

1. Repaso

En el material anterior de Números se vieron los módulos donde $a \equiv b \pmod{c}$ (se lee “ a es congruente a b módulo c ”) si y sólo si $a = ck + b$ para algún valor entero de k , es decir, el algoritmo de la división. Otra forma de ver esto es que a y b tienen el mismo residuo al dividirlos entre c .

Ejemplos rápidos

- $426 \equiv 166 \pmod{13}$
- $166 \equiv 36 \pmod{13}$
- $36 \equiv 10 \pmod{13}$
- $10 \equiv -3 \pmod{13}$
- $426 \equiv -3 \pmod{13}$

El último ejemplo nos dice que $426 = 13k - 3$, así que podemos saber que $13|426 + 3$ o $13|429$, lo cual es cierto.

Muchas veces trabajar con congruencias negativas hará que un problema se vuelva más simple.

2. Propiedades de las congruencias

1. $a \equiv a \pmod{n}$
2. Si $a \equiv b \pmod{n}$ entonces $b \equiv a \pmod{n}$
3. Si $a \equiv b \pmod{n}$ y $b \equiv c \pmod{n}$, entonces $a \equiv c \pmod{n}$.
4. Si $a \equiv b \pmod{n}$ y $c \equiv d \pmod{n}$, entonces $a + c \equiv b + d \pmod{n}$
5. Si $a \equiv b \pmod{n}$ y $c \equiv d \pmod{n}$, entonces $ac \equiv bd \pmod{n}$
6. Si $a \equiv b \pmod{n}$, entonces $a^k \equiv b^k \pmod{n}$ con $k \in \mathbb{N}$

Puedes encontrar las demostraciones de las 5 primeras propiedades en el material anterior de Números.

Para probar la propiedad 6 basta con aplicar k veces la propiedad 5.

3. Criterios de divisibilidad

Si recuerdas bien el primer material de Números del caótico 2020 fue Criterios de divisibilidad. En ese material se explicaba con divisibilidad algunos de los criterios de divisibilidad, pero es muy tardado comprobar los criterios con ese método. Gracias a los módulos podemos comprobar los mismos criterios y obtener el criterio de cualquier número entero, aunque algunos puede que no sean muy bonitos.

Supongamos que tenemos un número $A = D_9D_8D_7D_6D_5D_4D_3D_2D_1D_0$ donde cada D es un dígito, entonces su expansión decimal es $A = 10^9 * D_9 + 10^8 * D_8 + 10^7 * D_7 + 10^6 * D_6 + 10^5 * D_5 + 10^4 * D_4 + 10^3 * D_3 + 10^2 * D_2 + 10^1 * D_1 + 10^0 * D_0$, esto se ve muy feo lo escribiré de otra forma

$$\begin{array}{cccccccccc} 10^9 & 10^8 & 10^7 & 10^6 & 10^5 & 10^4 & 10^3 & 10^2 & 10^1 & 10^0 \\ D_9 & D_8 & D_7 & D_6 & D_5 & D_4 & D_3 & D_2 & D_1 & D_0 \end{array}$$

Ahora vamos usar un poco las propiedades de las congruencias, supongamos que tenemos al número $ab + cd$ y queremos ver su módulo n , entonces podemos obtener el módulo de cada letra y hacer el problema más sencillo. Te estarás preguntando qué tiene que ver esto con lo anterior, pues vamos a lo que nos interesa, los criterios de divisibilidad.

Criterio del 2. Si tenemos $A = D_9D_8D_7D_6D_5D_4D_3D_2D_1D_0$ y queremos ver cuánto es A módulo n podemos calcular el módulo 2 de la potencia de 10 de cada dígito, lo que nos dejaría

$$\begin{array}{cccccccccc} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ D_9 & D_8 & D_7 & D_6 & D_5 & D_4 & D_3 & D_2 & D_1 & D_0 \end{array}$$

En el caso de que A tenga más de 10 dígitos basta con ver que $10^{10} \equiv 10^9 * 10 \equiv 10 * 0 \equiv 0 \pmod{2}$. Así que no importa cuántos dígitos tenga A , siempre sucederá lo mismo.

