIT BOMBAY

CDEEP
IIT BOMBAY

Quantum Infromation and Computing

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

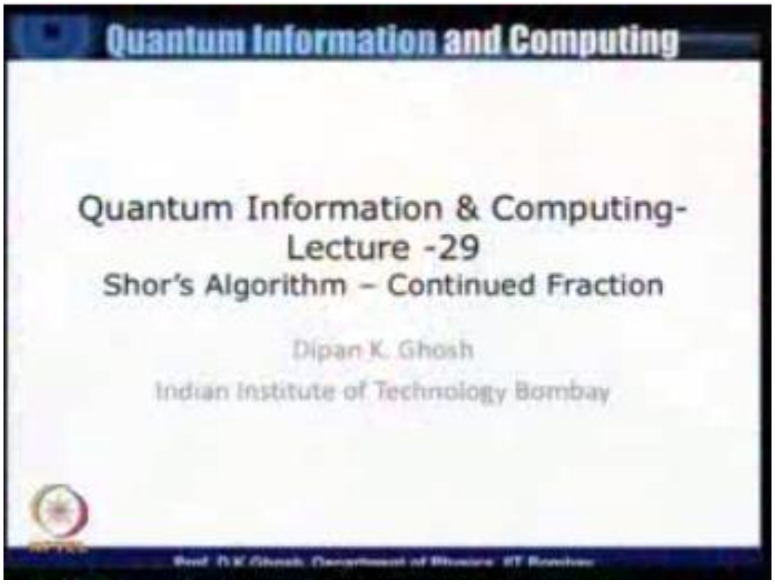
Modul No.05

Lecture No.29

Shor's Algorithm – Continued Fraction

In the last lecture and two or three lectures before that we had been discussing Shor's factorization algorithm today we will conclude that with a discussion on how exactly this algorithm is implemented as we have realized that the crux of the algorithm lies in finding the period of a function so let me quickly go through the part that we did so far.

(Refer Slide Time: 00:50)



Quantum Information and Computing

Quantum Information & Computing-
Lecture -29
Shor's Algorithm – Continued Fraction

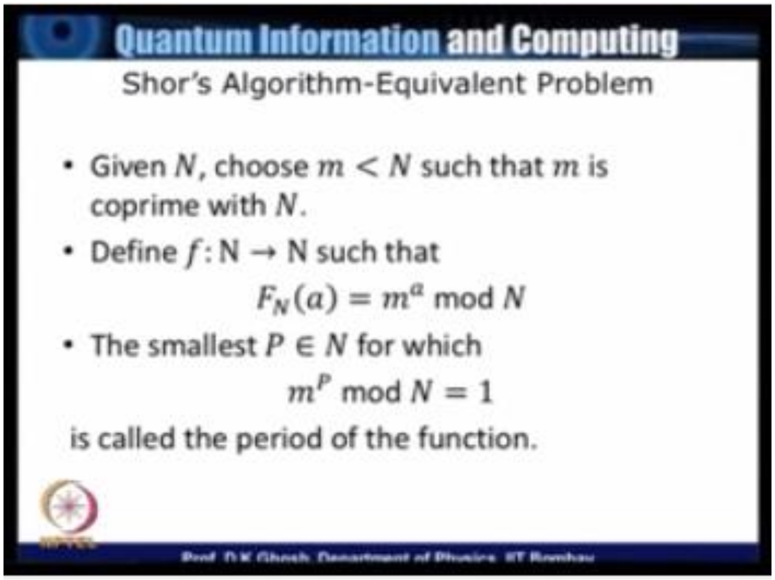
Dipan K. Ghosh

Indian Institute of Technology Bombay

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

In connection with that.

(Refer Slide Time: 00:53)



Quantum Information and Computing

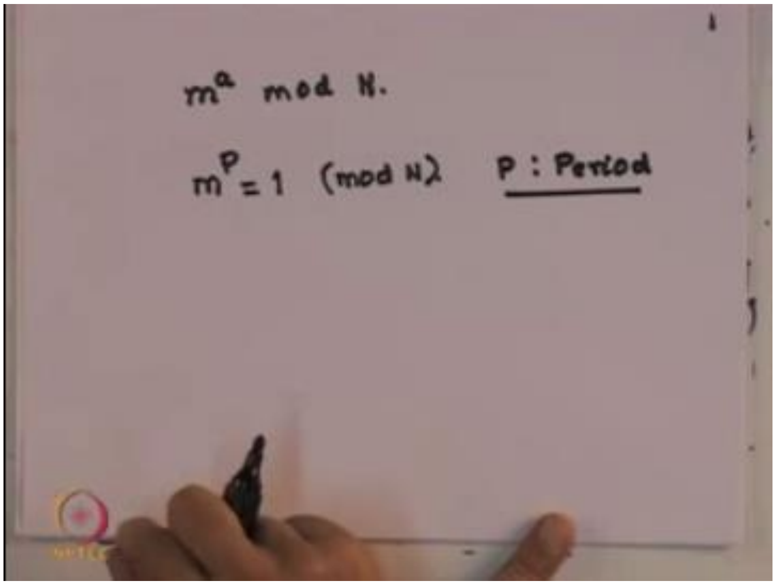
Shor's Algorithm-Equivalent Problem

- Given N, choose $m < N$ such that m is coprime with N.
- Define $f: \mathrm{N} \rightarrow \mathrm{N}$ 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. D.K Ghosh, Department of Physics, IIT Bombay

So what we said is given a number N choose a number m which is smaller than N such that m is co-prime within that if m and N do not have any common factors and for illustration purpose I have chosen a small number N = 55however the quantum computation is going to be necessary when number N is very large and is a composite product of two prime numbers now let us define a function which is given by.

(Refer Slide Time: 01:29)

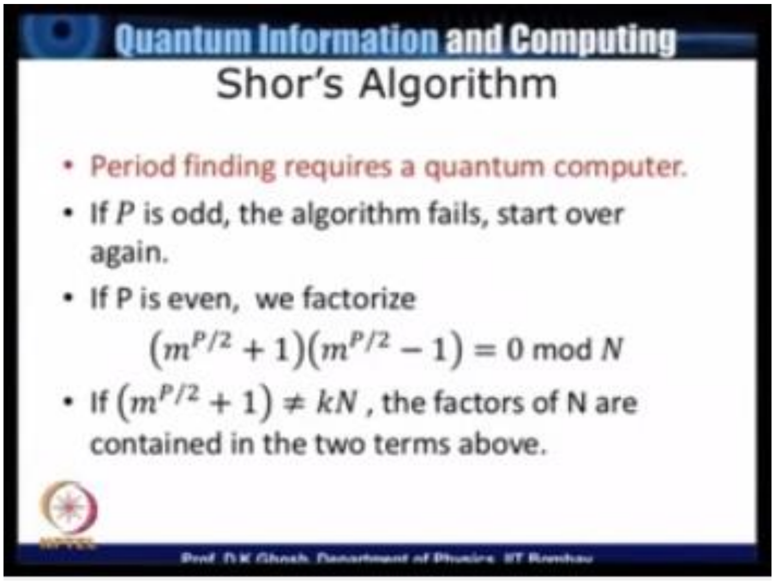


m^a mod N.

$m^P = 1$ (mod N) P : Period

m^a mod N so a is various powers and what we have seen is the smallest value of a which I have denoted as p for which $m^P = 1$ all these are modulus N this is the period of the function and our ability to factorize a large composite number lies.

(Refer Slide Time: 02:12)



Quantum Information and Computing

Shor's Algorithm

- Period finding requires a quantum computer.
- If P is odd, the algorithm fails, start over again.
- If P is even, we factorize

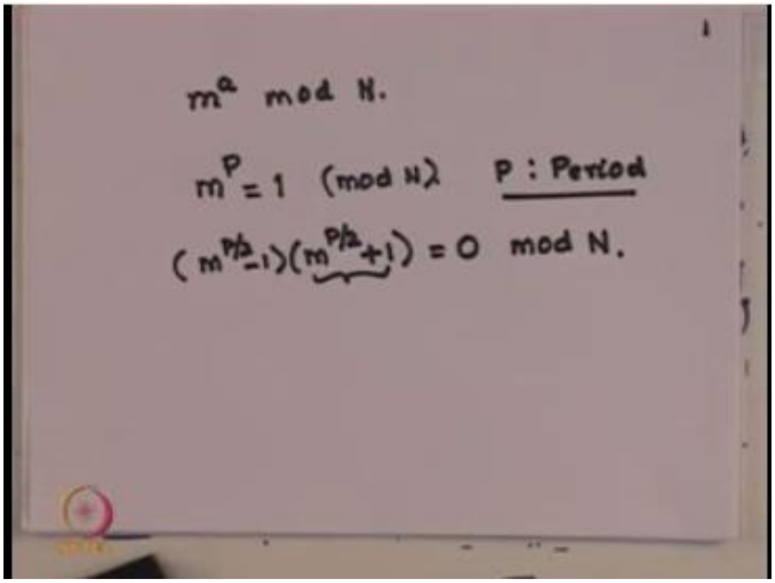
$$(m^{P/2}+1)(m^{P/2}-1) = 0 \bmod N$$

- If $(m^{P/2}+1) \neq kN$, the factors of N are contained in the two terms above.

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

In our being able to find p and as we have pointed out that for large composite numbers our only way is to have a quantum computer which can determine the period p so what we said is if this is true.

(Refer Slide Time: 02:28)



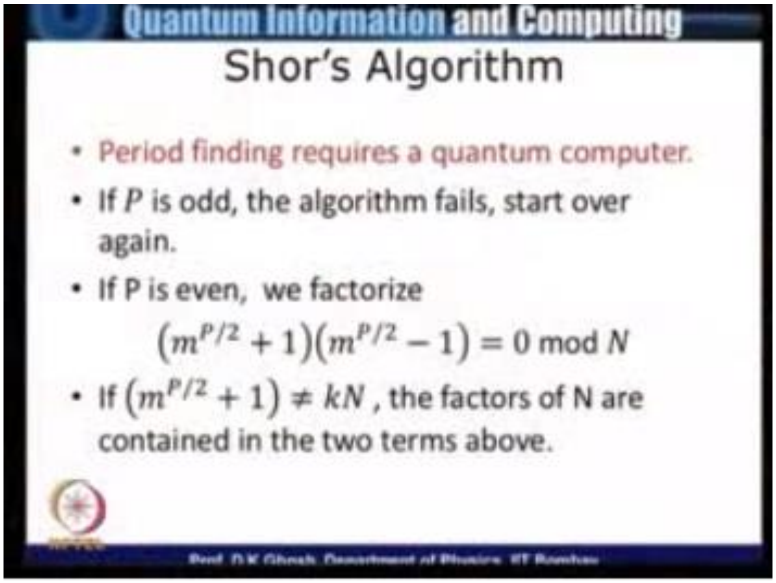
m^a mod N.

$m^p = 1 \pmod{N}$ $\underline{p : \text{Period}}$

$(m^{p/2}-1)(\underbrace{m^{p/2}+1}) = 0$ mod N.

Then $m^{p/2}$ – 1 x $m^{p/2}$ +1 that = 0 if p is even and If $m^{p/2}$ + 1is not a multiple of N then we can proceed with it.

(Refer Slide Time: 02:53)



Quantum Information and Computing

Shor's Algorithm

- Period finding requires a quantum computer.
- If P is odd, the algorithm fails, start over again.
- If P is even, we factorize

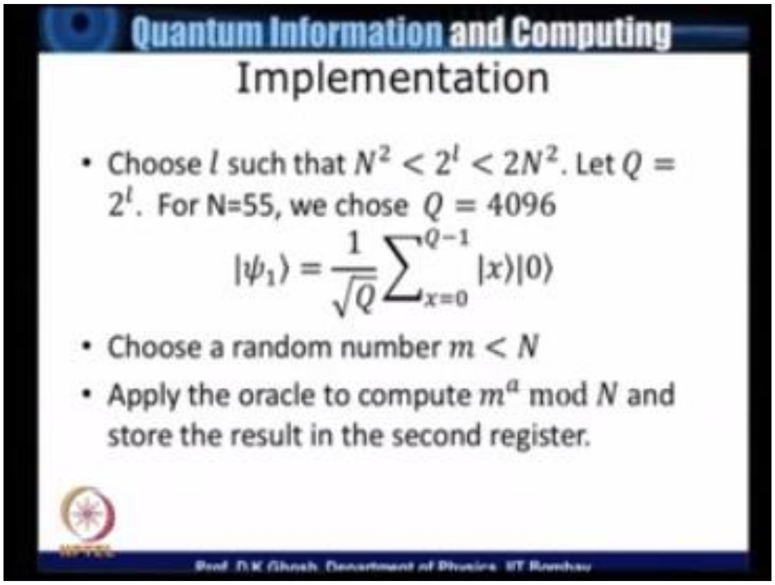
$$\left(m^{P/2}+1\right)\left(m^{P/2}-1\right)=0 \bmod N$$

- If $\left(m^{P/2}+1\right) \neq kN$, the factors of N are contained in the two terms above.

