Q. 1. Prove that the square of any odd integer always leaves a remainder of 1 when divided by 8.

Proof. Let $n = 2k + 1$ for some $k \in \mathbb{Z}$. Then

$$n^2 = (2k + 1)^2 = 4k^2 + 4k + 1 = 4k(k + 1) + 1.$$  

Either $k$ or $k + 1$ is an even integer. So, 8 divides $4k(k + 1)$. Hence, $n^2 \equiv 1 \mod 8$. □

Q. 2. Let $n$ be an integer greater than 1. Determine the value of

$$\gcd(n! + 1, (n + 1)! + 1).$$

Proof. Assume that $\gcd(n! + 1, (n + 1)! + 1) = d$. Then $n! + 1 = da$ for some $a \in \mathbb{Z}$. Equivalently, $n! = da - 1$. We have

$$(n + 1)! + 1 = (n + 1)n! + 1 = (n + 1)(da - 1) + 1 = da(n + 1) - n.$$  

So, $(n + 1)! + 1 \equiv 1 \mod d$. This is a contradiction unless $d = 1$. Therefore, $n! + 1$ and $(n + 1)! + 1$ must be relatively prime.

Alternatively, you may use Euclidean Algorithm to conclude that $d = 1$. □

Q. 3. Show that 328 divides $25^{80} - 3^{800}$.

Proof. We will use Euler’s Theorem to reduce the integers modulo 328. We have $\phi(328) = \phi(8)\phi(41) = 4 \cdot 40 = 160$. Also,

$$25^{80} - 3^{800} = (5^2)^{80} - (3^{160})^5 = 5^{160} - (3^{160})^5.$$  

Since, $(5, 328) = 1$ and $(3, 328) = 1$, we find $5 \equiv 1 \mod 328$ and $3 \equiv 1 \mod 328$. Therefore, $5^{160} - (3^{160})^5 \equiv 1 - 1 \equiv 0 \mod 328$. In other words, 328 divides $25^{80} - 3^{800}$. □

Q. 4. Let $p$ be a prime and let $1 \leq k \leq p - 1$ be an integer. Prove that

$$\left(\frac{p - 1}{k}\right) \equiv (-1)^k \mod p.$$  

Proof. By definition

$$\left(\frac{p - 1}{k}\right) = \frac{p!}{k!(p - 1 - k)!} = \frac{(p - 1)(p - 2) \cdots (p - k)}{k!}.$$  

MAT 312 - AMS 351
PRACTICE QUESTIONS for FINAL EXAM
SUMMER II, 2014
Notice that \( p - i \equiv -i \mod p \) for all \( i \in \{0, 1, \ldots, p\} \). Therefore,

\[
\binom{p-1}{k} = \frac{(p-1)(p-2) \cdots (p-k)}{k!} \equiv \frac{(-1)(-2) \cdots (-k)}{1 \cdot 2 \cdots k} \mod p \equiv (-1)^k \mod p.
\]

\(\square\)

Q. 5. Let \( G = \{a, b, c, d, f, g\} \) be a group with an operation \(*\) given by the table

<table>
<thead>
<tr>
<th>*</th>
<th>a</th>
<th>b</th>
<th>c</th>
<th>d</th>
<th>f</th>
<th>g</th>
</tr>
</thead>
<tbody>
<tr>
<td>a</td>
<td>d</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>b</td>
<td></td>
<td>g</td>
<td>d</td>
<td>c</td>
<td></td>
<td></td>
</tr>
<tr>
<td>c</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>d</td>
<td></td>
<td>d</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>f</td>
<td></td>
<td>f</td>
<td>g</td>
<td>d</td>
<td></td>
<td></td>
</tr>
<tr>
<td>g</td>
<td></td>
<td>c</td>
<td>a</td>
<td>f</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

a) Fill in the remainder of the group table (the identity element does not necessarily head the first column or the first row).

b) Write down the product table for the group \( S(3) \).

c) Show that \( G \) and \( S(3) \) are isomorphic (describe a group isomorphism between the two groups).

d) What is the smallest group of \( G \) that contains \( g \)?

**Proof.**

a) First, we determine the identity element of \((G, \ast)\). We look for an element \( e \in G \) satisfying \( e \ast e = e \). According to the table, \( d \ast d = d \). So \( d \) must be the identity element. Secondly, \( d \ast x = x = x \ast d \) for all \( x \in G \). Using this, we fill in the rows and columns represented by \( d \) to get

