Explorando el problema de las monedas

Taller para profesores - OLCOMA 2019

Daniel Campos y Adrián Naranjo

(Material en construcción)

Dados dos enteros positivos a y b, vamos a considerar problemas sobre sus combinaciones lineales; es decir, vamos a considerar números de la forma $am + bn$ con enteros m y n.

Ejercicio. *Dados 8 y 12, ¿se puede obtener 1 o 2? Con 5 y 13, ¿se puede obtener 1 o 7?*

Intentando resolver el problema nos damos cuenta que hay que tener cuidado de los **divisores comunes**. Por ejemplo, cualquier combinación lineal de 8 y 12 será divisible por 4, su **máximo común divisor**. Si dividimos por el máximo común divisor, entonces obtenemos dos números coprimos; para el resto de la exposición solo vamos a considerar este caso. Esto nos lleva a la siguiente pregunta:

Dados dos números coprimos, ¿cuáles números podemos obtener como combinaciones lineales?

Dos posibles problemas resultan dependiendo de las condiciones con las que queramos resolver el problema: si permitimos combinaciones lineales arbitrarias (es decir, m y n pueden tomar cualquier valor entero) o solo combinaciones lineales *no negativas*. Resolveremos el primer problema de dos maneras, una más técnica y "gráfica", y otra con un procedimiento constructivo llamado el **algoritmo de Euclides**. Al segundo problema se le conoce como el **problema de las monedas** y para resolverlo usaremos las ideas y resultados del primero.

1 Combinaciones lineales enteras

Ejercicio. *Escoja su par favorito de números coprimos y obtenga* 1 *como una combinación lineal.*

¿Por qué estamos tan interesados en obtener 1 como una combinación lineal? Una razón es que si resolvemos esto, entonces podemos producir cualquier otro número; por ejemplo, si $am + bn = 1$, entonces $a(2m) + b(2n) = 2$, y así en general.

Por lo tanto, nuestro problema se reduce a hallar enteros m y n tales que $am + bn = 1$. Otras formulaciones equivalentes del problema pueden ser: encontrar un entero m tal que $am-1$ sea divisible por b, o bien, encontrar un entero m tal que am deja residuo 1 al dividirse por b.

Si este fuera el caso, entonces existirían otros enteros (por ejemplo, $2m$, $3m$ y así sucesivamente) que dejan todos los demás residuos. Notemos también que al considerar el residuo de am módulo b es suficiente considerar el residuo de m módulo b, por lo que es suficiente considerar el caso $0 \leq m \leq b-1$.

Teorema 1.1. *Si* $(a, b) = 1$*, entonces los residuos módulo* b *del conjunto* $\{0, a, 2a, \ldots, (b-1)a\}$ *son los mismos que el conjunto de residuos* $\{0, 1, \ldots, b-1\}$*. En particular, existe* $0 \leq m \leq b-1$ *tal que* am *deja residuo* 1 *al dividirse por* b*.*

Una manera de visualizar esto es desplegando en filas y b columnas los números empezando desde cero. Cada una de estas columnas representa un residuo $\{0, 1, \ldots, b-1\}$. Marcamos los números

$\{0, a, 2a, \ldots\}$ y observamos (luego lo demostraremos) que estas se ubican sobre diferentes columnas. El ejemplo muestra la distribución con $a = 3$ y $b = 7$:

$\boxed{0}$	1	2	$\boxed{3}$	4	5	$\boxed{6}$
7	8	$\boxed{9}$	10	11	$\boxed{12}$	13
14	$\boxed{15}$	16	17	$\boxed{18}$	19	20
−−	−−	−−	−−	−−	−−	−−
$\boxed{21}$	22	23	$\boxed{24}$	25	26	$\boxed{27}$
28	29	$\boxed{30}$	31	32	$\boxed{33}$	34

Tenemos que desplegar los primeros b múltiplos de a en estas columnas. Si demostramos que no hay dos de ellos que vayan en la misma columna, entonces cada columna debe contener exactamente uno de ellos, que es exactamente el enuncadio del teorema. Si hubiera dos de ellos sobre la misma columna, digamos aj y ak, entonces b divide a su diferencia $a(j-k)$. Como $(a, b) = 1$, entonces esto implica que b debe dividir a $j - k$, lo cual no es posible porque $0 < |j - k| \leq b - 1$. Esto completa la demostración del teorema y la solución del problema.

