Universidad Nacional de Córdoba
Facultad de Matemáticas, Astronomía, Física y Computación
FAMAF

Matemática Discreta I

Resúmen

Integrantes: Ayala Facundo
Baudino Geremias

Profesor: Tiraboschi Leopoldo Alejandro

Índice de Contenidos

1. Números naturales

1.1. Aritmética

Aceptamos sin reparo que existe un conjunto de objetos llamados enteros. El conjunto de enteros se denotará por el símbolo especial $\mathbb{Z}$. Las propiedades de $\mathbb{Z}$ serán dadas por una lista de axiomas, a partir de las cuales seremos capaces de deducir todos los resultados sobre números enteros que necesitaremos en las cuestiones subsiguientes.

En la siguiente lista de axiomas a, b, c denotan enteros arbitrarios, y 0 y 1 denotan enteros especiales que cumplen las propiedades especificadas más abajo.

I1) $a + b$ *y* $a \cdot b$ pertenecen a $\mathbb{Z}$

I2) *Conmutatividad.* $a + b = b + a$; $ab = ba$.

I3) *Asociatividad.* $(a + b) + c = a + (b + c)$; $(a \cdot b) \cdot c = a \cdot (b \cdot c)$.

I4) *Existencia de elemento neutro.* Existen números $0, 1 \in \mathbb{Z}$ con $0 \neq 1$ tal que $a + 0 = a$; $a \cdot 1 = a$.

I5) *Distributividad.* $a \cdot (b + c) = a \cdot b + a \cdot c$.

I6) *Existencia del inverso aditivo.* Por cada a en $\mathbb{Z}$ existe un único entero a en $\mathbb{Z}$ tal que $a + (-a) = 0$.

I7) *Cancelación.* Si a es distinto de 0 y $a \cdot b = a \cdot c$, entonces $b = c$.

Estos axiomas nos permitirán demostrar algunas propiedades así como simplificar expresiones sin generar ambigüedades, veamos algunos ejemplos de propiedades demostradas a partir de los axiomas anteriormente enunciados.

Debido a la ley de asociatividad para la suma axioma (I3) $(a + b) + c$ es igual a $a + (b + c)$ y por lo tanto podemos eliminar los paréntesis sin ambigüedad. Es decir, denotamos

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

De forma análoga, usaremos la notación

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

Se puede demostrar la existencia del inverso aditivo debido a la ley de conmutatividad axioma (I2), es claro que del axioma (I4) se deduce que $0+a=a+0=a$ y $1\cdot a=a\cdot 1=a$. Análogamente, por el axioma (I2) y el axioma (I6) obtenemos que $a+a=a+(a)=0$.

Una propiedad que debemos mencionar es la siguiente:

$$si\ a,b,c\in\mathbb{Z}\ y\ a=b,\ \text{entonces}\ a+c=b+c\ y\ ac=bc.$$

Esto se debe a que la suma y el producto son operaciones que toman un par de enteros y devuelven otro entero. Si $a=b$, entonces el par a, c es igual al par b, c y por lo tanto devuelven la misma suma y el mismo producto.

Demostremos ahora que, para todo n entero, el opuesto de n es n, es decir que

$$-(-n)=n$$

El axioma (I6) nos dice que $(-n)$ es el único número que sumado a $-n$, da cero. Por lo tanto, para demostrar que $-(-n)=n$ basta ver que $(-n)+n=0$. Esto se cumple puesto que

$$(-n)+n=n+(-n)$$

$$=0$$

Por lo tanto $(-n)+n=0$.

A continuación, los axiomas enunciados también nos permitirán definir la resta o sustracción como una suma. Veamos entonces que

Definición
Si $a,b\in\mathbb{Z}$ definimos $a-b$ cómo la suma de a más el opuesto de b, es decir que $a-b:=a+(-b)$ por definición.

Ahora, demostremos una propiedad básica de la resta.

Demostremos que para dos enteros m y n cualesquiera

$$m-(-n)=m+n.$$

Por la definición de sustracción, $m-(-n)$ es la suma $m+(-(-n))$, es decir

$$m-(-n)=m+(-(-n)).$$

Por la demostración anterior sabemos que $-(-n)=n$ y por lo tanto $m-(-n)=m+(-(-n))=m+n$.

Ahora supongamos que existen dos enteros 0 y 0', que ambos cumplen el axioma (I4), esto es

$$a + 0 = a;\ a + 0' = a$$

Entonces para todo $a \in \mathbb{Z}$, $0 = 0'$ (Elemento neutro único)

$$0 + 0' = 0$$

$$0 + 0' = 0' + 0 = 0$$

El ejemplo anterior nos demuestra que hay un único elemento elemento que cumple el axioma (I4) en lo que respecta a la suma. A este elemento lo denotamos 0 y lo denominamos el elemento neutro de la suma. Lo mismo podemos probar con el elemento neutro respecto al producto

Lo mismo ocurre con el elemento neutro respecto al producto, es decir hay un único elemento, denotado 1, que satisface el axioma I4 en lo que se refiere al producto. A este elemento lo llamamos el elemento neutro del producto. Veamos el ejemplo de la regla de los signos y su demostración. Veamos que si $a, b \in \mathbb{Z}$ entonces tenemos

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

1.2. Ordenando los enteros

El orden natural de los enteros es tan importante como sus propiedades aritméticas. Desde el comienzo aprendemos los números en orden así como también el hecho de que 4 es mayor que 3, concepto que se convierte en algo de importancia práctica para nosotros.

Expresamos esta idea formalmente diciendo que existe una relación que indicamos $<$ ($a < b$ se lee: a es menor que b o también b es mayor que a). Solo cuatro axiomas se necesitan para especificar las propiedades básicas del símbolo $<$, y ellos son listados en lo que sigue. Como antes, a, b y c denotan enteros arbitrarios.

I8) *Ley de tricotomía.* Vale una y sólo una de las relaciones siguientes:

$$a < b,\ a = b,\ b < a.$$

I9) *Ley transitiva.* Si $a < b$ y $b < c$, entonces $a < c$

I10) *Compatibilidad de la suma con el orden.* Si a < b, entonces a + c < b + c.

I11) *Compatibilidad del producto con el orden.* Si $a < b$ y $0 < c$, entonces $ac < bc$.

Esta claro que podemos definir los otros símbolos de orden $>$, $\leq$ y $\geq$, en términos de los símbolos $<$ e $=$. Diremos que $m > n$ si $n < m$, diremos que $m \leq n$ si $m < n$ o $m = n$. Finalmente, diremos que $m \geq n$ si $m > n$ o $m = n$. Es importante notar que el axioma (I11) tiene una versión valedera para estos nuevos símbolos.

Proposición

Sean $a, b, c \in \mathbb{Z}$ podemos enunciar que

a) Si $c < 0$, entonces $0 < -c$.

b) Si $a < b$ y $c < 0$, entonces $ac > bc$.

Demostración

a) Sumando $-c$ a ambos miembros de la desigualdad $c < 0$, obtenemos $c+(-c) < 0+(-c)$ (compatibilidad de la suma con la relación de orden). Por los axiomas de inverso aditivo y elemento neutro, la expresión se reduce a $0 < -c$.

b) Como $a < b$, si sumamos a ambos miembros de la desigualdad $-a \ -b$, por la compatibilidad de la suma con $<$, obtenemos $a - a - b < b - a - b$ y por la aplicación reiterada de los axiomas de inverso aditivo y elemento neutro obtenemos $-b < -a$. Por a) sabemos que $0 < -c$, por lo tanto, por I11), $(-b)(-c) < (-a)(-c)$. Aplicando la regla de los signos obtenemos $bc < ac$ y por lo tanto $ac > bc$.

Ya hemos usado (en axioma I4) el símbolo $\neq$ que denota 'no es igual a' o bien 'es distinto a'. En general, cuando tachemos un símbolo, estamos indicando la negación de la relación que define. Por ejemplo, $a \not< b$ denota 'a no es menor que b'. $a \not< b$ es equivalente a $a \geqslant b$ por la ley de tricotomía axioma (I8), como $a \not< b$, entonces vale una de las dos afirmaciones siguientes, $a = b$ o $b < a$, es decir vale que $a \geqslant b$. De forma análoga se prueba que $a \not\leqslant b$ si y sólo si $a > b$, $a \not> b$ si y sólo si $a \leqslant b$ y $a \not\geqslant b$ si y sólo si $a < b$.

Debemos conocer también las siguiente propiedades de $\leqslant$. Sean $a, b, c \in \mathbb{Z}$ arbitrarios, entonces

O1) *Reflexividad.* $a \leqslant a$.

O2) *Antisimetría.* Si $a \leqslant b$ y $b \leqslant a$, entonces $a = b$.

O3) *Transitividad.* Si $a \leqslant b$ y $b \leqslant c$, entonces $a \leqslant c$.

Una relación que satisfaga las tres propiedades anteriores (reflexividad, antisimetría y transitividad) es llamada una relación de orden. Observar que $<$ no es una relación de orden, en el sentido de la definición anterior.

Podría parecer que ya tenemos todos los axiomas y propiedades que necesitamos de $\mathbb{Z}$ pero aún falta un axioma de vital importancia.

Observemos que todos los axiomas que enunciamos también los cumplen los números racionales $\mathbb{Q}$ y los números reales $\mathbb{R}$. ¿Cuál es la diferencia fundamental entre $\mathbb{Z}$, $\mathbb{Q}$ y $\mathbb{R}$?. Lo veremos a continuación.

1.2.1. Cota Inferior

Definimos a la cota inferior de un conjunto S como un numero, perteneciente o no al conjunto, que es menor que los elementos de ese conjunto.

Supongamos que X es un subconjunto de $\mathbb{Z}$; entonces diremos que el entero b es una cota inferior de X si $b \leqslant x$ para todo $x \in X$.

Algunos subconjuntos no tienen cotas inferiores: por ejemplo, el conjunto de los enteros negativos $-1, -2, -3, ...$, claramente no tiene cota inferior.

Por otro lado los conjuntos pueden tener más de una cota inferior pertenecientes o no al conjunto, veamos el siguiente ejemplo.

Ejemplo

$$-10, -9, -8, \textbf{-7}, \textbf{-6}, -5, -4, -3, -2, -1,\ 0,\ \textbf{1},\ \textbf{2},\ \textbf{3},\ 4,\ 5,\ 6,\ 7,\ 8,\ 9,\ 10$$

En este ejemplo los elementos de nuestro conjunto están en negrita, y podremos encontrar más de una cota inferior para el conjunto que tenemos, por ejemplo -9 y -10 que son cota inferior del mismo, sin embargo hay una cota inferior perteneciente al conjunto, veamos el siguiente concepto.

1.2.2. Mínimo

Se dice que un conjunto tiene un mínimo cuando encontramos una cota inferior perteneciente al conjunto, es decir un numero $b \in X$ que cumpla que $\forall x \in X, b \leq x$, entonces b será el mínimo de X.

En el ejemplo anterior vimos que teníamos números como -9 o -10 que son cotas inferiores de nuestro conjunto, sin embargo no pertenecen al mismo, pero también podemos ver que hay una cota inferior que es -7 la cual pertenece al conjunto y por lo tanto es el mínimo del mismo, pues $-7 < x$, $\forall x \in X$.

1.2.3. Axioma de buena ordenación

Nuestro último axioma para $\mathbb{Z}$ afirma algo que es aparentemente una propiedad obvia.

I12) *Axioma de buena ordenación.* Si S es un subconjunto de $\mathbb{Z}$ que no es vacío y tiene una cota inferior, entonces S tiene un mínimo.

Formalmente definido como

Para todo $S \subset \mathbb{Z}$ con $S \neq \varnothing$ se dice que S esta acotado inferiormente si S tiene un mínimo, esto es que existe un $b \in \mathbb{Z}$ tal que $b \leq s$, $\forall s \in S$

El axioma del buen orden nos da una justificación firme para nuestro intuitivo dibujo de los enteros: un conjunto de puntos regularmente espaciados sobre una linea recta, que se extiende indefinidamente en ambas direcciones como en la Fig. 2. En particular dice que no podemos acercarnos más y más a un entero sin alcanzarlo, de forma que el dibujo de la Fig. 3 no es correcto.

Figura 2: El dibujo correcto de $\mathbb{Z}$.

Figura 3: El dibujo incorrecto de $\mathbb{Z}$.

El hecho de que los enteros estén uniformemente separados nos lleva a decir que el conjunto $\mathbb{Z}$ es discreto y es esta propiedad la que lo diferencia del conjunto de racionales $\mathbb{Q}$ y el conjunto de reales $\mathbb{R}$, así como da origen al nombre de la materia 'Matemática Discreta'. En cálculo y análisis, los procesos de limite son fundamentales y es por eso que deben utilizarse conjuntos continuos y no los discretos.

1.3. Definiciones recursivas

1.3.1. Recursión

¿Qué es la recursión?

Recursión o recursividad es la forma en la cual se especifica un proceso basado en su propia definición. La recursión tiene la característica de construir a partir de un mismo tipo.

Un problema que pueda ser definido en función de su tamaño, sea este N, pueda ser dividido en instancias más pequeñas (<N) del mismo problema y se conozca la solución explícita a las instancias más simples, lo que conocemos como casos base, se puede aplicar inducción sobre las llamadas más pequeñas y suponer que quedan resueltas. Veamos un ejemplo.

Ejemplo

Conociendo que para la función factorial, los casos base 0 y 1 dan como resultado 1, y utilizando la formula recursiva de factorial, tenemos:

Definiremos a Factorial recursivamente como:

$Fact_{(0)} = 1$
$Fact_{(1)} = 1$
$Fact_n = n \cdot Fact_{(n-1)}$

Veamos que $Fact_4 = 24$

$Fact_{(4)} = 4 \cdot Fact_{3)}$
$Fact_{(3)} = 3 \cdot Fact_2$
$Fact_{(2)} = 2 \cdot Fact_1$
$Fact_{(1)} = 1 \cdot Fact_0$
$Fact_{(0)} = 1$

Luego resolvemos y esto es $4 \cdot 3 \cdot 2 \cdot 1 \cdot 1 = 24$

1.3.2. Sucesiones

Una sucesión es una aplicación cuyo dominio es el conjunto de los números naturales y su codominio es cualquier otro conjunto. Cada número resultante de ella es llamado término de la sucesión y al número de elementos ordenados(posiblemente infinitos) se le denomina longitud de la sucesión.

Una sucesión puede ser dada de forma explícita. Veamos algunos ejemplos.

- $U_n = 3n + 2$
- $W_n = (n + 1) \cdot (n + 2) \cdot (n + 3)$

Para calcular, en cada paso reemplazamos n en la fórmula de la sucesión y obtenemos el resultado. Por ejemplo $W_2 = (2 + 1) \cdot (2 + 2) \cdot (2 + 3) = 60$
Cuando una sucesión puede expresarse como combinación de un número determinado de operaciones elementales, diremos que tiene una formula cerrada.

A veces la sucesión que nos interesa no tiene una fórmula cerrada como las anteriores y podemos expresarla en forma recursiva. Veamos un ejemplo.

- $U_1 = 1$ (Caso base)
- $U_2 = 2$ (Caso base)
- $U_n = U_{n-1} + U_{n-2}$, para $n \geq 3$ (Caso recursivo)

- $U_3 = U_{3-1} + U_{3-2} = U_2 + U_1 = 2 + 1 = 3$
- $U_4 = U_{4-1} + U_{4-2} = U_3 + U_2 = 3 + 2 = 5$

Esta es la famosa sucesión de Fibonacci.

En base a los resultados podemos, en algunos casos, obtener una formula general para U_n

El principio de inducción nos permitirá probar este tipo de afirmaciones. La definición recursiva es muy utilizada y a veces la encontraremos escondida detrás de notaciones que veremos a continuación.

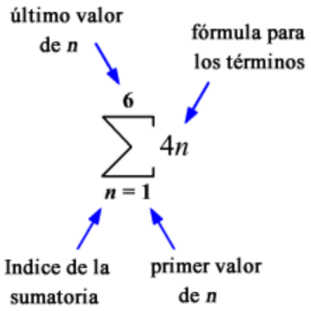
1.3.3. Definición recursiva de sumatoria

Sea n ∈ N sean a_i para $1 \leq i \leq n$, una secuencia de números (reales, enteros, etc.). Entonces $\sum_{i=1}^{n} a_i$ denota la función recursiva definida

$$\sum_{i=1}^{1} = a_1, \ \sum_{i=1}^{n} a_i = \sum_{i=1}^{n-1} a_i + a_n (n \geq 2)$$

En este caso decimos que $\sum_{i=1}^{n}$ es la sumatoria de los a_i de i=1 hasta n.

También podemos ver las partes que componen a la sumatoria



Entonces el resultado para la sumatoria genérica será

$$\sum_{i=1}^{n} a_i = a_1 + a_2 + ... + a_n$$

1.3.4. Definición recursiva de la productoria

Sea n ∈ N sean a_i para $1 \leq i \leq n$, una secuencia de números (reales, enteros, etc.). Entonces $\prod_{i=1}^{n} a_i$ denota la función recursiva definida

$$\prod_{i=1}^{1} a_i = a_1, \ \prod_{i=1}^{n} a_i = \prod_{i=1}^{n-1} a_i \cdot a_n \ (n \geq 2)$$

En este caso, decimos que $\prod_{i=1}^{n}$ es la productoria de los a_i de $i = 1$ a n.

Las partes que componen la productoria son las mismas que en la sumatoria solo que cambia en que entre cada termino van a estar multiplicándose y no sumándose

Entonces el resultado para la productoria genérica será

$$\prod_{i=1}^{n} a_i = a_1 \cdot a_2 \cdot ... \cdot a_n$$

1.3.5. Definición recursiva de n!

Sea n ∈ N, sean a_i para $1 \leq i \leq n$, una secuencia de números. En el caso de n! se puede definir como

- $0! = 1$ (por completitud)
- $1! = 1$
- $n! = n \cdot (n-1)!$ para $n \geq 2$

Así como también podemos definirlo como un caso especial de la productoria

$$n! = \prod_{i=1}^{n} i = 1 \cdot 2 \cdot ... \cdot n$$

1.3.6. Definición recursiva de x^n

También puede realizarse la definición de la 'n-esima potencia' de un numero: Sea x un número, si n ∈ ℕ, definimos

- $x^0 = 1$ (por completitud)
- $x^1 = x$
- $x^n = x \cdot x^{n-1}$ para $n \geq 2$

Por último podemos enunciar las propiedades de la potencia. Si $n, m \in \mathbb{N}$ se cumplen las siguientes propiedades:

- $x^n \cdot x^m = x^{n+m}$
- $(x^n)^m = x^{n \cdot m}$

1.4. El principio de inducción

¿Qué es la inducción?

La inducción es un razonamiento que permite demostrar proposiciones que dependen de una variable n que toma una infinidad de valores enteros. En términos simples, la inducción matemática consiste en el siguiente razonamiento.

Dado un número entero a que tiene la propiedad **P**, y el hecho de que si hasta cualquier número entero n con la propiedad **P** implique que $n+1$ también la tiene, entonces, todos los números enteros a partir de a tienen la propiedad **P**.

La demostración está basada en el axioma denominado principio de la inducción matemática. 'La inducción matemática nos demuestra que podemos subir tan alto como queramos en una escalera, si demostramos que podemos subir el primer peldaño (caso base) y que desde cada peldaño podemos subir al siguiente (paso inductivo)'.

Ahora queremos analizar la suma de los primeros n números impares, es decir que la fórmula recursiva sería tal que así $1+3+5+...+(2n-1)$.

Por la definición de la sumatoria tenemos que

$$a_1 = 1,\ a_n = a_{n-1} + 2n - 1$$

Analizando los primeros valores tenemos

- $a_1 = 1$,
- $a_2 = 1+3 = 4$,
- $a_3 = 1+3+5 = 9$,
- $a_4 = 1+3+5+7 = 16$

Si observamos, estos son los cuadrados de cada n, entonces $a_n = n^2$

Entonces podemos conjeturar que

$$1+3+5+...+(2n-1) = n^2$$

Para convencernos de que la fórmula es ciertamente correcta procederemos comprobando inicialmente para $n = 1$, y puesto que $1 = 1^2$, decimos que es correcto para un caso base.

Luego, supongamos que esta proposición es correcta para algún valor específico de n, digamos para $n = k$, de modo que

$$1+3+5+...+(2k-1) = k^2 \qquad \text{Simplemente cambiamos n por k}$$

Podemos utilizar esta definición para simplificar la expresión definida recursivamente a la izquierda de la igualdad cuando n es igual a $k+1$,

$$\begin{aligned} 1+3+5+...+(2k+1) &= 1+3+5+...+(2k-1)+(2k+1); \\ &= k^2+(2k+1); \\ &= (k+1)^2; \\ &= (n)^2 \end{aligned}$$

Por lo tanto si el resultado es correcto cuando $n=k$, también lo es cuando $n=k+1$. Se comienza observando que si es correcto cuando $n=1$, debe ser correcto cuando $n=2$, con el mismo argumento, cuando $n=2$ es correcto cuando $n=3$. Continuando de esta forma veremos que es correcto para todos los enteros positivos n.

La esencia de este argumento se llama **principio de inducción**.

1.4.1. Enunciado del principio de inducción

Supongamos que S es un subconjunto de $\mathbb{N}$ que satisface las condiciones

a) $1 \in S$,

b) para cada $k \in N$, si $k \in S$, entonces $k+1 \in S$

Entonces se sigue que $S = \mathbb{N}$

Demostración

Si la conclusión es falsa, $S \neq \mathbb{N}$ y el conjunto complementario S^c definido por

$$S^c = \{r \in \mathbb{N} | r \notin S\}$$

es no vacío.

Por el axioma de buena ordenación, S^c tiene un menor elemento (mínimo). Tenemos entonces un elemento mínimo r_0 en S^c. $r_0 \neq 1$, porque $1 \in S$, eso implica que r_0 es un natural > 1.

Como r_0 es el mínimo de los que no pertenecen a S, entonces $r_{0-1} \in S$, entonces $r_{0-1+1} \in S$, es decir $r_0 \in S$, lo cual es absurdo, y como el absurdo vino de suponer que $S \neq \mathbb{N}$ queda demostrado que $S = \mathbb{N}$.

El principio de inducción es útil para probar la veracidad de propiedades relativas a los números naturales.

Ejemplo

Demostrar que $X_n = n \cdot (n+1) \ \ \forall n \in \mathbb{N}$ conociendo que el entero X_n está definido recursivamente por

$$X_1 = 2, \ X_n = X_{n-1} + 2n \ \ \forall n | n \geq 2$$

Resolución

(Caso base) El resultado es verdadero cuando $n = 1$, pues $2 = 1 \cdot 2$; $2 = 2$

(Paso inductivo) Supongamos que el resultado verdadero cuando n = k, o sea que

$$X_k = k \cdot (k+1) \qquad \text{Hipótesis Inductiva (HI)}$$

En el paso inductivo queremos probar que

$$X_k = k \cdot (k+1) \implies X_{k+1} = (k+1) \cdot (k+2)$$

Cuando debemos probar esto, generalmente partimos del término de la izquierda de la tesis y luego de varios pasos(entre ellos la hipótesis inductiva), llegaremos al término de la derecha de la tesis. Entonces

$$\begin{aligned} X_{k+1} &= X_k + 2 \cdot (k+1); && \text{Por la definición recursiva } (X_n) \\ &= k \cdot (k+1) + 2(k+1); && \text{Por la hipótesis inductiva } (X_k) \\ &= k \cdot (k+1) + 2 \cdot (k+1); && \text{Por factor común de } (k+1) \\ &= (k+1) \cdot (k+2) \end{aligned}$$

Entonces el resultado es verdadero cuando $n = k + 1$ y por el principio de inducción, es verdadero para todos los enteros positivos.

Existen varias formas modificadas del principio de inducción. A veces es conveniente tomar como base inductiva el valor $n = 0$, algunas otras puede ser apropiado tomar un valor como 2 o 3 porque los primeros casos pueden ser excepcionales. Cada problema debe ser tratado según sus características.

Otra modificación útil es tomar como hipótesis inductiva la suposición de que el resultado es verdadero para todos los valores $n \leq k$, más que para $n = k$ solamente, y después probar para $(k + 1)$. Esta formulación es llamada a veces como el **principio de inducción completa**. Todas estas modificaciones pueden justificarse con cambios triviales en la demostración del principio de inducción.

1.4.2. Enunciado del principio de inducción completa

Supongamos que n_0 es cualquier entero (no necesariamente positivo) y sea $\mathbb{Z} \geq n_0$ el conjunto de enteros n tal que n $\geq n_0$. Sea S un subconjunto de $\mathbb{Z} \geq n_0$ que satisface las condiciones:

a) $n_0 \in S$

b) si h $\in$ S para todo h en el rango $n_0 \leq h \leq k$ entonces k+1 $\in$ S

Entonces se sigue que S = $\mathbb{Z} \geq n_0$

Lo que el principio de inducción completa dice es que no hay que restringirse al caso menor, sino que, podemos usar cualquier otro caso anterior.

Ejemplo

Para la función definida como

$$\begin{aligned} U_1 &= 3; \\ U_2 &= 5; \\ U_n &= 3 \cdot U_{n-1} - 2 \cdot U_{n-2} \quad \forall n \geq 3 \end{aligned}$$

probemos que $U_n = 2^n + 1$, para todo $n \in \mathbb{N}$.

