Matemática Discreta

Índice general

Prólogo

Este cuadernillo tiene la intención de introducir a los alumnos en temas de matemática discreta. Esta basado en el libro *Discrete Mathematics* de N. L. Biggs, Oxford University Press, 1993. Tiene aportes de A. Tiraboschi y un apéndice de grafos planares escrito por D. Penazzi.

CAPíTULO 1

Números Enteros

1.1. Aritmética

Todo lector de este libro conoce los *enteros*. En una etapa muy temprana de nuestras vidas conocemos los números enteros positivos o "números naturales"

$$1, 2, 3, 4, 5, \ldots$$

Más adelante introducimos el 0 (cero), y los enteros negativos

$$-1, -2, -3, -4, -5, \ldots$$

En matemática generalmente no nos preocupamos por el significado lógico y/o filosófico de estos objetos, pero necesitamos saber las propiedades que se supone que tienen. Si todos parten de las mismas suposiciones entonces todos llegarán a los mismos resultados. Estos supuestos son los llamados axiomas.

El punto de vista adoptado en este libro es el señalado antes. Aceptamos sin reparo que existe un conjunto de objetos llamados *enteros* conteniendo los enteros positivos y los negativos, y el cero, familiares en nuestra temprana educación y experiencia. 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. Empezaremos listando aquellos axiomas que tratan la suma y la multiplicación.

Adoptaremos las notaciones usuales $a + b$ para la suma de dos enteros a y b, y $a \times b$ (o frecuentemente solo ab) para su producto. Pensamos en $+$ y $\times$ como *operaciones* que a un par de enteros a y b les hacen corresponder un entero $a+b$ y otro $a \times b$. El hecho de que $a \times b$ y $a+b$ son enteros, y no algún objeto extraño como elefantes, es nuestra primera suposición (Axioma **I1**). En la siguiente lista de axiomas a, b, c denotan enteros arbitrarios, y 0 y 1 denotan enteros especiales que cumplen las propiedades especificadas en alguno de los siguientes axiomas.

I1. $a + b$ y ab pertenecen a $\mathbb{Z}$.
I2. $a + b = b + a$; $ab = ba$.
I3. $(a + b) + c = a + (b + c)$; $(ab)c = a(bc)$.
I4. $a + 0 = a$; $a1 = a$.
I5. $a(b + c) = ab + ac$.
I6. Por cada a en $\mathbb{Z}$ existe un único entero $-a$ en $\mathbb{Z}$ tal que $a + (-a) = 0$.

I7. Si a es distinto de 0 y $ab = ac$, entonces $b = c$.

Todos los axiomas corresponden a propiedades familiares de los enteros que aprendemos en distintos niveles de nuestra educación matemática. De ellas pueden deducirse la mayoría de las reglas aritméticas comunes de los enteros. Por ejemplo, podemos *definir* la operación de sustracción diciendo que $a - b$ es lo mismo que $a + (-b)$; y deducir las reglas elementales para la sustracción como en el siguiente ejemplo.

Ejemplo 1.1.1. Demuestre que para dos enteros m y n cualesquiera

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

Demostración. Por la definición de sustracción, $m - (-n)$ es lo sustracción que $m + (-(-n))$. Ahora del Axioma **I6** nos dice que $-(-n)$ es el único número que sumado a $-n$, da cero. Sin embargo n mismo cumple esto, puesto que

$$\begin{aligned} (-n) + n &= n + (-n) && \text{(Axioma \textbf{I2})} \\ &= 0 && \text{(Axioma \textbf{I6})} \end{aligned}$$

Por lo tanto $-(-n) = n$ y $m - (-n) = m + n$, como queríamos demostrar. □

Algunos resultados similares pueden encontrarse en los siguientes ejercicios. Como aún no tenemos todos los axiomas correspondientes a los enteros, los resultados no son particularmente interesantes, pero lo que importa es recordar que pueden ser probados sobre la base única de los axiomas.

1.1.1. Ejercicios.

1. La siguiente es una demostración de la fórmula $0x = 0$ usando solo los axiomas planteados antes. Escriba la demostración completa, explicando que axioma es usado en cada paso.
$$\begin{aligned} x(0 + 0) &= x0 \\ x0 + x0 &= x0 \\ -x0 + (x0 + x0) &= -x0 + x0 \\ (-x0 + x0) + x0 &= 0 \\ 0 + x0 &= 0 \\ x0 &= 0. \end{aligned}$$
2. Construya una demostración de la regla $(a + b)c = ac + bc$, explicando cada paso como en el ejercicio 1.
3. Como siempre x^2 denota xx. Demuestre que dados dos enteros a y b, entonces existe un único c tal que $(a + b)c = a^2 - b^2$.

4. Suponga que existen dos enteros 0 y $0'$ ambos cumpliendo el Axioma **I4**, esto es

$$a + 0 = a, \qquad a + 0' = a$$

para todo a de $\mathbb{Z}$. Demuestre que esto implica $0 = 0'$, por lo tanto 0 está en realidad caracterizado de manera única por el Axioma **I4**.

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 el orden 1,2,3,4,5, y el hecho de que 4 es "mayor" que 3 se convierte en algo de importancia práctica para nosotros. Expresamos esta idea formalmente diciendo números existe una relación de orden en $\mathbb{Z}$:

$$m \leq n \qquad (m, n \in \mathbb{Z}),$$

que debe satisfacer ciertos axiomas. Solo cinco axiomas se necesitan para especificar las propiedades básicas del símbolo $\leq$, y ellos son listados en lo que sigue. La numeración de los axiomas se continúa de la sección 1.1. Como antes, a, b y c denotan enteros arbitrarios.

I8. $a \leq a$.
I9. Si $a \leq b$ y $b \leq a$, entonces $a = b$.
I10. Si $a \leq b$ y $b \leq c$, entonces $a \leq c$.
I11. Si $a \leq b$, entonces $a + c \leq b + c$.
I12. Si $a \leq b$ y $0 \leq c$, entonces $ac \leq bc$.

Estos axiomas no aportan mucho de nuevo, pues encierran propiedades muy familiares; lo importante es que nos permiten deducir otros hechos igualmente familiares. Con esto en mente, los siguientes ejercicios deberían ser resueltos usando solo las propiedades contenidas en los Axiomas **I1**–**I12**.

1.2.1. Ejercicios.

1. Supongamos $a \leq b$. Sumando $-a$ y luego $-b$ a ambos lados de la desigualdad, demuestre que $-b \leq -a$. Deduzca que $a \leq b$ y $c \leq 0$, entonces $bc \leq ac$.
2. Demuestre que $0 \leq x^2$ para todo x en $\mathbb{Z}$ y deduzca que $0 \leq 1$.
3. Deduzca del ejercicio previo que $n \leq n + 1$ para todo n en $\mathbb{Z}$.

Esta claro que podemos definir los otros símbolos de orden $\geq$, $<$ y $>$, en términos del símbolo $\leq$. Por ejemplo, $m > n$ debe definirse $n \leq m$ y $m \neq n$. Usaremos estos símbolos cuando la situación lo requiera.

A primera vista podría parecer que ya tenemos todas las propiedades que necesitamos de $\mathbb{Z}$, pero sorprendéntemente, aún falta un axioma de vital importancia. Supongamos que X es un subconjunto de $\mathbb{Z}$; entonces diremos que el entero b es una **cota inferior** de X si

$$b \leq x \qquad \text{para todo} \quad x \in X.$$

Algunos subconjuntos no tienen cotas inferiores: por ejemplo, el conjunto de los enteros negativos $-1, -2, -3, \ldots$, claramente no tiene cota inferior. Por otro lado, el conjunto S denotado por los números resaltados en la Fig.1 tiene muchas cotas inferiores. Una mirada rápida nos dice que -9 por ejemplo es una cota inferior, mientras que una inspección más minuciosa revela que -7 es la "mejor" cota inferior, pues en realidad pertenece a S. En general, una cota inferior de un conjunto X que es a su vez es un elemento de X, es conocido como el **mínimo** de X .

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

FIGURA 1. El mínimo de S es -7.

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

I13. Si X es un subconjunto de $\mathbb{Z}$ que no es vacío y tiene una cota inferior, entonces X tiene un mínimo.

El Axioma **I13** es conocido como el **axioma del buen orden**. Una buena forma de entender su significado es considerar un juego en el cual dos personas eligen alternativamente un elemento de X, sujetos a la regla de que cada número debe ser estrictamente menor que el anterior. El axioma nos dice que cuando los números son enteros, el juego terminará; además el final se producirá cuando uno de los jugadores tenga el buen sentido de elegir el mínimo. Esta propiedad aparentemente obvia *no* se mantiene necesariamente cuando tratamos con números que no son enteros, porque X puede no tener un mínimo aunque tenga una cota inferior. Por ejemplo supongamos que X es el conjunto de fracciones $3/2, 4/3, 5/4, \ldots$ teniendo por forma general $(n+1)/n$, $n \geq 2$. Este conjunto tiene una cota inferior (1, por ejemplo) pero no tiene mínimo y por lo tanto los jugadores podrían seguir jugando para siempre, eligiendo fracciones más y más cercanas a 1.

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 (Fig. 1.2). En particular dice que no podemos acercarnos más y más a un entero sin alcanzarlo, de forma que el dibujo de la Fig. 1.3 no es correcto.

Fig. 1.2 El dibujo correcto de $\mathbb{Z}$.

Fig. 1.3 Un dibujo incorrecto de $\mathbb{Z}$.

El hecho de que haya espacios vacíos entre los enteros nos lleva a decir que el conjunto $\mathbb{Z}$ es *discreto* y es esta propiedad la que da origen al nombre "matemática discreta". En cálculo y

análisis, los procesos de límite son de fundamental importancia, y es preciso usar aquellos sistemas numéricos que son *continuos*, en vez de los discretos.

1.2.2. Ejercicios. (continuación)

1. En cada uno de los siguientes casos diga si el conjunto X tiene o no una cota inferior, y si la tiene, encuentre el mínimo.
   (i) $X = \{x \in \mathbb{Z} | x^2 \leq 16\}$.
   (ii) $X = \{x \in \mathbb{Z} | x = 2y \text{ para algún } y \in \mathbb{Z}\}$.
   (iii) $X = \{x \in \mathbb{Z} | x \leq 100x\}$.
2. Un subconjunto Y de Z se dice que tiene una **cota superior** c si $c \geq y$ para todo $y \in Y$. Una cota superior que además es un elemento de Y es llamada el **máximo** de Y. Use el Axioma **I13** para demostrar que si Y es no vacío y tiene una cota superior, entonces tiene máximo. [Ayuda: aplique el axioma al conjunto cuyos elementos son $-y$ $(y \in Y)$.]
3. Los enteros n que satisfacen $1 \leq n \leq 25$ están acomodados en forma arbitraria en un arreglo cuadrado de cinco filas y cinco columnas. Se selecciona el máximo de cada fila, y se denota s al mínimo entre ellos. De manera similar, el mínimo de cada columna es seleccionado y t denota al máximo entre ellos. Demuestre que $s \geq t$ y de un ejemplo en el cual $s \neq t$.

1.3. Definiciones recursivas

Sea $\mathbb{N}$ el conjuntos de enteros positivos, esto es

$$\mathbb{N} = \{n \in \mathbb{Z} | n \geq 1\},$$

y denotemos $\mathbb{N}_0$ el conjunto $\mathbb{N} \cup \{0\}$, esto es

$$\mathbb{N}_0 = \{n \in \mathbb{Z} | n \geq 0\}.$$

Si X es un subconjunto de $\mathbb{N}$ (o de $\mathbb{N}_0$) entonces automáticamente tiene una cota inferior, pues cada elemento x de X satisface $x \geq 1$ (o $x \geq 0$). Así, en este caso el axioma del buen orden toma la forma

si X es un subconjunto no vacío de $\mathbb{N}$ o $\mathbb{N}_0$

entonces X tiene un mínimo.

Esta la forma más usada en la práctica.

Nuestro primer uso del axioma del buen orden será para justificar un procedimiento muy usual. Frecuentemente encontramos una expresión de la forma u_n, donde n indica cualquier entero positivo: por ejemplo, podríamos tener $u_n = 3n+2$, o $u_n = (n+1)(n+2)(n+3)$. En estos ejemplos u_n es dado por una fórmula explícita y no existe dificultad en explicar como calcular u_n cuando se nos da un valor específico para n. Sin embargo en muchos casos no conocemos una fórmula para u_n; es más, nuestro problema puede ser encontrarla. En estos casos pueden darnos

ciertos valores de u_n para enteros positivos n pequeños, y una relación entre el u_n general y algunos de los u_r con $r < n$. Por ejemplo, supongamos nos es dado

$$u_1 = 1, \qquad u_2 = 2, \qquad u_n = u_{n-1} + u_{n-2} \qquad (n \geq 3).$$

Para calcular los valores de u_n para todo n de $\mathbb{N}$ podemos proceder como sigue:

$$\begin{aligned} u_3 &= u_2 + u_1 = 2 + 1 = 3, \\ u_4 &= u_3 + u_2 = 3 + 2 = 5, \\ u_5 &= u_4 + u_3 = 5 + 3 = 8, \end{aligned}$$

y así siguiendo. Éste es un ejemplo de una *definición recursiva*. Es "obvio" que el método dará un valor único de u_n para todo entero positivo n. Pero hablando estrictamente necesitamos el axioma del buen orden para justificar la conclusión a través de las siguientes líneas.

Supongamos que existe un entero positivo n para el cual u_n no está definido de manera única. Entonces por el axioma del buen orden existe un entero positivo mínimo m con esta propiedad. Como u_1 y u_2 están explícitamente definidos, m no es 1 o 2 y la ecuación $u_m = u_{m-1} + u_{m-2}$ es aplicable. Por la definición de m, u_{m-1} y u_{m-2} están definidos de manera única, y la ecuación nos da un valor único para u_m , contrariamente a la hipótesis. La contradicción surge de suponer que no está bien definido para algún n, y por lo tanto esta suposición debe ser falsa.

El lector no debe desanimarse por el uso de argumentos tan retorcidos para establecer algo que es "obviamente" verdadero. En primer lugar, no debemos usar resultados ilegítimamente (sin demostrarlos), y en segundo lugar, el hecho de que el resultado sea "obvio" simplemente indica que estamos trabajando con la correcta representación mental de $\mathbb{N}$ y $\mathbb{Z}$. Una vez que hemos establecido esa representación sobre bases firmes podemos empezar a extendernos y obtener resultados que no sean tan "obvios".

El método de definición recursiva aparecerá bastante seguido en el resto del libro. Existen otras formas de este procedimiento que se "esconden" por su notación. ¿Qué significan las siguientes expresiones?

$$\sum_{r=1}^{n} 2r - 1, \qquad 1 + 3 + 5 + \cdots + (2n - 1).$$

Claramente no basta decir que uno significa lo mismo que el otro, porque cada uno contiene un misterioso símbolo, $\sum$ y $\cdots$, respectivamente. Lo que deberíamos decir es que cada uno de ellos es equivalente a la expresión s_n, dada por la siguiente definición recursiva:

$$s_1 = 1, \qquad s_n = s_{n-1} + (2n - 1) \quad (n \geq 2).$$

Esto hace ver claro que ambos símbolos misteriosos son, en realidad, una forma de acortar una definición recursiva, y que por lo tanto son expresiones definidas para todo n en $\mathbb{N}$.

Ideas similares pueden aplicarse a la definición de productos tal como $n!$ (que se lee n *factorial*). Si decimos que

$$n! = \Pi_{i=1}^{n} i, \quad \text{o} \quad n! = 1 \times 2 \times 3 \times \cdots \times n,$$

el significado es bastante claro para cualquiera. Pero para precisar (y hacerlo claro para una computadora) debemos usar la definición recursiva

$$1! = 1, \qquad n! = n \times (n-1)! \quad (n \geq 2).$$

1.3.1. Ejercicios.

1. En el caso siguiente calcule (donde sea posible) los valores de u_1, u_2, u_3 y u_4 dados por las ecuaciones. Si no puede calcular los valores explique porque la definición no esta bien.

   (i) $u_1 = 1, \quad u_2 = 1, \quad u_n = u_{n-1} + 2u_{n-2} \quad (n \geq 3).$

   (ii) $u_1 = 1, \quad u_n = u_{n-1} + 2u_{n-2} \quad (n \geq 2).$

   (iii) $u_1 = 0, \quad u_n = nu_{n-1} \quad (n \geq 2).$

2. De una definición recursiva de la "n-ésima potencia" para todo $n \geq 1$.
3. Sea u_n definido por las ecuaciones

   $$u_1 = 2, \qquad u_n = 2^{u_{n-1}} \quad (n \geq 2).$$

   ¿Cuál es el primer valor de n para el cual no se puede calcular u_n usando una calculadora de bolsillo?
4. Escriba fórmulas explícitas para las expresiones u_n definidas por las siguientes ecuaciones.

   (i) $u_1 = 1, \quad u_n = u_{n-1} + 3 \quad (n \geq 2).$

   (ii) $u_1 = 1, \quad u_n = n^2 u_{n-1} \quad (n \geq 2).$

1.4. El principio de inducción

Supongamos que nos piden que demostremos el resultado

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

En otras palabras, debemos demostrar que la expresión de la izquierda definida recursivamente es igual a la definida explícitamente por la fórmula de la derecha, para todos los enteros positivos n. Podemos proceder como sigue.

La fórmula es ciertamente correcta cuando $n = 1$ puesto que $1 = 1^2$. Supongamos que es correcta para un valor específico de n, digamos para $n = k$, de modo que

$$1 + 3 + 5 + \cdots + (2k-1) = k^2.$$

Podemos usar esto para simplificar la expresión definida recursivamente a la izquierda cuando n es igual a $k+1$,

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

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

La esencia de este argumento es comúnmente llamada *principio de inducción*. Es una técnica poderosa, fácil de aplicar y la aplicaremos frecuentemente. Pero primero debemos examinar sus bases lógicas y para hacerlo necesitamos una formulación más general. Con S denotemos al subconjunto de $\mathbb{N}$ para el cual el resultado es correcto: por supuesto, nuestra intención es probar que S es todo $\mathbb{N}$. El primer paso es probar que 1 pertenece a S, y luego demostraremos que si k pertenece a S, también $k+1$. Entonces lo pensamos paso a paso y concluimos que $S=\mathbb{N}$. Afortunadamente el pensarlo paso a paso no es esencial, debido a que el principio de inducción es consecuencia de los axiomas que elegimos tan cuidadosamente para $\mathbb{Z}$ y $\mathbb{N}$. Más específicamente es consecuencia del axioma del buen orden.

TEOREMA 1.4.1. *Supongamos que S es un subconjunto de $\mathbb{N}$ que satisface las condiciones*

(i) $1 \in S$,

(ii) *para cada $k \in \mathbb{N}$, 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

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

es no vacío. Por el axioma del buen orden, S^{c} tiene un menor elemento m. Como 1 pertenece a S, $m \neq 1$. Se sigue que $m-1$ pertenece a $\mathbb{N}$ y como m es el mínimo de S^{c}, $m-1$ debe pertenecer a S. Poniendo $k=m-1$ en la condición (ii), concluimos que m esta en S, lo cual contradice el hecho de que m pertenece a S^{c}. De este modo, la suposición $S \neq \mathbb{N}$ nos lleva a un absurdo, y por lo tanto tenemos $S=\mathbb{N}$. □

En la práctica, generalmente presentamos una "demostración por inducción" en términos más descriptivos. El hecho de que el resultado es verdadero cuando $n=1$ se llama *base de la inducción* y la suposición de que es verdadero cuando $n=k$ es llamada *hipótesis inductiva*. Cuando se utilizan estos términos, no es necesario introducir explícitamente el conjunto S.

EJEMPLO 1.4.1. El entero x_n esta definido recursivamente por

$$x_1 = 2, \quad \text{y} \quad x_n = x_{n-1} + 2n \quad (n \geq 2).$$

Demuestre que

$$x_n = n(n+1) \qquad \text{para todo } n \in \mathbb{N}.$$

DEMOSTRACIÓN. (*Base de la inducción*) El resultado es verdadero cuando $n = 1$ pues $2 = 1 \times 2$. (*Hipótesis inductiva*) Supongamos que el resultado verdadero cuando $n = k$, o sea, $x_k = k(k+1)$. Entonces

$$\begin{aligned} x_{k+1} &= x_k + 2(k+1) && \text{por la definición recursiva} \\ &= k(k+1) + 2(k+1) && \text{por hipótesis inductiva} \\ &= (k+1)(k+2). \end{aligned}$$

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

Existen varias formas modificadas del principio de inducción. A veces es conveniente tomar como base inductiva el valor $n = 0$, por otro lado 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. (Esta formulación es llamada a veces el principio de inducción *completa*.) Todas esas modificaciones pueden justificarse con cambios triviales en la demostración del Teorema 1.4.1, como se indica en el ejercicio 6.

1.4.1. Ejercicios.

1. Use el principio de inducción para demostrar que

$$1^2 + 2^2 + \cdots + n^2 = \frac{1}{6}n(n+1)(2n+1)$$

para todos los enteros positivos n.

2. Haga una tabla de valores de

$$S_n = 1^3 + 2^3 + \cdots + n^3$$

para $1 \leq n \leq 6$. Basándose en su tabla sugiera una fórmula para S_n. [Ayuda:los valores de S_n son cuadrados perfectos.] Use el principio de inducción para establecer que la fórmula es correcta para todo $n \geq 1$. (Si el método falla ¡su fórmula es equivocada!)

3. Use el principio de inducción completa para demostrar que si u_n está definido recursivamente por

$$u_1 = 3, \qquad u_2 = 5, \qquad u_n = 3u_{n-1} - 2u_{n-2} \quad (n \geq 3),$$

entonces $u_n = 2^n + 1$ para todo entero positivo n.

4. Encuentre el menor entero positivo n_0 para el cual sea verdadero que $n! \geq 2^n$. Tomando el caso $n = n_0$ como la base inductiva, demuestre que el resultado vale para $n \geq n_0$.
5. En los siguientes casos encuentre los valores apropiados de n_0 para la base inductiva y demuestre que la afirmación es verdadera para todos los $n \geq n_0$.

$$\text{(i) } n^2 + 6n + 9 \geq 0, \qquad \text{(ii) } n^3 \geq 6n^2.$$

6. El siguiente Teorema incorpora todas las modificaciones del principio de inducción mencionadas antes.

TEOREMA 1.4.1*. *Supongamos que n_0 es cualquier entero (no necesariamente positivo), y sea X el conjunto de enteros $n \geq n_0$. Sea S un subconjunto de X que satisface las condiciones:*

(i) $n_0 \in S$,

(ii) *si $x \in S$ para todo x en el rango $n_0 \leq x \leq k$ entonces $k + 1 \in S$.*

Entonces se sigue que $S = X$.

Escriba la demostración del Teorema 1.4 y haga los cambios necesarios para demostrar el Teorema 1.4*.

1.5. Cociente y resto

Cuando somos chicos aprendemos que 6 "cabe" cuatro veces en 27 y el resto es 3, o sea

$$27 = 6 \times 4 + 3.$$

Un punto importante es que el resto debe ser menor que 6. Aunque, también es verdadero que, por ejemplo

$$27 = 6 \times 3 + 9,$$

debemos tomar el menor valor para el resto, de forma que "lo que queda" sea la más chico posible. El hecho de que el conjunto de posibles "restos" tenga un mínimo es una consecuencia del axioma del buen orden.

TEOREMA 1.5.1. *Sean a y b números enteros cualesquiera con $b \in \mathbb{N}$, entonces existen enteros q y r tales que*

$$a = b \times q + r \qquad y \qquad 0 \leq r < b.$$

DEMOSTRACIÓN. Debemos aplicar el axioma del buen orden al conjunto de los "restos"

$$R = \{x \in \mathbb{N}_0 | a = by + x \text{ para algún } y \in \mathbb{Z}\}.$$

Primero demostraremos que R no es vacío. Si $a \geq 0$ la igualdad

$$a = b0 + a$$

demuestra que $a \in R$, mientras que si $a < 0$ la igualdad

$$a = ba + (1 - b)a$$

demuestra que $(1 - b)a \in R$ (En ambos casos es necesario controlar que el elemento es no negativo.)

Ahora, como R es un subconjunto no vacío de $\mathbb{N}_0$, tiene un mínimo r, y como r esta en R se sigue que $a = bq + r$ para algún q en $\mathbb{Z}$. Además

$$a = bq + r \Rightarrow a = b(q + 1) + (r - b)$$

de manera que si $r \geq b$ entonces $r - b$ esta en R. Pero $r - b$ es menor que r, contradiciendo la definición de r como el menor elemento de R. Como la suposición $r \geq b$ nos lleva a una contradicción, solo puede ocurrir que $r < b$, como queríamos demostrar. □

Es fácil ver que el cociente q y el resto r obtenidos en el teorema son únicos. Supongamos que q' y r', también satisfacen las condiciones, esto es

$$b = bq' + r' \qquad \text{y} \qquad 0 \leq r' < b.$$

Si $q < q'$, entonces $q - q' \geq 1$, entonces tenemos

$$r' = a - bq' = (a - bq) + b(q - q') \geq r + b.$$

Como $r + b \geq b$, se sigue que $r' \geq b$ contradiciendo la segunda propiedad de r'. Por lo tanto la suposición $q' < q$ es falsa. El mismo argumento con q y q' intercambiados demuestra que $q < q'$ también es falsa. Entonces debemos tener $q = q'$, y en consecuencia $r = r'$,puesto que

$$r = a - bq = a - bq' = r'.$$

Una consecuencia importante del Teorema 1.5 es que justifica nuestro método usual de representación de enteros. Sea $t \geq 2$ un número entero, llamado **base** para los cálculos. Para cualquier entero positivo x tenemos, por la aplicación repetida del Teorema 1.5,

$$\begin{aligned} x &= tq_0 + r_0 \\ q_0 &= tq_1 + r_0 \\ &\dots \\ q_{n-2} &= tqn - 1 + r_{n-1} \\ q_{n-1} &= tq_n + r_n. \end{aligned}$$

Aquí cada resto es uno de los enteros $0, 1, \dots, t - 1$, y paramos cuando $q_n = 0$.Eliminando los cocientes q_i obtenemos

$$x = r_n x^n + r_{n-1} x^{n-1} + \cdots + r_1 t + r_0.$$

Hemos representado x (con respecto a la base t) por la secuencia de los restos, y escribimos $x = (r_n r_{n-1} \dots r_1 r_0)_t$. Convencionalmente $t = 10$ es la base para los cálculos hechos "a mano" y omitimos ponerle el subíndice, entonces tenemos la notación usual

$$1984 = (1 \times 10^3) + (9 \times 10^2) + (8 \times 10) + 4.$$

Esta notación posicional requiere símbolos solo para los enteros $0, 1, \dots, t-1$ .La base $t = 2$ es particularmente adaptable para los cálculos en computadoras porque los símbolos 0 y 1 pueden representarse físicamente por la ausencia o presencia de un pulso de electricidad o luz.

EJEMPLO 1.5.1. ¿Cuál es la representación en base 2 de $(109)_{10}$?

DEMOSTRACIÓN. Dividiendo repetidamente por 2 obtenemos

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

Por lo tanto

$$(109)_{10} = (1101101)_2.$$

□

1.5.1. Ejercicios.

1. Encuentre q y r que satisfagan el Teorema 1.5 cuando

   (i) $a = 1001,\ b = 11;$ (ii) $a = 12345,\ b = 234.$

2. Encuentre las representaciones de $(1985)_{10}$ en base 2, en base 5 y en base 11.
3. Encuentre las representación usual (base 10) de

   (i) $(11011101)_2;$ (ii)$(4165)_7.$

1.6. Divisibilidad

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

$$x = yq \quad \text{para algún} \quad q \in \mathbb{Z}.$$

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.

Cuando $x|y$ podemos usar el símbolo $\frac{x}{y}$ (o x/y) para denotar el entero q tal que $x = yq$. Cuando y no es un divisor de x tenemos que asignar un nuevo significado a la fracción x/y, puesto que este número no es un entero. El lector indudablemente, esta familiarizado con las reglas para manejar fracciones, y usaremos esas reglas de tanto en tanto, pero es importante recordar que las fracciones no han sido aún formalmente definidas en el contexto de este libro. Y es aún más importante recordar que x/y no es un elemento de $\mathbb{Z}$ a menos que y divida a x.

EJEMPLO 1.6.1. Demuestre que si c, d y n son enteros tales que

$$d|n \quad \text{y} \quad c|\frac{n}{d}$$

entonces

$$c|n \quad \text{y} \quad d|\frac{n}{c}.$$

DEMOSTRACIÓN. Como $d|n$ existe un entero s tal que $n = ds$, y n/d denota al entero s. Puesto que $c|n/d$ existe un entero t tal que

$$s = \frac{n}{d} = ct.$$

Se sigue que

$$n = ds = d(ct) = c(dt)$$

entonces $c|n$ y n/c denota al entero dt. Finalmente como $n/c = dt$ tenemos $d|n/c$, como queríamos demostrar. □

1.6.1. Ejercicios.

1. Demuestre que $x|0$ para todo $x \in \mathbb{Z}$,pero que $0|x$ solo cuando $x = 0$.
2. Muestre que si $c|a$ y $c|b$, entonces $c|xa + yb$ para cualesquiera enteros x,y.
3. Demuestre que si a y b son enteros tales que $ab = 1$ entonces $a = b = 1$ o $a = b = -1$ [Ayuda: a y b son o ambos positivos o ambos negativos]. Deduzca que si x e y son enteros tales que $x|y$ e $y|x$ entonces $x = y$ o $x = -y$.
4. Use el principio de inducción para demostrar que, para todo $n \geq 0$,

   (i) $n^2 + 3n$ es divisible por 2 (ii) $n^3 + 3n^2 + 2n$ es divisible por 6.

1.7. El máximo común divisor y el mínimo común múltiplo

Si a y b son enteros decimos que el entero d es un **máximo común divisor**, o **mcd**, de a y b si

$$\text{(i) } d|a \text{ y } d|b; \qquad \text{(ii) si } c|a \text{ y } c|b \text{ entonces } c|d$$

La condición (i) nos dice que d es un común divisor de a y b y la condición (ii) nos dice que cualquier divisor común de a y b es también divisor de d. Por ejemplo, 6 es un divisor común de 60 y 84, pero no es el mayor divisor común, porque $12|60$ y $12|84$ pero $12 \not| 6$ (el símbolo significa "no divide".)

Las condiciones (i) y (ii) no son suficientes para asegurar que dos enteros dados tienen un único mcd. Si d y d' satisfacen ambos las dos condiciones se sigue que

$$d|d' \qquad \text{y} \qquad d'|d.$$

Por lo tanto, por el ejemplo 1.6.3 , $d = d'$ o $d = -d'$. Por consiguiente para obtener un mcd único, es suficiente con imponer una tercera condición :

$$\text{(iii) } d \geq 0.$$

Decimos que el único entero d que satisface (i), (ii) y (iii) es el mcd de a y b, y escribimos $d = \text{mcd}(a, b)$. Por ejemplo, $12 = \text{mcd}(60, 84)$. Existe un famoso método[1] para calcular el mcd de dos enteros dados, basado en la técnica del cociente y el resto. Depende del siguiente hecho

$$a = bq + r \quad \Rightarrow \quad \text{mcd}(a, b) = (b, r).$$

Para demostrar esto debemos observar que si d divide a y b, entonces también divide a $a - bq$; y $a - bq = r$, luego divide a r. De este modo cualquier divisor común de a y b es también divisor común de b y r. Por otro lado si d divide b y r también divide a $a = bq + r$. La aplicación repetida de este simple hecho nos da un método para calcular el mcd.

Ejemplo 1.7.1. Encuentre el mcd de 2406 y 654.

Demostración. Tenemos

$$\begin{aligned}
\text{mcd}(2406, 654) &= \text{mcd}(654, 444) \text{ porque } 2406 = 654 \times 3 + 444, \\
&= \text{mcd}(444, 210) \text{ porque } \ 654 = 444 \times 1 + 210, \\
&= \text{mcd}(210, 24) \ \text{ porque } \ 444 = 210 \times 2 + 24, \\
&= \text{mcd}(24, 18) \ \ \text{ porque } \ 210 = 24 \times 8 + 18, \\
&= \text{mcd}(18, 6) \ \ \ \text{ porque } \ \ 24 = 18 \times 1 + 6, \\
&= 6 \qquad\qquad \text{porque } \ \ 18 = 6 \times 3
\end{aligned}$$

□

Por lo general, para calcular el mcd de enteros a y b (ambos ≥ 0) definimos q_i y r_i recursivamente por las ecuaciones.

$$\begin{aligned}
a &= bq_1 + r_1 \ \ (0 \leq r_1 < b) \\
b &= r_1 q_2 + r_2 (0 \leq r_2 < r_1) \\
r_1 &= r_2 q_3 + r_3 (0 \leq r_3 < r_2) \\
&\cdots \qquad\qquad .
\end{aligned}$$

[1]Obsérvese que con la aplicación de este método se puede demostrar fácilmente la existencia del mcd

Está claro que el proceso debe detenerse, porque cada resto es estrictamente menor que el anterior. Entonces los pasos finales son como siguen:

$$r_{k-4} = r_{k-3}q_{k-2} + r_{k-2}(0 \leq r_{k-2} < r_{k-3})$$
$$r_{k-3} = r_{k-3}q_{k-1} + r_{k-1}(0 \leq r_{k-1} < r_{k-2})$$
$$r_{k-2} = r_{k-1}q_k,$$

donde r_k es nulo y r_{k-1} es el mcd requerido. Este procedimiento es conocido como el **algoritmo de Euclides**, debido al matemático griego Euclides (300 a. c.). Es extremadamente útil en la práctica, y tiene importantes consecuencias teóricas.

TEOREMA 1.7.1. *Sean a y b enteros con $b \geq 0$ y sea $d = \text{mcd}(a, b)$. Entonces existen enteros m y n tales que*

$$d = ma + nb.$$

DEMOSTRACIÓN. De acuerdo con el cálculo hecho antes $d = r_{k-1}$ y usando la penúltima ecuación tenemos

$$r_{k-1} = r_{k-3} - r_{k-2}q_{k-1}.$$

Así, d puede escribirse en la forma $m'r_{k-2} + n'r_{k-3}$,donde $m' = -q_{k-1}$ y $n' = 1$. Sustituyendo r_{k-2} en términos de r_{k-3} y r_{k-4} obtenemos

$$d = m'(r_{k-4} - r_{k-3}q_{k-2}) + n'r_{k-3}$$

que puede escribirse de en la forma $m"r_{k-3} + n"r_{k-4}$, con $m" = n' - m'q_{k-2}$ y $n" = m'$. Continuando de esta forma obtendremos una expresión para d de la forma requerida.

□

Por el ejemplo, de los cálculos usados para encontrar el mcd de 2406 y 654 obtenemos

$$\begin{aligned}
6 &= \mathbf{24} - \mathbf{18} \times 1 \\
&= \mathbf{24} + (-1) \times (\mathbf{210} - \mathbf{24} \times 8) \\
&= -\mathbf{210} + 9 \times (\mathbf{444} - \mathbf{210} \times 2) \\
&= 9 \times \mathbf{444} + (-19) \times (\mathbf{654} - \mathbf{444} \times 1) \\
&= (-19) \times \mathbf{654} + 28 \times (\mathbf{2406} - \mathbf{654} \times 3) \\
&= 28 \times \mathbf{2406} + (-103) \times \mathbf{654}.
\end{aligned}$$

De este modo, la expresión requerida $d = ma + nb$ es

$$6 = 28 \times 2406 + (-103) \times 654.$$

Si el $\text{mcd}(a, b) = 1$ entonces decimos que a y b son coprimos y en este caso el Teorema 1.7.1 dice que existen enteros m y n tales que

$$ma + nb = 1.$$

Este hecho es muy útil. Por ejemplo, todos estamos familiarizados con la idea de que una fracción puede reducirse al "mínimo término", o sea a la forma a/b con a y b coprimos. El siguiente ejemplo establece que esta forma es única, y como veremos, el hecho clave de la demostración es que podemos expresar a 1 como $ma + nb$.

EJEMPLO 1.7.2. Supongamos que a, a', b, b' son enteros positivos que satisfacen

$$\text{(i)} \quad ab' = a'b; \qquad \text{(ii)} \quad \mcd(a, b) = \mcd(a', b') = 1.$$

Entonces $a = a'$ y $b = b'$.

(La condición (i)podría escribirse como $a/b = a'/b'$, pero preferimos usar esta forma que no asume ningún conocimiento sobre fracciones.)

DEMOSTRACIÓN. Como el $\mcd(a, b) = 1$ existen enteros m y n tales que $ma + nb = 1$. En consecuencia

$$b' = (ma + nb)b' = mab' + nbb' = (ma' + nb')b,$$

y por lo tanto $b|b'$. Por un argumento similar y usando el hecho de que el $\mcd(a', b') = 1$ deducimos que $b|b'$, por lo tanto $b = b'$ o $b = -b'$ y como b y b' son ambos positivos debemos tener $b = b'$. Ahora de (i) deducimos que $a = a'$ y el resultado esta demostrado. □

Si a y b son enteros decimos que el entero m es el **mínimo común múltiplo**, o **mcm**, de a y b si

$$\text{(i) } a|m \text{ y } b|m; \qquad \text{(ii) si } a|n \text{ y } b|n \text{ entonces } n|m; \qquad \text{(iii) } m \geq 0.$$

La condición (i) nos dice que m es múltiplo común de a y b, la condición (ii) nos dice que es mínimo y la condición (iii) nos asegura la unicidad. Por ejemplo hallemos el mínimo común múltiplo entre 8 y 14. Escribamos los múltiplos de ambos números y busquemos el menor común a ambos. Los primeros múltiplos de 8 son: $8, 16, 24, 32, 40, 48, 56, \ldots$. Los primeros múltiplos de 14 son: $14, 28, 42, 56, 72, \ldots$. Luego se tiene $\mcm(8, 14) = 56$.

El siguiente teorema garantiza la existencia del mcm.

TEOREMA 1.7.2. *Sean a y b enteros no nulos, entonces*

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

DEMOSTRACIÓN. Demostraremos que

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

es el mínimo común múltiplo de a, b.

Como

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

resulta que m es múltiplo de a y b.

Sea ahora n un múltiplo de a y b. Por Teorema 1.7.1, tenemos que existen r, s tales que $\mathrm{mcd}(a,b) = ra + sb$ y por lo tanto, dividiendo por $\mathrm{mcd}(a,b)$ y multiplicando por n, obtenemos:

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

Escribiendo $n = b'b = a'a$ (a', b' en $\mathbb{Z}$), resulta finalmente

$$n = rb'\frac{ab}{\mathrm{mcd}(a,b)} + sa'\frac{ab}{\mathrm{mcd}(a,b)} = \frac{ab}{\mathrm{mcd}(a,b)}(rb' + sa')$$

lo cual demuestra que m divide a n. □

En particular este resultado implica que si a y b son enteros coprimos, entonces $\mathrm{mcm}(a,b) = ab$.

1.7.1. Ejercicios.

1. Encuentre el mcd de 721 y 448 y expréselo en la forma $721m + 448n$ con $m, n \in \mathbb{Z}$.
2. Demuestre que si a, b y n son enteros no nulos, entonces $\mathrm{mcd}(na, nb) = n\,\mathrm{mcd}(a,b)$.
3. Demuestre que si existen enteros m y n tales que $mu+nv = 1$, entonces el $\mathrm{mcd}(u,v) = 1$.
4. Use el Teorema 1.7.1 y el Ej. 3 para demostrar que si el $\mathrm{mcd}(a,b) = d$, entonces
$$\mathrm{mcd}\left(\frac{a}{d}, \frac{b}{d}\right) = 1.$$
5. Sean a y b enteros positivos y sea $d = \mathrm{mcd}(a,b)$. Pruebe que existen enteros x e y que satisfacen la ecuación $ax + by = c$ si y solo si $d|c$.
6. Encuentre enteros x e y que satisfagan
$$966x + 685y = 70.$$

1.8. Factorización en primos

Se dice que un entero positivo p es **primo** si $p \geq 2$ y los únicos entero positivos que dividen p son 1 y p mismo. Luego un entero $m \geq 2$ no es un primo si y solo si puede escribirse como $m = m_1 m_2$ donde m_1 y m_2 son enteros estrictamente entre 1 y m.

