Thm: If a permutation is written as a disjoint union of cycles, then the order of the permutation is the LCM of the lengths of the cycles.
\[ e^y a = (1, 1, 4, 3) \]

\[ a^2 = (1 4 8 3)(1 4 8 3) = (1 8)(6 3) \]

\[ a^3 = (1 4 8 3)(1 8)(6 3) = (1 3 8 6) \]

\[ a^4 = (1 4 8 3)(1 3 8 6) = (1) \]
eg find $b^4$ if

$$b = (1368275)$$

$$b^4 = (1237658)$$

Note that if $c$ is a cycle of length $n$

$$|c| = n$$
Proof:

Suppose \( \delta = \alpha \beta \) where \( \alpha, \beta \) are disjoint, \( |\alpha| = m \), \( |\beta| = n \) and let \( k = \text{LCM} \circ \theta \ m, n \).
Then

\[ (\alpha \beta)^k = \alpha^k \beta^k = 1 \]

Since disjoint cycles commute

Thus \( |\sigma| \mid k \).

Let \( t = |\alpha \beta| \), so \( t \mid k \)
\[ (\alpha \beta)^t = 1 \implies \alpha^t \beta^t = 1 \]

\[ \therefore \alpha^t = \beta^t \]

But \( \beta^t \) can't have any symbols not in \( \beta \) and \( \alpha^t \) can't have any symbols not in \( \alpha \).
But, $\alpha$ and $\beta$ are disjoint, so the only way for $\alpha^t = \beta^{-t}$ is if $\alpha^t = 1 = \beta^{-t}$ (hence $\beta^t = 1$ too).

$\alpha^t = 1 \Rightarrow m | t$, and $\beta^t = 1 \Rightarrow n | t$

$\Rightarrow t$ is a multiple of $m$ and $n$, with $t \leq k$ from above. But $k$ is the least common multiple, so $t = k$. \checkmark
Def: a cycle of length 2 is called a transposition.

Theorem: Every permutation can be written (not necessarily uniquely) as a product of transpositions.
\[ (a_1, a_2, \ldots, a_n) = (a_1, a_n) (a_1, a_{n-1}) \ldots (a_1, a_3) (a_1, a_2) \]

Check:

\[ (1 \ 3 \ 4 \ 8 \ 2) = (1 2)(1 8)(1 6)(1 3) \]

And since we see, every permutation can be written as a disjoint union of cycles, we now can write each cycle as a product of transpositions, so the whole thing is a product of transpositions.
\[ s = (1 \ 3 \ 2 \ e) \ (1 \ 3 \ 2) \ (2 \ 6) \]

\[ = (1 \ 2) \ (3 \ 6) \]
Theorem:

If \( \alpha = \beta_1 \ldots \beta_r \)
and \( \alpha = \delta_1 \ldots \delta_s \)
where \( \beta_i, \delta_i \) are transpositions \( i \neq j \).
Then \( r \) and \( s \) have the same parity.
Proof:

First note that if

\[ 1 = S_1 \cdots S_n, \text{ with } S_i \text{ transpositions} \]

then \( n \) must be even.

Reason: Basically we can remove the \( S_i \)'s a pair at a time.
We are going to pick an element $a$ that appears among the $S_i$'s. If it appears as $(ab)(ba)$, then we can remove this pair.
Otherwise, reading left to right, find the first place a appears and move it to the right using

\[(ab)(ac) = (bc)(ab)\]
\[(ab)(cd) = (cd)(ab)\]
\[(ab)(bc) = (bc)(ac)\]
Since a can't be moved all the way to the right (otherwise won't get the identity)
So at some point it must get cancelled out, removing a pair of transpositions
Continue this process w/ one symbol at a time until the RHS of \( l = s_1 \ldots s_n \) has no more pairs left. Their can't be \( l = (ab) \) left, so \( n \) must have been even to start with.
Now if
\[ \alpha = \beta_1 \cdots \beta_r = \gamma_1 \cdots \gamma_s \]
\[ \Rightarrow \beta_1 \cdots \beta_r \gamma_1^{-1} \cdots \gamma_r^{-1} = 1 \]
\[ \Rightarrow r+s \text{ is even, so } r \text{ and } s \text{ have the same parity.} \]