Solution: Since m divides $o(G)$ and G is cyclic, $\exists$ a unique cyclic subgroup A of G of order m. Similarly, $\exists$ a unique cyclic subgroup B of G of order n. Now $o(A \cap B)$ divides $o(A) = m$ and $o(A \cap B)$ divides $o(B) = n$. Since $\gcd(m,n) = 1$, $o(A \cap B) = 1$, So, by a previous theorem of group theory,

$$o(AB) = \frac{o(A)\,o(B)}{o(A \cap B)} = \frac{mn}{1} = mn = o(G)$$

Since $AB \subseteq G$, $o(AB) = o(G)$ and G is finite, we must have $G = AB$. Hence $G = AB$, $A \cap B = \{e\}$, A and B are normal subgroups of G. So, $G = A \times B \simeq \mathbb{Z}_m \times \mathbb{Z}_n$

---

5. Let A and B be two cyclic groups of order m an n respectively. Show that $A \times B$ is a cyclic group if and only if $\gcd(m,n) = 1$

Solution: Let $A = \langle a \rangle$ for some $a \in A$ and $B = \langle b \rangle$ for some $b \in B$. Suppose $\gcd(m,n) = 1$. Let $g = (a,b)$. Then $g^{mn} = (a,b)^{mn} = (a^{mn}, b^{mn}) = (e_A, e_B)$, e_A and e_B are the identity elements of A and B respectively. Suppose $o(g) = t$. Then $(a,b)^t = (e_A, e_B)$ This implies that $a^t = e_A$, $b^t = e_B$. So, m divides t and n divides t Since $\gcd(m,n) = 1$, mn divides t. As $g^{mn} = (e_A, e_B)$, t divides mn So, $o(g) = mn$. Now $o(A \times B) = mn$ and $A \times B$ contains an element g of order mn

So, $A \times B$ is cyclic.

Conversely, assume that $A \times B$ is cyclic and $\gcd(m,n) = d \neq 1$. Let $(a,b) \in A \times B$. Then $o(a)$ divides m and $o(b)$ divides n

Now $\frac{mn}{d} = \frac{m}{d} \cdot n = m \cdot \frac{n}{d}$ is an integer and $\frac{mn}{d} < mn$.

Also, $(a,b)^{mn/d} = \left(a^{\frac{mn}{d}}, b^{\frac{mn}{d}}\right) = (e_A, e_B)$. Hence $A \times B$ does not contain any element of order mn. This implies that $A \times B$ is not cyclic, a contradiction. So, $\gcd(m,n) = 1$.

---

6. Show that $o(\mathrm{Aut}(\mathbb{Z}_2 \times \mathbb{Z}_2)) = 6$

Solution: $\mathbb{Z}_2 \times \mathbb{Z}_2 \simeq K$ where K is Klein's-4 group.

So, $K = \{e, a, b, ab\}$, e is the identity element, $a^2 = e$, $b^2 = e$ and $ab = ba$ gives the binary operation table.

Now it is enough to find the number of automorphisms of K. Let f be an automorphism of K. So, $f(e) = e$

Now as $o(f(x)) = o(x)$ for any $x \in K$. Now $o(a) = o(b) = o(ab) = 2$

Also if $f(a)$ and $f(b)$ is known then $f(ab)$ is also known as $f(ab) = f(a)f(b)$. As $o(a) = 2$

So $o(f(a)) = 2$ So, $f(a)$ is either a or b or ab

So, $f(a)$ is any one of the three elements a, b, and ab

Then $f(b)$ is any of the other two elements as $o(f(b)) = 2$ also. So, we can choose $f(a)$ and $f(b)$ together in $3 \times 2 = 6$ ways. So $o(\mathrm{Aut}\, K) = 6$

So, $o\left(\mathrm{Aut}\, \mathbb{Z}_2 \times \mathbb{Z}_2\right) = 6$

Theorem 3.1.1 (Cauchy's Theorem for finite abelian group):
Let G be a finite abelian group of order n, and p a prime dividing n. Then G has an element of order p.

Proof: We prove the theorem by mathematical induction on $n = o(G)$. If $n = 2$ then G is itself a subgroup of G of order 2 as 2 is a prime and 2 divides 2.

So, the theorem is true for $n = 2$.

Assume that the theorem is true for all abelian groups of order less than n and let G be an abelian group of order n. If for some proper subgroup H of G, p divides $o(H)$, then by induction hypothesis the subgroup H (and hence G) has an element of order p. Assume therefore, that for each proper subgroup H of G, p does not divide $o(H)$. For any proper subgroup H of G, $o(G) = o(H).o(G/H)$ (As G is abelian, H is a normal subgroup and G/H exists) and since p divides $o(G)$ and p does not divides $o(H)$, it follows that p divides $o(G/H)$. Since $o(G/H) < o(G)$, by induction hypothesis G/H has an element aH of order p. Hence $(aH)^p = H$, i.e., $a^p \in H$. If $o(H) = m$, then $(a^p)^m = e$, e is the identity element in G. We shall show that $b = a^m \neq e$ and b is the required element of order p. Suppose $b = a^m = e$. Then $(aH)^m = a^m H = eH = H$. Since p is relatively prime to m, there exists integers r and s such that $rp + sm = 1$. Hence $aH = a^{rp+sm}H$

$= (aH)^{rp}(aH)^{sm} = H$, which is a contradiction as $o(aH) = p$.

Hence $b = a^m \neq e$. Since $b^p = (a^m)^p = (a^p)^m = e$, we have the required element b of order p.

Note. As in theorem 3.11.1, G has an element of order p, hence a subgroup of order p.

Worked out Exercise 3.1.2 : 1. Show that an abelian group of order 22 is cyclic.

Proof : Let G be an abelian group of order 22. Since 11 divides $o(G)$, by Cauchy's theorem for finite abelian group, there exists

an element $a \in G$ such that $o(a) = 11$. Similarly as 2 divides $o(G)$, we have an element $b \in G$ such that $o(b) = 2$. As G is abelian $ab = ba$ and $\gcd(11, 2) = 1$

So, $o(ab) = o(a)o(b) = 11 \times 2 = 22$. ab is an element of order 22 in G. So, G is cyclic.

An important application for Cauchy's theorem for finite abelian group is that the converse of Lagrange's theorem holds for any finite abelian group as we shall prove next.

Theorem 3.1.3 Let G be a finite abelian group of order n. If m is a positive integer such that m divides n, then G has a subgroup of order m.

Proof: Since every group contains a subgroup $\{e\}$ of order 1, e is the identity element in G, we find that the theorem holds for $n=1$ and also for $m=1$. So, assume that $n>1$, $m>1$ and let us prove the theorem by mathematical induction on n. If $n=2$, then $m=2$. Hence G is itself a subgroup of order 2. Assume that the theorem holds for all abelian groups of order $2 \le k < n$. Consider an abelian group G of order n, and $1 < m$ is a divisor of n. Now m has a prime factor, say p. Since p divides n, by Cauchy's theorem for finite abelian group, G has an element of order p and hence a subgroup K of order p. As the group G is abelian, K is a normal subgroup of G. Then the quotient group G/K exists and it is abelian. Also $1 \le o(G/K) < o(G)$

Now $\exists$ integers m_1, m_2 such that $n = mm_1$ and $m = pm_2$ Hence $o(G/K) = \frac{n}{p} = \frac{mm_1}{p} = \frac{pm_2m_1}{p} = m_2m_1$