Exercise Set 7: Solution
Quantum Computation

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

(a) If r does not divide M, then $n \cdot r \pmod M$ is not a multiple of r when n reaches the first value such that $n \cdot r > M$, so H is not a subgroup of G in this case.

On the contrary, if r divides M, then any sum modulo M of any two elements of H remains a multiple of r, i.e., an element of H. Also, every element n in H admits an inverse $M - n$ which also belongs to H, so H is a subgroup of G in this case.

(b) The number of divisors of M corresponds to the number of different ways to choose prime factors among those available. The number of times p_1 can be chosen is a number between 0 and n_1, and similarly for the other prime factors, so the total number of choices, which is also equal to the total number of divisors of M, is given by

$$(n_1 + 1) \cdot (n_2 + 1) \cdots (n_k + 1)$$

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

(a) To check that G is a group, we need to check:
- The multiplication modulo N is an internal operation in G: indeed, if $\gcd(n, N) = 1$ and $\gcd(m, N) = 1$, then it also holds that $\gcd(n \cdot m \pmod N, N) = 1$.
- It is associative: this follows form the associativity of the multiplication modulo N.
- The neutral element 1 belongs to G: clear.
- Each element in G has an inverse in G: indeed, if $\gcd(n, N) = 1$, then Bézout's theorem implies there exist integers x, y such that $xn + yN = 1$, i.e., $xn \pmod N = 1$, which is exactly saying that x is the inverse of n modulo N, and the same equation also implies that $\gcd(x, N) = 1$, so x also belongs to G.

(b) The number of elements in G is equal to

$$(p-1) \cdot (q-1) = pq - p - q + 1 = N - p - q + 1 = (N-1) - (p-1) - (q-1)$$

Indeed, the set G contains all the elements between 1 and $N - 1$, except the $q - 1$ multiples of p and the $p - 1$ multiples of q.

(c) H is a subgroup of G because:
- For any two elements a^ℓ and a^m in H, it is clear that $a^\ell \cdot a^m \pmod N = a^{\ell+m} \pmod N$ also belongs to H (note that if $\ell + m \geq k$, then $a^{\ell+m} \pmod N = a^{\ell+m-k} \pmod N$).
- Also, each element a^ℓ in H has an inverse $a^{k-\ell}$ which belongs also to H.

(d) Lagrange's theorem states that $|H| = k$ divides $|G| = (p-1)\,(q-1)$. But by definition, k is the smallest integer such that $a^k (\text{mod } N) = 1$, which is nothing but the period of the function f defined as $f(x) = a^x \,(\text{mod } N)$. This implies inequality (1).

Remark: The above also implies that if $\gcd(a, N) = 1$, then $a^{(p-1)\,(q-1)}\,(\text{mod } N) = 1$, which is known as (a particular instance of) *Euler's theorem.*

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

(a) Every span(g), where g is a non-zero element of G, is a one-dimensional linear subspace of G. There are $5^2 = 25$ different elements in G, among which 24 are non-zero. But not all of them span a different subspace: each subspace has exactly 5 elements, so 4 non-zero elements, and because the set $\{0, 1, 2, 3, 4\}$ equipped with the addition modulo 5 is a field (because 5 is a prime number), we obtain that groups of 4 elements span the same subspace, so the total number of different subspaces is equal to $24/4 = 6$. Those are the following (found by exhaustive search):

$$\begin{array}{lll} H_0 = \text{span}\{(0,1)\} & H_1 = \text{span}\{(1,1)\} & H_2 = \text{span}\{(2,1)\} \\ H_3 = \text{span}\{(3,1)\} & H_4 = \text{span}\{(4,1)\} & H_5 = \text{span}\{(1,0)\} \end{array}$$

(b) The equivalence classes of H are: H, $H + (0, 1)$, $H + (0, 2)$, $H + (0, 3)$, $H + (0, 4)$ (where "+" denotes here the addition modulo 5).

(c) As 4 is not a prime number, $\{0, 1, 2, 3\}$ equipped with the addition and multiplication modulo 4 is *not* a field (because 2 has no multiplicative inverse), so the reasoning of part (a) does not hold, and there are actually in this case more subspaces than expected (9 in total instead of $(4^2 - 1)/3 = 5$). Here they are:

$$\begin{array}{lll} H_0 = \text{span}\{(0,1)\} & H_1 = \text{span}\{(1,1)\} & H_2 = \text{span}\{(2,1)\} \\ H_3 = \text{span}\{(3,1)\} & H_4 = \text{span}\{(1,0)\} & H_5 = \text{span}\{(0,2)\} \\ H_8 = \text{span}\{(2,2)\} & H_7 = \text{span}\{(1,2)\} & H_8 = \text{span}\{(2,0)\} \end{array}$$

Note that the 4 extra subspaces are all spanned by a vector with at least one component equal to 2.