22.2 Show that we can define a group homomorphism

$$f : \mathbb{Z}/mn\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$$

by $f(\overline{a}) := (p(\overline{a}), q(\overline{a}))$.
22.3 Suppose $\overline{a}$ is in the kernel of f, that is to say $f(\overline{a}) = 0 = (\overline{0}, \overline{0})$. Show that a is divisible by m and by n.
22.4 Under the hypothesis that m and n are relatively prime, show that this implies $\overline{a} = 0$. Conclude, under this hypothesis, that f is injective.
22.5 Explain why f injective implies f bijective, that is to say f is an isomorphism of groups.
22.6 Under the hypothesis that m and n are relatively prime, we give an alternate proof that f is surjective. Use the Bézout identity to write

$$um + vn = 1.$$

Suppose $(\overline{b}, \overline{c}) \in \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$. Set

$$a := vb + uc.$$

Show that $na \sim b \pmod{m}$ and $ma \sim c \pmod{n}$. Conclude that

$$f(\overline{a}) = (\overline{b}, \overline{c}).$$

Question 23. (*Finite commutative groups — I*)
23.1 Using the result of Question 22, show by induction that if $n_1, \ldots, n_k$ are positive integers that are pairwise relatively prime, then

$$\frac{\mathbb{Z}}{(n_1 \cdots n_k)\mathbb{Z}} \xrightarrow{\cong} \mathbb{Z}/n_1\mathbb{Z} \times \cdots \times \mathbb{Z}/n_k\mathbb{Z}.$$

Here is a variant. Let G be a finite commutative group, written additively $G = (G, +, 0)$. Suppose $g, h \in G$ are elements of orders m, n respectively. Recall that this means m is the smallest strictly positive integer such that $mg = 0$ (resp. n is the smallest strictly positive integer such that $nh = 0$). Suppose m and n are relatively prime. We would like to show that $g + h$ has order mn.

Use the Bézout identity to choose integers u, v such that $um + vn = 1$.
23.2 Show that $mn(g + h) = 0$. Here one must use that G is commutative (explain why?).
23.3 Suppose p is an integer such that $p \cdot (g + h) = 0$. Show that

$$p = (pu)m + (pv)n.$$