5

INNOVACIÓN DOCENTE

Desarrollo de destrezas en resolución de problemas de olimpiadas matemáticas

Coordinadores:
Daniel José Rodríguez Luis
Juan Miguel Ribera Puchades

UNIVERSIDAD DE LA RIOJA

Imagen: Dan Cristian Păduret

Editores
Daniel José Rodríguez Luis
Juan Miguel Ribera Puchades

Desarrollo de destrezas en resolución de problemas de olimpiadas matemáticas

UNIVERSIDAD DE LA RIOJA
2022

Nombres: Rodríguez Luis, Daniel José, editor | Ribera Puchades, Juan Miguel, editor.
Título: Desarrollo de destrezas en resolución de problemas de olimpiadas matemáticas / editores Daniel José Rodríguez Luis, Juan Miguel Ribera Puchades.
Descripción: Primera edición. | Logroño : Universidad de La Rioja, Servicio de Publicaciones, 2022.
Identificadores: ISBN 978-84-09-36497-8 (pdf)
Temas: Matemáticas | Problemas y ejercicios prácticos.
Clasificación: CDU 51(076) | Thema 1.0 PB | Thema 1.0 4CN

ISBN 978-84-09-36497-8 (pdf)

Depósito Legal: LR 1419-2022

Edita: Universidad de La Rioja, Servicio de Publicaciones

Diseño de cubierta: Servicio de Relaciones Institucionales y Comunicación de la Universidad de La Rioja

Imprime: ABZ impresores

Impreso en España – Printed in Spain

ÍNDICE GENERAL

RESUMEN

El Taller de Creatividad Matemática, en concreto, el Seminario de Problemas de Secundaria y Bachillerato de la Universidad de La Rioja (UR) ha servido desde sus inicios, hace más de veinte años, como punto de encuentro entre los distintos centros de enseñanza secundaria de La Rioja y la UR; especialmente para quienes están interesados en las matemáticas y en la resolución de problemas, concretamente los relativos a olimpiadas matemáticas. Sin embargo, la deslocalización existente en La Rioja, sumado al interés mostrado por el material generado en el Seminario de Problemas de Secundaria y Bachillerato, hizo necesaria la creación de un recurso formativo que pudiera ser utilizado por los estudiantes de forma autónoma y asíncrona. De esta forma, el trabajo que se ha ido desarrollando en los últimos años con los diferentes Proyectos de Innovación Docente (PID) ha tenido como objetivo principal acercar la UR a los estudiantes apasionados en la resolución de problemas y desafíos matemáticos. Más aún, el confinamiento domiciliario derivado de la COVID-19 puso de manifiesto la necesidad de diseñar nuevas metodologías de enseñanza y aprendizaje basadas en la formación a distancia.

El resultado de los diferentes proyectos se conoce como Curso Online de Olimpiadas Matemáticas (COOM) y es un material educativo compuesto por secuencias de vídeos destinadas al desarrollo de habilidades para la resolución de problemas de olimpiadas matemáticas que además incluye instrumentos de evaluación de los conocimientos adquiridos. En concreto, supone la continuación de diversos PID, entre los que se encuentran:

- "Seminario Online de Problemas Olímpicos de Matemáticas" (Curso 2016/2017).
- "Curso Online de Olimpiadas Matemáticas (MOOC-COOM)" (Curso 2017/2018).
- "Mejora y ampliación del COOM (MACOOM)" (Curso 2018/2019).
- "Evaluación y puesta en marcha del COOM (EVACOOM)" (Curso 2019/2020).
- "Perfeccionamiento de la accesibilidad del COOM (PACOOM)" (Curso 2020/2021).
- "Implantación del Diseño Universal de Aprendizaje al COOM (DUACOOM)" (Curso 2021/2022).

En el momento de la edición de este documento, se han completado satisfactoriamente un total de 22 secuencias didácticas para la formación no presencial. Cada una de estas secuencias en vídeo están destinadas a la enseñanza de diferentes metodologías clásicas de resolución de problemas, así como pautas para abordar

los problemas de olimpiadas matemáticas y que están disponibles en la plataforma https://urabierta.unirioja.es/ de la Universidad de La Rioja.

Con el objetivo de ofrecer múltiples formatos de representación del contenido, desde la dirección del COOM se ha considerado oportuno la elaboración de este libro de texto como recurso complementario a las secuencias en vídeo sobre resolución de problemas de olimpiadas matemáticas. Todo el material del COOM, tanto las secuencias en vídeo como el libro de texto, está orientado principalmente a estudiantes de Secundaria y Bachillerato, aunque también puede ser útil para estudiantes de primeros cursos de titulaciones científicas (Grado de Matemáticas, Grado de Informática, Grados en Ingeniería, entre otros), así como para docentes y formadores de olimpiadas matemáticas.

En este libro de texto cada capítulo representa una secuencia de vídeos alojados en la plataforma https://urabierta.unirioja.es/ y debe ser considerado como un como material adicional al contenido audiovisual del COOM, pudiendo encontrar notas adicionales, definiciones, ejemplos, soluciones a los retos propuestos en el COOM con un mayor nivel de detalle, así como problemas abiertos de profundización y perfeccionamiento de las destrezas expuestas en las secuencias de vídeo. Al inicio de cada capítulo se destaca una colección de palabras clave para que el lector pueda familiarizarse con la terminología de dicho capítulo, así como una breve introducción del contenido mediante notas históricas o situaciones de la vida cotidiana en las que aparece ese concepto matemático en cuestión.

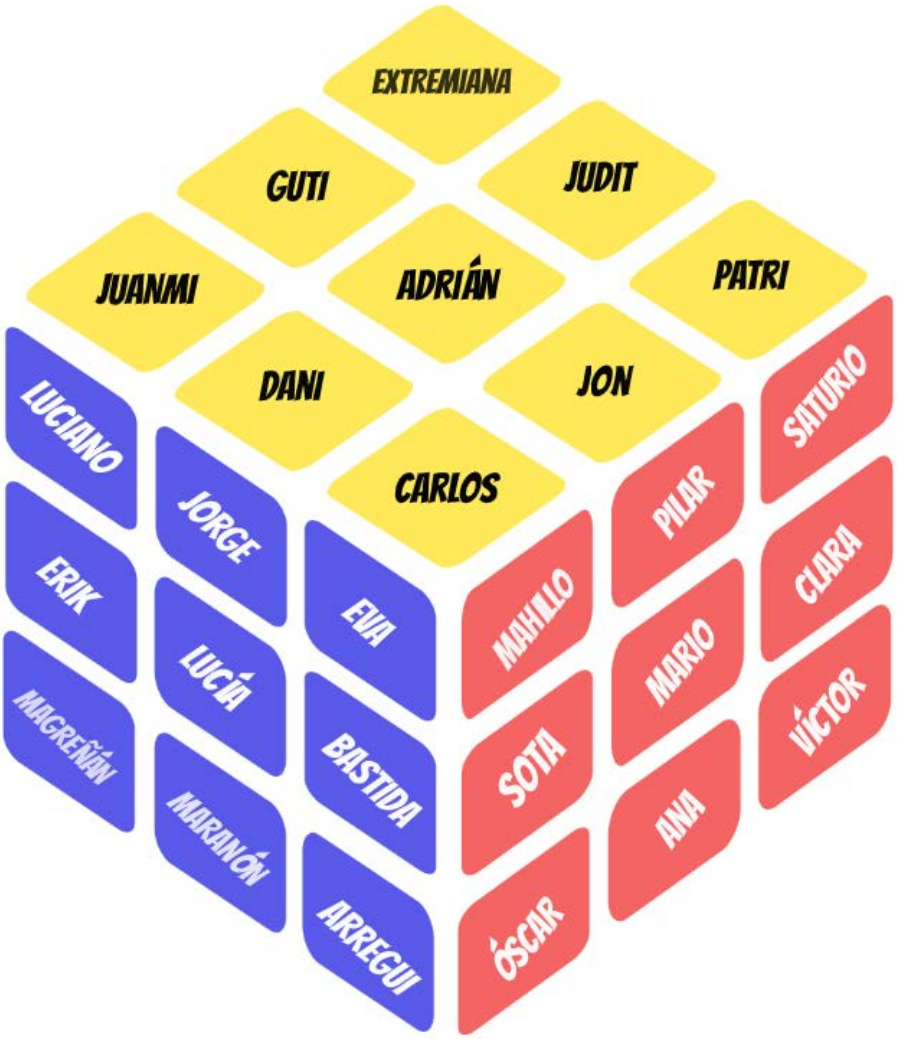
Todo el material del COOM, tanto las secuencias en vídeo como el libro de texto, ha sido elaborado por docentes preparadores de olimpiadas matemáticas de diferentes universidades (Universidad de La Rioja, Universidad de Zaragoza, Universidad Rey Juan Carlos, Universidad Complutense de Madrid, Universitat de València y Universitat Jaume I), así como por profesores de Matemáticas en Educación Secundaria de La Rioja y con la colaboración de estudiantes destacados de los últimos cursos del Grado en Matemáticas de la UR.

Por último, y no por ello menos importante, se quiere manifestar un agradecimiento especial a todas aquellas personas, entre profesores y estudiantes, involucrados en la elaboración de este material docente.

Abadías Ullod, Luciano (Universidad de Zaragoza).
Alonso Ortiz de Elguea, Jon Ander (Universidad de La Rioja).
Arenas Gómez, Alberto (Universidad de La Rioja).
Arregui Casaus, José Luis (Universidad de La Rioja).
Bastida Rodríguez, Miguel (IES Tierra Estella).
Benito Clavijo, María del Pilar (Universidad de La Rioja).
Bordel Vozmediano, Silvia (Universidad de La Rioja).
Carbonell Urtubia, Carlos (Universidad de La Rioja).
Carbonell Urtubia, Saturio (IES Gonzalo de Berceo).
Extremiana Aldana, José Ignacio (Universidad de La Rioja).
Gutiérrez Jiménez, José Manuel (Universidad de La Rioja).
Jiménez Gestal, Clara (Universidad de La Rioja).
Lanchares Barrasa, Víctor (Universidad de La Rioja).
Madiedo Castro, Óscar Reynaldo (Universidad Complutense de Madrid).
Magreñán Ruiz, Ángel Alberto (Universidad de La Rioja).
Mahillo Cazorla, Alejandro (Universidad de Zaragoza).
Maranón Grandes, Miguel (Universidad de La Rioja).

Marín Sánchez, Mario Alberto (Instituto Tecnológico de Costa Rica).
Mínguez Ceniceros, Judit (Universidad de La Rioja).
Murillo Ramón, Jesús (Universidad de La Rioja).
Navarro Quiles, Ana (Universitat de València).
Pascual Ortigosa, Patricia (Universidad de La Rioja).
Primo Tárraga, Eva (Universidad Rey Juan Carlos).
Ribera Puchades, Juan Miguel (Universitat de les Illes Balears).
Rodrigo Escudero, Adrián (Universidad de Zaragoza).
Rodríguez Luis, Daniel José (Universidad de La Rioja).
Roldán López, Jorge (Universidad de La Rioja).
Rotger García, Lucía (Universidad de La Rioja).
Sarrión Pedralva, Erik (Universitat Jaume I).
Sota Eguizábal, José Manuel (Universidad de La Rioja).

Sin vuestro esfuerzo y dedicación, nada de esto sería posible.



Agradecidos de todo corazón,

Daniel José Rodríguez Luis y Juan Miguel Ribera Puchades.

CAPÍTULO 1

1 EL PRINCIPIO DE INDUCCIÓN

José Ignacio Extremiana Aldana y Judit Mínguez Ceniceros
Universidad de La Rioja

Palabras clave

- *Números naturales*
- *Efecto dominó*
- *Base de la Inducción*
- *Hipótesis de la Inducción*

En este capítulo vamos a hablar de la reacción en cadena o el efecto dominó matemático. Es decir, vamos a hablar de cómo demostrar propiedades de los números naturales usando el principio de inducción matemática.

1.1 Introducción

Los días 18 y 19 de noviembre de 2004 en Donostia-San Sebastián tuvieron lugar *Las Jornadas sobre la Popularización de la Ciencia: las Matemáticas*, organizadas por la Sección de Matemáticas de la Universidad de País Vasco y la Real Sociedad Matemática Española (Comisión de Divulgación). Como resultado de estas Jornadas la Editorial Nivola publicó el Libro *Divulgar las Matemáticas* (Editorial Nivola, 2005). Una de las secciones de las Jornadas tenía como tema principal *Educación e Investigación*. Durante las sesiones de trabajo, uno de los ponentes, Juan Luis Vázquez, premio nacional de investigación en 2003 y, más tarde, conferenciante plenario en el Congreso Mundial de matemáticos 2006, defendió con entusiasmo que *"los números son el territorio de los matemáticos"*. Los participantes en la sección finalizaron la redacción de las conclusiones de la misma con la propuesta de dos eslóganes:

- ¡Ponga un matemático en su empresa!
- ¡El número es nuestro!

Afortunadamente, desde 2004, ha crecido de manera exponencial la consideración social de las matemáticas y cada vez son más las empresas que cuentan en su plantilla con matemáticos.

Efectivamente, los números son cosa de matemáticos. Los matemáticos somos (o debemos ser) "domadores" de números, expertos manipuladores que los analizan, estudian sus propiedades y relaciones, "los doman" y, una vez "domesticados", los ponen a disposición de la sociedad para que los utilice.

Como con las fieras, para "domar" números hay que *conocer bien su territorio*, saber en qué *familias se distribuyen*, cuáles son las *relaciones entre las familias*, *entender bien su comportamiento*, tanto cuando están en familia como individualmente. Un buen domador, para someter a sus presas, debe *intuir adecuadamente* cual va a ser su conducta y prever sus reacciones para evitar sorpresas desagradables y, por supuesto, *confirmar (o no) las intuiciones y previsiones*.

Una vez domados los números que se han estudiado, cuando se conocen las reglas universales que los rigen y los métodos que funcionan con ellos, se muestra a la sociedad (otros investigadores, programadores, ingenieros, economistas, empresarios, educadores, etc.) cómo han de utilizarse para obtener de ellos el máximo beneficio, y se advierte de los peligros de la mala utilización (como si fuesen gremlins).

Hay muchas clases de números, algunos de ellos se explican en Educación Primaria, como, por ejemplo, "los de contar" (que los matemáticos llamamos "naturales"), los negativos (que junto con los naturales forman la familia de los enteros) y los fraccionarios (que junto con los enteros forman la familia de los racionales). Los primeros números que se aprenden en la escuela, los primeros que utilizó la humanidad, son "los de contar". Los psicólogos y pedagogos han dedicado muchos esfuerzos para analizar cómo los humanos aprehendemos el concepto de número natural (de número, dicen ellos), y quienes se dedican a la didáctica a mostrar las mejores maneras de facilitar en los alumnos la comprensión y buen manejo de los números naturales y las operaciones que con ellos pueden realizarse.

Vamos a centrar nuestro estudio en los números naturales y adentrarnos un poco en su mundo que tiene todavía muchos territorios inexplorados y otros que, aunque han sido explorados, no son conocidos en su totalidad.

1.2 Algunos ejemplos de intuiciones de propiedades de familias de números naturales

Los matemáticos hemos descubierto que todo número natural puede descomponerse en producto de números primos de manera única. En este sentido, los números primos son como los ladrillos de los que están fabricados los números, de alguna manera, juegan el papel de los elementos químicos en la composición de las sustancias. La diferencia es que hay muchos más números primos que elementos químicos.

A pesar de su aparente simplicidad, los números naturales encierran muchos secretos y aplicaciones impensables. Por ejemplo, ¿quién podría imaginar hace 100 años que los números primos (una subfamilia de los números naturales) iban a ser imprescindibles para la seguridad en las comunicaciones?

Esta utilidad hace necesario descubrir números primos, saber dónde se esconden en el conjunto tan bien ordenado de los números naturales, y, si es posible, dar con una "fórmula" que nos proporcione tantos números primos como deseemos para usarlos cuando sea preciso.

A continuación, vamos a buscar números primos. Mostramos dos procedimientos de obtenerlos:

1. **Primer Procedimiento:** Después de buscar varias fórmulas, nos encontramos con el siguiente polinomio que genera números primos.

$$P(n) = n^2 + n + 41.$$

Vamos a comprobar que efectivamente obtenemos números primos calculando el valor que da el polinomio con los primeros números naturales. El Cuadro 1.1 muestra los valores que se obtienen.

n	p(n)
0	41
1	43
2	47
3	53
4	61
5	71
6	83
7	97
8	113
9	131
10	151
...	...
20	461
...	...
30	971
...	...
39	1421

Cuadro 1.1: Números primos usando el polinomio $P(n) = n^2 + n + 41$.

Animamos a quienes lean esto a completar la tabla con los números naturales que faltan y a comprobar que, efectivamente, todos los números naturales que se obtienen de $p(n)$ con los 40 primeros números naturales (incluimos el cero) son todos primos.

Después de ese esfuerzo, parece natural conjeturar que n^2+n+41 produce números primos para cualquier número natural n.

2. **Segundo Procedimiento:** Uno de los problemas clásicos, además de los conocidísimos cuadratura del círculo, trisección del ángulo y duplicación del cubo, era construir con regla y compás cualquier polígono regular de n lados. Este problema no se resolvió hasta 1837, cuando Wantzel completó la demostración del teorema enunciado por Gauss en sus *Disquisitiones Arithmeticae*. Un polígono regular de n lados puede construirse con regla y compás si n es producto de una potencia de 2 y números primos de Fermat distintos, y solo en ese caso.

   Un número primo de Fermat es un número de la forma $2^{2^p}+1$ (siendo p un número natural) y que, además, es primo. Para saber qué polígonos son construibles con regla y compás es necesario conocer los números de la forma $F_p = 2^{2^p}+1$ y saber si son primos o no. Vamos a calcular los números de Fermat.

p	F_p
0	$2^{2^0}+1=3$
1	$2^{2^1}+1=5$
2	$2^{2^2}+1=17$
3	$2^{2^3}+1=257$
4	$2^{2^4}+1=65537$
...	...

   Todos son números primos. Podemos conjeturar, de hecho Fermat así lo hizo, que para cualquier número natural F_p va a ser un número primo.

¡Olé! ¡Tenemos dos maneras de conseguir números primos! Quién los necesite que nos los pida. Somos capaces de proporcionarlos tan grandes como se quiera. Basta con utilizar, en cualquiera de las dos fórmulas generadoras, un número natural suficientemente grande.

Puede que estos razonamientos hayan convencido a algunos, pero ¡somos matemáticos! y los matemáticos no nos conformamos con mostrar, ¡tenemos que demostrar!, y para ello debemos desarrollar una cadena de razonamientos que prueben, sin ninguna duda, que la afirmación (la proposición, el teorema) que hemos enunciado es cierta. En las afirmaciones anteriores "hemos supuesto" que son ciertas. NO las hemos demostrado.

1.2.1 Comprobación de la validez de las intuiciones

La primera de las conjeturas es fácil de rebatir. Calculamos $p(40)$

$$p(40) = 40^2+40+41 = 1681 = 41^2,$$
$$p(41) = 41^2+41+41 = 1763 = 41\times 43.$$

Por lo tanto el polinomio $p(40) = n^2+n+41$ NO proporciona números primos para cualquier natural n.

Vamos con la segunda conjetura. Calculemos F_5

$$F_5 = 2^{2^5}+1 = 2^{32}+1 = 4.294.967.297.$$

¿Cómo se sabe que este número de 10 cifras es primo? La respuesta es sencilla. Calculamos su raíz cuadrada, que es, aproximadamente, 65536 y vamos dividiendo F_5 por todos los números primos menores que 65536. Si no es divisible por ninguno, el número es primo.

Este procedimiento es fácil de implementar en un ordenador, pero, como el lector ya habrá supuesto, para números "pequeños", de pocas cifras, un ordenador potente tarda muy poco en dar la respuesta; para números grandes, por ejemplo de 100 cifras, el coste operacional es tremendo y los ordenadores más potentes tardan mucho en dar la respuesta. Por eso hay que utilizar otros procedimientos.

Euler, después de la muerte de Fermat, en 1732, demostró que

$$F_5 = 2^{2^5} + 1 = 2^{32} + 1 = 4.294.967.297 = 641 \times 6.700.417.$$

Por lo tanto, la conjetura de Fermat (y nuestra) es incorrecta.

¿Qué pasa con los restantes números de Fermat? Vamos a calcular algunos:

- $F_6 = 2^{64} + 1 = 18.446.744.073.709.551.617 = 274.177 \times 67.280.421.310.721$
- $F_7 = 2^{128} + 1 = 340.282.366.920.938.463.463.374.607.431.768.211.457 =$
  $= 59.649.589.127.497.217 \times 5.704.689.200.685.129.054.721$
- $F_8 = 2^{256} + 1 = 115.792.089.237.316.195.423.570.985.008.687.907.853.269.984.$
  $665.640.564.039.457.584.007.913.129.639.937 =$
  $= 1.238.926.361.552.897 \times 93.461.639.715.357.977.769.163.558.199.606.896.584$
  $.051.237.541.638.188.580.280.321$

Estos tres son números compuestos. Desde 2003 sabemos que desde F_5 hasta F_{32} son todos números compuestos.

¿Conjeturamos que no hay más números primos de Fermat que los cinco primeros? Los dos ejemplos anteriores, muestran que no vale que una igualdad, una afirmación, se verifique para un gran número de números naturales. Para afirmar su validez, dado que es imposible verificarla para todos los números naturales, es preciso proporcionar un razonamiento que la demuestre.

Como curiosidad añadimos que Fermat no ha sido el único de los grandes matemáticos que ha hecho suposiciones erróneas. En el libro *Inducción en la Geometría* de I. Goloviná e I. M. Yaglóm (Editorial Mir, Moscú. Segunda Edición 1981) se muestra el siguiente ejemplo, G. W. Leibniz demostró que $\forall n \in \mathbb{N}, n^3 - n$ es divisible por 3, $n^5 - n$ es divisible por 5 y $n^7 - n$ es divisible por 7. Dedujo que para todo número impar k y $\forall n \in \mathbb{N}$, $n^k - n$ es divisible por k. Sin embargo, pronto se dio cuenta que $2^9 - 2 = 510$ NO es divisible por 9.

1.3 La inducción matemática: Un procedimiento para validar conjeturas de números naturales.

El Principio de Inducción Matemática es una técnica de demostración que sirve para probar propiedades de los números naturales. Su enunciado es el siguiente:

Definición 1.1 (Principio de Inducción Matemática)

Una propiedad $P(n)$ es cierta para todo $n \in \mathbb{N}$ si se cumplen:

a) La propiedad es cierta para $n = 1$, es decir, $P(1)$ es cierta. (Base de la Inducción)

b) Si suponemos que la propiedad es cierta para $n = k$ (Hipótesis de Inducción), entonces podemos probar que es cierta para $n = k + 1$. Es decir,

$$P(k) \quad \textit{verdadera} \quad \Longrightarrow \quad P(k+1) \quad \textit{verdadera}.$$

Por abreviar, en lo que sigue vamos a denotar por B.I. la Base de la Inducción y por H.I. la Hipótesis de Inducción, según la Definición 1.1.

Para hacernos una idea del significado pensemos en una sucesión infinita de fichas de dominó puestas de pie, como podemos ver en la Figura 1.1 (izquierda).