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

And the.

(Refer Slide Time: 02:54)



Quantum Information and Computing

Implementation

- Choose l such that $N^2 < 2^l < 2N^2$. Let $Q = 2^l$. For N=55, we chose $Q = 4096$

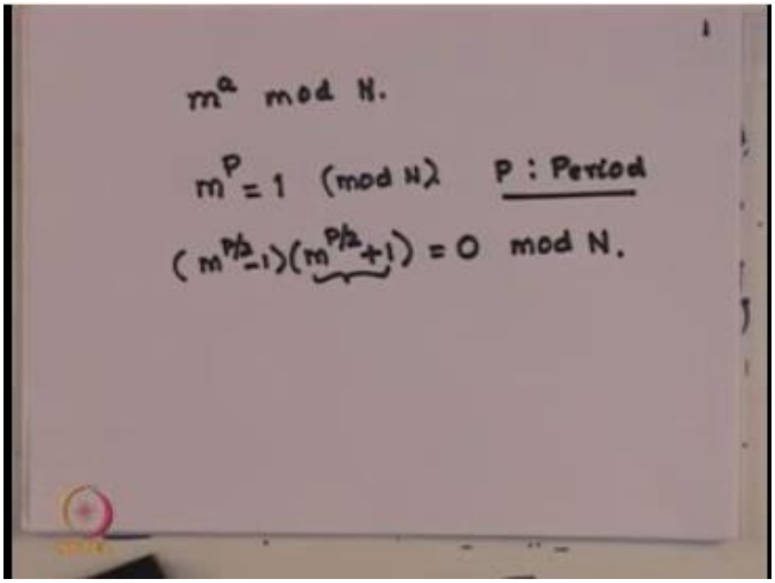
$$|\psi_1\rangle = \frac{1}{\sqrt{Q}}\sum_{x=0}^{Q-1}|x\rangle|0\rangle$$

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

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

Shor’s algorithm works what we said is in order to execute this algorithm we choose an l which is defined by 2^l lying between N^2 at $2N^2$ you can always check that it is always possible to find such a number l for instance for N= 55 we must choose Q which is given by 2^l i think this is a 12-digit or 12 bit register that we are choosing and Q = 4096 with this we first put both these registers in null state and then by passing the first register through a series of Hadamard gates we get the first register in a uniform linear combination of the computational basis States then what we do is we have the Oracle which would calculate this function.

(Refer Slide Time: 03:57)



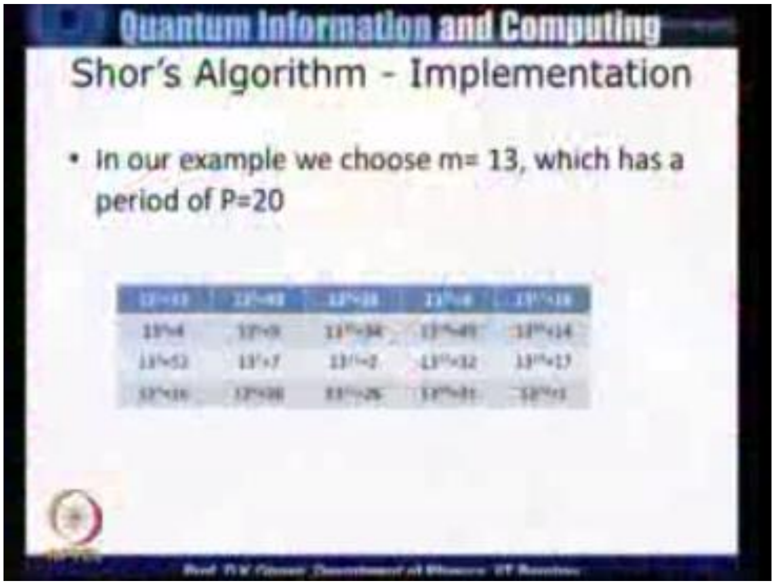
m^a mod N.

$m^P = 1 \pmod{N}$ P : Period

$(m^{P/2}-1)(\underbrace{m^{P/2}+1}) = 0 \mod N.$

m^a for various values of a and store all these things in this second register which is my target register which was initially put to be =0 we had chosen for illustration purpose N = 55 and m =13 and we had given you a table of various.

(Refer Slide Time: 04:23)



Quantum Information and Computing

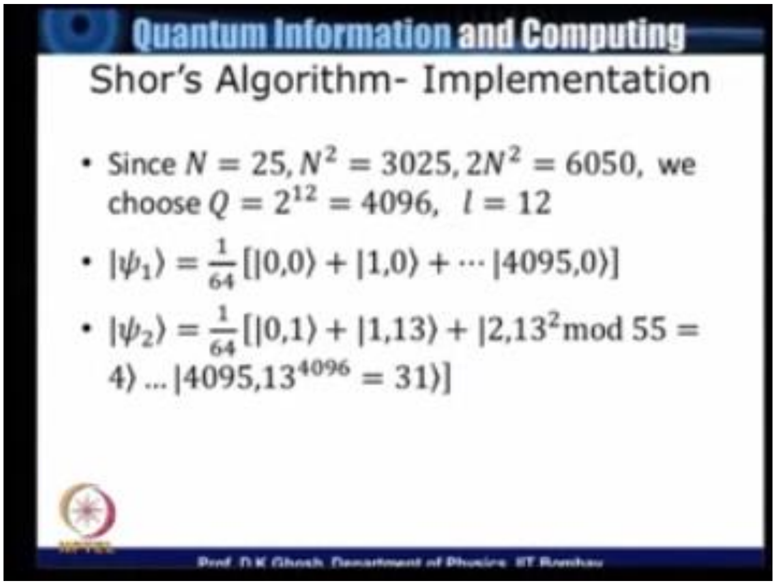
Shor's Algorithm - Implementation

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

$13^{1}=13$	$13^{5}=43$	$13^{9}=28$	$13^{13}=8$	$13^{17}=18$
$13^{2}=4$	$13^{6}=9$	$13^{10}=34$	$13^{14}=49$	$13^{18}=14$
$13^{3}=52$	$13^{7}=7$	$13^{11}=2$	$13^{15}=32$	$13^{19}=17$
$13^{4}=16$	$13^{8}=36$	$13^{12}=26$	$13^{16}=31$	$13^{20}=1$

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

(Refer Slide Time: 04:24)



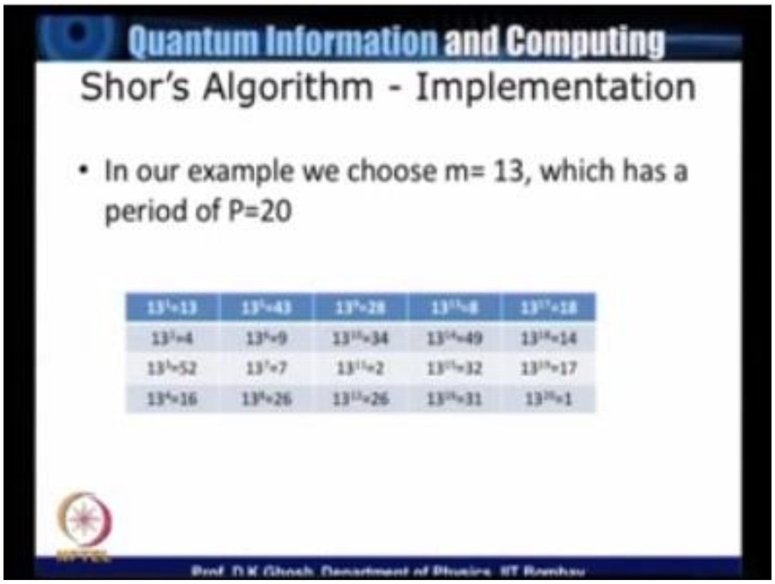
Quantum Information and Computing

Shor's Algorithm- Implementation

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

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

(Refer Slide Time: 04:25)



Quantum Information and Computing

Shor's Algorithm - Implementation

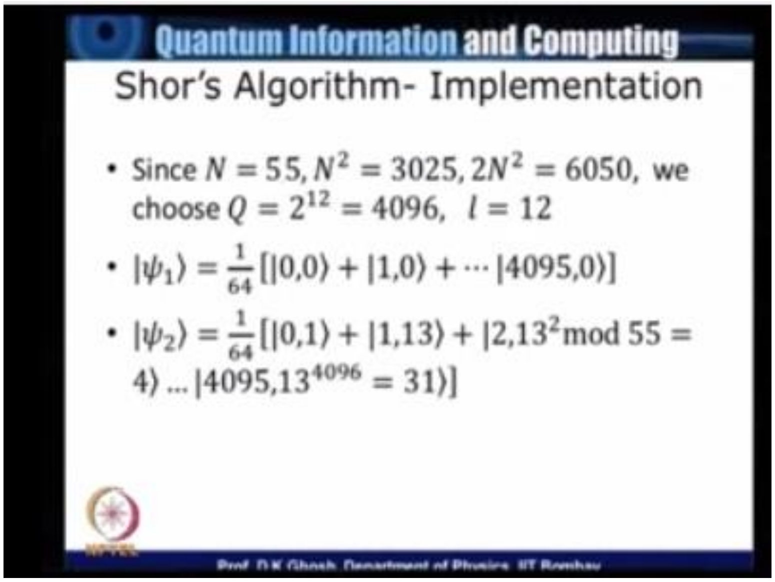
- In our example we choose m= 13, which has a period of P=20

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

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

Powers of 13 and we had seen that in this particular instance that number 13 has a period which is equal to 20 but we will assume this to illustrate how does one proceed with this.

(Refer Slide Time: 04:43)



Quantum Information and Computing

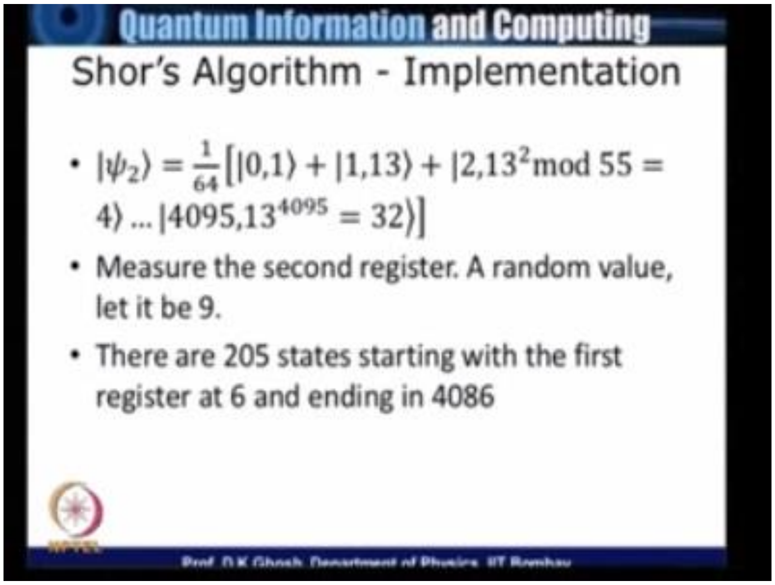
Shor's Algorithm- Implementation

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

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

Our next job if you recall having chosen a Q which is in this case 4096 a 12 qubit register what we do is write down the initial state first which is written as Ψ1 =1√4096 that is 64 and first register is now a linear combination of all the basis States which is written 01 2 3 up to 40 95 and the second register still continues to be in state 0 the Oracle computes m^a for various values for example N^1 m^2 etc. And puts the value in the second register there is a slight bit of an error in the last one it should be 13^{4095} because it starts with 0 and must end in 4095 and that number happens to be 32.

