Aritmética entera

Matemáticas Avanzadas

Relaciones

Definición Una relación R en un conjunto A se denomina **reflexiva**

si para todo $x \in A$, $(x, x) \in$ R .

Se dice que R es reflexiva si cada elemento x de A está relacionado consigo mismo

EJEMPLO Para A = {1, 2, 3, 4}, una relación R $\subseteq A \times A$ será reflexiva si R $\supseteq$ {(1, 1), (2, 2), (3, 3), (4, 4)}. Por tanto, R_1={(1,1), (2,2), (3,3)} no es una relación reflexiva en A, mientras que R_2= {(1, 1), (2, 2), (3, 3), (4, 4)} si es reflexiva en A.

Relaciones

EJEMPLO Dado un conjunto finito A con $|A|$ =n, resulta que $|A \times A| = n^2$, de modo que hay 2^{n^2} relaciones en A. ¿Cuántas son reflexivas?.

Si $A = \{a_1, a_2, \ldots, a_n\}$, una relación R en A es reflexiva si $\{(a_i, a_i) | 1 \le i \le n\} \subseteq$ R . Al considerar los otros $n^2 - n$ pares ordenados de $A \times A$ (los de la forma (a_i, a_j), $1 \le i, j \le n$, $i \ne j$) conforme se construye una relación reflexiva R en A, se incluye o excluye cada uno de estos pares ordenados, y por la regla del producto, existen $2^{(n^2-n)}$ relaciones reflexivas en A.

Relaciones

Definición La relación R en un conjunto A se llama **simétrica** si $(x, y) \in$ R $\Rightarrow (y, x) \in$ R para $x, y \in A$.

EJEMPLO Con $A = \{1, 2, 3\}$, se tiene que:

a)R_1={(1,2),(2,1),(1,3),(3,1)} es simétrica, no reflexiva;

b)R_2={(1,1),(2,2),(3,3),(2,3)}es reflexiva, no simétrica;

c)R_3={(1,1),(2,2),(3,3)};R_4={(1,1),(2,2),(3,3),(2,3),(3,2)} son reflexivas y simétricas.

Relaciones

Para contar las relaciones simétricas en $A=\{a_1,a_2, \ldots ,a_n\}$, se escribe $A\times A$ como $A_1\cup A_2$, donde $A_1=\{(a_i,a_j)\mid 1\le i,j\le n, i\ne j\}$ y $A_2=\{(a_i,a_i)\mid 1\le i\le n\}$ de modo que cada par en $A\times A$ está exactamente en uno de los conjuntos A_1,A_2. Para A_2, $|A_2| = |A\times A| - |A_1| = n^2-n = n(n-1)$, un entero par. El conjunto A_2 contiene $(1/2)(n^2-n)$ subconjuntos de la forma $\{(a_i,a_j),(a_j,a_i)\}, 1\le i<j\le n$. Al establecer una relación simétrica R en A, para cada par ordenado de A_1, se dispone de la selección usual de exclusión o inclusión. Para los $(1/2)(n^2-n)$ subconjuntos de pares ordenados en A_2, se dispone de las mismas opciones. Por tanto, por la regla del producto, hay $2^n \cdot 2^{(1/2)(n^2-n)} = 2^{(1/2)(n^2+n)}$ relaciones simétricas en A. *Al contar las relaciones en A que son reflexivas y simétricas, se tiene sólo una opción para cada par ordenado en A_1. De modo que hay $2^{(1/2)(n^2-n)}$, relaciones en A que son reflexivas y simétricas.*

Relaciones

Definición Para un conjunto A, una relación R en A se llama **transitiva** si $(x, y), (y, z) \in R \Rightarrow (x, z) \in R$. (De modo que si x "está relacionado con" y e y "está relacionado con" z, se desea "relacionar" x con z, representando y el papel de "intermediario".)

EJEMPLO Defínase la relación R en el conjunto $\mathbf{Z}^+$ por a R b si a divide b, por ejemplo, para alguna $c \in \mathbf{Z}^+$, $b = ca$. Ahora si xRy e yRz, resulta xRz?. xR$y \Rightarrow y = sx$, $s\in\mathbf{Z}^+$; yR$z \Rightarrow z = ty$, $t\in\mathbf{Z}^+$. En consecuencia, $z = ty = t(sx) = (ts)x$, $ts\in\mathbf{Z}^+$, de modo que xRz y R es transitiva. Además R es reflexiva, pero no simétrica, puesto que 2R6, pero no 6R2.

EJEMPLO Si A $=\{1, 2, 3, 4\}$, entonces $R_1=\{(1,1), (2,3),(3,4),(2,4)\}$ es una relación transitiva en A, mientras que $R_2=\{(1,3),(3,2)\}$ no lo es, pues $(1,2) \notin R_2$.

Relaciones

Definición Dada una relación R en un conjunto A, R se denomina ***antisimétrica*** si a R b, b R $a \Rightarrow a = b$. (En este caso, la única manera de tener a a "relacionado con" b y a b "relacionado con" a es que a y b sean uno y el mismo elemento de A).

EJEMPLO Para un universo dado U defínase la relación R en P(U) por $(A, B) \in$R si $A \subseteq B$, para $A, B \subseteq$ U; de modo que R es la relación de *subconjunto* y si A R B y B R A, entonces se tiene $A \subseteq B$, $B \subseteq A$, lo que equivale a $A = B$. En consecuencia, esta relación es antisimétrica, además de reflexiva y transitiva, pero no simétrica.

Antes de cometer el error de pensar que "no simétrica" es sinónimo de "antisimétrica", téngase en cuenta lo siguiente.

EJEMPLO Para A ={1, 2, 3}, la relación R en A dada por R = {(1, 2), (2, 1), (2, 3)} no es simétrica porque (3, 2) $\notin$R, y tampoco es antisimétrica, pues (1,2), (2,1) $\in$R pero $1 \neq 2$. La relación R_1={(1, 1), (2, 2)}es simétrica y antisimétrica.

Relaciones

¿Cuántas relaciones son antisimétricas en A?
Al escribir A x A ={(1,1),(2,2),(3,3)} $\cup$ {(1,2),(2,1),(1,3), (3,1),(2,3),(3,2)}. Se hacen dos observaciones al intentar construir una relación R antisimétrica en A.

