


$$m^a \pmod{N}.$$

$$m^P = 1 \pmod{N}.$$

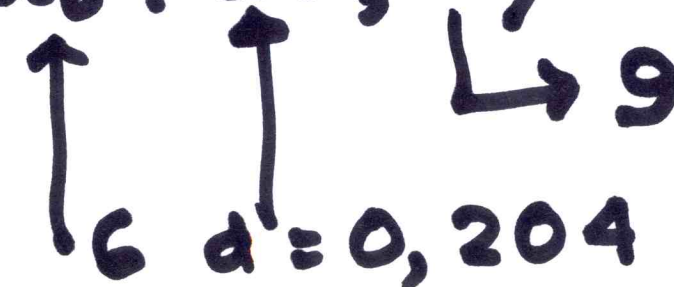
P : Period

$$(m^{P/2} - 1) \underbrace{(m^{P/2} + 1)} = 0 \pmod{N}.$$

205 states in the 1st  
 register 6, 26, 46, ... 4086


  
205.

$$|\Psi_3\rangle = \frac{1}{\sqrt{M}} \sum_{d=0}^{M-1} |x_0 + dP, k\rangle$$


  
6  $d=0, 204$  9

F.T

on  $\mathbb{Z}_Q$ 

3.

$$\begin{aligned}
 |\psi_A\rangle &= \frac{1}{\sqrt{MQ}} \sum_{y=0}^{Q-1} \sum_{d=0}^{M-1} e^{2\pi i y(x_0 + dP)/Q} |y, k\rangle \\
 &= \frac{1}{\sqrt{MQ}} \sum_{y=0}^{Q-1} e^{2\pi i y x_0 / Q} \left( \sum_{d=0}^{M-1} e^{2\pi i y d P / Q} \right) |y, k\rangle \\
 &= \frac{1}{\sqrt{MQ}} \sum_{y=0}^{Q-1} e^{2\pi i y x_0 / Q} \left( \sum_{d=0}^{M-1} z^d \right) |y, k\rangle
 \end{aligned}$$

$z = e^{2\pi i y P / Q}$

$$\sum_{d=0}^{M-1} z^d = \frac{1-z^M}{1-z}$$

$$z = e^{2\pi i y P/Q}$$

4

$$z = e^{2\pi i y P/Q}$$

$$\left| \sum_{d=0}^{M-1} z^d \right| = \left| \frac{z^{M/2} (z^{-M/2} - z^{M/2})}{z^{1/2} (z^{-1/2} - z^{1/2})} \right|$$

$$= \left| \frac{\sin\left(\frac{\pi y P M}{Q}\right)}{\sin\left(\frac{\pi y P}{Q}\right)} \right|$$

45

$$P(y_i) = \frac{1}{M^2} \left( \frac{\sin^2\left(\frac{\pi y_i P M}{Q}\right)}{\sin^2\left(\frac{\pi y_i P}{Q}\right)} \right)$$

$$\frac{y P}{Q} = n = \text{integer}$$

↑ Significant Probability

$$P(y_i) = \frac{M^2}{M^2 Q} = \frac{205}{409} \approx 0.05.$$

$$\frac{17}{47} = 0 + \frac{1}{47/17}$$

$$= 0 + \frac{1}{2 + \frac{13}{17}}$$

$$= 0 + \frac{1}{2 + \frac{1}{17/13}}$$

$$= 0 + \frac{1}{2 + \frac{1}{1 + \frac{4}{13}}}$$

$$= [0, 2, 1, 3, 4]$$

$$= 0 + \frac{1}{2 + \frac{1}{1 + \frac{1}{3 + \frac{1}{4}}}}$$

$$x = [a_0, a_1, \dots, a_n]$$

$$[a_0, a_1, \dots, a_j]$$

$j^{\text{th}}$  convergent of  $x$

$$\left(\frac{p}{q}\right) = \frac{z}{p}$$

$$\frac{408}{4096} = \frac{1}{10 + \frac{1}{25 + \frac{1}{2}}}$$

$\frac{1}{10}$ ,  $\frac{25}{251} > N \approx \frac{1}{4}$   
 Stop here.

10, 20, 30, 40, 50