

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.

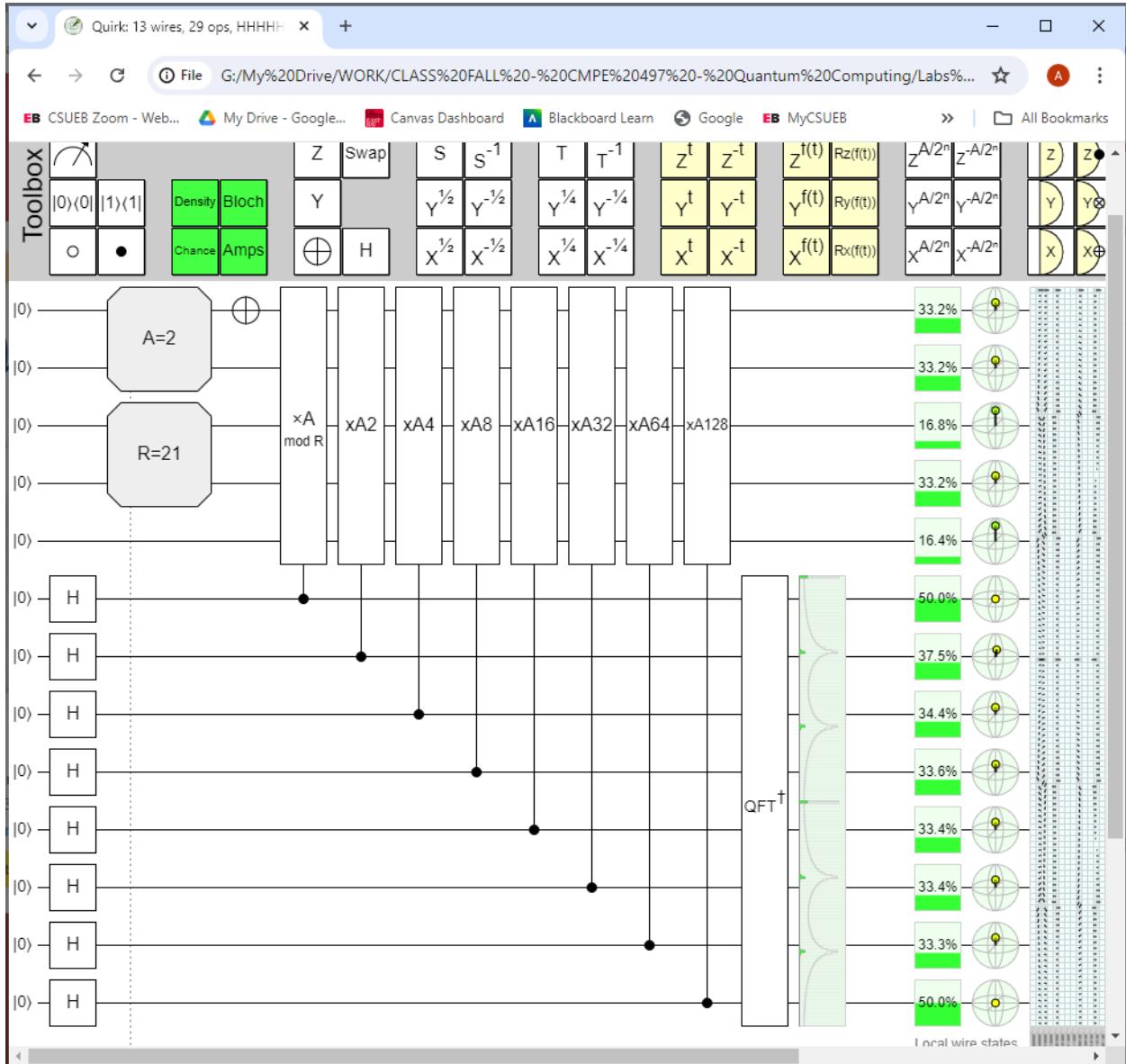
Probability	Binary approx. of s/r	Decimal approx. of s/r	Guess of s/r	$s^r \text{ mod } 21$
...	...	...	...	...
...	...	...	...	...

- 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  $m = 8$ :  $a^x \bmod N \rightarrow 2^x \bmod 21$



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

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

The screenshot shows a Google Colab notebook titled "Cont\_fraction.ipynb". The code cell contains the following Python script:

```

from fractions import Fraction

values = [0.16797, 0.33203, 0.5, 0.66797, 0.83203]
for i in values:
    print('Fraction = ', Fraction(i).limit_denominator(20))

```

The output of the code is displayed in the cell below:

```

Fraction =  1/6
Fraction =  1/3
Fraction =  1/2
Fraction =  2/3
Fraction =  5/6

```

The status bar at the bottom indicates "Connected to Python 3 Google Compute Engine backend".

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

Period  $r = 6$ .

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

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

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