Taller teoría de números

David Alexander Rativa Gutierrez

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 $a^2 \cong b^2 (\mathrm{mod} p)$, pruebe que $a \cong \pm b$.

   Dados un a y un $b \in Z$ arbitrarios, tales que $a^2 \equiv b^2 (\mathrm{mod} p)$ con p como un número primo, entonces $p \mid \left(a^2 - b^2\right) = (a - b)(a + b)$.
   por el Lema de Euler se puede afirmar que: Si n es un número entero y divide a un producto (ab) y es coprimo con uno de los factores, entonces n divide al otro factor.

   De tal modo se tiene $(a - b)$ es coprimo con p. teniendo en cuenta el lema de euler, se tiene que $p \mid (\ a + b)$ y que por definición de congruencia implica que $a \equiv -b (\mathrm{mod} p)$.
   Entonces, para $p \mid (a - b)$, dado que p tambien es coprimo a $(a + b)$, y por lo tanto $a \equiv b (\mathrm{mod} p)$. Así pues $a \equiv \pm b (\mathrm{mod} p)$ si $a^2 \equiv b^2 (\mathrm{mod} p)$.

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

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

$$19^1 \cong 4 \bmod 5$$
$$19^2 \cong 1 \bmod 5$$
$$19^3 \cong 4 \bmod 5$$
$$19^4 \cong 1 \bmod 5$$

Por lo cual

$$19^{19} \cong (19^4)^4 * 19^3$$
$$(19^4)^4 * 19^3 \cong 1^4 * 4$$
$$1^4 * 4 \cong 4$$

Por tanto

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

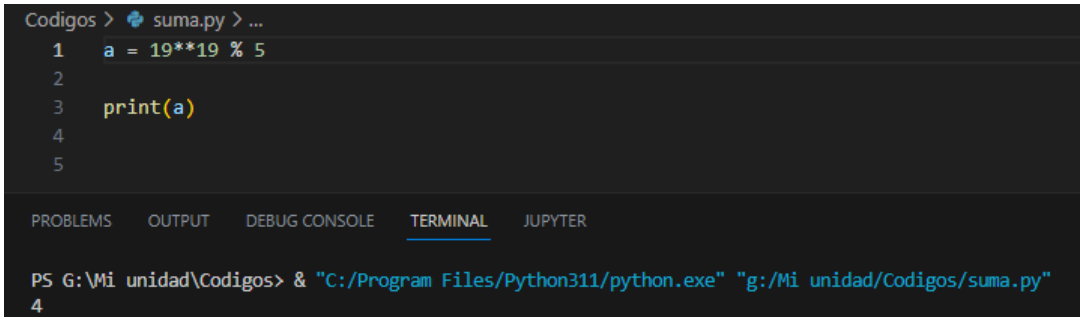

Figura 1: $19^{19}(\text{mod}5)$

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

Para hallar los dos últimos dígitos se puede hacer $n(mod100)$ 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

