Recall:

- **Lagrange's Theorem**: If G is a finite group and H is a subgroup of G, then $|H|$ divides G. Moreover, the number of distinct left (right) cosets of H in G, $[G : H]$, is $\frac{|G|}{|H|}$.
- **Corollary 2:** In a finite group, the order of each element of the group divides the order of the group. That is, $|a|$ divides $|G|$ for all $a \in G$, when $|G|$ is finite.
- **Corollary 3:** A group of prime order is cyclic.
- **Corollary 4:** Let G be finite and $a \in G$. Then $a^{|G|} = e$.
- **Corollary 5: Fermat's Little Theorem:** For every integer a and every prime p, $a^p \mod p = a \mod p$.

Theorem: Every group of order $2p$ (p prime) is either isomorphic to $\mathbb{Z}_{2p}$ or D_p.

Step 2 of proof: If $|a| = p$, show every element in $G \backslash <a>$ has order 2.

Assume $\exists b \in G \backslash <a>$ such that $|b| \neq 2$.

$|b| \neq 1$, since $b \neq e$; $|b| \neq 2p$, since G isn't cyclic. Thus $|b| = p$.

$< b > \neq < a >$, since $b \notin < a >$.

Suppose $< a > \cap < b > \neq \{e\}$. Then there exist $i, j \in \{1, 2, \ldots, p-1\}$ such that $b^i = a^j$.

$\left|<b>\right|$ prime $\Longrightarrow b^i$ generates $<b>$, so $\exists\ k \ni b = (b^i)^k = (a^j)^k \in <a>$.
$\rightarrow\!\times\!\leftarrow$

Thus $<a> \cap <b> = \{e\}$, so $\left|<a> \cup <b>\right| = p + (p-1)$, leaving only one element unaccounted for.

Yet there are p distinct elements of the form ba^k, none of which can be in $<a>$ or in $<b>$. $\rightarrow\!\times\!\leftarrow$ Thus $|b| = 2$.

Theorem: Every group of order $2p$ (p prime) is either isomorphic to $\mathbb{Z}_{2p}$ or D_p.

Step 3 of proof: All non-cyclic groups of order $2p$ are isomorphic.

$\exists a \in G$ with $|a| = p$, and $\exists b \in G$ with $|b| = 2$.

Lagrange's Theorem $\Rightarrow \exists$ exactly $\frac{2p}{p} = 2$ cosets of $<a>$ in G; since $b \notin <a>$, the two cosets are $<a>$ and $b<a>$.

Thus:

$$G = \{e, a, a^2, \ldots, a^{p-1}, b, ba, ba^2, \ldots, ba^{p-1}\}.$$

$\forall\ i = 1, 2, \ldots, p-1$, $a^i b \in G$, and obviously $a^i b \notin <a>$, so $|a^i b| = 2$.

Thus

$$a^i b = (a^i b)^{-1} = b^{-1} a^{-i-} = ba^{-i} = ba^{p-i}$$

Thus the Cayley table for any non-cylic group of order $2p$ is completely determined; this ends up meaning that all are isomorphic to each other.

1. **If $|\mathrm{G}| = 91$, show that G has an element of order 7.**

2. **Suppose that G is an Abelian group with an odd number of elements. Show that the product of all of the elements of G must be the identity.**

3. **Suppose that G is a group with more than one element, and that G has no proper non-trivial subgroups. Prove that $|G|$ is prime. (Do not assume at the outset that $|G|$ is finite).**

4. **Show that in a group G of odd order, the equation $x^2 = a$ has a unique solution for all $a \in G$.**

1. **If $|G| = 91$, show that G has an element of order 7.**
   Hint 1: What are the only possible orders elements of G can have?

2. **Suppose that G is an Abelian group with an odd number of elements. Show that the product of all of the elements of G must be the identity.**

3. **Suppose that G is a group with more than one element, and that G has no proper non-trivial subgroups. Prove that $|G|$ is prime. (Do not assume at the outset that $|G|$ is finite).**

4. **Show that in a group G of odd order, the equation $x^2 = a$ has a unique solution for all $a \in G$.**

1. **If $|\mathbf{G}| = \mathbf{91}$, show that G has an element of order 7.**
   Hint 1: What are the only possible orders elements of G can have?
   Hint 2: If $a \in G$ and $|a| = 91$, can you find an element with order 7?

