Congruencias

Alan Reyes-Figueroa

Teoría de Números

(Aula 07) 03.agosto.2021

Hacen su aparición en la obra de Gauss, *Disquisitiones Arithmeticae* (1801).

Definición

Sean $a, b \in \mathbb{Z}$, $n \in \mathbb{N}$, con $n > 1$. Definimos $a \equiv b \pmod{n}$ si, y sólo si, $n \mid a - b$. En ese caso, decimos que a ***es congruente con*** *b* ***módulo*** *n, o que a y b* ***son congruentes módulo*** *n.*
En caso contrario, escribirmos $a \not\equiv b \pmod{n}$, y decimos que a y n no son congruentes módulo n.

Ejemplo: $17 \equiv 3 \pmod{7}$, $\quad 11 \equiv -4 \pmod{3}$.

Ejemplo: $x^2 + y^2 \not\equiv 3 \pmod{4}$.
Solución: $x \equiv 0, 2 \pmod{4} \ \Rightarrow \ x^2 \equiv 0 \pmod{4}$; $x \equiv \pm 1 \pmod{4} \ \Rightarrow \ x^2 \equiv 1 \pmod{4}$.
Haciendo todas las combinaciones posibles, vemos que $x^2 + y^2 \equiv 0 + 0$ ó $0 + 1$ ó $1 + 1 \pmod{4}$, esto es, $x^2 + y^2 \equiv 0, 1, 2 \pmod{4}$.
Portanto $x^2 + y^2 \not\equiv 3 \pmod{4}$.

Propiedades (Propiedades de las Congruencias)

Para cualesquiera enteros $a, b, c, d, k, n \in \mathbb{Z}$, $n > 1$. *se tiene.*

1. *(Reflexividad)* $a \equiv a \pmod{n}$,
2. *(Simetría) si* $a \equiv b \pmod{n}$, *entonces* $b \equiv a \pmod{n}$,
3. *(Transitividad) Si* $a \equiv b \pmod{n}$, $b \equiv c \pmod{n}$, *entonces* $a \equiv c \pmod{n}$,
4. *(Compatibilidad con suma y resta)*
$$\begin{cases} a \equiv b \pmod{n} \\ c \equiv d \pmod{n} \end{cases} \Rightarrow \begin{cases} a + c \equiv b + d \pmod{n}, \\ a - c \equiv b - d \pmod{n}, \end{cases}$$
5. *(Compatibilidad con producto)*
$$\begin{cases} a \equiv b \pmod{n} \\ c \equiv d \pmod{n} \end{cases} \Rightarrow ac \equiv bd \pmod{n},$$
6. *Si* $a \equiv b \pmod{n}$, *entonces* $ka \equiv kb \pmod{n}$, *para todo* $k \in \mathbb{Z}$,
7. *Si* $a \equiv b \pmod{n}$, *entonces* $a^k \equiv b^k \pmod{n}$, *para* $k \geq 0$.

8. (Cancelación) Si $(n, c) = 1$, entonces $ac \equiv bc \pmod{n} \Rightarrow a \equiv b \pmod{n}$.

Prueba: (1.) Para todo $a \in \mathbb{Z}$, $n \in \mathbb{N}$, $n \mid 0 = a - a \Rightarrow a \equiv a \pmod{n}$.

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

(3.) $n \mid b - a$, $n \mid c - b \Rightarrow n \mid (b - a) + (c - b) = c - a \Rightarrow a \equiv c \pmod{n}$.

(4.) $n \mid b - a$, $n \mid d - c \Rightarrow n \mid (b - a) \pm (d - c) = (b \pm d) - (a \pm c) \Rightarrow a \pm c \equiv b \pm d \pmod{n}$.

(5.) $n \mid b - a$, $n \mid d - c \Rightarrow n \mid (b - a)c$ y $n \mid a(d - c)$. Luego,
$n \mid (b - a)c - a(d - c) = bc - ad \Rightarrow ad \equiv bc \pmod{n}$.

