Taller - Teoría de números

Matemáticas Discretas 2: 2023-1 | Universidad Nacional De Colombia

Juan Carlos Garavito Higuera

Índice

1. ¿Existen enteros a y b tal que $a+b=544$ y cuyo máximo común divisor es 11?.
2. Encuentre una regla de divisibilidad para 8 y para 16.
3. Si p es un número primo y $a^2 \equiv b^2 (mod\ p)$, pruebe que $a \equiv \pm b$.
4. Encuentre el resto cuando 19^{19} es dividido por 5.
5. Encuentre los últimos dos dígitos de 7^{7^7}.
6. Encuentre $\phi(n)$ para n=35, n=100, n=51200.
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?
8. ¿65.314.638.792 es divisible por 24?.
9. Pruebe que $n^p - n$ es divisible por p si p es un número primo.
10. Encuentre los enteros x y y tal que $314x+159y=1$.
11. Pruebe o controvierta la siguiente afirmación si $a^2 \equiv b^2 (mod\ m)$ entonces $a \equiv b (mod\ m)$ o $a \equiv -b (mod\ m)$.
12. Encuentre todos los enteros positivos tales que $1066 \equiv 1776 (mod\ m)$.
13. Muestre que la diferencia de dos cubos consecutivos nunca es divisible por 5.
14. Encuentre un entero positivo n tal que $3^2 \vee n$, $4^2 \vee n+1$, $5^2 \vee n+2$
15. ¿Cuál es el último digito de 7^{355}?
16. Muestre que $3k+4$ y $4k+5$ no tienen un factor común más grande que 1

Desarrollo

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

Para cumplir la condición: \begin{align}*& 544 = 11n + 11m \quad, : n,m \in \mathbb{Z} \ & \frac{544}{11} = (n+m) \quad, : (n+m) = k \in \mathbb{Z} \ & \frac{544}{11} = k \quad, \ text{donde } \frac{544}{11} = 49.4545 \notin \mathbb{Z} \ \end{align}*

De modo que NO existen enteros a y b tal que $a+b=544$ y su máximo común divisor sea 11.

---

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

Regla de divisibilidad para 8: Un número cumple divisibilidad con 8 si sus últimos 3 digitos (*aquellos de menor peso*) dan forma a un múltiplo de 8.

```
Ejemplo: 33.006.904
```

\begin{align}*&9(100) + 0(10) + 4 \quad% 8\ &4 + 0 + 4 \quad% 8\ &8 \quad% 8\ &0 \ end{align}*

Regla de divisibilidad para 16: Un número cumple divisibilidad con 16 si sus últimos 4 digitos (*aquellos de menor peso*) dan forma a un múltiplo de 16.

```
Ejemplo: 12.104.336
```

\begin{align}*&4(1000) + 3(100) + 3(10) + 6 \quad% 16\ &0 + 12 + 14 + 6 \quad% 16\ &26 + 6 \quad% 16\ &10 + 6 \quad% 16\ &16 \quad% 16\ &0 \end{align}*

---

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

Teniendo $a, b \in Z$ cualesquiera, tales que $a^2 \equiv b^2 (mod\ p)$ con p número primo, entonces $p \mid (a^2 - b^2) = (a-b)(a+b)$.

Según el *Lema de Euler*: 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.

En el primer caso se tiene \$ (a - b)\$ es coprimo con \$ p \$, puesto que p es primo por hipotesis. A partir del *lema de euler*, se tiene que $p \mid (a+b)$; que por definición de congruencia implica que $a \equiv -b (mod\ p)$.

Analogamente, para $p \mid (a-b)$, pues p tambien es coprimo a $(a+b)$, entonces $a \equiv b (mod\ p)$.

Así pues $a \equiv \pm b (mod\ p)$ si $a^2 \equiv b^2 (mod\ p)$.

□

---

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

Por pequeño teorema de Fermat, $19^4 \, mod \, 5 = 1$, entonces:

\begin{align} & (19^4)^4 \cdot 19^3 :%5 \ & 1 \cdot (15 + 4)^3 :%5 \ & (0 + 4)^3 :%5 \ & 4^2 \cdot 4 :%5 \ & 16 \cdot 4 :%5 \ & 1 \cdot 4 :%5 \ & 4 \end{align}

$ 19^{19} \mod 5 = 4 $

Para comprobar, se puede comprobar con python:

```
a = 19**19
b = 5
print(a%b)
```

```
4
```

---

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

Para hallar el ultimo digito de un entero n solo hace falta determinar $n(mod\,100)$. Entonces asignemos $n=7^{7^7}$.