Así que $A \equiv D_0 \pmod{2}$ y esto nos dice que para ver si un número es divisible entre 2 si y sólo si su último dígito es divisible entre 2, pero también nos dice que para ver con qué es congruente A módulo 2, basta con ver su último dígito.

Puedes repetir el mismo proceso para el criterio de las potencias de 2, 5 y 10.

Criterio del 3. Repetiremos el mismo proceso que con el 2, antes de eso hay que ver que $10 \equiv 1 \pmod{3} \rightarrow 10^k \equiv 1 \pmod{3}$, por lo que todas las potencias de 10 son congruentes a 1 $\pmod{3}$.

$$\begin{array}{cccccccccc} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ D_9 & D_8 & D_7 & D_6 & D_5 & D_4 & D_3 & D_2 & D_1 & D_0 \end{array}$$

Así que $A \equiv D_9 + D_8 + D_7 + D_6 + D_5 + D_4 + D_3 + D_2 + D_1 + D_0 \pmod{3}$. Entonces el criterio del 3 no sólo nos dice si un número es divisible entre 3, también nos dice cuál es su módulo.

Puedes repetir el mismo proceso para el criterio del 9.

Criterio del 11. Primero hay que ver que

$$10^0 \equiv 1 \pmod{11}$$

$$10^1 \equiv 10 \pmod{11} \text{ y } 10^1 \equiv -1 \pmod{11}$$

Así que $10^{n+1} \equiv 10^n * 10 \equiv -10^n \pmod{11}$, lo que nos dice que cada que se multiplique por 10 un número, será congruente al negativo del número original módulo 11.

$$\begin{array}{cccccccccc} -1 & 1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 & 1 \\ D_9 & D_8 & D_7 & D_6 & D_5 & D_4 & D_3 & D_2 & D_1 & D_0 \end{array}$$

Entonces $A \equiv D_0 - D_1 + D_2 - D_3 + D_4 - D_5 + D_6 - D_7 + D_8 - D_9 \pmod{11}$ lo que nos dice cómo calcular el módulo 11 de cualquier número y de paso ver si es múltiplo de 11.

Criterio del 7. Antes de ver el criterio hay que ver las congruencias de TODAS las potencias de 10 módulo 7 y para eso nos puede ayudar que $10 \equiv 3 \pmod{7}$.

$$10^0 \equiv 1 \pmod{7}$$

$$10^1 \equiv 3 \pmod{7}$$

$$10^2 \equiv 10 * 10 \equiv 3 * 3 \equiv 2 \pmod{7}$$

$$10^3 \equiv 10^2 * 10 \equiv 2 * 3 \equiv -1 \pmod{7}$$

$$10^4 \equiv 10^3 * 10 \equiv -1 * 3 \equiv -3 \pmod{7}$$

$$10^5 \equiv 10^4 * 10 \equiv -3 * 3 \equiv -2 \pmod{7}$$

$$10^6 \equiv 10^5 * 10 \equiv -2 * 3 \equiv 1 \pmod{7}$$

Como $10^6 \equiv 10^0 \pmod{7}$ esto nos dice que cada 6 potencias de 10 se repetirán las congruencias, ya que para aumentar la potencia de 10 se multiplica por 3 y los números obtenidos se repetirán. En resumen $10^n \equiv 10^{n+6} \pmod{7}$.

Entonces

$$\begin{matrix} -1 & 2 & 3 & 1 & -2 & -3 & -1 & 2 & 3 & 1 \\ \mathbf{D}_9 & \mathbf{D}_8 & \mathbf{D}_7 & \mathbf{D}_6 & \mathbf{D}_5 & \mathbf{D}_4 & \mathbf{D}_3 & \mathbf{D}_2 & \mathbf{D}_1 & \mathbf{D}_0 \end{matrix}$$

Así que $A \equiv D_0 + 3D_1 + 2D_2 - D_3 - 3D_4 - 2D_5 + D_6 + 3D_7 + 2D_8 - D_9 \pmod{7}$, esta ecuación nos dirá cuánto es A módulo 7. Se puede ver por cuánto se multiplicara cada dígito siguiendo el ciclo de congruencias.