<table>
<thead>
<tr>
<th>*</th>
<th>a</th>
<th>b</th>
<th>c</th>
<th>d</th>
<th>f</th>
<th>g</th>
</tr>
</thead>
<tbody>
<tr>
<td>a</td>
<td>d</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>b</td>
<td></td>
<td>g</td>
<td>d</td>
<td>c</td>
<td></td>
<td></td>
</tr>
<tr>
<td>c</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>d</td>
<td></td>
<td>d</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>f</td>
<td></td>
<td>f</td>
<td>g</td>
<td>d</td>
<td></td>
<td></td>
</tr>
<tr>
<td>g</td>
<td></td>
<td>c</td>
<td>a</td>
<td>f</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Every element of \( G \) has to appear exactly once in each row and column of the table. Following this rule we can place \( b \) and \( d \) in the last row: in the first column, \( a \ast a = d \) so \( g \ast a \) cannot be equal to \( d \). We must have \( g \ast f = d \), and hence \( g \ast a = b \):
Now, let us consider the first column. We need to place \( c \) and \( f \). Since, \( c \ast d = c \), we cannot have \( c \ast a = c \). So, \( c \ast a \) must be \( f \) and \( f \ast a = c \).

In the fifth row, we have \( f \ast b = a \) since we cannot have \( f \ast c = a \) (as \( g \ast c = a \)); and \( f \ast c = b \). Now the table has the form

By a similar consideration for the remaining entries, we get
b) For the multiplication table for $S(3)$ see Example 2 on page 157 of the textbook.

c) Let us define a map $\phi: G \rightarrow S(3)$. If $\phi$ is a group homomorphism then $\phi$ must map the identity $d$ of $G$ to the identity permutation id of $S(3)$. So, we set $\phi(d) = \text{id}$.

In $S(3)$, the elements of order 2 are $(1\ 2), (1\ 3), (2\ 3)$. On the other hand, in $G$, we have $a\ast a = d$, $b\ast b = d$ and $c\ast c = d$. Therefore, $\phi$ should identify $\{a, b, c\}$ with $\{(1\ 2), (1\ 3), (2\ 3)\}$ and $\{f, g\}$ with $\{(1\ 2\ 3), (1\ 3\ 2)\}$. – mapping an element of order 2 to an element of order 3 (or vice versa) in $S(3)$ by $\phi$ would cause problems (see the solution for Q.8.). So, let $\phi(f) = (1\ 2\ 3)$ and $\phi(g) = (1\ 3\ 2)$ (this is optional, we could also choose $\phi(f) = (1\ 3\ 2)$ and $\phi(g) = (1\ 2\ 3)$).

We will assign the values of $\phi$ at $a, b, c$ using the properties of group homomorphism. The key point is that $\phi$ ‘respects’ group operations on both $G$ and $S(3)$. For example, $\phi(a\ast b) = \phi(a)\phi(b)$, etc. We need to choose $\phi(a), \phi(b), \phi(c)$ among $(1\ 2), (1\ 3), (2\ 3)$ so that the following hold

\[(2\ 3)(1\ 2) = (1\ 2)(1\ 3) = (1\ 3)(2\ 3) = (1\ 3\ 2) = \phi(g),\]
\[(2\ 3)(1\ 3) = (1\ 3)(1\ 2) = (1\ 2)(2\ 3) = (1\ 2\ 3) = \phi(f).\]

So, let $\phi(a) = (1\ 2)$. Since $a\ast b = f$, we have
\n$$\phi(a\ast b) = \phi(a)\phi(b) = (1\ 2)\phi(b) = \phi(f) = (1\ 2\ 3).$$
Then we must have $\phi(b) = (2\ 3)$. This leaves $\phi(c) = (1\ 3)$. You can check that now $\phi(x\ast y) = \phi(x)\phi(y)$ for all $x, y \in G$ and $\phi$ is bijective. This ends the proof.

Alternatively, a bijection can be observed (after assigning $\phi(d) = \text{id}$) by comparing the two tables. If there is a bijection between two groups then their operation tables should ‘coincide’, possibly after a reordering of the rows and columns.

d) Let $H$ denote the smallest subgroup of $G$ containing $g$. Since $H$ is a subgroup it must also contain the identity element, which is $d$. So, $d \in H$. We have $g\ast g = f$, so $f \in H$ ($H$ is closed under $\ast$). As $f\ast f = g$ and $f\ast g = g\ast f = d \in H$, we conclude that $H = \{d, f, g\}$. $\square$

Q. 6. Let $f: G \rightarrow H$ be a group isomorphism. Prove that $G$ is commutative if and only if $H$ is commutative.

Proof. Assume that $G$ is commutative. Then $g_1g_2 = g_2g_1$ for all $g_1, g_2 \in G$. Let $h_1, h_2 \in H$. Since $f$ is an isomorphism, it is one-to-one and surjective. So, there exist unique elements $g_1, g_2 \in G$ such that $f(g_1) = h_1$ and $f(g_2) = h_2$. By the definition of a group homomorphism and $g_1g_2 = g_2g_1$, we get

$$h_1h_2 = f(g_1)f(g_2) = f(g_1g_2) = f(g_2g_1) = f(g_2)f(g_1) = h_2h_1.$$ 
So, $H$ is also commutative.

