# 14 Multiplication Modulo $m$ Meets Groups

In this section, we will be finding the largest subset of integers that forms a group under multiplication, modulo various numbers. We will then find a symmetry group which is isomorphic to each modulo multiplication group. Let's start with some small moduli first.

mod $3$

| $\cdot$ | $0$ | $1$ | $2$ |
|---|---|---|---|
| $0$ | $0$ | $0$ | $0$ |
| $1$ | $0$ | $1$ | $2$ |
| $2$ | $0$ | $2$ | $1$ |

mod $4$

| $\cdot$ | $0$ | $1$ | $2$ | $3$ |
|---|---|---|---|---|
| $0$ | $0$ | $0$ | $0$ | $0$ |
| $1$ | $0$ | $1$ | $2$ | $3$ |
| $2$ | $0$ | $2$ | $0$ | $2$ |
| $3$ | $0$ | $3$ | $2$ | $2$ |

1. Clearly some of these numbers cannot be elements of a group. For instance, in both cases, $0$ cannot be used, since it prevents the existence of an inverse. In the case of mod $4$, $2$ cannot be used either. Why not?
2. How could we have known that these numbers would not work in advance?
3. **Euler's totient function** $\varphi(m)$ tells us how many numbers are relatively prime to a given number $m$. That is, $\varphi(m)$ is the count of numbers $n$ such that $\gcd(m, n) = 1$. What does the maximum size of a group under multiplication mod $m$ have to do with this function?

Taking out the numbers which cannot be members of a group, we get these two tables:

mod $3$

| $\cdot$ | $1$ | $2$ |
|---|---|---|
| $1$ | $1$ | $2$ |
| $2$ | $2$ | $1$ |

mod $4$

| $\cdot$ | $1$ | $3$ |
|---|---|---|
| $1$ | $1$ | $3$ |
| $3$ | $3$ | $1$ |

We now have two groups isomorphic to each other, as well as to $C_2$, $D_2$, and $S_2$.

4. We will write tables for the largest possible groups under multiplication mod $5$ and mod $8$.
   (a) Make a prediction as to how many elements will be in each group.
   (b) Which numbers can you eliminate from consideration?
   (c) Do you think that the groups will be isomorphic to those of multiplication mod $3$ and mod $4$, or to each other?
   (d) Find the period of each element in the groups and write their **orbits**: the list of its powers until it reaches the identity.
   (e) Make the tables, and analyze them to confirm/correct your predictions.
   (f) Are there any subgroups?
5. Now use a program to find the largest possible group under multiplication mod $14$.
   (a) What are its elements?
   (b) Make a table of the group's orbits.
   (c) Make a group table.
   (d) It might be good to order the numbers at the top of the table so that they start with a $1$ and go by successive powers of $3$.
   (e) What group is it isomorphic to?
   (f) Does it have any subgroups; if so, what are they?
6. Now, a surprise: find the powers of $10$, mod $14$.
   (a) How long is the period of this orbit?
   (b) What number appears to be the identity element?
   (c) Make a table in which the identity element comes first.

(d) Find a number besides $10$ whose group of powers mod $14$ is isomorphic to this group.

(e) Are these groups isomorphic to a multiplication group of a smaller modulus?

7. To really tell if two groups are isomorphic, you can write their tables in such an order that they would be identical if you substituted them in place. Why is it helpful to first note the periods and orbits of each element?

If you want to dig deeper, here's some investigations you can try. Some of these questions are deeply connected to number theory.

- To which symmetry groups are there isomorphisms under multiplication mod $m$?
- Are there some symmetry groups which do not have a representation in multiplication mod $m$?
- Is there a way you can predict in advance what symmetry groups you can get from multiplication mod $m$, given $m$?
- Can you get every finite group? Note that there exist many, many more finite groups than we have talked about so far.
- What about particular classes of group, like cyclic, dihedral, commutative and noncommutative groups?
- If a group has $n$ members, what is the largest possible period an element can have? What other periods can it have? What do we know about the numbers of elements with each period? What about period of $1$ specifically?
- Every element of a group has an inverse by the definition of group. If an element is its own inverse, what is its period? If an element has period $p$, what is the period of its inverse?
- Will $n-1$ always be in the largest group under multiplication mod $n$? Why?
- What properties do the following types of groups have?

