34 Olimpiada Mexicana de MATEMÁTICAS Aguascalientes 2020

MÓDULOS

Ana del Socorro Viramontes Medina

1. Módulos

Definición. Sea n un número natural. Si a y b son enteros cualesquiera decimos que $a \equiv b(mod.n)$ (a es congruente con b módulo n) si $n \mid a-b$.

También se puede ver a b como el residuo de dividir $\frac{a}{n}$, si b es un número menor a n y mayor igual a 0.

Otra forma de verlo es con el algoritmo de la división. Si tenemos que $a \equiv b\ (mod\ n)$, entonces $a = nk + b$ con k siendo un entero.

Ejemplo: $17 \equiv 2(mod.5)$

Lo cual se puede ver como

$5 \mid (17-2) \rightarrow 5 \mid 15$

También se puede ver como al dividir $\frac{17}{5}$ se tiene un residuo de 2.

Cuando dos o más números tienen la misma congruencia bajo un mismo módulo, se dice que estos números pertenecen a una misma clase, por ejemplo, $17 \equiv 2(mod.5)$, $32 \equiv 2(mod.5)$, aquí $17, 2\ y\ 32$ son números de una misma clase módulo 5. Además, existen las congruencias negativas $17 \equiv -3(mod.5)$, lo cual podemos comprobar gracias a la definición, $5 \mid (17-(-3)) = 5 \mid 20$. Por lo que 2 y -3 pertenecen a una misma clase, módulo 5.

Propiedades. Sea $n \geq 1$ un entero. Para a, b, c y d enteros cualesquiera se tiene:

(C1) $a \equiv a(mod.n)$. Es decir, la relación de congruencia es reflexiva. (En otras palabras, todo número es congruente a sí mismo)

Como $a - a = 0 = n \times 0$, entonces $n \mid a-a$

(C2) Si $a \equiv b(mod.n)$ entonces $b \equiv a(mod.n)$. Esto es la relación de congruencia es simétrica.

Tenemos que $a - b = nk$ para algún entero k así que $b - a = n(-k)$

(C3) Si $a \equiv b(mod.n)$ y $b \equiv c(mod.n)$ entonces $a \equiv c(mod.n)$. Es decir, la relación de congruencia es transitiva. (dos números congruentes a un entero son congruentes entre sí)

Escribamos $a - b = nk$ y $b - c = nl$, con k y l enteros; entonces $a - b + b - c = nk + nl$, $a - c = n(k + l)$

(C4) Si $a \equiv b\ (mod.n)$ y $c \equiv d\ (mod.n)$ entonces $a + c \equiv b + d(mod.n)$

Queremos probar que $(a + c) - (b + d)$ es múltiplo de n; pero $(a + c) - (b + d)$ es igual a $(a - b) + (c - d)$ lo cuál es múltiplo de n, ya que $a - b$ y $c - d$ es múltiplo de n.

(C5) Si $a \equiv b(mod.n)$ y $c \equiv d(mod.n)$ entonces $ac \equiv bd(mod.n)$

Para esto queremos probar que $ac - bd$ es múltiplo de n, $ac - bd = ac - bc + bc - bd = (a - b)c + (c - d)b$, por hipótesis $a - b$ y $c - d$ son múltiplos de n, por lo que $(a - b)c$ y $(c - d)b$ son múltiplos al igual que su suma.

Ejemplo: Encontrar el residuo módulo 5 de $37^4 - 49(801) + 120$

No es necesario realizar las operaciones para llegar al residuo, sabemos que:

$37 \equiv 2(mod.5),\quad 49 \equiv 4(mod.5),\quad 801 \equiv 1(mod.5),\quad 120 \equiv 0(mod.5)$

$37 \cdot 37(mod.5) \equiv 2 \cdot 2(mod.5) \equiv 4(mod.5)$ por C5

$(37 \cdot 37) \cdot (37 \cdot 37)(mod.5) \equiv 4 \cdot 4$ (mod. 5) $\equiv 16(mod.5) \equiv 1(mod.5)$ por C5

$49 \cdot 801(mod.5) \equiv 4 \cdot 1(mod.5) \equiv 4\ (mod.5)$ por C5

$37^4 - 49(801)(mod.5) \equiv 1 - 4(mod.5) \equiv -3(mod.5)$ por C4

$37^4 - 49(801) + 120(mod.5) \equiv -3 + 0(mod.5) \equiv -3(mod.5)$ por C4

Luego, $-3 \equiv 2(mod.5)$, siendo 2 el residuo de la operación.

