Congruencias modulares

Este teónico de Matemática Discreta 2 se cla los Lumes y Miéncoles a las 11:00. Nótese que no decimos que la clase del Miéncoles se da a las 11 + 48 = 59 honas. Esto último resultanía poco pnáctico. La convención de dividin los días em 24 honas hace que los números 11 y 59 Repnesentem la misma hona: las 11:00. Pon otno lado, note que 11 y 59 tiemem el mismo Resto al dividin pon 24,

$$11 = 0 \cdot 24 + 11$$
$$59 = 2 \cdot 24 + 11.$$

Gemenalizando, cualquien número de la fonma $24k + 11$ Repnesenta las 11:00 demtno del sistema de numenación bajo el cual se Rige el Reloj. La teonía de congruencias modulanes nos ayudaná a modelan ésta y otnas convenciones conocidas.

Definición: Sea $n \in \mathbb{Z}$ fijo, y $a, b \in \mathbb{Z}$, dinemos que **a es congruente con b módulo n**, denotado pon

$$a \equiv b \pmod{n},$$

si $n \mid (a-b)$.

Observaciones:

① $a \equiv b \pmod 0$ si y solamente si $a = b$

② $a \equiv b \pmod n$ si y solamente si $a \equiv b \pmod{-n}$

③ $a \equiv 0 \pmod n$ si y solamente si $n \mid a$.

④ Para todo $a, b \in \mathbb{Z}$, existe $0 \leq r < |b|$ tal que $a \equiv r \pmod b$.

Ejemplo:

$59 \equiv 11 \pmod{24}$.

Las horas del día se cuentan módulo 24.

Los días de la semana se cuentan módulo 7.

Comencemos caracterizando el concepto de congruencia.

Proposición: $a \equiv b \pmod n$ si y solamente si a y b tienen el mismo resto al dividir por n.

- **Demostración:** Supongamos primero que $a \equiv b \pmod n$. Luego, existe $q \in \mathbb{Z}$ tal que $a - b = q \cdot n$. Por otro lado, por el teorema de la división entera, tenemos que

$a = k \cdot n + r$ con $0 \leq r, r' < |n|$ únicos.

$b = k' \cdot n + r'$

Luego, $a - b = (k - k')n + (r - r')$

$q \cdot n = (k - k')n + (r - r')$

$(q - k + k')n = r - r'$,

donde $0 \leq r < |m|$ y $0 \leq r' < |m|$ implica

$$-|m| < r - r' < |m|.$$

Entonces, al ser $r - r' = (q - k + k')m$, se tiene que $r - r' = 0$.

Ahora supongamos que a y b tienen el mismo resto al dividir por m.

$$a = k \cdot m + r$$
$$b = k' \cdot m + r$$

Luego, $a - b = (k - k')m$, de donde $m \mid (a - b)$, es decir, $a \equiv b \pmod{m}$. ■

Definición: Denotamos por $[b]_m$ al conjunto de todos los enteros congruentes con b módulo m.

$$[b]_m := \{ a \in \mathbb{Z} \mid a \equiv b \pmod{m} \}.$$

A b se le conoce como un representante de $[b]_m$

Observación: Por la proposición anterior,

$$[b]_m = \{ \ldots, b - 2m, b - m, b, b + m, b + 2m, \ldots \}.$$

Ejemplos:

① $[0]_2$ = conjunto de números pares.

$[1]_2$ = conjunto de números impares.

② $[0]_n$ = conjunto de múltiplos de n.

Proposición: Las siguientes afirmaciones se cumplen:

1) Reflexividad: $a \equiv a \pmod{n}$ para todo $a \in \mathbb{Z}$.

2) Simetría: Para todo $a, b \in \mathbb{Z}$, se tiene que $a \equiv b \pmod{n}$ implica que $b \equiv a \pmod{n}$.

3) Transitividad: Para todo $a, b, c \in \mathbb{Z}$, se tiene que si $a \equiv b \pmod{n}$ y $b \equiv c \pmod{n}$, entonces $a \equiv c \pmod{n}$.

