Matemática Discreta. Teoría de Grafos y Aplicaciones a Grupos

Mª Eugenia Redondo González

Curso 2022 - 2023

Tutora: Consuelo Martínez López

Trabajo Fin de Grado en Matemáticas

Facultad de Ciencias

Universidad de Oviedo

Índice

1. Prefacio

Me parece muy curioso cómo es que he acabado haciendo la parte que más me gusta de las matemáticas cuando ya estoy casi al final de la carrera. Al pertenecer al doble grado, no he podido acceder de forma fácil a estas matemáticas tan divertidas que en este texto tengo la suerte de presentar.

Para mí ha sido muy complicado ponerle nombre a eso que tanto me atraía de las matemáticas: la combinatoria, el triángulo de Pascal que en su día también tuve la fortuna de estudiar en profundidad junto con la secuencia de Fibonacci, la búsqueda de primos... resulta que todo eso me estaba esperando aquí al final y se llamaba *matemática discreta*.

Gracias a las ramas de probabilidad, grafos y álgebra que me han acompañado durante la carrera, he podido asentar mi pequeña base conceptual y lógica que ha crecido enormemente en este texto, el cual espero que la muestre o, en el peor de los casos, al menos deje entrever el entusiasmo que me acompañó mientras lo escribía.

También estoy especialmente agradecida por un libro que me ha enseñado tantas cosas curiosas, que lo ha hecho a un nivel en el que verdaderamente siento que he aprendido y en el que está basado la mayor parte de este trabajo; se trata del *Discrete Mathematics* de L. Lovász, J. Pelikán y K. Vesztergombi [1].

Tres partes tiene el título y en tres partes se divide este texto.

La primera de ellas está dedicada a introducir de manera general la matemática discreta. Dado que ésta engloba un sinfín de ramas, decidí que quería poner mis favoritas y las que más tenía ganas de estudiar. Podría haber hablado de probabilidad pero he dedicado una asignatura a su estudio. Podría haber hablado de congruencias pero también las he manejado bastante. Quizás podría haber hablado de criptografía pero, en concreto, de este tema no conozco apenas nada ni

he podido estudiarla en estos años, así que los conocimientos que he aprendido de criptografía he preferido guardármelos para mí.

Así pues, el primer tema vencedor es la combinatoria, a la cual dedico un pequeño apartado para asentar algunas fórmulas que se utilizan posteriormente y también con el objetivo de decir ¡lo he logrado! ¡He conseguido entender lo que en tantas asignaturas se ha pasado por alto por darlo ya por sabido!

El segundo puesto (no precisamente en el sentido de un pódium) lo ocupan los ya mencionados triángulo de Pascal y secuencia de Fibonacci y en él esperan muchas identidades y relaciones numéricas curiosas dispuestas a ser desveladas.

Y el bronce se lo quedan la teoría de números con especial focalización en los números primos: las nociones de factorización única, algunos resultados famosos tanto resueltos como irresolubles a día de hoy y tests actuales para saber cuándo un número es primo.

La parte más extensa del texto está dedicada a teoría de grafos, que ocupa la segunda sección principal. Quizás todos los conceptos iniciales que hay de grafos, conexión, cadenas eulerianas, ciclos hamiltonianos y árboles sean en cierta manera conocidos. Yo he intentado no entretenerme mucho en aquellas cosas que ya sabía y centrarme en aquellas en las que no. Especialmente interesante me ha parecido la parte de cadenas eulerianas y ciclos hamiltonianos y la que he dedicado al conteo y almacenamiento de árboles etiquetados y no etiquetados.

He puesto todo el esmero que he podido en incluir multitud de grafos a lo largo del texto. En su mayoría, los grafos están realizados mediante el programa *Grafos* de Alejandro Rodríguez Villalobos y posteriormente retocados para incluir etiquetados, flechas, colores y otros detalles. Aquellos grafos que no posean una referencia (y esto lo extiendo a toda figura presente en el texto) están realizados por mí, basándome en muchos casos en los ya existentes en el *Discrete Mathematics*[1]. Además, para la traducción de muchos de los conceptos de grafos he utilizado el *Algoritmos en grafos y redes* de B. Pelegrín, L.Cánovas y P. Fernández [2].

Si la teoría de grafos es el pilar del trabajo, entonces el apartado de coloreado de grafos es el pilar de teoría de grafos. Es la parte que más he disfrutado entendiendo y explicando y sólo puedo esperar que se disfrute y se entienda de igual manera. Comienzo hablando de la fórmula de Euler y de grafos planares, luego paso a pintar con 2 colores regiones y grafos planares, subo de escalón pintando grafos planares con un número arbitrario de colores y finalizo con los teoremas de los colores. En particular, explico el *teorema de los seis colores* y entro en detalle acerca del *teorema de los cinco colores*, demostrándolo con todas las herramientas utilizadas en los apartados precedentes.

La última sección del trabajo está dedicada... más que a "aplicaciones" de la teoría de grafos a grupos en general, yo diría a *una* aplicación concreta de la teoría de grafos a grupos. Es relativa a la pregunta de Burnside: "¿Un grupo periódico y finitamente generado es necesariamente finito?" El artículo en el que está basada esta sección es el de *On the Burnside problem for period groups* de Narain Gupta y Said Sidki [3]. Las permutaciones de nodos en los grafos dan lugar una asociación entre la teoría de grafos y el álgebra de manera que se pueden definir elementos como grafos isomorfos o incluso utilizar automorfismos de grafos como elementos generadores de grupos, que es la construcción que realizo aquí.

Y ahora sin más dilación...

2. Matemática discreta

La matemática discreta es una rama de las matemáticas que se encarga de estudiar objetos que se pueden contar y que se encuentran "separados unos de otros", resultando así casi antagónica al análisis, con el que nació la matemática moderna y que trata de estudiar el mundo "continuo".

Engloba la **combinatoria**, casa de contar; la **teoría elemental de números**, palacio de los enteros, de divisores, de números primos; la **teoría de grafos**, encargada de las formas en que se pueden relacionar los objetos; la **geometría finita**, confiada al conteo de regiones y a salvaguardar criaturas matemáticas antiquísimas y tan extrañas como fascinantes; y tiene conexiones con la **cartografía**, como última aplicación de la teoría de grafos y de la geometría juntas; o la misteriosa **criptografía**.

Con aplicaciones en programación lineal, teoría de códigos y de computación, es imposible que la matemática discreta pase desapercibida a día de hoy. Casi parece extraño que englobe una parte de las matemáticas más arcaicas que se encuentran formalizadas.

En esta primera sección vamos a pasar brevemente por algunas herramientas de conteo y combinatoria que casi en su totalidad necesitaremos para llevar a cabo los cálculos a lo largo de todo el texto. Estudiaremos también el triángulo de Pascal y la secuencia de Fibonacci, haciendo alusión a algunas de las muchas identidades que verifican y finalizaremos hablando un poco de teoría de números, focalizándonos en muchas propiedades relativas a los esquivos números primos.

2.1. Herramientas combinatorias

La combinatoria es una rama base de la matemática discreta que nos proporciona herramientas para *contar* de forma rápida y eficaz. Desde saber cuántas maneras existen de colocar a un cierto número de personas sentadas alrededor de una mesa, calcular la probabilidad de ganar la lotería o de tener exactamente las mismas cartas en dos manos distintas de una partida de mus, hallar las

diferentes posibilidades de agrupar o distribuir objetos e incluso cuantificar cuántos anagramas se pueden hacer a partir de una serie de letras.

Tiene aplicaciones en probabilidad, en teoría de números, en criptografía... por no hablar de incontables juegos. En este primer apartado, vamos a enunciar brevemente algunas herramientas combinatorias que en muchos casos nos servirán de apoyo para los temas principales de los que hablaremos en posteriores páginas.

En primer lugar, enunciamos dos fórmulas sencillas de conteo. La primera se refiere a la cantidad de subconjuntos que se pueden construir a partir de un conjunto dado.

Teorema 2.1. *Un conjunto con n elementos tiene 2^n subconjuntos.*

En efecto, basta preguntarse si cada uno de los elementos del conjunto está o no en un subconjunto. Para cada elemento sólamente hay dos opciones, que esté o no esté, con lo cual basta multiplicar el número de opciones n veces. Otra forma de visualizar el número de opciones es construir un *árbol binario*, noción que nos aparecerá más adelante cuando hablemos de grafos. También se puede utilizar el código binario escribiendo, dentro de un subconjunto, un "0" si un elemento no está en el subconjunto y un "1" si lo está. En este caso, además, el código binario nos ayuda a *numerar* los subconjuntos en una lista y por tanto también a encontrar qué elementos tiene un subconjunto del cual sólo conocemos su posición en la lista.

En el caso particular en el que el número de subconjuntos es muy grande, quizás es más interesante saber *cuán* grande es dicho número, lo que se traduce en calcular el número de cifras que posee. Para calcular el número de cifras nos podemos ayudar de los logaritmos.

Por ejemplo, si tenemos un conjunto de 100 elementos, sabemos por el teorema 2.1 que tiene 2^{100} subconjuntos. Se trata de un número que se puede calcular mediante ordenadores, pues en una calculadora de mano da error por exceso de cifras. Buscamos pues dicho número de cifras tratando de hacer una cota inferior y otra superior. Supongamos que 2^{100} tiene k cifras, entonces

se tiene que

$$10^{k-1} \leq 2^{100} < 10^k.$$

Tomando logaritmos y denotando $x = 100 \log 2 \approx 30.10$

$$k - 1 \leq x < k,$$

equivalentemente, $k - 1 = \lfloor x \rfloor$, de donde se obtiene fácilmente que $k = 31$.

La segunda fórmula básica de la que podemos hablar trata de determinar la cantidad de secuencias de longitud n compuestas por símbolos de un conjunto de cardinal k y está motivada por la forma de codificar en binario que mencionamos antes, donde en cada posición sólo existían dos opciones. Así, a cada posición se le pueden asignar un número k de posibilidades distintas.

Teorema 2.2. *El número de secuencias de longitud n compuestas por k posibles elementos es k^n.*

Este resultado se puede extender al caso en el que para existen diferentes conjuntos de elementos asociados a cada una de las posiciones de la secuencia.

Teorema 2.3. *Sean n conjuntos de $k_1, k_2, ..., k_n$ elementos cada uno. Si queremos formar una secuencia de símbolos tal que para rellenar cada posición i utilizamos un elemento del conjunto asociado a k_i, entonces el número total de secuencias que se pueden hacer es $k_1 \cdot k_2 \cdots k_n$.*

Un conjunto ordenado donde se especifica la posición que ocupa cada elemento se conoce como *lista*. Si tenemos una lista de n elementos y los reordenamos de forma que tengan diferente colocación a la original estamos realizando una *permutación*. Nos interesa determinar de cuántas maneras se pueden reordenar n elementos distintos, lo cual es fácil de ver: en la primera posición podemos colocar n elementos, en la segunda hay $n-1$ posibilidades ya que poseemos un elemento menos, en la tercera $n - 2$, y así se continúa hasta que en la penúltima hay 2 posibilidades y la última está determinada por el resto. Así, el número de permutaciones es el producto de todas estas posibilidades, que enunciamos con el siguiente teorema.

Teorema 2.4. *El número de permutaciones de n objetos es $n!$*

Cabe destacar que, al igual que hablamos antes de un árbol de decisión binario, podemos construir en este caso un árbol de decisión de permutaciones para visualizar el mismo resultado.

Aparte de las permutaciones, una segunda herramienta de combinatoria son las *variaciones*. Las variaciones sirven para seleccionar k elementos elegidos en un conjunto de n elementos, que tienen que ser todos distintos.

Teorema 2.5. *El número de subconjuntos ordenados de k elementos en un conjunto con n elementos es*

$$\frac{n!}{(n-k)!} = n(n-1)\cdots(n-k+1). \tag{2.1}$$

Una tercera herramienta combinatoria son las llamadas *combinaciones*, a partir de la cual se deriva uno de los resultados de conteo más importantes.[1]

Teorema 2.6. *El número de subconjuntos de k elementos en un conjunto de n elementos es*

$$\binom{n}{k} = \frac{n!}{k!(n-k)!} = \frac{n(n-1)\cdots(n-k+1)}{k!}. \tag{2.2}$$

Demostración. *En primer lugar hay que tener en cuenta que si contamos los subconjuntos ordenados se obtiene $n(n-1)\cdots(n-k+1) = n!/(n-k)!$, por el teorema 2.5. Si lo que queremos es el número de subconjuntos no ordenados, basta notar que cada subconjunto lo hemos contado de hecho $k!$ veces, luego debemos dividir por $k!$ la ecuación 2.1 y así se completa la prueba.* □

Los números escritos en la forma $\binom{n}{k}$ reciben el nombre de *coeficientes binomiales* y satisfacen, entre otras, las siguientes propiedades.

Identidad 2.1.

$$\binom{n}{k} = \binom{n}{n-k}. \tag{2.3}$$

[1] En este contexto estamos trabajando con permutaciones, variaciones y combinaciones *sin* repetición; es decir, los elementos de los conjuntos considerados son todos distintos

Demostración. *Resulta de sustituir sin más en la ecuación 2.2:*

$$\binom{n}{k} = \frac{n!}{k!(n-k)!} = \frac{n!}{(n-k)![n-(n-k)]!} = \binom{n}{n-k}. \qquad \square$$

Aunque también es interesante probar la identidad anterior interpretando el número combinatorio que hay en cada miembro. Sea un conjunto S de n elementos. El miembro de la izquierda cuenta los subconjuntos de S que tienen k elementos y el de la derecha los que tienen $(n-k)$. Para ver que estos dos números son iguales basta darse cuenta de que por cada subconjunto de k elementos existe un subconjunto correspondiente de $(n-k)$ elementos: su complementario en S, que contiene exactamente aquellos elementos de S que no están en el subconjunto de k elementos. Debido a esto, se emparejan los subconjuntos de k elementos con los de $(n-k)$, con lo que efectivamente existe el mismo número de cada tipo.

Identidad 2.2. *Si $n, k > 0$, entonces*

$$\binom{n}{k} = \binom{n-1}{k-1} + \binom{n-1}{k}. \tag{2.4}$$

Demostración. *Esta segunda identidad se comprueba a partir de la fórmula de combinaciones 2.2 y operando:*

$$\frac{n!}{k!(n-k)!} = \frac{(n-1)!}{(k-1)!(n-k)!}\frac{n}{k} = \frac{(n-1)!}{(k-1)!(n-k)!}\left[1 + \frac{n-k}{k}\right]$$

$$= \frac{(n-1)!}{(k-1)!(n-k)!} + \frac{(n-1)!(n-k)}{(k-1)!(n-k)!k} = \frac{(n-1)!}{(k-1)!(n-k)!} + \frac{(n-1)!}{k!(n-k-1)!},$$

donde los últimos dos sumandos nos dan los números combinatorios de la derecha. $\square$

Identidad 2.3. *Si $n, k > 0$, entonces*

$$\binom{n}{0} + \binom{n}{1} + \binom{n}{2} + \cdots \binom{n}{n-1} + \binom{n}{n} = 2^n. \tag{2.5}$$

Demostración. *Esta tercera identidad de nuevo se puede probar por interpretación a partir de*

un conjunto S de n elementos. En el miembro de la izquierda se tiene que el primer término cuenta los subconjuntos de S de 0 elementos (que sólo hay uno, $\emptyset$), el segundo cuenta los subconjuntos de S de un elemento, el siguiente de dos elementos, etc. Así, la suma total de los términos, que es el miembro de la izquierda, es el número total de subconjuntos de S, contados cada uno exactamente una sola vez. Por el teorema 2.1, sabemos que este valor es 2^n, luego se comprueba el resultado. □

Tras haber visto permutaciones, variaciones y combinaciones, finalizamos este apartado con una fórmula para estimar el número $n!$, que nos será de utilidad más adelante. No daremos su demostración porque es un poco liosa, aunque se puede encontrar en muchos libros de cálculo, véase [4].

Teorema 2.7. ***Fórmula de Stirling***

$$n! \sim \left(\frac{n}{e}\right)^n \sqrt{2\pi n} \tag{2.6}$$

Aquí $\sim$ significa aproximadamente igual en el sentido

$$\lim_{n\to\infty} \frac{n!}{\left(\frac{n}{e}\right)^n \sqrt{2\pi n}} = 1.$$

2.2. El triángulo de Pascal y los números de Fibonacci

El triángulo de Pascal, nombrado así por el matemático y filósofo francés Blaise Pascal (1623 - 1662) es una figura compuesta por números que resultan ser los coeficientes binomiales de los que hemos hablado en el apartado anterior. Se utiliza para estudiar algunas de sus propiedades y su construcción es tal que, en la n-ésima fila contiene los números $\binom{n}{0}, \binom{n}{1}, ..., \binom{n}{n}$. En la figura 1, se ha dibujado hasta $n = 7$ (notar que la "primera"fila es la 0-ésima).

$$\begin{array}{c}
\binom{0}{0} \\
\binom{1}{0}\ \binom{1}{1} \\
\binom{2}{0}\ \binom{2}{1}\ \binom{2}{2} \\
\binom{3}{0}\ \binom{3}{1}\ \binom{3}{2}\ \binom{3}{3} \\
\binom{4}{0}\ \binom{4}{1}\ \binom{4}{2}\ \binom{4}{3}\ \binom{4}{4} \\
\binom{5}{0}\ \binom{5}{1}\ \binom{5}{2}\ \binom{5}{3}\ \binom{5}{4}\ \binom{5}{5} \\
\binom{6}{0}\ \binom{6}{1}\ \binom{6}{2}\ \binom{6}{3}\ \binom{6}{4}\ \binom{6}{5}\ \binom{6}{6} \\
\binom{7}{0}\ \binom{7}{1}\ \binom{7}{2}\ \binom{7}{3}\ \binom{7}{4}\ \binom{7}{5}\ \binom{7}{6}\ \binom{7}{7}
\end{array}
\qquad
\begin{array}{c}
1 \\
1\quad 1 \\
1\quad 2\quad 1 \\
1\quad 3\quad 3\quad 1 \\
1\quad 4\quad 6\quad 4\quad 1 \\
1\quad 5\quad 10\quad 10\quad 5\quad 1 \\
1\quad 6\quad 15\quad 20\quad 15\quad 6\quad 1 \\
1\quad 7\quad 21\quad 35\quad 35\quad 21\quad 7\quad 1
\end{array}$$

Figura 1: Triángulo de Pascal con los coeficientes binomiales y los números explícitos

A continuación, vamos a probar algunas identidades que se pueden extraer del triángulo de Pascal a partir de una de sus propiedades más importantes que, de hecho, vimos para los coeficientes binomiales en la Identidad 2.2: se trata de que cada número del triángulo se obtiene a partir de la suma de los dos que están sobre él (teniendo en cuenta que en los lados exteriores siempre se ponen unos). Además, también sirve para construir las nuevas filas del triángulo. Recordamos aquí simplemente la ecuación:

$$\binom{n}{k} = \binom{n-1}{k-1} + \binom{n-1}{k}. \tag{2.7}$$

Los dos siguientes resultados hacen referencia a qué ocurre si sumamos y restamos de forma alternada las cifras de la n-ésima fila del triángulo de Pascal. El primero utiliza todas las cifras de la fila y el segundo utiliza las $k+1$ primeras.