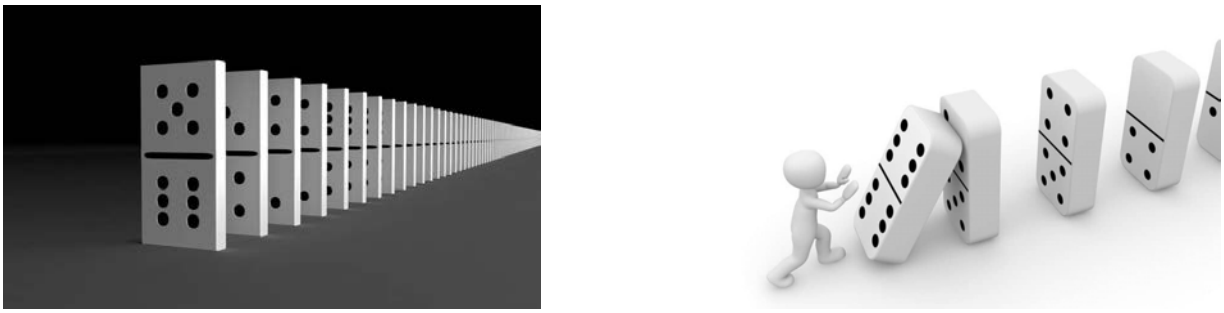


Figura 1.1: Representación del Principio de Inducción Matemática con fichas de dominó.

Si somos capaces de tirar la primera ficha como aparece en la Figura 1.1 (derecha) y estamos seguros de que las piezas están dispuestas de tal forma que cada ficha tirará la siguiente, por este efecto cadena, es seguro que todas las fichas del dominó caerán.

Ejemplo 1.1 Afirmamos que la suma de los n primeros números impares es n^2. Esto es

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

La intuición de que la igualdad es cierta nos la proporciona Figura 1.2.

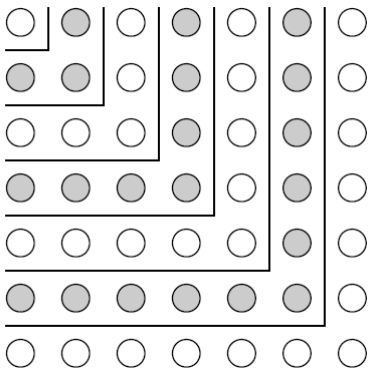


Figura 1.2: Suma de los n primeros números impares.

Para demostrar la afirmación utilizamos el método de inducción.

B.I. ¿Es cierta la igualdad para $n=1$? Sí. $1=1^2$.

H.I. Supuesta cierta la igualdad para $n=k$, ¿es cierta para $n=k+1$?
Supongamos que

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

¿Será cierta para $n=k+1$?, es decir, ¿será verdad la siguiente igualdad?

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

Usamos la Hipótesis de Inducción (H.I.) para escribir

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

Por tanto la fórmula es verdadera. Podemos afirmar, por ejemplo que

$$1+3+5+\cdots+100001 = 50000^2$$

Ejemplo 1.2 (El pequeño Teorema de Fermat). Afirmamos que si p es un número primo y $n \in \mathbb{N}$, entonces

$$n^p - n \quad \text{es divisible por } p.$$

Apliquemos el método de inducción.

B.I. $n = 1$, $1^p - 1 = 0$ que es divisible por p.

H.I. Supongamos que es cierto para $n = k$, es decir, $k^p - k$ es divisible por p ($k^p - k = m_1 p$).
¿Será cierto para $n = k+1$? Aplicamos la Hipótesis de Inducción (H.I.)

$$(k+1)^p - (k+1) = k^p + \sum_{j=1}^{p-1} \binom{p}{j} k^j + 1 - k - 1 = pm_1 + \sum_{j=1}^{p-1} \binom{p}{j} k^j.$$

Si $1 \leq j \leq p-1$,

$$\binom{p}{j} = \frac{p(p-1)\cdots(p-j+1)}{j!},$$

es divisible por p $\left(\binom{p}{j} = m_j p\right)$. Y por tanto

$$(k+1)^p - (k+1) = pm_1 + \sum_{j=1}^{p-1} m_j p k^j = pm_1 + p\sum_{j=1}^{p-1} m_j k^j = p\left(m_1 + \sum_{j=1}^{p-1} m_j k^j\right).$$

Como consecuencia de lo que acabamos de demostrar, sabemos (sin necesidad de comprobar nada) que el número $15^7 - 15$ es divisible por 7,o que $1234^{23} - 1234$ es divisible por 23.

1.4 Desarrollo metodológico

Para demostrar una igualdad, una proposición, una conjetura razonable por el método de inducción es fundamental comprobar que se cumplen las hipótesis a) y b) de la Definición 1.1 (¡las dos!). Si no se comprueba la Base de la Inducción (B.I.) es fácil llegar a absurdos. Por ejemplo, que todos los números naturales son iguales.

Ejemplo 1.3 (Necesidad de comprobar la base de la inducción). Afirmamos que para todo $n \in \mathbb{N}$, $n = n+1$ (es decir, que todos los números naturales son iguales). Supongamos que la afirmación es cierta para $n = k$, esto es, $k = k+1$. ¿Será cierto para $n = k+1$? Por hipótesis de inducción, como $k = k+1$, se sigue

$$k+1 = k+1+1 = k+2,$$

por tanto, según el método de inducción la afirmación es cierta $\forall n$ y todos los números naturales son iguales.

Esto es absurdo y el fallo está en no haber comprobado que se cumple la base de la inducción ($1 = 2$).

Para ser conscientes de la necesidad de demostrar la hipótesis de inducción, el ejemplo que hemos usado en la introducción, el polinomio de Euler $p(n) = n^2 + n + 41$ como generador de números primos, es un claro ejemplo. No basta con que la propiedad que deseamos validar se cumpla para "muchos" números naturales.

Ejemplo 1.4 (Otro ejemplo de la necesidad de demostrar la hipótesis de inducción). Sea el polinomio $x^n - 1$ con $n \in \mathbb{N}$, afirmamos que al factorizar este polinomio todos los coeficientes de sus factores tienen módulo 1.

Se puede comprobar (mejor utilizando un programa de cálculo simbólico como Mathematica, SAGE, Mapple,...) que la afirmación es cierta para $n = 1, 2, \ldots, 104$. Sin embargo, no es cierta para $n = 105$. En efecto,

$$\begin{aligned} x^{105} - 1 = (-1+x)(1+x+x^2)(1+x+x^2+x^3+x^4)(1+x+x^2+x^3+x^4+x^5+x^6) \\ (1-x+x^3-x^4+x^5-x^7+x^8)(1-x+x^3-x^4+x^6-x^8+x^9-x^{11}+x^{12}) \\ (1-x+x^5-x^6+x^7-x^8+x^{10}-x^{11}+x^{12}-x^{13}+x^{14}-x^{16}+x^{17}-x^{18}+x^{19}-x^{23}+x^{24}) \\ (1+x+x^2-x^5-x^6-2x^7-x^8-x^9+x^{12}+x^{13}+x^{14}+x^{15}+x^{16}+x^{17}-x^{20}-x^{22}-x^{24}-x^{26}-x^{28}+x^{31}+x^{32}+ \\ x^{33}+x^{34}+x^{35}+x^{36}-x^{39}-x^{40}-2x^{41}-x^{42}-x^{43}+x^{46}+x^{47}+x^{48}). \end{aligned}$$

Queda claro que para poder elevar a teorema una afirmación relativa a los números naturales no vale con que se compruebe para varios números naturales, aunque se compruebe para una gran cantidad. Es necesario, para "demostrar" la afirmación por el método de inducción, comprobar la base de la inducción y la hipótesis de inducción (las dos).

Ejemplo 1.5 (Conjetura errónea). Sea $S_n = \dfrac{1}{1\cdot 2} + \dfrac{1}{2\cdot 3} + \cdots + \dfrac{1}{n\cdot(n+1)}$.

Afirmamos que $S_n = \dfrac{n+1}{3n+1}$. Para ello, usamos el Principio de Inducción Matemática.

B.I. Veamos si es cierto para $n = 1$.

$$S_1 = \frac{1}{1\cdot 2} = \frac{1+1}{3\cdot 1+1}.$$

Luego se cumple.

H.I. Supongamos que es cierto para $n = k$, es decir,

$$S_k = \frac{k+1}{3k+1}.$$

Veamos si es cierto para $n = k+1$.

$$S_{k+1} = S_k + \frac{1}{(k+1)(k+2)} = \frac{k^3+4k^2+8k+3}{(k+1)(k+2)(3k+1)}.$$

Por lo tanto la afirmación es falsa. Con este ejemplo mostramos que, en ocasiones, el método de inducción también sirve para comprobar que una conjetura es falsa (aunque en este ejemplo era fácil comprobar la falsedad sin recurrir al método de inducción).

Nota: *Antes de finalizar esta sección y poner varios ejemplos de demostraciones por el método de inducción de algunas igualdades y afirmaciones nada evidentes, es preciso formular algunas precisiones y observaciones relativas al principio de inducción.*

1. *El método de inducción solo sirve para demostrar propiedades y relaciones que dependen de los números naturales.*
2. *Para aplicar el método de inducción no es imprescindible que la propiedad o relación comience a verificarse para $n = 1$. También sirve para demostrar propiedades que dependen de los números naturales $P(n)$ a partir de $n \geq n_0$; en este caso la base de la inducción será con $n = n_0$. Igualmente,*

puede utilizarse para probar una proposición para $n \in \mathbb{N} \cup \{0\}$; en este caso, la base de la inducción será $n = 0$.

3. *Supuesto que la afirmación es cierta para $n = k$, para probar que la afirmación es cierta para $n = k+1$, es preciso utilizar la hipótesis de inducción.*
4. *Si para demostrar la hipótesis de inducción relativa a los números naturales para $n = k+1$ necesitamos que sea cierta para $n = k$ y $n = k-1$, la base de la inducción tiene que ser cierta para $n = 1$ y $n = 2$ (para los dos primeros números naturales a partir de los cuales debemos demostrar la propiedad). Obviamente, esta observación se extiende al caso en el que para demostrar la hipótesis de inducción para $n = k$ es necesario utilizar que sea cierta para 3 o más números precedentes.*

1.5 Problemas resueltos

En esta sección damos algunos ejemplos en los que aplicando el método de inducción se demuestran propiedades y relaciones que en ningún caso son intuitivas.

Problema 1.1 Para cada $n \in \mathbb{N}$ existe un número tal que su expresión decimal consta de n dígitos, es divisible por 2^n y sus dígitos son 2's y 3's (o uno solo de los dos).

Solución *Aplicamos el Principio de Inducción Matemática:*

B.I. *Para $n = 1$, 2 es un número con 1 dígito que divisible por 2^1.*

H.I. *Supongamos que la afirmación es cierta para $n = k$, es decir, existe un número, m, de k dígitos que es divisible por 2^k y su expresión decimal sólo está formada por los dígitos 2 y 3.*
Por ser m divisible por 2^k, podemos escribir

$$m = 2^k j,\ j \in \mathbb{N}.$$

¿Será cierta la afirmación para $n = k+1$?

- *Si j es par, es decir, $j = 2r$. Tomamos el número*

$$2 \cdot 10^k + m,$$

que tiene $k+1$ dígitos y sólo contiene 2's y 3's en su expresión decimal. Veamos si es divisible por 2^{k+1}.

$$2 \cdot 10^k + m = 2 \cdot 2^k \cdot 5^k + 2^k \cdot j = 2^k(2 \cdot 5^k + 2r) = 2^{k+1}(5^k + r).$$

- *Si j es impar, $j = 2r+1$, tomamos número*

$$3 \cdot 10^k + m,$$

que tiene $k+1$ dígitos y sólo contiene 2's y 3's en su expresión decimal. ¿Es divisible por 2^{k+1}?

$3 \cdot 10^k + m = 3 \cdot 2^k \cdot 5^k + 2^k(2r+1) = 2^k(3 \cdot 5^k + 2r + 1) = 2^k(2s+1+2r+1) = 2^{k+1}(s+r+1)$.

Hemos utilizado que $3 \cdot 5^k$ es un número impar, por lo tanto, existe un número natural s tal que $3 \cdot 5^k = 2s+1$.

Problema 1.2 Para cada $N \in \mathbb{N}$, con $N > 1$ se cumple que

$$\sqrt{2\sqrt{3\sqrt{4 \cdots \sqrt{(N-1)\sqrt{N}}}}} < 3.$$

Solución *En primer lugar observemos que si $N = 1$ el enunciado no tiene sentido pues el primer número que aparece dentro de la primera raíz es 2. Aplicamos nuevamente el Principio de Inducción Matemática:*

B.I. *Para $N = 1$ obtenemos $\sqrt{2} < 3$, que se trata de una desigualdad cierta.*

H.I. *Para demostrar la hipótesis de inducción vamos a utilizar "inducción inversa". Comenzaremos demostrando que la desigualdad*

$$\sqrt{m\sqrt{(m+1)\sqrt{(m+2)\cdots\sqrt{(N-1)\sqrt{N}}}} < m+1.$$

es cierta para $m = N$ (que es muy fácil) y luego iremos "descendiendo" hasta llegar a $m = 2$.

- *Veamos si es cierto para $m = N$. La desigualdad, en este caso es*

$$\sqrt{N} < N+1,$$

que, obviamente, es cierta.

- *Supongamos que es cierto para $m+1 < N$, es decir*

$$\sqrt{(m+1)\sqrt{(m+2)\cdots\sqrt{(N-1)\sqrt{N}}} < m+2.$$

Entonces,

$$\sqrt{m\sqrt{(m+1)\sqrt{(m+2)\cdots\sqrt{(N-1)\sqrt{N}}}} < \sqrt{m(m+2)} < m+1.$$

Siguiendo este proceso concluimos que

$$\sqrt{2\sqrt{3\sqrt{4\cdots\sqrt{(N-1)\sqrt{N}}}} < 2+1 = 3.$$

Problema 1.3 En la década de los años 20 del s. XX, Wassily Kandinsky (1866-1944), uno de los pintores más influyentes de la historia y que entendía de Matemáticas y Física cuántica, experimentó en su obras con el círculo. *"Un círculo es una síntesis de las mayores oposiciones. Combina concéntrico y excéntrico en una forma y en equilibrio"*. En la Figura 1.3 se muestran dos de estas obras.

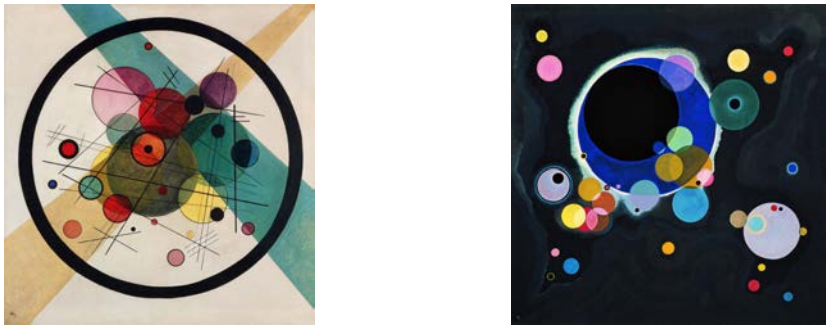


Figura 1.3: Obras de Kandinsky que involucra varios círculos.

Afirmamos que dados n círculos en el plano, Kandinsky puede pintar el "mapa" resultante únicamente con dos colores de manera que no haya regiones con frontera lineal común que tengan el mismo color (a este tipo de coloraciones se les denomina *coloración propia*).

Solución

- *Para $n = 1$ la afirmación, obviamente, es cierta (ver Figura 1.4). Kandinsky puede pintar el interior de la circunferencia con un color y el exterior con otro (marrón y blanco, por ejemplo).*

Figura 1.4: El caso para $n = 1$.

¿Qué ocurre cuando hay muchos círculos? Obviamente, si los círculos son exteriores todos a todos o a lo más tangentes (Figura 1.5), para dibujar con dos colores el mapa resultante, Kandinsky lo tiene muy fácil, pinta el interior de todos los círculos con un color (por ejemplo azul) y el exterior de otro (por ejemplo marrón).

No podemos dejar de mencionar un caso singular, que es el de los tres círculos entrelazados (anillos de Borromeo) para los que Kandinsky también tiene fácil pintar con dos colores. Pinta de un color la región que corresponde a la intersección de los tres círculos (el pintado de gris en la figura 1.6), de otro distinto la tres regiones que corresponden a las intersecciones de dos círculos, del primer color las tres regiones interiores a un solo círculo y del segundo color la región exterior a los tres círculos.

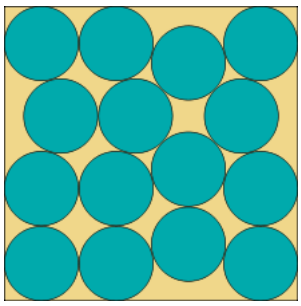


Figura 1.5: Muchos círculos tangentes.

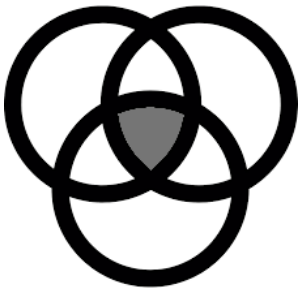


Figura 1.6: Anillos de Borromeo.

Los anillos de Borromeo se han utilizado como símbolo de la fuerza de la unión, llegando a significar a la Santísima Trinidad, figura 1.7, pues tomados dos a dos, los anillos están separados. El logo de la IMU (Unión Matemática Internacional), figura 1.8, es una variación de los anillos de Borromeo realizada por el matemático estadounidense John M. Sullivan.

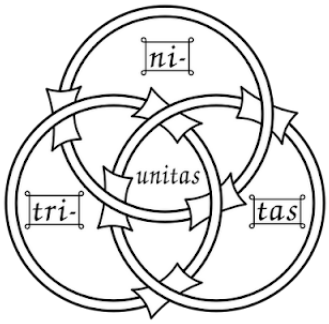


Figura 1.7: Santísima Trinidad.

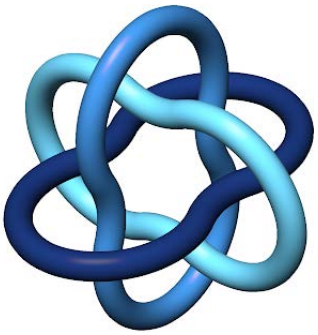


Figura 1.8: Logo de lal IMU.

Pero volvamos al problema que nos ocupa y demostremos la tesis.

- *Supongamos que la afirmación es cierta. Cuando hay dibujadas en el plano $n = k$ circunferencias Kandinsky puede pintar con dos colores el mapa que se produce en las condiciones establecidas.*
  Si se añade otra circunferencia (hay ahora $k+1$ circunferencias), Kandinsky realiza una nueva coloración de la siguiente manera: la parte "exterior" a esta nueva circunferencia la deja con los colores que tenía

antes de añadir esta última circunferencia; en la parte interior cambia los colores (donde había marrón se pone azul y donde había azul, marrón). Afirmamos que Kandinsky ha conseguido una coloración propia. En efecto:

- *dos regiones vecinas a través de esta nueva circunferencia tienen colores opuestos porque hemos invertido la coloración,*
- *dos regiones vecinas en el exterior de esta circunferencia tienen colores opuestos por hipótesis de inducción,*
- *dos regiones vecinas en el interior de esta circunferencia tienen colores opuestos por hipótesis de inducción.*

Problema 1.4 Si de entre los $2n$ primeros números naturales que escribiros de la forma $(1, 2, \ldots, 2n)$ se toman $n+1$ al azar y distintos entre sí, afirmamos que entre los números seleccionados existen al menos dos números tales que uno de ellos es divisible por el otro.

Solución *Aplicamos el Principio de Inducción Matemática:*

B. I. Si $n = 1$, en este caso, $2n = n + 1$, y $\{1, 2\}$ es el conjunto considerado. Obviamente se verifica la base de inducción.

H. I. Utilizamos para demostrar la hipótesis de inducción el método de reducción al absurdo.

Partimos de que entre los $2(n-1)$ primeros números naturales cuando se eligen al azar n números existen al menos 2 tales que uno divide al otro.

¿Sigue siendo cierto cuando tomamos los $2n$ primeros números? Supongamos que no, supongamos que entre los $2n$ primeros números, $1, 2, \ldots, 2n$, $n \geq 2$, se han encontrado $n+1$ $(a_1, \ldots, a_{n+1})$ números tales que ninguno de ellos es divisible por cualquier otro. Llamamos M_{n+1} al conjunto formado por esos $n+1$ números, todos menores o iguales que $2n$,

$$M_{n+1} = \{a_1, \ldots, a_{n+1}\}.$$

Veremos que si esto es cierto, también es cierto que entre los $2n-2$ números $1, 2, \ldots, 2n-2$ podemos encontrar n números tales que ninguno de los n números sea divisible por otro cualquiera. Lo que contradice el supuesto del que partimos. Tenemos cuatro posibilidades:

1. $2n-1 \notin M_{n+1}$ *y* $2n \notin M_{n+1}$.

   Quitamos un número $a_j \in M_{n+1}$. Entonces el conjunto $M_n = M_{n+1} \setminus \{a_j\}$ tiene n elementos ninguno de ellos mayor que $2n-2$ y ninguno divisible por cualquier otro.

2. $2n-1 \in M_{n+1}$ *y* $2n \notin M_{n+1}$. *En este caso, consideramos $M_n = M_{n+1} \setminus \{2n-1\}$. De los n que quedan en M_n ninguno es mayor que $2n-2$ y ninguno es divisible por otro.*

3. $2n-1 \notin M_{n+1}$ *y* $2n \in M_{n+1}$. *En este caso $M_n = M_{n+1} \setminus \{2n\}$ cumple nuestra condición.*

4. $2n-1 \in M_{n+1}$ *y* $2n \in M_{n+1}$. *Notar que $n \notin M_{n+1}$ porque $2n$ es divisible por n. Quitamos $2n-1$ y $2n$ del conjunto M_{n+1}. Denotamos*

   $$M_{n-1} = M_{n+1} \setminus \{2n-1, 2n\}.$$

   Sea ahora

   $$M_n = M_{n-1} \cup \{n\}.$$

   Así M_n tiene n números ninguno de ellos mayor que $2n-2$. Nos falta ver que ningún elemento de M_n divide a ningún otro. Sabemos que ningún elemento de M_{n-1} divide a ningún otro (todos pertenecen a

M_{n+1}), queda por ver que n no es divisible por ningún número de M_{n-1} y n no divide a ningún número de M_{n-1}.

(a). No existe un número en M_{n-1} divisible por n ya que ninguno es mayor que $2n-2$.

(b). n no es divisible por ningún número en M_{n-1} porque $2n$ no es divisible por ningún número de M_{n-1}.

Por tanto, si la proposición es falsa para los $2n$ números $1, 2, \ldots, 2n$, también es falsa para los $2(n-1)$ números $1, 2, \ldots 2n-2$.

Luego si la proposición es cierta para los $2(n-1)$ números $1, 2, \ldots 2n-2$, entonces también es cierta para los $2n$ números $1, 2, \ldots, 2n$.

Ejercicios Propuestos

1. Probar que, para cada $n \in \mathbb{N}$, existe un número de n dígitos que es divisible por 5^n y su expresión decimal contiene sólo los dígitos 5, 6, 7, 8 y 9.

