SUBGROUPS OF CYCLIC GROUPS

KEITH CONRAD

1. Introduction

In a group G, we denote the (cyclic) group of powers of some $g \in G$ by

$$\langle g \rangle = \{g^k : k \in \mathbf{Z}\}.$$

If $G = \langle g \rangle$, then G itself is cyclic, with g as a generator.

Examples of infinite cyclic groups include $\mathbf{Z}$, with (additive) generator 1, and the group $2^{\mathbf{Z}}$ of integral powers of the real number 2, with generator 2. The most basic examples of finite cyclic groups are $\mathbf{Z}/(m)$ with (additive) generator 1 and

$$\mu_m = \{z \in \mathbf{C}^\times : z^m = 1\}$$

with generator $e^{2\pi i/m} = \cos(2\pi/m) + i\sin(2\pi/m)$. Both have size m. The elements of μ_m lie at the vertices of a regular m-gon on the unit circle and include 1. (Don't forget this fundamental geometric picture of μ_m!)

Don't confuse the groups $\mathbf{Z}/(m)$ and $(\mathbf{Z}/(m))^\times$. The second, as a *set*, is a subset of the first, but it is not a subgroup and it is usually *not* cyclic (see Theorem A.2). For instance, $(\mathbf{Z}/(15))^\times$ is not cyclic. But many of the groups $(\mathbf{Z}/(m))^\times$ are cyclic, and we will take our examples from such groups which are cyclic.

Example 1.1. The group $(\mathbf{Z}/(23))^\times$ has size 22, and it is cyclic with 5 as a generator. (The elements 2 and 3 each have order 11, so they are not generators.)

In this handout, we describe the subgroups of a general cyclic group $G = \langle g \rangle$. Here are the main results, in brief:

- Every subgroup of G is cyclic.
- If G is infinite then each subgroup has the form $\langle g^n \rangle$ for a unique integer $n \geq 0$.
- If G is finite, of size m, then each subgroup has the form $\langle g^d \rangle$, where d is a unique positive divisor of m. For $k \in \mathbf{Z}$, $\langle g^k \rangle = \langle g^{(k,m)} \rangle$.
- The containment relations among subgroups of a cyclic group resemble divisibility relations among integers.

2. Subgroups are always cyclic

Let G be a cyclic group. We will show every subgroup of G is also cyclic, taking separately the cases of infinite and finite G.

Theorem 2.1. *Every subgroup of a cyclic group is cyclic.*

Proof. Let G be a cyclic group, with generator g. For a subgroup $H \subset G$, we will show $H = \langle g^n \rangle$ for some $n \geq 0$, so H is cyclic. The trivial subgroup is obviously of this form ($e = g^0$). So we may suppose H is non-trivial.

How are we going to find the $n \geq 1$ making $H = \langle g^n \rangle$? The idea is that every element in a subgroup of the form $\langle g^n \rangle$ looks like g^{nk}, so n is the smallest positive exponent among the

elements of this subgroup. With this in mind, given a non-trivial subgroup $H \subset G$, *define* n to be the smallest positive integer such that $g^n \in H$. (There are such powers; H contains some non-zero power of g, which becomes a positive power after inversion if necessary.)

Now we show any $h \in H$ is a power of g^n. (Any element of $\langle g^n \rangle$ lies in H, since g^n already does.) The whole group G is generated by g, so $h = g^a$ for some $a \in \mathbf{Z}$. We want $n|a$. Well, by the division theorem,

$$a = nq + r$$

for some integers q and r such that $0 \leq r < n$. Therefore

$$h = g^a = (g^n)^q g^r = g^r.$$

As $g^r \in H$ and $0 \leq r < n$, the minimality condition defining n implies r can't be positive, so $r = 0$. Thus $n|a$, so $h = g^a \in \langle g^n \rangle$. This proves $H = \langle g^n \rangle$. □

When g has infinite order, any g^n with $n \neq 0$ also has infinite order, so all non-trivial subgroups of an infinite cyclic group are again infinite cyclic groups.

In particular, a subgroup of an infinite cyclic group is again an infinite cyclic group.