1. Cualquier elemento $(x, x) \in A$ x A puede incluirse o excluirse sin importar si R es o no antisimétrica.
2. Para un elemento de la forma (x, y), $x \neq y$, se deben tener en cuenta (x,y) e (y,x) y nótese que hay tres opciones para que R permanezca antisimétrica: a) situar (x, y) en R; b) situar (y, x) en R; c) no situar (x, y) ni (y, x) en R. (Qué sucede si se sitúan (x, y) e (y, x) en R?)

De esta manera por la regla del producto, el número de relaciones antisimétricas en A es $(2^3)(3^3) = (2^3)(3^{(3^2-3)/2})$. Si $|A| = n > 0$, entonces hay $\left(2^n\right)\left(3^{(n^2-n)/2}\right)$ relaciones antisimétricas en A.

Relaciones

Definición La relación R en un conjunto A se denomina relación de o*rden parcial* si R es reflexiva, antisimétrica y transitiva.

EJEMPLO la relación de subconjunto es una relación de orden.

Definición Una *relación de equivalencia* R en un conjunto A es una relación reflexiva, simétrica y transitiva.

EJEMPLO Sea n$\in \mathbf{Z}^+$. Para $x, y \in \mathbf{Z}$, se define la *relación* R *de módulo n* por medio de x R y si y sólo si, $x - y$ es un múltiplo de n. Con $n = 7$, se halla que 9 R 2, -3 R 11, (14,0) $\in$ R pero no 3 R 7.

Para cualquier conjunto A, A x A es una relación de equivalencia en A, y si A = $\{a_1, a_2, \ldots, a_n\}$, la relación de equivalencia más pequeña en A es R = $\{(a_i, a_i) \mid 1 \le i \le n\}$

Si R es una relación en un conjunto A, entonces R es una relación de equivalencia y un orden parcial en A si y sólo si es la relación de igualdad en A.

Relaciones de Orden

Sea A un conjunto y R una relación en A. El par (A, R) se llama *conjunto parcialmente ordenado* si la relación R en A es un orden parcial, o una relación de ordenamiento parcial. Si a A se le denomina conjunto parcialmente ordenado, se sobre entiende que hay un orden parcial R en A que convierte a A en este conjunto parcialmente ordenado.

EJEMPLO Sea A el conjunto de cursos ofrecidos en una universidad. Defínase la relación R en A mediante x R y si x e y son el mismo curso o si x es un requisito previo para y. Entonces, R transforma a A en un conjunto parcialmente ordenado.

EJEMPLO Defínase R en A = {1, 2, 3, 4} por x R y, si , es decir, x divide a y. Entonces, R ={(1, 1), (2, 2), (3, 3), (4, 4), (1, 2), (1, 3), (1, 4), (2, 4)} es un orden parcial y (A, R) es un conjunto parcialmente ordenado.

Relaciones de Orden

EJEMPLO Para construir una casa hay ciertos trabajos, como excavar los cimientos, que deben realizarse antes de poder comenzar otras fases de la construcción . Si A es un conjunto de tareas que deben realizarse para construir una casa o completar un proceso especial de fabricación, se puede definir una relación R en A por x R y si x e y denotan la misma tarea o si la tarea x debe realizarse antes de comenzar la y. De esta manera se asigna un orden a los elementos de A, convirtiéndolo en un conjunto parcialmente ordenado.

EJEMPLO En el conjunto $A = \{1, 2, 3, 4, 5\}$, la relación R en A, definida por x R y si $x \leq y$, es un orden parcial, que transforma a A en un conjunto parcialmente ordenado que se puede denotar por $(A, \leq)$. Si $B = \{1, 2, 4\} \subset A$, el conjunto $=\{(1, 1), (2, 2), (4, 4), (1, 2), (1, 4), (2, 4)\}$ es un orden parcial en B.

Relaciones de Orden

En general si R es un orden parcial en A, entonces para cualquier subconjunto B de A, $(B \times B) \cap$ R convierte a B en un conjunto parcialmente ordenado, donde el orden parcial de B se induce de R.

Definición Si (A, R) es un conjunto parcialmente ordenado, se dice que A está *totalmente ordenado* si para toda $x, y \in A$ se cumple x R y o y R x. En este caso R se denomina *orden total*.

EJEMPLO En el conjunto **N,** la relación R definida por x R y si $x \leq y$ es un orden total. La relación de subconjunto aplicada a $A = P(U)$, $U = \{1, 2, 3\}$ es un orden parcial, pero no total: $\{1, 2\}, \{1, 3\} \in A$, pero ni $\{1, 2\} \subseteq \{1, 3\}$ ni $\{1, 3\} \subseteq \{1, 2\}$.

Relaciones de Orden

Definición Si (A, R) es un conjunto parcialmente ordenado;

- Un elemento $a \in A$ se llama *máximo* de A si $x \leq a$ para toda $x \in A$.
- Un elemento $a \in A$ se denomina *mínimo* de A si $a \leq x$ para toda $x \in A$.

Definición Si (A, R) es un conjunto parcialmente ordenado;

- Un elemento $x \in A$ se denomina mínimo si x R a, para todo $a \in A$.
- Un elemento $y \in A$ se denomina máximo si a R y para todo $a \in A$.

EJEMPLO Con la relación R "es menor o igual que" en el conjunto **Z**, (**Z**, ≤) es un conjunto parcialmente ordenado sin elemento máximo ni mínimo. No obstante, el conjunto parcialmente ordenado (N, ≤) tiene elemento mínimo 0, pero no máximo.

EJEMPLO Sean U = {1, 2, 3} y R la relación de subconjunto.

a) Con A = P(U), $(A, \subseteq)$ tiene a ∅ como elemento mínimo y a U como máximo.

b) Para B = la colección de subconjuntos no vacíos de U, $(B, \subseteq)$ tiene a U como elemento máximo. No existe elemento mínimo.

Relaciones de Orden

Teorema Si el conjunto parcialmente ordenado (A, R) tiene algún elemento máximo (mínimo), ese elemento es único.