Solución

(Caso base) El resultado es verdadero cuando $n = 1$, pues cuando $n = 1 : 3 = 2^1 + 1$; $3 = 3$, luego también vemos que es verdadero cuando $n = 2$, pues cuando $n = 2 : 5 = 2^2 + 1$

(Paso inductivo) Supongamos que el resultado verdadero cuando $n = k$, o sea que

$$U_k = 2^k + 1 \text{ para } 1 \leqslant n \leqslant k \text{ y } k \geq 2 \qquad \text{Hipótesis Inductiva (HI)}$$

En el paso inductivo queremos probar que

$$U_k = 2^k + 1 \text{ para } 1 \leqslant n \leqslant k \implies U_{k+1} = 2^{k+1} + 1$$

Se comienza con el término izquierdo de la tesis y se llega al término derecho de la misma, teniendo de por medio pasos como la hipótesis inductiva y la definición recursiva.

$$\begin{aligned} U_{k+1} &= 3 \cdot U_{k+1-1} - 2 \cdot U_{k+1-2}; \\ &= 3 \cdot (2^k + 1) - 2 \cdot (2^{k-1} + 1); \\ &= 3 \cdot 2^k + 3 - 2 \cdot 2^{k-1} - 2; \\ &= 3 \cdot 2^k - 2^k + 1; \\ &= 2 \cdot 2^k + 1; \\ &= (2^{k+1} + 1) \end{aligned}$$

2. Conteo

¿Qué es contar?

Contar es algo que todos sabemos realizar por naturaleza y se trata de enumerar distintos elementos, casos, cosas, etcétera. A veces puede no ser tan trivial y volverse un caso de estudio.

2.0.1. Cardinal de un conjunto

Un conjunto A es finito si podemos contar la cantidad de elementos que tiene. En ese caso denotamos $|A|$ la cantidad de elementos de A y la llamaremos el cardinal de A.

Por ejemplo los conjuntos

$$A = \{a, b, z, x, 1\}, \qquad B = \{1, 2, 3, 4, 5\}$$

Tienen 5 elementos, es decir, $|A| = |B| = 5$

Conjuntos como $\mathbb{Z}$, $\mathbb{N}$ o $\mathbb{R}$ son infinitos y por lo tanto no tiene sentido hablar de la cantidad de elementos de estos conjuntos. Para formalizar el concepto de cardinal se dice que dos conjuntos tienen el mismo cardinal si hay una biyección de uno a otro.

2.1. Principio de adición y multiplicación

2.1.1. Principio de adición

Dada dos actividades x e y, si se puede realizar x de n formas distintas o, alternativamente, se puede realizar y de m formas distintas. Entonces el número de formas de realizar 'x o y' es $n+m$. Es importante que no haya formas de x en y, y viceversa. En lenguaje de conjuntos esto sería

$$\text{Si } x \cap y = \varnothing \implies |x \cup y| = |x| + |y|$$

Ejemplo

Suponiendo que una persona va a salir a pasear y puede ir al cine donde hay 3 películas en cartelera o al teatro donde hay 4 obras distintas. Entonces tendrá un total de $3 + 4 = 7$ formas distintas de elegir el paseo.

Este es el principio más básico de conteo y se generaliza fácilmente. Sean $A_1, ..., A_n$ conjuntos finitos tales que $A_i \cap A_j = \varnothing$ cuando $i \neq j$, entonces

$$A_1 \cup ... \cup A_n = |A_1| + ... + |A_n|$$

Remarcamos que para aplicar el principio de adición es necesario que los eventos se excluyan mutuamente. El caso general es

$$|A \cup B| = |A| + |B| - |A \cap B|$$

2.1.2. Principio de multiplicación

Suponiendo que una actividad consiste de 2 etapas a realizar, y la primera etapa puede ser realizada de n_1 maneras y la segunda etapa puede realizarse de n_2 maneras, independiente de como se realizó la etapa 1, entonces el principio de multiplicación nos indica que

La actividad puede ser realizada de $n_1 \cdot n_2$ formas distintas.

Suponiendo que la persona del ejemplo anterior tiene tiempo y dinero para ir primero al cine y luego al teatro(3 y 4 posibilidades respectivamente) entonces tendrá $3 \cdot 4 = 12$ formas distintas de hacer el paseo.

Para saber cuando aplicar cada uno de estos dos principios debemos pensar en la temporalidad de los hechos, si la selección es simultanea aplicamos el principio de adición, caso contrario aplicamos el principio de multiplicación.

Ejemplo

¿Cuantos números de dos cifras se pueden hacer donde la primera cifra sea par y la segunda múltiplo de 3, siendo ambas cifras números menores que 10?

Solución

$$\begin{aligned} A = \text{Primer cifra } &= \{2,4,6,8\} \implies |A| = 4 \\ B = \text{Segunda cifra } &= \{0,3,6,9\} \implies |B| = 4 \end{aligned}$$

Al ser una independiente de otra y también tener 2 'etapas' de selección, utilizamos el principio de multiplicación, que indica que la actividad puede ser realizada de $n_1 \cdot n_2$ formas, es decir

$$|A| \cdot |B| = 4 \cdot 4 = 16$$

Formalmente, si A,B son conjuntos y definimos el producto cartesiano entre A y B como

$$A \times B = \{(a,b) : \ a \in A, \ b \in B\}$$

Entonces si A y B son conjuntos finitos se cumple que

$$|A \times B| = |A| \cdot |B|$$

Existiendo un caso especial cuando $A = B$

Ejemplo

¿Cuantas palabras de dos letras hay? (26 letras, sin importar si tienen o no significado).

Respuesta : $26 \cdot 26 = 26^2$. Esto debido a que la primer letra es independiente y otra etapa distinta de la selección de la segunda, por lo que en cada instancia podremos seleccionar 26 letras, esto nos dice que es $26 \cdot 26$ palabras diferentes de 2 letras.

2.2. Selecciones ordenadas con repetición

Proposición

Sean m, $n \in N$. Hay n^m formas de elegir ordenadamente m elementos de un conjunto de n elementos. Donde $n = |X|$ y m es la cantidad de elecciones.

Notación

Si elegimos a y b en forma ordenada, denotamos ab

Idea de la prueba

La prueba de esta proposición se basa en aplicar el principio de multiplicación $m-1$ veces. A nivel formal, debemos hacer inducción sobre m y usar el principio de multiplicación en el paso inductivo. Entonces tenemos que

$$\begin{aligned} |X^{n+1}| &= |X^n \times X| \\ &= |X^n| \cdot |X| \\ &= |X|^n \cdot |X| \\ &= |X|^{n+1} \end{aligned}$$

Veamos un ejemplo de selecciones ordenadas con repetición para terminar de entender el concepto.

Ejemplo

Sea $X = \{1, 2, 3\}$. ¿De cuantas formas puedo elegir dos de estos números de forma ordenada? Veamos que las posibilidades son

$$\begin{gathered} 11,\ 12,\ 13 \\ 21,\ 22,\ 23 \\ 31,\ 32,\ 33 \end{gathered}$$

Es decir, hay $9 = 3^2$ formas posibles. ¿Cómo justificamos esta conclusión?

El hecho de que el modo sea ordenado nos indica que temporalmente primero se escoge 1 y luego el otro, así sucesivamente hasta completar las selecciones, lo cual también, junto con que admitimos repetición, nos hace ver que una variable es independiente de otra y podamos tomar todos los casos posibles, es decir, $|X \times X|$

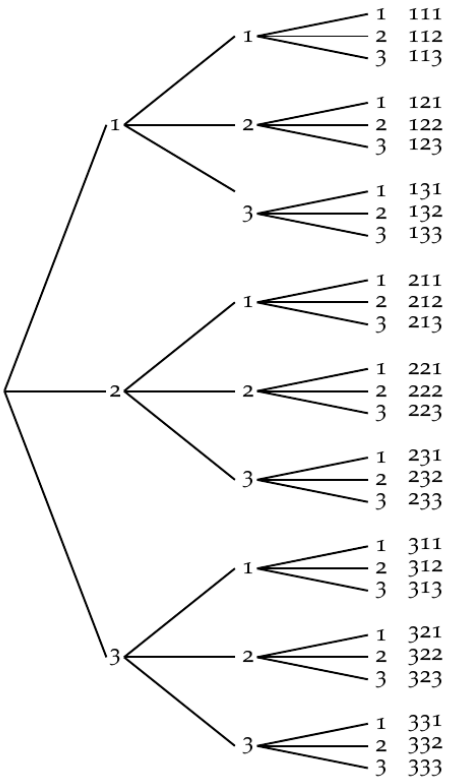
Entonces podemos elegir también 3 elementos de los integrantes de X, de forma que formemos subconjuntos de 3 elementos de 1,2 y 3 de forma ordenada y con repetición, tal que

$$\begin{gathered} 111,\ 112,\ 113,\ 121,\ 122,\ 123,\ 131,\ 132,\ 133 \\ 211,\ 212,\ 213,\ 221,\ 222,\ 223,\ 231,\ 232,\ 233 \\ 311,\ 312,\ 313,\ 321,\ 322,\ 323,\ 331,\ 332,\ 333 \end{gathered}$$

Lo que son un total de $27 = 3^3$ posibilidades de selección ordenada con repetición de 3 elementos del conjunto X.

Esto está denotado por $|X \times X \times X|$ que inductivamente es igual que $|X \times X| \cdot |X|$ y a su vez esto inductivamente es igual a $|X| \cdot |X| \cdot |X|$ o lo que es lo mismo que $|X|^3$, lo que para casos generales sería $|X|^P$

Un diagrama arbolado arbolado también nos ayuda a verlo, hagamos el diagrama del problema.



Este razonamiento es el enunciado en la **Proposición** anterior.

Proposición
La cantidad de subconjuntos de un conjunto de n elementos es 2^n.

Dado X un conjunto, denotamos $\mathcal{P}$(X) el conjunto formado por todos los subconjuntos de X, por ejemplo

$$\mathcal{P}(\{1,2\}) = \{\varnothing, \{1\}, \{2\}, \{1,2\}\}$$

Si X es un conjunto finito, la **Proposición** nos dice que

$$|\mathcal{P}(X)| = 2^{|X|}$$

Demostración

Veamos la demostración superficial de que $|\mathcal{P}(x)| = 2^{|x|}$, que dicho de otra forma, sería que $|x| = n \implies$ la cantidad de subconjuntos de X es 2^n.

Supongamos que $X = \{a_1, ..., a_n\}$ y sea $A \subseteq X$, entonces

$$\begin{aligned} a_1 \in A \oplus a_1 \notin A &= 2 \text{ posibilidades} \\ a_2 \in A \oplus a_2 \notin A &= 2 \text{ posibilidades} \\ &\vdots \\ a_n \in A \oplus a_n \notin A &= 2 \text{ posibilidades} \end{aligned}$$

Por lo que habrá 2^n posibles subconjuntos de un conjunto de n elementos.

Ejemplo

Sea X un conjunto de m elementos. Queremos contar cuántos subconjuntos tiene este conjunto. Por ejemplo, si $X = \{a, b, c\}$ los subconjuntos de X son exactamente

$$\varnothing, \{a\}, \{b\}, \{c\}, \{a, b\}, \{a, c\}, \{b, c\}, \{a, b, c\}.$$

Es decir, si X es un conjunto de 3 elementos, entonces tiene 8 o 2^3 subconjuntos.

Entonces cumple el patrón que hemos enunciado anteriormente, veamos que suponiendo que $A \subseteq X$ tenemos que

$$\begin{aligned} a \in A \text{ ó } a \notin A \quad &(2 \text{ posibilidades}) \\ b \in A \text{ ó } b \notin A \quad &(2 \text{ posibilidades}) \\ c \in A \text{ ó } c \notin A \quad &(2 \text{ posibilidades}) \end{aligned}$$

Luego, como cada selección es independiente del resto, por el principio de multiplicación tenemos en total $2 \cdot 2 \cdot 2 = 2^3 = 8$ posibilidades.

Entonces generalizamos diciendo que dado un elemento a, puede estar o no en el conjunto independientemente si los otros elementos están o no, por lo que tenemos 2 posibilidades por cada elemento, lo que resulta en 2^n posibilidades, donde n representa la cantidad de elementos del conjunto.

2.3. Selecciones ordenadas sin repetición

Estudiaremos entonces, las selecciones ordenadas de m elementos entre n en donde NO se permite la repetición. Es decir, si el conjunto es $A = \{a_1, a_2, ..., a_n\}$. Las selecciones deben ser del tipo

$$a_{i_1} a_{i_2} ... a_{i_m}$$

donde $a_{ij} \neq a_{ik}, si\ i \neq j \neq k$

Proposición

Si $n \geqslant m$ entonces existen

$$n \cdot (n-1) \cdot ... \cdot (n-(m-1)),\ \text{(m-factores)} = \frac{n!}{(n-m)!}\ \ \text{(Versión compacta)}$$

selecciones ordenadas y sin repeticiones de m elementos de un conjunto de n elementos.

Demostración

Para la prueba, tenemos que tener en cuenta el siguiente razonamiento: debemos seleccionar m-veces elementos de un conjunto de n elementos. La primera selección puede ser de cualquiera de los n objetos; la segunda selección debe recaer en uno de los $n-1$ elementos restantes. De manera similar, hay $n-2$ posibilidades para la tercera selección, y así sucesivamente. Cuando hacemos la m-esima selección, $m-1$ elementos ya han sido seleccionados, y entonces el elemento seleccionado debe ser uno de los $n-(m-1)$ elementos restantes.

2.3.1. Casos

Caso $n < m$

Principio de las casillas. Sean n y $m \in \mathbb{N}$. Si $n < m$, no hay ninguna selección ordenada y sin repetición de m elementos de un conjunto de n elementos.

Este principio también conocido como principio del palomar es intuitivamente trivial: si, por ejemplo hay mas personas que asientos, alguien se va a quedar parado.

Caso $n = m$ **(Permutación)**

Este es un caso muy particular, el cual incluso se le da un nombre especial debido a su infinidad de usos y nos dice que cuando $n = m$, entonces tenemos

$$n \cdot (n-1) \cdot ... \cdot (n-(n-1)) = n \cdot (n-1) \cdot ... \cdot 1 = n!$$

selecciones ordenadas y sin repetición de n elementos de un conjunto con n elementos.

De la formula anterior se deduce de que si n = m

$$n \cdot (n-1) \cdot ... \cdot (n-(m-1)),\ (m\text{-factores}) = \frac{n!}{(n-n)!}$$
$$n \cdot (n-1) \cdot ... \cdot (n-(m-1)),\ (m\text{-factores}) = \frac{n!}{(0)!}$$
$$n \cdot (n-1) \cdot ... \cdot (n-(m-1)),\ (m\text{-factores}) = n!$$

Las selecciones ordenadas y sin repetición de n elementos en un conjunto con n elementos se denominan **permutaciones** de grado n. Hay, pues, n! permutaciones de grado n.

Caso $n > m$

Este es el caso más general y está definido en la proposición inicial, podemos tomar cualquiera de las dos formas de definirlo, sin embargo es más visual y más utilizada la fórmula compacta

$$\frac{n!}{(n-m)!}$$

Para dejar más claro cada caso y analizar los usos de cada uno de ellos, haremos ahora algunos ejemplos de los mismos.

Ejemplo

Elegir de forma ordenada y sin repetición 2 elementos del conjunto $X = \{a, b, c\}$, tenemos entonces

$$ab, ac, ba, bc, ca, cb \qquad 6 \text{ posibles selecciones ordenadas sin repetición}$$

En los casos anteriores no era relevante lo que había en la selección anterior para realizar la selección actual.

Como hemos enunciado antes, si el conjunto es $X = \{a_1, a_2, ..., a_n\}$. Las selecciones deben ser del tipo

$$a_{i1}a_{i2}...a_{im} \ \text{ donde } a_{ij} \neq a_{ik}, si\ i \neq j \neq k$$

Por ejemplo, las selecciones de 3 elementos de forma ordenada y sin repetición de $\{1, 2, 3\}$ son exactamente

Tomamos el	Podemos seguir con	Obligatoriamente será		Resultará en
1	2	3	$\Longrightarrow$	123
1	3	2	$\Longrightarrow$	132
2	1	3	$\Longrightarrow$	213
2	3	1	$\Longrightarrow$	231
3	1	2	$\Longrightarrow$	312
3	2	1	$\Longrightarrow$	321

Las ternas con los tres números resultantes distintos serían 6 en total por el procedimiento anterior.

Notemos que
1er elemento $\implies$ 3 posibilidades: $1, 2, 3$
2do elemento $\implies$ 2 posibilidades: Distinto del primer elemento
3er elemento $\implies$ 1 posibilidad: El que falta de elegir

Tenemos entonces $3 \cdot 2 \cdot 1 = 3!$ posibles selecciones ordenadas y sin repetición.

Este ha sido un ejemplo ha sido del tipo $n = m$ (permutación), pues hemos seleccionado 3 elementos entre 3, ahora veamos otro ejemplo en el que debamos escoger 3 elementos entre 5.

Ejemplo
Si en un colectivo hay 9 asientos vacíos. ¿De cuantas formas pueden sentarse 3 personas?

Solución
Por la proposición de las selecciones ordenadas sin repetición: Debemos seleccionar 3 asientos entre 9, de todas las formas posibles.

Entonces decimos que se trata de ver cuantas selecciones ordenadas y sin repetición hay de 3 asientos entre 9.

La primer persona se puede sentar en cualquiera de los 9 asientos, luego, la segunda persona se puede sentar en cualquiera menos en el que sentó la primer persona, por último la tercer persona deberá elegir un asiento entré los que restan, es decir, ni el que está la primera ni la segunda persona.

Persona	Asientos
1ra	9 posibles
2da	9 - 1 posibles
3ra	9 - 2 posibles

Esto por lo tanto nos dará como resultado $9 \cdot 8 \cdot 7 = \frac{9!}{(9-3)!} = \frac{9!}{6!}$ posibilidades de sentar de diferente forma a 3 pasajeros en 9 asientos.

Ejemplo
Veamos un ejemplo en el que $n < m$.

¿De cuantas formas podemos sentar 15 personas en una mesa de 12 lugares?

Solución
Pues es sencillo notar que no hay forma de sentar 15 personas en 12 lugares, cuando la cantidad de objetos/personas/etc exceden la cantidad de puestos/lugares/etc en los que pueden posicionarse, pues no podremos encontrar una forma de hacerlo. Esto es lo enunciado en el Principio de las casillas.

Ejemplo importante

¿Cuantas permutaciones pueden formarse con las letras de 'Silvia'?

Solución

De primeras atinaremos a decir que las permutaciones en la palabra 'Silvia' son 6!, pues tenemos 6 letras, pero debemos ver que tenemos algunas restricciones que hacerle.

Como vemos, en la palabra 'Silvia' hay una letra que se repite, la 'i', y a la hora de ordenarlas, en el caso por ejemplo

$$...i...i'...$$

tendremos el mismo caso que en la permutación

$$...i'...i...$$

Esto nos lleva a tener que restringir las posibilidades en 2!, ya que van a repetirse esos casos.

Por lo que podemos afirmar que la cantidad de permutaciones en la que la palabra Silvia son $\frac{6!}{2!}$

Ejemplo

Si hay 10 personas ¿De cuantas formas puedo hacer una fila de 7 personas?

Solución

Tenemos que tomar del conjunto inicial de 10 personas, 7 de ellas, por supuesto que estos casos no admiten repetición ya que no podemos poner dos veces la misma persona, además que deben tener cierto orden, por lo que nuestra solución involucra una cantidad $n = 10$ elementos o personas y también una cantidad $m = 7$ de lugares o selecciones que debemos realizar, entonces veamos que esto es por la proposición inicial, $n - m + 1 = 10 - 7 + 1 = 4$, que son las posibilidades del último elemento.

Por lo tanto la solución es $10 \cdot ... \cdot 4 = 10 \cdot 9 \cdot 8 \cdot 7 \cdot 6 \cdot 5 \cdot 4$

2.4. Selecciones desordenadas y sin repetición

Este es uno de los casos más importantes ya que es el que modeliza mucho de los casos de la vida real.

Sea X un conjunto finito de n elementos.¿Cuantos subconjuntos de m elementos hay en X?. Veamos esto con un ejemplo.

Sea X un n-conjunto y $\{x_1, x_2, ..., x_n\}$ un m-subconjunto de X. Hay n formas de elegir el elemento x_1, $n-1$ formas de elegir el elemento x_2, $n-2$ formas de elegir el elemento x_3, etcétera, y finalmente $n-(m-1) = n-m+1$ formas de elegir el elemento x_m. Por el principio de la multiplicación hay

$$n \cdot (n-1) \cdot (n-2) \cdot ... \cdot (n-k) \cdot (n-m+1)$$

formas de elegir m elementos de X. Sin embargo, las $m!$ reordenaciones posibles de estos elementos representan el mismo conjunto. Luego, el numero buscado es

$$\frac{n \cdot (n-1) \cdot ... \cdot (n-m+1)}{m!}$$

Ejemplo

Sea $X = \{1, 2, 3, 4, 5\}$ y nos interesan los subconjuntos que puedan armarse de tres elementos.¿Cuantos subconjuntos habrá?.

Solución

Manualmente podemos ver que podemos formar

$\{1,2,3\},\ \{1,2,4\},\ \{1,2,5\},\ \{1,3,4\},\ \{1,3,5\},\ \{1,4,5\},\ \{2,3,4\},\ \{2,3,5\},\ \{2,4,5\},\ \{3,4,5\}$

Podríamos preguntarnos ¿Por qué sí consideramos $\{1,2,3\}$ y por qué no $\{1,3,2\}$?
Realmente en un subconjunto o conjunto en general no importa el orden por lo que $\{1,2,3\} = \{1,3,2\}$. Ambos están contemplados.

Sin embargo hacerlo manual cada vez será engorroso, entonces podemos tratar de buscar un patrón para calcularlo a través de una fórmula.

Podemos ver que debemos claramente restringir un total, entonces veamos que la forma de realizarlo es pensarlo con herramientas que ya conocemos.

Una forma de hacerlo es individualizar un subconjunto de tres elementos comenzando por seleccionar ordenadamente 3 elementos. (Selecciones ordenadas sin repetición o permutaciones).

Entonces habría, a priori, $5 \cdot 4 \cdot 3$ subconjuntos, pues ese es el número de selecciones sin repetición.

$$\left(\frac{n!}{(n-m)!}\right)$$

Peeeerooo... Está claro que vamos a tener algunas selecciones que determinan el mismo subconjunto. Por ejemplo cualquiera de las selecciones

$$\{1,2,3\},\ \{1,3,2\},\ \{2,1,3\},\ \{2,3,1\},\ \{3,1,2\},\ \{3,2,1\}$$

Determina el subconjunto $\{1,2,3\}$

Es decir las permutaciones de $\{1,2,3\}$ determinan el mismo subconjunto. Por lo tanto tenemos $m!$ selecciones ordenadas equivalentes que restringir. Esto dará como resultado que la cantidad de subconjuntos de m elementos a partir de uno de n elementos es

$$\frac{n!}{(n-m)! \cdot m!}$$

Gráficamente esto sería

$$\{1,2,3\},\ \{1,3,2\},\ \{2,1,3\},\ \{2,3,1\},\ \{3,1,2\},\ \{3,2,1\} \implies \{1,2,3\}$$

$$\{3,4,5\},\ \{3,5,4\},\ \{4,3,5\},\ \{4,5,3\},\ \{5,3,4\},\ \{5,4,3\} \implies \{3,4,5\}$$

Entonces, para el ejemplo anterior tenemos

$\frac{5!}{(5-3)! \cdot 3!} = \frac{5!}{2! \cdot 3!}$ posibles subconjuntos de 3 elementos de un conjunto de 5 elementos.

Proposición

Sea X un conjunto finito de n elementos. Entonces el número total de subconjuntos de m elementos de X es

$$\frac{n \cdot (n-1) \cdot \ldots \cdot (n-m+1)}{m!} = \frac{n!}{(n-m)! \cdot m!}$$

2.5. Número combinatorio

Este proposición anterior es tan importante que tiene un nombre y una notación particular.

2.5.1. Definición del número combinatorio

Sean n,m $\in N_0$, m $\geq$ n. Definimos

$$\binom{n}{m} = \frac{n!}{(n-m)! \cdot m!}$$

El número combinatorio está asociado al par $n,\ m$ con $m \leqslant n$. Y por razones que se verán mas adelante, se denomina el coeficiente binomial o numero combinatorio asociado al par $n,\ m$ con $m \geq n$.

Definimos también

$$\binom{n}{m} = 0,\ si\ m > n \qquad \text{(Convención)}$$

Hay unos pocos números combinatorios que son fácilmente calculables, estos son

$$\binom{n}{0} = \binom{0}{0} = \binom{n}{n} = 1 \quad \text{y} \quad \binom{n}{1} = \binom{n}{n-1} = n$$

Estos resultados se obtienen por aplicación directa de la definición (recordar que $0! = 1$).

Lo mismo ocurre si intercambiamos los ceros por unos, ya que $0! = 1! = 1$.

Veamos algunos ejemplos de aplicación del número combinatorio para dejar aún más claro el tema.

Ejemplo

¿Cuántos comités pueden formarse de un conjunto de 6 mujeres y 4 hombres, si el comité debe estar compuesto por 4 mujeres y 2 hombres?

