An idea which can be used only once is a trick. If one can use it more than once it becomes a method. G. Polya and G. Szego

Read: Keith Conrad's handout on characters of finite abelian groups (sections 1–4).

Exercise 1. (a) Express $(\mathbb{Z}/(63))^\times$ as a direct product of cyclic groups abstractly and then as a direct product of cyclic *subgroups*, each with an explicit generator from $(\mathbb{Z}/(63))^\times$.

(b) Use the explicit generating set found in part a to find all solutions to $a^3 \equiv 1 \bmod 63$.

Exercise 2. On $(\mathbb{Z}/(m))^r$ the dot product of $\mathbf{a} = (a_1, a_2, \ldots, a_r)$ and $\mathbf{b} = (b_1, b_2, \ldots, b_r)$ is

$$\mathbf{a} \cdot \mathbf{b} = a_1 b_1 + a_2 b_2 + \cdots + a_r b_r \bmod m.$$

For $\mathbf{a} \in (\mathbb{Z}/(m))^r$, let $\chi_{\mathbf{a}} \colon (\mathbb{Z}/(m))^r \to S^1$ by $\chi_{\mathbf{a}}(\mathbf{x}) = e^{2\pi i(\mathbf{a}\cdot\mathbf{x})/m}$. (It makes sense to talk about $e^{2\pi i a/m}$ where $a \in \mathbb{Z}/(m)$ since $a \equiv a' \bmod m \Rightarrow e^{2\pi i a/m} = e^{2\pi i a'/m}$.)

(a) Show each $\chi_{\mathbf{a}}$ is a character of $(\mathbb{Z}/(m))^r$.

(b) Show the mapping $(\mathbb{Z}/(m))^r \to ((\mathbb{Z}/(m))^r)\widehat{\ }$ given by $\mathbf{a} \mapsto \chi_{\mathbf{a}}$ is a group isomorphism.

Exercise 3. In $(\mathbb{Z}/(73))^\times$ the element 2 mod 73 has order 9, so the subgroup $\langle 2 \rangle$ has index $72/9 = 8$.

(a) Compute the indices of successive pairs of subgroups in the rising tower

$$\langle 2 \rangle \subset \langle 2, 3 \rangle \subset \langle 2, 3, 5 \rangle = (\mathbb{Z}/(73))^\times.$$

(b) Explicitly describe all 8 characters χ of $(\mathbb{Z}/(73))^\times$ that satisfy $\chi(2) = 1$ by extending characters stepwise through the rising tower in part a, as in the proof of Lemma 3.2 in the handout on characters. Describe each character by its values at $2^j 3^k 5^\ell$. Explain clearly why your choices for character values really work.

(c) Use the same method as part b to explicitly describe all 8 characters χ of $(\mathbb{Z}/(73))^\times$ that satisfy $\chi(2) = e^{2\pi i/3}$.

Exercise 4. Write the following functions $\mathbb{Z}/(4) \to \mathbb{C}$ as linear combinations of characters of $\mathbb{Z}/(4)$.

(a) $f(0) = 1, f(1) = 5, f(2) = 9, f(3) = i$.

(b) $f(0) = f(1) = -1,\ f(2) = 0,\ f(3) = 14$.

Exercise 5. If H is a subgroup of a finite abelian group G, let $H^\perp = \{\chi \in \widehat{G} : \chi = 1 \text{ on } H\}$. These are the characters of G that are trivial on H. It depends on both H and G. In part b of exercise 3 you computed $\langle 2 \bmod 73 \rangle^\perp$ in the character group of $(\mathbb{Z}/(73))^\times$.

(a) For a character χ on G, let $\chi|_H$ be its restriction to H. Show $\chi \mapsto \chi|_H$ is a surjective homomorphism $\widehat{G} \to \widehat{H}$ with kernel $H^\perp$, so $H^\perp$ is a subgroup of $\widehat{G}$ and $\widehat{G}/H^\perp \cong \widehat{H}$.

(b) Show $\widehat{G/H} \cong H^\perp$. (Hint: Think about a character in $\widehat{G/H}$ as a character on G.)

(c) The group $H^{\perp\perp} = (H^\perp)^\perp$ belongs to $\widehat{\widehat{G}}$. Show the isomorphism $G \to \widehat{\widehat{G}}$ from Pontryagin duality restricts to an isomorphism $H \to H^{\perp\perp}$. (This is stronger than saying $H^{\perp\perp} \cong H$: it says they are isomorphic in a *specific* way.)

(d) Use part c to show $H \mapsto H^\perp$ is a bijection between the subgroups of G and the subgroups of $\widehat{G}$. Then use this to help explain why, for each d dividing $|G|$, G has the same number of subgroups with order d as it does subgroups with index d.