

Dr. H. Joseph Straight
SUNY Fredonia
Smokin' Joe's Catalog of Groups: Cyclic Groups

Let $(G, *)$ be a group with identity e . Given $a \in G$ and a positive integer n , we define the *powers of a* recursively as follows:

$$\begin{aligned}a^0 &= e \\a^1 &= a \\a^n &= a * a^{n-1}\end{aligned}$$

If G is a finite group, then the list

$$e = a^0, \quad a = a^1, \quad a^2, \quad a^3, \quad \dots$$

must contain repeated elements. In fact, it is not difficult to show that the first element to repeat is e . The smallest positive integer n such that $a^n = e$ is called the **order of a** and is denoted by $|a|$. Note that e has order 1 and any nonidentity element of G has order at least 2.

If $a \in G$ has order $n > 1$, then the elements

$$e = a^0, \quad a = a^1, \quad \dots, \quad a^{n-1}$$

are n distinct elements of G , and these elements form a subgroup of G , called the **cyclic subgroup of G generated by a** , and denoted by $\langle a \rangle$. Note that, for $1 \leq s, t < n$,

$$(a^t)^{-1} = a^{n-t} \quad \text{and} \quad a^s * a^t = a^{s+t} = a^{(s+t) \bmod n}$$

If $G = \langle a \rangle$ for some element $a \in G$, then G is said to be a **cyclic group**, and a is called a **generator** for G .

Henceforth, unless stated otherwise, we shall think of the operation in an abstract group as “multiplication,” and shall denote products using juxtaposition. For example, we'll denote the product $a * b$ as simply ab .

Let $(G, *)$ be a group. The cardinality of G is termed the **order of the group**, and is denoted by $|G, *|$, or more simply by $|G|$ (the same way that the cardinality of G is usually denoted) when the group operation is understood. Thus, for example, if $G = \{e, a, b, c\}$, then we say that the group $(G, *)$ has order 4, and we write $|G| = 4$. Of course, it is possible for a group to have infinite order, as is the case for $(\mathbb{Z}, +)$ and the general linear group of invertible 2 by 2 matrices over \mathbb{R} under multiplication.

Warning to students: Don't confuse “order of a group” and “order of an element.” The order of a group is simply the number of elements it contains. The order of an element in a finite group is the smallest positive power of that element that yields the identity element of the group. Of course, if the group is finite and cyclic, then the order of the group is equal to the order of any generator for the group.

Any group of order at most 3 is cyclic. For example, let $G = \{e, a, b\}$ be a group of order 3 with identity element e . Then we have the following partial operation table for G :

	e	a	b
e	e	a	b
a	a		
b	b		

Consider the element ab . To determine this element, we employ the following result.

Result 1: In the operation table for a finite group, each element of the group appears exactly once in any row or in any column.



I like to call this the “Sudoku theorem,” since it says that the operation table for a finite group is similar to the solution to a Sudoku puzzle.

Back to the product ab , note that $ab \neq a$ (since we already have $ae = a$) and $ab \neq b$ (since we already have $eb = b$). It follows that $ab = e$; that is, a and b are inverses of each other. We can then further apply the key result to obtain that $aa = b$, $ba = e$, and $bb = a$. Thus, there is a unique abstract group of order 3, with operation table

	e	a	b
e	e	a	b
a	a	b	e
b	b	e	a

This group is cyclic, and both a and b are generators for it, since

$$a^0 = e, \quad a^1 = a, \quad a^2 = b \quad \text{and} \quad b^0 = e, \quad b^1 = b, \quad b^2 = a$$

What about groups of order 4? Is every group of order 4 a cyclic group?

If $G = \{e, a, b, c\}$ has order 4, then we have the following partial operation table:

	e	a	b	c
e	e	a	b	c
a	a			
b	b			
c	c			

Now then, if G is a group with identity e , then the function $r : G \rightarrow G$ defined by

$$r(x) = x^{-1}$$

is a permutation of G . That is, each element of G has an inverse, and no two distinct elements of G have the same inverse. Also, $r(e) = e$. Therefore, r is a permutation of $G - \{e\}$.

Let's apply this fact to the problem of finding the abstract groups of order 4. Given the partial operation table above, there are two cases to consider:

Case 1: $a^{-1} = c$ and $b^{-1} = b$ (that is, exactly one nonidentity element is its own inverse and, without loss of generality, we may assume that element is b).

Case 2: $a^{-1} = a$, $b^{-1} = b$, and $c^{-1} = c$ (that is, each nonidentity element is its own inverse).

In Case 1, the operation table for G looks like this:

	e	a	b	c
e	e	a	b	c
a	a			e
b	b		e	
c	c	e		

Using the Sudoku theorem, we have $ab = c$, and then we may continue to apply this result to complete the operation table. Therefore, in Case 1, the operation table for G is

	e	a	b	c
e	e	a	b	c
a	a	b	c	e
b	b	c	e	a
c	c	e	a	b

In this group cyclic? Yes, and a is a generator:

$$a^0 = e, \quad a^1 = a, \quad a^2 = b, \quad a^3 = a(a^2) = ab = c$$

Note that b is also a generator.

In Case 2, the operation table for G looks like this:

	e	a	b	c
e	e	a	b	c
a	a	e		
b	b		e	
c	c			e

Again, we apply the Sudoku theorem to deduce the following:

$$ab = c, \quad ac = b, \quad bc = a, \quad ba = c, \quad ca = b, \quad cb = a$$

Therefore, in Case 2, the operation table for G is

	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

This group is not a cyclic group. In fact, each nonidentity element has order 2. This group is called the **Klein four-group**, and will be denoted by K .

