1. In the end-game phase of the Oval Track puzzle show that any 4-cycle can always be reduced to a 2-cycle by using a 3-cycle. (Note: this is stated in the solution flow chart from the notes, here you are asked to prove this always works.)

   Solution: A 4-cycle has the form $(a\ b\ c\ d)$ which factors as

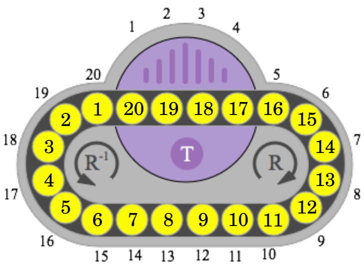
$$\begin{aligned}(a\ b\ c\ d) &= (a\ b)(a\ c)(a\ d)\\ &= (a\ b)(a\ c\ d)\end{aligned}$$

   Therefore, if the configuration of the puzzle is $(a\ b\ c\ d)$ then applying the 3-cycle $(a\ d\ c) = (a\ c\ d)^{-1}$ produces

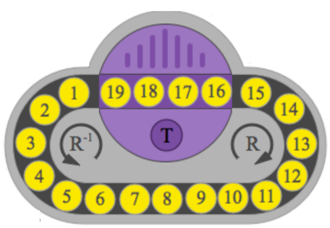
$$\begin{aligned}(a\ b\ c\ d)(a\ d\ c) &= (a\ b)(a\ c\ d)(a\ d\ c)\\ &= (a\ b)\end{aligned}$$

   which is a 2-cycle.

2. (a) For the oval track puzzle with 20-disks is the following configuration of disks solvable? Explain.



   (b) For the oval track puzzle with 19-disks is the following configuration of disks solvable? Explain.



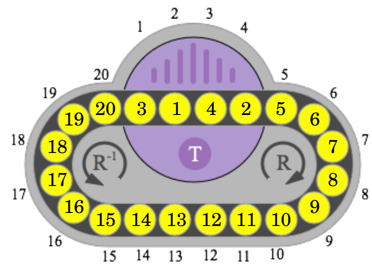
   Solution: (a) Yes, since $OT_{20} = S_{20}$, which means every permutation is solvable.

   (b) This configuration corresponds to the permutation

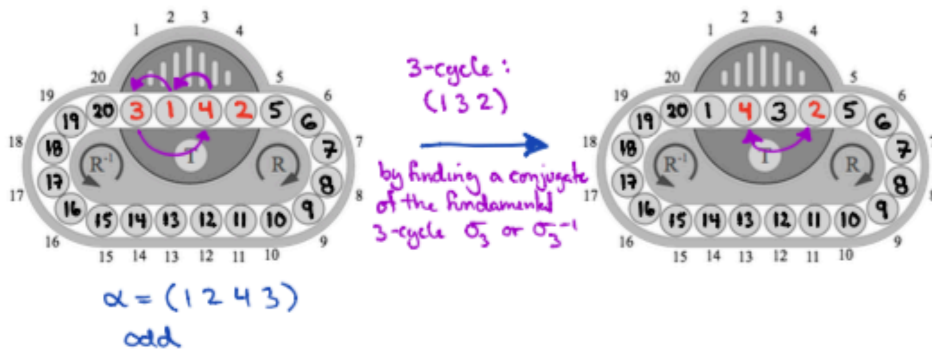
$$\alpha = (1\ 19)(2\ 18)(3\ 17)(4\ 16)(5\ 15)(6\ 14)(7\ 13)(8\ 12)(9\ 11)$$

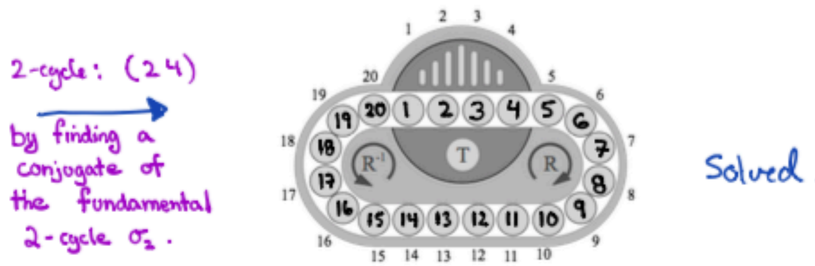
   which is odd (nine 2-cycles). However, $OT_{19} \leq A_{19}$ since both basic moves R and T are even (the former is a 19-cycle). Therefore, this configuration is not solvable.

