

Taller Teoría de Números

Carlos Arturo Murcia Andrade

12 de mayo de 2023



1 ¿Existen enteros a y b tal que $a + b = 544$ y $\gcd(a, b) = 11$?

Solución. Suponga que $\gcd(a, b) = 11$. Entonces, existen enteros c y d tales que $a = 11 * c$ y $b = 11 * d$.

Si reemplazamos los valores de a y b en $a + b = 544$ tenemos $11 * c + 11 * d = 544$. Operando, tenemos $c + d = \frac{544}{11}$.

Ahora, un número es divisible por 11 si la resta entre las sumas de las cifras impares y pares es también múltiplo de 11.

Al aplicar este criterio para 544 tenemos que $5 - 4 + 4 = 5$. 5 NO es divisible entre 11, ya que $5 \bmod 11 \neq 0$.

Por lo tanto, **no existen números** enteros a y b tales que $a + b = 544$ y que $\gcd(a, b) = 11$ \square

2 Encuentre un criterio de divisibilidad para el 8 y el 16.

Un número n es divisible entre 2 si existe un entero k tal que $n = 2k$.

Un número n es divisible entre 4 si existe un entero k tal que $n = 2 * 2k = 2^2 * k = 4k$.

Un número n es divisible entre 8 si existe un entero k tal que $n = 2 * 2 * 2k = 2^3 * k = 8k$.

Un número n es divisible entre 16 si existe un entero k tal que $n = 2 * 2 * 2 * 2k =$

$$2^4 * k = 16k.$$

En ese orden de ideas, se tiene que $1000/8 = 125$ y $10000/16 = 625$. Esto indica que cualquier número que sea múltiplo de 1000 es divisible entre 8 y cualquier número que sea múltiplo de 10000 es divisible por 16.

Esto implica que si las últimas 3 (2 o 1) cifras de un número son divisibles por 8, entonces el número es divisible por 8. Asimismo, si las últimas 4 (3, 2 o 1) cifras de un número son divisibles por 16, entonces el número es divisible por 16.

3 Si p es primo y $a^2 \equiv b^2 \pmod{p}$, demostrar que $a \equiv \pm b \pmod{p}$.

Solución. Suponga que p es primo y que $a^2 \equiv b^2 \pmod{p}$.

$a^2 \equiv b^2 \pmod{p}$ puede reescribirse como $a^2 - b^2 \equiv 0 \pmod{p}$. Y, asimismo, puede reescribirse como $(a - b)(a + b) \equiv 0 \pmod{p}$.

Esto quiere decir que $(a - b) \equiv 0 \pmod{p}$ y $(a + b) \equiv 0 \pmod{p}$. Es decir, $a \equiv -b \pmod{p}$ y $a \equiv b \pmod{p}$.

Por lo tanto, si p es primo y $a^2 \equiv b^2 \pmod{p}$, entonces, $a \equiv \pm b \pmod{p}$. \square

4 Hallar $19^{19} \pmod{5}$.

Es preciso considerar el Pequeño Teorema de Fermat para resolver este punto.

Teorema. Sea p un número primo, y sea a un número que NO sea múltiplo de p . Entonces: $a^{p-1} \equiv 1 \pmod{p}$. O, también: $a^p \equiv a \pmod{p}$ (esta última forma aplica independientemente de si a es múltiplo de p).

$19^{19} \pmod{5}$ puede ser expresado como $(19^5 * 19^5 * 19^5 * 19^4) \pmod{5}$.

Sabemos (por el Pequeño Teorema de Fermat) que: $19^4 \equiv 1 \pmod{5}$ y $19^5 \equiv 19 \pmod{5}$. Entonces:

$$\begin{aligned} 19^{19} &\equiv 19^5 * 19^5 * 19^5 * 19^4 \pmod{5} \\ 19^5 * 19^5 * 19^5 * 19^4 &\equiv 19 * 19 * 19 * 1 \pmod{5} \\ 19 * 19 * 19 * 1 &\equiv 19^3 \pmod{5} \\ 19^3 &\equiv 6859 \pmod{5} \end{aligned}$$

Es decir, $19^{19} \pmod{5} = 19^3 = 6859$.

