Matemáticas Discretas II - Taller teoría números

Fernando Novoa Salazar, Universidad Nacional de Colombia

12 de mayo de 2023

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

   Dado que a y b son múltiplos de 11, se pueden expresar como:

   $$a = 11k, a \in Z$$
   $$b = 11q, q \in Z$$

   entonces:

   $$a + b = 544$$
   $$11k + 11q = 544$$
   $$11(k + q) = 544$$
   $$k + q = \frac{544}{11}$$

   Al dividir $\frac{544}{11}$ por división larga, obtenemos:

   $$\frac{544}{11} = 11(49) + 5$$

   Entonces, $\frac{544}{11}$ no es un número entero, ya que el residuo de la división es diferente de 0, por lo tanto, no existen $k, q \in Z$ que cumplan la condición.

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

   Regla de divisibilidad para el 8:
   Dado que todo número se puede expresar como un número de la forma ...EDCBA donde cada letra representa un dígito:

   $$...EDCBA = ...ED \cdot 1000 + CBA$$

   Entonces es divisible por 8 si y solo si el número CBA es divisible por 8. Dado que 1000 es divisible por 8, y D representa las unidades de mil:

   $$1000 \equiv 0 (mod\, 8)$$

Lo que significa que cualquier múltiplo de 1000 también es divisible por 8. Entonces, podemos expresar el número original como un múltiplo de 1000 (que es divisible por 8) más el número CBA, y podemos determinar si el número original es divisible por 8 simplemente verificando si CBA es divisible por 8.

Regla de divisibilidad para el 16:
Dado que todo número se puede expresar de la forma ...FEDCBA donde cada letra representa un dígito:

$$...FEDCBA = ...E \cdot 10000 + DCBA$$

Entonces es divisible por 16 si y solo si el número DCBA es divisible por 16. Dado que 10000 es divisible por 16, y E representa las decenas de mil:

$$10000 \equiv 0 (mod\, 16)$$

Lo que significa que cualquier múltiplo de 10000 también es divisible por 16. Entonces, podemos expresar el número original como un múltiplo de 10000 (que es divisible por 16) más el número DCBA, y podemos determinar si el número original es divisible por 16 simplemente verificando si DCBA es divisible por 16.

3. Si p es un número primo y $a^2 \equiv b^2 (mod\, p)$, pruebe que $a \equiv \pm b$. Se parte de:

$$a^2 \equiv b^2 (mod\, p)$$
$$a^2 - b^2 \equiv 0 (mod\, p)$$
$$(a+b)(a-b) \equiv 0 (mod\, p)$$

Eso significa que p divide a (a + b)(a - b), además sabemos que a, b $\in$ Z, entonces (a+b)(a-b) es el producto de dos enteros, pero por el Lema de Euclides sabemos que p divide a alguno de los dos factores (porque es primo).
En caso de que divida al primer factor, se tiene:

$$(a+b) = kp$$
$$a = kp - b$$

entonces:

$$a \equiv -b (mod\, p)$$

O por otro lado se tiene:

$$(a-b) = kp$$
$$a = kp + b$$

Entonces:

$$a \equiv b(mod\, p)$$

Por eso si p es primo se cumple $a^2 \equiv b^2(mod\, p) \rightarrow a \equiv \pm b(mod\, p)$

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

   En general, para encontrar el resto de un número a elevado a una potencia b, módulo m, se puede usar la técnica de reducir al módulo m cada término de la expresión a^b y luego calcular el resultado final módulo m. En este caso, se puede usar la propiedad de que si $a \equiv b(mod\, m)$, entonces $a^n \equiv b^n(mod\, m)$ para cualquier entero positivo n. Entonces:

$$19 \equiv -1(mod\, 5)$$
$$19^{19} \equiv (-1)^{19} \equiv -1 \equiv 4(mod\, 5)$$

   Por ende, el resto de dividir 19^{19} entre 5 es igual a 4.

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

   Para encontrar los últimos dos dígitos de 7^{7^7}, usamos el teorema de Euler-Fermat.

