6.1

$$n = 4(9) + 6 \implies r = 6, q = 4.$$

6.3

$$n = -7(8) + 6 \implies r = 6, q = -7.$$

6.5

$$\gcd(32, 24) = 8.$$

6.9

The number of generators a cylic group of order n has is the quantity of numbers m such that $1 \geq m < n$ and $\gcd(m, n) = 1$, or equivalently the number of coprime numbers to n that are less than n. Since $1, 3, 5,$ and 7 are the only numbers less than 8 that satisfy this property, the number of generators for a cyclic group of order 8 is 4.

6.13

The generators of a group must be preserved under an isomorphism. Therefore the number of automorphisms on $\mathbb{Z}_6$ is the number of isomorphic mappings that preserve the mapping of the generators of $\mathbb{Z}_6$. The generators of $\mathbb{Z}_6$ are $1, 5$, therefore there are 2 automorphisms on $\mathbb{Z}_6$.

6.17

$$|\langle 25 \rangle| = \frac{42}{\gcd(42, 25)} = \frac{42}{3} = 14.$$

6.24

$$\begin{aligned} \langle 1 \rangle &= \langle 3 \rangle = \langle 5 \rangle = \langle 7 \rangle = \mathbb{Z}_8 \\ \langle 2 \rangle &= \{0, 2, 4, 6\} \\ \langle 4 \rangle &= \{0, 4\}. \end{aligned}$$

$$\begin{tikzcd} \langle 1 \rangle \arrow[d, dash] \\ \langle 2 \rangle \arrow[d, dash] \\ \langle 4 \rangle \arrow[d, dash] \\ \langle 0 \rangle \end{tikzcd}$$

6.25

$$
\begin{aligned}
|\langle 1\rangle| &= |\langle 5\rangle| = |\mathbb{Z}_6| = 6\\
|\langle 2\rangle| &= |\langle 4\rangle| = |\{0,2,4\}| = 3\\
|\langle 3\rangle| &= |\{0,3\}| = 2.
\end{aligned}
$$

6.44

Lemma 0.1. If G and G' are groups with a homorphism $\phi : G \to G'$, then for all integers n and $a \in G$,

$$\phi(a^n) = \phi(a)^n.$$

Proof. Proceed with induction over $\mathbb{N}_0$. Let G and G' be groups with a homomorphism ϕ. Let $a \in G$. Consider the base case when $n = 0$. Then $\phi(a^0) = \phi(e) = e' = \phi(e)^0$. Therefore the base case holds. Assume for some fixed $n \in \mathbb{N}_0$ that $\phi(a^n) = \phi(a)^n$. Then

$$\phi(a^{n+1}) = \phi(a^n)\phi(a).$$

since ϕ is a homomorphism. By the induction hypothesis,

$$
\begin{aligned}
\phi(a^{n+1}) &= \phi(a^n)\phi(a)\\
&= \phi(a)^n\phi(a)\\
&= \phi(a)^{n+1}.
\end{aligned}
$$

Therefore if ϕ is a homorphism, $\phi(a^n) = \phi(a)^n$ for $n \in \mathbb{N}_0$. Note that

$$e' = \phi(aa^{-1}) = \phi(a)\phi(a^{-1}),$$

meaning that $\phi(a^{-1}) = \phi(a)^{-1}$. Therefore by a similar induction argument above, $\phi(a^n) = \phi(a)^n$ for all integers n. ■

Theorem 0.1. If G is a cyclic group with generator a and G' is a group isomorphic to G, for every $x \in G$, $\phi(x)$ is determined entirely by $\phi(a)$.

Proof. Let G be a cylic group with generator a and let G' be a group isomorphic to G. Let ϕ be the isomorphism between G and G'. Let $x \in G$. Since G is cylic, there is an $n \in \mathbb{Z}$ such that $x = a^n$. By Lemma 0.1, $\phi(x) = \phi(a^n) = \phi(a)^n$. Therefore for every element $x \in G$, there is some integer n such that $\phi(x) = \phi(a)^n$, hence $\phi(x)$ is determined entirely by $\phi(a)$. ■

6.46

Proof. Let G be a group and let $a, b \in G$. Assume that ab has finite order n. That is there exists $n \in \mathbb{Z}$ such that $(ab)^n = e$. Consider then

$$\begin{aligned} b(ab)^n a &= (ba)^{n+1} \\ bea &= (ba)^{n+1} \\ ba &= (ba)^{n+1} \\ (ba)^n &= e. \end{aligned}$$

Therefore ba has an order $\leq n$. Assume towards contradiction that $|ba| < n$. Let $s < n$ such that $|ba| = s$. Then

$$\begin{aligned} (ba)^s &= e \\ a(ba)^s b &= aeb \\ (ab)^{s+1} &= ab \\ (ab)^s &= e. \end{aligned}$$

Thus the order of ab is less than or equal to s and hence less than n. This is a contradiction and therefore the order of ba must also be n. ■

6.47

Part A

The least common multiple of r and s is the smallest positive integer generator for the group

$$r\mathbb{Z} \cap s\mathbb{Z}.$$

Part B

The condition in which the least common multiple of r and s is their product is when they share no divisors greater than 1, or equivalently r and s are coprime.

