

Taller teoría de números

David Santiago Cruz Hernandez

Mayo 12 2023

1. ¿Existen enteros a y b tal que $a+b=544$ y cuyo máximo común divisor es 11?

Primero se deben buscar los números cuyo MCD (máximo común divisor) sea 11, estos pueden ser definidos de la forma $11a$, donde a es un número entero y tendrá un MCD = 11. Esto se debe a que 11 es un número primo y, por lo tanto, su único divisor positivo es 1 y el propio 11.

Dicho esto, se asume que $a = 11a$ y se puede usar la fórmula $544 = 11a + 11b$ para hallar un a o un b que satisfaga esta ecuación. No obstante, teniendo en cuenta que ambos números deben tener como MCD = 11 no existe un número de la forma $11a$ y de la forma $11b$ que de como resultado 544 y tengan 11 como MCD.

2. Encuentre una regla de divisibilidad para 8 y para 16.

Esto se puede determinar para un n si tiene la forma a_n, a_{n-1}, a_{n-2} el cual sea divisible por 8 sí y sólo sí el número a_{n-2}, a_{n-1} son divisibles por 8.

Esto se puede determinar de manera similar a la regla de divisibilidad para el número 16. Para un n si tiene la forma $a_n, a_{n-1}, a_{n-2}, a_{n-3}$ el cual sea divisible por 16 sí y sólo sí el número $a_{n-3}, a_{n-2}, a_{n-1}$ son divisibles por 16.

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

Como $a^2 \equiv b^2 \pmod{p}$, entonces se puede plantear como:

$$\begin{aligned} a^2 - b^2 &\equiv 0 \pmod{p} \\ a^2 - b^2 &= k \cdot p \end{aligned}$$

Como $a^2 - b^2$ es una diferencia de cuadrados, se puede plantear como:

$$(a - b)(a + b) = k \cdot p$$

Por lo tanto, p debe dividir a ambos términos (en paréntesis):

Como p divide a $(a - b)$, entonces se cumple que:

$$\begin{aligned} a - b &\equiv 0 \pmod{p} \\ a &\equiv b \pmod{p} \end{aligned}$$

Como p también divide a $(a + b)$, entonces se cumple que:

$$\begin{aligned} a + b &\equiv 0 \pmod{p} \\ a &\equiv -b \pmod{p} \end{aligned}$$

Por lo tanto, se cumple que:

$$a \equiv b \equiv -b \pmod{p} \rightarrow a \equiv \pm b \pmod{p}$$

4. Encuentre el resto cuando 19^{19} es dividido por 5.

Al realizar factor común a $19^{19} \cong \text{mod } 5$ se puede observar el siguiente patrón:

$$\begin{aligned} 19^1 &\cong 4 \text{ mod } 5 \\ 19^2 &\cong 1 \text{ mod } 5 \\ 19^3 &\cong 4 \text{ mod } 5 \\ 19^4 &\cong 1 \text{ mod } 5 \end{aligned}$$

Por lo cual

$$\begin{aligned} 19^{19} &\cong (19^4)^4 * 19^3 \\ (19^4)^4 * 19^3 &\cong 1^4 * 4 \\ 1^4 * 4 &\cong 4 \end{aligned}$$

Por tanto

$$19^{19} \cong 4(\text{mod } 5)$$

```

Códigos > suma.py > ...
1  a = 19**19 % 5
2
3  print(a)
4
5

PROBLEMS  OUTPUT  DEBUG CONSOLE  TERMINAL  JUPYTER

PS G:\Mi unidad\Códigos> & "C:/Program Files/Python311/python.exe" "g:/Mi unidad/Códigos/suma.py"
4

```

$$19^{19}(\text{mod } 5)$$

5. Encuentre los últimos dos dígitos de 7^{7^7} .

Para hallar los dos últimos dígitos se puede hacer $n(\text{mod } 100)$ Sabiendo que 7^{7^7} es un producto consecutivo de números impares, se puede utilizar la fórmula de los números impares $2k + 1$ por lo tanto:

$$7^{7^7} \cong \text{mod } 100$$

Por ley de los exponentes

$$\begin{aligned} 7^{(2k+1)(2k+1)} &\cong \text{mod } 100 \\ 7^{(4k^2+4k+1)} &\cong \text{mod } 100 \\ (7)4k^2 * 7 &\cong \text{mod } 100 \\ ((7)^2)^k * ((7)^2)^k * 7 &\cong \text{mod } 100 \\ 16807 &\cong 7 \text{ mod } 100 \end{aligned}$$

