Factoring N ($=21$)

Notation: left side (blue) is the theory, right side (green) is the example

Suppose $N = p \cdot q$ where p & q are prime numbers

*) Find $x \in \mathbb{N}$ such that $\boxed{x^2 \equiv 1 \bmod N}$

$\rightarrow x^2 - 1 \equiv 0 \bmod N$

$\Leftrightarrow x^2 - 1 = \boxed{(x+1)(x-1) \text{ is multiple of } N}$

$\Rightarrow$ only 3 possibilities:

1) $x+1$ is a multiple of N
2) $x-1$ is a multiple of N
} $*_1$

3) $x+1$ is a multiple of p $(x+1 = c_1 \cdot p)$
and $x-1$ is a multiple of q $(x-1 = c_2 \cdot q)$
$(\Rightarrow (x+1)(x-1) = (c_1 \cdot c_2)(p \cdot q) = (c_1 c_2) N)$

*) If 3) is true ($\Leftrightarrow$ 1) and 2) are false):

N is multiple of p and $x+1$ is multiple of p

$\Rightarrow$ greatest common divisor: $\gcd(N, x+1) = p$

$*_1$ Note: These two points can be summarized as $x \neq \pm 1 \bmod N$

$x^2 \equiv 1 \bmod 21$

$x=8$: $8^2 \equiv 1 \bmod 21$ ✓

$\rightarrow 8^2 - 1 \equiv 0 \bmod 21$

$8^2 - 1 = (8+1)(8-1) = 9 \cdot 7$

1) ✗ 9 is not multiple of 21
2) ✗ 7 is not multiple of 21

$\Rightarrow$ 3) must be true:

check $\boxed{\gcd(9,21) = 3}$ ✓
$\boxed{\gcd(7,21) = 7}$

Euclids algorithm to efficiently compute gcd:

$\gcd(9,21) = 3$

$21 = 2 \cdot 9 + 3$

$9 = 3 \cdot 3 + 0$

last non-zero remainder

⇒ Factoring :

Find x such that $x^2 \equiv 1 \bmod N$ and
$x \neq \pm 1 \bmod N$
x is called a non trivial square root of $1 \bmod N$

How to find $x = 8$

1) Pick random $a < N$. e.g $a = 2$
2) Check that a is not a prime factor of N
   $\Leftrightarrow \gcd(a, N) = 1$
3) $f(b) = a^b \bmod N$
   Find smallest r such that $f(r) = a^r \bmod N = 1$
4) if r is odd → go back to 1)
5) If $a^{r/2} \equiv -1 \bmod N$ go back to step 1 *2
6) Factors of N are $\gcd(a^{r/2} \pm 1, N)$

This works with probability $> \frac{1}{2}$

*2 : This condition makes sure that 1) $x+1$ is not a multiple of N (1) ↑ previous page

Not: condition 2): $x-1$ is not a multiple of N is always satisfied for $x = a^{r/2}$

Proof:
Suppose $x-1$ is a multiple of $N \Rightarrow x \equiv 1 \bmod N$ and $x = a^{r/2}$
but we defined r to be the smallest integer such that $a^r \bmod N = 1$ ↓

$f(b) = 2^b \bmod 21$

$2^0 \equiv 1 \pmod{21}$
$2^1 \equiv 2 \pmod{21}$
$2^2 \equiv 4 \pmod{21}$
$2^3 \equiv 8 \pmod{21}$
$2^4 \equiv 16 \pmod{21}$
$2^5 \equiv 11 \pmod{21}$
$2^6 \equiv 1 \pmod{21}$ ⇒ $r = 6$ ⇒ $a^{r/2} = 2^3 = 8$
$2^7 \equiv 2 \pmod{21}$
$2^8 \equiv 4 \pmod{21}$ ↓ check by calculation & prove it
⋮
$2^{12} \equiv 1 \pmod{21}$

⇒ $f(b) = 2^b \bmod 21$ is periodic with period r and is 1-1 on each interval. *3

Task for a quantum computer to find this period r.

*3 : So we don't need to find the smallest r such that $f(r) = a^r \bmod N = 1$
We just need to find the period of $f(b)$ which is exactly equal to r.

References (on which this part of the presentation was based on)

"Algorithms" by Dasgupta, Papadimitriou, Vazirani (www.cs.berkeley.edu/~vazirani/algorithms.html)
see chapt 10

"Quantum Computation and Quantum Information" by M.A. NIELSEN, I.L. CHUANG (10th Anniversary Edition)
see chapt 5