MATH. 5803. SEC. 001, QUANTUM COMPUTING, FALL 2023
M 11:30-12:00, W 11:30-12:00, F 11:30-12:20 1105 PHSC
AND F 6:00-6:50 VIA ZOOM

Homework 1, due 9/6/2023. Remember, you work in pairs.

1. Consider the RSA cryptosystem with the alphabet

$$A = \{0, 1, 2, 3, ..., 220\}.$$

The encription is done by raising the input to power 7. The encripted message 123 is received. What was the original message?

Since $221 = 13 \cdot 17$, $p = 13$ and $q = 17$. Hence $(p-1)(q-1) = 192$. You can find on the web that $d = 55$ is the inverse of 7 module 192. Hence the decripted message is

$$123^{55} \text{mod } 221 = 98\,.$$

2. Find a place on the web where you can play with the RSA.

3. Write down an integer that wolframalpha refuses to factor.

2019888888888888888888888888777777777777777775555555555555555555555555555

Homework 2, due 9/13/2023. Remember, you work in pairs.

4. Multiply the integers $2 \times 2 = 4$ using the Fast Fourier Transform algorithm, by hand. Show all steps. No calculators allowed.

5. Find a place on the web where you can compute the finite Fourier transform.

Homework 3, due 9/20/2023. Remember, you work in pairs.

6. Verify the following equality used in the 9/13/2023 lecture:

$$\sum_{y_0, y_1, \ldots, y_{n-1}=0}^{1} \left(\omega_1^{x_0 y_{n-1}} \delta_{y_{n-1}}\right) \otimes \left(\left(\omega_1^{x_1} \omega_2^{x_0}\right)^{y_{n-2}} \delta_{y_{n-2}}\right) \otimes \cdots \otimes \left(\left(\omega_1^{x_{n-1}} \omega_2^{x_{n-2}} \ldots \omega_n^{x_0}\right)^{y_0} \delta_{y_0}\right)$$
$$= \left(\delta_0 + \omega_1^{x_0} \delta_1\right) \otimes \left(\delta_0 + \omega_1^{x_1} \omega_2^{x_0} \delta_1\right) \otimes \cdots \otimes \left(\delta_0 + \omega_1^{x_{n-1}} \omega_2^{x_{n-2}} \ldots \omega_n^{x_0} \delta_1\right)$$

7. Let $R_j : Ł^2(\mathbb{F}_2) \to Ł^2(\mathbb{F}_2)$ be defined by

$$R_j(a_0\delta_0 + a_1\delta_1) = a_0\delta_0 + \omega_1 a_1\delta_1 \,.$$

Recall the Fourier transform $\mathcal{F}_2 : Ł^2(\mathbb{F}_2) \to Ł^2(\mathbb{F}_2)$

$$\mathcal{F}_2(a_0\delta_0 \;+\; a_1\delta_1) \;=\; a_0\frac{1}{\sqrt{2}}(\delta_0 \;+\; \delta_1) \;+\; a_1\frac{1}{\sqrt{2}}(\delta_0 \;-\; \delta_1) \;=\; \frac{a_0 + a_1}{\sqrt{2}}\delta_0 \;+\; \frac{a_0 - a_1}{\sqrt{2}}\delta_1$$

Check that for $x_0 = 0, 1$, $x_1 = 0, 1$, ...,

$$\begin{aligned}
\mathcal{F}_2\delta_{x_0} &= \frac{1}{\sqrt{2}}(\delta_0 + \omega_1^{x_0}\delta_1) \\
R_2\mathcal{F}_2\delta_{x_1} &= \frac{1}{\sqrt{2}}(\delta_0 + \omega_1^{x_1}\omega_2^{x_0}\delta_1) \\
\dots & \quad dots \\
R_2R_3\dots R_n\mathcal{F}_2\delta_{x_{n-1}} &= \frac{1}{\sqrt{2}}(\delta_0 + \omega_1^{x_1}\omega_2^{x_0}\dots\omega_n^{x_0}\delta_1)\,.
\end{aligned}$$

8. Deduce from 6 and 7 that

$$\mathcal{F}_{2^n}(\delta_{x_{n-1}} \otimes \dots \delta_{x_0}) = (\mathcal{F}_2\delta_{x_0}) \otimes (R_2\mathcal{F}_2\delta_{x_1}) \otimes \dots \otimes (R_2R_3\dots R_n\mathcal{F}_2\delta_{x_{n-1}})\,.$$