

**Implementation Aspects of Quantum Computing**  
**Prof. Debabrata Goswami**  
**Department of Chemistry**  
**Indian Institute of Technology, Kanpur**

**Lecture – 10**  
**Shor's Algorithm and QFT**

So, we are continuing on Shor's algorithm. So, here will do the Shor's Algorithm once more in the actual quantum stepwise and we will explain to you how this can be done stepwise.

(Refer Slide Time: 00:18)

**Shor's Algorithm - Preparing Data**

1. Load the input register with an equally weighted superposition of all integers from 0 to  $q-1$ . 0 to 255
2. Load the output register with all zeros.

The total state of the system at this point will be:

$$\frac{1}{\sqrt{256}} \sum_{a=0}^{255} |a, 000\rangle$$

Input Register      Output Register

Note: the comma here denotes that the registers are entangled

So, the first step which is very important is the preparation of the data. As I mentioned earlier please remember that although the quantum aspect of the process is being utilized in only one of the many steps of the Shor's Algorithm. The moment you are dealing with quantum data we have no choice but to essentially process the whole thing in a slightly different manner.

So, although the quantum principle is only going to be used may be not all the time, it will still be important to understand how this is done. So, in the first step which is preparing of the data will be loading the input register with an equally weighted superposition of all integers from 0 to  $q$  minus 1, which is basically 0 to 255 because we said we are dealing with 256 sets. So, the output register will be loaded with all 0s because we do not know anything about the output yet.

So, the total state of the system at this point will be the output registers all 0s and the input register containing every possible value from 0 to 255. The comma that I have just put here denotes the registers are entangled so that is actually very important. So, this particular part where we are preparing the data has the quantum part incorporated in it, in recognition of the fact that we are considering this to be in the entangled condition. So that is the part which is important in this quantum principle.

(Refer Slide Time: 02:16)

**Shor's Algorithm - Modular Arithmetic**

1. Apply the transformation  $x^a \bmod N$  to each number in the input register, storing the result of each computation in the output register.

Input Register	$7^a \bmod 15$	Output Register
$ 0\rangle$	$7^0 \bmod 15$	1
$ 1\rangle$	$7^1 \bmod 15$	7
$ 2\rangle$	$7^2 \bmod 15$	4
$ 3\rangle$	$7^3 \bmod 15$	13
$ 4\rangle$	$7^4 \bmod 15$	1
$ 5\rangle$	$7^5 \bmod 15$	7
$ 6\rangle$	$7^6 \bmod 15$	4
$ 7\rangle$	$7^7 \bmod 15$	13

The next part which is essentially modular arithmetic on this entire quantum system, is to apply the transformation  $x$  to the power  $a$  mod of  $N$  to each member of the input register, sorting the results of each computation in the output register.

So, these outputs register which was essentially unpopular or where all equally propagated with 0 are now going to have the values which are going to be the numbers, which have based on the values that we do and as you can see here these are now going to have repeats. So, this is the part which is one kind and this is the part if the other kind and this kind of shows up the principle that we have been talking about periodicity earlier.

(Refer Slide Time: 03:15)

Shor's Algorithm - Superposition  
Collapse

7. Now take a measurement on the output register. This will collapse the superposition to represent just one of the results of the transformation, let's call this value c.

Our output register will collapse to represent one of the following:

$|1\rangle$ ,  $|4\rangle$ ,  $|7\rangle$ , or  $|13\rangle$

For sake of example, lets choose  $|1\rangle$

So, once we have got in to this step which were all working with entangle qubits, we need to have the case were we can do as superposition collapse, so that we can understand the result because until that point of time we make the collapse we do not have the result and so we take a measurement on the output register and this will collapse the superposition into represent just one of the results of the transformation and if you call this value C, then this is exactly how it will look like or output register will collapse to represent one of the following. 1, 4, 7 or 13 because if you look at it these are the distinct number we are getting. Again the next time all it is just repeating. So, at any point of time if you look at the solution you will only get these four solutions that is it.

(Refer Slide Time: 04:32)

### Shor's Algorithm - Entanglement

ii. Since the two registers are entangled, measuring the output register will have the effect of partially collapsing the input register into an equal superposition of each state between 0 and  $q-1$  that yielded  $c$  (the value of the collapsed output register).

Since the output register collapsed to  $|1\rangle$ , the input register will partially collapse to:

$$\frac{1}{\sqrt{64}} |0\rangle + \frac{1}{\sqrt{64}} |4\rangle + \frac{1}{\sqrt{64}} |8\rangle + \frac{1}{\sqrt{64}} |12\rangle, \dots$$

The probabilities in this case are  $\frac{1}{64}$  since our register is now in an equal superposition of 64 values (0, 4, 8, ..., 252).