· Demostración:

1) $n \mid (a-a)$, por lo que $a \equiv a \pmod{n}$.

2) Supongamos $a \equiv b \pmod{n}$, es decir, $a-b = q \cdot n$ para algún $q \in \mathbb{Z}$. Luego, $b-a = (-q) \cdot n$, es decir, $n \mid (b-a)$. Por lo tanto, $b \equiv a \pmod{n}$.

3) Supongamos $a \equiv b \pmod{n}$ y $b \equiv c \pmod{n}$. Luego, existen $q, k \in \mathbb{Z}$ tales que:

$a-b = q \cdot n$ y $b-c = k \cdot n$.

Así, $a-c = (a-b)+(b-c) = (q+k)n$, de donde $n \mid (a-c)$.

La proposición anterior dice que $\equiv \pmod m$ es una Relación de equivalencia.

$[b]_m$ es la clase de equivalencia de b.

Ejemplo: $[0]_3 = \{\dots, -9, -6, -3, 0, 3, 6, 9, \dots\} = [3]_3$

$[1]_3 = \{\dots, -8, -5, -2, 1, 4, 7, \dots\} = [4]_3$

$[2]_3 = \{\dots, -10, -7, -4, -1, 2, 5, 8, \dots\} = [5]_3$

Note que $[0]_3 \cap [1]_3 = \emptyset$

$[1]_3 \cap [2]_3 = \emptyset$

$[2]_3 \cap [0]_3 = \emptyset$

y $\mathbb{Z} = [0]_3 \cup [1]_3 \cup [2]_3$

Teorema: Las siguientes afirmaciones se cumplen:

1) $[a]_m = [b]_m$ si y solamente si $a \equiv b \pmod m$.

2) $\mathbb{Z} = [0]_m \cup [1]_m \cup \dots \cup [m-1]_m$. Más aún, esta unión es disjunta.

· **Demostración**

1) Supongamos que $[a]_m = [b]_m$. Luego, $a \in [b]_m$, de donde $a \equiv b \pmod m$. Ahora, si $a \equiv b \pmod m$, se tiene $a \in [b]_m$. Luego, para todo $c \in [a]_m$, es decir $c \equiv a \pmod m$, se obtiene por transitividad que $c \equiv b \pmod m$, por lo cual $c \in [b]_m$ para todo $c \in [a]_m$, es decir, $[a]_m \subseteq [b]_m$.

La contención $[a]_m \supseteq [b]_m$ se prueba de manera análoga.

2) Sea $a \in \mathbb{Z}$. Por el teorema de la división entera, existen $q, r \in \mathbb{Z}$ únicos tales que $a = qm + r$ con $0 \leq r < |m|$. Así, $a \equiv r \pmod{m}$, por lo cual

$$a \in [r]_m \subseteq [0]_m \cup [1]_m \cup \cdots \cup [m-1]_m.$$

Por lo tanto, $\mathbb{Z} = [0]_m \cup [1]_m \cup \cdots \cup [m-1]_m$.

Por la parte 1), la unión anterior es disjunta. ∎

Ejemplo: ¿Si ahora son las 16:00, qué hora será dentro de 200 horas?

Sea h la hora buscada. Entonces,

$$h \equiv 16 + 200 \pmod{24}$$

$$h \equiv 216 \pmod{24}$$

Como $24 \mid 216$, tenemos que $216 \equiv 0 \pmod{24}$.

Por transitividad, $h \equiv 0 \pmod{24}$.

Por lo tanto, dentro de 200 horas serán las 00:00.

Proposición (propiedades de las congruencias):
Sean $a, b, c, d, m \in \mathbb{Z}$. Las siguientes afirmaciones se cumplen:

1) Si $a \equiv b \pmod{m}$ entonces $a+m \equiv b+m \pmod{m}$ y $am \equiv bm \pmod{m}$

2) Si $a \equiv b \pmod{m}$ y $c \equiv d \pmod{m}$, entonces $a+c \equiv b+d \pmod{m}$ y $ac \equiv bd \pmod{m}$.