2. Probar que $S_n = \dfrac{1}{1\cdot 2} + \dfrac{1}{2\cdot 3} + \cdots + \dfrac{1}{n\cdot(n+1)} = \dfrac{n}{n+1}$.

3. Probar que $S_n = 1^2 + 2^2 + 3^2 + \cdots + n^2 = \dfrac{n(n+1)(2n+1)}{6}$.

4. Probar que $S_n = 1\cdot 1! + 2\cdot 2! + 3\cdot 3! + \cdots + n\cdot n! = (n+1)! - 1$.

5. Probar que para todo número natural (incluimos el 0) $A_n = 11^{(n+2)} + 12^{(2n+1)}$ es divisible por 133.

6. Probar que para todo número natural $S_n = \dfrac{1}{\sqrt{1}} + \dfrac{1}{\sqrt{2}} + \cdots + \dfrac{1}{\sqrt{2n}} > \sqrt{n}$.

7. Probar que para todo número natural $n > 4$ se verifican las siguiente desigualdades

   a) $2^n > 2n + 1$; b) $2^n > n^2$.

8. Probar que para todo ángulo α y para todo número natural n (incluimos el 0) se verifica la siguiente igualdad

$$\cos\alpha \cos 2\alpha \cos 4\alpha \cdots \cos 2^n\alpha = \frac{\operatorname{sen} 2^{n+1}\alpha}{2^{n+1}\operatorname{sen}\alpha}.$$

Nota: *Los anteriores ejercicios están tomados del libro El método de la inducción matemática de I. S, Sominskii (Editorial Limusa, 1990).*

Nota: *El método de inducción matemática está explicado en muchos libros de matemáticas y es utilizado en numerosas demostraciones. Creemos que en estas breves notas se ha mostrado con suficiente claridad. Para profundizar un poco más, recomendamos los libros de Sominskii, y de Goloviná y Yaglóm, que forman parte de la colección Lecciones populares de Matemáticas de la Editorial Mir, que son los únicos referentes a este método que incluimos en la bibliografía. Consideramos que con estos dos libros se obtiene una visión muy completa del método de inducción matemática. El segundo puede ser considerado una continuación del primero.*

Bibliografía Adicional

1. Apostol, T. M. (1991). Inducción matemática, símbolos sumatorios y cuestiones relacionadas. *Calculus, Volume 1*. Editorial John Wiley & Sons, 457-515.
2. Engel, A. (1998). The Induction Principle. *Problem-Solving Strategies*. Editorial Springer, 205-220.

CAPÍTULO 2

2 ECUACIONES EN RECURRENCIA

José Manuel Gutiérrez Jiménez
Universidad de La Rioja

Palabras clave

- *Sucesiones*
- *Combinatoria*
- *Ecuación característica*
- *Matemática Discreta*

Las relaciones de recurrencia son una técnica que sirve para resolver algunos problemas combinatorios de forma sistemática. Pueden ser de gran utilidad para problemas donde el número de objetos a considerar depende de un parámetro que va creciendo, haciendo inviables otro tipo de recuentos. En ocasiones, hay que tener una buena dosis de ingenio para deducir una ley recurrente que nos permita abordar el problema.

2.1 Introducción

Antes de definir la que se entiende por una *recurrencia*. vamos a introducir algunos conceptos previos. Una sucesión es una función f definida sobre el conjunto de los números naturales $\mathbb{N} = \{1, 2, 3, \dots\}$:

$$f : \mathbb{N} \to \Omega.$$

Dependiendo de cómo sea el conjunto Ω, podemos tener diversos tipos de sucesiones:

- $\Omega = \mathbb{Z}$: sucesiones de números enteros.
- $\Omega = \mathbb{R}$: sucesiones de números reales.
- $\Omega = \mathbb{C}$: sucesiones de números complejos.
- $\Omega = \mathbb{R}^2$: sucesiones de vectores en el plano.
- $\Omega = \mathbb{R}^{m\times n}$: sucesiones de matrices de tamaño $m \times n$.

Aunque puede haber sucesiones definidas en los conjuntos anteriores y en muchos otros (espacios de funciones, por ejemplo), nuestro interés se centra en el caso de las sucesiones de números reales, $\Omega = \mathbb{R}$. Algunas matizaciones sobre la definición de sucesión:

- Se suele denotar $x_n = f(n)$ al n-ésimo término de la sucesión definida por f, que pasa a escribirse (x_n), e incluso, abusando de la notación, simplemente x_n.
- En algunos ejemplos puede ser conveniente definir la sucesión en $\mathbb{N} \cup \{0\} = \{0, 1, 2, 3, \dots\}$. Es más, el primer elemento del conjunto donde está definida la sucesión puede ser 1, 0, -1, 2 o cualquier otro número entero. Lo importante que a partir de un número dado estén todos los consecutivos hasta el infinito.

Una sucesión se puede definir de distintas maneras:

- Mediante una *fórmula explícita*, como por ejemplo $x_n = n + 2^n + (-1)^n$. En una sucesión dada de forma explícita, para calcular un término, simplemente hay que sustituir n por el valor correspondiente, como puede verse en el Cuadro 2.1.

n	1	2	3	5	10	25
x_n	2	7	10	36	1035	33554456

Cuadro 2.1: Algunos términos de la sucesión $x_n = n + 2^n + (-1)^n$.

- Mediante una *recurrencia*, como por ejemplo, $x_1 = 2,\ x_2 = 5,\ x_n = 3x_{n-1} - x_{n-2},\ n \geq 3$. En una sucesión dada de forma recurrente, para calcular un término, hay que calcular todos los anteriores, como se hace en el Cuadro 2.2.

n	3	4	5	6	7	8
x_n	13	34	89	233	610	1597

Cuadro 2.2: Primeros términos de la sucesión $x_n = 3x_{n-1} - x_{n-2}$, con $x_1 = 2$, $x_2 = 5$.

Dos problemas típicos relacionados con las recurrencias son los siguientes:

1. Encontrar la forma explícita de una sucesión dada en forma recurrente.
2. Plantear una recurrencia que nos ayude a resolver un problema combinatorio en el que, por ejemplo, sea necesario contar algo que dependa de un número natural n.

Vamos a ilustrar este planteamiento con un par de ejemplos clásicos.

Ejemplo 2.1 (Las torres de Hanoi, Edward Lucas, 1883) Tenemos una torre de n discos, apilados uno sobre otro en orden decreciente, insertados en una de tres agujas. El objetivo es pasar toda la torre de discos de una aguja a otra, moviendo sólo un disco cada vez y de forma que nunca puede colocarse un disco mayor sobre otro menor. Si, por ejemplo, tenemos $n = 64$ discos, ¿cuántos movimientos son necesarios para resolver el problema?

Nota: *El problema planteado por Lucas estaba basado en una leyenda en la que unos monjes tenían que mover los 64 discos. Cuando hubieren acabado su tarea, el mundo llegaría a su fin.*

Solución *Para resolver el problema, podemos tener en cuenta algunos consejos. El primero es introducir una notación adecuada. Por ejemplo, llamaremos T_n al número mínimo de movimientos necesarios para pasar una torre de n discos de una aguja a otra. Después podemos encontrar la solución del problema para los casos más sencillos. En este problema, para una torre con pocos discos. En la Figura 2.1 se muestra el caso de una torre con 3 discos.*

Así, es sencillo comprobar que $T_1 = 1; \quad T_2 = 3; \quad T_3 = 7; \quad T_4 = 15.$

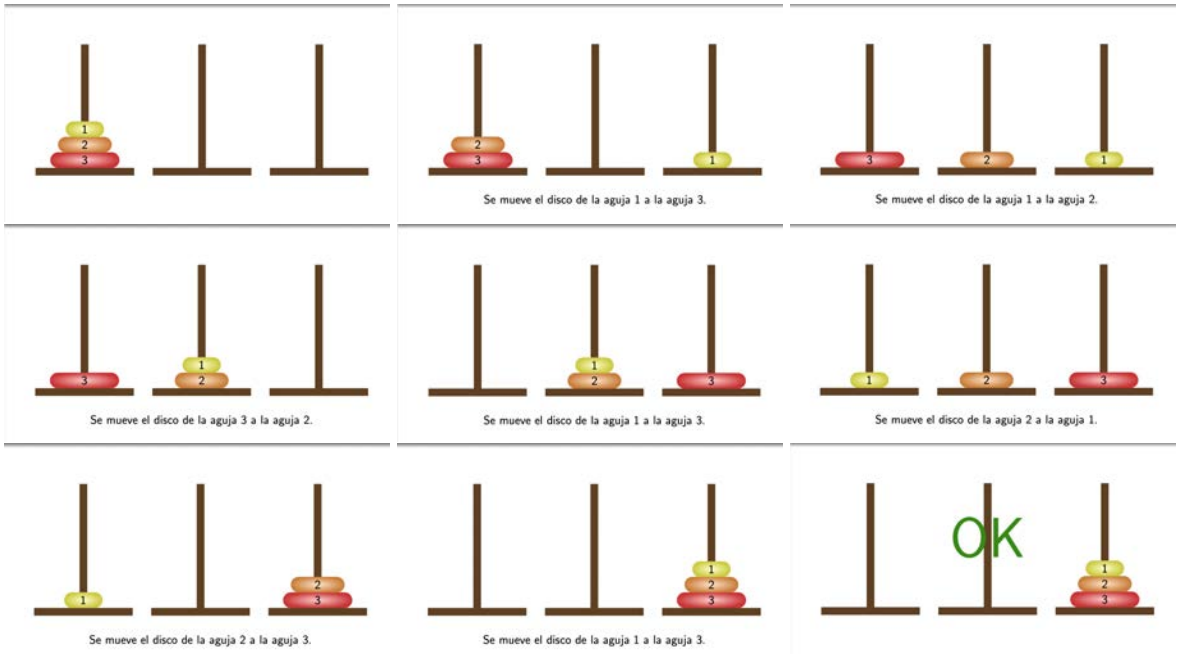


Figura 2.1: Movimientos necesarios en el problema de las Torres de Hanoi para el caso de 3 discos.

Una vez analizados los primeros casos y antes de calcular T_5 directamente, puede resultar conveniente buscar una estrategia recursiva *para resolver el problema. Dicha estrategia viene dada por los siguientes pasos:*

- *Paso 1: transferir los $n-1$ discos superiores a la aguja intermedia.*
- *Paso 2: pasar el último disco a la tercera aguja.*
- *Paso 3: mover los $n-1$ discos de la aguja intermedia a la tercera.*

En términos de T_n, el número de movimientos necesarios para transferir una torre de n discos es:

- *T_{n-1} para transferir los $n-1$ primeros discos a la aguja intermedia.*
- *Un movimiento para pasar el último disco a la tercera aguja.*
- *T_{n-1} para transferir los $n-1$ discos de la aguja intermedia a la tercera.*

Se llega así a la recurrencia:

$$T_n = 2T_{n-1} + 1, \qquad T_1 = 1. \tag{2.1}$$

Con ayuda de la recurrencia de la ecuación (2.1) *podemos resolver el problema combinatorio de las Torres de Hanoi. Incluso, para valores de* n *pequeños, podemos encontrar la solución sin muchas dificultades, como se muestra en el Cuadro 2.3.*

n	1	2	3	4	5	6	7	8
T_n	1	3	7	15	31	63	127	255

Cuadro 2.3: Primeros términos de la sucesión dada por (2.1).

Ahora bien, para valores de n *grandes el proceso se vuelve largo y pesado. Es conveniente buscar la forma explícita de la sucesión. A la vista de los primeros términos podemos conjeturar que*

$$T_n = 2^n - 1 \quad n \geq 1. \tag{2.2}$$

Sin embargo, esto no es una prueba. Una demostración rigurosa de la fórmula (2.2) *puede hacerse usando el principio de inducción. En primer lugar, tenemos que la base de la inducción se cumple, ya que para* $n = 1$ *se tiene* $T_1 = 2^1 - 1 = 1$*. En una segunda etapa, supongamos ahora que la fórmula es cierta para* $n < k$ *y probemos que entonces también es cierta para* $n = k$*. Como*

$$T_k = 2T_{k-1} + 1,$$

usando la hipótesis de inducción para $k - 1$*:*

$$T_k = 2(2^{k-1} - 1) + 1 = 2^k - 1,$$

por lo que la fórmula también es cierta para $n = k$*. De esta forma, hemos probado que* $T_n = 2^n - 1$ *para* $n \in \mathbb{N}$*. Para el problema de los monjes propuesto por Lucas (*$n = 64$*), se tiene que*

$$T_{64} = 18\,446\,744\,073\,709\,551\,615.$$

Para hacernos una idea de lo desorbitadamente grande que es esta cantidad, vamos a suponer que los monjes hacen un cambio cada segundo. Entonces, el mundo se acabaría aproximadamente 600 000 *millones de años después del primer movimiento. Teniendo en cuenta que la edad del Universo se estima que es* 13 770 *millones de años, han de pasar algo más de 43 veces la edad del Universo.*

Ejemplo 2.2 (Plano dividido por rectas de Jacob Steiner, 1826) ¿Cuál es el número máximo de regiones R_n en que queda dividido el plano por n rectas?

Solución *En este caso, el propio enunciado del problema ya nos proporciona una notación adecuada* R_n *para la solución del mismo. Antes de intentar resolverlo, hacemos un par de reflexiones que nos pueden ayudar a buscar la solución. Así, hacemos notar que para alcanzar el máximo número de regiones, no puede haber dos rectas paralelas ni tres rectas que sean concurrentes (esto es, que coinciden) en un punto.*

A continuación analizamos los casos más sencillos. Si no hay ninguna recta, $n = 0$*, sólo hay una región (*$R_0 = 1$*). Si hay una recta habrá dos regiones (*$R_1 = 2$*). Para dos rectas el número de regiones es* $R_2 = 4$ *y para tres rectas,* $R_3 = 7$*.*

El siguiente paso es buscar una recurrencia que nos permita resolver el problema. Si la recta n*-ésima corta a cada una de las* $n - 1$ *rectas anteriores, dicha recta queda dividida en* n *segmentos, cada uno de los cuales divide una región existente en dos partes. Por tanto*

$$R_n = R_{n-1} + n.$$

Como $R_0 = 1$, podemos encontrar una fórmula explícita para R_n usando la recurrencia una y otra vez. En efecto,

$$\begin{aligned} R_n &= R_{n-1} + n \\ &= R_{n-2} + (n-1) + n \\ &= R_{n-3} + (n-2) + (n-1) + n \\ &= \cdots \\ &= R_0 + 1 + 2 + \cdots + n = 1 + 1 + 2 + \cdots + n. \end{aligned}$$

Así, obtenemos finalmente la expresión

$$R_n = 1 + \frac{n(n+1)}{2}, \quad n \geq 0.$$

2.2 Recurrencias lineales

En ocasiones se puede encontrar un procedimiento para calcular el término general de una sucesión que viene dada de forma recurrente, como hemos visto en los ejemplos de la sección anterior. Lo mismo ocurre cuando tenemos una recurrencia lineal con coeficientes constantes. Existen técnicas que permiten determinar la solución en este caso y que se pueden encontrar en muchos libros de texto relacionados con la Combinatoria o la Matemática Discreta. Por sencillez, en esta sección vamos a plantear el caso de las recurrencias lineales de segundo orden. Los resultados y técnicas que vamos a desarrollar se pueden extender sin mucha complicación a órdenes superiores.

Definición 2.1

Una recurrencia lineal de segundo orden *es una sucesión (a_n) que viene definida de la forma*

$$a_{n+2} = c_1 a_{n+1} + c_2 a_n + f(n), \quad n \geq 0,$$

donde c_1 y c_2 son dos números reales conocidos y $f : \mathbb{N} \to \mathbb{R}$ es una función conocida. Para que (a_n) esté bien definida es necesario conocer los dos primeros términos, digamos a_0 y a_1. Si $f(n) \equiv 0$, la recurrencia se dice homogénea.

Presentamos a continuación, de forma muy resumida, una técnica para resolver recurrencias lineales de segundo orden. La misma está basada en encontrar todas las soluciones de la recurrencia homogénea asociada y una solución particular de la recurrencia no homogénea.

2.3 Recurrencias lineales homogéneas

Existe una técnica para encontrar el término general de una recurrencia lineal de segundo orden homogénea

$$a_{n+2} = c_1 a_{n+1} + c_2 a_n, \quad n \geq 0. \tag{2.3}$$

Se basa en los dos hechos siguientes:

1. El término general de una recurrencia lineal de primer orden homogénea $a_{n+1} = q a_n$, con $n \geq 0$, es de la forma $a_n = a_0 q^n$
2. Si (x_n) e (y_n) son dos sucesiones que satisfacen la ecuación (2.3), entonces la sucesión (z_n), tal que $z_n = Ax_n + By_n$, con $A, B \in \mathbb{R}$, también satisface la ecuación (2.3).

Como en las recurrencias de orden uno, podemos buscar si existen progresiones geométricas $a_n = \lambda^n$ que satisfacen

$$a_{n+2} = c_1 a_{n+1} + c_2 a_n, \quad n \geq 0.$$

Entonces, se tiene que cumplir $\lambda^{n+2} = c_1\,\lambda^{n+1} + c_2\,\lambda^n$. Dividiendo por λ^n, se obtiene la ecuación característica.

Definición 2.2

La ecuación característica *de una recurrencia lineal de segundo orden homogénea* (2.3) *es la siguiente ecuación polinómica de segundo grado*

$$\lambda^2 - c_1\lambda - c_2 = 0$$

Se distinguen tres situaciones, dependiendo de que las raíces de la ecuación característica sean:

- Dos números reales diferentes: λ_1 y λ_2. La solución es
$$a_n = A\lambda_1^n + B\lambda_2^n.$$
- Una única raíz doble λ. La solución es
$$a_n = (A + Bn)\lambda^n.$$
- Dos números complejos conjugados: $\lambda_1 = re^{i\theta}$ y $\lambda_2 = re^{-i\theta}$. La solución es
$$a_n = r^n(A\cos n\theta + B\,\mathrm{sen}\, n\theta).$$

En todos los casos, las constantes A y B se deducen de las condiciones iniciales a_0 y a_1.

Ejemplo 2.3 (La sucesión de Fibonacci) Este problema se atribuye a Leonardo de Pisa, alias *Fibonacci*, matemático italiano del siglo XII. Su enunciado es el siguiente: un hombre encerró a una pareja de conejos en un lugar rodeado por un muro por todas partes. ¿Cuántos pares de conejos pueden producirse a partir del par original durante un año si consideramos que cada pareja engendra al mes un nuevo par de conejos que se convierten en productivos al segundo mes de vida?

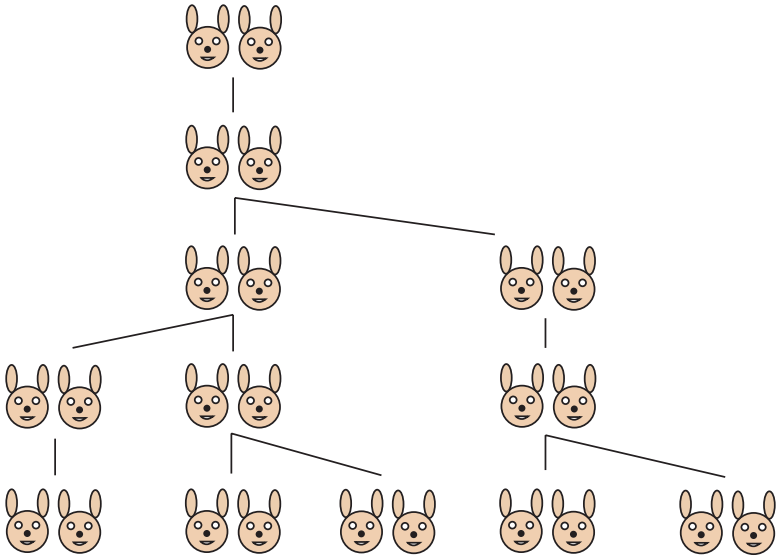


Figura 2.2: Evolución de la población de conejos en el problema de Fibonacci.

Solución *Para resolver el problema, empezamos siguiendo los consejos sugeridos en la sección anterior. En primer lugar, introducimos una notación adecuada llamando, por ejemplo, F_n al número de pares de conejos en el mes n-ésimo. Con ayuda de la Figura 2.2 analizamos lo que pasa en los primeros meses:*

$$F_1 = 1, \quad F_2 = 1, \quad F_3 = 2, \quad F_4 = 3, \quad F_5 = 5.$$

Con esta una información, podemos deducir una relación para los términos de la sucesión:

$$F_n = F_{n-1} + F_{n-2}, \quad n \geq 3.$$

La ecuación característica es, en este caso,

$$\lambda^2 - \lambda - 1 = 0.$$

Sus soluciones son $\lambda = (1 \pm \sqrt{5})/2$, por lo que la solución de la recurrencia es de la forma

$$F_n = A\left(\frac{1+\sqrt{5}}{2}\right)^n + B\left(\frac{1-\sqrt{5}}{2}\right)^n.$$

Los coeficientes A y B se determinan a partir de los dos primeros términos de la recurrencia, $F_1 = F_2 = 1$. Así, tenemos las siguientes ecuaciones:

$$\text{Para } n = 1: \qquad A\left(\frac{1+\sqrt{5}}{2}\right) + B\left(\frac{1-\sqrt{5}}{2}\right) = 1.$$

$$\text{Para } n = 2: \qquad A\left(\frac{1+\sqrt{5}}{2}\right)^2 + B\left(\frac{1-\sqrt{5}}{2}\right)^2 = 1.$$

Mediante una simple resta, las ecuaciones anteriores pueden escribirse como

$$(A+B) + \sqrt{5}(A-B) = 2,$$

$$3(A+B) + \sqrt{5}(A-B) = 2.$$

De aquí se deduce que $A + B = 0$ y $A - B = 2/\sqrt{5}$. Por lo que finalmente $A = 1/\sqrt{5}$, $B = -1/\sqrt{5}$. La solución para la sucesión de Fibonacci es

$$F_n = \frac{\left(\frac{1+\sqrt{5}}{2}\right)^n - \left(\frac{1-\sqrt{5}}{2}\right)^n}{\sqrt{5}}, \quad n \geq 1.$$

Los números F_n se llaman números de Fibonacci. *Notemos que, a pesar de su apariencia, por construcción, son números enteros.*

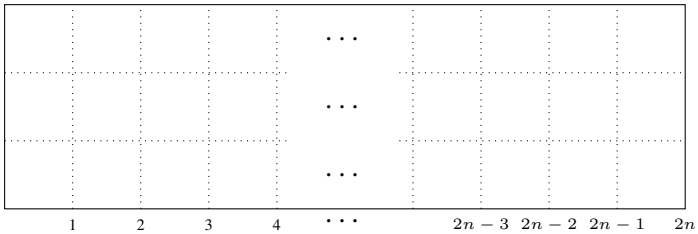
En la expresión de los números de Fibonacci, aparece una constante famosa, la razón áurea*,*

$$\phi = \frac{1+\sqrt{5}}{2},$$

también conocida como divina proporción*, sobre la cual se cuentan un gran número de curiosidades y propiedades.*

Por último, la solución al problema de los conejos planteado por Fibonacci es $F_{12} = 144$.