(Refer Slide Time: 05:46)



Quantum Information and Computing

Shor's Algorithm - Implementation

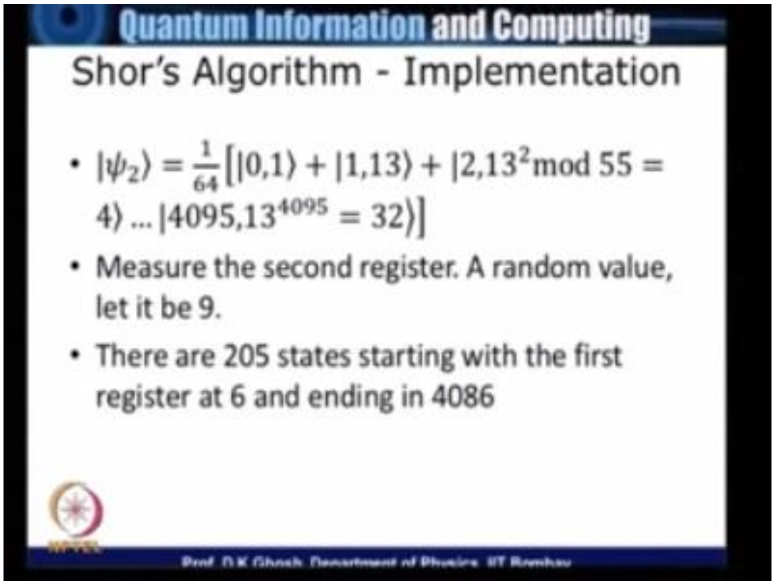
- $|\psi_2\rangle = \frac{1}{64}\left[|0,1\rangle + |1,13\rangle + |2,13^2 \text{mod } 55 = 4\rangle \ldots |4095,13^{4095} = 32\rangle\right]$
- Measure the second register. A random value, let it be 9.
- There are 205 states starting with the first register at 6 and ending in 4086

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

So this is this is what we have got and at that stage we measured the second register now when we measured the second register it will so a random number now you remember that even though we have written from one till 13^{4095} in the second register what actually happens is because of the periodicity of the function the values keep on repeating after every 20 because period was known to be 20 so therefore I get for the in the second register the values that we have listed in that table for 13 now it is one of those values.

Which will be randomly picked up if you measure the second register and for our purpose we have said that suppose that second register turned out to give us 9 as the measured value.

(Refer Slide Time: 06:47)



Quantum Information and Computing

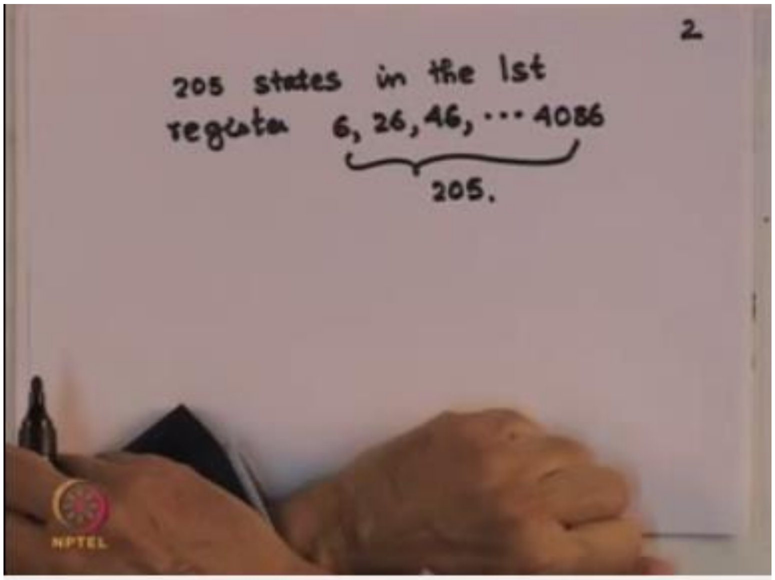
Shor's Algorithm - Implementation

- $|\psi_2\rangle = \frac{1}{64}\left[|0,1\rangle + |1,13\rangle + |2,13^2 \mathrm{mod}\ 55 = 4\rangle \ldots |4095,13^{4095} = 32\rangle\right]$
- Measure the second register. A random value, let it be 9.
- There are 205 states starting with the first register at 6 and ending in 4086

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

Now if the second register he has a nine then the minimum value for which this is valid as we have seen in table is six so I start with six then I have 26 46 66 etcetera etc, and go on till I finish this within 4096 now that will give us at 205 possible States so this 205 possible States start with 6.

(Refer Slide Time: 07:25)

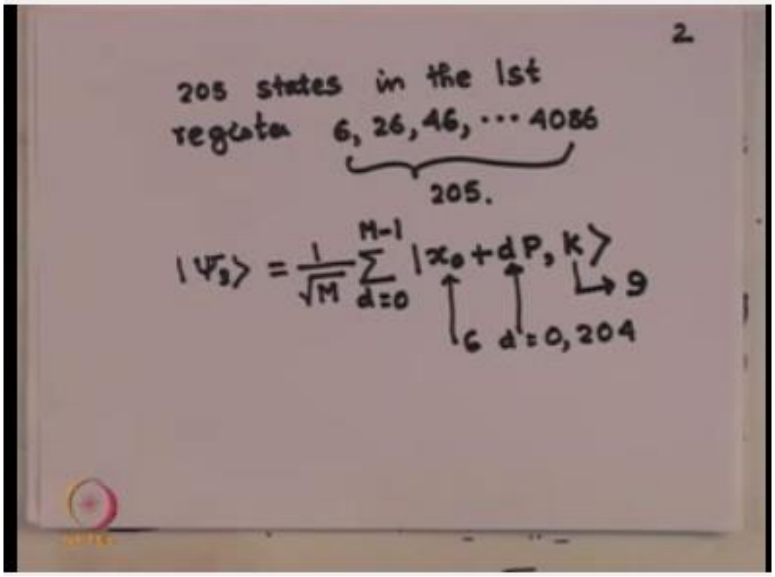


2

205 states in the 1st register $\underbrace{6, 26, 46, \cdots 4086}_{205.}$

In the first register so these numbers are 6 26 46 etcetera and the last number being 40 86 so these are 205 of them so what we said is this that when you are measuring a particular value in the second register the first register contains a linear combination of all those values of the computational basis for which the m^y if y if y is the index of the first register happens to be equal to that given K which in this case was nine so formally this.

(Refer Slide Time: 08:29)



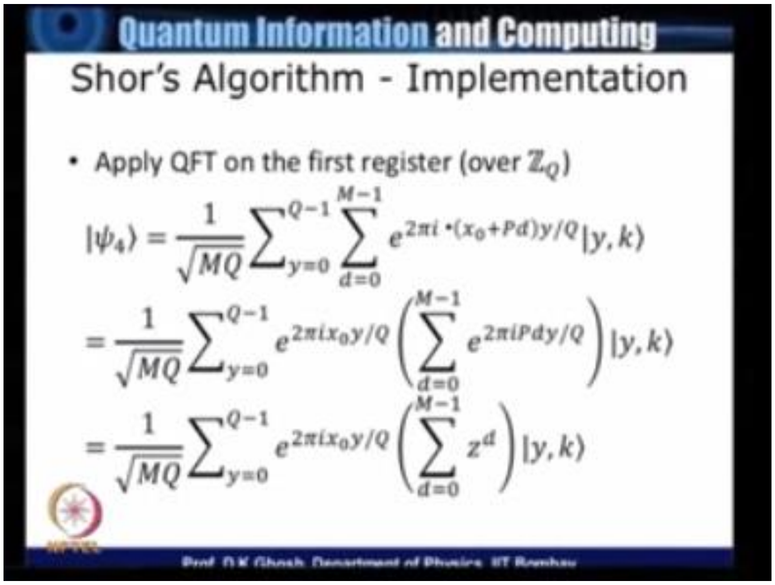
2

205 states in the 1st register $\underbrace{6, 26, 46, \cdots 4086}_{205.}$

$$|\Psi_3\rangle = \frac{1}{\sqrt{M}} \sum_{d=0}^{M-1} |\underset{\uparrow 6}{x_0} + \underset{\uparrow d = 0, 204}{d}P, \underset{\hookrightarrow 9}{k}\rangle$$

State Ψ3 was shown to be equal to 1√M this is the number of states which give you this result which in this case was 205 sum over d = 0 to M - 1 d is simply an index of which period which of the is it the first 22nd 23rd 20 etc. In which this state lies and this then would be the first one x_0 which is six in this case + d times p and this k that we have children for illustration purpose this x_0 was 6 and dis the number which goes from 0 to 200 for which was 205 numbers there and p for our calculation purposes happened to be 20 and K was chosen to be equal to 9 by saying that when we measure the second register 9 was thrown.

(Refer Slide Time: 09:35)



Quantum Information and Computing

Shor's Algorithm - Implementation

- Apply QFT on the first register (over $\mathbb{Z}_Q$)

$$|\psi_4\rangle = \frac{1}{\sqrt{MQ}}\sum_{y=0}^{Q-1}\sum_{d=0}^{M-1} e^{2\pi i \cdot (x_0+Pd)y/Q}|y,k\rangle$$

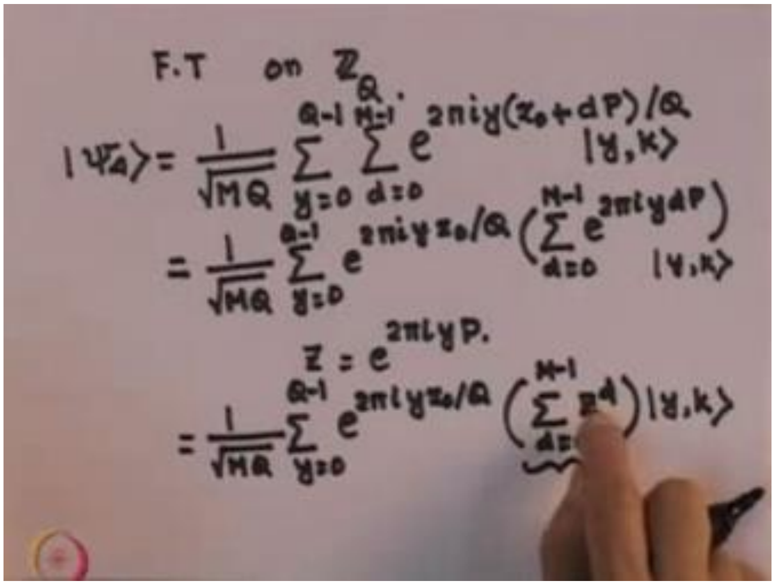
$$= \frac{1}{\sqrt{MQ}}\sum_{y=0}^{Q-1} e^{2\pi i x_0 y/Q}\left(\sum_{d=0}^{M-1} e^{2\pi i P d y/Q}\right)|y,k\rangle$$

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

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

At this stage we would apply a Fourier transform on the first register so let us look at what the Fourier transform dips now a Fourier transform is applied on the first register.

(Refer Slide Time: 09:49)



F.T on $\mathbb{Z}_Q$.

$$|\Psi_4\rangle = \frac{1}{\sqrt{MQ}} \sum_{y=0}^{Q-1} \sum_{d=0}^{M-1} e^{2\pi i y(x_0+dP)/Q} |y,k\rangle$$

$$= \frac{1}{\sqrt{MQ}} \sum_{y=0}^{Q-1} e^{2\pi i y x_0/Q} \left(\sum_{d=0}^{M-1} e^{2\pi i y d P}\right) |y,k\rangle$$

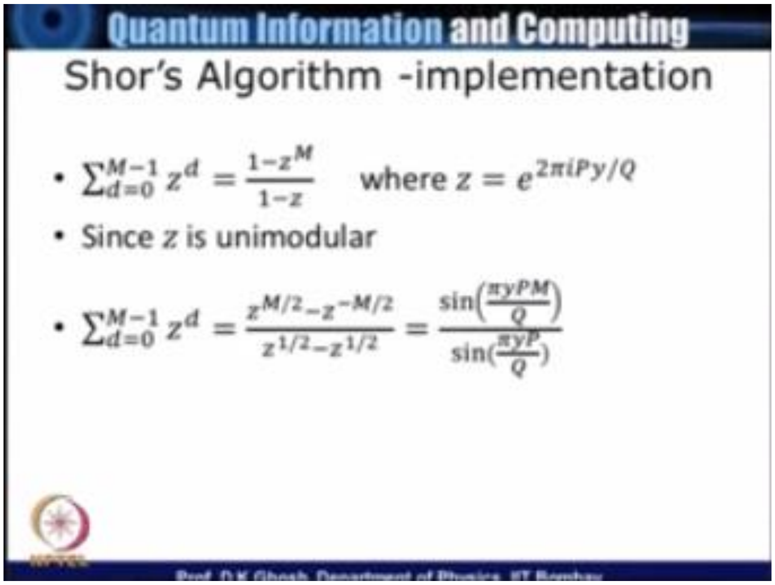
$$Z = e^{2\pi i y P}.$$

$$= \frac{1}{\sqrt{MQ}} \sum_{y=0}^{Q-1} e^{2\pi i y x_0/Q} \left(\underbrace{\sum_{d=0}^{M-1} Z^d}\right) |y,k\rangle$$

As on remember the first register when you apply the Fourier transform you have to have Q number of terms so therefore let us call it Ψ4 and Ψ4 = 1 √M which was already there in my expression 1/√Q which comes due to the Fourier transform ∑y=0 to Q-1 then I already had ∑d=1 to M-1 so $e^{2\pi iy}$ and this was $(x_0+dp)/Q$ and of course |y,k>. Now we would write this in a slightly modified form and this is 1/√MQ ∑y $e^{2\pi iyx0/Q}$ now what I do is, the ∑d let me put it inside d=0 to N-1 $e^{2\pi iydp}$ and |y,k>.

