

Divisors of Zero

Consider the integers modulo n . If n is **not** prime, there is a peculiarity: there exist two non-zero numbers in \mathbb{Z}_n such that their product is $0 \pmod n$. For example, $2 \times 3 \equiv 0 \pmod 6$. In this example, we would call 2 and 3 *divisors of zero* modulo 6. A divisor of zero, in this context, must be a positive number.

Theorem: If p is a prime number, then there are no divisors of zero modulo p .

Assume there are two numbers a and b that are divisors of a prime number p modulo p . Definitionally, $a, b \in \mathbb{Z}_p$ such that $a \times b \equiv 0 \pmod p$ and $a \neq 0, b \neq 0$. Using the definition of modulo, we can rewrite this as $k \times p + 0 = a \times b$ where $k \in \mathbb{Z}$. This means that p must evenly divide ab . Thus, p must evenly divide either a or b .

In the case where p evenly divides a , $np = a$ for some positive integer n . a must be non-zero, so $n \geq 1$. However, a is must be an integer in \mathbb{Z}_p , i.e. $\{1, 2, 3, \dots, p-1\}$. Therefore there is no $n \geq 1$ where $np = a$, so p cannot evenly divide a . The same logic can be used to show that p cannot evenly divide b . We've reached a contradiction: it is not possible for p to evenly divide a or b . We can thus conclude the initial assumption of two divisors of zero, a and b , modulo p , is false. There can be no divisors of zero modulo p .