Enfaticemos que de acuerdo a la definición, 1 *no* es primo. Los primeros primos son

$$2,\ 3,\ 5,\ 11,\ 17,\ 19,\ 23,\ 129,\ 31,\ 37,\ 41,\ 47.$$

El lector debe estar casi totalmente familiarizado con la idea de que cualquier entero positivo puede expresarse como producto de primos: por ejemplo

$$825 = 3 \times 5 \times 5 \times 11.$$

La existencia de esta factorización en primos para cualquier entero positivo es una consecuencia del axioma del buen orden: sea B el conjunto de enteros positivos que no tienen una factorización en primos; si$B$ no es vacío entonces, por el axioma del buen orden, tiene un mínimo m. Si m fuera un primo p entonces tendríamos la factorización trivial $m = p$; por lo tanto m no es primo

y $m = m_1 m_2$ donde $1 < m_1 < m$ y $1 < m_2 < m$. Como estamos suponiendo que m es el menor entero (≥ 2) que no tiene factorización en primos, entonces m_1 y m_2 tienen factorización en primos. Pero entonces la ecuación $m = m_1 m_2$ produce una factorización en primos de m, contradiciendo la suposición de que m era un elemento de B. Por lo tanto B debe ser vacío, y la afirmación esta probada.

1.8.1. Ejercicios.

1. Encuentre todos los primos p en el rango $100 \leq p \leq 120$.
2. Escriba la factorización en primos de 2011001 y 201000.
3. Demuestre que si p y p' son primos y $p|p'$ entonces $p = p'$.
4. Demuestre que si $n \geq 2$ y n no es primo entonces existe un primo p tal que $p|n$ y $p^2 \leq n$.
5. Use el resultado del ejercicio anterior para demostrar que si 467 no fuera primo entonces tendría un divisor primo $p \leq 19$. Deduzca que 467 es primo.

La facilidad con la que establecemos la existencia de la factorización de primos conlleva dos dificultades importantes. Primero el problema de encontrar los factores primos no es de ningún modo directo; y segundo no es obvio que exista una *única* factorización en primos para todo entero dado $n \geq 2$. El siguiente resultado es un paso clave en la demostración de la unicidad.

TEOREMA 1.8.1. *Si p es un primo y $x_1, x_2, \ldots, x_n$ son enteros tales que*

$$p|x_1 x_2 \ldots x_n$$

entonces $p|x_i$ para algún x_i ($1 \leq i \leq n$).

DEMOSTRACIÓN. Usemos el principio de inducción. El resultado es obviamente verdadero cuando $n = 1$ (base inductiva). Como hipótesis inductiva, supongamos que es verdadero cuando $n = k$.

Supongamos que $p|x_1 x_2 \ldots x_k x_{k+1}$ y sea $x = x_1 x_2 \ldots x_k$. Si $p|x$ entonces, por la hipótesis inductiva, $p|x_i$ para algún x_i en el rango $1 \leq i \leq k$. Si $p \not| x$ entonces (como p no tiene divisores excepto 1 y el mismo) tenemos $\text{mcd}(x, p) = 1$. Por el Teorema 1.7 existen enteros r y s tales que $rp + sx = 1$. Por lo tanto tenemos

$$x_{k+1} = (rp + sx)x_{k+1} = (rx_{k+1})p + s(xx_{k+1}),$$

y como p divide a ambos términos se sigue que $p|x_{k+1}$. De este modo, en ambos casos p divide uno de los x_i ($1 \leq i \leq k+1$), y por el principio de inducción el resultado es verdadero para todos los enteros positivos n. □

Un error común es asumir que el Teorema 1.8.1 se mantiene verdadero cuando reemplazamos el primo p por un entero arbitrario . Pero esto claramente absurdo : por ejemplo

$$6|3 \times 8 \quad \text{pero} \quad 6 \not|3 \quad \text{y} \quad 6 \not|8.$$

Ejemplos como éste nos ayudan a entender que el Teorema 1.8.1 expresa una propiedad muy significativa de los números primos. Además veremos que esta propiedad juega un papel crucial en el siguiente resultado, que a veces es llamado el *Teorema Fundamental de la Aritmética*.

TEOREMA 1.8.2. *La factorización en primos de un entero positivo $n \geq 2$ es única, salvo el orden de los factores primos.*

DEMOSTRACIÓN. Por el axioma del buen orden, si existe un entero para el cual el teorema es falso, entonces hay un entero mínimo $n_0 \geq 0$ con esta propiedad. Supongamos entonces que

$$n_0 = p_1 p_2 \dots p_k \quad \text{y} \quad n_0 = p'_1 p'_2 \dots p'_l,$$

donde los p_i $(1 \leq i \leq k)$ son primos, no necesariamente distintos, y los p'_i $(1 \leq i \leq l)$ son primos, no necesariamente distintos. La primera ecuación implica que $p_1 | n_0$, y la segunda ecuación implica que $p_1 | p'_1 p'_2 \dots p'_l$. Por consiguiente por Teorema 1.8.1 tenemos que $p_1 | p'_j$ para algún j $(1 \leq j \leq l)$. Re-ordenando la segunda factorización podemos asumir que $p_1 | p'_1$, y puesto que p_1 y p'_1 son primos, se sigue que $p_1 = p'_1$ (Ej. 1.8.3). Luego por el Axioma **I7**, podemos cancelar los factores p_1 y p'_1, y obtener

$$p_2 p_3 \dots p_k = p'_2 p'_3 \dots p'_l,$$

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 primas diferentes. Esto contradice la definición de n_0 como el mínimo entero sin factorización única. Por lo tanto el teorema es verdadero para $n \geq 2$. □

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

$$n = p_1^{e_1} p_2^{e_2} \dots p_r^{e_r},$$

donde $p_1, p_2, \dots, p_r$ son primos distintos y $e_1, e_2, \dots, e_r$ son enteros positivos. Por ejemplo $7000 = 2^3 \times 5^3 \times 7$.

EJEMPLO 1.8.1. Probar que si m y n son enteros tales que $m \geq 2$ y $n \geq 2$, entonces $m^2 \neq 2n^2$.

DEMOSTRACIÓN. Supongamos que la factorización prima de n contiene al 2 elevado a la x (donde x es cero si 2 no es factor primo de n). Entonces $n = 2^x h$, donde h es producto de primos más grandes que 2, luego

$$2n^2 = 2(2^x h)^2 = 2^{2x+1} h^2.$$

Por lo tanto 2 está elevado a una potencia *impar* en la factorización prima de $2n^2$.

Por otro lado, si $m = 2^y g$, donde g es producto de primos mayores que 2, entonces

$$m^2 = (2^y g)^2 = 2^{2y} g^2,$$

luego 2 está elevado a una potencia *par* (posiblemente cero) en la factorización prima de m^2. se sigue entonces que de ser $m^2 = 2n^2$ deberíamos tener dos factorizaciones primas diferentes del mismo número entero, contradiciendo al Teorema 1.8.2. Entonces $m^2 \neq 2n^2$. □

Es claro que la conclusión del Ejemplo vale también si nosotros permitimos que alguno de los enteros m o n valga 1. Luego podemos expresar el resultado diciendo que no hay enteros positivos m y n que cumplan

$$\left(\frac{m}{n}\right)^2 = 2$$

o equivalentemente, diciendo que la raíz cuadrada de 2 no puede ser expresada como una fracción m/n.

1.8.2. Ejercicios. (continuación)

1. Sean m y n enteros positivos cuyas factorizaciones primas son

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

   Probar que el mcd de m y n es $d = n = p_1^{k_1} p_2^{k_2} \dots p_r^{k_r}$ donde, para cada i en el rango $1 \le i \le r$, k_i es el mínimo entre e_i y f_i.
2. Probar que si m y n son enteros positivos, tales que $m \ge 2$ y $n \ge 2$, y $m^2 = kn^2$, entonces k es el cuadrado de un entero.
3. Use la identidad

$$2^{rs} - 1 = (2^r - 1)(2^{(s-1)r} + 2^{(s-2)r} + \dots + 2^r + 1)$$

   para probar que si $2^n - 1$ es primo, entonces n es primo.
4. Encontrar el mínimo n para el cual la recíproca del ejercicio anterior es falsa: esto es, n es primo pero $2^n - 1$ no lo es.

1.9. Ejercicios

1. Usar el principio de inducción para probar que $2^n > n + 1$ para todo entero $n \ge 2$.
2. Probar que

$$1^4 + 2^4 + \dots + n^4 = \frac{1}{30} n(n+1)(2n+1)(3n^2 + 3n + 1).$$

3. Probar que $4^{2n} - 1$ es divisible por 15 para todo entero $n \ge 1$.
4. Encontrar el mcd entre 1320 y 714, y expresar el resultado en la forma $1320x + 714y$ $(x, y \in \mathbb{Z})$.
5. Probar que 725 y 441 son coprimos y encontrar enteros x e y tales que $725x + 441y = 1$.
6. Encontrar una solución con números enteros de la ecuación

$$325x + 26y = 91.$$

7. El entero f_n es definido recursivamente por la ecuación

$$f_1 = 1, \qquad f_2 = 1, \qquad f_{n+1} = f_n + f_{n-1} \quad (n \ge 2).$$

   Probar que $\text{mcd}(f_{n+1}, f_n) = 1$ para todo $n \ge 2$.
8. Probar que si $\text{mcd}(a, x) = d$ y $\text{mcd}(b, x) = 1$, entonces $\text{mcd}(ab, x) = d$.

9. Usted tiene a disposición una cantidad ilimitada de agua, un gran contenedor y dos jarras de 7 y 9 litros respectivamente. ¿Cómo se las arreglaría usted para poner un litro de agua en el contenedor? Explique la relación entre su método y el Teorema 1.7.1.
10. Siguiendo la definición de mcd de dos enteros, defina el mcd de n enteros $a_1, a_2, \ldots, a_n$. Probar que si $d = \text{mcd}(a_1, a_2, \ldots, a_n)$, entonces existen enteros $x_1, x_2, \ldots, x_n$ tales que

$$d = x_1a_1 + x_2a_2 + \cdots + x_na_n.$$

11. Sea n un entero con las siguientes propiedades: (1) la descomposición prima de n no tiene factores repetidos (es decir n es de cuadrado libre) y (2) si p cualquier primo, entonces $p|n$ si y solo si $p - 1|n$.

    Encuentre el valor de n.
12. El entero u_n es definido por las ecuaciones

$$u_1 = 2, \qquad u_{n+1} = u_n^2 - u_n + 1 \ \ (n \geq 1).$$

    Encontrar el menor valor de n para el cual u_n no es primo y encontrar los factores de este u_n. ¿Es u_6 primo?.
13. Probar que los enteros definidos en el ejercicio anterior satisfacen

$$u_{n+1} = 1 + u_1u_2 \ldots u_n.$$

    Deducir que u_{n+1} tiene un factor primo que es diferente de todo factor primo que aparece en la descomposición de los $u_1, u_2, \ldots, u_n$. Con esto probar que el conjunto de primos no tiene máximo.
14. ¿Es 65537 primo?.
15. Probar que no existen enteros x, y, z, t para los cuales valga la relación

$$x^2 + y^2 - 3z^2 - 3t^2 = 0.$$

16. Probar que si $\text{mcd}(x, y) = 1$ y $xy = z^2$ para algún entero z, entonces $x = m^2$ y $y = n^2$ para ciertos enteros m, n.
17. Probar que si $\text{mcd}(a, b) = 1$, entonces $\text{mcd}(a + b, a - b)$ es 1 o 2.

CAPíTULO 2

Funciones y conteo

2.1. Funciones

Supongamos que X e Y son conjuntos. Decimos que f es una **función de X en Y**, si por cada x en X podemos especificar un único elemento $f(x)$ en Y. La notación estándar $f : X \to Y$ para una función f de X en Y. Es útil pensar a f como una regla que asigna a cada objeto x en Xun único $f(x)$ en Y. $f(x)$ es usualmente llamado el **valor** de f en x. Lo importante es que $f(x)$ este definida para todo x en X, y que hay un solo $f(x)$ por cada x.

Las funciones más comunes en matemática elemental son aquellas en las cuales X e Y son los conjuntos $\mathbb{N}$ o $\mathbb{Z}$ o algunos otros conjuntos de números. En este caso el método más simple para especificar una función es por medio de una fórmula. Por ejemplo, la regla:

$$f(n) = 3n + 4 \qquad (n \in \mathbb{N})$$

define la función f de $\mathbb{N}$ en $\mathbb{N}$ cuyo valor en n es $3n + 4$. Algunas funciones pueden requerir una definición por partes, como la función g de $\mathbb{Z}$ en $\mathbb{Z}$ dada por la regla:

$$g(x) = \begin{cases} x & \text{si} \quad x \geq 0 \\ -x & \text{si} \quad x \leq 0 \end{cases}$$

Esta función asigna a cada entero x su *valor absoluto*, usualmente escrito $|x|$. Por ejemplo, $|5| = |-5| = 5$.

Cuando $X = \mathbb{N}$, otra forma de especificar una función es el método de definición recursiva, explicado en la sección 1.3 . En esa sección hablamos (vagamente) de una expresión u_n definida para cada n en $\mathbb{N}$. Sería más preciso decir que u_n es solo una notación alternativa para $u(n)$, donde u es una función de $\mathbb{N}$ en un conjunto apropiado Y. Por ejemplo, las ecuaciones

$$u(1) = 1, \qquad u(2) = 2, \qquad u(n) = u(n-1) + u(n-2) \qquad (n \geq 3)$$

nos dan una definición recursiva de una función u de $\mathbb{N}$ a $\mathbb{N}$. Generalmente nos referimos a la lista de valores de esta función como una *sucesión* en este caso la sucesión es

$$1, 2, 3, 5, 8, 13, 21, \ldots$$

donde los tres puntos al final indican que la lista continúa indefinidamente. Por lo general una sucesión de miembros de un conjunto Y es solo otro nombre para una función de $\mathbb{N}$ en Y. (A veces es conveniente reemplazar $\mathbb{N}$ por $\mathbb{N}_0$ o algún otro conjunto de enteros.) Una sucesión puede

ser definida recursivamente, o por una fórmula, o de alguna otra manera, pero en todos los casos debemos tener un único elemento de Y para cada entero relevante n.

Una propiedad útil de las funciones es que, en algunas circunstancias, pueden ser combinadas. Específicamente, si nos dan funciones f de X a Y, y g de Y a Z, entonces hay una función de X a Z definida de la siguiente manera. Para cada x en X el valor $f(x)$ está en Y, y el valor de g en $f(x)$ es el elemento $g(f(x))$ de Z. Considerando esta operación de dos pasos como un paso único, tenemos una función de X en Z que lleva x a $g(f(x))$; y que es llamada la **composición** de las funciones $f : X \to Y$ y $g : Y \to Z$ escrita gf. Así

$$(gf)(x) = g(f(x)).$$

Es aconsejable recordar que (en este libro) gf significa "primero f, entonces g". Aunque fg es una especie de producto de g y f, esta forma de pensar nos puede conducir a conceptos erróneos. Si X, Y, Z son conjuntos diferentes, entonces gf se define como ya lo hicimos, pero fg no tiene sentido. Más aún, si gf y fg están ambas definidas, como cuando $X = Z$, no hay razón por la cual deberían ser iguales.

2.1.1. Ejercicios.

1. Las funciones s y t de $\mathbb{Z}$ en $\mathbb{Z}$ están definidas por

   $$s(x) = x + 1, \qquad t(x) = 2x \quad (x \in \mathbb{Z}).$$

   Muestre que st no es igual a ts.
2. Sea $X = \{1, 2, 3, 4, 5\}$ y sea $f : X \to X$ una función definida por

   $$f(1) = 2, \quad f(2) = 2, \quad f(3) = 4, \quad f(4) = 4, \quad f(5) = 4.$$

   Muestre que $ff = f$ .Encuentre una función g distinta de f tal que $gf = f$ y $fg = f$.
3. Sea U el conjunto de ciudadanos de Utopía. ¿Cuál de las siguientes expresiones define correctamente una función de U en U?
   (i) $f(x)$ es la madre de x.
   (ii) $g(x)$ es la hija de x.
   (iii) $h(x)$ es la esposa de x.
4. Suponga que f, g y h son funciones tales que la composición $h(gf)$ está definida. Muestre que $(hg)f$ también está definida, y $(hg)f = h(gf)$.

2.2. Funciones Suryectivas, Inyectivas y Biyectivas

Hay ciertos tipos de funciones que tienen nombres especiales.

Definición 2.2.1. La función $f(x)$ de X en Y es una **suryección** si cada y en Y es $f(x)$ de *al menos* un x en X. Es una **inyección** si cada y en Y es $f(x)$ de *a lo más* un x en X. Es una

biyección si es a la vez suryección e inyección, o sea, si cada y en Y es $f(x)$ de exactamente un x en X.

Ejemplo 2.2.1. Las siguientes fórmulas definen funciones de $\mathbb{Z}$ en $\mathbb{Z}$. ¿Cuáles son suryectivas, cuáles inyectivas y cuáles biyectivas?

$$\text{(i)} \quad f(x) = x^2; \qquad \text{(ii)} \quad g(x) = 2x; \qquad \text{(iii)} \quad h(x) = x + 2.$$

Demostración. (i) Como $f(x) = x^2$ y x^2 nunca es negativo, ningún entero negativo como -1 puede ser valor de f. Por lo tanto, no existe un entero x tal que $f(x) = -1$ y entonces f no es suryectiva. Además, hay algunos enteros y para los cuales hay dos soluciones a la ecuación $f(x) = y$ por ejemplo, tomando $y = 4$ tenemos $f(2)$ y $f(-2)$ ambos iguales a 4. Entonces no es inyectiva.

(ii) Como $g(x) = 2x$ y $2x$ es par, un entero impar como tres no puede ser valor de g. Por lo tanto, g no es suryectiva.. Por otro lado g es inyectiva.. Para probarlo, supongamos que hay dos enteros x y x' tal que $g(x)$ y $g(x')$ toman el mismo valor y, o sea, $2x = 2x'$. Cancelando el factor 2 tenemos $x = x'$, lo que implica que hay como máximo una solución a la ecuación $g(x) = y$, y luego g es inyectiva.

(iii) Si se nos dan un entero y, entonces tomando $x = y - 2$ tenemos

$$h(x) = x + 2 = y.$$

Entonces hay por lo menos un entero x tal que $h(x) = y$ y entonces h es suryectiva. Si hubiera dos de tales enteros x y x' deberíamos tener $x + 2 = x' + 2$, lo que implica que $x = x'$. Por lo tanto h es inyectiva. y, además, una biyección. □

Vale la pena remarcar que la técnica usada antes para probar que g y h son inyectivas es la más conveniente en la práctica. En general, si queremos probar que una función f es inyectiva asumimos $f(x) = f(x')$ y deducimos que $x = x'$.

Un tipo particular de función inyectiva tiene un nombre especial, si X es un subconjunto de Y entonces la función **inclusión** $i : X \to Y$, definida por $i(x) = x$ es claramente una inyección. Cuando $X = Y$ es una biyección y en este caso a veces se la llama función **identidad** en X. El siguiente teorema es muy útil.

Teorema 2.2.1. *Si $f : X \to Y$ y $g : Y \to Z$ son inyectivas entonces la composición $gf : X \to Z$ también lo es. Si f y g son suryectivas, también lo es gf y si f y g son biyectivas, también lo es gf.*

Demostración. Supongamos que $(gf)(x) = (gf)(x')$ como $g(f(x)) = g(f(x'))$ y g es inyectiva obtenemos que $f(x) = f(x')$ y como f es inyectiva, $x = x'$ por lo tanto gf es inyectiva.

Ahora si g es suryectiva, entonces para cualquier z en Z tenemos que $z = g(y)$ para algún y en Y, y si f es suryectiva hay algún x en X para el cual $f(x) = y$ así $z = g(f(x)) = (gf)(x)$, y gfes una suryección.

La proposición para biyecciones es una consecuencia directa de las dos precedentes. □

El concepto de biyección es fundamental para el proceso de conteo, como veremos en la próxima sección. Puede también formularse de otra manera, como se expone en lo siguiente.

Definición 2.2.2. Una función f de X en Y tiene una función **inversa** g de Y en X, si para todo x en X e y en Y,

$$(gf)(x) = x, \qquad \text{y} \qquad (fg)(y) = y$$

.

En otras palabras, gf es la función identidad en X y fg es la función identidad en Y.

Podría decirse que una función g revierte los efectos de f. Las ecuaciones en la definición pueden ser replanteadas en la forma equivalente:

$$f(x) = y \quad \Leftrightarrow \quad g(y) = x,$$

que es más cercana a la noción intuitiva de una función inversa. Por ejemplo dada una función f de $\mathbb{Z}$ en $\mathbb{Z}$ definida por $f(x) = x + 3$, una función inversa g puede ser encontrada señalando que

$$x + 3 = y \qquad \Leftrightarrow \qquad y - 3 = x,$$

Entonces $g(y) = y - 3$.

Por supuesto, no toda función tiene inversa. Pero si la hay, entonces es única. Porque si $f : X \to Y$, y g y g' ambas satisfacen las condiciones para ser una inversa de f, entonces (en particular) $g'f$ es identidad en X y fg es la identidad en Y. Entonces tenemos

$$g = (g'f)g = g'(fg) = g'.$$

Luego $g = g'$ y la inversa es única.

Este argumento justifica que hablemos de *la* inversa de f, (si existe) y el uso de notación f^{-1} para la única función inversa. Además, la inversa de f^{-1} es f, entonces $(f^{-1})^{-1} = f$.

Teorema 2.2.2. *Una función tiene inversa si y solo si es biyectiva.*

Demostración. Supongamos. que f es una biyección de X en Y. Para cada y en Y hay precisamente un x en X tal que $f(x) = y$. La regla $g(y) = x$ define una función de Y a X que es una inversa de f.

Por otro lado, supongamos que f tiene una inversa f^{-1}. Dado y en Y sabemos que $f(f^{-1}(y)) = y$, luego poniendo $x = f^{-1}(y)$ da $f(x) = y$. Entonces f es suryección. Para demostrar que f también es inyectiva supongamos que $f(x) = f(x')$. Aplicando f^{-1} a ambos lados de la ecuación obtenemos $x = x'$ como se requiere. □

Por supuesto una consecuencia inmediata de este teorema es que la inversa de una biyección es una biyección.

2.2.1. Ejercicios.

1. ¿Cuáles de las siguientes funciones de $\mathbb{Z}$ en $\mathbb{Z}$ son suryecciones, cuáles son inyecciones y cuáles son biyecciones?

$$\text{(i) } f(x) = x^3, \qquad \text{(ii) } g(x) = x - 3,$$
$$\text{(iii) } h(x) = 3x + 1, \qquad \text{(iv) } i(x) = x^2 + 1.$$

2. La función u de $\mathbb{N}$ en $\mathbb{N}$ es definida recursivamente por la siguiente regla:

$$u(1) = 1, \qquad u(n+1) = \begin{cases} (1/2)u(n) & \text{si } u(n) \text{ es par;} \\ 5u(n) + 1 & \text{en otro caso.} \end{cases}$$

   Demuestre que u no es ni inyectiva ni suryectiva.
3. Pruebe que si f y g son biyectivas, y gf esta definida, entonces la inversa de gf es $f^{-1}g^{-1}$.
4. Se dice que una función $f : X \to Y$tiene una **inversa a izquierda** $l : Y \to X$ si lf es la función identidad en X. Demuestre que:
   i)Si f tiene inversa a izquierda entonces es inyectiva ;
   ii)Si f es inyectiva entonces tiene una inversa a izquierda.
5. Formule y pruebe resultados sobre una *inversa a derecha* de $f : X \to Y$ que sean similares a los del ejercicio previo.

2.3. Conteo

¿Cuál es significado de decir que un conjunto tiene n miembros? Una manera de contestar esto es recordar como contamos conjuntos simples. Decimos las palabras uno, dos, tres, etc. y señalamos los objetos de a uno. Cuando cada objeto recibe un número, paramos, y el último número pronunciado es el número de elementos del conjunto. Para trasladar esta técnica de "decir y señalar" a lenguaje matemático debemos primero definir, para cada entero positivo n, el conjunto

$$\mathbb{N}_n = \{1, 2, 3, \ldots, n\}.$$

La técnica de decir y señalar asigna a cada miembro de $\mathbb{N}_n$ un miembro del conjunto X (el conjunto que esta siendo contado) en otras palabras, determina una función f de $\mathbb{N}_n$ en X. Además esta claro que la función f es una *biyección* porque si hemos contado correctamente, cada miembro de X recibe solo un número. Entonces, si X es un conjunto y n un entero positivo, y si hay una biyección de $\mathbb{N}_n$ en X, entonces podemos decir que el conjunto X tiene n elementos.

Debe señalarse que la definición no excluye explícitamente la posibilidad de que un conjunto tenga al mismo tiempo n elementos y m elementos, con m distinto de n. Es más, todos tenemos la experiencia de haber contado y recontado algunos conjuntos grandes de objetos como por ejemplo ovejas de un campo, obteniendo respuestas diferentes cada vez. El próximo teorema es la clave

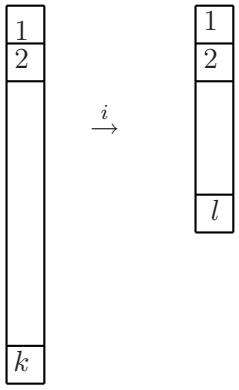


FIGURA 1. La supuesta inyección $i : \mathbb{N}_k \to \mathbb{N}_l$

para demostrar que esto sólo se debe a ineptitud práctica, y que hay una respuesta correcta. En otras palabras, un conjunto de n elementos no puede ser de m elementos, para $m \neq n$.

TEOREMA 2.3.1. *Si n y m son enteros positivos tales que $m < n$, entonces no existe una función inyectiva de $\mathbb{N}_n$ a $\mathbb{N}_m$.*

DEMOSTRACIÓN. Sea S el conjunto de enteros positivos n para los cuales existe una inyección de $\mathbb{N}_n$ en $\mathbb{N}_m$ para algún $m < n$. Si S no es vacío, entonces tiene un elemento k, y como k pertenece a S hay una inyección de $\mathbb{N}_k$ en $\mathbb{N}_l$ para algún $l < k$. No podemos tener $l = 1$, pues ninguna función de $\mathbb{N}_k$ en $\mathbb{N}_1$ puede tomar sólo el valor 1, y por lo tanto no puede haber una inyección definida sobre $\mathbb{N}_k$ para $k > 1$. Luego $l - 1$ es un entero positivo y la situación puede ser descrita en la Fig. 1.

Si ninguno de los valores $i(1), i(2), \ldots, i(k-1)$ es igual a l, entonces restringiendo i al conjunto $\mathbb{N}_{k-1}$, tenemos una inyección de $\mathbb{N}_{k-1}$ en $\mathbb{N}_{l-1}$. Por otro lado, si $i(b) = l$ para algún b en el rango $1 \leq b \leq k - 1$, entonces debemos tener $i(k) = c$ distinto de l, pues i es inyectiva. En este caso podemos construir una inyección i^* de $\mathbb{N}_{k-1}$ en $\mathbb{N}_{l-1}$ como se muestra en la Fig 2; esto es

$$i^*(b) = c, \qquad i^*(r) = i(r) \qquad (r \neq b).$$

En ambos casos la existencia de una inyección de $\mathbb{N}_{k-1}$ en $\mathbb{N}_{l-1}$ contradice la definición de k como el mínimo de S. Por lo tanto S debe ser vacío, y el teorema está probado. □

Supongamos que hay un conjunto X que tiene n elementos, y además m elementos para algún $n < m$. Se sigue que hay biyecciones

$$\beta : \mathbb{N}_n \to X, \qquad \gamma : \mathbb{N}_m \to X,$$

y por los resultados establecidos en la sección anterior, ambas γ^{-1} y $\gamma^{-1}\beta$ son también biyectivas. En particular, $\gamma^{-1}\beta$ es una inyección de $\mathbb{N}_n$ en $\mathbb{N}_m$, lo cual contradice al Teorema 2.3. De esta manera la proposición: "X tiene n elementos" vale para, como máximo, un entero positivo n.

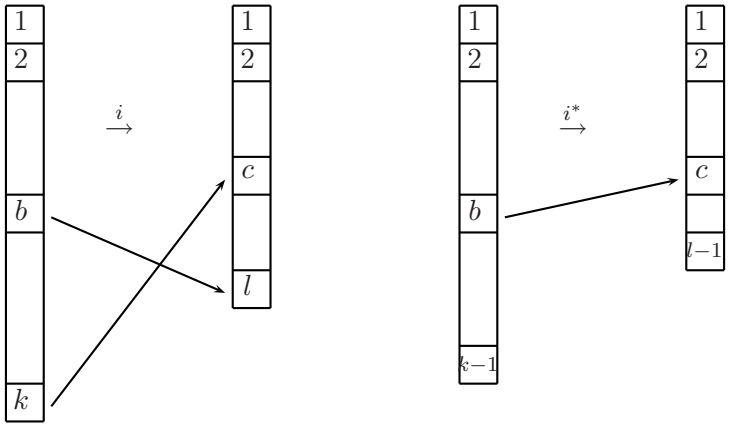


FIGURA 2. La construcción de i^* cuando $i(b) = l$

Cuando X tiene n elementos, escribimos $|X| = n$, y decimos que el **cardinal** de X es n. Para el conjunto vacío $\emptyset$ hacemos una definición especial pero razonable,

$$|\emptyset| = 0.$$

Cuando $|X| = n$ usualmente es conveniente poner

$$X = x_1, x_2, \ldots, x_n,$$

que en realidad otra manera de decir que existe una biyección β de $\mathbb{N}_n \to X$, tal que $\beta(i) = x_i$ $(1 \leq i \leq n)$.

Finalmente, una advertencia: hay conjuntos que no tienen un cardinal acorde con la definición. El conjunto $\mathbb{N}$ es un ejemplo. Volveremos sobre este tema en la sección 2.5.

2.4. El Principio de las Casillas

El Teorema 2.3.1, que fue probado para justificar la definición de cardinal, puede ser también usado en forma más práctica. Supongamos que tenemos un conjunto X, cuyos elementos llamaremos "objetos", y un conjunto Y cuyos elementos serán "casillas", o "cajas". Una *distribución* de los objetos en casillas es simplemente una función f de X en Y: si el objeto x va en la casilla y, entonces $f(x) = y$.

En este modelo la función es una suryección si cada casilla recibe por lo menos un objeto, y una inyección si cada casilla recibe como máximo un objeto. Ahora es claro que si hay más objetos que casillas entonces alguna casilla recibirá por lo menos dos elementos; en otras palabras, la función no puede ser inyectiva. Formalmente esto es consecuencia del Teorema 2.3. Supongamos $|X| = m$ y $|Y| = n$, donde $m > n$; entonces una inyección de X a Y produciría una inyección de $\mathbb{N}_m$ en $\mathbb{N}_n$, lo cual es imposible de acuerdo con el teorema. Esta observación se conoce usualmente

como el principio de las casillas:

Si m objetos son distribuidos en n casillas, y $m > n$,

entonces por lo menos una casilla recibe al menos dos objetos.

Hay muchas aplicaciones obvias de este principio, como por ejemplo:

(i) En un conjunto de 13 personas o más, hay por lo menos dos que cumplen años en el mismo mes.
(ii) En cualquier conjunto de un millón de personas, hay por lo menos dos con la misma cantidad de pelos en la cabeza.
(iii) En cualquier conjunto de 51 personas o más nacidos en Estados Unidos, hay al menos dos que han nacido en el mismo estado.

EJEMPLO 2.4.1. Demuestre que si X es cualquier conjunto de gente, hay dos miembros de X que tienen el mismo número de amigos. (Se asume que si x es amigo de x', entonces x' es amigo de x).

DEMOSTRACIÓN. Consideremos que la función f definida sobre X por la regla que, para cada elemento x de X,

$$f(x) = \text{número de amigos de x en X.}$$

Si $|X| = m$, los posibles valores de $f(x)$ son $0, 1, \ldots, m-1$, porque los amigos de x pueden ser todos los miembros de X menos x. Entonces f es una función de X al conjunto $Y = \{0, 1, \ldots, m-1\}$.

En este punto no podemos aplicar inmediatamente el principio de las casillas, porque Y tiene el mismo cardinal m que X. Sin embargo, si existe una persona x^* que tiene $m-1$ amigos, entonces x^* es amigo de todos los demás y consecuentemente no hay nadie sin amigos. En otras palabras, los números $m-1$ y 0 no pueden ser ambos valores de f. Por lo tanto f es una función de un conjunto de m elementos a un conjunto de $m-1$ (o menos) elementos, y el principio de las casillas nos dice que existen por lo menos 2 personas x_1 y x_2 tal que $f(x_1) = f(x_2)$, como queríamos ver. □

2.5. ¿Finito o Infinito?

Hemos evitado hasta ahora el uso de las palabras "finito" e "infinito", pero ahora estamos en condiciones de dar una definición formal.

DEFINICIÓN 2.5.1. Un conjunto X es **finito** si es vacío o si $|X| = n$ para algún entero positivo n. Un conjunto no finito es llamado **infinito**.

De acuerdo con la definición X es infinito si es no vacío y si no existe biyección de $\mathbb{N}_n$ en X para ningún $n \in \mathbb{N}$. Por supuesto el candidato más obvio de conjunto infinito es $\mathbb{N}$ mismo, y comenzaremos por convencernos de que $\mathbb{N}$ es realmente infinito.

Ciertamente $\mathbb{N}$ no es vacío, porque contiene, por ejemplo, al 1. Supongamos que existe una biyección β de $\mathbb{N}_n$ en $\mathbb{N}$ para algún entero positivo n. Como $\mathbb{N}_{n+1}$ es un subconjunto de $\mathbb{N}$, la inclusión $i : \mathbb{N}_{n+1} \to \mathbb{N}$ es una inyección y la composición

$$i\beta : \mathbb{N}_{n+1} \to \mathbb{N} \to \mathbb{N}_n$$

es también una inyección. Pero esto contradice el Teorema 2.3.1, entonces $\mathbb{N}$ es infinito como habíamos afirmado.

Un ejemplo más interesante de un conjunto infinito es el siguiente ejemplo. La demostración (que se atribuye a Euclides) es considerada una de las más elegantes piezas del razonamiento matemático.

Ejemplo 2.5.1. El conjunto P de números primos es infinito.

Demostración. P no es vacío, puesto que 2 es primo. Supongamos que P es finito, luego existe una biyección entre P y un conjunto $\{1, 2, \ldots, n\}$ y los primos pueden ser listados como $p_1, p_2, \ldots, p_n$. Debemos mostrar que esa lista no puede contener todos los primos. Consideramos el entero positivo

$$m = p_1 p_2 \ldots p_n + 1.$$

Ninguno de los primos $p_1, p_2, \ldots, p_n$ divide a m, pero por otro lado, sabemos que m tiene una factorización en primos. Por lo tanto esta factorización debe contener primos que no son están en $p_1, p_2, \ldots, p_n$ y nuestra propuesta de lista resulta incompleta. □

Teorema 2.5.1. *El conjunto no vacío X es infinito si y sólo si existe una inyección de $\mathbb{N}$ en X*

Demostración. Si X es infinito podemos definir una función de $\mathbb{N}$ en X recursivamente, de la siguiente manera. Tomemos $f(1)$ un elemento cualquiera de X, y si $f(1), \ldots, f(n)$ ya han sido definidos, tomamos $f(k+1)$ un elemento cualquiera de X que no esté entre los $f(1), \ldots, f(k)$. Esto significa que no hay dos valores de f iguales, entonces f es inyectiva. Más aún, la definición de $f(k+1)$ es siempre posible, puesto que si no hubiera ningún valor disponible para $f(k+1)$ tendríamos que $X = \{f(1), \ldots, f(k)\}$ y f sería una biyección entre $\mathbb{N}_k$ y X, lo que contradice la hipótesis que dice que X es infinito.

Recíprocamente, supongamos que hay una inyección f de $\mathbb{N}$ en X. Si X fuera finito deberíamos tener una biyección $\beta : \mathbb{N}_n \to X$ para algún entero positivo n, y en consecuencia tendríamos una cadena de inyecciones

$$\mathbb{N}_{n+1} \xrightarrow{i} \mathbb{N} \xrightarrow{f} X \xrightarrow{\beta^{-1}} \mathbb{N}_n$$

donde i es la inclusión. Entonces la composición de estas funciones es una inyección de $\mathbb{N}_{n+1}$ en $\mathbb{N}_n$, en contradicción con el Teorema 2.3.1. Por consiguiente X es infinito. □

De acuerdo con el Teorema 2.5.1, si se nos da un conjunto infinito X siempre podemos tratar de "contar" el conjunto construyendo una inyección f de $\mathbb{N}$ a X. En algunos casos seremos capaces de construir f de tal manera que todo elemento de X reciba un número. Si esto puede hacerse, entonces f es también sobreyectiva (y consecuentemente biyectiva), y en este caso diremos que X es **contable**. Por otro lado, si es imposible construir una biyección entre $\mathbb{N}$ y X diremos que X es **incontable**.

Reiteremos brevemente la distinción entre los términos finito e infinito, contable e incontable. Si existe un proceso de conteo que se termina, el conjunto es *finito*. Si existe un proceso de conteo que no termina pero que alcanza a cualquier elemento del conjunto, entonces el conjunto es *infinito*, pero *contable*. Si cualquier proceso de conteo nunca alcanza a todos los elementos, entonces el conjunto es *infinito* e *incontable*. Hablando sin precisión, en matemática discreta se trabaja con conjuntos finitos o contables, mientras que en cálculo y análisis se trabaja con conjuntos incontables tales como el conjunto $\mathbb{R}$ de los números reales.

Finalizamos este capítulo con unas palabras de advertencia. Las propiedades de los conjuntos finitos nos son muy familiares, y por esa razón nuestra intuición es una guía confiable para trabajar con ellos. Por ejemplo, nosotros aceptamos sin dudas la afirmación de que si A es un subconjunto de un conjunto finito B, entonces A es finito y $|A| \leq |B|$. (En realidad, la prueba de esto puede ser complicada, pero puede hacerse sobre la base de nuestro axiomas y definiciones usando, una vez más, el ubicuo Teorema 2.3.1) Por otro lado, la intuición puede ser una guía muy pobre cuando trabajamos con conjuntos infinitos. Esto es debido a que las definiciones que los matemáticos han hecho para mantener la consistencia lógica no siempre corresponden a nuestra ideas intuitivas.

Un ejemplo del extraño comportamiento de los conjuntos infinitos será suficiente. Sea E el subconjunto de $\mathbb{N}$ que consta de todos los enteros pares, $E = \{2, 4, 6, \ldots\}$. Es obvio que la función h de $\mathbb{N}$ a E definida por la regla $h(n) = 2n$ es una *biyección*, y que E es un subconjunto *propio* de $\mathbb{N}$, esto es, es un subconjunto que no es todo $\mathbb{N}$. Por consiguiente un conjunto infinito puede tener un subconjunto propio que está en biyección con el conjunto original.

2.5.1. Ejercicios.

1. Construyendo una inyección de $\mathbb{N}$ a X muestre que cada uno de los siguientes conjuntos es infinito:

   $$\text{(i)} \quad \mathbb{Z}, \qquad \text{i(i)} \quad \{x \in \mathbb{Z} | x < 0\}, \qquad \text{(iii)} \quad \{n \in \mathbb{N} | n \geq 10^6\}.$$

2. Probar que la función $f : \mathbb{N} \to \mathbb{Z}$ definida por

   $$f(n) = \begin{cases} n/2 & \text{si } n \text{ es par,} \\ -(n-1)/2 & \text{si } n \text{ es impar,} \end{cases}$$

   es una biyección. Use este resultado para exhibir otro ejemplo de "comportamiento extraño" referido en la parte final del parágrafo de arriba.

