

A LOOK AT EULER'S THEOREM

We want to take another look at multiplication in \mathbb{Z}_n . When the modulus is a prime number, we've seen that every non-zero element is invertible. When the modulus is composite, there were two types of elements: those which were invertible, and those which were divisors of zero (they weren't invertible).

We want to look at just the invertible elements, and we're only interested in *multiplication* (not addition).

First, we need to notice that the product of two invertible elements is invertible. This is fairly obvious once we think about it.

Once we notice this, it makes sense to write out multiplication tables of just the invertible elements. The subset of invertible elements of \mathbb{Z}_n is denoted \mathbb{Z}_n^\times .

Multiplication in \mathbb{Z}_{14}^\times :

\times	1	3	5	9	11	13
1	1	3	5	9	11	13
3	3	9	1	13	5	11
5	5	1	11	3	13	11
9	9	13	3	11	1	5
11	11	5	13	1	9	3
13	13	11	9	5	3	1

Recall the definition of additive order modulo n : the additive order of $a \in \mathbb{Z}_n$ is the smallest positive integer i such that $ia = 0$. Here ia stands for the sum

$$\underbrace{a + a + \cdots + a}_{i \text{ times}}$$

In the same manner, we can define the multiplicative order modulo n : the multiplicative order modulo n of $a \in \mathbb{Z}_n^\times$ is the smallest positive integer i such that $a^i = 1$.

Examples: 1) Clearly the multiplicative order of 1 is 1, and it's the only element of order 1 (regardless of the modulus n).

2). The order of all elements of \mathbb{Z}_8^\times (besides 1, of course) is 2.

3). The orders of the elements of \mathbb{Z}_{14}^\times are ...?

Fermat's Little Theorem: If p is a prime number and $a \in \mathbb{Z}_p^\times$, then $a^{p-1} = 1$. In particular, the multiplicative order of a divides $p - 1$.

Euler's Generalization of Fermat's Little Theorem: If $a \in \mathbb{Z}_n^\times$, then $a^{\phi(n)} = 1$. In particular, the multiplicative order of a divides $\phi(n)$.

Definition: Let $m \in \mathbb{Z}_n^\times$. We will say two elements $a, b \in \mathbb{Z}_n^\times$ are *congruent modulo m* if $a \cdot b^{-1}$ is some positive power of m . Another way to say this is $a = b \cdot m^i$ for some positive integer i .

The set of all b which are congruent to a modulo m will be written $[a]_m$.

Example: In \mathbb{Z}_{14}^\times , which elements are congruent to 1 modulo 9? Which elements are congruent to 11 modulo 3? Which are congruent to 3 modulo 11?

In \mathbb{Z}_8^\times , which elements are congruent to 3 modulo 5? Which elements are congruent to 5 modulo 5?

There are points we will consider about these notions of congruence. First, fix a \mathbb{Z}_n^\times and an element $m \in \mathbb{Z}_n^\times$.

#1: Show that the number of elements in $[m]_m$ is the order of m .

#2: Show that each $[a]_m$ has the same number of elements, no matter what $a \in \mathbb{Z}_n^\times$ we look at.

#3: Show that different ones don't overlap, i.e., $[a]_m \cap [b]_m = \emptyset$ if $[a]_m \neq [b]_m$.

#4: Conclude that the number of elements in $[m]_m$, i.e., the order of m , divides the total number of elements in \mathbb{Z}_n^\times . (By definition, this is $\phi(n)$.)

To get a handle on each of these four points, we should look at a few examples.