5 Hallar los últimos 2 dígitos de 7^{7^7} .

Hallar los últimos 2 dígitos de 7^{7^7} , también puede ser expresado como hallar $7^{7^7} \bmod 100$, o como hallar $7^{49} \bmod 100$.

Primero, es preciso hallar los patrones que involucran $7^i \bmod 100$, donde $i \in \mathbb{Z} > 0$.

$$7^1 \bmod 100 = 07$$

$$7^2 \bmod 100 = 49$$

$$7^3 \bmod 100 = 43$$

$$7^4 \bmod 100 = 01$$

$$7^5 \bmod 100 = 07$$

$$7^6 \bmod 100 = 49$$

$$7^7 \bmod 100 = 43$$

$$7^8 \bmod 100 = 01$$

Cada 4 iteraciones se repite el patrón, entonces, es preciso saber en qué “posición” dentro del patrón se encontraría el exponente 49 (hallando el residuo de dividirlo entre 4, el número de patrones).

$49 \bmod 4 = 1$. Es decir, $7^{49} \equiv 7^1 \pmod{100}$, lo que quiere decir que los últimos 2 dígitos de 7^{7^7} son 07.

6 Encuentre $\phi(n)$, para $n = 35$, $n = 100$ y $n = 51200$.

Este ejercicio nos pide hallar el Euler Totient de 35, 100 y 51200 respectivamente.

Para proceder, es necesario definir la función Euler Totient.

Definición. La función ϕ de Euler o Euler Totient es:

$$\phi(n) = |\{x : 1 \leq x \leq n \wedge \gcd(n, x) = 1\}|$$

el número de enteros positivos $x \leq n$ que no tienen divisores comunes con n .

Lema. 1. $\phi(1) = 1$

2. Si p es primo $\phi(p^a) = p^a - p^{a-1}$

3. Si $\gcd(m, n) = 1$, $\phi(m * n) = \phi(m) * \phi(n)$

Con esto en cuenta:

1. $\phi(35) = \phi(7 * 5) = \phi(7) * \phi(5) = (7^1 - 7^0) * (5^1 - 5^0) = (7 - 1) * (5 - 1) = 6 * 4 = 24$
2. $\phi(100) = \phi(2^2 * 5^2) = \phi(2^2) * \phi(5^2) = (2^2 - 2^1) * (5^2 - 5^1) = (2 - 1) * (25 - 5) = 2 * 20 = 40$
3. $\phi(51200) = \phi(2^{11} * 5^2) = \phi(2^{11}) * \phi(5^2) = (2^{11} - 2^{10}) * (5^2 - 5^1) = (2048 - 1024) * (25 - 5) = 1024 * 20 = 20480$

Se puede verificar esto si se corre en el Jupyter Notebook desarrollado en una ocasión anterior.

```
print("|||||")
print("Original number: " + str(n5))
print("φ(" + str(n5) + ") = " + str(calculate_euler_totient_using_lemma(n5)))
print("Original number: " + str(n6))
print("φ(" + str(n6) + ") = " + str(calculate_euler_totient_using_lemma(n6)))
print("Original number: " + str(n7))
print("φ(" + str(n7) + ") = " + str(calculate_euler_totient_using_lemma(n7)))
```

|||||

Original number: 35
 $\phi(35) = 24$
 Original number: 100
 $\phi(100) = 40$
 Original number: 51200
 $\phi(51200) = 20480$

7 Usted le pregunta a un robot que quiere comer. Él responde “48879”. Sabiendo que el robot piensa en hexadecimal, pero habla el decimal, ¿qué le debería dar de comer?

Es preciso tener consciencia del Teorema de la División para realizar este punto.

