UNIVERSIDAD NACIONAL DE COLOMBIA

INGENIERIA DE SISTEMAS Y COMPUTACIÓN

TÍTULO DEL TRABAJO
(TEORIA DE NÚMEROS)

BRAYAN SANTIAGO MALDONADO APARICIO

PROFESOR: FRANCISCO ALBEIRO GOMEZ JARAMILLO

MAYO - 2023

Taller - teoría de números

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

   Ya que sabemos que el M.C.D de a y b es 11, podemos afirmar que tanto a como b son múltiplos de 11. Por lo tanto: $a = 11x$ y $b = 11y$, donde x y y son enteros.

   Substituyendo en nuestra ecaución inicial:

   $$11x + 11y = 544 \approx 49,45$$

   Podemos reducir terminos dividiendo toda la ecuación por 11:

   $$x + y = \frac{544}{11}$$

   $$544(mod(11) = 5$$

   No existen números tales que a y b sean múltiplos de 11 y que a su vez sumen 544, debido a que 544 no es múltiplo de 11.

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

   Para determinar si un número es divisible por 8, es necesario verificar si las tres últimas cifras del número son divisibles por 8. Si las tres últimas cifras son divisibles por 8, entonces el número en sí también es divisible por 8.
   Los divisores de 16 son 1, 2, 4, 8 y 16. Debido a que 16 es un cuadrado perfecto, tiene un número impar de divisores, en este caso, 5. La factorización de 16 es igual a 4 al cuadrado, lo cual se puede escribir como $16 = 4^2 = 2^4$.

   Para determinar si un número es divisible por 16 utilizando un procedimiento específico, se realiza lo siguiente:

   Se toma el dígito de las unidades y se le resta seis veces el dígito de las decenas.
   Luego se le suma cuatro veces el dígito de las centenas.
   Finalmente, se le suma ocho veces el dígito de los millares.
   Si el resultado de esta operación es múltiplo de 16, entonces el número es divisible por 16.

3. **Si p es un número primo y a2 ≡ b2(mod p) , pruebe que a ≡ ± b.**

   Si usamos la propiedad: $a \equiv b$ (mod m) y $c \equiv d$ (mod m), $ac \equiv bd$ (mod m)
   Podríamos sustituir hacia atras de la siguiente manera:

   $$a^2 \equiv b^2(modp)$$

$$aa \equiv bb(modp)$$

$$a \equiv b(modp)$$

Por propiedades de los cuadrados sabemos que:

$$aa \equiv a^2 = (-a)(-a)$$

Entonces la siguiente congruencia:

$$a^2 \equiv b^2(modp)$$

Se cumple para b y $(-b)$
Así que podemos afirmar que $a \equiv \pm$ (mod p)

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

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

$$19^4 * 19^{15}mod(5)$$

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

5. **Encuentre los últimos dos dígitos de 7^7.**

Para poder encontrar los últimos dos dígitos de esta potencia es necesario calcular las primeras 7 potencias deel 7:

$$7^1 = 7$$

$$7^2 = 49$$

$$7^3 = 343$$

$$7^4 = 2401$$

$$7^5 = 16807$$

$$7^6 = 117649$$

$$7^7 = 823543$$

Al observar los ultimos dígitos de dichas potencias podemos darnos cuenta de que a partir de ciertas potencias se repite el patron cíclico de 4: 7,9,3,1

Por lo tanto para poder calcular los últimos 2 dígitos de la potencia a resolver, se hace necesario determinar el residuo que queda de aplicarle modulo 4:

$$7^1 = 3(mod4)$$

$$7^2 = 1(mod4)$$

$$7^3 = 3(mod4)$$

$$7^4 = 1(mod4)$$

$$7^5 = 3(mod4)$$

De igual forma que antes podemos darnos cuenta que los residuos se repiten en patrones de 2: 3,1,3,1
Ahora calculemos el residuo de 7^7 (mod 2):

$$7^1 = 1(mod2)$$

$$7^2 = 1(mod2)$$

$$7^3 = 1(mod2)$$

Entonces, el residuo de 7 elevado a la 7 elevado a la 7 dividido por 2 es 1.
Por lo tanto usando las siguientes congruencias podremos determinar los últimos dos dígitos: 7 elevado a la 7 elevado a la $7 \equiv 7^1 \equiv 7(mod100)$

Determinaando así que los últimos dos dígitos son 07.

