Quantum Algorithms: Quiz 11 2021-04-22

Name: ____________________________________

1. Let $\mathbb{G}$ be a finite Abelian group, and recall that we defined a bilinear operator $\mu(x, y)$ on $\mathbb{G}$ in the solution to the HSP for $\mathbb{G}$. State the definition of $\mu(x, y)$.

Solution: $\mathbb{G}$ is a finite Abelian group, so by the Fundamental Theorem of Finitely Generated Abelian Groups, there are integers $m_1, \ldots, m_n \in \mathbb{N}$ such that

$$\mathbb{G} \cong \prod_k \mathbb{Z}_{m_k}.$$

Represent elements $g \in G$ as tuples $g = (g_k)_k \in \prod \mathbb{Z}_{m_k}$. Define $\mu : \mathbb{G} \times \mathbb{G} \to \mathbb{C}^\times$ by

$$\mu(g, h) \coloneqq \prod \omega_k^{g_k h_k}, \qquad \omega_k \coloneqq e^{2\pi i/k}.$$