Teorema. *Suponga que $a \in \mathbb{Z}$ y $n \in \mathbb{Z} > 0$. Entonces, existen enteros q y r tales que: $a = q * n + r$. $0 \leq r < n$
 q es el cociente y r es el residuo.*

En este caso, es preciso “traducir” el mensaje “48879” de decimal a hexadecimal (el sistema hexadecimal tiene un total de 16 elementos y va de 0 – 9 y A – F). Es necesario implementar el Teorema de la División de manera iterativa. Esto permitirá descubrir las letras del mensaje desde la última hasta la primera. Entonces:

1. $48879 = 3054 * 16 + 15$. Esta letra equivale a 15, o en hexadecimal F .
2. $3054 = 190 * 16 + 14$. Esta letra equivale a 14, o en hexadecimal E .
3. $190 = 11 * 16 + 14$. Esta letra equivale a 14, o en hexadecimal E .

4. $11 = 0 * 16 + 11$. Esta letra equivale a 11, o en hexadecimal B .

Si se reordenan las letras, el robot desea comer “BEEF”, un pedazo de cordero (lo cual es extraño, porque no se supone que los robots sean carnívoros).

8 ¿Es 65314638792 divisible por 24?

Es preciso definir un criterio de divisibilidad para 24 antes de continuar.

Un número puede ser divisible por 24, siempre que sea divisible tanto por 3 como por 8 (ya que $8 * 3 = 24$).

Ya se probó en el ejercicio 2 el criterio de divisibilidad por 8. Entonces, se toman las tres últimas cifras, 792 y se verifica si este número puede ser dividido por 8. $792 \bmod 8 = 0$, ergo, este número es divisible por 8.

Ahora, se debe probar que el número sea divisible por 3, para ello se deben sumar todas las cifras del número y rectificar si ese resultado es divisible entre 3. Entonces, tenemos $6+5+3+1+4+6+3+8+7+9+2 = 54$ y $54 \bmod 3 = 0$, que quiere decir que el número es divisible por 3.

Por lo tanto, si el número es divisible por 8 y 3, entonces, el número es divisible por 24.

9 Demostrar que $n^p - n$ es divisible por p si p es un número primo.

Solución. Primero, es necesario definir el caso base: si $n = 1$, entonces $1^p - 1 = 0$ y 0 es divisible por cualquier primo p .

Con el caso base, definimos nuestra hipótesis inductiva: suponga que para cualquier entero $k > 0$, $k^p - k$ es divisible por cualquier primo p .

Entonces, procedemos con la inducción: ¿es cierto que $((k + 1)^p - (k + 1)) \bmod p = 0$?

Sea $a = k + 1$, si se reemplaza en $((k + 1)^p - (k + 1)) \bmod p = 0$ tenemos $(a^p - a) \bmod p = 0$. O sea, $a^p - a \equiv 0 \pmod{p}$. Si restamos a en ambos lados de la congruencia $a^p \equiv a \pmod{p}$.

Por el Pequeño Teorema de Fermat, es correcto decir que $a^p \equiv a \pmod{p}$, independientemente de si a es múltiplo de p o no.

Por lo tanto, $n^p - n$ es divisible por p si p es un número primo. \square

10 Encontrar los números enteros x y y tales que $314x + 159y = 1$.

Para resolver este punto, es preciso usar la identidad de Bézout (aplicar el Teorema de la División repetidamente hasta que el residuo sea 0 y después aplicar una sustitución hacia atrás).

Definición. *Dados dos enteros a y b , ambos diferentes de 0, y siendo d el Máximo Común Divisor. Entonces, existen enteros v y w tales que: $d = av + bw$.*

1. Se aplica el teorema de la división repetidamente hasta que el residuo sea cero.

- $a = 314, b = 159$
 $314 = q_1 * 159 + r_1 = 1 * 159 + 155 = 159 + 155$
- $b = 159, r_1 = 155$
 $159 = q_2 * 155 + r_2 = 1 * 155 + 4 = 155 + 4$
- $r_1 = 155, r_2 = 4$
 $155 = q_3 * 4 + r_3 = 38 * 4 + 3 = 152 + 3$
- $r_2 = 4, r_3 = 3$
 $4 = q_4 * 3 + r_4 = 1 * 3 + 1 = 3 + 1$
- $r_3 = 3, r_4 = 1$
 $3 = q_5 * 1 + r_5 = 3 * 1 + 0 = 3 + 0$
- $r_5 = 0$

2. $r_5 = 0$, entonces, $\text{mcd}(314, 159) = r_4 = d = 1$. Lo cual confirma que la ecuación planteada es correcta.