   Primero, observemos que 7 y 100 son primos relativos, es decir, no tienen factores primos en común. Entonces, podemos utilizar el teorema de Euler-Fermat, que establece que para cualquier entero a y primo relativo m, se cumple que:

$$a^{\phi(m)} \equiv 1(mod\, m)$$

   Donde $\phi(m)$ es la función phi de Euler, que cuenta el número de enteros positivos menores que m que son coprimos con m.

   En este caso, como 100 tiene como factores primos a 2 y a 5, se cumple que $\phi(100) = (2-1)(5-1) = 41 = 4$.

   Entonces, podemos encontrar los últimos dos dígitos de 7^{7^7} encontrando el residuo de 7^{7^7} modulo 100. Utilizando el teorema de Euler-Fermat, tenemos:

$$7^4 \equiv 1(mod\, 100)$$

   Por lo tanto:

$$7^{7^7} = 7^{(4k+3)} = 7^{4k} \cdot 7^3 \equiv 1^k \cdot 7^3 \equiv 7^3(mod\, 100)$$

Entonces, para encontrar los últimos dos dígitos de 7^{7^7}, simplemente necesitamos calcular el residuo de 7^3 modulo 100:

Primero calculemos 7^3:

$$7^3 = 7 \cdot 7 \cdot 7 = 343$$

Entonces, para calcular el residuo de 7^3 módulo 100, necesitamos encontrar los últimos dos dígitos de 343 porque el residuo de 7^3 módulo 100 es simplemente el residuo que queda después de dividir 343 entre 100. En otras palabras, necesitamos encontrar el resto de la división de 343 por 100, que es lo mismo que encontrar los últimos dos dígitos de 343. Por lo tanto, el residuo de 7^3 módulo 100 es 43.
Por lo tanto, los últimos dos dígitos de 7^{7^7} son 43.

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

   Para encontrar $\phi(n)$, se necesita conocer la descomposición en factores primos de n, ya que $\phi(n)$ se calcula multiplicando todos los factores primos distintos de n por $(1-1/p)$, donde p es el factor primo correspondiente.

   Para n=35, descomposición en factores primos de 35:

$$35 = 7 \cdot 5$$

$$\phi(35) = \phi(7 \cdot 5) = \phi(7) \cdot \phi(5) = (5-1) \cdot (7-1) = 24$$

   Para n=100, descomposición en factores primos de 100:

$$35 = (2^2) \cdot (5^2)$$

$$\phi(100) = \phi((2^2) \cdot (5^2)) = \phi(2^2) \cdot \phi(5^2) = (4-2) \cdot (25-5) = 40$$

   Para n=51200, descomposición en factores primos de 51200:

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

$$\phi(51200) = \phi((2^{11}) \cdot (5^2)) = \phi(2^{11}) \cdot \phi(5^2) = (2048-1024) \cdot (25-5) = 20480$$

   Se utiliza el hecho de que la función ϕ es multiplicativa, es decir, $\phi(ab) = \phi(a) \cdot \phi(b)$ para a y b primos relativos. También se utiliza que $\phi(p) = p-1$ para p primo.

7. Usted le pregunta a un robot qué quiere comer. Él responde "48879". Sabiendo que el robot piensa en hexadecimal pero habla en decimal, ¿qué le debería dar de comer?

Debemos convertir 48879_{10} a hexadecimal. Para convertir un número decimal a hexadecimal, lo dividimos por 16 y tomamos el residuo en cada paso en hexadecimal. Para el paso siguiente, tomamos el cociente obtenido en el paso anterior y lo dividimos por 16. El resultado final es la secuencia de residuos en hexadecimal leídos de abajo hacia arriba.

$$48879 \div 16 = 16(3054) + 15$$
$$15_{10} = F_{16}$$

$$3054 \div 16 = 16(190) + 14$$
$$14_{10} = E_{16}$$

$$190 \div 16 = 16(11) + 14$$
$$14_{10} = E_{16}$$

$$11 \div 16 = 16(0) + 11$$
$$11_{10} = B_{16}$$

El resultado es $BEEF_{16}$, es decir, el robot quiere carne de res.

8. ¿65.314.638.792 es divisible por 24?.