In general, we denote the abstract cyclic group of order n by C_n . If the element a is a generator for the group and e is the identity element, then the elements of C_n are

$$a^0 = e, \quad a^1 = a, \quad a^2, \quad \dots, \quad a^{n-1}$$

Since every element of a cyclic group is a power of the generator, and powers of the same element commute with each other, we can say that any cyclic group is an abelian group.

Next, we describe a way to “picture” a group as a labeled directed graph, called a **Cayley digraph** for the group.

Take C_4 , for example. Its Cayley digraph has four nodes, one for each element of the group. That is, the nodes are e , a , b , and c . Next, we need a generator for the group (or a generating set); let's use the generator a . Then, given nodes x and y , the Cayley digraph has a directed edge or arc from x to y , labeled a , provided $x * a = y$. This yields the Cayley digraph shown in Figure 1.

For this Cayley digraph, we don't need to explicitly label the arcs with the generator a — since there is an arc from node e to node a , we know that each arc represents multiplication on the right by a . For example, since there is an arc from b to c , the digraph tells us that $b * a = c$, and since there is an arc from c to e , the digraph tells us that $c * a = e$.

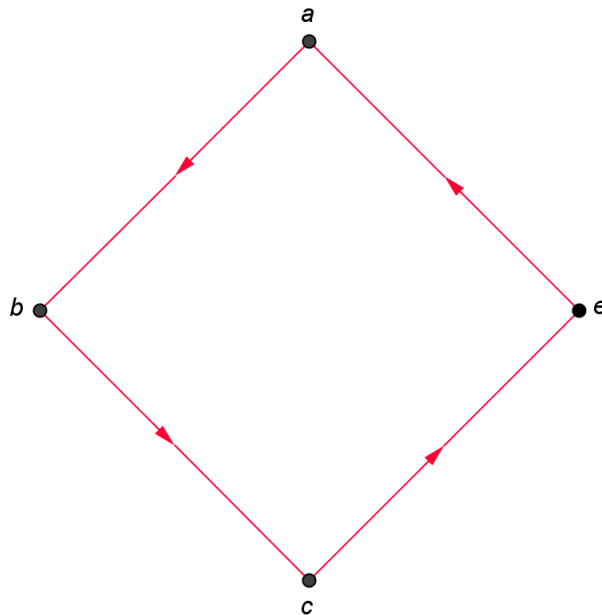


Figure 1 Cayley digraph for C_4 using generating set $\{a\}$

What about a Cayley digraph for the Klein four-group K ? This group does not have a single generator, since $a^2 = b^2 = c^2 = e$. Thus, we need at least two elements to generate K .

We claim that $\{a, b\}$ is a generating set; that is, that every element of K can be written as a product involving only a and b . To see this, note that

$$a^1 = a, \quad a^2 = e, \quad b^1 = b, \quad \text{and} \quad ab = c$$

Thus, the Cayley digraph for K using generating set $\{a, b\}$ has four nodes — $e, a, b,$ and c — and arcs labeled a and b . An arc from node x to node y is labeled a (b) provided $xa = y$ ($xb = y$).

Alternately, we can use different edge types, and/or colors, for the arcs labeled a and b . Let's use a solid arc, colored red, for any arc labeled a , and a dashed arc, colored blue, for any arc labeled b . The result is shown in Figure 2.

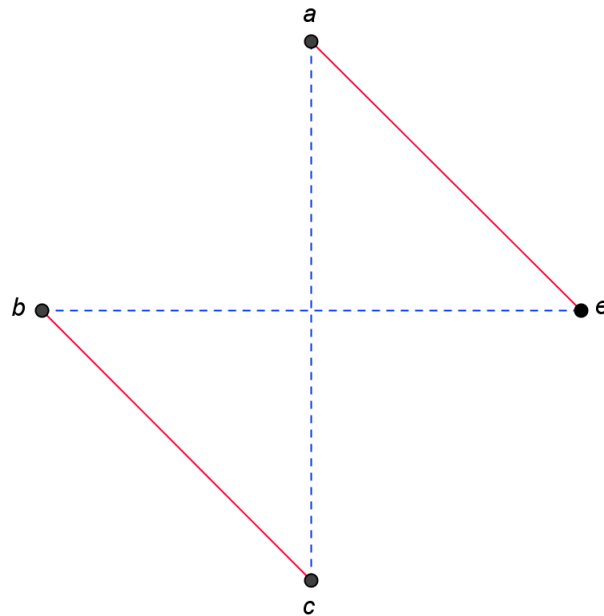


Figure 2 Cayley digraph for the Klein four-group K using generating set $\{a, b\}$

In the Cayley digraph for K shown in Figure 2, we have made a further simplification: since $a^2 = e = b^2$, if $xa = y$, then $ya = x$, and if $xb = y$, then $yb = x$. Thus, rather than having a pair of symmetric arcs between x and y labeled a (b), we use instead a single undirected edge labeled a (b).