Ejemplo 2.4 ¿De cuántas formas se puede cubrir un rectángulo de base $2n$, $n \in \mathbb{N}$, y altura 3 con baldosas de tamaño 2×1? Encuentra una recurrencia que te ayude a resolver el problema.



Solución *Para resolver el problema, introducimos una notación adecuada. Por ejemplo, llamaremos u_n al número de tales recubrimientos. Empezamos calculando los casos más sencillos. Por ejemplo, para $n = 1$, se tiene que $u_1 = 3$, como se ve en la Figura 2.3.*

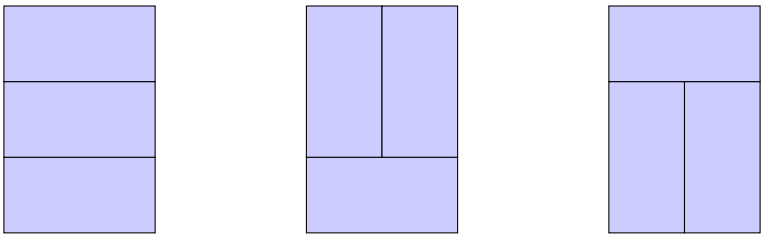


Figura 2.3: Soluciones al problema de las baldosas para $n = 1$.

Para $n = 2$, tenemos que cubrir un rectángulo 4×3. El número de recubrimientos posibles es $u_2 = 11$, como se aprecia en la Figura 2.4.

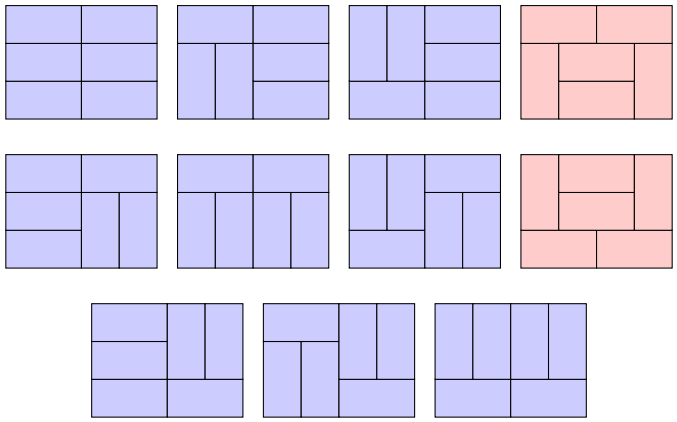


Figura 2.4: Soluciones al problema de las baldosas para $n = 2$.

Se puede llegar a una recurrencia para resolver el problema por razonamientos muy diversos. Por ejemplo, si volvemos a analizar el caso para $n = 2$, vemos que los posibles cubrimientos son:

- *3 veces los cubrimientos obtenidos para el caso $n = 1$, coloreados en azul.*
- *Más dos cubrimientos «especiales», que son los coloreados en rosa.*

En consecuencia, $u_2 = 3u_1 + 2 = 3 \times 3 + 2 = 11$..

Si analizamos el caso para $n = 3$, vemos que los posibles cubrimientos son:

- *Los del caso $n = 2$, adjuntando cada uno de los del caso $n = 1$ a la derecha ($3u_2$).*
- *Los del caso $n = 1$, adjuntando cada uno de los dos especiales de tamaño 3×4 a la derecha ($2u_1$).*
- *2 nuevos bloques especiales de tamaño 3×6 (véase la Figura 2.5).*

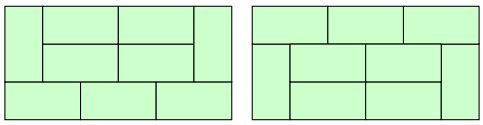


Figura 2.5: Los 2 nuevos bloques especiales de tamaño 3×6 en el problema de las baldosas para $n = 3$.

En consecuencia, $u_3 = 3u_2 + 2u_1 + 2 = 3 \times 11 + 2 \times 3 + 2 = 41$.

Repitiendo este razonamiento, llegamos a la expresión

$$a_{n+1} = 3a_n + 2a_{n-1} + 2a_{n-2} + \cdots + 2a_1 + 2,$$

Sin más que tener en cuenta que

$$a_n = 3a_{n-1} + 2a_{n-2} + 2a_{n-3} + \cdots + 2a_1 + 2.$$

y restar ambas expresiones, se obtiene la recurrencia:

$$a_{n+1} - a_n = 3a_n - a_{n-1} \Rightarrow a_{n+1} = 4a_n - a_{n-1}.$$

Si ahora queremos resolver la recurrencia para encontrar el término general de la misma, buscamos la ecuación característica, que en este caso es $\lambda^2 - 4\lambda + 1 = 0$. *Las raíces de la misma son* $\lambda_1 = 2 - \sqrt{3}$ *y* $\lambda_2 = 2 + \sqrt{3}$. *Por tanto*

$$a_n = A\lambda_1^n + B\lambda_2^n,$$

con $a_1 = 3$, $a_2 = 11$. *Para obtener* A *y* B *debemos resolver el sistema*

$$\begin{cases} A\lambda_1 + B\lambda_2 = 3 \\ A\lambda_1^2 + B\lambda_2^2 = 11 \end{cases}$$

para obtener finalmente la expresión explícita de la sucesión (a_n)

$$a_n = \frac{\left(3+\sqrt{3}\right)\left(2-\sqrt{3}\right)^n + \left(9+5\sqrt{3}\right)\left(2+\sqrt{3}\right)^n}{6\left(2+\sqrt{3}\right)}. \tag{2.4}$$

A pesar de su «fiera apariencia», esta sucesión está formada por números enteros positivos. Los primeros términos de esta sucesión se ven el el Cuadro 2.4.

n	1	2	3	4	5	6	7	8	9	10
a_n	3	11	41	153	571	2131	7953	29681	110771	413403

Cuadro 2.4: Primeros términos de la sucesión dada por la ecuación (2.4).

2.4 Recurrencias lineales no homogéneas

Consideremos ahora el caso de una recurrencia lineal no homogénea dada por la ecuación

$$a_{n+2} = c_1 a_{n+1} + c_2 a_n + f(n), \tag{2.5}$$

donde $f(n)$ es una función conocida de n, distinta de la función nula.

La solución general de la ecuación anterior depende de 2 constantes arbitrarias y su estructura es de la forma:

$$a_n = a_n^h + a_n^p,$$

donde a_n^h es la solución general de (2.5) con $f(n) = 0$ y a_n^p una solución particular de la ecuación (2.5).

El método de los *coeficientes indeterminados* es una técnica que permite encontrar soluciones particulares cuando $f(n) = p(n)r^n$, con $p(n)$ un polinomio de grado conocido y $r \in \mathbb{R}$ (generalizable a $\sum_{j=i}^{m} p_j(n)r_j^n$).

Si r no es solución de la ecuación característica de la recurrencia homogénea, este método consiste en buscar una solución de la forma

$$a_n^p = q(n)r^n.$$

Si r es raíz de la ecuación característica de multiplicidad m, entonces se busca $a_n^p = n^m q(n) r^n$.

En ambos casos, $q(n)$ y $p(n)$ son polinomios del mismo grado.

Ejemplo 2.5 Encuentra la solución de la recurrencia no homogénea $a_n = 4a_{n-1} - 6n$, $n \geq 1$, con $a_0 = 3$.

Solución *Es sencillo comprobar que la solución de la recurrencia honogénea $a_n = 4a_{n-1}$ es $a_n = C4^n$, con C una constante. Dado que el término independiente de la recurrencia no honogénea es $-6n$, esto es, un polinomio de grado 1, buscamos una solución particular de dicha recurrencia que sea de la forma $a_n = An + B$. Sin más que sustituir en la propia recurrencia, tenemos*

$$An + B = 4A(n-1) + 4B - 6n.$$

Igualando los coeficientes de ambos polinomios, tenemos que $A = 4A - 6$, $B = -4A + 4B$. Por tanto, $A = 2$, $B = 8/3$. La solución es $a_n = 2n + 8/3 + C4^n$.

La constante C la determinamos a partir de la condición inicial: $a_0 = 8/3 + C = 3$, luego $C = 1/3$ y la solución es

$$a_n = 2n + \frac{8 + 4^n}{3}.$$

2.5 Recurrencias no lineales

El problema de encontrar el patrón general que sigue una cierta sucesión de números puede dar lugar a recurrencias no lineales para las que, al contrario de las recurrencias lineales con coeficientes constantes, no existe un método general de resolución. Hay algunos resultados generales que pueden ayudar:

Proposición 2.1 (Regla del "bocadillo")

Si $a_n \leq b_n \leq c_n$ y las sucesiones (a_n) y (c_n) convergen al mismo límite L, entonces (b_n) también converge a L. Si $a_n \leq b_n$ y (a_n) tiende a infinito, entonces (b_n) también tiende a infinito.

Proposición 2.2 (Principio de Weierstrass)

Toda sucesión de números reales monótona y acotada es convergente.

Ejemplo 2.6 Demuestra que la sucesión definida por la recurrencia

$$a_0 = 0, \quad a_{n+1} = \sqrt{12 + a_n}, \quad n \geq 0,$$

es monótona creciente y acotada superiormente por 4. Encuentra su límite.

Solución *Usaremos unos razonamientos inductivos. En primer lugar, $a_0 < a_1$ pues $0 < \sqrt{12}$. Supongamos que $a_{n-1} < a_n$, entonces $a_n = \sqrt{a_{n-1} + 12} < \sqrt{a_n + 12} = a_{n+1}$, y (a_n) es creciente.*

Por otra parte, es claro que $a_0 = 0 < 4$. Supongamos $a_{n-1} < 4$, entonces $a_n = \sqrt{a_{n-1} + 12} < \sqrt{16} = 4$ y, por tanto, (a_n) está acotada superiormente.

En consecuencia, por el Principio de Weierstrass la sucesión (a_n) tiene un límite $L = \lim_{n\to\infty} a_n$, que podemos encontrar tomando límites en la propia expresión de la recurrencia:

$$L^2 = L + 12 \Longrightarrow L = 4, \text{ ya que necesariamente } L > 0.$$

Ejemplo 2.7 (La fórmula de Herón para aproximar raíces cuadradas) A Herón de Alejandría (10–70 d.C. aproximadamente) se le atribuye la fórmula para calcular el área de un triángulo, conocidos sus lados a, b y c:

$$\sqrt{s(s-a)(s-b)(s-c)}, \text{ con } s = (a+b+c)/2.$$

Para poder aplicarla, es necesario saber calcular raíces cuadradas o . . . al menos aproximarlas. Para calcular la raíz cuadrada de un número $A > 0$, se parte de una aproximación inicial a de $\sqrt{A}$ y se propone como nueva aproximación $(a + A/a)/2$. En general se repite el proceso para obtener la siguiente sucesión recurrente:

$$a_{n+1} = \frac{1}{2}\left(a_n + \frac{A}{a_n}\right), \quad n \geq 0.$$

Demuestra que esta sucesión converge, en efecto, a la raíz cuadrada de A.

Solución *Vamos a probar que si $a_0 > \sqrt{A}$, la sucesión definida por la recurrencia de Herón $a_{n+1} = f(a_n)$ con $f(x) = \frac{1}{2}\left(x + \frac{A}{x}\right)$, cumple $\sqrt{A} < a_{n+1} < a_n, \quad n \geq 0$. En consecuencia, es monótona decreciente y acotada inferiormente por $\sqrt{A}$, que es su límite.*

Notemos que $f(\sqrt{A}) = \sqrt{A}$. Además, f es creciente en $(\sqrt{A}, \infty)$, ya que $f'(x) > 0$ para $x > \sqrt{A}$. Entonces $a_1 < a_0$. En efecto,

$$a_1 = (a_0 + A/a_0)/2 < a_0 \iff a_0^2 > A,$$

que es cierto pues $a_0 > \sqrt{A}$. Por otra parte, veamos que $\sqrt{A} < a_1$. Por el Teorema del Valor Medio, existe $\xi_0 \in (\sqrt{A}, a_0)$ tal que

$$a_1 - \sqrt{A} = f(a_0) - f(\sqrt{A}) = f'(\xi_0)(a_0 - \sqrt{A}).$$

Como $f'(x) > 0$ para $x > \sqrt{A}$, es cierto $\sqrt{A} < a_1$.

De forma parecida se prueba por inducción que $\sqrt{A} < a_{n+1} < a_n$ para $n \geq 0$. Por el principio de Weierstrass, existe $L = \lim_{n\to\infty} a_n$, con $L \geq \sqrt{A}$. Tomando límites en la expresión de la sucesión:

$$L = \frac{1}{2}\left(L + \frac{A}{L}\right) \Rightarrow L^2 = A \overset{L\geq\sqrt{A}}{\Longrightarrow} L = \sqrt{A}.$$

Hemos visto que si se toma como punto de partida un valor $a_0 \in (\sqrt{A}, \infty)$ se obtiene una sucesión monótona decreciente a $\sqrt{A}$. Sin embargo, si $a_0 \in (0, \sqrt{A})$, $a_1 \in (\sqrt{A}, \infty)$. A partir de aquí la sucesión es monótona decreciente a $\sqrt{A}$. Este ejemplo pone de manifiesto la importancia del punto de partida a la hora de estudiar la convergencia de una sucesión recurrente no lineal.

El análisis gráfico de la función que define la sucesión,

$$f(x) = \frac{1}{2}\left(x + \frac{A}{x}\right)$$

nos permite hacer algunas consideraciones gráficas interesantes:. En primer lugar, los posibles límites[1] de la sucesión (a_n) son puntos fijos de f, es decir puntos tales que $f(L) = L$. Estos puntos son intersecciones de las gráficas de $y = f(x)$ y de la diagonal $y = x$.

Podemos hacer un análisis gráfico de una sucesión (a_n) obtenida por iteración de una función f siguiendo los siguientes pasos:

- *Dibujar sobre los mismos ejes las gráficas de $y = f(x)$ y de la diagonal $y = x$.*
- *Situar el punto de partida a_0 sobre el eje de abcisas y desplazarse verticalmente hasta la gráfica de $y = f(x)$, obteniendo un punto cuya abcisa es $f(a_0) = a_1$.*

[1] El límite de una sucesión, si existe, es único. Ahora bien, para distintos puntos de partida se obtienen sucesiones diferentes y, por tanto, posibles límites diferentes.

- *Desplazarse horizontalmente hasta la diagonal* $y = x$.
- *Volver a desplazarse verticalmente hasta cortar la curva* $y = f(x)$*, obteniendo un punto cuya abcisa es* $f(a_1) = a_2$.
- *Repetir el proceso las veces que se consideren oportunas.*

En la Figura 2.6 se muestra la representación gráfica de las iteraciones de $a_{n+1} = \frac{1}{2}\left(a_n + \frac{2}{a_n}\right)$*, con* $a_0 = 5$ *(izquierda) y* $a_0 = 0.3$ *(derecha). Ambas converge a* $\sqrt{2} \approx 1.41421$.

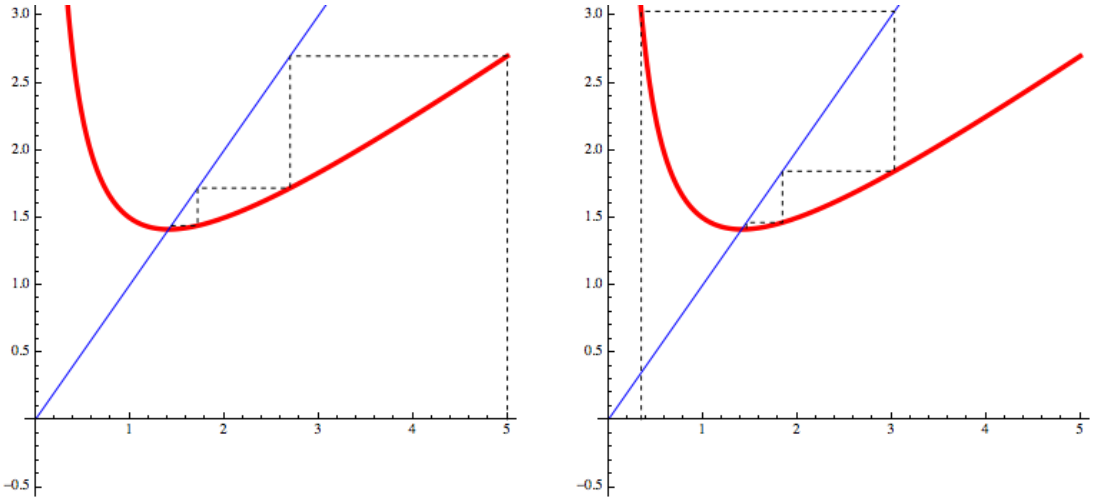


Figura 2.6: Análisis gráfico de un par de iteraciones dadas por la fórmula de Herón para aproximar $\sqrt{2}$.

Ejemplo 2.8 La función logística A pesar de su aparente sencillez, las iteraciones de la función logística

$$\ell_\lambda(x) = \lambda x(1-x), \quad \lambda \in \mathbb{R},$$

esconden interesantes sorpresas. Un experimento interesante es calcular, con ayuda de una calculadora o de un ordenador, unas cuantas iteraciones de

$$x_{n+1} = \ell_\lambda(x_n) = \lambda x_n(1-x_n)$$

para distintos puntos de partida y distintos valores de λ y ver qué ocurre.

Solución *Para fijar ideas, tomemos el punto de partida* $x_0 = 0.5$*, así como distintos valores de* λ.

1. $\lambda = 1$*: (x_n) es monótona decreciente a 0.*
2. $\lambda = 2$*: (x_n) es constantemente* $1/2$.
3. $\lambda = 2.5$*: (x_n) es convergente, de forma oscilante, a* 0.6.
4. $\lambda = 3.2$*: a partir de un cierto n, (x_n) va tomando los valores* 0.513045 *y* 0.799455.
5. $\lambda = 3.3$*: la tendencia repetitiva aumenta a cuatro términos* 0.38280, 0.826941, 0.500884 *y* 0.874997.
6. $\lambda = 3.8$*: no se aprecia ningún tipo de orden en los términos de la sucesión.*

Podemos estudiar con detalle la convergencia de la función logística en algunos casos:

1. $\lambda = 1$ *y* $x_0 = 1/2$*. En este caso* $x_{n+1} = \ell_1(x_n) = x_n(1-x_n)$*. Es muy sencillo comprobar que* $0 < x_{n+1} < x_n$ *para* $n \geq 0$*. Por lo tanto* $\lim_{n\to\infty} x_n = 0$.
2. $\lambda = 3/2$ *y* $x_0 = 1/2$*. Ahora* $x_{n+1} = \ell_{3/2}(x_n) = 3/2x_n(1-x_n)$ *y se tiene que* $1/3 < x_{n+1} < x_n$ *para* $n \geq 0$*. Por lo tanto* $\lim_{n\to\infty} x_n = 1/3$.
3. $\lambda = 2$ *y* $x_0 = 1/10$*. La sucesión está definida por* $x_{n+1} = \ell_2(x_n) = 2x_n(1-x_n)$ *y, en este caso,* $x_n < x_{n+1} < 1/2$ *para* $n \geq 0$*. En consecuencia,* $\lim_{n\to\infty} x_n = 1/2$.

El estudio para otros valores de λ es más complicado y requiere de técnicas y herramientas numéricas. Se puede detectar la aparición de comportamientos cíclicos e, incluso, de comportamientos caóticos.

Nota: *Hemos visto unas cuantas técnicas clásicas para trabajar con recurrencias, tanto lineales como no lineales. Existen muchas otras técnicas: cambios de variables, recurrencias dobles, funciones generadoras, etc.*

Ejercicios Propuestos

1. Se quiere recubrir un rectángulo de tamaño $2 \times n$ con baldosas de tamaños 2×2 y 2×1. Encuentra una relación de recurrencia para calcular a_n, el numero total de recubrimientos diferentes que pueden hacerse.

2. Busca el término general de la sucesión recurrente
$$a_0 = 1, \quad a_{n+1} = \frac{a_n}{1 + a_n}, \quad n \geq 0.$$

3. Estudia la convergencia de la sucesión $x_{n+1} = x_n(2 - x_n)$, $n \geq 0$, con $x_0 = 0.1$.

4. Un matemático despistado escribe mal la sucesión de Fibonacci, cambiando el signo de la suma por el del producto:
$$a_0 = 1 \quad a_1 = 2, \quad a_{n+1} = a_n a_{n-1}, \quad n \geq 1.$$
¿Cuál es la fórmula general de la sucesión obtenida?

5. Calcula la fórmula general de la sucesión (b_n) dada por
$$\begin{cases} b_1 = 8, \quad b_2 = 26, \\ n(n+1)b_{n+2} = 4n(n+2)b_{n+1} - 3(n+1)(n+2)b_n, \quad n \geq 0. \end{cases}$$

6. La sucesión (c_n) cumple
$$\begin{cases} c_1 = 1, \\ c_{n+m} + c_{n-m} = \dfrac{c_{2m} + c_{2n}}{2}, \quad m \geq n \geq 0. \end{cases}$$
Encuentra el término general de (c_n).

7. Se define la sucesión (d_n) por
$$\begin{cases} d_0 = d_1 = 1, \\ d_{n+1} = 1 + d_n d_{n-1}, \quad n \geq 1. \end{cases}$$
Prueba que d_{2017} no es divisible entre 4.

8. Se define la sucesión (e_n) por
$$\begin{cases} e_1 = e_2 = 1, \\ e_{n+1} = \dfrac{e_n^2 + 2}{e_{n-1}}, \quad n \geq 2. \end{cases}$$
Prueba que (e_n) es una sucesión de números enteros.

9. Tenemos n objetos numerados del 1 al n y tenemos n lugares para dejarlos, también numerados del 1 al n. Sea f_n el número de formas de dejar los objetos sin que haya ninguno en su lugar (este tipo de permutaciones se llaman *desarreglos* o *desórdenes*). Calcula una recurrencia para f_n y encuentra su término general.

Pista: Analiza los casos más sencillos para $f_1 = 0$, $f_2 = 1$, $f_3 = 2$, etc. Usa una notación adecuada que te ayude a buscar una recurrencia. Por ejemplo, puedes expresar los desarreglos de 3 elementos en forma de permutación:

$$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \qquad \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}.$$

Piensa en los desarreglos de n como elementos de la forma:

$$\begin{pmatrix} 1 & \dots & i & \dots \\ i & \dots & 1 & \dots \end{pmatrix}$$

y en los de la forma ($j \neq 1$)

$$\begin{pmatrix} 1 & \dots & i & \dots \\ i & \dots & j & \dots \end{pmatrix}$$

Prueba que $f_1 = 0$; $f_2 = 1$; $f_n = (n-1)(f_{n-1}+f_{n-2})$, $n \geq 3$. Equivalentemente, $f_0 = 1$; $f_n - nf_{n-1} = (-1)^n$, $n \geq 1$. La solución es

$$f_n = \sum_{k=0}^{\infty} \frac{(-1)^k}{k!}, \quad n \geq 0.$$

Bibliografía Adicional

1. Alegría, P. (2009). Sucesiones de recurrencia en la matemática recreativa. *Rev. Eureka Enseñ. Divul.Cien.*, **6** (3), 483-490. https://www.ehu.eus/~mtpalezp/descargas/eureka_2009.pdf
2. Engel, A. (1998). Sequences. *Problem-Solving Strategies*. Editorial Springer, 221-240.
3. Guitérrez Jiménez, J. M. & Lanchares Barrasa, V. (2010). *Elementos de matemática discreta*. Servicio de Publicaciones de la Universidad de La Rioja. https://dialnet.unirioja.es/servlet/libro?codigo=424510

CAPÍTULO 3

3 EL PRINCIPIO DEL PALOMAR

Víctor Lanchares Barrasa
Universidad de La Rioja

Palabras clave

- *Palomas y nidos*
- *Principio del palomar generalizado*
- *Combinatoria*

Cuando nos enfrentamos a la resolución de un problema matemático, uno tiende a pensar que se requieren técnicas y conocimientos sofisticados. Sin embargo, en algunas ocasiones, solo son necesarias algunas nociones o principios elementales, que podríamos decir que son de sentido común. No obstante, la aplicación de estos principios no siempre es evidente y es ahí donde radica la dificulatad. En este capítulo veremos una de las técnicas básicas para la resolución de algunos problemas, que van desde algunos muy elementales hasta otros de gran dificultad. La mayoría de ellos pertenecen a la clase de problemas en los que se pide demostrar la existencia o no de una determinada propiedad. En este sentido, como norma general, tendremos demostraciones no constructivas, es decir, demostraciones en las que no podemos dar un ejemplo concreto que pruebe nuestra afirmación.