1. multiplication mod $p$, a prime
2. multiplication mod $3^n$
3. multiplication mod $p^n$
4. multiplication mod $2^n$
5. multiplication mod $5^n$
6. multiplication mod a composite

For more weirdness, consider the multiplicative group of integers modulo $35$.[13] The set of integers relatively prime to $35$ is

$$\{1, 2, 3, 4, 6, 8, 9, 11, 12, 13, 16, 17, 18, 19, 22, 23, 24, 26, 27, 29, 31, 32, 33, 34\}.$$

| Num. | Orbit | Per. | Num. | Orbit | Per. |
|---|---|---|---|---|---|
| 1 | 1 | 1 | 18 | 18,9,22,11,23,29,32,16,8,4,2,1 | 12 |
| 2 | 2,4,8,16,32,29,23,11,22,9,18,1 | 12 | 19 | 19,11,34,16,24,1 | 6 |
| 3 | 3,**9**,27,**11**,33,**29**,17,**16**,13,**4**,12,**1** | 12 | 22 | 22,29,8,1 | 4 |
| 4 | 4,16,29,11,9,1 | 6 | 23 | 23,4,22,16,18,29,2,11,8,9,32,1 | 12 |
| 6 | 6,1 | 2 | 24 | 24,16,34,11,19,1 | 6 |
| 8 | 8,29,22,1 | 4 | 26 | 26,11,6,16,31,1 | 6 |
| 9 | 9,11,29,16,4,1 | 6 | 27 | 27,29,13,1 | 4 |
| 11 | 11,16,1 | 3 | 29 | 29,1 | 2 |
| 12 | 12,4,13,16,17,29,33,11,27,9,3,1 | 12 | 31 | 31,16,6,11,26,1 | 6 |
| 13 | 13,29,27,1 | 4 | 32 | 32,9,8,11,2,29,18,16,22,4,23,1 | 12 |
| 16 | 16,11,1 | 3 | 33 | 33,4,27,16,3,29,12,11,13,9,17,1 | 12 |
| 17 | 17,9,13,11,12,29,3,16,27,4,33,1 | 12 | 34 | 34,1 | 2 |

Figure 1: Orbits of elements mod $35$.

That's $24$ elements, so initial guesses about the associated group would include the rotation group of a cube (periods $1, 2, 3, 4$) and the rotation group of the regular $24$-gon (periods $1$,$2$,$3$,$4$,$6$,$8$,$12$,$24$). None of these

[13] This is usually denoted $(\mathbb{Z}/35\mathbb{Z})^\times$.

guesses turn out to be correct though. Let's create a table with the orbits and periods of each element, as shown in Figure 1.

The periods appear to be factors of $12$, which leads us to consider the rotation group of the regular dodecagon, $C_{12}$. But this has only half as many elements as our group. The dihedral group $D_{12}$, however, does have $24$ elements. Let's try matching up the elements in the two groups.

$$D_{12}: \text{ Rotations of } 0^\circ, 30^\circ, 60^\circ, 90^\circ, 120^\circ, 150^\circ, 180^\circ, 210^\circ, 240^\circ, 270^\circ, 300^\circ, 330^\circ$$

$0^\circ$ and $1$ are the identities, so they are paired up. Because $2$ has period $12$, we arbitrarily match it up with the $30^\circ$ rotation. The rest of the powers of $2$ mod $35$ are thus mapped, pairing up all the *rotations* of $D_{12}$.

| Rotation | Number |
|---|---|
| $0^\circ$ | $1$ |
| $30^\circ$ | $2$ |
| $60^\circ$ | $4$ |
| $90^\circ$ | $8$ |
| $120^\circ$ | $16$ |
| $150^\circ$ | $32$ |
| $180^\circ$ | $29$ |
| $210^\circ$ | $23$ |
| $240^\circ$ | $11$ |
| $270^\circ$ | $22$ |
| $300^\circ$ | $9$ |
| $330^\circ$ | $18$ |

But now we run into a problem. What do we pair up the reflections with? Reflections have period $2$, but only $3$ elements in our group have that property; we need $12$. So $D_{12}$ doesn't work, either!

In fact, this group is a completely new group! It is equal to $C_2 \times C_{12}$, the "product" of two groups we're familiar with. The definition of group product is beyond the scope of this book, but as you can see, the group order $24$ is indeed the product of the orders of the groups which comprise the product. This goes to show that we have barely scratched the surface of group theory as a subject. Hopefully you get to experience it more deeply in your later education.