Powers in modular math

mod 4 !

$0 \equiv 4 \equiv 8 \dots$ $\quad -1 = 4-1 = 3 \bmod 4$

$1 \equiv 5 \equiv 9 \dots$ $\quad -2 \equiv 2$

$2 \equiv 6 \equiv 10 \dots$ $\quad -3 \equiv 1$

$3 \equiv 7 \equiv 11 \dots$

$3^0 = 1$

$3^1 = 3$

$3^2 = 9 = 1$

$3^3 \equiv 3 \cdot 1 = 3$

$3^4 = 3^3 \cdot 3^1 = 3 \cdot 3 = 9 \equiv 1$

In this case we have a cycle in it, but it not necessarily exists for some different numbers

Some crypto algorithms take advantage of the randomness on these modulo numbers

The O of finding these patterns is $O(N-1)$ which N is the number we are in mod operate

Order → the first power r that ends a cycle (might not exist) ($x^r = 1 \bmod N$)

Order finding problem → take N and x, return the order

↳ Classically $O(N)$, quantum $O(\log N)$ using QFT

Shor's algorithm

↳ takes $N = pq$, which p and q are primes
↳ returns p and q

1: choose an x value that $2 < x < N$
2: find the order r. if it's odd, go back to the 1st step
3: check if $x^{(r/2)} + 1 = 0$. if it's true go back to 1:, else you have $(x^{r/2} - 1)(x^{r/2} + 1) = kN$

↳ this statement came from

$b = x^{r/2}$

$b^2 = x^r = 1 \bmod N$

$b^2 = 1 \bmod N$

$b^2 - 1 = 0 \bmod N$

$(b+1)(b-1) = 0 \bmod N$

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

this can be true when we must have either

$(x^{r/2} + 1) = 0$ or

$(x^{r/2} - 1) = 0$ or

$(x^{r/2} + 1)(x^{r/2} - 1) = kN \equiv 0 \bmod N$ ← the case we want

but $(x^{r/2} - 1) = 0 \bmod N$ can't be true, since:

$r/2 < r$ and $x^r = 1$

so $x^{r/2} \neq 1$, so $(x^{r/2} - 1) \neq 0$

however for $(x^{r/2} + 1) = 0 \bmod N$ we have 25% of chance to in fact have it

this way, we can say that

$N = pq \rightarrow kN = kpq$

we could also breakdown k as the following

$k = k_1 k_2$

$kN = (k_1 p)(k_2 q)$

$(x^{r_1} - 1)(x^{r_2} + 1) = (k_1 p)(k_2 q)$

namely $x^{r_1} - 1 = k_1 p$

$x^{r_2} + 1 = k_2 q$

after that, compute the $GCD(x^{r_1} - 1, N)$

$= GCD(k_1 p, pq)$

$= p$

and $GCD(x^{r_2} + 1, N)$

$= GCD(k_2 q, pq)$

$= q$

→ There's some improvement for this algorithm, already, this one is the first version

→ Quantum part (QPE)

$L = \lceil \log_2 N \rceil$ qubit on going to be used for U on $|\psi\rangle$

the basis vector space is: $\{0, \dots N-1\}$

define the operator as:

$U_x|y\rangle = |x\,y \mod N\rangle \rightarrow y \in \{0, \dots N-1\}$

$U_x|y\rangle = |y\rangle \rightarrow y \in \{N, \dots 2^L - 1\}$

U_x has r eigenvectors

$s = \{0, \dots, r-1\}$

$$|u_s\rangle = \frac{1}{\sqrt{r}} \sum_{k=0}^{r-1} e^{-i 2\pi s k / r} |x^k \mod N\rangle$$

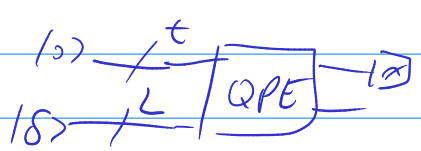
$$\varphi_s = s/r$$

$$U_x |u_s\rangle = e^{i 2\pi \frac{s}{r}} |u_s\rangle$$

(can't construct it directly once we don't know r

what we can do is computing:

$$|\delta\rangle = \frac{1}{\sqrt{r}} \sum_{s=0}^{r-1} |u_s\rangle = |1 \mod N\rangle_{\text{qubit}} = |00\dots01\rangle_L$$



↳ before the measurement we'll have all the eigenvectors as:

$$\frac{1}{\sqrt{r}} \sum_{s=0}^{r-1} |\tilde{\varphi}_s\rangle_t |u_s\rangle_L$$

and after learning all the first digits, we have $\hat{\varphi}_5$

$\hat{\varphi}_5$ is an approximation of φ_5

$\hat{\varphi}_5 \approx \frac{5}{n}$

↑

a $5/n$ is a rational number, we can write this as a continued fraction

ex: $\frac{9}{25} = 0 + \frac{1}{25/9} = 0 + \frac{1}{2 + 7/9} = 0 + \frac{1}{2 + \frac{1}{9/7}}$

$= 0 + \frac{1}{2 + \frac{1}{1 + 2/7}} = 0 + \frac{1}{2 + \frac{1}{1 + \frac{1}{3 + 1/2}}}$

then get → $[0, 2, 1, 3, 2]$

this form can be used to find close by rational numbers, just droping the last elment

$0 + \frac{1}{2 + \frac{1}{1 + \frac{1}{3}}} \rightarrow \frac{4}{15} = \frac{9}{25}$

← convergent of the continued fraction

and continue that way

so for that, we can use $\hat{\varphi}_s$ and find its continued fraction, then compute each convergent fraction (eg to $\frac{s}{r}$)
and finally check $x^r = 1 \bmod N$ for each r found in the convergents