Este mismo proceso se puede aplicar para cualquier número natural.

4. Congruencias útiles

Ya vimos cómo obtener TODAS las congruencias de la potencia de un número, ahora vamos a ver las posibles congruencias de un número al cuadrado, cubo, etc.

Supongamos que queremos encontrar todas las posibles congruencias de x^2 módulo 4, para eso hay que hacer los primeros casos de x .

x	$(\pmod{4})$
0	$0^2 \equiv 0 \pmod{4}$
1	$1^2 \equiv 1 \pmod{4}$
2	$2^2 \equiv 4 \equiv 0 \pmod{4}$
3	$3^2 \equiv 9 \equiv 1 \pmod{4}$

Bien, ya tenemos las congruencias para los 3 primeros valores de x , faltan infinitos valores, ¿cómo podemos calcular todos sin hacer un documento de infinitas páginas? Fácil, hay que usar el algoritmo de la división, supongamos que $x = 4k + r$ con $k \in \mathbb{Z}$ y $0 \leq r \leq 3$. Ahora $x^2 = (4k + r)^2 = 4^2k^2 + 4k * 2r + r^2$ y como $4^2k^2 + 4k * 2r \equiv 0 \pmod{4}$ entonces $x^2 \equiv r^2 \pmod{4}$ y ya calculamos el módulo de todos los residuos, así que ya podemos saber cuánto es x^2 módulo 4 para cualquier valor de x . Podemos ver que basta con ver el residuo de x sin importar el número natural al que esté elevado con el binomio de Newton.

Con lo anterior podemos ver que ningún número al cuadrado es congruente a 2 o 3 módulo 4, lo que es muy importante para muchos problemas.

Otro truco muy útil para ver las congruencias es usar números negativos, por ejemplo si queremos ver las congruencias de x^4 módulo 7, podemos probar con valores 0, 1, 2, 3, 4, 5 y 6, pero para esto tendríamos calcular 6^4 que no es algo muy trivial. Usando valores negativos

x	$(\text{mod } 7)$
0	$0^4 \equiv 0(\text{mod } 7)$
1	$1^4 \equiv 1(\text{mod } 7)$
2	$2^4 \equiv 16 \equiv 2(\text{mod } 7)$
3	$3^4 \equiv 81 \equiv 6(\text{mod } 7)$
-3	$(-3)^4 \equiv 81 \equiv 6(\text{mod } 7)$
-2	$(-2)^4 \equiv 16 \equiv 2(\text{mod } 7)$
-1	$(-1)^4 \equiv 1(\text{mod } 7)$

Con potencias pares podemos ver que hay cierta clase de simetría.

Hay ciertos módulos que nos pueden ayudar a resolver problemas, así como ver x^2 módulo 4, aquí hay una lista de algunos de las posibles congruencias

m	Cuadrados módulo m	Cubos módulo m
3	0, 1	0, 1, 2
4	0, 1	0, 1, 3
5	0, 1, 4	0, 1, 2, 3, 4
6	0, 1, 3, 4	0, 1, 2, 3, 4, 5
7	0, 1, 2, 4	0, 1, 6
8	0, 1, 4	0, 1, 3, 5, 7
9	0, 1, 4, 7	0, 1, 8
10	0, 1, 4, 5, 6, 9	0, 1, 2, 3, 4, 5, 6, 7, 8, 9
11	0, 1, 3, 4, 5, 9	0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10
12	0, 1, 4, 9	0, 1, 3, 4, 5, 7, 8, 9, 11
13	0, 1, 3, 4, 9, 10, 12	0, 1, 5, 8, 12
14	0, 1, 2, 4, 7, 8, 9, 11	0, 1, 6, 7, 8, 13
15	0, 1, 4, 6, 9, 10	0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14
16	0, 1, 4, 9	0, 1, 3, 5, 7, 8, 9, 11, 13, 15
17	0, 1, 2, 4, 8, 9, 13, 15, 16	0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16
18	0, 1, 4, 7, 9, 10, 13, 16	0, 1, 8, 9, 10, 17
19	0, 1, 4, 5, 6, 7, 9, 11, 16, 17	0, 1, 7, 8, 11, 12, 18
20	0, 1, 4, 5, 9, 16	0, 1, 3, 4, 5, 7, 8, 9, 11, 12, 13, 15, 16, 17, 19

Por lo general, es más útil usar los módulos que generen la menor cantidad de posibles valores. Por ejemplo, para analizar cuadrados es muy útil verlos módulo 8, ya que sólo pueden ser congruentes a 0, 1 o 4.