Demostración Supóngase que $x, y \in A$ y que ambos son elementos máximos. Como x es un elemento máximo, y R x. Así mismo, x R y, pues y es un elemento máximo. Como R es antisimétrico, $x = y$.

Definición Sea (A, R) un conjunto parcialmente ordenado con $B \subseteq A$.

- Un elemento $x \in A$ se llama *cota inferior* de B si x R b para toda $b \in B$.
- Si $y \in A$ y b R y, para toda $b \in B$, y se denomina *cota superior* de B.

Inducción

Un conjunto es **inductivo** si, para cada $a \in A$, entonces $a + 1$ también pertenece a A. El conjunto de los números naturales que incluye al 0 es un conjunto inductivo.

Los siguientes pasos se siguen para hacer demostraciones inductivas.

1. Probar que la proposición se cumple para 0.
2. Suponer que la proposición se cumple para n y probar que esto implica que se cumpla para $n + 1$.
3. Deducir que la proposición se cumple para todos los elementos de N.

Ejemplo 1

Sea $H_n = 0$ si $n = 0$ y $H_{n+1} = 1 + 2H_n$. Demostrar $H_n = 2^n - 1$

BI: $H_0 = 2^0 - 1 = 1 - 1 = 0$

HI: se cumple $H_n = 2^n - 1$

$H_{n+1} = 1 + 2H_n = 1 + 2(2^n - 1) = 1 + 2^{n+1} - 2 = 2^{n+1} - 1$

Conclusión:

$\forall n$: $H_n = 2^n - 1$

Ejemplo 2

Para todo n: $2(n + 2) \leq (n + 2)^2$.

BI: $2(0 + 2) \leq (0 + 2)^2$ o $4 = 4$

HI: $2(n + 2) \leq (n + 2)^2$.

$2(n + 1 + 2) \leq (n +1+ 2)^2$.

$2(n + 3) \leq (n + 3)^2$.

$2(n + 2) + 2 \leq (n + 3)^2$. $= n^2 + 6n + 9 = n^2 + 4n +4+2n+5$

$2(n + 2) + 2 \leq (n + 2)^2 + 2n+5$

Por la hipótesis inductiva eliminamos $2(n + 2) \leq (n + 2)^2$.

$2 \leq 2n+5$

Ya que esta se cumple para toda n, se cumple la hipótesis inductiva.

Ejemplo 3

Para todo $n^3 + 2n$ es divisible por 3.

BI: $0^3 + 2 \cdot 0 = 0 + 0 = 0$ es divisible por 3.

HI: $n^3 + 2n = 3k$

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

$= n^3+2n+3n^2+3n+3$

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

Este número es divisible por 3, por lo tanto se cumple la hipótesis inductiva.

Modificación de la base inductiva

La base inductiva no debe ser siempre con $n = 0$.

Podemos comenzar en cualquier n_0, tomando $P(n_0)$ como base de inducción.

$P(n_0)$

$\underline{\forall n(P(n \geq n_0) \rightarrow P(n+1))}$

$\forall n\, P(n \geq n_0)$

Ejemplo 4

Para todo $2^n < n!$ para $n \geq 4$.

BI: $2^4 < 4!$ o $16 < 24$

HI: $2^n < n!$

$2 \cdot 2^n = 2^{n+1} < 2 \cdot n! < (n+1) \cdot n! = (n+1)!$

Ejemplo 5

Para todo $1+2^3+3^3+4^3+\ldots+n^3 = (n(n+1)/2)^2$.

BI: $1 = (1(1+1)/2)^2 = 1^2 = 1$

HI: $1+2^3+3^3+4^3+\ldots+n^3 = (n(n+1)/2)^2$

$1+2^3+3^3+4^3+\ldots+n^3 + (n+1)^3 = (n(n+1)/2)^2 + (n+1)^3$

$= (n^2(n+1)^2/4) + (n+1)^3$

$= (n+1)^2(n^2 + 4(n+1))/4 = (n+1)^2 (n+2)^2/4 =$

$= ((n+1)(n+2)/2)^2$

Ejemplo 6

Para todo $3^{2n+1}+2^{n+2}$es divisible por 7.

BI: $3^1+2^1 = 7$

HI: $3^{2n+1}+2^{n+2} = 7m$

$3^{2(n+1)+1}+2^{(n+1+2)} = 3^{2n+3}+2^{n+3} = 3^2 3^{2n+1} + 2^1 2^{n+2} =$

$= 9x3^{2n+1} + 2x2^{n+2}$

$= 7x3^{2n+1} + 2x3^{2n+1} + 2x2^{n+2}$

$= 7x3^{2n+1} + 2(3^{2n+1} + 2^{n+2})$

$= 7x\ 3^{2n+1} + 2\ (7m)$

$= 7(3^{2n+1} + 2)$

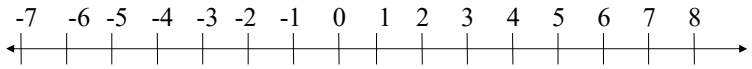
Conclusión: $3^{2n+1}+2^{n+2}$es divisible por 7.

El conjunto de los enteros

El conjunto de los enteros esta constituido por los números enteros negativos, los enteros positivos y el cero. Generalmente se representa mediante la letra **Z**.

Z = {…, -3, -2, -1, 0, 1, 2, 3, …}

La recta numérica sirve para representar gráficamente conjuntos de números.



El anillo de los enteros

Los enteros forman lo que se conoce como un *anillo*.

Un anillo es un conjunto dotado de las propiedades que se verán más adelante.

En los enteros se definen dos operaciones la suma y la multiplicación.

Las propiedades de estas operaciones se listan a continuación.

Valor absoluto de un entero

Definimos el valor absoluto como sigue.

El valor absoluto de a se denota por $|a| = a$ si $a > 0$ y $|a| = -a$ si $a < 0$. Símbolicamente: $a > 0 \rightarrow |a| = a \wedge a < 0 \rightarrow |a| = -a$

Es decir, el valor absoluto de un entero es el número que resulta al eliminar el signo que lo precede.