7^7 es un producto consecutivo de impares, así que el resultado también será impar, de esta forma: $7^7=2k+1$, entonces...

\begin{align} & 7^{7^7} :% 100\ & 7^{2k +1} :% 100\ & (7^{2})^k \cdot 7 :% 100 \quad , 7^2 :% 100 = 49\ & 49 \cdot 7 :% 100\ & 343:% 100\ & 43 \end{align}

Así tenemos que los ultimos digitos de $n=7^{7^7}$ son 43.

---

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

Usando el código explicado en el siguiente enlace: https://github.com/jgaravitoh/Matematicas-Discretas-2-Trabajos-2023-1S/blob/main/Tarea_6/Tarea_6_discretas_2_EulerTotient.ipynb

Tenemos los siguientes resultados:

```
|G| = 35
¿Es primo?: No

Euler Totient: 24
Tiempo: 0.0
```

```
...
    |G| = 100
    ¿Es primo?: No

    Euler Totient: 40
    Tiempo: 0.0
```

```
...
    |G| = 51200
    ¿Es primo?: No

    Euler Totient: 20480
    Tiempo: 0.0
```

Siendo:

$\phi(35) = 24$

$\phi(100) = 40$

$\phi(51200) = 20480$

---

1. 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?

El problema se puede resolver con el siguiente código:

```python
def decimal_a_hexadecimal(decimal):

    if decimal == 0:
        return '0'

    # Diccionario de correspondencia entre valores decimales y hexadecimales
    digitos_hex = "0123456789ABCDEF"

    # Lista para almacenar los dígitos hexadecimales
    resultado = []

    # Convertir el número decimal en hexadecimal
    while decimal > 0:
        residuo = decimal % 16  # Obtener el residuo de la división entre 16
        resultado.insert(0, digitos_hex[residuo])  # Insertar el dígito hexadecimal en la posición inicial
        decimal = decimal // 16  # Dividir el número decimal entre 16

    # Convertir la lista de dígitos hexadecimales en un string
    hexadecimal = ''.join(resultado)

    return hexadecimal

# Ejemplo de uso
numero_decimal = 48879
numero_hexadecimal = decimal_a_hexadecimal(48879)
print("El robot quiere comer ", numero_hexadecimal)
```

```
El robot quiere comer  BEEF
```

El robot quiere comer carne de res.

---

1. ¿65.314.638.792 es divisible por 24?.

Para saber si un número es divisible por 24 este debe ser divisible por 8 y por 3.

Para saber si es divisible por 3 la suma de sus cifras debe ser multiplo de 3, entonces:

\begin{align} & 6+5+3+1+4+6+3+8+7+9+2 mod(3)\ & 54 mod(3) = 0\ \end{align}

Para saber si es divisible por 8 la sus 3 ultimas cifras deben formar un múltiplo de 8, entonces:

\begin{align} & 792 mod(8) = 0\ \end{align}

En el caso de los números 3, 8 y 24, sus descomposiciones en factores primos son:

\begin {align} & 3 = 3 \ & 8 = {2^3} \ & 24 = {2^3} 3 \ \end{align*} Dado que 24 contiene los factores primos 2 y 3, cualquier número divisible por 24 debe ser divisible por ambos números.

---

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

Sea $n \in Z$ cualquiera y p un número primo. Se tienen 2 posibles casos, $ p \mid n$ y $ p \ nmid n$.

- Sea $ p \mid n$.

  Entonces p tambien divide cualquier escalar de n, incluyendo n^p, de modo que: \ begin{align} &n^p - n = p (\overline{k} - k)\ &n^p - n = p ℓ \ & p \mid (n^p - n) \ end{align}

- Sea $ p \nmid n \longrightarrow $ p, n coprimos.

  Entonces por el pequeño teorema de Fermat, $n^{p-1} \equiv 1 (mod\, p)$, de modo que: \ begin{align} (n^p - n) \equiv (n\cdot n^{p−1} - n)\quad ⟶:: &n(1) - n \pmod{p} \ & 0 \pmod{p}\ \end{align}

  \begin{align} ⟹ (n^p - n) \equiv 0 \pmod{p} \end{align}

  Lo que implica por definición de congruencia y divisibilidad $p \mid (n^p - n)$.