Theorem 2.1 tells us how to find all the subgroups of a finite cyclic group: compute the subgroup generated by each element and then just check for redundancies.

Example 2.2. Let $G = (\mathbf{Z}/(7))^\times$. We list in the following table the successive powers of an element until we hit 1.

a	$\langle a \bmod 7 \rangle$
1	$\{1\}$
2	$\{2, 4, 1\}$
3	$\{3, 2, 6, 4, 5, 1\}$
4	$\{4, 2, 1\}$
5	$\{5, 4, 6, 2, 3, 1\}$
6	$\{6, 1\}$

Each subgroup of $(\mathbf{Z}/(7))^\times$ is cyclic, so it must be in the above table. Taking into account that some subgroups are appearing more than once, $(\mathbf{Z}/(7))^\times$ has four subgroups: $\{1\}$, $\{1, 6\}$, $\{1, 2, 4\}$, and $\{1, 2, 3, 4, 5, 6\}$. (We have rewritten the elements in each subgroup in increasing order as integers, for lack of a better idea at this point.)

We will see in the next section a better way to systematically enumerate the subgroups of a finite cyclic group, which will avoid the kinds of redundancies we met in Example 2.2.

3. Enumerating subgroups of a cyclic group

By Theorem 2.1, every subgroup of $\mathbf{Z}$ (additive!) has the form $n\mathbf{Z}$ for some integer n, and we can take $n \geq 0$. Obviously different choices of $n \geq 0$ give us different subgroups. The story turns out to be the same for any infinite cyclic group.

Lemma 3.1. *If g is an element of infinite order in a group, then $g^k = g^\ell$ if and only if $k = \ell$. If g is an element of finite order m in a group, then $g^k = g^\ell$ if and only if $k \equiv \ell \bmod m$.*

Proof. If $g^k = g^\ell$ and $k \neq \ell$, we may suppose $k < \ell$. Then $g^{\ell - k} = e$, with $\ell - k \neq 0$, so g has finite order. Thus, contrapositively, if g has infinite order and $g^k = g^\ell$ then $k = \ell$.

The case of g with finite order is treated in the handout on orders of elements in a group. □

Theorem 3.2. *Each non-trivial subgroup of an infinite cyclic group has two generators, which are inverses of each other. Fixing one generator g of the whole group, we can write each subgroup in the form $\langle g^n\rangle$ for a unique $n \geq 0$.*

Proof. Theorem 2.1 tells us any subgroup has the form $\langle g^n\rangle$ for an integer n. Since $\langle g^n\rangle = \langle g^{-n}\rangle$, we can take $n \geq 0$. (Actually, the proof of Theorem 2.1 produced the n as a non-negative integer already, so we didn't really need this last argument to bring us to the case $n \geq 0$.) As long as we can prove g^n is the only generator of $\langle g^n\rangle$ with a positive exponent, then g^n and g^{-n} (its inverse) are the only generators of $\langle g^n\rangle$ at all.

If our subgroup is trivial, we must use $n = 0$, in which case the desired conclusions are all easy to check. Suppose we are working with non-trivial subgroups. Then we want to show, if n and n' are positive, that $\langle g^n\rangle = \langle g^{n'}\rangle$ only when $n = n'$. When those subgroups are equal, g^n and $g^{n'}$ are both powers of each other, so $g^n = g^{n's}$ and $g^{n'} = g^{nt}$ for some s and t in $\mathbf{Z}$. By Lemma 3.1, $n = n's$ and $n' = nt$, so n and n' divide each other. Therefore they are equal (since both are positive, so no sign ambiguity occurs). □

Corollary 3.3. *In an infinite cyclic group, with generator g, $\langle g^n\rangle \subset \langle g^{n'}\rangle$ if and only if $n'|n$.*

Notice the divisibility is in reverse order to the inclusion. This makes sense, *e.g.*, $\langle g^6\rangle \subset \langle g^2\rangle$ since g^6 is a power of g^2, while $2|6$ (not $6|2$).

