Taller de la OMM Aguascalientes
Teoría de Números

Combinación lineal

Dentro de las propiedades anteriores, hay una que requiere especial atención y será mucho más relevante cuando hagamos el salto a las congruencias.

Definición. Dados dos enteros a y b definimos una combinación lineal de a y b como un número de la forma

$$ax + by,$$

donde son también enteros. En la propiedad (10) de la clase de definiciones y propiedades de la división, demostramos que si es un divisor común de a y b , entonces divide a cualquier combinación lineal de éstos. Esto es cierto para cualquier divisor común pero será especialmente relevante para el máximo común divisor. Vamos a trabajar unos ejemplos para mostrar algunas propiedades relevantes de la combinación lineal.

Ejemplos

1. Expresar 0 como combinación lineal de 3 y de 11 de dos maneras distintas.

   Solución. Basta con encontrar una y podemos generar infinitas a partir de ésta. Veamos que

   $$0 = 3(11) + 11(-3)$$

   . Entonces, también se cumple que

   $$0 = 3(11)k + 11(-3)k,$$

   para todo entero k.

2. Encuentra un número impar que sea combinación lineal de 12 y de 46.

   Solución. Esto es imposible. Como 2 es divisor común de 12 y 46, divide a cualquier combinación lineal de ellos y es claramente imposible que 2 divida a un número impar.

3. Demuestra por qué es imposible encontrar enteros u, v tales que 6u + 9v = 2.

   Solución. Basta ver que estamos buscando una combinación lineal de 6 y de 9 que sea igual a 2. Como 3 es divisor común, tendría que pasar que 3 dividiera a 2, lo cual no pasa. Factorizando, vemos que

   $$3(2u + 3v) = 2$$

   del lado izquierdo de la igualdad tenemos un múltiplo de 3 pero del lado derecho no. Por lo tanto, esa igualdad es imposible.

Teorema. Si a, b, c están relacionados por la ecuación $b + c = k$, y un número d es divisor de cualesquiera dos de ellos, entonces también lo es del tercero.
Demostración. Si los números son $b, , c$, está claro pues lo anterior es una combinación lineal. Para cualquier otro caso, basta con despejar para obtener combinaciones lineales: $b = k - c$ o $c = k - b$.

Ejercicios

1. Expresar 1 como combinación lineal de -3 y de 4 de tres maneras distintas.

2. Expresar 20 como combinación lineal de 7 y de 4.

3. Sea k un entero positivo y sea $a = 13k + 1$ y $b = -26k + 4$. Demuestra que los únicos divisores positivos comunes posibles de a y b son $1, 2, 3$ o 6.

4. Raúl quiere llenar su cantimplora de 1L y lo único que puede hacer es llenar sus cubetas de 3L, 9L, 21L y 15L completas desde el río o pasar de una cubeta a otra cubeta agua siempre que se pase toda o toda la que cabe (no puede meter la cantimplora al río ni llenarla desde una cubeta si sobra en la cubeta). ¿Cómo puede hacer esto Raúl?

5. En un juego de fútbol americano, un equipo puede anotar 3 o 7 puntos. ¿Cuál es el número más grande de puntos que no puede anotar un equipo, suponiendo tiempo infinito?

6. Tres amigos estaban jugando a lanzar dados, quien tuviera el resultado más grande ganaba 4 puntos, y el que tuviera el resultado más chico ganaba 2. Después de jugar varias partidas anotaron sus puntos y cada uno dijo que los siguientes eran sus puntajes, Manuel 18 puntos, Jacsan 7 puntos y Chino 6 puntos. ¿Quién de ellos miente en sus puntajes?

7. Don Manuel tiene un tanque con mucha leche y dos cubetas, una de 5 litros y otra de 9 litros. ¿Puede medir 2 litros? ¿Cómo?

8. Prueba que ninguno de los números 1573, 157573, 15757573,... es un número primo.

9. Sean a, b enteros tales que $a + 5b$ y $5a - b$ son ambos divisibles por 2002. Pruebe que $a^2 + b^2$ también es divisible por 2002.

Máximo común divisor y mínimo común múltiplo

Estos dos temas se incluyen en el programa de primaria y secundaria así que no son nuevos al momento de llegar a la Olimpiada.

Definición. El mínimo común múltiplo de dos enteros a, b es el menor entero m tal que $a \mid m$ y $b \mid m$ La anterior definición es bastante directa porque los nombres son completamente explícitos: el mínimo común múltiplo de dos números es el menor de sus múltiplos comunes.