Next, we wish to determine the abstract groups of order 5. Let $G = \{e, a, b, c, d\}$ be a group order 5, and assume, as usual, that e is the identity element. Analyzing the situation for inverses, we see that there are three cases to consider:

Case 1: $a^{-1} = a$, $b^{-1} = b$, $c^{-1} = c$, and $d^{-1} = d$. In this case we have the following partial operation table:

	e	a	b	c	d
e	e	a	b	c	d
a	a	e			
b	b		e		
c	c			e	
d	d				e

Case 2: $a^{-1} = a$, $b^{-1} = b$, and $c^{-1} = d$ (that is, exactly two nonidentity elements are their own inverses). In this case, we have the following partial operation table:

	e	a	b	c	d
e	e	a	b	c	d
a	a	e			
b	b		e		
c	c				e
d	d			e	

Case 3: $a^{-1} = d$ and $b^{-1} = c$ (that is, no nonidentity element is its own inverse). In this case, we have the following partial operation table:

	e	a	b	c	d
e	e	a	b	c	d
a	a				e
b	b			e	
c	c		e		
d	d	e			

Exercise: Show that, in both Case 1 and Case 2, if we assume that the operation table is the operation table for a group of order 5, then we obtain a contradiction..

(a) In Case 1, if we assume $(G, *)$ is a group, then we may assume, without loss of generality, that $ab = c$. Apply the Sudoku theorem to obtain the following operation table:

	e	a	b	c	d
e	e	a	b	c	d
a	a	e	c	d	b
b	b	d	e	a	c
c	c	b	d	e	a
d	d	c	a	b	e

However, give an example to show that associative property fails to hold in the algebraic structure with this operation table. This yields a contradiction.

(b) In Case 2, if we assume that $(G, *)$ is a group, then we may again assume, without loss of generality, that $ab = c$. However, show that there is no way to complete the operation table consistent with the Sudoku theorem. ■

We have shown above that, if $G = \{e, a, b, c, d\}$ is a group with identity e , then G has the following partial operation table:

	e	a	b	c	d
e	e	a	b	c	d
a	a				e
b	b			e	
c	c		e		
d	d	e			

We may assume, without loss of generality, that $a^2 = b$ or $a^2 = d$. However, if $a^2 = d$, then there is no way to complete the operation table consistent with the Sudoku theorem.

Therefore, $a^2 = b$, and it follows from the Sudoku theorem that the operation table for G is

	e	a	b	c	d
e	e	a	b	c	d
a	a	b	c	d	e
b	b	c	d	e	a
c	c	d	e	a	b
d	d	e	a	b	c

Exercise: Show that the algebraic structure G with the operation table above is cyclic. It follows that the associative property holds, and hence G is a cyclic group. ■

In conclusion, there is a unique abstract group of order 5, namely, C_5 . Its Cayley digraph (using generator a) is shown in Figure 3.

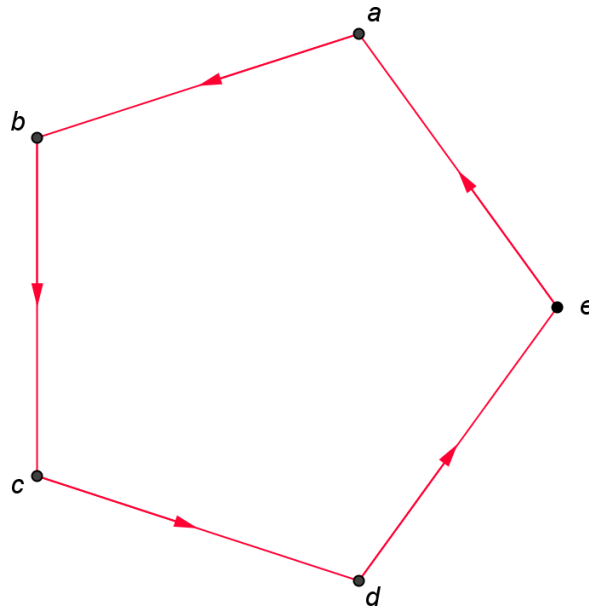


Figure 3 Cayley digraph for C_5 using generating set $\{a\}$

Next, we consider some concrete examples of cyclic groups.

Example 1: Given an integer $n > 1$, let \mathbb{Z}_n denote the *set of integers modulo n* :

$$\mathbb{Z}_n = \{0, 1, \dots, n - 1\}$$

This terminology comes from the fact that the integers between 0 and $n - 1$, inclusive, are the possible remainders that may be obtained when an integer m is divided by n .

Recall that the remainder operation is denoted by *mod*. Given an integer m , there exist, by the division algorithm, unique integers q and r such that

$$m = nq + r \quad \text{and} \quad 0 \leq r < n$$

In this context, m is called the *dividend*, n is called the *divisor*, q is called the *quotient*, and r is called the *remainder*. We write

$$r = m \bmod n$$

We define the binary operation of *addition modulo n* , denoted \oplus , on \mathbb{Z}_n as follows: for $x, y \in \mathbb{Z}_n$,

$$x \oplus y = (x + y) \bmod n$$

Exercise: Complete the following “addition table” for (\mathbb{Z}_7, \oplus) :

\oplus	0	1	2	3	4	5	6
0	0	1	2	3	4	5	6
1	1	2	3	4	5	6	0
2	2	3	4	5	6	0	1
3	3	4	5				
4	4	5	6				
5	5	6	0				
6	6	0	1				

In general, it can be shown that \oplus is an associative operation on \mathbb{Z}_n . Note that \oplus is also a *commutative* operation, since

$$x \oplus y = (x + y) \bmod n = (y + x) \bmod n = y \oplus x$$

for all elements x and y . Moreover, it is clear that 0 is the identity for \oplus , and for $x \in \mathbb{Z}_n$, $x \neq 0$, the (additive) inverse of x is $n - x$. Therefore, (\mathbb{Z}_n, \oplus) is an abelian group of order n , called the **group of integers modulo n** .