Proof. The condition $\langle g^n\rangle \subset \langle g^{n'}\rangle$ is the same as g^n being a power of $g^{n'}$, say $g^n = g^{n's}$ for some s. By Lemma 3.1, $n = n's$, so $n'|n$. □

Example 3.4. If $\langle g\rangle$ is an infinite cyclic group, the subgroups inside of $\langle g^6\rangle$ are those of the form $\langle g^{6s}\rangle$. The subgroups which contain $\langle g^6\rangle$ are $\langle g\rangle$, $\langle g^2\rangle$, $\langle g^3\rangle$, and $\langle g^6\rangle$.

Now we turn to the finite case.

Theorem 3.5. *In a finite cyclic group, each subgroup has size dividing the size of the group. Conversely, given a positive divisor of the size of the group, there is a subgroup of that size.*

Proof. Let $G = \langle g\rangle$, with size m. Any subgroup has the form $\langle g^k\rangle$ for some k. The size of this subgroup is the order of g^k, which is $m/(k, m)$ by the handout on orders of elements in a group. Therefore the size of each subgroup divides m.

Given a positive divisor d of m, we can write down an element of order d in terms of the chosen generator of G: $g^{m/d}$ has order $m/(m/d) = d$. Therefore $\langle g^{m/d}\rangle$ has size d. □

There is an essential strengthening of Corollary 3.5: for each divisor of the size of a (finite) cyclic group, there is *exactly one* subgroup of that size. To see why, we show how to change the generator of a subgroup into one with a "standard" form (in terms of the choice of a generator for the whole group), and then compare subgroups using such standardized generators (standardized in terms of the choice of a generator for the whole group).

Theorem 3.6. *Let $G = \langle g\rangle$ be a finite cyclic group, with size m. For $k \in \mathbf{Z}$, $\langle g^k\rangle = \langle g^{(k,m)}\rangle$. In particular, any subgroup of G has the form $\langle g^d\rangle$ where d is a positive divisor of m. Different values of d give subgroups with different sizes, so there is just one subgroup of G having a given size.*

Proof. We know by Theorem 2.1 that any subgroup of G is cyclic. Write it as $\langle g^k\rangle$. We will show g^k and $g^{(k,m)}$ are both powers of each other, so they generate the same subgroup.

Since $(k,m)|k$, g^k is certainly a power of $g^{(k,m)}$. To show $g^{(k,m)}$ is a power of g^k, we use Bezout's identity:

$$(k,m) = kx + my$$

for some $x, y \in \mathbf{Z}$. This tells us

$$g^{(k,m)} = g^{kx}g^{my} = g^{kx},$$

where we used $g^m = e$ to make the second simplification. (Here $m = \#G$, and we saw in class that $g^{\#G} = e$ in any finite abelian group, such as a finite cyclic group.)

Now we know any subgroup is generated by g^d, where d is some positive divisor of m. How large is such a subgroup $\langle g^d\rangle$? Since $d|m$, g^d has order m/d, so $\#\langle g^d\rangle = m/d$. If d and d' are different positive divisors of m, then $\langle g^d\rangle \neq \langle g^{d'}\rangle$ since the two subgroups have different sizes. □

Remark 3.7. In the enumeration of subgroups of G according to the divisors of $m = \#G$, the trivial subgroup corresponds to the divisor m.

Corollary 3.8. *In a finite cyclic group, two elements generate the same subgroup if and only if the elements have the same order.*

Proof. The order of an element is the size of the subgroup it generates, so elements generating the same subgroup have the same order. In the other direction, elements with the same order generate subgroups with the same size, and these subgroups are equal since there is just one subgroup with any possible size (Theorem 3.6). □

Remark 3.9. The conclusion of Corollary 3.8 is completely false for finite non-cyclic groups: equal order hardly has to imply elements generate the same subgroup. Consider $(\mathbf{Z}/(15))^\times = \{1, 2, 4, 7, 8, 11, 13, 14 \bmod 15\}$. The largest order of an element is 4, so this group is not cyclic. There are several subgroups of size 2, such as

$$\{1, 14\}, \quad \{1, 4\}, \quad \{1, 11\}.$$

Corollary 3.10. *Let G be a finite cyclic group. For subgroups H and H', $H \subset H'$ if and only if $\#H|\#H'$.*

Writing $G = \langle g\rangle$, $m = \#G$, $H = \langle g^n\rangle$, and $H' = \langle g^{n'}\rangle$, $\langle g^n\rangle \subset \langle g^{n'}\rangle$ if and only if $(n', m)|(n, m)$.

