UNIVERSIDAD NACIONAL DE COLOMBIA

Taller de Teoría de Números

por Iván Felipe Ayala Rengifo

12 de mayo de 2023

1. Teoría de Números - Preguntas

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

Para verificar la condición, podemos expresar a a y a b como dos enteros múltiplos de 11 de la siguiente manera:

$$a = 11v$$
$$b = 11w$$

Posteriormente, podemos reemplazar los valores de a y b en la ecuación original:

$$a + b = 544$$
$$11v + 11w = 544$$
$$v + w = 49$$

Esta última ecuación exige que v y w sean dos números enteros que sumados den 49, y sean además múltiplos de 11. Sin embargo, es bien sabido que la suma entre dos números múltiplos de 11 no puede dar un resultado que no sea múltiplo de 11, por lo que ningún número cumple la condición.

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

Algo a tener en cuenta con respecto a las reglas de divisibilidad entre 8 y 16 es que aplican para números de 4 y 5 dígitos, y que exigen conocimiento de los números que son múltiplos de 8 y 16 por debajo de los 4 dígitos.

Esto se debe a que, en el caso del número 8, su criterio de divisibilidad está en que para cualquier n, **el número formado por los últimos tres dígitos de n debe ser divisible por 8**.

Por ejemplo, el número 1344. En condiciones normales puede resultar complicado saber si es divisible entre 8, pero al tomar 344 y entender que 344 / 8 = 43, entonces podemos asegurar que el número es divisible por 8. Hay que tener en cuenta que esta regla únicamente aplica para números con 4 dígitos en adelante, ya que hay que tener conocimiento de si un número de tres digitos o menos es divisible entre 8.

Por otro lado, para el caso del número 16, la teoría es prácticamente la misma, solo que en lugar de ser tener en cuenta los primeros tres dígitos de un número n, **el criterio de divisibilidad entre 16 exige tomar el número conformado por los últimos cuatro dígitos de n y verificar que sea divisible entre 11.**

1.2.1. ¿Por qué funciona?

Para explicar el funcionamiento, se tomará un ejemplo válido para la regla de divisibilidad entre 8. El número 1344 es válido, ya que sus últimos tres dígitos (344) conforman un número divisible entre 8:

$$344/8 = 43$$

Tomando a 1344, al cual se le llamará n, es posible crear una descomposición por dígitos de la siguiente manera:

$$1344 = 1000 + 300 + 40 + 4$$

Esto es importante porque cada número de la expresión representa una cifra del número original. Es importante recordar que se necesita tomar los últimos tres dígitos del número y asegurarse de que sea un número divisible entre 8. Esto es porque, desde el cuarto dígito (que representa al 1000), ya hay una garantía de que el número en cuestión será divisible entre 8. 1000 / 8 = 125, por lo que 1000 y cualquier múltiplo de 1000 cumplen con la divisibilidad entre 8, asi que lo único que queda por asegurar es que la suma de los tres últimos dígitos (representando las centenas) sean un múltiplo de 8 también, para que la suma termine por dar en un número que también sea múltiplo de 8.

Todo lo anterior se basa en que siendo p y q dos números distintos divisibles entre n , entonces $p + q = r$ otro número divisible entre n.

Este mismo criterio aplica para 16, pero la garantía de 16 no empieza a partir de 1000, sino de 10000 ya que $10000/16 = 625$, por lo que se debe tener en cuenta la divisibilidad entre 16 de los primeros cuatro dígitos.

1.3. Si p es un número primo y $a^2 \equiv b^2(\mod p)$, pruebe que $a \equiv \pm b$.

La expresión inicial $a^2 \equiv b^2(\mod p)$ puede reescribirse, por propiedades de adición en aritmética modular, como $a^2 - b^2 \equiv 0(\mod p)$.

A partir de ello, es posible operar de la siguiente manera:

$$a^2 - b^2 \equiv 0(\mod p)$$
$$(a - b)(a + b) \equiv 0(\mod p)$$
$$(a + b) \equiv 0(\mod p) \text{ y } (a - b) \equiv 0(\mod p)$$

Por lo tanto, y nuevamente haciendo uso de las propiedades de la adición, se llega a que $a \equiv b$ y que $a \equiv -b$, es decir:

$$a \equiv \pm b$$

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

$$19^{19} mod(5)$$
$$19^4 19^4 19^4 19^4 19^3 mod(5)$$

Gracias al pequeño Teorema de Fermat, el cual indíca que:

$$a^{p-1} \equiv 1 mod(p)$$
con p un número primo y a no múltiplo de p

Se entiende que todo $19^4 mod(5)$ en la ecuación es igual a 1, con lo cual se pueden despejar de la ecuación para dejar:

$$19^3 mod(5)$$
$$6859\ mod(5) = 4$$

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

El ejercicio puede reescribirse como hallar a $7^{49} \mod (100)$.