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

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

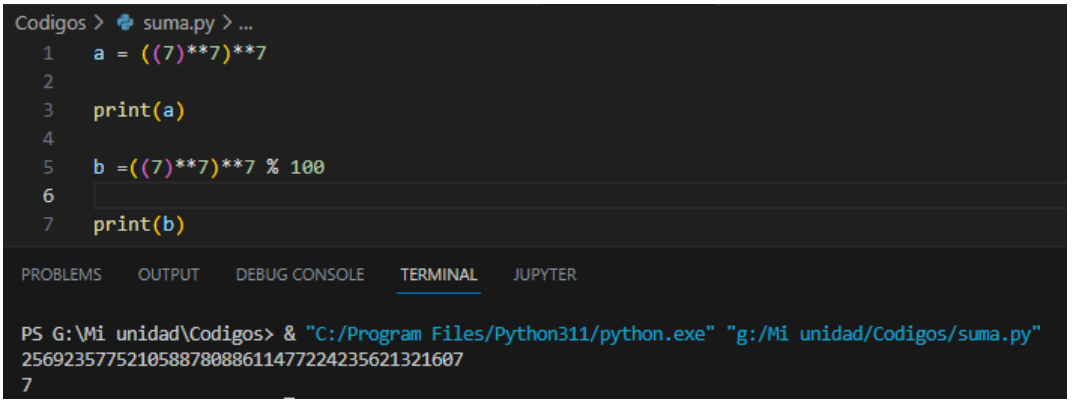

Figura 2: 7^{7^7}

6. Encuentre $\phi(n)$ para $n = 35, n = 100, n = 51200$.
Para ello se utiliza la función Totient de Euler bajo las siguientes propiedades:

$\phi(1) = 1$ - $\phi(p^a) = p^a - p^{a-1} = p^a\left(1 - \frac{1}{p}\right)$ - $mcd(m,n) = 1 \longrightarrow \phi(m \cdot n) = \phi(m)\phi(n)$
Donde, teniendo en cuenta la tercera propiedad, es posible descomponer el n es factores primos, tales que, $n = p_1^a p_2^b \cdots p_s^r$ y $mcd\,(p_x, p_y) = 1$, de modo que

$$\phi(n) = \phi\left(p_1^a\right)\phi\left(p_2^b\right)\cdots\phi\left(p_s^r\right)p_1^a\left(1-\frac{1}{p_1}\right)\cdots p_s^r\left(1-\frac{1}{p_s}\right), p_1^a\cdots p_s^r\left(1-\frac{1}{p_1}\right)\cdots\left(1-\frac{1}{p_s}\right)n\prod_1^s\left(1-\frac{1}{p_i}\right)$$

- 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:
      φ(35) = φ(5¹•7¹) = φ(5¹)•φ(7¹) = (5¹-5⁰)•(7¹-7⁰) = 24
```

Figura 3: $\phi(35) = 24$

- 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:
      φ(100) = φ(2²•5²) = φ(2²)•φ(5²) = (2²-2¹)•(5²-5¹) = 40
```

Figura 4: $\phi(100) = 40$

- n = 51200

```
                Orden del Grupo G: 51200

Tiempo de ejecución del Metodo Alternativo: 0.0 segundos.
→ Descomposición de Factores Primos de n: 2¹¹•5²
→ Número de Generadores Cíclicos de G:
     φ(51200) = φ(2¹¹•5²) = φ(2¹¹)•φ(5²) = (2¹¹-2¹⁰)•(5²-5¹) = 20480
```

Figura 5: $\phi(51200) = 20480$

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) iterando hasta que el cociente obtenido de la operación sea tal que $q < 16$.
   $10 = \mathrm{A}$
   $11 = \mathrm{B}$
   $12 = C$

$13 = D$
$14 = E$
$15 = F$

Figura 6: Algoritmo de la división aplicado al problema

Se concatenan los residuos hexadecimales de abajo hacia arriba:

El robot quiere ***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 $8 * 3$ 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:

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

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:

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

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.

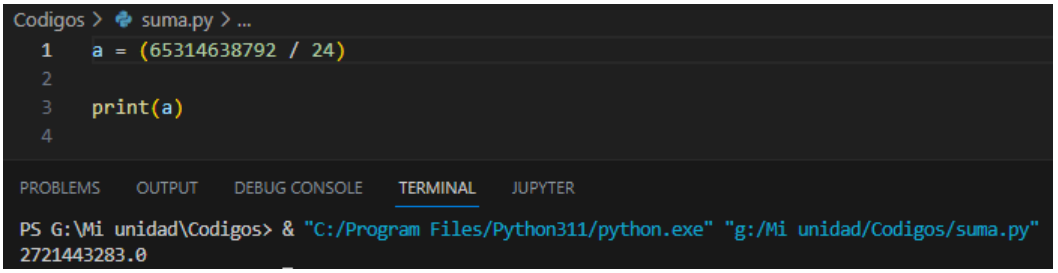

Figura 7: 65.314.638.792/24

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

   Sea un $n \in Z$ arbitrario y p un número primo. Se tienen los dos siguientes casos: $p \mid n$ y pn.
   Sea $p \mid n$.
   Se asume que p divide a cualquier escalar de n, incluyendo n^p, de modo que:

   $$n^p - n = p(\bar{k} - k)n^p - n = p\delta p \mid (n^p - n)$$

   Sea p, n números coprimos.

