Modular Arithmetic and Finite Group Theory

Consider a clock. There are 12 numbers the hour hand can be on. Also 3 hours after 10 is 1. Try adding together some numbers using this “clock arithmetic” What happens when you add 12 to something?

We have sums such as $6 + 8 = 2$
$7 + 8 = 3$
$5 + 24 = 5 + 2x12 = 5$

To make this different from normal arithmetic we will use $\equiv$ instead of of =.

This arithmetic is the same as looking at the remainder of a number after dividing it by 12, e.g.
$14 = 12 + 2 \equiv 2$, $15 = 12 + 3 \equiv 3$, $29 = 2x12 + 5 \equiv 5$, $54 = 4x12 + 6 \equiv 6$

We may want to divide by something else. So we will include the number we are dividing by, e.g.
$14 \equiv 2 \pmod{12}$ $19 \equiv 1 \pmod{6}$
It is called modular arithmetic (hence the mod).

1) Calculate the following numbers mod 12:
a) 64 b) 38 c) 12^2 d) 24^2 e) 99 f) 2521

2) Try these modulo 5:
a) 8 b) 43 c) 5^2 d) 8^2 e) 104 f) 1004

3) Try these modulo 2:
a) 5 b) 8 c) 5^2 d) 8^2 e) 28 f) 1115

We can also solve equations modulo a number, e.g.
$x \equiv 29 \pmod{8}$ has 5 as the smallest positive solution, $x = 8t + 5$ as the general solution.

You can try modulo some other numbers yourself. The solutions for the questions above are on the next page.

Next we will see how this relates to groups. First of all it is worth thinking about how many numbers we need when working modulo 12. The following computations may help.

$0 \equiv 0 \bmod 7$
$1 \equiv 1 \bmod 7$
$2 \equiv 2 \bmod 7$
$3 \equiv 3 \bmod 7$
$4 \equiv 4 \bmod 7$
$5 \equiv 5 \bmod 7$
$6 \equiv 6 \bmod 7$
$7 \equiv 0 \bmod 7$
$8 \equiv 1 \bmod 7$
$9 \equiv 2 \bmod 7$
$10 \equiv 3 \bmod 7$
etc.

Definition $\mathbb{Z}_n$ represents the whole numbers modulo n.

Example: $\mathbb{Z}_7 = \{0, 1, 2, 3, 4, 5, 6\}$ from the numbers used in the table above.
Example: $\mathbb{Z}_{12} = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11\}$
Remark: $\mathbb{Z}_n$ has n numbers in it.

Back to Groups

What has all of this got to do with groups? Is ($\mathbb{Z}_n$, +) a group? Yes! Our example of ($\mathbb{Z}$, +) at the beginning gives us most of what we need, with 0 being our identity element for the same reasons as before and any element 'a' has inverse '-a' which will be 'n-a' when working modulo n (i.e. in $\mathbb{Z}_n$).

Writing down this Group

For finite groups (those without an infinite number of elements) we can use a 'Cayley Table', named after the British Mathematician Arthur Cayley. For ($\mathbb{Z}_4$, +):

+	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

Figure 1

As reading across the column and down the row we have the answer, e.g.
1 + 2 = 3 and 2 + 2 = 0

4) Relating to Cayley tables

a) Write the Cayley table for ($\mathbb{Z}_2$, +), ($\mathbb{Z}_3$, +), and ($\mathbb{Z}_5$, +).

b) Which value of n for ($\mathbb{Z}_n$, +) gives us our clock arithmetic?

c) What does Figure 2 below represent? Compute some other Cayley tables similar to Figure 2. Are they all groups? Can you spot the pattern?

x	1	2	3	4
1	1	2	3	4
2	2	4	1	3
3	3	1	4	2
4	4	3	2	1

Figure 2

Answers

1) a) 4	b) 2	c) 0	d) 0	e) 3	f) 1
2) a) 3	b) 3	c) 0	d) 4	e) 4	f) 4
3) a) 1	b) 0	c) 1	d) 0	e) 0	f) 1