Congruencias

AlanLG

15 de Febrero 2024

§1 Lectura

Vamos a presentar el concepto de módulo en teoría de números, decimos que

$$a \equiv b \pmod{c} \iff c \mid a - b$$

y se lee "a" congruente a "b" módulo c, lo cuál es equivalente a decir que a y b dejan el mismo residuo al dividirse entre c. Por ejemplo tenemos que

$$\begin{aligned} 13 &\equiv 5 \pmod{4} \\ 101 &\equiv 13 \pmod{9} \\ 25 &\equiv 0 \pmod{5} \\ 11 &\equiv 3 \pmod{8} \end{aligned}$$

Algo importante es que nos da igual si los números son positivos o no, por ejemplo

$$\begin{aligned} 10 &\equiv -1 \pmod{11} \\ 19 &\equiv -2 \pmod{11} \end{aligned}$$

Esto es útil pues a veces puede ser más facil trabajar con residuos negativos.

Ejemplo 1.1
Si hoy es martes, ¿Qué día será en 2024 días?

La semana tiene 7 días, como $2024 \equiv 1 \pmod{7}$ entonces basta añadirle un día a martes y entonces es 2024 días será miércoles.

Esta nueva notación (módulos) nos permite trabajar más fácil con divisibilidades, es más práctica que la notación de $x \mid y$ (x divide a y), nos da una opción de trabajar una divisibildad como algo que sería similar a una ecuación, y además es útil pues conserva muchas propiedas intuitivas.

§1.1 Propiedades

Transitividad

$$\text{Si } a \equiv b \pmod{k} \text{ y } b \equiv c \pmod{k} \Rightarrow a \equiv c \pmod{k}$$

Suma

$$\text{Si } a \equiv b \pmod{k} \text{ y } x \equiv y \pmod{k} \Rightarrow a + x \equiv b + y \pmod{k}$$

Multiplicación

$$\text{Si } a \equiv b \pmod{k} \text{ y } x \equiv y \pmod{k} \Rightarrow ax \equiv by \pmod{k}$$

Potencia

$$\text{Si } a \equiv b \pmod{k} \Rightarrow a^n \equiv b^n \pmod{k}$$

División

¿Si $ax \equiv bx \pmod{k}$ podemos dividir por x y asegurar que $a \equiv b \pmod{k}$? no se puede, pongamos el ejemplo de la congruencia $3a \equiv 6 \pmod{12}$ no podemos dividir entre 3 y asegurar $a \equiv 2 \pmod{12}$, pues nota que $a \equiv 2, 6$ y $10 \pmod{12}$ también cumplen, es claro que no podemos dividir pues

$ax \equiv bx \pmod{k} \Rightarrow k \mid x(a - b)$ y puede suceder que k y x tengan factores en común

En realidad si se puede dividir pero hay que tener cuidado, la regla es que si

$$ax \equiv bx \pmod{k} \Rightarrow a \equiv b \pmod{\frac{k}{\text{mcd}(x, k)}}$$

Note que si $\text{mcd}(x, k) = 1$ entonces ¡si podemos dividir sin problemas!

§1.2 Ejercicios

Ejercicio 1.2 (Importante)**.** Trata de demostrar o de convercerte de que todas estas propiedades son verdad y que no estoy engañandote, puedes usar que cualquier número a se puede escribir como $a = k \cdot m + r$ donde r es el residuo de a al dividirse por k

Ejercicio 1.3. Demuestra que si $a \equiv b \pmod{n}$ y d es un divisor del número n entonces $a \equiv b \pmod{d}$

Ejercicio 1.4. Encuentra el residuo de 123×29 al dividirse por 13

Ejercicio 1.5. Encuentra el residuo de 13^{2023} al dividirse entre 12

Ejercicio 1.6. Encuentra todos los enteros k tales que $2024 \equiv 17 \pmod{k}$

Ejercicio 1.7. Encuentra el residuo de 2^{2023} al dividirse entre 7

Ejercicio 1.8. ¿Cuál es el dígito de las unidades de $1! + 2! + 3! + \cdots + 2024!$?

Ejercicio 1.9. Demuestra que si $3 \mid x^2 + y^2$ entonces $3 \mid x$ y $3 \mid y$

Ejercicio 1.10. Demuestra que ningún cuadrado perfecto es de la forma $\underbrace{11\cdots 1}_{\text{Solo 1´s}}$

Ejercicio 1.11. Demuestra que $a - b \mid a^n - b^n$ para todo entero n

Ejercicio 1.12. Demuestra que $a + b \mid a^n + b^n$ para todo entero n impar

Ejemplo 1.13 (Regional del Sureste Mexico 2014/4)
Encuentra todas las pareja de enteros positivos m y n tales que

$$n! + 5 = m^3$$

Tutorial.

