Factoring Prime Numbers With Shor's Algorithm

Aaron Barbosa

To factor N = 77, find x such that:

$x^2 = 1 \pmod{77}$

My initial guess is $x = 8$

Finding the period of modulo operation:

Determine q

Pick q as the smallest power of 2 with $N^2 \le q \le 2N^2$

$77^2 \le q \le 2 \cdot 77^2$
$5629 \le q \le 11858$

Therefore $q = 2^{13} = 8192$

Initialize Registers

$$|\Psi\rangle = \frac{1}{\sqrt{8192}} \cdot \sum_{a=0}^{8191} |a\rangle |8^a \pmod{77}\rangle$$

```
load psi.mat
psi
```

```
psi = 8192×2
     0     1
     1     8
     2    64
     3    50
     4    15
     5    43
     6    36
     7    57
     8    71
     9    29
     ⋮
```

```
% I've left out the normalization factor
% for now to make it more readable
```

Observe Register 2

$|\psi\rangle$ Collapses into states that are consistent with observation.

```
y = datasample(psi(1:10,2),1);

psi_new = find(psi(:,2) == y);
psi_new = [psi_new-1 y*ones(length(psi_new),1)];
sz_new = size(psi_new);

psi_new
```

```
psi_new = 819×2
     9    29
    19    29
    29    29
    39    29
    49    29
    59    29
    69    29
    79    29
    89    29
    99    29
     ⋮
```

Perform Quantum Fourier Transform on Register 1

$$|\Phi\rangle = \frac{1}{8192} \cdot \sum_{a=0}^{8191} \sum_{c=0}^{8191} e^{\frac{i2\pi ac}{512}} \cdot |c\rangle |8^a \pmod{77}\rangle$$

Measure Register 1

After the quantum fourier transform, the probability of measuring register 1 to be in state $|c\rangle$ is:

$$p(c) = \left| \frac{1}{8192} \cdot \sum_{a}^{8191} e^{\frac{i2\pi ac}{8192}} \right|^2 \text{ where } 8^a = 29 \pmod{77}$$

```
prob  = @(c) abs((1/8192)*sum_coefs(psi_new,c)).^2;
% See end of script for sum_coefs function
```

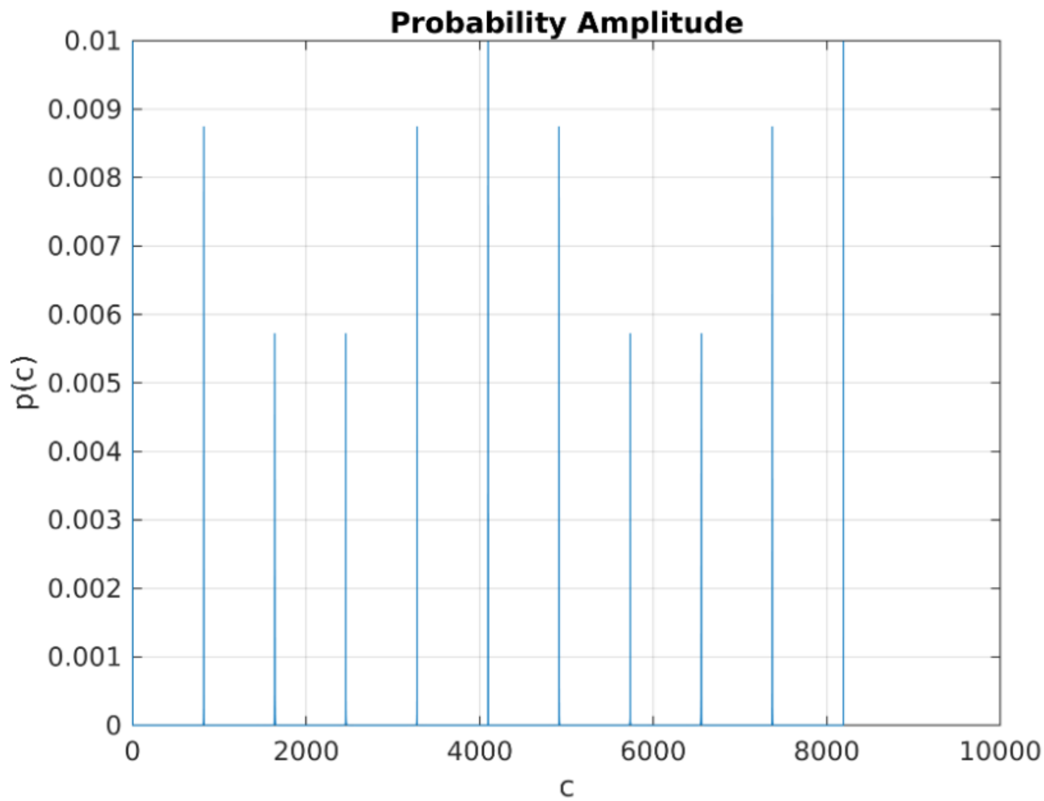
Plotting the Results:

```
x = [0:8192];

figure
plot(x,prob(x),'-')

title('Probability Amplitude')
xlabel('c')
ylabel('p(c)')
```

```
grid on
annotation('textarrow',[0.6322 0.6233],[0.6387 0.5387],'String','Peak at c = 5734')
```



Assume we get $|5734\rangle$:

Continued Fraction Convergence

$$\frac{y}{q} = \frac{5734}{8192} = \cfrac{1}{1 + \cfrac{1}{2 + \cfrac{1}{3 + \cfrac{1}{204 + \cfrac{1}{2}}}}}$$

Convergents:

$$\frac{1}{1} = 1$$

$$\cfrac{1}{1 + \cfrac{1}{2}} = \frac{2}{3}$$

$$\cfrac{1}{1 + \cfrac{1}{2 + \cfrac{1}{3}}} = \frac{7}{10}$$

$$\cfrac{1}{1+\cfrac{1}{2+\cfrac{1}{3+204}}} = \frac{1430}{2043}$$

Stop before denominator exceeds N = 77

$r_1 = 10$

Possible values of r are multiples of $r_1 = 10$

```
psi(1+10,:)
```

```
ans = 1×2
    10     1
```

```
psi(1+20,:)
```

```
ans = 1×2
    20     1
```

```
psi(1+30,:)
```

```
ans = 1×2
    30     1
```

```
psi(1+40,:)
```

```
ans = 1×2
    40     1
```

Period is $r = 10$

Finding Prime Factors

Period is $r = 10$

$x^r = 1 \pmod{77}$

r is even, so:

$$\left(x^{\frac{r}{2}}\right)^2 = 1 \pmod{77}$$

$$8^{10} = 1 \pmod{77}$$

$$8^{10} - 1^2 = 0 \pmod{77}$$

$$(8^5 - 1) * (8^5 + 1) = 0 \pmod{77}$$

Therefore 77 divides $(8^5 - 1) * (8^5 + 1)$. *77 Doesn't divide either, so this is done by the prime factors.*

One divides (8^5-1) *, the other divides* (8^5+1).

```
factor_1 = gcd(8^5-1,77)
```

```
factor_1 = 7
```

```
factor_2 = gcd(8^5+1,77)
```

```
factor_2 = 11
```

77 = 7 x 11

```
function s  = sum_coefs(p,c)
s = 0;
    for(a = 1:length(p))
        s = s + (exp((2*pi*i*p(a)*c/8192)));
    end
end
```