2. **Suppose that G is an Abelian group with an odd number of elements. Show that the product of all of the elements of G must be the identity.**

3. **Suppose that G is a group with more than one element, and that G has no proper non-trivial subgroups. Prove that $|G|$ is prime. (Do not assume at the outset that $|G|$ is finite).**

4. **Show that in a group G of odd order, the equation $x^2 = a$ has a unique solution for all $a \in G$.**

1. **If $|G| = 91$, show that G has an element of order 7.**
   Hint 1: What are the only possible orders elements of G can have?
   Hint 2: If $a \in G$ and $|a| = 91$, can you find an element with order 7?
   Hint 3: Is it possible for every non-identity element to have order 13?
2. **Suppose that G is an Abelian group with an odd number of elements. Show that the product of all of the elements of G must be the identity.**

3. **Suppose that G is a group with more than one element, and that G has no proper non-trivial subgroups. Prove that $|G|$ is prime. (Do not assume at the outset that $|G|$ is finite).**

4. **Show that in a group G of odd order, the equation $x^2 = a$ has a unique solution for all $a \in G$.**

1. **If $|\mathbf{G}| = 91$, show that G has an element of order 7.**
   Hint 1: What are the only possible orders elements of G can have?
   Hint 2: If $a \in G$ and $|a| = 91$, can you find an element with order 7?
   Hint 3: Is it possible for every non-identity element to have order 13?
2. **Suppose that G is an Abelian group with an odd number of elements. Show that the product of all of the elements of G must be the identity.**
   Hint 1: What does it mean for a number to be odd?
3. **Suppose that G is a group with more than one element, and that G has no proper non-trivial subgroups. Prove that $|G|$ is prime. (Do not assume at the outset that $|G|$ is finite).**
4. **Show that in a group G of odd order, the equation $x^2 = a$ has a unique solution for all $a \in G$.**

1. **If $|G| = 91$, show that G has an element of order 7.**
   Hint 1: What are the only possible orders elements of G can have?
   Hint 2: If $a \in G$ and $|a| = 91$, can you find an element with order 7?
   Hint 3: Is it possible for every non-identity element to have order 13?
2. **Suppose that G is an Abelian group with an odd number of elements. Show that the product of all of the elements of G must be the identity.**
   Hint 1: What does it mean for a number to be odd?
   Hint 2: Remember Lagrange's Thm and its corollaries
3. **Suppose that G is a group with more than one element, and that G has no proper non-trivial subgroups. Prove that $|G|$ is prime. (Do not assume at the outset that $|G|$ is finite).**
4. **Show that in a group G of odd order, the equation $x^2 = a$ has a unique solution for all $a \in G$.**

1. **If $|G| = 91$, show that G has an element of order 7.**
   Hint 1: What are the only possible orders elements of G can have?
   Hint 2: If $a \in G$ and $|a| = 91$, can you find an element with order 7?
   Hint 3: Is it possible for every non-identity element to have order 13?
2. **Suppose that G is an Abelian group with an odd number of elements. Show that the product of all of the elements of G must be the identity.**
   Hint 1: What does it mean for a number to be odd?
   Hint 2: Remember Lagrange's Thm and its corollaries
   Hint 3: What is distinctive about elements of order 2?
3. **Suppose that G is a group with more than one element, and that G has no proper non-trivial subgroups. Prove that $|G|$ is prime. (Do not assume at the outset that $|G|$ is finite).**

4. **Show that in a group G of odd order, the equation $x^2 = a$ has a unique solution for all $a \in G$.**

1. **If $|\mathbf{G}| = \mathbf{91}$, show that G has an element of order 7.**
   Hint 1: What are the only possible orders elements of G can have?
   Hint 2: If $a \in G$ and $|a| = 91$, can you find an element with order 7?
   Hint 3: Is it possible for every non-identity element to have order 13?
2. **Suppose that G is an Abelian group with an odd number of elements. Show that the product of all of the elements of G must be the identity.**
   Hint 1: What does it mean for a number to be odd?
   Hint 2: Remember Lagrange's Thm and its corollaries
   Hint 3: What is distinctive about elements of order 2?
3. **Suppose that G is a group with more than one element, and that G has no proper non-trivial subgroups. Prove that $|G|$ is prime. (Do not assume at the outset that $|G|$ is finite).**
   Hint 1: Break into cases - G is cyclic and G is not cyclic.

4. **Show that in a group G of odd order, the equation $x^2 = a$ has a unique solution for all $a \in G$.**

1. **If $|G| = 91$, show that G has an element of order 7.**
   Hint 1: What are the only possible orders elements of G can have?
   Hint 2: If $a \in G$ and $|a| = 91$, can you find an element with order 7?
   Hint 3: Is it possible for every non-identity element to have order 13?
2. **Suppose that G is an Abelian group with an odd number of elements. Show that the product of all of the elements of G must be the identity.**
   Hint 1: What does it mean for a number to be odd?
   Hint 2: Remember Lagrange's Thm and its corollaries
   Hint 3: What is distinctive about elements of order 2?
3. **Suppose that G is a group with more than one element, and that G has no proper non-trivial subgroups. Prove that $|G|$ is prime. (Do not assume at the outset that $|G|$ is finite).**
   Hint 1: Break into cases - G is cyclic and G is not cyclic.
   Hint 2: If G is not cyclic, what does $|G| > 1$ tell you?