3.1 Introducción

El *principio del palomar* o *principio de las cajas* nos presenta una afirmación que, aparentemente, no necesita demostración.

Proposición 3.1 (Principio del palomar)
Si distribuimos una serie de objetos en cajas y hay más objetos que cajas, entonces habrá una caja que contenga al menos dos objetos.

No es difícil formular una versión generalizada de este mismo principio, que ponemos ya en términos matemáticos.

Proposición 3.2 (Principio del palomar generalizado)
Si distribuimos $km+n$ objetos en m cajas, y $n \geq 1$, entonces alguna caja tiene al menos $k+1$ objetos.

Demostración Supongamos que ninguna de las m cajas tiene más de k objetos, y $n > 1$. Entonces, el número total de objetos es menor o igual que km, que es estrictamente menor que el total de objetos $km+n$. Así, hemos llegado a una contradicción, por lo que alguna caja tiene que tener más de k objetos, es decir, al menos $k+1$. ■

El origen de este principio se atribuye al matemático del siglo XIX Johann Peter Gustav Lejeune Dirichlet (1805-1859), quien lo aplicó para realizar algunas demostraciones en sus investigaciones matemáticas, por lo que también se conoce como principio de Dirichlet. Sin embargo, debemos remontarnos un par de siglos atrás, hasta el siglo XVII, para encontrar la que parece ser la primera aparición de este principio. Está relacionada con una sorprendente afirmación que sirve como punto de partida para ver la potencia del mismo:

"Es absolutamente necesario que haya dos hombres con el mismo número de pelos en la cabeza.[1]*"*

Con toda seguridad podemos afirmar que no hay ningún hombre que tenga más de un millón de pelos en la cabeza. Como en el mundo hay más de un millón de hombres, necesariamente debe haber dos de ellos con el mismo número de pelos.

Nota: *Tal como se dijo al principio, esto es una prueba de existencia y no podemos decir qué personas en concreto son las que tienen igual número de pelos.*

En el ejemplo que acabamos de ver, es fácil reconocer que el principio del palomar nos va a conducir a la solución. De hecho, es más o menos evidente identificar los objetos, o palomas, y las cajas, o nidos. En este caso, los nidos son los números comprendidos entre el 0 (para aquellos hombres que no tienen ningún pelo en la cabeza) y un millón (aquellos que tienen el mayor número posible de pelos), mientras que las palomas son todos los hombres que hay en el mundo. Antes de plantear una serie de ejercicios elementales, veamos un par de ejemplos más.

Ejemplo 3.1 Bruno tiene 10 bolsillos en el abrigo y 44 monedas de euro. Quiere meter las monedas en los bolsillos, de manera que en cada bolsillo haya un número distinto de monedas. ¿Es posible hacerlo?

Solución *En este caso los nidos van a ser los números del 0 al 9, que representan el número de monedas que*

[1] Jean Leurechon. *Récréation Mathematique: Composee De Plusieurs Problemes Plaisants Et Facetieux*, 1626.

puede haber en un bolsillo, mientras que las palomas serán los bolsillos. Si hubiera una paloma en cada nido, habríamos sido capaces de poner en cada uno de los 10 bolsillos un número distinto de monedas. Ahora bien, en ese caso tendríamos $0+1+2+3+4+5+6+7+8+9=45$ *monedas, pero eso no es posible, ya que solo hay 44 monedas. Esto quiere decir que alguno de los nidos está ocupado por más de una paloma o, lo que es lo mismo, hay la misma cantidad de monedas en dos de los bolsillos.*

Ejemplo 3.2 Un total de n equipos de fútbol se enfrentan entre sí jugando partidos todos los fines de semana hasta que al final se enfrenten todos contra todos. Pruébese que al acabar cada fin de semana siempre hay dos equipos que han jugado, hasta ese momento, el mismo número de partidos.

Solución *Identificamos los nidos como el número de partidos que ha podido jugar un equipo hasta ese momento. Este número puede variar entre 0, si todavía no ha jugado ningún partido, y* $n-1$*, si se ha enfrentado a todos los demás equipos. Así, tenemos* n *nidos y* n *equipos. Parece que no podemos aplicar el principio del palomar, pero analicemos un poco mejor la situación. Los nidos* 0 *y* $n-1$ *son incompatibles, pues no puede darse el caso de que un equipo haya jugado contra todos los demás y otro no haya jugado ningún partido. Por lo tanto el número de nidos es uno menos, es decir* $n-1$*. Como hay* n *equipos, en algún nido tiene que haber al menos dos equipos. Es decir, todas las semanas habrá al menos dos equipos que lleven jugados el mismo número de partidos.*

3.2 El principio del palomar y problemas aritméticos

Una vez que hemos visto algunas aplicaciones casi inmediatas del principio del palomar, vamos a pasar a conssiderar su aplicación a algunos problemas interesantes en el contexto de la aritmética. Esto nos va a permitir probar algunas propiedades que, con otras técnicas, sería más complicado de hacer. Para empezar, vamos a considerar un ejemplo bastante sencillo

Ejemplo 3.3 Probar que, dados 8 números naturales cualesquiera, siempre hay al menos dos cuya diferencia es múltiplo de 7.

Solución *En este caso los nidos van a ser los posibles restos que se obtienen al dividir un número por 7. Es decir, los números 0, 1, 2, 3, 4, 5, 6. En total hay 7 restos posibles. Como tenemos 8 números, podemos asegurar que habrá al menos dos de ellos que dejan el mismo resto al dividirlos por 7. Por tanto, la diferencia de estos dos números es divisible por 7.*

Nota: *Podemos generalizar el enunciado del ejemplo anterior a cualquier número. Así, podemos afirmar que, dada una colección de* $n+1$ *números, siempre hay dos de ellos cuya diferencia es un múltiplo de* n*.*

A aprtir de aquí, se puede explotar esta misma idea para abordar problemas más complejos. Este es el caso del siguiente ejemplo.

Ejemplo 3.4 Probar que existe al menos un número, cuyos dígitos son todos igual a 1, que es múltiplo de 7.

Solución *Consideremos los 8 números* $a_1=1$*,* $a_2=11$*,* $a_3=111$*,* $a_4=1111$*,* $a_5=11111$*,* $a_6=111111$*,* $a_7=1111111$*,* $a_8=11111111$*. Por el problema anterior, hay dos de ellos,* a_i*,* a_j *(*$i<j$*), cuya diferencia es múltiplo de 7. Es decir*

$$a_j-a_i=\underbrace{1\cdots1}_{j-i}\underbrace{0\cdots0}_{i}=\underbrace{1\cdots1}_{j-i}10^i=\dot{7},$$

donde $\dot{7}$ significa un múltiplo de 7. Puesto que 10^i no es múltiplo de 7, ya que 7 y 10 son primos entre sí (no tienen divisores comunes), entonces $\underbrace{1\cdots1}_{j-i}$ es múltiplo de 7.

Al igual que antes, podemos generalizar el enunciado del ejemplo anterior y formular la siguiente proposición.

Proposición 3.3

Si n y 10 son primos entre sí, entonces existe al menos un número, cuyos dígitos son todos iguales, que es múltiplo de n.

Explotando aún más la idea del Ejemplo 3.3 se puede abordar el siguiente problema.

Problema 3.1 Probar que existe una potencia de 3 que acaba en 001.

Solución *Como en los casos anteriores, tomamos los números $a_j = 3^j$, con $j = 1, \ldots, 1001$, es decir las primeras 1001 potencias de 3. Según lo que hemos visto, necesariamente dos de ellas dejan el mismo resto al dividir por 1000. Por tanto, existen índices i, j, con $i < j$, tales que $3^j - 3^i$ es múltiplo de 1000. Por otra parte,*

$$3^j - 3^i = 3^i(3^{j-i} - 1) = 10\dot{0}00.$$

Como 3 y 1000 no tienen divisores comunes, $3^{j-i} - 1$ es múltiplo de 1000, es decir, acaba en tres ceros. Por tanto, 3^{j-i} acaba en 001.

3.3 El principio del palomar y desigualdades

Los problemas relacionados con la aritmética no son los únicos en los que podemos aplicar el principio del palomar. Donde se revela también útil es en el terreno de las desigualdades, por su puesto no en todos los casos. De hecho, fue aquí donde Dirichlet lo aplicó con éxito. El siguiente ejemplo está en la línea de lo que Dirichlet llegó a probar sobre lo que se conoce como aproximaciones diofantinas de los números reales.

Ejemplo 3.5 Sea x un número real cualquiera. Probar que entre los números

$$x, 2x, 3x, \ldots, (n-1)x$$

hay al menos uno cuya distancia a un número entero es a lo sumo $1/n$.

Solución *Lo primero es ver que basta considerar la parte decimal de los $n-1$ números, que es lo que nos va a indicar la distancia a un entero. Ahora, dividimos el intervalo $[0,1]$ en n subintervalos de longitud $1/n$, como se muestra en la Figura 3.1*

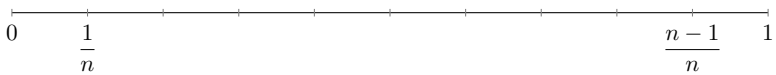


Figura 3.1: División del intervalo $[0,1]$ en n subintervalos.

Si al menos uno de los números está en el intervalo $[0, 1/n]$ o en el $[(n-1)/n, 1]$, ya estaría probado. Si este no fuera el caso, habría $n-1$ números distribuidos en $n-2$ intervalos y en uno de ellos habría al menos dos, digamos jx y kx, con $k > j$ (véase la Figura 3.2). Ahora bien, $(k-j)x$, es uno de los números que nos han dado y su distancia a un entero es claramente inferior a $1/n$, lo que contradice que no haya ningún número en el primer o último intervalo.

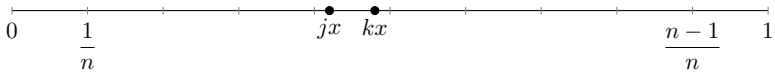


Figura 3.2: Los números jx y kx, con $k > j$, que están en el mismo subintervalo.

Nótese que el problema anterior es un problema de existencia, donde lo que se busca es probar que uno de los números dados, no importa en concreto cuál, verifica la propiedad deseada. En este sentido, no es un problema clásico de desigualdades como puede ser probar que, dados a y b, números reales cualesquiera, $a^2 + b^2 \geq 2ab$. Este matiz suele ser una pista para conducirnos al principio del palomar. Es decir, si tenemos que probar la existencia o no de alguna propiedad, el principo del palomar puede estar escondido detrás de la demostración. Esto es lo que sucede con el siguiente ejemplo.

Ejemplo 3.6 Probar que existen enteros a, b y c, no todos cero y cuyo valor absoluto es menor que 1.000.000, tales que

$$|a + b\sqrt{2} + c\sqrt{3}| < 10^{-11}.$$

Solución *La idea es considerar suficientes números en un determinado intervalo, de manera que pueda dividirse en partes de longitud apropiada y aplicar el pricipio del palomar para ver que dos de dichos números están en el mismo subintervalo. Lo que viene ahora es una cuestión de ajustar la cantidad de números y la longitud del intervalo. Para determinar la cantidad de números nos fijamos en la cota para los valores de los parámetros a, b y c. Como todos son menores que 1.000.000, vamos a considerar el siguiente conjunto de 10^{18} números*

$$S = \{r + s\sqrt{2} + t\sqrt{3} \mid 0 \leq r, s, t < 10^6 - 1\}.$$

El siguiente paso es dar una cota para los números de este conjunto. Pero esto no es muy difícil, pues basta tomaar $a = b = c = 1.000.000$. De esta manera obtenemos la cota $d = (1 + \sqrt{2} + \sqrt{3})10^6$. Entonces, para cada $x \in S$, $0 \leq x < d$. Como tenemos 10^{18} números, dividimos el intervalo $[0, d]$ en $10^{18} - 1$ partes iguales. Es decir, cada parte tiene una longitud $L = d/(10^{18} - 1) < 10^{-11}$. Como hay más números que partes en el intervalo $[0, d]$, por el principio del palomar, hay al menos dos elementos del conjunto S en un mismo subintervalo de longitud L. Si esos números son

$$s_1 = a_1 + b_1\sqrt{2} + c_1\sqrt{3}, \quad s_2 a_2 + b_2\sqrt{2} + c_2\sqrt{3},$$

entonces

$$s = (a_1 - a_2) + (b_1 - b_2)\sqrt{2} + (c_1 - c_2)\sqrt{3},$$

que está en el conjunto S, cumple que $|s| < L < 10^{-11}$.

3.4 El principio del palomar y problemas geométricos

El principio del palomar lo encontramos también en problemas de corte geométrico, donde los nidos, o palomares, pueden construirse gráficamente en algunos casos. Un ejemplo típico es el siguiente

Ejemplo 3.7 Prueba que, dados 5 puntos en un triángulo equilátero de lado 2, siempre podemos encontrar dos que están a distancia menor o igual que 1.

Solución *La idea es construir cuatro palomares, a partir de una división adecuada del triángulo equilátero en cuatro partes iguales. Esta división se ve en la Figura 3.3.*

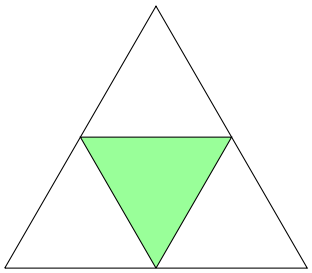


Figura 3.3: División del triángulo equilátero.

Observamos que el triángulo original se ha dividido en cuatro triángulos equiláteros de lado 1. Es evidente que, si tomamos 5 puntos, dos de ellos estarán en el mismo triángulo, por lo que su distancia no puede ser mayor que el lado del mismo, es decir 1.

Ejemplo 3.8 Dados 51 puntos en un cuadrado de lado 1, prueba que siempre podemos encontrar tres de ellos que pueden cubrirse con un círculo de radio 1/7.

Solución *Las condiciones del problema nos sugieren cuántos palomares debemos buscar. De hecho, al decirnos que hay al menos tres puntos, podemos pensar que hemos distribuido dos puntos en cada palomar y al final nos sobra uno que debemos de introducir en alguno de los palomares que ya tienen dos puntos. Así pues, buscamos 25 palomares, en los que habrá 2 puntos en cada uno de ellos y el punto 51 tendrá que estar en algún palomar con otros dos. Ahora bien, un cuadrado de lado 1 se puede dividir sin dificultad en 25 cuadrados de lado 1/5, como se muestra en la siguiente Figura 3.4. Por el principio del palomar, sabemos que en alguno de*

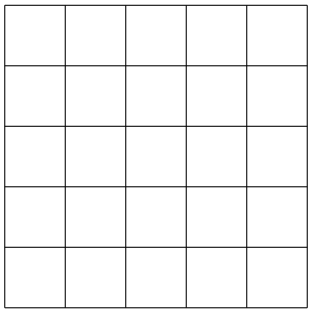


Figura 3.4: División de un cuadrado en 25 cuadrados de lado $1/5$.

estos cuadrados hay al menos tres puntos. Sin embargo, en el enunciado se habla de círculos. Para buscar el círculo, basta darse cuenta de que un cuadrado puede cubrirse con un círculo, cuyo radio, R, es la mitad de su diagonal. Como el lado del cuadrado es 1/5, se tiene

$$R = \frac{1}{5\sqrt{2}} < \frac{1}{7},$$

con lo que queda resuelto el problema.

Ejemplo 3.9 Se consideran 7 puntos en un rectángulo 3×4. Demuestra que siempre hay dos de ellos a distancia menor o igual que $\sqrt{5}$. Demuestra que esto sigue siendo cierto cuando se consideran 6 puntos.

Solución *Para resolver el primer apartado, construimos 6 palomares consistentes en rectángulos de dimensión* 2×1*, como se muestra en la Figura 3.5.*

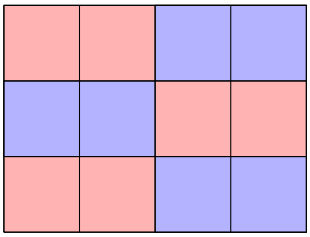


Figura 3.5: Construcción de 6 palomares.

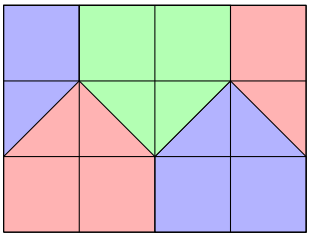


Figura 3.6: Construcción de 5 palomares.

La distancia máxima en cada uno de los palomares es igual a la diagonal del rectángulo, que es igual a $\sqrt{5}$*. Como hay 7 puntos y 6 palomares, hay al menos dos puntos a distancia no mayor que* $\sqrt{5}$*.*

Para la segunda parte, no valen los 6 palomares anteriores y hay que buscar 5 palomares en los cuales la distancia máxima siga siendo $\sqrt{5}$*. Eso puede conseguirse dividiendo el rectángulo como en la Figura 3.6.*

No siempre los problemas son del mismo tipo que los anteriores, la variedad de los mismos es muy grande y podemos ver aplicaciones del principio del palomar en problemas geométricos espaciales, aunque nosotros seguiremos en el plano, esta vez con problemas de coloración.

Ejemplo 3.10 Cada punto del plano está pintado de color rojo o de color azul. Probar que existe un rectángulo que tiene los cuatro vértices del mismo color.

Solución *Trazamos tres líneas paralelas, tal y como se muestra en la Figura 3.7, y sobre ellas vamos a encontrar los vértices de nuestro rectángulo.*

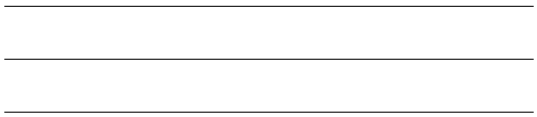


Figura 3.7: Líneas horizontales para construir el rectángulo.

La idea es situar sobre ellas suficientes puntos que nos permitan encontrar los vértices de nuestro rectángulo. Con tal fin, trazamos nueve líneas perpendiculares a las tres horizontales como en la Figura 3.8.

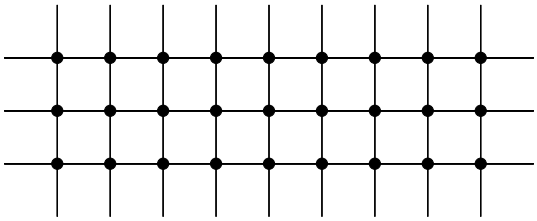


Figura 3.8: Intersección de la líneas verticales y horizontales.

Notemos que sobre cada línea vertical hay una terna de puntos, que son como resultado de la intersección de cada línea vertical con las tres líneas horizontales. Ahora bien, esos tres puntos pueden colorearse con dos colores de 8 formas diferentes (2 colores por cada punto). Las 8 diferentes coloración de esos tres puntos puede

verse en la Figura 3.9, donde hemos empezado por la primera fila coloreando todos los vértices son de color rojo y terminando en la octava columna coloreando todos los vértices de color azul.

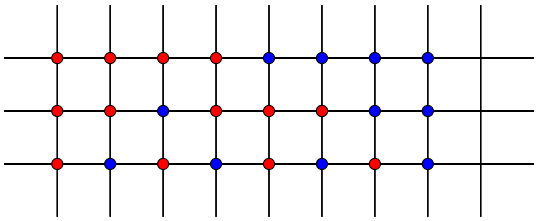


Figura 3.9: Las 8 posibles coloraciones de las ternas de puntos.

Cuando vayamos a colorear los tres puntos de la última recta, necesariamente tendremos que repetir una terna de colores y, de las ternas repetidas tendremos los vértices de nuestro rectángulo, ya que en cada terna hay siempre dos puntos del mismo color. El rectángulo cuyos vértices tienen la misma coloración, tal y como se muestra señalado en la Figura 3.10.

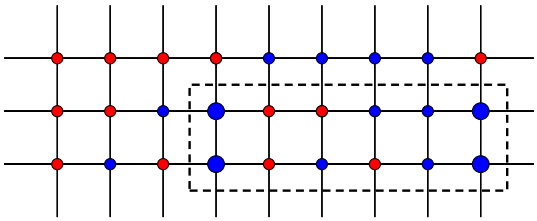


Figura 3.10: Rectángulo con los vértices del mismo color.

Ejercicios Propuestos

1. Una bolsa contiene bolas de cinco colores diferentes. ¿Cuál es el menor número de bolas que debemos sacar, sin mirarlas, para asegurar que tenemos dos del mismo color?

2. Pruébese que en un grupo de 37 personas hay al menos cuatro que han nacido en el mismo mes.

3. ¿Cuántas personas se necesitan para asegurar que hay dos que cumplen años el mismo día?

4. Si tenemos 10 pares de zapatos iguales, ¿cuántos zapatos debemos coger para asegurar que hemos sacado un par que nos podemos poner?

5. En un cajón hay 100 calcetines rojos, 80 verdes, 60 azules y 40 negros. Sacamos los calcetines al azar uno por uno, sin volverlos a meter en el cajón. ¿Cuál es el menor número de calcetines que debemos sacar para asegurar que hay al menos 10 pares de calcetines correctos?

6. Una persona toma al menos una aspirina diaria durante 30 días seguidos. Si ha tomado 45 aspirinas en total, pruébese que hay una serie de días consecutivos en los que ha tomado exactamente 14 aspirinas.

7. Dada una sucesión de n números enteros cualesquiera, no necesariamente diferentes, pruébese que siempre podemos elegir una subsucesión de términos consecutivos de manera que la suma de ellos es múltiplo de n.

8. Pruébese que, dados 52 números naturales cualesquiera, siempre hay dos cuya suma o cuya diferencia es múltiplo de 100.

9. Pruébese que existe al menos un número con sus cifras iguales a 1 y 3, al menos una de cada, que es múltiplo de 2021.

10. Sea a un número irracional. Pruébese que existen infinitos números racionales, $r = p/q$, tales que
$$|a - r| < \frac{1}{q^2}.$$

11. Pruébese que, dados 7 números enteros positivos menores o iguales que 126, siempre podemos encontrar dos de ellos, x, y, que satisfacen
$$1 < \frac{y}{x} \leq 2.$$

12. Tenemos un conjunto de 25 puntos en el plano de manera que, cualquiera que sean los tres que elijamos, hay dos de ellos que están a distancia menor que 1. Pruébese que existe un círculo de radio 1 que contiene al menos a 13 de dichos puntos.

