FACTORIZING AND PRIMALITY TESTING IS COUNTERINTUITIVE.

THERE ARE WAYS TO PROVE A NUMBER IS COMPOSITE W/O GIVING FACTORS.

E. G. WILSON'S THM.

P IS PRIME IFF

\((p-1)! + 1\) IS DIVISIBLE BY \(p\).

\(p = 2\) : 
\(1! + 1 = 2\) ✔

\(3\) : 
\(2! + 1 = 3\) ✔

\(4\) : 
\(3! + 1 = 7\) ✗

\(5\) : 
\(4! + 1 = 25\)  
\(5! + 1 = 120\) ✗

\(6\) : 
\(6! + 1 = 720\) ✗
State vector ($2^n$ elements) is not probabilities. $|\text{entry}|^2$ is prob. of that entry.

\[
\left| \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ -1 \\ \vdots \\ \pm 1 \end{pmatrix} \right| \text{ probs are } \frac{1}{4}
\]

\[
\left| \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 1 \\ \vdots \\ \pm 1 \end{pmatrix} \right| \text{ Illegal}
\]

You can't measure this directly but it affects future quantum ops.
GCD - GREATEST COMMON DIVISOR.

\[ \text{GCD}(6, 2) = 2 \]
\[ \text{GCD}(8, 9) = 1 \]
\[ \text{GCD}(10, 20) = 10 \]

LARGEST INT THAT DIVIDES BOTH INPUTS

\[ \text{GCD}(20, 24) = 4 \]

\[ N = \frac{24}{4} = 6 \]
\[ G = 3 \]

\[ 3^1 = 9 \equiv 2 \mod 3 \]
\[ 3^3 = 27 \equiv 6 \mod 3 \]

\[ 3^4 = 81 = 4 \quad 3^5 = 5 \]

\[ 3^6 = 1 \quad 3^7 = 3 \]

\[ 3^ \equiv 3^7 \mod 7 \quad p(7140) = 6 \]