Notación. Si el mínimo común múltiplo de dos enteros a, b es m, escribimos

$$[a, b] = m$$

, En algunos textos se denota también como MCM$[a, b]$.

El mínimo común múltiplo de dos números es a lo menos el más grande de ambos. Es obvio que si es más pequeño que el más grande, entonces no puede ser múltiplo del más grande. Por otro lado, el máximo común divisor de dos números es a lo más el más chico de ambos. Es obvio que si es más grande que el más pequeño, entonces no puede ser divisor del más pequeño.

Definición. El máximo común divisor de dos números (a, b) es d el mayor entero tal que $d \mid a$ y $d \mid b$.

Al igual que con el mínimo común múltiplo, la definición es bastante directa: el máximo común divisor es, de entre los divisores comunes, el mayor.

Notación. Si el máximo común divisor de dos números es a, b es d, escribimos

$$(a, b) = d$$

.

En algunos textos se denota también por $mcd(a, b)$.

Si tienes confusión entre si el múltiplo o el divisor es el mínimo o el máximo, piensa que no tiene sentido preguntarnos por el máximo común múltiplo, pues siempre podemos encontrar un múltiplo común más grande, ni tiene sentido preguntarnos por el mínimo común múltiplo, que siempre es 1.

Ahora que eres el chico más popular y que sabes el teorema fundamental de la aritmética, encontrar el mínimo común múltiplo o el máximo común divisor no debe ser muy complicado. Sólo sigue la siguiente receta: a) Encuentra la descomposición en primos de cada uno de los números cuyo MCM quieras encontrar.

(a) Para el mínimo común múltiplo, compara su descomposición en primos y escribe todos los primos que aparezcan en la potencia más grande que aparezcan.

(b) Para el máximo común divisor, escribe sólo los primos que aparecen en ambas descomposiciones a la menor potencia que aparezcan.

Lo anterior se puede generalizar sin mucho problema de dos a cualquier cantidad de números.

Una interesante relación entre estos dos números se establece en el siguiente teorema.

Teorema. Dados dos enteros a, b tenemos que

$$ab = [a, b]x(a, b)$$

.

Para calcular el máximo común divisor, nos podemos servir de los siguientes teoremas.

Teorema (Algoritmo de Euclides). Dados enteros a, b,

$$(m, n) = (m, n - km)$$

para cualquier entero k. En particular, si $n = km + r$,

$$(m, n) = (m, r).$$

Teorema. Dados enteros m, n donde k es un divisor común de ambos, tenemos que

$$(m, n) = k(\frac{m}{k}, \frac{n}{k}).$$

Ejercicios

1. Hallar el máximo común divisor , de los números 12, 30 y 18.
2. Escribir el máximo común divisor de 99 y 68 como combinación lineal de estos números.
3. Determinar si 7 y 20 son combinación lineal de 12 y 28; en caso afirmativo, escribir una combinación lineal en cada caso.
4. Encontrar $mcd(44, 531)$. Encontrar $mcd(16500, 1050)$.
5. Sean a, b, c, d, e enteros positivos que cumplen que $a = 2b = 3c = 4d = 6e$. ¿Cuál es el mínimo valor que puede tomar la suma $a + b + c + d + e$?
6. Yo voy diario al gimnasio. Pablo va al gimnasio cada 2 días. Luis va cada 3 días. Neto va cada 5 días. Germán va cada 12 días. Atari va cada 11 días. Si todos fuimos hoy al gimnasio, ¿en cuántos días nos volveremos a encontrar todos?
7. Un granjero tiene un montón de naranjas y mucho tiempo libre. Se da cuenta que si lo divide en 2 montones, en 3 montones, en 4 montones, en 13 montones o en 21 montones siempre un montón tiene exactamente 1 naranja más que los demás pero si los divide en 41 montones entonces todos tienen las mismas naranjas. ¿Cuál es la menor cantidad de naranjas que puede tener que cumplan todo eso?
8. Encuentra el máximo común divisor de los números

$$3^3 - 3, 5^5 - 5, 7^7 - 7, 9^9 - 9, ..., 2013^{2013} - 2013$$

9. ¿Es posible que el mínimo común múltiplo de los números del 1 al n sea exactamente 2008 veces el mínimo común múltiplo de los números del 1 al m ?

Este material fue tomado del libro "Diminuto Curso de Teoría de Números y Anexas".

Material selecionado por Roberto Kú y Horacio Sáenz.