Proof. Both H and H' are cyclic, by Theorem 2.1. Thus, if H is a subgroup of H', then $\#H|\#H'$ by Theorem 3.5. Conversely, suppose $\#H|\#H'$. Applying Theorem 3.5 to H', there is a subgroup $K \subset H'$ whose size is $\#H$. Then K will also be a subgroup of G with size $\#H$. Since G can only have one subgroup of any possible size, by Theorem 3.6, $K = H$.

We now translate this result into the language of explicit generators and exponents. Set $G = \langle g\rangle$, $m = \#G$, $H = \langle g^n\rangle$, and $H' = \langle g^{n'}\rangle$. Then $\langle g^n\rangle \subset \langle g^{n'}\rangle$ if and only if the order of g^n divides the order of $g^{n'}$. This is equivalent to $m/(n, m)$ dividing $m/(n', m)$, which is the same as $(n', m)|(n, m)$. □

Remark 3.11. When we describe containment of subgroups in terms of their sizes, smaller subgroups correspond to divisors. When we describe containment of subgroups in terms of exponents in the generators, smaller subgroups then correspond to multiples, which resembles Corollary 3.3.

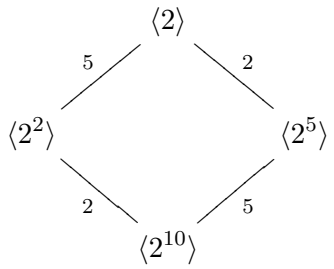
Example 3.12. Let $G = (\mathbf{Z}/(11))^\times$. This group has size 10, and is cyclic. One of its generators is 2.

k	1	2	3	4	5	6	7	8	9	10
$2^k \bmod 11$	2	4	8	5	10	9	7	3	6	1

The subgroups of $(\mathbf{Z}/(11))^\times$ are therefore

$$\langle 2\rangle, \quad \langle 2^2\rangle, \quad \langle 2^5\rangle, \quad \langle 2^{10}\rangle.$$

In the following diagram we draw the subgroups as a lattice, with the index of the smaller subgroup in the larger indicated on the line connecting the subgroups.



The top subgroup is $(\mathbf{Z}/(11))^\times$, the bottom one is $\{1\}$, and the others have order 2 and 5. Which of these subgroups is $\langle 3\rangle$? We will answer this in three ways.

Method 1: Compute the order of 3 in $(\mathbf{Z}/(11))^\times$. It is 5:

$$3^2 \equiv 9 \bmod 11, \quad 3^3 \equiv 5 \bmod 11, \quad 3^4 \equiv 4 \bmod 11, \quad 3^5 \equiv 1 \bmod 11.$$

(We could have found this from the previously computed table of powers of 2: since $3 \equiv 2^8 \bmod 11$, 3 has order $10/(8,10) = 5$.) There is just one subgroup of size 5, namely $\langle 2^2\rangle$, so this is $\langle 3\rangle$.

Method 2: The table of powers of 2 shows $3 \equiv 2^8 \bmod 11$, so 3 generates the same subgroup of $(\mathbf{Z}/(11))^\times$ as $2^{(8,10)} = 2^2$.

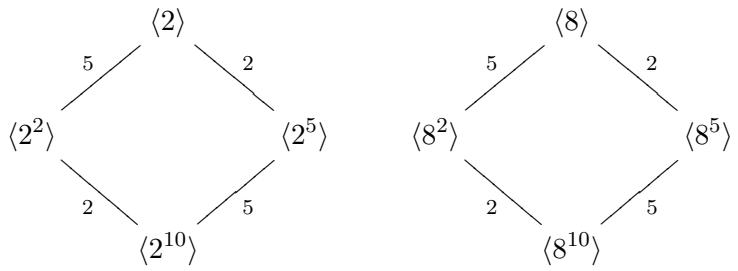
Method 3: Write out the intermediate subgroups explicity:

$$\langle 2^2\rangle = \{2^2, 2^4, 2^6, 2^8, 2^{10}\} = \{4, 5, 9, 3, 1\}, \quad \langle 2^5\rangle = \{2^5, 2^{10}\} = \{10, 1\}.$$

In this list, we see 3 shows up in just one, so that has to be the subgroup generated by 3. This is the worst of the three methods, in terms of efficiency.

