Congruencias en los números enteros

Objetivos. Definir el concepto de números enteros congruentes modulo n. Demostrar que esta relación binaria es una relación de equivalencia, y que las operaciones aritméticas "respetan" a esta equivalencia.

Requisitos. Divisibilidad de números enteros y sus propiedades principales.

Definición de la relación de congruencia

1. Definición de la relación de congruencia con cierto módulo. Sea $n \in \mathbb{N}$ y sean $a, b \in \mathbb{Z}$. Se dice que a y b son *congruentes módulo* n y se escribe $a \equiv b \pmod{n}$ o $a \overset{n}{\equiv} b$, si $n(a - b)$.

2. Teorema (la relación de congruencia de números enteros respecto a un módulo fijo es transitiva, simétrica y reflexiva). Sea $n \in \mathbb{N}$. Entonces la relación binaria $\overset{n}{\equiv}$ tiene las siguientes propiedades:

I. Propiedad transitiva: para cualesquier $a, b, c \in \mathbb{Z}$, si $a \overset{n}{\equiv} b$ y $b \overset{n}{\equiv} c$, entonces $a \overset{n}{\equiv} c$.

II. Propiedad simétrica: para cualesquier $a, b \in \mathbb{Z}$, si $a \overset{n}{\equiv} b$, entonces $b \overset{n}{\equiv} a$.

III. Propiedad reflexiva: para cualquier $a \in \mathbb{Z}$, $a \overset{n}{\equiv} a$.

3. Terminología. Cuando una relación binaria es transitiva, simétrica y reflexiva, se dice que es una *relación de equivalencia*. El Teorema 2 afirma que $\overset{n}{\equiv}$ es una relación de equivalencia.

4. Teorema (la relación de congruencia de números enteros respecto a un módulo fijo concuerda con las operaciones de adición y multiplicación). Sea $n \in \mathbb{N}$.

1. Si $a \overset{n}{\equiv} b$ y $c \overset{n}{\equiv} d$, entonces $a + b \overset{n}{\equiv} c + d$.

2. Si $a \overset{n}{\equiv} b$ y $c \overset{n}{\equiv} d$, entonces $ab \overset{n}{\equiv} cd$.