3) Factoring

$N = 15$, $k = 7$, $m = 4$

$\gcd(7, 15) = 1 \quad \Rightarrow$ OK, coprimes

$$|0,0\rangle \xrightarrow{H \otimes I} \frac{1}{\sqrt{2^4}} \left(|0\rangle + |1\rangle + |2\rangle + \dots + |15\rangle \right) |0\rangle$$

$$\xrightarrow{U_f} \frac{1}{\sqrt{2^4}} \Big(|0,1\rangle + |1,7\rangle + |2,4\rangle + |3,13\rangle + |4,1\rangle + |5,7\rangle + |6,4\rangle + |7,13\rangle + |8,1\rangle + |9,7\rangle + |10,4\rangle + |11,13\rangle + |12,1\rangle + |13,7\rangle + |14,4\rangle + |15,13\rangle \Big)$$

$$\xrightarrow{I \otimes \text{measur.}} \frac{1}{\sqrt{2^2}} \left(|3\rangle + |7\rangle + |11\rangle + |15\rangle \right) |13\rangle$$

(random result of measurement)

$$\xrightarrow{QFT \otimes I} \frac{1}{\sqrt{2^2}} \left(|0\rangle + |4\rangle + |8\rangle + |12\rangle \right) |13\rangle$$

$$\xrightarrow{\text{measur.} \otimes I} |12\rangle |13\rangle$$

(result)

If we measured $|0\rangle$ or $|8\rangle$ we would not get factors in the end $\Rightarrow$ re-run Shor's alg.

$$r = \frac{2^4}{\gcd(12, 2^4)} = \frac{16}{\gcd(12, 16)} = \frac{16}{4} = 4$$

$$\gcd(k^{r/2} \pm 1, N) = \begin{cases} \gcd(7^2 + 1, 15) = \gcd(50, 15) = 5 \\ \gcd(7^2 - 1, 15) = \gcd(48, 15) = 3 \end{cases}$$

We got both factors of 15