

# Modulos

## OMMJAL

EMMANUEL BUENROSTRO

3 August 2025

### §1 Principios

#### §1.1 Definición

**Definition 1.1.**  $a \equiv b \pmod{n}$  si  $n \mid a - b$

**Propiedades:** Si  $a \equiv b \pmod{n}$  y  $c \equiv d \pmod{n}$ :

1.  $a + c \equiv b + d \pmod{n}$
2.  $a - c \equiv b - d \pmod{n}$
3.  $ac \equiv bd \pmod{n}$
4.  $a^x \equiv b^x \pmod{n}$

Y en general cualquier operación con suma, resta, multiplicación se puede hacer.

**Remark.** Podemos notar que no se menciona la división, más adelante tratamos con esta.

#### §1.2 Lema de la Division de Euclides

Tomar  $a \bmod n$  en realidad lo que estamos haciendo es asignarle al entero  $a$  algun valor de  $\{0, 1, \dots, n-1\}$ , este valor es el residuo que deja  $a$  al dividirlo entre  $n$ , entonces vamos a demostrar que con la definición que tenemos si asignamos **exactamente** un valor de  $\{0, 1, \dots, n-1\}$

Vamos a considerarnos el conjunto de multiplos de 5 no negativos.

$$\{0, 5, 10, 15, 20, 25, 30, 35, 40, 45, 50, 55, \dots\}$$

Entonces, ¿Qué pasa con los números como 32, 33 que no estan en ese conjunto?, pues estan en medio entre 30 y 35, entonces podemos escribirlos como

$$32 = 5 \times 6 + 2$$

$$33 = 5 \times 6 + 3$$

$$34 = 5 \times 6 + 4$$

$$35 = 5 \times 6 + 5$$

$$36 = 5 \times 6 + 6$$

Pero 35 y 36 ya no estan en medio de 30 y 35 entonces mejores formas de escribirlos seria

$$35 = 5 \times 7 + 0$$

$$36 = 5 \times 7 + 1$$

Siguiendo esto obtenemos el lema:

**Lemma 1.2** (Lema de la Division de Euclides)

Para cualesquiera enteros  $a, b$  podemos encontrar **únicos** enteros  $q, r$  tales que

$$b = aq + r$$

con  $0 \leq r < a$ , donde  $q$  es el cociente y  $r$  el residuo.

*Proof.* Para ver que existen, unicamente haz este proceso: Inicia con  $r = b$  y  $q = 0$ , entonces mientras  $r \geq a$  restale  $a$  a  $r$  y sumale 1 a  $q$ , esto sigue siendo igual a  $b$ :

$$b = aq + r = aq + a + r - a = a(q + 1) + (r - a)$$

Entonces cuando finalmente  $r < a$  tienes unos enteros  $q, r$  que cumplan.

Ahora para ver que son únicos, haremos contradicción, si asumes que tienes dos parejas  $(q_1, r_1)$  y  $(q_2, r_2)$  que cumplen, entonces

$$aq_1 + r_1 = b = aq_2 + r_2$$

$$aq_1 - aq_2 = r_2 - r_1$$

$$a(q_1 - q_2) = r_2 - r_1$$

Entonces  $r_2 - r_1$  es múltiplo de  $a$ , pero como  $0 \leq r_1, r_2 < a$  entonces  $-a < r_2 - r_1 < a$ , y la unica posibilidad de que sea multiplo de  $a$  es que  $r_2 - r_1 = 0$  y  $r_1 = r_2$ , entonces  $aq_1 = aq_2 \Rightarrow q_1 = q_2$  y son la misma pareja, contradicción. □

Entonces  $b \equiv r \pmod{a}$  porque  $a \mid aq = b - r$ , y como  $r$  es único, entonces si asignamos exactamente un valor a cada entero positivo  $b$  modulo  $a$ .

En particular si  $x = aq_1 + r_1, y = aq_2 + r_2$  entonces  $x \equiv y \pmod{a} \iff r_1 = r_2$ .

**Exercise 1.3.** Prueba que para los negativos tambien sucede.

**Remark.** Usar modulos negativos suele servir para operaciones, por ejemplo  $n - 1 \equiv -1 \pmod{n}$ , entonces  $(n - 1)^2 \equiv (-1)^2 \equiv 1 \pmod{n}$ , algo que sin usar el modulo negativo sería bastante mas complejo.