13. Cada punto del plano está pintado de color rojo o de color azul. Pruébese que existen dos puntos del mismo color a distancia 1 (en realidad a una distancia arbitraria dada).

Bibliografía Adicional

1. Engel, A. (1998). The Box Principle. *Problem-Solving Strategies*. Editorial Springer, 59-84.

CAPÍTULO 4

4

POLINOMIOS

María del Pilar Benito Clavijo
Universidad de La Rioja

Palabras clave

- *Ecuación polinomial*
- *Función polinomial*
- *Raíz*
- *Algoritmo de división*
- *Regla de Ruffini*
- *Polinomio irreducible*
- *Teorema Fundamental del Álgebra*
- *Factorización*
- *Fórmulas de Cardano-Viète*
- *números de De Moivre*

Los polinomios son objetos muy útiles en la Ciencia. Permiten definir funciones polinomiales en entornos que van desde la Física y la Química hasta la Economía. Con ellos podemos aproximar otras funciones y construir estructuras denominadas "anillos" que generalizan propiedades de los números. Usados por babilonios y egipcios en problemas relacionados con ecuaciones de primer grado (papiros egipcios del año 2000 a.C.), los polinomios han captado el interés de matemáticos griegos, indios, árabes y europeos a lo largo de la historia. Nombres como Diofanto de Alejandría (s. III), Al-Juarizmi (s. IX), Ferro, Tartaglia y Cardano (s. XVI) participaron activamente en la introducción de las primeras notaciones y aritmética y en la resolución de ecuaciones polinómicas hasta grado 4 incluyendo fórmulas de cálculo de raíces. El primero en dar las reglas de las operaciones aritméticas con polinomios fue el matemático e ingeniero persa Al-Karaji (véase Figura 4.1) en el año 1000 d.C., quién investigó sobre coeficientes binomiales y la expansión $(x+y)^n$ conocida como teorema del binomio.

Figura 4.1: Abu Bakr ibn Muhammad ibn al-Husayn al-Karaji (953-1029 d.C).

4.1 Introducción

Dice el refrán que *una imagen vale más que mil palabras* para transmitir ideas, significados o esencias. Vamos a comenzar este capítulo con una figura y una pregunta que nos va a permitir introducir la noción de polinomio y sus elementos básicos. Observamos las gráficas en la Figura 4.2.

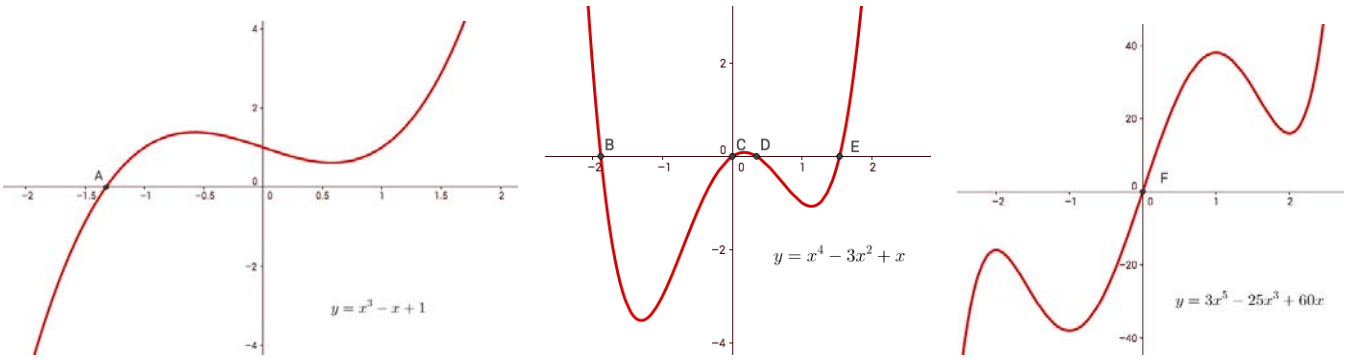


Figura 4.2: Gráficas de funciones reales de variable real.

¿Qué tienen en común las tres gráficas? Observamos que son funciones $f : \mathbb{R} \to \mathbb{R}$ de variable real que, si atendemos a la leyenda que aparece debajo de la imagen de cada una de ellas, se expresan en forma de suma en la que cada sumando contiene la variable x elevada a una cierta potencia n con n un entero positivo. Admitimos $n = 0$, declarando $x^0 = 1$. Este tipo de funciones se dicen *funciones polinomiales*.

La representación gráfica de tales funciones nos permite realizar un estudio cualitativo de las mismas, pero esta representación precisa de un estudio cuantitativo, esto es, evaluar la función en cada número real. Por ejemplo, $y = x^4 - 3x^2 + x$ nos proporciona los valores $y = 0$ para $x = 0$ e $y = -3$ si tomamos $x = -1$. En el primer caso, concluímos que la función se anula en $x = 0$, dicho de otra forma, la gráfica corta al eje de abcisas en el punto $(0, 0)$. También podemos decir que $x = 0$ es una solución de la *ecuación polinómica* (que es un caso especial de *ecuación algebraica*):

$$x^4 - 3x^2 + x = 0. \tag{4.1}$$

Esta última afirmación nos lleva a la descomposición en *factores*:

$$x^4 - 3x^2 + x = x \cdot (x^3 - 3x + 1). \tag{4.2}$$

La gráfica (b) nos informa de que hay otros tres cortes con el eje de abscisas (eje horizontal) y que denotaremos como $x = a, b, c$, que son las soluciones de la ecuación $x^3 - 3x + 1 = 0$. Esto nos lleva a la factorización:

$$p(x) = x^4 - 3x^2 + x = x \cdot (x^3 - 3x + 1) = x \cdot (x - a) \cdot (x - b) \cdot (x - c). \tag{4.3}$$

Los factores $x, x - a, x - b$ y $x - c$ no se pueden descomponer. Ahora bien, ¿podemos dar los valores exactos de a, b y c? La respuesta es afirmativa, y la podemos obtener gracias a la identidad trigonométrica $cos\, 3\alpha = 4cos^3\, \alpha - 3cos\, \alpha$, que nos permite comprobar que el número real $a = 2cos\, \dfrac{2\pi}{9}$ cumple $a^3 - 3a + 1 = 0$. Aplicando la *regla Ruffini* tenemos que $x^3 - 3x + 1 = (x - a) \cdot (x^2 + ax + a^3 - 3)$ y las otras dos soluciones, expresadas usando a, son $b, c = \dfrac{a \pm \sqrt{12 - 3a^2}}{2}$. Así, usando la aritmética de los números reales (suma y multiplicación), llegamos a la *factorización de polinomios*, muy importante en la aritmética de estos objetos.

Los contenidos que vamos a desarrollar en este capítulo tienen que ver con el carácter cuantitativo de las funciones polinomiales y la aritmética de los polinomios y las ecuaciones polinomiales.

Definición 4.1 (Polinomio y grado)

*Un **polinomio** es una suma de la forma $p(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0$, donde x se dice **variable** y $a_n, a_{n-1} \ldots, a_0$, conocidos como **coeficientes** del polinomio, son elementos de un anillo $\mathbb{A}$. Un término de la forma $a_k x^k$ se dice **monomio de grado** k. Si $a_n \neq 0$, el natural n es el **grado** de $p(x)$ y a_n se denomina **coeficiente director**. El coeficiente a_0 se llama **término independiente**. Si $a_n = 1$, diremos que $p(x)$ es un **polinomio mónico**. Los polinomios de grado cero se dicen **constantes**. Dos polinomios se dicen **iguales** si están formados por los mismos monomios, en particular, tienen el mismo grado y los mismos coeficientes.*
El conjunto todos los polinomios con coeficientes en $\mathbb{A}$, lo escribiremos en la forma $\mathbb{A}[x]$.

Nota: *Un anillo $\mathbb{A}$ es un conjunto con dos operaciones internas, llamadas suma $(a + b)$ y multiplicación (ab), y que cumplen ciertas propiedades. Aquí, a y b son elementos de $\mathbb{A}$ y las operaciones se dicen internas porque al sumar o multiplicar elementos de $\mathbb{A}$, el resultado es un elemento de $\mathbb{A}$. En este capítulo trabajaremos con polinomios con coeficientes en los anillos de enteros, racionales, reales y complejos, que denotaremos $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$ y $\mathbb{C}$ respectivamente. Los llamaremos anillos de números y a sus elementos números. En los anillos de números, la suma y el producto son conmutativos, $a + b = b + a$, $ab = ba$, y tenemos el uno, elemento neutro para el producto puesto que $1 \cdot a = a \cdot 1 = a$. Encontramos también el cero, $0 + a = a + 0 = a$, llamado elemento neutro de la suma, y el opuesto, $-a$ para cada elemento a, única solución en $\mathbb{A}$ de la ecuación $a + x = 0$. Esto permite presentar la diferencia $a - b = a + (-b)$, que es un elemento de $\mathbb{A}$ y operación válida en cualquier anillo. El conjunto $\mathbb{N}$ de números naturales está formado por los enteros positivos y el cero. Observamos que $\mathbb{N}$ no es anillo con las operaciones suma y multiplicación de números enteros ya que si calculamos la diferencia $m - n$ de dos naturales m y n y el minuendo, m, es mayor que el sustraendo, n, la diferencia está en $\mathbb{N}$, pero si el minuendo es menor, obtenemos un entero negativo, luego no está en $\mathbb{N}$. Las operaciones de $\mathbb{A}$, nos permiten sumar y multiplicar polinomios y hacen que el conjunto $\mathbb{A}[x]$ sea un anillo.*

Definición 4.2 (Ecuación polinomial, raíz y función polinomial)

*Dado un polinomio $p(x)$ de $\mathbb{A}[x]$, la expresión $p(x) = 0$ se dice **ecuación (algebraica) polinomial**. A sus soluciones, los valores de a, que pueden estar en $\mathbb{A}$ o en un conjunto que lo contenga, y tales que $p(a) = 0$, se les llama **ceros o raíces** del polinomio $p(x)$. Para un número cualquiera b, el **valor del polinomio en** b es:*

$$p(b) = a_n b^n + a_{n-1}b^{n-1} + \cdots + a_1 b + a_0. \tag{4.4}$$

*La expresión (4.4) permite asociar a $p(x)$ la función $f_{p(x)} : \mathbb{A} \to \mathbb{A}$ definida por $f_{p(x)}(b) = p(b)$ y a la que llamaremos **función polinomial** asociada al polinomio $p(x)$. De este modo, podemos interpretar los polinomios como funciones.*

Nota: *Al representar gráficamente los polinomios de grado impar con coeficientes reales observamos que todos tienen al menos una raíz real ya que son funciones continuas que toman valores negativos en $(-\infty, m)$ a partir de un cierto $m < 0$ y positivos en (m', ∞) para algún $m' > 0$. En la Figura 4.2 vemos dos polinomios de grado impar (observa el comentario previo en su gráfica) con una única raíz real y uno de grado par con todas sus raíces reales.*

Nota: *Generalizamos la expresión (4.4): dados dos polinomios $a(x)$ y $b(x)$, la expresión $a(b(x))$ representa el*

polinomio que resulta al sustituir la variable x en $a(x)$ por el polinomio $b(x)$. En anillos de números, si $a(x)$ y $b(x)$ tienen grados n y m, el grado del polinomio $a(b(x))$ es $m \cdot n$.

Ejemplo 4.1 Si $a(x) = x^2 + x + 1$, tenemos que $a(x^3) = (x^3)^2 + x^3 + 1 = x^6 + x^3 + 1$ es un polinomio de grado $6 = 2 \cdot 3$ y $a(x-1) = (x-1)^2 + (x-1) + 1 = x^2 - x + 1$ de grado 2.

El siguiente problema muestra el potencial cuantitativo de los polinomios aunque, por la forma en la que se enuncia, parece no tener relación alguna con ellos. El **truco:** encriptamos un número x_0 y, mediante operaciones básicas de sumas, productos y potencias, lo introducimos como solución de una ecuación polinomial. De este modo x_0 aparece como raíz de un cierto polinomio.

Problema 4.1 (Competition of the Mathematics Gazette, Bucharest 1943). Comprobar que siguiente igualdad entre números reales es cierta:

$$\sqrt[3]{20 + 14\sqrt{2}} + \sqrt[3]{20 - 14\sqrt{2}} = 4. \tag{4.5}$$

Solución *Si llamamos x_0 al número real que representa la expresión de la izquierda en la igualdad (4.5), $x_0 = \sqrt[3]{20 + 14\sqrt{2}} + \sqrt[3]{20 - 14\sqrt{2}}$, lo elevamos al cubo, usamos $(a+b)^3 = a^3 + 3a^2b + 3ab^2 + b^3$ y agrupamos:*

$$\begin{aligned} x_0^3 &= 20 + 14\sqrt{2} + 20 - 14\sqrt{2} + \\ &\quad 3\sqrt[3]{(20 + 14\sqrt{2})(20 - 14\sqrt{2})}(\sqrt[3]{20 + 14\sqrt{2}} + \sqrt[3]{20 - 14\sqrt{2}}) \\ &= 40 + 3x_0\sqrt[3]{400 - 392} = 40 + 6x_0. \end{aligned}$$

De este modo tenemos que x_0 es una solución de la ecuación $x^3 - 6x - 40 = 0$, equivalentemente, x_0 es una raíz real del polinomio $p(x) = x^3 - 6x - 40$. Ahora, $4^3 - 60 \cdot 4 - 40 = 0$, por tanto 4 es también una raíz real de $p(x)$. Aplicando la Regla de Ruffini, $x^3 - 6x - 40 = (x-4) \cdot (x^2 + 4x + 10)$. Las otras dos raíces de $q(x) = x^3 - 6x - 40$ son no reales, $\frac{1}{2}(-4 \pm i\sqrt{30})$. Por tanto $x_0 = 4$, lo que prueba (4.5).

4.2 Aritmética de los polinomios

En Educación Primaria aprendemos a sumar, multiplicar y dividir y a factorizar en números primos, a calcular máximo común divisor, $m.c.d.(a,b)$, y mínimo común múltiplo, $m.c.m.(a,b)$ (se usan números naturales a, b en las primeras etapas). Todas estas operaciones constituyen la aritmética de los números. Algo muy parecido sucede con los polinomios. En los primeros cursos de Educación Secundaria aprendemos a sumar, multiplicar y dividir polinomios, y también se nos enseña que la ecuación de segundo grado $ax^2 + bx + c = 0$ tiene, si el **discriminante** $\Delta = b^2 - 4ac$ es mayor o igual que cero, dos soluciones reales (una doble si $\Delta = 0$) que se expresan en la forma:

$$r_1, r_2 = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a} \tag{4.6}$$

y por tanto, $ax^2 + bx + c = a(x - r_1) \cdot (x - r_2)$. La fórmula (4.6) también es válida para calcular las raíces de polinomios de grado dos con coeficientes complejos.

Partiendo de las operaciones básicas de suma y multiplicación, las bases de la aritmética de los polinomios se encuentran en los siguientes resultados de polinomios con coeficientes en anillos de números, luego $\mathbb{A} = \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$. Los tres primeros son también válidos en anillos más generales.

Teorema 4.1 (Algoritmo de división)

Dados dos polinomios no nulos, $p(x), q(x)$, existen polinomios únicos $c(x)$ y $r(x)$ de modo que

$$p(x) = q(x) \cdot c(x) + r(x), \tag{4.7}$$

*con $r(x) = 0$ ó $\operatorname{grado} r(x) < \operatorname{grado} c(x)$ si $r(x) \neq 0$. En este caso se dice que $c(x)$ y $r(x)$ son el **cociente** y el **resto** de la división de $p(x)$ entre $q(x)$. Además, en el caso de que el resto sea nulo, se dice que $q(x)$ divide a $p(x)$, que $p(x)$ es divisible por $q(x)$, o que $q(x)$ es un **factor** de $p(x)$.*

Teorema 4.2 (Teoremas del resto y del factor)

Si $q(x) = x - a$, el resto de la división de $p(x)$ entre $q(x)$ es exactamente $p(a)$, el valor del polinomio en a. En particular, una condición necesaria y suficiente para que a sea una raíz de $p(x)$ es que $p(a) = 0$.

Nota: *La primera parte del teorema previo se conoce como **Teorema del resto**. La segunda es el **Teorema del factor** ya que, si $p(a) = 0$, el polinomio $x - a$ es un factor de $p(x)$ gracias al Algoritmo de división. La división de $p(x)$ por $x - a$ se puede realizar, y es recomendable hacerlo, usando el llamado **método de Ruffini**.*

Definición 4.3 (Polinomio irreducible)

*Si $\mathbb{A} = \mathbb{Q}, \mathbb{R}, \mathbb{C}$, un polinomio $p(x)$ de $\mathbb{A}[x]$ se dice **irreducible** o **primo** si no puede expresarse como producto de dos polinomios de $\mathbb{A}[x]$ de grados ≥ 1 y menores que el grado de $p(x)$.*

Ejemplo 4.2 Los polinomios de grado uno, $ax + b$, son irreducibles. Los de grado dos, $ax^2 + bx + c$, con coeficientes reales e irreducibles son los que cumplen $\Delta = b^2 - 4ac < 0$. En general, un polinomio $p(x)$ de grado 3 en $\mathbb{A}[x]$ de modo que la ecuación $p(x) = 0$ no tenga soluciones en $\mathbb{A}$, es irreducible y reducible en otro caso. De este modo tenemos que $x^3 - 3x + 1$ es reducible como polinomio de $\mathbb{R}[x]$ por ser de grado impar. Sin embargo, es irreducible como polinomio de $\mathbb{Q}[x]$ (ver Ejemplo 4.3).

Teorema 4.3 (Teorema de factorización única)

Todo polinomio de $\mathbb{A}[x]$ se puede expresar de manera única, salvo el orden, como producto de una constante (elemento de $\mathbb{A}$) y polinomios irreducibles y mónicos de $\mathbb{A}[x]$.

Otros resultados propios de polinomios con coeficientes en anillos de números:

Teorema 4.4 (Ceros racionales)

Sea $p(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_0$ un polinomio con coeficientes enteros y $\frac{r}{s}$ un racional expresado como fracción irreducible[a]. Si $p\left(\frac{r}{s}\right) = 0$, esto es, el número racional $\frac{r}{s}$ es raíz de $p(x)$, entonces r divide a a_0 y s divide a a_n.

[a] Dados $r, s \in \mathbb{Z}$ tales que $m.c.d.(r, s) = 1$, el número racional $\frac{r}{s}$ se dice **fracción irreducible**.

Ejemplo 4.3 El polinomio $q(x) = 3x^3 - x^2 + 3x - 1$ tiene como posibles raíces racionales $\frac{r}{s} = \pm\frac{1}{3}, \pm 1$. La única válida es $x = \frac{1}{3}$, luego $3x^3 - x^2 + 3x - 1 = (3x - 1)(x^2 + 1) = 3(x - \frac{1}{3})(x^2 + 1)$ y la segunda igualdad

es la factorización (única) de $q(x)$ en producto de irreducibles en $\mathbb{Q}[x]$ y $\mathbb{R}[x]$. El polinomio $a(x) = x^3 - 3x + 1$ no tiene raíces racionales ya que las únicas posibles son $\frac{r}{s} = \pm 1$ y al evaluar tenemos que $p(\pm 1) \neq 0$. De acuerdo con el Ejemplo 4.2, $a(x)$ es un polinomio irreducible en $\mathbb{Q}[x]$ por ser de grado 3 y no tener raíces en $\mathbb{Q}$. Sin embargo $a(x)$ tiene tres raíces reales. En efecto, como $p(0) \cdot p(1) < 0$, el **teorema de Bolzano** nos asegura que $p(x)$ tiene al menos una raíz en el intervalo $(0, 1)$. Las otras dos se localizan en los intervalos $(-2, -1)$ y $(1, 2)$ con el mismo argumento. Así tenemos el mismo polinomio $a(x)$ que es irreducible en $\mathbb{Q}[x]$ y que factoriza en $\mathbb{R}[x]$ como producto de tres irreducibles mónicos de grado uno, $a(x) = (x - r_1) \cdot (x - r_2) \cdot (x - r_1)$ con $r_i \in (-2, 2)$.

El ejemplo previo muestra que el caracter irreducible de un polinomio depende del anillo de números en el que lo estemos considerando. Los siguientes resultados explican este comportamiento.

Teorema 4.5 (Teorema Fundamental del Álgebra)

Todo polinomio no nulo $p(x)$ con coeficientes en un anillo de números $\mathbb{A}$ y de grado $n \geq 1$ tiene exactamente n raíces en el anillo de los números complejos[a]*, algunas de ellas ser iguales. Así, para el polinomio $p(x)$ podemos encontrar números complejos $r_1, \ldots, r_n$ que nos permiten facatorizarlo como producto de polinomios de grado 1:*

$$p(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_0 = a_n (x - r_1) \cdot (x - r_2) \cdot \cdots \cdot (x - r_n). \tag{4.8}$$

[a] Los números enteros, racionales y reales son números complejos en los que la parte imaginaria es nula.

Proposición 4.1 (Factorización de polinomios con coeficientes complejos)

Los polinomios irreducibles de $\mathbb{C}[x]$ son exactamente los de grado 1.

La Proposición 4.1, consecuencia inmediata del Teorema Fundamental del Álgebra y exclusivo de polinomios con coeficientes complejos se establece diciendo que $\mathbb{C}$ es un **cuerpo algebraicamente cerrado**. Como anillo de números, los complejos son un cuerpo, igual que los racionales y los reales, pero los dos últimos no son algebraicamente cerrados. En $\mathbb{Q}[x]$ podemos encontrar irreducibles de grado arbitrario y en $\mathbb{R}[x]$ de grado 1 o 2, debido a la construcción de los complejos como duplicado de los reales (i unidad imaginaria cumple $i^2 = -1$):

$$\mathbb{C} = \{a + bi : a, b \in \mathbb{R}\}. \tag{4.9}$$

Proposición 4.2 (Factorización de polinomios con coeficientes reales)

Si los coeficientes del polinomio $p(x)$ son números reales, las raíces complejas no reales aparecen de dos en dos, ya que si $a + bi$ es una raíz tal que $b \neq 0$, también lo es su conjugada, $a - bi$. El polinomio con raíces $a \pm bi$ es $x^2 - 2ax + (a^2 + b^2) = (x - (a + bi)(x - (a - bi))$. En particular, los factores irreducibles de los polinomios en $\mathbb{R}[x]$ son de grado 1 o bien de grado 2.

Nota: *Los resultados previos nos permiten concluir que todo polinomio de grado $m + s$ con m raíces reales factoriza en la forma (aquí $a_i^2 - 4b_i < 0$):*

$$p(x) = a_n (x - r_1) \cdot (x - r_2) \cdot \cdots \cdot (x - r_m) \cdot (x^2 + a_1 x + b_1) \ldots (x^2 + a_s x + b_s). \tag{4.10}$$

También nos dicen que la propiedad de que un polinomio sea o no irreducible depende fuertemente del anillo

de números con el que estemos trabajando y sus propiedades, como ilustran los Ejemplo 4.3 y Ejemplo 4.4.