So, for an example say let us say that we have collapsed to one and see what happens this is a result of that. So now, since the two registers are entangled, measuring the output register will have the effect of partially collapsing the input register into an equal superposition of each state between 0 and  $q$  minus 1 that yielded the value of the collapsed output register, this is the quantum aspect of this entire problem.

The very fact that my input output registers were entangled when I measured the output register, it automatically effected what was there and what happened was it partially collapse the input register into an equals super position of each state between 0 and 1, such that the result that we measured  $c$  of the collapse output register was there.

So, essentially if we have found the value of 1 as my output register, so considering the case that we are just saying, then the input register will partially collapse to this. The probabilities of each of these case as you can see would therefore be probability will be 1 over 64, since our register is now in an equals superposition of 64 values which range from 0 to 250, but if you notice we already have 0 4 8 so on so forth, that is periodicity sitting in there, but let us see how it works.

(Refer Slide Time: 06:14)

**Shor's Algorithm - QFT**

We now apply the Quantum Fourier transform on the partially collapsed input register. The Fourier transform has the effect of taking a state  $|a\rangle$  and transforming it into a state given by:

$$\frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} |k\rangle e^{2\pi i a k / N}$$

$$\frac{1}{\sqrt{256}} \sum_{a \in A} |a\rangle, |b\rangle$$

$$\frac{1}{\sqrt{256}} \sum_{k=0}^{255} |k\rangle e^{2\pi i a k / 256}$$

Note: A is the set of all values that  $7^a \bmod 15$  yielded 1. In our case  $A = \{0, 4, 8, \dots, 252\}$

So the final state of the input register after the QFT is:

$$\frac{1}{\sqrt{256}} \sum_{a \in A} \frac{1}{\sqrt{256}} \sum_{k=0}^{255} |k\rangle e^{2\pi i a k / 256}, |b\rangle$$

So, the quantum Fourier transform that you have been alluding to if you now apply that on the partially collapse input register what happens? The Fourier transform has the effect of taking as state a and transforming it to a state by given by this.

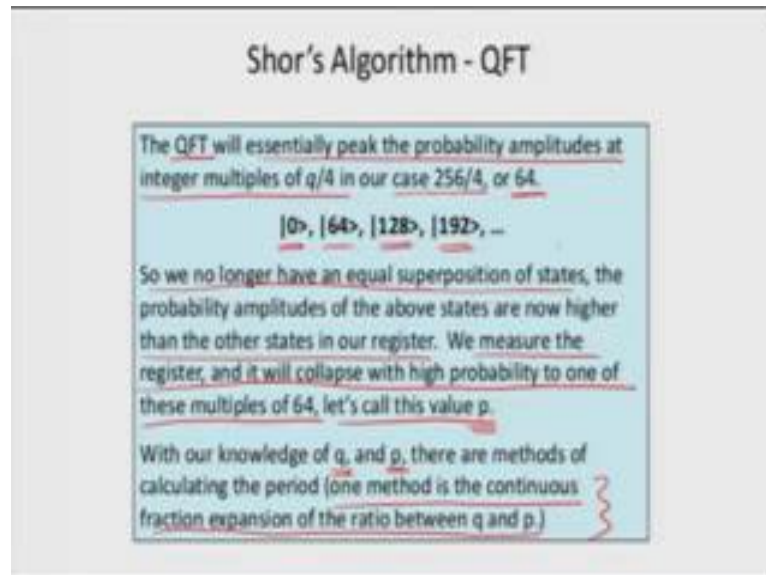
So, in order those of you do not remember, this is what quantum Fourier transformed does; essentially n if we are transform does which takes any state, you can in this case quantum state so itself bracket a, otherwise it is any state get state a which has been transformed into the other get state which has this particular exponential function, but associated with it and this is just the normalization that which is attach to this kind away transformation.

So, we get this as our overall solution for all of them a is the set of all values that 7 to the power a mod 15 yielded one. In our particular case a is going to have all these values, so final state of the input register after quantum to the transform will be of this kind.

Because I already have as I had mentioned in my last slide that this is my internal register, because all of these values 0 4 8 12 whatever, with these particular weight age factor can be represented by these; now it is in entangle mod with the value that I have just measured which is 1, which meant that when I apply the quantum Fourier transform, the other part, partially collapsed, the input register would now have this value. So, what will happen is the final state of the input register after the quantum Fourier transform

therefore, look like this entire thing which is as the result of getting 1 as my output register.

(Refer Slide Time: 08:44)



When I look at this what we have essentially done is, the quantum Fourier transform will essentially peak the probability amplitudes at integer multiple of  $q$  by 4 in our case 256 by 4 or 64.

