(Q1) Let $g \in G$ be an element of order m. In symbols: $g^m = e$. Now, if $d|m$, m/d is a integer. consider $g^{m/d}$.

$(g^{m/d})^d = g^m = e$. Thus, $g^{m/d} \in G$ is of order d.

(Q2) We use the following theorem in the proof: Every cyclic group of order n is isomorphic to $\mathbb{Z}/n\mathbb{Z}$.

If $|G| = p$, any non-trivial element of G has p as its order. Thus, $|\langle g\rangle| = p$ $(g \neq e)$ and $\langle g\rangle \leq G$ implies $\langle g\rangle = G$. Thus, the group G is cyclic with $p-1$ generators. Thus, by the above result, we conclude G is isomorphic to $\mathbb{Z}/p\mathbb{Z}$.

Proof of above result:
Let G be a finite group generated by $g \in G$; $\langle g\rangle = [e, g, g^2, \cdots g^{n-1}] = G$ of order n. Define a function $\varphi : G \to \mathbb{Z}/n\mathbb{Z}$ such that $\varphi(g) = 1$, and $\varphi(g^k) = k$ for some $k \in \mathbb{Z}^+$. First we show φ is a homomorphism.

$$\varphi(g_1 \odot g_2) = \varphi(g^m \odot g^n) = \varphi(g^{m+n}) = m+n$$
$$= \varphi(g^m) + \varphi(g^n).$$

Next, we show φ is an bijection
1. If $\varphi(g_1) = \varphi(g_2) \Rightarrow \varphi(g^m) = (g^n) \Rightarrow m = n$
Thus, $g^m = g^n = g^m$, $g_1 = g_2$

2. Next, consider the function $\phi(m) = g^m$ for $m \in \mathbb{Z}/n\mathbb{Z}$. Note that,

$$\varphi(\phi(m)) = \varphi(g^m) = m \quad \text{and}$$

$$\phi(\varphi(g^m)) = \phi(m) = g^m.$$ Thus, $\phi(x)$ is the inverse of $\varphi(x)$ and $\varphi(x)$ is surjective.

Since φ is a isomorphism between G and $\mathbb{Z}/n\mathbb{Z}$, $G \cong \mathbb{Z}/n\mathbb{Z}$.

(Q3)

- First we show that the group $G_1 \times G_2$ is closed under multiplication.

Let $h_1, g_1 \in G_1$ and $h_2, g_2 \in G_2$:

$\cancel{(h_1, g_2) * (g_2}$ $(h_1, h_2) * (g_1, g_2) = (h_1 *_1 g_1, h_2 *_2 g_2)$

Since G_1 is a group, by axiom (A0), $(h_1 *_1 g_1) \in G_1$ and since G_2 is a group, $(h_2 *_2 g_2) \in G_2$. Thus, $(h_1 *_1 g_1, h_2 *_2 g_2) \in G_1 \times G_2$.

- Next, we show that the group $G_1 \times G_2$ is closed under inverses.

Let $h \in G_1$ and $g \in G_2$, $(h, g)^{-1} = (h^{-1}, g^{-1})$

$(h, g) \cdot (h^{-1}, g^{-1}) = (h *_1 h^{-1}, g *_2 g^{-1}) = (e_1, e_2)$

Since G_1 is a group by axiom (A2) $h^{-1} \in G_1$ and G_2 is a group $\Rightarrow g^{-1} \in G_2$. Thus, $(h^{-1}, g^{-1}) \in G_1 \times G_2$.

Q.E.D. $\blacksquare$

(Q4)

- $(\mathbb{Z}/2\mathbb{Z})^\times = \langle 1 \rangle$
- $(\mathbb{Z}/3\mathbb{Z})^\times = \langle 2 \rangle$

  $2 \equiv 2 \pmod 3$

  $2 \times 2 \equiv 4 \equiv 1 \pmod 3$
- $(\mathbb{Z}/5\mathbb{Z})^\times = \langle 2 \rangle$

  $2 \equiv 2 \pmod 5$

  $2^2 \equiv 4 \pmod 5$

  $2^3 \equiv 8 \equiv 3 \pmod 5$

  $2^4 \equiv 16 \equiv 1 \pmod 5$
- $(\mathbb{Z}/7\mathbb{Z})^\times = \langle 5 \rangle$

  $5 \equiv 5 \pmod 7$

  $5^2 \equiv 25 \equiv 4 \pmod 7$

  $5^3 \equiv 125 \equiv 6 \pmod 7$

  $5^4 \equiv 2 \pmod 7$

  $5^5 \equiv 3 \pmod 7$

  $5^6 \equiv 1 \pmod 7$
- $(\mathbb{Z}/11\mathbb{Z})^\times = \langle 7 \rangle$

  (similar computation as above).