Solución

¿Cómo elegimos 4 mujeres entre 6? (Sin repetición y sin tener en cuenta el orden)

$$\text{La respuesta es: de } \binom{6}{4} \text{ formas diferentes}$$

¿Cómo elegimos 2 hombres entre 4? (Sin repetición y sin tener en cuenta el orden)

$$\text{La respuesta es: de } \binom{4}{2} \text{ formas diferentes}$$

Luego, como ambas selecciones están instanciadas, es decir que ninguna depende de la otra, aplicaremos el principio de la multiplicación, para así poder saber la cantidad total de diferentes comités posibles. Entonces tenemos

$$\binom{6}{4} \cdot \binom{4}{2} \text{ posibles formas de escoger el comité}$$

Ejemplo

¿De cuántas formas distintas se pueden escoger 5 cartas de una baraja de 52 cartas?

(a) Si no hay restricciones.

(b) Si debe haber tres picas y dos corazones.

(c) Si debe haber al menos una carta de cada palo.

Solución

Una baraja de 52 cartas está dividida en cuatro palos: Picas, Corazones, Diamantes y Tréboles. Además, cada palo está formado por 13 cartas, de las cuales 9 cartas son numerales y 4 literales. Se ordenan de menor a mayor rango de la siguiente forma: A, 2, 3, 4, 5, 6, 7, 8, 9, 10, J, Q, K.

(a) Como no nos imponen ninguna condición especial (no hay restricciones), entonces solo debemos determinar cuántos subconjuntos hay con 5 elementos (las 5 cartas que debemos escoger) de un conjunto de 52 objetos (el número total de cartas de la baraja), es decir, debemos hacer una selección sin orden de 5 cartas entre 52 cartas, esto es

$$\binom{52}{5} = \frac{52!}{(52-5)! \cdot 5!}$$

(b) En este caso, debemos elegir 3 cartas entre 13 (para las picas), y la cantidad de elecciones posibles es $\binom{13}{3}$. Por otro lado, para el palo de corazones, hay $\binom{13}{2}$ formas de elegir 2 cartas entre 13. Luego, por el principio de multiplicación, el resultado es

$$\binom{13}{2} \cdot \binom{13}{2}$$

(c) Como debe haber al menos una carta de cada palo, y hay 4 palos, entonces en cada elección de 5 cartas ineludiblemente tiene que haber dos del mismo palo. bien, si fijamos el palo que se repite, hay

$$\binom{13}{2} \cdot \binom{13}{1} \cdot \binom{13}{1} \cdot \binom{13}{1}$$

formas de elegir las 5 cartas. Como hay 4 palos, tenemos un total de

$$4 \cdot \binom{13}{2} \cdot \binom{13}{1} \cdot \binom{13}{1} \cdot \binom{13}{1} = 4 \cdot 13 \cdot 6 \cdot 13 \cdot 13 \cdot 13 = 24 \cdot 13^4$$

2.5.2. Propiedades básicas y simetría del numero combinatorio

Recordando las propiedades básicas que enunciamos anteriormente

$$\binom{n}{0} = \binom{n}{n} = 1 \quad , \quad \binom{n}{1} = \binom{n}{n-1} = n \quad \text{y} \quad \binom{n}{2} = \frac{n \cdot (n-1)}{2}$$

Si pensamos combinatoricamente, es decir, en subconjuntos de X = $\{1, 2, ..., n\}$, el primer inciso se refiere a que hay un único 0-conjunto, el $\varnothing$, y un único n-conjunto: X; mientras que el segundo inciso se refiere a que hay una cantidad n tanto de 1-conjuntos (los singuletes $\{1\}, \{2\}, ..., \{n\}$), como de (n-1)-conjuntos, es decir, sus complementos $X \setminus \{1\} = \{2, 3, ..., n\}$, $X \setminus \{2\} = \{1, 3, ..., n\}$, $X \setminus \{n\} = \{1, 2, ..., n-1\}$

El principio de simetría

El fenómeno de mas arriba vale en general; es decir, un conjunto de n elementos tiene la misma cantidad de k-subconjuntos que de $(n-k)$-subconjuntos. Esto es así pues cada conjunto de k elementos determina uno de $(n-k)$ elementos, su complemento; y, recíprocamente, cada conjunto de $n-k$ es el complemento de un único subconjunto de k elementos.

Proposición

Sean m, n $\in N_0$, tal que m $\leq$ n. Entonces

$$\binom{n}{m} = \binom{n}{n-m}$$

Demostración

$$\binom{n}{n-m} = \frac{n!}{(n-(n-m))! \cdot (n-m)!} = \frac{n!}{m!(n-m)!} = \frac{n!}{(n-m)!m!} = \binom{n}{m}$$

2.5.3. Enunciado del Cálculo del número combinatorio por el triángulo de Pascal

Sean m,n $\in$ N, tal que m $\leq$ n. Entonces

$$\binom{n+1}{m} = \binom{n}{m-1} + \binom{n}{m}$$

Esta fórmula nos indica que a partir de un n, un m y su anterior $(m-1)$ podemos conocer $n+1$, es decir el siguiente número combinatorio. Esta misma fórmula nos permite calcular los coeficientes binomiales de forma recursiva y nos provee de muchas herramientas algebraicas importantes.

Veamos entonces un esquema del cálculo del triángulo de Pascal, en el que es más visible como es construido.

$$
\begin{array}{c}
C_0^0 \\
C_0^1\ C_1^1 \\
C_0^2\ C_1^2\ C_2^2 \\
C_0^3\ C_1^3\ C_2^3\ C_3^3 \\
C_0^4\ C_1^4\ C_2^4\ C_3^4\ C_4^4 \\
C_0^5\ C_1^5\ C_2^5\ C_3^5\ C_4^5\ C_5^5 \\
C_0^6\ C_1^6\ C_2^6\ C_3^6\ C_4^6\ C_5^6\ C_6^6 \\
C_0^7\ C_1^7\ C_2^7\ C_3^7\ C_4^7\ C_5^7\ C_6^7\ C_7^7 \\
\vdots \\
C_0^n\ C_1^n\ C_2^n\ C_3^n \ldots C_{n-3}^n\ C_{n-2}^n\ C_{n-1}^n\ C_n^n
\end{array}
$$

Cada término es la suma de los dos números combinatorios inmediatos superiores, por ejemplo

$$\binom{4}{2} = \binom{3}{1} + \binom{3}{2}$$

$$6 = 3 + 3$$

Veamos esto en otro gráfico a continuación.

$$
\begin{array}{ccc}
\binom{0}{0} & & 1 \\
\binom{1}{0}\ \binom{1}{1} & & 1\ \ 1 \\
\binom{2}{0}\ \binom{2}{1}\ \binom{2}{2} & \Rightarrow & 1\ \ 2\ \ 1 \\
\binom{3}{0}\ \binom{3}{1}\ \binom{3}{2}\ \binom{3}{3} & & 1\ \ 3\ \ 3\ \ 1 \\
\binom{4}{0}\ \binom{4}{1}\ \binom{4}{2}\ \binom{4}{3}\ \binom{4}{4} & & 1\ \ 4\ \ 6\ \ 4\ \ 1
\end{array}
$$

A través de este gráfico podemos observar varias propiedades del número combinatorio, pues como vemos, podemos extender esta analogía infinitamente sin embargo la propiedad de la simetría siempre se cumplirá ya que está claro que se reflejan los resultados del triángulo de Pascal con respecto a su centro. Además podemos observar que los primeros resultados no triviales del triángulo de Pascal son el $\binom{4}{2}$ y el $\binom{4}{3}$ que están en la fila 4. Por último también podemos observar que para la fila $f \geqslant 2$ el segundo y el ante-último número de la fila indican el número de fila del triángulo.

2.5.4. Teorema del binomio

En álgebra elemental aprendemos las fórmulas

$$(a+b)^2 = a^2 + 2ab + b^2 \quad \text{y} \quad (a+b)^3 = a^3 + 3a^2b + 3ab^2 + b^3$$

Pero, ¿Qué ocurre para una operación $(a+b)^n$ donde $n \geqslant 4$? Aquí entra el teorema del binomio. El resultado general de una fórmula para $(a+b)^n$ es conocido como el teorema del binomio o binomio de Newton.

Teorema

Sea n un entero positivo. El coeficiente del termino $a^{n-r}b^r$ en el desarrollo de $(a+b)^n$ es el numero binomial $\binom{n}{r}$. Explícitamente tenemos

$$(a+b)^n = \binom{n}{0}a^n + \binom{n}{1}a^{n-1}b + \binom{n}{2}a^{n-2}b^2 + ... + \binom{n}{n}b^n$$

O escrito de una forma mas concisa, si $n > 0$ y $n \in \mathbb{N}$, entonces

$$(a+b)^n = \sum_{i=0}^{n} \binom{n}{i} a^{n-i}b^i$$

Y de allí sale que el número combinatorio $\binom{n}{i}$ es llamado coeficiente binomial $\binom{n}{i}$, porque es el coeficiente i-esimo del binomio de Newton de grado n.

Observación

Los coeficientes binomiales que intervienen en la formula de $(a+b)^n$, forman una fila en el triángulo de Pascal. Veamos que

$$\binom{n}{0}\ \binom{n}{1}\ \binom{n}{2}\ ...\ \binom{n}{n-2}\ \binom{n}{n-1}\ \binom{n}{n}$$

Para por ejemplo la fórmula de $(a+b)^4$ sería

$$(a+b)^4 = \binom{4}{0}a^4 + \binom{4}{1}a^3b + \binom{4}{2}a^2b^2 + \binom{4}{3}ab^3 + \binom{4}{4}b^4$$

El teorema del binomio puede usarse para deducir identidades en que estén involucrados los números binomiales.

Ejemplo importante

Probemos que

$$\binom{n}{0} + \binom{n}{1} + \binom{n}{2} + ... + \binom{n}{n} = 2^n$$

Esto quiere decir que la cantidad de subconjuntos de un conjunto con n elementos es 2^n (Teorema antes visto).

Solución

Debemos demostrar entonces la igualdad

$$\sum_{i=0}^{n} \binom{n}{i} = 2^n$$

Caso base: probemos para el caso mínimo donde $n = 1$.

$$\sum_{i=0}^{1} \binom{n}{i} = 2^1; \quad \binom{1}{0} + \sum_{i=1}^{1} \binom{n}{i} = 2; \quad 1 + \binom{1}{1} = 2; \quad 1 + 1 = 2$$

Y es así como queda demostrado el caso base de la igualdad.

Luego, veamos que

$$\begin{aligned} 2^n &= (1+1)^n \\ &= \sum_{i=0}^{n} \binom{n}{i} \cdot 1^i \cdot 1^{n-i} \\ &= \sum_{i=0}^{n} \binom{n}{i} 1 \cdot 1 \\ &= \sum_{i=0}^{n} \binom{n}{i} \\ &= \binom{n}{0} + \binom{n}{1} + \binom{n}{2} + ... + \binom{n}{n} \end{aligned}$$

Llegamos a la igualdad buscada, por lo que queda comprobada la igualdad para todo $n \in \mathbb{N}$.

Otra fórmula es por ejemplo la suma alternada de los números binomiales $\binom{n}{i}$ hasta $\binom{n}{n}$ que da como resultado 0 y como esta, podemos hacer muchas variantes de la fórmula.

Observación

La fórmula anteriormente demostrada tiene también una interpretación combinatoria, ya que nos permite nuevamente calcular la cantidad de subconjuntos de un conjunto con n elementos, que de hecho tiene una relación con el triángulo de Pascal donde representa una fila determinada de la misma.

2.6. Ejercicios de Conteo

Realicemos algunos ejercicios para esclarecer la unidad de conteo en su totalidad y cerrar luego el tema. Veamos entonces.

Ejercicio

¿Cuántos números naturales menores que 10^5, cuyos dígitos sean todos distintos existen?

Solución

El enunciado nos pide encontrar la cantidad de números que todos los dígitos sean distintos, por lo que debemos encontrar la cantidad de números distintos de un dígito, los de 2 dígitos, de 3, 4 y 5 dígitos, ya que deben ser menores que 10^5.

Podemos comenzar razonando que los números de un dígito son todos diferentes, como deben ser números naturales, pues no tomamos el cero, entonces tenemos 9 números distintos de un dígito, a esto debemos de sumarle los de dos dígitos, que como el primer dígito de los dos no puede ser el cero y luego, en el segundo ya gastamos un dígito (selección del primer dígito), pues tendremos 9 posibles dígitos para el primero y 9 también para la segunda posición, esto nos da como resultado $9 \cdot 9$ números de 2 dígitos con todos los dígitos diferentes.

Continuando con esta analogía podemos ver que tenemos

Cantidad de dígitos	Posibles combinaciones con todos distintos
1 dígito	$9 = (1, 2, ..., 9)$
2 dígitos	$9 \cdot 9 = 81$
3 dígitos	$9 \cdot 9 \cdot 8 = 648$
4 dígitos	$9 \cdot 9 \cdot 8 \cdot 7 = 4536$
5 dígitos	$9 \cdot 9 \cdot 8 \cdot 7 \cdot 6 = 27216$

Por lo que tenemos un total de $9 + 81 + 648 + 4536 + 27216 = 32490$ posibles números menores que 10^5 y con todos sus dígitos diferentes.

Ejercicio

¿De cuántas formas diferentes pueden repartirse 5 bolas verdes, 3 rojas y 2 azules en 10 urnas distintas de forma que cada urna contenga una bola?

Solución

Podemos ver en una selección cualquiera

V	V	V	V	V	R	R	R	A	A

Que este es un problema similar a uno ya realizado, en el que permutamos letras en una palabra, si pensamos cada bola como la inicial de su color (V, R, N) podemos utilizar la misma analogía, donde tomamos los posibles cambios y restringimos la consideración del orden de una misma letra, por ejemplo

$$V_1V_2V_3V_4V_5R_1R_2R_3A_1A_2 = V_1V_2V_3V_4V_5R_1R_2R_3A_2A_1$$

Por lo que la cantidad de permutaciones totales son

$$\frac{10!}{5! \cdot 3! \cdot 2!}$$

Ejemplo

Un ascensor de un centro comercial parte del sótano con 5 pasajeros y se detiene en 7 pisos. ¿De cuántas maneras distintas pueden bajar los pasajeros? ¿Y con la condición que no baje más de uno en el mismo piso?

Solución

Si no tenemos la restricción de no poder bajar en el mismo piso, entonces cada pasajero puede bajar en 7 pisos, y como lo que haga cierto pasajero es independiente de lo que haga el resto, utilizaremos el principio de multiplicación, dando como resultado

$$7 \cdot 7 \cdot 7 \cdot 7 \cdot 7 = 7^5$$

En cambio, si cuando se baja el primero no puede bajar un segundo pasajero, a este segundo le restarán 6 opciones a elegir, al siguiente en bajar le restaran 5 opciones de elegir donde bajar y con todos los pasajeros, por lo tanto, esto es

$$7 \cdot 6 \cdot 5 \cdot 4 \cdot 3 = \frac{7!}{2!}$$

3. Divisibilidad

3.0.1. Cociente y resto

Normalmente acostumbramos a realizar una división entera obteniendo un cociente y un resto a partir de un dividendo y un divisor. Por ejemplo

Aprendemos que 6 'cabe' cuatro veces en 27 y el resto es 3, o sea que

$$27 = 6 \cdot 4 + 3$$

Un punto importante es que el resto debe ser menor que 6. Aunque también sea cierto que

$$27 = 6 \cdot 3 + 9$$

Pero si el resto es mayor que el divisor, nos indica que el número entra al menos una vez más, es decir

$$27 = 6 \cdot 3 + 6 \cdot 1 + 3 = 6 \cdot 4 + 3$$

En la división debemos tomar el menor valor para el resto de forma que 'lo que queda' sea un número no negativo lo más chico posible.

El hecho de que el conjunto de posibles 'Restos' tenga un mínimo es consecuencia del axioma de buena ordenación.

3.1. El algoritmo de división

Teorema
Sean a y b números enteros cualesquiera con b $\in$ N, entonces existen enteros únicos q y r tales que

$$a = b \cdot q + r \ y \ 0 \leq r < b$$

A la q del teorema anterior lo llamaremos el cociente de b por a.

A r lo llamaremos el resto de dividir b por a.

3.2. Conversiones de base

¿Que es una base?

Una base hace referencia a la cantidad de símbolos que contendrá nuestro sistema numérico, lo que nos indica cuantos símbolos utilizaremos antes de tener que agregar otra cifra.

Este concepto es uno de los conceptos mas importantes de la computación nos permite convertir en distintas bases los números que queremos representar y esto tiene muchas utilidades.

Por ejemplo las computadoras interpretan, procesan, responden, etcétera en binario (base 2), debido a que los únicos dos símbolos que utiliza (0 y 1) son representados en la computadora con corriente 1 si pasa/llega corriente y 0 si no ocurre, luego, a través de compuertas lógicas podremos manipular el curso del pulso (1 o 0) para lograr un determinado objetivo.

Además de base 2 (binario), existen otras bases muy utilizadas y conocidas como la base 8 (octal), la base 10(decimal) que es la base en la que nosotros representamos los números y la base 16 (hexadecimal) la cual es utilizada en diversos campos de la computación.

3.2.1. Divisiones sucesivas

Supongamos que queremos transformar un número en base 10 en cualquier otra base, pues deberemos utilizar un procedimiento que nos permita realizarlo.

Teorema

Sea $b \geqslant 2$ un número entero, llamado base para los cálculos. Para cualquier entero positivo X tenemos, por la aplicación repetida del algoritmo de división.

$$\begin{aligned} x &= b \cdot q_0 + r_0 && (0 \leqslant r_0 < b) \\ q_0 &= b \cdot q_1 + r_1 && (0 \leqslant r_1 < b) \\ &\vdots \\ q_{n-2} &= b \cdot q_{n-1} + r_{n-1} && (0 \leqslant r_{n-1} < b) \\ q_{n-1} &= b \cdot q_n + r_n && (0 \leqslant r_n < b) \end{aligned}$$

Este procedimiento se detiene en el primer $q_{n-1} < b$ y el resultado de la conversión será el número en base decimal pero convertido en una base b.

Para encontrar este nuevo número en base b debemos tomar r_n como primer cifra, continuar por r_{n-1} hasta llegar a r_0 de forma que nuestro nuevo número será de la forma

$$(r_n r_{n-1} ... r_1 r_0)_b$$

3.2.2. Representación y notación

Luego representamos X (con respecto a la base b) por la secuencia de los restos y escribimos esto de la forma

$$X = (r_n r_{n-1} ... r_1 r_0)_b$$

Podemos decir entonces que X se representa como la cadena $r_n r_{n-1} ... r_1 r_0$ en cualquier base. O también que X es representado como $X = (r_n r_{n-1} ... r_1 r_0)_b$ donde b es la base correspondiente

Convencionalmente $b = 10$ es la base con la que realizamos cálculos y omitimos poner el subíndice, es decir, de omitirse el paréntesis y el subíndice indicando la base, entonces para X con $b = 10$ tenemos que

$$1984 = (1984)_{10}$$

Observación
Los dígitos numéricos disponibles (del 0 al 9) no nos alcanzan para representar un número en base 16, pues requerirá 16 símbolos. Entonces utilizaremos algunos caracteres especiales, la convención utilizada es

$$\text{A} = 10,\ \text{B} = 11,\ \text{C} = 12,\ \text{D} = 13,\ \text{E} = 14,\ \text{F} = 15$$

3.2.3. Polinomio característico

Supongamos que ahora queremos transformar de cualquier base $b \geqslant 2$ a base 10, pues también existe un procedimiento conocido como polinomio característico y este nos dice que

Teorema
Todo número natural X se puede escribir de una única forma cómo

$$X = r_n \cdot b^n + r_{n-1} \cdot b^{n-1} + ... + r_1 \cdot b + r_0$$

Donde $0 < r_n < b$ y $0 \leqslant r_i < b$ para $i = 0, 1, ..., n-1$

Este teorema es una consecuencia importante del algoritmo de división y es el que justifica nuestro método usual de representación de números. Podemos desarrollar en potencias de b con $b \in \mathbb{N} \wedge b \geqslant 2$.

3.2.4. Conversiones de b a b' con b y b' $\neq 10$

Aprendimos como convertir un número de base 10 a cualquier base y también de una base cualquiera a base 10, pero ¿Como convertir un número de cualquier base distinta de 10 a otra distinta de 10? Pues para ello procederemos de la siguiente forma

1) Convertimos el número en base b a base 10

2) Convertimos el número en base 10 a base b'

3.2.5. Ejemplos de conversiones de base

Veamos algunos ejemplos prácticos claves para terminar de comprender el tema.

Ejemplo

Tenemos el número $(207)_2$ y queremos convertirlo en base decimal(base 10).

Solución

Debemos tener mucho cuidado, ya que a priori deberíamos aplicar el polinomio característico y convertir a base 10 el número que nos dan como consigna, pero si observamos con detenimiento este número no existe, como vemos, su subíndice nos indica que este número esta representado en base 2, pero hay un inconveniente con eso, si un número es base 2 lo que significa que se representa con solo 2 elementos (0 y 1) y como podemos ver, tenemos números inexistentes para la base binaria. Este es un error muy común.

Ejemplo

Tenemos el número 109_{10} y queremos transformarlo a base 2 es decir a N_2

Solución

Para realizar esto utilizaremos el procedimiento de divisiones sucesivas que nos permitirá realizar la conversión de base 10 a cualquier otra base, entonces dividiendo sucesivamente por 2 obtenemos

$$\begin{aligned} 109 &= 2 \cdot 54 + \mathbf{1} \\ 54 &= 2 \cdot 27 + \mathbf{0} \\ 27 &= 2 \cdot 13 + \mathbf{1} \\ 13 &= 2 \cdot 6 + \mathbf{1} \\ 6 &= 2 \cdot 3 + \mathbf{0} \\ 3 &= 2 \cdot 1 + \mathbf{0} \\ 1 &= 2 \cdot 0 + \mathbf{1} \end{aligned}$$

Luego, el resultado de la conversión es ordenar los restos de abajo hacia arriba, es decir $(109)_{10} = (1001101)_2$

Ejemplo

Tenemos el número 3428 y queremos transformarlo a base 10 es decir a N_{10}

Solución

Para realizar esto utilizaremos el procedimiento del polinomio característico que nos permitirá realizar la conversión de cualquier base a base 10, entonces tenemos

$$(342)_8 = r_2 \cdot b^2 + r_1 \cdot b + r_0 = 3 \cdot 8^2 + 4 \cdot 8 + 2 = 3 \cdot 64 + 32 + 2 = 192 + 34 = (226)_{10}$$

Los demás ejemplos con todos los posibles escenarios quedan a cargo del lector

3.3. 'Divide a'

3.3.1. Definición de 'divide a'

Dados dos enteros x e y, decimos que y es un divisor de x, y escribimos $y|x$, si:

$$x = y \cdot q \text{ para algún } q \in \mathbb{Z}$$

También decimos que y es un factor de x, que y divide a x, que x es divisible por y, y que x es múltiplo de y.

Observaciones

Es importante ver que $y|x$ NO es un número, 'divide a' es una relación donde el valor puede ser Verdadero o Falso (booleano).

Si $y|x$, es decir si y es divisor de x, existe q tal que $x = y \cdot q$. Luego q también es un divisor de x, ya que x también es $q \cdot y$

Si $y|x$, con y != 0, denotamos $\frac{x}{y}$ al cociente de x dividido y, es decir

$$x = \left(\frac{x}{y}\right) \cdot y \;\equiv\; x = y \cdot \left(\frac{x}{y}\right) + 0$$

Notación

Si y no divide a x escribimos $y \nmid x$

3.3.2. Propiedades de 'divide a'

Veamos algunas propiedades básicas de la relación 'divide a'

Sean a, b, c y q $\in \mathbb{Z}$ entonces podemos enunciar las propiedades

a) $1|a$ y $a| \pm a$;

b) $a|0$ y 0 solo divide a 0;

c) Si $a|b$, entonces $a|b \cdot c$ para cualquier c;

d) Si $a|b$ y $a|c$, entonces $a|(b + c)$;

e) Si $a|b$ y $a|c$, entonces $a|(rb + sc)$ para cualesquiera $r,\ s \in \mathbb{Z}$;

f) Si $a|(b + c)$ y $a|c$, entonces $a|b$;

g) Si $a|b$, entonces $\pm a| \pm b$

Demostraciones

Veamos las demostraciones para cada uno de las propiedades básicas anteriores.

Demostración a

Veamos que $1|a$ y $a|a$ son intuitivas y están relacionadas, pues

$$1 \cdot a = a \;\Rightarrow\; 1|a,\; a = a \cdot 1 \;\Rightarrow\; a|a,\; -a = a \cdot (-1) \;\Rightarrow\; a|-a$$

Entonces demostramos que 1 divide a a, y que a divide a $\pm a$.

Demostración b

Veamos que el único número al que puede dividir el 0 es a el mismo, y si $a|0$, a tiene que ser multiplicado por un q tal que el resultado sea 0, por ende, el q será 0 y cualquier número divide 0, ya que cualquier número cumplirá que $a \cdot 0 = 0$.

$$0 = a \cdot 0,\; \text{Si } 0|a \;\Rightarrow\; \exists\, q \text{ tal que } a = 0 \cdot q = 0$$

Demostración c

Tenemos como hipótesis que $a|b \;\Rightarrow \exists\, q$ tal que $b = a \cdot q$ y queremos demostrar que $\exists\, q'$ tal que $b \cdot c = a \cdot q'$, y para ello nos preguntamos ¿Como debería ser q'?

Está claro que por hipótesis $q' = q \cdot c \;\Rightarrow b \cdot c = a \cdot q \cdot c$, luego q' debería de ser de la forma $a \cdot q \cdot c$
Esta propiedad nos dice que si b es múltiplo de a, un múltiplo de b es múltiplo de a.