Also, \mathbb{Z}_n is a cyclic group, and 1 is a generator, since

$$1^1 = 1, \quad 1^2 = 1 \oplus 1 = 2, \quad 1^3 = 1 \oplus 1^2 = 1 \oplus 2 = 3, \quad \dots, \quad 1^n = 0$$

Here, keep in mind that the operation is “addition modulo n ,” and hence, for $x \in \mathbb{Z}_n$ and for a positive integer k ,

$$x^k = x \oplus x \oplus \dots \oplus x \quad (k \text{ terms})$$



Example 2: We define the binary operation of *multiplication modulo n* , denoted \odot , on \mathbb{Z}_n as follows: for $x, y \in \mathbb{Z}_n$,

$$x \odot y = (xy) \bmod n$$

Note that, for any $x \in \mathbb{Z}_n$,

$$x \odot 1 = x = 1 \odot x$$

Thus, 1 is the identity for \odot . As with \oplus , it can be shown that \odot is an associative operation on \mathbb{Z}_n . It is also commutative, since

$$x \odot y = (xy) \bmod n = (yx) \bmod n = y \odot x$$

For any $x \in \mathbb{Z}_n$,

$$x \odot 0 = 0 = 0 \odot x$$

Thus, 0 does not have an inverse under \odot . So, if we want to have a group we must exclude 0 from the set of elements under consideration. Let

$$\mathbb{Z}_n^\# = \mathbb{Z}_n - \{0\} = \{1, 2, \dots, n - 1\}$$

Exercise: Complete the following “multiplication table” for $(\mathbb{Z}_7^\#, \odot)$ and verify that it is a group.

\odot	1	2	3	4	5	6
1	1	2	3	4	5	6
2	2	4	6	1	3	5
3	3	6				
4	4	1				
5	5	3				
6	6	5				

Having indicated the properties satisfied by \oplus and \odot , let's agree to denote these operations more simply using the familiar operand symbols: “+” for addition modulo n , and “ \cdot ” for multiplication modulo n . We rely on the context in which these symbols appear to determine their meaning. Thus, for instance, $7 + 11 = 18$ if + denotes addition in \mathbb{Z} or addition modulo 23, but $7 + 11 = 5$ if + denotes addition modulo 13.

In general, we define

$$U_n = \{x \in \mathbb{Z}_n^\# \mid x \text{ has a multiplicative inverse}\}$$

Thus (U_n, \odot) is an abelian group. We have the following basic results about this group..

Lemma 2: Let n be an integer, $n > 2$, and let $x \in \mathbb{Z}_n^\#$. If $xy = 0$ for some $y \in \mathbb{Z}_n^\#$, then $x \notin U_n$.

Proof: Let n be an integer, $n > 2$, let $x \in \mathbb{Z}_n^\#$, and assume $xy = 0$ for some $y \in \mathbb{Z}_n^\#$. Suppose, to the contrary, that x' is the multiplicative inverse of x in $\mathbb{Z}_n^\#$. Then

$$y = (1)y = (x'x)y = x'(xy) = x'(0) = 0$$

This is a contradiction, since $y \in \mathbb{Z}_n^\#$, and so the result is established. ■

Theorem 3: Let n be an integer, $n > 2$, and let $x \in \mathbb{Z}_n^\#$. Then $x \in U_n$ if and only if $\gcd(x, n) = 1$.

Proof: Let n be an integer, $n > 2$, and let $x \in \mathbb{Z}_n^\#$.

To show sufficiency, assume $\gcd(x, n) = 1$. Then there exist integers s and t such that

$$xs + nt = 1$$

that is, 1 and the integer xs differ by a multiple of n . It follows that

$$(xs) \bmod n = 1 \bmod n = 1$$

Thus, $x^{-1} = s \bmod n$, and it follows that $x \in U_n$.

Conversely, for necessity, assume $\gcd(x, n) = d > 1$, let $y = n/d$, and let $m = \text{lcm}(x, n)$. Then

$$xy = x \left(\frac{n}{d} \right) = \frac{xn}{d} \bmod n = m \bmod n = 0$$

It follows from the lemma that $x \notin U_n$. ■

Corollary 4: For any prime p , $(\mathbb{Z}_p^\#, \odot)$ is an abelian group. ■

Note that, if p is prime, then $\mathbb{Z}_p^\# = U_p$. What about the group (U_n, \cdot) in general? First of all, what is the order of this group? We see that the order of the group U_n is the cardinality of the set

$$\{x \mid x < n \text{ and } \gcd(x, n) = 1\}$$

This is the famous *Euler phi function*, $\phi(n)$. Usually, ϕ is considered to be a function on the set \mathbb{Z}^+ of positive integers, with $\phi(1)$ defined to be 1.