Let me define a quantity which is Z by $e^{2\pi iyP}$ so that this is now written as 1/√MQ ∑y $e^{2\pi iyx0/Q}$ and this is∑d=0 to N-1 of Z^d where Z has just been defined like this. Now let us look at what is this term Z^d notice of course this is a geometric series with a common ratio equal to Z.

(Refer Slide Time: 12:14)



Quantum Information and Computing

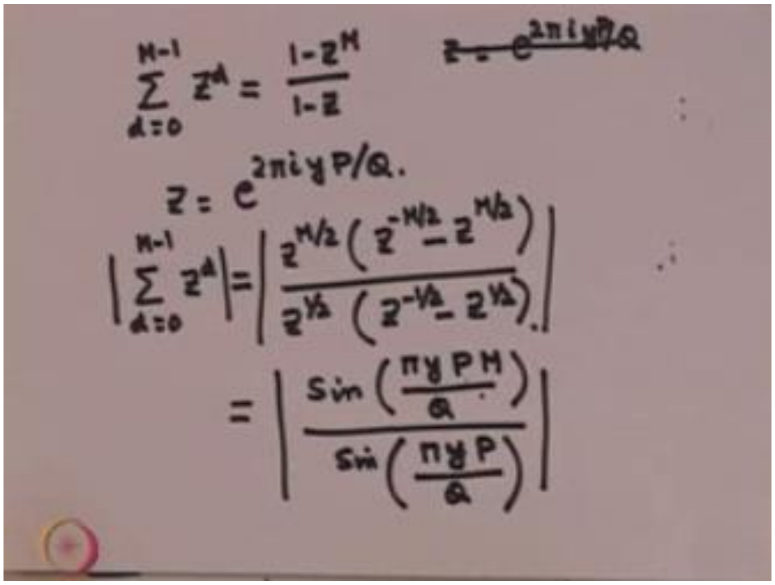
Shor's Algorithm -implementation

- $\sum_{d=0}^{M-1} z^d = \frac{1-z^M}{1-z}$ where $z = e^{2\pi i P y/Q}$
- Since z is unimodular
- $\sum_{d=0}^{M-1} z^d = \frac{z^{M/2}-z^{-M/2}}{z^{1/2}-z^{1/2}} = \frac{\sin\left(\frac{\pi y P M}{Q}\right)}{\sin\left(\frac{\pi y P}{Q}\right)}$

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

So I can easily do this ∑ so let us write down how much is

(Refer Slide Time: 12:21)



$$\sum_{d=0}^{M-1} Z^d = \frac{1-Z^M}{1-Z} \qquad \cancel{Z = e^{2\pi i y P/Q}}$$

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

$$\left|\sum_{d=0}^{M-1} Z^d\right| = \left|\frac{Z^{M/2}\left(Z^{-M/2} - Z^{M/2}\right)}{Z^{1/2}\left(Z^{-1/2} - Z^{1/2}\right)}\right|$$

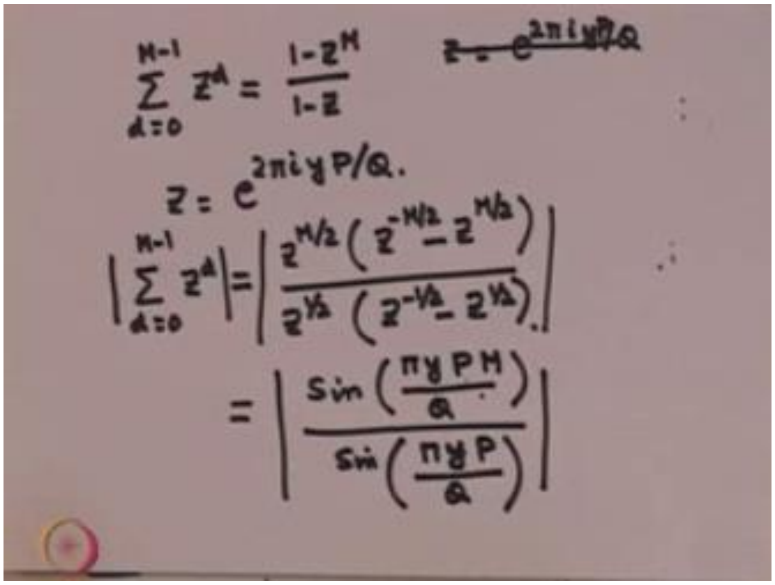
$$= \left|\frac{\sin\left(\frac{\pi y P M}{Q}\right)}{\sin\left(\frac{\pi y P}{Q}\right)}\right|$$

d=0 to M-1 of Z^d and that is equal to 1- Z^M/1-Z by standard formula which you have learned from school. And in this case my Z was just not defined to be equal to $e^{2\pi iy/Q}$ and a P there, so let me correct this here there should have been a divided by Q there which I had forgotten. Now please note that this thing Z it is unimodular because it is exponential of i times something and so therefore I can express this ∑ in a slightly different way. I can pull out Z ^{M} 2 and write this as $Z^{-M/2}$ – $Z^{M/2}$and pull out a $Z^{1/2}$ from here and get this as $Z^{-1/2}$-$Z^{1/2}$.

So when I take the modulus of such a quantity, because these are unimodular I get one from here and I am then left with this expression, and since Z has this structure I get this is equal to modulus of sin function of (πyPM/Q/sin(πyP/q) and of course modulus there. What does this actually show, it tells us that at that stage if I measure the first register which had a linear combination of all those states for which the value of the second register happen to be 9, and we have taken a Fourier transform their off.

So notice out of this 4096 possible states in the first register the those states will be projected out in a measurement which have a significant probability.

(Refer Slide Time: 15:25)



$$\sum_{d=0}^{M-1} z^{d} = \frac{1-z^{M}}{1-z} \qquad \cancel{z = e^{2\pi i y P/Q}}$$

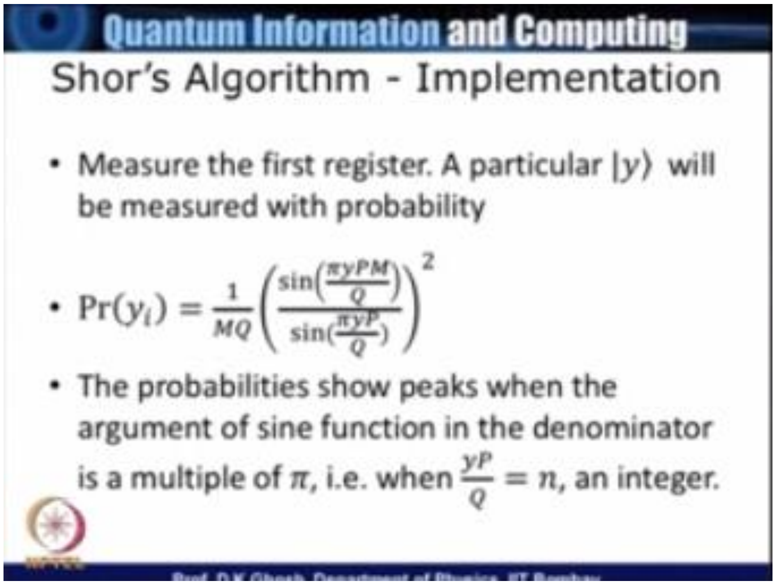
$$z = e^{2\pi i y P/Q}.$$

$$\left|\sum_{d=0}^{M-1} z^{d}\right| = \left|\frac{z^{M/2}\left(z^{-M/2} - z^{M/2}\right)}{z^{1/2}\left(z^{-1/2} - z^{1/2}\right)}\right|$$

$$= \left|\frac{\sin\left(\frac{\pi y P M}{Q}\right)}{\sin\left(\frac{\pi y P}{Q}\right)}\right|$$

Now square of this quantity is the probability, and so the slide here.

(Refer Slide Time: 15:32)



Quantum Information and Computing

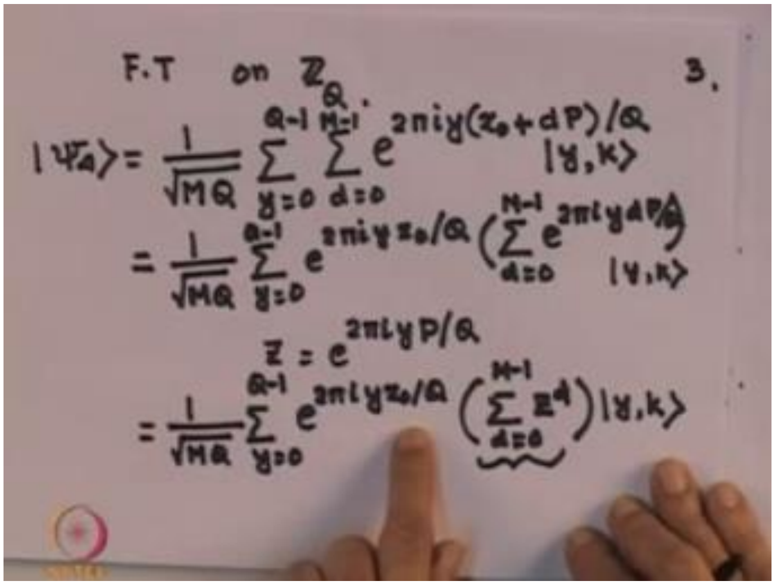
Shor's Algorithm - Implementation

- Measure the first register. A particular $|y\rangle$ will be measured with probability
- $\Pr(y_i) = \frac{1}{MQ}\left(\frac{\sin\left(\frac{\pi yPM}{Q}\right)}{\sin\left(\frac{\pi yP}{Q}\right)}\right)^2$
- The probabilities show peaks when the argument of sine function in the denominator is a multiple of π, i.e. when $\frac{yP}{Q} = n$, an integer.

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

Shows this thing that what is the probability so this is there was that 1/√MQ in my definition of ψ4.

(Refer Slide Time: 15:44)



F.T on $\mathbb{Z}_Q$. 3.

$$|\Psi_A\rangle = \frac{1}{\sqrt{MQ}} \sum_{y=0}^{Q-1} \sum_{d=0}^{M-1} e^{2\pi i y(x_0 + dP)/Q} |y, k\rangle$$

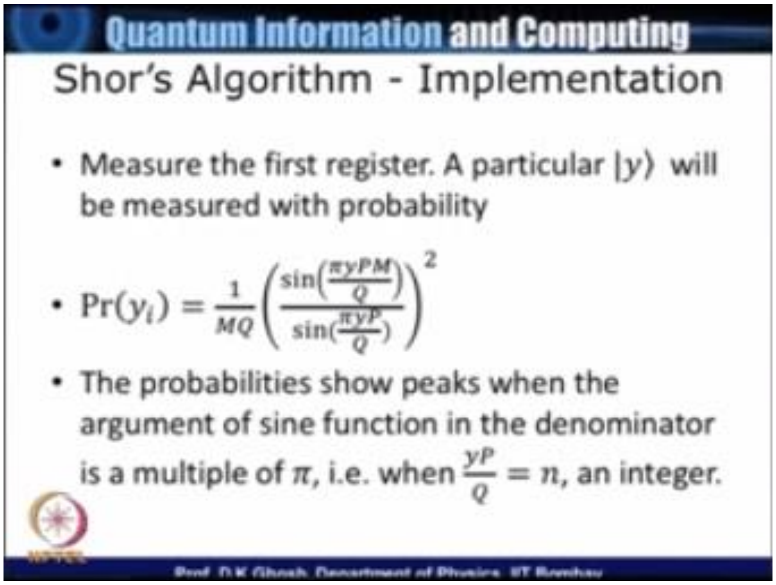
$$= \frac{1}{\sqrt{MQ}} \sum_{y=0}^{Q-1} e^{2\pi i y x_0/Q} \left(\sum_{d=0}^{M-1} e^{2\pi i y d P/Q} \right) |y, k\rangle$$

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

$$= \frac{1}{\sqrt{MQ}} \sum_{y=0}^{Q-1} e^{2\pi i y x_0/Q} \left(\underbrace{\sum_{d=0}^{M-1} Z^d} \right) |y, k\rangle$$

So therefore the probability square of this and this probability that I just now calculated, because this also has a modulus in my, this is also a new modular function.

