0100001011100110101001111011011011101001101111110000101010001001101010011011101011011000101001111000001111110100101000011010001010111111110001010110011111110000010101101111001101010110 1

## Shor factoring (1994): breaking RSA

- **Quantum evaluation of $y^a \bmod N$ for random y, and ALL a at once**
- **Determine period r, mod N: $y^r = 1$, so $(y^{r/2} - 1)*(y^{r/2} + 1) = 0$ -> will share factor with N**