

Sample Solution

8.1 Let  $m = 6$ .

Step 1 :  $\gcd(6, 35) = 1$ .

Step 2 :  $6^2 = 36 \equiv 1 \pmod{35}$ ,  $P = 2$ .

Step 3 :  $P = 2$  is even.

Step 4 :  $(6^1 - 1)(6^1 + 1) = 35 \equiv 0 \pmod{35}$ .

Step 5 :  $\gcd((6^1 - 1), 35) = 5$ ,  $\frac{35}{5} = 7$ ,  $35 = 5 \cdot 7$ .

8.2 Note that  $441 < 2^n < 882$ ;  $n = 9, Q = 2^n = 512$ . We can show that  $P = 6$  is the period of 11 in  $\mathbb{Z}_{21}$ . For example, use WolframAlpha to solve equation  $Mod[11^a, 21] = 1$ . Let  $f : \mathbb{N} \rightarrow \mathbb{N}$  be such that  $f(a) = m^a$ ,  $|\psi_0\rangle = |REG_1\rangle|REG_2\rangle = |00\dots 0\rangle|00\dots 0\rangle$ . Then  $|\psi_1\rangle = \frac{1}{\sqrt{Q}} \sum_x |x\rangle|0\rangle$ ,  $|\psi_2\rangle = U_f|\psi_1\rangle = \frac{1}{Q} \sum_x |x\rangle|f(x)\rangle$ .

Apply QFT on  $|REG_1\rangle$ , we yield  $|\psi_3\rangle = (\mathcal{F} \otimes I)|\psi_2\rangle = \frac{1}{512} \sum_x \sum_y \omega_n^{-xy} |y\rangle|f(x)\rangle$ .

Let  $Q = Pq + r, p \in \mathbb{N} \cup \{0\}, 0 \leq r < P, Q_0 = Pq$ . By the formula in p.145,

$$Prob(y) = \begin{cases} \frac{r \sin^2(\frac{\pi Py}{Q}(\frac{Q_0}{P} + 1)) + (P-r) \sin^2(\frac{\pi Py}{Q} \cdot \frac{Q_0}{P})}{Q^2 \sin^2(\frac{\pi Py}{Q})} & Py \not\equiv 0 \pmod{Q}, \\ \frac{r(Q_0+P)^2 + (P-r)Q_0^2}{Q^2 P^2} & Py \equiv 0 \pmod{Q}. \end{cases}$$

That is,

$$Prob(y) = \begin{cases} \frac{r \sin^2(\frac{3\pi y}{256}(\frac{Q_0}{6} + 1)) + (6-r) \sin^2(\frac{3\pi y}{256} \cdot \frac{Q_0}{6})}{262144 \sin^2(\frac{6\pi y}{512})} & 6y \not\equiv 0 \pmod{512}, \\ \frac{r(Q_0+6)^2 + (6-r)Q_0^2}{9437184} & 6y \equiv 0 \pmod{512}. \end{cases}$$

We see that  $Prob(y) \sim 0.167$  if  $Py \equiv 0 \pmod{Q}$  and  $Prob(y) \sim 0.00087$  if  $Py \not\equiv 0 \pmod{Q}$ .

8.3 Note that  $\frac{61}{45} = 1 + \frac{1}{2 + \frac{16}{13}} = 1 + \frac{1}{2 + \frac{1}{1 + \frac{13}{3}}} = 1 + \frac{1}{2 + \frac{1}{1 + \frac{1}{4 + \frac{1}{3}}}}$ . Therefore,  $\frac{61}{45} = [1, 2, 1, 4, 3]$ .

Note that  $\frac{121}{13} = 9 + \frac{1}{\frac{13}{4}} = 9 + \frac{1}{3 + \frac{1}{4}}$ . Therefore,  $\frac{121}{13} = [9, 3, 4]$

8.4 Note that  $\frac{37042}{1048576} = [0, 28, 3, 4, 88, 1, 4, 3]$ .

Let  $p_0 = a_0 = 0, q_0 = 1$ . For  $p_1 = 0 + 1 = 1; q_1 = 28$ , we have  $|\frac{1}{28} - \frac{37042}{1048576}| = \frac{1181073}{36700160} > \frac{1}{2Q}$ .

For  $p_2 = 3 + 0 = 3; q_2 = 3 \cdot 28 + 1 = 85$ , we have  $|\frac{3}{85} - \frac{37042}{1048576}| = \frac{2830871}{89128960} > \frac{1}{2Q}$ .

For  $p_3 = 13; q_2 = 368$ , we have  $|\frac{13}{368} - \frac{37042}{1048576}| = \frac{1}{12058624} < \frac{1}{2Q}$ .

Therefore,  $P = q_3 = 368$ .

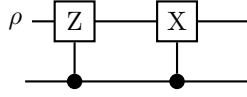
Note that  $\frac{65536}{1048576} = [0, 16]$ . We have  $p_1 = 1, q_1 = 16$  and  $|\frac{1}{16} - \frac{65536}{1048576}| = 0 < 1/(2Q)$ . So,  $P = 16$ .

9.1 Note that  $(U_a^\dagger \otimes (|\epsilon_a\rangle\langle\epsilon_a|)^\dagger)(U_a \otimes |\epsilon_a\rangle\langle\epsilon_a|) = I \otimes |\epsilon_a\rangle\langle\epsilon_a|$ .

If  $a \neq b$ , then  $(U_a^\dagger \otimes (|\epsilon_a\rangle\langle\epsilon_a|)^\dagger)(U_b \otimes |\epsilon_b\rangle\langle\epsilon_b|) = (U_a^\dagger U_b) \otimes (|\epsilon_a\rangle\langle\epsilon_a|)(0)\langle\epsilon_b| = 0$ .

Hence, we have  $U^\dagger U = (\sum_a U_a^\dagger \otimes (|\epsilon_a\rangle\langle\epsilon_a|)^\dagger)(\sum_b U \otimes (|\epsilon_b\rangle\langle\epsilon_b|)) = \sum_a I \otimes |\epsilon_a\rangle\langle\epsilon_a| = I \otimes I = I$ .

9.2 As a bit phase flip channel  $Y$  is composed of a  $Z$  gate and an  $X$  gate, we have circuit:



Let  $\rho = \frac{1}{2}(I - c_x\sigma_x + c_y\sigma_y - c_z\sigma_z)$ . Then

$$\mathcal{E}(\rho) = (1 - p)\rho + pY\rho Y^\dagger = \frac{1}{2} \begin{bmatrix} 1 + (1 - 2p)c_z & (1 - 2p)c_x - c_y i \\ (1 - 2p)c_x - c_y i & 1 - (1 - 2p)c_z \end{bmatrix}.$$

The quantum operation has produced a mixture of the Bloch vector states  $(c_x, c_y, c_z)$  and  $(-c_x, c_y, -c_z)$  with weights  $1 - 2p$  and  $p$  respectively. We see that complex part of the matrix is not affected by  $p$ . With the phase relaxation process, radius of the Bloch sphere is reduced along the  $x$ -axis and the  $z$ -axis to  $|1 - 2p|$ , resulting in the shape we see in Figure 9.2(d).