3) Si $a \equiv b \pmod{m}$ entonces $a^k \equiv b^k \pmod{m}$ para todo $k>0$.

4) **Congruencia polinomial:** Dado el polinomio

$$f(x) = c_k x^k + c_{k-1} x^{k-1} + \cdots + c_1 x + c_0$$

con $k>0$ y $c_0, c_1, \ldots, c_{k-1}, c_k \in \mathbb{Z}$, si $a \equiv b \pmod{m}$ entonces $f(a) \equiv f(b) \pmod{m}$.

5) Si $am \equiv bm \pmod{n}$ y $mcd(m,n)=1$, entonces $a \equiv b \pmod{n}$, donde $m \neq 0$

6) Si $m \mid n$ y $am \equiv bm \pmod{n}$, entonces $a \equiv b \left(\mod \frac{n}{m}\right)$, donde $m \neq 0$.

7) Si $am \equiv bm \pmod{n}$ entonces

$$a \equiv b \left(\mod \frac{n}{mcd(m,n)}\right), \text{ donde } m \neq 0.$$

Demostración:

1) $a \equiv b \pmod{n} \Rightarrow n \mid (a-b)$.

Como $a-b = (a+m)-(b+m)$, tenemos que

$n \mid [(a+m)-(b+m)]$, es decir, $a+m \equiv b+m \pmod{n}$.

Por otro lado, $n \mid (a-b) \Rightarrow n \mid m(a-b)$, es decir,

$n \mid (am-bm)$. Entonces, $am \equiv bm \pmod{n}$.

2) $\left.\begin{array}{l} a \equiv b \pmod{n} \Rightarrow n \mid (a-b) \\ c \equiv d \pmod{n} \Rightarrow n \mid (c-d) \end{array}\right\} \Rightarrow n \mid [(a-b)+(c-d)]$.

Luego, $n \mid [(a+c)-(b+d)]$, es decir,

$$a+c \equiv b+d \pmod{n}.$$

Por otro lado, usando la parte 1) obtenemos

$$\left.\begin{array}{l} a \equiv b \pmod{n} \Rightarrow ac \equiv bc \pmod{n} \\ c \equiv d \pmod{n} \Rightarrow bc \equiv bd \pmod{n} \end{array}\right\} \Rightarrow ac \equiv bd \pmod{n},$$

por la propiedad de transitividad.

3) Se sigue de aplicar k veces la parte 2).

4) Supongamos $a \equiv b \pmod{n}$. Por la parte 3), tenemos $a^2 \equiv b^2 \pmod{n}, \ldots, a^k \equiv b^k \pmod{n}$. Luego, por la parte 1), lo anterior implica que

$$c\,a \equiv c\,b \pmod{n}, \ldots, c_k a^k \equiv c_k b^k \pmod{n}.$$

Por la parte 2), obtenemos

$$c_k a^k + \cdots + c_2 a^2 + c_1 a \equiv c_k b^k + \cdots + c_2 b^2 + c_1 b \pmod{n}.$$

Finalmente, la parte 1) nos permite sumar c_0 a la congruencia anterior, por lo cual

$$c_k a^k + \cdots + c_2 a^2 + c_1 a + c_0 \equiv c_k b^k + \cdots + c_2 b^2 + c_1 b + c_0 \pmod{n},$$

es decir,

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

5) $am \equiv bm \pmod{n} \Rightarrow n \mid m(a-b)$.

Como $\operatorname{mcd}(m, n) = 1$, por el Lema de Euclides se tiene que $n \mid (a-b)$, es decir, $a \equiv b \pmod{n}$.

6) $am \equiv bm \pmod{n} \Rightarrow n \mid m(a-b) \Rightarrow \exists\, q \in \mathbb{Z} \;/\; m(a-b) = q \cdot n$

Como $m \neq 0$ y $m \mid m$, se tiene que $\frac{m}{m} \in \mathbb{Z}$ y

$a - b = q \cdot \frac{n}{m}$, es decir, $\frac{n}{m} \mid (a-b)$.

