# PROBLEM SET 05: CYCLIC QUANTUM FOURIER TRANSFORM AND HSP

**Exercise 0.1** (Recalling Defintions)**.** Define the

(i) quantum Fourier transform $F_N$ on a register $R$ with $n \geq \log N$ qubits.
(ii) hidden subgroup problem for the cyclic group $\mathbb{Z}/n$. In particular, why does finding $|H|$ give us a solution to the cyclic HSP?
(iii) Euclidean algorithm to compute $\gcd(n, m)$.[1]

**Exercise 0.2.** Show that

$$\sum_{s=0}^{|H|-1} e^{\frac{2\pi i s h k}{N}} = \begin{cases} 0, & H \nmid k \\ |H|, & |H| \mid k, \end{cases}$$

where all characters mean what they did in lecture.

**Exercise 0.3.** Prove that the quantum Fourier transform $F_N$ is, in fact, unitary.

**Exercise 0.4.** Read the *introduction* (§1) of Kuperberg's paper on the dihedral hidden subgroup problem.[2] Write up a brief summary of the content of this section.

University of Illinois Urbana-Champaign, Illinois, 61801
*Email address*: dheeran2@illinois.edu

*Date*: July 24, 2025.

[1] We did not cover this in lecture, but it is how we computed $|H|$ for the cyclic HSP algorithm. Look up the definition of the algorithm if you have not seen it before.

[2] See the course page for a link.