If we changed the choice of generator for the group, then our labels for the subgroups would change. For instance, take $8 = 2^3$ as the generator for $(\mathbf{Z}/(11))^\times$. Then the subgroups have generators 8^d for $d \in \{1, 2, 5, 10\}$. These are the elements

$$8^1 = 8, \quad 8^2 = 9, \quad 8^5 = 10, \quad 8^{10} = 1.$$

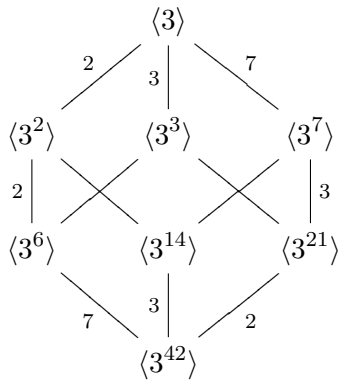


We can avoid generators and label the subgroups simply by their size: there is one of size 1, one of size 2, one of size 5, and one of size 10.

While some computational aspects of cyclic groups depend on the particular generator being used, the intrinsic group-theoretical properties of the cyclic group certainly don't depend on the choice of a generator. For instance, the statements of Theorems 2.1 and 3.5, the very end of Theorem 3.6, and Corollary 3.8 don't depend at all on the choice of a generator for their meaning.

Example 3.13. Let $G = (\mathbf{Z}/(49))^\times$. This is a group of size 42. (Its elements are represented by integers not divisible by 7, so it has $49 - 7 = 42$ members.) The reader can check 3 is a generator of $(\mathbf{Z}/(49))^\times$. The subgroups of $(\mathbf{Z}/(49))^\times$ are therefore $\langle 3^d \rangle$ where d runs through the divisors of 42:

$$\langle 3\rangle,\ \ \langle 3^2\rangle,\ \ \langle 3^3\rangle,\ \ \langle 3^6\rangle,\ \ \langle 3^7\rangle,\ \ \langle 3^{14}\rangle,\ \ \langle 3^{21}\rangle,\ \ \langle 3^{42}\rangle.$$



Which of these subgroups is $\langle 3^{12}\rangle$? It is $\langle 3^{(12,42)}\rangle = \langle 3^6\rangle$. That is, 3^{12} and 3^6 generate the same subgroup. Which of these subgroups is $\langle 6\rangle$? To answer this we compute the order of 6 mod 49. A tedious calculation shows the order is 14. The subgroup $\langle 3^d\rangle$ with size 14 is $\langle 3^{42/14}\rangle = \langle 3^3\rangle$, so $\langle 6\rangle = \langle 3^3\rangle$.

Example 3.14. Let $G = \mu_m$. When $d|m$, the complex d-th roots of unity are m-th roots of unity, so $\mu_d \subset \mu_m$. Conversely, if $\mu_d \subset \mu_m$, then $\#\mu_d | \#\mu_m$ by Corollary 3.5, so $d|m$. Theorem 3.6 tells us a finite cyclic group has just one subgroup of each possible size, so the subgroups of μ_m are exactly the groups μ_d as d runs over the positive divisors of m.

