Factoring

Any integer N can be written as

$$N = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_m^{\alpha_m}$$

where α_j are positive integers and p_j are primes.

Example 1

$$N = 15 = 3 \cdot 5, \ \alpha_1 = \alpha_2 = 1, \ p_1 = 3, p_2 = 5.$$

Definition 1 Greatest Common Divisor (GCD) *of integers a and b is the largest integer x s.t. $x|a$ and $x|b$ (here $|$ denotes "divides without a reminder")*

Example 2

$$a = 3 \cdot 3 \cdot 2 = 18, \ b = 3 \cdot 5 \cdot 2 = 30$$

$$\gcd(a, b) = 3 \cdot 2 = 6.$$

Let L be the number of bits in the binary representation of N, that is $N_2 = n_1 \cdots n_L$, $n_j = 0, 1$ (Ex. If $N = 15$, then $N_2 = \underbrace{1111}_{4bits}$)

Let z be an integer such that

1. $z^2 \pmod N = 1$
2. $z \pmod N \neq 1$ (if $z \pmod N = 1$, then $z^2 \pmod N = 1$, but we do not need this case)
3. $z \pmod N \neq N - 1$ (if $z \pmod N = N - 1$, then $z^2 \pmod N = 1$, and so we would like to exclude this possibility)

Theorem 1 $\gcd(z-1, N)$ *or(and)* $\gcd(z+1, N)$ *is (are) non-trivial factor(s) of N.*

Note that $\gcd(z - 1, N)$ and $\gcd(z + 1, N)$ can be computed using only $O(L^3) = O((\log_2 N)^3)$ operations using Euclid's algorithm.

Theorem 2 *Let x be an integer chosen uniformly randomly subject to requirements*

1. $1 \leqslant x \leqslant N-1$

2. *x is co-prime to N, i.e.* $\gcd(x, N) = 1$

Let r be the order of x, i.e., $x^r \pmod N = 1$. Then

$$\Pr(r \text{ is even and } x^{r/2} \pmod N \neq N-1) \geqslant 1 - \frac{1}{2^m}.$$

- If x is such as described in Theorem 2, then we take $z = x^{r/2}$.
- Recall that m is the number of primes in factorization of $N = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_m^{\alpha_m}$;
- Note that we do not need to check condition 3 formulated for Theorem 1, since since if $x^r/2 \pmod N = 1$ then the order of x is $r/2$, but we assumed that the order is r.

Algorithm for finding a factor of N

1. Randomly choose $x \in [1, N-1]$
2. If $\gcd(x, N) > 1$, then RETURN $\gcd(x, N)$ ($\gcd(x, N)$ is a nontrivial factor of N), go to Step 7.
   else: find the order r of $x \pmod N$ (use quantum computer here).

3. If r is even and $x^{r/2} \pmod N \neq N-1$, then assign $z = x^{r/2}$; else go to Step 1.

4. Compute $f_1 = \gcd(z-1, N)$ and $f_2 = \gcd(z+1, N)$.
5. If $f_1 | N$ RETURN(f_1).
6. If $f_2 | N$ RETURN(f_2).
7. The end.

Example 3 $N = 15$. *Assume we randomly took $x = 7$*

$$7^4 \pmod{15} = 1 \Rightarrow r = 4$$
$$x^{r/2} = 7^2 = 49,\ 49 \pmod{15} = 4 \Rightarrow 7^2 \pmod{15} \neq N-1 = 14$$
$$\Rightarrow z = x^{r/2} = 7^2 = 49$$
$$f_1 = \gcd(z-1, 15) = \gcd(48, 15) = 3$$
$$f_2 = \gcd(z+1, 15) = \gcd(50, 15) = 5$$

Both $f_1 = 3$ *and* $f_2 = 5$ *are factors of* $N = 15$.

Let us also find U *for these* N *and* x. *Recall that*

$$U|y\rangle \to |xy \pmod{15}\rangle.$$

We have $L = 4$ *and hence* U *is a* 16×16 *permutation matrix that conducts the mapping*

y	$7 \cdot y$	$7 \cdot y \pmod{15}$
0	0	0
1	7	7
2	14	14
3	21	6
$\vdots$	$\vdots$	$\vdots$

Using the correspondence between linear algebra notation and Dirac's notation, we get that the first 4 columns of U *are*

$$U = \begin{pmatrix} 1 & 0 & 0 & 0 & \\ 0 & 0 & 0 & 0 & \\ 0 & 0 & 0 & 0 & \\ 0 & 0 & 0 & 0 & \\ 0 & 0 & 0 & 0 & \cdots \\ 0 & 0 & 0 & 0 & \\ 0 & 0 & 0 & 1 & \\ 0 & 1 & 0 & 0 & \\ 0 & 0 & 0 & 0 & \\ 0 & 0 & 0 & 0 & \\ 0 & 0 & 0 & 0 & \\ 0 & 0 & 0 & 0 & \\ 0 & 0 & 0 & 0 & \\ 0 & 0 & 0 & 0 & \\ 0 & 0 & 1 & 0 & \\ 0 & 0 & 0 & 0 & \end{pmatrix},$$

Indeed this matrix moves $|0\rangle$ *to* $|0\rangle$*:*

$$U \cdot \begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix},$$

and $|1\rangle$ *into* $|7\rangle$

$$U \cdot \begin{pmatrix} 0 \\ 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}.$$