Primero creamos una regla de divisibilidad para el 24: todo número se puede expresar de la forma:

$$...FEDCBA = ...D \cdot 1000 + C \cdot 100 + B \cdot 10 + A$$
$$...D{\cdot}1000{+}C{\cdot}100{+}B{\cdot}10{+}A \equiv ...E{\cdot}(-8){+}D{\cdot}(-8){+}C{\cdot}(4){+}B{\cdot}10{+}A (mod\, 24)$$

Esto significa que cualquier número de la forma ...FEDCBA donde las letras representan dígitos, es congruente con el número resultante del dígito de unidades más 10 veces el número de las decenas más 4 veces el dígito de las centenas menos 8 veces la suma del resto de dígitos, con esto se puede desarrollar:

$$65314638792 \equiv (-8)(6+5+3+1+4+6+3+8)+7\cdot 4+9\cdot 10+2 (mod\, 24)$$
$$65314638792 \equiv (-8)(6+5+3+1+4+6+3+8)+28+90+2 (mod\, 24)$$
$$65314638792 \equiv (-8)(36)+28+90+2 (mod\, 24)$$
$$65314638792 \equiv -168 (mod\, 24)$$
$$65314638792 \equiv 0 (mod\, 24)$$

Por lo tanto, 65 314 638 792 es divisible por 24.

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

   De acuerdo a el pequeñoo teorema de Fermat, se puede afirmar si que si a y p son primos relativos se va a cumplir que:

   $$a^{p-1} \equiv 1(mod\, p)$$

   Por lo tanto, al ser p un número primo, se tiene que:
   $\neg(p|a) \rightarrow mcd(p, a) = 1$
   si p no divide a a, entonces son coprimos. Podemos afirmar lo siguiente:

   $$a^{p-1} \equiv 1(mod\, p)$$
   $$a^{p-1} \times a \equiv 1 \times a(mod\, p)$$
   $$a^p \equiv a(mod\, p)$$
   $$a^p - a \equiv a - a(mod\, p)$$
   $$a^p - a \equiv 0(mod\, p)$$

   Entonces, $(p - a)|p$.
   Por otro lado, si consideramos que $p|a$ entonces también tenemos que $p|a^p$ por ser múltiplo de a y además $\exists k \in Z$ tal que: $a^p = kp$
   $a^p - a = kp - a$.
   Como sabemos que e a es múltiplo de p podemos decir que $\frac{a}{p} \in Z$, entonces:

   $$a^p - a = p(k - \frac{a}{p}) + 0$$

   $\leftrightarrow a^p - a \equiv 0(mod\, p)$
   Por lo tanto, $n^p - n$ es divisible por p si p es un número primo.

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

    Para encontrar los enteros x e y que satisfagan $314x + 159y = 1$, usamos el algoritmo de Euclides:
    Empezamos buscando el máximo común divisor entre 314 y 159. Usando el algoritmo de Euclides tenemos:

    $$314 = 1 \cdot 159 + 155$$
    $$159 = 1 \cdot 155 + 4$$
    $$155 = 38 \cdot 4 + 3$$
    $$4 = 1 \cdot 3 + 1$$

    La última ecuación dice que $mcd(314, 159) = 1$.
    Ahora, haremos sustitución regresiva, usando las ecuaciones para encontrar x e y en términos de 314 y 159:

$$1 = 4 - 1 \cdot 3$$

$$1 = 4 - 1 \cdot (155 - 38 \cdot 4)$$

$$1 = 39 \cdot 4 - 155$$

$$1 = 39 \cdot (159 - 1 \cdot 155) - 155$$

$$1 = 39 \cdot 159 - 40 \cdot 155$$

$$1 = 39 \cdot 159 - 40 \cdot (314 - 1 \cdot 159)$$

$$1 = 79 \cdot 159 - 40 \cdot 314$$

Por lo tanto, hemos encontrado $x = -40$ e $y = 79$ como solución a la ecuación $314x + 159y = 1$.

Podemos comprobar remplazando en la ecuación:
$314(-40) + 159(79) = 1$
$-12560 + 12561 = 1$
$1 = 1$
Por lo tanto, los valores hallados son solución.