3. Todo primo, excepto 2 y 3, es de la forma $6m+1$ o $6m+5$ para algún entero m. Usar el método del ejemplo para probar que el número de primos de la forma $6m+5$ es infinito. [Ayuda: reemplace el $+1$ del método de Euclides por -1.]
4. Usar el Teorema 2.5.1 para probar que si X es un subconjunto de Y y X es infinito, entonces Y es infinito.
5. Sea X un subconjunto no vacío de $\mathbb{Z}$ que no tiene mínimo. Probar que se puede elegir una sucesión $x_1, x_2, \ldots$ de elementos de X tal que $x_n < x_{n-1}$ $(n \in \mathbb{N})$. Deducir que X es infinito.
6. Debido al ejercicio (5) un subconjunto S finito y no vacío de $\mathbb{Z}$ debe tener un mínimo. Probar que si S y T son subconjuntos finitos y no vacíos de $\mathbb{Z}$, entonces

$$\min(S \cup T) \leq \min S,$$
$$\min(S \cap T) \geq \min S.$$

2.6. Ejercicios

1. ¿Cuáles de las siguientes funciones son inyectivas, cuáles son suryectivas y cuáles son biyectivas?

   (i) $f(x) = 1 + x^2$, (ii) $g(x) = 1 + x^3$, (i) $h(x) = 1 + x^2 + x^3$.

2. Sea X un conjunto con $|X| = 3$. ¿Cuántas biyecciones diferentes f hay de X a X, y cuántas satisfacen $f = f^{-1}$?
3. Probar que si X es un conjunto finito y $g : X \to X$ es una inyección, entonces g es una biyección.
4. Probar que si X es un conjunto finito y $f : X \to X$ es una suryección, entonces f es una biyección.
5. Sea X un conjunto finito y $g : X \to X$ es una función tal que $g^2(x) = x$ para todo $x \in X$. Probar que g es una biyección.
6. Nos referiremos a los siguientes subconjuntos de $\mathbb{Z}$ como *bloques*:

   $$\{1,2,4\},\ \{2,3,5\},\ \{3,4,6\},\ \{4,5,7\},\ \{1,5,6\},\ \{2,6,7\},\ \{1,3,7\}.$$

   Definamos

   $$f(x,y) = \begin{cases} z & \text{si } x \neq y \text{ y } \{x,y,z\} \text{ es un bloque,} \\ x & \text{si } x = y. \end{cases}$$

   ¿Es f función? ¿Es una inyección?
7. Probar que si elegimos 5 puntos arbitrarios dentro de un cuadrado de lados de longitud 2, entonces hay dos puntos cuya distancia es menor o igual a $\sqrt{2}$.
8. Probar que si elegimos 10 puntos arbitrarios dentro de un triángulo equilátero de lados de longitud 1, entonces hay dos puntos cuya distancia es menor o igual a $1/3$.

9. ¿Cuántos puntos deben ser elegidos dentro de un cuadrado de lados de longitud 2 para asegurar que hay dos puntos cuya distancia es menor o igual a $\sqrt{2}/n$?
10. Probar que en cualquier conjunto de 172 números enteros debe haber un par de ellos cuya diferencia es divisible por 171. ¿Es esto cierto si cambiamos la palabra "diferencia" por "suma"?
11. Probar que el conjunto de enteros positivos cuyos dígitos (en la representación en base 10) son todos diferentes es finito. ¿Cuántos de ellos hay?
12. Un *punto reticulado* (*lattice point* en inglés) en el espacio usual de dimensión 3, es un punto con coordenadas enteras. Probar que si elegimos 9 puntos reticulados, entonces hay al menos un par de ellos en que el punto medio del segmento que los une es también un punto reticulado.
13. Sea $x_1, x_2, \ldots, x_r$ una sucesión de enteros distintos. Por cada i $(1 \leq i \leq r)$ denotemos m_i la longitud de la subsucesión más larga que comienza con x_i y es creciente. Denotemos n_i la longitud de la subsucesión más larga que comienza con x_i y es decreciente. Probar que la función f que asigna a cada i el par (m_i, n_i) es una inyección.
14. Probar que un subconjunto de un conjunto contable es contable.
15. Probar que la unión de dos conjuntos contables es contable.
16. Probar que la unión de una colección contable de conjuntos contables es contable.
17. Sea X un conjunto y sea Y el conjunto de todos los subconjuntos de X. Probar que no existe una biyección de X a Y.
18. Probar que el conjunto formado por todos los subconjuntos de $\mathbb{N}$ es un conjunto incontable.
19. Probar que si A es un subconjunto de un conjunto finito B, entonces A es finito y $|A| \leq |B|$.

CAPíTULO 3

Principios de conteo

3.1. Los principios de adición y multiplicación

Un objetivo importante de este curso es el desarrollo de técnicas efectivas de conteo de un conjunto finito X. Cuando X aparece a partir de un problema complejo, podemos necesitar técnicas de conteo complicadas. En este capítulo comenzaremos a desarrollar estos métodos.

Nuestra primer regla es tan simple que ha sido usada desde los comienzos de la civilización. Solo recientemente, y en el contexto del desarrollo estricto del tema, se le ha dado un status formal.

TEOREMA 3.1.1. *Si A y B son conjuntos finitos, no vacíos, y A y B son disjuntos (esto es $A \cap B = \emptyset$, el conjunto vacío), entonces*

$$|A \cup B| = |A| + |B|.$$

DEMOSTRACIÓN. Puesto que A y B son conjuntos finitos y no vacíos, podemos listar a A y B en la forma estándar:

$$A = \{a_1, \ldots, a_r\}, \qquad B = \{b_1, \ldots, b_s\}.$$

Debido a que A y B son disjuntos, $A \cup B$ puede ser listado de una manera similar:

$$A \cup B = \{c_1, c_2, \ldots, c_r, c_{r+1}, \ldots, c_{r+s}\}$$

donde

$$c_i = a_i \quad (1 \leq i \leq r) \qquad \text{y} \qquad c_{r+i} = b_i \quad (1 \leq i \leq s).$$

Luego $|A \cup B| = r + s = |A| + |B|$, que es lo que se quería a probar.

□

Es claro que esta regla aún es válida si A, o B, o ambos A y B, son vacíos. Más aún, la regla puede extenderse a la unión de un número cualquiera de conjuntos disjuntos $A_1, A_2, \ldots, A_n$ de la manera obvia:

$$|A_1 \cup A_2 \cup \cdots \cup A_n| = |A_1| + |A_2| + \cdots + |A_n|.$$

La prueba es un ejercicio fácil usando el principio de inducción. Las sencilla regla expuesta más arriba es llamada el *principio de adición*.

Por otro lado si A y B no son disjuntos, cuando sumamos $|A|$ y $|B|$ estamos contando $A \cap B$ dos veces. Entonces, para obtener la respuesta correcta debemos restar $|A \cap B|$:

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

Una generalización de este principio (llamado *principio del tamiz*) se puede ver en Apéndice I.

Una simple aplicación del principio de adición nos da una forma más general del principio de las casillas que aquella que fue dada en la sección 2.4. Supongamos que cierta cantidad de objetos se introduce en n cajas, y A_i denota los objetos que hay en la caja i $(1 \leq i \leq n)$. Puesto que los conjuntos A_i son disjuntos, entonces el número total de objetos es $|A_1| + |A_2| + \cdots + |A_n|$, y si ninguna caja contiene más que r objetos entonces este número es como mucho

$$r + r + \cdots + r = nr.$$

Revirtiendo este argumento, obtenemos el principio de las casillas generalizado:

si m objetos son distribuidos en n cajas y $m > nr$,

entonces una caja contiene como mínimo $r + 1$ objetos.

Ejemplo 3.1.1. Probar que en cualquier grupo de seis personas hay tres que se conocen mutuamente o tres que se desconocen mutuamente.

Demostración. Sea α cualquiera de las personas, y distribuya el resto de las personas en dos "cajas", la caja 1 contiene las personas conocidas por α y la caja 2 las personas desconocidas. Puesto que $5 > 2 \times 2$, una de las cajas contiene al menos tres personas.

Supongamos que la caja 1 contiene β, γ, y δ (y posiblemente otras personas). Si dos personas de $\{\beta, \gamma, \delta\}$ se conocen, digamos β y γ, entonces $\{\alpha, \beta, \gamma\}$ son conocidos mutuamente. Por otro lado si ningún par de $\{\beta, \gamma, \delta\}$ se conoce, entonces $\{\beta, \gamma, \delta\}$ es un conjunto de tres personas que se desconocen mutuamente.

Si lo que ocurre es que la caja 2 contiene tres o más personas, un argumento paralelo con conocidos y desconocidos intercambiados nos conduce a la misma conclusión.

□

La segunda regla general que daremos em esta sección es el principio de multiplicación:

Teorema 3.1.2. *Sea X e Y conjuntos finitos entonces el cardinal de $X \times Y$ es dado por*

$$|X \times Y| = |X| \times |Y|.$$

Demostración. $X \times Y = \{(x, y) | x \in X, y \in Y\}$, luego si fijamos x en X y denotamos $A_x = \{(x, y) | y \in Y\}$, es claro que $|A_x| = |Y|$ y $X \times Y = \cup_{x \in X} A_x$ una unión disjunta. Por el principio de adición obtenemos $|X \times Y| = |Y| + \cdots + |Y|$, una suma con $|X|$ sumandos, luego se deduce el resultado.

□

La generalización de este resultado a n conjuntos se expone en el ejercicio (5).

3.1.1. Ejercicios.

1. Las reglas de la competición de fútbol 5 de la Universidad de Folornia especifican que los miembros de cada equipo deben cumplir los años el mismo mes. ¿Cuántos alumnos de matemática son necesarios para garantizar la formación de un equipo?
2. ¿Qué es erróneo del siguiente argumento? Puesto que la mitad de los números n en el rango $1 \leq n \leq 60$ son múltiplos de 2, 30 de ellos no pueden ser primos. Puesto que un tercio de los números son múltiplos de 3, 20 no pueden ser primos. Por lo tanto a lo sumo 10 de ellos son números primos.
3. Escribir la prueba (usando inducción en n) del hecho que si $A_1, A_2, \ldots, A_n$ son conjuntos disjuntos, entonces
$$|A_1 \cup A_2 \cup \ldots \cup A_n| = |A_1| + |A_2| + \cdots + |A_n|.$$
4. Probar en cualquier conjunto de 10 personas hay cuatro que se conocen mutuamente o bien hay tres que se desconocen entre ellas.
5. Si $X_1, X_2, \ldots, X_n$ son conjuntos, el **conjunto producto** $X_1 \times X_2 \times \cdots \times X_n$ es definido como el conjunto de todas las n-uplas ordenadas $(x_1, x_2, \ldots, x_n)$, con $x_i \in X_i$ $(1 \leq i \leq n)$. Use el principio de inducción para probar que
$$|X_1 \times X_2 \times \cdots \times X_n| = |X_1| \times |X_2| \times \cdots \times |X_n|.$$

3.2. Funciones, palabras y selecciones

Consideraremos funciones (no necesariamente biyectivas) definidas sobre un conjunto de enteros positivos $\mathbb{N}_m$, y con valores en un conjunto Y dado. Los valores de función f determinan una m-upla.

$$(f(1), f(2), \ldots, f(m))$$

de elementos de Y. De acuerdo a la definición de producto de conjuntos (ejercicio 3.1.1 (5)) esta m-upla pertenece al conjunto $Y \times Y \times \cdots \times Y$ (m factores), que denotaremos Y^m. Cada elemento de Y^m es una m-upla $(y_1, y_2, \ldots, y_m)$ y corresponde a una función f de $\mathbb{N}_m$ en Y definida por las siguientes ecuaciones

$$f(1) = y_1, \quad f(2) = y_2, \quad \ldots, \quad f(m) = y_m.$$

Estas observaciones nos llevan a la conclusion de que una función es lógicamente la misma cosa que un elemento del conjunto producto Y^m.

Existe otra manera de ver esta relación, que es útil y practica. Si pensamos los elementos de Y como letras de un alfabeto, entonces la secuencia $f(1), f(2), \ldots, f(m)$ puede ser vista como

las m letras de una palabra. Por ejemplo, si Y es el alfabeto $\{a, b, c, d\}$ las palabra *cad* y *dad* corresponden a las funciones f y g definidas por

$$f(1) = c, \quad f(2) = a, \quad f(3) = b,$$
$$g(1) = d, \quad g(2) = a, \quad g(3) = g.$$

La función f, la 3-upla (c, a, b) y la palabra *cab*, son formalmente iguales. Entonces definimos una **palabra** de **longitud** m en el **alfabeto** Y como una función de $\mathbb{N}_m$ en Y.

Antes de usar esta idea debemos probar el resultado más general sobre conteo de conjuntos de funciones.

TEOREMA 3.2.1. *Sean X e Y conjuntos finitos no vacíos, y denotemos F el conjunto de funciones de X en Y. Si $|X| = m$ y $|Y| = n$, entonces*

$$|F| = n^m.$$

DEMOSTRACIÓN. Sea $X = \{x_1, x_2, \ldots, x_m\}$. Cada miembro f del conjunto F es una función de X en Y, y está determinada de forma única por la m-upla de sus valores $(f(x_1), f(x_2), \ldots, f(x_m))$. Esta m-upla pertenece a Y^m, luego

$$|F| = |Y^m| = n^m.$$

□

Del mismo modo podemos decir que el número de palabra de longitud m en un alfabeto Y de n símbolos es n^m. Por ejemplo, hay 26^3 palabras de tres letras en el alfabeto romano usual (asumiendo por supuesto que no hay restricciones de deletreo).

Existe otra manera importante de interpretar una función de $\mathbb{N}_m$ en Y, o equivalentemente, una palabra de longitud m en el alfabeto Y. Consideremos el trabajo de un linotipista en un trabajo de imprenta a la antigua. Para formar la palabra *cab*, selecciona una letra c de sus existencias, luego una a, luego una b. Suponemos que tiene que tiene existencias ilimitadas de letras, así que para formar la palabra *dad*, por ejemplo, él selecciona la d, luego la a, luego otra d. Cada palabra representa una selección ordenada de letras del alfabeto $Y = \{a, b, \ldots, z\}$, con repeticiones permitidas tantas veces como sea necesario.

En general podemos decir que una función desde $\mathbb{N}_m$ a Y es un modelo matemático de una *selección ordenada con repetición* de m cosas del conjunto Y. Por el Teorema 3.2.1, el número de tales selecciones es n^m, donde $|Y| = n$. (En secciones subsiguientes descubriremos como calcular selecciones que pueden ser ordenadas o desordenadas, y con o sin repetición.)

Esta simple regla para contar funciones (o palabras, o selecciones ordenadas con repetición) puede ser aplicada para obtener algunos resultados generales, como le siguiente ejemplo lo muestra.

EJEMPLO 3.2.1. Si X es un conjunto de n elementos, probar que el número total de subconjuntos es 2^n.

DEMOSTRACIÓN. Supongamos $X = \{x_1, x_2, \ldots, x_n\}$, y sea Y el alfabeto $\{0, 1\}$. Cualquier subconjunto S de X corresponde a una palabra de longitud n en Y, definida por la función

$$S(i) = \begin{cases} 0 & \text{si} \quad x_i \notin S, \\ 1 & \text{si} \quad x_i \in S. \end{cases}$$

Por ejemplo, si $n = 7$ y $S = \{x_2, x_4, x_5\}$, la palabra es 0101100. Usualmente pensamos al 0 representando **falso**, y 1 representando **verdadero**, entonces la palabra es construida controlado por turno cada elemento de X y colocando **falso** si no está en S, o **verdadero** si sí lo está.

En consecuencia el número de subconjuntos de X es el mismo que el número de palabras distintas de longitud n en el alfabeto $\{0, 1\}$, y esto es 2^n. □

3.2.1. Ejercicios.

1. ¿Cuántas banderas nacionales pueden ser construidas de tres franjas verticales, usando los colores rojo, blanco, azul, y verde? (Se asume que los colores pueden repetirse y que un borde vertical de la bandera es tomado como el borde junto al asta.)
2. Escriba todos los subconjuntos del conjunto $\{a, b, c, d\}$ y use la correspondencia dada en el ejemplo 3.2.1 para controlar que su lista es completa.
3. Las llaves son confeccionadas haciendo cortes de diferentes profundidades en una llave lisa. Si hay solo ocho profundidades posibles, ¿cuántas posiciones se requieren para hacer un millón de llaves diferentes? [Ayuda: para facilitar los cálculos use el hecho de que 2^{10} es un poco mas grande que 10^3.]
4. Probar que hay más de 10^{76} subconjuntos de el conjunto de subconjuntos de un conjunto de 8 elementos.

3.3. Inyecciones como selecciones ordenadas sin repetición

En muchas ocasiones tenemos que hacer selecciones ordenadas *sin* repetición. Aunque un compositor supuestamente debe tener una cantidad ilimitada de letras a su disposición, puede pasar que haya un solo objeto de cada tipo. Por ejemplo, si están seleccionando en un equipo de béisbol el orden para batear, ningún jugador puede ser seleccionado más de una vez.

El lenguaje de las funciones provee un modelo de esta situación. Hemos visto que una selección ordenada de m cosas de un conjunto Y corresponde a una función f de $\mathbb{N}_m$ en Y, donde $f(1)$ es el primer miembro de y seleccionado, y así siguiendo. Cuando permitimos repeticiones, es posible seleccionar el mismo objeto dos veces, esto es $f(r) = f(s)$ para $r \neq s$ en $\mathbb{N}_m$. Si esto está prohibido, o sea, si f es una *inyección*, entonces tenemos un modelo de una selección ordenada sin repetición.

TEOREMA 3.3.1. *El número de selecciones ordenadas sin repetición de m cosas del conjunto Y de tamaño n es el mismo que el número de funciones inyectivas de $\mathbb{N}_m$ en Y, y éste es*

$$n(n-1)(n-2)\cdots(n-m+1).$$

DEMOSTRACIÓN. Cada inyección i de $\mathbb{N}_m$ en Y ésta determinada de manera única por la selección ordenada de valores distintos $i(1), i(2), \ldots, i(m)$. La primera selección $i(1)$ puede ser de cualquiera de los n objetos; la segunda selección $i(2)$ debe recaer en uno de los $n-1$ objetos restantes. De manera similar, hay $n-2$ posibilidades para $i(3)$, y así sucesivamente. Cuando vamos a seleccionar $i(m)$, $m-1$ objetos ya han sido seleccionados, y entonces $i(m)$ debe ser uno de los $n-(m-1)$ objetos restantes. Por consiguiente el número total de selecciones es el propuesto. □

Por ejemplo, si tenemos un conjunto de 16 jugadores el número de formas de seleccionar un orden para batear para un equipo de béisbol de 9 es

$$16 \times 15 \times 14 \times 13 \times 12 \times 11 \times 10 \times 9 \times 8 = 4{,}151{,}347{,}200\ .$$

3.3.1. Ejercicios.

1. ¿De cuántas maneras se puede seleccionar el orden para batear de 11 jugadores entre un conjunto de 14?
2. ¿Cuántas palabras de cuatro letras se pueden formar con un alfabeto de 10 símbolos si no hay restricciones en el deletreado excepto que una letra no puede ser usada más de una vez?
3. Explique brevemente como haría usted una lista sistemática de todas las selecciones ordenadas y sin repetición, de tres cosas del conjunto $\{a, b, c, d, e, f\}$.
4. Sea $(n)_m = n(n-1)\cdots(n-m+1)$. Interpretando este número en términos de selecciones ordenadas sin repetición, probar que

   $$(n)_m \times (n-m)_{r-m} = (n)_r$$

   para cualesquiera enteros positivos tales que $n > r > m$.

3.4. Números binomiales

Muchas cuestiones prácticas de la Matemática Discreta toma la siguiente forma estándar¿De cuántas maneras puede seleccionarse cierto número de objetos de un conjunto dado? La respuesta a esta pregunta dependerá de si puede haber *repeticiones* de objetos o no, o de si importa o no el *orden* de la selección. Si el orden es importante, entonces debemos usar los modelos para selecciones ordenadas discutidos en las secciones 3.2 y 3.3; pero si no lo es, entonces es apropiado usar modelos diferentes, como ahora explicaremos. El modelo matemático de una *selección desordenada sin repetición* es muy simple. Cuando nos dan un conjunto X con n elementos y seleccionamos r de ellos, el resultado es un subconjunto Y de X con $|Y| = r$. Debe observarse

que en este modelo lo importante es el resultado de la selección (el conjunto Y), y no el proceso de selección. Además, no hay posibilidad de repetición, porque cada elemento de X está o no en Y, y ningún elemento puede seleccionarse dos veces.

Será conveniente referirnos a un conjunto X con n miembros como un **n-conjunto**, y un subconjunto Y de r elementos como un **r-subconjunto** de X. De este modo el número de selecciones desordenadas y sin repetición, de r elementos de un conjunto X de tamaño n es solo el número de r-subconjuntos del n-conjunto X. Por ejemplo, existen seis selecciones desordenadas, sin repetición, de dos elementos del conjunto $\{a, b, c, d\}$; que corresponden a los subconjuntos

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

Por lo general, el número de r-subconjuntos de un n-conjunto se denota con el símbolo

$$\binom{n}{r}.$$

Esto generalmente se lee como "n en r", y nos referiremos a él como un **número binomial**. Por ejemplo, acabamos de ver que existen seis 2-subconjuntos de un 4-subconjunto, y por lo tanto

$$\binom{4}{2} = 6.$$

Los siguientes ejercicios deben ser resueltos usando solo la definición de número binomial.

3.4.1. Ejercicios.

1. Probar que
$$\binom{n}{r} = 0 \qquad \text{si } r > n.$$
2. Encontrar los valores de
$$\binom{n}{0}, \ \binom{n}{1}, \ \binom{n}{n} \qquad \text{para todo } n \geq 1.$$
3. Probar que
$$\binom{n}{r} = \binom{n}{n-r} \qquad \text{para } 0 \leq r \leq n.$$

TEOREMA 3.4.1. *Si n y r son enteros positivos que satisfacen $1 \leq r \leq n$ entonces*

$$\binom{n}{r} = \binom{n-1}{r-1} + \binom{n-1}{r}.$$

DEMOSTRACIÓN. Sea X un n-conjunto, y supongamos que x es un elemento seleccionado de X. El conjunto de todos los r-subconjuntos de X puede ser separado en dos partes disjuntas U y V de la siguiente manera:

$$U = \text{ aquellos } r\text{-subconjuntos que contienen } x;$$

$$V = \text{ aquellos } r\text{-subconjuntos que no contienen } x.$$

Un r-subconjunto pertenece a U si (y solo si) cuando sacamos a x de él, obtenemos un $(r-1)$-subconjunto del $(n-1)$-conjunto $X - \{x\}$. Por lo tanto

$$|U| = \binom{n-1}{r-1}.$$

Por otro lado, un r-subconjunto está en V si (y solo si) es un r-subconjunto del $(n-1)$-conjunto $X - \{x\}$. Por lo tanto

$$|V| = \binom{n-1}{r}.$$

Se sigue por el principio de adición que el número total de r-subconjuntos es igual a $|U| + |V|$, y como este número es $\binom{n}{r}$ obtenemos el resultado. □

El Teorema 3.4.1 nos da un método recursivo para calcular los números binomiales puesto que si los numeros $\binom{n-1}{k}$ son conocidos para $0 \leq r \leq n$, entonces los números $\binom{n}{k}$ pueden ser calculados. Este cálculo a veces es representado en forma de triángulo, de esta manera:

						1								
					1		1							
				1		2		1						
			1		3		3		1					
		1		4		6		4		1				
	1		5		10		10		5		1			
1		6		15		20		15		6		1		
	7		21		35		35		21		7		1	

Esto es a veces llamado el triángulo de Pascal, debido a Blaise Pascal (1623-1662), aunque se lo conocía desde hacía ya mucho tiempo. Los números en la $(n+1)$-ésima fila son los números binomiales $\binom{n}{r}$ para $r = 0, 1, \ldots, n$. Los resultados del ejercicio 3.4.1 (2) implican que el borde está formado eternamente por unos, y el Teorema 3.4.1 nos dice que cada número es la suma de los números que están inmediatamente sobre él. Por lo tanto la tabla puede construirse fila por fila. Por ejemplo el cuarto número de la siguiente fila es

$$\binom{8}{3} = \binom{7}{2} + \binom{7}{3} = 21 + 35 = 56.$$

En algunas circunstancias es conveniente tener una fórmula explícita para los números binomiales

TEOREMA 3.4.2. *Si n y r son enteros positivos que satisfacen $1 \leq r \leq n$, entonces*

$$\binom{n}{r} = \frac{n(n-1)\cdots(n-r+1)}{r!} = \frac{n!}{r!(n-r)!}.$$

DEMOSTRACIÓN. Usemos el principio de inducción. Para $n = 1$ observemos que el resultado es verdadero cuando, puesto que $\binom{1}{1} = 1$ y la fórmula se reduce a $1/1! = 1$ también.

Para la hipótesis inductiva supongamos que el resultado es verdadero cuando $n = k$. Entonces por el Teorema 3.4.1 y por hipótesis inductiva,

$$\begin{aligned}\binom{k+1}{r} &= \binom{k}{r-1} + \binom{k}{r} \\ &= \frac{k(k-1)\cdots(k-r+2)}{(r-1)!} + \frac{k(k-1)\cdots(k-r+1)}{r!} \\ &= \frac{k(k-1)\cdots(k-r+2)}{(r-1)!}\left(1 + \frac{k-r+1}{r}\right) \\ &= \frac{k(k-1)\cdots(k-r+2)}{r!}.\end{aligned}$$

(Si $r = 1$ o $r = k+1$ tenemos que usar los valores $\binom{k}{0} = 1$ y $\binom{k}{k+1} = 0$, en vez de la fórmula). Se sigue que el resultado es verdadero cuando $n = k+1$, entonces, por el principio de inducción es verdadero para todos los enteros positivos n. □

Hay muchas interesantes y útiles identidades de los números binomiales y a pesar de que a veces pueden probarse usando la fórmula, generalmente es mejor basarse en la definición misma, o en la técnica recursiva del Teorema 3.4.1 Daremos ejemplos de ambos métodos.

EJEMPLO 3.4.1. Demuestre que

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

DEMOSTRACIÓN. La expresión del miembro izquierdo de la igualdad es la suma del número de r-subconjuntos de un n-conjunto, y de acuerdo al Ejemplo dado en las sección 3.4, el número es $2n$. □

EJEMPLO 3.4.2. Demuestre que

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

DEMOSTRACIÓN. En un ejercicio vimos que $\binom{n}{0} = 1$ y $\binom{n}{n} = 1$, considerando el Teorema **??**, el lado izquierdo de la ecuación de arriba es igual a

$$\begin{aligned}1 - \left\{\binom{n-1}{0} + \binom{n-1}{1}\right\} + \left\{\binom{n-1}{1} + \binom{n-1}{2}\right\} - \cdots \\ \cdots + (-1)^{n-1}\left\{\binom{n-1}{n-2} + \binom{n-1}{n-1}\right\} + (-1)^n.\end{aligned}$$

Cada término $\binom{n-1}{k}$ con k en el rango $1 \leq k \leq n-2$ ocurre con un signo positivo y un signo negativo, y por lo tanto estos términos se cancelan. Los términos restantes son

$$1 - \binom{n-1}{0} + (-1)^{n-1}\binom{n-1}{n-1} + (-1)^n = 1 - 1 + (-1)^{n-1} = (-1)^n,$$

lo cual es 0, como se requería. □

3.4.2. Ejercicios. (continuación)

1. Calcular las siguientes tres filas del triángulo de Pascal, respecto al ya hecho antes.
2. Evaluar $\binom{16}{4}$ y $\binom{17}{5}$.
3. Probar que el número de palabras de longitud n in el alfabeto $\{0,1\}$ que contienen exactamente r ceros, es $\binom{n}{r}$.
4. Probar la identidad

$$\binom{s-1}{0} + \binom{s}{1} + \cdots + \binom{s+n-2}{n-1} + \binom{s+n-1}{n} = \binom{s+n}{n},$$

donde s y n son enteros positivos. [Ayuda: si X es un $(s+n)$-conjunto e $Y = \{y_1, y_2, \ldots, y_n\}$ es un subconjunto específico de X, ¿cuál es el número de n-subconjuntos de X para los cuales y_r es el primer miembro de Y que no está en el subconjunto?]

5. Dar una prueba alternativa del ejercicio anterior, comenzando con la fórmula

$$\binom{s+n}{n} = \binom{s+n-1}{n} + \binom{s+n-1}{n-1},$$

y usando repetidamente el Teorema 3.4.1 para descomponer el último término.

3.5. Selecciones desordenadas con repetición

El número binomial $\binom{n}{r}$ se refiere al número de r-subconjuntos de un n-conjunto, o al número de selecciones sin repetición de r cosas de un conjunto de n cosas. Veamos ahora las selecciones desordenadas con repetición. Cuando los números en juego son chicos, es fácil listar todas las posibilidades. Por ejemplo existen 15 selecciones de cuatro cosas del conjunto $\{a, b, c\}$ con repetición permitidas, y son:

aaaa	*aaab*	*aaac*	*aabb*	*aacc*
aacc	*abbb*	*abbc*	*abcc*	*accc*
bbbb	*bbbc*	*bbcc*	*bccc*	*cccc*

Podemos demostrar que es posible dar una fórmula general para el número de selecciones con repetición, usando los números binomiales. La prueba de este hecho utiliza la representación de dichas selecciones como palabras en el alfabeto $\{0,1\}$; por ejemplo, la selección *abcc* será

representada por la palabra 101011. Los ceros son marcas que separan los tipos de objetos, y los unos nos dicen cuantos hay de cada objeto, de acuerdo al esquema tenemos

$$\begin{array}{cccccc} a & & b & & c & c \\ 1 & 0 & 1 & 0 & 1 & 1 \end{array}$$

Como hay dos marcas, que pueden ubicarse en cualquiera de las seis posiciones, el número total de selecciones en este caso es $\binom{6}{2} = 15$, como habíamos visto al listarlos. Debemos ahora probar la forma general de este resultado.

TEOREMA 3.5.1. *El número de selecciones con repetición de r objetos de un conjunto de n objetos es*

$$\binom{n+r-1}{r}.$$

DEMOSTRACIÓN. Como la selección es desordenada, podemos acomodar las cosas de manera que, dentro de cada selección, todos los objetos de un tipo dado estén primeros, seguidos por los objetos de otro tipo, y así sucesivamente. Cuando se ha hecho esto, podemos asignar a cada selección una palabra de longitud $n+(r-1)$ en el alfabeto $\{0,1\}$, con el método antes explicado. Esto es, si hay k_i objetos de el i-ésimo tipo ($1 \leq i \leq n$), entonces las primeras k_1 letras de la palabra son 1's seguidos por un único 0, seguido por k_2 1's, otro 0, y así sucesivamente. La función definida por esta regla es una biyección del conjunto de selecciones en el conjunto de palabras de longitud $n+r-1$ que contienen exactamente $n-1$ ceros. Los ceros pueden ocupar cualesquiera de las $n+r-1$ posiciones, o sea que el número de palabras es

$$\binom{n+r-1}{n-1} = \binom{n+r-1}{r},$$

que es lo que queríamos demostrar. □

En la Tabla 1 podemos resumir nuestros resultados acerca de los diferentes tipos de selección –ordenadas y desordenadas, con y sin repetición– de r elementos de un n-conjunto.

	Ordenadas	Desordenadas
Sin repetición	$n(n-1)\cdots(n-r+1)$	$\binom{n}{r}$
Con repetición	n^r	$\binom{n+r-1}{r}$

CUADRO 1

3.5.1. Ejercicios.

1. Escriba los valores de la tabla de arriba cuando $r = 2$ y $n = 3$, y en cada uno de los cuatro casos hacer una lista de las selecciones relevantes, tomando $\{a, b, c\}$ como el 3-conjunto.
2. Probar que cuando tres dados indistinguibles (entre si) son arrojados hay 56 posibles resultados ¿Cuál es el numero de resultados cuando son arrojados n dados indistinguibles?
3. Suponga que desarrollamos la expresión $(x + y + z)^n$ y que los términos son reunidos de acuerdo a las reglas elementales del álgebra: por ejemplo,

$$(x + y + z)^2 = x^2 + y^2 + z^2 + 2xy + 2xz + 2yz.$$

   ¿Cuál es el número de términos resultantes en la fórmula?
4. Probar que el número de n-uplas $(x_1, \ldots, x_n)$ de enteros no negativos que satisfacen la ecuación

$$x_1 + x_2 + \cdots + x_n = r$$

   es $\binom{n+r-1}{r}$. [Ayuda: suponga que una selección desordenada, con repetición, de r objetos de un conjunto de n objetos contiene x_i copias del objeto i $(1 \leq i \leq n)$.]

3.6. El teorema del binomio

En álgebra elemental aprendemos las formulas

$$(a + b)^2 = a^2 + 2ab + b^2, \qquad (a + b)^3 = a^3 + 3a^2b + 3ab^2 + b^3,$$

y a veces nos piden desarrollar la formula para $(a+b)^4$ y potencias mayores de $a+b$. El resultado general que da una formula para $(a + b)^n$ es conocido como el *teorema del binomio*.

TEOREMA 3.6.1. *Sea n un entero positivo. El coeficiente del termino $a^{n-r}b^r$ en el desarrollo de $(a + b)^n$ es el número binomial $\binom{n}{r}$. Explícitamente, tenemos*

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

DEMOSTRACIÓN. (Primera) Considerar que ocurre cuando multiplicamos n factores

$$(a + b)(a + b) \cdots (a + b).$$

Un término en el producto se obtiene seleccionando o bien a o bien b de cada factor. El número de términos $a^{n-r}b^r$ es solo el número de formas de seleccionar r b's (y consecuentemente $n - r$ a's), y por definición éste es el número binomial $\binom{n}{r}$. □

Demostración. (Segunda) Se hace por inducción en n. Si $n = 1$, el resultado es trivial. Supongamos que el resultado es cierto para $n-1$, es decir

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

Luego

$$\begin{aligned}
(a+b)^n &= (a+b)(a+b)^{n-1} \\
&= (a+b)\{\sum_{i=0}^{n-1} \binom{n-1}{i} a^{n-1-i} b^i\} && \text{por hip. inductiva} \\
&= \sum_{i=0}^{n-1} \binom{n-1}{i} a^{n-i} b^i + \sum_{i=0}^{n-1} \binom{n-1}{i} a^{n-1-i} b^{i+1} \\
&= \sum_{i=0}^{n-1} \binom{n-1}{i} a^{n-i} b^i + \sum_{i=1}^{n} \binom{n-1}{i-1} a^{n-i} b^i \\
&= a^n + \sum_{i=1}^{n-1} \{\binom{n-1}{i} + \binom{n-1}{i-1}\} a^{n-i} b^i + b^n \\
&= a^n + \sum_{i=1}^{n-1} \binom{n}{i} a^{n-i} b^i + b^n && \text{por Teorema 3.4.1} \\
&= \sum_{i=0}^{n} \binom{n}{i} a^{n-i} b^i.
\end{aligned}$$

□

Los coeficientes en el desarrollo pueden por lo tanto ser calculados con el método recursivo usado para los números binomiales (triángulo de Pascal) o usando la formula. Por ejemplo,

$$\begin{aligned}
(a+b)^6 &= \binom{6}{0} a^6 + \binom{6}{1} a^5 b + \binom{6}{2} a^4 b^2 + \binom{6}{3} a^3 b^3 \\
&\quad + \binom{6}{4} a^2 b^4 + \binom{6}{5} a b^5 \binom{6}{6} b^6 \\
&= a^6 + 6a^5 b + 15a^4 b^2 + 20a^3 b^3 + 15a^2 b^4 + 6ab^5 + b^6.
\end{aligned}$$

Por supuesto, podemos obtener otras formulas útiles si reemplazamos a y b por otras expresiones. Algunos ejemplos típicos son:

$$\begin{aligned}(1+x)^4 &= 1+4x+6x^2+4x^3+x^4;\\ (1-x)^7 &= 1-7x+21x^2-35x^3+35x^4-21x^5+7x^6-x^7;\\ (x+2y)^5 &= x^5+10x^4y+40x^3y^2+80x^2y^3+80xy^4+32y^5;\\ (x^2+y)^4 &= x^8+4x^3y+6x^4y^2+4x^2y^3+y^4.\end{aligned}$$

La expresión $a+b$ es conocida como un expresión *binómica* porque tiene dos términos. Como los números $\binom{n}{r}$ aparecen como los coeficientes en el desarrollo de $(a+b)^n$, generalmente se los llama *coeficientes binomiales*. De todos modos esta claro por la prueba del Teorema 3.6.1 que estos números aparecen en este contexto porque representan el número de formas de hacer ciertas selecciones. Por esta razón continuaremos usando el nombre de *números binomiales*, que se aproxima más al concepto que simbolizan.

Además de ser extremadamente útil en manipulaciones algebraicas, el teorema del binomio puede usarse para deducir identidades en que estén involucrados los números binomiales.

Ejemplo 3.6.1. Probar que

$$\binom{n}{0}^2+\binom{n}{1}^2+\binom{n}{3}^2+\cdots+\binom{n}{n}^2=\binom{2n}{n}.$$

Demostración. Usamos la igualdad

$$(1+x)^n(1+x)^n=(1+x)^{2n}.$$

De acuerdo con el teorema del binomio el miembro izquierdo es el producto de dos factores, ambos iguales a

$$1+\binom{n}{1}x+\cdots+\binom{n}{r}x^r+\cdots+x^n.$$

Cuando los dos factores se multiplican, un termino en x^n se obtiene tomando un termino del primer factor y un termino del segundo factor. Por lo tanto los coeficientes de x^n en el producto son

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

Como $\binom{n}{n-r}=\binom{n}{r}$, vemos que éste es el lado izquierdo de la igualdad requerida. Pero el lado derecho es $\binom{2n}{n}$ que es también el coeficiente de x^n en el desarrollo de $(1+x)^{2n}$, y entonces obtenemos la igualdad que buscábamos. □

3.6.1. Ejercicios.

1. Desarrollar las fórmulas de $(1+x)^8$ y $(1-x)^8$.
2. Calcular los coeficientes de
   (i) x^5 en $(1+x)^{11}$;
   (ii) a^2b^8 en $(a+b)^{10}$;
   (iii) a^6b^6 en $(a^2+b^3)^5$;
   (iv) x^3 en $(3+4x)^6$.
3. Usar la identidad $(1+x)^m(1+x)^n = (1+x)^{m+n}$ para probar que

$$\binom{m+n}{r} = \binom{m}{0}\binom{n}{r} + \binom{m}{1}\binom{n}{r-1} + \cdots \binom{m}{r}\binom{n}{0}$$

   donde m, n y r son enteros positivos y, $m \geq r$, y $n \geq r$.
4. Haciendo las sustituciones apropiadas en las fórmulas de $(1+x)^n$ y $(1-x)^n$ dar pruebas alternativas de los resultados establecidos en los Ejemplos 1 y 2 de la sección 3.4.
5. Probar que si r y s son enteros tal que $s|r$ y p es un primo tal que $p|r$ pero $p \not| s$, entonces $p|(r/s)$ [Ayuda: Escribir $r = st$.] Deducir que
   (i) El número binomial $\binom{p}{i}$ es divisible por p para todos los valores de i en el rango $1 \leq i \leq p-1$;
   (ii) $(a+b)^p - a^p - b^p$ es divisible por p para cualesquiera enteros a yb.