Demostración d

Tenemos como hipótesis que si $a|b$ entonces $\exists\, q$ tal que $b = a \cdot q$ y que si $a|c$ entonces $\exists\, q'$ tal que $c = a \cdot q'$ y queremos demostrar que $\exists\, t \in \mathbb{Z}$ tal que $b + c = a \cdot t$, para ello nos preguntaremos ¿Como elijo a t?

Está claro que por hipótesis $b + c = a \cdot q + a \cdot q' = a \cdot (q + q')$, por lo que t debería tener la forma $q + q'$.

Demostración e

Tenemos como hipótesis que si $a|b$ y $a|c$ entonces $\exists\, q,\; q'$ tal que $b = a \cdot q,\; c = a \cdot q'$

Luego, por hipótesis es claro que

$$\begin{aligned} rb + sc &= r \cdot (aq) + s \cdot (aq') \\ &= a \cdot (rq) + a \cdot (sq') \\ &= a \cdot (rq + sq') \end{aligned}$$

Entonces llegamos a la conclusión de que $a|rb + sc$

Demostración f

Tenemos como hipótesis que si $a|(b+c)$ y $a|c$, entonces $\exists\ q, q'$ tal que $b+c = a\cdot q,\ c = a\cdot q'$

Luego, por la propiedad e) si tomamos r = 1, s = -1, tenemos que a|(1·(b+c) + (-1)·c)

Posteriormente por la hipótesis nos queda que:

$$\begin{aligned} 1\cdot(b+c)+(-1)\cdot c &= 1\cdot(a\cdot q)+((-1)\cdot(a\cdot q') \\ 1\cdot(b+c)+(-1)\cdot c &= a\cdot q - a\cdot q' \\ (b+c)-c &= a\cdot q - a\cdot q' \\ b &= a\cdot(q-q') \end{aligned}$$

Entonces llegamos a la conclusión de que $a|b$

Demostración g

Tenemos como hipótesis que si $a|b$ entonces $\exists\ q$ tal que $b = a\cdot$ q y queremos demostrar que $\pm a| \pm b$.

Posteriormente por la hipótesis nos queda que

$$\begin{aligned} a|b \Rightarrow b = a\cdot q \Rightarrow b = (-a)\cdot(-q) &\text{ [Por regla de signos]} \Rightarrow -a|b \\ \Rightarrow -b = (a)\cdot(-q) &\text{ [Por regla de signos]} \Rightarrow \quad a|-b \\ \Rightarrow -b = (-a)\cdot(q) &\text{ [Por regla de signos]} \Rightarrow -a|-b \end{aligned}$$

3.3.3. Otras propiedades

Proposición

Sean $a,\ b \in \mathbb{Z}$, entonces podemos afirmar que

$$\text{Si } a\cdot b = 1 \ \Rightarrow\ a = b = 1 \ \vee\ a = b = -1$$

Demostración

a) Si a ∨ b valen 0, entonces a · b = 0 ≠ 1.

b) Si a > 0 ∧ b < 0 por el axioma de la compatibilidad del orden con el producto a · b < 0. Lo mismo ocurre si a < 0 ∧ b > 0

c) Si a > 0 ∧ b > 0 entonces a ⩾ 1 ∧ b ⩾ 1.
Luego, si a = 1, como a · b = 1, obtenemos 1 = a · b = 1 · b = b
Si a > 0 como b > 0 por el axioma de la compatibilidad del orden con el producto tenemos que a · b > b, es decir, 1 > b (por hipótesis), lo cual NO es cierto (b ∈ ℕ).
Por ende, queda demostrado que si a > 0 ∧ b > 0, entonces a = 1 ∧ b = 1.

d) Por último, si a < 0 ∧ b < 0, entonces -a > 0 ∧ -b > 0 ∧ (-a)·(-b) = a·b = 1.
Luego, por el enunciado de arriba, -a = -b = 1 y en consecuencia a = b = -1.

Proposición

Sean $a,\ b,\ c \in \mathbb{N}$, entonces podemos enunciar

D1) $a|a$ (Reflexividad);

D2) Si $a|b$ y $b|a$, entonces $a = b$ ó $a = -b$ (Antisimetria);

D3) Si $a|b$ y $b|c$, entonces $a|c$ (Transitividad)

Demostraciones

Veamos las demostraciones de las anteriores propiedades enunciadas

Demostración D1

Por el algoritmo de divisibilidad tenemos que

$$a = a \cdot 1 \ \Rightarrow \ a|a$$

Como vimos en la propiedad g de las propiedades básicas del 'divide a', con esta misma analogía podemos darnos cuenta que si $a|b$ entonces $\pm a| \pm b$.

Demostración D2

Veamos que se cumple la propiedad utilizando el algoritmo de la división.

Cómo $a|b \Rightarrow \exists$ q $\in \mathbb{Z}$ tal que $b = q \cdot a$

Cómo $b|a \Rightarrow \exists$ q' $\in \mathbb{Z}$ tal que $a = q' \cdot b$.

Luego, $b = q \cdot a = q \cdot (q' \cdot b) = (q \cdot q') \cdot b$.

Por el axioma de cancelación (cancelando b) obtenemos que $1 = q \cdot q'$. Por lo demostrado más arriba tenemos que, o bien $q = q' = 1$ y en consecuencia $a = b$, o bien $q = q' = -1$ y en consecuencia $a = -b$

Demostración D3

Veamos que se cumple la propiedad utilizando el algoritmo de la división y algunas de las propiedades anteriormente enunciadas.

Si $a|b \ \Rightarrow \exists$ q $\in \mathbb{Z}$ tal que $b = q \cdot a$

Si $b|c \ \Rightarrow \exists$ q $\in \mathbb{Z}$ tal que $c = q \cdot b$

Luego, $c = q' \cdot b \ \Rightarrow \ c = q' \cdot q \cdot a,\ c = a \cdot (q \cdot q')$

Entonces, es claro que $a|c$ y queda demostrada la propiedad D3

Observación

Las propiedades (D1), (D2) y (D3) nos dicen que 'divide a' es una relación de orden.

Hemos visto anteriormente que por ejemplo $\leqslant$, también es una relación de orden, sin embargo en la relación 'menor o igual que' se cumple que $a \leqslant b$ ó se cumple que $b \leqslant a$, es decir, no hay nada fuera del orden, obligatoriamente una se cumple, esto es llamado orden total, sin embargo existen otros muy estudiados que son los ordenes parciales como el 'divide a', en un orden parcial no cualquiera satisface la relación de una forma u otra, por ejemplo $2 \nmid 3 \ \wedge \ 3 \nmid 2$, es decir $a \nmid b \ \wedge \ b \nmid a$, en el orden parcial no todos los elementos están relacionados por esta relación de orden.

3.3.4. Ejemplos

Ejemplo

¿Es cierto que si $a|bc$, entonces $a|b$ ó $a|c$?

Solución

No, porque es cierto que por ejemplo $3|6 \cdot 2$ y $3|6$, pero por ejemplo $6|4.3$, sin embargo $6 \nmid 4$ y $6 \nmid 3$. (Contraejemplo)

Ejemplo

Determinar todos los divisores de 12.

Solución

Con unas pocas comprobaciones podemos ver que $1, 2, 3, 4, 6, 12$ dividen a 12, por lo tanto $\pm 1, \pm 2, \pm 3, \pm 4, \pm 6, \pm 1$ dividen a 12, es decir 12 tiene 12 divisores.

Ejemplo

Demostrar que $4^n - 1$ es divisible por 3 para todo $n \in \mathbb{N}$.

Solución

Veamos por inducción que este enunciado es verdadero.

(Caso base) $(n = 1)$ Entonces tenemos $4^1 - 1|3, \ 3|3$, lo que es verdadero y por lo tanto queda demostrada la propiedad para el caso base, ahora veamos el paso inductivo.

(Paso inductivo) Asumimos que la propiedad vale para algún k y debemos demostrarlo para algún $k+1$, entonces tenemos como hipótesis inductiva $= 3|4^k - 1$, y queremos probar (Tesis) que $3|4^{k+1} - 1$, veamos que

$$\begin{aligned} 4^{k+1} - 1 &= 4 \cdot 4^k - 1 \\ &= 4 \cdot (4^k - 1) + 4 - 1 \\ &= 4 \cdot (4^k - 1) + 3 \end{aligned}$$

Como $3|4^k - 1$ por hipótesis inductiva y $3|3$, entonces $3|n \cdot (4^k - 1) + 3$ para todo $n \in \mathbb{Z}$

3.4. Máximo común divisor

Definición

Si a y b son enteros alguno de ellos no nulo, decimos que un entero no negativo d es un máximo común divisor, o MCD, de a y b si:

a) $d|a$ y $d|b$

b) Si $c|a$ y $c|b \Rightarrow c|d$

Observaciones

La condición (a) de la definición nos dice que d es un común divisor de a y b.

La condición (b) de la definición nos dice que cualquier divisor común de a y b es también divisor de d. Y que si el divisor común de a y b, c, es mayor que 0, entonces $c \leqslant d$

Ejemplo

Queremos saber cual es el MCD entre 60 y 84 por lo que, en primer lugar, listaremos sus respectivos divisores.

- $60 = \mathbf{1},\ \mathbf{2},\ \mathbf{3},\ \mathbf{4},\ 5,\ \mathbf{6},\ 10,\ \mathbf{12},\ 15,\ 20,\ 30,\ 60$
- $84 = \mathbf{1},\ \mathbf{2},\ \mathbf{3},\ \mathbf{4},\ \mathbf{6},\ 7,\ \mathbf{12},\ 14,\ 21,\ 28,\ 42,\ 84$

Luego, seleccionaremos los divisores que tienen en común, es decir, los números que dividen a 60 y 84. Entonces:

Divisores en común: 1, 2, 3, 4, 6, 12

Luego, podríamos afirmar que 6 es un divisor pero si los analizamos detenidamente, no es el mayor de ellos ya que el 6 no satisface la propiedad b) mencionada anteriormente. Debido a que, por ejemplo, $12|60$ y $12|84$ pero $12 \nmid 6$.

Por consiguiente el divisor que cumple ambas propiedades, en este caso, es el número 12.

Puede que nos surjan ciertas preguntas como dados $a,\ b \in \mathbb{Z}$ arbitrarios, alguno de ellos no nulo ¿Existe el MCD? y ¿Cuantos MCD pueden tener un par de enteros?, esto es normal, y serán preguntas que nos ayudará a responder el teorema que enunciaremos a continuación

Teorema

Dados a y $b \in \mathbb{Z}$ y alguno de ellos no nulo, existe un único $d \in \mathbb{Z}$ que es el máximo común divisor

Notación

Sean $a,\ b \in \mathbb{Z}$, alguno de ellos no nulo, denotaremos $\text{mcd}(a,\ b)$ o $(a,\ b)$ al máximo común divisor entre a y b.

Demostración

Sin perdida de generalidad podemos suponer que $a \neq 0$. Sea:

$$S = \{m \cdot a + n \cdot b \ : \ m, n \in \mathbb{Z}, m \cdot a + n \cdot b > 0\}$$

Dónde $S =$ todas las combinaciones lineales enteras positivas de a y b.

Luego, como a o $-a \in S$, tenemos que $S \neq \varnothing$, luego, por el principio de buena ordenación, S tiene un mínimo el cuál es d.

Probaremos ahora que d es un máximo común divisor de a y b.

- La propiedad (b) nos dice que si $c|a$ y $c|b \Rightarrow c|d$. Vamos a demostrarla.
  Puesto que $d \in S$, existen $m, n \in \mathbb{Z}$ tal que $d = m \cdot a + n \cdot b$. Sea c tal que $c|a$ y $c|b$ por la propiedad que nos dice que si $a|b$ y $a|c$, entonces $a|(rb + sc)$ para cualesquiera $r, s \in \mathbb{Z}$, tenemos que $c|m \cdot a + n \cdot b$, es decir, $c|d$

- La propiedad (a) nos dice que $d|a$ y $d|b$. Vamos a demostrarla.
  Supongamos que $d \nmid a$, entonces $|a| = q \cdot d + r$ con $0 < r < d$ y $q \geqslant 0$.
  Entonces, $r = \pm a - q \cdot d$, $r = \pm a - q \cdot (m \cdot a + n \cdot b)$, $r = a(\pm 1 - q \cdot m) + (-q \cdot n) \cdot b$.
  Por lo tanto, $r < d \in S$, contradiciendo la hipótesis de que d es un mínimo de S. La contradicción vino de suponer que $d \nmid a$, por lo tanto $d|a$.
  Análogamente podemos probar que $d|b$.

- Unicidad. Vamos a demostrar que d es único.
  Sean d y d' dos enteros no negativos que satisfacen las propiedades del MCD, como $d'|a$ y $d'|b$ y d satisface la propiedad (b) de la definición de MCD, se deduce que $d|d'$.
  Intercambiando los papeles de d y d' se obtiene que $d'|d$. Luego, como $d, d' \geqslant 0$ por la propiedad de la antisimetria se obtiene que $d = d'$.

Ejemplo

Se quiere hallar el MCD del par de enteros $(174, 72)$

Solución

Veamos entonces de la forma que hasta ahora hemos visto, esto es viendo los divisores de ambos y luego los divisores comunes. Entonces

Divisores de 174: **1**, **2**, **3**, **6**, 29, 58, 87, 174

Divisores de 72: **1**, **2**, **3**, 4, **6**, 8, 9, 12, 18, 24, 36, 72

Entonces veamos que los divisores comunes son: 1, 2, 3, 6

Luego, 6 es divisor común de 174 y 72, y todos los demás divisores comunes (1, 2, 3) dividen a 6, por lo tanto $\text{mcd}(174, 72) = 6$

Pero nos preguntamos ¿Es esta una forma eficiente de calcular el MCD? Vemos que manualmente y en números pequeños esta es una forma muy intuitiva, sin embargo esto no es para nada eficiente cuando aumentamos un poco la cantidad de cifras de los números, y es una forma muy costosa computacionalmente hablando, de hecho este calculo manual como lo realizamos sería **imposible** de realizar en números más grandes.

Proposición

Sean a y $b \in \mathbb{Z}$ y alguno de ellos no nulo. Entonces existen $s, t \in \mathbb{Z}$ tal que.

$$(a,\ b) = s \cdot a + t \cdot b$$

Observación

Esta proposición nos dice que el mcd$(a,\ b)$ es una combinación lineal entera de a y b.

Demostración

La demostración de esta proposición es consecuencia inmediata de la demostración del teorema anterior.

Corolario

Sean a y $b \in \mathbb{Z}$ y b no nulo, entonces

$$(a,\ b) = 1 \Leftrightarrow \exists\ s,\ t \in \mathbb{Z} \text{ tales que } 1 = s \cdot a + t \cdot b$$

Demostración

Tenemos que $d = \text{mcd}(a,\ b) \Rightarrow d = s \cdot a + t \cdot b$ y queremos probar que si $(a,\ b) = 1 \Leftrightarrow 1 = s \cdot a + t \cdot b$ (para algunos s y t), entonces veamos que

$$(a,\ b) = 1 \Rightarrow \text{por } (a)\ 1 = s \cdot a + t \cdot b$$

Luego, si hacemos la vuelta $(\Leftarrow)\ 1 = s \cdot a + t \cdot b$. Sea $d \cdot a$ y $d \cdot b \Rightarrow d | s \cdot a + t \cdot b \Rightarrow d | 1 \Rightarrow d = 1$.

En conclusión el único divisor común de a y b es 1.

3.4.1. Enteros coprimos

Definición

Que un entero sea coprimo con otro entero, significa que no comparten factores primos, es decir que el único divisor común que tienen es el 1 o el -1. Con esto podemos confirmar que si el mcd$(a,\ b) = 1$, entonces decimos que a y b son coprimos.

Observaciones

(a) Por el corolario del teorema anterior $p,\ q$ coprimos $\Leftrightarrow$ existen $s,\ t \in \mathbb{Z}$ tales que $1 = s \cdot a + t \cdot b$

(b) NO es cierto que si existen $s,\ t \in \mathbb{Z}$ tales que $d = s \cdot a + t \cdot b \Rightarrow d = \text{mcd}(a,\ b)$ (solo si $d = 1$). Por ejemplo $4 = 2 \cdot 6 + 2 \cdot (-4)$ y mcd$(6,\ 4) = 2$

3.4.2. Propiedades básicas del MCD

Veamos algunas de las propiedades más sencillas del MCD.

a) $\text{mcd}(b,\ a) = \text{mcd}(a, b) = \text{mcd}(\pm a,\ \pm b)$

b) Si $a > 0,\ \text{mcd}(a,\ 0) = a$ y $\text{mcd}(a,\ a) = a$

c) $\text{mcd}(1,\ b) = 1$

d) Si $a \nmid 0,\ b\ \in\ \mathbb{Z}$, entonces $\text{mcd}(a,\ b) = \text{mcd}(a,\ b - a)$

Demostración a

Sea d = $\text{mcd}(a,\ b)$ que cumple con la definición de MCD, tenemos que:

a) $d|a$ y $d|b$

b) Si $c|a$ y $c|b \Rightarrow c|d$

Luego sea d' = $\text{mcd}(b,\ a)$ que cumple con la definición de MCD, tenemos que:

a') $d'|b$ y $d'|a$

b') Si $c|b$ y $c|a \Rightarrow c|d'$

Vamos a probar que $d = d'$

- Por (a) tenemos que $d|a \wedge d|b \Rightarrow d|b \wedge d|a$ (trivialmente por conmutatividad del $\wedge$) $\Rightarrow$ Por (b') $d|d'$
- Por (a') tenemos que $d'|b \wedge d'|a \Rightarrow d'|a \wedge d'|b$ (trivialmente por conmutatividad del $\wedge$) $\Rightarrow$ Por (b) $d'|d$
- Por último, si $d, d' \geqslant 0$ y $d|d' \wedge d'|d \Rightarrow d = d'$

Demostración b

Siendo $a > 0$ para demostrar que $\text{mcd}(a,\ 0) = a$ comprobamos que a cumple con la definición de MCD.

a) $a|a$ y $a|0$

b) Si $c|a$ y $c|0$ entonces $c|a$

Para el siguiente caso, haremos el mismo procedimiento.
Siendo $a > 0$, $\text{mcd}(a,\ a) = a$ si a cumple con la definición de MCD.

a) $a|a$ y $a|a$

b) Si $c|a$ y $c|a$ entonces $c|a$

Demostración c

Para demostrar que $\text{mcd}(1,\ b) = 1$ comprobamos que 1 cumple con la definición de MCD

a) $1|1$ y $1|b$

b) Si $c|1$ y $c|b$ entonces $c|1$

Demostración d

Sea $d = \text{mcd}(a,\ b)$, luego:

a) $d|a$ y $d|b$

b) $c|a$ y $c|b$ entonces $c|d$

Y queremos probar que:

a') $d|a$ y $d|b-a$

b') $c|a$ y $c|b-a$ entonces $c|d$

Por (a), $d|a$ y $d|b \Rightarrow d|b-a$ (a')

Si $c|a$ y $c|b-a \Rightarrow c|a+(b-a)=b \Rightarrow$ (b) $c|d \Rightarrow$ (b')

Esta última propiedad (propiedad D) nos permitirá encontrar el MCD de una forma diferente que es algo más eficiente pero sigue sin ser la mejor opción.

Veamos un ejemplo en el que aplicamos sucesivamente esta última propiedad.

Ejemplo

Encontrar el MCD entre el par de números(72, 174).

Solución

$$\begin{aligned}
\text{mcd}(72,\ 174) &= (72,\ 174-72) = (72,\ 102)\\
&= (72,\ 102-72) = (72,\ 30)\\
&= (30,\ 72)\\
&= (30,\ 72-30) = (30,\ 42)\\
&= (30,\ 42-30) = (30, 12)\\
&= (12,\ 30)\\
&= (12,\ 30-12) = (12,\ 18)\\
&= (12,\ 18-12) = (12,\ 6)\\
&= (6,\ 12)\\
&= (6,\ 12-6) = (6,\ 6)\\
&= 6
\end{aligned}$$

Vemos que esto es algo un poco más simple y eficiente ya que no necesitamos hallar los divisores de los números, cosa que no es sencilla con números grandes.

La próxima proposición nos provee de una herramienta aún mejor para calcular el MCD.

Proposición

Sean $a,\ b$ enteros no negativos con $b \neq 0$, entonces

$$a = b \cdot q + r \ \Rightarrow \ \text{mcd}(a,\ b) = \text{mcd}(b,\ r)$$

Observación

La proposición anterior nos dice que $(a,\ b)$ tiene los mismos divisores que $(b,\ r)$

Idea de la demostración

Para demostrar esto debemos observar que si c divide a a y b, entonces también divide a $a - b.q$;y como $a - b.q = r$, tenemos que $c|r$. De este modo cualquier divisor común de a y b es también divisor común de b y r. Por otro lado, si c divide a b y r también divide a $a = b.q + r$.
Es decir, c es divisor común de a y b si y solo si c es divisor común de b y r (*).
Luego, sea d =mcd(a, b) probaremos que d es el mcd entre b y r

a) Como $d|a$ y $d|b$, entonces por (*) tenemos que $d|b$ y $d|r$

b) Si $c|a$ y $c|r$ entonces por (*) $c|a$ y $c|b$ y debido a que d =mcd(a, b), se deduce que $c|d$

Entonces, con el mismo ejemplo veamos el algoritmo

Ejemplo

Encontrar el MCD entre el par de números(72, 174).

Solución

Veamos que utilizando el algoritmo anteriormente enunciado podemos simplificar varios pasos

$$\begin{aligned}
174 = 72 \cdot 2 + 30 \ &\Rightarrow \ (124,\ 72) = (72,\ 30) \\
72 = 30 \cdot 2 + 12 \ &\Rightarrow \ (72,\ 30) \ = (30,\ 12) \\
30 = 12 \cdot 2 + 6 \ &\Rightarrow \ (30,\ 12) \ = (12,\ 6) \\
12 = 6 \cdot 2 + 0 \ &\Rightarrow \ (12,\ 6) \ = (6,\ 0) = 6
\end{aligned}$$

Este algoritmo es conocido como algoritmo de Euclides, está basado en el algoritmo de la división, el mismo es muy importante y de hecho es el más eficiente para hallar el MCD entre dos números.

3.4.3. Algoritmo de Euclides

Para calcular el MCD de enteros a y b, con $b > 0$, definimos q_i y r_i recursivamente de la forma $r_0 = a,\ r_1 = b$, y

$$\begin{array}{lrcll} \text{(e1)} & r_0 & = & r_1 \cdot q_1 + r_2 & (0 < r_2 < r_1) \\ \text{(e2)} & r_1 & = & r_2 \cdot q_2 + r_3 & (0 < r_3 < r_2) \\ & \vdots & & & \\ \text{(ei)} & r_{i-1} & = & r_i \cdot q_i + r_{i+1} & (0 < r_{i+1} < r_i) \\ & \vdots & & & \\ \text{(ek)} & r_{k-1} & = & r_k \cdot q_k + 0 & \end{array}$$

Este algoritmo nos provee del MCD de dos números arbitrarios, de forma rápida y eficiente. Esta es la formalización de los ejemplos anteriores. El algoritmo consta en la repetición del algoritmo de la división teniendo en cuenta la propiedad de si $a \neq 0,\ b \in \mathbb{Z} \ \Rightarrow\ (a,\ b) = (a,\ b-a)$ hasta llegar a $\text{mcd}(a,\ 0)$, donde frenamos y sabremos que entonces el mcd es a.

Entonces $r_k = \text{mcd}(a,\ b)$ #último resto no nulo

- El proceso se detiene en el primer resto r_i igual a 0
- El proceso debe detenerse, porque cada resto no nulo es positivo y estrictamente menor que el anterior.

Teorema
Sean a y b enteros con $b > 0$, entonces el máximo común divisor es el último resto no nulo obtenido en el algoritmo de Euclides (r_k).

Idea de la demostración

$$r_{i-1} = r_i \cdot q_i + r_{i+1} \ \Rightarrow\ \text{mcd}(r_{i-1},\ r_i) = \text{mcd}(r_i,\ r_{i+1})$$

- El algoritmo de Euclides es fácilmente implementable en un lenguaje de programación.

Recordemos la proposición que dice que Sean $a,\ b \in \mathbb{Z}$, uno de ellos no nulo, entonces $d = s \cdot a + t \cdot b$.
Entonces para calcular s y t en el caso que $b > 0$, la ecuación (ei) es

$$r_{i-1} = r_i \cdot q_i + r_{i+1}$$

Esto implica que

$$r_{i+1} = r_{i-1} - r_i \cdot q_i$$

Lo que nos dice que r_i puede ser calculado usando r_{i-1} y r_{i-2}, luego

$$\begin{aligned} r_k &\text{ puede ser calculado con } r_{k-1} \text{ y } r_{k-2} \\ r_{k-1} &\text{ puede ser calculado con } r_{k-2} \text{ y } r_{k-3} \\ &\vdots \\ r_3 &\text{ puede ser calculado con } r_2 \text{ y } r_1 \\ r_2 &\text{ puede ser calculado con } r_1 = b \text{ y } r_0 = a \end{aligned}$$

Veamos un ejemplo utilizando esta conclusión anterior para calcular s y t

Ejemplo

Encontrar d, el MCD entre 174 y 72 y escribir $d = s \cdot 174 + t \cdot 72$

Solución

Procedemos a encontrar primero el MCD entre a y b utilizando el algoritmo de Euclides

$$\begin{aligned} &\text{(e1)} \quad 174 = 72 \cdot 2 + 30 \;\Rightarrow\; (124,\ 72) = (72,\ 30) \\ &\text{(e2)} \quad 72 = 30 \cdot 2 + 12 \;\Rightarrow\; (72,\ 30) = (30,\ 12) \\ &\text{(e3)} \quad 30 = 12 \cdot 2 + 6 \;\Rightarrow\; (30,\ 12) = (12,\ 6) \\ &\text{(e4)} \quad 12 = 6 \cdot 2 + 0 \;\Rightarrow\; (12,\ 6) = (6,\ 0) = 6 \end{aligned}$$

Luego para calcular s y t tal que $6 = s \cdot 174 + t \cdot 72$ debemos ir despejando para encontrar la ecuación, entonces

$$\begin{aligned} 6 &= 30 - 12 \cdot 2 = 30 - 2 \cdot (72 - 30 \cdot 2) \\ &= 30 + (-2) \cdot 72 + 4 \cdot 30 = 5 \cdot 30 + (-2) \cdot 72 \\ &= 5 \cdot (174 - 72 \cdot 2) + (-2) \cdot 72 \\ &= 5 \cdot 174 + (-10) \cdot 72 + (-2) \cdot 72 \\ &= 5 \cdot 174 + (-12) \cdot 72 \end{aligned}$$

Entonces encontramos s y t que valen 5 y -12 respectivamente.