Habiendo terminado la prueba, podemos volver a ver el problema[1]. El argumento de la prueba y la figura muestran lo mismo: si hay dos múltiplos que se encuentran sobre la misma columna entonces ab divide su diferencia. Un último comentario: si d es el máximo común divisor de A y B, entonces podemos escribir $A = da$ y $B = db$ con $(a, b) = 1$. De esta manera existen m y n tales que $am + bn = 1$ y por lo tanto $Am + Bn = d$. Como d divide a cualquier combinación lineal de A y B, concluimos entonces que los números que se pueden representar de esta forma son exactamente *todos* los múltiplos de d.

1.1 Algoritmo euclidiano

En esta sección elaboramos una manera más sistemática de encontrar el máximo común divisor de dos enteros positivos. A este procedimiento se le conoce como el **algoritmo euclidiano**. Como consecuencia de esto obtenemos una combinación lineal que es igual al máximo común divisor.

Sean a y b los enteros positivos y supongamos sin pérdida de generalidad que $a > b$. Vamos a definir una sucesión $\{c_n\}$ de la siguiente manera: $c_0 = a$, $c_1 = b$, y para $n \geq 1$ definimos c_{n+1} como el residuo al dividir c_{n-1} por c_n. El proceso se detiene cuando $c_{n+1} = 0$.

Ejemplo. *Llevemos a cabo la construcción con $a = 48$ y $b = 10$. Vamos a encerrar los términos de la sucesión:*

$$\boxed{48} = 4 \cdot \boxed{10} + \boxed{8}$$

$$\boxed{10} = 1 \cdot \boxed{8} + \boxed{2}$$

$$\boxed{8} = 4 \cdot \boxed{2} + \boxed{0}$$

Vamos a estar interesados en el último término no nulo de la sucesión, que en este caso es 2.

Ejercicio. *Lleve a cabo el algoritmo para los pares de números* $(12, 80)$, $(35, 90)$, $(37, 101)$ *y* $(300, 2019)$.

Con el resultado del ejemplo y de este ejercicio nos atrevemos a realizar la siguiente conjetura:

El último término no nulo de la sucesión es el máximo común divisor de los primeros dos términos.

Antes de demostrar la conjetura observamos lo siguiente: c_{n+1} es una combinación lineal de c_{n-1} y c_n. Como consecuencia de esto se sigue que todos los términos de la sucesión son combinaciones lineales de $c_0 = a$ y $c_1 = b$. Esto implica que el máximo común divisor de a y b divide a todos los términos de

[1] En [6], Pólya propone esto ("Mirar atrás") como el cuarto paso en la solución de un problema.

la sucesión, y en particular divide al último. Por lo el máximo común divisor es menor o igual que el último término.

Otra observación necesaria es que el último término no nulo no solo divide al anterior, sino a todos los demás. En efecto, si c_N es este término, entonces c_N divide a c_{N-1} porque $c_{N+1} = 0$. Además, la relación

$$c_{N-2} = q \cdot c_{N-1} + c_N,$$

muestra que c_N divide a c_{N-2}, y continuando de esta manera se demuestra la segunda observación. Esto implica que c_N divide a a y b, y por lo tanto c_N es menor o igual que el máximo común divisor.

Las dos observaciones anteriores implican que el último término debe ser igual al máximo común divisor, como queríamos demostrar.

1.2 Problemas

Ejercicio. *Si $(a, b) = 1$ y $am_1 + bn_1 = am_2 + bn_2$, ¿qué se puede decir sobre m_1, m_2, n_1, n_2?*

Problema 1. *Dos amigos tienen un refresco de 2 L y dos envases de 750 mL y 1250 mL. ¿Cómo pueden hacer para dividirlo en dos cantidades iguales? Ver [4].*

Problema 2. *Suponga que hay dos jarrones de 3 y 7 litros, y es permitido llenarlos, vaciarlos y vertir uno en el otro. Muestre cómo se pueden obtener exactamente 1, 2, 4, 5 y 6 litros.*

Problema 3. *Para preparar un desayuno perfecto, un chef decide hervir un huevo exactamente por 15 minutos. Él tiene dos relojes de arena, uno de 7 minutos y otros de 11 minutos. ¿Cómo debe hacer para preparar su desayuno? ¿Cuántas veces debe voltear los relojes? ¿Cuál es el número mínimo de vueltas que necesita? Ver [4] o [5].*

Problema 4 (IMO 1959)**.** *Demuestre que la fracción $(21n + 4)/(14n + 3)$ es irreducible para todo $n \in \mathbb{N}$.*

2 Combinaciones lineales no negativas

Ahora consideramos el problema de representar números de la forma $am + bn$ con m y n enteros no negativos. Al igual que en el problema anterior, empezamos considerando el caso en que a y b son coprimos.