Resolver ecuaciones polinomiales $p(x) = 0$ no es algo sencillo. Factorizar, en general, tampoco. Ambos problemas resultan ser interesantes. Observamos que factorizar un polinomio es el primer paso para resolver una ecuación polinomial debido a que, los anillos de números $\mathbb{A} = \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ son **anillos íntegros**, esto es, $(x, y) = (a, 0), (0, b)$ con $a, b \in \mathbb{A}$ son las únicas soluciones de la ecuación $x \cdot y = 0$. Vamos a ver un par de métodos de factorización: el **método de completar cuadrados** y el llamado **método de coeficientes indeterminados**. En lo que se refiere a las raíces, en la siguiente sección explicaremos algunas relaciones aritméticas entre ellas.

Ejemplo 4.4 (Métodos de factorización de polinomios). Factorizar, si es posible, los polinomios $x^4 + 4$ y $x^4 + 1$ ¿Son polinomios irreducibles?

Solución *Denotamos, en general,* $\mathbb{A} = \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$. *Los polinomios del enunciado no tienen ninguna raíz real puesto que* $a^4 + 4 \geq 4 > 0$ *y* $a^4 + 1 \geq 1 > 0$. *Procedemos primero con el* método de coeficientes indeterminados. *Como consecuencia del Teorema Fundamental del Álgebra, sabemos que (aquí aparecen los coeficientes* a, b, c, d *como elementos de* $\mathbb{A}$ *que hay que determinar)*

$$x^4 + 4 = (x^2 + ax + b) \cdot (x^2 + cx + d). \tag{4.11}$$

Desarrollando la parte derecha e igualando coeficientes de mismo grado en x*, obtenemos las relaciones:*

$$\begin{aligned} a + c &= 0 \\ a \cdot c + b + d &= 0 \\ ad + bc &= 0 \\ b \cdot d &= 4 \end{aligned}$$

Como el polinomio tiene coeficientes enteros, se buscan en primer lugar soluciones enteras para algunos de los coeficientes a, b, c, d. *En este caso, de* $b \cdot d = 4$*, llegamos a que* $(b, d) = (\pm 1, \pm 4), (\pm 2, \pm 2)$. *Desde* $b = d = 2$*, llegamos a que* $a = -c$ *y* $a^2 = 4$*, luego:*

$$x^4 + 4 = (x^2 + 2x + 2) \cdot (x^2 - 2x + 2) \tag{4.12}$$

es la única posibilidad de descomponer como producto de polinomios reales y la única factorización en $\mathbb{Q}[x]$ *y en* $\mathbb{Z}[x]$. *En el segundo caso, de forma análoga llegamos a las mismas ecuaciones a excepción de que* $b \cdot d = 1$*, luego* $b = d = \pm 1$ *es la única posibilidad de solución entera y, de* $b = d = 1$ *llegamos a la factorización en polinomios reales (observa que el sistema no tiene soluciones enteras, luego* $x^4 + 1$ *no se puede factorizar en* $\mathbb{Z}[x]$ *ni tampoco en* $\mathbb{Q}[x]$*):*

$$x^4 + 1 = (x^2 + \sqrt{2}x + 1) \cdot (x^2 - \sqrt{2}x + 1). \tag{4.13}$$

Además, el polinomio $x^4 + 1$ *es irreducible en* $\mathbb{Q}[x]$ *y en* $\mathbb{Z}[x]$ *ya que* $\sqrt{2}$ *no es racional, pero es reducible en* $\mathbb{R}[x]$ *y* $\mathbb{C}[x]$. *El polinomio* $x^4 + 4$ *es reducible en cualquiera de los anillos comentados. Los polinomos de grado* 2 *que aparecen en (4.12) y (4.13) son irreducibles en* $\mathbb{R}[x]$ *pero reducibles en* $\mathbb{C}[x]$.

Observamos que, completar cuadrados*, es un método mucho más simple para llegar a las factorizaciones:*

$$x^4 + 4 = (x^2 + 2)^2 - 4x^2 = (x^2 + 2x + 2) \cdot (x^2 - 2x + 2) \tag{4.14}$$

$$x^4 + 1 = (x^2 + 1)^2 - 2x^2 = (x^2 + \sqrt{2}x + 1) \cdot (x^2 - \sqrt{2}x + 1). \tag{4.15}$$

¡¡EuReKa!!, *dos líneas para factorizar completando cuadrados ¿Quién necesita conocer el método de coeficientes indeterminados?* **No hay que venirse arriba con dos simples ejemplos**. *Responde a la pregunta*

tras intentar, con las técnica de completar cuadrados, llegar a que $p(x) = x^5 + x^4 - 2x^3 + x^2 - 2x + 1 = (x^2 + x + 1)(x^3 - 3x + 1)$. *Los factores de* $p(x)$ *son irreducibles en* $\mathbb{Q}[x]$ *y en* $\mathbb{Z}[x]$. *En el Ejercicio 4.3 hemos comprobado que el segundo factor descompone en* $\mathbb{R}[x]$ *en la forma* $x^3 - 3x + 1 = (x - a) \cdot (x - b) \cdot (x - c)$, *donde* a, b *y* c *son números reales (no racionales) tales que* $-2 < a, b, c < 2$.

Nota: *Las factorizaciones de polinomios en* $\mathbb{Z}[x]$ *y* $\mathbb{Q}[x]$ *son equivalentes para polinomios* $p(x) \in \mathbb{Z}[x]$ *que sean* ***primitivos****, esto es, el máximo común divisor de sus coeficiente no nulos es igual a* 1. *La afirmación es válida apoyándonos en el llamado* ***Criterio de irreducibilidad de Gauss****, y funciona porque el anillo* $\mathbb{Q}$ *es el* ***cuerpo de fracciones*** *de* $\mathbb{Z}$. *Este argumento es el que nos permite concluir que, como el sistema previo a la factorización* (4.13) *no tiene soluciones enteras para todos los coeficientes ya que* $(a, c) = \pm(\sqrt{2}, -\sqrt{2})$, *el polinomio* $x^4 + 1$ *es irreducible como polinomio con coeficiente en* $\mathbb{Z}$ *y en* $\mathbb{Q}$. *En el caso de* $x^4 + 4$, *la factorización* (4.12) *procede de las soluciones enteras del sistema previo. El Criterio de Gauss nos garantiza en el* Ejemplo 4.4 *que, si no encontramos soluciones enteras, tampoco existen racionales. Como puedes comprobar,* **las propiedades de los anillos de coeficientes son fundamentales en cuestiones de factorización.**

Y terminamos planteando una ecuación polinomial, sin soluciones racionales (luego tampoco enteras), con tres soluciones reales y 5 complejas. Factorización y pista en el enunciado son las claves para resolverla.

Problema 4.2 Sabiendo que $cos\, 3\alpha = 4cos^3\, \alpha - 3cos\, \alpha$, resuelve la ecuación $x^5 + x^4 - 2x^3 + x^2 - 2x + 1 = 0$.
Solución *Sea* $p(x) = x^5 + x^4 - 2x^3 + x^2 - 2x + 1$. *Utilizando el método de coeficientes indeterminados, llegamos a la factorización* $p(x) = (x^2 + x + 1)(x^3 - 3x + 1)$. *Las dos raíces del primer factor son* $r_1, r_2 = \dfrac{-1 \pm i\sqrt{3}}{2}$. *Para el segundo, la identidad trigonométrica nos lleva lleva a que* $r_3 = 2cos\, \dfrac{2\pi}{9}$ *cumple* $r_3^3 - 3r_3 + 1 = 0$. *Usando el método de Ruffini, llegamos a la factorización* $x^3 - 3x + 1 = (x - r_3)(x^2 + r_3 x + r_3^2 - 3)$. *Por tanto, las otras dos soluciones son* $r_4, r_5 = \dfrac{r_3 \pm \sqrt{12 - 3r_3^2}}{2}$.

4.3 Identidades, raíces y números de De Moivre

El Teorema Fundamental del Álgebra nos permite factorizar un polinomio en la forma

$$p(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_0 = a_n (x - r_1) \cdot (x - r_2) \cdot \cdots \cdot (x - r_n). \tag{4.16}$$

Desarrollando la parte derecha e igualando coeficientes del mismo grado en x, obtenemos:

Proposición 4.3 (Fórmulas de Cardano-Viète)

Si $p(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_0$ *y* $r_1, r_2, \ldots, r_n$ *son sus raíces, entonces:*

$$\begin{aligned} r_1 + r_2 + \cdots + r_n &= -\frac{a_{n-1}}{a_n} \\ r_1 \cdot r_2 + r_1 \cdot r_2 + \cdots + r_{n-2} \cdot r_{n-1} + r_{n-2} \cdot r_n + r_{n-1} \cdot r_n &= \frac{a_{n-2}}{a_n} \\ &\cdots \\ r_1 \cdot r_2 \cdot \cdots \cdot r_n &= (-1)^n \frac{a_0}{a_n} \end{aligned}$$

Las identidades anteriores son más conocidas como **Fórmulas de Cardano** y se perfilan en 1545 (Ars Magna, Gerolamo Cardano, 1501-1576), en conexión con soluciones de la ecuación de grado 3. Franciscus Viète (1540-1603) hizo aportaciones a las soluciones de ecuaciones de grado 3 con cambios de variable, implantó las

notaciones para los datos de los problemas y se dio cuenta de la relación entre las raíces y los coeficientes de un polinomio. Estas fórmulas combinan las dos formas distintas de ver un polinomio: una como producto de factores de grado uno y otra como suma de monomios. Veamos un ejemplo de aplicación de tales expresiones y cómo usar la información obtenida para resolver un problema enunciado con identidades.

Ejemplo 4.5 Consideramos el polinomio genérico de grado tres, $p(x) = x^3 + px + q$, llamado **cúbica reducida**. Si a, b, c son las raíces de $p(x)$ (las podemos localizar en $\mathbb{C}$), tenemos que:

$$\begin{aligned} a+b+c &= 0 \\ a\cdot b + a\cdot c + b\cdot c &= p \\ a\cdot b\cdot c &= -q \end{aligned}$$

Vamos a usar las relaciones del ejemplo previo para resolver el siguiente problema. Observamos el uso de la cúbica reducida para probar una identidad.

Problema 4.3 (Chinese Mathematical Competition, 1957). Suponiendo que $a+b+c=0$, prueba la siguiente identidad

$$\frac{a^2+b^2+c^2}{2}\cdot\frac{a^5+b^5+c^5}{5} = \frac{a^7+b^7+c^7}{7}.$$

Solución *Consideramos el polinomio $p(x) = (x-a)\cdot(x-b)\cdot(x-c)$. Por las Fórmulas de Cardano-Viète, como $a+b+c=0$, tenemos que $p(x) = x^3 + px + q$ es una cúbica reducida si declaramos:*

$$a\cdot b + a\cdot c + b\cdot c = p, \quad \text{y} \quad a\cdot b\cdot c = -q.$$

Por tanto:

$$a^2+b^2+c^2 = (a+b+c)^2 - 2(a\cdot b + a\cdot c + b\cdot c) = -2p.$$

Por otro lado, como $a^3 = -p\cdot a - q, b^3 = -p\cdot b - q$ y $c^3 = -p\cdot c - q$, tenemos que

$$a^3+b^3+c^3 = -(a+b+c) - 3q = -3q$$

y de las identidades $a^4 = -p\cdot a^2 - q\cdot a$, $b^4 = -p\cdot b^2 - q\cdot b$ y $c^4 = -p\cdot c^2 - q\cdot c$, obtenemos

$$a^4+b^4+c^4 = -p(a^2+b^2+c^2) - q(a+b+c) = 2p^2.$$

De forma análoga tenemos

$$a^5+b^5+c^5 = -p(a^3+b^3+c^3) - q(^2+b^2+c^2) = 5p\cdot q, \quad \text{y}$$
$$a^7+b^7+c^7 = -p(a^5+b^5+c^5) - q(^4+b^4+c^4) = -5p^2\cdot q - 2p^2\cdot q = -7p^2\cdot q.$$

De todo lo anterior, la identidad pedida es inmediata.

El siguiente resultado permite expandir potencias en sumas y la definición posterior pone nombre y propiedades a las **raíces de la unidad**.

Teorema 4.6 (Teorema del binomio)

El desarrollo de la potencia de orden $n \geq 1$ del binomio $x+y$ viene dada por la expresión:

$$(x+y)^n = \binom{n}{0}x^n + \binom{n}{1}x^{n-1}y + \cdots + \binom{n}{n-1}xy^{n-1} + \binom{n}{n}y^n. \tag{4.17}$$

La expresión es válida al sustitutir x e y por elementos de anillos de números.

Definición 4.4 (Raíces de 1 y de -1)

Las raíces de los polinomios x^n-1 y x^n+1 se dicen ***n-raíces de*** *1 y -1 respectivamente. Las expresiones complejas de las mismas son:*

$$\alpha=\cos\frac{2\pi}{n}+i\text{sen}\,\frac{2\pi}{n},\alpha^2,\ldots,\boldsymbol{\alpha^k=\cos\frac{2k\pi}{n}+i\text{sen}\,\frac{2k\pi}{n}},\ldots,\alpha^{n-1},\alpha^n=1$$

$$\beta=\cos\frac{3\pi}{n}+i\text{sen}\,\frac{3\pi}{n},\beta^2,\ldots,\boldsymbol{\beta^k=\cos\frac{3k\pi}{n}+i\text{sen}\,\frac{3k\pi}{n}},\ldots,\beta^{n-1},\beta^n=-1.$$

Las raíces de la unidad (de orden $n\geq 1$) se dicen también ***números de De Moivre****.*

Nota: *La* ***fórmula de De Moivre****, fechada en 1707, para cualquier número real x y cualquier entero positivo k, afirma que:*

$$(\cos x+i\text{sen}\,x)^k=\cos kx+i\text{sen}\,kx. \tag{4.18}$$

Esta fórmula nos dice que que $\cos x+i\text{sen}\,x$ es una de las k-raíces del complejo $\cos kx+i\text{sen}\,kx$. Se puede obtener desde la conocida ***fórmula de Euler****, $e^{ix}=\cos x+i\text{sen}\,x$, que aparece en 1741 y nos proporciona una expresión para las n-raíces de un complejo cualquiera $z=a+bi$ usando la* ***expresión polar*** *del mismo $z=r(\cos x+i\text{sen}\,x)$ en función de su módulo $r=+\sqrt{a^2+b^2}$ y su argumento $x=\text{arctg}\,\frac{b}{a}$. Las expresiones de tales raíces son:*

$$\alpha_k=\sqrt[n]{r}(\cos\frac{x+2k\pi}{n}+i\text{sen}\,\frac{x+2k\pi}{n}),k=0,\ldots,n-1. \tag{4.19}$$

Ejemplo 4.6 Tenemos que $x^3-1=(x-1)(x^2+x+1)=(x-1)(x-\alpha)(x-\alpha^2)$ con $\alpha=\frac{-1+i\sqrt{3}}{2}$ y $x^4+1=(x-\beta)(x-\beta^2)(x-\beta^3)(x-\beta^4)$ donde $\beta=\frac{-\sqrt{2}+i\sqrt{2}}{2}$. Aquí,

$$\alpha=\cos\frac{2\pi}{3}+i\text{sen}\,\frac{2\pi}{3}\quad\text{y}\quad\beta=\cos\frac{3\pi}{2}+i\text{sen}\,\frac{3\pi}{2} \tag{4.20}$$

Además, como $x^4+1=(x^2+\sqrt{2}x+1)\cdot(x^2-\sqrt{2}x+1)$, β y β^7 son las raíces del factor $x^2+\sqrt{2}x+1$. Por otro lado, si $\gamma=\cos\frac{2\pi}{6}+i\text{sen}\,\frac{2\pi}{6}=\frac{1+i\sqrt{3}}{2}$, tenemos que $\gamma^2=\alpha$ y, desde $x^6-1=(x^3-1)(x^3+1)$, $\gamma^3=-1$ y $\gamma^4=\alpha^2$, concluímos que $x^3+1=(x-\gamma)(x-\gamma^3)(x-\gamma^5)$.

Nota: *Observa que para cualquier complejo z, si b y c satisfacen la identidad $b^n=z$ y $c^n=-z$, las raíces x^n-z son $b\alpha^k$ $(k=0,\ldots,n-1)$ y $c\beta^k$ $(k=0,\ldots,n-1)$ las de x^n+z, donde α y β son los números complejos descritos en* Definición 4.4.

Proposición 4.4

Geométricamente, las n-raíces de la unidad son números complejos $a+ib$ que se localizan com pares $(a,b)\in\mathbb{R}^2$ en el círculo unitario del plano real. En este plano, las n-raíces forman los vértices de un polígono regular de n lados (n-gon) con cen centro en el origen de coordenadas, $O(0,0)\in\mathbb{R}^2$, y un vértice en el punto $P(1,0)\in\mathbb{R}^2$ para todo $n\geq 3$.

Ejemplo 4.7 (Otras identidades). Si la suma $x+y$ representa al binomio $x+1$ ó $x-1$, usando el Teorema 4.6 llegamos a

[F-1.6.1] $(x+1)^n=\binom{n}{0}x^n+\binom{n}{1}x^{n-1}+\cdots+\binom{n}{n-1}x+\binom{n}{n}$,

y sus generalizaciones que se obtienen aplicando la fórmula [F-1.6.1] previa con el cambio $y = \frac{x}{a}$:

$$(x+a)^n = a^n(\frac{x}{a}+1)^n = a^n(y+1)^n \tag{4.21}$$

[F-1.6.2] $\frac{x^n-1}{x-1} = x^{n-1} + \ldots x^{n-2} + \cdots + x + 1,$

y sus generalizaciones cambiando $y = \frac{x}{a}$ y aplicando la fórmula [F-1.6.2]:

$$\frac{x^n - a^n}{x-a} = a^{n-1}\frac{y^n-1}{y-1} \tag{4.22}$$

[F-1.6.3] Para n impar, $\frac{x^n+1}{x+1} = x^{n-1} - x^{n-2} + \cdots - x + 1,$

y sus generalizaciones aplicando la fórmula [F-1.6.3] y cambiando $y = \frac{x}{a}$:

$$\frac{x^n + a^n}{x+a} = a^{n-1}\frac{y^n+1}{y+1}. \tag{4.23}$$

[F-1.6.4] Para n par, $\frac{x^n-1}{x+1} = x^{n-1} - x^{n-2} + \cdots + x - 1,$

y sus generalizaciones aplicando la fórmula [F-1.6.4] con el cambio con $y = \frac{x}{a}$:

$$\frac{x^n + a^n}{x+a} = a^{n-1}\frac{y^n+1}{y+1}. \tag{4.24}$$

4.4 Problemas resueltos

Terminamos la sección con algunos problemas modelo que usan las identidades y técnicas derivadas de la aritmética de polinomios que hemos presentado en las secciones previas.

Problema 4.4 Si $\alpha^5 = 1$, calcula $\alpha + \frac{1}{\alpha}$. Deduce de la información previa el valor de $\cos 72°$.

Solución *Sea* $a = \alpha + \frac{1}{\alpha}$. *Tenemos que* α *es raíz de* $p(x) = x^5 - 1 = (x-1)(x^4+x^3+x^2+x+1)$. *Si* $\alpha = 1$, *entonces* $a = 2$. *En otro caso,* $\alpha^4 + \alpha^3 + \alpha^2 + \alpha + 1 = 0$. *Dividimos la ecuación entre* α^2, *arreglamos y llegamos a:*

$$\alpha^2 + \alpha + 1 + \frac{1}{\alpha} + \frac{1}{\alpha^2} = 0 = (\alpha + \frac{1}{\alpha})^2 + (\alpha + \frac{1}{\alpha}) - 1 = a^2 + a - 1. \tag{4.25}$$

Esto nos proporciana las soluciones $a = \frac{\pm\sqrt{5}-1}{2}$. *Finalmente,* $\cos 72° = \cos\frac{2\pi}{5}$. *Tomamos la* 5*-raíz* $\alpha = \cos\frac{2\pi}{5} + i\text{sen}\,\frac{2\pi}{5}$ *y observamos que* $\alpha^4 = \frac{1}{\alpha} = \cos\frac{2\pi}{5} - i\text{sen}\,\frac{2\pi}{5}$ *(*$\alpha \cdot \alpha^4 = 1$*). De este modo* $\cos 72° = \frac{1}{2}(\alpha + \frac{1}{\alpha}) = \frac{\sqrt{5}-1}{4}$ *por ser un número real positivo.*

Problema 4.5 Encontrar todos los números primos de la forma $n^4 + 4$.

Nota: *Un natural* $n \in \mathbb{N}$ *se dice primo si las soluciones de la ecuación* $p = a \cdot b$ *en* $\mathbb{N}$ *son* $(a,b) = (1,p), (p,1)$.

Solución *Como* $n^4 + 4 = (n^2+2n+2)(n^2-2n+2)$, *para que un número de esta forma sea primo tiene que ocurrrir que* $n^2 + 2n + 2 = 1$, *luego* $0 = n^2 + 2n + 1 = (n+1)^2$ *o que* $n^2 - 2n + 2 = 1$ *luego* $0 = n^2 - 2n + 1 = (n-1)^2$. *Las demás posibilidades dan números compuestos. Por tanto* $n = \pm 1$ *y el único primo de esta forma es* $p = 5$.

Problema 4.6 Encontrar el resto de la división de $p(x^5)$ entre $p(x)$ donde $p(x) = x^4 + x^3 + x^2 + x + 1$.

Solución *Observamos que* $x^5-1=(x-1)(x^4+x^3+x^2+x+1)=(x-1)p(x)$*, luego las raíces de* $p(x)$ *son las* 5*-raíces de 1 distintas de* 1.

$$p(x^5)=x^{20}+x^{15}+x^{10}+x^5+1=(x^{20}-1)+(x^{15}-1)+(x^{10}-1)+(x^5-1)+5$$

Ahora

$$\begin{aligned}x^{20}-1&=(x^5)^4-1=(x^5-1)(x^{15}+x^{10}+x^5+1)\\x^{15}-1&=(x^5)^3-1=(x^5-1)(x^{10}+x^5+1)\\x^{10}-1&=(x^5)^2-1=(x^5-1)(x^5+1)\end{aligned}$$

lo que nos dice que el resto de la división es 5 *ya que* $p(x)=(x^5-1)(x^{15}+2x^{10}+3x^5+4)+5$.

Problema 4.7 Si $p(x)$ es un polinomio con coeficientes enteros, entonces el entero $p(b)-p(a)$ es divisible por $b-a$ para cualquier par de enteros a,b.

Solución *Usando el Algoritmo de la División y el Teorema del resto tenemos que* $p(x)=(x-a)\cdot c(x)+p(a)$*. Evaluamos esta expresión en* $x=b$ *y obtenemos la igualdad de enteros* $p(b)=(b-a)p(b)+p(a)$*, que la podemos escribir en la forma* $p(b)-p(a)=(b-a)p(b)$*, lo que prueba el resultado.*

Problema 4.8 Sea $p(x)$ un polinomio con coeficientes enteros tal que la ecuación $p(x)=7$ tiene al menos cuatro soluciones enteras. Demostrar que la ecuación $p(x)=14$ no tiene soluciones enteras.