Identidad 2.4.

$$\sum_{k=0}^{n}(-1)^k\binom{n}{k}=0. \tag{2.8}$$

Demostración. *En el sumatorio:*

$$\binom{n}{0}-\binom{n}{1}+\binom{n}{2}-\binom{n}{3}+\cdots+(-1)^n\binom{n}{n}$$

se reemplazan los términos según la ecuación 2.7: $\binom{n-1}{0}=\binom{n}{0}$*; los intermedios* $\binom{n}{1}=\binom{n-1}{0}+\binom{n-1}{1}$, $\binom{n}{2}=\binom{n-1}{1}+\binom{n-1}{2}$*, etc. y, finalmente,* $\binom{n}{n}=\binom{n-1}{n-1}$ *(ambos extremos son 1). Así,*

$$\binom{n-1}{0}-\left[\binom{n-1}{0}+\binom{n-1}{1}\right]+\left[\binom{n-1}{1}+\binom{n-1}{2}\right]-\cdots$$
$$\cdots+(-1)^{n-1}\left[\binom{n-1}{n-2}+\binom{n-1}{n-1}\right]+(-1)^n\binom{n-1}{n-1},$$

luego el segundo término de cada corchete se cancela con el primero del siguiente corchete y por tanto el resultado es 0. □

Como anticipamos, si en vez de sumar todos los términos de la fila n-ésima cogemos los $k+1$ primeros se tiene la siguiente identidad.

Identidad 2.5.

$$\sum_{j=0}^{k}(-1)^j\binom{n}{j}=(-1)^k\binom{n-1}{k}. \tag{2.9}$$

Demostración. *Desarrollando el sumatorio:*

$$\binom{n}{0} - \binom{n}{1} + \binom{n}{2} - \binom{n}{3} + \cdots + (-1)^k \binom{n}{k},$$

y reemplazando los términos según la ecuación 2.7, se llega a

$$\binom{n-1}{0} - \left[\binom{n-1}{0} + \binom{n-1}{1}\right] + \left[\binom{n-1}{1} + \binom{n-1}{2}\right] - \cdots$$
$$\cdots + (-1)^k \left[\binom{n-1}{k-1} + \binom{n-1}{k}\right].$$

De nuevo aquí se cancelan todos los términos menos el último, por tanto el resultado da $(-1)^k \binom{n-1}{k}$. □

Otra de las interesantes relaciones numéricas que se dan en el triángulo de Pascal se halla a partir de la suma de los cuadrados de las cifras de cada fila. Por ejemplo, para las cinco primeras filas:

Fila	Suma de términos al cuadrado
0	$1^2 = 1$
1	$1^2 + 1^2 = 2$
2	$1^2 + 2^2 + 1^2 = 6$
3	$1^2 + 3^2 + 3^2 + 1^2 = 20$
4	$1^2 + 4^2 + 6^2 + 4^2 + 1^2 = 70$

Tabla 1: Suma de los cuadrados de las cifras de la n-ésima fila del triángulo

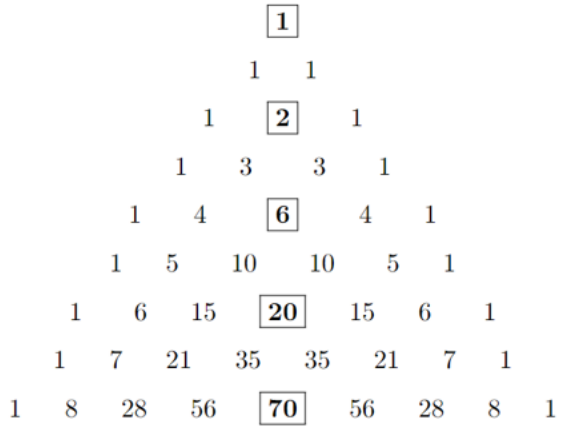


Figura 2: Triángulo de Pascal hasta la octava fila con los términos centrales señalados

Se reconocen estos términos como los correspondientes a la columna central del triángulo. Debido a que sólo tienen término central las filas pares, se sugiere la siguiente identidad.

Identidad 2.6.

$$\sum_{k=0}^{n} \binom{n}{k}^2 = \binom{2n}{n}. \tag{2.10}$$

Demostración. *Como ya hicimos en el apartado precedente, se puede dar una interpretación de ambos lados de la ecuación anterior en términos de la cantidad de subconjuntos dentro de un conjunto dado.*

El lado derecho es el número de subconjuntos de tamaño n que se pueden hacer dentro de un conjunto de $2n$ elementos, sea $S = \{1, 2, ..., 2n\}$.

El lado izquierdo tiene una interpretación un poco más intrincada. Considerando un término $\binom{n}{k}^2$ cualquiera, se quiere ver que es el número de subconjuntos de n elementos de S que contiene exactamente k elementos de $T := \{1, 2, ..., n\}$. El modo de elegir un subconjunto de tamaño n de S es elegir k elementos de T y $n - k$ elementos de $S \setminus T$. Lo primero se puede hacer de $\binom{n}{k}$ formas distintas y lo segundo de $\binom{n}{n-k}$ formas. De esta manera, elegir subconjuntos de tamaño n del conjunto S teniendo k elementos de T es:

$$\binom{n}{k} \cdot \binom{n}{n-k} = \binom{n}{k}^2.$$

Así, para obtener el número total de subconjuntos de tamaño n de S, habría que sumar el término $\binom{n}{k}^2$ anterior para $k = 0, 1, ..., n$, lo que concluye la prueba. □

Al sumar todos los términos de una fila del triángulo, a diferencia de cuando usamos la suma alternada en la identidad 2.4, nos estamos refiriendo a la identidad 2.3 que ya vimos para los coeficientes binomiales. Ésta la demostramos interpretando sus dos lados, aunque ahora podríamos hacerlo valiéndonos de la ecuación 2.7. Cabe destacar que, por el contrario, no se conoce una expresión sencilla para expresar la suma de los $k+1$ primeros términos de la fila, cosa que sí logramos ver con la suma alternada presente en la identidad 2.5.

Veamos una última relación entre los números presentes en el triángulo de Pascal. En esta ocasión, en vez de trabajar con filas, vamos a trabajar con la suma de términos que se encuentren en una diagonal, empezando por un 1 de la frontera:

$$\begin{aligned} 1 &= 1, \\ 1+3 &= 4, \\ 1+3+6 &= 10, \\ 1+3+6+10 &= 20, \\ 1+3+6+10+15 &= 35, \\ 1+3+6+10+15+21 &= 56. \end{aligned}$$

Como se puede observar en la figura 3, estas sumas en la diagonal dan precisamente los términos de la diagonal inmediatamente inferior.

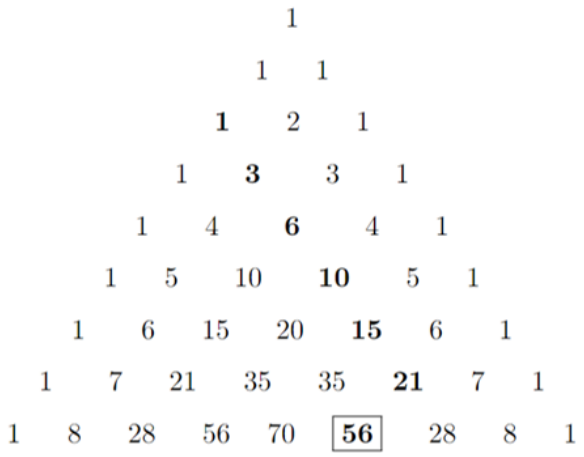


Figura 3: Triángulo de Pascal hasta la octava fila con una diagonal y su suma señaladas

Se intenta probar pues la siguiente identidad, que vamos a escribir en función de una diagonal que vaya de izquierda a derecha por facilidad en la notación, aunque se cumpla también para las diagonales contrarias por ser el triángulo simétrico.

Identidad 2.7.

$$\sum_{j=0}^{k} \binom{n+j}{j} = \binom{n+k+1}{k}. \tag{2.11}$$

Demostración. *Desarrollando la igualdad, tenemos:*

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

Vamos a probarla por inducción sobre k.

Si $k = 0$: la identidad se queda en $1 = 1$ luego es claramente cierta (para $k = 1$ es igualmente trivial, pues $1 + (n + 1) = n + 2$).

Hipótesis de inducción sobre k: supongamos que la identidad se cumple para un valor k, tal y como lo tenemos escrito.

Probemos que se cumple para $k+1$: es decir, queremos ver que

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

Por hipótesis de inducción, sustituimos los $k+1$ primeros términos del miembro de la izquierda en la expresión anterior. De este modo,

$$\binom{n+k+1}{k}+\binom{n+k+1}{k+1}=\binom{n+k+2}{k+1}$$

que, de hecho, es lo mismo que resulta de aplicar la propiedad básica del triángulo de Pascal, la ecuación 2.7, a $\binom{n+k+2}{k+1}$. Por tanto se verifica el resultado. □

Ya hemos visto algunas relaciones numéricas interesantes del triángulo de Pascal, además de algunas de sus características como la simetría, su construcción a partir de las filas anteriores y una rápida visualización y cálculo de grandes coeficientes binomiales. Quizás una de las propiedades más curiosas de esta figura es que la famosa secuencia de los números de Fibonacci se puede obtener a partir de la suma de términos en las "semidiagonales" del triángulo.[2]

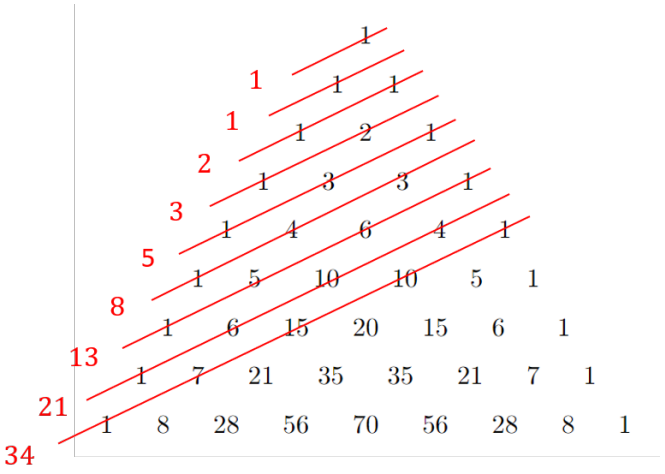


Figura 4: Obtención de los números de Fibonacci a partir del triángulo de Pascal

[2] ¡Y con esto ya hemos sumado términos del triángulo desde todo tipo de direcciones y podemos finalmente dejarlo tranquilo!

Los *números de Fibonacci*, llamados así por el matemático italiano del siglo XIII Leonardo Fibonacci, constituyen una secuencia de números en la que cada término se obtiene a partir de la suma de los dos anteriores. En efecto, se puede ver que la secuencia obtenida a partir del triángulo coincide con:

$$0, 1, 1, 2, 3, 5, 8, 13, 21, 34, 55, 89, 144, 233, ...$$

Los números de Fibonacci están definidos pues, por una relación de *recurrencia*. Hay quienes prefieren empezar la secuencia con 0, como hemos hecho aquí, para lo cual se propone la siguiente relación.

Definición 2.1. *La secuencia de Fibonacci se puede obtener a partir de* $F_0 = 0, F_1 = 1$ *y para* $n \geq 1$*:*

$$F_{n+1} = F_n + F_{n-1}. \tag{2.12}$$

Aunque también se puede tomar $F_1 = 1, F_2 = 1$ y $F_{n+1} = F_n + F_{n-1}$ para $n \geq 2$, para que la secuencia comience en 1 (que es la que propiamente vendría dada por el triángulo de Pascal).

Existen numerosas identidades que involucran los números de Fibonacci y la mayoría de ellas se resuelven de forma sencilla utilizando inducción. Por ello, en esta parte se va a demostrar una de las relaciones por inducción, de otras identidades simplemente dejaremos la fórmula, veremos además cómo construir la secuencia si en vez de empezar por dos "unos"se toman dos números arbitrarios A y B y finalmente obtendremos la secuencia original a partir de una fórmula que no es la de recurrencia.

Primero, vamos a visualizar las siguientes igualdades, que corresponden a la suma de los n primeros números de Fibonacci (desde $n = 0$ hasta $n = 5$):

$$\begin{aligned} 0 &= 0, \\ 0 + 1 &= 1, \\ 0 + 1 + 1 &= 2, \\ 0 + 1 + 1 + 2 &= 4, \\ 0 + 1 + 1 + 2 + 3 &= 7, \\ 0 + 1 + 1 + 2 + 3 + 5 &= 12. \end{aligned}$$

Notar que, si se suma 1 a la parte derecha de cada igualdad, se obtiene la secuencia de Fibonacci de nuevo, desplazada dos términos por delante, lo cual podemos expresar mediante la siguiente identidad.

Identidad 2.8.

$$\sum_{k=0}^{n} F_k = F_{n+2} - 1$$

Demostración. *Por inducción sobre n, como ya habíamos anticipado.*
Si $n = 0$ (o $n = 1$): la identidad es claramente cierta tal y como se ha expuesto antes.
Hipótesis de inducción para $n - 1$: supongamos que se verifica que

$$F_0 + F_1 + \cdots + F_{n-1} = F_{n+1} - 1.$$

Probemos que se cumple para n:

$$F_0 + F_1 + \cdots + F_n = (F_0 + F_1 + \cdots F_{n-1}) + F_n = (F_{n+1} - 1) + F_n,$$

Sin más que agrupar sumandos y utilizar la hipótesis de inducción. Al introducir la definición

de recurrencia 2.12 para $n+2$, finalmente:

$$(F_{n+1}-1)+F_n = F_{n+2}-1. \qquad \square$$

Algunas otras identidades entre los números de Fibonacci que se pueden demostrar también por inducción son las siguientes.

Identidades 2.10.

$$\sum_{k=1}^{2n-1} F_k = F_{2n}, \tag{2.13}$$

$$\sum_{k=0}^{2n}(-1)^k F_k = F_{2n-1}-1, \tag{2.14}$$

$$\sum_{k=0}^{n} F_k^2 = F_n \cdot F_{n+1}, \tag{2.15}$$

$$F_{n-1}F_{n+1} - F_n^2 = (-1)^n. \tag{2.16}$$

$$F_n^2 + F_{n+1}^2 = F_{2n-1} \tag{2.17}$$

La secuencia de Fibonacci surgió a raíz de un problema que planteó el propio Leonardo: *Un granjero cría conejos, los cuales dan a luz a partir del segundo mes de vida y desde entonces una vez por mes, sin que en ningún momento muera ninguno. ¿Cuántos conejos hay en el n-ésimo mes si se empieza con un conejo?*. Dejando de lado lo poco realista que es el problema, nos interesa preguntarnos cuál es el resultado si el granjero comienza con A conejos y al final del primer mes compra $B-A$ nuevos conejos, de manera que tenga B conejos durante el segundo mes.

Resulta que para obtener el número de conejos en el n-ésimo mes en este caso, sea E_n, se tiene para cada A y B una secuencia de Fibonacci *modificada*: $E_0 = A$, $E_1 = B$ y $E_{n+1} = E_n + E_{n-1}$, que podemos expresar en función de los F_n según el resultado siguiente.

Teorema 2.8. *Sean $E_0 = A$ y $E_1 = B$ los dos primeros términos de una secuencia que se construye como la de los números de Fibonacci, entonces el término E_n de la secuencia viene*

dado por:

$$E_n = F_{n-1}A + F_nB. \tag{2.18}$$

Demostración. *Por inducción sobre n.*

Si $n = 1$: $E_1 = F_0\ A + F_1\ B = 0 \cdot A + 1 \cdot B = B$, *se cumple.*

Hipótesis de inducción para $n-1$: supongamos que se verifica la fórmula hasta un valor $n-1$, $E_{n-1} = F_{n-2}A + F_{n-1}B$.