Por lo tanto los dos últimos dígitos de 7^{7^7} son 07

```

Codigos > suma.py > ...
1  a = ((7)**7)**7
2
3  print(a)
4
5  b = ((7)**7)**7 % 100
6
7  print(b)

```

PROBLEMS OUTPUT DEBUG CONSOLE TERMINAL JUPYTER

```

PS G:\Mi unidad\Codigos> & "C:/Program Files/Python311/python.exe" "g:/Mi unidad/Codigos/suma.py"
256923577521058878088611477224235621321607
7

```

$$7^{7^7}$$

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

- $n = 35$

```

Orden del Grupo G: 35

Tiempo de ejecución del Metodo Alternativo: 0.001 segundos.
→ Descomposición de Factores Primos de n: 51·71
→ Número de Generadores Cíclicos de G:
    ψ(35) = ψ(51·71) = ψ(51)·ψ(71) = (51-50)·(71-70) = 24

```

$$\phi(35) = 24$$

- $n = 100$

```

Orden del Grupo G: 100

Tiempo de ejecución del Metodo Alternativo: 0.001 segundos.
→ Descomposición de Factores Primos de n: 22·52
→ Número de Generadores Cíclicos de G:
    ψ(100) = ψ(22·52) = ψ(22)·ψ(52) = (22-21)·(52-51) = 40

```

$$\phi(100) = 40$$

- $n = 51200$

```

Orden del Grupo G: 51200

Tiempo de ejecución del Metodo Alternativo: 0.0 segundos.
→ Descomposición de Factores Primos de n:  $2^{11} \cdot 5^2$ 
→ Número de Generadores Cíclicos de G:
 $\varphi(51200) = \varphi(2^{11} \cdot 5^2) = \varphi(2^{11}) \cdot \varphi(5^2) = (2^{11} - 2^{10}) \cdot (5^2 - 5^1) = 20480$ 

```

$$\phi(51200) = 20480$$

7. Usted le pregunta a un robot que quiere comer. El responde "48.879". Sabiendo que el robot piensa en hexadecimal pero habla el decimal, ¿Qué le debería dar de comer?.

Se debe convertir el mensaje del robot (en decimal), a su pensamiento original (en hexadecimal). Para ello, se va a utilizar este algoritmo de la división iterativo en 16 (Base hexadecimal):

```

Algoritmo de la División:  $a = q \cdot n + r$ 

a = 48879, n = 16

48879 = 3054 \cdot 16 + 15
3054 = 190 \cdot 16 + 14
190 = 11 \cdot 16 + 14
11 = 0 \cdot 16 + 11

```

$$15 = F, 14 = E, 14 = E, 11 = B$$

Se concatenan los residuos hexadecimales de abajo hacia arriba:

*The Robot want: **BEEF***

8. ¿65.314.638.792 es divisible por 24?.

Para verificar que 65.314.638.792 es divisible por 24 se puede establecer reglas de divisibilidad que verifiquen que esta divisibilidad sea posible. Podemos expresar el 24 como $8 \cdot 3$ y si las reglas de divisibilidad para 8 y para 3 se cumplen, también se debe cumplir para 24

Primero se debe establecer la regla de divisibilidad para 8 considerando sus tres últimas cifras. Si estas tres cifras forman un número que sea divisible por 8, quiere decir que el número original es divisible por 8. De tal manera que:

$$\begin{aligned}
 a &= qn + r \\
 792 &= (8 * n) + r \\
 792 &= (8 * 99) + 0
 \end{aligned}$$

Entonces, 65.314.638.792 es divisible por 8.