3. Consider the configuration of the oval track puzzle shown below. To solve the puzzle we just need to use two fundamental moves: $\sigma_2 = (1\ 3)$ and $\sigma_3 = (1\ 7\ 4)$, and their conjugates. Provide an outline of the steps involved in solving this configuration, indicate which move (a 2-cycle or a 3-cycle) you are using at each step, and draw the resulting configuration. You do not need to find the sequence β to conjugate σ_2 or σ_3, just provide an outline of the solution steps.



Solution:





4. **Permutations: decompositions into 2-cycles of the form $(1\ m)$:**

   We know that every permutation in S_n can be expressed as a product of 2-cycles. Show the stronger result that every permutation in S_n can be expressed as a product of 2-cycles of the form $(1\ m)$, where $2 \leq m \leq n$.

   (This is equivalent to showing that every permutation is obtainable on the Swap puzzle where the only legal move is to swap the contents of any box with box 1. You may use the Swap puzzle to investigate this statement, but the argument you present should be described in terms of permutations.)

   Solution: For any $1 \leq i < j \leq n$, let $j = i + m$, then we have

   $$(i\ j) = (i\ i{+}m) = (i\ i{+}1)(i{+}1\ i{+}2)\cdots(i{+}m{-}2\ i{+}m{-}1)(i+m-1\ i+m)(i{+}m{-}1\ i{+}m{-}2)\cdots(i{+}1\ i{+}2)(i\ i{+}1)$$

   This has the form $\gamma(i+m-1\ i+m)\gamma^{-1}$, where γ moves tile i to the right by swapping with its neighbour each step.

   In other words, to swap i and j first move i to the right by swapping with its neighbour each time, then once it is next to j swap i and j. Then move j to the left by swapping with its neighbour each time, until it is in box i.

5. **Permutations: decompositions into 4-cycles:**

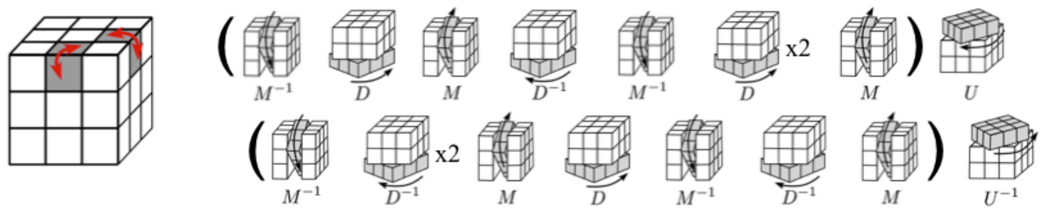
   Can every permutation in S_n, for $n \geq 4$, be written as a product of 4-cycles? Justify your answer.

Solution: Yes. This is since every 2-cycle can be written as a product of 4-cycles:

$$(a\ b) = (a\ b\ c\ d)(a\ b\ c\ d)(a\ c\ b\ d).$$

(You can find such a decomposition by using your Swap board with only four boxes: set-up the board so tiles 1 and 2 are switched, then solve using 4-cycles. For example, $(1\ 2) = (1\ 2\ 3\ 4)(1\ 2\ 3\ 4)(1\ 3\ 2\ 4)$.)

6. (a) Consider the following move sequence for flipping adjacent edges. What is the purpose of the initial part of the sequence consisting of $M^{-1}DMD^{-1}M^{-1}D^2M$?



(b) Using the above sequence, or a slight modification of it, come up with <u>three</u> different ways to flip two opposite edges (the uf and the ub edges).

Solution: (a) It flips the edge cubie in the uf position, it doesn't do anything else to cubies in the up-layer. It does mess cubies up in the bottom layer. This means it is a good candidate to use as a commutator with U.

(b) Let $E_2 = [\alpha, U]$ be the commutator in part (a).

① $E_2(\mathcal{U} E_2 \mathcal{U}^{-1})$

② Modify E_2 as $[\alpha, U^2]$

③ conjugate E_2: $B^{-1}R^{-1}E_2RB$

7. Suppose $G = \{e, a, b, c, d, f\}$ is a group with Cayley table

	e	a	b	c	d	f
e	e					
a		e				
b		f				
c				e	a	
d		c	a			
f		b	c	a	e	

Fill in the blank entries.