5. Inverso multiplicativo

Así como en las igualdades, en las congruencias existen ecuaciones, por ejemplo $ax + b \equiv c \pmod{d}$, donde a, b y c son números conocidos y queremos encontrar el valor de x .

Por ejemplo, si tenemos

$$5x + 13 \equiv 9 \pmod{11}$$

Primero aplicándole módulo 11 a todos los términos para trabajar con valores lo más pequeños posibles

$$5x + 2 \equiv -2 \pmod{11}$$

Ahora, en las congruencias podemos sumar o restar términos a ambos lados sin que se afecte el resultado. Entonces

$$5x \equiv -4 \pmod{11}$$

IMPORTANTE: Por la propiedad 5, podemos multiplicar ambos lados de la congruencia por el mismo número, **PERO** no podemos dividir a ambos lados de la congruencia así como así. Para eso necesitamos obtener al inverso multiplicativo.

En el caso anterior necesitamos obtener el inverso multiplicativo del 5 módulo 11. Digamos que m es el inverso, entonces cumplirá que $5m \equiv 1 \pmod{11}$. Para encontrar el valor de m podemos hacerlo con talacha

m	$5m \pmod{11}$
1	$5 \equiv 5 \pmod{11}$
2	$10 \equiv -1 \pmod{11}$
3	$15 \equiv 4 \pmod{11}$
4	$20 \equiv -2 \pmod{11}$
5	$25 \equiv 3 \pmod{11}$
6	$30 \equiv -3 \pmod{11}$
7	$35 \equiv 2 \pmod{11}$
8	$40 \equiv -4 \pmod{11}$
9	$45 \equiv 1 \pmod{11}$

Así que ya obtuvimos que $m = 9$. Regresando al ejemplo, teníamos que $5x \equiv -4 \pmod{11}$, si lo multiplicamos a ambos lados por 9 o -2 , ya que $9 \equiv -2 \pmod{11}$, tenemos que

$$-10x \equiv 8 \pmod{11}$$

$$\rightarrow x \equiv 8 \pmod{11}$$

LISTO, se podría decir que ya despejamos a x , ¿pero cómo lo comprobamos? Usaremos el algoritmo de la división. Por lo anterior sabemos que x es un número de la forma $x = 11k + 8$, con k un número entero. Sustituyendo esto en la congruencia original

$$\begin{aligned} 5x + 13 &\equiv 9 \pmod{11} \\ \rightarrow 5(11k + 8) + 13 &\equiv 9 \pmod{11} \\ \rightarrow 55k + 40 + 13 &\equiv 9 \pmod{11} \\ \rightarrow 53 &\equiv 9 \pmod{11} \end{aligned}$$

Lo último es cierto ya que $53 = 4 * 11 + 9$.

Si no me creen que sí se cumple, démosle un valor a la k , por ejemplo 7. Entonces $x = 11 * 7 + 8 = 85$. Entonces

$$5(85) + 13 \equiv 425 + 13 \equiv 38 * 11 + 7 + 11 + 2 \equiv 7 + 2 \equiv 9 \pmod{11}$$

Ahora, hay ciertos atajos para encontrar el inverso multiplicativo. Por ejemplo, habíamos visto que $5(2) \equiv -1 \pmod{11}$, entonces si multiplicamos por 10 y -1 a cada lado, tendríamos que $5(2)(10) \equiv (-1)(-1) \equiv 1 \pmod{11}$. Entonces $5(20) \equiv 1 \pmod{11}$, así se podría ver que 20 es otro inverso multiplicativo, como $20 \equiv 9 \pmod{11}$ también podríamos haber obtenido el 9 de esta forma.