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

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

$$\phi(35) = \phi(7.5) = \phi(7^1)\phi(5^1)$$

$$= (7^1 - 7^{1-1})((5^1 - 5^{1-1})$$

$$= (7-1)(5-1)$$

$$= (6)(4)$$

$$= 24$$

$$\phi(100) = \phi(2^2.5^2) = \phi(2^2)\phi(5^2)$$

$$= (2^2 - 2^{2-1})((5^2 - 5^{2-1})$$

$$= (4 - 2)(25 - 5)$$

$$= (2)(20)$$

$$= 40$$

$$\phi(51200) = \phi(2^{11}.5^2) = \phi(2^{11})\phi(5^2)$$

$$= (2^{11} - 2^{11-1})((5^2 - 5^{2-1})$$

$$= (2048 - 1024)(25 - 5)$$

$$= (1024)(20)$$

$$= 20480$$

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, que le debería dar de comer?**

   Empecemos por hallar el residuo de 48879 (mod 16):

$$48879 mod(16)$$

$$3.16.293 = 3.3.5431$$

$$3^2.5431 mod(16)$$

$$9.7 mod(16)$$

$$63 mod(16)$$

$$-1 mod(16)$$

$$15 mod(16)$$

Ahora le restaremos al numero original su residuo y le hallaremos su residuo:

$$48879 - 15 = 48864$$

$$3054 mod(16)$$

$$3 * 1018$$

$$3 * 2 * 509$$

$$6 * 496 + 13 mod(16)$$

$$6 * 13 mod(16)$$

$$78 mod(16)$$

$$-2 mod(16) = 14$$

De forma que ya tenemos dos residuos 15 y 14

Ahora solo nos queda hallar los otros modulos:

$$3054 - 14 = 3040 mod(16)$$

$$= 190$$

$$190 = 192 - 2 mod(16) = 14$$

$$190 - 14 = 176$$

$$176 mod(16) = 11$$

De modo que si juntamos todos los residuos encontrados obtenemos: 15,14,14,11. Numeros que en base 16(hexadecimal) representan: B,E,E,F
Lo que nos da como resulado "BEEF" es decir que el robot quiere de comer Carne de Res.

8. **¿65.314.638.792 es divisible por 24?.**
   Para saber si dicho número es divisible por 24 se hace más fácil descomponer el 24 en factores primos: ´[2.2.2.3] y evaluar la divisibilidad del número con dichos factores, 2 y 3:

Divisibilidad por 2: Un número es divisible por 2 si el último dígito es par (0, 2, 4, 6 u 8). En este caso, el último dígito de 65,314,638,792 es 2, por lo que el número es divisible por 2.

Divisibilidad por 3: Un número es divisible por 3 si la suma de sus dígitos es divisible por 3. Podemos sumar los dígitos del número:$6 + 5 + 3 + 1 + 4 + 6 + 3 + 8 + 7 + 9 + 2 = 54$. La suma de los dígitos es 54, y como 54 es divisible por 3, el número 65,314,638,792 también es divisible por 3.
Dado que el número es divisible tanto por 2 como por 3, podemos concluir que 65,314,638,792 es divisible por 24.

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

Para esto estudiaremos dos casos específicos:

Caso 1: n es divisible por p:

Si n es divisible por p, entonces n se puede expresar como el producto de p y algún número entero k, es decir, n = kp. Si sustituimos esta expresión en la expresión original $(n^p - n)$, tenemos:

$$(kp)^p - (kp) = k^p * p^{p-1} * p - k * p^2$$

$$(kp)^p - (kp) = (k^p * p^{p-1} - k * p) * p$$

Dado que $(k^p * p^{p-1} - k * p)$ es un número entero, podemos sustituirlo por otro entero m. Por lo tanto, podemos afirmar que la expresión $(n^p - n)$ es divisible por p.

Caso 2: n no es divisible por p:

En el caso en el que n no sea divisible por p, podemos aplicar el pequeño teorema de Fermat. Según este teorema, para cualquier número entero n y un número primo p, la expresión n^p - n es divisible por p. Por lo tanto, podemos concluir que $(n^p - n)$ es divisible por p en este caso.

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

$$314 = 1 - 159 + 155$$

$$159 = 1 * 155 + 4$$

$$155 = 38 * 4 + 3$$

$$4 = 31 + 1$$

Por lo que:

$$155 = 314 + (1)159$$

$$4 = -314 + (2)159$$

$$3 = (39)314 + (-77)159$$

$$1 = (-40)314 + (79)159$$

Por lo tanto:

$$x = -40$$

$$y = 79$$

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).**

Según el teorema de Fermat:

$$a^2 \equiv b^2(mod(m))$$

$$aa \equiv bb(mod(m))$$

$$a \equiv b$$

$$a \equiv b(mod(m))$$

$$a^2 \equiv b(mod(m))$$

$$aa \equiv (-b)(-b)(mod(m))$$

$$a \equiv -b$$

$$-a \equiv b$$

Lo que prueba la expresión inicial.