Solution:

	e	a	b	c	d	f
e	e	a	b	c	d	f
a	a	e	d	$\boxed{f}$	$\boxed{b}$	c
b	b	f	e	d	c	a
c	c	d	f	e	a	b
d	d	c	a	$\boxed{b}$	$\boxed{f}$	e
f	f	b	c	a	e	d

In a group, if $x^2 = x$ then multiplying both sides by x^{-1} we get $x = 1$

Therefore, only the identity is a solution to $x^2 = x$.

From the table we see e is the identity. Therefore we can fill out row 1 and column 1.

To fill out the rest of the table we keep Lemma 10.1 (a) in mind:

Every element of G must appear in every row and every column.

I will write down the order in which entries can be filled in (can you determine the reasons?)

1. $ca = d$ (column a missing d)
2. $ff = d$ (row f missing d)
3. $cf = b$ (row c must contain b, but columns a and b already have b's in them)
4. $cb = f$ (row c is only missing an f)
5. $df = e$ (row d must contain e, but columns c & d already have e's in them)
6. $bf = a$ (column f must contain a, but rows a & d already have a's in them)
7. $af = c$ (column f missing c)
8. $ab = d$ (this can be neither b nor f since these are in column b already)
9. $bb = e$ (column b missing e)
10. $bc = d$
11. $bd = c$

(10), (11): row b missing d & c, couldn't have $bc = c$ & $bd = d$ since $b \neq e$.

dd is either b or f. If $dd = b$, then $d^3 = db = a$, $d^4 = da = c$, $d^5 = dc = f$ & $d^6 = df = e$ $\Rightarrow$ $\text{ord}(d) = 6$ $\Rightarrow$ Group is cyclic $\Rightarrow$ Group is abelian. This is a contradiction since clearly it isn't.

Therefore, $dd = f$. The rest of the table follows. $\square$

If you want to see for sure that this Cayley table really represents a group notice it is just the group S_3 where $e = \varepsilon$, $a = (1,2)$, $b = (1,3)$, $c = (2,3)$, $d = (1,2,3)$, $f = (1,3,2)$

8. **All about commutators.**

   (a) Let $\alpha, \beta \in S_n$. Show that the commutator $[\alpha, \beta]$ is an even permutation.

   (b) For g, h in a group G, show that $[g, h]^{-1} = [h, g]$.

   (c) For g, h, k in a group G, show that $[g, h]^k = [g^k, h^k]$.

Solution: (a) Write α and β as a product of 2-cycles:

$$\alpha = \sigma_1\sigma_2 \cdots \sigma_k, \quad \beta = \tau_1\tau_2 \cdots \tau_\ell,$$

where σ_i, τ_j are 2-cycles. Then

$$\begin{aligned}[\alpha,\beta] &= \alpha\beta\alpha^{-1}\beta^{-1}\\ &= \sigma_1\sigma_2\cdots\sigma_k\tau_1\tau_2\cdots\tau_\ell\sigma_k^{-1}\cdots\sigma_2^{-1}\sigma_1^{-1}\tau_\ell^{-1}\cdots\tau_2^{-1}\tau_1^{-1}\end{aligned}$$

is a product of $2k+2\ell = 2(k+\ell)$ 2-cycles. Hence, $[\alpha,\beta]$ is even.

(b)

$$\begin{aligned}[g,h]^{-1} &= (ghg^{-1}h^{-1})^{-1}, && \text{by definition of commutator}\\ &= hgh^{-1}g^{-1}, && \text{by property of inverses of products}\\ &= [h,g], && \text{by definition of commutator.}\end{aligned}$$

(c)

$$\begin{aligned}[g^k,h^k] &= [k^{-1}gk, k^{-1}hk], && \text{by definition of } g^k \text{ and } h^k\\ &= (k^{-1}gk)(k^{-1}hk)(k^{-1}g^{-1}k)(k^{-1}h^{-1}k), && \text{by definition of commutator}\\ &= k^{-1}g(kk^{-1})h(kk^{-1})g^{-1}(kk^{-1})h^{-1}k, && \text{by associativity}\\ &= k^{-1}g(e)h(e)g^{-1}(e)h^{-1}k, && \text{by property of inverses}\\ &= k^{-1}ghg^{-1}h^{-1}k, && \text{by property of identity}\\ &= k^{-1}[g,h]k\\ &= [g,h]^k\end{aligned}$$

9. Let G be a group of order 34. What are the possible orders of the elements of G?

Solution: The order of an element must divide the order of the group. Since the divisors of 34 are $1, 2, 17, 34$ then the order of an element of G is possibly

$$1,\ 2,\ 17,\ \text{or } 34.$$

10. Let $G = \{e, a, b, c\}$ be a group, where e is the identity.
(a) Assume G has an element of order 4, say a. Then there must be a second element of order 4, say c. Write out the Cayley table for G.
(b) Assume G does not have an element of order 4, then every (non-identity) element has order 2. If $ab = c$ write out the Cayley table for G.