So what will happen is will be getting values like 0, 64 128,192 and so on so forth. So, we no longer have an equal's superposition of states as we have started. So, that was the basic thing to understand here, that although we started with the equal superposition the act of measurement of one of them created the input states to also have changed, such that it no longer represents an equal superposition and the quantum Fourier transform essentially peaks the probability amplitudes in such a way that we can now distinguish them and we no longer have an equal superposition to state the probability amplitudes of the above states of now higher than the other states in our register.

We measure the register and it will collapse with high probability to one of these multiples of 64 let us call this value  $p$ . With our knowledge now of  $q$  and  $p$  there are method of calculating the period of this function, one method is the continuous fraction expansion of the ratio between  $q$  and  $p$ .

Now, this is again a classical principle and I can explain that in a minute, now this classical principle works out and since we have now essentially measured both the cases both  $q$  and  $p$  we are in the classical domain. So, we can easily do the rest of the process in a classical way; however, until now whatever we did was quantum mechanical. Although we used many principles of classical economic, but we have to remember that this quantum Fourier transform was essential to sort of understand or highlight the differences from the equal superposition state in order to collapse them to the periodic function. So, it was essentially the one which find out the way how thinks are; in a state which can now be used very simply to get to period of the function and in this case particularly it is like continuous fraction expansion and let us to see how that works.

(Refer Slide Time: 11:28)

**Shor's Algorithm - The Factors**

Now that we have the period, the factors of  $N$  can be determined by taking the greatest common divisor of  $N$  with respect to  $x^{(P/2)} + 1$  and  $x^{(P/2)} - 1$ . The idea here is that this computation will be done on a classical computer.

We compute:

$\text{Gcd}(7^{4/2} + 1, 15) = 5$

$\text{Gcd}(7^{4/2} - 1, 15) = 3$

Successfully factored 15!

Now, that we have the period, the factors of  $N$  can be determine by taking the greater common deviser  $N$  with respect to  $x$  to the power  $p$  divided by 2 plus 1, and  $x$  super  $p$  by 2 minus 1 that idea here is that the computation will be done on a classical computer. Now this part is all classical, that is because any way we are out about cubic system entanglement everything else associated is done.

So, for instance then in this particular case when we know the numbers, we have periodicity coming out as 4. So, it will be 7 divide into the power 4 by 2 plus 1, 15 gcd of that is 5 and the other one gcd of 7 to the power 4 divided two ways to minus 115 is three. So, here we have successfully factor 15. Now the point is for a simple severe

problem where we wanted to explain the idea to you it is how this goes, but if you want to generalize it this is where we had started with this can be done in a much more effective manner.

(Refer Slide Time: 12:35)

The slide is titled "Shor's Algorithm - Problems". It contains the following text:

- The QFT comes up short and reveals the wrong period. This probability is actually dependant on your choice of  $q$ . The larger the  $q$ , the higher the probability of finding the correct probability.
- The period of the series ends up being odd.

In the center, there is a light blue box with the text: "If either of these cases occur, we go back to the beginning and pick a new  $x$ ."

- Quantum modular exponentiation, much slower than the quantum Fourier transform.

Now, let me also look at a few aspects which can be of concerned while we are doing this, the few problems to look at is that the quantum Fourier transform comes of short and reveals the wrong period, how to handle that? The probability is actually dependent on your choice of the  $q$ , the larger the  $q$  the higher the probability of finding the correct probability.

So, that is the point which we have to remember that if you want to choose so even for factoring a number like 15, we choose  $q$  to be as largest to 56. If I have chosen say 64 or 8 or something small like that, the probability of finding the right answer would have been much wrong and the period would have been a difficulty.

So, the reason why this happens is that if you really want to find a period of any function, you really want to see how this one behaves so you want enough cycles to go and so if you are working with a very small number to start with, the finding of the period the oscillation or whatever you want to do in this would be difficult more and more difficult so it is better use a larger number to work with this. The period of series ends up being odd.



Now, this is one of the case where we have to actually just go back and pick a new number to start with, because start with a new co prime in that particular case because if the period of the series ends up being odd then the further on whatever we want do does not work properly because as you can see the final step essentially mean that we have to actually compute gcd of the period function divided by 2 and once you have odd number this does not come out be a proper way of looking at the fractions and so you can run into trouble. So, it is not a good idea if you have odd numbers to go forward.

The other part of the problem is that it may be a situation where you can actually get into a quantum modular exponentiation problem, which can be much slower than the quantum Fourier transform and we always often want to avoid this modular exponentiation part which we generally do and we always stick to the quantum Fourier transform method. Quantum modular exponentiation can be always applied, but it is not going to benefit us so we do not want get into those as processes.