Probemos que se cumple para n:

$$\begin{aligned} E_n &= E_{n-1} + E_{n-2} = (F_{n-2}A + F_{n-1}B) + (F_{n-3}A + F_{n-2}B) \\ &= [(F_n - F_{n-1})A + F_{n-1}B] + [(F_{n-1} - F_{n-2})A + (F_n - F_{n-1})B] \\ &= [(F_n - F_{n-1})A + F_{n-1}B] + [(F_{n-1} - (F_n - F_{n-1}))A + (F_n - F_{n-1})B] \\ &= (F_n - F_{n-1} + F_{n-1} - F_n + F_{n-1})A + (F_{n-1} + F_n - F_{n-1})B = F_{n-1}A + F_nB. \end{aligned}$$

donde se ha usado la hipótesis de inducción y la definición 2.12 para sustituir los valores de F_{n-3} y F_{n-2}. □

Por último, vamos a expresar los números de Fibonacci a partir de una fórmula que involucre el valor n, sin ser de recurrencia. Para ello, el primer paso es ver que el cociente de dos números consecutivos de la secuencia se aproxima de hecho... ¡al número áureo! $\phi = \frac{1+\sqrt{5}}{2} \approx 1.61803...$

$$\left\{ \frac{F_{i+1}}{F_i} \;\middle|\; i \in \mathbb{N} \right\} = \{1, 2, 1.5, 1.66667, 1.60000, 1.62500, 1.61538, 1.61905, 1.61765, 1.61818, ...\}$$

El segundo paso, consiste en darse cuenta de que los cocientes parecen comportarse como una progresión geométrica, y por tanto formular una progresión de este tipo que satisfaga una relación de recurrencia parecida a 2.12. Proponemos $G_n = c \cdot q^n$ con $q, c \neq 0$ verificando 2.12, luego $G_{n+1} = G_n + G_{n-1}$ y, sustituyendo:

$$c \cdot q^{n+1} = c \cdot q^n + c \cdot q^{n-1} \ \sim \ q^2 = q + 1.$$

Hallamos los dos valores de q con los que se obtienen dos progresiones geométricas posibles que verifican 2.12, G_n y G'_n :

$$q = \frac{1+\sqrt{5}}{2} \approx 1.618034 \qquad \longrightarrow \qquad G_n = c\left(\frac{1+\sqrt{5}}{2}\right)^n,$$
$$q' = \frac{1-\sqrt{5}}{2} \approx -0.618034 \qquad \longrightarrow \qquad G'_n = c\left(\frac{1-\sqrt{5}}{2}\right)^n.$$

El tercer paso consiste en ver que cada una de estas progresiones por separado no dan lugar a F_n ya que, por ejemplo $G_0 = G'_0 = c \neq 0$. No obstante, como cada una satisface la relación 2.12

$$G_{n+1} - G'_{n+1} = (G_n + G_{n-1}) - (G'_n + G'_{n-1}) = (G_n - G'_n) + (G_{n-1} - G'_{n-1}),$$

$G_n - G'_n$ también verifica 2.12. Construimos $F_0 = G_0 - G'_0$ y tomamos $c = 1/\sqrt{5}$ luego $F_1 = G_1 - G'_1 = c\sqrt{5} = 1$ y junto con la relación anterior se pueden calcular los números de Fibonacci a partir de ambas progresiones: $F_n = G_n - G'_n$. De esta manera se establece el siguiente resultado.

Teorema 2.9. *Los números de Fibonacci se obtienen de la fórmula:*

$$F_n = \frac{1}{\sqrt{5}}\left(\left(\frac{1+\sqrt{5}}{2}\right)^n - \left(\frac{1-\sqrt{5}}{2}\right)^n\right) \tag{2.19}$$

Demostración. *Por inducción sobre n.*

Si $n = 0$ (o $n = 1$): la identidad es cierta sin más que sustituir el valor de n.

Hipótesis de inducción para $n-1$: supongamos que se verifica la identidad hasta $n-1$.

Probemos que se cumple para n: a partir de la definición 2.12 y sustituyendo por hipótesis de

inducción:

$$\begin{aligned}
F_n &= F_{n-1} + F_{n-2} \\
&= \frac{1}{\sqrt{5}}\left(\left(\frac{1+\sqrt{5}}{2}\right)^{n-1} - \left(\frac{1-\sqrt{5}}{2}\right)^{n-1}\right) + \frac{1}{\sqrt{5}}\left(\left(\frac{1+\sqrt{5}}{2}\right)^{n-2} - \left(\frac{1-\sqrt{5}}{2}\right)^{n-2}\right) \\
&= \frac{1}{\sqrt{5}}\left(\left(\frac{1+\sqrt{5}}{2}\right)^{n-2}\left(\frac{1+\sqrt{5}}{2}+1\right) - \left(\frac{1-\sqrt{5}}{2}\right)^{n-2}\left(\frac{1-\sqrt{5}}{2}+1\right)\right) \\
&= \frac{1}{\sqrt{5}}\left(\left(\frac{1+\sqrt{5}}{2}\right)^{n} - \left(\frac{1-\sqrt{5}}{2}\right)^{n}\right). \qquad \square
\end{aligned}$$

Así finaliza nuestro estudio de algunas propiedades del triángulo de Pascal y el tratamiento de los números de Fibonacci. En el siguiente apartado trataremos un ámbito más grande en el que se incluyen estas criaturas matemáticas.

2.3. Teoría elemental de números

Una de las áreas principales de la matemática discreta es la de *teoría de números* en la que se recogen las propiedades de los números enteros. Nació en la Grecia de la Edad Antigua y el hecho de que tenga cerca de 2500 años no sólo la convierte en una de las ramas más veneradas de todas las matemáticas, sino que también plantea la cuestión de que posiblemente ya esté casi todo descubierto dentro del mundo $\mathbb{Z}$.

Pero resulta que no podríamos estar más lejos de la verdad. Existen planteamientos de relaciones entre números enteros para los cuales a día de hoy no existe demostración formal por muy evidente que parezca el enunciado establecido. También existen otros resultados probados sólo apenas en el último siglo gracias, en parte, al avance de la tecnología y al desarrollo de programas de computación, que son capaces de analizar números gigantescos.

Y si desde hace tantos siglos ha existido una trepidante curiosidad por los números de $\mathbb{Z}$, no digamos ya la que acecha los números *primos*...

Un número $p \in \mathbb{Z}, p > 1$ recibe el nombre de *primo* si $\nexists\, l \in \mathbb{Z}, l \notin \{1, -1, p, -p\}$ tal que $l \mid p$. Es decir, un entero $p > 1$ es primo si no se puede escribir como producto de dos enteros mayores que 1 y menores que él. Por el contrario, un $n \in \mathbb{Z}, n > 1$ que no sea primo se dice *compuesto* (del inglés "composite").

Si un número entero mayor que uno no es primo, entonces se puede descomponer como producto de números primos. Además, dicha factorización es única. Este problema fue probado ya por los matemáticos de la antigua Grecia y también vamos a demostrarlo aquí, en el Teorema 2.10. Cabe destacar, no obstante, que a pesar de la importancia del resultado, a día de hoy no se conoce ningún método eficiente que ayude a calcular dicha descomposición.

Por supuesto, para encontrar la descomposición de números pequeños existen algunos trucos básicos: si el número es par entonces será múltiplo de 2, si la suma de sus cifras es múltiplo de 3 entonces será múltiplo de 3, si la última cifra acaba en 0 o 5 entonces es múltiplo de 5, etc.

Para los números grandes, los ordenadores prueban la divisibilidad primo por primo. En 2003, se conocía la descomposición de números de hasta 140 dígitos y no es probable que se conozca la de aquellos de 400 cifras o más en los próximos años. De hecho, la dificultad de encontrar las descomposiciones crece de forma exponencial con el número de dígitos.

Teorema 2.10. *Todo entero positivo se puede escribir como producto de primos, y esta factorización es única salvo por el orden de los factores primos.*

Demostración. *Lo primero es fácil de comprobar: si un entero mayor que 1, sea l, no es un primo, entonces se puede escribir como producto de dos enteros mayores que 1 y menores que él. Si alguno de estos dos últimos no es primo entonces repetimos lo anterior y lo escribimos como producto de otros dos enteros mayores que 1 y menores que él (si ninguno es primo reescribimos ambos). Reiterando el proceso, debemos acabar únicamente con un producto de primos igual a l. Por otro lado si l es un primo, entonces ya está descrito como producto de primos.*

Probemos ahora la unicidad. Supongamos que existen enteros con dos posibles factorizaciones en primos, y de todos ellos elijamos al más pequeño, sea n. Descompongamos n en dos

factorizaciones en primos:

$$n = p_1 \cdot p_2 \cdots p_m = q_1 \cdot q_2 \cdots q_k.$$

Supongamos, sin pérdida de generalidad, que p_1 *es el primo más pequeño de entre todos los factores* q_i *y* p_j *con* $i \in \{1, ..., k\}$, $j \in \{1, ..., m\}$. *Notar que* p_1 *no puede estar presente en las dos factorizaciones a la vez porque si no podríamos dividir ambas por* p_1 *y obtendríamos un número menor que* n *con dos factorizaciones, lo cual no puede ocurrir por la elección de* n.

$\forall i \in \{1, ..., k\}$ *se divide cada factor* q_i *por* p_1 *con resto:* $q_i = p_1 a_i + r_i$ *tal que* $0 \lneqq r_i < p_i$ *(*$r_i \neq 0$ *ya que el primo* p_1 *no puede ser divisor de otro primo* q_i*) y se define* $n' := r_1 \cdot r_2 \cdots r_k$.

Veamos que n' *tiene dos factorizaciones en primos. Una de ellas proviene de la definición de* n'. *Los* $r_i, i \in \{1, ..., k\}$ *no tienen por qué ser todos primos, pero los que no lo son pueden descomponerse en factores primos. Por otro lado, notar que* $p_1 \mid n'$ *ya que se puede escribir* n' *de la forma:*

$$n' = (q_1 - a_1 p_1)(q_2 - a_2 p_1) \cdots (q_k - a_k p_1),$$

y desarrollando, p_1 *divide a todos los términos. Esto es así porque* p_1 *divide a todos los términos que contengan a* p_1 *y el término restante es* $q_1 q_2 \cdots q_k = n$, *que también es divisible entre* p_1. *Así pues, se divide* n'/p_1 *y se continúa descomponiendo hasta tener la segunda factorización de* n' *en primos.*

Ambas factorizaciones son necesariamente diferentes porque p_1 *se encuentra en la segunda pero no en la primera, ya que todos los factores primos son estrictamente menores que* p_1.

Así, se tiene dos factorizaciones de n'. *Sin embargo, dado que* $r_i < p_1 < q_i$, $n' = r_1 r_2 \cdots r_k < q_1 q_2 \cdots q_k = n$, *se concluye que* $n' < n$, *lo que es una contradicción, pues habíamos supuesto que* n *era el menor entero con dos factorizaciones en primos.* □

El argumento que hemos utilizado para demostrar este resultado se conoce como *contraejemplo minimal*, "minimal criminal" en inglés. Se trata de una mezcla entre una prueba por reducción al absurdo y una prueba por inducción, ya que partimos de asumir la hipótesis que nos llevará a contradicción para el número más pequeño posible (el "criminal").

Otro de los resultados muy conocidos acerca de los números primos es uno que fue probado por Euclides en el siglo III a. C., aunque posteriormente se han dado varias posibles maneras de demostrarlo dada la sencillez de sus argumentos.

Teorema 2.11. *Existen infinitos números primos.*

Demostración. *Tenemos que demostrar que para cualquier entero positivo n, existe un número primo mayor que n. Sea $n! + 1 \in \mathbb{Z}$ y sea p uno de los primos en su factorización (notar que si no se factoriza en más primos es que él mismo es primo y claramente sería mayor que n). Supongamos que $p \leq n$, entonces $p \mid n! = n \cdot (n-1) \cdot (n-2) \cdots 2 \cdot 1$ ($n!$ es el producto de todos los enteros menores que n). Pero como $p \mid n! + 1$ y $p \mid n! \Rightarrow$ [3] $p \mid (n! + 1) - n! \Rightarrow p \mid 1$, lo cual no puede ocurrir. Por tanto, $p > n$.* □

La pregunta natural que surge tras saber que existen infinitos primos es acerca de su distribución en el conjunto de los enteros; en la figura 5, por ejemplo, se han representado los primos hasta el 1000. Aparentemente, no parece haber un patrón regular que explique cada cuántos números se puede encontrar un primo. Sin embargo, considerar la siguiente lógica: el 2 elimina de $\mathbb{Z}$ a la mitad de posibles candidatos a primo, pues son múltiplos suyos, el 3 a un tercio de ellos (aunque algunos ya los hubiéramos descartado por ser múltiplos de 2, como el 6), etc. Mejor que preguntarnos cada cuánto nos encontramos con un primo, ¿por qué no ver cuántos números compuestos consecutivos existen?

Figura 5: Gráfico señalando con barras los números primos entre 0 y 1000[5].

Teorema 2.12. *Para cualquier entero k existen k enteros compuestos consecutivos.*

[3] Si $a \mid b$ y $a \mid c \Rightarrow a \mid b - c$

Demostración. *Se puede probar con un argumento similar al de la demostración del Teorema 2.11. Sea* $n = k + 1$ *y consideremos los enteros:*

$$n! + 2, n! + 3, ..., n! + n.$$

Se tiene que ninguno de estos números es primo. El primero es divisible entre 2*, puesto que es par, al serlo* $n!$ $\forall n \in \mathbb{N}$*. El segundo es divisible entre* 3*, puesto que* $n! = n \cdot (n-1) \cdots 3 \cdot 2 \cdot 1$ *(asumiendo* $n > 2$*). Se ve que, de hecho,* $i \mid n! + i$ $\forall i = 2, 3, ..., n$*, por lo que se concluye que todos esos números no son primos y hemos encontrado* $n - 1 = k$ *enteros compuestos consecutivos.*

Así pues, podemos encontrar dos números primos consecutivos que están a una distancia el uno del otro mayor que cualquier k entero que queramos. Por el contrario, lo más cerca que pueden estar dos primos es siempre con una separación de un número par en medio (salvo el 2 y el 3). A dos primos cuya diferencia es dos se los conoce como *primos gemelos*. Por ejemplo, (3,5), (17,19) o (431,433) son parejas de primos gemelos.

Gracias a la computación, se sabe que hay primos gemelos de centenares de dígitos, aunque no se conoce con certeza si existen infinitos de ellos. Casi seguro que hay infinitos, pero en estos últimos 2000 años no se ha hallado una prueba formal que lo demuestre.

Como consecuencia también del Teorema 2.12, podemos preguntarnos si las ristras de números compuestos de una longitud k hacen que no existan primos de un determinado número de dígitos. La respuesta, no obstante, es negativa. Veremos un ejemplo más ilustrativo de ella tras el siguiente resultado.

Dejando un poco de lado las intrincadas maneras en las que se distribuyen los primos, ¿podríamos decir cuántos de ello hay hasta el entero n? A lo largo del siglo XVIII se observó empíricamente una fórmula que parecía aproximarse a esta respuesta, la cual denotamos $\pi(n)$. No obstante, su demostración no llegó hasta más de un siglo después, en 1896, de la mano de Hadamard y de la Vallée Poussin.

Teorema 2.13. ***El teorema del número primo.*** *Sea $\pi(n)$ el número de primos entre 1 y n Entonces*

$$\pi(n) \sim \frac{n}{\ln n}. \tag{2.20}$$

Se muestra la gráfica de la relación 2.20 en la figura 6 aunque la prueba es complicada, por lo que no la expondremos aquí. En cambio, daremos un ejemplo de su aplicación. Si queremos ver cuántos primos hay de 200 dígitos, nos fijamos primero en que estos números están entre 10^{199} y 10^{200} y después aplicamos la ecuación 2.20:

$$\frac{10^{200}}{200\ln 10} - \frac{10^{199}}{199\ln 10} \approx 1.95 \cdot 10^{197}.$$

Dado que hay $10^{200} - 10^{199} = 9 \cdot 10^{199}$ enteros de 200 dígitos, habrá un primo por cada 460 enteros de 200 dígitos aproximadamente:

$$\frac{9 \cdot 10^{199}}{1.95 \cdot 10^{197}} \approx 460.$$

Evidentemente, para ejemplificar que siempre va a haber primos de cualquier número de dígitos, no estamos dando argumentos muy precisos. Y además, hay que tener en cuenta que la relación acaba desviándose de la función de conteo de primos a medida que aumenta n, como se puede ver en las gráficas. Una aproximación más precisa viene dada por la función *logaritmo integral*: $\int_o^\infty \frac{dt}{\ln t}$ [6].

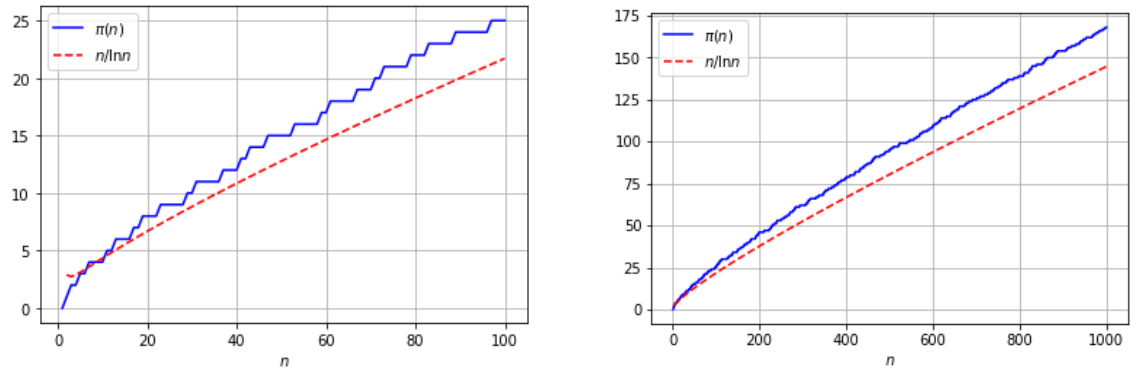


Figura 6: Gráficas de $\pi(n)$ y de $n/\ln n$ para n hasta 100 y hasta 1000.

A continuación, vamos a mencionar brevemente algunos otros famosos resultados sobre números primos, de formulación e idea muy sencilla y demostración fuera de nuestro alcance. Algunos han sido resueltos en los últimos años, otros siguen siendo a día de hoy, meras *conjeturas*.

Las primeras a las que nos referimos surgieron en 1742 a raíz de un intercambio de cartas entre Euler y Goldbach [7]. La conjetura de Goldbach establece que *todo entero par mayor que 2 se puede escribir como la suma de dos primos* y a día de hoy sigue sin estar resuelta. En cambio, en la década de 1930, Vinogradov probó para grandes números y quitando quizás la posibilidad de un número finito de excepciones, la conjetura (débil) de Goldbach, que establece que *todo entero impar mayor que 5 se puede escribir como la suma de tres primos.*

A mediados del siglo XIX, Chebyshev (o Tchebychev, o Tchebycheff, ¡o Tschebyscheff!) enunció y probó que *siempre hay un número primo entre* n *y* $2n$.

También ha sido probado recientemente que *siempre hay un primo entre dos cubos consecutivos.* Sin embargo el que *siempre hay un primo entre dos cuadrados consecutivos.* continúa sin solución.

A día de hoy se conocen algunos tests para comprobar si un número muy grande es primo. Por ejemplo, el *test de Fermat* utiliza que si un número p es primo entonces $p \mid 2^p - 2$ y también que si $p \neq 2$, entonces $p \mid 2^{p-1} - 1$. El test de Fermat también puede generalizarse respecto a una base a: se cumple que un entero positivo $n > 1$ es primo si y sólo si: $n \mid a^{n-1} - 1$ para toda base $a = 1, 2, 3, ..., n - 1$.