Con esto se nos presenta otra duda, ¿siempre podremos encontrar el inverso de un número a módulo n ? La respuesta es sí, siempre y cuando a y n sean primos relativos.

Demostración

Si a y n son primos relativos, entonces $(a, n) = 1$.

Usando el algoritmo de Euclides, $(a, n) = (a - kn, n) = (a - kn, n - (a - kn)q)$, supongamos que con esos pasos ya obtenemos que $a - kn - (n - (a - kn)q)r = 1$, entonces $a - kn - rn + aqr - knqr = a(1 + qr) + n(-k - r - kqr) = 1$, si $c = 1 + qr$ y $d = -k - r - kqr$, entonces $ac + nd = 1$. Si el algoritmo de Euclides tuviera más pasos también se podría factorizar de la misma forma, esa lo puedes demostrar tú.

Con lo anterior podemos ver que siempre existirán parejas de números que $ac + nd = 1$, en general, para cada valor de c siempre existirá un valor de d que cumplirá

y viceversa (para esto puedes investigar las ecuaciones diofantinas o puedes preguntar). Así que si tomamos $d = 0$, entonces existirá un valor c que cumplirá que $ac + n(0) = ac = 1$, donde c sería el inverso multiplicativo de a módulo n .

6. Unas propiedades más

7. Si $ax \equiv bx \pmod{n}$ entonces $a \equiv b \pmod{n}$ si y sólo si x y n son primos relativos
8. Si $d = (a, n)$ y $d \nmid b$, entonces $a \not\equiv b \pmod{n}$
9. $ax \equiv bx \pmod{nx}$ si y sólo si $a \equiv b \pmod{n}$

Para la propiedad 7 basta con ver que existirá una m tal que sea inverso multiplicativo de x módulo n , así que $xm \equiv 1 \pmod{n} \rightarrow axm \equiv a \equiv bxm \equiv b \pmod{n}$.

Para la propiedad 8 veremos que $a = da'$ y $n = dn'$. Por el algoritmo de la división, si la congruencia se cumpliera tendríamos que $da' = dn' + b$ pero como $d \mid da'$ entonces d debe de dividir a $dn' + b$, pero como $d \mid dn'$, entonces d debe dividir a b lo cual no es cierto. Así que no es posible llegar a la congruencia.

La propiedad 9 se puede probar de una forma parecida a la propiedad 8. Tenemos que $ax \equiv bx \pmod{nx} \Leftrightarrow ax = nx(k) + bx$, dividiendo ambos lados entre x , entonces $a = n(k) + b \Leftrightarrow a \equiv b \pmod{n}$.

Ejemplos

- $440x \equiv 32 \pmod{7} \Leftrightarrow 55x \equiv 4 \pmod{7} \Leftrightarrow -x \equiv 4 \pmod{7} \Leftrightarrow -6x \equiv x \equiv 24 \equiv 3 \pmod{7}$, entonces $x = 7k + 3$.
- $4x \not\equiv 3 \pmod{8}$.
- $900x + 100 \equiv 1300 \pmod{1900} \Leftrightarrow 9x + 1 \equiv 13 \pmod{19} \Leftrightarrow 9x \equiv -7 \pmod{19} \Leftrightarrow 9(36)x \equiv x \equiv -2(-7) \equiv 14 \pmod{19}$, entonces $x = 19k + 14$.

7. Sistemas de congruencias

Como vimos anteriormente las congruencias se pueden comportar como ecuaciones, así que también se deben de poder comportar como sistemas de ecuaciones y de ahí el nombre **Sistemas de congruencias**.

