Clase Congruencias

Eduardo Salas Jiménez

1. Introducción

En matemática olímpica, los números enteros son de gran importancia, así como su estudio y amplio conocimiento de los mismos, propiedades y relaciones. Hasta el momento, es de esperar que las personas que se apasionan por estos temas de la teoría de números, tenga un conocimiento, ya sea elemental o desarrollado, acerca de conceptos como divisor y múltiplo, número primo o compuesto, entre otros.

Con los conceptos que forman la base de una extensa área, se inicia a ver diversos conceptos más elaborados como el de máximo común divisor, mínimo común múltiplo, y resultados importantes como la división euclidiana, o las reglas para determinar cuando un número a es divisible por otro entero d. También, un gran resultado que es primordial en la teoría de números es el Teorema Fundamental de la Aritmética.

Con este repaso de conceptos y resultados, es posible darse cuenta que las herramientas con las que se cuenta en este punto, son escasas. Hay problemas para los cuáles no tenemos el conocimiento para enfrentarlos, o quizás la dificultad se incremente y puede resultar tedioso resolver problemas. Muchas veces, vemos patrones en los números, y en esto se basa la divisibilidad.

Veremos que, si tenemos una cuadrícula de altura infinita, y de ancho 5, y vamos acomodando los enteros en orden, como se muestra a continuación:

$$\begin{array}{|c|c|c|c|c|} \hline \vdots & \vdots & \vdots & \vdots & \vdots \\ -5 & -4 & -3 & -2 & -1 \\ 0 & 1 & 2 & 3 & 4 \\ 5 & 6 & 7 & 8 & 9 \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ \hline \end{array}$$

obtenemos a todos los números que son múltiplos de 5 en la primer columna, así mismo, en la columna $r+1$, están todos los números de la forma $5k+r$.

Esto puede darnos ideas para poder manipular la divisibilidad por 5 de una forma más fácil. Por ejemplo, si tenemos un número en la columna del 1, y a dicho número le sumo un múltiplo de 5, el resultado estará también en la columna del 1. Sin embargo, si a dicho número le sumamos $5k+3$, este resultado se ubicará a la columna del 4.

Con este tipo de observaciones, se puede suponer que los números ubicados en la misma columna tienen comportamientos similares o interesantes, para efectos de la divisibilidad por 5.

El mismo arreglo se puede realizar con 2, 3, 2020 o n columnas, lo que nos lleva a estudiar estas columnas con un lenguaje y estructura más formal. Esto es parte de lo que va a motivar el concepto de congruencias modulares en este pequeño material introductorio.

El dividir números en grupos o columnas es más natural de lo que parece, pues esto se puede ver con las horas del día, los días de la semana o los meses del año, así como en los pulsos que se cuentan en el baile o en la música, así como otros muchos ejemplos de la vida cotidiana.

Es posible que a la hora de abordar conceptos como clases o representantes en un módulo, nos venga a la mente la imagen de estas columnas de números, y similarmente al sustituir números en congruencias. Sin más, procederemos a introducir y desarrollar esta poderosa herramienta.

2. Definiciones y propiedades

Definición 1. Sea n un entero positivo. Si a y b son enteros cualesquiera, decimos que $a \equiv b \pmod{n}$ si $n|a-b$. Se lee como:

a es congruente con b en módulo n.

Una vez definidas las congruencias y el lenguaje estándar a utilizar en módulos, recordamos las columnas en el arreglo de la introducción, así como lo importante que es conocer en qué columna se encuentra un número. Con esta motivación procedemos a dar las siguientes tres definiciones.

Definición 2. Dado un número natural n, a cada conjunto de números congruentes entre sí se le llama *clase* (módulo n) y cualquier elemento de ese conjunto se le llama *representante de la clase*. Si a es cualquier representante de una clase, denotaremos por $\overline{a}$ a la clase a la que pertenece este número.

Definición 3. Dado un entero positivo n, vamos a definir el siguiente conjunto $\mathbb{Z}_n = \{\overline{0}, \overline{1}, \overline{2}, \ldots, \overline{n-1}\}$, es decir, todas las clases que existen en módulo n.