   $$(n^p - n) = \left(n\delta n^{p-1} - n\right)$$

   Por el pequeño teorema de Fermat, $n^{p-1} \equiv 1(\mathrm{mod}p)$, de tal manera que:

   $$\begin{gathered} n\left(n^{p-1}\right) - n \pmod{p} \\ n(1) - n \pmod{p} \\ 0 \pmod{p} \\ (n^p - n) \equiv 0 \pmod{p} \end{gathered}$$

   Lo que implica por definición de congruencia y divisibilidad

   $$p \mid (n^p - n).$$

   Por lo tanto, $p \mid (n^p - n)$ únicamente si p es primo.

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

    Se tiene $a = 314, b = 159$, de tal manera que x y y son equivalentes a los números de Bézout, tales que, $mcd(a, b) = 1 = ax + by$.

    Es posible entonces aplicar el algoritmo de Bézout para los números de Bézout para hallar los respectivos coeficientes. De tal manera que:

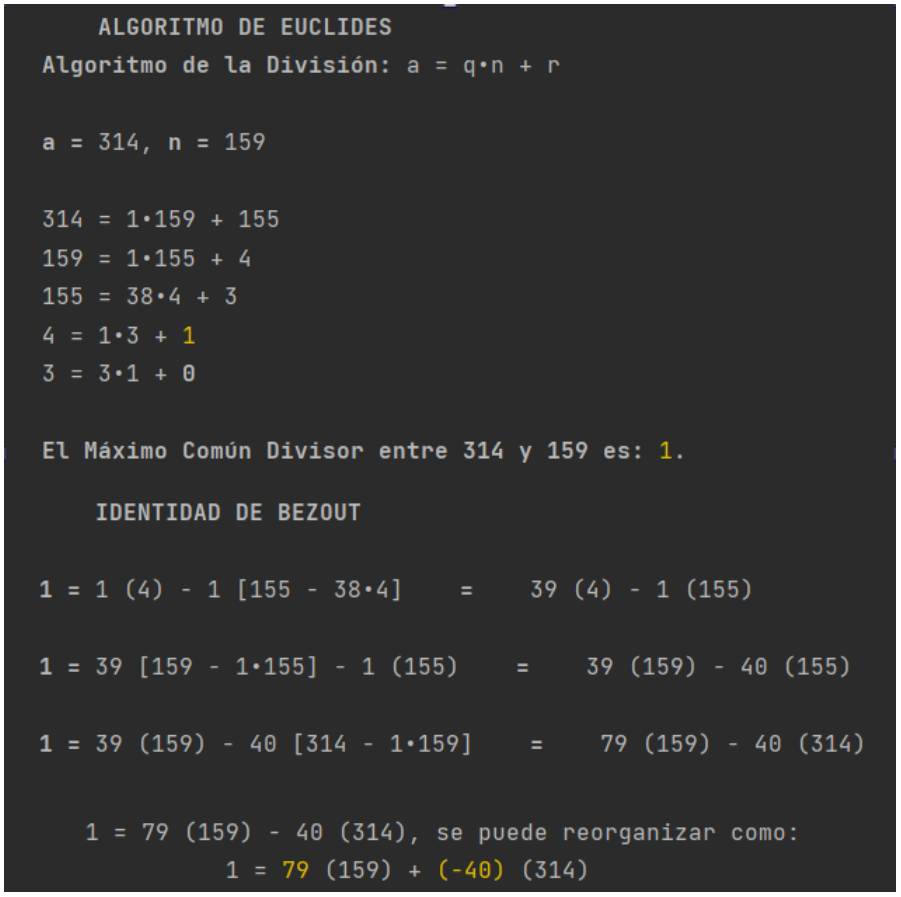

Figura 8: $x = -40$, $y = 79$

De modo que.

