Section 2.2, problem 16. (a) Let G be a cyclic group of order 6. How many of its elements generate G?

(b) Answer the same question for cyclic groups of order 5, 8, and 10.

(c) How many elements of a cyclic group of order n are generators for that group?

Solution 1. We will first prove the general fact that all elements of order k in a cyclic group of order n, where k and n are relatively prime, generate the group. This implies that if n is prime, the $n-1$ elements other than the identity generate the group.

First, notice that elements of the form x^p where p and n are not relatively prime cannot generate the group. To see this, let

$$p = ak, n = bk$$

where $a < b$ and $1 < k \in \mathbf{Z}$. Then the largest possible order of x^p would be b, since

$$x^{pb} = x^{bak} = (x^{bk})^a = (x^n)^a = 1^a = 1.$$

However, $b < n = bk$, so the order of $x^p < n$, so x^p cannot be a generator.

Now notice that an element of the form x^q where q and n are relatively prime has order n. To see this, note that we only have to show that x^q has order at least n, since it clearly has order at most n. Assume x^q is of order j, where $j < n$. Then

$$(x^q)^j = x^{qj} \quad \text{implying that } qj = ln \text{ for some } l \in \mathbf{Z}.$$

However, since n doesn't divide q, n must divide j, which is impossible since $j < n$.

Therefore x^q has order n, and its n powers are distinct (see page 47 in Artin), so x^q must generate the group.

Now we can easily see that in a cyclic group of order 5, x, x^2, x^3, and x^4 generate this group. In a cyclic group of order 6, x and x^5 generate the group. In a cyclic group of order 8, x, x^3, x^5, and x^7 generate the group. In a cyclic group of order 10, x, x^3, x^7, and x^9 generate the group.

Section 2.2, problem 16. (a) Let G be a cyclic group of order 6. How many of its elements generate G?

(b) Answer the same question for cyclic groups of order 5, 8, and 10.

(c) How many elements of a cyclic group of order n are generators for that group?

Solution 2. a.

$G = \{1, a, a^2, a^3, a^4, a^5 \mid a^6 = 1\}$.

a and a^5 generate G

a^2 doesn't generate G because $(a^2)^4 = a^2$

a^3 doesn't generate G because $(a^3)^3 = a^3$

a^4 doesn't generate G because $(a^4)^4 = a^4$

Since in these cases $x^n = x$ and $x < 6$, they don't generate G.

b.

$G = C_5$

a, a^2, a^3, a^4 generate G.

$G = C_8$

a, a^3, a^5, a^7 generate G.

$G = C_{10}$

a, a^3, a^7, a^9 generate G.

c.

Let $a^q \in C_n$

a^q is a generator of C_n if and only if q and n are relatively prime.

Proof that a^q is a generator then q and n must be relatively prime:

Assume that q and n aren't relatively prime. This means that they have a common factor that I will call k. Therefore $q = kx$, and $n = ky$ for some integers x and y. This means that $a^{qy} = a^{kxy} = a^{xky} = a^{xn} = a^{nx} = 1^x = 1$. Therefore the order of a is y which is defined to be less than n which means that a isn't a generator. Therefore if a^q is a generator then q and n are relatively prime.

Proof if q and n are relatively prime, then a^q is a generator:

I need to show that if $(a^q)^r = 1$, then $r = xn$ for some integer x. I know qr must be a multiple of n for $a^{qr} = 1$ because if $qr \neq xn$ then $a^{rq} \neq 1$. Therefore qr must equal some xn. Since q and n are relatively prime, the first point that qr could equal xn is if $r = n$ and $x = q$. This shows that a^q has order n. Therefore a^q is a generator if q and n are relatively prime.

Therefore a^q is a generator if and only if q and n are relatively prime.

Section 2.2, problem 16. (a) Let G be a cyclic group of order 6. How many of its elements generate G?

(b) Answer the same question for cyclic groups of order 5, 8, and 10.

(c) How many elements of a cyclic group of order n are generators for that group?

Solution 3. (a) G has two elements that generate G. These two elements are x and x^5. Refer to part c for a proof of this.

(b) C_5 has four generators. These are x, x^2, x^3, and x^4.
C_8 has four generators. These are x, x^3, x^5, and x^7.
C_{10} has four generators. These are x, x^3, x^7, and x^9.
Refer to part c for a proof that these and only these are generators.

(c) Let $C_n = \{1, x, \ldots, x^{n-1} \mid x^n = 1\}$.

Claim: x^i generates C_n iff i is mutually prime to n.