Example 3.15. The group $(\mathbf{Z}/(13))^\times$ is cyclic (a generator is 2), with size 12. The subgroups have size 1,2,3,4,6, and 12. The subgroup of size 4 contains just the subgroups of sizes 1, 2, and 4, and the subgroup of size 3 is contained in the subgroups of sizes 3, 6, and 12. Using the explicit generator of the whole group, we get generators for the subgroups:

d	Subgp. of size d
1	$\langle 1\rangle$
2	$\langle 2^6\rangle$
3	$\langle 2^4\rangle$
4	$\langle 2^3\rangle$
6	$\langle 2^2\rangle$
12	$\langle 2\rangle$

4. Abstract versus concrete cyclic groups

The properties we have discussed for cyclic groups and their subgroups have relied on nothing about such groups other than their sizes. This is in the nature of things: cyclic

groups of the same size are structurally more or less the same thing. Without being completely precise (yet) about what this means, let's see why any infinite cyclic group essentially resembles $\mathbf{Z}$ and any finite cyclic group of size m essentially resembles $\mathbf{Z}/(m)$.

Suppose G is a cyclic group. Choose a generator, say g. We can write each element of G in the form g^k for an integer k. Lemma 3.1 tells us that if G is infinite then g^k determines k as an integer, while if G is finite of size m then g^k determines k as an integer modulo m: $g^k = g^\ell$ if and only $k \equiv \ell \bmod m$. In either case, the way g^k and g^ℓ multiply coincides with the way the exponents add: $g^k g^\ell = g^{k+\ell}$. This suggests we can set up a correspondence between G and $\mathbf{Z}$ or some $\mathbf{Z}/(m)$, as follows:

- If G is infinite, let $g^k \in G$ correspond to $k \in \mathbf{Z}$.
- If $\#G = m$, let $g^k \in G$ correspond to $k \bmod m \in \mathbf{Z}/(m)$.

These correspondences are meaningful only because of Lemma 3.1, which lets us extract knowledge of the exponent from knowledge of the power as either an integer (when G is infinite) or as an integer modulo m (when $\#G = m$). The multiplication in G corresponds to the addition in $\mathbf{Z}$ or $\mathbf{Z}/(m)$, depending on the size of G. Therefore we are able to translate all the behavior of an abstract cyclic group into behavior in the concrete additive groups of integers or integers modulo m. By *following the exponents*, any abstract cyclic group becomes one of the basic cyclic groups $\mathbf{Z}$ or $\mathbf{Z}/(m)$ for some $m > 0$. (Note $m = 1$ corresponds to the trivial cyclic group of size 1.) Therefore any two abstract cyclic groups of the same size are very similar kinds of groups, since they have the same "model" group built out of integers.

(Since $\mathbf{Z} = \mathbf{Z}/(0)$, we can actually use the notation $\mathbf{Z}/(m)$ in all cases, taking $m = 0$ in the case of infinite cyclic groups. Note congruence modulo 0 is just ordinary equality.)

While we have argued that any two cyclic groups of the same size are essentially interchangeable insofar as their abstract mathematical features are concerned, there is an important *practical* consideration: it is easy to write down a generator of the additive cyclic groups $\mathbf{Z}$ and $\mathbf{Z}/(m)$ (use 1 in either case), but other cyclic groups need not have a generator that can be written down easily.

An important example to keep in mind in this respect is $(\mathbf{Z}/(p))^\times$, where p is prime. This group has size $p - 1$ and it can be proved to be cyclic (but we don't include a proof here). To this day, no method of finding a generator of $(\mathbf{Z}/(p))^\times$ is known to be more efficient than essentially trying 2, then 3, and so on. Who cares? Well, the difficulty of breaking a certain public key crytosystem (due to El Gamal) depends on the difficulty of working with generators of $(\mathbf{Z}/(p))^\times$.

Appendix A. More applications

Our first application of the structure of subgroups of cyclic groups is a non-constructive proof of Bezout's identity. The proof here is completely independent of Euclid's algorithm, which is how the identity is proved in a constructive way.

Theorem A.1. *For any $a, b \in \mathbf{Z}$, we have*

$$a\mathbf{Z} + b\mathbf{Z} = (a, b)\mathbf{Z}, \quad a\mathbf{Z} \cap b\mathbf{Z} = [a, b]\mathbf{Z}.$$

In particular, there are x and y such that $ax + by = (a, b)$.

Proof. Given two subgroups H and K of $\mathbf{Z}$, we can construct two other subgroups out of them: $H + K$ (the set of sums, one term from H and the other term from K) and $H \cap K$.