(a) Si $n \geq 6$ entoces $9 \mid n!$

(b) Entonces si analizamos la ecuación $\pmod 9$ debe suceder que

$$m^3 \equiv 5 \pmod 9$$

(c) Analiza las congruencias de los primos $\pmod 6$

(d) Puedes hacer una tabla como la siguiente y darte cuenta que no existe m tal que m^3 deje residuo 5 al dividirse por 9

m	m^3
0	0
1	1
2	8
3	0
4	1
5	8
6	0
7	1
8	8

Ejemplo 1.14 (OMM 1990/3)
Prueba que $n^{n-1} - 1$ es divisible por $(n-1)^2$ para toda $n > 2$

Tutorial.

(a) Escribe a

$$n^{n-1} - 1 = (n-1)\big((n^{n-2} + n^{n-3} + \cdots n + 1\big)$$

(b) El primer término es $n - 1$ entonces basta probar que $n - 1$ divide a la suma larga

(c) Nota que $n \equiv 1 \pmod n - 1$

§2 Problemas

Problema 2.1. Demuestra que la ecuación $x^2 - 7 = 45y$ no tiene soluciones con $x, y \in \mathbb{Z}$

Problema 2.2. Encuentra el último dígito de los siguiente números

$$\text{a)}2^{2023} \qquad \text{b)}13^{13^{13}} \qquad \text{c)}117^{117}$$

Problema 2.3. Demuestra que para toda $n \in \mathbb{N}$

$$7 \mid 3^{2n+1} + 2^{n+2}$$

Problema 2.4. Se sabe que 2^{29} tiene 9 dígitos distintos, ¿Cuál es el dígito que no tiene?

Problema 2.5. Demuestra que para todo n el número $n^5 + 4n$ es divisible por 5

Problema 2.6. Demuestra que para todo primo $p > 3$ se cumple que $24 \mid p^2 - 1$

Problema 2.7. Demuestra que 2023 divide a la suma

$$1^{2023} + 2^{2023} + 3^{2023} + \cdots 2021^{2023} + 2022^{2023}$$

Problema 2.8. Demuestra los criterios de divisibilidad de 1 al 11 sin inculuir el del 7

Problema 2.9 (USAJMO 2011/1)**.** Encuentre, con prueba, todos los números enteros positivos n para los cuales $2^n + 12^n + 2011^n$ es un cuadrado perfecto.

Problema 2.10. ¿Qué números se pueden ver como diferencia de dos cuadrados perfectos?

Problema 2.11 (Freshman's dream)**.** Demuestra que para todos $a, b \in \mathbb{Z}$, y p un primo se cumple que

$$(a + b)^p \equiv a^p + b^p$$

Problema 2.12 (IMO 1964/1)**.**

(a) Encuentre todos los números enteros positivos n para los cuales $2^n - 1$ es divisible por 7.

(b) Demuestre que no existe un entero positivo n para el cual $2^n + 1$ sea divisible por 7.

Problema 2.13 (IMO 1986/1)**.** Sea d cualquier entero no igual a $2, 5$ o 13. Prueba que podemos escoger dos enteros distintos a y b en el conjunto $\{2, 5, 13, d\}$ tal que $ab - 1$ no es un cuadrado perfecto

Problema 2.14. Demuestra que $n \mid 2^{n!} - 1$ para todo n impar

Problema 2.15 (1 IMO SL/2002)**.** ¿Cuál es el entero positivo más pequeño t tal que existan enteros $x_1, x_2, \ldots, x_t$ con

$$x_1^3 + x_2^3 + \ldots + x_t^3 = 2002^{2002}\,?$$

§3 Hints

2.1. analiza los residuos de los cuadrados $\pmod 5$ y $\pmod 9$

2.2. Simplificalo módulo 10

2.3. $3^{2n+1} \equiv 3 \cdot \left(3^2\right)^n \equiv 3 \cdot 2^n \pmod 7$

2.4. $2^29 \equiv (1 + 2 + \cdots 9) - x \pmod 9$ dónde x es el dígito que falta

2.5. Analiza cada residuo de n y evaluálo en $n^5 + 4n$

2.6. Puedes analizar los residuos que dejan los primos al dividirse entre 8 y 3 y luego analizar a $p^2 - 1$ en esos residuos.

2.7. Junta el último sumando con el primero, el segundo con el penúltimo y así sucesivamente

2.8. un número $n = \overline{a_k a_{k-1} a_{k-2} \cdots a_2 a_1 a_0}$ se puede escribir como $n = 10^k a_k + 10^{k-1} a_{k-1} + \cdots 10 a_1 + 10^0 a_0$

2.9. analiza $\pmod 3$ y luego $\pmod 4$

2.10. Usa $\pmod 4$ y da un ejemplo para los demás

2.11. Binomio de Newton

2.12. Analiza a $n \pmod 3$ y mira que residuos que dejan las potencias de 2 al dividirse por 7

2.13. Asume que $2d-1$, $5d-1$, $13d-1$ son todos cuadrados, analízalos módulo 4 y luegó mod 5

2.14. Demuestra que existe un entero d tal que $2^d \equiv 1 \pmod n$ y $d \leq n$

2.15. La respuesta es $t = 4$ usa $\pmod 9$ para demostrar que $t \leq 4$ no es alcanzable