No obstante, no resulta completamente satisfactorio, pues existen algunos tipos de números que pasan el test de Fermat y no son primos e incluso otros que pasan el test generalizado para cualquier base a que sea coprima a ellos; es decir, n satisface $n \mid a^{n-1} - 1$ para todo a tal que $(n, a) = 1$. Los primeros se conocen como *pseudoprimos* y los segundos como *números de Carmichael.*

En la década de 1970, surgió el *test de Rabin-Miller* que mejoró ligeramente el test de Fermat solucionando el problema de los números de Carmichael y se basa en la idea de descomponer $a^{n-1}-1$ en un producto de factores. Por ejemplo, para el número 561, que es el primer número de Carmichael,

$$\begin{aligned} a^{560}-1 &= (a^{280}-1)(a^{280}+1) \\ &= (a^{140}-1)(a^{140}+1)(a^{280}+1) \\ &= (a^{70}-1)(a^{560}+1)(a^{140}+1)(a^{280}+1) \\ &= (a^{35}-1)(a^{35}+1)(a^{70}+1)(a^{140}+1)(a^{280}+1). \end{aligned}$$

Suponiendo que 561 fuera primo, $561 \mid a^{560}-1$ para todo $1 \leq a \leq 560$ y si un primo divide a un producto entonces también tiene que dividir a alguno de los factores. Así, 561 debería dividir a alguno de los factores de la última línea, pero para $a = 2$ esto no se cumple.

El test de Miller-Rabin es una elaboración de esta idea: dado un entero impar $n > 1$ que queramos ver que es primo, elegimos un entero a del rango $1 \leq a \leq n-1$ cualquiera, consideramos $a^n - a = a(a^{n-1}-1)$ y lo factorizamos siguiendo la identidad $x^2-1 = (x-1)(x+1)$ todo lo que podamos. Finalmente se verifica que al menos uno de los factores tiene que ser divisible entre n.

Si el test falla entonces n no es primo, pero si no falla ¡aún puede ocurrir que n no sea primo! Entonces entra en juego el repetir el test una gran cantidad de veces y a usar probabilidad aunque, en general, la probabilidad de cometer error es pequeña y este test es ampliamente utilizado.

Respecto a números compuestos, si tenemos uno muy grande y lo queremos descomponer en el producto de dos más pequeños, no existe ningún método eficiente que nos ayude a hacerlo ni tan siquiera una prueba matemática de que dicho método no existe. Pero dentro de lo malo, hay que mirar el lado positivo y es que gracias a que no se conoce ningún procedimiento óptimo de descomposición, los números encuentran otras utilidades en ramas como la criptografía.

3. Teoría de grafos

Extraño es encontrar un libro de teoría de grafos que no comience ilustrando esta rama principal de la matemática discreta mencionando el problema con la que probablemente se originó: el conocido como los puentes de Königsberg.

Cuenta la historia [8] que la ciudad de Königsberg (actual Kaliningrado) estaba dividida en cuatro distritos separados por el río Pregel, que atravesaba la zona. Los distritos estaban conectados entre sí por siete puentes y las gentes del lugar se preguntaban si existía alguna forma de cruzar por todos ellos exactamente una sola vez durante el mismo paseo. En 1736, Leonhard Euler publicó la solución al problema tras haberlo modelizado matemáticamente: era imposible realizar aquellas andanzas.[4]

Se puede llegar a esa conclusión completando una lista con todas las posibles rutas a seguir partiendo desde cada distrito, pero sería poco práctico y únicamente aplicable a este problema en particular. Euler logró formular un criterio general para saber si ese paseo sería posible en una ciudad con cualquier número de distritos y puentes, lo que resultó en el primer teorema conocido acerca de la teoría de grafos, aunque el término no se empezaría a utilizar hasta un siglo después.

Figura 7: Los puentes de Königsberg el grafo que modeliza el problema [9].

[4]Cabe destacar que actualmente sí se puede realizar dicho paseo por la ciudad, puesto que dos de los puentes fueron derribados durante la Segunda Guerra Mundial dejando, curiosa y tristemente, resuelto el problema.

Así que, ¿qué es un grafo? De forma ilustrativa, un grafo es un diagrama de puntos (o de pequeños círculos para visualizarlos mejor) que pueden estar unidos por una serie de líneas que indican algún tipo de relación. No se trata de una representación geométrica exacta, esto es, no es relevante que las líneas sean curvas o rectas; lo único importante es qué dos puntos une cada línea. Este simple diagrama, normalmente representado en un plano, contiene toda la información que se necesita para resolver un problema de teoría de grafos. En la figura 7 se puede ver el grafo que modeliza el problema de los puentes de Königsberg.

A lo largo de esta sección, resumiremos algunas nociones básicas de grafos junto con resultados principales de teoría, nos centraremos en un tipo especial de grafos llamados árboles y dedicaremos un apartado a hablar del coloreado de grafos para concluir con el llamado *teorema de los cuatro colores*.

3.1. Preliminares

En este apartado introductorio vamos a centrarnos en los componentes de un grafo, algunos tipos especiales de grafo, el concepto de conexión a partir de cadenas y ciclos y finalmente *cadenas eulerianas* y *ciclos hamiltonianos*.

3.1.1. Nociones básicas

Un grafo es un par formado por un conjunto de *nodos* (o *vértices* o *puntos*), V, que representan objetos cualesquiera y un conjunto de parejas de nodos, E, tal que una pareja de nodos $\{u, v\}$ indica que existe una conexión entre los nodos u y v. Lo denotamos así: $G = (V, E)$.

Un grafo se dice que es *orientado* (o *dirigido*) si se tiene en cuenta el orden de la conexión entre dos nodos; es decir, si $\{u, v\} \neq \{v, u\}$. En este caso, los pares de nodos reciben el nombre de *arcos* y se suelen dibujar mediante flechas para indicar el sentido. Si no importa el orden en que se escriban los nodos el grafo se dice que es *no orientado* (o *no dirigido*); es decir, se considera que $\{u, v\} = \{v, u\}$ y estos pares reciben el nombre de *aristas* o *ejes*, que se dibujan sin flechas.

Si $|V|$ es finito diremos que G es *finito*. Si dos nodos $u, v \in V$ están conectados por una arista o arco, diremos que son *adyacentes*. Los nodos adyacentes a un nodo u se dice que son sus nodos *vecinos*. Definimos también el *grado de incidencia de un vértice* como el número de nodos vecinos de dicho vértice. Si estamos considerando grafos orientados se puede diferenciar entre el *grado de incidencia de entrada* y el *grado de incidencia de salida*, según el sentido de los arcos entrantes y salientes a los nodos vecinos.

La arista o arco $\{u, v\}$ se denotará sencillamente por uv. En un grafo puede haber una arista que conecte un nodo consigo mismo: uu, lo que se conoce como *bucle*. También puede ocurrir que exista un número p de aristas que conecten u y v, por lo que el grafo se llama *p-Grafo* o *multigrafo de orden p*. El tipo más habitual de grafos son los *1-grafos*. Si un 1-grafo no contiene bucles, hablaremos de un grafo *simple*.

Vamos a trabajar con grafos finitos, simples y no orientados a no ser que especifiquemos lo contrario.

Existen también algunas estructuras asociadas a un grafo que merecen mención. Dado un grafo $G = (V, E)$ se definen:

- *Subgrafo*: un subgrafo $G' = (V', E')$ del grafo G es un grafo tal que $V' \subseteq V$ y $E' \subseteq E$.
- *Subgrafo inducido*: es un subgrafo de la forma $G' = (V, E')$.
- *Grafo inducido*: es un subgrafo de la forma $G_W = (W, E_W)$ con $W \subseteq V$ y $E_W = \{uv \in E : u, v \in W\}$.
- *Grafo complementario*: llamamos grafo complementario de G al grafo $\bar{G} = (V, \bar{E})$ siendo $\bar{E} = \{uv : uv \notin E\}$.

Ahora que ya hemos resumido muchos de los conceptos básicos, vamos a ilustrar algunos resultados básicos de teoría de grafos.

Supongamos que en una fiesta hay 47 personas, y vamos a intentar probar que siempre al menos una de ellas conoce a un número par de las otras. Este es un claro ejemplo de problema que es muy fácil resolver mediante grafos (evidentemente se podría hacer una larga lista con los conocidos de cada uno de los invitados, pero resultaría en un proceso largo). También se puede empezar resolviendo el problema con un número más pequeño. Lo primero que notamos, en ese caso, es que si el número de invitado es par, el resultado no tendría por qué ser cierto. Si la fiesta tuviera solo 12 personas y todas se conocieran entre sí, cada una de ellas conocería a las otras once, y por tanto no habría ninguna que conociera a un número par de las otras.

Así que, mejor que el planteamiento anterior, y con esa idea de que si el número de invitados es par o impar influye en la solución, vamos a tratar de resolver un problema más general: *en una fiesta con un número impar de invitados, siempre hay al menos uno que conoce a un número par de los otros.* Si consideramos $V = \{invitados\}$ y $E = \{invitados\ que\ se\ conocen\}$ tenemos, en lenguaje de grafos: *si un grafo tiene un número impar de nodos, entonces tiene un nodo con grado de incidencia par.*

Pero dibujando algunos ejemplos sencillos, como los de la figura 8, se ve que este enunciado no lo cumple sólamente un nodo, sino un número impar de nodos. Es decir, *si un grafo tiene un número impar de nodos, entonces el número de nodos con grado de incidencia par es impar.* Y, análogamente, experimentando con grafos con un número par pequeño de nodos, se ve que *si un grafo tiene un número par de nodos, entonces el número de nodos con grado de incidencia par es par.*

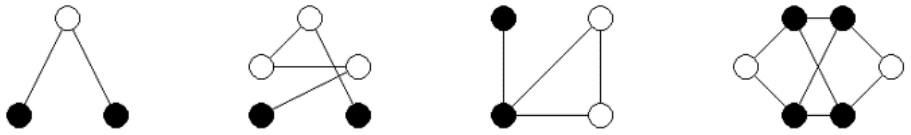


Figura 8: cuatro grafos con los nodos pintados en blanco si su grado de incidencia es par y en negro si es impar.

Llegados a este punto, si en vez de fijarnos en los nodos con grado de incidencia par, lo hacemos con los que tienen grado de incidencia impar, logramos unificar los dos enunciados anteriores en el siguiente teorema.

Teorema 3.1. *En todo grafo, el número de nodos con grado de incidencia impar es par.*

Demostración. *Se toma un grafo sin aristas cualquiera, en cuyo caso el grado de incidencia de cada nodo es 0, que es par, y vamos añadiendo las aristas progresivamente (ver figura 9), con lo que cambia la paridad del grado de incidencia de los nodos que se unen:*

- *si los nodos adyacentes de la nueva arista tenían ambos grado par, entonces el número de nodos con grado impar aumenta 2 unidades;*
- *si los nodos adyacentes de la nueva arista tenían ambos grado impar, entonces el número de nodos con grado impar decrece 2 unidades;*
- *si un nodo adyacente de la nueva arista tenía grado par y el otro tenía grado impar, entonces el número de nodos con grado impar se mantiene.*

Por tanto, si el número de nodos con grado impar era par antes de añadir la nueva arista, se mantiene par tras añadir la nueva arista. □

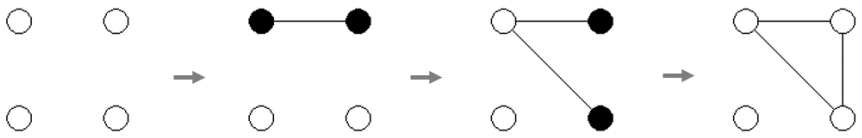


Figura 9: Construcción de un grafo arista por arista. En blanco los nodos con grado de incidencia par y en negro los de incidencia impar.

Otra noción que se puede estudiar a partir del problema anterior es intentar encontrar el número de aristas que contiene un grafo. Para ello se suman los grados de incidencia de todos los nodos. No obstante, como nos encontramos en grafos no orientados, la arista uv y la arista vu que son la misma, se están contando dos veces, por lo que es necesario dividir la suma final entre dos.

Teorema 3.2. *La suma de los grados de incidencia de todos los nodos de un grafo es el doble del número de aristas.*

De hecho, con este resultado se puede obtener una nueva prueba del Teorema 3.1: es consecuencia inmediata que la suma de todos los grados de incidencia en cualquier grafo es un número par. Si omitimos los términos pares de esta suma el resultado sigue siendo par. Es decir, la suma de todos los grados de incidencia impares es par, lo cual solo es posible si el número de grados de incidencia impar es también par (ya que la suma de un número impar de términos impares es impar).

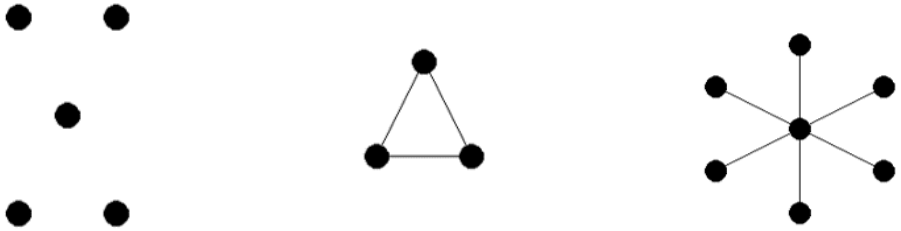
3.1.2. Conexión

En este apartado, comenzaremos mencionando varios tipos notables de grafos y nos centraremos en los conceptos de caminos y ciclos, que dan lugar a la *conexión* en grafos.

Los grafos más simples que hay son aquellos denominados *grafos vacíos* que tienen un número cualquiera de nodos pero no contienen ninguna arista.

En la situación opuesta nos encontramos con los grafos que más aristas poseen: aquellos que para cualquier par de nodos existe una arista que los une; reciben el nombre de *grafos completos de n nodos* y se denotan por K_n. Este tipo de grafos nos aparecerá en apartados posteriores porque tienen algunas cualidades interesantes. Se sabe, por ejemplo, que poseen $\binom{n}{2}$ aristas, ya que en términos de combinatoria se refiere a la cantidad de maneras en que se puede poner una arista entre 2 nodos si en total se tienen n nodos.

Un último tipo de grafos que mencionamos aquí es el *grafo estrella* que, como su propio nombre señala, es aquel en el que un único nodo se conecta al resto. Si este grafo tiene n nodos tendrá, por tanto $n-1$ aristas.



(a) Grafo vacío de 5 nodos. *(b) Grafo completo K_3.* *(c) Grafo estrella de 7 nodos.*

Figura 10: Algunos tipos especiales de grafos

En un grafo no orientado, una secuencia alternante de aristas y nodos consecutivos que empieza en un nodo y finaliza en otro nodo se conoce como *cadena*. El primer y último nodo del camino se denominan *extremos*. Si además conectamos los nodos extremos se obtiene un *ciclo*. Se llama *longitud* al número de aristas que conforman una cadena o un ciclo y en particular un ciclo de longitud k se suele llamar *k-ciclo*.

Cabe destacar que, para el caso de grafos orientados, se prefiere el uso del término *camino* en vez de cadena y *circuito* en vez de ciclo.

Una *cadena simple* es un tipo de cadena en la que cada arista aparece una sola vez. Además, hablaremos de *cadena elemental* si cada vértice aparece una sola vez. De forma más matemática, dado un grafo G, una *cadena elemental* es una secuencia de nodos $v_0, v_1, ..., v_k$ tales que v_i es adyacente a V_{i+1} $\forall i \in \{0, ..., k-1\}$. Si en una cadena $v_0 = v_k$, entonces se dice que es un *ciclo elemental*.

- Si una cadena elemental posee n nodos entonces tiene $n-1$ aristas.
- Una cadena elemental es una cadena simple: en una cadena simple, si un nodo v posee varias aristas de paso, es posible trazar la cadena sin repetir dichas aristas aunque se pase por el vértice v varias veces; en cambio una cadena elemental impide volver a pasar por el nodo v si ya se ha hecho una vez, dejando las aristas que se conectan a él inutilizadas.

- Se puede decir que una cadena elemental es una cadena sin repeticiones (ni de nodos ni de aristas).
- Como curiosidad, en inglés se denomina *walk* a una cadena y *path* a una cadena elemental.

Dado un grafo G y u, v y w tres nodos suyos, si u y v están conectados por una cadena elemental P y v y w están conectados por otra cadena elemental Q, entonces los nodos u y w están claramente conectados, porque se puede recorrer primero el tramo entre u y v, y después el tramo v y w. Sin embargo, cabe destacar que concatenar las cadenas P y Q, no necesariamente da lugar a otra cadena elemental, ya que pueden intersecarse en aristas y nodos que tengan en común.

Para construir una cadena elemental entre u y w a partir de los anteriores, bastaría comenzar el camino P en u y seguirlo hasta encontrarnos con el primer nodo en común que haya con el camino Q, para acabar recorriendo Q hasta llegar a w. De esta manera, claramente cada uno de los nodos por los que transcurre nuestra cadena es distinto a los demás ya que los nodos de P no están en Q, los de Q no están en P y sólo hay un único nodo común.

Un grafo G se dice que es *conexo* si para cada dos nodos del grafo existe un cadena que los une. Más precisamente, si para cada dos nodos del grafo u y v existe un cadena de extremos u y v que es un subgrafo de G.

Llamamos *componente conexa de un grafo* G a un subgrafo maximal H de G que es conexo. Es decir, H es una componente conexa si es conexa y cualquier otro subgrafo de G que contenga a H no es conexo.

3.1.3. Cadenas eulerianas y ciclos hamiltonianos

Son de especial importancia los llamados *caminos eulerianos* y *caminos hamiltonianos* en grafos orientados, aunque también se pueden estudiar en grafos no orientados y por eso vamos a referirnos a ellos como *cadenas eulerianas* y *cadenas hamiltonianas*.

Dado un grafo no orientado, una *cadena euleriana* es una cadena que que recorre todas las aristas del grafo exactamente una sola vez. Si es cerrado, hablaremos de un *ciclo euleriano*. Existe un interés especial en ver si un grafo contiene una cadena o ciclo euleriano porque tiene muchas aplicaciones, como por ejemplo, planificar un viaje por distintas ciudades o para limitar los costes en problemas de distribución.

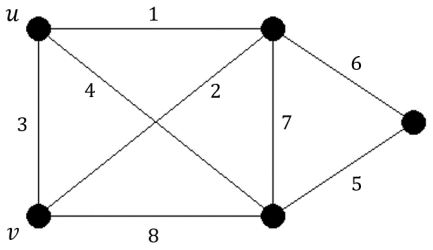


Figura 11: Grafo con cadena euleriana de u a v.