3.5. Mínimo común múltiplo

Definición

Si a y $b \in \mathbb{Z}$ decimos que un entero no negativo m es el mínimo común múltiplo, o mcm, de a y b si

a) $a|m$ y $b|m$;

b) si $a|n$ y $b|n$ entonces $m|n$

La condición (a) nos dice que m es múltiplo común de a y b, y la condición (b) nos dice que cualquier otro múltiplo de a y b también debe ser múltiplo de m.

Ejemplo

Se quiere encontrar el mcm$(8,\ 14)$.
Escribamos los múltiplos de ambos números y busquemos el menor común a ambos.
Listemos los primeros múltiplos de ambos hasta encontrar el primero en común

- Múltiplos de 8: 8, 16, 24, 32, 40, 48, 56
- Múltiplos de 14: 14, 28, 42, 56, 72,

Luego se tiene que mcm$(8,\ 14) = 56$, es decir el mínimo que tienen en común. Los siguientes en común son múltiplos del mínimo común, $112 = 56 \cdot 2,\ 168 = 56 \cdot 3,\ \ldots$

Nos faltaría comprobar que cualquier múltiplo común de 8 y 14 es múltiplo de 56, pero eso se deduce fácilmente de los resultados que veremos a continuación.

3.5.1. Relación entre MCD y mcm

Teorema

Sean a y b enteros no nulos, entonces decimos:

$$mcm(a,b) = \frac{ab}{mcd(a,b)}$$

En particular este resultado implica que si a y b son enteros coprimos, entonces $mcm(a,b) = a \cdot b$

Demostración

Demostraremos que

$$m = \frac{a \cdot b}{\text{mcd}(a,b)}$$

Es el mínimo común múltiplo de a y b

Luego, como

$$m = \frac{a \cdot b}{\text{mcd}(a,b)} = \frac{a}{\text{mcd}(a,b)} \cdot b = a \cdot \frac{b}{\text{mcd}(a,b)}$$

Resulta que m es múltiplo de a y b, y por lo tanto se satisface la propiedad (a) de la definición MCM.

Veamos ahora que sucede respecto a la propiedad (b): Sea $n \in \mathbb{Z}$ tal que $a|n$ y $b|n$. Como existen enteros r y s tales que:

$$\text{mcd}(a,b) = r \cdot a + s \cdot b$$

Dividiendo esta ecuación por $\text{mcd}(a,b)$ y multiplicando por n, obtenemos la siguiente ecuación:

$$n = r \cdot \frac{a}{\text{mcd}(a,b)} \cdot n + s \cdot \frac{b}{\text{mcd}(a,b)} \cdot n$$

Escribiendo $n = b' \cdot b = a' \cdot a$ con $a', b' \in \mathbb{Z}$ y haciendo los reemplazos en la ecuación anterior, resulta finalmente.

$$n = r \cdot b' \frac{a \cdot b}{\text{mcd}(a,b)} \cdot n + s \cdot a' \cdot \frac{b \cdot a}{\text{mcd}(a,b)} \cdot n = \frac{a \cdot b}{\text{mcd}(a,b)} \cdot (r \cdot b' + s \cdot a')$$

En particular este resultado implica que si a y b son enteros coprimos, entonces $\text{mcm}(a,b) = a \cdot b$
Retomando entonces el ejemplo anterior veamos que

Solución

$$\begin{aligned} 14 &= 8 \cdot 1 + 6 \\ 8 &= 6 \cdot 1 + 2 \\ 6 &= 2 \cdot 2 + 2 \\ 2 &= 2 \cdot 1 + 0 \end{aligned}$$

Es claro entonces que $\text{mcd}(8,\ 14) = 2$, luego $\text{mcm}(8,\ 14) = \frac{8 \cdot 14}{2} = 56$

Ejemplo

Demostrar que si $a,\ b$ y n son enteros no nulos, entonces mcd$(na, nb) =$ n $\cdot$mcd$(a,\ b)$

Solución

Sea $d = (a, b)$, debemos probar que $n.d = (n.a, n.b)$

a) $d|a$ y $d|b$

b) Si $c|a$ y $c|b \Rightarrow c|d$

$\Downarrow$

a') $n.d|n.a$ y $n.d|n.b$

b') $c|n.a$ y $c|n.b \Rightarrow c|n.d$

a') Reescribiendo, por (a) tenemos $a = d.q_1$ y $b = d.q_2$
Luego, $n.a = d.q_1$ y $n.b = d.q_2$, es decir, $n.d|n.a$ y $n.d|n.b$

b') Sea c tal que $c|n.a$ y $c|n.b$
Ahora bien $d = r.a + s.b \Rightarrow n.d = s.(n.a) + t.(n.b)$
Luego, $c|n.a$ y $c|n.b \Rightarrow c|s.(n.a) + t.(n.b) = n.d$
Esto prueba b')

3.6. Factorización prima

3.6.1. Número primo

Definición

Se dice que un entero positivo p es primo si $p \geqslant 2$ y los únicos enteros positivos que dividen p son 1 y el mismo.

Luego, un entero $m \geqslant 2$ no es un primo si y solo si existe m_1 divisor de m tal que $m_1 \neq 1,\ m$, es decir, con $1 < m_1 < m$. Sea m_2 el cociente de m por m_1: es claro que $m_2 \neq 1,\ m$ y por lo tanto $1 < m_2 < m$. Concluyendo.

Un entero $m \geqslant 2$ no es un primo si y sólo si $m = m_1 \cdot m_2$ donde m_1 y m_2 son enteros estrictamente entre 1 y m.

De acuerdo a la definición de número primo, 1 NO es primo.

Veremos que todo número entero positivo puede expresarse como producto de primos. Por ejemplo

$$825 = 3 \cdot 5^2 \cdot 11$$

Conocemos que 3, 5 y 11 son números primos.

Si el entero es negativo, es (-1) por un producto de primos. Con el mismo ejemplo podemos verlo

$$-825 = (-1) \cdot 3 \cdot 5^2 \cdot 11$$

Teorema

Todo entero mayor que 1 es producto de primos. También consideramos los números primos como producto de primos.

Idea de la demostración

Consideremos el conjunto B como

$$B = \{n > 1 \ : \ n \text{ No es producto de primos}\}$$

- Si $B \neq 0$, por buena ordenación existe m mínimo de B
- m no es primo, entonces $m = m_1 \cdot m_2$ con $1 < m_1,\ m_2 < m$
- Como $m_1,\ m_2 < m$, ambos son productos de primos.
- Luego $m_1 \cdot m_2 = m$ es producto de primos. Lo cual es ABSURDO

Que m sea producto de primos y a la vez sea parte de los que no son producto de primos es un absurdo y el absurdo es resultado de suponer que $B = \varnothing$

Observación
Por el teorema, decimos que todo $\mathbb{Z} > 1$ admite una factorización con factores primos.

Ejemplo
Encontrar la factorización en números primos de 201000.

Solución
Esto se hace dividiendo sucesivamente los números hasta llegar a factores primos.

$$\begin{aligned} 201000 &= 201 \cdot 1000 \\ &= 3 \cdot 67 \cdot 10 \cdot 10 \cdot 10 \\ &= 3 \cdot 2 \cdot 5 \cdot 2 \cdot 5 \cdot 2 \cdot 5 \cdot 67 \\ &= 2^3 \cdot 3 \cdot 5^3 \cdot 67 \end{aligned}$$

Sabemos que 2,3,5 y 67 son primos y por lo tanto hemos obtenido la descomposición en primos de 201000

Dato: En criptografía los números primos son muy utilizados, pues muchos algoritmos de protección de transacciones se basan en que es difícil descomponer números grandes en factores primos.

Observación
Sea $a \in \mathbb{Z}$ y p primo, entonces

a) Si $p \nmid a$, entonces $\text{mcd}(a,\ p) = 1$ (coprimos)

Demostración
Sea $d = \text{mcd}(a,\ p) \ \Rightarrow\ d|a \ \wedge\ d|p \ \Rightarrow$ si $d|p,\ d = 1$ ó $d = p \ \Rightarrow$ si $p \nmid a,\ d = 1$

b) Si p y p' son primos y $p|p'$ entonces $p = p'$

Demostración

$$p|p' \ \Rightarrow\ p = 1 \text{ ó } p = p' \ \Rightarrow\ \text{Si } p \text{ es primo}, p \neq 1 \ \Rightarrow\ p = p'$$

¿Cómo determinamos si un número es o no es primo? Dijimos que una forma de verlo es probar con todos los divisores, pero hay una forma más corta de realizarlo probando solo con algunos divisores. El lema nos dice que

Lema (Este lema nos permite establecer el criterio de la raíz).
Si $n > 0$ no es primo, entonces existe $m > 0$ tal que $m|n$ y $m \leqslant \sqrt{n}$ (si no es primo, existe divisor $\leqslant \sqrt{n}$).

Demostración

Como n no es primo $\Rightarrow\ n = m_1 \cdot m_2$ con $1 < m_1,\ m_2 < n$

Supongamos que $m_1,\ m_2 > \sqrt{n}\ \Rightarrow\ n = m_1 \cdot m_2 > \sqrt{n} \cdot \sqrt{n}$

$$n > \sqrt{n}^2 = n > n \ \textit{ABSURDO}$$

Luego, o $m_1 \leqslant \sqrt{n}$ o $m_2 \leqslant \sqrt{n}$ Ya que el absurdo vino de suponer que $m_1 > \sqrt{n}$ y $m_2 > \sqrt{n}$ por esto, uno de ellos es menor.

El contrarrecíproco del lema anterior, es el criterio de la raíz. Contrarrecíproco: $P \Rightarrow Q\ \equiv\ \neg Q \Rightarrow \neg P$

Proposición

Sea $n \geqslant 2$. Si para todo m tal que $1 < m \leqslant \sqrt{n}$ se cumple que $m \nmid n$, entonces n es primo.

Corolario

Sea $n \geqslant 2$. Si para todo p primo tal que $1 < p \leqslant \sqrt{n}$ se cumple que $p \nmid n$, entonces n es primo.

Ejemplo

Verifiquemos si 467 es primo o no.

Solución

Si no utilizamos el criterio de la raíz deberíamos hacer 465 divisiones: deberíamos comprobar si $m|467$ con $1 < m < 467$

Pero por el criterio de la raíz y como $\sqrt{467} = 21,61...$ solo debemos comprobar si $m|467$ para $2 \leqslant m \leqslant 21$ (20 comprobaciones). Una sencilla comprobación muestra que los números 2,3,...,20,21 no dividen a 467 y por lo tanto 467 es primo. Pero, por el corolario, podríamos comprobar solo si los primos menores e iguales a $\sqrt{n}$ dividen a 467 y ver así que 467 es primo. (8 comprobaciones)

Teorema

Sea p un numero primo

a) Si $p|ab$ entonces $p|a$ o $p|b$

b) $a_1, a_2, ..., a_n$ son enteros tales que $p|a_1a_2...a_n$

Entonces p$|a_i$ para algún a_i $(1 \leq$ i $\leq$ n).

Demostración a

Se tiene que p es primo y $p|a \cdot b$ (hipótesis) y queremos demostrar que $p|a$ ó $p|b$.
Cómo p es primo $\text{mcd}(p, a) = 1$ ó p.
Si $\text{mcd}(p,\ a) = p \Rightarrow p|a$.
Si $\text{mcd}(p,\ a) = 1 \Rightarrow$ (por propiedad de MCD) $\Rightarrow 1 = s \cdot p + t \cdot a$.
Luego, multiplico esa expresión por b y nos queda

$$b = s \cdot p \cdot b + t \cdot a \cdot b$$

Cómo $p|p$ y $p|a \cdot b$, por la hipótesis, $\Rightarrow p|(s \cdot y) \cdot p + t \cdot (a \cdot b) = y$, es decir, $p|y$.

Demostración b

Para demostrar esta propiedad usaremos el principio de inducción.

- Caso Base: Para $n = 1$ el resultado es obviamente verdadero.
- Caso Inductivo: Supongamos que el resultado es verdadero para $n = k$, es decir $p|a_1a_2...a_k$, entonces $p|a_i$ para algún i con $1 \leqslant$ i $\leqslant$ k (Hipótesis Inductiva)
- Supongamos $p|a_1a_2...a_k.a_{k+1}$ y sea $a = a_1.a_2, ..., a_k$.
- Si $p|a$ entonces por la hipótesis inductiva $p|a_i$ para algún a_i en el rango de $1 \leqslant$ i $\leqslant$ k.
- Si $p \nmid a$ entonces, por la propiedad (a) se sigue que $p|a_{k+1}$. De este modo, en ambos casos p divide a uno de los a_i ($1 \leqslant$ i $\leqslant$ k+1.)

Observaciones

La propiedad (a) es muy importante y podríamos definir número primo como aquel número que cumple esta propiedad.

Un error común es asumir que la propiedad (a) se mantiene verdadera cuando reemplazamos el primo p por un entero arbitrario pero esto claramente es falso. Por ejemplo

$$6|3 \cdot 8 \text{ pero } 6 \nmid 3 \text{ y } 6 \nmid 8$$

La propiedad (a) juega un papel crucial en la demostración del siguiente enunciado que es llamado el teorema fundamental de la aritmética.

3.6.2. Teorema fundamental de la aritmética

Teorema

Comúnmente conocido como el teorema fundamental de la aritmética, este teorema establece que la factorización en primos de un entero positivo $\geqslant 2$ es única, salvo el orden de los factores primos.

Luego todo entero positivo n puede escribirse como un único producto de primos (no necesariamente distintos) de la forma

$$m = q_1 \cdot q_2 \cdot ... \cdot q_{m-1} \cdot q_m$$

En la práctica a menudo reunimos los primos iguales en la factorización y escribimos

$$n = {p_1}^{e_1} \cdot {p_2}^{e_2} \cdot {p_3}^{e_3} \cdot ... \cdot {p_r}^{e_r}$$

Donde $p_1, p_2, ..., p_r$ son primos distintos y $e_1, e_2, ..., e_r$ son enteros positivos que indican la cantidad de repeticiones de ese número primo.

Demostración

Por el axioma del buen orden, si existe un entero para el cual el teorema es falso, entonces hay un entero mínimo $n0 \geqslant 0$ con esta propiedad. Supongamos entonces que:

$$n_0 = p_1.p_2, ..., p_k \qquad y \qquad n_0 = p'_1.p'_2, ..., p'_f$$

En donde los p_k $(1 \leqslant i \leqslant k)$ son primos, no necesariamente distintos, y los p'_f $(1 \leqslant i \leqslant f)$ son primos, no necesariamente distintos.
La primera ecuación implica que $p_1 | n_0$ y la segunda ecuación implica que $p_1 | p'_1.p'_2, ..., p'_f$. Por la propiedad (b) del teorema anterior tenemos que $p_1 | p'_j$ para algún $(1 \leqslant j \leqslant f)$.
Reordenando la segunda factorización podemos asumir que $p_1 | p'_1$ y puesto que p_1 y p'_1 son primos, se sigue que , por propiedad, $p_1 = p'_1$.
Luego por el axioma de la cancelación, podemos cancelar los factores p_1 y p'_1, y obtener:

$$p_2.p_3, ..., p_k = p'_2.p'_3, ..., p'_f$$

Y llamemos a esto n_1. Pero supusimos que n_0 tenía dos factorizaciones diferentes, y hemos cancelado el mismo número $(p_1 = p'_1)$ en ambas factorizaciones, luego n_1 tiene también dos factorizaciones diferentes.
Esto contradice la definición de n_0 como el mínimo entero sin factorización única.
Por lo tanto el teorema es verdadero para $n \geqslant 2$.

Ejemplo

Encontrar la descomposición prima de 7000

Solución

Entonces tenemos que

$$\begin{aligned} 7000 &= 1000 \cdot 7 \\ &= 7 \cdot 10 \cdot 10 \cdot 10 \\ &= 7 \cdot 2 \cdot 5 \cdot 2 \cdot 5 \cdot 2 \cdot 5 \end{aligned}$$

Entonces encontramos que $7000 = 7 \cdot 2 \cdot 5 \cdot 2 \cdot 5 \cdot 2 \cdot 5$ pero suele ser más conveniente escribirlo como $7000 = 2^3 \cdot 5^3 \cdot 7$

Proposición

Existen infinitos números primos

Demostración

Haremos la demostración por el absurdo. Asumamos que existen finitos números primos.

Sean $p_1, p_2, ..., p_r$ todos los números primos (finitos)

Sea p primo tal que $p|n \Rightarrow$ existe i tal que $p = p_i$

Sea $n = p_1, p_2, ..., p_r + 1$

Ahora bien $p_i|n$ y $p_i|p_1, p_2, ..., p_r$, luego $p_i|n - p_1, p_2, ..., p_r = 1$

Entonces $p_i|1$. Absurdo

El absurdo viene de suponer que hay finitos números primos y es por ello que queda demostrado que hay infinitos primos.

Ejemplo importante

Probemos que si m y n son enteros tal que $m \geqslant 2$ y $n \geqslant 2$, entonces $m^2 \neq 2 \cdot n^2$

Demostración

$$\begin{aligned} &(\text{Entero pos } \geqslant 2) \quad n = 2^x \cdot {p_2}^{e_2} \cdot ... \cdot {p_r}^{e_r} \quad (p_i \text{ todos primos distintos de } 2) \\ &\qquad \Rightarrow \; n^2 = 2^{2x} \cdot {p_2}^{2e_2} \cdot ... \cdot {p_r}^{2e_r} \qquad (a \cdot b)^n = a^n \cdot b^n \;\wedge\; (a^n)^m = a^{n \cdot m} \\ &(*) \quad \Rightarrow \; 2 \cdot n^2 = 2^{2x+1} \cdot {p_2}^{2e_2} \cdot ... \cdot {p_r}^{2e_r} \qquad a^n \cdot a^m = a^{n+m} \end{aligned}$$

$$\begin{aligned} &\text{y } m = 2^y \cdot {q_2}^{f_2} \cdot ... \cdot {q_s}^{f_s} \quad (q_i \text{ todos los primos distintos de } 2) \\ &(**) \qquad m^2 = 2^{2y} \cdot {q_2}^{2f_2} \cdot ... \cdot {q_s}^{2f_s} \end{aligned}$$

Por unicidad de la descomposición, $(*) \neq (**)$, es decir $m^2 \neq n^2 \;\Leftarrow\; 2^{2x+1} \neq 2^2$

Estos no son iguales y demuestra que solo hay una forma de descomponer números en factores primos.

Observación

El ejemplo anterior nos dice que

$$m^2 \neq 2 \cdot n^2 \;\Rightarrow\; \frac{m^2}{n^2} \neq 2 \;\Rightarrow\; \left(\frac{m}{n}\right)^2 \neq 2 \;\Rightarrow\; \frac{m}{n} \neq \sqrt{2}$$

Es decir, $\sqrt{2}$ no es un número racional.

Notación

Sean m y n dos enteros positivos, a veces es conveniente escribir la factorización prima de ambos números usando los mismos primos. Los primos que usamos son los que se encuentran en la factorización prima de alguno de los dos, o de ambos, de la forma

$$m = {p_1}^{e_1} \cdot {p_2}^{e_2} \cdot ...{p_r}^{e_r}, \qquad n = {p_1}^{f_1} \cdot {p_2}^{f_2} \cdot ...{p_r}^{f_r}$$

Con $e_i,\ f_i \geqslant 0$ para $i = 1, ..., r$ y e_i o/y f_i distinto de cero.

Ejemplo

Veamos la factorización prima de 168 y 495

Solución

Tras ejecutar el procedimiento que acostumbramos, vemos que

$$168 =, \qquad 495 = 3^2 \cdot 5^1 \cdot 11^1$$

Luego, por la notación que hemos visto conveniente anteriormente, expresamos esto como

$$168 = 2^3 \cdot 3^1 \cdot 5^0 \cdot 7^1 \cdot 11^0;$$
$$495 = 2^0 \cdot 3^2 \cdot 5^1 \cdot 7^0 \cdot 11^1$$

Veremos ahora un resultado que se puede deducir fácilmente del teorema fundamental de la aritmética (TFA)

Proposición

Sean m y $n \geqslant\ 2$ con

$$m = {p_1}^{e_1} \cdot {p_2}^{e_2}, ..., {p_r}^{e_r} \qquad y \qquad n = {p_1}^{f_1} \cdot {p_2}^{f_2}, ..., {p_r}^{f_r}$$

En donde p_i primo y e_i y $f_i \geqslant 0$ para todo $i = 1, ..., r$

Que significa que $m|n$ si y solo si la descomposición prima tiene los mismos factores y los factores de m son menores o iguales que los de n.

Entonces $m|n$ si y solo si $e_i \leqslant f_i$ para todo i. Por ejemplo

$p^2|p^3$

$p \cdot q^2|p^2 \cdot q^3$

$p^2 \cdot q \nmid p \cdot q^2$

Demostración

(⇒) Por la descomposición de m es claro que $p_i{}^{e_i}|m$. Como m|n, entonces $p_i{}^{e_i}|n$. Es decir, $n = p_i{}^{e_i} \cdot u$. Es claro por TFA entonces $e_i \leqslant f_i$

(⇐) Como $e_i \leqslant f_i$ tenemos que $p_i{}^{e_i}|p_i{}^{f_i}$, para $1 \leqslant i \leqslant r$. Luego.

$$p_1{}^{e_1} \cdot p_2{}^{e_2}, ..., p_r{}^{e_r}|p_1{}^{f_1} \cdot p_2{}^{f_2}, ..., p_r{}^{f_r}$$

Es decir $m|n$

Ahora veremos que es muy fácil calcular el MCD y el mcm de un par de números conociendo sus descomposiciones primas.

Proposición

Sean m y n enteros positivos cuyas factorizaciones primas son

$$m = p_1{}^{e_1} \cdot p_2{}^{e_2}, ..., p_r{}^{e_r} \qquad \text{y} \qquad n = p_1{}^{f_1} \cdot p_2{}^{f_2}, ..., p_r{}^{f_r}$$

a) El MCD de m y n es $d = p_1{}^{k_1} \cdot p_2{}^{k_2}, ..., p_r{}^{k_r}$ donde para cada i en el rango $1 \leqslant i \leqslant r$, k_i es el mínimo entre e_i y f_i

b) El mcm de m y n es $u = p_1{}^{h_1} \cdot p_2{}^{h_2}, ..., p_r{}^{h_r}$ donde para cada i en el rango $1 \leqslant i \leqslant r$, h_i es el máximo entre e_i y f_i

Demostración a

Sea c tal que $c|n$ y $c|m$, entonces los primos que intervienen en la factorización de c son $p_1, ..., p_r$ y por lo tanto $c = p_1{}^{t_1} \cdot p_2{}^{t_2}, ..., p_r{}^{t_r}$. Además, cómo $c|n$ y $c|m$ tenemos que $t_i \leqslant e_i, f_i$ y por lo tanto $t_i \leqslant k_i = \min(e_i, f_i)$.

De esto se deduce que $c|p_1{}^{k_1} \cdot p_2{}^{k_2}, ..., p_r{}^{k_r} = d$. Por otro lado, es claro que $p_1{}^{k_1} \cdot p_2{}^{k_2}, ..., p_r{}^{k_r}$ divide a m y n y se deduce el resultado.

Ejemplo

Se quiere encontrar el MCD y el mcm del par de números $(2^3 \cdot 3^2,\ 2^1 \cdot 3^3)$

Solución

Entonces vemos los menores e_i para el MCD y los mayores para el mcm, por lo que tenemos que

$$\text{mcd}(2^3 \cdot 3^2,\ 2^1 \cdot 3^3) = 2^1 \cdot 3^2$$
$$\text{mcm}(2^3 \cdot 3^2,\ 2^1 \cdot 3^3) = 2^3 \cdot 3^3$$

4. Aritmética modular

4.1. Congruencia

Definición

Sean a y b enteros y m un entero positivo. Diremos que a es congruente a b módulo m, y escribimos

$$a \equiv b \ (mod\ m)$$

Si $a - b$ es divisible por m

Observar que $a \equiv 0 \ (mod\ m) \ \Leftrightarrow \ m|a$, y que $a \equiv b \ (mod\ m) \ \Leftrightarrow \ a - b \equiv 0 \ (mod\ m)$

Ejemplo

$$15 \equiv 8 \ (\text{mod } 7) \ \Leftrightarrow \ 7|15 - 8 \ = \ 7|7$$

$$20 \equiv 38 \ (\text{mod } 3) \ \Leftrightarrow \ 3|20 - 38 \ = \ 3| - 18$$

Vemos entonces que estos 2 ejemplos son ciertos por el resultado obtenido al final.