(6.) Aplicando (4.) k-veces consecutivas, con $c = a$, $d = b$, se obtiene, $ka \equiv kb \pmod{n}$.

(7.) Aplicando (5.) k-veces consecutivas, con $c = a$, $d = b$, se obtiene, $a^k \equiv b^k \pmod{n}$.
Otra alternativa es ver que si $a \equiv b \pmod{n}$, entonces $n \mid b - a$
$\Rightarrow n \mid (b - a)(b^{k-1} + ab^{k-1} + \ldots + a^{k-2}b + a^{k-1}) = b^k - a^k$. Así, $a^k \equiv b^k \pmod{n}$.

(8.) Suponga que $ac \equiv bc \pmod{n}$, con $(n, c) = 1$. Entonces $n \mid bc - ac = (b - a)c$. Por el lema de Eulices, como $(n, c) = 1$, entonces $n \mid b - a \Rightarrow a \equiv b \pmod{n}$. $\square$

Obs! Dados $a \in \mathbb{Z}$ y $n \in \mathbb{Z}^+$, por el Algoritmo de la División, existen $q, r \in \mathbb{Z}$ tales que $a = qn + r$, con $0 \leq r < n$. Entonces, por definición de congruencia, $n \mid -qn = r - a$ $\Rightarrow \; a \equiv r \pmod{n}$. Porque hay n opciones para r, vemos que todo entero es congruente módulo n exactamente con uno de los valores residuos $0, 1, 2, \ldots n-1$; en particular, $a \equiv 0 \pmod{n}$ si, y sólo si, $n \mid a$.

Definición

El conjunto de n enteros $0, 1, 2, \ldots, n-1$ se denomina el ***conjunto de residuos mínimos no negativos*** *o* ***residuos canónicos****, módulo n.*
En general, una colección de n números enteros $a_1, a_2, \ldots, a_n$ forman un ***conjunto completo de residuos*** *(o un* ***sistema completo de residuos****) módulo n si cada a_i es congruente a alguno de los números $0, 1, 2, \ldots, n-1$, módulo n.*

Ejemplo: $-12, -4, 11, 13, 22, 82, 91$ constituyen un sistema completo de residuos módulo 7.

Obs! $S = \{a_i\}_{i=1}^n \subset \mathbb{Z}$ es un sistema de residuos módulo $n \;\Leftrightarrow\; a_i \not\equiv a_j \pmod{n}$, para $i \neq j$.

Teorema

Para enteros arbitrarios $a, b \in \mathbb{Z}$, $a \equiv b \pmod{n} \;\Leftrightarrow\;$ a y b dejan el mismo residuo cuando se divide por n.

Prueba: $(\Rightarrow)$ Si $a \equiv b \pmod{n}$, de modo que $n \mid b - a$ y $b = a + kn$ para algún entero k. Suponga que en la división entre n, a deja un cierto residuo r; es decir, $ab = qn + r$, con $0 \leq r < n$. Por lo tanto, $b = a + kn = (qn + r) + kn = (q + k)n + r$, por lo que b tiene el mismo residuo que a.
$(\Leftarrow)$ Por otro lado, suponga que podemos escribir $b = q_1n + r$ y $b = q_2n + r$, con el mismo residuo $0 \leq r < n$ Entonces,

$$b - a = (q_2n + r) - (q_1n + r) = (q_2 - q_1)n,$$

de modo que $n \mid b - a$. Esto es $a \equiv b \pmod{n}$. $\square$

Ejemplo: -56 y -11 pueden escribirse como $-56 = (-7)9 + 7$, $-11 = (-2)9 + 7$.
Esto muestra que $-56 \equiv -11 \pmod{9}$.