La cuestión de si un grafo contiene una cadena euleriana es, de hecho, la misma pregunta al problema del paseo sobre los puentes de Königsberg que mencionamos al comienzo de esta sección y, a continuación, se muestra la solución general que formuló Euler.

Teorema 3.3. *Se da uno de los siguientes casos:*

(a) Si un grafo conexo tiene más de dos nodos con grado impar, entonces no posee ninguna cadena euleriana.

(b) Si un grafo conexo tiene exactamente dos nodos con grado impar, entonces posee una cadena euleriana. Cada cadena euleriana debe empezar en uno de estos dos nodos y acabar en el otro.

(c) Si un grafo conexo no tiene nodos con grado impar, entonces posee cadenas eulerianas. Además, cada cadena euleriana es un ciclo euleriano.

Demostración. *En primer lugar, notar que si un nodo v tiene grado impar, entonces todas las cadenas eulerianas deben comenzar o terminar en v, ya que si no siempre quedaría una de las aristas sin recorrer. De forma análoga, se puede ver que si un nodo v tiene grado par, entonces toda cadena euleriana ora comienza y finaliza en v, ora empieza y finaliza en cualquier otro nodo del grafo. Esta observación implica directamente (a) y las segundas aserciones en (b) y (c).*

Así pues, sólo queda por probar que si un grafo conexo tiene 0 o 2 nodos con grado impar, entonces posee una cadena euleriana. Vamos a probar la parte (c), para ver cuáles son los razonamientos.

Supongamos que el grafo no contiene ningún nodo con grado impar. Sea v cualquiera de sus nodos. Consideramos una cadena cerrada que empieza y termina en v y usa cada arista como mucho una vez. Esta cadena siempre existe porque podemos tomarla tal que se componga únicamente del nodo v, aunque notar que queremos que sea lo más larga posible. Tomamos pues la mayor cadena cerrada que cumpla lo anterior, sea W, y queremos comprobar que W es una cadena euleriana.

Por reducción al absurdo supongamos que no lo es. Entonces existe al menos una arista, e, que no se encuentra en W. Esta arista se puede elegir de manera que W pasa por lo menos por uno de sus dos vértices. De hecho, si p y q son los vértices de e y W no pasa por ninguno de ellos, entonces se puede tomar la cadena elemental de p a v (que existe porque el grafo es conexo) y mirar el primer nodo r en esta cadena elemental que también está en W. Sea $e' = sr$ la arista de la cadena elemental justo anterior a r. Así, W no pasa a través de e (porque no pasa a través de s), por lo que podemos reemplazar e por e' cuyo extremo r está en W.

Así, sea e la arista que no está en W pero cuyo extremo p sí que se encuentra en W. Entonces comenzamos una nueva cadena W' en p. La empezamos pasando por e y continuamos teniendo cuidado de que no usemos las aristas de W y no usemos ninguna de las aristas dos veces.

En algún momento la cadena se atasca en un nodo u, supongamos $u \neq p$, tal que tiene grado par. W utiliza un número par de las aristas que inciden en u y W' utiliza una de entrada, por lo que se tiene un número impar de aristas que no son aristas ni de W ni de W'. Pero esto significa que en realidad W' puede continuar a partir de u, y el único nodo donde se atasca es el p.

Esto significa que W' es una cadena cerrada. Así, cogemos una cadena, W'' tal que empieza en v, sigue la cadena elemental W hasta el nodo p, después la cadena elemental W' que retorna hasta p y finalmente retoma W hasta volver a v. W'' es una cadena que comienza y termina en v, utiliza cada arista del grafo una sola vez y es más larga que W, por lo que llegamos a

contradicción. □

Una pregunta similar a la de las cadenas eulerianas fue formulada por William R. Hamilton en 1856. En vez de tratar encontrar una cadena que utilizara todas las aristas de un grafo sin que se repitiera ninguna, ¿se podía hacer lo mismo con los nodos? La cuestión acabó conociéndose como *el problema del ciclo de Hamilton.*

Un *ciclo hamiltoniano* es un ciclo que contiene los nodos del grafo. Parece una bonita simetría que las cadenas eulerianas se encarguen de seleccionar las aristas sin que se repita ninguna y los ciclos hamiltonianos se encarguen de marcar el orden de los nodos sin que se repita ninguno.

Sin embargo, la bonita simetría acaba en el enunciado del problema. El conocimiento que tenemos acerca de los ciclos hamiltonianos es mucho menor que el de las cadenas eulerianas. No se conoce ninguna manera eficiente de ver si un grafo contiene un ciclo hamiltoniano y no existe ninguna condición realmente útil que sea necesaria y suficiente para encontrar tal ciclo en un grafo. Un grafo con un número alto de nodos puede tener un ciclo hamiltoniano frente a otro con un número mucho menor de nodos. En la figura 12 se aprecia un caso en el que ocurre esto.

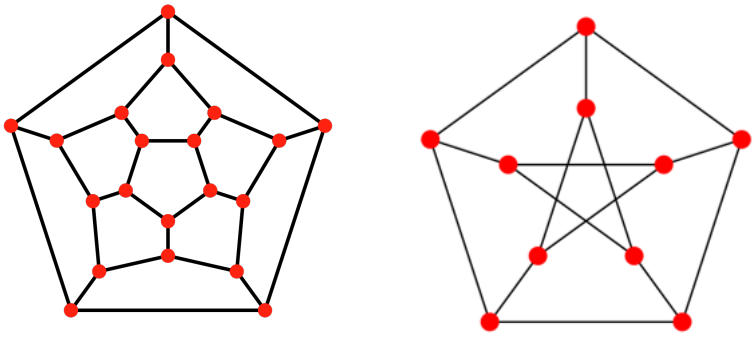


Figura 12: A la izquierda, grafo dodecaedro [10] con ciclo hamiltoniano y a la derecha, grafo de Petersen [11] sin ciclo hamiltoniano.

3.2. Árboles

Mencionamos los árboles al introducir la matemática discreta, como ayuda para problemas de enumerar y conteo. En este apartado, veremos más propiedades acerca de este tipo especial de grafos.

3.2.1. Nociones básicas

Formalmente, un grafo $G = (V, E)$ se dice que es un *árbol* si es conexo y no contiene ningún ciclo. Además, si se le quita una arista se vuelve inconexo y si se le añade una arista entonces tiene al menos un ciclo.

Teorema 3.4. *Los árboles son minimalmente conexos y maximalmente acíclicos:*

(a) Un grafo G es un árbol si y sólo si es conexo pero al eliminar una cualquiera de sus aristas se vuelve inconexo.

(b) Un grafo G es un árbol si y sólo si no contiene ningún ciclo, pero al añadirle una arista cualquiera se crea un ciclo.

Demostración.

(a)

$\Rightarrow$ *Como G es un árbol, por definición es conexo. Por reducción al absurdo, supongamos que al eliminar una arista cualquiera uv el subgrafo resultante, G' es conexo. En ese caso existiría un camino P en G' que une los vértices u y v. Si añadimos de nuevo la arista uv a G', resulta que el camino P y la arista uv formarían un ciclo en G, lo cual es una contradicción porque por definición, G es un árbol.*

$\Leftarrow$ *Claramente G es conexo, luego sólo falta ver que no tiene ciclos. Por reducción al absurdo, supongamos que G contiene un ciclo C. Entonces, si eliminamos una arista cualquiera de C se obtiene un grafo conexo, lo cual contradice la hipótesis.*

(b)

$\Rightarrow$ *Como G es un árbol, por definición es acíclico. Añadirle cualquier arista tiene que dar lugar a un ciclo, pues por ser un árbol es conexo y existe un camino entre un par cualquiera de nodos.*

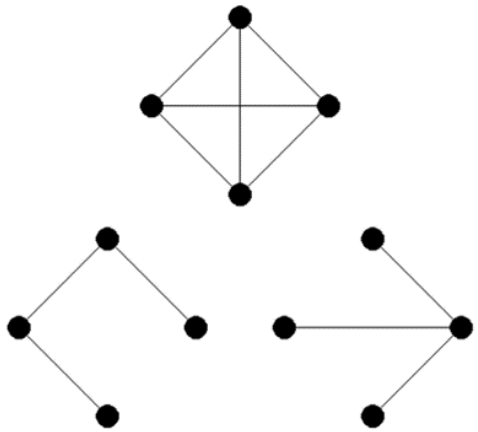
Si no diera lugar a un ciclo significaría que uno de los dos nodos no está conectado con ningún otro del grafo, contradiciendo la conexión de G.
$\Leftarrow$ Por hipótesis el grafo G es acíclico. Si al añadirle cualquier arista a G se forma un ciclo entonces es conexo, ya que o bien dos nodos cualesquiera u y v están conectados por una arista o bien al añadir una arista que los conecta se crea un ciclo, que contiene un camino entre u y v en el grafo original. Así, G es un árbol. □

Tras haber visto la definición y dos caracterizaciones de árbol, veamos algunos conceptos y propiedades ligados a ellos.

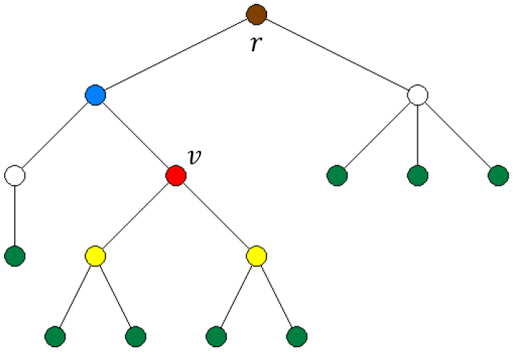
Si tenemos un grafo conexo y al quitarle una arista se obtiene un grafo inconexo se dice que la arista es una *arista puente*. Por lo visto en el teorema anterior, es claro que **toda arista de un árbol es una arista puente**. Por otro lado, si de un grafo conexo cualquiera (que puede tener ciclos) se van suprimiendo aristas pero se mantiene el mismo conjunto de nodos, el tipo de árbol al que se llega recibe el nombre de *árbol de unión* y no tiene por qué ser único (ver figura 13a). En un árbol, se puede elegir un nodo cualquiera y llamarlo *raíz* con motivo de diferenciarlo del resto y de recibir algunas características.

Sea un árbol $G = (V, E)$ con raíz $r \in V$ y $r \neq v \in V$, entonces **existe un único camino que une $\boldsymbol{v}$ y $\boldsymbol{r}$**. El nodo del camino más próximo a v es el *nodo padre de v* y el resto de nodos vecinos de v son los *nodos hijos de v*. La raíz r es el único nodo cuyos vecinos son todos hijos suyos y no tiene padre. Además, un nodo puede tener un número cualquiera de nodos hijos, pero si no tiene ningún hijo y es distinto de la raíz se dirá que es una *hoja*, completando así nuestro glosario del jardín de los grafos (ver figura 13b).

Ahora que conocemos qué tipo de grafos son los árboles, podemos estudiar cómo construirlos. Vamos a hacerlo partiendo de un único nodo, para lo que primero necesitamos el resultado siguiente.



(a) El grafo completo K_4 en la parte superior y dos posibles árboles de unión



(b) Árbol con raíz r y hojas en verde. En azul el nodo padre de v, en amarillo los nodos hijos de v.

Figura 13: Algunos ejemplos de árboles

Teorema 3.5. *Todo árbol con al menos dos nodos tiene al menos dos nodos de grado 1.*

Demostración. *Sea $G = (V, E)$ un árbol tal que $|V| \geq 2$, y sea $v_0 \in V$ cualquiera. Tomemos un camino P de v_0 a cualquier otro nodo tal que no se repitan aristas (lo cual es posible a no ser que lleguemos a un nodo con grado 1, en cuyo caso el camino finaliza y la prueba está completa). Dicho nodo tiene que aparecer en algún momento ya que si no, llegaríamos a algún otro nodo por que cual P ya pasó y en ese caso existiría un ciclo, lo cual contradice que G sea un árbol. Así pues, tenemos que existe al menos un nodo de grado 1.*

Para encontrar otro nodo de grado 1 basta tener en cuenta que en un camino sin repetición de vértices sólo hay dos nodos que tengan grado 1, los nodos extremos. Si v_0 tiene grado 1 la prueba estaría completa. Si tiene grado mayor que 1, entonces se añade a P la arista que une v_0 con uno de sus vecinos que no esté en P, sea v_1 y se comprueba si v_1 tiene grado 1. Este proceso continúa de manera recursiva hasta que se encuentre un nodo que tenga grado 1, el cual tiene que existir, ya que si no en algún momento el camino pasaría por algún nodo repetido, lo que daría lugar a un ciclo y de nuevo es contradicción porque G es un árbol. □

Así, se puede definir un método de construcción de árboles llamado *procedimiento crece-árboles.*

Procedimiento crece-árboles

1. Crear un nodo.
2. Repetir el siguiente paso un número cualquiera de veces: dado cualquier grafo G, crear un nuevo nodo y conectarlo mediante una nueva arista a cualquier nodo de G.

Todo grafo obtenido a partir del procedimiento crece-árboles es un árbol, y cualquier árbol se puede obtener a partir de este método.

Este mecanismo permite además establecer nuevas propiedades sobre los árboles, como conocer el número de aristas que tiene a partir, exclusivamente, de su número de nodos.

Teorema 3.6. *Todo árbol de n nodos tiene $n-1$ aristas.*

Demostración. *Utilizando el procedimiento crece-árboles, se comienza por un nodo que tiene grado 0 y en cada paso se añade un nodo nuevo que se conecta con una arista nueva al nodo anterior. Por ello la diferencia entre el número de nodos y aristas se mantiene.*

3.2.2. Almacenamiento y número de árboles

Al igual que en la primera sección estudiamos problemas de contar, podemos relacionar ahora ese ámbito con el de árboles. En este apartado, vamos a ver cuántos árboles pueden construirse con un número n cualquiera de nodos dados. Para ello, es importante tener en cuenta la siguiente clasificación para saber cuándo dos árboles se consideran iguales:

- Si asignamos a cada nodo un número: $0, 1, 2, ...n-1$, entonces dos árboles son iguales siempre que los mismos pares de nodos estén conectados en uno y otro grafo. Llamaremos a estos grafos *árboles etiquetados.*

- Si no asignamos a cada nodo un número, entonces dos árboles son iguales siempre que se puedan reordenar los nodos tal que a partir de un árbol se pueda obtener el otro. Es decir, son *isomorfos*: existe una correspondencia biyectiva entre los nodos del primer árbol y del segundo, de manera que dos nodos conectados en el primer árbol por una arista se corresponden con otros dos conectados por una arista en el segundo árbol. Llamaremos a estos grafos *árboles no etiquetados*.

Árboles etiquetados

El número de árboles etiquetados proviene de una fórmula muy simple pero cuya demostración es, de hecho, bastante complicada por lo que no la exponemos aquí. Se trata del *teorema de Cayley*.

Teorema 3.7. ***Teorema de Cayley*** *El número de árboles etiquetados de n nodos es* n^{n-2}.

Se pueden intuir algunas ideas de su demostración si nos preguntamos cómo podemos almacenar en un ordenador los árboles no etiquetados de n nodos. Entre otros, aquí mencionamos tres métodos principales para hacer esto y lo ejemplificamos para el árbol de la figura 14.

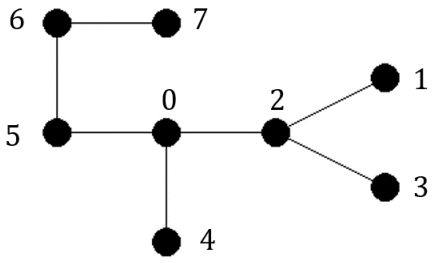


Figura 14: Un árbol etiquetado

- La matriz de adyacencia.

Es la forma típica de almacenar, no sólo árboles sino también grafos, tanto orientados como no orientados. La matriz es cuadrada, de tamaño $n \times n$. La posición (i, j) de la matriz es un

1 si existe una arista del nodo i al j y un 0 si no la hay. Notar que en grafos no orientados la matriz que se obtiene es simétrica respecto a la diagonal y además todos los elementos (i, i) de la diagonal son 0, puesto que estamos tratando con grafos simples. Así, para almacenarla en el ordenador, se requieren $(n^2 - n)/2$ bits, por lo que se trata de un método computacionalmente bastante costoso. La matriz para almacenar el árbol de la figura 14 es:

$$\begin{matrix} 0 & 0 & 1 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{matrix}$$

- Lista de aristas.

Una segunda opción es listar todas las aristas del árbol especificando sus nodos, para lo que basta una matriz con 2 filas y $n - 1$ columnas. Los dos nodos situados en cada columna establecen dónde debe haber una arista. Existen algunos inconvenientes, como que ahora se necesitan enteros de 0 a $n - 1$ en vez del código binario de la matriz de adyacencia, o que hay mucha libre elección de qué orden seguir para anotar las aristas. Sin embargo, el número de bits que se emplean en este método es de $2n \log_2 n$ bits, mucho menos que para la matriz de adyacencia. Aquí mostramos un posible código para almacenar el árbol 14

$$\begin{matrix} 1 & 2 & 2 & 0 & 0 & 5 & 6 \\ 2 & 3 & 0 & 4 & 5 & 6 & 7 \end{matrix}$$

- El código padre.

En principio se coloca la estructura de dos filas igual que en el método anterior. Se toma el nodo etiquetado con el 0 como la raíz. Entonces se pueden listar los dos nodos de las aristas

comenzando por aquel que está más lejos de la raíz y poniendo en segundo lugar el otro. Así, para cada arista, el nodo escrito en la parte inferior es el padre del nodo escrito justo encima. La raíz no aparece en la fila superior porque no tiene nodo padre. El orden de listar las aristas es el propio orden del etiquetado. Lo que ocurre es que la primera fila no nos aporta información luego se puede suprimir, aunque tiene la desventaja que no todo código produce un árbol. En este método se emplean pues $(n-1)\lceil \log_2 n \rceil$ bits, mejora al anterior y es bastante eficiente. El código padre del árbol de la figura 14 se muestra con ambas filas:

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

Árboles no etiquetados

El número de árboles no etiquetados, al que vamos a denotar T_n, (siendo de nuevo n el número de nodos), es mucho más complicado de calcular que el de árboles etiquetados y, de hecho, no se conoce una fórmula exacta para hallarlo. Así que en su lugar, vamos a obtener unas cotas de su valor aproximado.

