UNIVERSIDAD NACIONAL DE COLOMBIA
SEDE BOGOTÁ

MATEMÁTICAS DISCRETAS II

Francisco Albeiro Gomez Jaramillo

Sergio Alejandro Nova Pérez
Ingeniería de Sistemas y computación
Facultad Ingeniería

TALLER TEORÍA DE NÚMEROS

Sergio Alejandro Nova Pérez

Mayo 2023

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

No existen.

Para que el máximo común divisor de dos números sea 11, ambos números deben tener a 11 como un factor común. Además, dado que la suma de dos números impares es un número par, y la suma de dos números pares es un número par, al menos uno de los números debe ser par y el otro impar.

Dado que 544 es un número par, el número impar que sumado a él produce 544 debe ser también par. Por lo tanto, podemos escribir la suma como: 544 = 11k + 2m, donde k y m son enteros

De esta expresión podemos ver que el número 2m debe ser par, por lo que m debe ser un número par. Ahora podemos probar algunos valores para m y comprobar si existe algún entero k que satisfaga la ecuación anterior.

Si m = 2, entonces 2m = 4, y tenemos:

544 = 11k + 4
540 = 11k
k = 49.09...

Este valor de k no es un entero, por lo que la elección de m = 2 no funciona.

Si m = 4, entonces 2m = 8, y tenemos:

544 = 11k + 8
536 = 11k
k = 48.72...

Este valor de k tampoco es un entero, por lo que la elección de m = 4 tampoco funciona.

Si m = 6, entonces 2m = 12, y tenemos: 544 = 11k + 12

532 = 11k
k = 48.36...

Una vez más, este valor de k no es un entero, por lo que la elección de m = 6 tampoco funciona.

Podemos seguir probando valores para m, pero como hemos visto que ningún valor de k es un entero, podemos concluir que no 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.

Solución

Regla de Divisibilidad del 8

Primera Opción

Debemos tener en cuenta que para que cualquier número sea divisible por el número 8, sus últimas 3 cifras tienen que ser un múltiplo de 8. Para comprender de mejor manera,se analiza el siguiente ejemplo.

n = 10992

Dado este número, se analizan las tres últimas cifras del número, estas son 992, después de obtener esta cifra, la dividimos sobre 8, realizando la operación tendremos un resultado de 124, dado que es un número entero podemos concluir que el número en principio

Segunda Opción

En relación a esta opción, se puede afirmar que si el n en cuestión es divisible tanto por 2 como por 4, es divisible por 8. Un ejemplo de ello sería el siguiente.

n = 232 ; con base a lo anteriormente mencionado, aplicamos la división de n | 2 y n | 4, para el primer caso de n | 2, basados en la regla de divisibilidad del 2, se tiene que un número entero es divisible por 2 SI su última cifra es 0, 2, 4, 6, o 8. Y por el otro lado, cuando n lo dividimos sobre 4, de igual manera, basados en la regla de divisibilidad del 4, se tiene que un número es divisible por 4 si el número formado por sus dos últimas cifras es divisible por 4, como podemos observar en ambos casos, se cumplen las reglas de divisibilidad, de esta manera podemos comprobar que la afirmación al principio descrita en la segunda opción es verdadera.

Ahora con números más grandes, como por ejemplo el 65.314.638.792, si aplicamos la segunda opción, de manera rápida podemos deducir que este número es divisible por 8, ya que cumple con la regla de divisibilidad del 2, pues su última cifra es el 2 y con la regla de divisibilidad del 4, observamos que el 92 es múltiplo de 4 y por ende podemos decir que el número dado es divisible por 8.

Regla de Divisibilidad del 16

Para que un entero n sea divisible por 16, debe ser divisible tanto por 8 como por 2, esto de manera simultánea, es decir, el n tiene que ser dividido entre 8 y 2, solo así, se puede obtener un número que sea divisible por 16.

Ejemplo: n = 784 ; aplicando las reglas anteriores, tenemos a n | 8 ^{n} | 2 , siguiendo los pasos anteriores, n | 8 = 98 ^{n} | 2 =392, dado estos resultados podemos deducir que el número 784 es divisible por 16.

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

Según la regla de la potencia si $a \equiv b \pmod{n}$,entonces $a^m \equiv b^m \pmod{n}$ Teniendo lo anterior en cuenta.

$$\begin{gathered} b^2 = -b * -b \\ b^2 = b * b \\ \text{Por lo cual en conclusión se tiene que} \\ a^2 \equiv b^2 (\mathit{mod}\ p) \\ a * a \equiv -b * -b (\mathit{mod}\ p) \Longleftrightarrow a * a \equiv b * b (\mathit{mod}\ p) \\ a \equiv \pm b \end{gathered}$$

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

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

$$\begin{gathered} 19^1 \cong 4\ \mathit{mod}\ 5 \\ 19^2 \cong 1\ \mathit{mod}\ 5 \\ 19^3 \cong 4\ \mathit{mod}\ 5 \\ 19^4 \cong 1\ \mathit{mod}\ 5 \end{gathered}$$

Por lo cual

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

Por tanto

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

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

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

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

por ley de los exponentes

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

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

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

Se encuentra programado y esta en el https://github.com/snovap/Discrete-Mathematics-Homework-II.git en el apartado de taller teoría de números

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?

