Use Shor's algorithm to factor $N = 21$. Choose $a = 2$.

Use Quirk to implement the period finding algorithm with an 8-bit approximation of s/r, i.e., $m = 8$.

You may collaborate with other students, but you must submit your solutions.

Submit:

- Screenshot of the modular exponentiation circuit.
- Table similar to what you submitted in the previous lab.

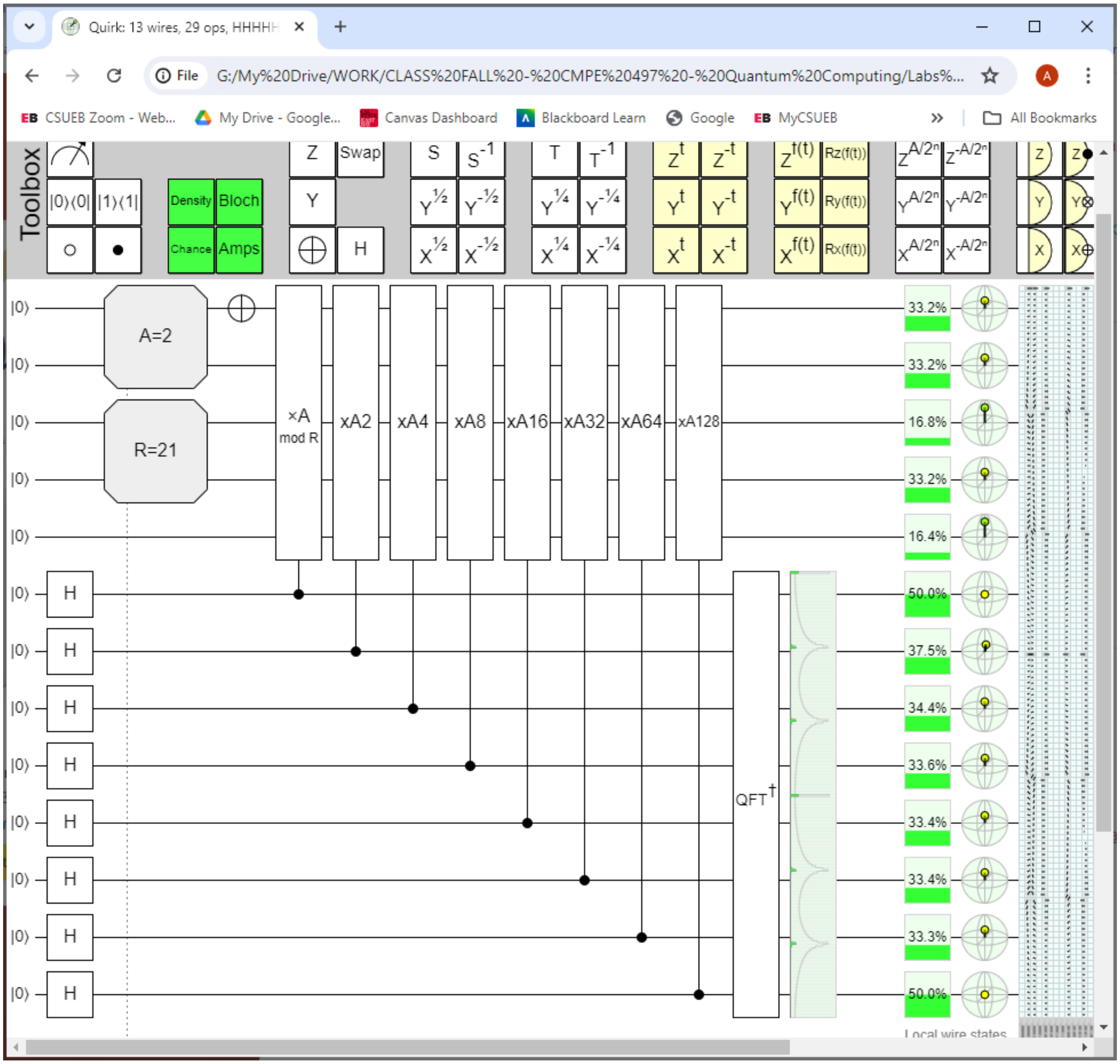
Probability	Binary approx. of s/r	Decimal approx. of s/r	Guess of s/r	s^r mod 21
…	…	…	…	…
…	…	…	…	…

- Answer these questions:
  - What is the period r?
  - Find p and q. You must show your work!
- HTML file of the quantum circuit.