Proposición

Sean a y b enteros y m un entero positivo. Entonces $a \equiv b$ (mod m) si y solo si a y b tienen el mismo resto en la división por m.

Demostración

Si $a = m \cdot n + r$ y $b = m \cdot k + s$, con $0 \leqslant r, \ s < m$, podemos suponer, sin perdida de generalidad, que $r \leqslant s$, luego

$$b - a = m \cdot (k - n) + (s - r) \ \text{ con } 0 \leqslant s - r < m$$

Se sigue que $s - r$ es el resto de dividir $b - a$ por m es 0, y por lo tanto $s - r = 0$ y $s = r$

Si a y b tienen el mismo resto en la división por m, entonces $a = m \cdot n + r$ y $b = m \cdot k + r$, luego $a - b = m \cdot (n - k)$ que es divisible por m.

Ejemplo

Probar que $38 \equiv 23$ (mod 5)

Solución

Tenemos que $38 \equiv 23$ (mod 5), entonces podemos tratar de expresarlos como productos de 5, de la forma

$$38 = 5 \cdot 7 + 3$$
$$23 = 5 \cdot 4 + 3$$

Entonces vemos que como coincide el resto, es cierto que $38 \equiv 23$ (mod 5)

Así como separamos $\mathbb{Z}$ en números pares e impares, la propiedad anterior nos permite expresar $\mathbb{Z}$ como una unión disjunta de m subconjuntos.

Es decir, dado $m \in \mathbb{Z}$, si

$$\mathbb{Z}_r = \{x \in \mathbb{Z} \ : \ \text{el resto de dividir } x \text{ por } m \text{ es } r\}$$

Entonces vemos que

$$\mathbb{Z}_r = \mathbb{Z}_{[0]} \cup \ \mathbb{Z}_{[1]} \cup ... \cup \mathbb{Z}_{[m-1]}$$

Cada subconjunto está determinado por el resto, por ejemplo $\mathbb{Z}_{[0]}$ tiene resto 0, así $\mathbb{Z}_{[1]}$, $\mathbb{Z}_{[2]}$, hasta $\mathbb{Z}_{[m-1]}$

4.1.1. Propiedades de la congruencia modulo m

Es fácil verificar que la congruencia modulo m verifica las siguientes propiedades

a) Es reflexiva, es decir $x \equiv x \pmod{m}$

b) Es simétrica, es decir si $x \equiv y \pmod{m}$, entonces $y \equiv x \pmod{m}$

c) Es transitiva, es decir, si $x \equiv y (\text{mod } m)$ e $y \equiv z (\text{mod } m)$, entonces $x \equiv z (\text{mod} m)$.

Demostración

Demostremos entonces cada una de estas propiedades anteriormente enunciadas.

a) Esta propiedad se demuestra fácilmente debido a que $x - x = 0$, y eso implica que es divisible por m.

b) Esta propiedad se demuestra fácilmente debido a que si $x \equiv y \pmod{m}$, entonces $x - y = k \cdot m$, y por lo tanto $y - x = (-k) \cdot m$.

c) Esta última propiedad también es fácilmente demostrable debido a que si $x \equiv y \pmod{m}$, entonces $x - y = k \cdot m$, y si $y \equiv z \pmod{m}$, entonces $y - z = l \cdot m$, por lo tanto tenemos que

$$x - z = (x - y) + (y - z) = (k + l) \cdot m$$

Estas tres propiedades nos dicen que es congruencia modulo m es una relación de equivalencia, y además, que es compatible con la suma y la multiplicación, de hecho allí reside su utilidad.

Teorema

Sea m un entero positivo y sean x_1, x_2, y_1, y_2 enteros tales que

$$x_1 \equiv x_2 \pmod{m}, \quad y_1 \equiv y_2 \pmod{m}$$

Entonces se cumple que

a) $x_1 + y_1 \equiv x_2 + y_2 \pmod{m}$,

b) $x_1 \cdot y_1 \equiv x_2 \cdot y_2 \pmod{m}$,

c) si $x \equiv y \pmod{m}$ y $j \in \mathbb{N}$, entonces $x^j \equiv y^j \pmod{m}$

Demostración

Demostremos entonces cada una de las anteriormente mencionadas propiedades.

(a) Por hipótesis $\exists x,\ y$ tal que $x_1 - x_2 = m \cdot x$ e $y_1 - y_2 = m \cdot y$. Luego,

$$\begin{aligned}(x_1 + y_1) - (x_2 + y_2) &= (x_1 - x_2) + (y_1 - y_2) \\ &= m \cdot x + m \cdot y \\ &= m \cdot (x + y)\end{aligned}$$

Y por consiguiente el lado izquierdo es divisible por m.

(b) Aquí tenemos

$$\begin{aligned}x_1 \cdot y_1 - x_2 \cdot y_2 &= x_1 \cdot y_1 - x_2 \cdot y_1 + x_2 \cdot y_1 - x_2 \cdot y_2 \\ &= (x_1 - x_2) \cdot y_1 + x_2 \cdot (y_1 - y_2) \\ &= m \cdot x \cdot y_1 + x_2 \cdot m \cdot y \\ &= m \cdot (x \cdot y_1 + x_2 \cdot y)\end{aligned}$$

Y de nuevo el lado izquierdo es divisible por m

(c) Lo haremos por inducción sobre j

Es claro que si $j = 1$ el resultado es verdadero. Supongamos ahora que el resultado vale para j - 1, es decir

$$x^{j-1} \equiv y^{j-1} \pmod{m}$$

Como $x \equiv y \pmod{m}$, por (b) tenemos que

$$x^{j-1} \cdot x \equiv y^{j-1} \cdot y \pmod{m},$$

Es decir, tenemos que

$$x^j \equiv y^j \ x^{j-1} \equiv y^{j-1} \pmod{m}$$

Hemos demostrado entonces la validez de la propiedad (c).

Proposición

Sea $(x_n x_{n-1}...x_0)_{10}$ la representación del entero positivo x en base 10, entonces

$$x \equiv x_0 + x_1 + ... + x_n \pmod 9$$

(si la suma de los dígitos es divisible por 9, entonces el número es divisible por 9)

Demostración

Observemos que $10 \equiv 1 \pmod m \Rightarrow 10^k \equiv 1^k \equiv 1 \pmod m$

Por la definición de representación en base 10, tenemos que

$$x = x_0 + 10^1 \cdot x_1 + ... + 10^n \cdot x_n$$

Luego, como $10^k \cdot x_k \pmod 9$, entonces $x \equiv x_0 + x_1 + ... + x_n \pmod 9$.

También existe la regla del 3, del 5 y del 11, y son interesantes casos de estudio.

Corolario

Sea $x = (x_n x_{n-1}...x_0)_{10}$, entonces $9|x \Leftrightarrow 9|x_0 + x_1 + ... + x_n$

Demostración

Por la proposición anterior

$$x \equiv x_0 + x_1 + ... + x_n \pmod 9 \qquad (*)$$

Entonces,

$$\begin{aligned} 9|x &\Leftrightarrow x \equiv 0 \pmod 9 && \text{por hipótesis} \\ &\Leftrightarrow x_0 + x_1 + ... + x_n \equiv 0 \pmod 9 && \text{por } (*) \\ &\Leftrightarrow 9|x_0 + x_1 + ... + x_n \end{aligned}$$

Entonces queda demostrado el corolario de la regla del nueve, veamos ahora un ejemplo utilizándolo.

Ejemplo

Probar que $54321 \cdot 98765 \neq 5363013565$

Solución

Demostremos entonces la proposición anterior, veamos que los anteriores números modulo 9 son

$$54321 \equiv 5+4+3+2+1 \equiv 15 \equiv 15-9 \equiv 6 \pmod 9$$
$$98765 \equiv 9+8+7+6+5 \equiv 35 \equiv 8+3\cdot 9 \equiv 8 \pmod 9$$

Entonces

$$54321 \cdot 98765 \equiv 6 \cdot 8 \equiv 48 \equiv 4+8 \equiv 12 \equiv 3+1\cdot 9 \equiv 3 \pmod 9$$

Mientras que

$$5363013565 \equiv 5+3+6+3+0+1+3+5+6+5 \equiv 37 \equiv 1+4\cdot 9 \equiv 1 \pmod 9$$

Luego vemos que $54321 \cdot 98765 \neq 5363013565$

4.2. Ecuación lineal de congruencia

Definición

Estudiaremos el problema de encontrar los $x \in \mathbb{Z}$ tal que

$$ax \equiv b \ (mod\ m)$$

Es fácil ver que el problema no siempre admite solución, sea este el caso de $2x \equiv 3\ (mod\ 2)$ el cual no posee ninguna solución en $\mathbb{Z}$, pues cualquiera sea $k \in \mathbb{Z}$, $2k-3$ es impar, por ende, no es divisible por 2.

Notemos además que si x_0 es solución de la ecuación, también lo es $x_0 + km$ de manera que si la ecuación posee una solución, posee infinitas soluciones. Para evitar la ambigüedad de infinitas soluciones, nos limitaremos a considerar las soluciones tales que $0 \leqslant x < m$.

Ejemplo

La solución general de la ecuación $3x \equiv 7 \pmod{11}$ es $6+11k$ con $k \in \mathbb{Z}$.

Esto es debido a que si probamos con los enteros x tales que $0 \leqslant x < 11$, veremos que la ecuación admite una única solución, a saber $x = 6$. Las demás soluciones se obtienen tomando $6+11k$. Por otra parte, si tomamos que u también es solución de la ecuación tenemos que

$$3u \equiv 7 \pmod{11} \quad y \quad 3\cdot 6 \equiv 7 \pmod{11} \quad \Rightarrow \quad 3u \equiv 3\cdot 6 \pmod{11}$$

Por lo tanto $3\cdot(u-6)$ es múltiplo de 11. Como 11 no divide a 3 se tiene que $11|(u-6)$, es decir, $u = 6+11k$. Así demostramos que todas las soluciones son de la forma $6+11k$ con $k \in \mathbb{Z}$.

Veamos a continuación otro ejemplo utilizando la ecuación lineal de congruencia.

Ejemplo

Encontrar $0 \leqslant x < 109$ solución de la ecuación $74 \cdot x \equiv 5 \pmod{109}$.

Solución

Podemos ver que el MCD del par (74, 109) es 1, ya que 74 y 109 son coprimos. Entonces existen $s,\ t \in \mathbb{Z}$ tal que

$$1 = s \cdot 74 + t \cdot 109$$

Luego, como $t \cdot 109 \equiv 0 \pmod{109}$

$$1 \equiv s \cdot 74 \pmod{109}$$

Multiplicando por 5 la ecuación anterior, tenemos

$$5 \equiv 5s \cdot 74 \pmod{109}$$

Eso implica que $5s$ es solución de $74 \cdot x \equiv 5 \pmod{109}$

Con el algoritmo de euclides obtenemos,

$$1 = 28 \cdot 74 + (-19) \cdot 109$$

Por lo anterior, $5 \cdot 28 = 140$ es solución de la ecuación, es decir,

$$74 \cdot 140 \equiv 5 \pmod{109}$$

Pero $140 > 109$, sin embargo $140 - 109 = 31$ también es solución, pues $109 \equiv 0 \pmod{109}$

Luego la solución es $x = 31$, pues

$$74 \cdot 31 \equiv 5 \pmod{109} \quad \text{y } 0 \leqslant 31 < 109$$

Observación

Analicemos un caso particular, el de la ecuación general $ax \equiv b\ (mod\ m)$ si $\text{mcd}(a,\ m) = 1$. Dado esto, sabemos que existen enteros $r\ y\ s$ tales que $1 = r \cdot a + s \cdot m$ y por lo tanto, si multiplicamos por b tenemos que, $b = (r \cdot b) \cdot a + (s \cdot b) \cdot m$ por lo tanto, nuestra ecuación nos quedaría:

$$a \cdot (r \cdot b) \equiv b\ (mod\ m)$$

Es decir $r \cdot b$ es solución de la ecuación. Veremos que el caso general se hace de la misma forma.

Introduzcamos entonces el caso general de la ecuación lineal de congruencia

Teorema

Sean $a,\ b$ números enteros y m un entero positivo y denotemos $d = \text{mcd}(a,\ m)$. La ecuación

$$ax \equiv b \pmod{m}$$

Admite solución si y solo si $d|b$, y en este caso dada x_0 una solución, todas las soluciones son de la forma

$$x = x_0 + kn,\ \text{con } k \in \mathbb{Z}\ y\ n = \frac{m}{d}$$

Demostración

Como d = mcd$(a,\ m)$, existen $r,\ s \in \mathbb{Z}$ tales que:

$$d = r \cdot a + s \cdot m$$

Si $d|b$, entonces existe $h \in \mathbb{Z}$ tal que $b = d \cdot h$. Si multiplicamos h la ecuación de arriba, obtenemos

$$d \cdot h = (r \cdot h) \cdot a + (s \cdot h) \cdot m$$

Luego $a \cdot (r \cdot h) \equiv a \cdot (r \cdot h) + (s \cdot h) \cdot m \equiv d \cdot h \equiv b\ (mod\ m)$, y por lo tanto $r \cdot h$ es solución de la ecuación lineal de congruencia.

Por otro lado, si $a \cdot x \equiv b \pmod{m}$, entonces $a \cdot x - b = k \cdot m$ para algún k, o sea.

$$b = a \cdot x + (-k) \cdot m$$

De lo cuál se sigue que si $d|a$ y $d|m$, entonces $d|b$ y por lo tanto mcd$(a,\ m)|b$.

Por lo tanto hemos demostrado que la condición necesaria y suficiente para que la ecuación $a \cdot x \equiv b \pmod{m}$ admita una solución es que mcd$(a,\ m)|b$.

En el caso de $d|b$ veamos ahora cuales son todas las soluciones posibles de la ecuación general. Sean x_1, x_2 soluciones, es decir:

$$a \cdot x_1 \equiv b \pmod{m}$$

$$a \cdot x_2 \equiv b \pmod{m}$$

Entonces, restando miembro a miembro, obtenemos:

$$a \cdot x_1 - a \cdot x_2 \equiv b - b \equiv 0 \pmod{m}$$

Es decir, x_1, x_2 son soluciones de la ecuación si y sólo si $y = x_1 - x_2$ es solución de la ecuación lineal de congruencia.

$$a \cdot y \equiv 0 \pmod{m}$$

Por ende,

Si $\text{mcd}(a,\ m) = 1$ es claro que la ecuación $a \cdot y \equiv 0 \pmod{m}$ tiene como solución todos los y tales que $m|y$, es decir todos los múltiplos de m.

Si $\text{mcd}(a,\ m) > 1$, la ecuación $a \cdot y \equiv 0 \pmod{m}$ tiene como solución todos los y tales que $a \cdot y = m \cdot k$ para algún k. Si dividimos por d, podemos decir que todas las soluciones son todos los y tales que $(a/d) \cdot y = (m/d) \cdot k$, es decir todos los y tal que $(m/d)|(a/d) \cdot y$. Como m/d y a/d son coprimos, las soluciones son todos los múltiplos de m/d.

Sean x_0 y x tal que $a \cdot x_0 \equiv b \pmod{m}$ y $a \cdot x \equiv b \pmod{m}$ entonces $a \cdot (x_0 - x) \equiv b \pmod{m}$ y por lo tanto $x_0 - x = k \cdot n$ para algún k. Es decir, cualquier x es solución lineal de congruencia es de la forma $x_0 = x + k \cdot n$ para algún k

Proposición

Sirve para calcular las soluciones. Sean $a,\ b,\ m \in \mathbb{Z},\ d > 0$ tales que $d|a$, $d|b$, $d|m$. Entonces

$$ax \equiv b \pmod{m} \ \Leftrightarrow\ \frac{a}{d} \cdot x \equiv \frac{b}{d} \left(\text{mod } \frac{m}{d}\right)$$

Donde d es común divisor de todos.

Demostración

$$\begin{aligned} ax \equiv b \pmod{m} &\Leftrightarrow m|ax - b \\ &\Leftrightarrow ax - b = m \cdot q \\ &\Leftrightarrow \frac{a}{d} \cdot x - \frac{b}{d} = \frac{m}{d} \cdot q \qquad\qquad \Leftrightarrow \frac{a}{d} \cdot x \equiv \frac{b}{d} \pmod{\frac{m}{d}} \end{aligned}$$

La proposición anterior nos permite reducir las ecuaciones al caso $ax \equiv b \pmod{m}$ con $(a,\ m) = 1$

Veamos un ejemplo de su aplicación práctica.

Ejemplo

Encontrar todos los $x \in \mathbb{Z}$ tales que

$$6x \equiv 9 \pmod{21} \qquad (*)$$

Solución

Veamos que el $\text{mcd}(6,\ 21) = 3$, entonces, por la proposición anterior veamos que

$$\begin{aligned} 3 &\equiv (-3) \cdot 6 + 1 \cdot 21 \pmod{21} \\ 3 &\equiv (-3) \cdot 6 \pmod{21} \\ 6 \cdot (-9) &\equiv 3 \pmod{21} \end{aligned}$$

Luego -9 es solución de $6x \equiv 9 \pmod{21}$. Por el teorema todas las soluciones son de la forma $x = -9 + k \cdot 7$

Método general para la resolución de la ecuación

Concluyendo y gracias a la demostración anterior podemos obtener un método general para encontrar soluciones de la ecuación lineal de congruencia.

$$a \cdot x \equiv b \pmod{m} \qquad \text{con } \text{mcd}(a,\ m)|b$$

a) Encontrar, usando el algoritmo de Euclides, r y s tales que:

$$d = mcd(a,\ m) = r \cdot a + s \cdot m$$

b) Como $d|b$, tenemos que $b = t \cdot d$ y multiplicamos la ecuación anterior por t:

$$d \cdot t = (r \cdot t) \cdot a + (s \cdot t) \cdot m$$

c) Finalmente obtenemos, $b = d \cdot t = (r \cdot t) \cdot a + (s \cdot t) \cdot m \equiv (r \cdot t) \cdot a \pmod{m}$
Luego, $x_0 = r \cdot t$ es la solución de la ecuación lineal de congruencia.

d) Toda solución de la ecuación lineal de congruencia es $x = x_0 + k \cdot (m/d)$ con $k \in \mathbb{Z}$

4.3. Teorema de Fermat

El siguiente lema, también llamado teorema pequeño o débil de Fermat, nos sirve de preparación para la demostración del Teorema de Fermat.

Lema

Sea p un numero primo, entonces

a) $p|\binom{p}{r}$, con $0 < r < p$

b) $(a+b)^p \equiv a^p + b^p \pmod{p}$ (El sueño del pibe)

Demostración

a) Escribamos el numero binomial de otra forma:

$$\binom{p}{r} = \frac{p!}{(p-r)! \cdot r!} = p \cdot \frac{(p-1)!}{(p-r)! \cdot r!}$$

Luego, multiplico cada término por $(p-r)! \cdot r!$ de tal manera que:

$$\binom{p}{r} \cdot (p-r)! \cdot r! = p! = p \cdot (p-1)!$$

Luego por definición de divide:

$$p|\binom{p}{r} \cdot (p-r)! \cdot r!$$

Recordemos la propiedad de que si $p|a \cdot b \ \Rightarrow p|a \vee p|b$

Luego,

$$p|\binom{p}{r} \vee p|(p-r)! \vee p|r!$$

Sin embargo, si prestamos atención por hipótesis tenemos $r < p$ por lo que r no tiene un factor primo p en su descomposición prima, lo que contradice al teorema fundamental de la aritmética, por ende $p \nmid r$ y por consiguiente y gracias a la definición de $n!$ tenemos que $p \nmid r!$

Por otro lado, teniendo por hipótesis que $r > 0$ tenemos que $(p-r) < p$ y por las mismas razones anteriores $p \nmid (p-r)!$
Por ende, queda demostrado que

$$p|\binom{p}{r}$$

b) Por la propiedad anterior tenemos que

$$p|\binom{p}{r}$$

Luego, por el teorema del binomio de Newton tenemos que

$$(a+b)^p = \sum_{i=0}^{p} \binom{p}{i} \cdot a^i \cdot b^{n-i}$$

Sin embargo, como $p|\binom{p}{r} \Rightarrow \binom{p}{r} \equiv 0 \pmod{p}$ Por ende, todos los términos de la sumatoria a excepción de los extremos van a ser 0, por lo que tenemos

$$\sum_{i=0}^{p} \binom{p}{i} \cdot a^i \cdot b^{n-i} \equiv 0 \pmod{p} \qquad si \qquad 0 < i < p$$

Luego se deduce el resultado y finalmente nos queda que

$$(a+b)^p \equiv \binom{p}{0} \cdot a^0 \cdot b^p + \binom{p}{p} \cdot a^p \cdot b^0 \equiv a^p + b^p \pmod{p}$$

Enunciemos entonces el teorema de Fermat, un importante teorema demostrado en el siglo 18.

Teorema
Sea p un número primo y a un número entero. Entonces

$$a^p \equiv a \pmod{p}$$

Demostración

Supongamos que $a \geqslant 0$, entonces hagamos inducción en a.

Caso base: si $a = 0$, el resultado es trivial.

Caso Inductivo: Supongamos que el resultado es verdadero para $a = k$, es decir, $k^p \equiv k \pmod{p}$ (Hipótesis Inductiva). Probemos para $a = k + 1$.
Tenemos entonces $(k+1)^p \equiv k^p + 1^p \pmod{p}$ lo cual es verdad por la propiedad (b) del lema anterior.
Luego tenemos que por propiedad de la potencia $1^n = 1$ y por la hipótesis inductiva $k^p \equiv k \pmod{p}$.
Por ende nos queda:

$$(k+1)^p \equiv k^p + 1^p \equiv k + 1 \pmod{p}$$

. Luego, queda demostrado que $a^p \equiv a \pmod{p}$ cuando $a > 0$

Analicemos el caso si $a < 0$

Si $a < 0 \;\Rightarrow\; -a > 0$ y ya vimos que $(-a)^p \equiv -a \pmod{p}$, es decir que $(-1)^p \cdot a^p \equiv (-1) \cdot a \pmod{p}$
Luego si $p \neq 2$, entonces $(-1)^p = -1$ y se deduce el resultado.
Luego si $p = 2$, entonces $(-1)^p = 1$, pero cómo $1 \equiv -1 \pmod{2}$ obtenemos también $a^p \equiv a \pmod{p}$

Corolario

Si a y p coprimos y p es primo, entonces

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

Este último también se conoce como teorema de Fermat.

Demostración

Por Fermat $a^p \equiv a \pmod{p}$, es decir:

$$p | (a^p - a) = a \cdot (a^{(p-1)} - 1)$$

Como $p \nmid a$, tenemos que $p | (a^{(p-1)} - 1)$ esto debido a la propiedad de p divide.

Finalmente obtenemos que $a^{(p-1)} \equiv 1 \pmod{p}$

Ejemplo

Calcular $2^{3845} \equiv r \pmod{13}$ $\qquad (0 \leqslant r \leqslant 13)$

Solución

Por el corolario del teorema de Fermat, sabemos que $2^{12} \equiv 1 \pmod{13}$, entonces podemos ver que se puede resolver por las propiedades de la potenciación de la siguiente forma

$$3843 = 12 \cdot 320 + 3 \;\Rightarrow\; 2^{3843} \equiv 2^{12 \cdot 320 + 3} \equiv \left(2^{12}\right)^{320} \cdot 2^3 \equiv 1^{320} \cdot 2^3 \equiv 8 \pmod{13}$$

Existe otra versión similar solo que para cualquier número y no solo para uno de modulo primo.

Definición

Sea $n \geqslant 1$, la función de Euler se define

$$\phi(n) := |\{x \ : \ \text{mcd}(x,\ n) = 1 \ \wedge \ 1 \leqslant x < n\}|$$

Cardinalidad del conjunto de coprimos con $n = \phi(n)$

Teorema

Si n un entero positivo y a un número entero coprimo con n, entonces

$$a^{\phi(n)} \equiv 1 \ (\text{mod } n)$$

Teorema más general que el teorema de Fermat, que puede utilizarse para cualquier número.

5. Grafos

Usaremos la siguiente definición en lo que sigue. Dado un conjunto X un 2-subconjunto es un subconjunto de X de dos elementos.

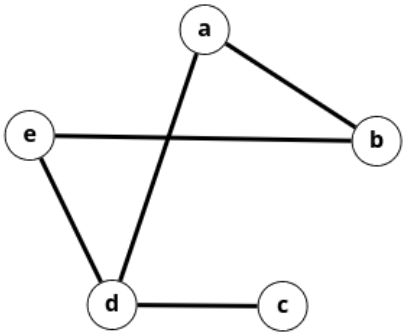
Definición
Un grafo G consiste de un conjunto finito V, cuyos miembros son llamados vértices, y un conjunto de 2-Subconjuntos de V, cuyos miembros son llamados aristas.

Usualmente escribiremos $G = (V,\ E)$ y diremos que V es el conjunto de vértices y E es el conjunto de aristas.

Un ejemplo de un grafo típico $G = (V,\ E)$ es dado por los conjuntos

$$V = \{a, b, c, d, e\}, \qquad E = \{\{a, b\}, \{a, d\}, \{b, e\}, \{c, d\},$$

Este ejemplo y la definición misma no suelen ser muy esclarecedoras, y solamente cuando consideramos la representación pictórica de un grafo es cuando entendemos un poco mas la definición.