3.7. Ejercicios

1. Una ficha del juego de dominó puede ser representada con el símbolo $[x|y]$, donde x e y son miembros del conjunto $\{0,1,2,3,4,5,6\}$. Los números x e y pueden ser iguales. Explique por que el número total de fichas de dominó es 28 y no 49.
2. ¿De cuántas formas se pueden elegir un casillero negro y uno blanco en un tablero de ajedrez de tal forma que los dos casilleros no estén ni en la misma fila ni en la misma columna?
3. Supongamos que en clase hay m mujeres y n varones. ¿De cuántas formas puedo ordenar a todos los alumnos en una hilera de manera que todas las mujeres queden juntas?
4. Supongamos que tenemos un dominó generalizado en que las fichas toman su par de valores entre 0 y n. Sea k un entero en el rango $0 \leq k \leq n$. Probar que el número de fichas $[x|y]$ en que $x+y = n-k$ es igual al número de fichas en que $x+y = n+k$.
5. Denotemos u_n la cantidad de palabras de longitud n en el alfabeto $\{0,1\}$ que tienen la propiedad de no tener dos ceros consecutivos. Probar que

$$u_1 = 2, \qquad u_2 = 3, \qquad u_n = u_{n-1} + u_{n-2} \quad (n \geq 3).$$

6. Desarrollar $(x+y)^9$ y $(x-y)^9$.

7. Calcular el coeficiente de

   (i) x^6 en $(1+x)^{12}$,

   (ii) a^3b^7 en $(a+b)^{10}$,

   (iii) a^4b^6 en $(a^2+b)^8$.

8. Probar que
$$\binom{n}{r}\binom{r}{k} = \binom{n}{k}\binom{n-k}{r-k}.$$

9. Se dibujan todas las posibles diagonales que conectan a un conjunto de n puntos en el círculo y se observa que no hay tres rectas que se cruzan en un mismo punto ¿Cuántos puntos internos de intersección hay?

10. Probar que el número de formas de distribuir n bolas idénticas en m cajas con etiquetas, algunas de las cuales puede quedar vacía es
$$\binom{n+m-1}{n}.$$

11. Probar que si $n \geq m$, entonces
$$\binom{m}{m} + \binom{m+1}{m} + \cdots + \binom{n}{m} = \binom{n+1}{m+1}.$$

12. Sea X un n-conjunto. Probar que

    (i) existe un conjunto de $\binom{n-1}{k-1}$ k-subconjuntos de X tales que cada par de ellos tiene intersección no vacía.

    (ii) existe un conjunto de $\binom{n}{n^*}$ subconjuntos de X con la propiedad que ninguno contiene a otro. Aquí n^* es igual a $n/2$ si n es par y a $\frac{1}{2}(n-1)$ si n es impar.

CAPíTULO 4

Aritmética Modular

4.1. Congruencias

Una de las más familiares particiones de un conjunto es la partición de $\mathbb{Z}$ en enteros pares y enteros impares. Es decir $\mathbb{Z}$ es la unión disjunta del conjunto de números pares y el de los números impares. Es claro que dos números x_1, x_2 tienen la misma paridad si $x_1 - x_2$ es divisible por 2. Para expresar este hecho es usual la notación

$$x_1 \equiv x_2 \pmod 2$$

y se dice que x_1 es *congruente* a x_2 *módulo* 2. Es decir x_1 y x_2 son ambos pares o ambos impares si y solo si x_1 es congruente a x_2 módulo 2.

Claramente esta definición se puede extender a cualquier entero positivo m.

Definición 4.1.1. Sean x_1 y x_2 enteros y m un entero positivo. Diremos que x_1 es **congruente** a x_2 **módulo** m, y escribimos

$$x_1 \equiv x_2 \pmod m$$

si $x_1 - x_2$ es divisible or m.

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

(1) Es *reflexiva* es decir $x \equiv x \pmod m$.
(2) Es *simétrica*, es decir si $x \equiv y \pmod m$, entonces $y \equiv x \pmod m$.
(3) Es *transitiva*, es decir si $x \equiv y \pmod m$ e $y \equiv z \pmod m$, entonces $x \equiv z \pmod m$.

La primera propiedad es debido a que $x - x$ es cero y por lo tanto divisible por m. La segunda se debe a que si $x - y = km$, entonces $y - x = (-k)m$. Finalmente, podemos demostrar la tercera de la siguiente forma, puesto que $x - y = km$ y $y - z = lm$, tenemos que $x - z = (x - y) + (y - z) = (k + l)m$.

La utilidad de las congruencias reside principalmente en el hecho de que son compatibles con las operaciones aritméticas. Específicamente, tenemos el siguiente Teorema.

Teorema 4.1.1. *Sea m un entero positivo y x_1, x_2, y_1, y_2 enteros tales que*

$$x_1 \equiv x_2 \pmod m, \qquad y_1 \equiv y_2 \pmod m.$$

Entonces

$$\textit{(i)}\ x_1 + y_1 \equiv x_2 + y_2 \pmod{m}, \qquad \textit{(ii)}\ x_1 y_1 \equiv x_2 y_2 \pmod{m}.$$

DEMOSTRACIÓN. (i) Por hipótesis tenemos que existen enteros x, y tales que $x_1 - x_2 = mx$ e $y_1 - y_2 = my$. Se sigue que

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

y por consiguiente el lado izquierdo es divisible por m, como queríamos demostrar.

(ii) Aquí tenemos

$$\begin{aligned}x_1 y_1 - x_2 y_2 &= (x_1 - x_2) y_1 + x_2 (y_1 - y_2)\\ &= mxy_1 + x_2 my\\ &= m(xy_1 + x_2 y),\end{aligned}$$

y de nuevo el lado izquierdo es divisible por m. □

EJEMPLO 4.1.1. Sea $(x_n x_{n-1} \dots x_0)_{10}$ la representación del entero positivo x en base 10. Probar que

$$x \equiv x_0 + x_1 + \cdots + x_n \pmod{9}$$

y use este resultado para verificar el siguiente cálculo

$$54\,321 \times 98\,765 = 5\,363\,013\,565.$$

DEMOSTRACIÓN. Observemos primero que $10^k \equiv 1 \pmod{9}$. Hagamos esto por inducción. Si $k = 0$ el resultado es obvio. Supongamos que $10^{k-1} \equiv 1 \pmod{9}$, como $10 \equiv 1 \pmod{9}$, por (ii) del Teorema 4.1.1, obtenemos $10^{k-1} \times 10 \equiv 1 \times 1 \pmod{9}$.

Por la definición de representación en base 10, tenemos que $x = x_0 + 10x_1 + \cdots + 10^n x_n$, por el párrafo anterior y Teorema 4.1.1 obtenemos que $x_k 10^k \equiv x_k \pmod{9}$ y por Teorema 4.1.1 de nuevo se deduce que $x \equiv x_0 + x_1 + \cdots + x_n \pmod{9}$.

Escribamos $\theta(x)$ en vez de $x_0 + x_1 + \cdots + x_n$. Hemos visto que $\theta(x) \equiv x \pmod{9}$. Por la parte (ii) del Teorema 4.1.1 tenemos

$$\theta(x)\theta(y) \equiv xy \pmod{9},$$

y por consiguiente si $xy = z$ debemos tener $\theta(x)\theta(y) \equiv \theta(z) \pmod{9}$. En el cálculo que se tiene en el ejemplo

$$\theta(54\,321) = 15, \quad \theta(98\,765) = 35, \quad \theta(5\,363\,013\,565) = 37,$$

y

$$\theta(15) = 6, \quad \theta(35) = 8, \quad \theta(37) = 10.$$

Puesto que 6×8 no es congruente a 10 (mód 9) se sigue que 15×35 no es congruente a 37 (mód 9) y que $54\,321 \times 98\,765$ no es congruente a $5\,363\,013\,565$ (mód 9). En consecuencia el cálculo está errado.

Este procedimiento a veces es llamado "regla del nueve". □

Otra propiedad importante es que $a \equiv b \pmod{m}$ si y solo si a y b tienen el mismo resto en la división por m: si $a = mh + r_a$ y $b = mk + r_b$, con $0 \leq r_a, r_b < m$, podemos suponer, sin perdida de generalidad, que $r_a \leq r_b$, entonces

$$b - a = m(k - h) + (r_b - r_a) \quad \text{con } 0 \leq r_b - r_a < m.$$

Se sigue que $r_b - r_a$ es el resto de dividir $b - a$ por m. Luego $a \equiv b \pmod{m}$ si y solo si $a - b \equiv 0 \pmod{m}$ si y solo si $m|b - a$ si y solo si $r_b = r_a$.

Así como antes podíamos separar $\mathbb{Z}$ en los números pares e impares, la propiedad anterior nos permite expresar $\mathbb{Z}$ como una unión disjunta de m subconjuntos. Es decir si $Z_i = \{x \in \mathbb{Z} : \text{el resto de dividir } x \text{ por } m \text{ es } i\}$, entonces

$$\mathbb{Z} = Z_0 \cup Z_1 \cup \cdots \cup \mathbb{Z}_{m-1}.$$

4.1.1. Ejercicios.

1. Sin hacer ninguna "multiplicación larga" probar que

   (i) $1\,234\,567 \times 90\,123 \equiv 1 \pmod{10}$

   (ii) $2468 \times 13\,579 \equiv -3 \pmod{25}$

2. Usar la regla del nueve para verificar que dos de las siguientes ecuaciones son falsas. ¿Qué se puede decir de la otra ecuación?

   (i) $5783 \times 40\,162 = 233\,256\,846$,

   (ii) $9787 \times 1258 = 12\,342\,046$,

   (iii) $8901 \times 5743 = 52\,018\,443$.

3. Encontrar el resto de dividir 3^{15} por 17 y el de dividir 15^{81} por 13.
4. Sea $(x_n x_{n-1} \ldots x_0)_{10}$ la representación en base 10 de un entero positivo x. Probar que

   $$x \equiv x_0 - x_1 + x_2 + \cdots + (-1)^n x_n \pmod{11},$$

   y use este resultado para verificar si $1\,213\,141\,516\,171\,819$ es divisible por 11.

4.2. Ecuación lineal de congruencia

Se trata primero de estudiar en general el problema de resolución de la ecuación en x

$$ax \equiv b \pmod{m}. \tag{1}$$

Es fácil ver que el problema no admite siempre solución, por ejemplo $2x \equiv 3 \pmod 2$ no posee ninguna solución en $\mathbb{Z}$, pues cualquiera se $k \in \mathbb{Z}$, $2k-3$ es impar, luego no es divisible por 2.

Notemos además que si x_0 es solución de la ecuación (1), 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 $0 \leq x < m$.

Ejemplo 4.2.1. La solución general de la ecuación $3x \equiv 7 \pmod{11}$ es $6 + km$ con $k \in \mathbb{Z}$.

Demostración. Claramente la ecuación admite una única solución x, con $0 \leq x < 11$, a saber $x = 6$. Otras soluciones se obtienen tomando $6 + 11k$. Por otra parte si u es también solución de la ecuación, se tiene $3u \equiv 3 \times 6 \pmod{11}$, por lo tanto $3(u-6)$ es múltiplo de 11. Como 11 no divide a 3 se tiene que $11|(u-6)$, o sea $u = 6 + 11k$. □

Analicemos ahora la situación general de la ecuación $ax \equiv b \pmod m$. Si $\mathrm{mcd}(a, m) = 1$, entonces sabemos que existen enteros r y s tales que $1 = ra + sm$ y por lo tanto $b = (rb)a + (sb)m$, o sea que

$$a(rb) \equiv b \pmod{m},$$

es decir rb es solución de la ecuación.

Si $\mathrm{mcd}(a, m)|b$, entonces la ecuación

$$\frac{a}{\mathrm{mcd}(a,b)}x \equiv \frac{m}{\mathrm{mcd}(a,b)} \pmod{\frac{m}{\mathrm{mcd}(a,b)}}$$

admite solución pues

$$\mathrm{mcd}\left(\frac{a}{\mathrm{mcd}(a,b)}, \frac{b}{\mathrm{mcd}(a,b)}\right) = 1$$

y entonces admite solución la ecuación general.

Por otro lado si $ax \equiv b \pmod m$, entonces $ax - b = km$ para algún m, o sea

$$b = ax + (-k)m$$

de la cual se sigue que si $d|a$ y $d|m$, entonces $d|b$ y por lo tanto $\mathrm{mcd}(a, m)|b$.

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

Ejemplo 4.2.2. Hallar las soluciones de la ecuación $42x \equiv 50 \pmod{76}$ con $0 \leq x < 76$.

DEMOSTRACIÓN. Tenemos que $\mathrm{mcd}(76, 42) = 2$ y $2|50$ y por lo tanto la ecuación tiene solución. Utilizando la idea anterior de dividir por $\mathrm{mcd}(a, m)$ consideramos la ecuación $21x \equiv 25$ (mód 38), la cual sí tiene solución, pues $\mathrm{mcd}(38, 21) = 1$. Ahora bien, si multiplicamos $21x$ y 25 por 2, obtenemos la ecuación $42x \equiv 50 \pmod{38}$ que si tiene una solución coprima con 38, es solución de la ecuación original. Como $42 \equiv 4 \pmod{38}$ y $50 \equiv 12 \pmod{38}$, hallemos una solución de $4x \equiv 12 \pmod{38}$. Claramente 3 es solución a esta ecuación y también a la ecuación original. Más aún podemos observar que 3 y $3 + 38 = 41$ son las únicas soluciones comprendidas entre 0 y 76. □

4.2.1. Ejercicios.

1. Si x_0 es solución de la ecuación $ax \equiv b \pmod{m}$, entonces las soluciones no congruentes entre si módulo m son
$$x_0, x_0 + \frac{m}{\mathrm{mcd}(a,b)}, x_0 + 2\frac{m}{\mathrm{mcd}(a,b)}, \ldots, x_0 + (\mathrm{mcd}(a,b) - 1)\frac{m}{\mathrm{mcd}(a,b)}.$$
2. Resolver las siguientes ecuaciones lineales de congruencia
$$\text{(i)} \quad 2x \equiv 1 \pmod{7} \qquad \text{(ii)} \quad 3970x \equiv 560 \pmod{2755}.$$

4.3. Teorema de Fermat

El siguiente Lema nos sirve de preparación para la demostración del Teorema (o fórmula) de Fermat.

LEMA 4.3.1. *Sea p un número primo, entonces*

(i) $p|\binom{p}{r}$, *con* $0 < r < p$,
(ii) $(a + b)^p \equiv a^p + b^p \pmod{p}$.

DEMOSTRACIÓN. (i) Como r y $p - r$ son menores que p y p es primo, tenemos que el factor p no aparece en la descomposición prima de $r!$ y $(p - r)!$. Como $\binom{p}{r} = \frac{p!}{r!(p-r)!} = p\frac{(p-1)!}{r!(p-r)!}$ es un número entero, tenemos entonces que $\frac{(p-1)!}{r!(p-r)!}$ es entero y $p|\binom{p}{r}$.

(ii) Por el Teorema del binomio (Teorema 4.3) sabemos que
$$(a + b)^p = \sum_{i=0}^{p} \binom{p}{i} a^i b^{p-i}.$$
Por (i) es claro que $\binom{p}{i} a^i b^{p-i} \equiv 0 \pmod{p}$, si $0 < i < p$. Luego se deduce el resultado. □

El siguiente es el llamado Teorema de Fermat.

TEOREMA 4.3.2. *Sea p un número primo y a número entero. Entonces*
$$a^p \equiv a \pmod{p}.$$

DEMOSTRACIÓN. Supongamos que $a \geq 0$, entonces hagamos inducción en a. Si $a = 0$, el resultado es trivial. Supongamos el resultado probado para k, es decir $k^p \equiv a \pmod{p}$. Entonces $(k+1)^p \equiv k^p + 1^p \equiv k + 1 \pmod{p}$. La primera congruencia es debido al Lema 4.3.1 (ii) y la segunda es válida por hipótesis inductiva.

Si $a < 0$, entonces $-a > 0$ y ya vimos que $(-a)^p \equiv -a \pmod{p}$, es decir que $(-1)^p a^p \equiv (-1)a \pmod{p}$. Si $p \neq 2$, entonces $(-1)^p = -1$ y se deduce el resultado. Si $p = 2$, entonces $(-1)^p = 1$, pero como $1 \equiv -1 \pmod{2}$, obtenemos también $a^p \equiv a \pmod{p}$. □

Supongamos que a y p son coprimos, por Fermat $p|(a^p - a) = a(a^{(p-1)} - 1)$. Como p no divide a a, tenemos que $p|(a^{(p-1)} - 1)$, es decir *si a y p coprimos entonces* $a^{(p-1)} \equiv 1 \pmod{p}$. Este último enunciado es también conocido como Teorema de Fermat.

La función de Euler $\phi(n)$, para $n \geq 1$, está definida como el cardinal del conjunto de los x entre 1 y n que son coprimos con n (ver Apéndice II). El Teorema de Fermat admite la siguiente generalización, llamada Teorema de Euler: si n un entero positivo y a un número entero coprimo con n, entonces

$$a^{\phi(n)} \equiv 1 \pmod{n}$$

(ver ejercicio (4)).

4.3.1. Ejercicios.

1. Usar el Teorema de Fermat para calcular el resto de dividir 3^{47} por 23.
2. Si m coprimo con n, entonces $ma \equiv mb \pmod{n}$ si y solo si $a \equiv b \pmod{m}$.
3. Sean $x_1, \ldots, x_k$ los números coprimos con n comprendidos entre 1 y n (es decir $k = \phi(n)$) y sea y coprimo con n. Entonces hay un reordenamiento de $yx_1, \ldots, yx_k$, es decir una permutación σ de $1, \ldots, k$, tal que $x_i \equiv yx_{\sigma_i} \pmod{n}$, para $1 \leq i \leq k$. [Ayuda: como y coprimo con n, existe v tal que $yv \equiv 1 \pmod{n}$].
4. Demostrar el Teorema de Euler. [Ayuda: Sean $x_1, \ldots, x_k$ los números coprimos con n comprendidos entre 1 y n, por el ejercicio anterior $y^{\phi(n)} x_1 \ldots x_k = yx_1 \ldots yx_k \equiv x_1 \ldots x_k \pmod{n}$. Como $u = x_1 \ldots x_k$ coprimo con n, existe v tal que $uv \equiv 1 \pmod{n}$].

4.4. El criptosistema RSA

Una de las aplicaciones más elementales y difundidas de la aritmética es en el diseño de sistemas criptográficos. El RSA es el más conocido de ellos y será presentado en esta sección.

Por criptosistema nos referimos a sistemas de encriptamiento o codificación esencialmente pensados para proteger la confidencialidad de datos que se desean transmitir. Entre los criptosistemas encontramos los de clave privada y los de clave pública. Los de clave privada son aquellos en que tanto el emisor como el receptor conocen una función, digamos f y una palabra , digamos x, tanto la función como la palabra deben ser confidenciales o más comúnmente solo la palabra debe ser confidencial. Cuando el emisor desea enviar un mensaje M, entonces aplica la función a M y x, es decir $M' = f(M, x)$, envía M' y el receptor aplica la función inversa y recupera M,

es decir $M = f^{-1}(M', x)$. En los sistemas de clave pública el receptor conoce una clave privada y (no compartida por nadie) y publicita una clave pública x, de la misma manera que antes si alguien desea enviar un mensaje M al receptor debe hacer $M' = f(M, x)$, pero el receptor para decodificar debe hacer $M = g(M', y)$, donde g es una función adecuada. Una ventaja evidente de los sistemas de clave pública es que no es necesario poner en conocimiento del emisor ninguna clave confidencial, más aún cualquier persona puede enviar en forma confidencial datos a otra persona que ha publicitado su clave.

Rivest, Shamir y Adleman descubrieron el primer criptosistema práctico de clave pública, que es llamado RSA. La seguridad del RSA se basa en la dificultad de factorizar números enteros grandes. Este sistema es el más comúnmente recomendado para uso en sistemas de clave pública. La mayor ventaja del RSA es que no incrementa el tamaño del mensaje y que puede ser usado para proveer privacidad y autenticación (firma digital) en las comunicaciones. Su principal desventaja es que su implementación se basa en exponenciación de números enteros grandes, una operación que consume recursos de la computadora, aunque esto es cada vez menos significante.

Antes de describir el RSA digamos que se basa fuertemente en el Teorema de Euler visto en la sección anterior. En el caso del RSA se aplica al producto de dos primos, es decir si tenemos p y q números primos, es fácil calcular $\phi(pq) = (p-1)(q-1)$ y entonces

$$a^{(p-1)(q-1)} \equiv 1 \pmod{pq}$$

si a y pq son coprimos.

En el sistema RSA cada usuario que desee recibir mensajes encriptados hace los siguientes pasos:

1. selecciona dos primos p y q al azar y de alrededor de 100 dígitos cada uno (longitud considerada segura en este momento),
2. calcula el producto pq
3. selecciona un número al azar e con $e < pq$ y $\text{mcd}(e, \phi(pq)) = 1$. El número e es usualmente pequeño, por ejemplo podría ser 3.
4. encuentra el único d que satisface la ecuación

$$de \equiv 1 \pmod{\phi(pq)}$$

   con $0 \leq d < \phi(pq)$. La existencia de este d es clara pues al ser e y $\phi(pq)$ coprimos existen d y s tales que $de - s\phi(pq) = 1$. Más aún, como d es positivo, claramente también lo es s.
5. Publicita la clave pública (e, R) donde $R = pq$.
6. Obviamente no da a conocer ni p, ni q y mantiene segura la clave privada d.

Un emisor desea encriptar un mensaje M expresado en un entero grande pero con menos de los dígitos que tiene p o q, en este caso menos de 100 dígitos. Para ello crea el mensaje C usando

la clave pública (e, R) y calculando

$$C \equiv M^e \pmod{R}, \qquad \text{con } 0 \leq C < R.$$

El receptor descifra el mensaje usando la clave privada d y calculando:

$$M \equiv C^d \pmod{R}.$$

Esta fórmula se deduce de las siguientes congruencias módulo pq:

$$\begin{aligned} C^d \equiv M^{ed} &\equiv M^{1+s\phi(pq)} && \text{(por (4))} \\ &\equiv M^1 M^{s\phi(pq)} && \text{(Teorema de Euler)} \\ &\equiv M^1 \equiv M \pmod{pq}. \end{aligned}$$

El RSA también puede ser usado para un sistema de autenticación puesto que el encriptado y el decriptado son operaciones conmutativas. Esto es, para que el receptor sepa sin duda alguna quien le envía el mensaje el emisor encripta su filiación con su clave privada d, calculando $S \equiv F^d \pmod{pq}$ (F es la filiación). Luego la filiación puede ser verificada por cualquiera usando la clave pública (e, pq) del emisor, calculando $F \equiv S^e \pmod{pq}$

4.5. Ejercicios

1. Determine todas las posibles soluciones de las congruencias

$$\text{(i)} \quad 5x \equiv 1 \pmod{11}, \qquad \text{(ii)} \quad 5x \equiv 7 \pmod{15}.$$

2. Sin hacer demasiadas cuentas verifique que 192 837 465 564 738 291 es divisible por 11.
3. Resolver la ecuaciones

$$\text{(i)} \quad 5x \equiv 12 \pmod{13}, \qquad \text{(ii)} \quad x^2 - x \equiv 1 \pmod{11}.$$

4. ¿Cuál es el último dígito de la representación en base 10 de 7^{93}.
5. Usar que $1001 = 7 \times 11 \times 13$ para construir una prueba para la división para los número 7, 11 y 13 similar a la prueba del 9.

CAPíTULO 5

Grafos

5.1. Grafos y sus Representaciones

Los objetos a los cuales llamaremos *grafos* son muy útiles en Matemática Discreta. Su nombre se deriva del hecho de que pueden ser entendidos con una notación gráfica (o pictórica), y en este aspecto solamente se parecen a los familiares gráficos de funciones que son estudiados en matemática elemental. Pero nuestros grafos son bastante diferentes de los gráficos de funciones y están más relacionados con objetos que en le lenguaje diario llamamos "redes" (networks).

DEFINICIÓN 5.1.1. 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**. Nosotros usualmente escribiremos $G = (V, E)$ y diremos que V es el **conjunto de vértices** y E es el **conjunto de aristas**.

La restricción a un conjunto finito no es esencial, pero es conveniente para nosotros debido a que no consideraremos "grafos" infinitos en este libro.

Un ejemplo típico de un grafo $G = (V, E)$ es dado por los conjuntos

$$V = \{a, b, c, d, z\}, \qquad E = \{\{a, b\}, \{a, d\}, \{b, z\}, \{c, d\}, \{d, z\}\}.$$

Este ejemplo y la definición misma no son demasiado esclarecedores, y solamente cuando consideramos la *representación pictórica* de un grafo es cuando se hace la luz.

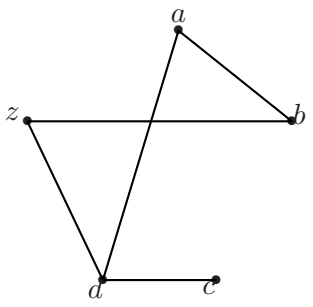


FIGURA 1. Una representación pictórica de un grafo.

Nosotros representamos los vértices como puntos, y unimos dos puntos con una linea siempre y cuando el correspondiente par de vértices está en una arista. Luego la Fig. 1 es una

representación pictórica del grafo dado en el ejemplo arriba. Esta clase de representación es extremadamente conveniente para trabajar "a mano" con grafos relativamente pequeños. Más aún, esta representación es de gran ayuda para formular y comprender argumentos abstractos. Nosotros damos a continuación un ejemplo frívolo.

Ejemplo 5.1.1. El profesor Mc Brain y su mujer Abril dan una fiesta en la cual hay otras cuatro parejas de casados. Las parejas, cuando arriban, estrechan la mano a algunas personas, pero, naturalmente, no se estrechan la mano entre marido y mujer. Cuando la fiesta finaliza el profesor pregunta a los otros a cuantas personas han estrechado la mano, recibiendo 9 respuestas diferentes. ¿Cuántas personas estrecharon la mano de Abril?

Demostración. Construyamos un grafo cuyos vértices son la gente de la fiesta, y hay una arista $\{x, y\}$ siempre y cuando x e y se hayan estrechado las manos. Puesto que hay nueve persona aparte del profesor Mc Brain, y que una persona puede estrechar a lo sumo a otras 8 personas, se sigue que las 9 respuestas diferentes que ha recibido el profesor deben ser 0, 1, 2, 3, 4, 5, 6, 7, 8. Denotemos los vértices con estos números y usemos M para Mc Brain. Así obtenemos la representación pictórica de la Fig. 2

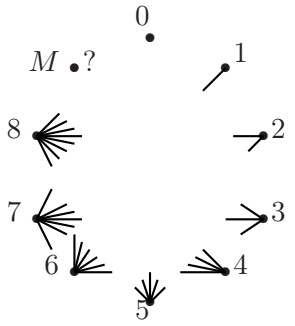


Figura 2. La fiesta de Abril

Ahora, el vértice 8 alcanza a todos los otros vértices excepto uno, el cual debe por lo tanto representar a la esposa de 8. Este vértice debe ser el 0 el cual por cierto que no está unido al 8 (ni obviamente a ningún otro). Luego 8 y 0 son una pareja de casados y 8 está unido a 1, 2, 3, 4, 5, 6, 7 y M. En particular el 1 está unido al 8 y ésta es la única arista que parte del 1. Por consiguiente 7 no esta unido al 0 y al 1 (únicamente), y la esposa de 7 debe ser 1, puesto que 0 esta casado con 8. Continuando con este razonamiento vemos que 6 y 2, y 5 y 3 son parejas de casados. Se sigue entonces que M y 4 están casados, luego el vértice 4 representa a Abril, quien estrechó la mano de cuatro personas. □

Aunque la representación pictórica es intuitivamente atractiva para los seres humanos, es claramente inútil cuando deseamos comunicarnos con una computadora. Para lograr esto debemos representar el grafo mediante cierta clase de lista o tabla. Diremos que dos vértices x e y de un

grafo son **adyacentes** cuando $\{x, y\}$ es una arista. (También diremos que x e y son **vecinos**.) Entonces podemos representar un grafo $G = (V, E)$ por su **lista de adyacencia**, donde cada vértice v encabeza una lista de aquellos vértices que son adyacentes a v. El grafo de Fig. 1 tiene la siguiente lista de adyacencia:

a	b	c	d	z
b	a	d	a	b
d	z		c	d
			z	

5.1.1. Ejercicios.

1. A tres casas A, B, C se les debe conectar el gas, el agua y la electricidad: G, W, E. Escribir la lista de adyacencia para el grafo que representa este problema y construir una representación pictórica del mismo. ¿Puede usted encontrar un dibujo en el cual las líneas que representan las aristas no se crucen?
2. Los senderos de un jardín han sido diseñados dándoles forma de **grafo rueda** W_n, cuyos vértices son $V = \{0, 1, 2, \ldots, n\}$ y sus aristas son

   $$\{0,1\}, \quad \{0,2\}, \ldots, \{0,n\},$$
   $$\{1,2\}. \quad \{2,3\}, \ldots, \{n-1,n\}, \quad \{n,1\}.$$

   Describa una ruta por los senderos de tal forma que empiece y termine en le vértice 0 y que pase por cada vértice una sola vez.
3. 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. ¿Cuántas aristas tiene K_n? ¿Para cuales valores de n podemos hacer una representación pictórica de K_n con la propiedad que las líneas que representan las aristas no se corten?
4. Un *3-ciclo* en un grafo es un conjunto de tres vértices mutuamente adyacentes. Construir un grafo con cinco vértices y seis aristas que no contenga 3-ciclos.

5.2. Isomorfismo de grafos

En este punto nosotros debemos enfatizar que un grafo esta definido como una entidad matemática abstracta. Es en este contexto que nosotros discutiremos el importante problema de que idea queremos expresar cuando decimos que dos grafos son "el mismo".

Claramente lo importante de un grafo no son los nombres con que designamos a los vértices, ni su representación pictórica o cualquier otra representación. La propiedad característica de un grafo es la manera en que los vértices están conectados por aristas. Esto motiva la siguiente definición.

DEFINICIÓN 5.2.1. Dos grafos G_1 y G_2 se dicen 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 $\{\alpha(x), \alpha(y)\}$ es una arista de G_2 si y solo si $\{x, y\}$ es una arista de G_1. La biyección α es llamada un **isomorfismo**.

Por ejemplo, considere los dos grafos de la Fig. 3. En este caso hay una biyección entre el conjunto de vértices de G_1 y el conjunto de vértices de G_2 la cual tiene la propiedad requerida; esta biyección es dada por

$$\alpha(a) = t, \quad \alpha(b) = v, \quad \alpha(c) = w, \quad \alpha(d) = u.$$

Podemos comprobar que a cada arista de G_1 le corresponde una arista de G_2 y viceversa. Por ejemplo, a la arista bc de G_1 le corresponde la arista vw de G_2, y así siguiendo. (Usaremos la abreviación xy para la arista $\{x, y\}$, recordando que una arista es un par desordenado, es decir xy es lo mismo que yx.)

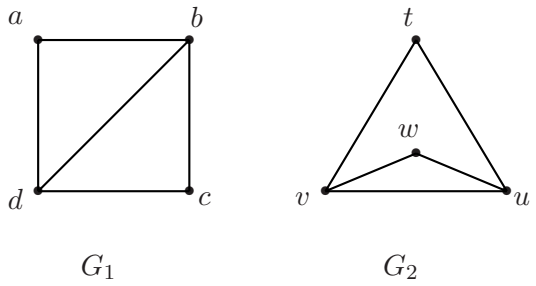


FIGURA 3. G_1 y G_2 son isomorfos

Cuando, como en la Fig. 3, dos grafos G_1 y G_2 son isomorfos usualmente nos referiremos a ellos como que son "el mismo" grafo.

Para mostrar que dos grafos no son isomorfos, nosotros debemos demostrar que no hay una biyección entre el conjunto de vértices de uno con el conjunto de vértices de otro, que lleve las aristas de uno en las aristas del otro.

Si dos grafos tienen diferente número de vértices, entonces no es posible ninguna biyección, y los grafos no pueden ser isomorfos. Si los grafos tienen el mismo número de vértices, pero diferente número de aristas, entonces hay biyecciones pero ninguna de ellas puede ser un isomorfismo. Aún si los grafos tienen el mismo número de vértices y aristas, no necesariamente son isomorfos. Por ejemplo, los dos grafos de la Fig. 4 tienen cinco vértices y siete aristas pero no son isomorfos. Una manera de ver esto es observar que los vértices a, b, d, e forman un subgrafo completo de G_1 (cada par de ellos está conectado por una arista). Cualquier isomorfismo debe llevar estos

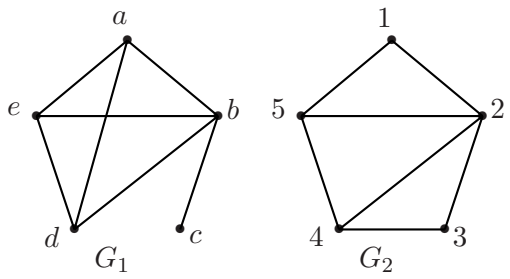


FIGURA 4. G_1 y G_2 no son isomorfos

vértices en cuatro vértices de G_2 con la misma propiedad, y puesto que no hay tal conjunto de vértices en G_2 no puede haber ningún isomorfismo.

5.2.1. Ejercicios.

1. Probar que los grafos mostrados en la Fig. 5 no son isomorfos.

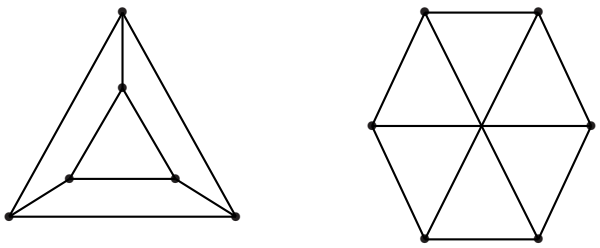


FIGURA 5. Probar que estos grafos no son isomorfos

2. Encontrar un isomorfismo entre los grafos definidos por las siguientes listas de adyacencias. (Ambas listas especifican versiones de un grafo famoso conocido como **grafo de Petersen**).

a	b	c	d	e	f	g	h	i	j
b	a	b	c	d	a	b	c	d	e
e	c	d	e	a	h	i	j	f	g
f	g	h	i	j	i	j	f	g	h

0	1	2	3	4	5	6	7	8	9
1	2	3	4	5	0	1	0	2	6
5	0	1	2	3	4	4	3	5	7
7	6	8	7	6	8	9	9	9	8

3. Sea $G = (V, E)$ el grafo definido como sigue. El conjunto de vértices V es el conjunto de todas las palabras de longitud tres en el alfabeto $\{0, 1\}$, y el conjunto de aristas E contiene aquellos pares de palabras que difieren exactamente en una posición. Probar que G es isomorfo al grafo formado por las esquinas y aristas de un cubo.

5.3. Valencias

La **valencia** de un vértice v en un grafo $G = (V, E)$ es el número de aristas de G que contienen a v. Usaremos la notación $\delta(v)$ para la valencia de v, formalmente

$$\delta(v) = |D_v|, \quad \text{donde} \quad D_v = \{e \in E | v \in e\}.$$

El grafo descrito en Fig. 1 tiene $\delta(a) = 2$, $\delta(b) = 2$, $\delta(c) = 1$, $\delta(d) = 3$, $\delta(z) = 2$. El primer teorema de la teoría de grafos nos dice que la suma de estos números es dos veces el número de aristas.

TEOREMA 5.3.1. *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:*

$$\sum_{v \in V} \delta(v) = 2|E|.$$

DEMOSTRACIÓN. La valencia de un vértice v indica la cantidad de "extremos" de aristas que "tocan" a v. Es claro que hay $2|E|$ extremos de aristas, luego la suma total de las valencias de los vértices es $2|E|$. □

Hay un útil corolario de este resultado. Diremos que un vértice de G es **impar** si su valencia es impar, y **par** si su valencia es par. Denotemos V_i y V_p los conjuntos de vértices impares y pares respectivamente, luego $V = V_i \cup V_p$ es una partición de V. Por Teorema 5.3.1, tenemos que

$$\sum_{v \in V_i} \delta(v) + \sum_{v \in V_p} \delta(v) = 2|E|.$$

Ahora cada término en la segunda suma es par, luego esta suma es un número par. Puesto que el lado derecho también es un número par, la primera suma debe ser también par. Pero la suma de números impares solo puede ser par si el número de términos es par. En otra palabras:

el número de vértices impares es par.

Este resultado es a veces llamado el "handshaking lemma" (handshake=estrechar la mano, darse la mano), debido a que se puede interpretar en términos de gente y darse la mano: dado un conjunto de personas, el número 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.** En este caso, el resultado del Teorema 5.3.1 se traduce

$$r|V| = 2|E|.$$

Muchos de los grafos que aparecen en las aplicaciones son regulares. Ya conocemos los grafos completos K_n; ellos son regulares, con valencia $n - 1$. De geometría elemental conocemos los polígonos de n lados, los cuales en teoría de grafos son llamados **grafos cíclicos** C_n. Formalmente,

podemos decir que el conjunto de vértices de C_n es $\mathbb{Z}_n$, y los vértices i y j están unidos si $j = i+1$ o $j = i-1$ en $\mathbb{Z}_n$. Claramente, C_n es un grafo regular con valencia 2, si $n \geq 3$.

Una aplicación importante de la noción de valencia es en el problema de 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. Esto nos da otra manera para distinguir los grafos de la Fig 4, puesto que el primer grafo tiene un vértice de valencia 1 y el segundo no.

Una extensión de esta idea se da en el ejercicio 5.3.1(4).

5.3.1. Ejercicios.

1. ¿ Es posible que las siguientes listas sean las valencias de todos los vértices de un grafo? Si así lo fuera, dar una representación pictórica de tal grafo. (Recuerde que hay a lo más una arista que una un par de vértices dados.)

   (i) $2, 2, 2, 3.$ (ii) $1, 2, 2, 3, 4.$

   (iii) $2, 2, 4, 4, 4.$ (iv) $1, 2, 3, 4.$

2. Si $G = (V, E)$ es un grafo, el **complemento** G^c de G es el grafo cuyo conjunto de vértices es V y cuyas aristas unen aquellos vértices que no son unidos por G. Si G tiene n vértices y sus valencias son $d_1, d_2, \ldots, d_n$, ¿cuáles son las valencias de G^c?
3. Encuentre todos los grafos posibles (no isomorfos) que pueda, que sean regulares, 4-valentes y con 7 vértices. [Ayuda: considere el complemento de esos grafos.]
4. Suponga que G_1 y G_2 sean grafos isomorfos. Para cada $k \geq 0$ sea $n_i(k)$ el número de vértices de G_i que tienen valencia k $(i = 1, 2)$. Probar que $n_1(k) = n_2(k)$.
5. Probar que si G es un grafo con al menos dos vértices, entonces G tiene dos vértices con la misma valencia.

5.4. Caminos y ciclos

Frecuentemente usamos grafos como modelos de situaciones prácticas que involucran rutas: los vértices representan ciudades o cruces, y cada arista representa una ruta o cualquier otro forma de comunicación. Las definiciones de esta sección se comprenderán mejor con esta clase de ejemplo en mente.

Definición 5.4.1. Una **caminata** en un grafo G es una secuencia de vértices

$$v_1, v_2, \ldots, v_k,$$

tal que v_i y v_{i+1} son adyacentes $(1 \leq i \leq k-1)$. Si todos los vértices son distintos, una caminata es llamada un **camino**.

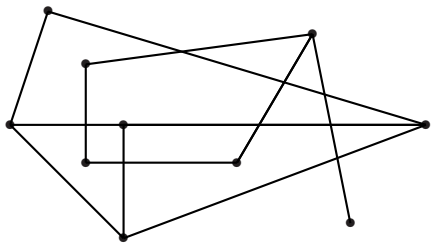


FIGURA 6. Un grafo con dos componentes

Es decir, una caminata especifica una ruta en G: del primer vértice vamos a uno adyacente, de éste 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 y luego tomar la dirección contraria y regresar a x. En un camino, cada vértice es visitado solo una vez.