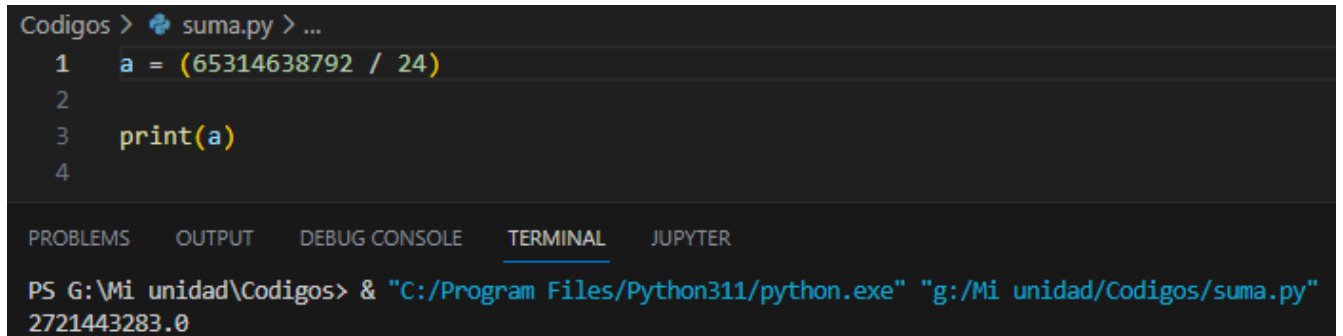
Ahora se debe establecer la regla de divisibilidad para 3 considerando la suma de todas sus cifras. Si la sumatoria de todas las cifras forman un número que sea divisible por 3,

quiere decir que el número original es divisible por 3. De tal manera que:

$$\begin{aligned} a &= qn + r \\ 6 + 5 + 3 + 1 + 4 + 6 + 3 + 8 + 7 + 9 + 2 &= (3 * n) + r \\ 54 &= (3 * n) + r \\ 54 &= (3 * 18) + 0 \end{aligned}$$

Entonces, 65.314.638.792 es divisible por 3.

Por lo anterior se demuestra que si 65.314.638.792 es divisible por 8 y 3 entonces es divisible por 24.



```
Codigos > suma.py > ...
1 a = (65314638792 / 24)
2
3 print(a)
4

PROBLEMS OUTPUT DEBUG CONSOLE TERMINAL JUPYTER
PS G:\Mi unidad\Codigos> & "C:/Program Files/Python311/python.exe" "g:/Mi unidad/Codigos/suma.py"
2721443283.0
```

$$65.314.638.792/24$$

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

Como p es un número primo, y considerando que n no es divisible por p , se puede utilizar el **Pequeño Teorema de Fermat**, que establece que: $n^{p-1} \equiv 1 \pmod{p}$

Así que, si se multiplica por n a ambos lados, se obtiene que:

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

Se operan las potencias:

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

Se despeja n , y se obtiene que:

$$n^p - n \equiv 0 \pmod{p}$$

Por lo tanto, $n^p - n$ SI es divisible por p :

$$n^p - n = k \cdot p$$

10. Encuentre los enteros x y y tal que $314x + 159y = 1$.

```

    ALGORITMO DE EUCLIDES
    Algoritmo de la División:  $a = q \cdot n + r$ 

     $a = 314, n = 159$ 

     $314 = 1 \cdot 159 + 155$ 
     $159 = 1 \cdot 155 + 4$ 
     $155 = 38 \cdot 4 + 3$ 
     $4 = 1 \cdot 3 + 1$ 
     $3 = 3 \cdot 1 + 0$ 

    El Máximo Común Divisor entre 314 y 159 es: 1.

    IDENTIDAD DE BEZOUT

     $1 = 1 (4) - 1 [155 - 38 \cdot 4] = 39 (4) - 1 (155)$ 

     $1 = 39 [159 - 1 \cdot 155] - 1 (155) = 39 (159) - 40 (155)$ 

     $1 = 39 (159) - 40 [314 - 1 \cdot 159] = 79 (159) - 40 (314)$ 

     $1 = 79 (159) - 40 (314)$ , se puede reorganizar como:
     $1 = 79 (159) + (-40) (314)$ 

```

$$x = -40, y = 79$$

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

Para comprobar o refutar esta afirmación, se tomará como ejemplo los siguientes números:

Sea $m = 15, a = 2$ y $b = 8$.