(Refer Slide Time: 15:53)



Quantum Information and Computing

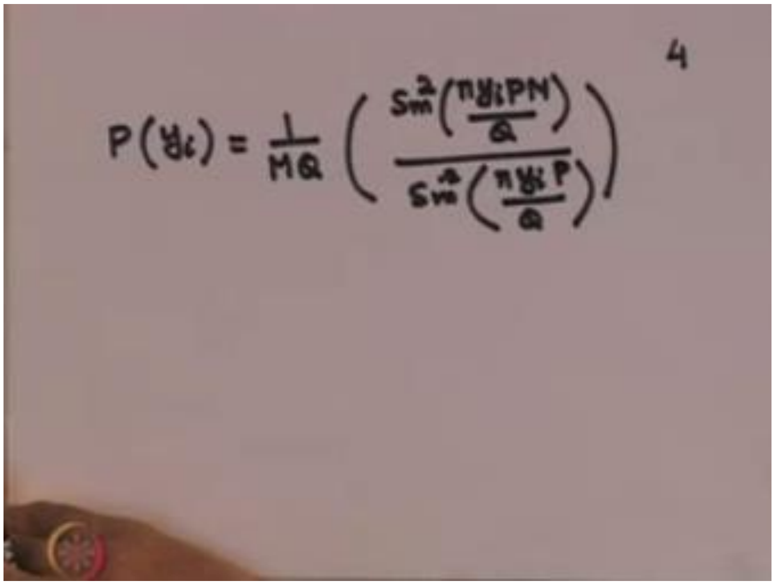
Shor's Algorithm - Implementation

- Measure the first register. A particular $|y\rangle$ will be measured with probability
- $\Pr(y_i) = \frac{1}{MQ}\left(\frac{\sin\left(\frac{\pi y P M}{Q}\right)}{\sin\left(\frac{\pi y P}{Q}\right)}\right)^2$
- The probabilities show peaks when the argument of sine function in the denominator is a multiple of π, i.e. when $\frac{yP}{Q} = n$, an integer.

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

So therefore, the probability of having a particular value of y when you measure the first register.

(Refer Slide Time: 16:03)

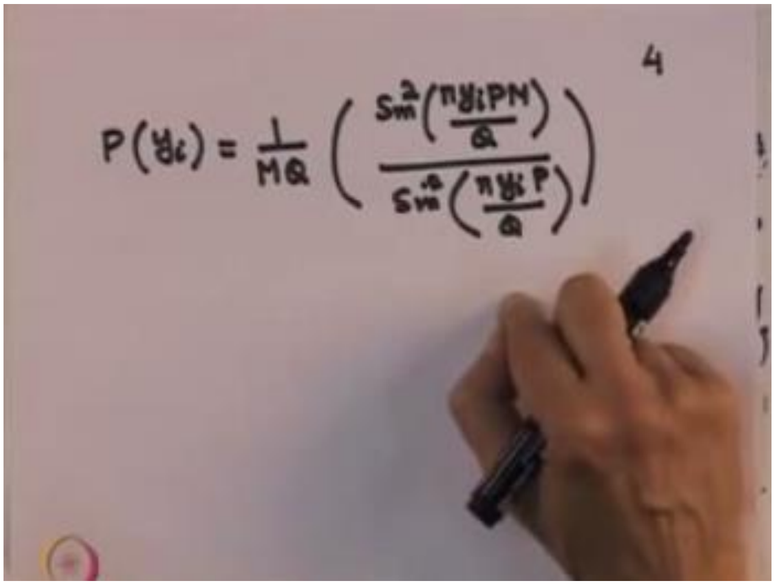


4

$$P(y_i) = \frac{1}{MQ}\left(\frac{\sin^2\left(\frac{\pi y_i P N}{Q}\right)}{\sin^2\left(\frac{\pi y_i P}{Q}\right)}\right)$$

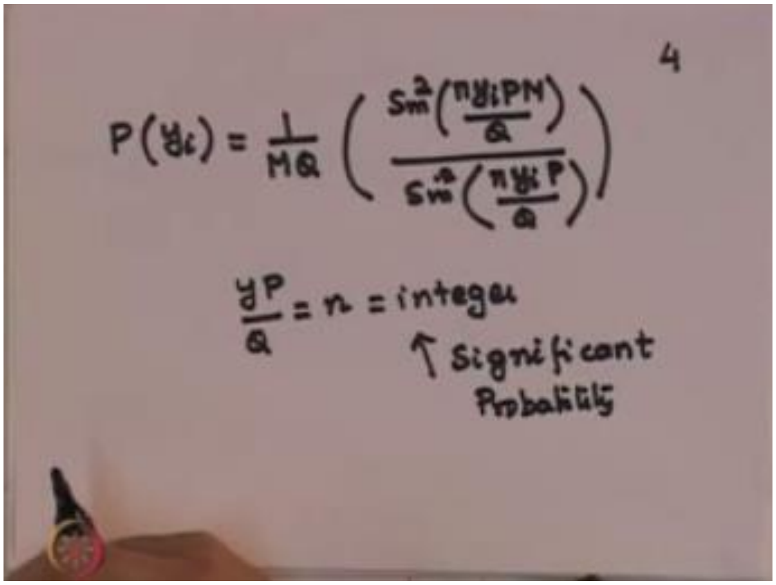
Let us say probability of a particular y_i is given by 1/MQ ($\sin^2$ (πyiPM/Q)/$\sin^2$(πyiP/Q)) this is the function with which you have some familiarity in the password, because this is the type of function which came up in many interference related problems. In any case this is basically.

(Refer Slide Time: 16:43)


4
$P(y_i) = \frac{1}{MQ}\left(\frac{\sin^2\left(\frac{\pi y_i P N}{Q}\right)}{\sin^2\left(\frac{\pi y_i P}{Q}\right)}\right)$

Sin^2 αx/sin^{2}x type of function, and these functions have a peak when the argument of the denominator becomes well multiple of π, because in that case both the denominator and the numerical values like this is not a multiple of π, then you can calculate and this probability turns out to be extremely small. Now so therefore these significant probability out of those 4086 states that we had will appear when this.

(Refer Slide Time: 17:25)



4

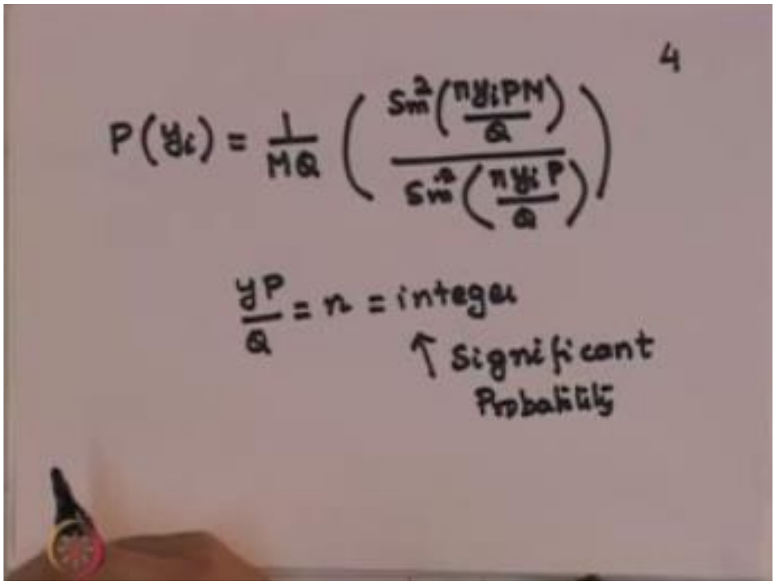
$$P(y_i) = \frac{1}{MQ}\left(\frac{\sin^2\left(\frac{\pi y_i P N}{Q}\right)}{\sin^2\left(\frac{\pi y_i P}{Q}\right)}\right)$$

$$\frac{yP}{Q} = n = \text{integer}$$

↑ Significant Probability

yP/Q if this is an integer then the denominator will blow out, so this will give me significant probability of projecting a particular y. Now we already know what these locations of these things are because we have back calculated and know that P=205, sorry P=20 and Q of course we know.

(Refer Slide Time: 18:08)



4

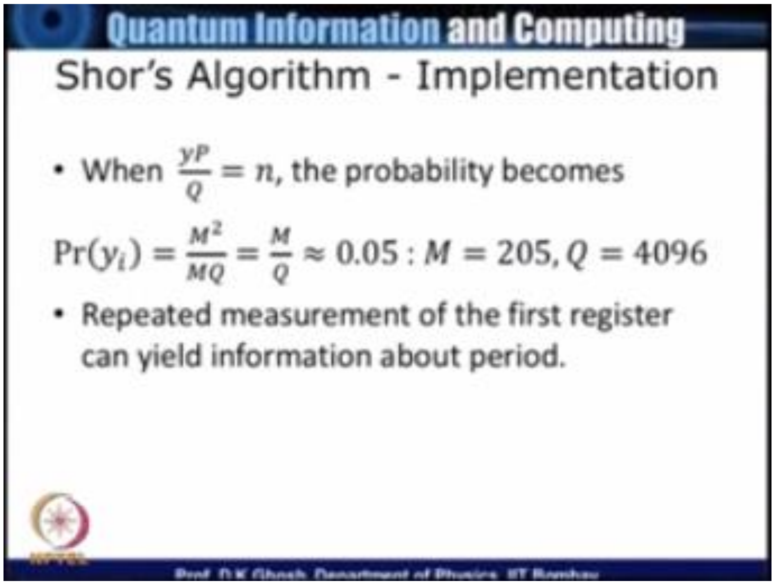
$$P(y_i) = \frac{1}{MQ}\left(\frac{\sin^2\left(\frac{\pi y_i P N}{Q}\right)}{\sin^2\left(\frac{\pi y_i P}{Q}\right)}\right)$$

$$\frac{yP}{Q} = n = \text{integer}$$

↑ Significant Probability

What is it and so therefore we are aware that when this function will give me that. In other words I am looking for the condition that okay, the probability is this.

(Refer Slide Time: 18:24)



Quantum Information and Computing

Shor's Algorithm - Implementation

- When $\frac{yP}{Q} = n$, the probability becomes

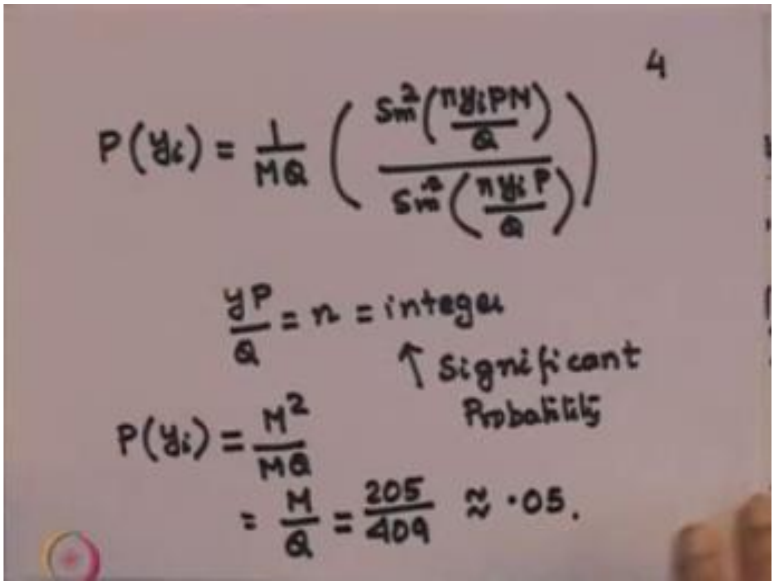
$$\Pr(y_i) = \frac{M^2}{MQ} = \frac{M}{Q} \approx 0.05 : M = 205, Q = 4096$$

- Repeated measurement of the first register can yield information about period.

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

Let us look at the slide there and when this happens, this thing.

(Refer Slide Time: 18:30)



4

$$P(y_i) = \frac{1}{MQ}\left(\frac{\sin^2\left(\frac{\pi y_i P M}{Q}\right)}{\sin^2\left(\frac{\pi y_i P}{Q}\right)}\right)$$

$$\frac{yP}{Q} = n = \text{integer}$$

↑ Significant Probability

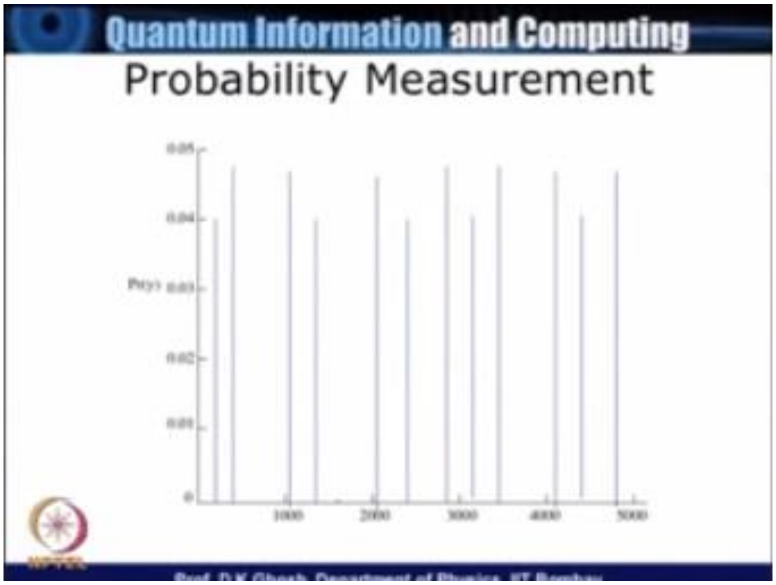
$$P(y_i) = \frac{M^2}{MQ}$$

$$= \frac{M}{Q} = \frac{205}{409} \approx .05.$$

Will approach M^2 because this is $\sin^2 \alpha x/ \sin^2 \alpha$ and when $\alpha \sin^2$, $\sin^2 x$ and when x tends to 0 this has a limit α^2 so in this case it is M^2 so therefore it is M^2/MQ, so the probability for which yi is our most likely to come out will be given by M^2/MQ which is equal to M/Q. And if you putting the values of M=205/4096 this works out approximately equal to 0.05 that is about 5%. So if you make a measurement of the first register in all likelihood, you will get those values of y being projected out for which the y are multiple of 205 or there about.