(Refer Slide Time: 15:26)

### The Continued Fractions Algorithm

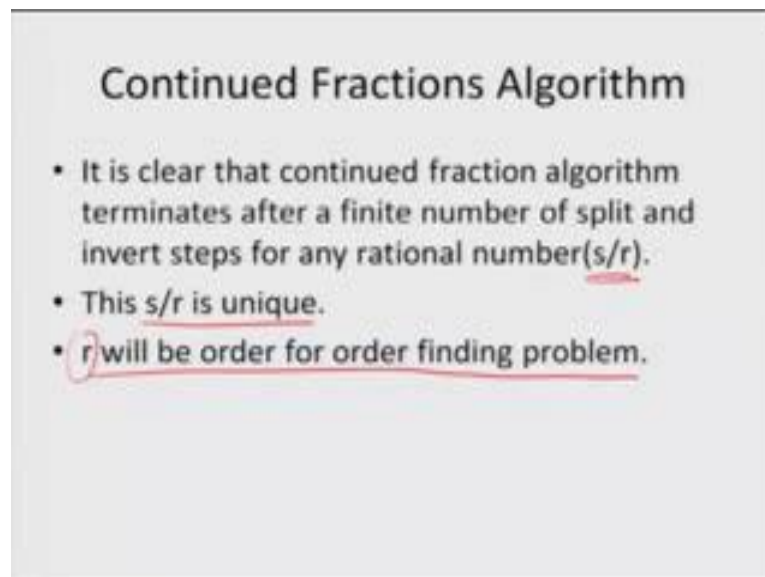
- Continued fraction is an expression of the form-
 
$$[a_0, \dots, a_M] = a_0 + \frac{1}{a_1 + \frac{1}{a_2 + \frac{1}{\dots + \frac{1}{a_M}}}}$$
- where  $a_0, a_1, \dots, a_m$  are positive integers.
- Any rational number can be represented as continued fraction.
- We say that  $[a_0, a_1, \dots, a_m]$  is convergent of  $[a_0, a_1, \dots, a_M]$  for  $m < M$ .
- Example:  $\frac{11}{13} = 0 + \frac{1}{2 + \frac{1}{5 + \frac{1}{2 + \frac{1}{1 + \frac{1}{2 + \frac{1}{2 + \frac{1}{2}}}}}}}$   
 $[0, 2, 5, 2, 1, 2, 2, 2]$

Now, the other part which has mention was the continued fraction algorithm and here is one of the cases, it is a continued fraction is an expression of the form where we can represent function series by just in terms of the fractional part of the starting point. So if I have mathematical form contains a 0 all the way up to a m if it can be represented in this form, then I can actually look at these and get a continued fraction approach in this way.

All of the guesses will work if  $a_0$  to  $a_m$  are all positive integers and any rational number actually can be represented as continued fraction. So, generally we say that the  $a_0$  to  $a_m$  components are a convergent of any of these sets of  $a_0$  to say  $a_m$  where, so small  $m$  versus large  $m$  whenever we have these two cases, we know that we can find out or we can state that these one of them is a subset or essentially a convergent form of the other in the case that small  $m$  is less than capital  $M$ .

So, you can have an example here, for example if you have the number 31 by 13, you can write it down in the form of continued fraction. So, basically 31 by 13 can be written in terms of 2 plus 1 by 13 or 2 plus 1 over 13 by 5 which is then in equivalent to this form and then that can be again brought down to this form; essentially what I am doing is I am bringing it down to a form where all the terms have similar forms. So, we get 2 is the first term, second term we get also 2, third time I get is 1, fourth one I get is also 1 and finally, we get the term 2. So, this is how a continued fraction can be represented for a number which has been given takes a little bit practice, but once you understand the representation as we have just shown you here in an example would be able to do this that is the idea.

(Refer Slide Time: 18:29)



### Continued Fractions Algorithm

- It is clear that continued fraction algorithm terminates after a finite number of split and invert steps for any rational number  $s/r$ .
- This  $s/r$  is unique.
- $r$  will be order for order finding problem.

Continued fraction algorithm terminates after a finite number of split is and inverts steps for any rational number  $s$  over  $r$ . So, that is actually good thing all right, this  $s$  over  $r$  is unique and  $r$  will be the order of the order finding problem and that is the advantage of

use in the continued fraction algorithm because you can always then find the order of the function.

So, for example, for  $N$  equal to 15, if you go through now the entire process which we have just now discussed all through several time.

(Refer Slide Time: 19:02)

### Example

- For  $N = 15$
- Choose a random co-prime integer  $x = 7$
- We get the order  $r = 4$  for the function  
$$f = x^r \pmod N$$
- So  $\gcd(x^2 - 1, 15) = 3$  is a non-trivial factor of 15.
- And  $\gcd(x^2 + 1, 15) = 5$  is another non-trivial factor.