Para obtener una cota inferior, notar primero que cada árbol no etiquetado puede ser etiquetado de $n!$ formas distintas, pero no por ello nos salen $n!$ árboles distintos. Por ejemplo, si el árbol es una estrella, permutar las hojas da lugar a la misma estrella, así que una estrella sin etiquetar en realidad da lugar a n estrellas etiquetadas.

Así, un árbol sin etiquetar da lugar a, como máximo, $n!$ árboles etiquetados, y como el número de árboles etiquetados es n^{n-2}, se tiene que $n^{n-2}/n! \leq T_n$. Aproximando por la fórmula de Stirling 2.6:

$$\frac{n^{n-2}}{n!} \approx \frac{n^{n-2}}{(n/e)^n\sqrt{2\pi n}} = \frac{e^n}{n^{5/2}\sqrt{2\pi}} \ll n^{n-2},$$

de manera que el número de árboles no etiquetados es mucho menor que el de árboles

etiquetados. En la siguiente tabla, se muestra la cantidad de árboles de uno y otro tipo para un número pequeño de nodos.

n	Árboles etiquetados	Árboles no etiquetados
1	1	1
2	1	1
3	3	1
4	16	2
5	125	3

Tabla 2: Número de árboles etiquetados y no etiquetados para un número n de nodos

Para obtener una cota superior de T_n, conviene pensar en cómo se podrían almacenar este tipo de grafos sin necesidad de numerar sus nodos, es decir, únicamente por su forma y sin tener en cuenta qué nodo está asignado a qué número. Existe una manera sencilla de lograr este almacenamiento y consiste en el llamado *código planar*.

Elegida una raíz de un árbol no etiquetado de n nodos, se dibuja el grafo en el plano evitando que las aristas se crucen entre sí y se recorren en un mismo camino, partiendo de la raíz, las aristas de ida y vuelta hasta alcanzar todos los nodos y finalizar de nuevo en la raíz. El código planar es una secuencia de ceros y unos tal que un 1 indica un alejamiento de la raíz (seguir una arista a la ida) y un 0 indica un acercamiento hacia la raíz (recorrer una arista de vuelta). Tiene algunas propiedades:

- Tiene una longitud de $2(n-1)$ cifras, ya que un árbol tiene $n-1$ aristas y éstas se recorren dos veces,
- Siempre empieza con un 1, dado que la primera arista del árbol que une la raíz con otro vértice, se recorre primero de ida (si el árbol tiene $n = 1$, realmente no existe código planar, al no haber ninguna arista, pero en este caso es trivial almacenarlo y lo que nos interesa es tratar con árboles de un número n grande de nodos).
- Tiene el mismo número de ceros y unos, claramente, puesto que cada arista se recorre una vez de ida y otra vez de vuelta.

- Todo árbol no etiquetado está determinado de forma única por un código planar, ya que tan sólo basta con dibujar las aristas y nodos a medida que se sigue la secuencia de cifras.

Una cota superior de T_n es el número de posibles códigos planares para un árbol no etiquetado de n nodos: $2^{2(n-1)} = 4^{n-1}$, ya que en cada una de las $2(n-1)$ posiciones del código, hay dos posibilidades: 0 o 1. Así, se pueden recoger ambas cotas en el siguiente resultado:

Teorema 3.8. *El número de árboles no etiquetados, T_n, siendo n el número de nodos satisface:*

$$\frac{n^{n-2}}{n!} \leq T_n \leq 4^{n-1}.$$

Realmente, cómo este problema de conteo está orientado al almacenaje de árboles de gran tamaño, se pueden cambiar las cotas por unas más fácil de recordar, como por ejemplo si $n > 30$:

$$2^n \leq T_n \leq 4^n.$$

Y por último, cabe destacar que el uso del código planar no es del todo óptimo. En primer lugar, porque para cada árbol puede haber muchos códigos planares (dependiendo del nodo que se elija como raíz y del dibujo en el plano) y, en segundo lugar, porque no toda secuencia binaria de longitud $2(n-1)$ es un código planar (como vimos en las propiedades anteriores, tiene que empezar en 1 y tener el mismo número de ceros y unos). Sin embargo, es muy eficiente a la hora de codificar árboles no etiquetados, porque para n nodos, sólo utiliza $2n$ bits. Como para $n > 30$ hay más de 2^n árboles no etiquetados, no podríamos codificarlos todos con secuencias de n bits, ya que como máximo tendríamos 2^n secuencias posibles y no serían suficientes.

3.3. El teorema de los cuatro colores

Entramos en la parte más vivaz de este texto con intención de hablar un poco acerca del *teorema de los cuatro colores*, según el cual, cuatro colores bastan para colorear las regiones de cualquier mapa sobre un plano. Para ello, veremos brevemente una fórmula que relaciona el número de aristas, vértices y regiones de un tipo de grafo llamado *planar* y hablaremos del coloreado de regiones y grafos con un número k de colores.

3.3.1. Grafos planares y la fórmula de Euler

Un *grafo planar* es un tipo de grafo que se puede dibujar en un plano, tal que sus nodos representan diferentes puntos del plano y sus aristas, continuas y curvilíneas, unen dichos puntos y no se intersecan entre ellas. Vamos a asumir también que estos grafos son conexos. Los grafos planares dividen el plano en varias regiones que se conocen como *países*, de los cuales uno será infinito mientras que el resto serán finitos.

Euler estaba trabajando en una fórmula que relacionara el número de vértices, aristas y caras de algunos poliedros convexos:

Poliedro	Vértices	Aristas	Caras
Cubo	8	12	6
Tetraedro	4	6	4
Prisma triangular	6	9	5
Prisma pentagonal	10	15	7
Pirámide pentagonal	6	10	6
Dodecaedro	20	30	12
Icosaedro	12	30	20

Tabla 3: Algunos poliedros convexos con el número de sus respectivos vértices, aristas y caras.

y dedujo que:

$$\textit{número de caras} + \textit{número de vertices} = \textit{número de aristas} + 2.$$

De hecho, se puede transformar a los poliedros convexos en grafos dibujados sobre un plano, donde las caras son las regiones delimitadas en el plano, y las aristas y vértices de los poliedros son respectivamente aristas y vértices en el grafo. Se puede obtener una fórmula similar a la anterior pero en el ámbito de los grafos planares, conocida como la **fórmula de Euler**:

$$f + n = e + 2, \tag{3.1}$$

siendo f = número de regiones, n = número de vértices y e = número de aristas.

Existen grafos sencillos de dibujar que no son planares. Un ejemplo es K_5, el grafo completo de 5 nodos, que se puede ver en la figura 15. Para probar que efectivamente no es planar se puede hacer distinguiendo en un gran número de casos y utilizando algunas propiedades intuitivas acerca de curvas en el plano pero que pueden dar lugar a confusión. En lugar de eso, se puede hacer de manera más simple y elegante mediante la fórmula de Euler.

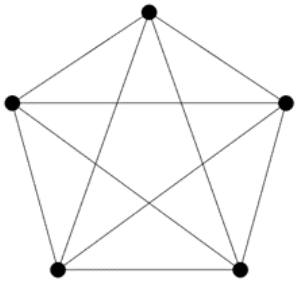


Figura 15: Grafo K_5

Teorema 3.9. *El grafo completo K_5 de 5 nodos no es un grafo planar.*

Demostración. *Supongamos que K_5 es un grafo planar. Entonces se puede dibujar en el plano sin que ninguna de sus aristas interseque con otra. Como tenemos $n = 5$ nodos y $e = \binom{5}{2} = 10$ aristas, utilizando la fórmula de Euler 3.1 se tienen $f = 10 + 2 - 5 = 7$ países. Cada país tiene como mínimo 3 aristas de frontera, así que como mínimo se deberían tener $\frac{3 \cdot 7}{2} = 10.5$ aristas en total (dividimos entre 2 porque hemos contado cada arista para dos países diferentes) pero $10 \not> 10.5$, luego llegamos a contradicción.* □

Otra aplicación de la fórmula de Euler es establecer una cota superior para el número de aristas de un grafo planar. Tanto el anterior teorema como el que enunciaremos a continuación, nos servirán más adelante cuando procedamos a colorear mapas.

Teorema 3.10. *Un grafo planar de n nodos tiene a lo sumo $3n-6$ aristas.*

Demostración. *Sea un grafo planar con n nodos, e aristas y f regiones. Aparte de la fórmula de Euler, se puede encontrar otra relación entre dichos números contando el número de aristas a partir del de las regiones. Se sabe que cada cara ha de tener al menos 3 aristas de frontera y éstas se cuentan 2 veces por ser limítrofes entre dos regiones, luego $e \geq \frac{3}{2}f \Leftrightarrow f \leq \frac{2}{3}e$. Introduciéndolo en la fórmula de Euler (3.1):*

$$e+2 = n+f \leq n+\frac{2}{3}e \;\Rightarrow\; 3e+6 \leq 3n+2e \Rightarrow e \leq 3n-6. \qquad \square$$

3.3.2. Colorear regiones circulares y grafos con dos colores

Dibujamos una serie de círculos en un plano, de manera que lo dividan en varias regiones y consideramos que dos regiones son *vecinas* si tienen una arco de frontera común (es decir, no se consideran vecinas si únicamente son tangentes en uno o dos puntos). Pongamos que queremos colorear el plano únicamente con blanco y gris, ¿se puede hacer de manera que las regiones vecinas sean de colores distintos?

Teorema 3.11. *Las regiones formadas por n círculos en un plano se pueden colorear de blanco y gris de manera que dos regiones vecinas tengan colores opuestos.*

Demostración. *La prueba se realiza por inducción sobre n, el número de círculos.*
Si $n=1$: el plano se divide en dos regiones, la de fuera y la de dentro del círculo, luego se puede colorear una de blanco y otra de gris.
Hipótesis de inducción para $n-1$: supongamos que el plano con $n-1$ círculos puede ser coloreado en blanco y gris.
Veamos que se cumple para n: añadimos un círculo C al plano y recoloreamos las regiones, ver figura 16:

- *Fuera de C los colores se mantienen como estaban.*
- *Dentro de C se intercambian los colores que ya estaban pintados.*

En efecto, se verifica el resultado. Basta con estudiar lo que ocurre con todos los arcos dibujados en el plano.

- *Si el arco está fuera de C: las dos regiones adyacentes ya tenían colores opuestos.*
- *Si el arco está dentro de C: las regiones adyacentes son de colores opuestos porque originalmente eran opuestos y únicamente se intercambiaron.*
- *Si el arco es parte de C: originalmente las regiones adyacentes al arco estaban unidas y tenían el mismo color. Tras añadir C al plano, la región interior cambió de color y la exterior se mantuvo como estaba, luego tienen colores opuestos.* □

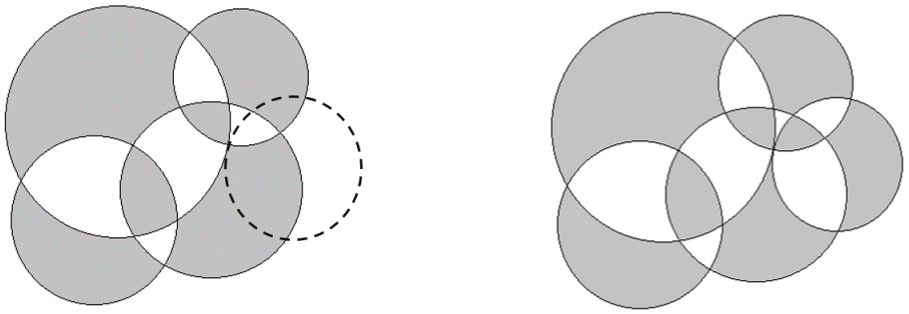


Figura 16: Círculo C punteado y posterior recombinación de colores

El problema anterior de colorear regiones formadas por círculos se puede formular como un problema de colorear los nodos de un grafo con dos colores. Notar que, pintar los grafos con colores significa pintar sus nodos de manera que los que son adyacentes tienen que tener colores distintos. A cada región del plano le corresponde un nodo y a cada frontera común se le asigna una arista entre los dos nodos. Dos vértices del grafo están conectados por una arista si y sólo si las correspondientes regiones tienen una frontera común (de nuevo no se consideran regiones vecinas aquellas que sean tangentes en uno o dos puntos).

Colorear un grafo también puede servir para modelizar otro tipo de problemas no relacionados con planos. Por ejemplo, se quieren formar dos equipos de igual número de personas, pero todas

conocen a alguien con quien no se llevan bien, relación que se representa mediante las aristas de la figura 17. Al pintar los nodos del grafo para distinguir los equipos, se ve que lo que se tiene es un *grafo bipartito*, un tipo de grafo en el que sus nodos se dividen en dos clases, A y B, tal que todas las aristas conectan un nodo de A con uno de B.

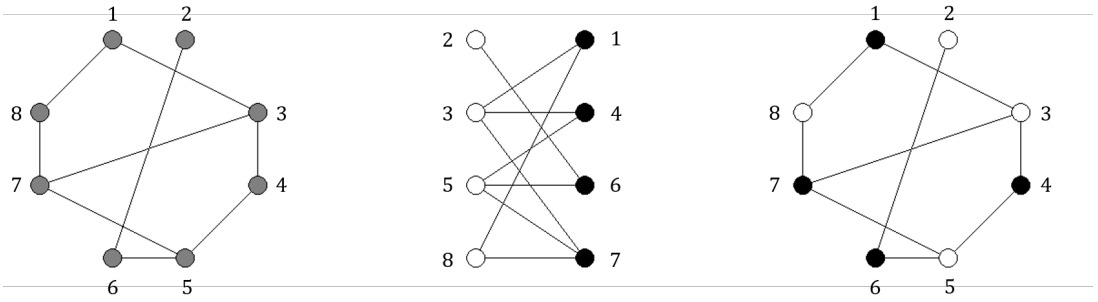


Figura 17: Grafo que da lugar a una bipartición y a una clasificación en equipos blanco y negro.

Lo que deseamos conseguir es una condición que nos asegure qué grafos se pueden colorear con dos colores o, en otras palabras, que nos diga cuándo un grafo puede ser bipartito. Para un grafo con vértices aislados se puede utilizar un sólo color; si el grafo tiene al menos una arista entonces se necesitarán al menos dos colores; si en el grafo hay un triángulo de aristas entonces se necesitarán como mínimo tres... Pero un grafo no necesita tener un triángulo para que no se pueda colorear con dos colores ya que, si se toma por ejemplo un pentágono, es fácil ver que siempre acabaremos teniendo dos nodos adyacentes de igual color. El siguiente resultado da una condición necesaria y suficiente para que un grafo se pueda pintar con sólo dos colores, al cual llamaremos *2-coloreable*.

Teorema 3.12. *Un grafo es 2-coloreable si y sólo si no contiene ningún ciclo de longitud impar.*

Demostración.

$\Rightarrow$ *Por el contrarrecíproco: supongamos que un grafo contiene al menos un ciclo de longitud impar y fijémonos en uno concreto. Partiendo de uno de los nodos del ciclo, sea u, al que coloreamos de negro, recorremos el ciclo alternando negro y blanco. Sin embargo, como el ciclo tiene longitud impar, retornaremos al nodo u con un desfase de un color, por lo que se tendrá*

que u es adyacente a un nodo negro y por tanto el grafo no es 2-coloreable.

$\Leftarrow$ *Supongamos que un grafo no contiene ningún ciclo de longitud impar, ver figura 18.*

1. *Tomamos uno de sus vértices, sea v, que coloreamos de negro.*

2. *A cada uno de sus vértices vecinos lo coloreamos de blanco. Notar que entre estos vecinos no puede existir ninguna arista que los una, pues en ese caso el grafo tendría un triángulo (ciclo impar).*

3. *A cada uno de los vecinos no pintados de estos últimos vértices blancos los coloreamos de nuevo de negro. Por un lado, se sabe que no existe ninguna arista que conecte uno de estos vértices con v, porque se tendría un ciclo de longitud 3. Por otro lado, tampoco pueden existir aristas que conecten estos últimos nodos entre sí, ya que entonces se tendrían ciclos de longitud 3 o 5.*

4. *Se continúa coloreando el resto del grafo y se ve que no puede existir ninguna arista entre vértices del mismo color. Por reducción al absurdo, supongamos que sí exista una arista entre los vértices w y $\hat{w}$ del mismo color. Tomamos el camino P que retorna desde w hasta v y el camino Q que retorna desde $\hat{w}$ hasta v. Se tiene que $long(P) + long(Q) = 2t$ con $t \in \mathbb{N}$, luego la longitud suma de ambos caminos es par y al añadir la arista $w\hat{w}$ se tendría un ciclo de longitud impar, luego contradicción.* □

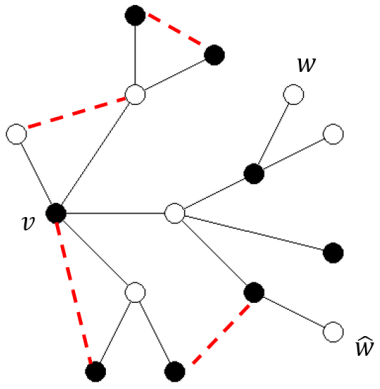


Figura 18: Grafo sin ciclos impares. En rojo y punteadas, algunas de las aristas prohibidas.

Cabe destacar que este resultado no sólo proporciona un método de encontrar ciclos de longitud impar si resulta que el grafo no es 2-coloreable, sino que además, nos proporciona un algoritmo para encontrar grafos 2-coloreables en el caso de que lo sean.

3.3.3. Colorear grafos con k colores

Una vez conocida la regla por la cual se pueden pintar grafos 2-coloreables, cabe preguntarse cuál es el procedimiento para 3 o, en general, para un número k. Notar que lo que se desea, en muchos casos, es encontrar el menor k con el que se puede pintar un grafo.

Un grafo que se pueda colorear con k colores se dice que es *k-coloreable* y el menor k para el cual un grafo es k-coloreable recibe el nombre de *número cromático* del grafo.

Evidentemente, si un grafo posee n nodos, el máximo número de colores con el que se pueda colorear será n. Además, en el grafo completo K_n se tiene número cromático n, puesto que cada nodo es adyacente al resto y por tanto se necesitan n colores distintos para pintarlo.