Observaciones

- $\{a,\ b\} = \{b,\ a\}$, los conjuntos tienen la propiedad de que no importa el orden, es decir, en este caso las aristas no tienen direcciones, es decir que en este caso la arista indica que a se encuentra unido con b y b lo está con a.
- La representación pictórica es intuitivamente atractiva pero no es útil cuando deseamos comunicarnos con una computadora.
- Debemos representar el grafo mediante conjuntos o una tabla, usualmente llamada tabla de adyacencia.

Definición

Diremos que dos vértices x e y de un grafo son adyacentes cuando $\{x,\ y\}$ es una arista.

Definición

Podemos representar un grafo $G = (V,\ E)$ por su lista de adyacencia, donde cada vértice V encabeza una lista de aquellos que son adyacentes a V.

Ejemplo

Vimos que el grafo $G = (V,\ E)$ está dado por

$$V = \{a, b, c, d, e\}, \qquad E = \{\{a, b\}, \{a, d\}, \{b, e\}, \{c, d\}, \{d, e\}$$

Su lista de adyacencia es

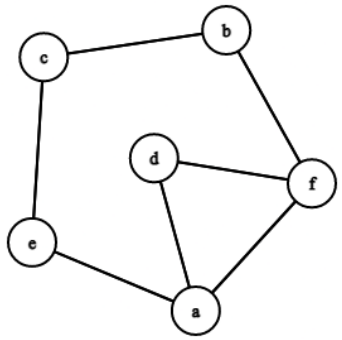
a	b	c	d	e
b	a	d	a	b
d	e		c	d
			e	

En python el grafo estaría representado por la lista de listas

$$[[b,\ d],\ [a,\ e],\ [d],\ [a,\ c,\ e],\ [b,\ d]]$$

Ejemplo 2

A partir del siguiente grafo, realice la lista de adyacencia.



Entonces veamos que su lista de adyacencia es:

a	b	c	d	e	f
d	c	b	a	a	a
e	f	e	f	c	b
f					d

Definición

Por cada entero positivo n definimos el grafo completo K_n como el grafo con n vértices y en el cual cada par de vértices es adyacente.

La lista de adyacencia de K_n es una lista donde en la columna del vértice i están todos los vértices menos i (n-1 vértices).

¿Cuantas aristas tiene K_n?

De cada vértice 'salen' $n-1$ aristas, las que van a otros vértices.

Si sumamos n veces las $n-1$ aristas es claro que estamos contando cada arista dos veces, por ejemplo $\{2,1\}$ y $\{1,2\}$.

Luego el número total de aristas de K_n es $\frac{n\cdot(n-1)}{2}$

Ejemplos

Veamos algunos ejemplos y su disposición conveniente

Entonces podemos ver la cantidad de aristas de cada grafo a partir de la fórmula enunciada anteriormente, luego la cantidad de aristas de cada uno son

$$K_1 = 0 = \frac{1\cdot(1-1)}{2}$$
$$K_2 = 1 = \frac{2\cdot(2-1)}{2}$$
$$K_3 = 3 = \frac{3\cdot(3-1)}{2}$$
$$K_4 = 6 = \frac{4\cdot(4-1)}{2}$$

El grafo K_n o grafo completo tiene la máxima cantidad de aristas posibles.

Observemos que esta es una demostración, usando grafos, de que

$$\sum_{i=1}^{n-1} i = \frac{n\cdot(n-1)}{2}$$

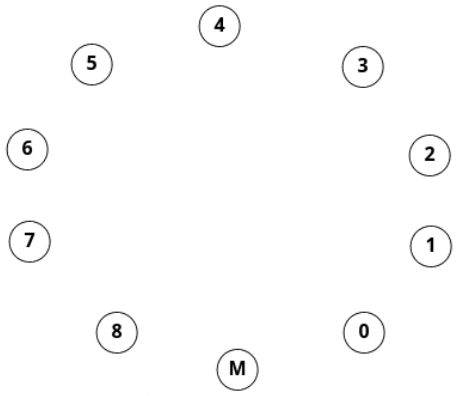
Ejemplo

Mario y su mujer Abril dan una fiesta en la cual hay otras cuatro parejas de casados. Las parejas, cuando llegan, estrechan la mano a algunas personas, pero, naturalmente, no se estrechan la mano entre marido y mujer. Cuando la fiesta finaliza, Mario pregunta al resto a cuantas personas han estrechado la mano, recibiendo 9 respuestas diferentes. Se quiere saber entonces ¿Cuantas personas estrecharon la mano de Abril?

Solución

Construyendo un grafo cuyos vértices son las personas que asisten a la fiesta y las aristas del grafo son las $\{x, y\}$ siempre y cuando x e y se hayan estrechado la mano.

Puesto que hay 9 personas aparte de Mario y que una persona puede estrechar la mano a lo sumo a otras 8 personas, se sigue que las 9 respuestas diferentes que ha recibido Mario deben ser 0, 1, 2, 3, 4, 5, 6, 7, 8.



Si son 9 respuestas diferentes y como máximo se estrechaba la mano a 8 personas, entonces cada integrante estrechó la mano de 0 a 8 veces. Ahora debemos saber cuantas estrechó la mujer de Mario, Abril.

Luego, el vértice 8 alcanza a todos los otros vértices excepto uno, el cual debe representar a la esposa de 8. Este vértice debe ser el 0 el cual además no es adyacente a 8.

Se sigue que 8 y 0 son una pareja de casados y 8 es adyacente a 1,2,3,4,5,6,7 y M. En particular 1 ya es adyacente al 8 y ésta es la única arista que parte del 1.

Por consiguiente 7 no está unido al 0 ni al 1 y si lo está al 2,3,4,5,6,8 y M. La esposa de 7 debe ser 1, puesto que 0 es la pareja de 8.

Continuando con este razonamiento vemos que 6 y 2, y 5 y 3 son parejas de casados. Se sigue que M y 4 están casados, luego el vértice que representa a Abril es el 4, quién estrechó la mano a 4 personas.

Ejemplo

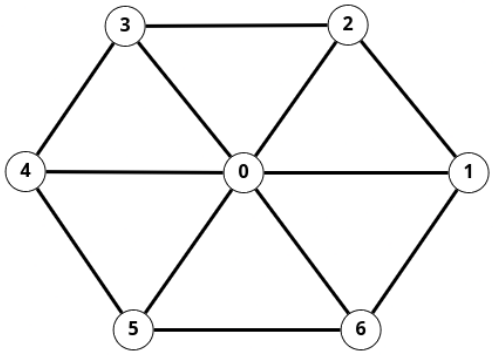
Los senderos de un jardín han sido diseñados dándoles forma de grafo rueda W_n, cuyos vértices son $V = \{0, 1, 2, ..., n\}$ y sus aristas son

$$\text{Los rayos de la rueda: } \{0,1\}, \{0,2\}, ..., \{0,n\}$$
$$\text{Perímetro de la rueda: } \{1,2\}, \{2,3\}, ..., \{n-1,n\}, \{n,1\}$$

Describir una ruta por los senderos de tal forma que empiece y termine en el vértice 0 y que pase por cada vértice una sola vez.

Solución

Primero dibujemos el grafo para darnos cuenta por que se llama rueda, por ejemplo veamos W_6



El dibujo nos orienta como puede ser una ruta: 0, 1, 2, 3, 4, 5, 6, 0.

En general una respuesta es 0, 1, 2, 3, ..., $n-1$, n, 0.

Los grafos rueda tienen sentido a partir de W_3, es decir $n \geqslant 3$, pero se ven como rueda a partir de $n \geqslant 5$.

Observación

La representación gráfica es una representación topológica, ya que no importa la forma ni la longitud, si no que lo que importan son las relaciones entre los objetos.

5.1. Isomorfismo de grafos

Ahora nos preguntamos ¿Cuándo consideramos a dos grafos 'iguales'?

5.1.1. Preliminares

Definición

Dado dos conjuntos X, Y diremos que una aplicación $f : X \to Y$ es biyectiva si para cada $y \in Y$ existe un único $x \in X$ tal que $f(x) = y$.

Una propiedad importante de las funciones biyectivas es

Teorema

f es biyectiva si y sólo si f tiene inversa, es decir existe $f^{-1} : Y \to X$, tal que

$$f(f^{-1}(y)) = y \ \forall y \in Y \quad \wedge \quad f(f^{-1}(x)) = x \ \forall x \in X$$

Ejemplo

La función $f : \{1, 2, 3\} \to \{a, b, c\}$ definida $f(1) = c$, $f(2) = b$, $f(3) = a$ es biyectiva y su inversa es

$$f^{-1}(a) = 3, \quad f^{-1}(b) = 2, \quad f^{-1}(c) = 1$$

5.1.2. Definición

Definición

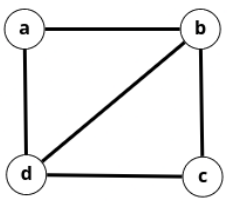
Dos grafos G_1 y G_2 se dice que son isomorfos cuando existe una biyección α entre el conjunto de vértices de G_1 y el conjunto de vértices de G_2 tal que

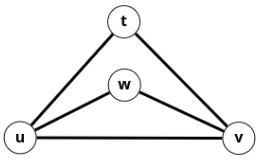
- Si $\{x, y\}$ es una arista de G_1 entonces $\{\alpha(x), \alpha(y)\}$ es una arista de G_2 y recíprocamente,
- Si $\{z, w\}$ es una arista de G_2 entonces $\{\alpha^{-1}(z), \alpha^{-1}(w)\}$ es una arista de G_1

Equivalentemente, diremos que α es un isomorfismo si es una biyección entre el conjunto de vértices de G_1 y el conjunto de vértices de G_2 tal que por cada $\{z, w\}$ arista de G_2, existe una y solo una $\{x, y\}$ arista de G_1 tal que $\{\alpha(x), \alpha(y)\} = \{z, w\}$

Ejemplo

Dados dos grafos G_1 y G_2, veamos si son isomorfos o no





Solución

Veamos que estos son isomorfos, de hecho una biyección es dada por

$$\alpha(a) = t,\ \alpha(b) = v,\ \alpha(c) = w,\ \alpha(d) = u$$

Podemos comprobar que a cada arista de G_1 le corresponde una arista de G_2 y viceversa.

Observaciones

Demostrar que dos grafos son isomorfos es un problema complicado, de hecho no es un problema computable.

Para demostrar que dos grafos no son isomorfos debemos demostrar que no hay una biyección entre el conjunto de vértices de uno con el conjunto de vértices del otro, que lleve las aristas de uno al otro. Este problema tampoco es computable.

Algunas formas más fáciles de descartar un isomorfismo pueden ser

- Contar que tengan la misma cantidad de vértices, si dos grafos tienen diferente número de vértices, entonces no es posible ninguna biyección y por lo tanto los grafos no pueden ser isomorfos.
- Contar que tengan la misma cantidad de aristas, si los grafos tienen la misma cantidad de vértices pero distinta de aristas, entonces hay biyecciones de vértices pero ninguna de ellas puede ser un isomorfismo.

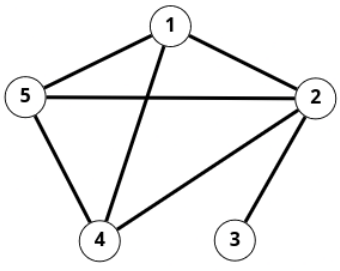
Definición

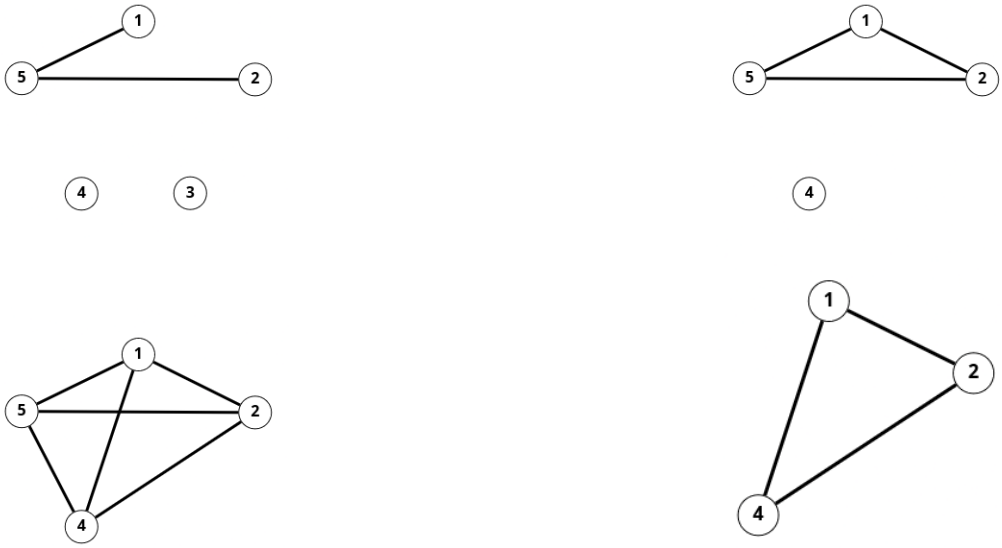
Sea $G = (V, E)$ un grafo. Se dice que $G' = (V', E')$ es subgrafo de $G = (V, E)$ si

1. G' es un grafo por si mismo
2. $V' \subset V$, $E' \subset E$

Ejemplo

Algunos subgrafos de





Subgrafos de G_1

Es claro que un isomorfismo lleva a un subgrafo de G_1 hacia un subgrafo isomorfo. Este resultado es una herramienta que puede ser útil para ver si dos grafos no son isomorfos. Es decir, si en un grafo encontramos un subgrafo, para que un grafo sea isomorfo debe también tener el subgrafo.

Ejemplo

Dado dos grafos G_1 y G_2 determinar si son o no isomorfos.

Solución

En este caso G_1 y G_2 no son isomorfos, pues $K_4 \subset G_1$ y $K_4 \not\subset G_2$. Entonces, más allá de tener la misma cantidad de vértices y aristas G_1 y G_2 no son grafos isomorfos y lo demostramos con la regla enunciada anteriormente.

Atención

Pueden existir sub-grafos que se encuentren en ambos, pero de encontrarse uno que no, entonces los grafos no son isomorfos, pues debe cumplirse que si se encuentra en uno, también se encuentre en el otro para todo sub-grafo de ambos.

5.2. Valencia o Grado

Definición

La valencia o grado de un vértice v en un grafo $G = (V, E)$ es el número de aristas de G que contienen v, es decir, la cantidad de aristas vinculadas (que salen o que llegan) con v. Usaremos la notación $\delta(v)$ para la valencia de v, que formalmente esta definida como

$$\delta(v) = |D_v|, \text{donde } D_v = \{e \in E | v \in e\}$$

$\delta(v)$ = cardinal del conjunto de las aristas, tal que v es vértice de dicha arista.

Ejemplo

En vez de darle un nombre al vértice, colocar el número de valencia que tiene el mismo

Solución

Gráficamente es muy visible la cantidad de aristas vinculadas a un vértice, en el conjunto de E, para saber el grado de cada vértice, contamos la cantidad de ocurrencias del mismo, y en la lista de adyacencia es la altura de la columna de dicho vértice.

Ejemplo

Supongamos que queremos encontrar la lista de adyacencia y el grado de los vértices de un grafo $G = (V, E)$ definido como

$$v = \{a,\ b,\ c,\ d,\ z\} \qquad E = \{\{a,\ b\}, \{a,\ b\}, \{a,\ b\}, \{a,\ b\}, \{a,\ b\}\}$$

Solución

Entonces la lista de adyacencia será

a	b	c	d	z
b	a	d	c	b
d	z		z	d
			a	

Y por lo tanto los grados de los vértices son $\delta(a) = 2,\ \delta(b) = 2,\ \delta(c) = 1, \delta(d) = 3, \delta(z) = 2$

Teorema

La suma de los valores de las valencias $\delta(v)$, tomados sobre todos los vértices v del grafo $G = (V, E)$, es igual a dos veces el número de aristas

$$\sum_{v \in V} \delta(v) = 2 \cdot |E|$$

Demostración

La valencia de un vértice v indica la cantidad de 'extremos' de aristas que 'tocan' a v. Es claro que hay $2 \cdot |E|$ extremos de aristas, luego la suma total de las valencias de los vértices es $2 \cdot |E|$.

Hay un útil corolario de este resultado. Diremos que un vértice v es impar si su valencia o grado es impar, y par si su valencia es par.

Denotemos V_i el conjunto de vértices impares y V_p el conjunto de vértices pares, luego $V = V_i \cup V_p$ es una partición de V. Luego

$$\sum_{v \in V_i} \delta(v) + \sum_{v \in V_p} \delta(v) = 2 \cdot |E|$$

Entonces

$$\sum_{v \in V_i} \delta(v) = 2 \cdot |E| - \sum_{v \in V_p} \delta(v) \qquad \text{Es par}$$

Esto nos dice que cada término en la segunda sumar es par, luego esta suma es un numero par. Puesto que el lado derecho también es un numero par, la primera suma debe ser un numero par. Pero la suma de números impares solo puede ser par si el numero de términos es par. En otras palabras:

Teorema

El numero de vértices impares es par. Este resultado es a veces llamado 'Handshaking Lemma'.

Dado un conjunto de personas, el numero de personas que le ha dado la mano a un número impar de miembros del conjunto es par.

Un grafo en el cual todos los vértices tienen la misma valencia r se llama regular con valencia r, o r-valente. Luego

$$r \cdot |V| = 2 \cdot |E|$$

Tenemos por ejemplo K_n es regular $(n-1)$-valente, y C_n, el polígono de n-lados. Si $n \geqslant 3$, C_n es regular de valencia 2.

C_n es llamado grafo cíclico de n vértices. Formalmente $C_n = (V, E)$, con

$$V = \{1, 2, ..., n\}, \qquad E = \{\{1, 2\}, \{2, 3\}, ..., \{n, 1\}\}$$

y el gráfico de por ejemplo C_6 es

Ejemplo

Veamos las valencias del grafo rueda 0, 1, ..., n

Solución

De forma general, un grafo W_n tiene $(n-1)$ aristas en el vértice 0 y 3 aristas en el resto de vértices, si n es impar entonces hay una cantidad de vértices impares, par. Si n es par hay un vértice par y n vértices pares.

Debemos saber que no hay forma general de determinar si un grafo es isomorfo a otro o no, para determinarlo debemos ayudarnos de los conceptos teóricos que los definen.

Una aplicación importante de valencias es determinar si dos grafos son o no isomorfos.

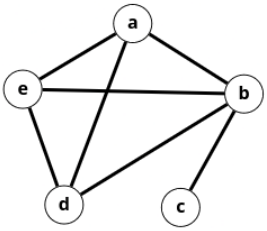
Si $\alpha : V_1 \to V_2$ es un isomorfismo entre G_1 y G_2, y $\alpha(v) = w$, entonces cada arista que contiene a v se transforma en una arista que contiene a w.

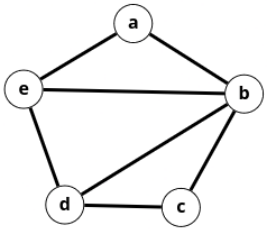
En consecuencia $\delta(v) = \delta(w)$. Por otro lado, si G_1 tiene un vértice x, con valencia $\delta(x) = \delta_0$ y G_2 no tiene vértices con valencia δ_0, entonces G_1 y G_2 no pueden ser isomorfos.

Entonces, una forma de determinar el isomorfismo es mirar la lista de valencias, si no son iguales, entonces G_1 y G_2 no pueden ser isomorfos.

Ejemplo

Esto nos da otra manera de ver que estos dos grafos no son isomorfos





Puesto que el primer grafo tiene un vértice de $\delta(v) = 1$ y el segundo no tiene ninguno con $\delta(v) = 1$.

Una extensión de esta idea se da en la siguiente proposición.

Proposición

Sean G_1 y G_2 grafos isomorfos. Para cada $k \geqslant 0$ sea $n_i(k)$ el numero de vértices de G_i que tienen valencia k $(i = 1,\ 2)$. Entonces $n_1(k) = n_2(k)$

Es decir, si hay 5 vértices de valencia 1 en G_1 tiene que haber 5 vértices de valencia 1 en G_2, si no, no pueden ser isomorfos.

Demostración

Hemos visto mas arriba que si $\alpha : V_1 \to V_2$ es un isomorfismo entre G_1 y G_2 y $v \in V_1$, entonces $\delta(v) = \delta(\alpha(v))$.

Luego, la cantidad de vértices con valencia K en G_1 es igual a la cantidad de vértices con valencia K en G_2.

Atención

Que cumplan la proposición anterior no hace a dos grafos isomorfos, si no que es una condición necesaria para que lo sean. En el siguiente ejemplo, no se aplica el criterio anterior.

Ejemplo

Probar que los siguientes grafos no son isomorfos

Solución

La diferencia y lo que hace que no sean isomorfos es que G_1 tiene un sub-grafo K_3 y G_2 no lo tiene.

Si vemos, estos dos grafos tienen misma cantidad de vértices, de aristas y su tabla de valencias, sin embargo, no cumple con el isomorfismo, es decir, no existe la biyección entre G_1 y G_2

Entonces, para que dos grafos sean isomorfos, debe cumplirse que

1. Misma cantidad de vértices $|V_1| = |V_2|$.
2. Misma cantidad de aristas $|E_1| = |E_2|$.
3. Misma lista de valencias.
4. G_1 contener todos los sub-grafos posibles de G_2 y viceversa.

Resultado del teorema anterior.

Corolario

Si G_1 y G_2 son grafos, G_1' sub-grafo de G_1 y no existe sub-grafo de G_2 isomorfo a G_1', entonces G_1 y G_2 no son isomorfos.

5.3. Caminatas, caminos y ciclos

Definición

Una **caminata** en un grafo G es una secuencia de vértices

$$v_1, v_2, ..., v_k,$$

tal que v_i y v_{i+1} son adyacentes (Quiere decir que están conectados mediante una arista) $(1 \leq i \leq k-1)$.

Si todos los vértices son distintos, una caminata es llamada **camino**.

Por otro lado llamaremos **recorrido** a una caminata que repite vértices y no aristas.

Es decir una caminata especifica una ruta en G: del primer vértice vamos a uno adyacente, de este a otro adyacente y así siguiendo. En una caminata podemos visitar cualquier vértice varias veces, y en particular, podemos ir de un vértice x a otro y luego tomar la dirección contraria y regresar a x. Mientras que en un camino, cada vértice es visitado solo una vez.

Llamaremos **ciclo** a una caminata v_1,v_2,...,v_k con $k \geqslant 3$ y cuyos vértices son distintos exceptuando los extremos, es decir que v_1,v_2,...,v_{k-1} es un camino de al menos tres vértices y $v_1 = v_k$. A menudo diremos que es un k-ciclo o un ciclo de longitud k en G.

Definiremos cómo **circuito** a una caminata v_1,v_2,...,v_k con $k \geqslant 3$ donde $v_1 = v_k$ pero puede repetir vértices y aristas.

Observación de ciclos y circuitos
$k \geqslant 3$, si no, es imposible hacer una caminata cerrada.

Un ciclo siempre será un circuito pero un circuito puede no ser un ciclo.

Ejemplo
caminatas, caminos, recorridos, circuitos y ciclos en el siguiente grafo

Caminata = p, q, t, s, q, r, u.
Camino = p, q, s, r, u, t.
Recorrido = p, s, r, u, t, s, q
Ciclo = p, q, s, r, u, t, p.
Circuito = p, q, t, s, r, u, t, s, p

Una caminata es isomorfa a algo así

Debido a que vuelve a los mismos vértices.

Un camino es isomorfo a una recta, debido a que no se repiten vértices.

Un ciclo es isomorfo a estructuras poligonales, debido a que en su trayecto no se repiten vértices, pero el último es el mismo vértice que el primero.

Lema
Sea G un grafo. Entonces, x e y pueden ser unidos por una caminata si y solo si x e y pueden ser unidos por un camino.

Idea de la demostración

($\Leftarrow$) Es trivial, si puedo llegar de x a y por un camino, entonces puedo por una caminata, pues todo camino es caminata.

($\Rightarrow$) Si puedo llegar de x a y por una caminata, también podre por un camino, eliminando los bucles, pues esto es lo único que diferencia una caminata de un camino.

Notación

Escribiremos $x \sim y$ siempre que los vértices x e y de G puedan ser unidos por un camino en G, de forma rigurosa significa que existe un camino $V_1, V_2, ..., V_k$ en G con $x \equiv V_1$ e $y \equiv V_k$.

Definición

Sea G un grafo, diremos que es conexo si cumple que $x \sim y$ para cualquier x, y vértices en G. El lema anterior implica que $\sim$ es una relación de equivalencia.

Ejemplo

Veamos un ejemplo de un grafo conexo y otro no conexo

Cuando tenemos grafos no conexos, tenemos sub-grafos sin ningún tipo de conexión, como en G_2, veamos que todo grafo puede dividirse en sub-grafos conexos llamados componentes conexas.

Ejemplo

Veamos en G que no hay relación alguna entre los sub-grafos G_1, G_2, G_3. Estas son las componentes conexas de G.