Ejercicio. *Suponga que $a = 2$. Si b es un número impar, ¿cuáles números se pueden representar en cada caso? ¿Qué pasa con $a = 3$ y b coprimo con 3?*

El ejercicio anterior nos brinda evidencia para realizar la siguiente conjetura:

> *Existe un entero $N = N(a, b)$, tal que si $k \geq N$, entonces existen enteros no negativos m y n tales que $k = am + bn$.*

Ejercicio. *Conjeture una fórmula para $N(a, b)$ basándose en los casos anteriores. Si siente que no tiene la información suficiente, puede empezar calculando $N(4, 5)$, $N(4, 7)$, $N(4, 9)$ y quizá pueda hacer una conjetura.*

1	2	3	4	5	6	7
8	9	10	11	12	13	14
15	16	17	18	19	20	21
22	23	24	25	26	27	28
29	30	31	31	32	33	34

Posiblemente haya conjeturado que $N(a,b) = ab - a - b + 1 = (a-1)(b-1)$. No es fundamental, pero es muy útil, darse cuenta de que la fórmula es **simétrica** con respecto a a y a b. Esto es de esperarse, pues no hay diferencia entre los roles que juegan ambas variables.

Debemos probar dos cosas: primeramente, $N(a,b) \geq ab - a - b + 1$, es decir, $ab - a - b$ no puede ser representado de esta manera. En segundo lugar, $N(a,b) \leq ab - a - b + 1$, es decir, que todo número estrictamente mayor a $ab - a - b$ es representable de dicha manera.

Empecemos con la primera: suponga por contradicción que

$$ab - a - b = am + bn,$$

para algunos $m, n \geq 0$. Esto implica que

$$ab = a(m+1) + b(n+1).$$

Por ende, a divide a $b(n+1)$. Como $(a,b) = 1$, se sigue que a divide $n+1$; y por lo tanto ab divide a $b(n+1)$. Como $b(n+1) > 0$ obtenemos que $ab \leq b(n+1)$. Análogamente, $ab \leq a(m+1)$. Esto nos da una contradicción debido a que

$$ab = a(m+1) + b(n+1) \geq ab + ab = 2ab,$$

y $ab > 0$. Demostraremos ahora la segunda parte. Hemos probado que si $c > 0$, entonces existen $m, n \geq 0$ tales que

$$ab - a - b + c = am + bn.$$

Esto es lo mismo que requerir que exista $m \geq 0$ tal que

$$\frac{ab - a - b + c - am}{b}$$

es un entero no negativo, es decir, $ab - a - b + c - am$ es no negativo y es divisible por b. La condición de divisibilidad equivale a decir que $a(m+1) - c$ es divisible por b, mientras que la condición de no negatividad se puede reescribir como

$$a(b - 1 - m) - b + c \geq 0.$$

Note que Teorema 1.1 nos dice que existe algún $m \in \{0, 1, \ldots, b-1\}$ que hace a $a(m+1) - c$ divisible por b. Solo nos falta verificar la no negatividad. Podemos separar esto en dos casos, que son sugeridos de la forma en que reacomodamos la expresión anterior.

Caso 1: $m = b - 1$. Esto implica que $a(m+1) = ab$, y como $a(m+1) - c$ es divisible por b, se sigue que c es divisible por b. Como $c > 0$ tenemos que$c \geq b$. Obtenemos entonces que

$$a(b - 1 - m) - b + c = c - b \geq 0.$$

Caso 2: $m \in \{0, 1, \ldots, b-2\}$. En este caso obtenemos que $b - 1 - m \geq 1$, y así

$$a(b - 1 - m) - b + c \geq a - b + c.$$

En general esta expresión no tiene por qué ser no negativa. Sin embargo, como a y b tienen el mismo rol, podemos asumir sin pérdida de generalidad que $a > b$ (si este no fuera el caso, podríamos repetir nuestro argumento anterior intercambiando los roles de a y b). Con esto obtenemos que

$$a(b - 1 - m) - b + c \geq a - b + c > c > 0,$$

con lo que concluye la prueba del resultado

Comentario. *Es interesante notar cómo la simetría (y romper la simetría también) fue importante para resolver el problema cuando no parecía ser relevante.*

Comentario. *Es útil notar que, bajo la suposición de que $a > b$, si $t \geq (a-1)(b-1)$ pudimos producir una representación $t = am + bn$ con $0 \leq m \leq b-1$.*

Una pregunta interesante que está relacionada es la siguiente.