(Q13)

Consider the set : $(\mathbb{Z}/n\mathbb{Z})^{\times} = [a \in \mathbb{Z}^{+} : (a,n) = 1]$

Note that $(\mathbb{Z}/n\mathbb{Z})^{\times}$ forms a group, since inverses exist (all other properties are almost trivial to verify). Here's how:

$a \in (\mathbb{Z}/n\mathbb{Z})^{\times} \Rightarrow \gcd(a,n) = 1$, by bezouts lemma, there exist integers x_1 and x_2 st:

$ax_1 + nx_2 = 1$. Re-arranging, we have:

$nx_2 = 1 - ax_1$

$n \mid (1 - ax_1) \Rightarrow 1 \equiv ax_1 \pmod{n}$. Thus, x_1 is the inverse of a.

Now, note that $|(\mathbb{Z}/n\mathbb{Z})^{\times}| = \varphi(n)$ (by def). by lagranges theorem, the order of any a in $(\mathbb{Z}/n\mathbb{Z})^{\times}$ ~~is~~ divides $\varphi(n)$. In other words,

$$a^d \equiv 1 \pmod{n}$$

where d is such that $d \mid \varphi(n)$, or $\exists m \in \mathbb{Z} : \varphi(n) = md$. Thus,

$$(a^d)^m \equiv 1^m \pmod{n}$$

$$a^{dm} \equiv 1 \pmod{n}$$
$$a^{\varphi(n)} \equiv 1 \pmod{n}.$$

This proves that, if $a < n$ and $\gcd(a,n) = 1$, then $a^{\varphi(n)} \equiv 1 \pmod{n}$. If $a > n$, then one can find $b \in (\mathbb{Z}/n\mathbb{Z})^\times$ st $b \equiv a \pmod{n}$.

(Q11) For this problem, we assume Bezouts lemma, that if a and b are integers, and $d = \gcd(a,b)$ then there exist integers x_1 and x_2 such that: $ax_1 + bx_2 = d = \gcd(a,b)$.

We give a proof by induction, and induct on k.

1. Base case, $k = 2$ (Bezout's Lemma)

2. Inductive Hypothesis, we assume for any $k \in \mathbb{Z}$, we can find integers, $x_1, \cdots, x_k$ st $a_1x_1 + \cdots + a_nx_n = \gcd(a_1, \cdots, a_n) = d$

3. Inductive step: Let $\gcd(a_1, \cdots, a_n) = d$. Then, $\gcd(a_1, \cdots, a_n, a_{n+1})$ $(a_{n+1} \in \mathbb{Z})$, $= \gcd(d, a_{n+1})$. Thus, by bezout's, there exist $y_1, y_2 \in \mathbb{Z}$ st
$dy_1 + a_{n+1}y_2 = \gcd(d, a_{n+1}), = \gcd(a_1, \cdots, a_{n+1})$
By, the IH,

$(a_1x_1 + \cdots + a_nx_n)y_1 + a_{n+1}y_2$

$$= (a_1)(x_1y_1) + \cdots + (a_n)(x_ny_1) + (a_{n+1})(y_2) = \gcd(a_1, \cdots, a_{n+1}).$$

Thus, the theorem is true for the $(n+1)^{\text{th}}$ case which completes the proof.

(Q10) Let $m = p_1^{\nu_1} p_2^{\nu_2} \cdots p_n^{\nu_n}$ (for distinct primes)

- Define x_i = (m but with the i^{th} prime totally removed from its PF)
  $x_i = p_1^{\nu_1} p_2^{\nu_2} \cdots p_{i-1}^{\nu_{i-1}} p_{i+1}^{\nu_{i+1}} \cdots p_n^{\nu_n}$.

- Now note that $\gcd(x_i, x_j)$ (WLOG, $i < j$) is $p_1^{\nu_1} \cdots p_{i-1}^{\nu_{i-1}} p_{i+1}^{\nu_{i+1}} \cdots p_{j-1}^{\nu_{j-1}} p_{j+1}^{\nu_{j+1}} \cdots p_n^{\nu_n}$.