Ejemplo

Encuentra todos los valores de x que cumplen

$$x \equiv 1 \pmod{3}$$

$$x \equiv 5 \pmod{7}$$

Solución

Resolviendo la primera congruencia tendríamos que $x = 3k + 1$, sustituyendo esto en la segunda congruencia

$$3k + 1 \equiv 5 \pmod{7}$$

$$\rightarrow 3k \equiv 4 \pmod{7}$$

$$\rightarrow k \equiv 6 \pmod{7}$$

Así que $k = 7q + 6$, por lo tanto $x = 3(7q + 6) + 1 = 21q + 19$

8. Problemas

1. Prueba que $31|30^{99} + 61^{100}$
2. Prueba que $66|43^{101} + 23^{101}$
3. Prueba que entre cualesquiera 51 enteros, existen dos con cuadrados congruentes módulo 100.
4. Encuentra el residuo de $10^{10} + 10^{100} + 10^{1000} + \dots + 10^{10000000000}$ al ser dividido entre 7.
5. ¿Cuántos números naturales n no mayores que 10000 son tales que $2^n - n^2$ es divisible entre 7?
6. ¿Existe algún número natural n tal que $n^2 + n + 1$ es divisible entre 1995?
7. Prueba que $11^{n+2} + 12^{2n+1} \equiv 0 \pmod{133}$ para cualquier $n \in \mathbb{N}$.
8. Sea n un número natural tal que $n + 1 \equiv 0 \pmod{4}$. Prueba que la suma de todos los divisores de n también es divisible por 24.
9. (1994 AIME) La secuencia

$$3, 15, 24, 48, \dots$$

Consiste en los múltiplos positivos de 3 que son un número al cuadrado menos 1. ¿Cuál es el residuo del 1994 término de la secuencia cuando es dividido entre 1000?

10. Demuestra que para toda n entera sucede que $3804|(n^3 - n)(5^{8n+4} + 3^{4n+2})$.
11. Si p es un primo mayor que 3, prueba que $24|p^2 - 1$.
12. Encontrar todos los enteros x que satisfagan $4x + 20 \equiv 27x - 1 \pmod{5}$.

13. Encontrar todos los enteros x que satisfagan la congruencia $3x + 1 \equiv 15x - 7 \pmod{20}$.
14. Encontrar todos los enteros x que satisfagan la congruencia $3x + 1 \equiv 15x - 4 \pmod{20}$.
15. Encontrar todos los enteros x que satisfagan la congruencia $14x - 22 \equiv x + 3 \pmod{7}$.
16. Encontrar todos los enteros x que satisfagan la congruencia $12x + 7 \equiv 4x - 6 \pmod{21}$.
17. Encontrar todos los enteros x que satisfagan la congruencia $6x + 6 \equiv 1 - 4x \pmod{15}$.
18. Encontrar todos los enteros x que satisfagan la congruencia $-9x + 2 \equiv 3x - 2 \pmod{4}$.
19. Encontrar todos los enteros x que satisfagan la congruencia $4x + 1 \equiv 1 - 5x \pmod{3}$.
20. Encuentra los posibles valores de x en las siguientes congruencias
- $43x + 143 \equiv 2 \pmod{9}$
 - $545x + 212 \equiv 93 \pmod{11}$
 - $429x + 117 \equiv 468 \pmod{65}$
 - $39x - 23 \equiv 43 \pmod{12}$
 - $4323x + 4 \equiv 19 \pmod{22}$
21. Resolver el sistema de congruencias
- $$\begin{aligned} 2x &\equiv 1 \pmod{7} \\ x &\equiv 1 \pmod{5} \\ 2x - 3 &\equiv 29 - 2x \pmod{6} \\ x + 3 &\equiv 5x - 3 \pmod{2} \end{aligned}$$
22. Resolver el sistema de congruencias
- $$\begin{aligned} x &\equiv 1 \pmod{2} \\ x &\equiv 1 \pmod{3} \\ x &\equiv 1 \pmod{4} \\ x &\equiv 1 \pmod{5} \\ x &\equiv 1 \pmod{6} \\ x &\equiv 1 \pmod{7} \\ x &\equiv 1 \pmod{8} \\ x &\equiv 1 \pmod{9} \\ x &\equiv 1 \pmod{10} \end{aligned}$$
23. (OMM 2016) Decimos que un número entero no-negativo n contiene a otro entero no-negativo m , si los dígitos de su expansión (o desarrollo) decimal aparecen en forma consecutiva en la expansión (o desarrollo) decimal de n . Por ejemplo, 2016 contiene a 2, 0, 1, 6, 20, 16, 201 y 2016. Determina el mayor número entero n que no contiene a ningún múltiplo de 7.