MTH101: Symmetry

Tutorial 04

Problem 1. Write out the multiplication table for the group $U(12)$.

Solutions. $U(12) = \{\overline{1}, \overline{5}, \overline{7}, \overline{11}\}$. As an example, let us look at the product $\overline{5} \cdot \overline{11}$. To calculate this, first we take a representative from each coset and multiply them together. For instance, we take the representative 5 from the coset $\overline{5} = 5 + 12\mathbb{Z}$ and the representative 11 from $\overline{11} = 11 + 12\mathbb{Z}$. The product 55 leaves remainder 7 when divided by 12. So it is in the coset $\overline{7} = 7 + 12\mathbb{Z}$. Thus, $\overline{5} \cdot \overline{11} = \overline{7}$. All other products can be calculated in this way and we get the following table:

	$\overline{1}$	$\overline{5}$	$\overline{7}$	$\overline{11}$
$\overline{1}$	$\overline{1}$	$\overline{5}$	$\overline{7}$	$\overline{11}$
$\overline{5}$	$\overline{5}$	$\overline{1}$	$\overline{11}$	$\overline{7}$
$\overline{7}$	$\overline{7}$	$\overline{11}$	$\overline{1}$	$\overline{5}$
$\overline{11}$	$\overline{11}$	$\overline{7}$	$\overline{5}$	$\overline{1}$

□

Problem 2. What is the remainder when you divide 2^{343} by 37.

Solution. We want to compute 2^{343} modulo 37. As 2 is coprime to 37, the coset $\overline{2}$ is an element of $U(37)$. As p is a prime number, every positive integer less than 37 is coprime to 37. Thus, $U(37) = 36$. Thus, $\overline{2}^{36} = 1$ in $U(36)$. In other words $2^{36} \equiv 1(\mod 37)$. As $343 = 36 \times 9 + 19$, we see that

$$2^{343} = (2^{36})^9 \times 2^{19} \equiv 1^9 \times 2^{19} \mod 37.$$

So, we just need to compute the value of 2^{19} modulo 37. This can be calculated by brute force.

As $2^5 \equiv -5 \mod 37$, we see that

$$2^{10} \equiv 25 \equiv -12 \mod 37$$

and

$$2^{15} \equiv (-12) \times (-5) \equiv 60 \equiv 23 \mod 37.$$

So

$$2^16 \equiv 46 \equiv 9 \mod 37,$$

$$2^17 \equiv 18 \mod 37,$$

$$2^18 \equiv 36 \equiv -1 \mod 37$$

and so

$$2^19 \equiv -2 \equiv 35 \mod 37.$$

Thus, the remainder after dividing 2^{343} by 37 is 35. □

Problem 3. Prove that if n is an odd number, then $n^2 \equiv 1(\mod 8)$.

Solution. Any odd integer is congruent to 1, 3, 5 or 7 modulo 8. So, it suffices to check that the squares of these four numbers are congruent to 1 modulo 8. This is done by actual calculation: $1^2 = 1$, $3^2 = 9 = 8 \cdot 1 + 1$, $5^2 = 25 = 8 \cdot 3 + 1$ and $7^2 = 49 = 8 \cdot 6 + 1$.

Another way to prove this is as follows:

Any odd number is of the form $2n+1$. So we calculate $(2n+1)^2 = 4n^2+4n+1 = 4n(n+1)+1$. As the product of any two consecutive integers is always even, $2|n(n+1)$. So $8|4n(n+1)$. So $(2n+1)^2 \equiv 1 \mod 8$.

□

Problem 4. Let G be a group. Let

$$Z = \{z | z \in G \text{ and } zg = gz \text{ for all } g \in G\}.$$

Prove that Z is a subgroup of G.

Solution. As $1 \cdot g = g \cdot 1 = g$ for any $g \in G$, we see that $1 \in Z$.

If $z \in Z$, $zg = gz$ for any $g \in G$. We take an arbitrary $h \in G$ and use this property for $g = h^{-1}$. Thus, we get that $zh^{-1} = h^{-1}z$. Compute the inverse of both sides of this equation. We have

$$(zh^{-1})^{-1} = (h^{-1})^{-1} \cdot z^{-1} = hz^{-1}$$

and

$$(h^{-1}z)^{-1} = z^{-1} \cdot (h^{-1})^{-1} = z^{-1}h.$$

So, we get $hz^{-1} = z^{-1}h$. Thus, $z^{-1} \in Z$.

If $z_1, z_2 \in Z$, we want to show that $z_1z_2 \in Z$. Thus, we want to show that for any $g \in G$, $(z_1z_2)g = g(z_1z_2)$. As $z_1, z_2 \in Z$, we know that $z_1g = gz_1$ and $z_2g = gz_2$. Thus,

$$(z_1z_2)g = z_1(z_2g) = z_1(gz_2) = (z_1g)z_2 = (gz_1)z_2 = g(z_1z_2).$$

Thus, we see that $z_1z_2 \in Z$.

Thus, Z is a subgroup. □

Problem 5. List all generators of the groups $\mathbb{Z}/9\mathbb{Z}$, $\mathbb{Z}/12\mathbb{Z}$ and $\mathbb{Z}/20\mathbb{Z}$. What do you think will be the generators of $\mathbb{Z}/n\mathbb{Z}$ in general?

Solution. The brute force way of doing this is to compute the orders of all elements in each of these groups. An element is a generator of the group if and only if its order is equal to the order of the group. (We will see a quicker way to do this in Lecture 11.)

For example, what is the order of $\overline{2}$ in $\mathbb{Z}/9\mathbb{Z}$. For this, we must find the smallest integer n such that $\overline{2n} = \overline{0}$ in $\mathbb{Z}/9\mathbb{Z}$. It is easy to check that the smallest such integer is 9. Thus, the order of $\overline{2}$ in this group is $\mathbb{Z}/2\mathbb{Z}$. Thus, this is a generator.

Checking in this manner, the generators for these groups are seen to be the following:

- For $\mathbb{Z}/9\mathbb{Z}$: $\overline{1}, \overline{2}, \overline{4}, \overline{5}, \overline{7}, \overline{8}$.
- For $\mathbb{Z}/12\mathbb{Z}$: $\overline{1}, \overline{5}, \overline{7}, \overline{1}1$.
- For $\mathbb{Z}/20\mathbb{Z}$: $\overline{1}, \overline{3}, \overline{7}, \overline{9}, \overline{11}, \overline{13}, \overline{17}, \overline{19}$.

The detailed solution for general n is given in Lecture 11. □

Problem 6. Is the group $U(8)$ cyclic?

Solution. For a group to be cyclic, it must have a generator. The group $U(8)$ has for elements: $\overline{1}$, $\overline{3}$, $\overline{5}$ and $\overline{8}$. Thus, a generator, if it exists, must have order 4. However, it is easy to check that each of these elements as order 2. (We already did this calculation in the solution to Problem 3.) □