# Challenge problems

1. For a positive integer $n$, the (discrete) Fourier transform of a function $f\colon \mathbb{Z}/n\mathbb{Z} \to \mathbb{C}$ is the function $\hat{f}\colon \mathbb{Z}/n\mathbb{Z} \to \mathbb{C}$ defined as

$$\hat{f}(b) = \frac{1}{\sqrt{n}} \sum_{a=0}^{n-1} f(a) \exp(2\pi i a b/n).$$

We say that $f$ is *flat* if $|f(a)| = 1$ for all $a \in \mathbb{Z}/n\mathbb{Z}$.

Give an example of a function $f\colon \mathbb{Z}/n\mathbb{Z} \to \mathbb{C}$ such that both $f$ and $\hat{f}$ are flat, for each $n \in \{2, 3, 4, 6\}$.

*Bonus question:* Can you find such an $f$ when $n$ is an arbitrary odd prime number?

2. Consider a positive integer $n$ and a function $f\colon \mathbb{Z}/n\mathbb{Z} \to \mathbb{C}$ such that both $f$ and $\hat{f}$ are *flat* in the sense of the previous problem. Let $s \in \mathbb{Z}/n\mathbb{Z}$ be a fixed element (assumed to be unknown, and called the *hidden shift*) and consider the shifted function $g(a) = f(a - s)$. Assume we have access to the following quantum oracles (unitary operators on a quantum register indexed by $\mathbb{Z}/n\mathbb{Z}$, given by their action on basis states $|a\rangle$):

- the quantum Fourier transform, sending $|a\rangle$ to $\frac{1}{\sqrt{n}} \sum_{b=0}^{n-1} \exp(2\pi i a b/n) |b\rangle$;
- the inverse quantum Fourier transform, sending $|b\rangle$ to $\frac{1}{\sqrt{n}} \sum_{a=0}^{n-1} \exp(-2\pi i a b/n) |a\rangle$;
- an oracle for $g$, sending $|a\rangle$ to $g(a) |a\rangle$;
- an oracle for $1/\hat{f}$, sending $|b\rangle$ to $\hat{f}(b)^{-1} |b\rangle$.

Give a quantum algorithm that determines the hidden shift $s$ with probability 1, using each of the oracles for $g$ and $1/\hat{f}$ at most once.

3. Let $p$ be a prime number and let $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ be the field of $p$ elements. Let $\mathbb{F}_p^\times$ be its unit group, i.e. the group of invertible residue classes modulo $p$. (It is known that $\mathbb{F}_p^\times$ is cyclic.) We consider a non-constant group homomorphism $\chi\colon \mathbb{F}_p^\times \to \mathbb{C}^\times$. Let $s \in \mathbb{F}_p$. Determine the value of the sum

$$\sum_{\substack{a \in \mathbb{F}_p \\ a \neq 0, s}} \overline{\chi(a)} \chi(a - s).$$

(Your answer may depend on $p$, $\chi$ and $s$.)

4. With the notation as in the previous problem, consider in addition a non-constant group homomorphism $\psi\colon \mathbb{F}_p \to \mathbb{C}^\times$ where $\mathbb{F}_p$ is viewed as an additive group, so that $\psi$ satisfies $\psi(a + b) = \psi(a)\psi(b)$. We define

$$G = \sum_{a \in \mathbb{F}_p^\times} \psi(a)\chi(a).$$

Show that $|G| = \sqrt{p}$.