Now assume that $H$ is commutative. Let $g_1, g_2 \in G$. Then $f(g_1g_2) = f(g_1)f(g_2)$. Since $f(g_1), f(g_2) \in H$, $f(g_1)f(g_2) = f(g_2)f(g_1)$. So,

$$f(g_1g_2) = f(g_1)f(g_2) = f(g_2)f(g_1) = f(g_2g_1)$$
which implies that $g_1g_2 = g_2g_1$ and $G$ is commutative. $\square$
Q. 7. Let \( H \) and \( K \) be subgroups of a group \( G \). Prove that \( H \cup K \) is a subgroup of \( G \) if and only if either \( H \subseteq K \) or \( K \subseteq H \).

Proof. Let us assume that \( H \cup K \) is a subgroup of \( G \) and show that either \( H \subseteq K \) or \( K \subseteq H \). The statement “\( H \subseteq K \) or \( K \subseteq H \)” is equivalent to “\( H \setminus K = \emptyset \) or \( K \setminus H = \emptyset \)”.

So, assume that \( H \setminus K \neq \emptyset \) and \( K \setminus H \neq \emptyset \). Let \( x \in H \setminus K \) and \( y \in K \setminus H \). Then, \( x, y \in H \cup K \). Since \( H, K \) and \( H \cup K \) are all subgroups, we have \( x^{-1} \in H \), \( y^{-1} \in K \) and \( xy \in H \cup K \). Now, \( xy \in H \cup K \) implies that \( xy \in H \) or \( xy \in K \).

If \( xy \in H \) then \( x^{-1}xy = y \in H \). This is a contradiction.

If \( xy \in K \) then \( xy^{-1} = x \in K \). This is also a contradiction. So, \( H \setminus K = \emptyset \) or \( K \setminus H = \emptyset \).

On the other hand, if \( H \subseteq K \) or \( K \subseteq H \) then \( H \cup K = H \) or \( H \cup K = K \). In either case \( H \cup K \) is a subgroup.

\( \square \)

Q. 8. Prove that there exists no isomorphism between the groups \( G_7 \) and \( S(3) \).

Proof. Notice that, since \( G_7 = \langle [3]_7 \rangle \), \( G_7 \) is a cyclic group of order 6 (\( [3]_7 \) has multiplicative order 6). On the other hand, \( S(3) \) is not cyclic (there is no permutation of order 6 in \( S(3) \)). Let us assume that there exists an isomorphism \( f: G_7 \rightarrow S(3) \) and find a contradiction.

Since \( f \) is a group homomorphism, \( f \) maps the identity of \( G_7 \) to the identity of \( S(3) \): \( f([1]_7) = \text{id} \). Assume that \( f([3]) = \pi \) for some \( \pi \in S(3) \). The order of \( \pi \) is then either 1, 2 or 3. The order of \( \pi \) cannot be 1 because the only permutation of order 1 is the identity permutation and \( f \) is assumed to be one-to-one. If the order of \( \pi \) is 2 then

\[
\text{id} = \pi^2 = f([3]_7)f([3]_7) = f([3]_7[3]_7) = f([3]_7^2).
\]

As \( f([1]_7) = \text{id} \), we must have \([3]_7^2 = [1]_7 \) (\( f \) is one-to-one). This is a contradiction.

Similarly, assuming the order of \( \pi \) is 3 also yields a contradiction. Therefore there can be no isomorphism between \( G_7 \) and \( S(3) \). \( \square \)

Q. 9. Let \( G \) be a group and \( x \in G \) such that \( x^2 \neq e \) but \( x^6 = e \). Prove that \( x^4 \neq e \) and \( x^5 \neq e \). What can you say about the order of \( x \) in \( G \)?

Proof. The assumption \( x^6 = e \) implies that \( x^4x^2 = e \) and then \( x^4 = x^{-2} \). Since \( x^2 \neq e \), \( x^{-2} \neq e \). So, \( x^4 \neq e \).

Multiplying both sides of \( x^6 = e \) by \( x^{-1} \) gives \( x^5 = x^{-1} \). Now, \( x^{-1} \neq e \) since otherwise, \( x^{-1} = e \) would imply \( x^{-2} = e \). So, \( x^5 \neq e \).

It follows that the order of \( x \) in \( G \) is either 3 or 6. \( \square \)
Q. 10. Let $X$ be a finite set. Is $P(X)$, the set consisting of all subsets of $X$, a group with the set operation $\cup$? Why (not)?

Proof. The operation $\cup$ on $P(X)$ is associative and closed. The identity element is $\emptyset \in P(X)$. However, there is no set $B \in P(X)$ for any $A \in P(X)$ satisfying $A \cup B = \emptyset$. Therefore, $(P(X), \cup)$ is not a group. $\square$