$|4| = 4$

$|-33| = 33$

$|+45| = 45$

Propiedades

Axioma 1. Propiedad conmutativa de la suma. Si a y $b \in \mathbf{Z}$, entonces

$$a + b = b + a$$

Axioma 2. Propiedad asociativa de la suma. Si a, b y $c \in \mathbf{Z}$, entonces

$$(a + b) + c = a + (b + c)$$

Axioma 3. Elemento neutro de la suma. Si $a \in \mathbf{Z}$, entonces

$$a + 0 = 0 + a = a$$

Axioma 4. Inverso aditivo. Si $a \in \mathbf{Z}$, entonces

$$a + (-a) = (-a) + a = 0$$

Propiedades

Axioma 5. Propiedad conmutativa de la multiplicación. Si a y $b \in \mathbf{Z}$, entonces

$$ab = ba$$

Axioma 6. Propiedad asociativa de la multiplicación. Si a, b y $c \in \mathbf{Z}$, entonces

$$(ab)c = a(bc)$$

Axioma 7. Elemento neutro de la multiplicación. Si $a \in \mathbf{Z}$, entonces

$$a1 = 1\ a = a$$

Axioma 8. Propiedad distributiva de la multiplicación y la suma. Si a, b y $c \in \mathbf{Z}$, entonces

$$a(b + c) = ac + ab$$
$$(a + b)c = ac + bc$$

Propiedades del anillo de los enteros

Ley de cancelación
Se cumple la siguiente proposición: si a, b y $c \in \mathbf{Z}$ **y** $a + b = a + c$, entonces $b = c$.

Demostración. Suponemos $a + b = a + c$. Sumamos a cada miembro de la igualdad el inverso aditivo de a.

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

Por la propiedad asociativa.

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

Por el axioma de elemento inverso de la suma.

$$0 + b = 0 + c$$

Dado que 0 es el elemento neutro de la suma.

$$b = c \qquad \square$$

Propiedades del anillo de los enteros

Si a y $b \in \mathbf{Z}$ **y** $a + b = a$, entonces $b = 0$.

Para todo entero $a0 = 0a = 0$.

Se cumple que $-(-a) = a$.

Se cumple la siguiente *regla de signos* para el producto de dos enteros.

$$(-a)b = -ab$$
$$(-a)\,(-b) = ab$$

Diferencia de enteros

Definimos la diferencia de dos enteros de la siguiente manera.

Si a y $b \in \mathbf{Z}$, $a - b$ es la diferencia de a y b y se calcula como.

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

Se cumple la siguiente ley distributiva.

Si a y $b \in \mathbf{Z}$, $a(b - c) = ab - ac$

Ley de cancelación para la multiplicación

Si a, b y $c \in \mathbf{Z}$, y $a \neq 0$, entonces $ab = ac$ implica $b = c$.

Demostración. Ya $ab = ac$ que tenemos que $ab - ac = 0$, de donde $a(b - c) = 0$ y como $a \neq 0$, entonces $b - c = 0$, o $b = c$. □

Divisibilidad

Un entero a es *divisible* por un entero b si existe un entero c tal que:

$$a = b \cdot c$$

Se dice que a es un *múltiplo* de b.

Un número que tiene solo dos divisores, 1 y el mismo, se llaman número *primo*.

Los números que no son primos se les llama *compuestos*.

Se suele expresar de la forma $a|b$, que se lee a divide a b, o a es divisor de b.

Propiedades de la divisibilidad

Sean a, b, y $c \in Z$. Tenemos las siguientes propiedades básicas:
$a|a$ (Propiedad Reflexiva).
Si $a|b$ y $b|c$, entonces $a|c$ (Propiedad Transitiva).
Si $a|b$, entonces $|a| \leq |b|$.
Si $a|b$ y $b|a$, entonces $|a| = |b|$.
Si $a|b$ y $a \neq 0$, entonces $b/a|b$.
Si $a|b$ y $a|c$ entonces $a|(b+c)$.
Si $a|b$ y c es un entero, entonces $a|bc$.
Si $c|a$ y $c|b$, entonces $c|ar+bs$, *para r y s arbitrarios*.

Ejemplos:

5|5 es cierto	5| 30 y 30|150, 5|150
5| 20, 20/5=4|20	3|18 y 3|21, 3|39
7|49, entonces 7|49*2=98	6|12 y 6|18, 6|(3*12+2*18)=72

Combinación lineal

Una *combinación lineal* de dos enteros a, b es una expresión de la forma

$$ar + bs$$

Donde r y s son enteros.

Un entero c divide a los enteros a y b si y solo si c divide a cualquier combinación lineal de a y b.

Ejemplo: sea $a = 12$, $b = 18$ y $c = 6$, entonces

$6 = 12r + 18s$ donde r = –1 y s = 1

Una condición necesaria para que un número g sea combinación lineal de a y b es que g sea divisible entre todo divisor común de a y b.

Ejemplos

Probar que 52 no es combinación lineal de 20 y 15.

Divisores de 20 y 15 es 5

$5 \nmid 52$ por lo tanto no existe una combinación lineal

Encuentre una combinación lineal de 12 en términos de 98, 102.

102 – 98 = 4, 12 = 3*4, entonces 3*102 – 3*98 = 12

Pruebe que si c = 30n+6, entonces *c* no es combinación lineal de 1020 y 210.

Divisores de 1020 y 210 son: 2, 3, 5, 10, 15 y 30.

Divisores de 30n+6 son: 2, 3, 6, etc. No tiene como divisor a 5, por lo tanto no es posible obtener una combinación lineal.

Algoritmo de la división .

Sean $a \in Z$ y $b \in N$. Entonces existen $q, r \in Z$ con $0 \leq r < |b|$ tales que $a = bq + r$. Además, q y r son únicos.

Demostración. Sea $a>0$ y $b>0$. Considere los enteros de la forma $a – bs$. Sea $r = a – bq >= 0$ el menor de estos enteros. De aquí

$$a = bq + r$$

Si $r \geq b$, ya que $r = a – bq$, obtenemos $r – b = a – bq – b = a – b(q + 1)$, puesto que $r \geq b$, resulta que

$$a – b(q + 1) >= 0$$

Contradice el echo que r es el menor entero no negativo de la forma $a – bs$, ya que $a – b(q+1) = r – b < r = a – bq$. Por lo cual queda demostrado que $r <b$.

