QUIZ ONE ANSWERS

1 Mandatory Section

Q1)

Is $U(16)$ a cyclic group?

Answer: **NO**
Theorem: All subgroups of a cyclic group are cyclic.
Contrapositive: If a group has a non-cyclic subgroup, then it's not cyclic.
Observe that the subgroup $\{1, 7, 9, 15\}$ of $U(16)$ is not cyclic[1].

Q2)

Consider the Cayley table of the group G, cells contain the value row$\times$ column:

$\times$	1	-1	a	$-a$	b	$-b$	c	$-c$
1	1	-1	a	$-a$	b	$-b$	c	$-c$
-1	-1	1	$-a$	a	$-b$	b	$-c$	c
a	a	$-a$	-1	1	c	$-c$	$-b$	b
$-a$	$-a$	a	1	-1	$-c$	c	b	$-b$
b	b	$-b$	$-c$	c	-1	1	a	$-a$
$-b$	$-b$	b	c	$-c$	1	-1	$-a$	a
c	c	$-c$	b	$-b$	$-a$	a	-1	1
$-c$	$-c$	c	$-b$	b	a	$-a$	1	-1

How many subgroups does the group G have? (count the trivial ones too)

Answer: **6**

Order 1	$\{1\}$
Order 2	$\{1, -1\}$
Order 4	$\{1, -1, a, -a\}$
Order 4	$\{1, -1, b, -b\}$
Order 4	$\{1, -1, c, -c\}$
Order 8	$\{1, -1, a, -a, b, -b, c, -c\}$

[1] The Klein Four Group.

Q3)

Let D_3 be the group of symmetries of the equilateral triangle.
Define a map $[\cdot,\cdot] : D_3 \times D_3 \to D_3$ defined by $[a,b] = aba^{-1}b^{-1}$.
Let $H := \Big\{[g,h] \mid \text{any two } g,h \in D_3\Big\}$
Is H a subgroup of D_3?

Answer: **YES**
$H = \{e, R_{120}, R_{240}\}$ which is a subgroup of D_3.
A Sage script to compute this:

```
sub = []
H = DihedralGroup(3)
for g in H:
    for h in H:
       temp = g*h*g^-1*h^-1
       if temp not in sub:
          sub.append(temp)
print(sub)
```

2 Optional Section

Q4)

The point A, given below, belongs to the cyclic subgroup $\left\langle \left(\frac{a}{p}, \frac{b}{p}\right) \right\rangle$ of the group of rational points on the unit circle where $a > b > 0$ and p is an odd prime such that $p \equiv 1 \pmod 4$.

Find $\left(\frac{a}{p}, \frac{b}{p}\right)$

ANSWER FORMAT: `a/p<space>b/p`.

For instance, if you think the answer is $\left(\frac{3}{5}, \frac{4}{5}\right)$, type: `4/5 3/5`

Answer: $\left(\frac{1855}{2017}, \frac{792}{2017}\right)$

Lemma: All elements of $\left\langle \left(\frac{a}{p}, \frac{b}{p}\right) \right\rangle$ have denominators of the form p^n

Factoring the denominator in A, we obtain $(2017)^{21}$.
Thus our task becomes finding the Pythagorean triple $(a, b, 2017)$
Observe that 2017 decomposes[2] as $44^2 + 9^2$.
Recall[3], Pythagorean triplets have the form $(m^2 - n^2, 2mn, m^2 + n^2)$
Hence $a = 1855$ and $b = 792$.

[2] Multiple proofs for this exist, even a one-liner.
[3] Euclid devised this.

Q5)

Let a, b be non-identity elements in a group G such that $a^{-1}ba = b^2$
If a has an order of 31, what is the order of b?
If you think it cannot be determined, type : `NA`

Answer: 2,14,74,83,647 $(2^{31} - 1)$
Observe that $\left(a^{-1}ba\right)^2 = a^{-1}b^2a$.
Substituting b^2 back in, $a^{-1}b^2a = a^{-2}ba^2$
However $\left(a^{-1}ba\right)^2 = b^4$, thus $a^{-2}ba^2 = b^4$
Using this inductively, we obtain $a^{-31}ba^{31} = b^{2^{31}}$
Since a is of order 31, we obtain $b^{2^{31}-1} = e$.
$2^{31} - 1$ is a prime[4] and since $b \neq e$, the order of b must be $2^{31} - 1$.

Q6)

How many times do you need to repeat the rubik's cube algorithm `RULD` from the solved state to return back to the solved state?
The algorithm is read as:

```
move the right face clockwise
move the top face clockwise
move the left face clockwise
move the down face clockwise
```

A picture showing the first use of the algorithm:

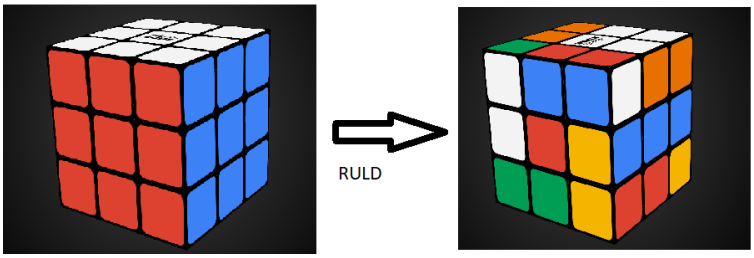

Figure 1: `RULD`

Answer: 315
SAGE has many Rubik's Cube™ functionalities as well.
SAGE encodes a clockwise movement of each face as an element from the permutation group S_{48}.

[4] Primes that are repeating ones in binary..

SAGE maps the state obtained after `RULD` algorithm (rightmost in Figure 1). The number of times `RULD` needs to be applied to revert back to the solved state is equivalent to finding the order of the element that this state is mapped to.
A Sage script to solve the order question:

```
# instantiate the cube
R = CubeGroup()
# encode the RULD algorithm
alg = R.move("R1*U1*L1*D1*")[0]
# obtain the order
print(alg.order())
```