Definición 4. Sea n un entero positivo, entonces llamamos a un conjunto $C = \{r_0, r_1, r_2, \ldots, r_{n-1}\}$ un *Sistema Completo de Residuos* módulo n, si todo entero es congruente a exactamente uno de los elementos C, en módulo n. Se puede ver que Z_n es un Sistema Completo de Residuos módulo n.

Definición 5. Sea n un entero positivo, llamamos a un conjunto $R = \{r_0, r_1, r_2, \ldots, r_{\phi(n)}\}$ un *Sistema Reducido de Residuos* módulo n, si todo entero k, tal que $(k, n) = 1$, es congruente a exactamente un elemento de R. Nótese que en R están todos los elementos de algún C que son primos relativos con n.

Proposición 1. Sea n un número natural y sean a, b enteros. Suponga que $a = nq_1 + r_1$ y $b = nq_2 + r_2$, donde q_1, q_2, r_1, r_2 son enteros y además $0 \leq r_1, r_2 < n$. Entonces $a \equiv b \pmod{n}$ si y solo si $r_1 = r_2$.

Propiedades. Sea n un entero positivo. Si a, b, c, d, m son todos números enteros, entonces se tiene que:

(i) $a \equiv a \pmod{n}$.

(ii) $a \equiv b \pmod{n} \implies b \equiv a \pmod{n}$.

(iii) $a \equiv b \pmod{n}$ y $b \equiv c \pmod{n} \implies a \equiv c \pmod{n}$.

(iv) $a \equiv b \pmod{n}$ y $c \equiv d \pmod{n} \implies a + c \equiv b + d \pmod{n}$.

(v) $a \equiv b \pmod{n}$ y $c \equiv d \pmod{n} \implies ac \equiv bd \pmod{n}$.

(vi) $a \equiv b \pmod{n} \implies a^m \equiv b^m \pmod{n}$.

Principio de Sustitución. Para efectuar operaciones (sumar y multiplicar) dentro de una congruencia entre expresiones, es posible sustituir cualquier número de alguna expresión por otro que sea congruente a este, y se conserva la validez de dicha congruencia.

Más propiedades.

(i) Si d es un divisor de n, y $a \equiv b \pmod{n}$, entonces $a \equiv b \pmod{d}$, pero el recíproco no siempre es cierto, basta ver que $1 \equiv 3 \pmod{2}$, pero $1 \not\equiv 3 \pmod{4}$, a pesar de que $2|4$.

(ii) Sean n_1, n_2 enteros positivos con $m = (n_1, n_2)$. Entonces, si $a \equiv b \pmod{n_1}$ y $a \equiv b \pmod{n_2}$, esto implica que $a \equiv b \pmod{m}$.

Proposición 2. Sea n un entero positivo. Si a es un entero tal que $(a, n) = 1$, entonces existe un entero b tal que $ab \equiv 1 \pmod{n}$. En este caso, diremos que a es *invertible* y que b es un inverso de a en módulo n. También se suele expresar este inverso como a^{-1}. Recíprocamente, si para a, b enteros se cumple que $ab \equiv 1 \pmod{n}$, entonces a y n son primos relativos.

Proposición 3. Si a y n son primos relativos, entonces:

$$ab \equiv ac \pmod{n} \iff b \equiv c \pmod{n}$$

Definición 6. Sea n un entero positivo. Decimos que un entero a es *Residuo cuadrático* módulo n, si existe un entero k tal que $a \equiv k^2 \pmod{n}$.

3. Teoremas importantes

Algunos de los teoremas más importantes a la hora de resolver problemas utilizando congruencias se enuncian a continuación.

Definición 7. Para un número natural n, definimos la función $\phi : \mathbb{N} \to \mathbb{N}$ tal que $\phi(n)$ denota la cantidad de enteros positivos menores o iguales a n que son primos relativos con n. Por ejemplo, $\phi(1) = 1$, $\phi(5) = 4$, $\phi(6) = 2$. En particular, si p es un número primo, se sabe que $\phi(p) = p - 1$.