3. Se procede a aislar los residuos:

- $r_1 = a - q_1 * b$
 $155 = 314 - 1 * 159$ (Ec. 1)
- $r_2 = b - q_2 * r_1$
 $4 = 159 - 1 * 155$ (Ec. 2)
- $r_3 = r_1 - q_3 * r_2$
 $3 = 155 - 38 * 4$ (Ec. 3)
- $r_4 = r_2 - q_4 * r_3$
 $1 = 4 - 1 * 3$ (Ec. 4)

4. Una vez se hayan aislado los residuos, se procede a hacer la “sustitución hacia atrás”:

- $1 = 4 - 1 * 3$
- $1 = 4 - 1 * (155 - 38 * 4)$
(reemplazo de Ec. 3 en Ec. 4)

- $1 = 4 - 1 * 155 + 38 * 4$
(se distribuye el paréntesis)
- $1 = 39 * 4 - 1 * 155$
(se agrupan términos comunes)
- $1 = 39 * (159 - 1 * 155) - 1 * 155$
(reemplazo de Ec. 2 en Ec. 4)
- $1 = 39 * 159 - 39 * 155 - 1 * 155$
(se distribuye el paréntesis)
- $1 = 39 * 159 - 40 * 155$
(se agrupan términos comunes, ya se “encontró” el término $b = 159$)
- $1 = 39 * 159 - 40 * (314 - 1 * 159)$
(reemplazo de Ec. 1 en Ec. 4)
- $1 = 39 * 159 - 40 * 314 + 40 * 159$
(se distribuye el paréntesis)
- $1 = 79 * 159 - 40 * 314$
(se agrupan términos comunes, ya se “encontró” el término $a = 314$)

Ahora, se tiene que $ax + by = d$. Es decir, $314x + 159y = 1$. Entonces $x = -40$ y $y = 79$. Por lo que $1 = 314*(-40) + 159*79 = (-12560) + 12561$.

11 Probar o refutar la siguiente afirmación: si $a^2 \equiv b^2 \pmod{m}$ entonces $a \equiv b \pmod{m}$ o $a \equiv -b \pmod{m}$.

Solución. Supongamos que $a^2 \equiv b^2 \pmod{m}$. Queremos demostrar que esto implica que $a \equiv b \pmod{m}$ o $a \equiv -b \pmod{m}$.

Empecemos por considerar el caso en el que $a \equiv b \pmod{m}$. En este caso, la afirmación es trivialmente verdadera, ya que a y b son congruentes módulo m . Ahora, supongamos que $a \not\equiv b \pmod{m}$. Esto significa que $a - b \not\equiv 0 \pmod{m}$. Queremos demostrar que en este caso, necesariamente se cumple que $a \equiv -b \pmod{m}$.

Dado que $a^2 \equiv b^2 \pmod{m}$, podemos escribirlo como $(a - b)(a + b) \equiv 0 \pmod{m}$. Esto implica que $(a - b)(a + b)$ es divisible por m .

Si m es un número primo, entonces podemos aplicar la propiedad de que si un producto es divisible por un número primo, al menos uno de los factores debe ser divisible por ese número primo. En este caso, llegaríamos a la conclusión de que $a - b \equiv 0 \pmod{m}$ o $a + b \equiv 0 \pmod{m}$. Por lo tanto, la afirmación sería cierta.

Sin embargo, si m no es un número primo, no podemos utilizar directamente esa propiedad. En su lugar, debemos considerar los casos posibles para los factores $(a - b)$ y $(a + b)$.

Si $(a - b)$ y $(a + b)$ son ambos divisibles por m , entonces podemos afirmar que

$a \equiv -b \pmod{m}$.