Entonces, $a \equiv b \left(\text{mód } \frac{n}{m}\right)$.

7) Sea $d = \operatorname{mcd}(m, n)$.

$am \equiv bm \pmod{n} \Rightarrow n \mid m(a-b) \Rightarrow m(a-b) = q \cdot n$ para algún $q \in \mathbb{Z}$.

$\frac{m}{d}, \frac{n}{d} \in \mathbb{Z}$. Luego, $\frac{m}{d}(a-b) = q \cdot \frac{n}{d}$,

de donde $\frac{n}{d} \mid \frac{m}{d}(a-b)$. Como $\operatorname{mcd}\left(\frac{m}{d}, \frac{n}{d}\right) = 1$, se tiene por el Lema de Euclides que

$\frac{n}{d} \mid (a-b)$, es decir, $a \equiv b \left(\text{mód } \frac{n}{d}\right)$. ∎

Ejemplo:

① Halle el resto de dividir 37^{7541} entre 7.

$35 \equiv 0 \pmod 7$

$37 \equiv 2 \pmod 7$

$37^{7541} \equiv 2^{7541} \pmod 7$

Por otro lado, $7541 = 3 \cdot 2513 + 2$, y además

$2^3 \equiv 1 \pmod 7 \Rightarrow (2^3)^{2513} \equiv 1^{2513} \pmod 7$

$\Rightarrow 2^{7539} \equiv 1 \pmod 7$

$\Rightarrow 2^{7541} \equiv 4 \pmod 7$

Por transitividad, $37^{7541} \equiv 4 \pmod 7$

② ¿Qué día de la semana fue el 25 de agosto de 1825?

Sabemos que el 25/08/2023 es un día viernes, por lo cual debemos contar el número de días transcurridos desde el 25/08/1825 al 25/08/2023. Para empezar, han transcurrido 198 años, lo cual da lugar a

$$198 \cdot 365 \text{ días.}$$

Al número anterior le agregamos los días de desfase causados por los años bisiestos. Entre 1825 y 2023 han habido 48 años bisiestos, por lo cual han transcurrido $48 + 198 \cdot 365$ días desde el 25/08/1825 hasta el 25/08/2023.

Como los días de la semana se cuentan módulo 7, debemos hallar el resto de dividir por 7 el número anterior, para poder determinar el día de la fecha 25/08/1825.

$$365 \equiv 1 \pmod 7$$

$$198 \cdot 365 \equiv 198 \pmod 7$$

Por otro lado, $198 \equiv 2 \pmod 7$. Luego,

$$198 \cdot 365 \equiv 2 \pmod 7$$

$$48 + 198 \cdot 365 \equiv 50 \pmod 7,$$

donde $50 \equiv 1 \pmod 7$. Por lo tanto,

$$48 + 198 \cdot 365 \equiv 1 \pmod 7,$$

es decir, ha transcurrido un día módulo 7 desde el 25/08/1825 hasta el 25/08/2023, por lo que podemos concluir que el 25/08/1825 fue Jueves.

Criterios de divisibilidad

Sea $a = (a_m a_{m-1} \cdots a_1 a_0)_{10} \in \mathbb{N}$. Entonces,

1) a es divisible por 3 si y solamente si $a_0 + a_1 + \cdots + a_{m-1} + a_m$ es divisible por 3.

2) a es divisible por 9 si y solamente si $a_0 + a_1 + \cdots + a_{m-1} + a_m$ es divisible por 9.

Probaremos solamente el criterio de divisibilidad por 9, ya que el del 3 se demuestra de forma análoga.