Si $a > 0$ y $a < b$, $a = b \cdot 0 + a$ y $a< b$, lo cual demuestra el teorema en este caso.

Supongamos que existen q' y r' además de q y r, tales que

$$a = bq + r \qquad r < b$$

$$a = bq' + r' \qquad r' < b$$

De las anteriores obtenemos

$$b(q - q') = r' - r$$

De donde

$$|b||q - q'| = |r' - r|$$

Pero $|r' - r| < b$, lo anterior implica que

$$|b||q - q'| = 0 \text{ y } |r' - r| = 0$$

Como $|b| \neq 0$, se tiene que

$$q = q' \text{ y } r = r'$$

Omitiremos los casos de a o b o ambos negativos.

37

Sea $a = 436$ y $b = 17$

$436 = 17 \cdot 25 + 11$ por lo que $q = 25$ y $r = 11$

Sea $a = -436$ y $b = -17$

$-436 = -17 \cdot 25 - 11$

Pero -11 no sirve como residuo ya que es negativo, por tanto

$-436 = -17 \cdot 26 + 6$

$q = 26$ y $r = 6$ y $0 \leq r = 6 < |-17| = 17$

Sea $a = -436$ y $b = 17$

$-436 = 17 \cdot (-25) - 11 = 17 \cdot (-25) + 17(-1) + 17 - 11 =$

$-436 = 17 \cdot (-26) + 6$

$q = -26$ y $r = 6$ y $0 \leq r = 6 < |-17| = 17$

Sea $a = 436$ y $b = -17$

$436 = (-17) \cdot (-25) + 11$

$q = -25$ y $r = 11$

38

Máximo común divisor

Dados dos enteros a y b distintos de 0, decimos que el entero $d>1$ es un *máximo común divisor* (denotado por (a, b) o mcd(a, b)), de a y b si $d|a$, $d|b$ y para cualquier otro $c \in Z$ tal que $c|a$ y $c|b$, entonces $c|d$.

Algunas propiedades del máximo común divisor

mcd(a, b) = mcd($|a|$, $|b|$)
mcd (ka, kb) = $|k|$ mcd(a, b)
Si $a|b.c$ y mcd(a, b) =1, entonces $a|c$
mcd(a, b) = $d \Leftrightarrow d|a$, $d|b$ y mcd(a/d, b/d)=1

Propiedades

Si a y b son enteros positivos y $d = as + bt$ es su combinación lineal positiva mínima, entonces todo divisor de d es divisor también de a y b.

Demostración. Tenemos que $a = dq + r$ con $0 \le r < |d|$, sustituyendo $d = as + bt$, se tiene

$$a = (as + bt)q + r$$

O $\quad r = a(1 - sq) - btq \quad$ *r es combinación lineal de a y b*

Pero como $0 \le r < d$ y d es la combinación positiva mínima de a y b, resulta que $r = 0$, es decir, $a = dq$ y por tanto $d|a$

De igual forma se demuestra que $d|b$.

Corolario: el mcd(a, b) es la combinación mínima positiva de a y b.

Coprimos

Dos números a y b son *primos entre si* (co*primos*) si su máximo común divisor es 1. Es decir, a y b son primos entre si, si y solo si,

$$1 = as + bt$$

Proposición: Si $a|bc$ y mcd(a, b) =1, entonces $a|c$.

Demostración.

$1 = as + bt$, entonces $c = asc + btc$

Ahora bien, $a|a$ y $a|bc$, a divide a la combinación lineal $a(sc) + (bt)t = c$, por lo tanto $a|c$.

41

Primos Relativos

Teorema. $\forall\ a,b,p \in Z$, si $mcd(a,p) = 1$ y $mcd(b,p) = 1 \Rightarrow mcd(ab,p) = 1$.

Prueba. Se tienen las siguientes ecuaciones: $ax + py = 1$ y $bx' + py' = 1$.

Al multiplicar y ordenar las ecuaciones se obtiene: $ab(xx') + p(axy' + bx'y + pyy') = 1$. Por lo que 1 es un elemento positivo de la combinación lineal de ab y p.

Se puede decir que los enteros $n_1, n_2, \ldots, n_k$ son parejas de primos relativos si, $i \neq j$, $mcd(n_i, n_j) = 1$.

Teorema de Bézout. Los números enteros a y b son primos relativos cuando existen dos enteros x y y tales que $ax + by = 1$. De forma equivalente, b tiene un inverso para el producto módulo a, existe un número entero y tal que $by \equiv 1 \pmod{a}$.

42

El algoritmo de Euclides

Para calcular el **mcd** de dos enteros a y b (ambos ≥ 0, suponemos $a \geq b$) se definen q_i y r_i recursivamente mediante las ecuaciones:

$a = bq_1 + r_1 \quad (0 \leq r_1 < b)$
$b = r_1 q_2 + r_2 \quad (0 \leq r_2 < r_1)$
$r_1 = r_2 q_3 + r_3 \quad (0 \leq r_3 < r_2)$
....
$r_{k-3} = r_{k-2} q_{k-1} + r_{k-1} \quad (0 \leq r_{k-1} < r_{k-2})$
$r_{k-2} = r_{k-1} q_k \quad (r_k = 0)$

El máximo común divisor es el último residuo diferente de 0.

Ejemplo de algoritmo de Euclides

$a = 246$, $b = 118$

$a/b = 246/118 = 2 + 10/118$, $q_1 = 2$, $r_1 = 10$

$b/r_1 = 118/10 = 11 + 8/10$, $q_2 = 11$, $r_2 = 8$

$r_1/r_2 = 10/8 = 1 + 2/8$, $q_3 = 1$, $r_3 = 2$

$r_2/r_3 = 8/2 = 4$, $q_4 = 2$, $r_4 = 0$,

mcd(246, 118) = 2

Mcd como combinación lineal

El mcd de a y b se puede expresar como la combinación positiva mínima lineal de a y b.

