

Z_n^* : the multiplicative group modulo n

The hardest thing about Z_n^* is the elements. The elements are those x from 1 to $n - 1$ which are *relatively prime* to n . That is, x has no common factor with n . (**Note:** This is not the same thing as saying x is itself prime!) Here are some small n with the list of elements:

Z_3^* : Elements: 1, 2

Z_4^* : Elements: 1, 3

Z_5^* : Elements: 1, 2, 3, 4

Z_6^* : Elements: 1, 5

Z_7^* : Elements: 1, 2, 3, 4, 5, 6

Z_8^* : Elements: 1, 3, 5, 7

Z_9^* : Elements: 1, 2, 4, 5, 7, 8

Z_{10}^* : Elements: 1, 3, 7, 9

Z_{11}^* : Elements: 1, 2, 3, 4, 5, 6, 7, 8, 9, 10

Z_{12}^* : Elements: 1, 5, 7, 11

Notice that when n is a *prime* number then the elements are all of the elements $1, 2, \dots, n - 1$. This is a very important special case for these groups. We shall generally use the letter p to denote a prime integer so that when we write Z_p^* (or Z_p) we shall be tacitly assuming that p is prime.

The operation for Z_n^* is multiplication, but the result is reduced modulo n . For example, in Z_{11}^* we have $6 \cdot 7 = 42$, but dividing 42 by 11 gives a remainder of 9 so $6 \cdot 7 = 9$. The inverse of x , denoted x^{-1} (this will be the standard notation when the group operation is multiplication) is that y for which $1 = x \cdot y = y \cdot x$. As ordinary multiplication is Abelian (that is, the order doesn't matter) so is multiplication in Z_n^* .

Watch the asterisk! The groups Z_n and Z_n^* are very different!

A Table for Z_{10}^*

-	1	3	7	9
1	1	3	7	9
3	3	9	1	7
7	7	1	9	3
9	9	7	3	1

A Table for Inverses

x	x^{-1}
1	1
3	7
7	3
9	9