SOLUTION

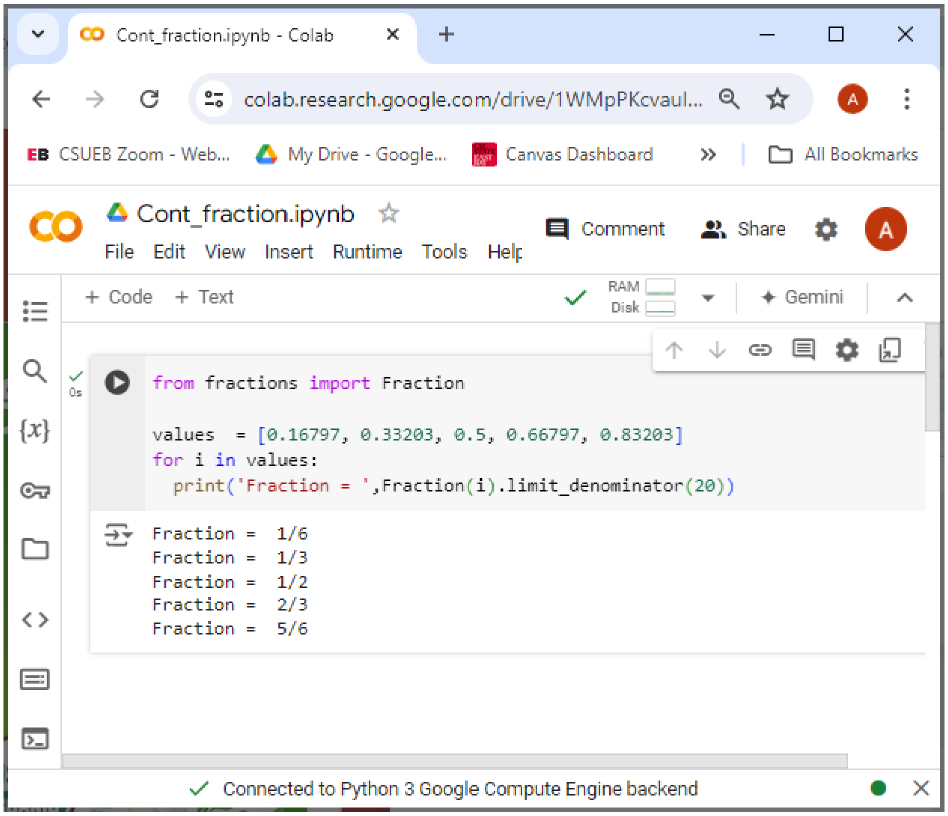
Step 1: $N = 21, a = 2 \rightarrow \gcd(2{,}21) = 1.$

Step 2: find the period using the period finding algorithm with $m = 8$: $a^x mod\ N \rightarrow 2^x mod\ 21$



Use binary fraction calculator: https://www.omnicalculator.com/math/binary-fraction

And python code for continued fraction to find the period $r < N \to r < 21$



Probability	Binary approx. of s/r	Decimal approx. of s/r	Guess of s/r	2^r mod 21
16.67%	$\|0000\ 0000\rangle$	0.00000	NA	NA
11.40%	$\|0010\ 1011\rangle$	0.16797	1/6	1
11.40%	$\|0101\ 0101\rangle$	0.33203	1/3	8
16.67%	$\|1000\ 0000\rangle$	0.5	1/2	4
11.40%	$\|1010\ 1011\rangle$	0.66797	2/3	8
11.40%	$\|1101\ 0101\rangle$	0.83203	5/6	1

Period $r = 6$.

- r is even.
- Is $a^{r/2}$ mod $N = (N-1)$? No, since $2^3\ mod\ 21 = 8\ \neq 20$

Step 3: calculate the factors – $a = 2, r = 6$

- $p = \gcd\left(a^{r/2} - 1, N\right) = \gcd(7{,}21) = 7$
- $q = \gcd\left(a^{r/2} + 1, N\right) = \gcd(9{,}21) = 3$