And as you go away from it this you can check it very easily as you go away from those values the probability significantly dies down. I have taken a.

(Refer Slide Time: 19:50)



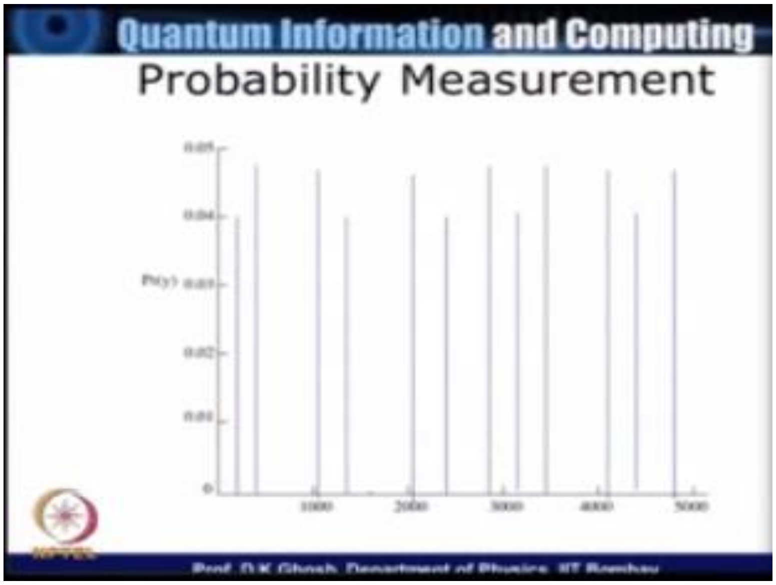
Quantum Information and Computing

Probability Measurement

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

Small calculation using these, and sort of trying to find out what are the likely values. So assuming certain number of measurements that I have made and this I simply did by randomly picking numbers which are close to multiples of 205 few of them because they are the ones which are likely to come out and if you calculate the probability.

(Refer Slide Time: 20:17)



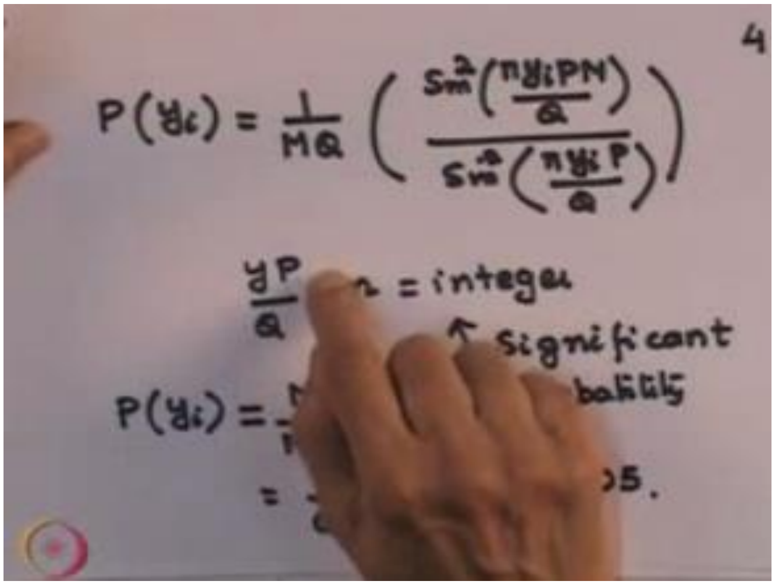
Quantum Information and Computing

Probability Measurement

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

The probability will show picks like this the 0.05 is approximately the upper limit of it. So the question now is that we having known what the period of the function is we could use all these argument to determine the principle, but let us look at what is it that we actually want what do you want is that this quantity.

(Refer Slide Time: 20:48)



4

$$P(y_i) = \frac{1}{MQ}\left(\frac{\sin^2\left(\frac{\pi y_i P N}{Q}\right)}{\sin^2\left(\frac{\pi y_i P}{Q}\right)}\right)$$

$\frac{yP}{Q}$ = integer

↑ significant

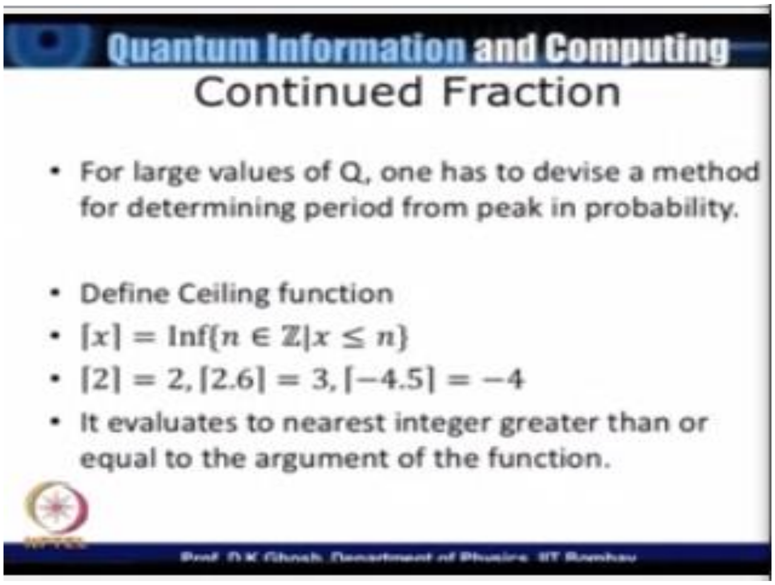
bability

$P(y_i) =$

$=$ 05.

YP/Q should be an integer so if I want YP/Q to be an integer.

(Refer Slide Time: 20:56)



Quantum Information and Computing

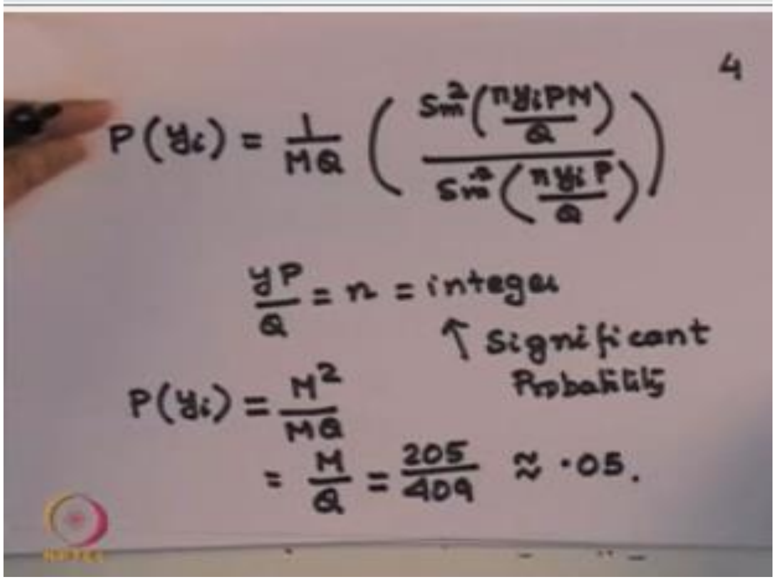
Continued Fraction

- For large values of Q, one has to devise a method for determining period from peak in probability.
- Define Ceiling function
- $\lceil x \rceil = \text{Inf}\{n \in \mathbb{Z} | x \leq n\}$
- $\lceil 2 \rceil = 2, \lceil 2.6 \rceil = 3, \lceil -4.5 \rceil = -4$
- It evaluates to nearest integer greater than or equal to the argument of the function.

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

I need to have a reasonably smart way of determining which for.

(Refer Slide Time: 21:05)



4

$$P(y_i) = \frac{1}{MQ}\left(\frac{\sin^2\left(\frac{\pi y_i P M}{Q}\right)}{\sin^2\left(\frac{\pi y_i P}{Q}\right)}\right)$$

$$\frac{yP}{Q} = n = \text{integer}$$

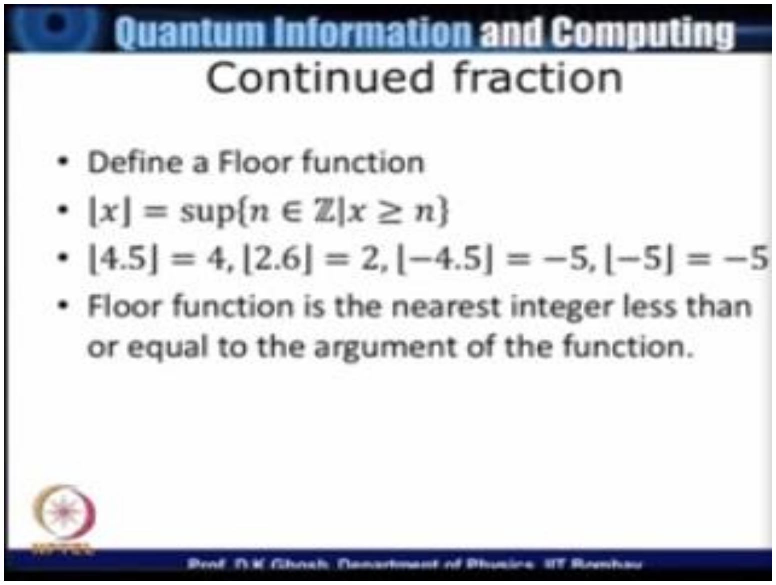
↑ Significant Probability

$$P(y_i) = \frac{M^2}{MQ}$$

$$= \frac{M}{Q} = \frac{205}{409} \approx \cdot 05.$$

What should be the value of P corresponding to a given n the Q is the question one and having known what are the values of Y which are likely to be projected out when we measure the first register how do I determine.

(Refer Slide Time: 21:24)



Quantum Information and Computing

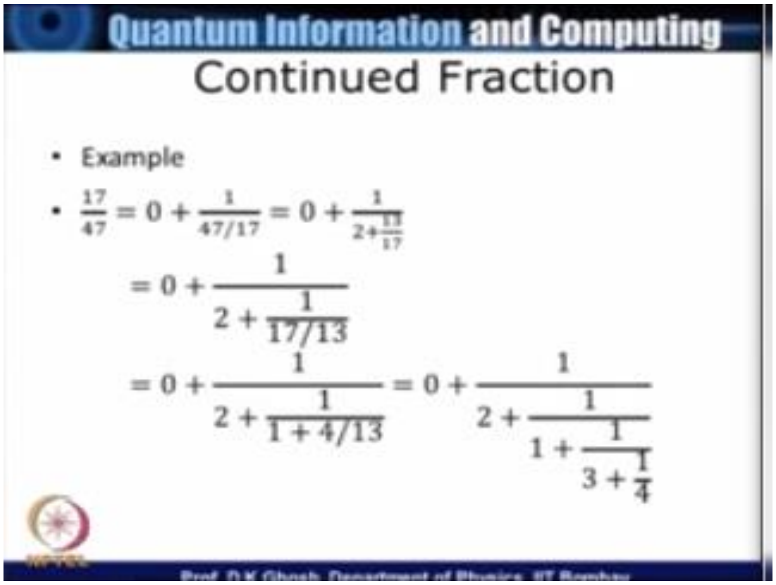
Continued fraction

- Define a Floor function
- $\lfloor x \rfloor = \sup\{n \in \mathbb{Z} | x \geq n\}$
- $\lfloor 4.5 \rfloor = 4, \lfloor 2.6 \rfloor = 2, \lfloor -4.5 \rfloor = -5, \lfloor -5 \rfloor = -5$
- Floor function is the nearest integer less than or equal to the argument of the function.

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

There is a reasonably smart and fast way of determining this and this is known as the method of continued fraction you must have been already familiar with that is the continued fraction in your school but let me give you a short review of what a continual fraction is.

