Given \( n \in \mathbb{Z} \) and \( N \geq 1 \), we define \( n \mod N \in \{0, \cdots, N-1\} \) to be the remainder of the euclidean division of \( n \) by \( N \). We recall that the map
\[
n \in \mathbb{Z} \mapsto n \mod N \in \mathbb{Z}/N\mathbb{Z}
\]
is a group homomorphism.

**Exercise 3 – Solution.**

1. We first define
\[
k(a,b) := (a,b) \oplus \cdots \oplus (a,b) = (ka \mod 3, kb \mod 5)
\]
k times

A positive integer number \( N \) is the order of \((1,1)\) in \( \mathbb{Z}_3 \times \mathbb{Z}_5 \) if two following conditions are satisfied : \( N(1,1) = (0 \mod 3, 0 \mod 5) \), and \( N \) is the smallest number. It is easy to check that for all \( 1 \leq k < 15, k(a,b) \neq (0 \mod 3, 0 \mod 5) \), and \( 15(1,1) = (0 \mod 3, 0 \mod 5) \). This implies that the order of \((1,1)\) is 15.

2. Since the order of \((1,1)\) is equal to the order of \( \mathbb{Z}_3 \times \mathbb{Z}_5 \), we obtain that \( \mathbb{Z}_3 \times \mathbb{Z}_5 \) is a cyclic group spanned by \((1,1)\). On the other hand, it is clear that \( \mathbb{Z}_{15} \) is a cyclic group of order 15, which implies that
\[
\mathbb{Z}_3 \times \mathbb{Z}_{15} \cong \mathbb{Z}_{15}.
\]
One also can prove that the following map is an isomorphism :
\[
\phi : \mathbb{Z}_3 \times \mathbb{Z}_5 \rightarrow \mathbb{Z}_{15}, (1,1) \rightarrow 1.
\]

3. There is no element in \( \mathbb{Z}_2 \times \mathbb{Z}_2 \) of order 4, but the order of 1 in \( \mathbb{Z}_4 \) is 4. Thus there is no isomorphism between \( \mathbb{Z}_2 \times \mathbb{Z}_2 \) and \( \mathbb{Z}_4 \).

4. To solve this part, we use the following :

For any finite group \( G \) and an element \( x \in G \), if \( x^N = e \) for some \( N \in \mathbb{N} \) then the order of \( x \) divides \( N \).

It is clear that \( ppmc[m,n](1,1) = (0 \mod m, 0 \mod n) \). This implies that the order of \((1,1)\) in \( \mathbb{Z}_m \times \mathbb{Z}_n \) divides \( ppmc[m,n] \).

5. If \( m \) and \( n \) are relatively prime, then \( ppmc[m,n] = mn \). On the other hand, if \( N(1,1) = (0 \mod m, 0 \mod n) \), then \( ppmc[m,n] \) divides \( N \) since \( m \) and \( n \) are relatively prime. This implies that the order of \((1,1)\) is \( ppmc[m,n] \).

6. Since \( m \) and \( n \) are relatively prime, one can use the same arguments as in part (2) to indicate that
\[
\mathbb{Z}_m \times \mathbb{Z}_n \cong \mathbb{Z}_{mn}.
\]

**Exercise 4 – Solution.**

1. Since \( G \) is a finite group, we have that for every element \( g \in G \), the order of \( g \) divides the order of \( G \). On the other hand, the order of \( G \) is a prime, this leads to that the order of \( g \) is either 1 or \( p \).

2. Since \( G \) is a finite group of order prime \( p \), there is always exists an element \( g \) with \( \text{ord}(g) > 1 \). Therefore, \( \text{ord}(g) = p \). Thus \( G \) is a cyclic group spanned by \( g \). On the other hand, \( \mathbb{Z}_p \) is a cyclic group of order \( p \) spanned by 1. This implies that there is an isomorphism between \( G \) and \( \mathbb{Z}_p \). Note that one also can prove by setting a map as in the exercise 3(2).

**Exercise 6 – Solution.**
1. Suppose that \((N, n) = d\). This implies that \(N = dt\) and \(n = dk\) for some \(t, k \in \mathbb{N}\). In order to prove that \(N/\langle N, n \rangle\) is the order of \(g^n\), we need to check the following properties:

\[ (g^n)^N = e \]

and if \(m\) is a positive integer with \((g^n)^m = e\), then \(m \geq N/(n, N)\). Indeed, \((g^n)^N = g^{nk} = (g^N)^k = e^k = e\). For the second property, suppose that \(m < N/(n, N)\). Then we have \(m\) divides \(N/(n, N)\), which implies that \(N = mt(n, N)\) for some \(t > 1 \in \mathbb{N}\). On the other hand, we have \(g^{nm} = e\), which implies that \(nm = Nx\) for some \(x \in \mathbb{N}\). Therefore \(n = tx(n, N)\). From this, we obtain \(\langle n, N \rangle = t(n, N)\) with \(t > 1\). This leads to a contradiction.

2. We have that \(g^n\) is a generator of \(G\) if and only if the order of \(g^n\) is \(N\). From the first part, we have that the order of \(g^n\) is \(N\) if and only if \((N, n) = 1\).

3. To prove that the map

\[ \phi : \{d | N\} \rightarrow (g^d)^Z \]

is a bijection, we check the following:

i. The map \(\phi\) is injective. Indeed, for \(d_1, d_2\) which are different divisors of \(N\), we have \((g^{d_1})^Z \neq (g^{d_2})^Z\), since if \((g^{d_1})^Z = (g^{d_2})^Z\), then the order of \(g^{d_1}\) is equal to the order of \(g^{d_2}\). This implies that \(N/d_1 = N/d_2\). In other words, \((g^{d_1})^Z = (g^{d_2})^Z\) if and only if \(d_1 = d_2\).

ii. Let \((g^n)^Z\) be a subgroup of \(G\), then it is easy to check that \((g^n)^Z = (g^{(N, n)})^Z\), thus \(\phi((N, n)) = (g^n)^Z\).