Demostración: Primero veamos que a y $a_0 + a_1 + \cdots + a_m$ tienen el mismo resto al ser divididos por 9, es decir,

$$a \equiv (a_0 + a_1 + \cdots + a_m) \pmod 9. \quad (*)$$

Tenga en cuenta además que

$$a = a_m \cdot 10^m + \cdots + a_k 10^k + \cdots + a_1 \cdot 10 + a_0.$$

Para probar la consecuencia $(*)$, empezamos notando que

$$10 \equiv 1 \pmod 9.$$

Luego, por propiedades de las congruencias, para cada $k \in \{0, 1, \ldots, n\}$ se tiene que

$$10^k \equiv 1^k \pmod 9$$

$$10^k \equiv 1 \pmod 9$$

$$a_k \cdot 10^k \equiv a_k \cdot 1 \pmod 9$$

$$a_k 10^k \equiv a_k \pmod 9.$$

Entonces, por la propiedad de congruencia polinomial, tenemos que

$$a_m 10^m + \cdots + a_k 10^k + \cdots + a_1 10 + a_0 \equiv a_m + \cdots + a_k + \cdots + a_1 + a_0 \pmod 9$$

$$a \equiv (a_m + \cdots + a_1 + a_0) \pmod 9$$

Si $9 \mid a$, entonces $9 \mid (a_m + \cdots + a_1 + a_0)$, ya que a y $a_m + \cdots + a_1 + a_0$ tienen el mismo resto al dividirse por 9. De manera similar, si $9 \mid (a_m + \cdots + a_1 + a_0)$ entonces $9 \mid a$. ■

Ecuaciones lineales con congruencia de una variable

Anteriormente resolvimos el problema de hallar $x \in \mathbb{Z}$ tal que

$$ax \equiv 1 \pmod{n}.$$

Sabemos que no siempre hay solución, como es el caso de

$$2x \equiv 1 \pmod{4}.$$

Podemos generalizar el problema de la siguiente forma: dados $a, b \in \mathbb{Z}$, y $n \in \mathbb{Z}$ fijo, queremos hallar todos los $x \in \mathbb{Z}$ tales que

$$ax \equiv b \pmod{n},$$

dentro del caso en el cual tales x existen.

Para tal fin, ayuda un poco recordar la teoría de ecuaciones diofánticas. Lo haremos mediante un ejemplo.

Ejemplo: Determine si $9x \equiv 1 \pmod{3}$ tiene solución. De ser el caso, encuéntrelas.

$9x \equiv 1 \pmod{3} \iff 9x - 1 = 3y$ para algún $y \in \mathbb{Z}$

Es decir, $9x \equiv 1 \pmod{3}$ tiene solución si la ecuación diofántica $9x - 3y = 1$ tiene solución. Como $\text{mcd}(9, 3) = 3 \nmid 1$, tenemos que $9x - 3y = 1$ no tiene solución. Por lo tanto, $9x \equiv 1 \pmod{3}$ no tiene solución.

- Determine si $9x \equiv 1 \pmod{10}$ tiene solución. En caso afirmativo, encuéntrelas.

$9x \equiv 1 \pmod{10} \iff$ Existem $x, y \in \mathbb{Z}$ tales que

$$9x - 10y = 1$$

$$\iff \text{mcd}(9, 10) = 1 \mid 1.$$

Tenemos entonces que $9x \equiv 1 \pmod{10}$ tiene solución. Como

$$9(-1) - 10(-1) = 1,$$

tenemos que todas las soluciones de $9x \equiv 1 \pmod{10}$ son de la forma

$$x = -1 + k \cdot \frac{(-10)}{\text{mcd}(9, 10)}$$

$$x = -1 - 10k, \text{ con } k \in \mathbb{Z}.$$

Como dato adicional, vemos que si $-1 - 10k_1$ y $-1 - 10k_2$ son soluciones de $9x \equiv 1 \pmod{10}$, entonces $-1 - 10k_1 \equiv -1 - 10k_2 \pmod{10}$.

Formalicemos las observaciones de los ejemplos anteriores en resultados. Básicamente, lo que va a ocurrir es una reescritura de los resultados de la teoría de ecuaciones diofánticas en la notación de congruencias modulares.