Ejemplo:

$a = 348$ y $b = 228$

$348 = 1x228 + 120$

$228 = 1x120 + 108$

$120 = 1x108 + 12$

$108 = 9x12$

mcd = 12

$12 = 120 - 108$

$= 120 - (228 - 120)$

$= 2x120 - 228$

$= 2x(348 - 228) - 228$

$= 2x348 - 3x228$

$\text{mcd}(a, b) = 2a - 3b$

$= 696 - 684 = 12$

Ejemplos

Calcule (84, 30): Utilizando el algoritmo de Euclides tenemos:

$84 = 2(30) + 24$

$30 = 1(24) + 6$

$24 = 4(6) + 0$

Entonces (84, 30) = 6. Además, de las ecuaciones anteriores obtenemos

$6 = 30 - 24 = 30 - (-2(30) + 84) = 3(30) + (-1)84$

y hemos escrito a 6 como la mínima combinación lineal positiva entre 84 y 30.

Calcule (–35,–48): Utilizando el algoritmo de Euclides tenemos:

$-35 = 1(-48) + 13$
$-48 = -4(13) + 4$
$13 = 3(4) + 1$
$4 = 4(1) + 0$

Entonces (–35,–48) = 1. Además, de las ecuaciones anteriores obtenemos

$1 = 13 - 3(4) = 13 - 3(-48+4(13)) = -3(-48) - 11(13)$
$= -3(-48) - 11(-35 - 1(-48))$
$= 8(-48) - 11(-35)$

y hemos escrito a como la mínima combinación lineal positiva entre –35y –48.

Algoritmo de Euclides

- Si se factoriza dos números enteros *a* y *b*:

$$\left.\begin{aligned} a &= p_1^{e_1} p_2^{e_2} \cdots p_n^{e_n} \\ b &= p_1^{f_1} p_2^{f_2} \cdots p_n^{f_n} \end{aligned}\right\} mcd(a,b) = p_1^{\min(e_1,f_1)} p_2^{\min(e_2,f_2)} \cdots p_n^{\min(e_n,f_n)}$$

- **Teorema de recursión del MCD.** Para cualquier par de números enteros positivos *a* y *b* (ambos no pueden ser 0, sólo alguno de ellos) $mcd(a,b) = mcd(b, a \bmod b)$.
  - Ejemplo: $mcd(30,21) = mcd(21,9) = mcd(9,3) = mcd(3,0) = 3$.
- El método funciona también si *a* y *b* son negativos. Basta trabajar con los valores absolutos de estos números.

Algoritmo de Euclides

- La aplicación recursiva del **lema de Euclides** (o teorema de recursión del MCD) proporciona un método para calcular el MCD, y se llama **algoritmo de Euclides**.
- **Algoritmo de Euclides.** Dados dos enteros a y b tales que $a \geq b > 0$, el algoritmo va calculando valores a_i, b_i, c_i y r_i, asociados a valores crecientes de un índice $i \geq 0$.
- El algoritmo funciona de la siguiente manera:
  - Se comienza calculando $a_0 = a$ y $b_0 = b$.
  - Calculados a_i y b_i, para un cierto subíndice i, puede ocurrir:
    - Si $b_i = 0$, el cálculo termina. Se toma $d = a_i$ y se puede asegurar que $d = mcd(a,b)$.
    - Si $b_i > 0$, se calcula $c_i = a_i \ div \ b_i$ y $r_i = a_i \ mod \ b_i$ y se continua con $a_{i+1} = b_i$, $b_{i+1} = r_i$.
- En la práctica, los cálculos necesarios para ejecutar el algoritmo se pueden organizar en una tabla con varias columnas, en las cuales se van registrando los valores de i, a_i, b_i, c_i y r_i.

Algoritmo de Euclides

Algoritmo de Euclides tradicional implementado de manera recurrente

Función $\mathrm{mcd}\,(a, b)$:

Si $b = 0$ **entonces:**

El resultado es a

En otro caso:

El resultado es $\mathrm{mcd}\,(b, a \text{ mód } b)$

Algoritmo de Euclides tradicional implementado de manera iterativa

Función $\mathrm{mcd}\,(a, b)$:

Mientras $b \neq 0$ **haga lo siguiente:**

$(a, b) \leftarrow (b, a \text{ mód } b)$

El resultado es a

Algoritmo de Euclides

Teorema de Lamé e Identidad de Bézout

- **Teorema de Lamé.** $\forall k \in Z$ y $k \geq 1$, si $a > b \geq 1$ y $b < F_{k+1} \Rightarrow$ la función euclidiana $mcd(a,b)$ realiza k recursiva llamadas.
- El **Torema de Bézout** afirma que el MCD de dos números enteros se puede expresar como combinación lineal de dichos números con coeficientes enteros; es decir, dados $\forall a,b \in Z$ tales que $d = mcd(a,b)$, se pueden encontrar dos coeficientes enteros $\exists m,n \in Z$ de manera que se cumpla $d = am + bn$, o equitativamente $d = ma + nb$.
- Dados enteros a y b y su máximo común divisor d = mcd(a, b), se denomina identidad de Bézout a la expresión de la forma ax + by = d x, y ∈ Z
- Estos teoremas generan el algoritmo de Euclides extendido.

Algoritmo de Euclides Extendido

- El algoritmo de Euclides extendido permite, además de encontrar el MCD de dos números enteros a y b, expresarlo como una combinación lineal, es decir, encontrar números enteros x y y tales que $d = mcd(a,b) = ax + by$, $\forall x,y \in Z$.
- Este algoritmo retorna una tripleta (d,x,y).
  - Ejemplo: $Euclides(99,78) = (3,-11,14) \Rightarrow mcd(99,78) = 3 = 99 \bullet -11 + 78 \bullet 14$.
- $\forall a,b \in Z+$, si $a > b > 0 \Rightarrow$ la función realiza $O(\log b)$ llamadas recursivas.
- En el cálculo práctico de m y n se parte de la tabla utilizada para el cálculo de $d = mcd(a,b)$ por el algoritmo de Euclides.
- Suponga que k sea el valor del índice i con el que ha terminado el cálculo de $d = mcd(a,b)$, se van calculando valores m_i y n_i asociados a valores decrecientes de un índice i, comenzando por $i = k$, del siguiente modo:
  - Se comienza calculando $m_k = 1$ y $n_k = 0$.
  - Luego, los valores i comprendidos entre $k - 1$ y 0 se recorren en orden decreciente y para cada uno de ellos se calcula $m_i = n_{i+1}$ y $n_i = m_{i+1} - n_{i+1} \bullet c_i$.
  - Se toman . $m = m_0$ y $n = n_0$.
- La tabla utilizada en el algoritmo de Euclides se le agrega dos columnas, en las que se van registrando los valores m_i y n_i.