(Refer Slide Time: 21:46)



Quantum Information and Computing

Continued Fraction

- Example
- $\frac{17}{47} = 0 + \frac{1}{47/17} = 0 + \frac{1}{2+\frac{13}{17}}$

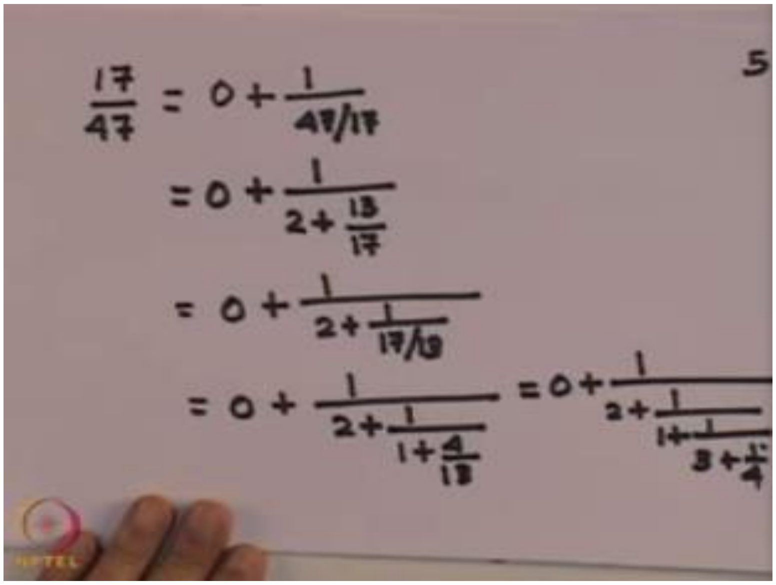
$$= 0 + \frac{1}{2 + \frac{1}{17/13}}$$

$$= 0 + \frac{1}{2 + \frac{1}{1 + 4/13}} = 0 + \frac{1}{2 + \frac{1}{1 + \frac{1}{3 + \frac{1}{4}}}}$$

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

So I will beat by giving an example you can read up any school level book to find out what it actually is.

(Refer Slide Time: 21:55)



5

$$\frac{17}{47} = 0 + \frac{1}{47/17}$$

$$= 0 + \frac{1}{2 + \frac{13}{17}}$$

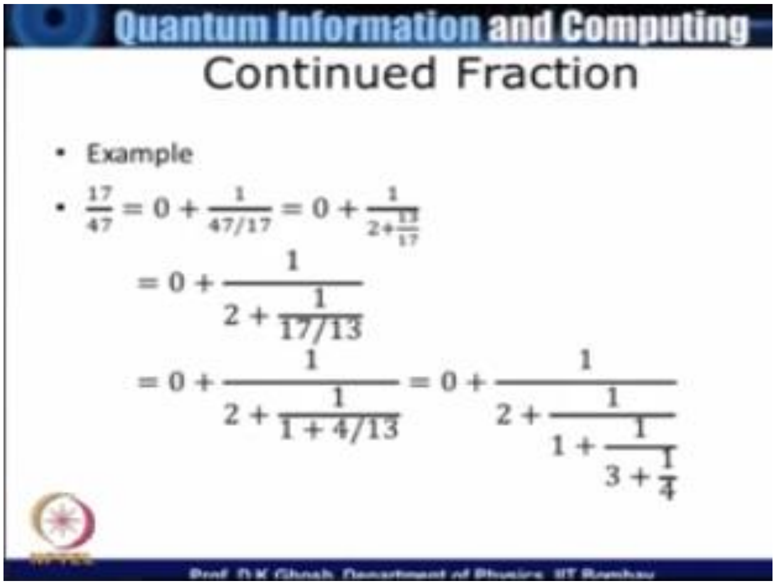
$$= 0 + \frac{1}{2 + \frac{1}{17/13}}$$

$$= 0 + \frac{1}{2 + \frac{1}{1 + \frac{4}{13}}} = 0 + \frac{1}{2 + \frac{1}{1 + \frac{1}{3 + \frac{1}{4}}}}$$

So let me take this number 7/47, 17/47 so how do I express this as a continue fraction so first thing is to find out it is integral part which in all our cases it will become zero because we have said that there would be a number here and this will be the bigger number. So this is 0 + now you write this as 1/47 /17.

Now this now will be 1/ again determine the integer part which is 2 in this case so 2 + 13 / 17 repeat this 1/2+1/17/13 see every time this smaller fraction you write as 1divided by the inverting that form fraction so it is 0+1/2+1/1+4/13 and that finally gives me 0 / 1 + 1 / 1 + 1/ 1 / 13 / 4 which is 3 + 1 / 4 now when I reach one here my expansion in the form of continued fraction stops and then what I do is the following.

(Refer Slide Time: 23:39)



Quantum Information and Computing

Continued Fraction

- Example
- $\frac{17}{47} = 0 + \frac{1}{47/17} = 0 + \frac{1}{2+\frac{13}{17}}$

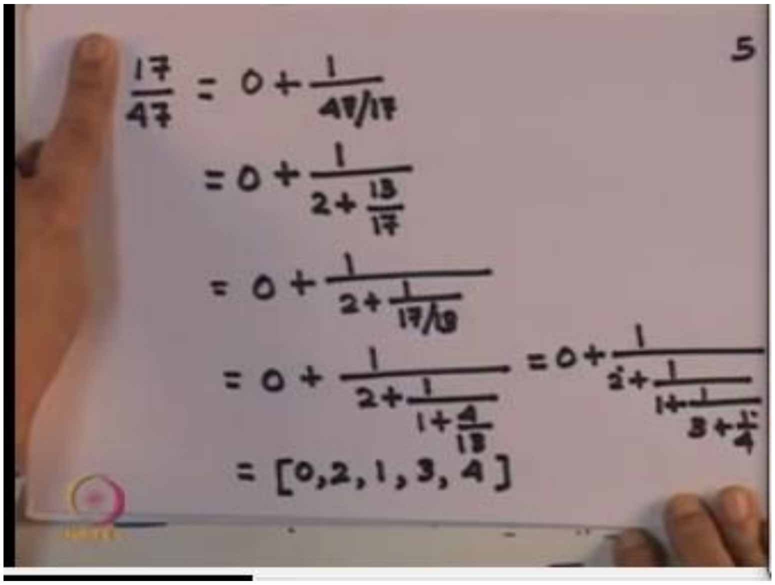
$$= 0 + \cfrac{1}{2 + \cfrac{1}{17/13}}$$

$$= 0 + \cfrac{1}{2 + \cfrac{1}{1 + 4/13}} = 0 + \cfrac{1}{2 + \cfrac{1}{1 + \cfrac{1}{3 + \frac{1}{4}}}}$$

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

I said that.

(Refer Slide Time: 23:42)



5

$$\frac{17}{47} = 0 + \frac{1}{47/17}$$

$$= 0 + \frac{1}{2 + \frac{13}{17}}$$

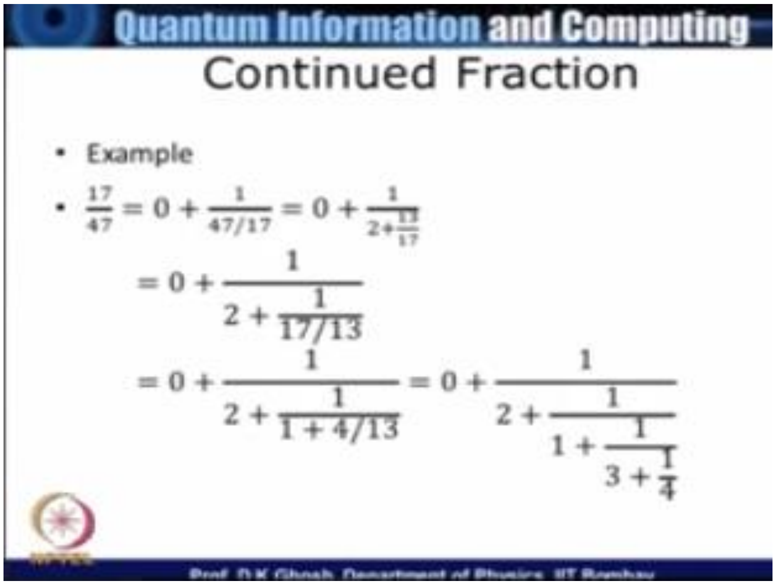
$$= 0 + \frac{1}{2 + \frac{1}{17/13}}$$

$$= 0 + \frac{1}{2 + \frac{1}{1 + \frac{4}{13}}} = 0 + \frac{1}{2 + \frac{1}{1 + \frac{1}{3 + \frac{1}{4}}}}$$

$$= [0, 2, 1, 3, 4]$$

This number is expressed as 0 2 these numbers 1 3 and finally 4. So given this you can immediately write down any this is the expansion given and you know what it is good actually for.

(Refer Slide Time: 24:09)



Quantum Information and Computing

Continued Fraction

- Example
- $\frac{17}{47} = 0 + \frac{1}{47/17} = 0 + \frac{1}{2+\frac{13}{17}}$

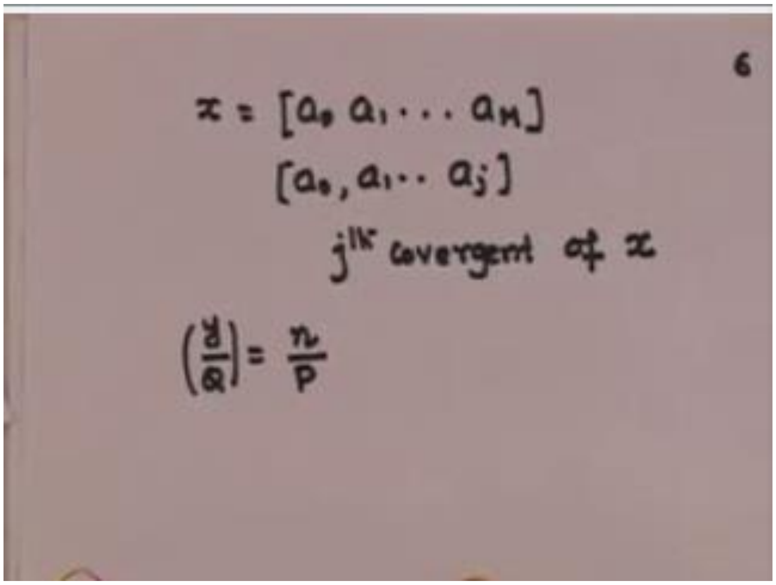
$$= 0 + \cfrac{1}{2 + \cfrac{1}{17/13}}$$

$$= 0 + \cfrac{1}{2 + \cfrac{1}{1 + 4/13}} = 0 + \cfrac{1}{2 + \cfrac{1}{1 + \cfrac{1}{3 + \cfrac{1}{4}}}}$$

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

So therefore if I have a number X whose continued fraction is given.

(Refer Slide Time: 24:20)



6

$x = [a_0\ a_1 \cdots a_M]$

$[a_0, a_1 \cdots a_j]$

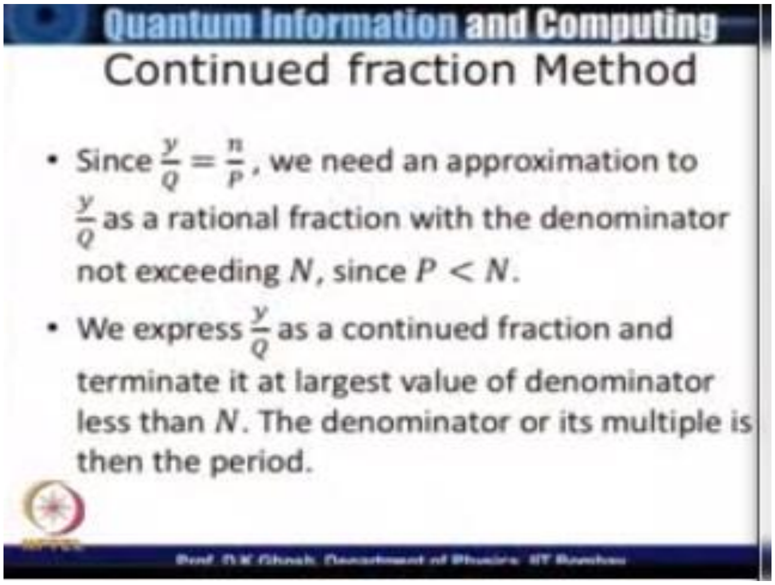
j^{th} covergent of x

$\left(\frac{y}{Q}\right) = \frac{n}{P}$

What I do is this I say that x is equal to some a_0 a_1 up to let us say a_m and supposing I stop this at a_0 a_1 up to A_J then I will say this is J^{th} convergent of X, so what we want now is how to express y/q as n / P is what you are looking for so y / q is the rational fraction and we want to find the period so what the, what we do is we express y / 2 as a continued fraction and look at various convergence of it.