$$x = -40 y = 79$$

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

Para comprobar o refutar esta afirmación, se tomará como ejemplo los siguientes números:
Sea $m = 15, a = 2$ y $b = 8$.
Se tiene que:

$$a^2 \cong 2^2 \cong 4 \cong 4 (\mathrm{mod} 15)$$
$$b^2 = 8^2 = 64 \equiv 4 (\mathrm{mod} 15)$$

Por lo tanto,

$$a^2 \equiv b^2 (\mathrm{mod} 15).$$

Sin embargo, no es cierto que

$$a \equiv b (\mathrm{mod} 15) \text{ o } a \equiv -b (\mathrm{mod} 15), \text{ ya que:}$$
$$a = 2 \equiv 2 (mod 15)$$
$$b = 8 \equiv 8 (mod 15)$$

y tampoco se cumple que

$$a \equiv -b (mod 15), \text{ ya que:}$$
$$a = 2 \equiv 13 (mod 15)$$
$$-b = -8 \equiv 7 (mod 15)$$

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

12. Encuentre todos los enteros positivos tales que $1066 \cong 1776 (\mathrm{mod} m)$.

Teniendo en cuenta las propiedades de la aritmética modular, se puede transformar la expresión inicial:

$$\begin{gathered} 1066 \equiv 1776 \pmod{m} \\ 1066 - 1066 \equiv 1776 - 1066 \pmod{m} \\ 0 \equiv 710 \pmod{m} \end{gathered}$$

Dada la expresión equivalente resultante, se determina que m es todos los enteros divisores de 710 .

$$m \in \left\{ x : 710 \mid x, x \in Z^{+} \right\}$$

Dicho esto, se hace un algoritmo para calcular estos divisores de 710:

```
Codigos > suma.py > divisores
1   def divisores(n):
2     divisores = []
3     for i in range(1, int(n**0.5) + 1 ):
4       if n % i == 0:
5         divisores.extend([i, int(n/i)])
6     return sorted(divisores)
7
8   n = 710
9   print( f'Divisores para {n}:\n{divisores(n)}' )

PROBLEMS  OUTPUT  DEBUG CONSOLE  TERMINAL  JUPYTER

PS G:\Mi unidad\Codigos> & "C:/Program Files/Python311/python.exe" "g:/Mi unidad/Codigos/suma.py"
Divisores para 710:
[1, 2, 5, 10, 71, 142, 355, 710]
```

Figura 9: Algoritmo para calcular los divisores de 710

De tal manera que:

$$m \in \{1, 2, 5, 10, 71, 142, 355, 710\}$$

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

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

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

Se sabe que un número entero arbitrario se puede expresar como: $5k, 5k+1, 5k+2, 5k+3, 5k+4, 5k+5, ...5k+n$
Entonces, para $n = 5k$:

$$\begin{gathered} \delta = 5(3)(5k+1) + 1 \\ \delta - 1 = 5k \\ \delta \cong 1 (\mathrm{mod} 5) \end{gathered}$$

De tal modo se tiene que para $n = 5k + 1$:

$$\delta = 3(5k+1)(5k+2)+1$$
$$\delta = 5(3)(5k^2+2k+k)+6+1$$
$$\delta - 7 = 5k$$
$$\delta \cong 7 \cong 2(\text{mod}5)$$

Para $n = 5k+2$:

$$\delta = 3(5k+2)(5k+3)+1$$
$$\delta = 5(3)(5k^2+3k+2k)+18+1$$
$$\delta - 19 = 5k$$
$$\delta \cong 19 \cong 4(\text{mod}5)$$

Para $n = 5k+3$:

$$\delta = 3(5k+3)(5k+4)+1$$
$$\delta = 5(3)(5k^2+4k+3k)+36+1$$
$$\delta - 37 = 5k$$
$$\delta \cong 37 \cong 2(\text{mod}5)$$