4. **Show that in a group G of odd order, the equation $x^2 = a$ has a unique solution for all $a \in G$.**

1. **If $|G| = 91$, show that G has an element of order 7.**
   Hint 1: What are the only possible orders elements of G can have?
   Hint 2: If $a \in G$ and $|a| = 91$, can you find an element with order 7?
   Hint 3: Is it possible for every non-identity element to have order 13?
2. **Suppose that G is an Abelian group with an odd number of elements. Show that the product of all of the elements of G must be the identity.**
   Hint 1: What does it mean for a number to be odd?
   Hint 2: Remember Lagrange's Thm and its corollaries
   Hint 3: What is distinctive about elements of order 2?
3. **Suppose that G is a group with more than one element, and that G has no proper non-trivial subgroups. Prove that $|G|$ is prime. (Do not assume at the outset that $|G|$ is finite).**
   Hint 1: Break into cases - G is cyclic and G is not cyclic.
   Hint 2: If G is not cyclic, what does $|G| > 1$ tell you?
   Hint 3: If G is cyclic, what does it mean to have infinite order?
4. **Show that in a group G of odd order, the equation $x^2 = a$ has a unique solution for all $a \in G$.**

Solutions:

1. **If $|\mathbf{G}| = \mathbf{91}$, show that G has an element of order 7.**

   For all $a \in G$, $|a|$ divides 91 $\Longrightarrow |a| = 1$, 7, 13, or 91.

   If there is an $a \in G$ with $|a| = 91$, then a^{13} has order 7.

   Thus if G does *not* have *any* elements of order 7, every non-identity element must have order 13. Is this possible?

   Elements of order 13 come in chunks of 12: if $|a| = 13$, then $|a^2|, |a^3|, \ldots, |a^{12}| = 13$ also.

   There can be no overlap between two cyclic subgroups of order 13. That is, if $b \in G, |b| = 13, b \notin <a>$, then $b^k \notin <a>\ \forall 1 \leq k < 13$. For suppose $b^k \in <a>, b^k \neq e$. Then $<b^k> \subseteq <a>$. But $<b^k> = <b>$.

   Since 12 does not divide 90 (the number of non-identity elements), there must be some elements that are not of order 13. Thus there must be elements of order 7.

Solutions:

2. **Suppose that G is an Abelian group with an odd number of elements. Show that the product of all of the elements of G must be the identity.**
   $|G| = 2k + 1 \Rightarrow \exists$ even number of non-identity elements.

   $2 \not| |G| \Rightarrow \nexists$ element of order 2 by Corollary 2 to Lagrange's Theorem $\Rightarrow$ no element is its own inverse

   Let $a_1, a_2, \ldots, a_k$ be k distinct non-identity elements of G, non of which are inverses of each other.

   G Abelian $\Rightarrow$ we can write the product of the elements of G as

   $$e * a_1 * a_1^{-1} * a_2 * a_2^{-1} * \ldots a_k * a_k^{-1},$$

   and this product is clearly e.

Solutions:

3. **Suppose that G is a group with more than one element, and that G has no proper non-trivial subgroups. Prove that $|G|$ is prime. (Do not assume at the outset that $|G|$ is finite).**

   $|G| > 1 \Rightarrow a \neq e$.

Case 1: $G \neq < a >$.

Because $a \neq e$, $\{e\} \subset < a >$, and because $a \in G$ but $G \neq < a >$, we know $< a > \subset G$. Thus $< a >$ is a proper subgroup of G. $-\!\!\times\!\!-$

Case 2: $G = < a >$.

If $|G| = \infty$, then $|a| = \infty$, and so there does not exist $i \neq j$ such that $a^i = a^j$. Thus $a \notin < a^2 >$, and so $\{e\} \subset < a^2 > \subset < a > -\!\!\times\!\!-$.

Thus $|G| = n < \infty$.

If n is not prime, the FToCG $\Rightarrow$ there is one subgroup for each divisor. Thu n must be prime.

Solutions:

4. **Show that in a group G of odd order, the equation $x^2 = a$ has a unique solution for all $a \in G$.**
The equation $x^2 = a$ for some $a \in G$ would not have a unique solution if
   - there exists $g, h \in G$ such that $g^2 = h^2$.
   or
   - there is *no* $g \in G$ such that $g^2 = a$

   In other words, the equation $x^2 = a$ has a unique solution for all $a \in G \Leftrightarrow$ the mapping $\phi : G \to G$ is one-to-one and onto.

   From your last problem set, you know that ϕ is an automorphism of G if there is no element of order 2 in G.

   Since $|G|$ is odd, there *is* no element of order 2, and so ϕ *is* one-to-one and onto.