Exercise Set 6

Quantum Computation

Exercise 1 *Subgroups of $\mathbb{Z}/M\mathbb{Z}$*

Let $M \geq 1$ be an integer and $G = \mathbb{Z}/M\mathbb{Z} = \{0, 1, 2, \ldots, M-1\}$ be the group equipped with the addition modulo M.

(a) Show that for $r \geq 1$ fixed (and also $r \leq M$), the set

$$H = \{n \cdot r \,:\, 0 \leq n \leq \frac{M-1}{r}\}$$

is a subgroup of G if and only if r divides M.

(b) Let us assume that the prime factorization of M is given by

$$M = p_1^{n_1} \cdot p_2^{n_2} \cdots p_k^{n_k}$$

where $p_1, \ldots, p_k$ are (distinct) primes and $n_1, \ldots, n_k$ are integers. What is the number of distinct divisors of M (which is equal to the number of distinct subgroups of G)?

Exercise 2 *Upper bound on the period of $f(x) = a^x$ (mod N)*

Let us consider an integer $N = p \cdot q$, where p and q are distinct primes. Let $1 \leq a \leq N-1$ be another integer such that $\gcd(a, N) = 1$. The aim of the present exercise is to show that in this case, the period r of the function $f : \mathbb{Z}/N\mathbb{Z} \to \mathbb{Z}/N\mathbb{Z}$ defined as $f(x) = a^x \pmod N$ satisfies the inequality

$$r \leq (p-1)\,(q-1) \tag{1}$$

(a) Let $G = \{1 \leq n \leq N-1 \,:\, \gcd(n, N) = 1\}$. Show that this set, equipped with the *multiplication modulo N*, is a group.

(b) Under the assumption that $N = p \cdot q$, where p and q are distinct primes, what is the number of elements in G?

(c) Let $a \in G$ and consider the set

$$H = \{1,\, a,\, a^2 \pmod N,\, a^3 \pmod N, \ldots,\, a^{k-1} \pmod N\}$$

where $k \geq 1$ is the smallest integer such that $a^k (\text{mod } N) = 1$. Show that H is a subgroup of G.

(d) Use then Lagrange's theorem to conclude that inequality (1) holds.

Exercise 3 *One-dimensional linear subspaces of* $G = \{0, 1, \ldots, q-1\}^2$

(a) Let us first consider the 2-dimensional vector space $G = \{0, 1, 2, 3, 4\}^2$, equipped with the addition modulo 5 (e.g., if $x = (2, 3)$ and $y = (1, 4)$, then $x + y = (3, 2)$). Describe all the one-dimensional linear subspaces H of G.

Hint: You may first ask yourself how many exist?

(b) Let $H = \text{span}\{(1, 1)\}$. Describe the equivalence casses of H. (Again, how many exist?)

(c) Consider now $G = \{0, 1, 2, 3\}^2$, equipped with the addition modulo 4. Describe all the one-dimensional linear subspaces H of G.