Let me do this once more from all the steps for  $N$  equal to 15, we choose the random co prime integer  $x$  is equal to 7. We get the order  $r$  equal to 4 from the function as we have done before which is  $x$  to the power  $r \pmod N$ . So, the gcd of this function is 3 which is a non trivial factor of 15 and the gcd of the plus formed, 15 is another non trivial factor and. So, that is how we have done this.

(Refer Slide Time: 19:48)

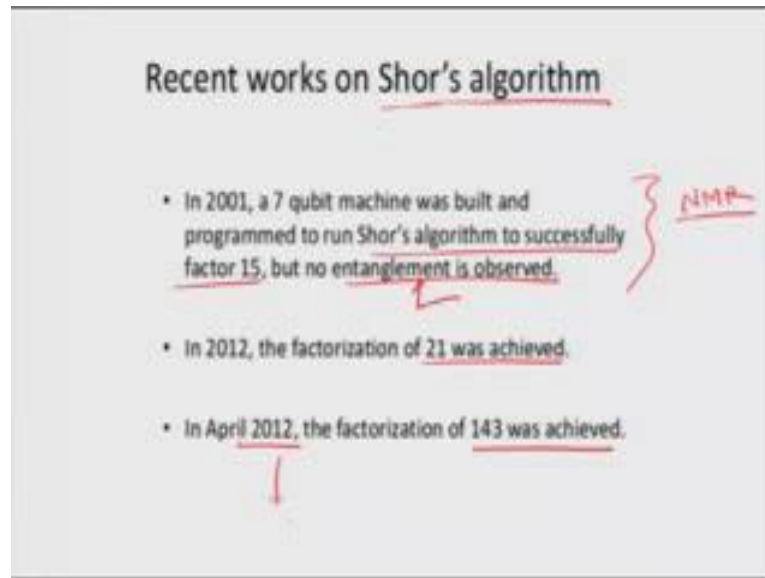


Now, there are several applications of Shor's algorithm, one is the as we discussed earlier in very beginning is the encryption problem. So, the factoring is very important for encryption because what happens is that if you have a large enough integer, it will take a long time for any computer to find it is primes and therefore, it is an important approach of being encryption which is what is happening here today nowadays that is the principle.

It also very effective in terms of quantum stimulation, because in many applications of quantum stimulation we require factorization as the part of problem and then there are many other cases where the technology aspects come in will deal with that later. There are issues related to both technology as well as theory, but we will get into these things later on we have just listed a few of them here.

Anyway cryptography related to your factorization issues and not being able to factorization issues these are technologies which are used to how to do this problem and spin off the theory lies in complexity theory DMRG theory, represent ability theory not all of this are important for this particular course, is just mentioned here to completeness.

(Refer Slide Time: 21:20)



Recent works on Shor's algorithm is something which is of interest in 2001 for example, a 7 qubit machine was built and programmed to run the Shor's algorithm to successfully factor number 15, but no entanglement was observed. This was because this was done in an NMR machine in an NMR machine it is extremely difficult to observe entanglement, although the process of factorization is possible it is a something which is very difficult to observe that so that was one thing.

In 2012 the principle was updated better and factorization was of 21 was achieved and in April 2012 the factorization of 143 as was also achieved. So, presently the process of Shor's algorithm becoming better and better is in hope I am sure they have been more work beyond the 2012 which has done a lot on Shor's algorithm; however, many a time it is not just the number which matters, but it is more important to find out how you can do better in terms of understanding and that is why the first few are mentioned here. Later on it is more important to understand whatever you have missed when we were doing the Shor's algorithm in earlier cases. So, that is one part of the problem that we have finished.

Now, the other thing which I wanted to do here was to actually give you a few examples of the applications and building scenario which I have been doing earlier also in a couple of time, not sure how these are going to come by right now I will just take a many time get back you on that.

So, after having gone through this entire process of Shor's algorithm completely in many different steps over two lectures.

(Refer Slide Time: 23:36)

### Shor's Algorithm

- It contains five steps, with only STEP 2 requires use of quantum computer.

STEP 1: Choose a random integer  $m < N$ , such that they are co-prime.

STEP 2: Use a quantum computer to determine the unknown period  $P$  of the function-  
 $f_{m,N}(x) = m^x \bmod N$

STEP 3: If ,  
 $P = \text{odd integer}$ , go to STEP 1.  
 $P = \text{even integer}$ , go to STEP 4.

I would like to actually do this once more in one go. So that you are able to understand how this entire process goes. So, it is a process of revisit. So, let me actually tell you we have done as of now.

The Shor's algorithm essentially contains of five steps, with technically only step two requires the use of quantum computer; however, as we have mentioned over and over again, use of qubit is make sure that we are essentially going to always use most of the step in this process to be in the quantum, except one we have started measure. So that I will mention where we go to point where we have started the measure. So, we need not follow the quantum way anymore.