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

□

---

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

Sea a = 314 y b = 159...

```
def Euclides(a,b):
    if a%b != 0:
        a, b = b, a % b
        return Euclides(a,b)
    return b
```

```python
def main():
    print("El MCD es: "+ str(Euclides(314,159)))

main()
```

```
El MCD es: 1
```

De modo que x y y son equivalentes a los números de Bézout, tales que, $mcd(a,b)=1=ax+by$. Es posible aplicar el Algoritmo para los números de Bézout para hallar dichos coeficientes:

```python
def bezout(a, b):
    """
    Calcula el máximo común divisor de dos números enteros a y b,
    así como los coeficientes x e y que satisfacen la identidad de
Bezout.
    """
    x0, x1, y0, y1 = 1, 0, 0, 1  # Inicializa los valores de x e y
    while b != 0:
        q, a, b = a // b, b, a % b  # Calcula el cociente y el resto
        x0, x1 = x1, x0 - q * x1   # Actualiza los valores de x
        y0, y1 = y1, y0 - q * y1   # Actualiza los valores de y
    return x0, y0  # Devuelve el MCD y los coeficientes x e y

def main():
    # Ejemplo de uso
    a = 314
    b = 159

    x, y = bezout(a, b)

    print("Coeficientes de Bezout: x =", x, ", y =", y)
main()
```

```
Coeficientes de Bezout: x = -40 , y = 79
```

Siendo entonces:

$x=-40$

$y=79$

---

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

Razonando por contraejemplo...

Sea $a=2, b=8, m=15 \in Z$

$a^2=4$ y $b^2=64$.

Con $4 \equiv 64 \pmod{15}$, de modo que $a^2 \equiv b^2 \pmod{m}$.

Sin embargo, no es cierto que $2 \equiv 8 \pmod{15}$ o $2 \equiv -8 \pmod{15}$. Para a, en ambos casos es congruentes a 2. Para b, es congruente a 8 y 7 respectivamente.

Por lo tanto, la afirmación es falsa porque $a^2 \equiv b^2 \pmod{m} \Rightarrow a \equiv b \pmod{m}$ o $a \equiv -b \pmod{m}$ no se cumple en todos los casos.

□

---

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

La expresión inicial se puede transformar de la siguiente manera:

\begin{align} &1066 \equiv 1776 \pmod{m}\ &1066 - 1066 \equiv 1776 - 1066 \pmod{m}\ &0 \equiv 710 \pmod{m} \end{align}

A partir de la expresión equivalente resultante, se determina que m es todos auquellos enteros divisores de 710. \begin{align} m \in {x : 710\mid x, :: x \in \mathbb{Z^+} } \end{align}

Es posible desarrollar un codigo sencillo para hallar dicho conjunto.

```
import math
def encontrar_divisores(n):
    divisores = []

    for i in range(1, int(n**0.5) + 1):  #Limita el ciclo hasta la raiz del número.
        if n % i == 0:
            divisores.append(i)
            if i != n // i:  # Evita duplicados si el número es un cuadrado perfecto
                divisores.append(n // i)

    divisores.sort()  # Ordena la lista de divisores
    return divisores

# Ejemplo de uso


n = 710
divisores = encontrar_divisores(n)
print("Los divisores de", n, "son:", divisores)
```

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

Entonces \begin{align} m \in {1, 2, 5, 10, 71, 142, 355, 710} \end{align}

---

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

Sea $n \in Z$ cualquiera, se tiene que \begin{align} & (n+1)^3 - n^3 \equiv : \ell \ & ℓ= n^3 + 3n^2 + 3n + 1 - n^3\ &\ell = 3n(n+1) + 1 \end{align}

Sabemos que cualquier número entero se puede expresar como una de las formas siguientes: $5k$, $5k+1$, $5k+2$, $5k+3$, $5k+4$.

1. $n=5k$ \begin{align} & \ell = (3)(5k)(5k +1) +1\ & \ell - 1 = 5 \overline{k} \ & ⟹ \ell ≡ 1 \pmod{5} \text{ , por definicion de congruencia} \end{align}