But then approximate by that fraction for which the denominator starts exceeding the original number n.

(Refer Slide Time: 25:31)



Quantum Information and Computing

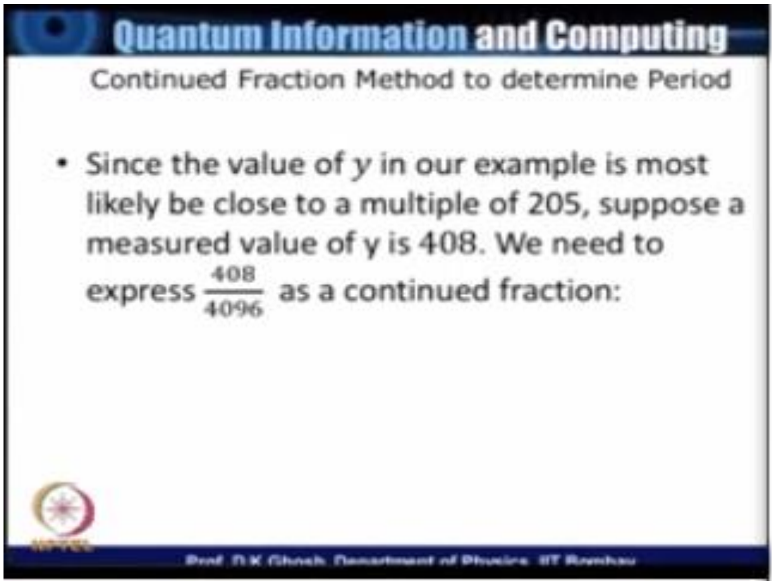
Continued fraction Method

- Since $\frac{y}{Q} = \frac{n}{P}$, we need an approximation to $\frac{y}{Q}$ as a rational fraction with the denominator not exceeding N, since $P < N$.
- We express $\frac{y}{Q}$ as a continued fraction and terminate it at largest value of denominator less than N. The denominator or its multiple is then the period.

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

So let me illustrate.

(Refer Slide Time: 25:32)



Quantum Information and Computing

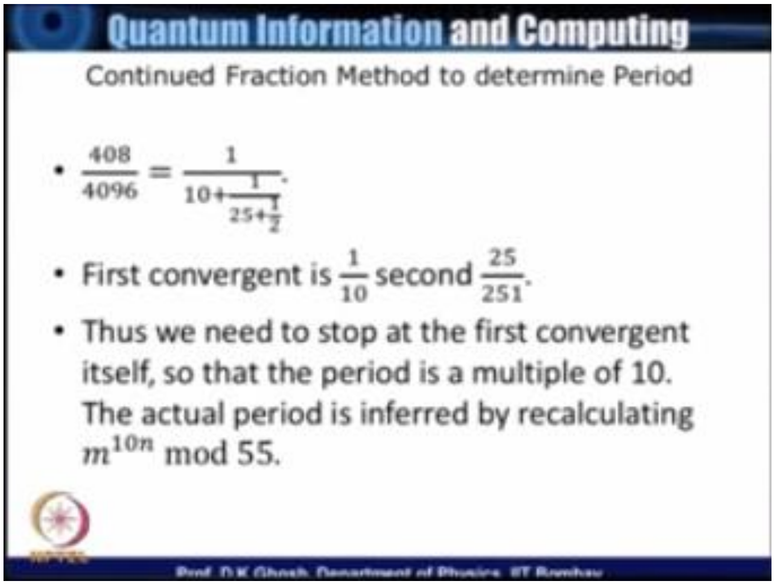
Continued Fraction Method to determine Period

- Since the value of y in our example is most likely be close to a multiple of 205, suppose a measured value of y is 408. We need to express $\frac{408}{4096}$ as a continued fraction:

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

How it works.

(Refer Slide Time: 25:35)



Quantum Information and Computing

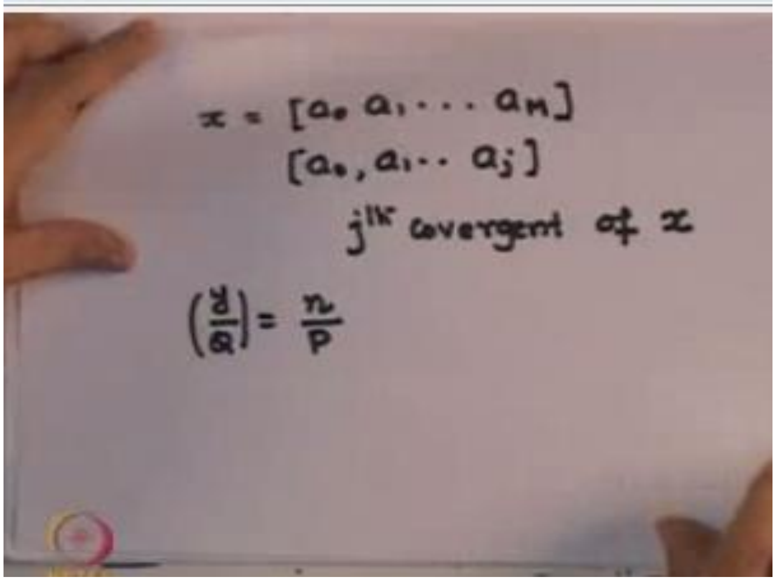
Continued Fraction Method to determine Period

- $\frac{408}{4096} = \frac{1}{10+\frac{1}{25+\frac{1}{2}}}$.
- First convergent is $\frac{1}{10}$ second $\frac{25}{251}$.
- Thus we need to stop at the first convergent itself, so that the period is a multiple of 10. The actual period is inferred by recalculating m^{10n} mod 55.

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

So we have.

(Refer Slide Time: 25:39)



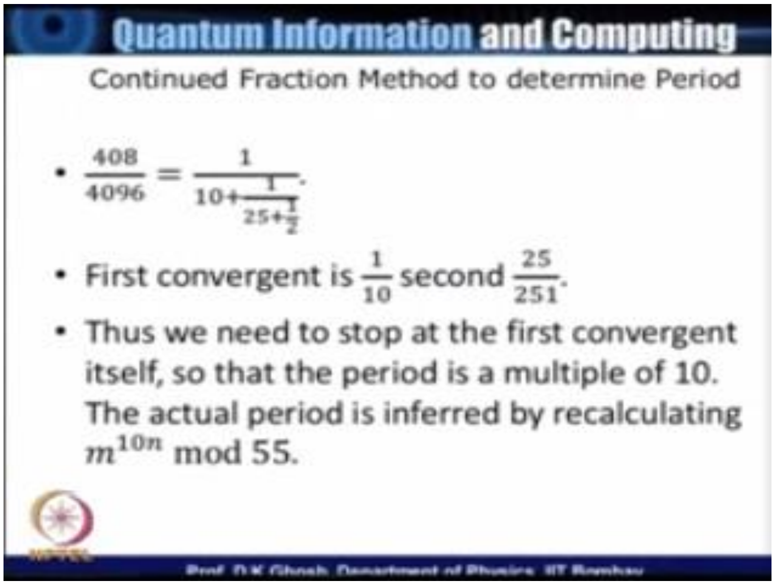
$x = [a_0\ a_1 \cdots a_n]$

$[a_0, a_1 \cdots a_j]$

j^{th} covergent of x

$\left(\frac{y}{Q}\right) = \frac{r}{P}$

(Refer Slide Time: 25:40)



Quantum Information and Computing

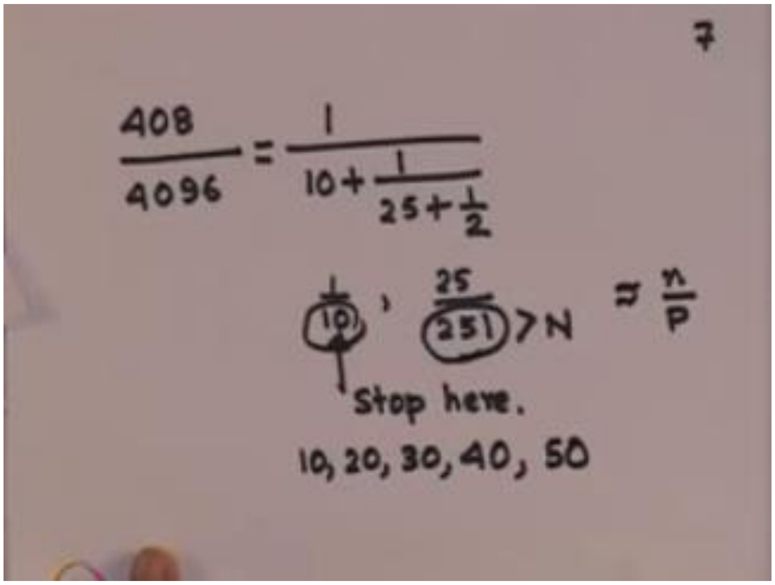
Continued Fraction Method to determine Period

- $\frac{408}{4096} = \frac{1}{10+\frac{1}{25+\frac{1}{2}}}$.
- First convergent is $\frac{1}{10}$ second $\frac{25}{251}$.
- Thus we need to stop at the first convergent itself, so that the period is a multiple of 10. The actual period is inferred by recalculating m^{10n} mod 55.

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

This number suppose I my result gave me 408 this is one of the possibilities because 205 x 2 is 410 and supposing I got 408.

(Refer Slide Time: 25:51)



7

$$\frac{408}{4096} = \cfrac{1}{10+\cfrac{1}{25+\cfrac{1}{2}}}$$

$$\frac{1}{\boxed{10}} , \frac{25}{\boxed{251}} > N \approx \frac{n}{P}$$

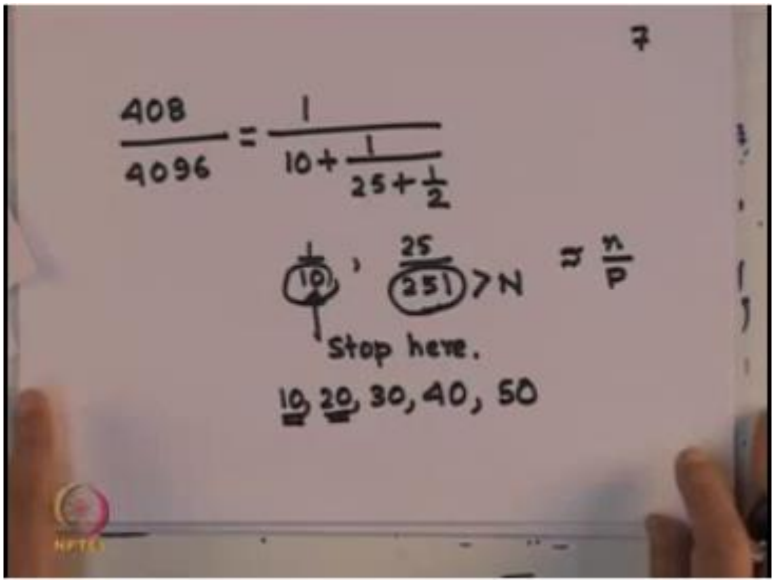
Stop here.

10, 20, 30, 40, 50

So I have 408 / 4096 I will not repeat this calculation but you can immediately check that this can be expressed as 1 / 10 + 25 + 1 / 2. So what are my various convergent my first convergent is simply 1 / 10. Now if you look at the second convergent this is obtained by removing this and the second convergent will then be 25/251.

But by this time this has already exceeded n so therefore I stop at the first convergent since 1 /10 is an approximation to this it means that and remember I am looking for an approximation which is n / p. So therefore, this number 10 must be in multiple because if there is a common factor between N and P that will canceled, and you can immediately see the possibilities are 10, 20 etc 30, 40, 50.Because after that will become 60 and we will exceed n and we have to stop. At that stage what you do is find out what is A^p

(Refer Slide Time: 27:20)



7

$$\frac{408}{4096} = \cfrac{1}{10 + \cfrac{1}{25 + \frac{1}{2}}}$$

$$\frac{1}{\boxed{10}}, \quad \frac{25}{\boxed{251}} > N \quad \approx \frac{n}{p}$$

Stop here.

$\underline{10}, \underline{20}, 30, 40, 50$

So if it is 10 I have given you already table 13^p and you will immediately see 13^{20} will become one, so this is a very fast way of finding out a period after having a measurement of the first register. With this we conclude our discussion of Shor's algorithm and the reason why you have spent so much of time on this particular algorithm is as we have pointed out this is one situation where a problem which is not solvable by the classical computers in polynomial time can be solved in a time with unit in time and resource or a complexity of the order of polynomial in logarithm of the import.

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