¿Qué podemos decir acerca de los números pequeños que no pueden ser escritos en esta forma?

Ejercicio. *Devuélvase a sus ejemplos y vea los números que no pudieron ser expresados de esta forma. ¿Puede ver algún patrón? ¿Cuál es el número de dichos elementos?*

Con los ejemplos, hacemos la siguiente afirmación.

Si $t \leq (a-1)(b-1)$, entonces t puede ser expresado en la forma $am + bn$ si y solamente si $ab - a - b - t$ no lo puede ser.

Una cosa que es fácil de ver es que si t puede ser representado de esta forma entonces $ab - a - b - t$ no puede ser representado. De lo contrario, sería posible escribir su suma, $ab - a - b$, de esta forma y ya vimos que esto no es posible. Sólo falta mostrar el converso.

De la parte anterior sabemos que podemos representar cualquier número en la forma $t = am + bn$, con m, n números enteros, no necesariamente no negativos. Podemos asumir que $0 \leq m \leq b-1$, "pasando el contenido" a b. En tal caso, tenemos que

$$ab - a - b - t = ab - a - b - am - bn = a(b - 1 - m) + b(-n - 1).$$

Note que $b - 1 - m \geq 0$ y que no es posible que ambos n y $(-n - 1)$ sean negativos simultáneamente. Esto muestra que t o $ab - a - b - t$ puede ser representado de la manera que queremos, y esto concluye la prueba de nuestra afirmación.

2.1 Problemas

Problema 5 (AIME 1994)**.** *Hay 94 bloques, que miden $4 \times 10 \times 19$, están puestos uno encima del otrode manera que se forma una torre de 94 bloques. Cada bloque se puede orientar de tal modo que contribuya 4, 10 o 19 a la altura total de la torre. Determine la totalidad de alturas de la torre que se puede lograr usando todos los bloques.*

Problema 6 (IMO 1983)**.** *Sean a, b, c números primos relativos dos a dos. Muestre que el mayor número que no puede ser expresado en la forma $mab + nbc + pca$, con m, n, p números no negativos, es $2abc - ab - bc - ca$.*

Problema 7 (Art of Problem Solving, [1])**.** *Sean $a_1, a_2, \ldots, a_n$ números enteros positivos y coprimos dos a dos. Muestre que el mayor número que no puede ser expresado en la forma*

$$\sum_{k=1}^{n} m_k \prod_{j \neq k} a_j,$$

con $m_1, \ldots, m_n$ números no negativos, es

$$(n-1)a_1 \ldots a_n - \sum_{k=1}^{n} \prod_{j \neq k} a_j.$$

Problema 8 (Putnam 1991)**.** *Determine si existe un número real L tal que si m y n son números enteros mayores que L, entonces un rectángulo $m \times n$ puede ser expresado como una unión de rectángulos 4×6 y 5×7, que se intersequen a lo sumo en su frontera.*

Problema 9. *Sea $A \subseteq \mathbb{N}$ un conjunto cerrado bajo suma tal que $\mathbb{N} \setminus A$ es infinito. Demuestre que existe un entero $n \geq 2$ que divide a todos los elementos de A.*

Referencias

[1] Art of Problem Solving, *No two of which have a common divisor greater than 1*, artofproblemsolving.com/community/c6h60800p366618.

[2] Art of Problem Solving, *Chicken McNugget Theorem*, artofproblemsolving.com/wiki/index.php?title=Chicken_McNugget_Theorem.

[3] M. Beck, *The "Coin Exchange Problem" of Frobenius*, math.sfsu.edu/beck/papers/frobeasy.slides.pdf.

[4] A. Bogomolny, *Three Glass Problem*, Interactive Mathematics Miscellany and Puzzles, cut-the-knot.org/water.shtml y cut-the-knot.org/water2.shtml.

[5] A. Bogomolny, *Hourglass Problem, solution*, Interactive Mathematics Miscellany and Puzzles, cut-the-knot.org/hg_solution.shtml.

[6] G. Pólya, *How to Solve It. A New Aspect of Mathematical Method*, Princeton University Press, 1988.

[7] N. Sato, *Number Theory*, artofproblemsolving.com/articles/files/SatoNT.pdf.