Se tiene que:

$$\begin{aligned} a^2 &\cong 2^2 \cong 4 \cong 4 \pmod{15} \\ b^2 &= 8^2 = 64 \equiv 4 \pmod{15} \end{aligned}$$

Por lo tanto,

$$a^2 \equiv b^2 \pmod{15}.$$

Sin embargo, no es cierto que

$$a \equiv b \pmod{15} \text{ o } a \equiv -b \pmod{15}, \text{ ya que:}$$

$$a = 2 \equiv 2 \pmod{15}$$

$$b = 8 \equiv 8 \pmod{15}$$

y tampoco se cumple que

$$a \equiv -b \pmod{15}, \text{ ya que:}$$

$$a = 2 \equiv 13 \pmod{15}$$

$$-b = -8 \equiv 7 \pmod{15}$$

Por lo tanto, se tiene que la afirmación es falsa.

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

$$\begin{aligned} 1066 &\equiv 1776 \pmod{m} \\ 1066 &= 1776 + m \cdot k. \\ 1066 - 1776 &= 0 + m \cdot k. \\ -710 &= 0 + m \cdot k. \\ -710 &\equiv 0 \pmod{m}. \end{aligned}$$

Como es congruente con 0, se puede tomar tanto negativo, como su valor positivo (ya que los posibles K son múltiplos de m).

$$710 = 0 + m \cdot k.$$

Por lo tanto, basta con calcular los divisores positivos de 710 (aquellos numero que cumplen con la expresión anterior: $710 = 0 + m \cdot k$)

Los divisores positivos de 710 son:
[1, 2, 5, 10, 71, 142, 355]

Números que cumplen con la expresión: $710 = 0 + m \cdot k$

13. Muestre que la diferencia de dos cubos consecutivos nunca es divisible por 5.

Sea un $n \in \mathbb{Z}$ arbitrario, dada la afirmación:

$$\begin{aligned} (n+1)^3 - n^3 &\cong \delta = n^3 + 3n^2 + 3n + 1 - n^3 \\ \delta &= 3n(n+1) + 1 \end{aligned}$$

Se sabe que un número entero arbitrario se puede expresar como: $5k, 5k+1, 5k+2, 5k+3, 5k+4, 5k+5, \dots, 5k+n$

Entonces, para $n = 5k$:

$$\begin{aligned} \delta &= 5(3)(5k+1) + 1 \\ \delta - 1 &= 5k \\ \delta &\cong 1 \pmod{5} \end{aligned}$$

De manera análoga se tiene que para $n = 5k+1$:

$$\begin{aligned} \delta &= 3(5k+1)(5k+2) + 1 \\ \delta &= 5(3)(5k^2 + 2k + k) + 6 + 1 \\ \delta - 7 &= 5k \\ \delta &\cong 7 \cong 2 \pmod{5} \end{aligned}$$

Para $n = 5k+2$:

$$\begin{aligned} \delta &= 3(5k+2)(5k+3) + 1 \\ \delta &= 5(3)(5k^2 + 3k + 2k) + 18 + 1 \\ \delta - 19 &= 5k \\ \delta &\cong 19 \cong 4 \pmod{5} \end{aligned}$$

Para $n = 5k+3$:

$$\begin{aligned} \delta &= 3(5k+3)(5k+4) + 1 \\ \delta &= 5(3)(5k^2 + 4k + 3k) + 36 + 1 \end{aligned}$$

$$\begin{aligned}\delta - 37 &= 5k \\ \delta &\cong 37 \cong 2 \pmod{5}\end{aligned}$$

Para $n = 5k + 4$:

$$\begin{aligned}\delta &= 3(5k + 4)(5k + 5) + 1 \\ \delta &= 5(3)(5k^2 + 5k + 4k) + 60 + 1 \\ \delta - 61 &= 5k \\ \delta &\cong 61 \cong 1 \pmod{5}\end{aligned}$$

Por lo tanto, no existe un $n, (n + 1) \in \mathbb{Z}$ cuya diferencia de sus cubos tenga una división exacta entre 5.