UNIVERSIDAD DEL VALLE DE GUATEMALA

Ejemplo: Mostramos que $41 \mid 2^{20} - 1$.
Observe que $2^5 \equiv 32 \equiv -9 \pmod{41}$, de donde $2^{20} = (2^5)^4 \equiv (-9)^4 \equiv 81 \cdot 81 \pmod{41}$. Pero $81 \equiv -1 \pmod{41} \;\Rightarrow\; 81 \cdot 81 \equiv 1 \pmod{41}$.
Esto muestra que $2^{20} - 1 \equiv 81 \cdot 81 - 1 \equiv 1 - 1 \equiv 0 \pmod{41}$.

Ejemplo: Hallar el residuo de $1! + 2! + 3! + 4! + \ldots + 99! + 100!$ al dividir por 12.
Comenzamos observando que $4! \equiv 24 \equiv 0 \pmod{12}$; así, para $k \geq 4$, se tiene que

$$k! = 4! \cdot 5 \cdot 6 \cdots k \equiv 0 \cdot 5 \cdot 6 \cdots k \equiv 0 \pmod{12}.$$

De esta manera,

$$1! + 2! + 3! + 4! + \ldots + 100! \equiv 1! + 2! + 3! + 0 + \ldots + 0 \equiv 9 \pmod{12}.$$

Congruencias

Vimos que una de las propiedades básicas de congruencias es que si $ca \equiv cb \pmod{n}$ entonces $a \equiv b \pmod{n}$, siempre que $(c, n) = 1$. Cuando $(c, n) \neq 1$ la cancelación en general no vale. Por ejemplo, $2(4) \equiv 2(1) \pmod{6}$, pero $4 \not\equiv 1 \pmod{6}$.

Con las precauciones adecuadas, se puede permitir la cancelación

Teorema

Si $ca \equiv cb \pmod{n}$, entonces $a \equiv b \pmod{\frac{n}{d}}$, donde $d = (c, n)$.

Prueba: Por hipótesis, $n \mid cb - ca$ y podemos escribir $c(b-a) = cb - ca = kn$, para algún $k \in \mathbb{Z}$. Como $(c, n) = d$, existen enteros primos relativos r, s que satisfacen $c = dr$, $n = ds$. Sustituyendo en la ecuación anterior,

$$dr(b-a) = kds \qquad \Rightarrow \qquad r(b-a) = ks,$$

de modo que $s \mid r(b-a)$. Como $(r, s) = 1$, el Lema de Euclides garantiza que $s \mid b - a$. Portanto, $a \equiv b \pmod{s}$; en otras palabras, $a \equiv b \pmod{\frac{n}{d}}$. $\square$

Corolario

Si $ca \equiv cb \pmod{n}$*, y* $(c, n) = 1$*, entonces* $a \equiv b \pmod{n}$*.* $\square$

Corolario

Si $ca \equiv cb \pmod{p}$*, y* $p \nmid c$*, con* p *primo, entonces* $a \equiv b \pmod{p}$*.*

<u>Prueba</u>: Las condiciones p primo y $p \nmid c$ implican que $(c, p) = 1$. $\square$

Ejemplo: Considere la congruencia $42 \equiv 15 \pmod{2}7$. Como $(3, 27) = 3$, debido al teorema anterior podemos "cancelar" el factor 3 en la congruencia. Así $14 == \equiv 5 \pmod{9}$. Una ilustración adicional es la congruencia $-35 \equiv 45 \pmod{8}$. Aquí, 5 y 8 son primos relativos, y podemos cancelar el factor 5 para obtener $-7 \equiv 9 \pmod{8}$.

Obs! En el teorema, no es necesario que $c \not\equiv 0 \pmod{n}$, pues en ese caso tendrías $c \equiv 0 \pmod{n} \;\Rightarrow\; (c, n) = n$, y la conclusión sería $a \equiv b \pmod{1}$, se mantiene automáticamente para todos entero a y b.

Ejemplos

Ejemplo: Hallar el residuo de la división $5^{3^{20}}$ entre 13.