Teorema de Euler. Sea n un entero positivo y a un entero tal que $(a, n) = 1$. Entonces:

$$a^{\phi(n)} \equiv 1 \pmod{n}$$

Si consideramos el teorema anterior para n un número primo, evidentemente sigue siendo válido pues es un caso particular. Además, si se tuviera que $(a, n) \neq 1$ para n primo, esto quiere decir que $n|a$, y así mismo $n|a^n$. Esto se resume en el siguiente teorema:

Pequeño Teorema de Fermat. Sea p un número primo y a cualquier entero. Entonces:

$$a^p \equiv a \pmod{p}$$

Teorema de Wilson. Sea p es un número primo, entonces:

$$(p-1)! \equiv -1 \pmod{p}$$

4. Ejercicios

1. Determine el residuo de dividir $2020^{506} + 506^{45} + 45^{11}$ por 11.

2. Encuentre el último dígito de $3 \cdot 18^6 + 15 \cdot 2019 - 65^4$.

3. Determine el residuo al dividir $2018^{2019} \cdot 2019^{2018}$ por 5?

4. Encuentre el residuo al dividir $1 + 2019 + 2019^2 + \cdots + 2019^{2018} + 2019^{2019}$ por 2020.

5. **Regla de divisibilidad del 9:** Demuestre que todo entero positivo n es congruente con la suma de las cifras que lo forman en módulo 9.

6. **Regla de divisibilidad del 3:** Demuestre que todo entero positivo n es congruente con la suma de las cifras que lo forman en módulo 3.

7. **Regla de divisibilidad del 11:** Demuestre que un entero positivo es divisible por 11 si y solo si la diferencia entre la suma de sus cifras en posiciones pares con la suma de sus cifras en posiciones impares es divisible por 11.

5. Problemas

1. Encuentre todas las parejas de enteros positivos m, n que satisfacen la igualdad:

$$5n^m - 4n = 2$$

2. Suponga que el número 7^{2019} está escrito en una pizarra con todas sus cifras. Entonces se borra la primera cifra (a la izquierda) y se suma al número que queda. Este proceso se repite hasta obtener un número N de diez cifras. Pruebe que N no puede tener todos sus dígitos distintos.

3. Encuentre todos los enteros positivos n para los cuales $2^n - 1$ es divisible por 7.

4. Demuestre que la ecuación $a^2b^2 + b^2c^2 + 3b^2 - a^2 - c^2 = 2005$ no tiene soluciones enteras.

5. Encuentre todas las parejas de enteros positivos no compuestos (p, q), es decir, primos o 1, tal que satisfacen la igualdad:

$$p^6 - q^4 = 6p + 3q$$

6. Sean x, y enteros tales que $x^2 - 2xy + y^2 - 5x + 7y$ y $x^2 - 3xy + 2y^2 + x - y$ son ambos múltiplos de 17. Demuestre que $xy - 12x + 15y$ también lo es.

7. Demuestre que para todo número primo p distinto de 2 y de 5, existen infinitos múltiplos de p, de la forma $111\ldots11$ (escrito solo con 1's).

8. Se tiene $(a_n)_n$ una sucesión, tal que $a_n = 2 \cdot 10^{n+1} + 19$, Determine todos los primos $p \leq 19$ para los cuales existe un $n \geq 1$ para el cual p divide a a_n.

9. Encuentre todas las tripletas de enteros positivos (x, y, z) tales que:

$$x^2 + y^2 + z^2 = 2011$$

10. Encuentre todos los primos p y q tales que $p^3 - q^5 = (p + q)^2$.

11. Determine el menor entero positivo n para el cual existan enteros positivos $a_1, a_2, \ldots, a_n$ menores o iguales a 15 y no necesariamente distintos, tales que los últimos cuatro dígitos de la suma $a_1! + a_2! + \cdots + a_n!$ sean 2001.

12. Encuentra todos los enteros positivos p, q y r, con p y q números primos, que satisfacen la igualdad:

$$\frac{1}{p+1} + \frac{1}{q+1} - \frac{1}{(p+1)(q+1)} = \frac{1}{r}$$