It is not difficult to determine that, for any prime p and any positive integer k ,

$$\phi(p^k) = p^k - p^{k-1} = p^{k-1}(p - 1)$$

This is because the only integers less than or equal to p^k and not relatively prime to p^k are the multiples of p , namely,

$$p, \quad 2p, \quad \dots, \quad p^{k-1}p$$

In particular, for any prime p , $\phi(p) = p - 1$, and, for any positive integer k ,

$$\phi(2^k) = 2^{k-1}$$

In addition, it is not difficult to show that ϕ is *multiplicative* — that is, if n_1 and n_2 are positive integers and $\gcd(n_1, n_2) = 1$, then

$$\phi(n_1 n_2) = \phi(n_1) \phi(n_2)$$

The two facts noted above allow $\phi(n)$ to be computed for any positive integer n , provided one has the canonical factorization of n . For example:

$$\begin{aligned} \phi(360) &= \phi(2^3 \cdot 3^2 \cdot 5^1) \\ &= \phi(2^3) \cdot \phi(3^2) \cdot \phi(5) \\ &= (2^2) \cdot (3^1(3 - 1)) \cdot (4) \\ &= 2^5 \cdot 3^1 = 96 \end{aligned}$$

So, U_{360} is an abelian group of order 96 and, in general, U_n is an abelian group of order $\phi(n)$. Is it cyclic?

If U_n is cyclic and a is a generator for it, then $1 < a < n$ and the list of group elements

$$(a^1, a^2, \dots, a^{\phi(n)})$$

is a permutation of U_n . Such an a is called a *primitive root modulo n* .

Let's first consider the case when n is an odd prime p . In this case,

$$U_p = \mathbb{Z}_p^\# = \{1, 2, \dots, p-1\}$$

and $\phi(p) = p-1$. Let's try a few values of p and see if we can find a primitive root modulo p .

For $p = 3$, we have

$$2^1 = 2 \quad \text{and} \quad 2^2 = 1$$

so 2 is a primitive root modulo 3.

For $p = 5$, we have

$$2^1 = 2, \quad 2^2 = 4, \quad 2^3 = 3, \quad \text{and} \quad 2^4 = 1$$

so 2 is a primitive root modulo 5.

Perhaps 2 is always a primitive root modulo p . Let's try $p = 7$:

$$2^1 = 2, \quad 2^2 = 4, \quad 2^3 = 1, \quad 2^4 = 2, \quad 2^5 = 4, \quad \text{and} \quad 2^6 = 1$$

Thus, 2 is not a primitive root modulo 7. We know this as soon as we compute $2^3 = 1$, for at this point we know that $|2| = 3$, and the list of powers of 2 modulo 7 just keeps repeating the 3-cycle (2, 4, 1).

Is 3 a primitive root modulo 7? Let's see:

$$3^1 = 3, \quad 3^2 = 2, \quad 3^3 = 6, \quad 3^4 = 4, \quad 3^5 = 5, \quad \text{and} \quad 3^6 = 1$$

Yes! The number 3 is a primitive root modulo 7.

What about $p = 11$? Again, we try 2 first:

$$\begin{aligned} 2^1 = 2, \quad 2^2 = 4, \quad 2^3 = 8, \quad 2^4 = 5, \quad 2^5 = 10 \\ 2^6 = 9, \quad 2^7 = 7, \quad 2^8 = 3, \quad 2^9 = 6, \quad 2^{10} = 1 \end{aligned}$$

Thus, 2 is a primitive root modulo 11.

In the general case we have the following important result.

Theorem 5 (Gauss, 1801): For any odd prime p , there exists a primitive root modulo p ■

Unfortunately, no one knows a formula for finding primitive roots. Emil Artin conjectured that there are infinitely many primes for which 2 is a primitive root, but this conjecture remains unproved.

Next, let's consider the case when n is composite. The first numbers to investigate are $n = 4$ and $n = 6$. For $U_4 = \{1, 3\}$, 3 is the generator, whereas for $U_6 = \{1, 5\}$, 5 is the generator. Hence, 3 is the primitive root modulo 4 and 5 is the primitive root modulo 6.

Next, consider $n = 8$. Since $U_8 = \{1, 3, 5, 7\}$, the potential primitive roots modulo 8 are 3, 5, and 7. However, $3^2 = 1$, $5^2 = 1$, and $7^2 = 1$, so there are no primitive roots modulo 8. Therefore, the group U_8 is not cyclic. In fact, it can be shown that the group U_8 has the same structure as the Klein four-group K .

Exercise: In each part, find a primitive root for the given value of n , or show that no primitive root modulo n exists.

- | | |
|--------------|--------------|
| (a) $n = 9$ | (b) $n = 10$ |
| (c) $n = 12$ | (d) $n = 14$ |
| (e) $n = 15$ | (f) $n = 16$ |

■

For primitive roots in general, we have the following result.

Theorem 6: The number 2 is a primitive root modulo 3 and the number 3 is a primitive root modulo 4. For $n > 4$, there exists a primitive root modulo n if and only if $n = p^k$ or $n = 2 \cdot p^k$ for some odd prime p and some positive integer k .

■

Corollary 7: The groups U_3 and U_4 are cyclic. For $n > 4$, the group U_n is cyclic if and only if $n = p^k$ or $n = 2 \cdot p^k$ for some odd prime p and some positive integer k .

■

Given $x \in U_n$, we have an efficient method for finding x^{-1} . It is based on the *Euclidean algorithm*. We next present a recursive version of this method.