Part C

Proof. Let $d = ir + js$ be the gcd of r and s and $l = qr = ts$ be the least common multiple of r and s. Note that $ld = lir + ljs = tisr + qjsr = (ti + qj)sr$ meaning ld is a multiple of rs. Additionally there are integers a, b such that $r = ad$ and $s = bd$. Therefore $rs = abdd = (abd)d$. Since $abd = rb = sa$, abd is a multiple of both r and s, meaning $abd = lz$ for some integer z. Therefore $rs = lzd = (ld)z$, meaning rs is a multiple of ld. Since $rs|ld$ and $ld|rs$, $rs = ld$. ■

6.48

Proof. Let G be a group with a finite number of subgroups. Note that G can be expressed as the union of all its cylic subgroups because every element of G generates a cyclic subgroup containing g. Since G has finite subgroups, it has a finite number of cyclic subgroups. None of these cyclic subgroups can be infinite otherwise they would be isomorphic to $\mathbb{Z}$ which has an infinite number of subgroups. Therefore G has a finite amount of finite cyclic subgroups. Therefore G is the union of a finite set of finite subgroups, meaning G itself is also finite. ■

6.53

Proof. Let G be a cyclic group of order n. Let m be an integer such that $m|n$. Note that $G \simeq \mathbb{Z}_n$. Therefore solving $x^m = e$ is the same as solving $mx \equiv 0 \pmod{n}$ with $0 \leq x < n$. Note that $mx \equiv 0 \pmod{n}$ is the same as $mx = nq$ for $q \in \mathbb{Z}$. Hence $x = \frac{nq}{m}$. Additionally, since $x < n$, $\frac{nq}{m} < n$ meaning $q < m$. Therefore the solutions to $x^m = 0$ are of the form $x = \frac{nq}{m}$ where $q \in \{0, 1, 2, \ldots, m-1\}$. Therefore there are m solutions to $x^m = e$ when $m|n$. ■

6.54

Proof. Let G be a cyclic gorup of order n and let $m \in \mathbb{Z}$ with $1 < m < n$ and $m \nmid n$. Just like in 6.53, the problem of finding the solutions to $x^m = e$ is the same as solving for $mx \equiv 0 \pmod{n}$ with $0 \leq x < n$. Note that $0, \frac{n}{d}, \frac{2n}{d}, \ldots, \frac{(m-1)n}{d}$ are all solutions. Assume towards contradiction that there is a solution r that isnt enumerated above. Since $mr \equiv 0 \pmod{n}$, $mr = nq$ for some integer q, meaning $r = \frac{nq}{m}$. Let $m = xd$ and $n = yd$ where $d = \gcd(m, n)$ and $x, y \in \mathbb{Z}$. Then

$$r = \frac{ydq}{xd} = \frac{yq}{x}.$$

Since x and y are coprime, x must divide q. Therefore there is an integer s such that $q = xs$. Then

$$r = \frac{yq}{x} = \frac{yxs}{x} = ys = \frac{ns}{d}.$$

Since $r < n$, $s < d$ meaning s takes on a value between 0 and $d - 1$. However, this means r is one of the enumereated solutions from the beginning. Therefore there are d solutions. ■

6.55

Proof. Let p be a prime and consider $\mathbb{Z}_p$. Since p is prime, every integer less than p is coprime. Therefore every integer less than p and greater than 0 generates $\mathbb{Z}_p$. Therefore the only subgroups are $\mathbb{Z}_p$ and the trivial group, hence $\mathbb{Z}_p$ has no proper non-trivial subgroups. ■

6.56

Part A

Proof. Let G be an abelian group and let $H \leq G$ and $K \leq G$ be cyclic with coprime orders r and s respectively. Let a be the generator of H and b be the generator of K. Note that since G is abelian that $(ab)^{rs} = a^{rs}b^{rs} = (a^r)^s(b^s)^r = e$. Assume towards contradiction that there is some $n \in \mathbb{Z}$ less than rs such that $(ab)^n = e$. This implies that $a^n = b^{-n}$. Let $x = a^n = b^{-n}$. Note that $x \in H$ and $x \in K$. Therefore x produces a subgroup of H with an order dividing r and a subgroup of K with an order dividing s. Since r and s are coprime, $x = e$ so that $|\langle x \rangle| = 1 = \gcd(r, s)$. Therefore $a^n = b^n = e$. However in this case n is divisible by both r and s, meaning $n = rs$. This contradicts the assumption that $n < rs$, hence rs is the smallest positive integer such that $(ab)^{rs} = e$. Therefore ab generates a cyclic subgroup of G with order rs. ■

Part B

Proof. Let G be an abelian group and let $H \leq G$ and $K \leq G$ be cyclic with orders r and s respectively. Let a be the generator of H and b be the generator of K. Let $d = \gcd(r, s)$ and $s = dq$ where $\gcd(q, r) = 1$. Then $rq = \frac{rs}{d}$ is the least common multiple of r and s. Note that $|\langle a \rangle| = r$ and $|\langle b^d \rangle| = q$. Part (A) states then that ab^d generates a cyclic subgroup of $rq = \mathrm{lcm}(r, s)$. ■