Solución:
$5^4 \equiv 1 \pmod{13}$. Además, los residuos de dividir 5^n por 13 se repiten en ciclos de 4:

$$\begin{aligned}
5^0 &\equiv 1 \pmod{13}, & 5^4 &\equiv 1 \pmod{13},\\
5^1 &\equiv 5 \pmod{13}, & 5^5 &\equiv 5 \pmod{13},\\
5^2 &\equiv -1 \pmod{13}, & 5^6 &\equiv -1 \pmod{13},\\
5^3 &\equiv -5 \pmod{13}, & 5^7 &\equiv -5 \pmod{13}, \ \ldots
\end{aligned}$$

Por otro lado, tenemos que $3 \equiv -1 \pmod{4}$, de modo que $3^{20} \equiv (-1)^{20} \equiv 1 \pmod{4}$. Esto es, 3^{20} deja residuo 1 al dividirse por 4. Así, $5^{3^{20}} \equiv 5^1 \equiv 5 \pmod{13}$.

Ejercicio: Hallar el residuo de la división de 3^{1000} entre 101.

Ejemplo: Muestre que la ecuación diofantina $x^3 - 117y^3 = 5$ no admite soluciónes enteras.

Solución:
117 es múltiplo de 9, y tenemos

$$x^3 - 117y^3 = 5 \qquad \Leftrightarrow \qquad x^3 \equiv 5 \pmod 9.$$

Si analizamos los residuos cúbicos módulo 9, cuando x recorre cualquier sistema de residuos, tenemos

$x \pmod 9$	0	1	2	3	4	5	6	7	8
$x^3 \pmod 9$	0	1	8	0	1	8	0	1	8

O sea, x^3 sólo puede dejar residuos 0, 1 u 8 módulo 9. Así, si (x, y) fuese una solución de la ecuación, tendríamos $x^3 \equiv 5 \pmod 9$, algo imposíble. Portanto, dicha ecuación no posee soluciones enteras.

Ejemplo: Sea a un número entero impar. Demuestre que $2^{2^n} + a^{2^n}$ y $2^{2^m} + a^{2^m}$ son primos relativos para todos $m, n \in \mathbb{Z}^+$, con $n \neq m$.

Solución:
Sin pérdida, supongamos que $m > n$. Para cualquier primo p dividiendo $2^{2^n} + a^{2^n}$, y

$$a^{2^n} \equiv -2^{2^n} \pmod{p}.$$

Elevamos al cuadrado ambos lados de la ecuación $m - n$ veces para obtener

$$a^{2^m} = \left(a^{2^n}\right)^{2^{m-n}} \equiv \left(-2^{2^n}\right)^{2^{m-n}} \equiv 2^{2^m} \pmod{p}.$$

Como a es impar, tenemos $p \neq 2$, luego $2^{2^m} + 2^{2^m} = 2^{2^m+1} \not\equiv 0 \pmod{p}$, de modo que

$$a^{2^m} \equiv 2^{2^m} \not\equiv -2^{2^m} \pmod{p}.$$

Por tanto, $p \nmid a^{2^m} + 2^{2^m}$, lo que muestra el resultado deseado.

Obs! Cuando $a = 1$, esto conduce a una propiedad de los números de Fermat $2^{2^n} + 1$.

Bases

La notación usual para números naturales es chamada la notación **base 10**, con dígitos $0, 1, 2, \dots, 9$. Esto significa por ejemplo, que

$$196883 = 1 \cdot 10^5 + 9 \cdot 10^4 + 6 \cdot 10^3 + 8 \cdot 10^2 + 8 \cdot 10^1 + 3 \cdot 10^0.$$

El siguiente resultado muestra cómo escribir cualquier natural en cualquier base $d > 1$.