For $x \in U_n$, let y denote the inverse of x . If $x = 1$, then $y = 1$. Suppose $x > 1$. Let $r = n \bmod x$ with $n = xq + r$ (that is, q is the quotient when n is divided by x). Then, by the Euclidean algorithm, $\gcd(x, n) = \gcd(r, x) = 1$, so $r \in U_x$. Recursively, let $x' = r$ and $n' = x$, and suppose we can find y' , the inverse of x' in $U_{n'}$. Then

$$(x'y') \bmod n' = 1$$

(Here, $x'y'$ denotes the product of x' and y' in \mathbb{Z} .) Letting t' denote the quotient obtained when $x'y'$ is divided by n' , we have

$$x'y' - n't' = 1$$

Thus,

$$1 = x'y' - n't' = (n - xq)y' - xt' = ny' - x(qy' + t')$$

It follows that

$$-x(qy' + t') \bmod n = 1$$

and therefore,

$$y = -(qy' + t') \pmod n$$

Algorithm 1: Given $n \geq 2$, and $x \in U_n$, this algorithm finds the inverse y of x .

0. If $x = 1$, then $y = 1$.

1. Otherwise, let $r = n \pmod x$ and let q be such that $n = xq + r$. Let $x' = r$ and $n' = x$, and apply the algorithm recursively to find y' , the inverse of x' in $U_{n'}$. Also, let t' be the quotient obtained when $x'y'$ is divided by n' . Then

$$y = -(qy' + t') \pmod n \quad \clubsuit$$

■

Example 3: In U_{53} , find:

(a) 14^{-1}

(b) 20^{-1}

Solution: For part (a), our goal is to complete the following table:

n	x	q	r	t	y
53	14				

In particular, we want to obtain the value of $y = x^{-1}$ and place it in row 1 and column 6. Each time we apply the algorithm recursively — that is, each time we apply step 1 of the algorithm, we will add a row to the table.

To begin, since $x = 14$ and 14 is greater than 1, we apply step 1. So, we divide 53 by 14, obtaining a quotient of $q = 3$ and a remainder of $r = 11$. These values are placed in columns 3 and 4 of the table, respectively. To find the inverse of 14 in U_{53} , the algorithm says that we must first find the inverse of 11 in U_{14} . Thus, we add a second row to our table for this new problem. Now, our table looks like this:

n	x	q	r	t	y
53	14	3	11		
14	11				

In row 2, since $x = 11$ and $11 > 1$, we again apply step 1. Dividing 14 by 11, we obtain a quotient of 1 and a remainder of 3. Thus, to find the inverse of 11 in U_{14} , we must first find the inverse of 3 in U_{11} . So we add a third row to our table for this new problem, and now our table looks like this:

n	x	q	r	t	y
53	14	3	11		
14	11	1	3		
11	3				

Now then, it is not difficult to determine, via “guess and check,” say, that 4 is the inverse of 3 in U_{11} . To check this, note that $4 \cdot 3 = 12$ and $12 = 11(1) + 1$; hence $4 \cdot 3 \pmod{11} = 1$. Thus, the values of t and y in row 3 of the table are 1 and 4, respectively. We may then apply \clubsuit to find the value y in row 2, etc.

However, for the sake of fully illustrating the algorithm, let's continue to apply step 1 until we obtain an x -value of 1. Doing so leads to the following:

n	x	q	r	t	y
53	14	3	11		
14	11	1	3		
11	3	3	2		
3	2	1	1		
2	1			0	1

In row 5, $x = 1$, and $1^{-1} = 1$. Therefore, the value of y in row 5 is 1. Also, since $xy = 1 \cdot 1 = 1$ and $n > 1$, dividing xy by n yields a quotient of 0. Hence, the value of t in row 5 is 0. **THIS WILL ALWAYS BE THE CASE** — that is, if we continue to add rows to the table until we get a row in which $x = 1$, then, in that row, $t = 0$ and $y = 1$.

Once we have obtained the values of t and y in some row, we apply \clubsuit to obtain the value of y in the preceding row. It may be helpful to express \clubsuit in words, so let's repeat it here:

$$y = -(qy' + t') \pmod{n}$$

In words, this says the following: To obtain the value of y in some row, say row i : Multiply the value of q in row i by the value of y in row $i + 1$; next, add the value of t in row $i + 1$ to this product; next, negate this number; finally, compute the remainder when this last number is divided by the value of n in row i .

For example, to find the value of y in row 4, we have:

$$y = -(qy' + t') \bmod n = -(1(1) + 0) \bmod 3 = -1 \bmod 3 = 2$$

Also, in row 4, $xy = 4$ and $n = 3$, and the quotient when 4 is divided by 3 is 1; hence, the value of t in row 4 is 1. So now our table looks like this:

n	x	q	r	t	y
53	14	3	11		
14	11	1	3		
11	3	3	2		
3	2	1	1	1	2
2	1			0	1

Next, we use ♣ to compute the value of y in row 3:

$$y = -(qy' + t') \bmod n = -(3(2) + 1) \bmod 11 = -7 \bmod 11 = 4$$

So $xy = 12$ and $n = 11$, and the quotient when 12 is divided by 11 is 1. Hence, the value of t row 3 is 1. Thus, our table now looks like this:

n	x	q	r	t	y
53	14	3	11		
14	11	1	3		
11	3	3	2	1	4
3	2	1	1	1	2
2	1			0	1

Again, we use ♣ to compute the value of y in row 2:

$$y = -(qy' + t') \bmod n = -(1(4) + 1) \bmod 14 = -5 \bmod 14 = 9$$

So $xy = 99$ and $n = 14$, and the quotient when 99 is divided by 14 is 7. Hence, the value of t in row 2 is 7. Thus, our table now looks like this:

n	x	q	r	t	y
53	14	3	11		
14	11	1	3	7	9
11	3	3	2	1	4
3	2	1	1	1	2
2	1			0	1

Finally, we use \clubsuit to compute the value of y in row 1:

$$y = -(qy' + t') \bmod n = -(3(9) + 7) \bmod 53 = -34 \bmod 53 = 19$$

Therefore, in U_{53} , $14^{-1} = 19$.