Escribamos $x \sim y$ siempre y cuando los vértices x e y de G puedan ser unidos por un camino en G: hablando en forma rigurosa, esto significa que hay un camino $v_1, v_2, \ldots, v_k$ en G con $x = v_1$ e $y = v_k$. Es un asunto sencillo verificar que $\sim$ es una relación de equivalencia en el conjunto de vértices V de G, luego podemos partir a V en clases de equivalencia disjuntas. Dos vértices están en la misma clase si ellos pueden ser unidos por un camino, y están en clases diferentes si no podemos encontrar tal camino.

DEFINICIÓN 5.4.2. Supongamos que $G = (V, E)$ es un grafo y que la partición de V en las clases de equivalencia de $\sim$ es

$$V = V_1 \cup V_2 \cup \cdots \cup V_r.$$

Denotemos con E_i $(1 \leq i \leq r)$ al subconjunto de E que contiene todas las aristas cuyos finales están en V_i. Entonces los grafos $G_i = (V_i, E_i)$ son llamados las **componentes** de G. Si G tiene solo una componente diremos entonces que el grafo es **conexo**.

La terminología casi explica por si misma el significado de estas definiciones. El grafo mostrado en la Fig. 6 tiene dos componentes, y por consiguiente no es conexo. La descomposición de un grafo en componentes es muy útil, puesto que muchas propiedades de los grafos pueden ser establecidas considerando las componentes separadamente. Por esta razón, teoremas acerca de grafos a menudo son probados solo para la clase de grafos conexos.

Cuando un grafo de moderado tamaño es dado por una representación pictórica es bastante fácil determinar si es o no conexo. Sin embargo, cuando un grafo es dado por una lista de adyacencia necesitaremos un algoritmo eficiente para decidir si es o no conexo. Llamaremos **ciclo** a una caminata $v_1, v_2, \ldots, v_{r+1}$ cuyos vértices son distintos exceptuando los extremos, es

decir que $v_1 = v_{r+1}$. El grafo tiene r vértices distintos y r aristas, a menudo diremos que es un **r-ciclo**, o un ciclo de **longitud** r.

Ejemplo 5.4.1. Dos miembros del Departamento de Matemática de la Universidad de Folornia planean tomar sus vacaciones en la isla de Wanda. La Fig. 7 representa los lugares de interés turístico de la isla y las carreteras que los unen. La Dra. E. Chunner es una turista por naturaleza, y desea visitar cada lugar una vez y volver al punto de partida. El Dr. R. Dodder es un explorador, y desea atravesar todos los caminos solo una vez, a él lo tiene sin cuidado si regresa o no al lugar del cual partió. ¿Podrán encontrar las rutas que desean los Drs. Chunner y Dodder?

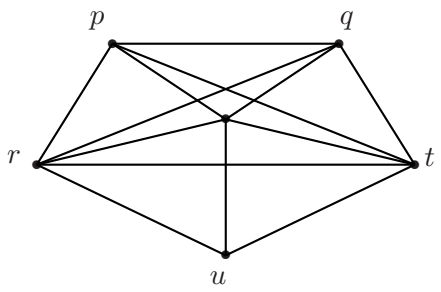


Figura 7. El gran tour

Demostración. La Dra. C puede usar diferentes rutas para alcanzar su objetivo: una posibilidad es el ciclo p, q, t, s, u, r, p.

Sin embargo, el Dr. D está en un apuro. Llamemos x al punto de partida y llamemos y al punto de llegada, y supongamos por el momento que $x \neq y$. Entonces él usa una arista con extremo en x para partir y cada vez que vuelve a x debe arribar y partir por nuevas aristas. Luego, usa un número impar de aristas con extremo en x, y por consiguiente x debe ser un vértice impar. De manera análoga, y debe ser también un vértice impar, puesto que Dr. D usa dos aristas cada vez que pasa por y, y una más al finalizar en y. Los restantes vértices deben ser pares, puesto que cada vez que el Dr. llega a un vértice intermedio parte de nuevo, y por consiguiente usa dos aristas.

Resumiendo, una ruta para el Dr. D que empiece y finalice en vértices distintos x e y , es solo posible si hay dos vértices impares (que son x e y) y el resto de los vértices es par. Pero en el grafo de la Fig. 7 el valor de las valencias es: $\delta(p) = 4$, $\delta(q) = 4$, $\delta(r) = 5$, $\delta(s) = 5$, $\delta(t) = 5$, y $\delta(u) = 3$. Luego hay demasiados vértices impares, y por lo tanto no existe la ruta que el Dr. D desea. Si permitimos la posibilidad de que $x = y$, la situación es aún peor, pues en este caso todos los vértices son pares. □

En general, la ruta de la Dra. C es un ciclo que contiene todos los vértices del grafo dado. Tales ciclos fueron estudiados por el matemático irlandés W.R. Hamilton (1805-65), y en consecuencia

un ciclo con esta propiedad es llamado un **ciclo hamiltoniano**. En nuestro ejemplo, fue muy fácil encontrar un ciclo hamiltoniano, pero este fue un caso muy especial y no representativo. Para ciertos grafos, puede ser un problema difícil decidir si un ciclo hamiltoniano existe o no.

Por otro lado , el problema del Dr. D puede ser fácilmente resuelto. Una caminata que use cada arista de un grafo solo una vez es llamada una **caminata euleriana**, debido a que Euler fue el primero en estudiar estas caminatas. El encontró que si $x \neq y$, una condición necesaria para que exista una caminata euleriana que comience en x y finalice en y es que x e y deben ser vértices impares y el resto debe ser par, mientras que si $x = y$ la condición es que todos los vértices deben ser pares. Es decir que una condición necesaria para que exista una caminata euleriana en un grafo G es que G debe tener a lo más dos vértices impares. Más aún, puede probarse que esta condición es también suficiente. Puesto que es sencillo calcular las valencias de los vértices de un grafo, es relativamente sencillo decidir si un grafo tendrá o no una caminata euleriana.

5.4.1. Ejercicios.

1. Encontrar el número de componentes de el grafo cuya lista de adyacencia es

a	b	c	d	e	f	g	h	i	j
f	c	b	h	c	a	b	d	a	a
i	g	e		g	i	c		f	f
j		g			j	e			

2. ¿Cuántas componentes conexas tiene el grafo de la fiesta de Abril (sección 5.1)?
3. Encontrar un ciclo hamiltoniano en el grafo formado por los vértices y aristas de un cubo.
4. El año que viene el Dr. Chunner y el Dr. Dodder desean visitar la isla de Meanda, donde los lugares interesantes y las caminos que los unen están representados por el grafo que tiene la siguiente lista de adyacencia

0	1	2	3	4	5	6	7	8
1	0	1	0	3	0	1	0	1
3	2	3	2	5	4	5	2	3
5	6	7	4		6	7	6	5
7	8		8		8		8	7.

   ¿Es posible encontrar rutas para Chunner y Dodder que satisfagan lo pedido en el *Ejemplo*?
5. Un ratón intenta comer un $3 \times 3 \times 3$ cubo de queso. Él comienza en una esquina y come un subcubo de $1 \times 1 \times 1$, para luego pasar a un subcubo adyacente. ¿Podrá el ratón terminar de comer el queso en el centro?

5.5. Árboles

DEFINICIÓN 5.5.1. Diremos que un grafo T es un **árbol** si cumple con las dos propiedades siguientes:

(T1) T es conexo;
(T2) no hay ciclos en T.

Algunos árboles típicos han sido dibujados en la Fig. 8. A causa de su particular estructura y propiedades, los árboles aparecen en diversas aplicaciones de la matemática, especialmente en investigación operativa y ciencias de la computación. Comenzaremos el estudio de ellos estableciendo algunas propiedades sencillas.

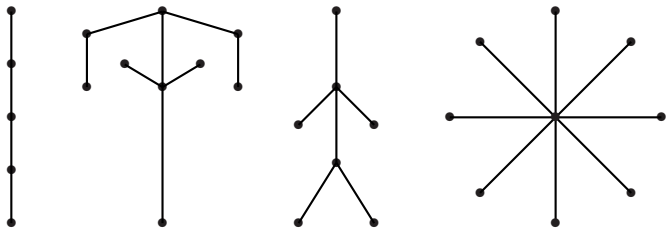


FIGURA 8. Algunos árboles

TEOREMA 5.5.1. *Si $T = (V, E)$ es un árbol con al menos dos vértices, entonces:*

(T3) *Para cada par x, y de vértices existe un único camino en T de x a y.*
(T4) *El grafo obtenido de T removiendo alguna arista tiene dos componentes, cada una de las cuales es un árbol.*
(T5) $|E| = |V| - 1$.

DEMOSTRACIÓN. (T3) Puesto que T es conexo, existe un camino de x a y, digamos

$$x = v_0, v_1, \ldots, v_r = y.$$

Si existiera otro camino, digamos

$$x = u_0, u_1, \ldots, u_s = y,$$

consideremos i el más pequeño subíndice para el cual se cumple que $u_{i+1} \neq v_{i+1}$ (Fig. 9).

Puesto que ambos caminos finalizan en y ellos se encontrarán de nuevo, y entonces podemos definir j como el más pequeño subíndice tal que

$$j > i \quad \text{y} \quad v_j = u_k \quad \text{para algún } k.$$

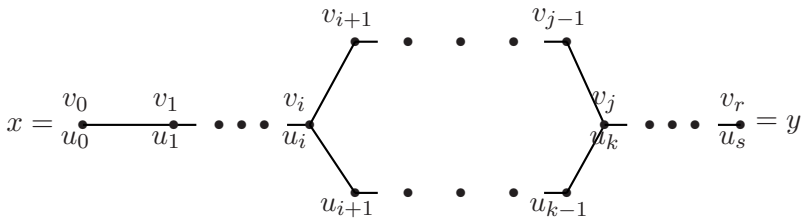


FIGURA 9. Dos caminos diferentes determinan un ciclo

Entonces $v_i, v_{i+1}, \ldots, v_j, u_{k-1}, u_{k-2}, \ldots, u_{i+1}, v_i$ es un ciclo en T, y esto contradice a las hipótesis. Por consiguiente solo existe un camino en T de x a y.

(T4) Supongamos que uv es una arista en T, y sea $S = (V, E')$ el grafo con el mismo conjunto de vértices que T y con el conjunto de aristas $E' = E - uv$. Sea V_1 el conjunto de los vértices x de T para los cuales existe un único camino en T de x a v que pasa por u. Claramente, este camino debe finalizar con la arista uv, pues sino T tendría un ciclo. Sea V_2 el complemento de V_1 en V.

Cada vértice en V_1 se une por un camino en S a u, y cada vértice en V_2 se une por un camino en S a v, pero no existe camino de u a v en S. Se sigue entonces que V_1 y V_2 son las dos componentes del conjunto de vértices de S. Cada componente es conexa (por definición), y no contiene ciclos, pues sino habría ciclos en T. Es decir que las dos componentes son árboles.

(T5) El resultado es cierto cuando $|V| = 1$, puesto que el árbol de un vértice no tiene aristas.

Supongamos que es cierto para árboles con k o menos vértices. Sea T un árbol con $|V| = k+1$, y sea uv una arista en T. Si $T_1 = (V_1, E_1)$ y $T_2 = (V_2, E_2)$ son los árboles que se obtienen removiendo uv en T, tenemos que

$$|V_1| + |V_2| = |V|, \qquad |E_1| + |E_2| = |E| - 1.$$

Aplicando la hipótesis inductiva a T_1 y T_2 obtenemos

$$|E| = |E_1| + |E_2| + 1 = |V_1| - 1 + |V_2| - 1 + 1 = |V| - 1,$$

como nosotros deseábamos. Por consiguiente el resultado es cierto para todos lo enteros positivos. □

Las propiedades (T1)-(T5) nos dan maneras alternativas de definir árboles. Por ejemplo la propiedad (T3) puede ser considerada como la propiedad que define un árbol, en vez de (T1) y (T2). Ya hemos probado que (T3) es consecuencia de las propiedades (T1) y (T2), luego solo queda por probar que la recíproca también vale (ejercicio 5.5.1 3.

5.5.1. Ejercicios.

1. Hay seis diferentes (es decir, no isomorfos entre si) árboles con seis vértices: haga un dibujo de ellos.
2. Sea $T = (V, E)$ un árbol con $|V| \geq 2$. Usando la propiedad (T5) y el Teorema 5.3.1 probar que T tiene al menos dos vértices con valencia 1.
3. Probar que la propiedad (T3) implica (T1) y (T2).
4. Una **foresta** es un grafo que satisface (T2) pero no necesariamente (T1). Probar que si $F = (V, E)$ es una foresta con c componentes entonces

$$|E| = |V| - c.$$

5.6. Coloreando los vértices de un grafo

Un problema que se nos presenta frecuentemente en la vida moderna es aquel de confeccionar un horario para un conjunto de eventos de tal manera de evitar interferencias. Consideremos ahora un caso muy simple, que nos servirá de ejemplo para mostrar como la teoría de grafos puede ayudar al estudio de este problema.

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 a v_1 y v_2, v_1 y v_4, v_3 y v_5, v_2 y v_6, v_4 y v_5, v_5 y v_6 y v_1 y v_6. ¿Cuántas horas son necesarias para poder confeccionar un horario en el cual no haya interferencias?

Podemos representar la situación por un grafo (Fig. 10). Los vértices corresponden a las seis clases, y las aristas indican las interferencias potenciales.

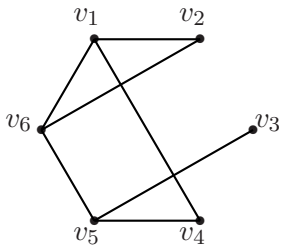


FIGURA 10. El grafo para un problema de horarios

Un horario el cual 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

En términos matemáticos, tenemos una partición del conjuntos de vértices en cuatro partes, con la propiedad que ninguna parte contiene un par de vértices adyacentes del grafo. Un descripción

más gráfica utiliza la función

$$c : \{v_1, v_2, v_3, v_4, v_5, v_6\} \to \{1, 2, 3, 4\}$$

la cual asigna cada vértice (curso) a la hora que le corresponde. Usualmente, nosotros hablamos de colores asignados a los vértices, en vez de horas, pero claramente la naturaleza exacta de los objetos $1, 2, 3, 4$ no es importante. Podemos usar el nombre de colores reales, rojo, verde, azul , amarillo, o podemos hablar del color 1, color 2, etc. Lo importante es que los vértices que son adyacentes en el grafo deben tener diferentes colores.

Definición 5.6.1. Una **coloración de vértices** de un grafo $G = (V, E)$ es una función $c : V \to \mathbb{N}$ con la siguiente propiedad:

$$c(x) \neq c(y) \quad \text{si} \quad \{x, y\} \in E.$$

El **número 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 otra palabras, $\chi(G) = k$ si y solo 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 la Fig. **??**, vemos que nuestro primer intento de horario es equivalente a una coloración de vértices con cuatro colores. El mínimo número de horas necesarias será el número cromático del grafo, y la pregunta es ahora si este número es cuatro o menor que cuatro. Un rápido intento con tres colores nos da la solución de este problema:

Color 1	Color 2	Color 3
v_1	v_2 y v_5	v_3, v_4 y v_6.

Más aún, hacen falta por lo menos tres colores, puesto que v_1, v_2, y v_6 son mutuamente adyacentes y por lo tanto deben tener diferentes colores. Luego concluimos que el número cromático del grafo es 3.

En general, para probar que el número cromático de un grafo dado es k, debemos hacer dos cosas:

(i) encontrar una coloración de vértices usando k colores;
(ii) probar que ninguna coloración de vértices usa menos de k colores.

5.6.1. Ejercicios.

1. Encontrar el número cromático de los siguientes grafos:
   (i) un grafo completo K_n;
   (ii) un grafo cíclico C_{2r} con un número par de vértices;
   (iii) un grafo cíclico C_{2r+1} con un número impar de vértices.
2. Determine los números cromáticos de los grafos descritos en la Fig. 11.

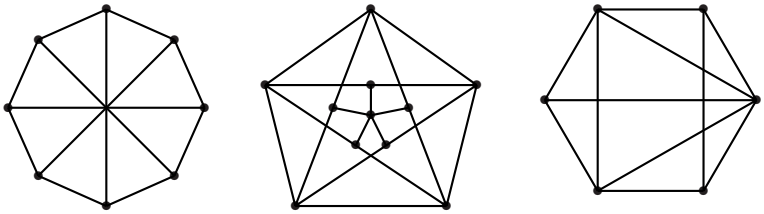


FIGURA 11. Encontrar el número cromático

3. Describir todos los grafos G tales que $\chi(G) = 1$.

5.7. El algoritmo greedy para coloración de vértices

Es bastante difícil encontrar el número cromático de un grafo dado. En realidad, no se conoce ningún algoritmo para este problema que trabaje en "tiempo polinomial", y la mayoría de la gente cree que tal algoritmo no existe. Sin embargo hay un método simple de hacer una coloración cromática usando un "razonable" número de colores.

El método consiste en asignar los colores de los vértices en orden, de tal manera que cada vértice recibe el primer color que no haya sido ya asignado a alguno de sus vecinos. En este algoritmo insistimos en hacer la mejor elección que podemos en cada paso, sin mirar más allá para ver si esta elección nos traerá problemas luego. Un algoritmo de esta clase se llama a menudo un **algoritmo greedy (goloso)**.

El algoritmo greedy para coloración de vértices es fácil de programar. Supóngase que hemos dado a los vértices algún orden $v_1, v_2, \ldots, v_n$. Asignemos el color 1 a v_1; para cada v_i $(2 \leq i \leq n)$ formamos el conjunto S de colores asignados a los vértices v_j $(1 \leq j < i)$ que son adyacentes a v_i, y le damos a v_i el primer color que no está en S. (En la práctica, pueden ser usados métodos más sofisticados de manejar los datos.)

Algoritmo greedy para coloración de vértices

asignemos el color 1 *a* v_1;
`for i:=2 to n  do`
`{`
    sea S *el conjunto de colores*;
    `for j:= 1 to i-1  do`
    `{`
        `if (`v_j *es adyacente a* v_i`)` *agregue el color de* v_j *a* S;
    `}`
    `k:=1;`
    `while (`*el color* k *está en* S`) do`

```
        {
        k:=k+1;
        asigne el color k a v_i;
        }
    }
```

Debido a que la estrategia greedy es corta de vista, el número de colores que usará será normalmente más grande que le mínimo posible. Por ejemplo, el algoritmo greedy aplicado en el grafo de Fig. **??** da precisamente le coloración de vértices con cuatro colores que fue propuesta anteriormente, luego encontramos otra coloración con tres colores. Por supuesto todo depende del orden que se elige inicialmente para los vértices. Es bastante fácil ver que si se elige el orden correcto, entonces el algoritmo greedy nos da la mejor coloración posible (ejercicio **??** (2). Pero hay $n!$ órdenes posibles, y si tuviéramos que controlar cada uno de ellos, el algoritmo requeriría "tiempo exponencial".

Más allá de esto, el algoritmo greedy es útil tanto en la teoría como en la práctica. Probaremos ahora dos teoremas por medio de la estrategia greedy.

TEOREMA 5.7.1. *Si G es un grafo con valencia máxima k, entonces*

(i) $\chi(G) \leq k+1$,
(ii) *si G es conexo y no regular , $\chi(G) \leq k$.*

DEMOSTRACIÓN. (i) Sea $v_1, v_2, \ldots, v_n$ un ordenamiento de los vértices de G. Cada vértice tiene a lo más k vecinos, y por consiguiente el conjunto S de los colores asignados por el algoritmo greedy a los vértices v_j que son adyacentes a v_i $(1 \leq j < i)$ tiene como máximo cardinal k. Por consiguiente al menos uno de los colores $1, 2, \ldots, k+1$ no está en S, y el algoritmo greedy asigna entonces el primero de estos a v_i.

(ii) Para probar esta parte debemos elegir un orden especial de los vértices, comenzando con v_n y yendo hacia atrás. Puesto que G tiene valencia máxima k y es no regular, existe al menos un vértice G cuya valencia es menor que k: llamémoslo v_n. Listemos los vecinos de v_n como $v_{n-1}, v_{n-2}, \ldots, v_{n-r}$; hay a lo más $k-1$ de ellos. A continuación listemos los vecinos de v_{n-1} (excepto v_n y sus vecinos), y observemos que como la valencia es a lo más k hay a lo más $k-1$ de estos vértices. A continuación listemos los vecinos de v_{n-2} que no hayan sido listados antes, y así siguiendo. Puesto que G es conexo, en determinado momento podremos listar todos los vértices de G. Más aún, el método de construcción asegura que cada vértice es adyacente a lo más a $k-1$ de sus predecesores en el orden $v_1, v_2, \ldots, v_n$.

Usando el mismo argumento que en la parte (i) (pero para este orden) se sigue que el algoritmo greedy requerirá a lo más k colores. Luego $\chi(G) \leq k$. □

La parte (ii) del teorema es falsa si permitimos que G sea regular. El lector que haya respondido correctamente al ejercicio 5.6.1 1 será capaz de dar dos ejemplos de este hecho: los grafos

completos, y los grafos cíclicos de longitud impar, ambos requieren $k+1$ colores. Si embargo, puede ser demostrado que estos son los únicos contraejemplos.

Otra consecuencia útil del algoritmo greedy se refiere a grafos G son $\chi(G) = 2$. Para tales grafos, los conjuntos V_1 y V_2 de vértices de colores 1 y 2 respectivamente, forman una partición de V, con la propiedad que cada arista tiene un vértice en V_1 y el otro en V_2. Por esta razón, cuando $\chi(G) = 2$, diremos que G es **bipartito**. Una coloración de vértices con dos colores de un cubo se ilustra en la Fig. 12, junto a un dibujo alternativo que enfatiza la naturaleza bipartita del grafo. Usualmente usaremos esta clase de dibujo cuando trabajemos con grafos bipartitos.

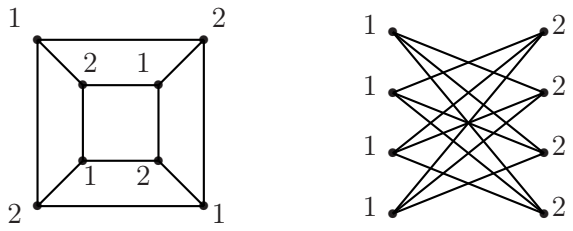


FIGURA 12. El cubo es un grafo bipartito

TEOREMA 5.7.2. *Un grafo es bipartito si y solo si no contiene ciclos de longitud impar.*

DEMOSTRACIÓN. Si hay un ciclo de longitud impar, entonces se requieren tres colores, solamente para colorear este ciclo, y- el número cromático del grafo es por ende al menos tres. Luego si el grafo es bipartito, no puede tener ciclos de longitud impar.

Recíprocamente, supongamos que G es un grafo sin ciclos de longitud impar. 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 esta en el *nivel 0*. A continuación, listemos la lista de vecinos de v_1 (excepto v_1), llamémoslos $v_2, v_3, \ldots, v_r$; diremos que estos vértices están en el *nivel 2*. Continuando de esta manera, definimos el *nivel* l como todos aquellos vértices adyacentes a los del *nivel* $l-1$, exceptuando aquellos previamente listados en el *nivel* $l-2$. Cuando ningún nuevo vértice puede ser agregado de esta forma, obtenemos la componente G_0 de G (si G es conexo $G_0 = G$).

El hecho crucial producido por este orden es que un vértice del nivel l solo puede ser adyacente a vértices de los niveles $l-1$ y $l+1$, y no a vértices del mismo nivel. 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, y los caminos pueden ser elegidos de tal manera que z sea el único vértice común (Fig. 13). Si x e y fueran adyacentes, habría un ciclo de longitud $2m+1$, lo cual contradice la hipótesis.

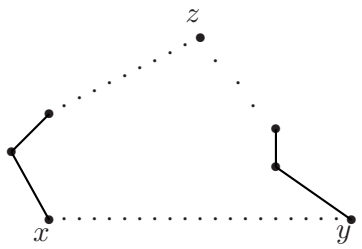


FIGURA 13. Vértices adyacentes en el mismo nivel inducen un ciclo impar

Se deduce entonces que el algoritmo greedy asigna el color 1 a los vértices en el nivel $0, 2, 4, \ldots$, y el color 2 a los vértices en los niveles $1, 3, 5, \ldots$. Por consiguiente $\chi(G_0) = 2$. Repitiendo el mismo argumento para cada componente de G obtenemos el resultado deseado. □

5.7.1. Ejercicios.

1. Encontrar órdenes de los vértices del grafo del cubo (Fig. 12) para los cuales el algoritmo greedy requiera 2, 3 y 4 colores respectivamente.
2. Probar que para cualquier grafo G existe un orden de los vértices para el cual el algoritmo greedy requiera $\chi(G)$ colores. [Ayuda: use un coloreado de vértices de $\chi(G)$ colores para definir el orden.]
3. Denotemos $e_i(G)$ el número de vértices del grafo G cuya valencia es estrictamente mayor que i. Use el algoritmo greedy para probar que si $e_i(G) \leq i + 1$ para algún i, entonces $\chi(G) \leq i + 1$.
4. El grafo M_r ($r \geq 2$) se obtiene a partir del grafo cíclico C_{2r} añadiendo aristas extras que unen los vértices opuestos. Probar que

   (i) M_r es bipartito cuando r es impar,

   (ii) $\chi(M_r) = 3$ cuando r es par y $r \neq 2$,

   (iii) $\chi(M_2) = 4$.

5.8. Ejercicios

1. ¿Para qué valores de n es verdadero que el grafo completo K_n tiene una caminata euleriana.
2. Usar el principio de inducción para probar que si $G = (V, E)$ es un grafo con $|V| = 2m$, y G no tiene 3-ciclos, entonces $|E| \leq m^2$.
3. Sea $X = \{1, 2, 3, 4, 5\}$ y denotemos V el conjunto de los 2-subconjuntos de X. Denotemos E el conjunto de pares de elementos de V que son disjuntos entre si (como subconjuntos de X). Probar que este grafo es otra versión del grafo de Petersen (ejercicio 5.2.1 (2).

4. Sea G un grafo bipartito con un número impar de vértices. Probar que G tiene un ciclo hamiltoniano.
5. El k-**cubo** Q_k es el grafo cuyos vértices son las palabras de longitud k en el alfabeto $\{0,1\}$ y cuyas aristas unen palabras que difieren en exactamente una posición. Probar que:

   (i) Q_k es regular de valencia k,

   (ii) Q_k es bipartito.
6. Probar que el grafo Q_k definido en el ejercicio anterior tiene un ciclo hamiltoniano.
7. Probar que el grafo de Petersen no tiene ciclos hamiltonianos.
8. En el juego del dominó las reglas especifican que las fichas deben ser puestas en una linea de tal forma que en dos fichas adyacentes coinciden los números adyacentes, es decir si $[x|y]$ está al lado de $[x'|y']$ debe ser $y = x'$. Mirando las fichas de dominó $[x|y]$ con $x \neq y$ como las aristas del grafo completo K_7 probar que existe un juego de dominó donde se utilizan todas las fichas.
9. Calcular el número de caminatas eulerianas de K_7 y el número de juegos de dominó completos.
10. Probar que si $\alpha : V_1 \to V_2$ es un isomorfismo de grafos entre $G_1 = (V_1, E_1)$ y $G_2 = (V_2, E_2)$ entonces la función $\beta : E_1 \to E_2$ definida por

$$\beta\{x, y\} = \{\alpha(x), \alpha(y)\} \qquad (\{x, y\} \in E_1)$$

    es una biyección.
11. Si G es un grafo regular k-valente con n vértices, entonces

$$\chi(G) \geq \frac{n}{n-k}.$$

12. Construir cinco grafos regulares conexos mutuamente no isomorfos con valencia 3 y ocho vértices.
13. Probar que el grafo completo K_{2n+1} es la unión de n ciclos hamiltonianos sin aristas comunes.
14. ¿Es posible para un caballo visitar todos los casilleros de un tablero de ajedrez exactamente una vez y volver al casillero original? Interprete su respuesta en términos de ciclos hamiltonianos en un cierto grafo.
15. El **grafo impar** O_n se define de la siguiente manera (cuando $k \geq 2$): los vértices son los $(k-1)$-subconjuntos de un $(2k-1)$-conjunto, y las aristas unen los conjuntos disjuntos. (Luego O_3 es el grafo de Petersen). Probar que $\chi(O_k) = 3$ para $k \geq 2$.
16. Probar que si G es un grafo con n vértices, m aristas y c componentes entonces

$$n - c \leq m \leq \frac{1}{2}(n-c)(n-c+1).$$

Construir ejemplos mostrando que ambos extremos de las desigualdades pueden ser alcanzados para todos los valores de n y c con $n \geq c$.

17. Una sucesión $d_1, d_2, \ldots, d_n$ es **gráfica** si existe un grafo cuyos vértices pueden ser ordenados en la forma $v_1, v_2, \ldots, v_n$ de tal forma que $\delta(v_i) = d_i$ $(1 \leq i \leq n)$. Probar que si una sucesión $d_1, d_2, \ldots, d_n$ es gráfica y $d_1 \geq d_2 \geq \cdots \geq d_n$ entonces

$$d_1 + d_2 + \cdots + d_n \leq k(k-1) + \sum_{i=k+1}^{n} \min(k, d_i)$$

para $1 \leq k \leq n$.

18. Sea $G = (V, E)$ un grafo con al menos tres vértices tal que

$$\delta(v) \geq \frac{1}{2}|V| \qquad (v \in V).$$

Probar que G tiene un ciclo hamiltoniano.

19. Probar que si $\tilde{G}$ es el complemento del grafo G, entonces $\chi(G)\chi(\tilde{G}) \leq n$, donde n es el número de vértices de G.

CAPíTULO 6

Árboles

6.1. Contando las hojas de un árbol con raíz

Recordemos que un árbol es un grafo conexo que no contiene ciclos. Los árboles aparecen en contextos diferentes y a menudo un vértice del árbol se distingue de los otros. Por ejemplo en el árbol genealógico que describe la descendencia de un rey, nosotros podemos enfatizar la posición especial del rey poniéndolo en lo más alto del árbol. En general, nosotros llamaremos al vértice notable la **raíz** del árbol, y a un árbol con una raíz específica lo llamaremos **árbol con raíz**. (Esta terminología, aunque estándar, tiene el defecto que en la representación pictórica la raíz aparece en lo más alto del árbol y el árbol 'crece' hacia abajo.)

Para el estudio de un árbol con raíz es natural ubicar los vértices en niveles, de la misma manera que lo hicimos para los grafos bipartitos en la sección 5.7. Diremos que el vértice raíz es el *nivel 0* y que sus vecinos forman el *nivel 1*. Para cada $k \geq 2$, el *nivel k* está formado por aquellos vértices que son adyacentes a vértices del nivel $k-1$, excepto aquellos que ya pertenecen al nivel $k-2$. El árbol con raíz representado en la Fig. 1 puede ser dibujado nuevamente como se lo muestra a la derecha de manera de visualizar los niveles.

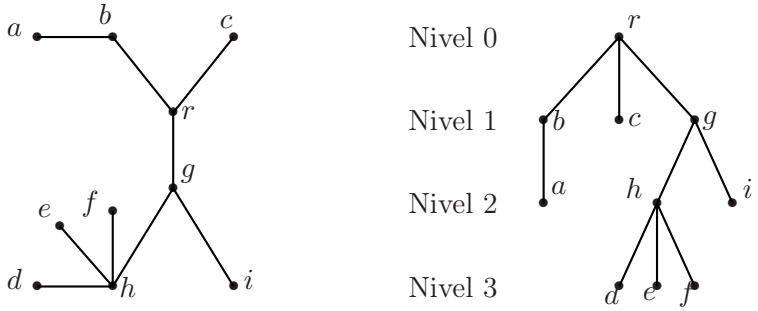


FIGURA 1. Un árbol con raíz y sus niveles

Un vértice en un árbol con raíz se llama una **hoja** si pertenece al nivel i ($i \geq 0$) y no es adyacente a ningún vértice del nivel $i+1$. Un vértice que no es una hoja es llamado **interno**. La **altura** de un árbol con raíz es el máximo valor de k para el cual el nivel k es no vacío. Luego el árbol de la Fig. 1 tiene seis hojas, cuatro vértices internos y su altura es tres.

6.1.1. Ejercicios.

1. En la siguiente tabla $n_5(h)$ es el número de árboles con raíz no isomorfos que tienen 5 vértices y altura h. (Dos árboles con raíz son isomorfos si hay un isomorfismo de grafos, sin considerar la raíz, que lleva la raíz de uno en la del otro.) Verifique la tabla construyendo los ejemplos para cada caso.

$$\begin{array}{rcccc} h: & 1 & 2 & 3 & 4 \\ n_5(h): & 1 & 4 & 3 & 1 \end{array}$$

2. Si consideramos los árboles comunes (sin raíz), ¿cuál es el número de árboles no isomorfos con 5 vértices? Hacer una lista y controlar que la lista del ejercicio anterior sea completa.
3. Construir dos árboles con raíz no isomorfos ambos con 12 vértices, 6 hojas y altura 4.

Las dos propiedades que usamos en la sección 5.5 para definir un árbol tienen consecuencias obvias cuando pensamos los vértices por niveles. Puesto que todo árbol es conexo (propiedad T1) entonces cada vértice pertenece a algún nivel. Más importante aún, puesto que un árbol no tiene ciclos (propiedad T2) cada vértice v del nivel i es adyacente a uno y solo uno u del nivel $i-1$. A veces enfatizaremos esto diciendo que u es el *padre* de v o que v es un *hijo* de u. Cada vértice, excepto el raíz, tiene un único padre, pero un vértice puede tener una cantidad arbitraria de hijos (incluso ninguno). Claramente, un vértice es una hoja si y solo si no tiene hijos.

En muchas aplicaciones ocurre que cada padre (vértice interno) tiene la misma cantidad de hijos. Cuando cada padre tiene m hijos diremos que el árbol es **m-ario**, en particular cuando $m = 2$ diremos que el árbol es *binario* y cuando $m = 3$ diremos que es *ternario*.

TEOREMA 6.1.1. *La altura de un árbol con raíz m-ario con l hojas es por lo menos* $\log_m l$.

DEMOSTRACIÓN. Puesto que

$$h \geq \log_m l \quad \Leftrightarrow \quad m^h \geq l$$

es suficiente probar la afirmación equivalente: todo árbol con raíz m-ario de altura h tiene a lo más m^h hojas. La demostración es por inducción sobre h.

Claramente la afirmación es verdadera cuando $h = 0$ puesto que en este caso el árbol es solo un vértice (la raíz) que es una hoja. Supongamos que la afirmación es verdadera cuando $0 \leq h \leq h_0$ y sea T un árbol con raíz m-ario de altura $h_0 + 1$. Si eliminamos la raíz y las aristas a las cuales pertenece obtenemos m árboles $T_1, \ldots, T_m$ cuyas raíces son los vértices del nivel 1 de T. Cada T_i es un árbol con raíz de altura h_0 o menos, luego por hipótesis inductiva tiene a lo más m^{h_0} hojas. Pero las hojas de T son precisamente las hojas de los árboles $T_1, \ldots, T_m$ y por consiguiente el número de hojas es a lo más $m \times m^{h_0} = m^{h_0+1}$.

Por el principio de inducción completa se sigue que la afirmación es verdadera para todo $h \geq 0$. □

Puesto que $\log_m l$ no es generalmente un número entero, el teorema anterior puede ser mejorado un poco. Por ejemplo si $m = 3$ y $l = 10$ la desigualdad

$$h \geq \log_m l = 2,0959\ldots$$

implica que $h \geq 3$. En general podemos decir que

$$h \geq \lceil \log_m l \rceil,$$

donde $\lceil x \rceil$ denota el menor entero z tal que $z \geq x$.

Una aplicación frecuente del Teorema 6.1.1 es en los *árboles de decisión*. Cada vértice interno de un árbol de decisión representa una decisión y los posibles resultados de esa decisión son las aristas que unen ese vértice con los vértices del nivel siguiente. Los posibles resultados finales del procedimiento son las hojas del árbol. Si el resultado de una decisión puede ser solo verdadero o falso entonces tenemos un árbol binario. A continuación daremos un ejemplo con un árbol ternario.

Ejemplo 6.1.1. (El problema de la moneda falsa) Supongamos que tenemos una moneda genuina con la etiqueta 0 y que tenemos otras r monedas indistinguibles de 0 por la apariencia excepto que tienen las etiquetas $1, 2, \ldots, r$. Se sospecha que una moneda podría ser falsa, es decir o más liviana o más pesada. Probar que son necesarias al menos $\lceil \log_3(2r + 1) \rceil$ pesadas en una balanza para decidir que moneda (si hay alguna) es falsa y en ese caso ver si es más pesada o liviana. Muestre un procedimiento que use exactamente este número de pesadas cuando $r = 4$.

Demostración. Hay $2r + 1$ posibles resultados finales u hojas en el árbol de decisión:

$$B, 1P, 1L, \ldots, rP, rL;$$

donde B significa que todas las monedas son buenas, iL significa que la moneda i es más liviana y iP que es más pesada. El árbol de decisión es ternario, puesto que hay tres posibles resultados de cada decisión (es decir de cada pesada entre un grupo de monedas y otro). Estos son:

$$\begin{aligned} < &: \text{el grupo de la izquierda es más liviano} \\ = &: \text{los dos grupos pesan igual} \\ > &: \text{el grupo de la izquierda es más pesado.} \end{aligned}$$

Por consiguiente la altura del árbol de decisión es al menos $\lceil \log_3(2r + 1) \rceil$.

Cuando $r = 4$ entonces $\lceil \log_3(2r + 1) \rceil = 2$, y la solución con dos pesadas se gráfica en la Fig. 2

□

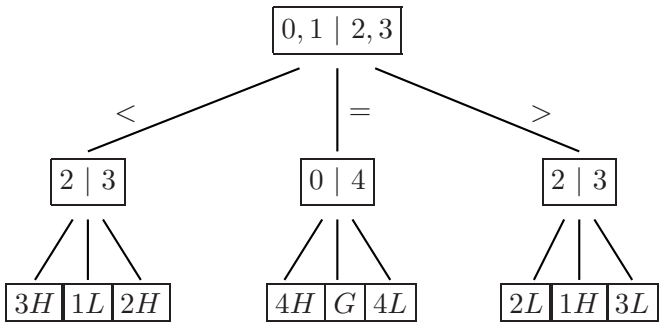


FIGURA 2. Solución del problema de la moneda falsa cuando $r = 4$

6.1.2. Ejercicios. (continuación)

1. Suponga que se organiza un campeonato de fútbol-5 donde participan 20 equipos. El campeonato es por eliminación simple y no hay empates. Construir un esquema para el torneo basado en un árbol con raíz y pruebe que son necesarias al menos 5 rondas.
2. ¿Cuál es la cota inferior en el número de pesadas necesarias en el problema de la moneda falsa (ver el Ejemplo anterior) cuando son seis monedas? Desarrolle un esquema que logre este número de pesadas.
3. Considere la siguiente variante del problema de la moneda falsa. Hay ocho monedas y sabemos que hay exactamente una que es más liviana. Todas las demás son genuinas pero no hay ninguna moneda con la etiqueta 0. Encontrar una cota inferior teórica del número de pesadas necesarias para detectar la moneda falsa y probar que este número puede ser alcanzado.

6.2. Árboles expandidos y el problema MST

Supongamos que $G = (V, E)$ es un grafo conexo y que T es un subconjunto de E tal que

(i) cada vértice de G pertenece a una arista en T;
(ii) las aristas de T forman un árbol.

En esta caso decimos que T es un **árbol expandido** para G. Por ejemplo, un árbol expandido para el grafo de la Fig. 3 se indica con las líneas más gruesas.

