Please show your work and write only in pen. Notes are forbidden. Calculators, and all other electronic devices, are forbidden. Brains are encouraged, but at most one may be used per exam.

1: Please state Lagrange’s Theorem correctly.
Up to minor variations in wording or choices of symbols, you should say something close to the following:

Lagrange’s Theorem Given any finite group $G$ with subgroup $H$, $\#H|\#G$.

Note 1: It appears that Lagrange merely discussed some special cases of the theorem we attribute to him: the first proof appears to have been one published by Pietro Abbati Marescotti in 1803.

Note 2: A slightly more high-brow version, which works for infinite groups too, is the following:

Given any group $G$ with subgroup $H$, let $\{gH \mid g \in G\}$ denote the set of left cosets of $H$ in $G$. Then $H \times \{gH \mid g \in G\}$ and $G$ have the same cardinality.
2: (a) Please prove that if \( G \) is any non-cyclic group of cardinality 4, then there are exactly three elements of order 2.
(b) Continuing (a), please show that if the three order 2 elements of \( G \) are \( \alpha, \beta, \gamma \), then \( \alpha \beta = \gamma \). (Note that the order of the labelling doesn’t matter!)

(a) Such a \( G \) clearly has 3 non-identity elements. By Lagrange’s Theorem, their orders must be 2 or 4. Since \( G \) is not cyclic, there can be no order 4 elements and we are done.

(b) In essence, any equality but \( \alpha \beta = \gamma \) would yield a contradiction. Here is what happens in each case:
1. \( \alpha \beta = e \implies \alpha = \beta^{-1} \implies \alpha = \beta \) (since \( \beta^2 = e \implies \beta = \beta^{-1} \)), and this contradicts \( \alpha \neq \beta \).
2. \( \alpha \beta = \alpha \implies \beta = e \) and this contradicts \( \beta \) having order 2.
3. \( \alpha \beta = \beta \) would contradict \( \alpha \) having order 2, by an argument almost identical to that of (2).

So the only possibility remaining is \( \alpha \beta = \gamma \). Note that it is conceivable that \( \alpha \beta = \gamma \) could lead to a contradiction too, so we should at this point construct a group where such an identity holds. \( V \) (the Klein 4-group) is just such an example. In fact, we can even label the elements any way we like, provided \( \alpha, \beta, \) and \( \gamma \) are assigned to distinct order 2 elements. ■
Someone (truthfully) tells you that $G$ has an element $a$ satisfying $a^{47} = e$. Someone else (truthfully) tells you that $a$ also satisfies $a^{50} = e$. Prove that $a$ must be the identity element.

The key here is to express 1 as an integer linear combination of 47 and 50, and then apply the identity to powers of $a$. To do the former, we can either guess cleverly, or just use the Extended Euclidean Algorithm. Going the latter route, we obtain

\[
\begin{align*}
50 &= 1 \cdot 47 + 3 \\
47 &= 15 \cdot 3 + 2 \\
3 &= 1 \cdot 2 + 1 \\
2 &= 2 \cdot 1 + 0
\end{align*}
\]

and thus we need to invert the matrix

\[
M := \begin{bmatrix}
1 & 1 \\
1 & 0
\end{bmatrix} \begin{bmatrix}
15 & 1 \\
1 & 0
\end{bmatrix} \begin{bmatrix}
1 & 1 \\
1 & 0
\end{bmatrix} \begin{bmatrix}
2 & 1 \\
1 & 0
\end{bmatrix} = \begin{bmatrix}
50 & 17 \\
47 & 16
\end{bmatrix}
\]

The inverse is \( \frac{1}{1} \begin{bmatrix}
16 & -17 \\
-47 & 50
\end{bmatrix} \) (and \( \det M = 1 \) since the number of matrices in our product above is even), so we at last obtain $16 \cdot 50 - 17 \cdot 47 = 1$.

To conclude, note then that $e = e \cdot e = e^{16}e^{-17} = (a^{50})^{16}(a^{47})^{-17} = a^{16 \cdot 50 - 17 \cdot 47} = a^1 = a$. ■
4: Please prove that all groups of cardinality $\leq 5$ are Abelian.

Done in class...
Please prove that any group $G$ with $g^2 = e$ for all $g \in G$ must be Abelian.

Let $a, b \in G$ be any two elements of our group. By assumption, $a^2 = e$. So then

$$a = a^{-1},$$

(1)

by multiplying the previous identity by $a^{-1}$ on the right. Similarly,

$$b = b^{-1}$$

(2)

(since $b^2 = e$) and $ab = (ab)^{-1} = b^{-1}a^{-1}$ (since $(ab)^2 = e$).

To conclude, we thus obtain $ab = b^{-1}a^{-1} = ba$ by applying (1) and (2). ■
Please prove that for any nonnegative integer $k$ and a prime $p$, we have $\varphi(p^k) = p^k - p^{k-1}$.

Done in class.
Please prove that, for any distinct primes $p$ and $q$, $\varphi(pq) = \varphi(p)\varphi(q)$.

Done in class.
Please prove Euler’s Theorem: Given any integers $a$ and $m$ with $\gcd(a, m) = 1$, 
\[ a^{\varphi(m)} \equiv 1 \mod m. \]
Done in class.