Exercise 7: Characters, Diffie-Hellman and Discrete Logarithm

$\boxed{1.}$ Here we will be proving a theorem you used in the lecture about **Characters**:

Claim 7.1

> *Any finite Abelian (commutative) group G is isomorphic to its dual group, $\hat{G} := \hom(G, \mathbb{C}) = \{\chi : G \to \mathbb{C} : \chi$ homomorphism$\}$, the groups of its characters.*

(a) Let $\chi \in \hat{\mathbb{Z}}_n$ be a character of the cyclic group of order n. Prove that $\chi(a) = \omega^a$ for an n'th root of unity ω. Conclude that $|\mathbb{Z}_n| = \hat{\mathbb{Z}}_n|$.

(b) Let ω be a primite n'th root of unity, meaning $\omega^k \neq 1$ for any $k < n$ while $\omega^n = 1$. Define $\varphi : \mathbb{Z}_n \to \hat{\mathbb{Z}}_n$ by $\varphi(a) = \chi_a$ where $\chi_a(x) = \omega^{ax}$. Show this is an isomorphism (a homomorphism that is a bijection, or equivalently a homomorphism with an inverse homomorphism). Conclude $\mathbb{Z}_n \cong \hat{\mathbb{Z}}_n$.

(c) Let G, H be two finite Abelian groups. Show that $\widehat{G \times H} \cong \hat{G} \times \hat{H}$. Use the structure theorem for finite Abelian groups (which was quoted in the lecture) to conclude that for any finite Abelian group G, $G \cong \hat{G}$.

2. The Diffie-Hellman key exchange protocol goes like this:

Public Keys: Alice and Bob decide and publicly state a prime number $p \in \mathbb{N}$ (and by that decide on the cyclic group to be used $\mathbb{Z}_p^*$), and a generator for the multiplicative group $g \in \mathbb{Z}_p^* : \{g, g^2, \ldots, g^{p-1}\} = \mathbb{Z}_p^*$.

Temporary Keys: Both Alice and Bob choose private keys at random $a, b \in \{1, \ldots, p-1\}$ respectively.

Sending: They compute $A = g^a \pmod{p}$ and $B = g^b \pmod{p}$ and send each other the results.

Shared secret: Finally they compute $A^b \pmod{p} = g^{ab} \pmod{p} = B^a \pmod{p}$ which becomes their private shared information. This can be used as a key for any symmetric private-key cryptographic protocol.

The correctness of the protocol is clear. Let's talk about its security and see a quantum algorithm that breaks it, due to Shor:

(a) The security hinges on the belief that a specific problem is hard to solve. Define the exact problem that needs to be solved in order for an eavesdropper to know the private shared key at the end of the protocol. Show that if, given p, g and $g^a \pmod p$ we could have computed a efficiently, called Discrete Logarithm, then we would have solved this problem and hence broken the Diffie-Hellman protocol's security.

(b) In the rest of the subquestions we will develop Shor's quantum algorithm for solving Discrete Logarithm.

Given p, g and $h = g^a \pmod p$, define the function $f : \mathbb{Z}_{p-1} \times \mathbb{Z}_{p-1} \to \mathbb{Z}_p^*$ by $f(x, y) := g^x h^y \pmod p$. Find the periodicity of f, i.e. find $(r_1, r_2) \in \mathbb{Z}_{p-1} \times \mathbb{Z}_{p-1}$ such that for every $x, y \in \mathbb{Z}_{p-1}$ and $k \in \mathbb{Z}$, $f(x + kr_1, y + kr_2) = f(x, y)$ and $f(x + r_1', y + r_2') \neq f(x, y)$ if there is no k for which $(r_1', r_2') = (kr_1, kr_2)$. For the sake of simplicity of the next subquestions, choose such a pair (r_1, r_2) with minimal r_2 (as a positive integer).

(c) In the algorithm we'll prepare the state $\frac{1}{p-1} \sum_{x=0}^{p-2} \sum_{y=0}^{p-1} |x, y, f(x, y)\rangle$. What is the state this collapses to, if we measure the register with the value of f? You may hide the normalisation in a vague "C". Use the previous subquestion to write the state as a uniform superposition over the register of y.

(d) Define the Quantum Fourier Transform over $\mathbb{Z}_n$ by $QFT_n |x\rangle = \frac{1}{\sqrt{n}} \sum_{y=0}^{n-1} e^{2\pi i \frac{xy}{n}} |y\rangle$. We will see in the lecture that this is implementable efficiently by a quantum circuit and used in Shor's factoring algorithm.

On the two registers that were not measured, we perform $QFT_{p-1} \otimes QFT_{p-1}$. What is the outcome? What is the probability to get the pair j, k when measuring the two registers in the computational bases? (keep it as an absolute-value-squared of a sum that does not depend on the value of f)

(e) Use a theorem we saw in the lecture to prove that for a finite Abelian group G and a character of it χ,

$$\sum_{g \in G} \chi(g) = \delta_{\chi=1} |G|$$

i.e. the sum is $|G|$ if χ is the trivial character and otherwise it vanishes.

Use that to prove that for an m'th roof of unity ω, $\sum_{j=0}^{m-1} \omega^j = m\delta_{\omega=1}$, i.e. it's m if $\omega = 1$ and 0 for any other m'th root of unity.

(f) Derive a condition for the values of j, k that is both necessary and sufficient for the probability to be non-zero. Prove that under the condition you found the (strictly-positive) probability does not depend on the values of j, k, so we get a uniform distribution over those pairs satisfying this condition.

(g) Prove that for large enough p, under uniform distribution over such pairs from the previous subquestion, there is a good probability for j to be coprime to $p-1$, and thus invertible in $\mathbb{Z}_{p-1}$. For that you may use the fact that $\Phi(m) > c\frac{m}{\log(\log(m))}$ for a constant c and $m > 2$. Show that in this case we can compute a given j, k.

Good probability means a probability that allows us to repeat the protocol a number of times that is still polynomial in the input size, specifically, that is at most $polylog(p-1)$, to get with high probability (greater than a constant) a j coprime to $p - 1$.