Es fácil hacer "crecer" un árbol expandido: tome un vértice arbitrario v del "árbol parcial" inicial y agregue aristas con un extremo en v y el otro extremo que no pertenezca al árbol parcial inicial. El árbol expandido de la Fig. 3 puede construirse haciéndolo crecer desde el vértice a y conectando los otros vértices en el orden b, c, e, f, d, h, g, usando las aristas ab, ac, ae, cf, fd, fh, hg. En general, si hay n vértices nosotros deberemos hacer $n-1$ pasos, después de los cuales tendremos $1 + (n-1) = n$ vértices y $n-1$ aristas (el cual es el número correcto de acuerdo al Teorema 5.5.1).

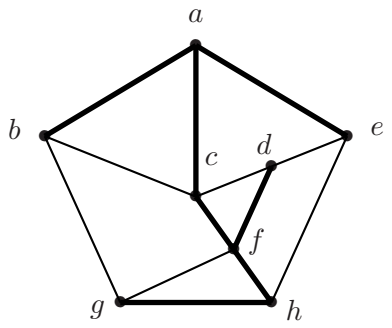


FIGURA 3. Un grafo y uno de sus árboles expandidos

Verifiquemos que el método siempre funciona: sea S el conjunto de vértices del árbol parcial que se ha logrado en un paso intermedio, es decir que S no es ni vacío ni todo V. Si no existe una arista que tenga un extremo en S y el otro en el complemento $\overline{S}$, entonces no existe un camino entre S y $\overline{S}$ y por lo tanto G es disconexo, lo cual contradice las hipótesis. Por consiguiente siempre existe una arista disponible en cada etapa de la construcción.

6.2.1. Ejercicios.

1. Encontrar árboles expandidos para el cubo (Fig. 12) y para el grafo de Petersen.
2. Muestre esquemáticamente todos los árboles expandidos del grafo completo K_4 (hay 16).

Los árboles expandidos son útiles en muchos contextos. Por ejemplo, supongamos que cierta cantidad de ciudades deben ser unidas de a pares por gasoductos de tal forma que quede una red de gasoductos conexa. Algunos pares de ciudades puede ser imposible unirlas por razones geográficas y cada posible conexión tiene asociada un costo de construcción. Formalmente, tenemos un grafo $G = (V, E)$ cuyos vértices son ciudades y sus aristas son las posibles conexiones. Además tenemos una función w de E a $\mathbb{N}$ de tal forma que $w(e)$ representa el costo de construcción de la arista e. Diremos que G y w es un **grafo con pesos** y que w es la **función de pesos**.

En el problema del gasoducto lo que se pretende es construir una red conexa al mínimo costo. Un red de ese tipo corresponde a un árbol expandido T para G cuyo peso total

$$w(T) = \sum_{e \in T} w(e)$$

es lo mas pequeño posible. Nos referiremos a este problema como el **problema MST** (del inglés MST = minimum spanning tree = árbol expandido mínimo) para el grafo con pesos G.

Dado que los valores de w son enteros positivos, claramente el problema MST debe tener solución, puesto que hay solo un número finito de árboles expandidos T para G y cada uno de ellos da un valor entero positivo $w(T)$. En otras palabras, existe un árbol expandido mínimo T_0

tal que

$$w(T_0) \leq w(T)$$

para todos los árboles expandidos T de G. Sin embargo puede haber varios con la misma propiedad.

Un algoritmo simple para el problema MST se basa en aplicar la estrategia greedy al método explicado anteriormente. Específicamente: en cada paso se agrega la arista "más barata" que une un nuevo vértice al árbol parcial. (Si hay varias aristas con la misma propiedad se selecciona una de ellas.) Por ejemplo, si en la Fig. 4 comenzamos con u, luego debemos agregar aristas en el orden uv, ux, uy, yz. Por otro lado, si comenzáramos por y, entonces agregamos las aristas en el orden yz, yu, uv, ux.

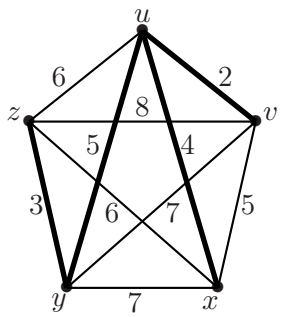


FIGURA 4. Un árbol expandido mínimo

Un primera impresión nos dice que sería bastante sorprendente que el algoritmo greedy funcione para el problema MST, especialmente cuando recordamos que el algoritmo greedy para el problema de coloración de vértices no siempre produce una coloración con el menor número posible de colores. Pero en el caso del problema MST se tiene más suerte.

TEOREMA 6.2.1. *Sea $G = (V, E)$ grafo conexo con función de pesos $w : E \to \mathbb{N}$, y supongamos que T es el árbol expandido para G construido por el algoritmo greedy. Entonces*

$$w(T) \leq w(U)$$

para todo árbol expandido U de G.

DEMOSTRACIÓN. Denotemos $e_1, e_2, \ldots, e_{n-1}$ las aristas de T en el orden en que aplicamos el algoritmo greedy. Si $U = T$ el resultado es obviamente verdadero. Si $U \neq T$ entonces hay aristas de T que no están en U y supongamos que la primera es e_k. Denotemos S el conjunto de vértices en el árbol parcial que se construye por el greedy justo antes de agregar e_k y sea $e_k = xy$ donde x está en S e y no está en S. Puesto que U es un árbol expandido existe un camino de x a y y si uno viaja a través de este camino encontrará una arista e^* con un vértice en S y el otro no.

Ahora bien, cuando e_k es seleccionada para T en el algoritmo greedy, e^* es también candidata a ser seleccionada, pero no lo es. Por consiguiente debemos tener que $w(e^*) \geq w(e)$. Si e^* aparece en T, entonces por el razonamiento anterior es una arista que viene después (en el orden dado) de e_k.

El resultado de remover e^* de U y reemplazarla por e_1 es un árbol expandido U_1, para el cual

$$w(U_1) = w(U) - w(e^*) + w(e_k) \leq w(U).$$

Más aún, la primera arista de T que no está en U_1 aparece después de e_k en el orden dado. En consecuencia podemos repetir el procedimiento obteniendo una sucesión de árboles expandidos $U_1, U_2, \ldots$, con la propiedad que cada uno tiene una secuencia inicial de aristas en común con las aristas de T más larga que el anterior y además $w(U_i) \geq w(U_{i+1})$. El proceso termina cuando obtenemos un árbol expandido U_r igual a T y tenemos

$$w(T) = w(U_r) \leq w(U_{r-1}) \leq \cdots \leq w(U_1) \leq w(U),$$

como queríamos demostrar. □

Existe una forma de ir viendo el progreso del algoritmo por medio de una tabla de tres columnas.

I	II	III
x	y	$w(xy)$
.	.	.
.	.	.
.	.	.

La Columna I lista los vértices que no están en S, que es el conjunto de vértices ya conectados al árbol parcial. Para cada x en la Columna I la correspondiente entrada y en la Columna II es un vértice en S tal que la arista xy es una de las aristas más baratas que unen el vértice x con alguno de S. La Columna III contiene el valor $w(xy)$.

En el i-ésimo paso de la construcción tenemos que $|S| = i$ y hay $n-i$ vértices en la Columna I. Tenemos entonces que seleccionar una de las entradas más pequeñas de la Columna III, digamos $w(x_0y_0)$, y esto conlleva $n - i - 1$ comparaciones. Ahora debemos actualizar la tabla debido a que agregamos x_0 a S por medio de la arista x_0y_0. Primero debemos borrar la fila cuya primera posición tiene a x_0. Después en cada fila debemos verificar si la entrada correspondiente a la Columna II puede ser reemplazada por x_0 o no. Es decir para la fila $x \quad y \quad w(xy)$ debemos verificar si xx_0 es arista y si lo fuera y además $w(xx_0) < w(xy)$, entonces debemos reemplazar y por x_0. Esto agrega otras $n - i - 1$ comparaciones. El número total de comparaciones requeridas

es

$$\sum_{i=1}^{n-1} 2(n-i-1) = (n-1)(n-2).$$

Esto nos dice que para encontrar un MST de un grafo deben hacerse alrededor de n^2 operaciones.

6.2.2. Ejercicios. (continuación)

1. Usar el algoritmo greedy para encontrar un MST del grafo representado en la Fig. 6.5. ¿Es en este caso el MST único?

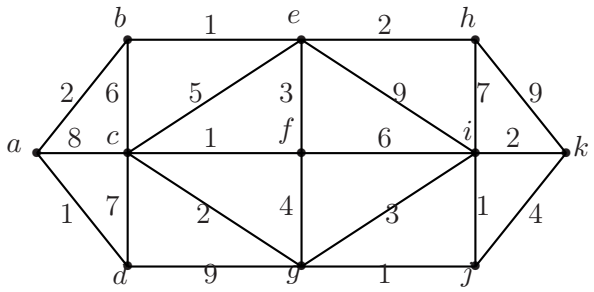


FIGURA 5. Encontrar el MST

1. Sea G un grafo con pesos cuyos vértices son x, a, b, c, d, e, f y cuyas aristas y pesos vienen dados por la siguiente tabla:

xa	xb	xc	xd	xe	xf	ab	bc	cd	de	ef	fa
6	3	2	4	3	7	6	2	3	1	8	6.

   Encontrar todos los árboles expandidos mínimos para G.
2. Suponga que T es un árbol expandido mínimo en un grafo con pesos K y sea e^* una arista de K que no es de T. Sea e una arista de T perteneciente al único camino en T que une los vértices de e^*. Probar que $w(e) \leq w(e^*)$.
3. Escribir un "programa" para el algoritmo greedy basado en el método tabular mostrado más arriba.

6.3. Ejercicios

1. Sea T un árbol con raíz m-ario con n vértices, l hojas e i vértices internos. Probar que

$$n = mi + 1$$

   y encontrar la ecuación de l en términos de m y n.

2. Para cada uno de los seis diferentes árboles (sin raíz) con seis vértices (ver el ejercicio 5.5.1) (1), encontrar el número de elecciones esencialmente diferentes que podemos hacer de un vértice para designarlo como raíz. En base a esto calcular el número de árboles con raíz diferentes que tengan seis vértices.
3. Probar que el número de árboles expandidos mínimos diferentes en K_5 es 125 (no trate de listarlos).
4. Denotemos los vértices del grafo completo K_n con $1, 2, \ldots, n$, y para cada árbol expandido T de K_n definamos el **símbolo de Prüfer** $(p_1, p_2, \ldots, p_{n-2})$ de la siguiente manera: el símbolo de Prüfer de un árbol con dos vértices es 0, el símbolo de Prüfer de un árbol T con n vértices es $(j, q_1, \ldots, q_{n-3})$ donde
   (a) Si i es el primer vértice de T (en el orden dado) que tiene valencia uno, entonces j es el único vértice adyacente a i.
   (b) $(q_1, \ldots, q_{n-3})$ es el símbolo de Prüfer del árbol que se obtiene a partir de T eliminando la arista ij.

   Probar que la construcción del símbolo de Prüfer define una biyección desde el conjunto de árboles expandidos de K_n al conjunto de $(n-2)$-uplas ordenadas del conjunto $\{1, 2, \ldots, n\}$. Deducir de lo anterior que K_n tiene n^{n-2} árboles expandidos.
5. Supongamos que tenemos cuatro monedas y sabemos que una de ellas puede ser falsa (más liviana o más pesada) . Probar que encontrar la moneda falsa (si existe) requiere teóricamente al menos dos pesadas, pero que este número no es posible lograrlo. (En este problema no se da un moneda verdadera.)

CAPíTULO 7

Apéndice I
Más principios de conteo

7.1. Contando conjuntos de pares

Frecuentemente nosotros debemos contar cosas que pueden ser descritas más naturalmente como pares de objetos, que como objetos simples. Suponga, por ejemplo, que el Departamento de Matemática de la Universidad de Folornia está calculando la carga docente para el corriente año. Para hacer esto el profesor McBrain hace una tabla como la Tabla 1

	Cálculo	Matemática Discreta	Álgebra
Angus	*	*	
Benjamín		*	*
Clara	*	*	
...			
Zoot	*	*	*

Cuadro 1

En la tabla, cada fila corresponde a un estudiante, cada columna corresponde a un curso, y si el estudiante x toma el curso y entonces un asterisco es colocado en la posición (x, y) de la tabla. El número total de asteriscos es la carga docente del departamento. En otras palabras, el problema es contar el conjunto S de pares (x, y) tales que el alumno x esta tomando el curso y. En general, dados dos conjuntos X e Y podemos definir el **conjunto producto** $X \times Y$ como el conjunto de *todos* los pares ordenados (x, y), así que el problema general es contar un subconjunto S de $X \times Y$.

Por la tabla del profesor McBrain es claro que hay dos formas de hacer el cálculo. Podemos contar el número de cursos tomados por cada alumno y sumar los resultados, o podemos contar el número de estudiantes que toman cada curso y sumar los resultados. Naturalmente, recibiremos la misma respuesta por cualquier método.

Podemos precisar más aún estas ideas de la siguiente manera. supongamos que un subconjunto S de $X \times Y$ es especificado por los asteriscos en una tabla como la del profesor McBrain, como en la Tabla 2.

	$\cdot$	$\cdot$	$\cdot$	y	$\cdots$	Total fila
$\cdot$	$*$		$*$		$*$	$\cdot$
$\cdot$						$\cdot$
$\cdot$		$*$		$*$		$\cdot$
x	$*$	$*$			$*$	$r_x(S)$
$\cdot$		$*$	$*$	$*$		$\cdot$
$\cdot$						$\cdot$
$\cdot$	$*$				$*$	$\cdot$
Total columna	$\cdot$	$\cdot$	$\cdot$	$c_r(S)$	$\cdots$	$\lvert S\rvert$

Cuadro 2

El primer método es contar los asteriscos en la fila x y encontrar el total de la fila $r_x(S)$, para cada x en X. El total entonces se obtiene sumando los totales de las filas, que es

$$|S| = \sum_{x \in X} r_x(S).$$

El segundo método es contar las marcas en la columna y encontrar el total de la columna $c_y(S)$, para cada y en Y. En este caso el total es obtenido sumando todos los totales de la columnas: w

$$|S| = \sum_{y \in Y} c_y(S).$$

El hecho de que tengamos dos expresiones distintas para $|S|$ es comúnmente usado en la práctica para controlar la aritmética. El mismo hecho puede también ser útil en la teoría, porque a veces podemos derivar resultados bastantes inesperados igualando ambas expresiones. Pero, antes de ir a las aplicaciones, debemos formular el principio y algunas de sus consecuencias inmediatas como un teorema.

Teorema 7.1.1. *Sea X e Y conjuntos finitos no vacíos, y sea S un subconjunto de $X \times Y$. Entonces valen los siguientes resultados.*

(i) El cardinal de S es dado por

$$|S| = \sum_{x \in X} r_x(S) = \sum_{y \in Y} c_y(S),$$

donde $r_x(S)$ y $c_y(S)$ son los totales de las filas y columnas descritos antes.

(ii) Si $r_x(S)$ es una constante r, independiente de x, y $c_y(S)$ es una constante c, independiente de y, entonces

$$r|X| = c|Y|.$$

(iii) (El principio de multiplicación) El cardinal de $X \times Y$ es dado por

$$|X \times Y| = |X| \times |Y|.$$

DEMOSTRACIÓN. (i) El "conjunto de asteriscos en la fila x" puede ser definido formalmente como el conjunto de pares en S cuyo primer componente es x, entonces $r_x(S)$ es el cardinal de ese conjunto. Como estos conjuntos (los $r_x(S)$) son disjuntos, el hecho de que $|S|$ es igual a la suma de los números $r_x(S)$ se sigue del principio de adición. El resultado para el total de las columnas se prueba del mismo modo.

(ii) Si $r_x(S) = r$ para todo x que pertenece a S, entonces hay $|X|$ términos en la primera expresión para $|S|$ y cada uno de ellos es igual a r. Por lo tanto,

$$|S| = r|X|.$$

Del mismo modo, $|S| = c|Y|$, y se deduce el resultado.

(iii) En el caso especial $S = X \times Y$, el total de la fila es $r_x(S) = |Y|$, para cada x en X. Por lo tanto, por (ii), $|X \times Y| = |X| \times |Y|$. □

EJEMPLO 7.1.1. Supongamos que el profesor McBrain ha decretado que, por conveniencias administrativas, cada estudiante deberá asistir a exactamente cuatro de los siete cursos disponibles. Los reportes de asistencia indican que el numero de personas que asistieron a los cursos fueron 52, 30, 30, 20, 25, 12, 18. ¿Qué conclusión podemos sacar?

DEMOSTRACIÓN. Sea n el numero total de estudiantes. Como se supone que cada alumno debe asistir a cuatro cursos, la carga docente total calculada por el método "totales de filas" es $4n$. Por otro lado, los reportes de asistencia dan "totales de columnas", deberíamos entonces tener

$$4n = 52 + 30 + 30 + 20 + 25 + 12 + 18 = 187.$$

Pero esto es imposible, pues 187 no es divisible por 4. Debemos descartar la posibilidad de que los reportes sean erróneos, entonces la única conclusión valida es que algunos estudiantes están salteando clases. Por supuesto, así fue. □

7.1.1. Ejercicios.

1. En la clase de cálculo de la Dra. Cynthia Agnes, 32 de los estudiantes son muchachos. Cada muchacho conoce cinco de las chicas de la clase y cada chica conoce ocho de los muchachos. ¿Cuántas chicas hay en la clase?
2. Supongamos que tenemos algunos subconjuntos de $\mathbb{N}_8$, con la propiedad que cada uno tiene cuatro elementos, y que cada elemento de $\mathbb{N}_8$ pertenece a exactamente tres de estos subconjuntos. ¿Cuántos subconjuntos hay? Encontrar una colección de subconjuntos de $\mathbb{N}_8$ que satisfaga lo anterior.
3. ¿Es posible encontrar una colección de subconjuntos de $\mathbb{N}_8$ tales que cada uno tenga tres elementos y cada elemento pertenezca exactamente a cinco de ellos?

4. Si $X_1, X_2, \ldots, X_n$ son conjuntos, el **conjunto producto** $X_1 \times X_2 \times \cdots \times X_n$ es definido como el conjunto de todas las n-uplas ordenadas $(x_1, x_2, \ldots, x_n)$, con $x_i \in X_i$ $(1 \leq i \leq n)$. Use el principio de inducción para probar que

$$|X_1 \times X_2 \times \cdots \times X_n| = |X_1| \times |X_2| \times \cdots \times |X_n|.$$

5. En un lenguaje simple hay 26 letras y cada palabra tiene cuatro letras. Cualquier disposición de las letras, incluyendo repeticiones, es permitido. ¿Cuántas palabras hay? ¿Cuantas palabras hay que no contengan la letra b?

7.2. El principio del tamiz

El principio más básico del conteo (Teorema 3.1) dice que $|A \cup B|$ es la suma de $|A|$ y $|B|$, cuando A y B son conjuntos disjuntos. Si A y B no son disjuntos, cuando sumamos $|A|$ y $|B|$ estamos contando $A \cap B$ dos veces. Entonces, para obtener la respuesta correcta debemos restar $|A \cap B|$:

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

Un método similar puede aplicarse a tres conjuntos. Cuando sumamos $|A|$, $|B|$ y $|C|$, los elementos de $A \cap B$, $B \cap C$, y $C \cap A$ son contados dos veces (si no están en los tres conjuntos). Para corregir esto, restamos $|A \cap B|$, $|B \cap C|$ y $|C \cap A|$. Pero ahora los elementos de $A \cap B \cap C$, contados originalmente tres veces, han sido descontados tres veces. Luego, para conseguir la respuesta correcta, debemos sumar $|A \cap B \cap C|$. Así

$$|A \cup B \cup C| = \alpha_1 - \alpha_2 + \alpha_3,$$

donde

$$\alpha_1 = |A| + |B| + |C|, \qquad \alpha_2 = |A \cap B| + |B \cap C| + |C \cap A|,$$
$$\alpha_3 = |A \cap B \cap C|.$$

Este resultado es un caso simple de lo que suele ser llamado, por razones obvias, el principio de inclusión y exclusión. También se lo llama el *principio del tamiz*.

TEOREMA 7.2.1. *Si $A_1, A_2, \ldots, A_n$ son conjuntos finitos, entonces*

$$|A_1 \cup A_2 \cup \ldots \cup A_n| = \alpha_1 - \alpha_2 + \alpha_3 + \cdots + (-1)^n \alpha_n,$$

donde α_i es la suma de los cardinales de las intersecciones de los conjuntos tomados de a i por vez ($1 \leq i \leq n$).

DEMOSTRACIÓN. Debemos demostrar que cada elemento x de la unión hace una contribución neta de 1 al miembro de la derecha. Supongamos que x pertenece a k de los conjuntos $A_1, A_z, \ldots, A_n$. Entonces x contribuye con k en la suma $\alpha_1 = |A_1| + \cdots + |A_n|$. En la suma α_2, x contribuye 1 en $|A_i \cap A_j|$ cuando A_i y A_j están entre los k conjuntos que contienen a x. Existen $\binom{k}{2}$ de esos pares, por lo tanto $\binom{k}{2}$ es la contribución de x a α_2. En general la contribución de x

a α_i $(1 \leq i \leq n)$ es $\binom{k}{i}$. Por lo tanto el total con que contribuye x al lado derecho de la igualdad es

$$\binom{k}{1} - \binom{k}{2} + \cdots + (-1)^{k-1}\binom{k}{k},$$

porque los términos con $i > k$ dan cero.

Por el teorema del binomio aplicado a $(1-1)^k = 0$, se deduce que la expresión de arriba es igual a $\binom{k}{0}$, que vale 1. □

Un corolario simple del Teorema 7.2.1 es a menudo más útil en la práctica. Supongamos que $A_1, A_2, \ldots, A_n$ son subconjuntos de un conjunto dado X con $|X| = N$. Entonces el número de elementos de X que no están en ninguno de esos subconjuntos es

$$\begin{aligned} |X - (A_1 \cup A_2 \cup \ldots \cup A_n)| &= |X| - |A_1 \cup A_2 \cup \ldots \cup A_n| \\ &= N - \alpha_1 + \alpha_2 - \cdots + (-1)^n \alpha_n. \end{aligned}$$

Ejemplo 7.2.1. Hay 73 estudiantes en el primer año de la Escuela de Artes de la Universidad de Folornia. De ellos, 52 saben tocar el piano, 25 el violin y 20 la flauta; 17 pueden tocar tanto el piano como el violin, 12 el piano y la flauta; pero solo Osbert Smugg puede tocar los tres instrumentos ¿Cuántos alumnos no saben tocar ninguno de esos instrumentos?

Demostración. Con V, P y F denotaremos los conjuntos de estudiantes que saben tocar el violin, el piano y la flauta respectivamente. Usando la información dada tenemos que

$$\begin{aligned} \alpha_1 &= |P| + |V| + |F| = 52 + 25 + 20 = 97 \\ \alpha_2 &= |P \cap V| + |V \cap F| + |P \cap F| = 17 + 7 + 12 = 36 \\ \alpha_3 &= |P \cap V \cap F| = 1. \end{aligned}$$

Por consiguiente, el número de estudiantes que o pertenecen a ninguno de los tres conjuntos P, V y F es

$$73 - 97 + 36 - 1 = 11.$$

□

Ejemplo 7.2.2. Ejemplo Una secretaria ineficiente tiene n cartas distintas y n sobres con direcciones ¿De cuántas maneras puede ella arreglárselas para meter cada carta en un sobre equivocado? (Esto es comúnmente llamado el *problema del desarreglo* del cual hay varias formulaciones pintorescas.)

Demostración. Podemos considerar cada carta y su correspondiente sobre como si estuvieran etiquetadas con un entero i en el rango $1 \leq i \leq n$. El acto de poner las cartas en los sobres puede describirse como una permutación π de $\mathbb{N}_n$: $\pi(i) = j$ si la carta i va en el sobre j. Necesitamos saber el número de **desarreglos**, esto es, las permutaciones π tales que $\pi(i) \neq i$ para todo i en $\mathbb{N}_n$.

Denotemos A_i $(1 \leq i \leq n)$ el subconjunto de S_n (el conjunto de permutaciones de $\mathbb{N}_n$) que contiene aquellos π tales que $\pi(i) = i$. Diremos que los elementos de A_i *fijan* i. Por el principio del tamiz, el número de desarreglos es

$$d_n = n! - \alpha_1 + \alpha_2 - \cdots + (-1)^n \alpha_n,$$

donde α_r es la suma de los cardinales de las intersecciones de los A_i tomando r por vez. En otras palabras, α_r es el número de permutaciones que fijan r símbolos dados, tomando todas las maneras de elegir los r símbolos. Ahora hay $\binom{n}{r}$ maneras de elegir r símbolos, y el número de permutaciones que los fijan es solo el número de permutaciones de los restantes $n - r$ símbolos, que es $(n - r)!$ Por lo tanto

$$\alpha_r = \binom{n}{r}(n-r)! = \frac{n!}{r!}, \qquad d_n = n!\left(1 - \frac{1}{1!} + \frac{1}{2!} - \cdots + (-1)^n \frac{1}{n!}\right).$$

□

7.2.1. Ejercicios.

1. En una clase de 67 estudiantes de matemática, 47 leen francés, 35 leen alemán y 23 leen ambos lenguajes ¿Cuántos estudiantes no lee ninguno de los dos lenguajes? Si además 20 leen ruso, de los cuales 12 también leen francés, 11 leen alemán y 5 leen los tres lenguajes, ¿cuántos estudiantes no leen ninguno de los tres lenguajes?
2. Encuentre el número de formas de ordenar las letras A,E,M,O,U,Y en una secuencia de tal forma que las palabras ME e YOU no aparezcan.
3. Calcule el número d_4 de desarreglos de $\{1, 2, 3, 4\}$ y escriba, en la notación cíclica, las permutaciones relevantes.
4. Use el principio de inducción para probar que la fórmula para d_n satisface la recursión

$$d_1 = 0, \quad d_2 = 1, \quad d_n = (n-1)(d_{n-1} + d_{n-2}) \ (n \geq 3).$$

5. Probar que el número de desarreglos de $\{1, 2, \ldots, n\}$ en el cual un objeto dado (digamos el 1) está en un 2-ciclo es $(n-1)d_{n-2}$. Utilizando esto dar una prueba directa de la fórmula recursiva del ejercicio anterior.

CAPíTULO 8

Apéndice II
La función de Euler

8.1. La función de Euler

En esta sección probaremos un útil e importante teorema, usando sólo los conceptos de conteo más básicos.

El teorema se refiere a las propiedades de divisibilidad de los enteros. Recordemos que dos enteros x e y son *coprimos* si el $\mathrm{mcd}(x, y) = 1$. Por cada $n \geq 1$ sea $\phi(n)$ el número de enteros x en el rango $1 \leq x \leq n$ tal que x y n son coprimos. Podemos calcular los primeros valores de $\phi(n)$ haciendo una tabla (Tabla 1).

n	Coprimos a n	$\phi(n)$
1	1	1
2	1	1
3	1, 2	2
4	1, 3	2
5	1, 2, 3, 4	4
6	1, 5	2
7	1, 2, 3, 4, 5, 6	6
8	1, 3, 5, 7	4

CUADRO 1

	f	1	2	3	4	5	6	7	8	9	10	11	12	$\phi(d)$
d														
1		12												1
2		6												1
3		4	8											2
4		3		9										2
6		2				10								2
12		1				5		7				11		4
														12

Cuadro 2

La función es llamada **función de Euler**, debido a Leonhard Euler (1707-1783). Cuando n es primo, digamos $n = p$, cada uno de los enteros $1, 2, \ldots, p-1$ es coprimo con p, entonces tenemos

$$\phi(p) = p - 1 \qquad (p \text{ primo}).$$

Nuestra tarea ahora es probar un resultado respecto a la suma de los valores $\phi(d)$, donde los d son todos los divisores de un número positivo n dado. Por ejemplo, cuando $n = 12$, lo divisores d son 1, 2, 3, 4, 5, 6 y 12, podemos ver que

$$\begin{aligned} &\phi(1) + \phi(2) + \phi(3) + \phi(4) + \phi(6) + \phi(12) \\ &= 1 + 1 + 2 + 2 + 2 + 4 \\ &= 12. \end{aligned}$$

Debemos demostrar que la suma es siempre igual al entero n dado.

Teorema 8.1.1. *Para cualquier n entero positivo,*

$$\sum_{d|n} \phi(d) = n.$$

Demostración. Sea S el conjunto de pares de enteros (d, f) que satisfacen

$$d|n, \qquad 1 \le f \le d, \qquad \text{mcd}(f, d) = 1.$$

La Tabla 2 muestra S cuando $n = 12$; la "marca" que indica que (d, f) pertenece a S es un número cuya importancia explicaremos en seguida. Por lo general, el número de "marcas" en la

fila d es el número de f's en el rango $1 \leq f \leq d$ que satisfacen que el $\text{mcd}(d, f) = 1$; esto es $\phi(d)$. Por lo tanto, contando S por el método de las filas obtenemos

$$|S| = \sum_{d|n} \phi(d).$$

Para demostrar que $|S| = n$ debemos construir una biyección β de S en $\mathbb{N}_n$. Dado un par (d, f) en S, definimos

$$\beta(d, f) = fn/d.$$

En la tabla, $\beta(d, f)$ es la "marca" en la fila d y la columna f. Como $d|n$, el valor de β, es un entero y como $1 \leq f \leq d$, entonces $\beta(d, f)$ pertenece a $\mathbb{N}_n$.

Para probar que β es una inyección observemos que

$$\beta(d, f) = \beta(d', f') \quad \Rightarrow \quad fn/d = f'n/d' \quad \Rightarrow \quad fd' = f'd.$$

Pero f y d son coprimos, así como también lo son f' y d', así que podemos concluir (como en el ejemplo de la sección 1.7) que $d = d'$ y $f = f'$.

Para demostrar que β es una suryección, supongamos que nos dan un x que pertenece a $\mathbb{N}_n$. Sea g_x el mcd de x y n, y sea

$$d_x = n/g_x, \qquad f_x = x/g_x.$$

Puesto que g_x es un divisor de x y n, entonces d_x y f_x son enteros, y como g_x es el mcd, d_x y f_x son coprimos. Ahora

$$\beta(d_x, f_x) = f_x n/d_x = x,$$

y por lo tanto β es suryectiva.

Luego β es biyectiva y $|S| = n$, como queríamos demostrar. □

8.1.1. Ejercicios.

1. Encontrar los valores de $\phi(19), \phi(20), \phi(21)$.
2. Probar que si x y n son coprimos, entonces lo son $n - x$ y n. Deducir que $\phi(n)$ es par para todo $n \geq 3$.
3. Probar que, si p es un primo y m es un entero positivo, entonces un entero x en el rango $1 \leq x \leq p^m$ *no* es coprimo a p^m si y solo si es un múltiplo de p. Deducir que $\phi(p^m) = p^m - p^{m-1}$.
4. Encontrar un contraejemplo que confirme que es falsa la conjetura $\phi(ab) = \phi(a)\phi(b)$, para enteros cualesquiera a y b. Trate de modificar la conjetura de tal forma que no pueda encontrar un contraejemplo.
5. Probar que para cualesquiera enteros positivos n y m se cumple:

$$\phi(n^m) = n^{m-1}\phi(n).$$

6. Calcular $\phi(1000)$ y $\phi(1001)$.

8.2. Una aplicación aritmética del principio del tamiz

Por cientos de años los matemáticos han estudiado problemas sobre números primos y la factorización de los enteros. Nuestra breve discusión sobre estos temas en los primeros capítulos debería haber convencido al lector de que estos problemas son difíciles, porque los primos mismos se encuentran irregularmente distribuidos, y porque no hay una forma directa de encontrar la factorización en primos de un entero dado. De todos modos, si se nos da la factorización en primos de un entero, es relativamente fácil responder ciertas preguntas sobre sus propiedades aritméticas. Supongamos, por ejemplo que queremos listar todos los divisores de un entero n y sabemos que la factorización de n es

$$n = p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r}.$$

Entonces un entero d es divisor de n si y solo si no tiene divisores primos distintos de los de n, y ningún primo divide más veces a d que a n. Visto así, los divisores son precisamente los enteros que pueden escribirse de la forma

$$d = p_1^{f_1} p_2^{f_2} \cdots p_r^{f_r},$$

donde cada f_i $(1 \leq i \leq r)$ satisface $0 \leq f_i \leq e_i$. Por ejemplo dado que $60 = 2^2 \times 3 \times 5$ podemos listar rápidamente todos los divisores de 60.

Un problema similar es encontrar el número de enteros x en el rango $1 \leq x \leq n$ que son coprimos con n. En la sección 8.1 denotamos este número con $\phi(n)$, el valor de la función ϕ de Euler en n. Ahora demostraremos que si la factorización en primos de n es conocida, entonces $\phi(n)$ puede ser calculado por el principio del tamiz.

Ejemplo 8.2.1. ¿Cuál es el valor de $\phi(60)$? En otras palabras, ¿cuántos enteros x en el rango $1 \leq x \leq 60$ satisfacen $\text{mcd}(x, 60) = 1$?

Demostración. Sabemos que $60 = 2^2 \times 3 \times 5$, así que podemos contar el números de enteros x en el rango $1 \leq x \leq 60$ que no son divisibles por 2, 3 o 5. Con $A(2)$ denotemos el subconjunto de $\mathbb{N}_{60}$ que contiene los enteros que *son* divisibles por 2, con $A(2,3)$ aquellos que *son* divisibles por 2 y 3, y así sucesivamente, entonces tenemos

$$\begin{aligned}\phi(60) &= 60 - |A(2) \cup A(3) \cup A(5)| \\ &= 60 - |A(2) + A(3) + A(5)| \\ &\quad + (|A(2,3) + |A(2,5)| + |A(3,5)|) - |A(2,3,5)|,\end{aligned}$$

por el principio del tamiz. Ahora $|A(2)|$ es el número de múltiplos de 2 en $\mathbb{N}_{60}$ que es $60/2 = 30$. Del mismo modo $|A(2,3)|$ es el número de múltiplos de 2×3, que es $60/(2 \times 3) = 10$, y así siguiendo, por lo tanto

$$\phi(60) = 60 - (30 + 20 + 10) + (10 + 6 + 4) - 2 = 16.$$

□

El mismo método puede ser usado para dar una fórmula explícita para $\phi(n)$ en el caso general.

TEOREMA 8.2.1. *Sea $n \geq 2$ un entero cuya factorización es $n = p_1^{e_1} p_2^{e_2} \dots p_r^{e_r}$. Entonces*

$$\phi(n) = n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)\cdots\left(1 - \frac{1}{p_r}\right).$$

DEMOSTRACIÓN. Denotemos A_j el subconjunto de $\mathbb{N}_n$ que contiene los múltiplos de p_j ($1 \leq j \leq r$). Entonces

$$\begin{aligned}\phi(n) &= n - |A_1 \cup A_2 \cup \cdots \cup A_r| \\ &= n - \alpha_1 + \alpha_2 - \cdots + (-1)^r \alpha_r\end{aligned}$$

donde α_i es la suma de los cardinales de las intersecciones de los conjuntos tomados de a i. Una intersección típica como

$$A_{j_1} \cup A_{j_2} \cup \cdots \cup A_{j_i}$$

contiene los múltiplos de $P = p_{j_1} \times p_{j_2} \times \cdots \times p_{j_i}$ en $\mathbb{N}_n$, y estos son los números

$$P, 2P, 3P, \dots, \left(\frac{n}{p}\right) P.$$

Luego la cardinalidad de una intersección típica es n/P, y α_i es la suma de términos como

$$\frac{n}{P} = n\left(\frac{1}{p_{j_1}}\right)\left(\frac{1}{p_{j_2}}\right)\cdots\left(\frac{1}{p_{j_i}}\right).$$

Se sigue que

$$\begin{aligned}\phi(n) = n - n\left(\frac{1}{p_1} + \frac{1}{p_2} + \cdots + \frac{1}{p_r}\right) + n\left(\frac{1}{p_1 p_2} + \frac{1}{p_1 p_3} + \cdots\right) + \cdots \\ \cdots + (-1)^r \left(\frac{1}{p_1 p_2 \cdots p_r}\right) \\ = n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)\cdots\left(1 - \frac{1}{p_r}\right).\end{aligned}$$

□

CAPíTULO 9

Apéndice III
Permutaciones

9.1. Permutaciones

Una **permutación** de un conjunto finito no vacío X es una biyección de X en X. (Frecuentemente tomamos X como $\mathbb{N}_n = \{1, 2, \ldots, n\}$.) Por ejemplo una permutación típica de $\mathbb{N}_5$ es la función α definida por las ecuación

$$\alpha(1) = 2, \quad \alpha(2) = 4, \quad \alpha(3) = 5, \quad \alpha(4) = 1, \quad \alpha(5) = 3.$$

Una biyección de un conjunto finito en si mismo es necesariamente una inyección, y al mismo tiempo cualquiera de estas inyecciones va a ser una biyección (ejercicio 2.6 (3)). De esta forma, el numero de permutaciones de un n-conjunto es el mismo que el número de inyecciones de $\mathbb{N}_n$ en si mismo, y por el Teorema 3.5.1 este número es

$$n(n-1)(n-2)\cdots 1 = n!.$$

Denotemos el conjunto de todas las permutación de $\mathbb{N}_n$ con S_n. Por ejemplo, S_3 contiene las $3! = 6$ permutaciones siguientes:

$$\begin{array}{ccc} 1 & 2 & 3 \\ \downarrow & \downarrow & \downarrow \\ 1 & 2 & 3 \end{array} \quad \begin{array}{ccc} 1 & 2 & 3 \\ \downarrow & \downarrow & \downarrow \\ 1 & 3 & 2 \end{array} \quad \begin{array}{ccc} 1 & 2 & 3 \\ \downarrow & \downarrow & \downarrow \\ 2 & 1 & 3 \end{array} \quad \begin{array}{ccc} 1 & 2 & 3 \\ \downarrow & \downarrow & \downarrow \\ 2 & 3 & 1 \end{array} \quad \begin{array}{ccc} 1 & 2 & 3 \\ \downarrow & \downarrow & \downarrow \\ 3 & 1 & 2 \end{array} \quad \begin{array}{ccc} 1 & 2 & 3 \\ \downarrow & \downarrow & \downarrow \\ 3 & 2 & 1 \end{array}$$

En la práctica, usualmente asignamos alguna interpretación concreta a un elemento de S_n. Como en el sección previa, podemos usar la interpretación "selecciones ordenadas sin repetición" donde, en este caso seleccionamos los elementos de $\{1, 2, 3, \ldots, n\}$ en algún orden hasta que no queda ninguno. Una interpretación relacionada es que una permutación efectúa un *reacomodamiento* de $\{1, 2, 3, \ldots, n\}$; por ejemplo, la permutación α vista más arriba efectúa el reacomodamiento de 12345, en 24513, así:

$$\begin{array}{ccccc} 1 & 2 & 3 & 4 & 5 \\ \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\ 2 & 4 & 5 & 1 & 3 \end{array}$$

En algunas circunstancias es conveniente mirar una permutación y el correspondiente reacomodamiento como la misma cosa, pero esto puede traer dificultades si debemos considerar sucesivos reacomodamientos. Es importante tener en cuenta que

una permutación es una función con ciertas características.