Para $n = 5k+4$:

$$\delta = 3(5k+4)(5k+5)+1$$
$$\delta = 5(3)(5k^2+5k+4k)+60+1$$
$$\delta - 61 = 5k$$
$$\delta \cong 61 \cong 1(\text{mod}5)$$

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

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

Se determina el siguiente sistema de congruencias:

$$\begin{aligned} n &\equiv 0 \pmod 9 \\ n+1 &\equiv 0 \pmod{16} \\ n+2 &\equiv 0 \pmod{25} \end{aligned}$$

El cual es equivalente a:

$$\begin{aligned} n+2 &\equiv 2 \pmod 9 \\ n+2 &\equiv 1 \pmod{16} \\ n+2 &\equiv 0 \pmod{25} \end{aligned}$$

Aplicando el teorema del resto chino:

$$m = 3^2 4^2 5^2 = 3600$$
$$M_1 = 4^2 5^2 = 400$$
$$M_2 = 3^2 5^2 = 225$$
$$M_3 = 3^2 4^2 = 144$$

Para determinar los inversos se hace uso del algoritmo de Bézout.

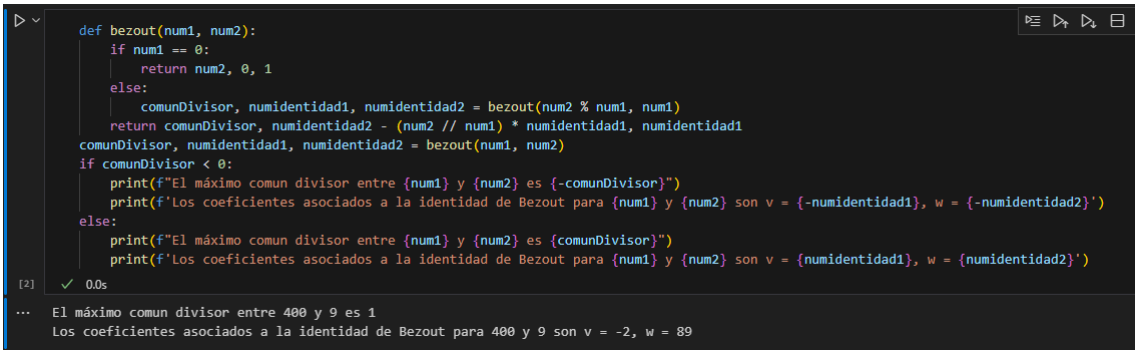

Figura 10: Algoritmo para calcular los inversos de 400

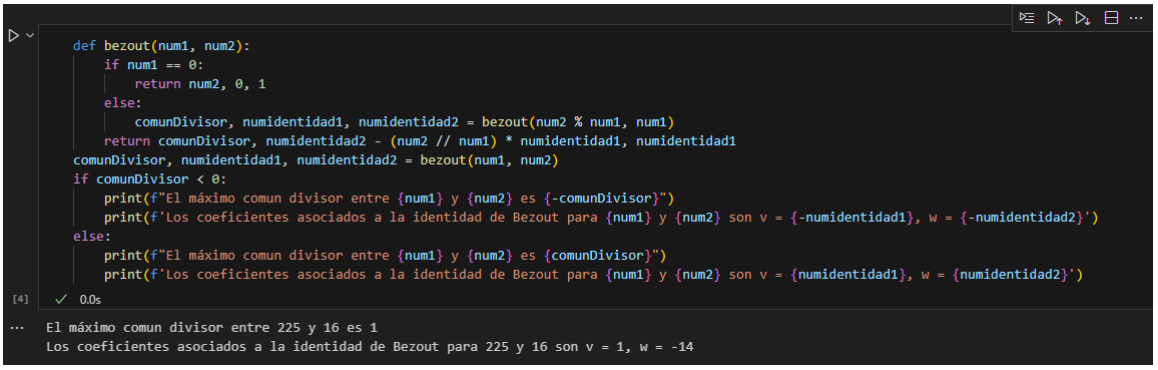

Figura 11: Algoritmo para calcular los inversos de 225

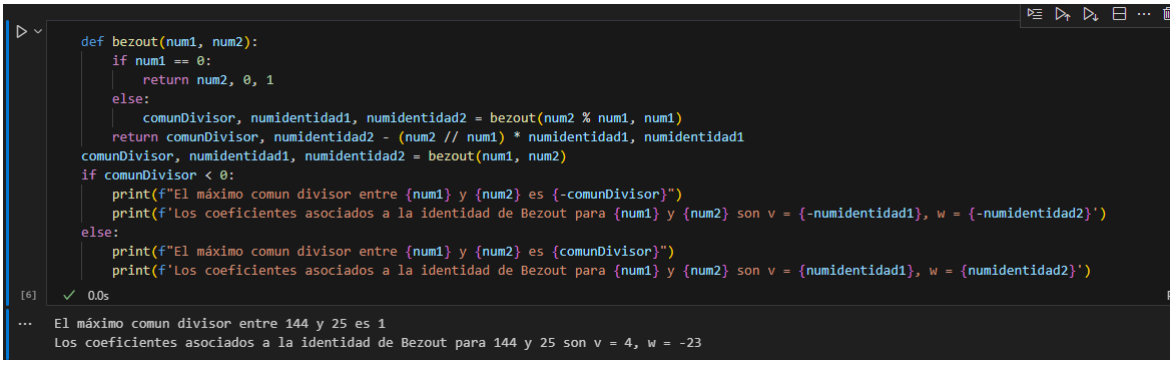

Figura 12: Algoritmo para calcular los inversos de 144