### §1.3 ¿Cómo se usa?

Los modulos tienen distintos usos, creo que los dos más usuales es cosas directamente relacionadas con la divisibilidad (o por ejemplo calcular algun modulo), o el poder resolver distintas ecuaciones diofantinas (con enteros) al acotar bastante en que casos se puede y no se puede.

Veamos unos problemas de ejemplo.

#### Example 1.4

Encuentra que valores de  $n$  se tiene que  $3 \mid n^2 + 1$ .

*Solution.* Como queremos que  $3 \mid n^2 + 1$  entonces queremos que  $3 \mid n^2 - (-1)$  y entonces quieres  $n^2 \equiv -1 \pmod{3}$ .

Otra forma de ver esto, es que si  $3 \mid n^2 + 1$  entonces

$$\begin{aligned} n^2 + 1 &\equiv 0 \pmod{3} \\ n^2 &\equiv -1 \pmod{3} \end{aligned}$$

Puedes moverlo como si fuera una ecuación normal.

Entonces ahora vamos a ver todos los posibles casos de  $n^2 \pmod{3}$ .

| $n \pmod{3}$ | $n^2 \pmod{3}$ |
|--------------|----------------|
| 0            | 0              |
| 1            | 1              |
| 2            | $4 \equiv 1$   |

Entonces podemos notar que no hay ningun caso donde  $n^2 \equiv -1 \pmod{3}$  entonces no hay soluciones.

□

#### Example 1.5

¿Cuál es el residuo de  $2^{2025}$  al dividirlo entre 7?

*Solution.* Vamos a ver los primeros casos de potencias de 2 modulo 7.

$$2^1 \equiv 2, 2^2 \equiv 4, 2^3 \equiv 1, 2^4 \equiv 2$$

Entonces podemos ver que volvemos al 2, pero el residuo de una potencia de 2 depende totalmente del residuo anterior, entonces si se repite una se va a hacer un ciclo, en este caso el ciclo es

$$2 \rightarrow 4 \rightarrow 1$$

Entonces ahora lo que nos importa es ver cuanto es 2025 modulo 3 (porque el ciclo es de tamaño 3), y como  $2025 \equiv 0 \pmod{3}$  entonces  $2^{2025} \equiv 1 \pmod{7}$ . □

---

"Aquí mataron mucha gente"

---

El líder de Perú en Tiananmen Square

## §2 Problemas

### §2.1 Calcular mods

**Problem 2.1.** Obten tres números que sean congruentes a  $a \pmod{m}$  para:

- $a = 2, m = 3$
- $a = -1, m = 11$
- $a = 52, m = 17$
- $a = -16, m = 6$

**Problem 2.2.** Calcula  $a$  donde  $a \in \{0, 1, \dots, 6\}$  y:

$$11 \cdot 18 \cdot 2322 \cdot 13 \cdot 19 \equiv a \pmod{7}$$

**Problem 2.3.** Demuestra que si  $x \equiv 11 \pmod{24}$  entonces  $3x \equiv 1 \pmod{8}$

**Problem 2.4.** Si en este momento son las 10 de la mañana, ¿Qué hora será en 2500 horas?

**Problem 2.5.** Encuentra el último dígito de  $2 \times 325 + 3 \times 8^7 \times 5104 + 123^5$ .

**Problem 2.6.** Resuelve para  $x$ :

1.  $12x \equiv 1 \pmod{23}$
2.  $x^2 \equiv 1 \pmod{23}$
3.  $x^2 \equiv 1 \pmod{8}$
4.  $x(x+5) \equiv 6 \pmod{10}$

## §2.2 Usar mods pt 1

**Problem 2.7.** ¿Para cuáles enteros  $n$  se tiene que  $4 \mid 3n^3 + 1$  ?

**Problem 2.8.** Demuestra el criterio de divisibilidad del 3, el cual dice que un número es divisible entre 3 si la suma de sus dígitos es divisible entre 3.

**Problem 2.9.** Demuestra el criterio de divisibilidad del 4, el cual dice que un número es múltiplo de 4 si el número formado por sus dos últimos dígitos es múltiplo de 4.

