

## TAE-2: Poster Presentation

### Residue Class

#### Definition

The set of elements (such as integers) that leave the same remainder when divided by a given modulus

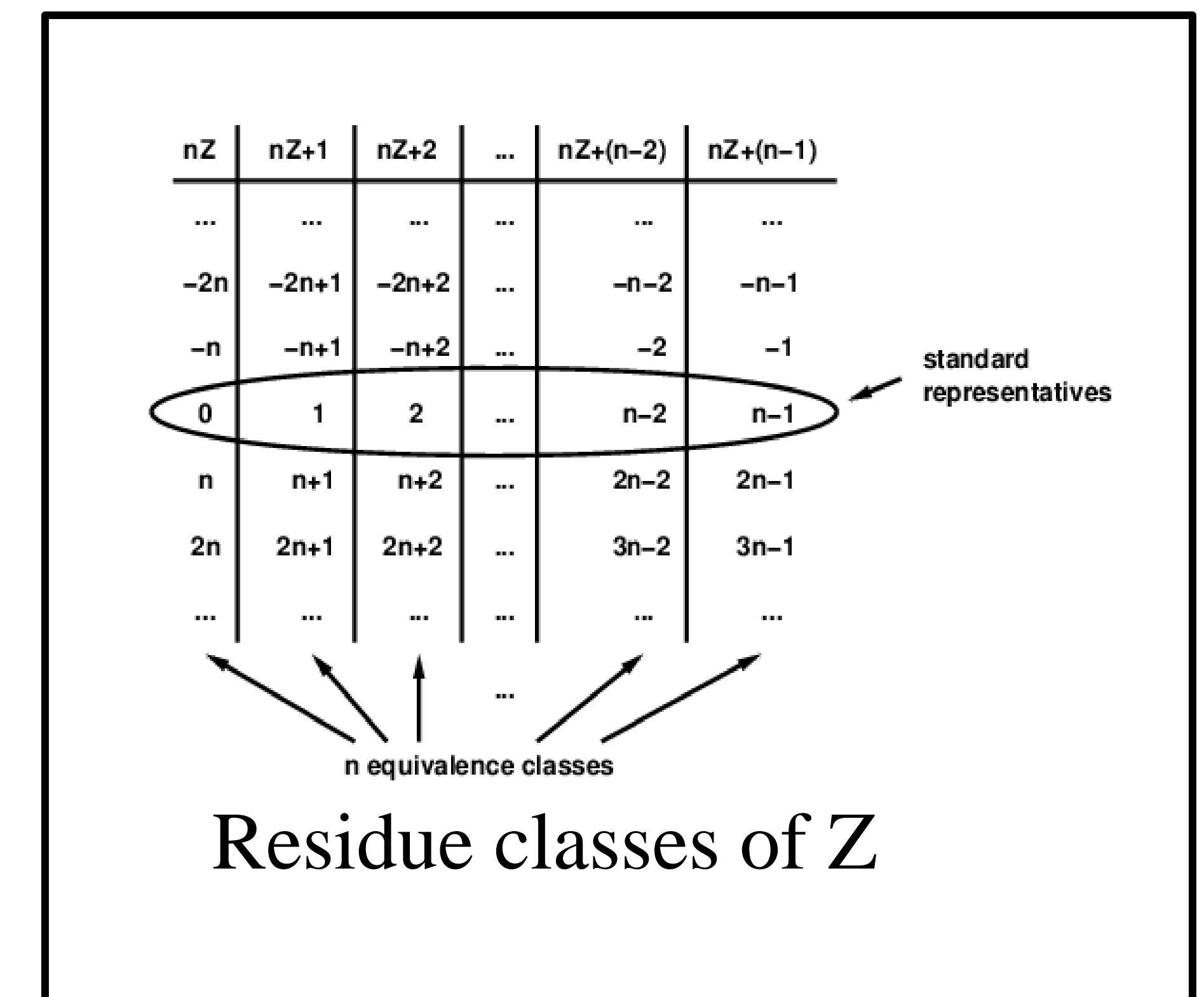
An equivalence class for the equivalence relation of congruence modulo  $n$ . So, two integers are in the same class if they have the same remainder upon division by  $n$ . If  $[a]$  denotes the residue class modulo  $n$  containing  $a$ , the residue classes modulo  $n$  can be taken as  $[0], [1], [2], \dots, [n-1]$ .

The sum and product of residue classes can be defined by

$$[a] + [b] = [a + b], \quad [a][b] = [ab],$$

where it is necessary to show that the definitions here do not depend upon which representatives  $a$  and  $b$  are chosen for the two classes.

With this addition and multiplication, the set, denoted by  $\mathbf{Z}_n$ , of residue classes modulo  $n$  forms a ring (in fact, a commutative ring with identity). If  $n$  is composite, the ring  $\mathbf{Z}_n$  has divisors of zero, but when  $p$  is prime  $\mathbf{Z}_p$  is a field.



A69 Soham Tiwari  
A70 Amaan Nalband  
A71 Shravan Singh  
A72 Pratik Jade