Unit Groups of Modulo n

R. Corless, E. Heapes, L. Ward

NUIG

What is a Unit Group?

A unit group of integers modulo n is the set of non-negative integers from the set $\{0, 1, \ldots, n-1\}$ that are coprime to n. This is a group, under the operation of multiplication mod n.

Where have we seen modulo before?

Many of us will have seen modulo before, in maths or physics modules, but we see and think in modulo everytime we look at a one everyday object! Can you name this object? (Answer bottom right!)

U_n = Coprimes of n

For example, $n = 15$. U_{15} represents the elements of Z_{15} that are coprime to 15, forming a group under the operation of multiplication mod 15.

The identity element of U_{15} is 1. Looking at the table we can see that each element in U_{15} has an inverse such that $x(x^{-1}) = 1$. We know that multiplication is associative, and we can see that only elements of U_{15} are calculated when applying the operation to each element of the set. Therefore U_{15} is closed, associative, has inverses AND an identity element. This mean that U_{15} is a group. We can see that there is symmetry either side of the main diagonal in the table, showing that U_{15} is commutative, making U_{15} an abelian group.

	1	2	4	7	8	11	13	14
1	1	2	4	7	8	11	13	14
2	2	4	8	14	1	7	11	13
4	4	8	1	13	2	14	7	11
7	7	14	13	4	11	2	1	8
8	8	1	2	11	4	13	14	7
11	11	7	14	2	13	1	8	4
13	13	11	7	1	14	8	4	2
14	14	13	11	8	7	4	2	1

Fig. 1: U_{15}

Is it commutative?

Take for example, 7. Here are some examples!

$7 * 4 = 4 * 7 = 13$

$7 * 1 = 1 * 7 = 7$

$7 * 13 = 13 * 7 = 1$

$U_{n \in \mathbf{P}} = \{1, \ldots, n-1\}$

For any Z_n, where n is a positive integer, if n is a prime number then all numbers $\{1, \ldots, n-1\}$ are coprime to n.

For Example ...

$U_7 = \{1, 2, 3, 4, 5, 6\}$ All the conditions for an abelian group are still met, it has an identity (1), inverses, commutative, associativity and it is closed.

	1	2	3	4	5	6
1	1	2	3	4	5	6
2	2	4	6	1	3	5
3	3	6	2	5	1	4
4	4	1	5	2	6	3
5	5	3	1	6	4	2
6	6	5	4	3	2	1

Fig. 2: U_7

U_n for all $n = 2^{\mathbb{N}}$

For any Z_n where $0 < n$ if n is of base 2 then we can easily find out how many elements are coprime to n from the equation $n/2$.

In the table above we have chosen $n = 8$, and we can see that U_8 has 4 (=(8/2)) elements.

This is a special case of a unit group of integers.

	1	3	5	7
1	1	3	5	7
3	3	1	7	5
5	5	7	1	3
7	7	5	3	1

Fig. 3: $2^{\mathbb{N}}$

The Clock! When we read a clock we're reading in modulus! $11am + 2hrs = 1pm$, the same as $(11 + 2 \bmod 12 = 1)$