Функция Эйлера

Функция эйлера от числа равна произведению количества чисел наибольший делитель которых равен 1

1+0+0+0+1

ф(6) = (1,2,3,4,5) = (1+0+0+0+1) = 2

1+0+0+0

ф(5) = (1,2,3,4) = (1+0+0+0) = 1

Конечное поле

Конечное поле обозначается как: Zq
q - порождающая
Z - список чисел от 0 до q
Рассмотрим пример:
Z_{12} = [1-1,2-1,3-1,4-1,5-1,6-1,7-1,8-1,9-1,10-1,11-1,12-1]

Остатки от деления на q

Если мы хотим узнать значение какой либо опирации в конечном поле Zq то мы просто можем взять два числа x,y сделать какую либо операцию и мы получим значение Z по модулю q
$x * y \equiv Z \pmod q$