Quantum Factoring Algorithm
FQC Online Classes 2020

By

Dr. Vivekanand Bhat

Dept. of CSE

MIT Manipal

Modular Arithmetic and Greatest Common Divisor (GCD)

Modular Arithmetic: Given any positive integers x and n, x can be written uniquely in the form

$$x = kn + r$$

Where k is a non-negative integer, the result of dividing x by n, and the remainder r lies in the range 0 to n-1.

Example: If we divide 18 by 7 we get the answer 2, with remainder of 4.

$$18 = 2 \times 7 + 4$$

Definition: The GCD of two integers a and b is the largest integer which is a divisor of both a and b. We write this number as GCD(a, b).

Example: The GCD (18, 12) = 6

The divisors of 18 are: 1, 2, 3, 6, 9, 18

The divisors of 12 are: 1, 2, 3, 4, 6, 12

The largest common element is 6.

Euclid's Algorithm

- The GCD can be computed efficiently using Euclid's Algorithm:

$$\gcd(a,b) = \begin{cases} b & \text{if } a \mod b = 0 \\ \gcd(b, a \mod b) & \text{else} \end{cases}$$

with $a > b$

.

- Example: GCD(18, 12) = GCD(12, 18 mod 12) $\qquad$ 18 = 1 x 12 + 6

  = GCD(12, 6) = 6 $\qquad$ 12 = 2 x 6 + 0

Note: If GCD (a, b) = 1 ⇒ a and b co-prime.

Example: GCD (25, 16) = 1

⇒ 25 and 16 co-prime

Classical Factoring Algorithm

- Given N, we have to compute p and q such that N = p . q.
- For positive integers a and N (a < N). The order of *a* modulo *N* is defined to be the smallest integer *r* such that

$$a^r = 1 \bmod N.$$

- For example, the order of 2 (mod 3) is 2 since $2^2 \equiv 1 \pmod 3$, the order of 3 modulo 5 is 4 (since $3^2 = 9 \equiv 4 \pmod 5$; $3^3 = 27 \equiv 2 \pmod 5$; and $3^4 = 81 \equiv 1 \pmod 5$.)
- Another way to say this is that the order of *a* is just the period of the function

$$f(x) = a^x \bmod N$$

If r (where r is even) is the order of *a* mod *N*, then $GCD(N, a^{\frac{r}{2}}+1) and GCD(N, a^{\frac{r}{2}}-1)$

are the factors of N.

Classical Factoring Algorithm

- Example: Find the order of 2^x (mod 63), and use it to factor 63.
- $2 = 2$, $2^2 = 4$, $2^3 = 8$, $2^4 = 16$, $2^5 = 32$, $2^6 = 64 \equiv 1 \bmod 63$
- Hence order of 2 is 6.
- Then GCD $(63, 2^3 + 1)$ and GCD $(63, 2^3 - 1)$ are factors of 63.
- GCD(63, 9) = 9 and GCD(63, 7) = 7 are factors of 63.
- $63 = 9 .7$

Period finding

- Suppose a function $f(x) = f(x + r)$, then $f(x)$ is said to have period r.

Example: The following function is of period 2

x	0	1	2	3	4	5	6	7
$f(x) = 11^x \bmod 15$	1	11	1	11	1	11	1	11

Shor's factoring Algorithm

1. Choose a random integer $a < N$, *such that* GCD(a, N) = 1.
2. Quantum algorithm

   Create two quantum registers of required size and entangle them.

   Find period r of $f(x) = a^x \bmod N$.
3. If r is even and $a^{r/2} \neq -1 \bmod N$, then compute $p = \text{GCD}(N, a^{r/2} + 1)$ and

   $q = \text{GCD}(N, a^{r/2} - 1)$, which are factors of N. Otherwise go back to Step 1 and select different "a".

Note: Not every choice of a leads to a success, i. e. there are integers that will not work (failures)

Shor's Algorithm Example

- Example: Find of Factors of the number N = 15 using Shor's algorithm
- Create two Quantum Registers as follows:
- Register 1 (**$|\Psi_1>$**) : k = 3 qubits for representing the numbers 0 to 7 ($\leq N/2$)
  Register 2 (**$|\Psi_2>$**) : m = 4 qubits for the numbers 0 to 15 ($\leq N$)
  Choose a number $a \leq 15$ (with gcd(a, 15) = 1), e. g. a = 11
- Initialize all 7 (3+4) qubits to |0>
- **$|\Psi> = |0000000> = |\Psi_1> |\Psi_2> = |000> |0000>$**
- Randomize the first register. i.e. apply Hadamard gate to each of the three qubits in |000>

$$|\Psi> = (\frac{1}{\sqrt{2}}(|0>+|1>).\frac{1}{\sqrt{2}}(|0>+|1>).\frac{1}{\sqrt{2}}(|0>+|1>))|0000>$$

Shor's Algorithm Example

$$|\Psi> = \frac{1}{\sqrt{8}}(\underbrace{|000}_{0}> + \underbrace{|001}_{1}> + \underbrace{|010}_{2}> + ... + \underbrace{|111}_{7}>)|0000>$$

$$|\Psi> = (\frac{1}{\sqrt{8}}\sum_{k=0}^{7}|k>)|0000>$$

- Evaluate ***f*(*x*)** = a^x mod$N$ (here 11^x mod 15) for all x in the 1st register (0…7) simultaneously (quantum parallelism). Store the result in the 2nd register
- The values of f(x) are:

x	0	1	2	3	4	5	6	7
f(x) = 11^x mod 15	1	11	1	11	1	11	1	11

Shor's Algorithm Example

- The result of the simultaneous evaluation of ***f*(*x*) = *a*^{x}** mod ***N*** (here **11^x** mod **15**) for all ***x*** in 1st register (**0 … 7**) is in the 2nd register

$$|\Psi> = \frac{1}{\sqrt{8}}(|\underbrace{000}_{0}>|\underbrace{0001}_{1}> + |\underbrace{001}_{1}>|\underbrace{1011}_{11}> + \ldots + |\underbrace{111}_{7}>|\underbrace{1011}_{11}>)$$

$$|\Psi> = \frac{1}{\sqrt{8}}([|\underbrace{000}_{0}> + |\underbrace{010}_{2}> + |\underbrace{100}_{4}> + |\underbrace{110}_{6}>]|\underbrace{0001}_{1}>$$

$$+[|\underbrace{001}_{1}> + |\underbrace{011}_{3}> + |\underbrace{101}_{5}> + |\underbrace{111}_{7}>]|\underbrace{1011}_{11}>)$$

Shor's Algorithm Example

- Register 1 contains now the period ***r*** of interest, but only for identical measurement results in register 2.
- The searched for period ***r*** (here ***r* = 2**) is the distance between the components (**0, 2, 4, 6** or **1, 3, 5, 7**) in the 1st register for a single state of the 2nd register (1 or 11)
- The factors of N = 15 are p = GCD(N, $a^{r/2} + 1$) = GCD(15, 12) = 3 and

  q = GCD(N, $a^{r/2} - 1$) = GCD(15,10) = 5
- N = p . q = 3.5 = 15