Algoritmo de Euclides Extendido

Algoritmo de Euclides extendido implementado de manera recurrente

Función $Euclides\ (a, b)$:

Si $b = 0$ **entonces:**

El resultado es $(a, 1, 0)$

En otro caso:

$(d, s, t) \leftarrow Euclides\ (b, a \bmod b)$

El resultado es $(d, t, s - (a \div b)\ t)$

Algoritmo de Euclides extendido implementado de manera iterativa

Función $Euclides\ (a, b)$:

$(s, t, s', t') \leftarrow (1, 0, 0, 1)$

Mientras $b \neq 0$ **haga lo siguiente:**

Divida a entre b para obtener un cociente q y un residuo r

$(a, s, t, b, s', t') \leftarrow (b, s', t', r, s - s'\ q, t - t'\ q)$

El resultado es (a, s, t)

Algoritmo de Euclides Extendido

Algoritmo de Euclides extendido implementado de manera iterativa con matrices

Función $Euclides\ (a, b)$:

$$Q \leftarrow \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

Mientras $b \neq 0$ **haga lo siguiente:**

Divida a entre b para obtener un cociente q y un residuo r

$$Q \leftarrow \begin{pmatrix} 0 & 1 \\ 1 & -q \end{pmatrix} \times Q$$

$(a, b) \leftarrow (b, r)$

El resultado es $(a, Q_{1\ 1}, Q_{1\ 2})$

Algoritmo de Euclides Extendido

i	Residuos r_i	Cocientes c_i	m_i	n_i	Combinación Lineal $d = mcd(a,b) = ax + by$
0	a	*	1	0	a
1	b	*	0	1	b
2	r_{i-2} mod r_{i-1}	r_{i-2} / r_{i-1}	$m_{i-2} - c_i * m_{i-1}$	$n_{i-2} - c_i * n_{i-1}$	r_{i-2} mod r_{i-1} = $a*m_i + b*n_i$

Algoritmo de Euclides Extendido

i	Residuos r_i	Cocientes c_i	m_i	n_i	Combinación Lineal $d = mcd(a,b) = ax + by$
0	662	*	1	0	662 = 662*1 + 414*0
1	414	*	0	1	414 = 662*0 + 414*1
2	248	1	1	-1	248 = 662*1 + 414*-1
3	166	1	-1	2	166 = 662*-1 + 414*2
4	82	1	2	-3	82 = 662*2 + 414*-3
5	**2**	2	**-5**	**8**	2 = 662*-5 + 414*8
6	0	41	207	-331	0 = 662*207 + 414*-331

Algoritmo de Euclides Extendido

i	Residuos r_i	Cocientes c_i	m_i	n_i	Combinación Lineal $d = mcd(a,b) = ax + by$
0	252	*	1	0	252 = 252*1 + 198*0
1	198	*	0	1	198 = 252*0 + 198*1
2	54	1	1	-1	54 = 252*1 + 198*-1
3	36	3	-3	4	36 = 252*-3 + 198*4
4	**18**	1	**4**	**-5**	18 = 252*4 + 198*-5
5	0	2	-11	14	0 = 252*-11 + 198*14

Ecuaciones diofánticas

Se llama ecuación diofántica a cualquier ecuación algebraica con coeficientes enteros, de la que nos interesan exclusivamente las soluciones que tenga dentro del conjunto de los números enteros.

Transeúnte, ésta es la tumba de Diofanto: es él quien con esta sorprendente distribución te dice el número de años que vivió. Su niñez ocupó la sexta parte de su vida; después, durante la doceava parte su mejilla se cubrió con el primer bozo. Pasó aún una séptima parte de su vida antes de tomar esposa y, cinco años después, tuvo un precioso niño que, una vez alcanzada la mitad de la edad de su padre, pereció de una muerte desgraciada. Su padre tuvo que sobrevivirle, llorándole, durante cuatro años. De todo esto se deduce su edad.

$$\frac{x}{6}+\frac{x}{12}+\frac{x}{7}+5+\frac{x}{2}+4=x$$

Ecuaciones diofánticas

Una ecuación lineal con dos incógnitas es una expresión de la forma $ax + by = c$ con $a, b,c \in \mathbb{Z}.\in \mathbb{Z}$.
Teniendo en cuenta la identidad de Bézout: Sean a, b dos números enteros y d=mcd (a, b). Entonces existen dos números enteros x e y tales que ax+by=d

El algoritmo de Euclides para el cálculo del máximo común divisor, nos sirve para encontrar los valores x e y que establece la identidad de Bézout, el mcd(a, b)=r_{n+1} sustituyendo el valor de los restos se obtiene la combinación lineal.

Teorema: La ecuación diofántica lineal $ax+by=c$ tiene solución si y sólo si
$d = mcd\ (a, b) \mid c$

59

Ecuaciones diofánticas

Teorema: La ecuación diofántica lineal $ax+by=c$ tiene solución si y sólo si
$d = mcd\ (a, b) \mid c$

Demostración:

=>) Supongamos que la ecuación $ax+by=c$ tiene solución. Como $d=mcd(a, b)$, existen a', b' números enteros tales que $a=a'd$, $b=b'd$. Sustituyendo en la ecuación: $a'dx+b'dy=c$ => $d(a'x+b'y)=c$ y por tanto $d \mid c$

<=) Supongamos $d \mid c$. Entonces existe un entero c' tal que $c= c'd$.
Pero la identidad de Bézout garantiza la existencia de dos enteros x_0 e y_0 tales que $ax_0+by_0=d$. Multiplicando esta ecuación por c', se tiene $c'ax_0+c'by_0= c'd=c$. Por lo que $x= c'x_0$, $y=c'y_0$ es una solución

60

Ecuaciones diofánticas

La demostración del teorema anterior, nos da la clave para buscar una solución particular de una ecuación diofántica o por el contrario nos dirá si no tiene solución.