De modo que.

$$v_1 = -2v_2 = 1$$

Por lo tanto:

$$\begin{aligned} \text{n+2} = \; & 2\left(4^2 5^2\right)(-2) + 1\left(3^2 5^2\right)(1) + 0 \\ & = -1600 + 225 \\ & = -1375 \\ & -1375 \pmod{m} \\ & (2225 - 3600) \pmod{3600} \\ & (2225 - 0) \pmod{3600} \\ & n = 2225 - 2 \\ & n = 2223 \end{aligned}$$

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

Para ello se debe determinar un $n(\text{mod}10)$.
Para $n = 7^{355}$

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

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

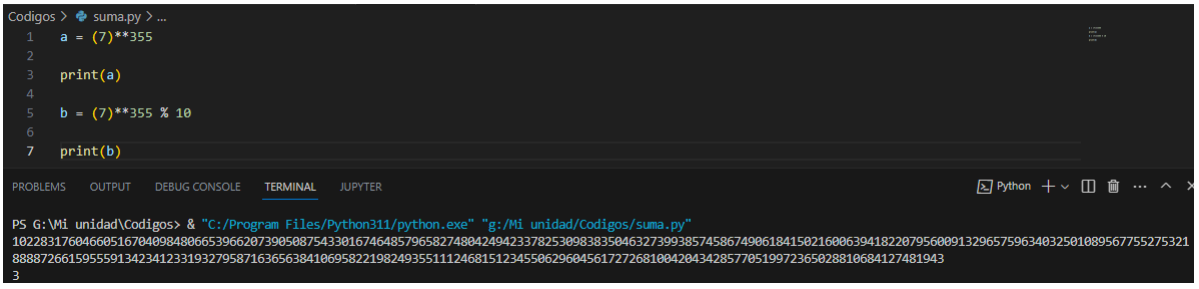

Figura 13: 7^{355}

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

Para ello, se debe suponer $d \in Z$ 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:

$$4k + 5 \cong 3k + 4(\text{mod}d)$$
$$4k + 5 - 3k + 4 = dn$$
$$k + 1 = dn$$
$$k = dn - 1$$

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

$$3(dn - 1) + 4 = dm$$
$$4 - 3 = d(m - 3n)$$
$$1 = d\beta$$

Dado que $\beta \in Z, \beta = 1/d$, 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.