La dificultad que entraña la búsqueda de un resultado para encontrar grafos 3-coloreables es tal que, de hecho, a día de hoy, no se conoce ninguno tan sencillo como para los grafos 2-coloreables. Este enorme salto de complejidad provoca que el método más fiable sea el puro ensayo y error.

Dado un grafo cualquiera con n nodos, tratamos de pintarlo de rojo, verde y azul. En la figura 19 se muestra el principio de este algoritmo.

1. Tomamos un nodo del grafo, sea a, y sin pérdida de generalidad lo pintamos de rojo.
2. Uno de los vecinos de a, sea b, lo pintamos de azul, también sin que de momento exista ninguna restricción.
3. Tomamos otro vecino de a, sea c.

- Si está unido a b por una arista entonces obligatoriamente lo tenemos que pintar de verde.
- Sin embargo, si no existe la arista bc, tenemos dos opciones para c: podemos pintarlo de verde o azul. Elegimos y continuamos pintando el resto de los nodos de la misma manera.

Si en un paso posterior resulta que un nodo tiene un vecino de cada color, es que la última elección ha sido la incorrecta, por lo que hay que retroceder y probar con la otra opción.

En el mejor de los casos, este método proporciona una manera de colorear el grafo en caso de que este sea 3-coloreable. En el peor, se concluirá que el grafo no es 3-coloreable, habiendo tomado el algoritmo un tiempo de $2^{n/2}$.

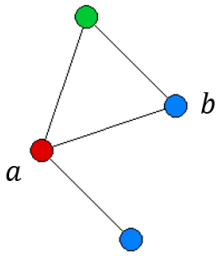


Figura 19: Grafo 3-coloreable.

Esta situación se repite para un número arbitrario k de colores con los que queramos pintar el grafo. Sin embargo, sí que existe un teorema que nos permite saber si un grafo es k-coloreable en un caso especial:

Teorema 3.13. ***El Teorema de Brook.*** *Si todo nodo de un grafo tiene grado como máximo d, entonces el grafo se puede colorear con $d+1$ colores.*

Demostración. *Utilizando el principio de inducción sobre el número de vértices del grafo G. G tiene menos de $d+1$ vértices:, claramente puede ser coloreado con $d+1$ o menos colores. Hipótesis de inducción: suponemos que el teorema es cierto para G con menos de n vértices. Probemos el resultado para n: omitamos de G un nodo cualquiera v y las aristas adyacentes a él. El grafo resultante, G' tiene $n-1$ vértices y cada uno tiene máximo un grado d. Por hipótesis de inducción, entonces el G' puede ser coloreado con $d+1$ colores. Como v tiene como máximo*

a d nodos vecinos, pero tenemos $d+1$ colores, hay un color que no tiene ninguno de sus vecinos. Así, pintando v de dicho color, se concluye que G se puede pintar con $d+1$ colores. □

Notar que la condición del teorema de Brook es suficiente pero no necesaria, puesto que existen grafos con alto n y alto d pero que son 2-coloreables.

Por último, supongamos que queremos ver si un grafo es k-coloreable, aunque tenemos sospechas de que no lo es porque ni el teorema de Brook ni el método de ensayo y error falla por tratarse, por ejemplo, de grafos muy extensos. En ese caso, si se encuentran $k+1$ nodos del grafo formando un grafo completo, K_{k+1}, como el número cromático es $k+1$, se concluye que el grafo no es k-coloreable. Claro que, llegar a esta conclusión sería una gran suerte, pues para cualquier entero positivo existen grafos que no contienen subgrafos completos y aún así no son k-coloreables.

3.3.4. Colorear mapas con k colores

Vimos en una sección previa que siempre se podía pintar con 2 colores un plano con regiones delimitadas por círculos. Evidentemente se trataba de un problema sencillo de modelizar y resolver, pero en cartografía el coloreado de mapas es un cometido habitual.

Debido a que los mapas de verdad tienen complejísimas configuraciones, no es de extrañar que se necesiten más de dos colores para pintarlos. De hecho, es sencillo ver que incluso un mapa de cuatro regiones a veces necesita cuatro colores para ser pintado. Lo elegante es comprobar que, de hecho ¡cuatro colores bastan para colorear cualquier mapa planar!

El problema, llamado originalmente *la conjetura de los cuatro colores*, fue propuesto por primera vez por Francis Guthrie en Inglaterra en 1852 y durante décadas se trató como un mero problema de entretenimiento. Sin embargo, en torno a 1870 la dificultad en la obtención de una solución comenzó a intrigar a los matemáticos de entonces. A lo largo del siglo siguiente, numerosas soluciones fueron presentadas y refutadas, como por ejemplo la de Alfred Kempe en

1879, que se mantuvo invicta durante más de diez años. Finalmente, en 1976, Kenneth Appel y Wolfang Haken confirmaron la teoría. Aunque el modo de hacerlo no fue una demostración matemática en sí, sino mediante un ordenador que probó combinación tras combinación de grafos durante más de mil horas.

Desde entonces, se conoce al problema como *el teorema de los cuatro colores* y, tras unas mejoras en la clasificación de algunos casos de grafos y gracias al desarrollo de la tecnología, actualmente los ordenadores tardan mucho menos en "demostrarlo". Sin embargo, a día de hoy aún no se ha encontrado una prueba matemática *pura* para el teorema.

Es por ello, que aquí vamos a intentar demostrar un enunciado un poco más sencillo: que cinco colores bastan para colorear cualquier mapa planar. Aunque, para ello comenzamos por un resultado aún más sencillo todavía: que seis colores bastan para colorear cualquier mapa planar. La modelización del problema se realiza (¡cómo no!) mediante grafos.

¿A qué nos referimos exactamente con *mapa planar*? Se trata de un mapa que está asociado a un grafo planar. En cada uno de las regiones o países del mapa vamos a elegir un punto al que vamos a llamar *capital* del país. Si dos países comparten frontera, entonces podemos unir sus dos correspondientes capitales mediante una línea, una "vía de tren" si lo queremos visualizar mejor. Esta vía de tren, por tanto, es tal que atraviesa dos países y cruza la frontera entre ellas **una** sola vez. Más aún, podemos diseñar estas líneas de manera que **no intersequen** con ninguna otra del mapa.

El grafo formado por el conjunto de vértices que son las capitales de los países y el conjunto de aristas que son las vías de tren se trata de un grafo planar y recibe el nombre de *grafo dual del mapa original*.

Unos comentarios previos acerca del grafo dual [12]:

- El grafo dual, G', se define respecto a otro grafo, G. Es necesario que G sea un grafo

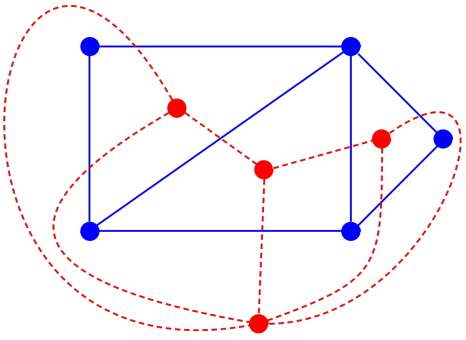
reposando sobre una superficie plana o esférica. Si G reposa sobre otra superficie topológica, como un toro, el grafo dual no tiene por qué existir.

- Si G' es el grafo dual de G, entonces G es el dual de G'. G y G' se llaman, en conjunto, *grafos duales*.
- El grafo dual de un grafo G no tiene por qué ser único.

Y otros comentarios a tener en cuenta enfocados a lo que vamos a hacer:

- En el caso de que dos regiones compartan varios trozos de frontera separados, para nuestros propósitos basta con que la "vía de tren" que une las capitales vecinas cruce por sólo uno de dichos trozos, ver figura 20a.
- En un mapa planar existe un segundo grafo que es aquel cuyos nodos son los puntos donde confluyen las fronteras de **al menos tres** países y cuyas aristas son las fronteras de los países. Este grafo puede que se trate de un *multigrafo*, ver figura 20b.
- A pesar de que necesitemos modelizar el problema a partir de multigrafos, no nos tenemos que preocupar por ellos porque de lo que vamos a hablar va a ser de un mapa planar y su grafo dual.

(a) La frontera común entre Rusia y China posee dos partes separadas por Mongolia. Aquí sólo consideramos una de dichas partes para construir la "vía de tren" [13].



(b) Grafo dual G' (en azul) de un multigrafo G (en rojo). Punteadas en rojo las fronteras de los países. Los vértices azules corresponderían a las capitales [14].

Figura 20: Parte de un mapa planar (izquierda) y dos grafos duales (derecha)

El problema consiste pues en **colorear el grafo dual** como lo veníamos haciendo: dos nodos adyacentes no pueden ser del mismo color. Podemos reescribir así nuestros teoremas de pintar mapas en k colores, por pintar grafos planares en k colores.

La condición para que un grafo sea 6-coloreable según el teorema de Brook, (3.13), es que *todos* los nodos del grafo tengan como máximo grado 5. No podemos aplicar el teorema a nuestro caso porque un grafo planar arbitrario no cumple necesariamente esta condición; sin embargo, del procedimiento de la demostración se puede saber que un grafo es 6-coloreable si tiene *al menos un* nodo de grado como máximo 5 y eso ocurre también con todos sus subgrafos.

Lema 3.1. *Si todo subgrafo de G tiene un nodo de grado como máximo d, entonces G es $(d+1)$-coloreable.*

Demostración. *Omitimos uno de los vértices de G de grado a lo sumo d, v, y pintamos recursivamente el grafo resultante con $d+1$ colores. Podemos extender este coloreado hasta v ya que como tiene a lo sumo d vecinos, siempre nos va a sobrar un color.* □

Lema 3.2. *Todo grafo planar tiene un nodo de grado como máximo 5.*

Demostración. *Por reducción al absurdo, supongamos que los n nodos del grafo G tienen grado al menos 6. Entonces, el número de aristas será como mínimo $6n/2$ (dividimos entre 2 porque cada una la estamos contando dos veces), es decir, $3n$. Pero esto contradice el teorema 3.10, que decía que como máximo un grafo planar tiene $3n-6$ aristas.* □

Teorema 3.14. ***El Teorema de los Seis Colores.*** *Todo grafo planar puede ser coloreado con 6 colores.*

Demostración. *Dado que todos los subgrafos de un grafo planar son también grafos planares, a partir del lema 3.2 se sabe que tienen un nodo de grado máximo 5, así que se puede aplicar el lema 3.1 y por tanto se tiene que todo grafo planar es 6-coloreable.* □

Demostremos ahora que todo grafo planar es 5-coloreable pintando los nodos uno por uno y usando el lema 3.2.

Teorema 3.15. ***El Teorema de los Cinco Colores.*** *Todo grafo planar puede ser coloreado con 5 colores.*

Demostración. *Sea un grafo planar con n nodos, Vamos a usar inducción sobre n.*
Si un grafo planar tiene menos de 5 *nodos: entonces claramente es 5-coloreable.*
Hipótesis de inducción: supongamos que un grafo planar cualquiera con menos de n nodos (y más de 5) es 5-coloreable.
Probémoslo para un grafo planar con n nodos: por ser un grafo planar, según el lema 3.2, tiene un nodo v con grado máximo 5.

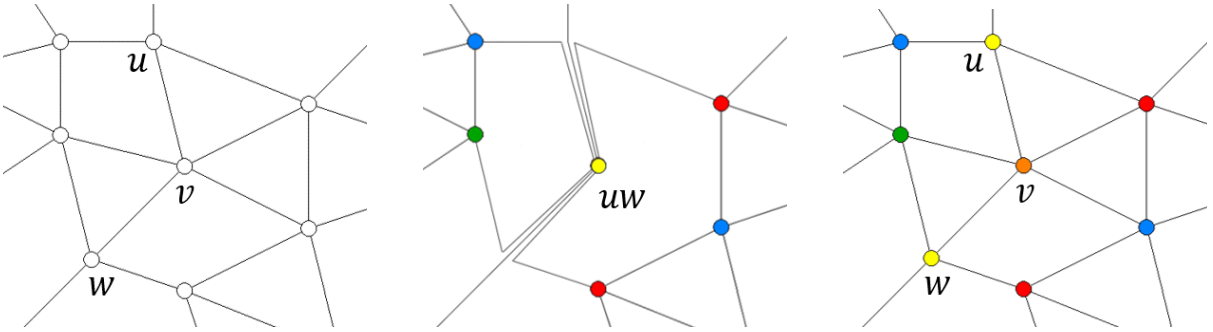
- *Si $gr(v) \leq 4$: se puede eliminar v y pintar el resto del grafo con 5 colores por hipótesis de inducción. Entonces, se encuentra un color para v distinto al de sus vecinos porque, como máximo, v tiene cuatro vecinos.*
- *Si $gr(v) = 5$: sean u y w dos vecinos de v. Se elimina v del grafo y se unifican u y w en un mismo nodo que vamos a llamar uw. Luego se extienden las aristas que previamente llegaban por separado a u y a w para que ahora lleguen a uw. Dado que este es un grafo planar con menos de n nodos, por hipótesis de inducción lo podemos colorear con 5 colores, de modo que uw adquiere un color, sea amarillo. Después, al separar u y w y devolver v a su posición original, u y w tienen ambos color amarillo, lo que significa que los 5 vecinos de v están coloreados con 4 colores, y por tando el restante es con el que pintamos v.*

  Los ***dos problemas con los que nos podemos encontrar*** *son los siguientes:*

  (1) Existe un tercer nodo p unido por una arista a u y por otra arista a w. Al unificar ambos puntos nos queda un 2-grafo y habíamos dicho que no íbamos a trabajar con multigrafos. ***El problema aquí se resuelve ignorando una de las dos aristas que irían a parar a uw en la fase de unificación****. El grafo continuaría siendo planar, de modo que se puede colorear con 5 colores y p tendría un color distinto a u y a w.*

  (2) u y w están conectados por una arista entre sí que daría lugar a un bucle en uw en la fase de unificación. Al separar de nuevo u y w, serían nodos adyacentes del mismo

color. ***Resolvemos esta situación sin más que tomar otros dos cualesquiera vecinos de v para realizar la fusión****. El problema no se puede dar en todas las parejas entre vecinos de v porque se tendría un subgrafo completo de 5 nodos dentro del grafo planar... y como hemos visto a lo largo de estos últimos apartados,* K_5 ***no*** *es planar.* □



(a) Nodo v de grado 5 *(b) Nodo uw y coloreado* *(c) Vuelta a la posición original*

Figura 21: Formación del nodo uw en el teorema de los cinco colores si $gr(v) = 5$

Finalizamos la sección de teoría de grafos enunciando el *teorema de los cuatro colores* y con un ejemplo de mapa coloreado así.

Teorema 3.16. ***El Teorema de los Cuatro Colores.*** *Todo grafo planar puede ser coloreado con 4 colores.*

Figura 22: Provincias de España en la Península Ibérica [15] coloreadas en cuatro colores.

4. Aplicaciones a Grupos

Una de las principales aplicaciones de la combinatoria en teoría de grupos, vista en la asignatura de Álgebra I, está ligada a las acciones de grupos. El teorema de Polya-Burnside, mezclando ideas de matemática discreta y de teoría de grupos, nos permite calcular el número de órbitas de la acción de un grupo sobre un conjunto.

Teorema 4.1. ***Teorema de Polya-Burnside****. Sea G un grupo finito que actúa sobre un conjunto finito X. Para cada $g \in G$, consideramos $Fix(g) = \{(x, g) \in X \times G \mid g(x) = x\}$ el conjunto de elementos de X que quedan fijos por la acción del elemento $g \in G$. Si N es el número de órbitas de X bajo la acción de G, entonces*

$$N = \frac{1}{|G|} \sum_{g \in G} \big|Fix(g)\big|. \tag{4.1}$$

En esta sección, vamos a ver una aplicación de teoría de grafos a grupos. En particular, trataremos de resolver la pregunta general de Burnside "un grupo periódico finitamente generado, ¿es necesariamente finito?" [3]. Antes que nada, comentar que un grupo periódico es aquel en el que todo elemento tiene orden finito [16]. Por tanto, un grupo finito es finitamente generado y periódico. El problema de Burnside plantea el recíproco, es decir, si ser periódico y finitamente generado es condición suficiente para tener la finitud.

La respuesta, dada por Golod, es negativa. Golod construyó para cada primo p un p-grupo infinito finitamente generado. La demostración se realiza a partir de una construcción indirecta y se basó en su trabajo sobre álgebras con Šafarevič. Más recientemente, Grigorčuk planteó otra posible forma de responder a partir de una construcción directa de un 2-grupo infinito generado por 3 elementos de orden 2 [17].

Nuestro objetivo será ver la construcción directa de un p-grupo infinito con dos generadores, cada uno con orden p, para cualquier primo impar p. Veremos que dicho grupo es un subgrupo del grupo de automorfismos de un árbol regular infinito de grado p, donde un *grafo regular de*

grado k es aquel en el todos sus nodos tienen el mismo grado k [18]. También comprobaremos dos propiedades del grupo: tiene exponente infinito, es decir, no existe una cota superior del orden de los elementos del grupo; y es residualmente finito, es decir, el grupo posee una familia de subgrupos de índice finito que se cortan en el subgrupo trivial.

En primer lugar, definimos los dos generadores, que van a ser dos automorfismos y veremos que ambos tienen orden p.

Definición 4.1. *Sea p un primo impar y sea $T(0)$ el árbol regular infinito de grado p con vértice 0, que interpretaremos como su raíz, y tal que para cada vértice u de $T(0)$ existen p subárboles regulares $T(u,1),...,T(u,p)$ -con raíces $(u,1),...,(u,p)$-, cada uno isomorfo a $T(0)$. Para cada vértice u de $T(0)$ definimos un automorfismo:*

$$t(u) : T(u) \longrightarrow T(u) \tag{4.2}$$

que viene dado por $t(T(u,p)) := T(u,1)$ y $t(T(u,j)) := T(u,j+1)$ para $j = 1,...,p-1$.

Notar que el automorfismo definido en 4.2 tiene **orden p** y fija el vértice u. Se trata de una aplicación que actúa como una permutación cíclica: mueve subárboles de uno en uno hacia la derecha y al último lo lleva a la primera posición. También lo podemos ver como una permutación de conjuntos de vértices (separados por ";"): $u,1,k(1),...,k(l);u,2,k(1),...,k(l);...;u,p,k(1),...,k(l)$ para todo $l \geq 0$, siendo $u,i,k(1),...,k(l)$ los vértices del subárbol $T(u,i)$ con $i = 1,...,p$.