Ejemplo: La ecuación *5x+3y=16* tiene solución ya que *mcd(5, 3)=1|16*. Además como por el algoritmo de Euclides *5·(-1)+3·2=1*, multiplicando la ecuación por 16 tenemos: *5·(-16)+3·(32)=16*, luego una solución de la misma es x_0=*-16,* y_0=*32*.

Ejemplo: La ecuación *2x+10y=1* no tiene solución porque mcd (2, 10)=2 y no divide a 1.

Teorema: Si *d=mcd(a, b), d | c y* x_0 *e* y_0 son una solución de la ecuación diofántica lineal *ax+by=c* , entonces las soluciones vienen dadas por:

$$X = x_0 + \frac{b}{d} t$$

$$Y = y_0 - \frac{a}{d} t$$

donde t es un número entero.

61

Teorema fundamental de la aritmética

Teorema de factorización única (teorema fundamental de la aritmética). Todo número entero distinto de 1 se puede expresar de la forma

$$a = p_1 p_2 p_3 \ldots p_h \qquad (1)$$

donde $p_1 p_2 p_3 \ldots p_h$ son números primos positivos.

62

Demostración

Demostración. Suponga que existe un conjunto M de números que no pueden expresarse como en (1). Demostraremos que M = ∅.

Suponga que a es el menor elemento de M, si a es primo, $a = p_1$, lo cual contradice la suposición de M.

Ahora suponga que a es compuesto y entonces $a = bc$, con $1 < b < a$ y $1 < c < a$. Como a es el mínimo elemento de M, b y c se pueden expresar de la forma (1).

$b = p_1 p_2 p_3 \ldots p_n$ y $c = q_1 q_2 q_3 \ldots q_r$

Entonces $a = p_1 p_2 p_3 \ldots p_n q_1 q_2 q_3 \ldots q_r$

Pero esta es una expresión de la forma (1), lo que contradice la existencia de M.

63

Demostración

Ahora demostraremos que la factorización es única. Suponga que existen dos factorizaciones para a

$$a = p_1 p_2 p_3 \ldots p_n$$

$$a = q_1 q_2 q_3 \ldots q_r$$

Igualando

$$p_1 p_2 p_3 \ldots p_n = q_1 q_2 q_3 \ldots q_r$$

como p_1 divide al producto de la izquierda, debe dividir al producto de la derecha, digamos que divide a q_1. Nos queda

$$p_2 p_3 \ldots p_n = q_2 q_3 \ldots q_r$$

Análogamente, se puede decir para $p_2 = q_2$, $p_3 = q_3$, hasta llegar a tener $1 = q_h q_{h+1} \ldots q_r$ si $h < t$, lo cual es imposible, similarmente si $t < h$, de ahi que $h = t$, con lo que queda demostrado.

64

Mínimo común múltiplo

El *Mínimo Común Múltiplo* (denotado $[a, b]$ o mcm(a, b)) de dos números a y b es el entero más pequeño que es divisible por ambos números a y b.

Ejemplo: $a = 6$ y $b = 10$

Los múltiplos de a son {6, 12, 18, 24, 30, 36, …}

Los múltiplos de b son {10, 20, 30, …}

La intersección de estos dos conjuntos es el conjunto {30, 60, 90, …} el más pequeño de estos valores es el mcm(6, 10) =30

65

Mcd * mcm

Proposición: Si a y b son enteros positivos, entonces el producto de a y b es igual al producto de su mcd y mcm. Es decir ab = mcd$(a,b)\cdot$mcm(a,b) = $(a, b)[a, b]$.

Demostración:

Sea m = mcm(a,b), $m|ab$ y sea d tal que $md = ab$.

Como m es múltiplo de a y b, $m = ar = bs$, entonces

$md = ard = bsd = ab$, por lo que $rd = b$ y $sd = a$ por tanto $\boldsymbol{d|a}$ **y** $\boldsymbol{d|b}$. (1)

Por otro lado d' un divisor de a y b, $d'|a$ $d'|b$. Sean a' y b' tales que $a = d'a'$ y $b = d'b'$

Sea m' un múltiplo común de a y b dado por $m' = a'b'd' = ab' = a'b$. m' es un múltiplo de m, es decir $m' = mt$.

$mtd' = m'd' = a'b'd'd' = ab = md$, entonces td' = d o $\boldsymbol{d'|d}$.(2)

Las condiciones (1) y (2) significan que d es divisor de a y b y que d es dividido por cualquier divisor de a y b, por lo tanto d es el mcd lo que implica que ab = mcd$(a,b)\cdot$mcm(a,b)

66

Mcd, mcm y factorización

Se puede demostrar que para dos números a y b con factorizaciones en primos dadas por

$$a = p_1^{m_1} p_2^{m_2} p_3^{m_3} \cdots p_n^{m_n}$$
$$b = p_1^{s_1} p_2^{s_2} p_3^{s_3} \cdots p_n^{s_n}$$

el mcd y el mcm se pueden expresar como

$$mcd(a,b) = p_1^{r_1} p_2^{r_2} p_3^{r_3} \cdots p_n^{r_n}$$
$$mcm(a,b) = p_1^{t_1} p_2^{t_2} p_3^{t_3} \cdots p_n^{t_n}$$

Donde $r_i = \min\{m_i, s_i\}$ y $t_i = \max\{m_i, s_i\}$

Referencias

Sánchez-Rubio García, C., Ripollés Amela, M. (2000)
Manual de matemáticas para preparación olímpica
Castelló de la Plana: Universitat Jaume I
Guelfond, A. O., (1979) Resolución de ecuaciones en números enteros.
Lecciones populares. Moscú: MIR
Crespo Casteleiro D.
Preparación Olimpiadas Matemáticas
Ramírez Benavides k.D.
Matemática Discretas