- $7^1 \mod (100) = 7$
- $7^2 \mod (100) = 49$
- $7^3 \mod (100) = 43$
- $7^4 \mod (100) = 1$
- $7^5 \mod (100) = 7$
- $7^6 \mod (100) = 49$
- $7^7 \mod (100) = 43$
- $7^8 \mod (100) = 1$

Se puede observar que hay un ciclo que se repite cada 4 potencias con base 7 tal y como se ve en la lista anterior. Entonces:

$$49 \mod (4) = 1 //$$
$$7^1 \mod (100) = 7$$

Lo anterior implica que $7^{49} \mod (100) = 7$, lo cual determina a los últimos dos dígitos como 07.

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

El cálculo de lo solicitado puede hacerse aprovechando las propiedades del Euler Totient, lo cual se puede traducir a código como se mostrará a continuación.

Es importante recordar que el Euler Totient de un número n cuenta con ciertas propiedades que alivian la computación.

- $\phi(1) = 1$
- Para p un número primo, $\phi(p^a) = p^a - p^{a-1}$
- Si MCD (m,n) = 1, $\phi(m,n) = \phi(m)\phi(n)$

Es posible descomponer a cualquier número en factores primos con potencias que ayuden a dar con el resultado deseado, como lo hace el código a continuación:

```
def Descomposicion (n):

  NumerosPrimos = []

  for i in range(2,n+1):
    while n % i == 0:
      NumerosPrimos.append(i)
      n = n/i
  return NumerosPrimos
```

```
def TraduccionAPotencias (set, lista):

  ListaFinal = [] #Esta lista guarda en duplas los números primos, y a su derecha el valor de la potencia

  i = 0
  while i < len(set):
    target = list(set)
    potencia = lista.count(target[i])
    ListaFinal.append(target[i])
    ListaFinal.append(potencia)
    i = i+1
  #print(ListaFinal)
  return ListaFinal
```

```python
def EulerTotierPrimo (lista):
  #Esta función únicamente aplica para números primos.
  i = 0

  EulerTotierFinal = 1

  while i< len(lista):
    EulerTotierFinal = EulerTotierFinal * (((lista[i])**(lista[i+1]))-(lista[i])**((lista[i+1])-1))
    i = i+2
  return EulerTotierFinal

# ------------------------------------------------------------------------ #
```

```python
for i in range(3):
  if i==0:
    Valor = 35
  elif i==1:
    Valor = 100
  elif i==2:
    Valor = 51200

  DescomposicionEnPrimos = Descomposicion(Valor)
  PrimosSinRepetir = set(DescomposicionEnPrimos)

  PrimosFinal = TraduccionAPotencias(PrimosSinRepetir, DescomposicionEnPrimos)


  EulerTotier = EulerTotierPrimo(PrimosFinal)

  #print((DescomposicionEnPrimos))

  print("El Euler Totient de "+str(Valor)+" es "+str(EulerTotier))
```

Figura 1. Código con el funcionamiento del Euler Totient

Como output respectivo de cada número solicitado, se da:
El Euler Totient de 35 es 24 El Euler Totient de 100 es 40 El Euler Totient de 51200 es 20480

1.7. Usted le pregunta a un robot que quiere comer. El responde “48.879”. Sabiendo que el robot piensa en hexadecimal pero habla el decimal, que le debería dar de comer?

Como pequeña especulación, hay que tener en cuenta que el lenguaje hexadecimal cuenta con las letras desde la A hasta la F, por lo que la comida en cuestión debe estar entre ese límite de caracteres. Eso limita las opciones del robot para escoger comida.

Ahora bien, para entender la petición del robot es preciso traducir el output del robot de vuelta a hexadecimal, para entender qué es lo que estaba pensando.