Any subgroup of $\mathbf{Z}$ is cyclic, so we must have

$$a\mathbf{Z} + b\mathbf{Z} = c\mathbf{Z}, \quad a\mathbf{Z} \cap b\mathbf{Z} = d\mathbf{Z}$$

for some integers c and d. Without loss of generality, c and d are non-negative. We will show $c = (a, b)$ and $d = [a, b]$.

The elements of $c\mathbf{Z}$ are the multiples of c. Since $a = a\cdot 1 + b\cdot 0$, we obtain $c|a$. Similarly, $c|b$, so c is a (non-negative) common divisor of a and b. Since $c \in a\mathbf{Z} + b\mathbf{Z}$, we get $c = ax + by$ for some x and y in $\mathbf{Z}$. Then any common divisor of a and b is a common divisor of $ax + by = c$, which means $c = (a, b)$. That $d = [a, b]$ is left to the reader. □

Here is a neat application of Theorem 3.6: a strong constraint on those m for which $(\mathbf{Z}/(m))^\times$ could be a cyclic group.

Theorem A.2. *If $(\mathbf{Z}/(m))^\times$ is cyclic, then m must be 2, 4, an odd prime power, or twice an odd prime power.*

Proof. The idea is this: for any m *other* than 2, 4, an odd prime power, or twice an odd prime power, we will construct two different subgroups of size 2. There can't be two subgroups of the same size in a cyclic group, by Theorem 3.6, so $(\mathbf{Z}/(m))^\times$ is not cyclic!

One subgroup of $(\mathbf{Z}/(m))^\times$ with size 2 is generated by -1. We will find an element of order 2 other than -1. Such a "fake" square root of 1 modulo m generates a second subgroup of size 2.

First suppose m is a power of 2 other than 2 or 4: $m = 2^s$ with $s \geq 3$. Then $1 + 2^{s-1} \bmod 2^s$ squares to 1, and $1 + 2^{s-1} \not\equiv \pm 1 \bmod 2^s$ since $s > 2$.

The moduli m left to consider are those which are not a prime power or twice an odd prime power. Let m be such a number (m could be 15, 90, and so on). Then there is a way of writing $m = ab$ where $(a, b) = 1$ and $a, b > 2$. (For instance, let a be the largest power of some odd prime dividing m and take for b the complementary divisor, *e.g.*, $90 = 9 \cdot 10$ or $5 \cdot 18$.) By Bezout, we can write

$$1 = ax + by$$

for some $x, y \in \mathbf{Z}$. Let

$$\begin{aligned} t &= ax - by \\ &= 1 - 2by \\ &= -1 + 2ax. \end{aligned}$$

We will show $t^2 \equiv 1 \bmod m$ and $t \not\equiv \pm 1 \bmod m$. (Our choice of t may seem strange at first, although those who have seen some number theory will recognize in the next paragraph that our choice was dictated with the Chinese remainder theorem in mind, for moduli a and b.)

The different formulas for t show $t \equiv -1 \bmod a$ and $t \equiv 1 \bmod b$, so $t^2 \equiv 1 \bmod a$ and $t^2 \equiv 1 \bmod b$. Then a and b both divide $t^2 - 1$, so (since a and b are relatively prime) $m|(t^2 - 1)$. We have $t^2 \equiv 1 \bmod m$.

To show $t \not\equiv \pm 1 \bmod m$, we argue by contradiction. If $t \equiv 1 \bmod m$, then $t \equiv 1 \bmod a$. Already we have $t \equiv -1 \bmod a$, so $1 \equiv -1 \bmod a$. This is impossible, since $a > 2$. Similarly, since $t \equiv 1 \bmod b$ and $b > 2$, we can't have $t \equiv -1 \bmod m$. □

Corollary A.2 actually captures exactly those m for which $(\mathbf{Z}/(m))^\times$ is not cyclic: when m is 2, 4, an odd prime power, or twice an odd prime power, then $(\mathbf{Z}/(m))^\times$ *is* cyclic. The proof is omitted.