**Problem 2.10.** Demuestra el criterio de divisibilidad de  $2^n$ , el cual dice que un número es divisible por  $2^n$  si el número formado por los últimos  $n$  dígitos es múltiplo de  $2^n$ .

**Problem 2.11.** Demuestra que un número es divisible por  $5^n$  si el número formado por los últimos  $n$  dígitos es múltiplo de  $5^n$ .

**Problem 2.12.** Encuentra los enteros  $n$  tales que  $n^2 \equiv 1 \pmod{8}$ .

**Problem 2.13.** Encuentra los enteros  $x$  tales que  $12x \equiv 1 \pmod{23}$ .

**Problem 2.14.** Para un entero positivo  $n$ , sea  $A(n)$  la suma de los dígitos de  $n$ , por ejemplo  $A(24135) = 5 + 3 + 1 + 4 + 2$ . Prueba que  $n \equiv A(n) \pmod{9}$ .

**Problem 2.15.** Se tienen 2003 tarjetas numeradas del 1 al 2003 y colocadas hacia abajo en orden en un mójon (la tarjeta con el 1 aparece arriba). Sin mirar se quitan tres tarjetas consecutivas hasta que solo quedan dos tarjetas. ¿Es posible que haya quedado la tarjeta con el 1002?

**Problem 2.16.** ¿Puede 222222 ser un cuadrado perfecto?

## §2.3 Usar mods pt2

**Problem 2.17.** Demuestra que  $a - b \mid a^n - b^n$  para  $n$  entero no negativo.

**Problem 2.18.** Demuestra que los números primos mayores a 3 son 1 o 5 (mod 6).

**Problem 2.19.** Demuestra que si para  $x, y$  enteros entonces si  $3 \mid x^2 + y^2$  se tiene que  $3 \mid x$  y  $3 \mid y$ .

**Problem 2.20.** Demuestra que si  $7 \mid x^3 + y^3 + z^3$  entonces 7 divide a alguno de  $x, y, z$ .

**Problem 2.21.** Demuestra que si  $a^2 \equiv b^2 \pmod{p}$  donde  $p$  es primo entonces  $a \equiv b \pmod{p}$  o  $a \equiv -b \pmod{p}$ .

**Problem 2.22.** Demuestra que un número es multiplo de 7 si el número formado por los numeros excepto el ultimo digito - el doble de el ultimo digito es multiplo de 7.

**Problem 2.23.** Encuentra todas las tripletas de enteros positivos  $(k, m, n)$  tal que  $7^k = 9^m + 2^n$ .

**Problem 2.24.** Para un entero positivo  $n$ , sea  $A(n)$  la suma alternada de los digitos de  $n$ , por ejemplo  $A(24135) = 5 - 3 + 1 - 4 + 2$ . Prueba que  $n \equiv A(n) \pmod{11}$ .

**Problem 2.25.** Prueba que si  $p$  y  $8p - 1$  son ambos primos entonces  $8p + 1$  es compuesto.

**Problem 2.26.** Prueba que

$$(x - 1^2)(x - 2^2)(x - 3^2)(x - 4^2)(x - 5^2)(x - 6^2) \equiv x^6 - 1 \pmod{13}$$

**Problem 2.27.** Sea  $S$  la suma siguiente:

$$S = 1 + 2 + 3 + \dots + 2025$$

Encuentra el residuo cuando  $S$  es dividido entre 7.

**Problem 2.28 (AIME 2010/1).** Encuentra el residuo cuando  $9 \times 99 \times \dots \times 99 \dots 9$  con 999 9's al final es dividido entre 1000.

**Problem 2.29.** Demuestra que

$$2025 \mid 1^{2025} + 2^{2025} + 3^{2025} + \dots + 2025^{2025}$$

**Problem 2.30.** Determina todas las soluciones enteras no negativas  $(n_1, n_2, \dots, n_{14})$  a

$$n_1^4 + n_2^4 + \dots + n_{14}^4 = 1599$$

**Problem 2.31.** La secuencia de enteros positivos  $a_1, a_2, \dots$  esta definida de la siguiente forma:  $a_1 = 2019, a_2 = 2020, a_3 = 2021$  y para todo  $n \geq 1$

$$a_{n+3} = 5a_{n+2}^6 + 3a_{n+1}^3 + a_n^2$$

Prueba que la secuencia no contiene números de la forma  $m^6$  donde  $m$  es un entero positivo.