Para traducir un número a hexadecimal, es preciso dividir el número entre 16 de manera recursiva hasta llegar a tener un cociente menor a 16. Una vez hecho esto, el número Hexadecimal consistirá de la concatenación de el último cociente obtenido con los residuos de las demás operaciones, empezando desde la última operación obtenida hasta la primera realizada, de la siguiente manera:

$$48879/16 = 3054+ \underline{15}$$
$$3054/16 = 190+ \underline{14}$$
$$190/16 = \underline{11} + \underline{14}$$

Siguiendo lo establecido anteriormente, el número en hexadecimal sería:

$$11\ 14\ 14\ 15$$

sin embargo, es importante recordar que el hexadecimal representa valores del 0 al 15, pero los número del 10 al 15 están representados por las letras A, B, C, D, E, F respectivamente, por lo que lo que el robot quiere comer es **BEEF**.

1.8. ¿65.314.638.792 es divisible por 24?.

El criterio de divisibilidad de 24 es un criterio compuesto, dado que como es de esperar, el número debe cumplir con:

- Ser divisible entre 3. Es decir, que sus dígitos sumen un múltiplo de 3.
- Ser divisible entre 8. Es decir, que sus últimos tres dígitos sean divisibles entre 8 como conjunto.

¿Es 65314638792 divisible por 3?

$$6+5+3+1+4+6+3+8+7+9+2 = 54$$
$$5+4 = 9$$

El número es en efecto divisible por 3.
¿Es 65314638792 divisible por 8?

$$792/8 = 99$$

El número es en efecto divisible por 8.
CONCLUSIÓN. El número sí es divisible por 24.

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

Teniendo a cualquier entero a, podemos expresar lo requerido en el enunciado como $(a^p - a)$ mód $p = 0$. Esta afirmación se puede convertir en el enunciado del Pequeño Teorema de Fermat, ya que este indica que $(a^p - a) \equiv a \mod (p)$ independientemente de si a es múltiplo de p o no. Esta congruencia implica que, en efecto, $n^p - n$ es divisible por p si p es un número primo.

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

Este ejercicio se puede resolver mediante el uso de la identidad de Bézout:

$$314x + 159y = 1$$
—
$$314 = (1)159 + 155$$
$$159 = (1)155 + 4$$
$$155 = (38)4 + 3$$
$$4 = (1)3 + 1$$
$$3 = (3)1 + 0$$
—
$$155 = 314 - (1)159$$
$$4 = 159 - (1)155$$
$$3 = 155 - (38)4$$
$$1 = 4 - (1)3$$
—
$$1 = 4 - (1)3$$
$$1 = 4 - (1)(155 - (38)4)$$
$$1 = 4 - (1)155 + (38)4$$
$$1 = -155 + (39)4$$
—
$$1 = -155 + (39)(159 - (1)155)¡$$
$$1 = -155 + (39)159 - (39)155$$
$$1 = (39)159 - (40)155$$
—
$$1 = (39)159 - (40)(314 - (1)159)$$
$$1 = (39)159 - (40)314 + (40)159$$
$$1 = (79)159 - (40)314$$
—

La respuesta final es $x = -40, y = 79$.

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

La expresión inicial $a^2 \equiv b^2(\mod p)$ puede reescribirse, por propiedades de adición en aritmética modular, como $a^2 - b^2 \equiv 0(\mod p)$.

A partir de ello, es posible operar de la siguiente manera:

$$a^2 - b^2 \equiv 0(\mod p)$$
$$(a-b)(a+b) \equiv 0(\mod p)$$
$$(a+b) \equiv 0(\mod p) \text{ y } (a-b) \equiv 0(\mod p)$$

Por lo tanto, y nuevamente haciendo uso de las propiedades de la adición, se llega a que $a \equiv b$ y que $a \equiv -b$, es decir:

$$a \equiv \pm b$$

1.12. Encuentre todos los enteros positivos tales que $1066 \equiv 1776(\mod m)$.

```
[ ]  mValidos = []

     for i in range (1, 1776):
       a = 1066 % i
       b = 1776 % i

       if a == b:
         mValidos.append(i)

     print(mValidos)

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

Figura 2. Código simple que encuentra lo solicitado.

RESPUESTA: Los números que cumplen con el requisito de m son $1, 2, 5, 10, 71, 142, 355, 710$.

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

Es de hecho bastante fácil de demostrar, ya que el criterio de divisibilidad entre cinco exige que el último dígito sea 0 o 5.

Partiendo de ese hecho, es preciso tener en cuenta que el último dígito a obtener es calculable de manera segura gracias a las propiedades de la multiplicación, que favorecen la permanencia del último dígito. Los últimos dígitos de los números cubos siguen la siguiente fórmula:

- Si el último dígito del número es 1, entonces el primer dígito de su cubo será 1.
- Si el último dígito del número es 2, entonces el primer dígito de su cubo será 8.
- Si el último dígito del número es 3, entonces el primer dígito de su cubo será 7.
- Si el último dígito del número es 4, entonces el primer dígito de su cubo será 4.
- Si el último dígito del número es 5, entonces el primer dígito de su cubo será 5.
- Si el último dígito del número es 6, entonces el primer dígito de su cubo será 6.
- Si el último dígito del número es 7, entonces el primer dígito de su cubo será 3.
- Si el último dígito del número es 8, entonces el primer dígito de su cubo será 2.
- Si el último dígito del número es 9, entonces el primer dígito de su cubo será 9.
- Si el último dígito del número es 0, entonces el primer dígito de su cubo será 0.

Los números cubos tienen esta terminación de dígitos en el orden presentado en la lista, por lo que al restar dos cubos consecutivos, hay que poner especial atención en los últimos dígitos para verificar si se puede dividir entre cinco el número obtenido de la resta. Sin embargo, es fácil de observar que ningún número al que se le reste su inmediato siguiente en la lista va a dar ni 5 ni 0 en ningún momento, por lo que la diferencia entre cubos seguidos garantiza un número indivisible entre 5.

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

Este punto, en otras palabras, pide un número que sea múltiplo de 9, de 16 y de 25.

Para ello, deberemos cumplir los criterios de divisibilidad de los tres números. La manera más sencilla de hacer esto es suplir los requisitos de 25 y 16, y por último aplicar el criterio de 9 que es el menos demandante.

Para empezar, el número n debe cumplir que sus últimos dos dígitos sean múltiplos de 25. Esto es que sean $00, 25, 50$, o 75.

Paso seguido, hay que buscar un número de cuatro digitos con esa terminación que sea múltiplo de 16.

El número más pequeño que cumple este requisito es 1200, ya que $1200/16 = 75$.

Por último, podemos añadir libremente números a 1200 que cumplan la condición de que la suma de todos los dígitos sea múltiplo de 9.

Una de las posibles soluciones, aunque no la única, sería 61200, que cumple los criterios de divisibilidad de los tres números presentados, y por lo tanto es múltiplo de todos.

1.15. ¿Cuál es el último digito de 7^{355}?

Una vez más es posible aprovecharnos de las propiedades de la potencia de un número, que nos permite saber cuál será el último dígito del número potenciado en cuestión a partir del último dígito del número original.

- Se empieza con 7^2, así que se considera que cualquier número terminado en 7 al multiplicarse por 7 dará con un número terminado en 9.
- Un número terminado en 9 que se multiplique por 7 dará como resultado un número terminado en 3.
- Un número terminado en 3 que se multiplique por 7 dará como resultado un número terminado en 1.
- Un número terminado en 1 que se multiplique por 7 dará como resultado un número terminado en 7.

El numeral cuatro completa un ciclo que se repite cuantas veces sea el valor del exponente que eleva al 7, con lo cual podemos usar aritmetica modular basados en los elementos del siguiente ciclo:

$$(7, 9, 3, 1)$$

El ciclo tiene un tamaño de 4 elementos, por lo que se trabajará con un módulo 4. Además el valor al que le debemos sacar el módulo será las veces que se multiplicará por 7, por lo que la expresión final resulta en:

$$355 \mod (4) = 3$$

Esto indica que el último dígito de 7^{355} es el que se encuentra en la posición 3 del ciclo, es decir, el número 3.

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

Como prueba de contradicción, se hace la suposición de que $3k + 4$ y $4k + 5$ NO son coprimos; es decir, MCD($3k + 4$,$4k + 5$) $\neq 1$. Es decir, d ¿1.

Por consiguiente, es posible expresar los términos dados de la siguiente manera:

$$3k + 4 = dn$$
$$4k + 5 = dm$$
con n y m enteros cualquiera.

A partir de lo anterior, es posible reordenar las operaciones de la siguiente manera igualando con k:

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

Esto básicamente nos deja con el resultado de que $d = 1$ y $(4n - 3m) = 1$, por lo que el MCD solamente puede llegar a ser 1, confirmando que los elementos iniciales son coprimos