Order Finding

Given $a<N$, $\gcd(a,N)=1$, find the order of N in $\mathbb{Z}_N^*$, i.e the smallest $r>0$, s.t $a^r \equiv 1 \pmod N$.

- The order of a is the period of the function $f_{N,a}(x) = a^x \pmod N$. $x \in \mathbb{Z}$. The function is classically computable by repeated squaring, efficiently. So, we can use the Period Finding over $\mathbb{Z}$ algorithm to solve this problem. [Remark: we only deal with $0 \le x < N^2$]

Remark: How to convert a classical computation of f ($f_{N,a}$) into a quantum one? It is important to return the auxillary $|0\rangle$ qubits into their previous state - otherwise, the "garbage" can affect the algorithms.

Shor's Algorithm

Factoring: Given N, find factorization.

Classically: Quadratic Sieve: $2^{\sqrt{\log N}}$

Number Field Sieve: $2^{\sqrt[3]{\log N}}$ [Oded Regev: "Why would anything with 3 in it would be the best?!"]

Claim: It is enough to find a nontrivial solution to $x^2 \equiv 1 \pmod N$.

Proof: Since $x^2 - 1 \equiv 0 \pmod N$, we have $N \mid (x-1)(x+1)$. Since the solution is not trivial, $N \nmid (x-1)$, $N \nmid (x+1)$. So $\gcd(N, x+1)$ is a nontrivial factor of N. □

Algorithm: Choose a random $a \in \{2, \dots, N-2\}$.

- If $\gcd(a,N) \neq 1$, we're done. Assume $\gcd(a,N)=1$.
- Compute the order r of a in $\mathbb{Z}_N^*$. If r is even, and $a^{r/2} \not\equiv -1 \pmod N$, then we are done, because by definition of r, $(a^{r/2})^2 \equiv 1 \pmod N$ and $a^{r/2} \not\equiv 1 \pmod N$.

In the rest of the proof, we'll show that this happens with good probability, assuming $N \neq p^k$.

- In order to check if $N = p^k$, we can compute roots of N, until we find an integer one. Obviously, $k \le \log N$, so we can just check 1 by 1.

For simplicity, assume $N = p \cdot q$ for 2 primes p, q:

By CRT, there is an isomorphism from $\mathbb{Z}_{pq}^*$ and $\mathbb{Z}_p^* \times \mathbb{Z}_q^*$:

$\mathbb{Z}_{pq}^* \ni a \longmapsto (a \bmod p,\ a \bmod q)$

So choosing a uniform a from $\mathbb{Z}_N^*$ is eqivalent to choosing a_1 uniformly from $\mathbb{Z}_p^*$ and choosing a_2 uniformly from $\mathbb{Z}_q^*$, and defining $a = (a_1, a_2)$.

Moreover, for any $a = (a_1, a_2)$. $\mathrm{ord}(a) = \mathrm{lcm}(\mathrm{ord}(a_1), \mathrm{ord}(a_2))$.

Write $r_1 = \mathrm{ord}(a_1)$, $r_2 = \mathrm{ord}(a_2)$ and $r_1 = 2^{k_1} \cdot \mathrm{odd}$, $r_2 = 2^{k_2} \cdot \mathrm{odd}$. (So $r = 2^{\max(k_1, k_2)} \cdot \mathrm{odd}$)

Notice that if $k_1 \neq k_2$, then r is even (not both are 0), and either r_1 or r_2 divide $\frac{r}{2}$, therefore either $a_1^{r/2}$ or $a_2^{r/2}$ is 1. Therefore, $a^{r/2} \not\equiv -1 \pmod N$ ($-1 = (-1, -1)$), and we're done.

To summarize, we need $k_1 \neq k_2$.

Claim: Let $m = 2^k \cdot \mathrm{odd}$. Then a random element of $\mathbb{Z}_m$ has order (additive, not multiplicative)

$2^k \cdot \mathrm{odd}$ with probability $1/2$, $2^{k-1} \cdot \mathrm{odd}$ with probability $\frac{1}{4}$, ...,

$2 \cdot \mathrm{odd}$ w.p $1/2^k$, odd w.p $1/2^k$.

Proof: Exercise.

Since $\mathbb{Z}_{p_1}^* \cong \mathbb{Z}_{p_1 - 1}$, $\mathbb{Z}_q^* \cong \mathbb{Z}_{q-1}$, we obtain that for any fixed value of k_1, the probability that $k_1 = k_2$ is at most $1/2$.

Exercise: Extend to all N (not only $N = pq$)

Exercise: Prove reverse reduction: solve "order finding" using factoring.

Discrete Log [Shor]

Consider $\mathbb{Z}_p^*$ for some prime p. Given a generator g, and an element a, find s s.t.: $g^s \equiv a \pmod p$.

- Consider the function $f: \mathbb{Z}_{p-1} \times \mathbb{Z}_{p-1} \to \mathbb{Z}_p^*$ defined by $f(x,y) = g^x \cdot a^y \pmod p$

Algorithm: 1)- Create $\frac{1}{p-1} \cdot \sum_{x=0}^{p-2} \sum_{y=0}^{p-2} |x, y, f(x,y)\rangle$

2) Measure 3rd register : $\frac{1}{\sqrt{p-1}} \sum_{y=0}^{p-2} |x_0 - sy, y\rangle$

3) Apply the QFT over $\mathbb{Z}_{p-1} \times \mathbb{Z}_{p-1}$ which is simply $QFT_{p-1} \otimes QFT_{p-1}$, yielding $\frac{1}{(p-1)^{3/2}} \sum_{j=0}^{p-2} \sum_{k=0}^{p-2} \sum_{y=0}^{p-2} e^{2\pi i j (x_0 - sy)/(p-1) + 2\pi i k y/(p-1)} \cdot |j, k\rangle$.

4) Measure. Probability of measuring j, k is

$$\frac{1}{(p-1)^3} \cdot \left| \sum_{y=0}^{p-2} e^{\frac{2\pi i}{p-1} \cdot (j \cdot (x_0 - sy) + ky)} \right|^2 =$$

$$= \frac{1}{(p-1)^3} \cdot \left| \sum_{y=0}^{p-2} e^{2\pi i/(p-1) \cdot y \cdot (k - js)} \right|^2 = \begin{cases} 1/p-1 & k - js \equiv 0 \pmod{p-1} \\ 0 & k - js \equiv 0 \pmod{p-1} \end{cases}$$

So we know that $k \equiv js \pmod{p-1}$.

If $\gcd(j, p-1) = 1$ then we can compute $s \equiv k \cdot j^{-1} \pmod{p-1}$.

That happens w.p. $\frac{\varphi(p-1)}{p-1}$ which is $\Omega\left(\frac{1}{\log\log p}\right)$. ($j$ is uniform in $\mathbb{Z}_{p-1}$)

Remark: This is a solution to the Hidden Subgroup Problem (HSP) over $\mathbb{Z}_{p-1}^2$ with hidden subgroup $\langle (1, -s) \rangle$.