The value of t in row 1 is a byproduct of checking our answer. Note that $14 \cdot 19 = 266$ and $266 = 53(5) + 1$. Thus, $t = 5$, and we see that $14 \cdot 19 = 266$ is, indeed, 1 more than a multiple of 53. The final table for part (a) is

n	x	q	r	t	y
53	14	3	11	5	19
14	11	1	3	7	9
11	3	3	2	1	4
3	2	1	1	1	2
2	1			0	1

Exercise. Complete the table for part (b).

n	x	q	r	t	y
53	20				



Let G be a group of order n and let $a \in G$. Then, by the celebrated theorem of Lagrange, the order of a must be a factor of n . Of fundamental interest for the purpose of our catalog is this question: Given a group G of order n and a factor m of n , how many elements of order m does G have?

We first answer this question for cyclic groups.

Theorem 8: Let G be a cyclic group of order $n \geq 2$ and let g be a generator for G . Then, for any integer k , $0 \leq k < n$,

$$|g^k| = \frac{n}{\gcd(k, n)} = \frac{\text{lcm}(k, n)}{k}$$

Proof: Under the stated hypothesis, let $d = \gcd(k, n)$ and let e be the identity of G . We first show that $|g^d| = n/d$. Well,

$$(g^d)^{n/d} = g^n = e$$

Furthermore, for any positive integer $t < n/d$, $(g^d)^t = g^{dt} \neq e$, since $dt < n$.

Next, we show that $|g^k| = |g^d|$; in fact, we show the stronger result that $\langle g^k \rangle = \langle g^d \rangle$. To show this, it suffices to show that $g^k \in \langle g^d \rangle$ and $g^d \in \langle g^k \rangle$.

Since d is a factor of k , it is clear that $g^k \in \langle g^d \rangle$. To show other subgroup membership, note that, since $d = \gcd(k, n)$, there exist integers s and t such that

$$d = ns + kt \tag{*}$$

Moreover, for any integer m , if we let $s' = s - mk$ and $t' = t + mn$, then

$$d = ns' + kt'$$

Hence, we may assume that the integer t in \clubsuit is positive. Therefore,

$$d \bmod n = (kt) \bmod n$$

and it follows that $g^d = g^{kt} = (g^k)^t \in \langle g^k \rangle$. ■

Corollary 9: For integers k and n with $0 \leq k < n$, the order of k in \mathbb{Z}_n is given by

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

Theorem 10: Let G be a cyclic group of order $n \geq 2$ and let m be a positive factor of n . Then G has $\phi(m)$ elements of order m .

Proof: Let G be a cyclic group of order $n \geq 2$ with generator g , let m be a positive factor of n and let k be an integer, $1 \leq k < n$. Clearly, G has $\phi(1) = 1$ element of order 1, namely, the identity element e . Also, G has $\phi(n)$ elements of order n , since

$$|g^k| = n \leftrightarrow \frac{n}{\gcd(k, n)} = n \leftrightarrow \gcd(k, n) = 1$$

For $1 < m < n$, we see from the proof of Theorem 8 that g^k has order m if and only if g^d has order m , where $d = \gcd(k, n)$. Moreover,

$$|g^d| = m \leftrightarrow \frac{n}{\gcd(d, n)} = m \leftrightarrow \frac{n}{d} = m \leftrightarrow d = \frac{n}{m}$$

Thus, all the elements in G having order m are in the subgroup of G generated by $g^{n/m}$, which is a cyclic group of order m . As shown above, a cyclic group of order m has $\phi(m)$ generators, and this establishes the result. ■

Corollary 11: Given an integer $n \geq 2$ and a positive factor m of n , the number of elements of order m in \mathbb{Z}_n is $\phi(m)$. ■

Corollary 12: Let k be a positive integer and let p be an odd prime. Then, for $n = p^k$ or $n = 2p^k$, the number of primitive roots modulo n is $\phi(p^{k-1}(p-1))$. ■

Using elementary methods, we showed earlier that, for $n \in \{2, 3, 5\}$ there is a unique group of order n , up to isomorphism, namely, the cyclic group of order n . More generally, let p be a prime, and let G be a group of order p . Then, by Lagrange's theorem, every nonidentity element of G has order p , and it follows that G is cyclic.

Theorem 13: Given a prime p , the cyclic group of order p is a unique group of order p , up to isomorphism. ■

So, given a prime p , the section in our catalog listing the groups of order p will be brief, consisting of a single entry. However, we could give that entry as the abstract cyclic group of order p , C_p , having presentation

$$C_p = \langle a \mid |a| = p \rangle$$

or as the group \mathbb{Z}_p , or, as the group $U_p = \mathbb{Z}_p^\#$.

We briefly mention infinite cyclic groups.

