Theorem 4.1 Criterion for $a^i = a^j$.
Let G be a group, and let $a \in G$. If $|a| = \infty$, then all distinct powers of a are distinct elements. If a has finite order $n \in \mathbb{Z}^+$, then $\langle a \rangle = \{e, a^1, \ldots, a^{n-1}\}$ is a set of n distinct elements, and $a^i = a^j$ iff n divides $i - j$.

Proof.
Case $|a| = \infty$.
Suppose to the contrary that $a^i = a^j$ for distinct integers $i > j \in \mathbb{Z}$.
Then $a^{i-j} = e$, and the order of a is at most $i - j \in \mathbb{Z}^+$. (Contradiction)

Case $|a| = n \in \mathbb{Z}^+$.
We claim that the elements $\{e, a^1, \ldots, a^{n-1}\}$ are all distinct, and equal $\langle a \rangle$.

First, assume to the contrary that $e, a^1, \ldots, a^{n-1}$ are not all distinct.
Then $a^i = a^j$ for some i, j with $0 \leq j < i \leq n - 1$, to get
$0 < i - j < n$ and $a^{i-j} = e$, contradicting $|a| = n$.

Second, we show any $a^k \in \langle a \rangle$ is one of the elements $e, a^1, \ldots, a^{n-1}$.
Let $k \in \mathbb{Z}$ and write $k = qn + r$ with $q \in \mathbb{Z}$ and $0 \leq r < n$.
Then $a^k = a^{qn+r} = (a^n)^q a^r = a^r$, and therefore $\langle a \rangle = \{e, a^1, \ldots, a^{n-1}\}$.

Finally, we claim $a^i = a^j$ iff n divides $i - j$.
($\Rightarrow$) Let $i, j \in \mathbb{Z}$ and assume $a^i = a^j$.
Writing $i - j = nq + r$ with $q \in \mathbb{Z}$ and $0 \leq r < n$, we have
$e = a^{i-j} = a^{qn+r} = (a^n)^q a^r = a^r$.
But the order of a is $n > r$, and so r must be zero, and thus n divides $i - j$.

($\Leftarrow$) Let $i, j \in \mathbb{Z}$ and assume n divides $i - j$.
By definition of divides, $i - j = nq$ for some $q \in \mathbb{Z}$.
Then $a^{i-j} = a^{nq} = (a^n)^q = e$, and therefore $a^i = a^j$.

This completes the proof of the theorem. □

Theorem 4.2 $\langle a^k \rangle = \langle a^{\gcd(n,k)} \rangle$**.**
Let a be an element of order n in a group and let k be a positive integer.
Then $\langle a^k \rangle = \langle a^{\gcd(n,k)} \rangle$ and $|a^k| = n/\gcd(n,k)$.

Proof.
Claim 1: $\langle a^k \rangle = \langle a^{\gcd(n,k)} \rangle$.
For Claim 1, set $d = \gcd(n,k)$, and write $k = dr$ by definition of gcd.
We prove this by showing that each subgroup contains the cyclic generator of the other side.
($\subseteq$) We have $a^k = a^{dr} = (a^d)^r$, and so $a^k \in \langle a^{\gcd(n,k)} \rangle$.
($\supseteq$) By gcd as a linear combination (Thm. 0.2), write $d = ns + kt$ for some $s, t \in \mathbb{Z}$.
Then $a^d = a^{ns+kt} = (a^n)^s (a^k)^t = (a^k)^t \in \langle a^k \rangle$.
This proves Claim 1.

We now prove the second part of the conclusion with the following string of equations, where Claim 2 is deferred until below:

$$\begin{aligned} |a^k| &= |\langle a^k \rangle| && \text{by Corollary 1 of Theorem 4.1} \\ &= |\langle a^{\gcd(n,k)} \rangle| && \text{by Claim 1} \\ &= |a^{\gcd(n,k)}| && \text{by Corollary 1 of Theorem 4.1} \\ &= n/\gcd(n,k) && \text{by Claim 2.} \end{aligned}$$

Rather than proving $|a^{\gcd(n,k)}| = n/\gcd(n,k)$ for any $k \in \mathbb{Z}^+$, we prove the Claim 2 in a slightly more general setting.

Claim 2: For any divisor d of n, $|a^d| = n/d$.
Let d be a divisor of n, so that $n/d \in \mathbb{Z}^+$ since n is a positive integer.
Since $(a^d)^{n/d} = a^n = e$, the order of a^d is at most n/d.
Suppose to the contrary that $(a^d)^i = e$ for some $1 \leq i < n/d$.
Then $a^{di} = e$ for $1 \leq di < n$, contradicting $|a| = n$.
Therefore the order of a^d is at least n/d.
Combining $|a^d| \leq n/d$ and $|a^d| \geq n/d$ gives $|a^d| = n/d$, proving Claim 2.

This completes the proof of the theorem. □

Theorem 4.3 Fundamental Theorem of Cyclic Groups.
Every subgroup of a cyclic group is cyclic. Moreover, if $|\langle a\rangle| = n$, then the order of any subgroup of $\langle a\rangle$ is a divisor of n; and, for each positive divisor k of n, the group $\langle a\rangle$ has exactly one subgroup of order k—namely, $\langle a^{n/k}\rangle$.

Proof.

Claim 1. If H is a subgroup of $\langle a\rangle$ then H is cyclic.
Let H be a subgroup of $\langle a\rangle$.

Case 1. $H = \{e\}$
If $H = \{e\}$, then H is cyclic since $\{e\} = \langle e\rangle$.