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

    Se controvierte, con a=2, b=8 y m = 15 ya que se cumple:

    $$2^2 \equiv 8^2 (mod\, 15)$$

    $$4 \equiv 64 (mod\, 15)$$

    Pero no se cumple:

    $$2 \equiv 8 (mod\, 15)$$

    y tampoco se cumple:

    $$2 \equiv -8 (mod\, 15)$$

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

    Para encontrar todos los enteros positivos que satisfagan la congruencia $1066 \equiv 1776 (mod\, m)$, podemos restar 1066 de ambos lados y simplificar:

    $$1066 \equiv 1776 \pmod{m}$$

    $$1066 - 1776 \equiv 0 \pmod{m}$$

$$-710 \equiv 0 \pmod{m}$$

Por lo tanto, necesitamos encontrar los enteros positivos que dividan a 710.
Podemos factorizar 710 como $2 \cdot 5 \cdot 71$, por lo que los divisores positivos de 710 son 1, 2, 5, 10, 71, 142, 355 y 710.

Cada uno de estos números es un posible valor para m que satisfaga la congruencia original. Podemos verificar que cada valor funciona sustituyéndolo en la congruencia original:

$$1066 \equiv 1776 \pmod{1}$$
$$1066 \equiv 1776 \pmod{2}$$
$$1066 \equiv 1776 \pmod{5}$$
$$1066 \equiv 1776 \pmod{10}$$
$$1066 \equiv 1776 \pmod{71}$$
$$1066 \equiv 1776 \pmod{142}$$
$$1066 \equiv 1776 \pmod{355}$$
$$1066 \equiv 1776 \pmod{710}$$

Por lo tanto, los enteros positivos que satisfacen la congruencia $1066 \equiv 1776(modm)$ son 1, 2, 5, 10, 71, 142, 355 y 710.

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

Usamos pruebas por casos.

Supongamos que tenemos dos cubos consecutivos, $(n-1)^3 y n^3$, y queremos demostrar que su diferencia, $n^3 - (n-1)^3$, nunca es divisible por 5.

Primero, notemos que la diferencia entre dos cubos consecutivos se puede expresar como:

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

Entonces, si queremos demostrar que esta expresión nunca es divisible por 5, podemos probar que no hay ningún entero n para el cual $3n^2 - 3n + 1$ es divisible por 5.

Tomando módulo 5, podemos reducir la expresión a:

$$3n^2 - 3n + 1 \equiv n^2 - n + 1 (mod\, 5)$$

Ahora, podemos comprobar que $n^2 - n + 1$ nunca es divisible por 5 para cualquier entero n. En particular, podemos verificar cada caso posible:

Cuando $n \equiv 0(mod\,5) \rightarrow n^2 - n + 1 \equiv 1(mod\,5)$
Cuando $n \equiv 1(mod\,5) \rightarrow n^2 - n + 1 \equiv 2(mod\,5)$
Cuando $n \equiv 2(mod\,5) \rightarrow n^2 - n + 1 \equiv 2(mod\,5)$
Cuando $n \equiv 3(mod\,5) \rightarrow n^2 - n + 1 \equiv 2(mod\,5)$
Cuando $n \equiv 4(mod\,5) \rightarrow n^2 - n + 1 \equiv 1(mod\,5)$

En todos los casos, se obtiene un residuo distinto de cero, lo que demuestra que $n^2 - n + 1$ no es divisible por 5 para ningún entero n. Por lo tanto, la diferencia de dos cubos consecutivos nunca es divisible por 5.

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

Partimos de:

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

$$n + 1 \equiv 0(mod\,16)$$

$$n + 2 \equiv 0(mod\,25)$$

este sistema de equivalencias también se puede expresar como:

$$n + 3 \equiv 3(mod\,9)$$

$$n + 3 \equiv 2(mod\,16)$$

$$n + 3 \equiv 1(mod\,25)$$

Así que se puede resolver con el Teorema del Resto Chino, primero se define $m = 9 \cdot 16 \cdot 25$, entonces tenemos que:

$$M_1 = 16 \cdot 25 = 400$$

$$M_2 = 9 \cdot 25 = 225$$

$$M_3 = 16 \cdot 9 = 144$$

Hallamos los inversos y_k:

$$y_1 = 400y_1 \equiv 1(mod\,9)$$

$$400y_1 = 9k + 1$$

$$400y_1 - 9k = 1$$

Se descomponen con el algoritmo de Euclides:

$$400 = 9(44) + 4$$

$$9 = 4(2) + 1$$

$$4 = 4(1) + 0$$

Hacemos sustitución regresiva:

