Recall S_4 . Is there a subgroup of order eight? Though this question could be answered by direct calculation, we'll show here that there is one without calculating it.

Recall that conjugacy is an equivalence relation. Let $Cl(a)$ denote the equivalence class of a.

Let $G_a = \{g \in G \mid ga=ag\}$ Last time we showed this is a subgroup.
Theorem A: $|Cl(a)| = [G: G_a]$ (i.e the size of the conjugacy class of a equals the number of left cosets of G_a in G).
Proof: Let $H= Cl(a)$. We define a function F from $Cl(a)$ to {xH} by:

$$F(xax^{-1}) = xH.$$

First we show 1-1. Suppose $F(xax^{-1}) = F(yay^{-1})$. Then:

$xH=yH \Rightarrow$

$y^{-1}x \in H$ (Lemma proved earlier) $\Rightarrow$

$y^{-1}xa=ay^{-1}x$ (definition of H) $\Rightarrow$

$xax^{-1} = yay^{-1}$ (a little algebra)

Proving 1-1.

Onto is easy. $F(xax^{-1}) = xH$ and for any xH, xax^{-1} is in $Cl(a)$.

Finally we need to show that F is well-defined. I.e. Suppose $xax^{-1} = yay^{-1}$. Then we get $y^{-1}xa=ay^{-1}x$ which tells us that $y^{-1}x \in H$ and hence that xH=yH, showing that Fis well defined.

Thus we've shown that $|Cl(a)| = [G: G_a]$

Now we can answer the original question. {(1,2)(3,4), (1,3)(2,4), (1,4)(2,3)} is a conjugacy class with three members. We can call it: $Cl((1,2)(3,4))$. Thus 3 = [G:Ga] where a=(1,2)(3,4). Therefore |Ga|=8

Define Z(G) = All elements in G that commute with every other element. In an abelian group, Z(G)=G. Note that $g \in Z(G)$ iff $\mathcal{C}l(a) = \{a\}$.

Using theorem A, we can show:

If $|G| = p^n$ where p is a prime, then Z(G) is non-trivial.

Proof:
We can write: $|G| = \Sigma \, | \, \mathcal{C}l(a) \, |$ where we sum over distinct classes.
If we group the singleton classes together we get:
$|G| = |Z(G)| + \Sigma^* \, | \, \mathcal{C}l(a) \, |$
Where the Σ^* denotes summing over distinct classes with at least two members. But now we invoke theorem A (and LaGrange) to see that each $| \, \mathcal{C}l(a) \, |$ divides p^n . I.e. $|\mathcal{C}l(a)| = p^k$. Therefore p divides each term in the sum. But p also divides |G| . Hence p divides |Z(G)|. Therefore $|Z(G)| \geq p$.