Se encuentra programado y esta en el https://github.com/snovap/Discrete-Mathematics-Homework-II.git en el apartado de taller teoría de números

8 ¿65.314.638.792 es divisible por 24?

Se encuentra programado y esta en el https://github.com/snovap/Discrete-Mathematics-Homework-II.git en el apartado de taller teoría de números

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| $n\ y\ pn$.
Sea $p \mid n$
Se asume que p mide a cualquier escalar de n, incluyendo a n^p, de modo que:

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

Sea p,n números coprimos

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

Por el pequeño teorema de fermat, n$^{p-1} \equiv 1(\ mod\ p), detalmaneraque:$

$$\text{n}(\text{n}^{p-1}) \text{ - n (mod p)}$$
$$\text{n}(1) \text{ - n (mod p)}$$
$$0 \text{ (mod p)}$$

Lo que implica por definición de congruencia y divisibilidad

$$\text{p} \mid (n^p - n)$$

por lo tanto, p | $(n^p - n)$ *únicamente si p es primo*

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

Solución
314 y 159 aplicando la identidad de bezout:

$$314 = 1 *159 + 55$$
$$159 = 1 *155 + 4$$
$$155 = 38 *4 + 3$$
$$4 = 1 *3 + 1$$
$$3 = 3 *1 + 0$$

Aislar los residuos:

$$155 = 314 - (1 *159)$$
$$4 = 159 - (1*155)$$
$$3 = 155 - (38 *4)$$
$$1 = 4 - (1 *3)$$

Sustitución en reversa:

$$1 = 4 -3$$
$$1 = 4 - (155 - (38 *4))$$
$$1 = 4(39) - 155$$
$$1 = 49(159-155) - 155$$
$$1 = 159 (39) + 155 (-40)$$
$$1 = 159 (39) - 40(314-159)$$
$$1 = 159 (79) + 314 (-40)$$
$$1 = 12561 + (- 12560)$$
$$1 = 1$$

Por lo tanto, los números son: X =-40 y Y = 79

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

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

$$a^2 \cong 2^2 \cong 4 \cong 4(mod\ 15)$$
$$b^2 = 8^2 = 64 \cong 4(mod\ 15)$$

Por lo tanto;

$$a^2 \equiv b^2(mod\ 15)$$

Sin embargo, no es cierto que

$$a \equiv b(mod\ 15)\ o\ a \equiv -b(mod\ 15), ya\ que$$
$$a \equiv 2 \equiv 2(mod\ 15)$$
$$b \equiv 8 \equiv 8(mod\ 15)$$

Y tampoco se cumple que

$$a \equiv -b(mod\ 15), ya\ que$$
$$a \equiv 2 \equiv 13(mod\ 15)$$
$$- b \equiv -8 \equiv 7(mod\ 15)$$

En conclusión se tiene que la información es falsa

12 **Encuentre todos los enteros positivos tales que $1066 \equiv 1776(\text{ mod m})$.**

Solución

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

$$1066 \equiv 1776\ (mod\ m)$$
$$1066 - 1066 \equiv 1776 - 1066\ (mod\ m)$$
$$0 \equiv 710\ (mod\ m)$$

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

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

Figure 1: Ejercicio 12

A continuación se presenta un algoritmo para calcular los divisores de 710

Podemos observar que

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

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

Planteamos la información:

$$\text{a}^3 \text{ - (a + 1)}^3 \equiv 0 \text{ (} mod \text{ 5)}$$
$$\text{- 3 a}^2 \text{ - 3a - 1} \equiv 0 \text{ (} mod \text{ 5)}$$

Para esto debe ser posible :

$$\text{- 3 a}^2 \text{ - 3a - 1} \equiv 5 * n$$
$$\text{(- 3 a}^2 \text{ - 3a - 1) / 5} \equiv n$$

No existe un entero el cual $n^2 = 5$ para hacer cumplir la expresión anterior, por lo tanto se demuestra que es falso

$$\text{a}^3 \text{ - (a + 1)}^3 \equiv 0 \text{ (} mod \text{ 5)}$$

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

Se encuentra programado y esta en el https://github.com/snovap/Discrete-Mathematics-Homework-II.git en el apartado de taller teoría de números

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

Solución Para ello se debe determinar un n (mod 10)

Para n = 7^{355}

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

De esta manera, se puede asegurar 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**

Solución

Para esto, se debe tener en cuenta que $d \in Z$
tal que d>1 y d | 3k + 4 así como d | $4k + 5$. Entonces, la división de estos mismos factores por d tienen el mismo residuo:

$$4\text{k} + 5 \cong 3k + 4 (mod 10)$$
$$4\text{k} + 5 - 3\text{k} + 4 = \text{dn}$$
$$\text{k} + 1 = \text{dn}$$
$$\text{k} = \text{dn} -1$$

Como d ∈ 3k + 4 por hipótesis, 3k + 4 = dm , reemplazando:

$$(3\text{d} - 1) + 4 = \text{dm}$$
$$4 - 3 = \text{d} (\text{m} - 3\text{n})$$
$$1 = \text{d}\beta$$

Dado que $\beta \in Z$ β = 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