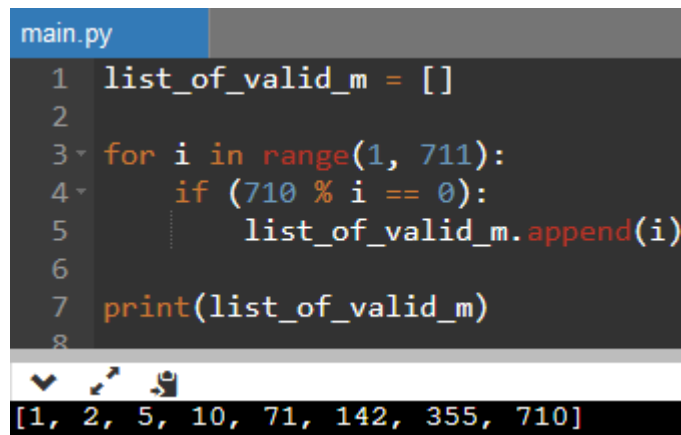
Si $(a - b)$ no es divisible por m , pero $(a + b)$ sí lo es, entonces podemos afirmar que $a \equiv b \pmod{m}$. Esto se debe a que si $(a + b)$ es divisible por m , pero $(a - b)$ no lo es, la única forma de que su producto sea divisible por m es que el factor $(a - b)$ "compense" la falta de divisibilidad.

En cualquier otro caso, es decir, si $(a - b)$ es divisible por m pero $(a + b)$ no lo es, no podemos llegar a ninguna conclusión sobre la congruencia entre a y b módulo m .

En resumen, si $a^2 \equiv b^2 \pmod{m}$, podemos concluir que $a \equiv b \pmod{m}$ o $a \equiv -b \pmod{m}$ si $(a - b)$ y $(a + b)$ son ambos divisibles por m . Si esto no se cumple, no podemos determinar una relación específica entre a y b módulo m . Por lo tanto, la afirmación dada no es siempre verdadera en el caso general. \square

12 Encontrar todos los enteros positivos tales que $1066 \equiv 1776 \pmod{m}$.

$1066 \equiv 1776 \pmod{m}$ puede ser reescrito como $1776 - 1066 \equiv 1066 - 1066$. Que es lo mismo que escribir $710 \equiv 0 \pmod{m}$. Entonces, es necesario hallar los m que cumplan con la siguiente ecuación $710 \bmod m = 0$. Realizando un código en Python, tenemos.



```
main.py
1 list_of_valid_m = []
2
3 for i in range(1, 711):
4     if (710 % i == 0):
5         list_of_valid_m.append(i)
6
7 print(list_of_valid_m)
8
```

[1, 2, 5, 10, 71, 142, 355, 710]

Es decir, todos los m que cumplen con $1066 \equiv 1776 \pmod{m}$ son 1, 2, 5, 10, 71, 142, 355 y 710.

13 Mostrar que la diferencia de dos cubos consecutivos nunca es divisible entre 5.

Solución. Es necesario probar que $(n^3 - (n - 1)^3) \bmod 5 \neq 0$, para cualquier entero n . Para empezar, suponga que $(n^3 - (n - 1)^3) \bmod 5 = 0$.

Si operamos, tenemos que $(n^3 - (n-1)^3) \bmod 5 = (3n^2 - 3n + 1) \bmod 5 = (3n(n-1) + 1) \bmod 5 = 0$.
 $(3n(n-1) + 1) \bmod 5 = 0$ implica que la expresión $(3n(n-1) + 1)$ es múltiplo de 5. O sea, $(3n(n-1) + 1) = 5f$ donde f es cualquier entero (que será el múltiplo de 5). Si desarrollamos:

$$\begin{aligned}(3n(n-1) + 1) &= 5f \\ 3n(n-1) &= 5f - 1 \\ n(n-1) &= \frac{5f-1}{3}\end{aligned}$$

Si esto es cierto, $\frac{5f-1}{3}$ debe ser un número entero. Ahora, suponga que $f = 3k$, donde k es un entero cualquiera. Entonces, reemplazando se tiene:

$$\begin{aligned}n(n-1) &= \frac{5(3k) - 1}{3} \\ n(n-1) &= \frac{15k - 1}{3} \\ n(n-1) &= 5k - \frac{1}{3}\end{aligned}$$

Esto quiere decir que $5k - \frac{1}{3}$ será un entero más una parte decimal. Por lo que bajo ninguna circunstancia será un entero. Es decir, no existe f entero que satisfaga la expresión $(3n(n-1) + 1) = 5f$.