Solution: (a) Let a have order 4. Then a^2 has order 2 and a^3 has order 4. Thus $a^3 = c$, and $a^2 = b$.

Sample calculations:

$$\begin{aligned}ac &= aa^3 = a^4 = e\\ bb &= a^2a^2 = a^4 = e.\end{aligned}$$

Cayley table:

G	e	a	b	c
e	e	a	b	c
a	a	b	c	e
b	b	c	e	a
c	c	e	a	b

(b) Every element (except e) has order 2. Assume $ab = c$.

Sample calculations:

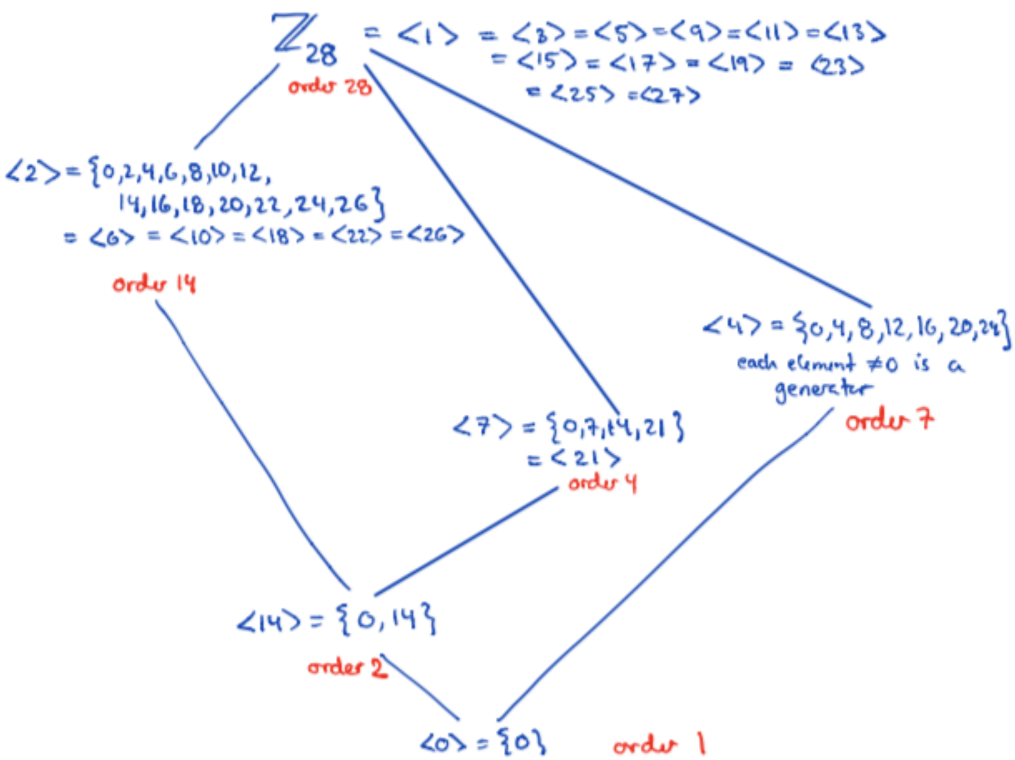
$$\begin{aligned} ab = c &\Rightarrow a(ab) = ac \\ &\Rightarrow a^2 b = ac \\ &\Rightarrow b = ac \end{aligned}$$

Cayley table:

G	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

11. List all subgroups of $\mathbb{Z}_{28}$ and the generators for each subgroup.

Solution:



Altenatively, we can list the subgroups in a table.

subgroup	**order**	**list of all possible generators**
$\langle 1\rangle = \mathbb{Z}_{28}$	28	$1, 3, 5, 9, 11, 13, 15, 17, 19, 23, 25, 27$
$\langle 2\rangle = \{0, 2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26\}$	14	$2, 6, 10, 18, 22, 26$
$\langle 4\rangle = \{0, 4, 8, 12, 16, 20, 24\}$	7	$4, 8, 12, 16, 20, 24$
$\langle 7\rangle = \{0, 7, 14, 21\}$	4	$7, 21$
$\langle 14\rangle = \{0, 14\}$	2	14
$\langle 0\rangle = \{0\}$	1	0