- Thus, $\gcd(x_1, x_2) = p_3^{\nu_3} \cdots p_n^{\nu_n}$ (the divisor of x_i is of the form $p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_{i-1}^{\alpha_{i-1}} p_{i+1}^{\alpha_{i+1}} \cdots p_n^{\alpha_n}$ where $0 \le \alpha_i \le \nu_i$). And,
  $\gcd(x_1, x_2, x_3) = \gcd(\gcd(x_1, x_2), x_3)$

  $= \gcd(p_3^{\nu_3} \cdots p_n^{\nu_n}, p_1^{\nu_1} p_2^{\nu_2} p_4^{\nu_4} \cdots p_n^{\nu_n})$

  $= p_4^{\nu_4} \cdots p_n^{\nu_n}$.

Thus, by induction (or simply continuing in this manner),
$\gcd(x_1, \cdots x_k) = p_{k+1}^{\nu_{k+1}} p_{k+2}^{\nu_{k+2}} \cdots p_n^{\nu_n}$
when $k = n$, this becomes 1.

Chineese Remainder Theorem

(Q12) We prove a more general case:

a. Given a group G, and normal subgroups H_1, H_2 of G, we have that there exists a injective homomorphism between $G\backslash(H_1 \cap H_2)$ and $G/H_1 \times G/H_2$. Moreover, if $G = H_1H_2$, Then $G/(H_1 \cap H_2) \cong G/H_1 \times G/H_2$.

Proof.

- Consider the function $\varphi: G/(H_1 \cap H_2) \rightarrow G/H_1 \times G/H_2$ such that $\varphi(gL) = (gH_1, gH_2)$ for all $g \in G$ (note: $L = H_1 \cap H_2$).

$$\varphi(g_1L \odot g_2L) = \varphi((g_1 \cdot g_2)L) = ((g_1 \cdot g_2)H_1, (g_1 \cdot g_2)H_2)$$

$$= (g_1H_1 \odot g_2H_1, g_1H_2 \odot g_2H_2)$$

$$= (g_1H_1, g_1H_2) \times (g_2H_1, g_2H_2)$$

$$= \varphi(g_1L) \times \varphi(g_2L) \qquad [g_1, g_2 \in G]$$

Since $\varphi(g_1L \odot g_2L) = \varphi(g_1L) \times \varphi(g_2L)$, φ is a homomorphism.

- Next, we prove φ is injective:

Assume $\varphi(g_1L) = \varphi(g_2L)$

$$(g_1H_1, g_1H_2) = (g_2H_1, g_2H_2)$$

$$g_1H_i = g_2H_i \qquad (1 \leq i \leq 2)$$

Thus, $(g_2)^{-1}(g_1) \in H_i \Rightarrow (g_2)^{-1}(g_1) \in L$

$\Rightarrow g_1L = g_2L$

For part II, we use the counting theorem:

$$|H_1H_2| = \frac{|H_1| \times |H_2|}{|H_1 \cap H_2|}$$

We show that $|G/L| = |G/H_1 \times G/H_2|$, and since φ is injective, we know that φ has to be surjective.

$$\begin{aligned}
|G/H_1 \times G/H_2| &= |G/H_1| \times |G/H_2| \\
&= \frac{|G|}{|H_1|} \times \frac{|G|}{|H_2|} \\
&= \frac{|G|^2}{|H_1 \cdot H_2|} = \frac{|G|^2}{|H_1 \times H_2|} \\
&= \frac{|G|^2}{|H_1H_2|\,|H_1 \cap H_2|} = \frac{|G|^2}{|G|\,|H_1 \cap H_2|}
\end{aligned}$$

(Note that $|G| = |H_1H_2|$, since $G = H_1H_2$)

$$\begin{aligned}
&= \frac{|G|}{|H_1 \cap H_2|} = [G : H_1 \cap H_2] \\
&= |G/H_1 \cap H_2|
\end{aligned}$$

Q.E.D.

We can generalize the above theorem to an arbitrary number of normal subgroups $H_1, \cdots, H_n$:

$$G/(H_1 \cap \cdots \cap H_n) \cong G/H_1 \times \cdots \times G/H_n.$$

We can apply this to the following setting:

- $G = (\mathbb{Z}, +)$
- $H_1 = m\mathbb{Z}$
- $H_2 = n\mathbb{Z}$

where $\gcd(m,n) = 1$.

Since $\gcd(m,n) = 1 \Rightarrow (m\mathbb{Z})(n\mathbb{Z}) = \mathbb{Z}$ (linearly independent set in $\mathbb{Z}$), and thus

$$\mathbb{Z}/(mn)\mathbb{Z} \cong \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$$

which is the base case of the chineese remainder theorem.