# The Group of Units in the Integers Modulon



Matt O'Reilly and Clare Callaghan fermoymatt@gmail.com, clareanncallaghan@gmail.com

#### Introduction

The group  $Z_n$  consists of the elements  $\{0, 1, 2, \ldots, n-1\}$  with addition mod n as the operation. You can also multiply elements of  $Z_n$ , but you do not obtain a group: The element 0 does not have a multiplicative inverse, for instance. However, if you confine your attention to the units in  $Z_n$  the elements which have multiplicative inverses, you do get a group under multiplication mod n. It is denoted  $U_n$ , and is called **The group of units** in  $Z_n$ .

In Modular Arithmetic, The Integers coprime to n from the set  $\{0, 1, 2, ..., n-1\}$  of n non-negative integers form a group under multiplication mod n, called The multiplicative group of integers mod n.

### The set of Units in $\mathbb{Z}_n$

**Proposition**. Let  $U_n$  be the set of units in  $\mathbb{Z}_n$ ,  $n \ge 1$ . Then  $U_n$  is a group under multiplication mod n. **Proof.** To show that multiplication mod n is a binary operation on  $U_n$ , We must show that the product of units is a unit. Suppose  $a, b \in U_n$ . Then a has a multiplicative inverse  $a^{-1}$  and b has a multiplicative inverse  $b^{-1}$ . Then;

> $(b^{-1}a^{-1})(ab) = b^{-1}(a^{-1}a)b = b^{-1}(1)b = b^{-1}b = 1,$  $(ab)(b^{-1}a^{-1}) = a(bb^{-1})a^{-1} = a(1)a^{-1} = aa^{-1} = 1.$

Hence,  $b^{-1}a^{-1}$  is the multiplicative inverse of ab, and ab is a unit. Therefore, multiplication mod n is a binary operation on  $U_n$ . We'll take it for granted that multiplication mod n is associative. The identity element for multiplication mod n is 1, and 1 is a unit in  $\mathbb{Z}_n$ . Finally, every element of  $U_n$  has a multiplicative inverse, by definition. Therefore,  $U_n$  is a group under multiplication mod n.

## The Groups of Units in $\mathbb{Z}_{14}$

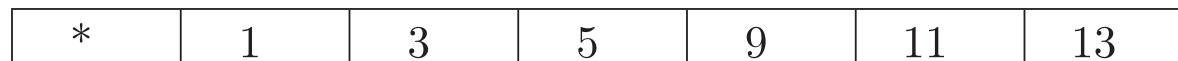
 $U_{14}$  consists of the elements of  $1_{14}$  which are relatively prime to 14. Thus,

 $U_{14} = \{1, 3, 5, 9, 11, 13\}.$ 

You multiply elements of  $U_{14}$  by multiplying as if they were integers, then reducing mod 14. For example,

 $11 \cdot 13 = 143 = 3 \mod 14$ , so  $11 \cdot 13 = 3$ mod 14.

Here's the multiplication table for  $U_{14}$ :



| 1  | 1  | 3  | 5  | 9  | 11 | 13 |
|----|----|----|----|----|----|----|
| 3  | 3  | 9  | 1  | 13 | 5  | 11 |
| 5  | 5  | 1  | 11 | 3  | 13 | 9  |
| 9  | 9  | 13 | 3  | 11 | 1  | 5  |
| 11 | 11 | 5  | 13 | 1  | 9  | 3  |
| 13 | 13 | 11 | 9  | 5  | 3  | 1  |

Notice that the table is symmetric about the main diagonal. Multiplication mod 14 is commutative, and  $U_{14}$  is an Abelian group.

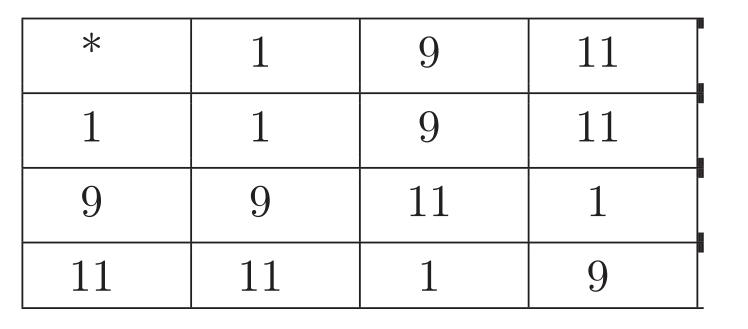
## Lagranges Theorem

**Lagrange's Theorem:** Let G be a finite group and H a subgroup of G. Then the order of H divides the order of G. **Proof:** Suppose  $g \in G$ , then gH has the same number of elements as H. To see this, write k for the order of H and write  $h_1, h_2, \ldots, h_k$  for the elements of H. So the elements of gH are  $gh_1, gh_2, \ldots, gh_k$ . To prove that every element in this list is unique, suppose that ghi = ghj for  $i, j \in \{1, \ldots, k\}$ . Multiplying both sides of this equation on the left by  $g^{-1}$  gives hi = hj and hence i = j. So ghi are distinct for i = 1, ..., k and the coset gH has the same number of elements as H. If  $g_1, g_2 \in G$ , then either the cosets  $g_1H$  and  $g_2H$  are equal to each other or they are disjoint from each other. Once we have shown this we can see that each element of G appears in exactly one coset, thus the number of elements of G is  $|H| + |H| + \cdots + |H|$  (k times) = k|H|. So, the order of G is an integer multiple of H.

We can use Lagranges Theorem to make it much easier to find a subgroup of the group of units in  $Z_{14}$ . We can immediately rule out any subgroups of order 4 or 5 and look either for subgroups of order 2 or 3.

 $H = \{1, 9, 11\}$ 

The multiplication table for H is :



Multiplication remains as the group operation. H is closed under multiplication mod 14. Associativity is inherited from the Group of Units mod 14. H contains the Identity Element and also contains an inverse for every element. Therefore H is a group (and a subgroup of  $U_{14}$ ).