Proposición Sea G Grafo y $x,\ y,\ z$ vértices de G. Entonces,

1. $x \sim x$ (reflexividad del $\sim$)
2. $x \sim y$ entonces $y \sim x$ (simetría del $\sim$)
3. $x \sim y$, $y \sim z$ entonces $x \sim z$ (transitividad del $\sim$)

Demostración

1. El camino de x relaciona x con x.
2. Si $x = x_1,\ x_2,\ ...,\ x_k = y$ es un camino de x a $y = x_k,\ ...,\ x_2,\ x_1 = x$ es un camino de y a x
3. $x \sim x \Rightarrow$ Hay un camino de x a y
   $y \sim z \Rightarrow$ Hay un camino de y a z
   Pegando los caminos en y, obtenemos un camino de x a z

Es por ello que $\sim$ es un símbolo de equivalencia

5.4. Caminatas Eulerianas y Ciclos Hamiltonianos

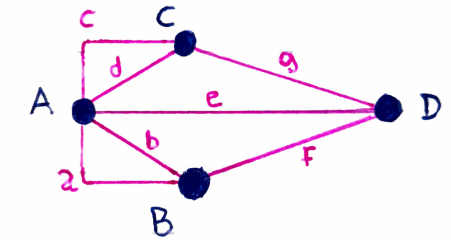
Origen

¿Es posible cruzar todos los puentes de Königsberg pasando una y solo una vez por cada uno?

Esta fue la pregunta que se hizo Euler que dio nacimiento a la teoría de grafos.

Realizando esta abstracción, Euler se dio cuenta de que existían 4 regiones (A, B, C, D) y 7 puentes que las conectaban (a, b, c, d, e, f , g).

Posteriormente, Leonard simplificó aún más su problema y realizó una abstracción un poco más clara para estudiarlo, un nuevo tipo de representación, un grafo.



En el que cada región es un vértice y a cada puente le corresponde una arista.

Entonces ahora el problema se reduce a encontrar una caminata que use cada arista (o puente) una y solo una vez.

Hasta aquí Euler solo abstrajo el problema poniéndolo en un lenguaje donde las posibilidades de resolverlo son mayores (es mas adecuado), y ahí Euler se dio cuenta que suponiendo que salgamos de un vértice cualquiera, cada vez que llego a un vértice, tengo que volver a salir, entonces cada vez que paso por un nodo quemo 2 puentes, y a excepción del punto final e inicial, cada vez que entro a un nodo tengo que salir, entonces cada punto que no es inicial o final tiene que tener valencia par.

Como en el ejemplo de los puentes de Königsberg, todos los vértices tienen valencia par, el mismo posee solución alguna.

Luego, Euler razonó que si hay 2 vértices de valencia impar y el resto de valencia par, si existe solución y los vértices de valencia impar son los de origen y llegada. Este fue el nacimiento de la teoría de grafos.

Luego, el algoritmo general fue publicado por diversos autores, entonces formalizando

Observación

$$\alpha(A) = 5,\ \alpha(B) = 3,\ \alpha(c) = 3,\ \alpha(D) = 3$$

Euler, abstrayéndose del problema concreto, razonó

- Supongamos que el vértice de partida es x, el de llegada es y. A todos los demás los llamaremos vértices intermedios.
- En un vértice intermedio cada vez que entro por un puente salgo por otro. Eso me .ªporta"2 a la valencia.
- Terminando el proceso usaremos todos los puentes, por lo tanto en cada vértice intermedio la cantidad de entradas mas la cantidad de salidas es la valencia. Como la cantidad de entradas es igual a la de salidas, la valencia en los vértices intermedios es par.

Concluyendo

- Si hay una caminata que pasa por cada puente una y solo una vez, la cantidad de vértices con valencia impar es a lo sumo 2.
- Como todos los vértices tienen valencia impar, el problema no tiene solución.

Veremos luego que, el problema de los puentes de Königsberg puede ser generalizado y también vale la recíproca.

Ejemplo

¿Es posible recorrer el siguiente grafo con una caminata que pase por cada vértice una sola vez y volver al de partida? ¿Es posible hacer una caminata que pasa por cada arista una sola vez?

Solución

Para la primer pregunta una posibilidad es el ciclo dado por:

$$p,\ q,\ t,\ s,\ u,\ r,\ p$$

La segunda pregunta tiene respuesta negativa ya que las valencias son:

$$\alpha(p) = 4,\ \alpha(q) = 4,\ \alpha(s) = 5,\ \alpha(r) = 5, \alpha(u) = 4,\ \alpha(t) = 5$$

Como en los puentes de Königsberg, al haber más de 2 vértices de valencia impar, no es posible recorrer todas las aristas una sola vez.

Definición

Un **ciclo hamiltoniano** en un grafo G es un ciclo que contiene a todos los vértices del grafo.

Una **caminata euleriana** en un grafo G es una caminata que usa todas las aristas de G exactamente una vez. Una caminata euleriana que comienza y termina en un mismo vértice se llama también circuito euleriano.

Teorema
Un grafo conexo con mas de un vértice tiene un circuito euleriano si y solo si todos los vértices tienen grado par.

Un grafo conexo con más de un vértice posee caminatas eulerianas de V a W, con $V \neq W$ si y solo si V y W, son los únicos vértices de grado impar.

Concluimos en que si hay 0 vértices de valencia impar existe una caminata euleriana que parte de un vértice y llega al mismo, también se lo conoce como circuito euleriano. Otro caso es que haya 2 vértices de valencia impar, en este también existirá una caminata euleriana donde el vértice inicial es distinto al vértice final y ambos son los que tienen valencia impar respecto al resto de vértices con valencia par. Por último, si hay 2 o más vértices de valencia impar, no existe caminata euleriana.

Idea de la demostración
Observemos que toda caminata que no repite aristas (recorrido maximal) en un grafo par se detiene en el origen.

Algoritmo de Hierholzer
Para encontrar caminatas eulerianas en un grado par:

1. Paso 1. Elija cualquier vértice inicial y haga un recorrido maximal (recorrido cerrado, puede no cubrir todas las aristas).
2. Paso Iterativo.
   i) Mientras exista un vértice U en la caminata ya realizada, pero que tenga aristas que no formen parte de la caminata, inicie otro recorrido maximal (será de U a U) siguiendo las aristas no utilizadas.
   ii) Inserte esta caminata a la caminata anterior en U para formar una caminata nueva (más larga).
   iii) Si no cubrió todas las aristas vuelva a i).

En el paso iterativo el sub-grafo que obtenemos luego de quitar las aristas recorridas es par. Esto nos permite hacer caminatas cerradas por aristas no utilizadas desde cada vértice con aristas no utilizadas.
El caso de un grafo donde todas las valencias son pares excepto 2 se puede reducir al anterior, si deseamos una caminata euleriana que empiece por v y termine en w.

- Comenzamos en v y hacemos una caminata que no repita aristas hasta que se detenga
- Eliminamos

Ejemplo

Encontremos un circuito euleriano del siguiente grafo Suponiendo que tomamos el recorrido maximal

u, t, s, r, u. En este no podremos continuar sin repetir aristas, pero sí hay vértices donde tenemos aristas no recorridas, y entonces realizamos otro recorrido maximal desde alguno de estos vértices con aristas por recorrer, por ejemplo t, q, s, p, r, q, p, t.

Ahora hemos recorrido todas las aristas por lo que no podemos encontrar otro recorrido maximal sin pisar los anteriores, todo ha sido recorrido, pero vemos que tenemos dos recorridos maximales, entonces debemos insertar el segundo recorrido maximal encontrado, en el primero.

Para insertar uno en el otro veamos que el segundo comienza y termina en t, lo que nos va a permitir insertar sin problemas el segundo recorrido donde en el primero t, luego volverá a t y continuará el primer recorrido, completando así la totalidad de las aristas.

$u,\ t,\ q,\ s,\ p,\ r,\ q,\ p, t,\ s,\ r,\ u$ *Primer recorrido*

Segundo recorrido

Y así queda aplicado el algoritmo de Hierholzer dando como resultado una de las posibles caminatas eulerianas.

Cuando el primer recorrido inicia y termina en un vértice diferente al inicial se procede igual, se busca otro recorrido maximal entre las aristas que queden libres, hasta que no haya libres y luego se reemplazan en el recorrido principal.

Debemos de saber que existen códigos de los algoritmos para encontrar recorridos maximales y el algoritmo de Hierholzer.

5.5. Arboles

Definición

Diremos que un grafo T es un árbol si cumple que es conexo y no hay ciclos en T.

Los arboles permiten modelar muchos problemas de la vida real, por ejemplo, los algoritmos de decisión, donde se bifurcan o separan los resultados según la decisión. (Arboles de decisión). Estos aparecen especialmente en investigación operativa y ciencias de la computación.

El siguiente lema nos resultara útil para probar una parte del teorema fundamental de esta sección.

Lema

Sea $G = (V,\ E)$ es un grafo conexo, entonces $|E| \geqslant |V| - 1$

Demostración

Como G es conexo existe una caminata que recorre todos los vértices de G:

$$V_1,\ V_2,\ ...,\ V_r$$

Renombremos los vértices de G con números naturales de forma tal que el primer vértice de la caminata sea 1, el segundo 2 y cada ve que aparece un vértice que no ha sido nombrado se le asigna el numero siguiente.

Luego la caminata comienza en 1 y termina en n, donde $n = |v|$

Observación

Si i tal que $1 < i \leqslant n$ tenemos que la caminata tiene la forma.

$$1, ...,\ j_i,\ i, ...,\ j_n,\ n$$

Dónde $j_i < i$, luego es claro que

$$\{j_2,\ 2\}, \{j_3,\ 3\}, ..., \{j_n,\ n\}$$

Forman un conjunto de $n - 1$ aristas distintas en G

El siguiente teorema nos da 4 nociones equivalentes a la definición de árbol.

Teorema

Si $T = (V,\ E)$ es un grafo conexo con al menos dos vértices, entonces son equivalentes las siguientes propiedades.

T_1) T es un árbol.

T_2) Para cada par $x,\ y$ de vértices existe un único camino en T de x a y.

T_3) El grafo obtenido en T removiendo alguna arista tiene dos componentes, cada una de las cuales es un árbol.

T_4) $|E| = |v| - 1$.

Este teorema puede demostrarse haciendo las pruebas.

$$T_1 \Rightarrow T_2 \Rightarrow T_3 \Rightarrow T_4 \Rightarrow T_1$$

Luego, toda la equivalencia se deduce de estas implicaciones, por ejemplo:

$$T_1 \Leftrightarrow T_4 \text{ pues} = \begin{cases} T_1 \Rightarrow T_2 \Rightarrow T_3 \Rightarrow T_4 \\ T_4 \Rightarrow T_1 \end{cases}$$

Podemos verlo así:

Idea de la demostración

- $(T_1 \Rightarrow T_2)$ Si hubiera dos caminos podríamos formar un ciclo.
- $(T_2 \Rightarrow T_3)$ Sea $G' = T - uv$ Como hay un único camino de u a v, G' tiene dos componentes conexas: T_1 la componente conexa de u y T_2
- $(T_3 \Rightarrow T_4)$ Se hace por inducción completa sobre el numero de vértices y usando la propiedad T_3
- $(T_4 \Rightarrow T_1)$ $|E| = |v| - 1$ y supongamos que T no es árbol $\Rightarrow$ Hay un ciclo $\Rightarrow$ Podemos sacar una arista uv y sigue siendo conexo $\Rightarrow$ $|E - uv| = |V| - 2$ y conexo. Absurdo por el lema.

5.6. Coloreo y número cromático

Problema

Supongamos que queremos realizar un horario de actividades sin interferencias.

Ejemplo

Supongamos que deseamos hacer un horario con seis cursos de una hora, $v_1,\ v_2,\ v_3,\ v_4,\ v_5,\ v_6$. Entre la audiencia potencial hay gente que desea asistir simultáneamente a

$$\{v_1,\ v_6\},\ \{v_1,\ v_2\},\ \{v_1,\ v_4\},\ \{v_3,\ v_5\},\ \{v_2,\ v_6\},\ \{v_4,\ v_5\},\ \{v_5,\ v_6\}$$

¿Cuantas horas son necesarias para poder confeccionar el horario en el cual no haya interferencias?

Solución

Podemos representar la situación con un grafo donde los vértices son los cursos y las aristas o conexiones, el interés de la audiencia de hacer ambos. Entonces

Las aristas entonces son las interferencias potenciales. Esto quiere decir que no podemos dar en la misma hora aquellos cursos que están conectados por una arista. Ej V_5 y V_6

Un horario que cumple con la condición de evitar interferencias es el siguiente

Hora 1	Hora 2	Hora 3	Hora 4
V_1 y V_3	V_2 y V_4	V_5	V_6

Es una partición del conjunto de vértices en cuatro partes con la propiedad que ninguna parte contiene un par de vértices adyacentes del grafo. Claramente le corresponde una función

$$C : \{v_1,\ v_2,\ v_3,\ v_4,\ v_5,\ v_6\} \to \{1,\ 2,\ 3,\ 4\}$$

Dónde

$$C_{v_1} = C_{v_3} = 1\ ;\ C_{v_2} = C_{v_4} = 2\ ;\ C_{v_5} = 3\ ;\ C_{v_6} = 4$$

También podemos representar esta función como un coloreo de vértices donde dos vértices adyacentes tienen distintos colores.

Cualquiera de las formas de representar el resultado nos daría una solución (quizás no la mejor).

Esto es llamado coloreo, donde asignamos etiquetas a los vértices de tal forma que 2 vértices con la misma etiqueta no tienen una arista que los una.

Formalizando el coloreo de vértices podemos enunciar.

Definición.
Una coloración de vértices de un grafo $G = (V,\ E)$ es una función $C : V \to \mathbb{N}$ con la siguiente propiedad

$$C(x) \neq C(y)\ si\ \{x,\ y\} \in E$$

El numero cromático de G, denotado $\chi(G)$ se define como el **mínimo** entero K para el cual existe una coloración de vértices de G usando K-Colores.

En otras palabras, $\chi(G) = k$ si y sólo si existe una coloración de vértices C la cual es una función de V a $\mathbb{N}_k$, y k es el mínimo entero con esta propiedad.
Volviendo al ejemplo de los horarios, nuestro primer intento fue de 4 colores.

Un rápido intento con tres colores nos da la solución de este problema

Hora 1	Hora 2	Hora 3
V_1	V_2 y V_5	V_3, V_4 y V_6

Mas aún, hace falta por lo menos tres colores, puesto que V_1, V_2 y V_6 forman un grafo completo K_3, es decir, son mutuamente adyacentes.

Luego concluimos que el número cromático del grafo o problema es 3.

Podemos representar la coloración en el grafo de la forma

Como vemos en la selección, tenemos un subgrafo G' que es equivalente a un grafo K_3, es decir, 3 vértices están conectados y son adyacentes mutuamente, entonces necesitaremos como mínimo 3 colores para pintar a G.

Atención

Cuando encontramos un subgrafo G' equivalente a algún K_n, el número cromático $\chi(G)$ tiene que ser mayor o igual a n.

En general, para probar que el número cromático de un grafo dado es k, debemos proceder de la siguiente forma

a) Encontrar una coloración de vértices usando k colores.

b) Probar que ninguna otra coloración de vértices usa menos de k colores.

¿Existe algún algoritmo general eficiente para encontrar el número cromático? No, sin embargo existen algoritmos para encontrar una coloración de vértices que aunque no es óptima nos da un resultado satisfactorio. Estos algoritmos son del orden del $n!$.

Ejemplo

¿Cuantos son los colores necesarios para pintar un grafo completo K_n?

Solución

Veamos el ejemplo del K_4

Comencemos dándole el color 1 a A, luego como B es adyacente a A, le asignaremos el color 2, continuamos por C que al ser adyacente con A y B le damos el color 3 y por último D que al ser adyacente con A, B, C le tendremos que otorgar el color 4. Este es el número cromático de K_4, pues al ser todos los vértices mutuamente adyacentes podemos ver que para algún grafo K_n, el número cromático $\chi(G)$ será la cantidad de vértices (n) del grafo.

A partir de esta reflexión podemos enunciar

Proposición
Si el grafo $G = (V, E)$ tiene un subgrafo G' equivalente a K_n, entonces $\chi(G) \geqslant n$

Veamos ahora el caso de los grafos cíclicos.

Ejemplo
¿Cuantos colores necesitamos como mínimo para colorear un grafo cíclico C_n?

Solución
Veamos algunos ejemplos

Como A, B y C son mutuamente adyacentes
cada vértice tendrá su color. $\chi(C_3) = 3$

Como A y B son adyacentes llevan 1 y 2, pero C
no es adyacente con A y D no lo es con B,
por lo que llevan 1 y 2. Entonces $\chi(C_4) = 2$

Con la misma analogía que el caso anterior
completamos A, B, C y D pero al colorear E vemos
que es adyacente a A y D, por lo que le corresponde
el color 3, entonces $\chi(C_5) = 3$

Podemos continuar y veremos que $\chi(C_n)$ es 2 si n es par y $\chi(C_n)$ es 3 si n es impar.

Como dijimos, existen algoritmos que no son exactos pero nos sirve su respuesta ya que es bastante aproximada, esto nos lleva a introducir un tipo de algoritmo.

5.7. Algoritmos Greedy

Definición

Los algoritmos greedy o golosos son un tipo de algoritmos 'ingenuos', que eligen lo mejor en el momento pensando en que será lo mejor para después, son algoritmos no previsores.

Por ejemplo, el algoritmo para encontrar caminatas eulerianas es un algoritmo greedy, ya que en el momento no se preocupa y elige el primer camino que encuentre libre, y continua así hasta ya no poder avanzar, si aún quedan aristas, realiza el mismo proceso con las restantes. En este caso, el algoritmo greedy nos da una solución perfecta, a veces ocurre así, ser ingenuo a veces es conveniente.

5.7.1. Algoritmo greedy para la coloración de vértices

No se conoce ningún algoritmo general para encontrar el numero cromático de un grafo que trabaje en 'tiempo polinomial', sin embargo, hay un método simple de hacer una coloración cromática usando un 'razonable' numero de colores.

El algoritmo es muy sencillo y se puede escribir en una sola línea. Si hay vértices no coloreados, elegimos un vértice no coloreado y le otorgamos un color que no tengan sus vecinos.

En este algoritmo hacemos la mejor elección que podemos en cada paso, sin mirar más allá para ver si esta elección nos traerá problemas, y es por ello que es un algoritmo greedy. El algoritmo greedy es fácil de programar.

Supóngase que hemos dado a los vértices algún orden $v_0,\ v_1, ...,\ v_n$

- Asignemos el color 0 a v_0.
- Tomamos v_i el siguiente vértice de la lista y S = el conjunto de colores asignados a los vértices $v_j (0 \leqslant j < i)$ que son adyacentes a v_i.
  - Le damos a v_i el primer color que no está en S.
- Si $i < n$ volvemos a hacer el procedimiento del paso anterior para $i = i + 1$

Debido a que la estrategia greedy es 'corta de vista' o no previsora, el numero de colores que usara sera normalmente mas grande que el mínimo posible.

Ejemplo

Aplicar el algoritmo greedy a

Solución

El orden de los vértices es $v_1,\ v_2,\ v_3,\ v_4,\ v_5,\ v_6$

El algoritmo es

- Paso 1: v_1 tiene colores vecinos S $= 0 \Rightarrow v_1$ color 0.
- Paso 2: v_2 tiene colores vecinos S $= \{0\} \Rightarrow v_2$ color 1.
- Paso 3: v_3 tiene colores vecinos S $= 0 \Rightarrow v_3$ color 0.
- Paso 4: v_4 tiene colores vecinos S $= \{0\} \Rightarrow v_4$ color 1.
- Paso 5: v_5 tiene colores vecinos S $= \{0, 1\} \Rightarrow v_5$ color 2.
- Paso 6: v_6 tiene colores vecinos S $= \{0, 1, 2\} \Rightarrow v_6$ color 3.

Es decir, el coloreo queda

El orden que se elige inicialmente para los vértices es fundamental para establecer la coloración. Es bastante fácil ver que si se elige el orden correcto, entonces el algoritmo greedy nos da la mejor coloración posible pero hay $n!$ ordenes posibles, y si tuviéramos que controlar cada uno de ellos, el algoritmo requeriría 'tiempo factorial'.

Ejemplo

Aplicar el algoritmo greedy al siguiente grafo donde el orden de los vértices es $v_3,\ v_4,\ v_6,\ v_2,\ v_5,\ v_1$

Solución

El algoritmo es

- Paso 1: v_3 tiene colores vecinos S $= 0 \Rightarrow v_3$ color 0.
- Paso 2: v_4 tiene colores vecinos S $= 0 \Rightarrow v_4$ color 0.
- Paso 3: v_6 tiene colores vecinos S $= 0 \Rightarrow v_6$ color 0.
- Paso 4: v_2 tiene colores vecinos S $= \{0\} \Rightarrow v_2$ color 1.
- Paso 5: v_5 tiene colores vecinos S $= \{0,\} \Rightarrow v_5$ color 1.
- Paso 6: v_1 tiene colores vecinos S $= \{0,\ 1\} \Rightarrow v_1$ color 2.

Podemos representar en el grafo la coloración

El coloreo queda igual a como vimos antes.

El orden fue elegido de la siguiente forma: dado el coloreo con colores $\chi(G)$, se elige, en el orden, primero los vértices de un solo color que haya mayor cantidad, luego de otro color que haya mayor cantidad, etc.

Más allá que el algoritmo greedy no soluciona el problema, el algoritmo es útil tanto en la teoría como en la práctica.

Probaremos ahora algunos resultados por medio de la estrategia greedy.

Teorema

Si G es un grafo con valencia máxima K, entonces.

a) $\chi(G) \leqslant k + 1$

b) Si G es conexo y no regular, $\chi(G) < K$

No regular significa que habrá vértices de valencia máxima K, pero también habrá vértices con valencia mas chica.

Demostración

a) Sea $v_1,\ v_2, ..,\ v_n$ un ordenamiento cualquiera de los vértices de G.
Para cada vértice v, si S son los colores de los vecinos a $v \Rightarrow |s| \leqslant k$

b) Sea v_n un vértice con $\delta(v_n) < k$.

1) Sean $v_{n-1},\ v_{n-2}, ..,\ v_{n-r}$ los adyacentes a v_n. Hay como máximo $k-1$ de ellos.
2) Luego se van eligiendo los adyacentes a v_i que no están listados antes $(n > u \geqslant 1)$
3) Si $i < n$ el vértice v_i tiene un adyacente a nivel superior $\Rightarrow v_i$ tiene como máximo $k-1$ adyacentes a nivel inferior.
4) Si $i < n$, usando greedy y por (3), se puede colorear v_i con un color en $\{1, ..., k\}$
5) Por (1) se puede colorear v_n con un color en $\{1, .., k\}$

5.8. Grafos bipartitos

Definición
Sea G un grafo diremos que G es bipartito si $\chi(G) = 2$. Es decir, si se puede colorear con dos colores.

Ejemplo
Notemos que G_1 y G_2 son isomorfos

Bipartito significa 2 partes, y como vemos, podemos enfatizar la diferencia en el cubo (G_1) obteniendo G_2 en el que cada columna es una parte separada de la otra, donde ningún vértice se conecta con otro de la misma columna, como en G_2.

Una consecuencia importante del algoritmo greedy es el siguiente teorema

Teorema
Un grafo es bipartito si y sólo si no contiene ciclos de longitud impar.

Demostración

($\Rightarrow$) El contrarrecíproco: Si G tiene un ciclo de longitud impar $\Rightarrow$ No es bipartito.
Esto es cierto, pues un ciclo de longitud impar requiere 3 colores.

($\Leftarrow$) Supongamos que G es un grafo sin ciclos de longitud impar y conexo. Construiremos un orden de G para el cual el algoritmo greedy producirá una coloración de vértices con dos colores.

- Elijamos cualquier vértice y llamémoslo V_1; diremos que V_1 está en el nivel 0
- A continuación, listemos la lista de vecinos de V_1, llamémoslos V_2, V_3, ..., V_r; diremos que estos vértices están en el nivel 1.
- Continuando de esta manera, definimos el i como todos aquellos vértices adyacentes a los de nivel $i-1$, exceptuando aquellos previamente listados en el nivel $i-2$.

Cuando ningún nuevo vértice puede ser agregado de esta forma, obtenemos G (pues es conexo).

El hecho crucial producido por este orden es que un vértice del nivel i solo puede ser adyacente a vértices de los niveles $i-1$ e $i+1$, y no a vértices del mismo nivel.

Gráficamente podemos ver a los niveles de la siguiente forma

Veamos el por que 2 vértices del mismo nivel no pueden ser adyacentes

Supongamos que x e y son vértices en el mismo nivel.

Entonces ellos son unidos por caminos de igual longitud m a algún vértice z de un nivel anterior.

Los caminos pueden ser elegidos de tal manera que z sea el único vértice común.

Si x e y fueran adyacentes, habría un ciclo de longitud $2m + 1$, lo cual contradice la hipótesis.

Se deduce entonces que el algoritmo greedy asigna

- El color 1 a los vértices en el nivel 0, 2, 4, 6...
- El color 2 a los vértices en el nivel 1, 3, 5, 7...

Por consiguiente $\chi(G) = 2$ (Bipartito)

Veamos esto en el ejemplo anterior

5.9. Grafos planares

Definición

Un grafo planar es una representación de un mapa.
Se llaman planares porque se pueden dibujar sin cortes, es decir, sin que ninguna arista corta a otra.

Ejemplo

Solución

Se puede hacer un grafo a partir de un mapa donde cada país es un vértice y están conectados por una arista si son limítrofes.

Dibujemos el grafo planar de nuestro mapa ejemplo.

Pregunta

¿Cuál es el mínimo numero de colores para colorear un mapa de tal forma que dos regiones limítrofes no tengan el mismo color?

Respuesta

4. Con 4 colores podremos colorear cualquier mapa.