## §2.4 Mas problemas

Puede que ocupes mas cosas (Como Fermat o Euler) aqui.

**Problem 2.32.** Encuentra todos los primos  $p$  tales que  $13^{2p-1} + 17$  es divisible por  $p$ .

**Problem 2.33** (PUMaC 2012 N A3). Definimos la secuencia  $\{x_n\}$  de la siguiente forma:  $x_1 \in \{5, 7\}$  y para todo  $k \geq 1, x_{k+1} \in \{5^{x_k}, 7^{x_k}\}$ . Por ejemplo los posibles valores de  $x_3$  son:  $5^{5^5}, 5^{5^7}, 5^{7^5}, 5^{7^7}, 7^{5^5}, 7^{5^7}, 7^{7^5}$ . ¿Cuál es la suma de todos los posibles valores para los ultimos dos digitos de  $x_{2012}$ .

**Problem 2.34** (IMOSL 2000 N1). Encuentra todos los enteros positivos  $n \geq 2$  que cumplen que para todos los enteros positivos coprimos con  $n$   $a, b$  se cumple que

$$a \equiv b \pmod{n} \text{ si y solo si } ab \equiv 1 \pmod{n}$$

### §3 ¿Y la división?

#### §3.1 Definición de inverso

Al momento de hacer la división ocupamos la existencia de *inversos*. Al hacer división en los reales, si queremos dividir  $x$  entre  $y$ , lo que en realidad estamos haciendo es multiplicar  $x$  por el *inverso* de  $y$  el cual es representado como  $\frac{1}{y}$ .

¿Y qué cumplen los inversos? En los reales lo que cumplen es que el inverso de un real  $a$ , es aquel que cumple

$$a \cdot a^{-1} = 1$$

Entonces eso justo coincide con lo que conocemos de  $\frac{1}{a}$ .

Entonces si estamos trabajando mod  $n$ , un entero  $a$  tiene inverso si existe un  $a^{-1}$  con

$$a \cdot a^{-1} \equiv 1 \pmod{n}$$

Y este existe si y solo si  $\gcd(a, n) = 1$ .

Podemos ver un ejemplo cuando  $n = 7$ .

| Número | Inverso mod 7 |
|--------|---------------|
| 1      | 1             |
| 2      | 4             |
| 3      | 5             |
| 4      | 2             |
| 5      | 3             |
| 6      | 6             |

Mostrandonos que efectivamente en este caso si existen, entonces vamos a demostrar esto.

#### §3.2 Maquinaria a usar



## §4 Teoremitas útiles

### Theorem 4.1 (Pequeño Teorema de Fermat)

Si  $p$  es primo y  $a \in \mathbb{Z}$  entonces

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

Tambien generalmente conocido como

### Theorem (Pequeño Teorema de Fermat)

Si  $p$  es primo y  $a \in \mathbb{Z}$  y  $(a, p) = 1$  entonces

$$a^{p-1} \equiv 1 \pmod{p}$$

*Proof.* Notemos que para  $a$  tal que  $p|a$  si cumple porque  $a^p \equiv 0 \equiv a \pmod{p}$ .

Para los  $a$  con  $(p, a) = 1$ . se tiene que

$$\{a, 2a, 3a, \dots, (p-1)a\}$$

es una permutación de

$$\{1, 2, 3, \dots, p-1\}$$

en mod  $p$ .

**Prueba.** Todos los números  $a, 2a, 3a, \dots, (p-1)a$  tiene distintos modulos  $p$ , ya que si hay dos iguales  $ia$  y  $ja$  con  $i \neq j$  entonces

$$ia - ja = a(i - j) \equiv 0 \pmod{p}$$

y como  $(a, p) = 1$  entonces  $i - j \equiv 0 \pmod{p} \Rightarrow i \equiv j \pmod{p}$ , pero  $1 \leq i, j \leq p-1$  entonces  $i = j$ , una contradicción. Entonces si es una permutación.

Asi que si multiplicamos todos se tiene que

$$a \cdot 2a \cdot 3a \cdots (p-1)a \equiv 1 \cdot 2 \cdots (p-1) \pmod{p}$$

entonces

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

$$\Rightarrow a^{p-1} \equiv 1 \pmod{p}$$

□