C 7 9/21/20 P1

FACTORING 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.

DIV?

P = 2	1! + 1 = 2	←
3	2! + 1 = 3	←
4	3! + 1 = 7	×
5	4! + 1 = 25	—
6	5! + 1 = 121	×
7	6! + 1 = 721	—

STATE VECTOR (2^N ELEMENTS)

IS NOT PROBABILITIES.

$|\text{ENTRY}|^2$ IS PROB. OF THAT ENTRY

$$\begin{pmatrix} \frac{1}{2} \\ \frac{1}{2} \\ \frac{1}{2} \\ \frac{1}{2} \end{pmatrix}$$ PROBS ARE $\frac{1}{4}$

$$\begin{pmatrix} \frac{1}{2} \\ \frac{1}{2} \\ -\frac{1}{2} \\ \frac{1}{2} \end{pmatrix}$$ LEGAL

YOU CAN'T MEASURE THIS DIFFERENCE BUT IT AFFECTS FUTURE QUANTUM OPS.

GCD = GREATEST COMMON DIVISOR.

GCD(6,2) = 2

GCD(8,9) = 1

GCD(10,20) = 10

LARGEST INT THAT DIVIDES BOTH INPUTS

GCD(20,24) = 4

N = ~~10~~ ~~12~~ 7 GCD(3,7) = 1

a = 3

$3, 3^2 = 9 \xrightarrow{\text{mod } 7} 2 \quad 3^3 = 27 \Rightarrow 6$

$3^4 = 81 = 4 \quad 3^5 = 5$

$3^6 = 1 \quad 3^7 = 3$

$3^1 = 3^7 \pmod 7$ PERIOD = 6