So, the first step is the random integer finding, which is going to be less than  $N$  such that they are co prime. So given a number  $N$  that we want to factorize, we are going to choose an integer  $m$  which is less than the number that we are going to factorize such that they are going to be co prime that is the first step. Now this can be classical; however, the point you have to note is that this part would also mean that we are strict in ourselves on the qubit space that we are going to use for a quantum computer. So, that is why this is something where we want to keep as many qubit is as available to us.

The next step after setting it up which is technically a classical one is to use quantum computer to determine the non period of the function. So, that is the p for the period the function which we showed that it could done by using quantum Fourier transform in the most effective manner, initially we create the entanglement between the input states and the output states.

The output states essentially contain nothing to start out, but it is entangle to the input register that we have created and then we can apply quantum Fourier transform to go ahead and find out how they can be distinguish from being equal superposition to a point that we can then follow it on to the next step were we can find the period. The period finding can be done in a continued fraction manner, which is again a classical step once we get there then everything further on can be done in a classical manner.

So, the step 3 which is where the period if it is integer does not allow to further because the next periods the next part essentially involve mathematics, which would not work precisely if we keep using the odd integer. So, we have to go back to step one and start the process again; however, it is an integer even integer.

(Refer Slide Time: 26:44)

**Shor's Algorithm**

- STEP 4: Since P is even,  
→  $(m^{P/2} - 1)(m^{P/2} + 1) = m^P - 1 = 0 \pmod N$   
If  $m^{P/2} + 1 = 0 \pmod N$ , then go to STEP 1.  
If  $m^{P/2} + 1 \neq 0 \pmod N$ , then go to STEP 5.
- STEP 5: Compute  $d = \gcd(m^{P/2} - 1, N)$ .
- Exit with the answer d.

Then we can go to the step where we can find out the cases of mods between the plus 1 and minus 1 case of the number that we have found with the periods, and we can find out the case were if we get trivial solution then we go back to the first step. If we do not get

the trivial solution we can continue on to get the final solution which will be the factors of the numbers that we have chosen. So, this is basically the principle.

(Refer Slide Time: 27:19)

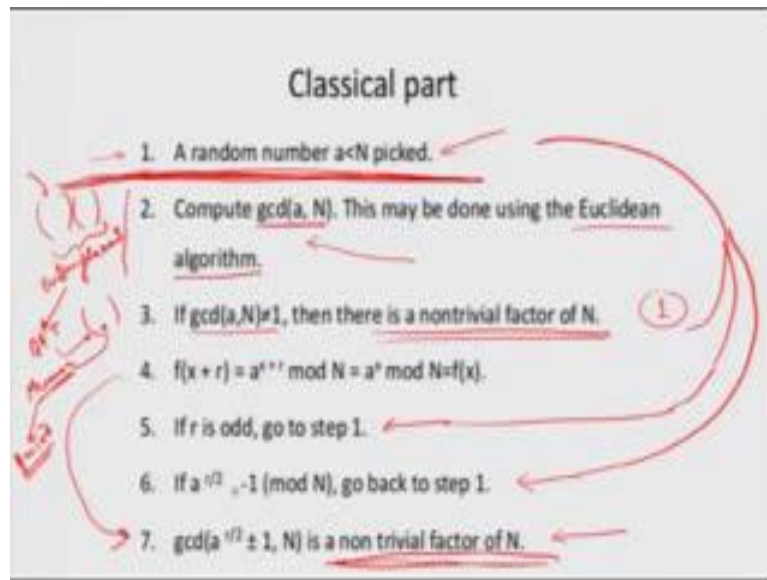
**Classical Part**

- The order-finding problem:
- Given:  $x$  and  $N$ ,  $x < N$  and  $\gcd(x, N) = 1$ .  
 $\Rightarrow$  The order of  $x$  is the least positive integer,  $r$  such that  $x^r = 1 \pmod{N}$
- Classical Part include <sup>the</sup> four steps except STEP 2.

The order finding problem can be classical, but when the case when we are actually using quantum mechanics we generally also would like to put this under the quantum sense by applying a quantum Fourier transform; however, once we have measured the periods or once we have measured the factors. Once again we do the process continued fraction to be able to get this problem and then we can go ahead with the first part. So, the classical part essentially includes four steps except the step 2 which we did.



(Refer Slide Time: 28:04)



So, in the classical form the random number is the one which is chosen, then this part which is again which is doing the Euclidean arithmetic which does the gcd finding, can all be done by using Euclidean arithmetic. So, in between this random number generation part to the part where we are going to find the orders we do the critical step of setting up the register and the output register, setting up the entanglement after them and finding quantum Fourier transform.