Analogamente,

1. $n=5k+1$ \begin{align} & \ell = 3(5k +1)(5k +2) +1\ & \ell = 5(3)(5k^2 + 2k + k) + 6 + 1\ & \ell - 7 = 5 \overline{k}\ & ⟹ \ell ≡ 7 ≡ 2 \pmod{5} \end{align}
2. $n=5k+2$ \begin{align} & \ell = 3(5k +2)(5k +3) +1\ & \ell = 5(3)(5k^2 + 3k + 2k) + 18 + 1\ & \ell - 19 = 5 \overline{k}\ & ⟹ \ell ≡ 19 ≡ 4 \pmod{5} \end{align}
3. $n=5k+3$ \begin{align} & \ell = 3(5k +3)(5k +4) +1\ & \ell = 5(3)(5k^2 + 4k + 3k) + 36 + 1\ & \ell - 37 = 5 \overline{k}\ & ⟹ \ell ≡ 37 ≡ 2 \pmod{5} \end{align}
4. $n=5k+4$ \begin{align} & \ell = 3(5k +4)(5k +5) +1\ & \ell = 5(3)(5k +4)(k +1) +1\ & \ell = 5(3)(5k^2 + 5k + 4k) + 60 + 1\ & \ell - 61 = 5 \overline{k}\ & ⟹ \ell ≡ 61 ≡ 1 \pmod{5} \end{align}

De modo que no existen $n, (n+1) \in Z$, tales que la diferencia de sus cubos tenga división exacta entre 5.

□

---

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

Es posible determinar el sistema de congruencias siguiente.

\begin{align} &n≡0\pmod{9} \ &n+1≡0\pmod{16} \ &n+2≡0\pmod{25} \ \end{align} Que es equivalente \begin{align} &n+2≡2\pmod{9} \ &n+2≡1\pmod{16} \ &n+2≡0\pmod{25} \ \end{align}

Aplicando el teorema del resto chino:

\begin{align} &m = 3^24^25^2 = 3600\ &M_1 = 4^25^2 = 400 \ &M_2 = 3^25^2 = 225 \ &M_3 = 3^24^2 = 144\ \end{align}

Para determinar los inversos podemos hacer uso del algoritmo de Bézout.

```
def main(a, b):
  v,w = bezout(a,b)
```

```python
    d = a*v + b*w

    print( f'Para {a}v ≡ 1 mod({b}):\nv = {v}  \n' )

m = [9, 16, 25]; M = [400, 225, 144]
for i, j in zip(M , m): main(i, j)
```

```
Para 400v ≡ 1 mod(9):
v = -2

Para 225v ≡ 1 mod(16):
v = 1

Para 144v ≡ 1 mod(25):
v = 4
```

De modo que. \begin{align} &v_1 = -2 \ &v_2 = 1 \ \end{align}

Finalmente

\begin{align} n+2 &= 2(4^25^2)(-2) + 1(3^25^2)(1) + 0\ &= -1600 + 225\ &= -1375 \ &⟶ \quad -1375 \pmod{m}\ & \quad \quad \quad (2225 - 3600) \pmod{3600}\ & \quad \quad \quad (2225 - 0) \pmod{3600}\ & \quad \quad \quad 2225 \ &\ n &= 2225 - 2\ n &=\ mathbf{2223} \end{align}

Esto lo podemos comprobar rapidamente gracias a python:

```python
n = 2223
print( n % 9 )
print( (n+1) % 16 )
print( (n+2) % 25 )
```

```
0
0
0
```

---

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

Para hallar el ultimo digito de un entero n, basta con determinar $ n \pmod{10}$. Sea $n=7^{355}$.

\begin{align} &7^{354 +1} \quad% 10 \quad ,354 = 2n \ &(7^2)^n \cdot 7 \quad% 10\ \end{align}

Con $n=177$ impar.

\begin{align} &9 \cdot 7 \quad% 10\ &63 \quad% 10\ &3 \end{align}

De modo que el ultimo digito de 7^{355} es 3.

Esto lo podemos además, comprobar gracias a python:

```
print( (7**355) % 10)
```

```
3
```

---

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

Supongase existe $d \in Z$ tales que $d > 1 $ y $\quad d \mid 3k+4 $ tanto como $d \mid 4k+5 $. Entonces la división de estos dos factores en d tiene el mismo resto:

\begin{align} *& 4k+5 \equiv 3k+4 \pmod d \ & 4k + 5 - 3k - 4 = dn\ & k + 1 = dn\ & k = dn - 1\ \end{align}*

Ahora, como $ d \mid 3k+4 $ por hipotesis, $ 3k+4 = dm $, remplazando:

\begin{align} *& 3(dn -1) +4 = dm \ & 4 - 3 = d(m - 3n)\ & 1 = dℓ\ \end{align}*

Como $\ell \in Z$, $\ell = 1/d$, donde d debe ser un divisor de 1, es decir, $d = 1$. No obstante $d > 1$ por hipotesis, lo que es un absurdo.

Por lo tanto, por reducción al absurdo, $3k+4$ y $4k+5$ no tienen un factor común más grande que 1.

□