Cuando las permutaciones son tratadas como funciones es claro como deben combinarse. Consideremos α la permutación de $\mathbb{N}_5$ antes mencionada, y sea β la permutación de $\mathbb{N}_5$ dada por

$$\beta(1) = 3, \quad \beta(2) = 5, \quad \beta(3) = 1, \quad \beta(4) = 4, \quad \beta(5) = 2.$$

La función compuesta $\beta\alpha$ es la permutación definida por $\beta\alpha(i) = \beta(\alpha(i))$ $(1 \leq i \leq 5)$, esto es

$$\beta\alpha(1) = 5, \quad \beta\alpha(2) = 4, \quad \beta\alpha(3) = 2, \quad \beta(4)\alpha = 3, \quad \beta\alpha(5) = 1.$$

(Recordemos que, como siempre, $\beta\alpha$ significa "primero α, entonces β".) En términos de reacomodamientos tenemos

$$\begin{array}{cccccc} & 1 & 2 & 3 & 4 & 5 \\ \alpha & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\ & 2 & 4 & 5 & 1 & 3 \end{array}$$

$$\begin{array}{cccccc} & 1 & 2 & 3 & 4 & 5 \\ \beta & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow. \\ & 5 & 4 & 2 & 3 & 1 \end{array}$$

Existen cuatro características de la composición de permutaciones de gran importancia, y están listadas en el próximo teorema.

TEOREMA 9.1.1. *Las siguientes propiedades valen en el conjunto S_n de todas las permutaciones de $\{1, 2, 3, ..., n\}$.*

(i) *Si π y σ pertenecen a S_n, entonces $\pi\sigma$ también.*

(ii) *Para cualesquiera permutaciones π, σ, τ en S_n,*

$$(\pi\sigma)\tau = \pi(\sigma\tau).$$

(iii) *La función identidad, denotada por* id *y definida por* $\mathrm{id}(r) = r$ *para todo r en $\mathbb{N}_n$, es una permutación y para cualquier σ en S_n, tenemos*

$$\mathrm{id}\,\sigma = \sigma\,\mathrm{id} = \sigma.$$

(iv) *Para toda permutación π en S_n hay una permutación inversa π^{-1} en S_n tal que*

$$\pi\pi^{-1} = \pi^{-1}\pi = \mathrm{id}\,.$$

Demostración. La afirmación (i) se sigue inmediatamente del hecho de que la composición de dos biyecciones es una biyección (Teorema 2.2.1), y la afirmación (ii) una propiedad estándar de la composición (ejercicio 2.1.1 (4)). La afirmación (iii) es obvia, y la afirmación (iv) se sigue del hecho de que toda biyección tiene una inversa (Teorema 2.2.2).

□

Es conveniente tener una notación más compacta para las permutaciones. Consideremos otra vez la permutación α de $\{1, 2, 3, 4, 5\}$, y notemos en particular que

$$\alpha(1) = 2, \qquad \alpha(2) = 4, \qquad \alpha(4) = 1.$$

Así α lleva 1 a 2, 2 a 4 y 4 a 1, y por esta razón decimos que los símbolos 1,2,4 forma un *ciclo* (de longitud 3). Del mismo modo, los símbolos 3 y 5 forman un ciclo de longitud 2, y escribimos:

$$\alpha = (1\,2\,4)(3\,5).$$

Esta es la *notación cíclica* para α. Cualquier permutación π puede ser escrita cíclicamente de la siguiente manera:

> comencemos con algún símbolo (digamos el 1) y veamos el efecto de π sobre él y sus sucesores hasta que alcancemos el 1 nuevamente;
> elijamos un símbolo que todavía no haya aparecido y construyamos el ciclo que se deriva de él;
> repitamos el procedimiento hasta que se terminen los símbolos.

Por ejemplo, la permutación β definida antes tiene la notación cíclica

$$\beta = (1\,3)(2\,5)(4),$$

donde observamos que el símbolo 4 forma un ciclo "degenerado" por sí solo, puesto que $\beta(4) = 4$. En algunas ocasiones podemos omitir estos ciclos de longitud 1 cuando escribimos una permutación en notación cíclica, puesto que corresponden a símbolos que no son afectados por la permutación. Sin embargo, usualmente es útil *no* adoptar esta convención hasta que uno se familiariza con la notación.

Aunque la representación de una permutación en notación cíclica es esencialmente única, hay dos manera obvias en las que podemos cambiar la notación sin alterar la permutación. Primero, cada ciclo puede empezar en cualquiera de sus símbolos; por ejemplo $(7\,8\,2\,1\,3)$ y $(1\,2\,7\,8\,2)$ describen el mismo ciclo. Segundo, el orden de los ciclos no es importante; por ejemplo $(1\,2\,4)(3\,5)$ y $(3\,5)(1\,2\,4)$ denotan la misma permutación. Pero las características importantes son el número de ciclos, la longitud del ciclo, y la disposición de los símbolos dentro de los ciclos, y éstas están determinadas de manera única. Por eso, la rotación cíclica nos dice bastantes cosas útiles sobre una permutación.

Ejemplo 9.1.1. Cartas numeradas del 1 al 12 son distribuidas en una mesa en la manera en que se muestra en la parte izquierda de la tabla que sigue. Luego las cartas son levantadas por

filas (de izquierda a derecha y de arriba hacia abajo) y se redistribuyen con el mismo arreglo, pero por columnas, no por filas (de arriba hacia abajo y de izquierda a derecha), apareciendo como se muestra en la parte derecha de la tabla.

$$\begin{array}{cccc} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 7 & 8 & 9 \\ 10 & 11 & 12 \end{array} \qquad\qquad \begin{array}{ccc} 1 & 5 & 9 \\ 2 & 6 & 10 \\ 3 & 7 & 11 \\ 4 & 8 & 12 \end{array}$$

¿Cuántas veces debe repetirse este procedimiento hasta que las cortas aparezcan dispuestas como estaban inicialmente?

DEMOSTRACIÓN. Sea π la permutación que efectúa el reordenamiento; esto es $\pi(i) = j$ si la carta j aparece en la posición previamente ocupada por la carta i. Trabajando con la notación cíclica para π encontramos que

$$\pi = (1)(2\ 5\ 6\ 10\ 4)(3\ 9\ 11\ 8\ 7)(12).$$

Los ciclos degenerados (1) y (12) indican que las cartas 1 y 12 nunca cambian de posición. Las otros ciclos tienen longitud 5, así que cuando el proceso se haya realizado 5 veces las cartas reaparecerán en sus posiciones originales. Otra forma de expresar el resultado es decir que $\pi^5 = \mathrm{id}$, donde π^5 representa las cinco repeticiones de la permutación π. □

9.2. Ejercicios

1. Escribir en notación cíclica la permutación que realiza el siguiente reordenamiento:

$$\begin{array}{ccccccccc} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\ 3 & 5 & 7 & 8 & 4 & 6 & 1 & 2 & 9 \end{array}.$$

2. Sean σ y τ las permutaciones de $\{1, 2, \ldots, 8\}$ cuyas representaciones en la notación cíclica son

$$\sigma = (1\,2\,3)(4\,5\,6)(7\,8), \qquad \tau = (1\,3\,5\,7)(2\,6)(4)(8).$$

   Escribir en notación cíclica $\sigma\tau$, $\tau\sigma$, σ^2, σ^{-1}, τ^{-1}.
3. Resolver el problema presentado en el *Ejemplo* cuando hay 20 cartas acomodadas en 5 filas de 4.
4. Probar que hay exactamente tres elementos de S_4 que tienen dos ciclos de longitud 2, escritos en la notación cíclica.
5. Sea K el subconjunto de S_4 que contiene la identidad y las tres permutaciones descritas en el ejercicio previo. Escribir la "tabla de multiplicación" para K, interpretando la multiplicación como la composición de permutaciones.

6. Calcular en número total de permutaciones σ de $\mathbb{N}_6$ que satisfacen $\sigma^2 = \text{id}$ y $\sigma \neq \text{id}$.
7. Sean α y β permutaciones de $\mathbb{N}_9$ cuyas representaciones en la notación cíclica son:

$$\alpha = (1237)(49)(58)(6), \qquad \beta = (135)(246)(789).$$

   Escribir en notación cíclica $\alpha\beta$, $\beta\alpha$, α^2, β^2, α^{-1}, β^{-1}.
8. Sea $X_1 = \{0, 1\}$, y para $i \geq 2$ definamos X_i como el conjunto de subconjuntos de X_{i-1}. Encontrar el valor más pequeño para el cual $|X_i| > 10^{100}$.
9. Por cada entero i en el rango $1 \leq i \leq n-1$ definimos τ_i como la permutación de $\mathbb{N}_n$ que intercambia i e $i+1$ y no afecta los otros elementos. Explícitamente

$$\tau_i = (1)(2)\cdots(i-1)(i\ i+1)(i+2)\cdots(n).$$

   Probar que toda permutación de $\mathbb{N}_n$ puede ser expresada en términos de $\tau_1, \tau_2, \ldots, \tau_{n-1}$.
10. Una permutación de $\mathbb{N}_n$ que tenga solo un ciclo (necesariamente de longitud n) es llamada *cíclica* . Probar que hay $(n-1)!$ permutaciones cíclicas de $\mathbb{N}_n$.
11. Un mazo de 52 cartas es dividido en dos partes iguales y luego se alternan las cartas de una y otra parte. Es decir si la numeración original era $1, 2, 3, \ldots, 54$, el nuevo orden es $1, 27, 2, 28, \ldots$¿Cuántas veces se debe repetir este procedimiento para obtener de nuevo el mazo original?

CAPíTULO 10

Apéndice IV
Grafos planares

Daniel Penazzi

10.1. Grafos Planares

Usualmente el diagrama de un grafo se realiza en el plano por la comodidad que esto representa. Esto no significa que todo grafos sea lo que se denomina un **grafo planar**. ¿Qué es un grafo planar? Es un grafo tal que *existe* un diagrama del grafo en el plano tal que no hay ningún cruce de aristas. Por ejemplo, el grafo K_3 es claramente planar (Fig. 1 (a)). Claro que podríamos dibujar a K_3 como en la Fig. 1 (b) y no parecería planar.

(a) (b)

FIGURA 1. Dibujos de K_3

Pero la definición es que un grafo es planar si se **puede** dibujar en el plano sin cruces de aristas, no si **todo** dibujo no tiene cruces. (Si la definición fuera así, ningún grafo seria planar, pues siempre se puede dibujar cualquier grafo con cruces.) Otro ejemplo, ya visto, K_4 puede ser dibujado como en la Fig 2 (a) y no parece planar, pero dibujado como en la Fig. 2 (b) muestra que K_4 es planar.

(a) (b)

FIGURA 2. Dibujos de K_4

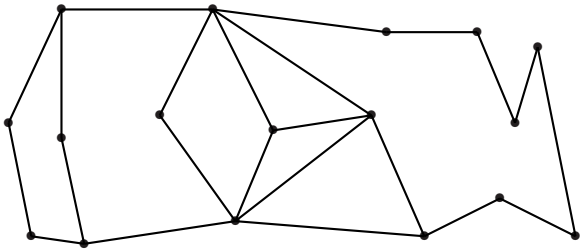


FIGURA 3. Un grafo planar

En vista de estos ejemplos, una pregunta es ¿existen grafos no planares? Por ejemplo si dibujáramos K_{16} parecería imposible que fuera planar, dada la gran cantidad de cortes, pero ¿cómo podemos estar seguros?

Observemos primero que si G es planar y H es subgrafo de G, entonces H es planar, pues, si podemos dibujar a G en el plano sin cortes de aristas, entonces H que esta "metido" en G, también puede ser así dibujado. Así, como ya vimos que K_4 es planar, sabemos que todo subgrafo de él es planar; es decir, todo grafo con cuatro o menos vértices es planar. Esta observación tiene consecuencias en la otra dirección también: si encontramos un grafo H que **no** sea planar, entonces todo grafo G que lo tenga como subgrafo deberá necesariamente ser no planar, pues si G fuera planar, H también lo seria. Así, si queremos probar que K_{16} no es planar, bastará con encontrar algún subgrafo mas sencillo de el que no lo sea. De hecho, probaremos que K_5 no es planar, con lo cual todos los grafos K_n, con $n \geq 5$ son no planares.

En lo que sigue veremos un arma poderosa para probar que un grafo es no planar: la llamada "fórmula de Euler". Supongamos que un grafo **sí** es planar. Escojamos un diagrama de él en el plano (puede haber muchos, escojamos uno). Este diagrama divide al plano en varias regiones. Por ejemplo, si G esta representado por el dibujo de la Fig. 3, entonces se obtienen regiones que numeraremos como en la Fig. 4 (1 es la región "exterior" a todo el grafo).

En realidad, también podríamos considerar a la región formada por las regiones 3 y 4 juntas, o 2, 5 y 6 juntas, etc. Pero nuestra preocupación estará centrada en una de estas regiones "simples", a las cuales llamaremos **caras**.

Observemos que no podemos hablar propiamente de las caras del grafo (aunque a veces lo haremos así) pues ellas son en realidad dependientes del diagrama, no del grafo. Sin embargo, algo puede decirse acerca de ellas:

TEOREMA 10.1.1. *(Fórmula de Euler) Sea G un grafo conexo, con v vértices, y e aristas. Supongamos que en algún diagrama planar de G, existen f caras. Entonces, $v - e + f = 2$.*

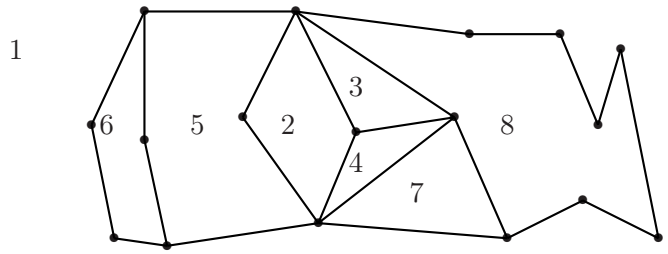


FIGURA 4. Regiones de un grafo planar

Antes de ver la prueba, observemos que, puesto que v y e dependen de G y no del diagrama, la fórmula de Euler dice que no importa como dibujemos a G en el plano (siempre y cuando esto sea posible), entonces siempre obtendremos $e - v + 2$ caras. Por lo tanto, el *número* de caras es algo independiente del diagrama, y podemos hablar del "número de caras de un grafo planar". Otra observación es que en el número de caras estamos contando la cara infinita, es decir, la exterior a todo el grafo. Finalmente, observemos que se pide que G sea conexo. La fórmula debe ser alterada en caso contrario.

DEMOSTRACIÓN DEL TEOREMA 10.1.1. Supongamos que la fórmula de Euler no sea cierta. Es decir, supongamos que existen grafos planares para los cuales la fórmula no es válida. Tomemos, de todos estos contraejemplos, alguno con e tan chico como sea posible, y llamemos G a ese grafo. Observemos que G debe tener por lo menos un ciclo, pues si fuera acíclico, como es conexo, sería un árbol. Ahora bien, en un árbol, $e = v - 1$. Además, por ser acíclico, no hay caras, salvo la cara infinita, es decir, f seria 1. Pero entonces $v - e + f = v - (v-1) + 1 = v - v + 1 + 1 = 2$ y G no sería un contraejemplo. Así pues, G tiene al menos un ciclo. Sea xy alguna arista perteneciente a algún ciclo, y consideremos $H = G - xy$. Como xy pertenece a algún ciclo, es una arista que separa dos caras en G. Esas dos caras ahora son una sola en H. (Ver Fig. 5).

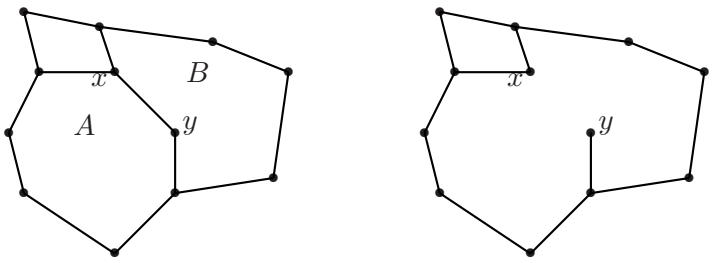


FIGURA 5. Eliminar una arista

Así, si f_H, e_H y v_H denotan el número de caras, aristas y vértices de H respectivamente, tenemos que $f_H = f - 1$. Además, como borramos una arista, $e_H = e - 1$, y como el número de vértices no cambia, $v_H = v$.

Pero, $e_H = e - 1$ es menor que e, y G era un contraejemplo con un número tan chico como fuera posible de aristas, por lo tanto, H no es un contraejemplo, es decir, $v_H - e_H + f_H = 2$. Reemplazando, obtenemos:

$$v - e + f = v_H - (e_H + 1) + f_H + 1 = v_H - e_H - 1 + f_H + 1 = v_H - e_H + f_H = 2,$$

lo cual dice que G no es un contraejemplo, absurdo. □

La fórmula de Euler es una herramienta muy poderosa en la teoría de grafos planares. Para empezar, permite probar que un grafo planar no puede tener muchas aristas, en relación a sus vértices

Corolario 10.1.2. *Sea G un grafo planar con al menos 3 vértices. Entonces, $e \leq 3v - 6$, donde e es el número de aristas y v el número de vértices de G.*

Demostración. Consideremos las caras de G. Si es una cara distinta de la cara infinita, es porque viene de un ciclo. Ahora bien, todo ciclo debe tener por lo menos 3 aristas, así que podemos concluir que hay por lo menos 3 aristas en el borde de esa cara. Si, en cambio, es la cara infinita y el grafo tiene más de tres aristas entonces "toca" 3 o más aristas. Si el grafo tiene menos de 3 aristas (y ningún ciclo), es uno de los de la Fig. 6. Como estamos suponiendo que hay al menos 3 vértices, en realidad solo hay que considerar el último caso, y ese tiene $e = 2$, $v = 3$, y $2 \leq 3 \times 3 - 6$.

Figura 6. Grafos acíclicos con menos de 3 aristas

Así pues, podemos suponer que en nuestro grafo, todas las caras tienen al menos 3 aristas en su borde. Es decir:

$$3 \leq \text{Número de aristas en el borde de cara 1}$$
$$3 \leq \text{Número de aristas en el borde de cara 2}$$
$$\vdots$$
$$3 \leq \text{Número de aristas en el borde de cara } f.$$

Si sumamos estas desigualdades, del lado izquierdo obtendremos $3f$. En el lado derecho, cada arista puede, o bordear dos caras, o bordear una. Pero ciertamente, no puede haber aristas que

sean borde de 3 caras. Así, si sumamos en el lado izquierdo, la suma nos dará menor o igual a $2e$. Por lo tanto, $3f \leq 2e$. Tomando la fórmula de Euler y multiplicándola por 3, obtenemos: $3v - 3e + 3f = 6$. Usando ahora $3f \leq 2e$, tenemos

$$6 = 3v - 3e + 3f \leq 3v - 3e + 2e = 3v - e,$$

es decir, $e \leq 3v - 6$. □

Este corolario nos permite probar inmediatamente la no planaridad de un número significativo de grafos. Por ejemplo, recordemos que queríamos ver que K_5 era no planar. Esto lo obtenemos en forma directa, pues K_5 tiene 5 vértices y 10 aristas, por lo tanto, si fuera planar debiéramos tener que $10 \leq 3{,}5 - 6 = 15 - 6 = 9$, lo cual no es cierto.

10.2. El problema del agua-luz-gas

Este es un conocido problema de escuela primaria: existen tres casas, y tres centrales: la del agua, la de la luz y la del gas. Trazar las cañerías desde las centrales a las casas sin que se crucen. Una solución (pero haciendo trampa) es mandar las tres cañerías a una casa, y de ella sacarlas las tres a la otra, y de ella las tres a la otra:

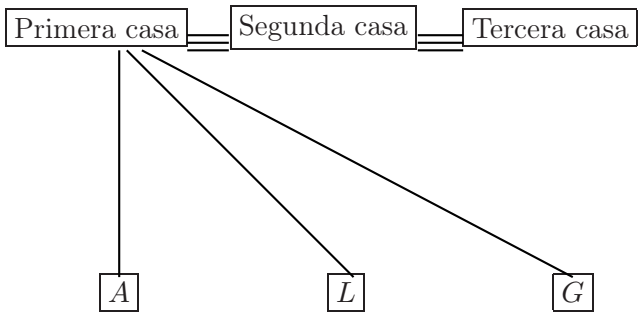


FIGURA 7. Una solución tramposa

En realidad, no permitiremos el uso de intermediarios, es decir el problema será llevar directamente la cañería desde cada central a cada casa. En el lenguaje de la teoría de grafos, consiste en representar, en el plano, al grafo $K_{3,3}$ (Fig. 8).

La pregunta es entonces si $K_{3,3}$ es planar o no. Veamos si podemos usar esta fórmula que probamos recién: $K_{3,3}$ tiene 9 aristas, y 6 vértices. Desafortunadamente, $3{,}6 - 6 = 18 - 6 = 12$ es ciertamente mayor que 9, así que solo sabemos que quizás es planar. Pero, observemos que $K_{3,3}$, por ser bipartito, no tiene ningún triángulo como subgrafo. Así pues, deduciremos la no planaridad de $K_{3,3}$ del siguiente

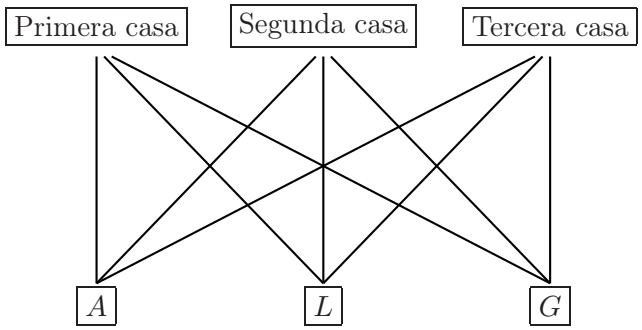


FIGURA 8. Luz-agua-gas es $K_{3,3}$

COROLARIO 10.2.1. *Si G es un grafo planar con por lo menos 3 vértices y que no tiene ningún triángulo como subgrafo, entonces $e \leq 2v - 4$.*

DEMOSTRACIÓN. Es similar a la demostración del Corolario 10.1.2, pero como no hay triángulos, todo ciclo tiene por lo menos 4 aristas, es decir, cada cara esta bordeada por al menos 4 aristas. Las únicas excepciones con al menos 3 vértices son:

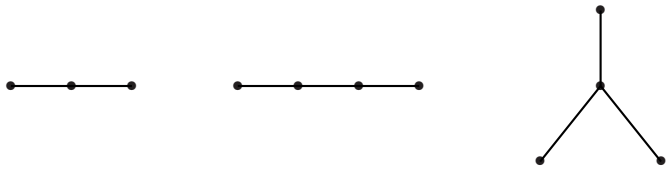


FIGURA 9. Grafos acíclicos con menos de 4 aristas y al menos 3 vértices

En el primer caso, $e = 2$, $v = 3$ y $2{,}3 - 4 = 6 - 4 = 2$. En el segundo y terceros, $e = 3$, $v = 4$ y $2{,}4 - 4 = 8 - 4 = 4 \geq 3$. Así pues, podemos suponer que cada cara esta bordeada por al menos 4 aristas. Sumando cara a cara, como antes, obtenemos ahora $4f \leq 2e$, es decir, $2f \leq e$. Multiplicando la fórmula de Euler por 2, tenemos: $4 = 2v - 2e + 2f \leq 2v - 2e + e = 2v - e$, es decir, $e \leq 2v - 4$. □

Retornando a $K_{3,3}$, como no tiene triángulos, podemos aplicar este corolario, y si fuera planar, debería cumplirlo. Pero habíamos dicho que $K_{3,3}$ tiene 9 aristas y 6 vértices, y $2{,}6-4 = 12-4 = 8$. Por lo tanto, $K_{3,3}$ no es planar.

Una ultima observación acerca de grafos planares: existe un teorema muy interesante, de difícil demostración (la prueba tiene 31 casos y subcasos para considerar) debido a Kuratowski, que dice que K_5 y $K_{3,3}$ son los dos grafos "básicos" no planares, en el siguiente sentido: un grafo G es no planar si y solo si existe un subgrafo de G, digamos H, tal que H se "ve" como K_5 o

como $K_{3,3}$, es decir, H es uno de ellos, excepto que tal vez, "agregue" en alguna o algunas aristas, vértices en el medio. Por ejemplo, H puede lucir como

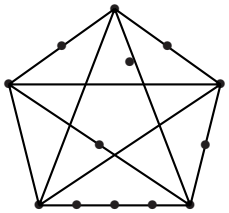


Figura 10

10.3. El teorema de los cuatro colores

Juntaremos ahora lo que hemos visto en esta sección con lo que vimos en la anterior, para tratar uno de los problemas mas famosos y recalcitrantes de la teoría de grafos, a saber: ¿cuántos colores se necesitan para colorear un grafo planar? En otras palabras, si quiero estar seguro de poder colorear propiamente los vértices de cualquier grafo planar, ¿cuántos colores necesito tener? De hecho, una pregunta más básica sería si existe una cantidad finita de colores que me permitan colorear cualquier tipo de grafo planar, por grande que sea. (Es claro que la respuesta para grafos en general es negativa, pues K_n requiere n colores.) Como K_4 es planar, sabemos que necesitamos por lo menos 4 colores. No podemos decir que necesitamos necesariamente 5, pues hemos visto que K_5 no es planar. Pero, podría haber otro grafo, complicado pero planar, que requiera 5, o más, colores. A mediados del siglo pasado la conjetura de que bastan 4 colores fue hecha, y en 1879 A. Kempe publicó una prueba de este hecho, que paso a llamarse el teorema de los cuatro colores. Desafortunadamente para Kempe, en 1889 (diez años después) otro matemático, P. Heawood, probó que la prueba de Kempe contenía un error. Heawood no fue completamente destructivo: mostró que adaptando la prueba de Kempe, podía probarse que con 5 colores bastaba para colorear cualquier grafo planar (el teorema de los cinco colores). Así pues, quedo planteado el problema de saber si el teorema de los cuatro colores era cierto, o bien si existía algún grafo planar para el cual 5 colores fueran necesarios. (Pero, al menos, gracias a Heawood, no era necesario buscar alguno que necesitara 6, o 7 u 8 colores, pues no existen, gracias al teorema de los cinco colores.) De hecho, en ese mismo artículo, Heawood probó más cosas: existe algo llamado género de un grafo, que es un número entero no negativo. Heawood demostró que existía una fórmula (expresión aritmética) que para cada género $g \geq 1$ da la cantidad de colores que permite colorear todos los grafos de género g. Los grafos planares tiene género igual a 0 y aplicando la fórmula para $g = 0$ obtenemos el número 4. Sin embargo, Heawood pudo probar que la fórmula es válida si g es mayor o igual a 1. El hecho de que esta fórmula existiera "convenció" a mucha gente de que el teorema de los cuatro colores debía ser cierto y que una prueba no tardaría en hallarse.

Sin embargo, pese al esfuerzo de muchos matemáticos y pese al desarrollo de la teoría el teorema de los cuatro colores no pudo probarse hasta 1975, cuando dos matemáticos norteamericanos, K. Appel y W. Haken, lo probaron. Más aún, no pudieron probarlos solos, sino que debieron usar la "ayuda" de un poderoso (para esa época) computador. Así, aún cuando el teorema fue probado, un gran sentimiento de desconfianza se generó, sobretodo en una época en la cual el acceso fácil a tiempo de computador no era común. Veinte años han pasado y la prueba ahora a sido controlada numerosas veces y no genera tanta resistencia como antes. Aún así, si alguien pudiese publicar una prueba que fuese "leíble por humanos" sería muy bien bienvenido.

Obviamente por lo dicho arriba, no daremos una prueba del teorema de los cuatro colores. Sí daremos una del teorema de los cinco colores, mencionando donde se halla la dificultad para el de cuatro, y dando una idea de que es lo que Appel y Haken (y el computador) hicieron.

LEMA 10.3.1. *Sea G un grafo planar. Entonces, existe un vértice de G de valencia 5 o menos.*

DEMOSTRACIÓN. Si el orden de G es menor o igual a 2, esto es obvio, pues la valencia de cualquier vértice no superará 2. Así, podemos suponer que hay al menos 3 vértices, y por lo tanto, sabemos que $e \leq 3v - 6$, donde e es el numero de aristas y v el de vértices.

Supongamos ahora que la valencia de todos los vértices sea al menos 6. Entonces, si sumamos las valencias de todos los vértices, la suma sera mayor o igual a $6v$. Pero la suma de todos las valencias es igual a $2e$ (lema del apretón de manos). Así, tenemos que $2e \geq 6v$. Por otro lado, como $e \leq 3v - 6$, tenemos que $2e \leq 6v - 12$, es decir, obtenemos $6v - 12 \geq 2e \geq 6v$, o $-12 \geq 0$, lo cual es un absurdo. □

TEOREMA 10.3.2. *(Teorema de los cinco colores) Si G es planar, $\chi(G) \leq 5$.*

DEMOSTRACIÓN. Supongamos que no sea cierto. De todos los contraejemplos al teorema, escojamos uno con la menor cantidad de vértices posible y llamémosle G. Por el lema anterior, existe un vértice x de G con valencia menor o igual a 5. Consideremos $H = G - x$, que es un grafo con menos vértices que G y por lo tanto no puede ser un contraejemplo; es decir, $\chi(H) \leq 5$. Así, podemos colorear H con 5 colores. Si la valencia de x en G es $0, 1, 2, 3$ o 4, los vértices adyacentes a x "usan" a lo sumo 4 de los 5 colores, así que podemos colorear a x con el quinto color, y tendríamos que $\chi(G) = 5$, lo cual no es posible pues G es un contraejemplo. Así pues, podemos suponer que la valencia de x es 5. Ahora bien, si los cinco vértices adyacentes a x no usan cinco colores, estamos como antes, y podemos colorear a x con el color faltante. Así, no solo podemos suponer que hay cinco vértices adyacentes a x, sino también que cada uno esta coloreado con un color distinto. Llamemos a estos vértices y, z, u, w, t, y supongamos que y de color 1, z de color dos, etc.

Supongamos primero que no haya, entre y y u, ningún camino tal que el color de todos sus vértices sea 1 o 3. Entonces, podemos cambiarle el color a y, de color 1 a color 3. Además, a los vértices adyacentes a y que tengan color 3, les cambiamos el color de 3 a 1. A los vértices

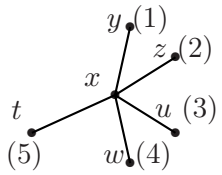


FIGURA 11

adyacentes a estos, que tengan color 1, los cambiamos a 3, y así sucesivamente. Después de realizar todos estos cambios, todavía tenemos un coloreo propio. Ahora bien, como estamos suponiendo que no hay ningún camino de color 1 y 3 exclusivamente entre y y u, resulta que u no cambia de color, es decir, retiene el color 3. Pero y ahora tiene también el color 3, y ningún otro vértice adyacente a x tiene el color 1. Pero, entonces, podemos colorear a x con el color 1 sin problemas, absurdo pues $\chi(G) \geq 6$.

Así pues, existe un camino con todos los vértices de color 1 y 3 entre y y u. Igualmente, si no hubiera ningún camino con todos los vértices de color 2 y 4 entre z y w, le podemos cambiar el color a z de 2 a 4 sin problemas, y colorear a x con el color 2. Así, también podemos suponer que existe un camino con todos los vértices de color 2 y 4 entre z y w.

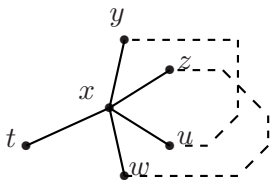


FIGURA 12. Caminos de y a u y de z a w

Por la Fig. 12 es claro que tenemos un problema: ¿por donde se cruzan los caminos A y B? Más precisamente, el camino A, junto con las aristas xy y xu, forma un ciclo C. Este ciclo tiene un interior y un exterior. El ciclo D formado por B y las aristas xz, xw cruza al ciclo C en el punto x, pues la arista xz esta en el interior y la arista xw en el exterior de C. Por lo tanto, D debe cruzar a C en algún otro punto. Pero no puede hacerlo, pues en el resto, C esta coloreado con los colores 1 y 3, y D con los colores 2 y 4. Hemos llegado a una contradicción. □

Analicemos un poco la prueba: hemos probado dos cosas 1) todo grafo planar debe tener una de las siguientes "configuraciones", es decir, parte de él debe lucir como alguno de los grafos de la Fig. 13.

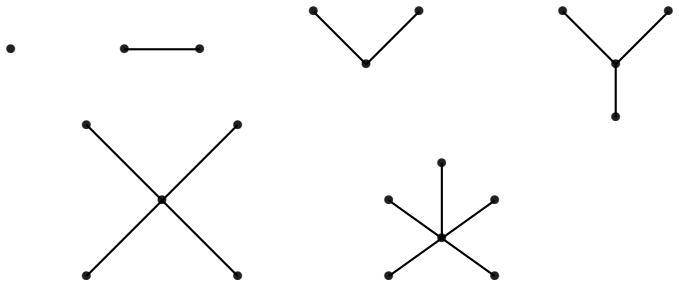


FIGURA 13. Posibles configuraciones

Esto lo probamos con el Lema 10.3.1. Es decir, probamos que ese conjunto de configuraciones es lo que se llama *inevitable*.

Además, probamos que si un grafo planar tiene una de esas configuraciones, puede ser coloreado con 5 colores (esto es lo que hicimos en el teorema). Es decir, probamos que ese conjunto de configuraciones es lo que se llama *irreducible* (para 5 colores). Kempe creyó que había sido capaz de probar que todo grafo planar que tuviera esas configuraciones podía ser coloreado con 4 colores, y muchos autores después de Heawood trataron de probar lo mismo. Pero luego se descubrieron nuevas técnicas, tanto para probar que un conjunto de configuraciones es irreducible, como para probar que es inevitable. Lo que no se podía hacer era encontrar un conjunto que fuera al mismo tiempo irreducible (para 4 colores) e inevitable. Finalmente, Appel y Haken encontraron un conjunto que satisfacía esas propiedades. Solo que en vez detener 6 elementos, como en el caso del teorema de 5 colores, el conjunto de Appel y Haken tiene 1480 elementos, y ningún ser humano es capaz de probarlo, sino que es necesario un computador para comprobar la inevitabilidad e irreducibilidad.

CAPíTULO 11

Apéndice V
Ejercicios adicionales

Este apéndice pretende ser una guía de trabajos prácticos ordenada y completa para un curso basado en los contenidos de este cuadernillo. Debido a ello, es posible encontrar en este apéndice ejercicios que ya se encuentran en el interior del libro.

11.1. Números enteros

1. Pruebe las siguientes afirmaciones usando los axiomas de números enteros (una vez probada una afirmación a partir de los axiomas, usted puede usarla para demostrar otra afirmación):
   (a) $-(a+b) = -a - b \quad \forall\, a, b \in \mathbb{Z}$.
   (b) $-(ab) = (-a)b = a(-b) \quad \forall\, a, b \in \mathbb{Z}$.
   (c) $(-1)a = -a \quad \forall\, a \in \mathbb{Z}$.
   (d) $-(-a) = a \quad \forall\, a \in \mathbb{Z}$.
   (e) $(-a)(-b) = ab \quad \forall\, a, b \in \mathbb{Z}$.
   (f) $a(b-c) = ab - ac \quad \forall\, a, b, c \in \mathbb{Z}$.
   (g) $a^2 - b^2 = (a-b)(a+b) \quad \forall\, a, b \in \mathbb{Z}$.
   (h) Si $b \in \mathbb{Z}$ y $a + b = a \ \forall\, a \in \mathbb{Z}$, entonces $b = 0$.
2. Pruebe las siguientes afirmaciones usando los axiomas de números enteros y/o los axiomas de la relación de orden en $\mathbb{Z}$:
   (a) $a \leq b \Rightarrow -b \leq -a \quad \forall\, a, b \in \mathbb{Z}$.
   (b) $a, b, c \in \mathbb{Z}$, $a \leq b$ y $c \leq 0 \ \Rightarrow \ bc \leq ac$.
   (c) $a^2 \geq 0 \quad \forall\, a \in \mathbb{Z}$.
   (d) $0 \leq 1$.
   (e) $a \leq a + 1 \quad \forall\, a \in \mathbb{Z}$.
3. Sean $a, b \in \mathbb{Z}$.
   (a) Pruebe que si a y b son pares, entonces $a + b$ y ab también lo son.
   (b) Determine la paridad de $a + b$ y ab en los casos restantes.
   (c) ¿Cuál es la paridad de los siguientes números enteros?: $3a^2+1$, $a(a+1)$, $(a-1)(a+1)$, $(-1)^a 3$, $(a+7)(a+8)$.
4. Encuentre todos los enteros n que verifiquen:

(a) $\mid n-2 \mid = 8$.
(b) $\mid n-2 \mid > 8$.
(c) $\mid n-1 \mid + \mid n-2 \mid > 1$.
(d) $\mid n-1 \mid \mid n+2 \mid = 3$.

5. Determine si los siguientes conjuntos poseen cota inferior. En caso afirmativo, encuentre la cota inferior máxima.
   (a) $A = \{z \in \mathbb{Z} \,/\, z = 10 - n^2 \text{ para algún } n \in \mathbb{N}\}$.
   (b) $B = \{z \in \mathbb{Z} \,/\, z = 10 + n^2 \text{ para algún } n \in \mathbb{N}\}$.
   (c) $C = \{z \in \mathbb{Z} \,/\, z^2 \leq 100z\}$.
6. *Axioma del buen orden: Todo subconjunto no vacío de* $\mathbb{N}$ *acotado inferiormente posee un elemento mínimo.*
   (a) Pruebe que todo subconjunto no vacío de $\mathbb{Z}$ acotado inferiormente posee un elemento mínimo.
   (b) Pruebe que todo subconjunto de $\mathbb{Z}$ acotado superiormente posee un elemento máximo (dado $A \subset \mathbb{Z}$, x es llamado elemento máximo de A sii x es cota superior de A y $x \in A$).
7. Pruebe por inducción que para todo $n \in \mathbb{N}$ se verifica:
   (a) $\sum_{i=1}^{n} i = \frac{n(n+1)}{2}$
   (b) $\sum_{i=1}^{n} i^2 = \frac{n(n+1)(2n+1)}{6}$
   (c) $\sum_{i=1}^{n} i^3 = (\frac{n(n+1)}{2})^2$
   (d) $3^n \geq 1 + 2^n$
   (e) $n! \leq n^n$
   (f) Si $a > -1$, entonces $(1+a)^n \geq 1 + na$
   (g) $\sum_{i=0}^{n}(2i+1) = (n+1)^2$
   (h) $\sum_{i=0}^{n} a^i = \frac{a^{n+1}-1}{a-1} \;\; \forall\, a \in \mathbb{R},\; a \neq 1$
   (i) $x^n - y^n = (x-y)(x^{n-1} + x^{n-2}y + \cdots + xy^{n-2} + y^{n-1}) \;\; \forall\, x, y \in \mathbb{R}$
8. Pruebe que para todo $n, m \in \mathbb{N}$ se verifica:
   (a) $x^n x^m = x^{n+m} \;\; \forall\, x \in \mathbb{R}$
   (b) $(x^n)^m = x^{nm} \;\; \forall\, x \in \mathbb{R}$
   (c) $(xy)^n = x^n y^n \;\; \forall\, x, y \in \mathbb{R}$

   [Ayuda: fije m y haga inducción sobre n.]
9. Considere las siguientes desigualdades:

$$\text{(i) } 100n \geq n^2, \qquad \text{(ii) } 8n + 1 \leq 8n.$$

   Determine en cada caso cual(es) de las siguientes proposiciones se verifica(n):
   (a) "Es verdadero para $n = 1$".
   (b) "Si es verdadero para n, entonces es verdadero para $n + 1$".

   ¿Puede usar el principio de inducción para afirmar que (i) y/o (ii) valen $\forall\, n \in \mathbb{N}$?.