Definición 4.2. *Para cada vértice u de $T(0)$ definimos una secuencia infinita, $S(u)$ de vértices de forma inductiva como sigue:*

$$\begin{aligned} S(u) &= u,1;u,2;...;u,p-1;S(u,p) \\ &= u,1;u,2;...;u,p-1;u,p,1;u,p,2;...;u,p,p-1;S(u,p,p), \end{aligned}$$

donde los vértices los hemos separado con " ;". A partir de la secuencia anterior, definimos un

segundo automorfismo

$$a(u) : T(u) \longrightarrow T(u) \tag{4.3}$$

que viene dado por $a(u) = t(u,1)t^{-1}(u,2)i(u,3)...i(u,p-1)a(u,p)$. *Aquí*

- t *es el automorfismo definido por 4.2,* t^{-1} *es su inverso;*
- $i(u,j)$ *es el automorfismo identidad de* $T(u,j)$ *y*
- $a(u,p)$ *es el automorfismo correspondiente de* $T(u,p)$. *Es decir,*

$$a(u,p) = t(u,p,1)t^{-1}(u,p,2)i(u,p,3)...i(u,p,p-1)a(u,p,p).$$

Notar que el automorfismo definido en 4.3 tiene **orden p** y fija cada uno de los vértices $u; u,p; u,p,p; ...$

En particular, cuando $p = 3$, se tiene que $a(u) = t(u,1)t^{-1}(u,2)a(u,3)$ sin automorfismos identidad en el medio.

En la figura 23 se puede ver el árbol $T(u)$ para $u = 0$. Veamos en ella la actuación de los dos automorfismos sobre $u = 0$ y la definición de $S(0)$:

- El automorfismo 4.2, $t(0)$, fija la raíz 0 y mueve cíclicamente las raíces de los p subárboles.
- La secuencia $S(0)$ recorre de izquierda a derecha los vértices del primer nivel menos el último, el $0,p$; luego los del segundo nivel del subárbol con raíz $0,p$ menos el último, el $0,p,p$; luego los del tercer nivel del subárbol con raíz $0,p,p$ menos el último...
- Finalmente el automorfismo 4.3, $a(0)$, fija la raíz 0 y los vértices $(0,1),(0,2),...,(0,p)$ del primer nivel. Después, mueve los vértices del árbol de raíz $(0,1)$ como el automorfismo $t(0,1)$, los vértices del árbol de raíz $(0,2)$ como el inverso de $t(0,1)$, deja fijos los vértices de los árboles de raíz $(0,3),...,(0,p-1)$ y, al llegar al $(0,p)$ baja un nivel y repite el proceso con los árboles de raíces $(0,p,1),...,(0,p,p)$. Notemos que deja fijos los vértices de la forma $(0,p,p,p,...)$ y también los de los árboles del 3 al $p-1$.

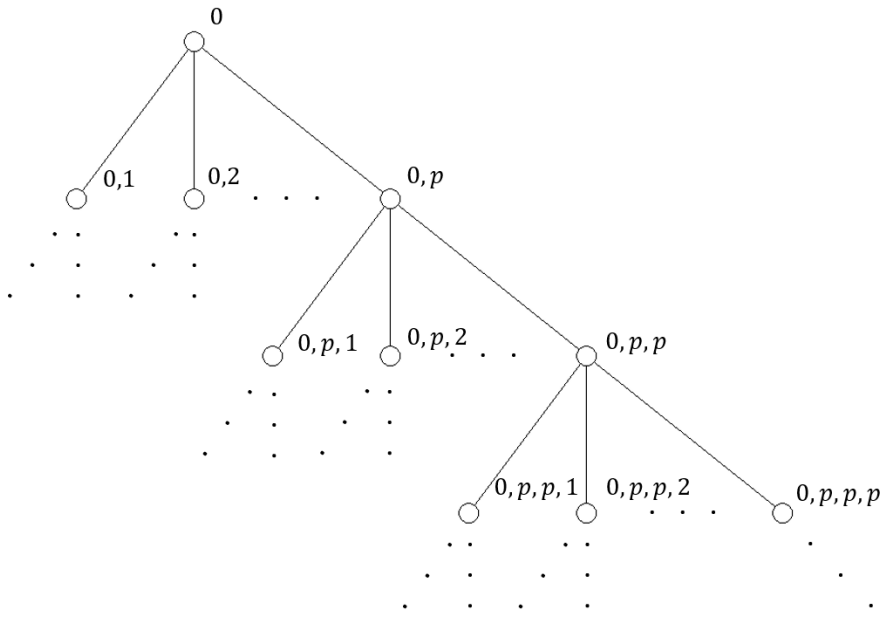


Figura 23: Árbol $T(0)$ infinito para un primo impar p y con los vértices etiquetados.

Una última anotación es que en este caso al hablar de *árbol regular de grado* p, nos referimos al *grado de salida* o *número de descendientes* de cada nodo, como si el árbol fuera un grafo dirigido. Es decir, no estamos teniendo en cuenta el grado de la raíz 0, que evidentemente es una unidad menos que el del resto de nodos.

Estamos ahora en condiciones de ver el resultado que nos responde negativamente a la pregunta de Burnside.

Teorema 4.2. *Sea p un primo impar y sea $G(0)$ el grupo generado por los automorfismos $t(0)$ y $a(0)$ definidos en 4.2 y en 4.3 respectivamente. Entonces $G(0)$ es un p-grupo infinito.*

Demostración. *Sustituyendo $u = 0$ en 4.3 y denotando $G(u)$ al grupo generado por $t(u)$ y $a(u)$ se puede ver que*

$$\begin{aligned} a(0) &= t(0,1)t^{-1}(0,2)i(0,3)...i(0,p-1)a(0,p) \\ &\in G(0,1) \times G(0,2) \times G(0,3) \times ... \times G(0,p-1) \times G(0,p). \end{aligned}$$

Simplificamos la notación anterior como una p-tupla; llamamos: $\alpha = (t, t^{-1}, i, ..., i, a)$.

Para cada $j = 0, 1...p-1$, *el elemento* $\alpha_j := t^{-j}(0)a(0)t^j(0)$ *está en* $G(0,1) \times G(0,2) \times G(0,3) \times ... \times G(0,p-1) \times G(0,p)$ *y se obtiene como una permutación cíclica de una p-tupla como la anterior. Así, se tiene que:*

$$\begin{aligned} \alpha_0 &= (t, t^{-1}, i, ..., i, a_0) \\ \alpha_1 &= (t^{-1}, i, i, ..., a_0, t) \\ &\vdots \\ \alpha_{p-1} &= (a_0, t, t^{-1}, ..., i, i) \end{aligned} \tag{4.4}$$

Vamos a denotar $H(0)$ *el subgrupo de* $G(0)$ *generado por* $\alpha_0, ..., \alpha_{p-1}$. *Entonces se tiene que* $H(0) \trianglelefteq G(0)$ *tal que* $[G(0) : H(0)] = p$. *Dado que los* $G(0,j)$ *son isomorfos a* $G(0)$ *y H(0) es producto subdirecto de los* $G(0,j)$, *se sigue que* ***$G(0)$ es un grupo infinito***.

Falta ver que $G(0)$ *es un p-grupo, es decir, queremos ver que todos los elementos de* $G(0)$ *tienen orden potencia de p. Sea* $g \in G(0)$, *entonces* $g = ht^j$ *donde* $h = h(a_0, ..., a_{p-1})$ *es una palabra en* $a_0, ..., a_{p-1}$. *Probaremos por inducción sobre la longitud de g que g es un p-elemento.*

Si g tiene longitud 1, entonces g es de orden p ya que $g = \alpha_i$ *o* t^r.

Sea g de longitud $m+1 \geq 2$ *y supongamos por inducción que todos los elementos de longitud menor o igual que m son p-elementos.*

- *Caso 1:* $g = h(a_0, ..., a_{p-1})t^{p-j}$ *con* $j \in \{1, ..., p-1\}$ *Entonces el elemento h tiene longitud* $m = \lambda(0) + \lambda(1) + ... + \lambda(p-1)$ *donde* $\lambda(k)$ *es la contribución a la longitud dada por* a_k. *Ahora bien,*

  $$g^p = hh^{t^j}...h^{t^{(p-1)j}}$$

  es un elemento de $H(0)$ *con longitud mp y tiene la propiedad de que la contribución a la longitud dada por cada* a_k *es* $\lambda(0) + ... + \lambda(p-1) = m$. *Si expresamos* g^p *como una p-tupla por 4.4 se ve que para cada j, la componente en* $G(0,j)$ *de* g^p *es un elemento de* $H(0,j)$ *de longitud como mucho m y por ello es un p-elemento por hipótesis de inducción. Así g es un p-elemento.*

- *Caso 2: $g = h(a_0, ..., a_{p-1}) \in H(0)$.*

  Entonces h tiene una longitud $m+1 = \lambda(0) + ... + \lambda(p+1)$. Si expresamos h como una p-tupla a partir de 4.4 resulta que la componente asociada a $G(0,j)$ tiene una longitud $\lambda(p-j)$ o $\lambda(p-j)+1$ dependiendo de si la componente es o no un elemento de $H(0,j)$.

  - *Si la componente tiene longitud $\lambda(p-j)$ entonces, por hipótesis de inducción y como $\lambda(p-j) \leq m$, es un p-elemento.*
  - *Si la componente tiene longitud $\lambda(p-j)+1$ y $\lambda(p-j)+1 \leq m$ entonces, por hipótesis de inducción, es un p-elemento.*
  - *Si la componente tiene longitud $\lambda(p-j)+1 = m+1$ se tiene que $m = 1$ y, por el Caso 1 y la hipótesis de inducción, es un p-elemento.*

En cualquiera de los dos casos g es un p-elemento, con lo que ***$G(0)$ es un p-grupo.*** □

A continuación, veremos dos propiedades del grupo $G(0)$: que tiene exponente infinito y que es residualmente finito. El *exponente* de un grupo G es el menor n tal que $\forall g \in G$, $g^n = 1$. Por otro lado, un grupo G se dice que es *residualmente finito* [19] si $\forall g \in G, g \neq 1$ existe una imagen finita G^* homomorfa a G tal que $g^* \neq 1$, donde g^* es la imagen de g en G^*.

Propiedad 4.1. *$G(0)$ tiene exponente infinito.*

Esto se tiene porque para cada elemento de orden p^k, se puede construir otro de orden p^{k+1}.

Propiedad 4.2. *$G(0)$ es residualmente finito.*

Demostración. *Sea V el conjunto de los vértices del árbol $T(0)$, entonces $V = \cup_{k=0}^{\infty} V_k$ donde V_k es el conjunto de los p^k vértices que hay en el nivel k-ésimo del árbol.*

Todo elemento $g \in G(0)$ induce una permutación $\prod_k(g)$ del conjunto V_k para $k \geq 0$. Así, $\prod_k : G(0) \to \mathrm{Perm}(V_k)$ define un homomorfismo del grupo $G(0)$ al grupo de permutaciones de V_k. Dado entonces $g \neq 1$ en $G(0)$, existe un entero positivo mínimo k tal que $\prod_k(g) \neq e$ siendo e el elemento identidad de $\mathrm{Perm}(V_k)$ y, por lo tanto, $g \notin \mathrm{Ker} \prod_k$.

Como $G(0)/\mathrm{Ker} \prod_k$ es finito, se tiene que $G(0)$ es residualmente finito. □

5. Conclusiones

Comenzamos la primera sección introduciendo tres de las ramas principales de la matemática discreta. Gracias a las fórmulas de conteo obtuvimos las expresiones de los coeficientes binomiales, además de manejarnos con las permutaciones y las variaciones. Los coeficientes binomiales nos dieron pie, en el segundo apartado, a hablar sobre el triángulo de Pascal, sobre el que obtuvimos numerosas identidades que nos permitieron analizar esta curiosa figura desde muchos ángulos (un poco literalmente). A partir del propio triángulo de Pascal, hallamos la secuencia de los números de Fibonacci, estudiamos algunas de sus relaciones y nos encontramos de manera inesperada con el número áureo. Todo lo dado hasta entonces (menos, de hecho, el número áureo) lo englobamos en la muy resumida teoría de números de este texto.

Claramente esta última se trata de una rama muy extensa por lo que el estudio se centró en la "pequeña" parte de los números primos y compuestos y en el manejo de la divisibilidad. Demostramos resultados tan antiguos como que la factorización de un número en primos es única y que existen infinitos números primos y también estudiamos con un poco más de profundidad algunos conceptos de la distribución de primos en la recta de enteros. Mencionamos algunos enigmas que fueron surgiendo a medida que se desarrollaba la matemática con los siglos hasta la era moderna, y finalizamos con los test de números primos y su actual cálculo mediante ordenadores.

La parte más extensa de este trabajo es sin duda la de teoría de grafos. En las primeras secciones se mencionó mucha terminología de la manera más resumida posible, y recalcando, sobre todo, aquellos conceptos que personalmente me eran más desconocidos. La parte de cadenas eulerianas nos llevó a demostrar el teorema que el propio Euler propuso para resolver la cuestión de los puentes de Königsberg, aquel que originó esta inmensa teoría que continúa creciendo imparablemente gracias a la tecnología. Vimos muchos tipos de grafos notables pero, sobre todo en el segundo apartado, nos centramos en los árboles y discutimos cuestiones de conteo y almacenamiento en el ordenador.

Por supuesto, aún hay muchas más cosas sobre grafos y árboles que se podrían contar y discutir, pero en cuanto llegamos a la linde del bosque, la parte más colorida del texto se abrió paso de nuevo con Euler y los grafos planares. Vimos como colorear regiones circulares y grafos con dos colores, nos extendimos a colorear grafos de un mayor número de colores... de grafos pasamos a mapas... y culminamos con el famoso teorema que dio nombre a toda la subsección.

Y ya en el final, nos adentramos en la respuesta dada a la pregunta de Burnside a partir de un ejemplo en cuya construcción retomamos los árboles y conceptos de grupos. Así, encontramos un grupo finitamente generado tal que todos sus elementos tienen orden finito, aunque en este caso se trata de un grafo infinito, el único entre todos los grafos que hemos visto aquí. Completamos de esta manera el tratamiento de esos conceptos que en un primer momento parecían tan abstractos, pero que han mostrado su enorme utilidad.

Referencias

[1] Lovász L. y Pelikán J. y Vesztergombi K. *Discrete Mathematics. Elementary and beyond.* EE.UU.: Springer-Verlag, 2003.

[2] Pelegrín B. y Cánovas L. y Fernández P. *Algoritmos en grafos y redes.* 1.ª ed. España: PPU - Promociones y publicaciones universitarias, 1992.

[3] Narain Gupta y Said Sidki. «On the Burnside problem for periodic groups». En: *Mathematische Zeitschrift* 182 (ene. de 1983), págs. 385-388. DOI: 10.1007/BF01179757.

[4] Apostol T. M. *Calculus - Volumen 2. Cálculo con funciones de varias variables y álgebra lineal, con aplicaciones a las ecuaciones diferenciales y a las probabilidades.* 2.ª ed. España: Editorial Reverté S. A., 1989, págs. 749-752.

[5] Lovász L. y Pelikán J. y Vesztergombi K. *Discrete Mathematics. Elementary and beyond.* EE.UU.: Springer-Verlag, 2003, pág. 90.

[6] Miguel Ángel Crespo y Julio Bernués. *El Logaritmo Integral: Números primos y algo más.* 2022. arXiv: 2205.07564 [math.HO].

[7] H. A. Helfgott. *The ternary Goldbach conjecture is true.* 2014. arXiv: 1312.7748 [math.NT].

[8] P. Taylor. *What Ever Happened to Those Bridges?* 2000. URL: https://web.archive.org/web/20091114030637/http://www.amt.canberra.edu.au/koenigs.html (visitado 09-03-2023).

[9] Wikipedia Commons. *El problema de los puentes de Königsberg.* 2019. URL: https://ingenieriabasica.es/el-problema-de-los-puentes-de-konigsberg/ (visitado 05-04-2023).

[10] Wikipedia Commons. *File:Dodecahedron schlegel.* 2020. URL: https://commons.wikimedia.org/wiki/File:Dodecahedron_schlegel.svg (visitado 05-04-2023).

[11] MathWorld–A Wolfram Web Resource. Weisstein Eric W. *Petersen Graph.* 2023. URL: https://mathworld.wolfram.com/PetersenGraph.html (visitado 19-06-2023).

[12] H. Whitney. «Non separable and planar graphs». En: *Transactions of the American Mathematical Society* 34.2 (1932), págs. 339-362. URL: https://search-ebscohost-com.uniovi.idm.oclc.org/login.aspx?direct=true&AuthType=ip,uid&db=edsjsr&AN=edsjsr.10.2307.1989545&lang=es&site=eds-live&scope=site (visitado 12-06-2023).

[13] EcuRed. *Mapa de Mongolia*. 2011. URL: https://www.ecured.cu/Mongolia#/media/File:Mapa_de_Mongolia.jpg (visitado 18-06-2023).

[14] Wikipedia Commons. *File:Dual graphs*. 2012. URL: https://commons.wikimedia.org/wiki/File:Duals_graphs.svg (visitado 18-06-2023).

[15] Dibujos.net. *Dibujo de las provincias de España para Colorear*. URL: https://geografia-espanola.dibujos.net/las-provincias-de-espana.html (visitado 27-03-2023).

[16] Larry C. Grove. *Algebra*. EE.UU.: Dover, 2004, pág. 194.

[17] Maleah. Mortorff. *William Burnside: Theory of Groups of Finite Order and the Burnside Problem*. EE.UU., 2016. URL: https://digitalcommons.liberty.edu/honors/566 (visitado 12-06-2023).

[18] Wai-Kai. Chen. *Graph theory and its engineering applications*. Singapur, 1997. URL: https://archive.org/details/graphtheoryitsen00chen/page/28/mode/2up (visitado 12-06-2023).

[19] Magnus. Wilhelm. «Residually finite groups». En: *Bulletin of the American Mathematical Society* 75.2 (1969), págs. 305-316. URL: https://projecteuclid.org/journals/bulletin-of-the-american-mathematical-society/volume-75/issue-2/Residually-finite-groups/bams/1183530287.full?tab=ArticleFirstPage (visitado 12-06-2023).