$$1 = 9 - 4(2)$$

$$4 = 400 - 9(44)$$

$$1 = 2(400 - 9(44)) + (9 - 2(4)) - 2(400 - 9(44))$$

$$1 = 9(89) - 2(400)$$

$$1 = (-2)(400) - (-9)(89)$$

Debido a esto y_1 = -2, -2 $\equiv$ 7(mod 9):

$$y_2 = 225y_2 \equiv 1(mod 16)$$

$$225y_2 = 16k + 1$$

$$225y_2 - 16k = 1$$

Descomponemos con el algoritmo de Euclides:

$$225 = 16(14) + 1$$

$$16 = 16(1) + 0$$

Del algoritmo despejamos $y_2 = 1, 1 \equiv -15(mod\, 16)$

$$y_3 = 144y_3 \equiv 1(mod\, 25)$$

$$144y_3 = 25k + 1$$

$$144y_3 - 25k = 1$$

Descomponemos con el algoritmo de Euclides:

$$144 = 25(5) + 19$$

$$25 = 19 + 6$$

$$19 = 3(6) + 1$$

$$6 = 6(1) + 0$$

Hacemos sustitución regresiva:

$$1 = 19 - 3(6)$$

$$6 = 25 - 19$$

$$19 = 144 - 25(5)$$

$$1 = 144 - 25(5) - 3(25 - (144 - 25(5)))$$

$$1 = 144 - 25(5) - 3(-144 + 6(25))$$

$$1 = 4(144) - 25(23)$$

Con todas las variables halladas, despejamos n:

$$x = a_1M_1y_1 + a_2M_2y_2 + a_3M_3y_3$$

$$n + 3 = 3(400)7 + (2)(225)(1) + (1)(144)(4)$$

$$n + 3 = 9426$$

$$n = 9423$$

Además, hay que tener en cuenta que n no es único, por lo cual también se puede despejar de la forma:

$$n + 3 = 3(400)7 + (2)(225)(-15) + (1)(144)(4)$$

$$n + 3 = 2226$$

$$n = 2223$$

Como las congruencias se cumplen solo para 3 se puede concluir que n es 2223.

15. ¿Cuál es el último dígito de 7^{355}?
Observemos que los últimos dígitos de las potencias de 7 siguen un patrón:

$$7^1 = 7$$

$$7^2 = 49$$

$$7^3 = 343$$

$$7^4 = 2401$$

$$7^5 = 16807$$

$$7^6 = 117649$$

$$7^7 = 823543$$

$$7^8 = 5764801$$

$$7^9 = 40353607$$

$$7^{10} = 282475249$$

$$...$$

A partir de 7^4, el último dígito de las potencias de 7 se repite cada 4 potencias: 7, 9, 3, 1. Específicamente, el último dígito de 7^n es 7 cuando $n \equiv 1\, mod\, 4$.

Entonces, para encontrar el último dígito de 7^{355}, podemos encontrar el resto de 355 dividido por 4.

$$355/4 = 88, \, resto \, 3$$

Por lo tanto, el último dígito de 7^{355} es el mismo que el último dígito de 7^3, es decir, el último dígito de 343, que es 3.

Por lo tanto, 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.

Tomamos $j = k + 1$, y definimos d como el factor común más grande de los dos números, d es entero y positivo. Planteamos:

$$3k + 4 = 3k + (3 + 1) = 3(k + 1) + 1 = 3j + 1$$

$$3j + 1 = pd, p \in Z$$

$$j = \frac{pd - 1}{3}$$

$$y$$

$$4k + 5 = 4k + (4 + 1) = 4(k + 1) + 1 = 4j + 1$$

$$4j + 1 = td, t \in Z$$

$$j = \frac{td - 1}{4}$$

Se iguala j:

$$j = j$$

$$\frac{pd - 1}{3} = \frac{td - 1}{4}$$

$$4pd - 4 = 3td - 3$$

$$4pd - 3td = 1$$

$$d(4p - 3t) = 1$$

Dado que se llegó a la forma:

$$dm = 1$$

y d tiene que ser positivo y entero, $d \geq 1$ y m tiene que ser un número entero porque $p, t \in Z$, entonces d tiene que ser 1.