Case 2. $H \neq \{e\}$
If $H \neq \{e\}$, we show that $H = \langle a^m\rangle$, where a^m is the smallest positive power of a in H.
Since $H \neq \{e\}$, H does in fact contain a^t for some nonzero $t \in \mathbb{Z}$.
By closure under inverses, H contains both a^t and a^{-t}.
One of these is a positive power, so the set of positive powers of a in H is nonempty.
By the Well-Ordering Principle, let m be the smallest such positive power with $a^m \in H$.

We now prove that $\langle a^m\rangle = H$:
($\subseteq$) By closure, $\langle a^m\rangle \subseteq H$.
($\supseteq$) Let $a^k \in H$, where k is some integer.
Using the division algorithm, write

$$k = mq + r \qquad \text{for } 0 \leq r < m.$$

Therefore

$$\begin{aligned} a^k &= a^{mq+r} = a^{mq}a^r, \qquad \text{or} \\ a^r &= a^k a^{-mq}. \end{aligned}$$

By closure of H, $a^r \in H$ since a^k and a^{-mq} are in H.
But m is the smallest positive power of a in H, and so $r = 0$.
Therefore $a^k = a^{mq}$ is in $\langle a^m\rangle$ by closure.

This proves $\langle a^m\rangle = H$ and completes the proof of Claim 1.

Theorem 4.2 $\langle a^k \rangle = \langle a^{\gcd(n,k)} \rangle$**.**
Let a be an element of order n in a group and let k be a positive integer. Then $\langle a^k \rangle = \langle a^{\gcd(n,k)} \rangle$ and $|a^k| = n/\gcd(n,k)$.

Theorem 4.3 Fundamental Theorem of Cyclic Groups.
Every subgroup of a cyclic group is cyclic. Moreover, if $|\langle a \rangle| = n$, then the order of any subgroup of $\langle a \rangle$ is a divisor of n; and, for each positive divisor k of n, the group $\langle a \rangle$ has exactly one subgroup of order k — namely, $\langle a^{n/k} \rangle$.

Claim 1. If H is a subgroup of $\langle a \rangle$ then H is cyclic.

Claim 2. If $|\langle a \rangle| = n$, then the order of any subgroup of $\langle a \rangle$ is a divisor of n.
Let H be a subgroup of $\langle a \rangle$.
Case 1. If $H = \{e\}$ the claim is true since $|H| = 1$ divides n.
Case 2. Otherwise, assume $H \neq \{e\}$.
By Claim 1, $H = \langle a^m \rangle$, where m is the smallest power of a in H.
Now use the division algorithm to write

$$n = mq + r \qquad \text{for } 0 \leq r < m.$$

Noting that $a^n = e$ is in H, we again have

$$\begin{aligned} n &= mq + r \qquad \text{for } 0 \leq r < m, \text{ or} \\ a^r &= a^n a^{-mq} \\ &= a^{-mq}, \end{aligned}$$

where $a^{-mq} \in H$ by closure since $a^m \in H$.
But m is the smallest positive power of a in H and so $r = 0$.
Therefore $n = mq$ and

$$\begin{aligned} |\langle a^m \rangle| &= n/\gcd(n,m) \qquad \text{by Theorem 4.2} \\ &= q \qquad \text{since } n = mq \text{ with } n, m \in \mathbb{Z}^+. \end{aligned}$$

Therefore $|H| = q$ which divides n.
This completes the proof of Claim 2.

Theorem 4.2 $\langle a^k \rangle = \langle a^{\gcd(n,k)} \rangle$**.**
Let a be an element of order n in a group and let k be a positive integer. Then $\langle a^k \rangle = \langle a^{\gcd(n,k)} \rangle$ and $|a^k| = n/\gcd(n,k)$.

Theorem 4.3 Fundamental Theorem of Cyclic Groups.
Every subgroup of a cyclic group is cyclic. Moreover, if $|\langle a \rangle| = n$, then the order of any subgroup of $\langle a \rangle$ is a divisor of n; and, for each positive divisor k of n, the group $\langle a \rangle$ has exactly one subgroup of order k — namely, $\langle a^{n/k} \rangle$.

Claim 1. If H is a subgroup of $\langle a \rangle$ then H is cyclic.

Claim 2. If $|\langle a \rangle| = n$, then the order of any subgroup of $\langle a \rangle$ is a divisor of n.

Claim 3. If $|\langle a \rangle| = n \in \mathbb{Z}^+$ and k is a positive divisor of n, then $\langle a^{n/k} \rangle$ is the one and only subgroup of $\langle a \rangle$ of order k.

Let k be a divisor of n. Then

$$\begin{aligned} |\langle a^{n/k} \rangle| &= n/\gcd(n, n/k) && \text{by Theorem 4.2} \\ &= n/(n/k) && \text{by Theorem 4.2} \\ &= k. \end{aligned}$$

Now let $H \leq \langle a \rangle$ and assume $|H| = k$.
From Claim 1 we know H is cyclic.
From Claim 2 and its proof, $H = \langle a^m \rangle$, where m is a divisor of n.
Then $m = \gcd(n, m)$ and

$$\begin{aligned} k &= |a^m| && \text{since } |a^m| = |\langle a^m \rangle| \\ &= |a^{\gcd(n,m)}| && \text{by Theorem 4.2} \\ &= n/\gcd(n,m) && \text{by Theorem 4.2} \\ &= n/m && \text{by Claim 2.} \end{aligned}$$

Therefore $m = n/k$ and $H = \langle a^{n/k} \rangle$.

This completes the proof of Claim 3.

This completes the proof of Theorem 4.3. □