So, that we could make sure that the member of the input bit is are different and we started off from equal superposition here. These different set of number are then helping us to find the measure of their numbers the collapsed measure numbers and those measure numbers are then utilized in a continued fraction method to find the period and once the period of the function is found then that can be again used to find the gcd and then the factors and then we can keep on going back and forth by this principle.

(Refer Slide Time: 29:47)

### Shor's Algorithm - Periodicity

- An important result from Number Theory:  
 $F(a) = x^a \bmod N$  is a periodic function
- Choose  $N = 15$  and  $x = 7$  and we get the following:  
 $7^0 \bmod 15 = 1$   
 $7^1 \bmod 15 = 7$   
 $7^2 \bmod 15 = 4$   
 $7^3 \bmod 15 = 13$   
 $7^4 \bmod 15 = 1$   
⋮

So, the only path which is quantum mechanical is essentially embedded in this part which is where the part is explained, you can for trivial problems you can actually see how it works in terms of the classical way of finding the way of periodicity, you find the values of all the possibilities of raising it to the numbers and then taking the mods and getting the values and you can see that every fourth number after every four numbers in this particular example of factorize in 15, with a choice of the co prime 7, after every fourth number the repeating starts so we have period of 4. Now this in the quantum way of looking is able to happen is possible to be made understood when we do the registers.

(Refer Slide Time: 30:35)

### Quantum Part (Order Finding)

Choose a power of 2,  
 $Q = 2^l$  such that  
 $N^2 \leq Q < 2N^2$ ,

And consider  $f$  restricted to the set  $\{0, 1, \dots, Q-1\}$   
Where  $f(y) = \sum_{j=0}^{l-1} \frac{1}{\sqrt{2}} \omega^{xy}$   
 $\omega = e^{2\pi i/Q}$ ,  $Q$ -th root of unity

(Refer Slide Time: 30:37)

**Shor's Algorithm (quantum)**  
To Factor an odd integer  $N$  (Let's choose  $N=15$ ):

1. Choose an integer  $q$  such that  $N^2 < q < 2N^2$  let's pick 256
2. Choose a random integer  $x$  such that  $\text{GCD}(x, N) = 1$  let's pick 7
3. Create two quantum registers (these registers must also be entangled so that the collapse of the input register corresponds to the collapse of the output register)

- Input register: must contain enough qubits to represent numbers as large as  $q-1$ . up to 255, so we need 8 qubits
- Output register: must contain enough qubits to represent numbers as large as  $N-1$ . up to 14, so we need 4 qubits

And this is what was being explored explained here, where we choose the number such that we were able to first pick the particular value of  $x$ . Once we pick the value of  $x$  which is the co prime, then we went into the  $Q \pmod{N}$  and in this  $Q \pmod{N}$  it was important that the integer that we choose will be large enough. Now that also we have seen in the pit falls of the Shor's algorithm case that this larger enough number is important and. So, this is something where this part is to be taken care once more.

So, once we have understood this idea that the principle of picking the value of the co prime is the part which is classical, we have to be careful in making sure that we choose the number  $q$  which lies between the  $N^2$  and  $2N^2$  values, that is the part which is not going to be too small then we can use that number to set up our registers. Because this number  $q$  is something where the periodicity will be finally coming out from and if the numbers are too small then our periodicity does not form find out to be good. So, that is the reason why these are the periods where we have to be careful, the quantum part was once again explained slightly better here when we use the Fourier transform method to sort of make sure that one of the registers which is input register which was effected as a result of measuring the output register could be made to set in away. So, that it can be utilized later to find the period.

(Refer Slide Time: 32:00)

### Quantum Order finding

1. Initial state  $|\psi_0\rangle = |Reg1\rangle|Reg2\rangle = |0\rangle|1\rangle$
2. Create Superposition: Apply the Fourier Transform to Reg 1.
 
$$|\psi_1\rangle = \frac{1}{\sqrt{Q}} \sum_{x=0}^{Q-1} |x\rangle |1\rangle$$
3. Apply the unitary transformation  $U_f$ , to Reg2.
 
$$|\psi_2\rangle = \frac{1}{\sqrt{Q}} \sum_{x=0}^{Q-1} |x\rangle |1\rangle \xrightarrow{U_f} |\psi_2\rangle = \frac{1}{\sqrt{Q}} \sum_{x=0}^{Q-1} |x\rangle |f(x)\rangle$$

(Refer Slide Time: 32:24)

### Quantum Order Finding

4. Apply the Fourier Transform to Reg1.
 
$$|\psi_2\rangle = \frac{1}{\sqrt{Q}} \sum_{x=0}^{Q-1} |x\rangle |f(x)\rangle \xrightarrow{FT} |\psi_3\rangle = \frac{1}{Q} \sum_{x=0}^{Q-1} \sum_{y=0}^{Q-1} e^{-ixy} |y\rangle |f(x)\rangle$$
5. Make a measurement on the first register, obtaining  $y$ .
6. Find period  $P$  via continued fractions for  $y/2^L$ .