12. **Encuentre todos los enteros positivos tales que 1066 $\equiv$ 1776(mod m).**
Para esto primero realizaremos la siguiente operación:

$$1066 \equiv 1776(mod(m))$$

$$1066 \equiv +1776(mod(m))$$

$$710 = 7152$$

Los divisores de 710 son los siguientes:

$$D = 1, 2, 5, 10, , 71, 142, 355, 710$$

Por lo tanto, podemos afirmar que 1066 es congruente con 1776 modulo m para cualquier m perteneciente al conjunto D.

$$1066 \equiv 1776(modm) \forall m \in D$$

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

Si consideramos un número n perteneciente al conjunto de los números enteros y asumimos que n tiene la forma 2k, donde k es un entero, entonces:

$$n + 1 = 2k + 1$$

$$(n+1)^3 - n^3 = (2k+1)^3 - (2k)^3$$

$$= 8k^3 + 12k^2 + 6k + 1 - 8k^3$$

$$= 3(4k^2 + 2k) + 1$$

Ahora digamos que:

$$m = 3(4k^2 + 2k) + 1$$

$$m \equiv 1(mod(5))$$

Entonces, en todos los casos en los que se divide m por 5, siempre queda un residuo de 1, lo que indica $(n+1)^3 - n^3$ no es divisible por 5.

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

$$a \equiv b(mod(m))$$

$$n|a - b|$$

$$n \equiv 0(mod(3^2))$$

$$n \equiv -1(mod(4^2))$$

$$n \equiv -2(mod(5^2))$$

Entonces:

$$n \equiv 0(mod(9))$$

$$n \equiv -15(mod(16))$$

$$n \equiv 23(mod(25))$$

$$n = 9k$$

Ahora:

$$15(mod(16)) \equiv 9k(mod(16))$$

$$15(9)^{-1}(mod(16)) \equiv k(mod(16))$$

$$15(7)(mod(16)) \equiv k(mod(16))$$

$$9(mod(16)) \equiv k(mod(16))$$

Por lo que:

$$K = 9 + 16m$$

$$n = 9(9 + 16m)$$

$$n = 81 + 114m$$

$$n \equiv 23(mod(25))$$

Ahora podemos observar lo siguiente:

$$81 + 144m \equiv 23(mod(25))$$

$$19 + 81m \equiv 23(mod(25))$$

$$6 + 19m \equiv 23(mod(25))$$

$$19m \equiv 17(mod(25))$$

$$m \equiv 17(19^{-1})(mod(25))$$

$$m \equiv 17(6)(mod(25))$$

$$m \equiv 2(mod(25))$$

$$m \equiv 25q + 2$$

Por lo que podemos concluir lo siguiente:

$$n = 81 + 114(25q + 2$$

$$n = 81 + 3600q + 288$$

$$n = 369 + 3600q$$

$$n = 369(mod(3600))$$

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

Inicialmente busquemos algún patron en las potencias de 7:

$$7^1 = 7$$

$$7^2 = 49$$

$$7^3 = 343$$

$$7^4 = 2401$$

$$7^5 = 16807$$

$$7^6 = 117649$$

Si observamos los últimos dígitos de cada resultado nos damos cuenta que siguen un patron cíclico de [7,9,3,1] y que se repiten cada 7 potencias.

El número 355 se puede expresar como el resultado de multiplicar 7 por 71.

Teniendo en cuenta que el ciclo de repeticiones de los números de la forma 7^n se produce cada n+4, si restamos a 71 las posiciones de 4 que podamos (4 * 18 = 68), entonces:

$$7^{71-68} = 7^3$$

$$7^3 = 343$$

Teniendo así 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**

Digamos que existe un factor común mayor que 1 para las expresiones $3k + 4$ y $4k + 5$. A este factor común lo llamaremos b.

Por lo tanto si b es factor común de $3k+4$ y $4k+5$, tiene que dividir las dos expresiones exactamente.

Lo que expresaremos de la siguiente manera:

$$(3k+4)mod(b) = 0$$

$$(4k+5)mod(b) = 0$$

$$(4k+5) - (3k+4) = k+1$$

Entonces si b es factor común de ambas expresiones también se debe de dividir la diferencia $(k+1)$ de forma exacta.

Entonces:

$$(k+1)(mod(b)) = 0$$

$$(b-1+1)(mod(b) = b(mod(b)) = 0$$

Para que esto sea posible b debe de tener el valor de 1
Por lo que las expreciones $3k+4$ y $4k+5$ no tienen un factor común mayor de 1, ya que cualquier potencial factor común tiene que dividir 1 y dejar un residuo, lo cual no es posible.