Ejemplo: Encontrar la última cifra de $2 \times 325 + 3 \times 8^7 \times 5104 + 123^5$

Para encontrar la última cifra, conviene analizar las congruencias módulo 10.

$$2 \times 325(mod.10) \equiv 2 \times 5(mod.10) \equiv 10(mod.10) \equiv 0(mod.10)$$

$$8^7(mod.10) \equiv (-2)^7(mod.10) \equiv -128(mod.10) \equiv -8(mod.10) \equiv 2(mod.10)$$

$$3 \times 8^7 \times 5104(mod.10) \equiv 3 \times 2 \times 4(mod.10) \equiv 24(mod.10) \equiv 4\ (mod.10)$$

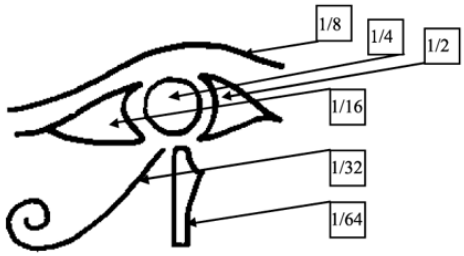
$$123^5(mod.10) \equiv 3^5(mod.10) \equiv 3^2 \cdot 3^2 \cdot 3(mod.10) \equiv 9 \cdot 9 \cdot 3(mod.10)$$
$$\equiv (-1) \cdot (-1) \cdot 3(mod.10) \equiv 3\ (mod.10)$$

$$2 \times 325 + 3 \times 8^7 \times 5104 + 123^5 (mod. 10) \equiv 0 + 4 + 3 (mod. 10) \equiv 7 (mod. 10).$$

En este problema podemos ver que para hacer operaciones menos complejas a veces conviene usar una congruencia negativa en lugar de una congruencia positiva.

2. Datos de vital importancia

1. El ojo de Horus era un símbolo muy importante para los antiguos egipcios y cada una de sus partes se vinculaba a una fracción:



Las fracciones del Ojo de Horus

   El 1/64 que falta para el entero es una parte del ojo que Horus perdió en las aguas del Nilo durante la lucha que libró contra su tío Seth para vengar la muerte de Osiris, su padre, y que nunca recuperó, aunque Toth la recreó posteriormente.
   https://elibro.net/es/ereader/uaa/127786?page=154
2. Los balones de fútbol son esferas embaldosadas con pentágonos y hexágonos, inspirados en un poliedro llamado fullereno, que se corresponde con la estructura cristalina del C60.
   https://elibro.net/es/lc/uaa/titulos/37796

3. Problemas

1. Si $k \equiv 1\ (mod\ 4)$, ¿a qué es congruente $6k + 5\ (mod\ 4)$?
2. ¿Cuál es el residuo cuando se divide 9^{2013} entre 8?
3. ¿Cuál es el último dígito de 3^{1234}?
4. ¿Cuál es el último dígito de 7^{2015}?
5. ¿Cuál es el dígito de las unidades de $1! + 2! + 3! + \cdots + 100!$?
6. Demuestra que $41|2^{20} - 1$
7. ¿Cuál es el último dígito de 7^{7^7}?
8. Demuestra que $7|2222^{5555} + 5555^{2222}$
9. Demuestra que $n^3 + 2n$ es divisible por 3 para cualquier entero positivo n que se elija
10. Demuestra que $n^5 + 4n$ es divisible por 5 para cualquier entero positivo n
11. Demuestra que la diferencia de dos cubos perfectos consecutivos no puede ser múltiplo de 3
12. Prueba que:
    a. Todo primo mayor a 2 es congruente a 1 o 3 módulo 4
    b. Todo primo mayor a 3 es congruente a 1 o 5 módulo 6

13. Demuestra que si $n \equiv 4\ (mod\ 9)$, entonces n no puede escribirse como la suma de tres cubos.
14. ¿Cuál es el dígito de las unidades de $\sum_{k=1}^{2019} k^2 + k$?
15. Si n es un entero positivo mayor que 1 tal que $2^n + n^2$ es un número primo, demuestra que $n \equiv 3\ (mod\ 6)$
16. Demuestra que $2019|1^{2019} + 2^{2019} + 3^{2019} + \cdots + 2017^{2019} + 2018^{2019} + 2019^{2019}$

4. Vídeos

Congruencias

https://youtu.be/AkTCcu__Kxw