So, the way it was done was take the idea of measuring the first register and then to the second register which was left over was then continued to go ahead with the continued fraction approach. So, here is the once more the idea of the preparing the data which we focused on today, where we loaded the input register with an equally weighted superposition all the integers from 0 to minus 1 with the value of  $q$ , that we had chosen the number better be a large number otherwise it will be difficult to get the proper period and then the total system at that point is then utilized as an entangle set with the input register and the output register.

We measure the output register when we apply the transformation  $x$  to power  $a \bmod a$  to each member of the input register, this is the quantum approach; store the result of each computation in the output register. These output register measure essentially ensures that the input register values dependant on the exact value that is measured is the output register.

So, of all the possibilities, here we go when we make a measurement of the output register this will collapse the superposition to just one step. Now this is the part which is most important because it is a entangle situation once we have focused on one of the measurement that we make which is just one, then the rest of the result which exists in the input register is now collapsed also to represent only one of the following sets.

So, once we say that our output register will collapse to represent one of following of the possibilities, we have in turn also affected the input register. So, this is the part which is very important where we remove the equal's equation principle of the input registration case, because of the way how thinks are now. So, when we take a measurement of the output register, this will collapse to superposition to just one of the result of the transformation and once we choose that let say the value  $C$  in this case it can be any one of them.

In this particular example we had to chosen 1 then the input registers also got transformed from their original value but please note it would still be in an equal superposition of each state between 0 to  $q - 1$  which yielded the  $c$  state. So, this is the part which is very important still that the input register still remains in an equal superposition once we have done this collapse measurement of the output case.

So, the partially collapsed input register will of this kind, with each probability coming out as  $1/64$  which means these are all equals superposition. Now with this we cannot go further because if we have equal superposition now, we do not have a way of going forward to find periodicity or other things in a quantum register, we have to do something more and that is the part where we applied quantum Fourier transform. Once we applied the quantum Fourier transform the partially collapse input register the Fourier transform has the effect of taking the state and transform it into a state which has the periodicity sitting in their which makes the inputs set no longer equivalent that is the most important part here.

So, in our particular case what happened was, the final state of the input register after the quantum Fourier transform ended up being something like that, which is entangled to our measurement that we serve which is 1 which meant that it peaks the probability amplitudes at integer multiples of  $q$  by 4 which in our particular case is 64, and we no longer have equal superposition of states. So, only those states which are represented as 0, 64, 128, 192 and so forth, multiples of 64 which have been seen the others which we suppose to have equal superpositions are no longer available in that sense.

So, in this particular way if we now measure the register it will collapse to the high probability one of these multiples of 64, which we can call as some value  $p$ . Now given the value of now  $p$  and the  $q$  that we started off with, we can then find methods, classical methods which will help us to find the period of this. So, this allows us methods of finding calculating the periods, one method is continuous fraction approach expansion approach of the ratio between  $q$  and  $p$  which is quite popular in turns out to be computationally quite good and that is the classical one which I have shown later on, in one of the slides to show it to you as to how that represents the actual result that we are looking for.

So, for example, once we have so that actually gives you period. So, basically once you do this you would be finding out that that will give rise to the period of 4 and once we get that we can essentially automatically calculate the two factors. Now in order to get to that period of 4, so these are the error parts that we look at, but in order to get to the period of 4 what we did was we basically showed you an example where we essentially showed how the continued fraction principle works? We took any 2 numbers and we showed that you know basically can write it down in terms of this and write it in these forms. Similarly if you do that for the case that we are looking at for any rational number there is a unique value and the number as long as the value which is going to be given by.

So, what we will be finding is we will be finding  $s$  over  $r$  where this  $r$  is going to be  $s$  over  $r$  will be unique, the  $r$  will be the order of the finding process of the problem and that is what we found and this is the way will finally showed you, that for the number 15 found in a random co prime integer  $x$ , which is 7 we got the we get the order  $r$  for the function by applying this principle. Once we get that which is how we showed in terms

of continued fraction methods and others we can go and find out the non trivial factors of 15 and that was the basic idea.

So, with this I hope we have understood the principle of Shor's algorithm to a level that it can be utilized and implemented in the quantum way and this is one of the cases where the actual entanglement of process of quantum qubit is I have being utilize and. So, this is the most effective approach and shows exponential advantage over the classical case.

In the next few cases lectures would go into more and more application based on all the understanding that we are developed as of now.

Thank you