En conclusión, la diferencia de dos cubos consecutivos, nunca será divisible entre 5. \square

14 Encuentre un entero positivo n tal que $3^2|n$, $4^2|n+1$, $5^2|n+2$.

Para resolver este problema, se puede utilizar el Teorema del Resto Chino. Siguiendo las condiciones dadas, se tiene el siguiente sistema de congruencias:

$$\begin{aligned}n &\equiv 0 \pmod{3^2} \\ n+1 &\equiv 0 \pmod{4^2} \\ n+2 &\equiv 0 \pmod{5^2}\end{aligned}$$

Ahora, es preciso encontrar m , es decir, el producto de los módulos: $m = 3^2 \cdot 4^2 \cdot 5^2 = 1800$

A continuación, se calcula los residuos inversos y_i para cada módulo m_i utilizando el algoritmo extendido de Euclides. Los residuos inversos satisfacen la propiedad de que $n_i * y_i \equiv 1 \pmod{n_i}$, donde n_i es el módulo correspondiente. En este caso, los residuos inversos son:

$$y_1 = 100$$

$$y_2 = 25$$

$$y_3 = 144$$

Finalmente, la solución para el sistema de congruencias es: $n = (0 \cdot 3^2 \cdot 100 + 1 \cdot 4^2 \cdot 25 + 2 \cdot 5^2 \cdot 144) \pmod{1800}$

Simplificando esta expresión, se obtiene: $n = 3600 + 400 + 1440 \equiv 5600 \equiv 800 \pmod{1800}$

Por lo tanto, un entero positivo n que satisface las condiciones dadas es $n = 800$.

15 ¿Cuál es el último dígito de 7^{355} ?

Hallar el último dígito de 7^{355} significa hallar $7^{355} \pmod{10}$.

Primero, es preciso hallar los patrones que involucran $7^i \pmod{10}$, donde $i \in \mathbb{Z} > 0$.

$$7^1 \pmod{10} = 7$$

$$7^2 \pmod{10} = 9$$

$$7^3 \pmod{10} = 3$$

$$7^4 \pmod{10} = 1$$

$$7^5 \pmod{10} = 7$$

$$7^6 \pmod{10} = 9$$

$$7^7 \pmod{10} = 3$$

$$7^8 \pmod{10} = 1$$

Cada 4 iteraciones se repite el patrón (al igual que $7^i \pmod{100}$), entonces, es preciso saber en qué “posición” dentro del patrón se encontraría el exponente 355 (hallando el residuo de dividirlo entre 4, el número de patrones).

$355 \pmod{4} = 3$. Es decir, $7^{355} \equiv 7^3 \pmod{10}$, lo que quiere decir que el último dígito de 7^{355} es 3.

16 Muestre que $3k+4$ y $4k+5$ no tienen un factor común más grande que 1.

Mostrar que $3k+4$ y $4k+5$ no tienen un factor común más grande que 1 es mostrar que $3k+4$ y $4k+5$ son números coprimos (aquellos cuyo único divisor común es 1).

Solución. Suponga que $3k+4$ y $4k+5$ NO son coprimos. O sea, $\gcd(3k+4, 4k+5) \neq 1$

Ahora, se puede expresar $3k+4$ y $4k+5$ de la siguiente manera: $3k+4 = d * n$ y $4k+5 = d * m$ (donde n y m son enteros cualquiera).

Simplificando las ecuaciones se tiene:

$$\begin{aligned}k &= \frac{dn-4}{3} = \frac{dm-5}{4} \\4dn-16 &= 3dm-15 \\d(4n-3m) &= 1\end{aligned}$$

Esto quiere decir que $d = 4n - 3m = 1$, lo que implica que el máximo común divisor solo puede ser 1. Entonces, $3k+4$ y $4k+5$ son coprimos. \square