Proof: If i is mutually prime to n, $mi \neq n$ for some $1 < m \in \mathbf{Z} < n$. This implies $x^{ni} = \underbrace{x^i \ldots x^i}_{n} = 1$, but there is not a $x^{mi} = 1$. This gives order of $|x^i| = n$ and thus that x^i generates C_n.

If i is not mutually prime to n, $mi = n$ for some $1 < m \in \mathbf{Z} < n$. This implies $x^{mi} = x^{ni} = 1$. This gives order $|x^i| = m < n$ and thus x^i cannot generate C_n, it generates C_m.

Therefore x^i generates C_n iff i is mutually prime to n.

Section 2.2, problem 16. (a) Let G be a cyclic group of order 6. How many of its elements generate G?

(b) Answer the same question for cyclic groups of order 5, 8, and 10.

(c) How many elements of a cyclic group of order n are generators for that group?

Solution 4. (a) Let $G = C_6$ be the cyclic group of order 6. Then $G = \{1, x, x^2, x^3, x^4, x^5 \mid x^6 = 1\}$ and we can examine the order of each element of G. Since the elements of G themselves generate cyclic subgroups, this will tell use which elements generate G. Let $\langle g \rangle$ denote the group generated by the element $g \in G$. Then $\langle g \rangle = G$ if and only if $|\langle g \rangle| = |G| = 6$. The order of the elements of G are as follows

$$\begin{aligned} |\langle 1 \rangle| &= 1 \\ |\langle x \rangle| &= 6 \\ |\langle x^2 \rangle| &= 3 \\ |\langle x^3 \rangle| &= 2 \\ |\langle x^4 \rangle| &= 3 \\ |\langle x^5 \rangle| &= 6. \end{aligned}$$

Therefore there are only two elements of G which generate G. As described above, they are precisely the elements of order 6. Here x and x^5 are the two elements which generate G.

(b) As before, one could write out the order of each element in the cyclic groups C_5, C_8, and C_{10} in order to see which ones generate their group. However, this would be a time consuming and rather mindless activity. How then can one get a better understanding of this problem? One way is to consider the group C_5. Every element of C_5 has order 5 and therefore generates C_5. So then, what is special about C_5? Notice that 5 is prime and that therefore all exponents of the elements of C_5 are relatively prime to 5. This suggests a good way of checking whether or not an element generates the whole group. In fact, if we look back at part a), then we would see that the two elements which generate C_6 have nonzero exponents relatively prime to 6. Indeed, as we will see in part c), this test suffices to determine the generators of a cyclic group. Thus, assuming this test is valid, we will find the generators of C_5, C_8, and C_{10}.

As noted before, all elements of C_5 (except for the identity element) generate C_5. Consider $C_8 = \{1, x, x^2, x^3, x^4, x^5, x^6, x^7 \mid x^8 = 1\}$, then the set of generators are those elements which have exponent relatively prime to 8. Mainly, any element in the set $\{x, x^3, x^5, x^7\}$ will generate C_8. Similarly, C_{10} is generated by any of the elements of the set $\{x, x^3, x^7, x^9\}$ will generate C_{10}.

See part c for a proof of our claim.

(c) Let $G = \{1, x, x^2, \ldots, x^{n-1} \mid x^n = 1\}$ be the cyclic group of order n and let a be an element of G. Then the exponent of a is less than n and greater than or equal to 0:

$$a = x^j \quad 0 \leq j < n.$$

As promised, we claim that the elements which generate G are those who's exponent is relatively prime to n. This can be seen as follows.

If j divides n, then $(x^j)^m = x^n$ where $m = \frac{n}{j}$. In this case $m < n$ and m represents the m elements of G that x^i generates. Since $1 = x^n = (x^j)^m$, if we multiply by x^j we will have

$$x^j(x^j)^m = x^j \cdot 1 = x^j.$$

This says that we will keep repeating the same m powers of x^j. Now suppose one of the factors of j divides n. Then we can write

$$x^{cd} = x^j$$

where $cd = j$. Thus j is a multiple of c. But we have already seen that if c divides n, then x^c does not generate C_n. Consequently x^{cd} cannot generate C_n.

All other elements generate C_n. We can see this by letting x^k be such that k does not divide n nor do any of its factors (k is relatively prime to n). In this case we have

$$\frac{\text{lcm}(k,n)}{k} = n$$

where lcm denotes the least common multiple of k and n. This says precisely that we are able to create all n elements of G with the powers of x^k.