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

- $3^2 \mid n$

Como 3^2 divide a n , se puede expresar como:

$$\begin{aligned}n &= k \cdot 3^2 \\ n &= k \cdot 9\end{aligned}$$

Por lo tanto, cualquier múltiplo de 9 (expresado como $k \cdot 9$),
corresponde al entero positivo n :

$$\begin{aligned}18 &= 2 \cdot 3^2 \rightarrow 3^2 \mid 18 \\ 27 &= 3 \cdot 3^2 \rightarrow 3^2 \mid 27 \\ 36 &= 4 \cdot 3^2 \rightarrow 3^2 \mid 36\end{aligned}$$

- $4^2 \mid n + 1$

Como 4^2 divide a $n + 1$, se puede expresar como:

$$\begin{aligned}n + 1 &= 0 + k \cdot 4^2 \\ n + 1 &= 0 + k \cdot 16 \\ n &= -1 + k \cdot 16 \\ n &\equiv -1 \pmod{16}\end{aligned}$$

Por lo tanto, n corresponde al cualquier número positivo que cumpla con la congruencia:

$$\begin{aligned}15 &\equiv -1 \pmod{16} \rightarrow 4^2 \mid 15 + 1 \\ 31 &\equiv -1 \pmod{16} \rightarrow 4^2 \mid 31 + 1 \\ 47 &\equiv -1 \pmod{16} \rightarrow 4^2 \mid 47 + 1\end{aligned}$$

- $5^2 \mid n + 2$

Como 5^2 divide a $n + 2$, se puede expresar como:

$$\begin{aligned}n &= k \cdot 5^2 \mid n + 2 \quad n + 2 = 0 + k \cdot 25 \\ n &= -2 + k \cdot 25 \\ n &\equiv -2 \pmod{25}\end{aligned}$$

Por lo tanto, n corresponde al cualquier número positivo que cumpla con la congruencia:

$$\begin{aligned}23 &\equiv -2 \pmod{25} \rightarrow 5^2 \mid 23 + 2 \\ 48 &\equiv -2 \pmod{25} \rightarrow 5^2 \mid 48 + 2 \\ 73 &\equiv -2 \pmod{25} \rightarrow 5^2 \mid 73 + 2\end{aligned}$$

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

Para ello se debe determinar un $n \pmod{10}$.

Para $n = 7^{355}$

$$\begin{aligned}
&7^{354+1} \bmod 10 \\
&(7^2)^n \bmod 10 \\
&9 * 7 \bmod 10 \\
&63 \bmod 10 \\
&3
\end{aligned}$$

De esta manera, se puede afirmar que el último dígito de 7^{355} es 3.

```

Codigos > suma.py > ...
1  a = (7)**355
2
3  print(a)
4
5  b = (7)**355 % 10
6
7  print(b)

```

PROBLEMS OUTPUT DEBUG CONSOLE TERMINAL JUPYTER

PS G:\Mi unidad\Codigos> & "C:/Program Files/Python311/python.exe" "g:/Mi unidad/Codigos/suma.py"

1022831760466051670409848066539662073905087543301674648579658274804249423378253098383504632739938574586749061841502160063941822079560091329657
888872661595591342341233193279587163656384106958221982493551112468151234550629604561727268100420434285770519972365028810684127481943
3

$$7^{355}$$

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

Para ello, se debe suponer $d \in \mathbb{Z}$ tal que $d > 1$ y $d \mid 3k + 4$ así como $d \mid 4k + 5$. Por lo tanto, la división de estos factores por d tiene el mismo residuo:

$$\begin{aligned}
4k + 5 &\cong 3k + 4 \pmod{d} \\
4k + 5 - 3k + 4 &= dn \\
k + 1 &= dn \\
k &= dn - 1
\end{aligned}$$

Como $d \in 3k + 4$ por hipótesis, $3k + 4 = dm$, reemplazando:

$$\begin{aligned}
3(dn - 1) + 4 &= dm \\
4 - 3 &= d(m - 3n) \\
1 &= d\beta
\end{aligned}$$

Dado que $\beta \in \mathbb{Z}, \beta = 1/d$, donde d debe ser un divisor de 1, en otras palabras, $d = 1$. Pero, dado que $d > 1$ entonces por hipótesis demuestra que es un absurdo. Así pues, $3k + 4$ y $4k + 5$ no tienen un factor común más grande que 1.