10. En cada uno de los siguientes casos, se define u_n recursivamente. Demuestre por inducción completa la definición explícita de u.
    (a) Si $u_1 = 3$, $u_2 = 5$ y $u_n = 3u_{n-1} - 2u_{n-2}$ para todo $n \geq 3$, entonces $u_n = 2^n + 1 \ \ \forall\, n \in \mathbb{N}$.
    (b) Si $u_1 = 2$ y $u_{n+1} = 2u_n + 1$ para todo $n \geq 1$, entonces $u_n = 2^n + 2^{n-1} - 1 \ \ \forall\, n \in \mathbb{N}$.
11. Sea u_n definida recursivamente por: $u_1 = 2$, $u_n = 2 + \sum_{i=1}^{n-1} 2^{n-2i} u_i \ \ \forall\, n \geq 1$.
    (a) Calcule u_2 y u_3.
    (b) Proponga una fórmula para el término general u_n y pruébela por inducción.
12. Demuestre por inducción las siguientes desigualdades, hallando previamente un $n_0 \in \mathbb{N}$ que sirva de base para la inducción:
    (a) $n! \geq 2^n$.
    (b) $n^3 \geq 10n^2$.
    (c) $n^2 + 6n + 8 \geq 0$.
    (d) $n^4 \leq 4^n$.
13. Demostrar por inducción que la solución propuesta verifica la recursión:
    $$a_0 = 1,\ a_1 = 2,\ a_n = 4a_{n-1} - 3a_{n-2} \quad \Rightarrow \quad a_n = \tfrac{3^n+1}{2} \ \ \forall\, n.$$
14. Sean $a, b, c \in \mathbb{Z}$. Demuestre las siguientes afirmaciones:
    (a) Si $ab = 1$, entonces $a = b = 1 \ \vee \ a = b = -1$.
    (b) Si $a \neq 0$, $b \neq 0$, $a|b$ y $b|a$, entonces $a = b \ \vee \ a = -b$.
    (c) Si $a \neq 0$, $a|b$ y $a|c$, entonces $a|(b + c) \ \wedge \ a|(b - c)$.
    (d) Si $a \neq 0$, $a|b$ y $a|(b + c)$, entonces $a|c$.
    (e) Si $a \neq 0$ y $a|b$, entonces $a|bc$.
15. Sean $a, b, c \in \mathbb{Z}$. ¿Cuáles de las siguientes afirmaciones son verdaderas?. Justifique su respuesta.
    (a) $a|bc \ \Rightarrow \ a|b \ \vee \ a|c$.
    (b) $a|(b + c) \ \Rightarrow \ a|b \ \vee \ a|c$.
    (c) $a|c$ y $b|c \ \Rightarrow \ ab|c$.
    (d) $a|c$ y $b|c \ \Rightarrow \ (a + b)|c$.
    (e) $a, b, c > 0 \ \wedge \ a = bc \ \ \Rightarrow \ \ a \geq b \ \wedge \ a \geq c$.
16. Sea $n \in \mathbb{N}, n > 1$. Demuestre el siguiente resultado: sea n un número primo, entonces para todo $p > 0$ primo tal que $p^2 \leq n, \ \ p \not| n$. [Ayuda: (i) Pruebe que si $n \in \mathbb{N}, n \neq 1$ y n no es primo, entonces $\exists\, t \in \mathbb{N}$ tal que $1 < t < n$ y $t|n$. (ii) Si n satisface las hipótesis de (i), entonces el conjunto $\{t \in \mathbb{N} : 1 < t < n \ \wedge \ t|n\}$ tiene un elemento mínimo. (iii) Todo entero distinto de 1 y de -1 es divisible por un número primo.]
17. (a) Determine cuáles de los siguientes números son primos: -79, 113, 123, -131, 137, 141, -401.
    (b) Dé todos los números primos positivos menores que 100.

18. Encuentre el cociente y el resto de la división en $\mathbb{Z}$ de b por a:

(i) $b = 2466,\ a = -11$. (ii) $b = -98,\ a = 73$. (iii) $b = -98,\ a = -73$.

(iv)$b = 32,\ a = 41$. (v) $b = 32,\ a = -41$. (vi) $b = -32,\ a = 41$.

19. Sean $a, b \in \mathbb{Z}$ tales que $b \neq 0$, $a - b = 175$ y la división de a por b tiene cociente 15 y resto 7. Halle a y b.
20. Denotemos (a, b) el máximo común divisor entre a y b y $[a, b]$ el mínimo común múltiplo entre a y b. Sean $a, b, c, \in \mathbb{Z}$. Pruebe las siguientes afirmaciones:
    (a) $(a, b) = |a| \ \Leftrightarrow \ a|b$.
    (b) p primo $\wedge\, p|ab \ \Rightarrow \ p|a \ \vee \ p|b$.
    (c) $(a, b) = 1 \ \wedge \ a|c \ \wedge \ b|c \ \Rightarrow \ ab|c$.
    (d) $(a, b) = 1 \ \wedge \ a|bc \ \Rightarrow \ a|c$.
21. Calcule $(a, a + 3)$ y $[a, a + 3]$.
22. (a) Calcule el máximo común divisor y expréselo como combinación lineal de los números dados:
        (i) 14 y 35, (ii) 11 y 15, (iii) 12 y 52, (iv) 12 y -52.
    (b) Calcule el mínimo común múltiplo de los números dados en el item (a).
23. Sean $a, b \in \mathbb{Z}, b \neq 0$. Determine el cociente y el resto de la división de $(b - a)$ por b a partir de la división de a por b.
24. Dado $m \in \mathbb{Z}$, $m \neq 0$, halle los posibles restos de la división de m^2 y m^3 por p, con $p = 3$, 5 y 8.
25. (a) Pruebe que el producto de tres enteros consecutivos es divisible por 6.
    (b) Pruebe que el producto de cuatro enteros consecutivos es divisible por 24.
26. (a) Pruebe que $\nexists\, n \in \mathbb{Z}$ tal que $4|(n^2 + 2)$.
    (b) Pruebe por inducción que $n^2 + 3n$ es divisible por 2 $\forall\ n \in \mathbb{N}$.
27. Pruebe que $2n + 1$ y $\frac{1}{2}n(n + 1)$ son coprimos $\ \forall\ \ n \in \mathbb{Z}$.
28. Pruebe que no existen enteros x e y que satisfagan $x + y = 100$ y $(x, y) = 3$.
29. Pruebe que si p es un primo positivo, entonces:
    (a) $(p, (p - 1)!) = 1$.
    (b) $p|(2^n + 3^n) \ \wedge \ p|(2^m + 3^m) \ \wedge \ n < m \ \Rightarrow \ p|(3^{m-n} - 2^{m-n})$.
    (c) $(2^n + 3^n, 2^{n+1} + 3^{n+1}) = 1$.
30. Dados dos enteros cualesquiera, pruebe que su suma y su diferencia son de la misma paridad.
31. (a) Pruebe que todo número impar es de la forma $4m \pm 1$ con $m \in \mathbb{Z}$. ¿Es cierta la recíproca?.
    (b) Pruebe que todo entero impar que no es múltiplo de 3 es de la forma $6m \pm 1$ con $m \in \mathbb{Z}$.

32. (a) Sean $a, b \in \mathbb{Z},\ b \neq 0$, y sea r el resto de la división de a por b. Pruebe que $(a, b) = (b, r)$.
    (b) Encuentre el máximo común divisor de los números dados: (i) 7469 y 2464, (ii) 2947 y -3997, (iii) -1109 y -4999.
33. Encuentre todos los enteros positivos que satisfagan simultáneamente las ecuaciones $(a, b) = 10$ y $[a, b] = 100$.
34. (a) Pruebe que $7|(a^2 + b^2)$ si y solo si $7|a$ y $7|b$.
    (b) ¿Es lo mismo cierto para 5?.
35. Sean $a, b \in \mathbb{Z}$ no simultáneamente nulos y sea $m \in \mathbb{Z}$ tal que $m|a$ y $m|b$. Pruebe que:
    (a) $a|b \ \Leftrightarrow \ \frac{a}{d}|\frac{b}{d}$
    (b) $(\frac{a}{m}, \frac{b}{m}) = \frac{(a,b)}{m}$
36. ¿Existen enteros m y n tales que
    (a) $m^4 = 27$?.
    (b) $m^2 = 12n^2$?.
    (c) $m^3 = 47n^3$?.
37. (a) Sea $H \subset \mathbb{Z},\ H \neq \emptyset$, cerrado para la suma y para la resta. Demuestre que existe $d \in \mathbb{Z}$ tal que $H = \{dk \ / \ k \in \mathbb{Z}\}$ (este es el conjunto de todos los múltiplos enteros de d y se denota $d\mathbb{Z}$).
    (b) Sean $a, b \in \mathbb{Z}$ no simultáneamente nulos y sea $H = \{ka + tb \ / \ k, t \in \mathbb{Z}\}$. Pruebe que $H = (a, b)\mathbb{Z}$.
38. Pruebe que si $(a, b) = 1$, entonces $(a + b, a^2 + b^2 - ab)$ es 1 ó 3.

11.2. Funciones y conteo

1. Grafique los siguientes conjuntos de $\mathbb{N} \times \mathbb{R}$:
    (a) $\{1\} \times \mathbb{R}$
    (b) $\mathbb{N} \times \{1\}$
    (c) $\{(n, z) \ : \ n = [z]\}$ ($[z]$ es el mayor entero menor o igual que z y se denomina *parte entera de z*)
    (d) $\{(x, y) \ : \ [x + y] \in \{2, 3\}\}$
    (e) $\{(x, y) \ : \ x, [y] \text{ son coprimos}\} \cap (\{n \in \mathbb{N} \ : \ 1 \leq n \leq 10\} \times [1, 10])$
2. Considere las siguientes funciones de $\mathbb{N}$ en $\mathbb{N}$:

$$f(n) = n + 1, \qquad g(n) = \max\{1, n - 1\}, \qquad h(n) = \begin{cases} 10 - n & \text{si } 1 \leq n < 10 \\ n & \text{si } 10 \leq n \end{cases}$$

    (a) Analice inyectividad y suryectividad de cada una de ellas.
    (b) Pruebe que $g \circ f = id$, donde $id(n) = n \ \forall\, n$ (función identidad).
    (c) Pruebe que $h \circ h = id$.
    (d) ¿Existen $f', g' : \mathbb{N} \mapsto \mathbb{N}$ tales que $g' \circ g = id$ y $f' \circ f = id$?.

(e) ¿Existe $h' : \mathbb{N} \mapsto \mathbb{N}$, $h' \neq h$, tal que $h' \circ h = id$?.

3. Se dice que una función $f : X \mapsto Y$ tiene inversa a izquierda si existe una función $g : Y \mapsto X$ tal que $g \circ f = id_X$ $(id : X \mapsto X)$.
   (a) Defina inversa a derecha.
   (b) Pruebe que si f tiene inversa a izquierda, entonces f es 1 a 1 (inyectiva).
   (c) Pruebe que si f tiene inversa a derecha, entones f es sobre (suryectiva).
4. Pruebe que si $g : X \mapsto X$ es inyectiva y X es finito, entonces g es una biyección.
5. Pruebe que cualquier subconjunto de $\{2, 3, \ldots, 50\}$ que tiene más de 16 elementos contiene dos números cuyo máximo común divisor no es 1.
6. Pruebe que todo subconjunto de n+1 números tomados de $\{1, 2, 3, \ldots, 2n\}$ contiene dos números tales que uno divide al otro.
7. Se eligen 5 puntos en un triángulo equilátero de lado 1. Pruebe que al menos dos de ellos están a una distancia menor que $1/2$.
8. En cada uno de los siguientes casos encuentre el valor apropiado de n y escriba una biyección $f : \mathbb{N}_n \to X$.
   (a) $X = \{2, 4, 6, 8, 10\}$.
   (b) $X = \{-3, -8, -13, -18, -23, -28\}$.
9. Mostrar que si $|X| = n$ y existe una biyección de X a Y, entonces $|Y| = n$.
10. Construyendo una inyección de $\mathbb{N}$ a X, mostrar que cada uno de los siguientes conjuntos X es infinito:
    (i) $\mathbb{Z}$, (ii) $\{x \in \mathbb{Z}/x < 0\}$, (iii) $\{n \in \mathbb{N}/n > 10^6\}$.
11. Probar que si X es un subconjunto de Y, y X es infinito, entonces Y es infinito.
12. Demuestre que la unión (disjunta) de dos conjuntos numerables es numerable.
13. Dar una biyección entre $\mathbb{N} \times \mathbb{N}$ y $\mathbb{N}$. Deducir que $\mathbb{Q}$ es numerable.

11.3. Combinatoria

1. Llamamos **palabra** a cualquier sucesión de letras del alfabeto usual. Sea A el conjunto de palabras de 4 letras.
   (a) Calcule $|A|$.
   (b) ¿Cuántas palabras que no terminen en b tiene A?.
   (c) ¿Cuántas palabras que no usen la letra b tiene A?.
   (d) ¿Cuántas palabras de A cumplen con la condición de no repetir letras?.
2. Llamamos **alfabeto** a un conjunto Σ de símbolos (**letras**). Con Σ^* denotamos el conjunto de **palabras**, es decir el conjunto de sucesiones finitas de elementos de Σ. Ejemplo: si $\Sigma = \{a, b, c\}$, entonces las siguientes son palabras:

   $$abc \quad aaaaa \quad bbac \quad a \quad \epsilon \text{ (palabra vacía).}$$

   Si $|\Sigma|$ es finito, ¿cuántas palabras de n letras tiene Σ^*?.

3. Si Σ es un alfabeto, llamamos **lenguaje** a un subconjunto A de Σ^*. Si A, B son lenguajes, definimos $AB = \{w_1 w_2 \ : \ w_1 \in A \ \wedge \ w_2 \in B\}$.

   Sea $\Sigma = \{a, b, c\}$ y sean $A = \{a, ab\}$, $B = \{\epsilon, b, bb\}$.

   (a) Calcule AB.

   (b) ¿Es $AB = BA$?.

   (c) ¿Es $|AB| = |A||B|$?.

4. ¿Cuántas palabras diferentes pueden formarse permutando las letras de la palabra PALABRAS?. ¿Cuántas permutando RESTRICCIONES?.

5. (a) ¿De cuántas maneras pueden sentarse 8 personas en una mesa circular?.

   (b) ¿De cuántas maneras pueden sentarse 6 hombres y 6 mujeres en una mesa circular si nunca deben quedar dos mujeres juntas?.

6. ¿De cuántas formas pueden fotografiarse 10 matrimonios en hilera de manera que los esposos estén juntos?.

7. (a) ¿Cuántas diagonales tiene un polígono regular de n lados?.

   (b) Dadas dos rectas paralelas en el plano, n puntos sobre una de ellas y m sobre la otra, ¿cuántos triángulos pueden formarse con vértices en esos puntos?.

   (c) En un cuadrado se marcan n puntos en cada lado (distintos de los vértices). ¿Cuántos triángulos quedan determinados por esos puntos?.

8. Dado el conjunto $\{1, 2, 3, 4, 5, 6, 7, 8, 9\}$, ¿de cuántas maneras se pueden extraer 3 números cuyo producto sea múltiplo de 8?; ¿y de 7?.

9. ¿Cuántos números naturales impares menores que 10000 hay?.

10. ¿Cuántas señales pueden enviarse con un conjunto de 5 banderas, 3 blancas y 2 azules, dispuestas en un mástil?.

11. ¿De cuántas maneras se puede descomponer el número 6 como suma de tres números en $\mathbb{N} \cup \{0\}$?.

12. En una asamblea de accionistas hay 6 personas que han solicitado hacer uso de la palabra. ¿De cuántas maneras diferentes pueden ordenarse para hablar si es que no se ha establecido ningún sistema de prioridades?.

13. (a) ¿De cuántas maneras pueden colocarse 10 libros en un estante con 10 casilleros si 4 de ellos prefijados deben ocupar siempre el mismo lugar?.

   (b) ¿Cuántas maneras de colocar los 10 libros habrá si los 4 libros de la parte (a) pueden intercambiarse entre sí?.

14. En un proceso de manufactura hay 6 operaciones distintas que se realizan secuencialmente. Es necesario seleccionar 6 personas de entre 15 para que se atiendan dichas operaciones con la condición que el señor T sea el elegido para atender ya sea la primera o la última operación. Siendo todas las otras operaciones tareas que requieren el mismo esfuerzo, ¿cuántas maneras diferentes hay de elegir a esas personas?.

15. Mostrar que el número de palabras de longitud n en el alfabeto $\{0,1\}$ que contiene exactamente r ceros es $\binom{n}{r}$.
16. Probar por **inducción** que
$$\binom{s+n}{n} = \binom{s+n-1}{n} + \binom{s+n-1}{n-1}$$
17. Usando la identidad $(1+x)^m(1+x)^n = (1+x)^{m+n}$ probar que
$$\binom{m+n}{r} = \binom{m}{0}\binom{n}{r} + \binom{m}{1}\binom{n}{r-1} + \cdots + \binom{m}{r}\binom{n}{0}$$
donde m, n, r son enteros positivos, $m \geq r$ y $n \geq r$.
18. Muestre que si r y s son enteros tales que $s|r$, y p es un primo tal que $p|r$ pero $p \nmid s$, entonces $p|(r/s)$. Deducir que:
    (a) p divide a $\binom{p}{i}$ para todo i con $1 \leq i \leq p-1$;
    (b) $(a+b)^p - a^p - b^p$ es divisible por p para todo entero a y b.
19. Un señor tiene 12 amistades, 7 damas y 5 caballeros. Su esposa tiene 12 amistades, 5 damas y 7 caballeros. ¿De cuántas formas pueden invitar a 6 damas y 6 caballeros con la condición que haya 6 invitados de la señora y 6 del señor?.

11.4. Congruencias

Sea I un conjunto no vacío, finito o infinito, y suponga que a cada $i \in I$, le asignamos un conjunto X_i. Entonces decimos que tenemos una familia de conjuntos, escribimos
$$\mathcal{H} = \{X_i \ / \ i \in I\}$$
y nos referimos a I como el conjunto de índices.

Definición 11.4.1. Una **partición** de un conjunto X es una familia $\{X_i / i \in I\}$ de subconjuntos no vacíos de X tal que

(i) X es la unión de los conjuntos X_i $(i \in I)$.
(ii) Cada par X_i, X_j $(i \neq j)$ es disjunto.

Los subconjuntos X_i son llamados partes de la partición.

Supongamos que $\{X_i / i \in I\}$ es una partición del conjunto X. Escribimos xRy si x e y están en el mismo X_i, y decimos que x está *relacionado* con y. La relación R definida de esta manera, tiene tres propiedades. Si x, y, z son miembros cualesquiera de X, tenemos:

xRx	Propiedad *reflexiva*
$xRy \Rightarrow yRx$	Propiedad *simétrica*
xRy y $yRz \Rightarrow xRz$	Propiedad *transitiva*.

Una relación R en un conjunto X se dice una **relación de equivalencia** si es reflexiva, simétrica y transitiva.

Recíprocamente una relación de equivalencia definida en un conjunto X determina una partición de X. Para ver esto, empecemos definiendo la **clase de equivalencia** de x, como sigue:

$$C_x = \{y \in X / \ yRx\}$$

C_x es el subconjunto de X que contiene a aquellos y relacionados a x en la relación de equivalencia dada. Es importante notar que, en general, el subconjunto C_x puede tener diferentes nombres. En efecto, si x y z están relacionados, entonces las clases de equivalencia C_x y C_z son la misma.

TEOREMA 11.4.1. *Si R es una relación de equivalencia en un conjunto X, entonces las distintas clases de equivalencia con respecto a R forman una partición de X.*

1. Encuentre todas las particiones de los siguientes conjuntos:
   (i) $\emptyset$, (ii) $\{a\}$, (iii) $\{a, b\}$, (iv) $\{a, b, c\}$.
2. Encuentre las particiones determinadas por las siguientes relaciones de equivalencia en $\mathbb{Z}$:

   (a) $xRy \Leftrightarrow |x| = |y|$, (d) $xRy \Leftrightarrow \exists\, z \in \mathbb{Z} \ : \ x = y + z$,

   (b) $xRy \Leftrightarrow 2|(x - y)$, (e) $xRy \Leftrightarrow x^2 = y^2$,

   (c) $xRy \Leftrightarrow 3|(x - y)$.

3. Analice reflexividad, simetría y transitividad de las siguientes relaciones en $\mathbb{Z}$:

   (a) $xRy \Leftrightarrow x|y$, (c) $xRy \Leftrightarrow x + y = 7$,

   (b) $xRy \Leftrightarrow x \leq y$, (d) $xRy \Leftrightarrow 5|(x - y)$.

4. Se define en $\mathbb{N}$ la siguiente relación: $nRm \Leftrightarrow 3|(n^2 - m^2)$.
   (a) Muestre que R es una relación de equivalencia.
   (b) Dé cuatro elementos de la clase del 0.
   (c) Dé cuatro elementos de la clase del 1.
   (d) ¿Hay otras clases de equivalencia?.
5. Se define en $\mathbb{R}$ la siguiente relación: $xRy \Leftrightarrow x - y \in \mathbb{Z}$. Encuentre un conjunto $A \subset \mathbb{R}$ con la siguiente propiedad: $\forall \ x \in \mathbb{R} \ \exists! \ y \in A$ tal que xRy
6. Si a es congruente a b módulo m denotemos $a \equiv b\,(m)$. Analizar la validez de las siguientes afirmaciones

   (a) $11 \equiv -1\,(6)$, (b) $31 \equiv -18\,(7)$, (c)$3 \equiv 0\,(2)$,

   (d) $3 \equiv 3\,(2)$, (e) $10^2 \equiv 10\,(3)$, (f) $1 \equiv -1\,(2)$.

7. Pruebe las siguientes propiedades:

(a) $\forall\, a \in \mathbb{Z},\ \ a \equiv a\,(m)$.
(b) $\forall\, a, b \in \mathbb{Z},\ \ a \equiv b\,(m) \Leftrightarrow b \equiv a\,(m)$.
(c) $\forall\, a, b, c \in \mathbb{Z},\ \ , a \equiv b\,(m)\ \ ,\ b \equiv c\,(m), \Rightarrow a \equiv c\,(m)$.
(d) $\forall\, a, b, c \in \mathbb{Z},\ \ , a \equiv b\,(m) \quad \Leftrightarrow a + c \equiv b + c\,(m)$.
(e) $\forall\, a, b, c \in \mathbb{Z},\ \ , a \equiv b\,(m) \quad \Leftrightarrow a + mc \equiv b\,(m)$.
(f) $\forall\, a, b, c \in \mathbb{Z},\ \ , a \equiv b\,(m) \quad \Rightarrow ac \equiv bc\,(m)$.
(g) $\forall\, a \in \mathbb{Z},\ \ , a \equiv 0\,(m) \quad \Leftrightarrow m$ divide a a.
(h) $\forall\, a, b \in \mathbb{Z},\ \ , a \equiv b\,(m) \quad \Leftrightarrow a$ y b tienen el mismo resto en la división por m.

De (h) resulta

$$a \equiv b\,(m) \quad \Leftrightarrow m \text{ divide } (b - a) \quad \Leftrightarrow r_a = r_b$$

donde r_a es el resto de la división de a por m (análogamente para r_b).

Nota: Las tres primeras propiedades de la relación de congruencia (a), (b), (c) expresan que ésta es una relación de equivalencia en $\mathbb{Z}$. Como tal determina una partición en $\mathbb{Z}$. Una clase de equivalencia está formada por todos los enteros congruentes entre sí. Por ejemplo, si m es 5, las clases de equivalencia son:

$$\mathbb{Z}_0 = \{..., -10, -5, 0, 5, 10, ...\} = \{5k \ \ / \ \ k \in \mathbb{Z}\}$$

$$\mathbb{Z}_1 = \{..., -9, -4, 1, 6, 11, ...\} = \{5k + 1 \ \ / \ \ k \in \mathbb{Z}\}$$

$$\mathbb{Z}_2 = \{..., -8, -3, 2, 7, 12, ...\} = \{5k + 2 \ \ / \ \ k \in \mathbb{Z}\}$$

$$\mathbb{Z}_3 = \{..., -7, -2, 3, 8, 13, ...\} = \{5k + 3 \ \ / \ \ k \in \mathbb{Z}\}$$

$$\mathbb{Z}_4 = \{..., -6, -1, 4, 9, 14, ...\} = \{5k + 4 \ \ / \ \ k \in \mathbb{Z}\}$$

La propiedad (h) caracteriza a la congruencia: dice que la congruencia módulo m clasifica a los enteros por su resto en la división por m. *Dos enteros son equivalentes si y sólo si poseen el mismo resto en la división por* m.

Una aplicación

Sea $a \in \mathbb{N}$. Escrito en forma decimal es

$$a = a_r 10^r + ... + a_2 10^2 + a_1 10 + a_0 \quad 0 \leq a_i \leq 9\ ,\ i = 0, 1, ..., r$$

Tenemos

$$10 \equiv 1\,(3)$$
$$10^2 \equiv 1\,(3)$$

$$\forall\, n \quad 10^n \equiv 1\,(3) \;\; (probarlo)$$

por lo tanto

$$a_0 \equiv a_0\,(3)$$

$$10a_1 \equiv a_1\,(3)$$

$$a_r 10^r \equiv a_r\,(3)$$

y por la propiedad (d) podemos sumar miembro a miembro y obtener

$$a \equiv a_r + ... + a_2 + a_1 + a_0\,(3)$$

lo cual dice que a y la suma de los dígitos $a_r + ... + a_2 + a_1 + a_0$ del desarrollo decimal de a tienen el mismo resto en la división por tres. De esto resulta la regla de divisibilidad por tres: un número es divisible por tres sii ...

1. (a) Justifique la regla de divisibilidad por 9 siguiendo los pasos anteriores.
   (b) Estudie la divisibilidad por 11. [Ayuda: $10 \equiv -1\,(11)$].
2. Halle la cifra de las unidades y la de las decenas del número 7^{15}.
3. Halle todos los x que satisfacen:

   (a) $x^2 \equiv 1\,(4)$, (e) $x^4 \equiv 1\,(16)$,

   (b) $x^2 \equiv x\,(12)$, (f) $3x \equiv 1\,(5)$,

   (c) $x^2 \equiv 2\,(3)$, (g) $2x \equiv 5\,(6)$,

   (d) $x^2 \equiv 0\,(12)$, $(h) 3x^3 \equiv 20\,(8)$.

4. Obtenga el resto en la división de:
   (i) 2^{21} por 13, (ii) 3^8 por 5, (iii) 8^{25} por 127.
5. Halle el resto en la división de x por 5 y por 7 para:
   (i) $x = 1^8 + 2^8 + 3^8 + 4^8 + 5^8 + 6^8 + 7^8 + 8^8$, (ii) $x = 3{,}11{,}17{,}71{,}101$.
6. Encuentre el resto en la división de a por b en los siguientes casos e indique lo que esto significa en la relación de congruencia módulo n:

   (i) $a = 11^{13}, 13^8 b = 12$, (iii) $a = 4^{1000} b = 7$,

   (ii) $a = 123^{456} \quad b = 31$, (iv) $a = 7^{83} b = 10$.

11.5. Grafos y árboles

1. Para cada entero positivo n definimos el *grafo completo* K_n como el grafo con n vértices en el cual cada par de vértices es adyacente. ¿Cuántas aristas tiene K_n? ¿Para cuáles valores de n se puede encontrar un dibujo de K_n con la propiedad que las líneas representan las aristas sin cruzarse?

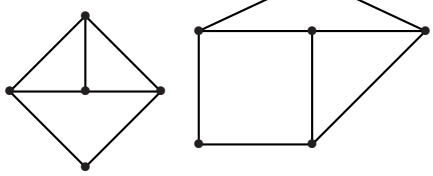
2. Encuentre un isomorfismo entre los grafos por las siguientes listas. (Ambas listas especifican versiones de un famoso grafo conocida como *grafo de Petersen*.)

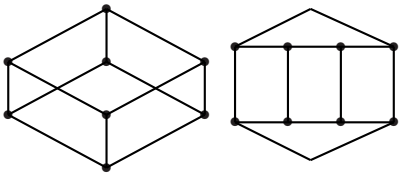
a	b	c	d	e	f	g	h	i	j		0	1	2	3	4	5	6	7	89
b	a	b	c	d	a	b	c	d	e		1	2	3	4	5	0	1	0	26
e	c	d	e	a	h	i	j	f	g		5	0	1	2	3	4	4	3	57
f	g	h	i	j	i	j	f	g	h		7	6	8	7	6	8	9	9	98

3. (a) Encuentre todos los grafos de 5 vértices y 2 aristas no isomorfos entre sí.
   (b) ¿Cuál es el máximo número de aristas que puede tener un grafo de 5 vértices?
4. Para cada una de las siguientes secuencias, encuentre un grafo que tenga exactamente las valencias indicadas o demuestre que tal grafo no existe:

   (a) $3, 3, 1, 1$ (d) $3, 2, 2, 1$
   (b) $3, 3, 2, 2, 1, 1$ (e) $4, 1, 1, 1, 1$
   (c) $7, 3, 3, 3, 2, 2$ (f) $4, 1, 1, 1$

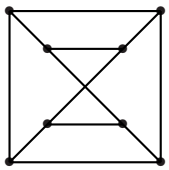
5. Demuestre que los siguientes pares de grafos son isomorfos (encuentre un isomorfismo):

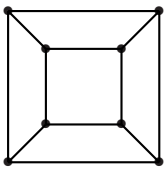
   (a) 

   (b) 

6. Sean $G = (V, E)$ y $G' = (V', E')$ dos grafos isomorfos y sea α un isomorfismo entre ellos. Pruebe las siguientes afirmaciones:
   (a) $|V| = |V'|$ y $|E| = |E'|$.
   (b) $\delta(v) = \delta(\alpha(v)) \ \forall \ v \in V$.
7. Sean $G = (V, E)$ y $G' = (V', E')$ dos grafos y sea $\alpha : V \mapsto V'$ una función tal que $\delta(v) = \delta(\alpha(v)) \ \forall \ v \in V$.
   (a) ¿Puede afirmar que α es un isomorfismo?.
   (b) ¿Puede afirmarlo si $|V| = 3$ ó 4?.
8. Encuentre una función del grafo A al B que preserve valencias. ¿Es un isomorfismo?.

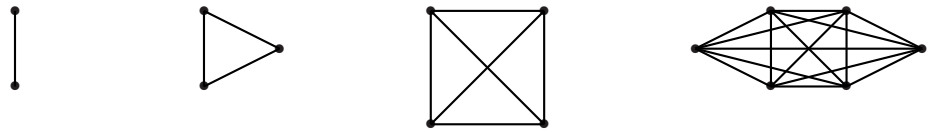
A: B:





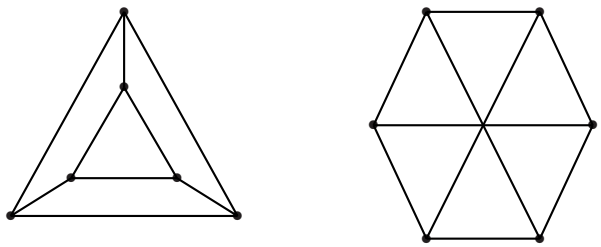
9. Pruebe que si G es un grafo con más de un vértice, entonces existen dos vértices con la misma valencia.
10. (a) Halle el complemento de los siguientes grafos:

(i) (ii) (iii) (iv)



(b) Si $V = \{v_1 \dots v_n\}$ y $\delta(v_i) = d_i \ \ \forall \ i = 1, \dots, n$, calcule las valencias de el grafo complemento.

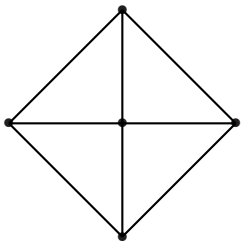
11. Sea $G = (V, E)$ un grafo y sean $v, w \in V$ tales que existe una caminata que une v con w. Construya un camino que una v con w.
12. Pruebe que los siguientes grafos no son isomorfos:



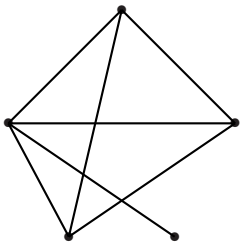
13. Considere K_8.
    (a) ¿Cuántos subgrafos isomorfos a K_5 hay?.
    (b) ¿Cuántos caminos de tres aristas hay entre dos vértices cualesquiera?.
    (c) ¿Cuántos isomorfismos hay de K_n en sí mismo?.
14. Sea $G = (V, E)$ un grafo. Se dice que $G' = (V', E')$ es **subgrafo** de $G = (V, E)$ si $V' \subset V$, $E' \subset E$ y todos los vértices que son extremos de las aristas de E' están en V'.

Dados los siguientes grafos:

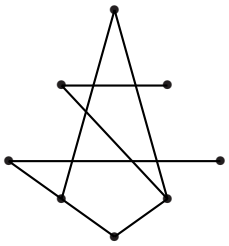
(1)



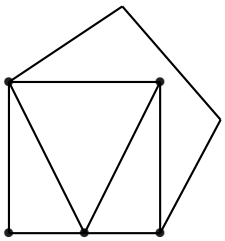
(2)



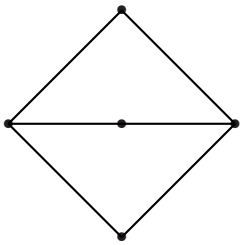
(3)



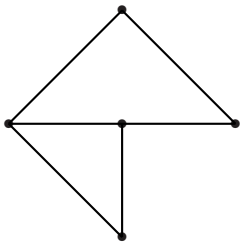
(4)



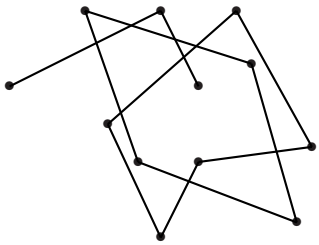
(5)



(6)



(7)



(a) Determine en cada caso si existen subgrafos completos de más de 2 vértices.
(b) Para el grafo (1), dé todos los caminos que unen a con b.
(c) Dé caminatas eulerianas que unan a con b en los grafos (2), (3) y (4).
(d) Para (5) y (6), decir si existen ciclos hamiltonianos partiendo de a.
(e) Determinar cuales de los siguientes pares de grafos son isomorfos:
    (i) (4) y (2),
    (ii) (5) y (6),

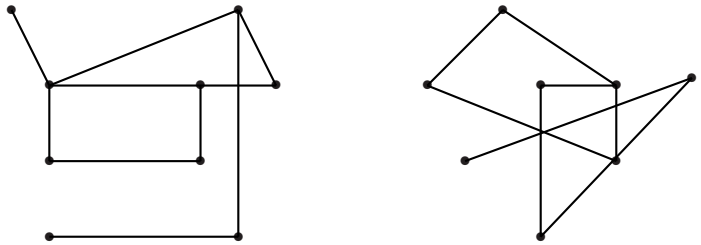
(iii) (5) y (1).

(f) Halle las componentes conexas del grafo (7).

15. Pruebe que si G es un grafo en el que cada vértice tiene valencia mayor que 1, entonces G tiene un ciclo.
16. Pruebe que si $n \geq 2$, entonces todo grafo de n vértices y al menos n aristas tiene un ciclo.
17. Sea $G = (V, E)$ un grafo conexo y sea $e \in E$. Pruebe que $G - \{e\}$ es conexo sí y sólo si e forma parte de algún ciclo.
18. Pruebe que todo grafo conexo de n vértices tiene al menos $n - 1$ aristas.
19. Sea $G = (V, E)$ un grafo conexo y sea $e \in E$. Se dice que e es un **puente** si al quitarle a G la arista e el grafo deja de ser conexo.

    Considere los siguientes grafos:

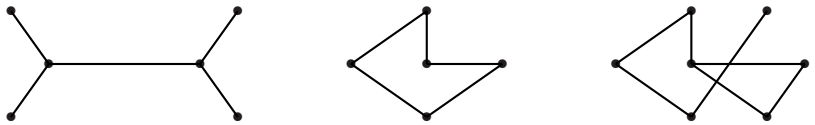
    (A) (B)



    Determine todos los puentes en A y B.

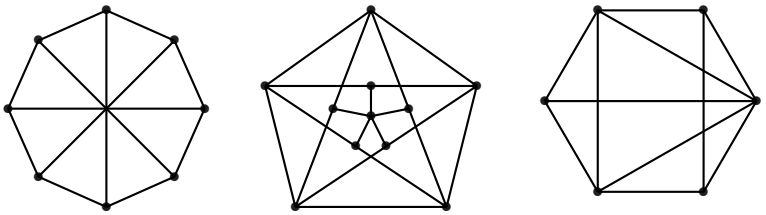
20. Dé todos los árboles de 6 vértices no isomorfos.
21. Pruebe que si $T = (V, E)$ es un árbol y $|V| \geq 2$, entonces existen al menos dos vértices con valencia 1 (hojas). Usar ejercicio 8.
22. Sea $G = (V, E)$ un grafo con $|V| = n$. Pruebe que las siguientes afirmaciones son equivalentes:
    (a) G es un árbol.
    (b) G es conexo y, cualquiera sea $e \in E$, $G - \{e\}$ no es conexo.
    (c) G es acíclico y si se le agrega una arista deja de serlo.
    (d) G es acíclico y tiene $n - 1$ aristas.
    (e) G es conexo y tiene $n - 1$ aristas.
23. (a) Encuentre todos los árboles expandidos de los siguientes grafos.

(i) (ii) (iii)



(b) Para cada uno de los grafos anteriores, encuentre las aristas que están en todos los árboles expandidos.
(c) Caracterice las aristas que están en todos los árboles generadores de un grafo conexo.

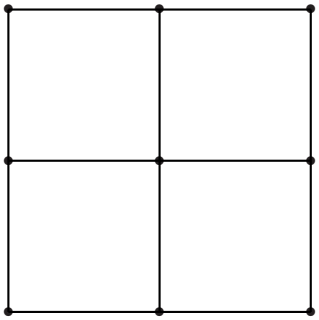
24. Encuentre los números cromáticos de los siguientes grafos:
(a) K_n (grafo completo de n vértices).
(b) C_n (ciclo de n vértices).
(c) El dibujo



25. Encuentre distintas numeraciones de los vértices de un cubo, de manera que el algoritmo greedy requiera 2, 3 y 4 colores.
26. Pruebe que para todo grafo se puede encontrar un orden de los vértices tal que el algoritmo greedy requiera una cantidad de colores igual al número cromático del grafo.
27. Sea Q_k el grafo que tiene como vértices las palabras de longitud k del alfabeto $\{0, 1\}$ y cuyas aristas unen las palabras que difieren en exactamente una posición.
(a) Dibuje Q_i para $i < 4$.
(b) Pruebe que Q_k es regular con valencia k.
(c) Pruebe que Q_k es bipartito.
28. Para $r \geq 2$, el grafo M_r se obtiene del grafo C_{2r} agregando las aristas que unen vértices opuestos. Pruebe que:
(a) r impar $\Rightarrow$ M_r es bipartito.
(b) r par y $r > 2$ $\Rightarrow$ $\Xi(M_r) = 3$.

(c) $\Xi(M_2) = 4$.

29. (a) Tiene el siguiente grafo un ciclo hamiltoniano?



(b) Sea G un grafo bipartito con una cantidad impar de nodos. Mostrar que G no tiene ciclos hamiltonianos.

30. Llamamos N_h al número de árboles con raíz no isomorfos de 5 vértices y altura h (dos árboles con raíz son isomorfos si existe un isomorfismo de grafos que lleva raíz en raíz). Halle N_h para $h = 1, 2, 3, 4$.
31. Construya dos árboles con raíz que posean 12 vértices, 6 hojas, tengan altura 4 y no sean isomorfos.
32. En un torneo de tenis participan 20 jugadores. el torneo se desarrolla usando el siguiente principio: el perdedor es eliminado. Pruebe que el ganador jugó al menos 5 partidos.
33. Encuentre árboles de expansión para el cubo y el grafo de Petersen.
34. Encuentre todos los árboles de expansión del grafo K_4.
35. Use el algoritmo de greedy para encontrar un árbol de expansión mínimo para el grafo del ejercicio 28 a). ¿Es único?
36. Sea G el grafo con vértices x, a, b, c, d, f y aristas con pesos dadas por:

xa	xb	xc	xd	xe	xf	ab	bc	cd	de	ef	fa
6	3	2	4	3	7	6	2	3	1	8	6

Encuentre todos los árboles expandidos mínimos.

Índice alfabético