12. List all the elements of $U(8)$ and write out its Cayley table.

Solution: Cayley table:

U(8)	1	3	5	7
1	1	3	5	7
3	3	1	7	5
5	5	7	1	3
7	7	5	3	1

13. List all the elements of $U(21)$. What is the order of 4? What is the order of 5?

Solution:

$U(21) = \{1, 2, 4, 5, 8, 10, 11, 13, 16, 17, 19, 20\}$

order of 4: $4^2 = 16$
$4^3 = 64 \equiv 1 \pmod{21}$
Therefore,
$\text{ord}(4) = 3.$

order of 5: $\text{ord}(5) \mid |U(21)| \Rightarrow \text{ord}(5) \mid 12.$

$5^2 = 25 \equiv 4 \pmod{21}$
$5^3 = 5\cdot5^2 \equiv 5\cdot4 \equiv 20 \pmod{21}$
$5^4 = 5\cdot5^3 \equiv 5\cdot20 \equiv 5(-1) \equiv -5 \equiv 16 \pmod{21}$
$5^6 = 5^3\cdot5^3 \equiv 20\cdot20 \equiv 40\cdot10 \equiv 19\cdot10 \equiv -2\cdot10 \equiv 1 \pmod{21}$

Therefore,
$\text{ord}(5) = 6.$

14. List all the elements of $U(16)$. What is the order of 9? What is the order of 15?

Solution:

$U(16) = \{1, 3, 5, 7, 9, 11, 13, 15\}$, $|U(16)| = 8$

Possible orders of elements are: 1, 2, 4, 8

$9^2 = 81 \equiv 5(16) + 1 \equiv 1 \pmod{16} \Rightarrow \text{ord}(9) = 2$

$15^2 \equiv (-1)(-1) \equiv 1 \pmod{16} \Rightarrow \text{ord}(15) = 2.$

15. Show that for $n \geq 3$ the group $U(2^n)$ is not cyclic?
Hint: Can you find two elements of order 2? Further hint: have another look at the previous question.

Solution:

For $n \geq 3$, the group $U(2^n)$ contains elements

$$a = 2^{n-1} + 1 \quad \text{and} \quad b = 2^n - 1,$$

and each of these has order 2:

$$\begin{aligned} a^2 = (2^{n-1}+1)^2 &= 2^{2n-2} + 2^n + 1 \\ &= 2^n(2^{n-2}) + 2^n + 1 \\ &\equiv 1 \pmod{2^n} \end{aligned}$$

$$b^2 = (2^n - 1)^2 = 2^{2n} - 2^n \cdot 2 + 1 \equiv 1 \pmod{2^n}$$

A cyclic group has at most one element of order 2, therefore $U(2^n)$ is not cyclic for $n \geq 3$.

16. $U(49)$ is a cyclic group with 42 elements. If b is a generator, what are the other generators?

Solution:

$U(49)$ is cyclic with 42 elements.

There are $\varphi(42) = \varphi(2 \cdot 3 \cdot 7) = 1 \cdot 2 \cdot 6 = 12$ generators.

Let b be one generator, then any generator has the form b^k where $\gcd(k, 42) = 1$. $(k = 1, 5, 11, 13, 17, 19, 23, 25, 29, 31, 37, 41)$

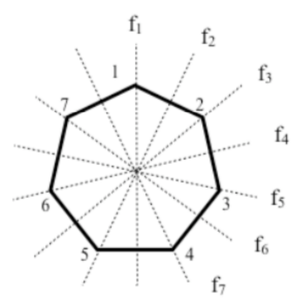
Thus the list of generators is:

$$b, b^5, b^{11}, b^{13}, b^{17}, b^{19}, b^{23}, b^{25}, b^{29}, b^{31}, b^{37}, b^{41}$$

17. Consider the regular 7-gon shown in the picture. Let r denote a clockwise rotation through $\frac{360}{7}$ degrees. The elements of D_7 are

$$D_7 = \{1, r, r^2, r^3, r^4, r^5, r^6, f_1, f_2, f_3, f_4, f_5, f_6, f_7\}$$

where f_i denotes a reflection across a line as shown the figure. Determine the element of D_7 corresponding to $f_1 r f_6$.



Solution: Consider vertex 1, under the symmetries it moves as follows: $1 \xrightarrow{f_1} 1 \xrightarrow{r} 2 \xrightarrow{f_2} 5$ Therefore, $f_1 r f_2$ is a rotation taking 1 to 5, so it is r^4:

$$f_1 r f_2 = r^4.$$