Consider, for example, the group (\mathbb{Q}^+, \cdot) of positive rational numbers under multiplication, and let H be the set of nonnegative powers of 2:

$$H = \{2^0 = 1, 2^1 = 2, 2^2 = 4, 2^3 = 8, \dots\}$$

Note that H is not a group — that is, it is not a subgroup of (\mathbb{Q}^+, \cdot) — since H is not closed under inverses. In order for H to be a group, it needs to contain

$$2^{-1} = \frac{1}{2}, \quad 4^{-1} = \frac{1}{4} = 2^{-2}, \quad 8^{-1} = \frac{1}{8} = 2^{-3}, \quad \dots$$

If we include these, and let

$$G = \{2^m \mid m \in \mathbb{Z}\}$$

then G is a group — in fact, it is a subgroup of (\mathbb{Q}^+, \cdot) — and it makes sense to write $G = \langle 2 \rangle$ and to say that G is the cyclic subgroup of (\mathbb{Q}^+, \cdot) generated by 2.

In general, we say that a group (or subgroup) G is *cyclic* provided

$$G = \{a^m \mid m \in \mathbb{Z}\}$$

for some element $a \in G$, with the understanding that, for $n \in \mathbb{Z}^+$, $a^{-n} = (a^{-1})^n$. In this case, the element a is called a *generator* for G , and we write $G = \langle a \rangle$.

The prototype for an infinite cyclic group is the group $(\mathbb{Z}, +)$ of integers under addition. Here, 1 is a generator. Note that, since the operation in this group is addition:

$$\begin{aligned} & \vdots \\ 1^{-2} &= (-1)^2 = (-1) + (-1) = -2 \\ 1^{-1} &= (-1)^1 = -1 \\ 1^0 &= 0 \text{ (the identity element of } (\mathbb{Z}, +) \text{)} \\ 1^1 &= 1 \\ 1^2 &= 1 + 1 = 2 \\ & \vdots \end{aligned}$$

Note that -1 is also a generator.

If we take an integer $k > 1$, we can compute $\langle k \rangle$, the cyclic subgroup of \mathbb{Z} generated by k . For example, when $k = 3$, we obtain

$$\dots \quad 3^{-2} = -6, \quad 3^{-1} = -3, \quad 3^0 = 0, \quad 3^1 = 3, \quad 3^2 = 6, \quad \dots$$

Thus, $\langle 3 \rangle = \{\dots, -6, -3, 0, 3, 6, \dots\} = 3\mathbb{Z}$. In general, $\langle k \rangle = k\mathbb{Z}$.

Additional Exercises

1. Complete the following operation table for $(\mathbb{Z}_8, +)$.

+	0	1	2	3	4	5	6	7
0								
1								
2								
3								
4								
5								
6								
7								

- Complete the operation table for (U_{15}, \cdot) . Also, for each element, indicate its inverse.
- Label the nodes so that the directed graph shown in Figure 4 is the Cayley digraph for (U_{11}, \cdot) using generating set $\{2\}$.
- Construct the Cayley digraph for (U_{16}, \cdot) using generating set $\{3, 7\}$.
- Find a primitive root modulo 18.

14. Let p be an odd prime and let k be a positive integer. Let g be a primitive root modulo p^k . Fact: If g is odd, then g is a primitive root modulo $2p^k$; otherwise, $g + p^k$ is a primitive root modulo $2p^k$. Apply this result to find a primitive root modulo:

(a) $2 \cdot 23^2 = 1058$

(b) $2 \cdot 41^2 = 3362$

15. With reference to Exercise 12, it is known that, if g is a primitive root modulo p , then g is a primitive root modulo p^k unless, in U_{p^2} ,

$$g^{p-1} = 1$$

Find the smallest prime p for which the smallest primitive root g modulo p is not a primitive root modulo p^2 .

16. Let n be an integer, $n > 4$, such that U_n is cyclic, and let g be a primitive root modulo n . Then

$$(g^0 = 1, g^1, g^2, \dots, g^{\phi(n)-1})$$

is a permutation of U_n . Thus, given $x \in U_n$, there is a unique exponent t , $0 \leq t < \phi(n)$, such that $g^t = x$. We call t the *discrete logarithm of x modulo n using base g* , and we write

$$\text{dlog}_g(x) = t \pmod{n}$$

or simply $\text{dlog}_g(x) = t$, if the modulus n is understood. (Some books use the term *index* instead of discrete logarithm.)

(a) Complete the following table of discrete logarithms modulo 13 using base 2.

x	1	2	3	4	5	6	7	8	9	10	11	12
$\text{dlog}_2(x)$	0											

(b) Complete the following table of discrete logarithms modulo 22 using base 7.

x	1	3	5	7	9	13	15	17	19	21
$\text{dlog}_7(x)$	0									

(c) For $x_1, x_2 \in U_n$, show that

$$\text{dlog}(x_1 x_2) = \text{dlog}(x_1) + \text{dlog}(x_2) \quad \heartsuit$$

with the addition on the right-hand side being addition modulo $\phi(n)$.

(d) Apply \heartsuit to compute $9 \cdot 11$ in U_{13} .

(e) For $x \in U_n$ and $k \in \mathbb{Z}^+$, show that

$$\text{dlog}(x^k) = k\text{dlog}(x)$$

♠

with the multiplication on the right-hand side being performed in $\mathbb{Z}_{\phi(n)}$.

(f) Apply ♠ to compute 17^7 in U_{22} .

17. Show that the group $(\mathbb{Q}, +)$ is not a cyclic group.
18. Show that the group (\mathbb{Q}^+, \cdot) is not a cyclic group.