Teorema (Representación en Bases)

Sean $n \in \mathbb{N}$, y $d > 1$. Existe una única secuencia (los dígitos de n en la base d) $a_0, a_1, \dots, a_k, \dots$ con las siguientes propiedades

1. *para todo $k \in \mathbb{N}$, $0 \leq a_k < d$,*
2. *existe $m \in \mathbb{N}$ tal que $a_k = 0$, para tod $k \geq m$,*
3. *$n = \sum_{k \geq 0} a_k d^k$.*

<u>Prueba</u>: Usando el Algoritmo de la División, escribimos $n = n_0 = n_1 d + a_0$, $0 \leq a_0 < d$, $n_1 = n_2 d + a_1$, $0 \leq a_1 < d$; y en general, $n_k = n_{k+1} d + a_k$, con $0 \leq a_k < d$, y vale (1).

Bases

Afirmamos primero que $n_k = 0$, para algún $k \in \mathbb{N}$. De hecho, si $n_0 < d^m$, entonces $n_1 = \left\lfloor \frac{n_1}{d} \right\rfloor < d^{m-1}$, y, más generalmente, por inducción se muestra que $n_k < d^{m-k}$. En particular, para $k \geq m$, tenemos $n_k < 1 \;\Rightarrow\; n_k = 0$.
Se sigue de ahí que $a_k = 0$, para todo $k \geq m$, lo que muestra (2).

Para mostrar (3), procedemos por inducción sobre $m+1$ el número de dígitos a_j no nulos. Para $m = 0$, $n = n_0 < d$ $n = 0 \cdot d + a_0 \;\Rightarrow\; n = a_0 = a_0 \cdot d^0$.
Supongamos válida la propiedad para todo número entero con a lo sumo m dígitos en su representación base d. Entonces, si $n = (a_m \cdots a_1 a_0)_d$, tenemos que $n_1 = dn + a_0$. En particular $n_1 = (a_m \cdots a_1)_d$. Por la hipótesis inductiva aplicada a n_1

$$n = dn + a_0 = d\Big(\sum_{j=0}^{m-1} a_{j+1}d^j\Big) + a_0 = \sum_{j=0}^{m-1} a_{j+1}d^{j+1} + a_0 = \sum_{j=1}^{m} a_j d^j + a_0 = \sum_{j=0}^{m} a_j d^j.$$

Para la unicidad, suponga que n admite dos representaciones en base d: $\sum_{j\geq 0} a_k d^k = n = \sum_{k \geq 0} b_k d^k$. Si las secuencias $\{a_k\}$ y $\{b_k\}$ son distintas, existe un menor índice j tal que $a_j \neq b_j$. Tomamos

Bases

$$a_j + \sum_{k>j} a_k d^{k-j} = b_j + \sum_{k>j} b_k d^{k-j} \quad \Rightarrow \quad a_j - b_j = \sum_{k>j} (b_k - a_k) d^{k-j},$$

lo que muestra que $d \mid a_j - b_j$. Pero $0 \leq a_k, b_k < d \;\Rightarrow\; 0 \leq |a_j - b_j| < d$, implica que $a_j - b_j = 0$, y portanto $a_j - b_j$ no puede ser un múltiplo de d, un absurdo. Esto muestra que la representación en base d es única. $\square$

Notación: Ignorando los ceros iniciales, escribimos $n = (a_m a_{m-1} \cdots a_1 a_0)_d = \sum_{k=0}^{m} a_k d^k$, y llamamos a ésta la **representación en base** d **de** n.

Ejemplo: La representación binaria de $n = 105$ es

$$105 = 1\dot{2}^6 + 1 \cdot 2^5 + 0 \cdot 2^4 + 1 \cdot 2^3 + 0 \cdot 2^2 + 0\dot{2} + 1 = 2^6 + 2^5 + 2^3 + 1,$$

o, en forma compacta, $105 = (1101001)_2$.

Ejemplo: Por otro lado, la representación $(1001111)_2$ corresponde a

$$n = 1 \cdot 2^6 + 0 \cdot 2^5 + 0 \cdot 2^4 + 1 \cdot 2^3 + 1 \cdot 2^2 + 1 \cdot 2 + 1 = 2^6 + 2^3 + 2^2 + 1 = 79.$$