Solución *Llamamos* r_1,r_2,r_3 *y* r_4 *a las soluciones enteras de la ecuación* $p(x)=7$*, luego* $p(r_i)=7$*, y suponemos que hay otro entero* c *de modo que* $p(c)=14$*. El polinomio* $q(x)=p(x+c)-7$ *tiene coeficientes enteros y* r_i-c *para* $i=1,2,3,4$ *son cuatro de sus raíces y* $q(0)=7$*. Usamos la información del Problema 7 con los enteros* $b=r_i-c$ *y* $a=0$ *y tenemos que cada entero* r_i-c *divide a* $q(r_i-c)-q(0)=-7$*. Como los únicos divisores enteros de* -7 *son* $\{\pm1,\pm7\}$ *y* r_i-c *proporcionan cuatro enteros distintos, la única posibilidad es que las cuatro raíces* r_i-c *sean* $\pm1,\pm7$*. Usamos el Algoritmo de la división y el Teorema del resto (cuatro veces) en* $\mathbb{Z}[x]$ *y llegamos a que existe un polinomio* $c(x)$ *con coeficientes enteros de modo que:*

$$q(x)=(x-1)\cdot(x+1)\cdot(x-7)\cdot(x+7)\cdot c(x) \tag{4.26}$$

Sustituimos $x=0$ *en la ecuación (4.26) y tenemos* $7=q(0)=49\cdot c(0)$*, lo cual no es posible. Por tanto el entero* c *no puede existir, lo que prueba el enunciado por reducción al absurdo.*

Problema 4.9 ¿Para qué valores $n\in\mathbb{N}$ el polinomio $p(x)$ es un factor de $x^{2n}+x^n+1$?

Solución *Observamos que* $x^r-1=(x-1)\cdot(x^{r-1}+x^{r-2}+\cdots+x+1)$*. Si evaluamos* x *en* x^3 *en la igualdad previa, tenemos que:*

$$x^{3r}-1=(x^3)^r-1=(x^3-1)\cdot(x^{3(r-1)}+x^{3(r-2)}+\cdots+x^3+1). \tag{4.27}$$

Por tanto $x^3-1=(x-1)(x^2+x+1)$ *es un factor de* $x^{3r}-1$ *para todo* $r\in\mathbb{N}$*, y* x^2+x+1 *también lo es . Observamos que cualquier natural* n *es de la forma* $3r,3r+1$ *'o* $3r+2$*. Así, si* $n=3r$*, tenemos que* $x^{6r}+x^{3r}+1=(x^{6r}-1)+(x^{3r}-1)+3=(x^2+x+1)q(x)+3$*. Por unicidad de cociente y resto en el algoritmo de división,* x^2+x+1 *no es factor* $x^{6r}+x^{3r}+1$ *pues el resto de la división es* $3\neq0$*. En el caso* $n=3r+1$*,*

$$x^{6r+2}+x^{3r+1}+1=x^2(x^{6r}-1)+x(x^{3r}-1)+(x^2+x+1)=(x^2+x+1)s(x). \tag{4.28}$$

Luego x^2+x+1 *es factor si* $n=3r+1$*. Finalmente, en el caso* $n=3r+2$ *también llegamos a que* x^2+x+1 *es factor:*

$$\begin{aligned}&x^{6r+4}+x^{3r+2}+1=x^4(x^{6r}-1)+x^2(x^{3r}-1)+(x^4+x^2+1)=\\&x^4(x^{6r}-1)+x^2(x^{3r}-1)+x(x^3-1)=(x^2+x+1)t(x).\end{aligned}$$

Problema 4.10 (United States of American Mathematical Olympiad, 1975). Si $p(x)$ es un polinomio de grado n tal que $p(k) = \dfrac{k}{k+1}$ para $0 \leq k \leq n$, calcula $p(n+1)$.

Solución *El valor de $p(k)$ nos dice que el polinomio $(x+1)p(x) - x$ tiene como raíces $0, 1, \ldots n$, luego factoriza en la forma:*

$$(x+1)p(x) - x = a \cdot x \cdot (x-1) \cdot \cdots \cdot (x-n). \tag{4.29}$$

En (4.29), sutituímos $x = -1$ y obtenemos que $1 = a(-1)^{n+1}(n+1)!$ y que

$$p(x) = \frac{(-1)^{n+1}x \cdot (x-1)\ldots(x-n)/(n+1)! + x}{x+1}. \tag{4.30}$$

De $x = n+1$ en (4.30) concluímos que $p(n+1) = 1$ si n es impar y $p(n+1) = \dfrac{n}{n+2}$ si n es par.

Por último, a modo de curiosidad histórica, en el Cuadro 4.1 se puede observar el lenguaje escrito empleado por Al-Karaji para referirse a las diversas potencias para un variable desconocida, así como para sus respectivos inversos. Por ejemplo, vemos que Al-Karaji denota por "cosa" (en inglés "thing") a la variable independiente x, mientras que utiliza el vocablo "parte-cosa" (en inglés "part-thing") para referirse a la inversa de x, esto es, a la expresión x^{-1}.

Al-Karaji (1000 d.C.)	Actual	Al-Karaji (1000 d.C.)	Actual
cube-cube	x^6	part-cube-cube	$x^{-6} = 1/x^6$
square-cube	x^5	part-square-cube	$x^{-5} = 1/x^5$
square-square	x^4	part-square-square	$x^{-4} = 1/x^4$
cube	x^3	part-cube	$x^{-3} = 1/x^3$
thing	x^1	part-thing	$x^{-1} = 1/x$
unit	1	-	-

Cuadro 4.1: Notación para polinomios adoptada por Al-Karaji (1000 d.C.).

Ejercicios Propuestos

1. Calcula el valor de la suma de los cuadrados de las tres raíces del polinomio $x^3 + 3x^2 - 7x + 1$.

2. Calcula todos los polinomios con coeficientes reales tales que $xp(x-1) = (x+1)p(x)$.
   Pista: Usa $q(x) = (x+1)p(x)$ y su relación con la ecuación dada.

3. Calcula las soluciones reales de la ecuación $\sqrt[4]{97 - x} + \sqrt[4]{x} = 5$.
   Pista: Llama $a = \sqrt[4]{97 - x}$ y $b = \sqrt[4]{x}$ y manipula la ecuación.

4. Sean α, β raíces del polinomio $x^2 - 6x + 1$. Si $r_n := \alpha^n + \beta^n$, prueba que $n \geq 2$, $r_n = 6r_{n-1} - r_{n-2}$ y que r_n es un número entero no divisible por 5 para todo $n \geq 0$.
   Pista: Juega con la recurrencia del enunciado y las Fórmulas de Cardano-Viète.

5. Dado el polinomio $p(x) = x^4 + \square x^3 + \square x^2 + \square x + \square$, en el que cada cuadrado $\square$ representa un hueco donde se colocar un coeficiente, se plantea el siguiente juego entre dos jugadores: Alternativamente, el primer y el segundo jugador eligen un hueco vacío y colocan en él un entero no nulo hasta rellenar los cuatro huecos. Si el polinomio resultante tiene al menos dos raíces enteras gana el segundo jugador, en otro caso el ganador es el primero. Prueba que, eligiendo la estrategia adecuada, el primer jugador siempre puede ganar. (Fase local de la XLVI Olimpiada Matemática Espa ñola, Alicante 2010.)

6. * Encuentra los pares de polinomios $(a(x), b(x))$ con coeficientes reales tales que su composición, $a(b(x))$, de como resultado un polinomio que factoriza en la forma $a(b(x)) = b(x)x^2$. (South Africa MO 2013, Problema 4)

7. * Si $p(x)$, $q(x)$, $r(x)$ y $s(x)$ son polinomios tales que
$$p(x^5) + xq(x^5) + x^2 r(x^5) = (1 + x + x^2 + x^3 + x^4)s(x),$$
   demostrar que $p(x)$ es divisible entre $x - 1$. (United States of American Mathematical Olympiad, 1976)
   Pista: Evalúa la ecuación dada en las 5-raíces de uno $\alpha, \alpha^2, \alpha^3, \alpha^4$ que son distintas de 1 observando que la parte derecha se anula.

Nota: *Los ejercicios con * son de mayor grado de dificultad. Bien por desarrollo elaborado (Ejercicio 6) o porque requieren de una idea feliz (Ejercicio 7).*

Bibliografía Adicional

1. Engel, A. (1998). Polynomials. *Problem-Solving Strategies*. Editorial Springer, 245-270.
2. Lehmann, C. H. (2004). *Álgebra*. Editoral Limusa.
3. Swokowski, E. W. & Cole, J. A. (2009). *Álgebra y trigonometría con geometría analítica*. Editorial Cengage Learning.

CAPÍTULO 5

5 TEORÍA DE GRAFOS

Patricia Pascual Ortigosa
Universidad de La Rioja

Palabras clave

- *Grafo*
- *Grafo dirigido*
- *Grafo de Euler*
- *Grafo de Hamilton*
- *Grafos coloreables*

La Teoría de Grafos es una rama de las Matemáticas que comenzó a desarrollarse hace más de tres siglos y, desde sus inicios, ha ido mostrando su amplio abanico de utilidades.

Un grafo no es más que un conjunto de puntos (vértices) y líneas que los unen (aristas) que nos pueden ayudar desde saber si podemos recorrer todos los puentes de una ciudad sin repetir ninguno hasta optimizar la ruta de un autobús en una ciudad.

En este capítulo haremos un breve repaso del inicio de la Teoría de Grafos y daremos conceptos clave que nos serán de gran ayuda para poder resolver ejercicios de Olimpiadas Matemáticas.

5.1 Introducción

La Teoría de Grafos tiene su origen en una ciudad llamada Kaliningrado (véase Figura 5.1), anexionada a Rusia en el año 1945. La ciudad de Kaliningrado se encuentra en la desembocadura del río Pregel y, antiguamente, era conocida por el nombre de Königsberg. Una imagen de la antigua ciudad de Königsberg se puede ver en la Figura 5.2.

Figura 5.1: Ciudad de Kaliningrado.

Figura 5.2: Ciudad de Königsberg.

Quizá, a quién esté leyendo esto, la ciudad de Königsberg le resulte familiar o crea que ha escuchado ese nombre en algún sitio... ¡y es más que probable! La Teoría de Grafos tiene su origen en Königsberg. Vamos a ver cómo surgió. Si os fijáis en el centro de la ciudad de Königsberg -Figura 5.3-, podéis observar que hay cuatro regiones separadas por el río Pregel. Cada una de ellas está conectada con las otras a través de puentes. En concreto, hay siete. Así, los ciudadanos de Königsberg se plantearon la siguiente pregunta: *¿Es posible dar un paseo de forma que, comenzando en cualquiera de las regiones y pasando una única vez por cada puente, regresemos a la región de partida?*

Quizá la persona que esté leyendo esto piense: "¡Qué fácil! Hago todas las posibles opciones que hay y seré capaz de responder la pregunta". Querido lector, para aquí un momento. Coge papel y boli. Pon tu cerebro a pleno funcionamiento y trata de pensar una solución a este problema. ¿Ya lo has hecho? ¡Pues continuemos! Puede que hayáis usado la *fuerza bruta* para resolver el problema (está bien no quedarnos parados si no se nos ocurre otra forma de resolverlo), puede que se os haya ocurrido otra forma de resolverlo (si es así, me encantaría ver la forma que se os ha ocurrido) o puede que no se os haya ocurrido nada -a los que no hayáis encontrado la respuesta, lo siento por el *spoiler*, pero todos tendríais que haber llegado a la misma respuesta: no es posible dar dicho paseo por el centro de Königsberg.

Llegados a este punto, querido lector, te estarás preguntando qué tiene que ver todo esto con las matemáticas. Me has hablado de Königsberg, me has hablado de unos puentes y de un paseo pero, y la Teoría de Grafos, ¿dónde está? Allá vamos.

El matemático Leonhard Euler (1707 – 1783) fue el encargado de encontrar las matemáticas en este problema... ¡y de iniciar una teoría! La Teoría de Grafos. La solución planteada por Euler en su trabajo *Los siete puentes de Königsberg* (1736) fue general. Es decir, no servía únicamente para el caso particular de la ciudad de Königsberg, si no que se podía utilizar para cualquier región parecida. Y, ¿qué es lo que se le ocurrió? ¡Vamos a verlo!

Euler realizó una abstracción del mapa: cada región del mapa, la representó por un punto y, cada puente entre las regiones (puntos, en la abstracción) lo representó con una línea que unía dichas regiones.

De nuevo, para un momento. Coge papel y boli. Trata de realizar la abstracción del mapa de la Figura 5.3 con la información que tienes. Piénsalo un poco. No te rindas a la primera. ¿Ya? Si no se te ha ocurrido cómo hacer la abstracción, no te preocupes. Lo importante es intentarlo. Trata de seguir pensándolo conforme va avanzando la explicación de cómo hacerlo. Si has sido capaz de hacerlo, vamos a comprobar si hemos llegado al mismo resultado.

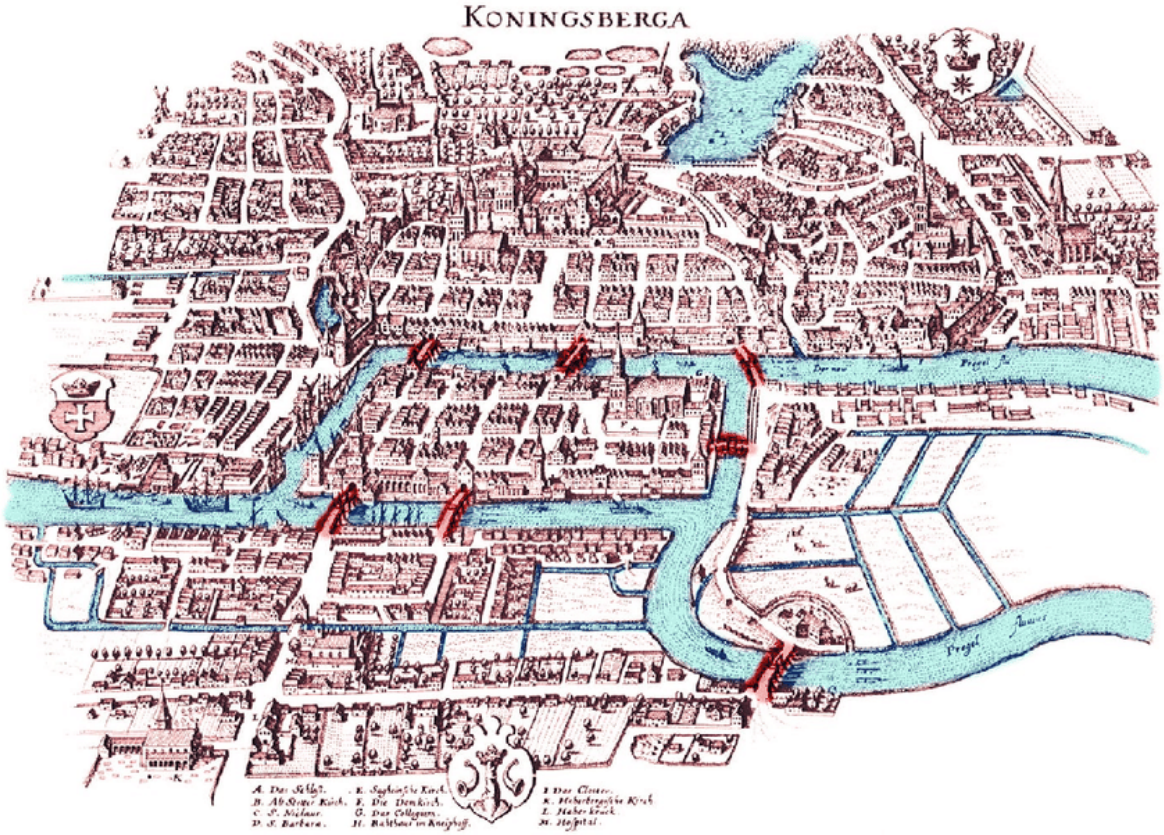


Figura 5.3: Centro de la ciudad de Königsberg.

Vamos a trabajar, como hemos dicho anteriormente, con la Figura 5.3. Si nos fijamos bien, el centro de Königsberg cuenta con cuatro regiones (la región superior, la región inferior, la región central - que parece una "isla"- y la región de la derecha). Por cada una de las regiones, dibujaremos un punto. Cuatro regiones, cuatro puntos. Bien. Vamos ahora a ver qué pasa con los puentes. Tenemos lo siguiente:

- La región superior está unida con la región central (y viceversa) por dos puentes. Es decir, el punto que representa a la región superior y el punto que representa a la parte central estarán conectados por dos líneas.
- La región superior está comunicada con la región derecha por un puente. Por lo tanto, los puntos que representan a la región superior y la región derecha estarán unidos por una línea.
- La región central está comunicada con la región inferior por dos puentes. En nuestra abstracción del mapa, los puntos que representan a la parte central y a la parte inferior estarán conectados con dos líneas.
- La región central y la región derecha están counicadas por un puente, por lo que el punto que representa a la región central estará unido con una línea al punto representando a la región derecha.
- Por último, el punto que representa a la región derecha y el punto que representa a la región inferior estarán conectados por una línea puesto que las regiones están comunicadas por un único puente.

Este proceso de abstracción del mapa queda resumido en la Figura 5.4 que, para el que no lo haya adivinado todavía, es un *grafo*.

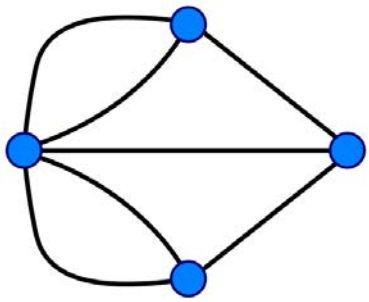


Figura 5.4: Grafo asociado al centro de la ciudad de Königsberg.

Espero que todos hayáis llegado a este grafo. De nuevo, os voy a pedir que os toméis un momento para ver si se os ocurre, mirando el grafo que hemos obtenido, la respuesta para la pregunta *¿Es posible dar un paseo de forma que, comenzando en cualquiera de las regiones y pasando una única vez por cada puente, regresemos a la región de partida?* Poned un temporizador de cinco minutos. Tratad de pensar, nuevamente, qué podéis hacer. Cinco, cuatro, tres, dos, uno... ¡volvemos! El razonamiento que vamos a hacer ahora va a ser un poco más completo de lo que necesitamos para responder la pregunta.

Vamos a responder a la pregunta sin tener en cuenta que la región inicial y final son la misma. Observad que, si llegamos a una región, la única forma de salir de ella es por otra línea diferente porque, recordad que solo podíamos recorrer los puentes una vez. Por lo tanto, las regiones deben tener un número par de líneas: una para entrar y otra para salir. Pero... ¿en todas las regiones ocurre esto? Tomaos un minuto para pensar si esto es así. Seguramente os hayáis percatado de que las regiones inicial y final pueden tener un número impar de aristas entrando/saliendo de ellas. Esto es así puesto que en estas regiones podríamos salir, volver a entrar y salir de nuevo. O, en la inicial, podríamos salir y no volver a ella, resultando un número impar de aristas y pasando por el puente una única vez. Usando el mismo razonamiento, a la región final podríamos entrar y no volver a salir, teniendo esta un único puente de entrada. Es decir, *para poder pasar por todos los puentes una única vez, sería necesario un grafo en el que todos los vértices tengan un número par de aristas entrando o saliendo de ellos, salvo en los vértices inicial y final*. En el caso de la pregunta que hemos planteado nosotros, hay una pequeña diferencia: la región de inicio tiene que ser la misma que la de llegada. Por lo tanto, la región de inicio/final también debe de tener un número par de aristas. Así, *para poder pasar por todos los puentes una única vez y que la región inicial sea la misma que la final, necesitaríamos un grafo en el que todos los vértices tengan un número par de aristas entrando o saliendo de ellos*.

Centrándonos de nuevo en nuestro problema inicial, podemos observar que todos los vértices del grafo de la Figura 5.4 tienen un número impar de aristas entrando o saliendo de él. Teniendo en cuenta el razonamiento que hemos hecho en el párrafo anterior, la respuesta es que *no es posible dar un paseo de forma que, comenzando en cualquiera de las regiones, pasar una única vez por cada puente y regresar a la región de partida*.

Ejemplo 5.1 Mi casa y la de mis amigos están comunicadas de la siguiente forma:

- Desde mi casa, puedo ir a casa de Juanmi cruzando un puente por encima de las vías del tren o también puedo ir a casa de Dani, cruzando un puente que hay sobre el río.
- Desde casa de Juanmi se puede venir a mi casa cruzando el puente de las vías; también se puede ir a casa de Jorge, cruzando el puente por encima del río; y a casa de Judit, cruzando las vías del tren.

- Desde la casa de Jorge, se puede ir a la casa de Juanmi o a la casa de Judit a la que podemos ir cruzando un puente por encima de la vía o un puente por debajo.
- Desde casa de Ángela, se puede ir a casa de toda la cuadrilla menos a la mía.
- Desde la casa de Dani, se puede ir a mi casa o a la de Judit.

Un día, reunidos toda la cuadrilla de amigos, surgió la duda de si era posible que, saliendo de cualquiera de las casas, fuera posible recorrer todas las conexiones que hay entre ellas y volver a llegar a la casa desde la que habíamos salido. Dani dice que da igual quién sea el que comience la ronda, que nunca será posible pasar por todos los puentes y túneles una única vez y regresar al punto de partida. Jorge, por su parte, dice que seguro que desde una de las casas podremos hacerlo. Estoy indecisa y no sé a quién darle la razón. ¿Me ayudáis a pensarlo?

Lo primero que vamos a hacer va a ser una abstracción de las conexiones que hay entre las casas. Es decir, vamos a dibujar el grafo asociado. Tomaos vuestro tiempo. Releed de nuevo la introducción si es necesaria. Tratad de hacerlo sin mirar. ¿Ya lo habéis intentado? ¡Pues continuamos!

El grafo asociado a las conexiones entre las casas de mis amigos se puede ver en la Figura 5.5.

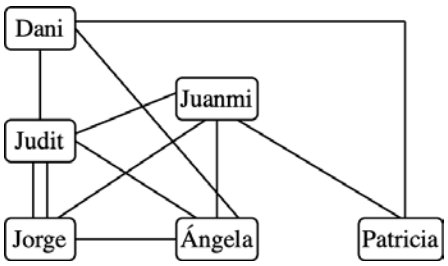


Figura 5.5: Grafo asociado a las conexiones entre las casas de mis amigos.

Observando el grafo, y gracias al razonamiento que hemos hecho antes, tenemos que darle la razón a Dani: como, por ejemplo, la casa de Dani tiene tres salidas/entradas, no va a ser posible recorrer todas y cada una de las conexiones que existen entre nuestras casas y volver al punto inicial. ¡Gracias por ayudarme a resolverlo!

5.2 Conceptos clave

Una vez que hemos puesto en contexto cómo nació la Teoría de Grafos, toca ponerse un poco técnico y dar definiciones y conceptos clave de manera rigurosa. Que no os asuste ese *palabro* que acabáis de leer. Riguroso quiere decir preciso. Y, en matemáticas, tenemos que ser precisos.

Como os digo, esta sección va a contener mucha información y toda ella relevante a la hora de resolver los problemas de las Olimpiadas Matemáticas. Aunque las definiciones puedan parecer demasiado largas y complejas, leedlas con atención. Tratad de entenderlas. Escribid con vuestras palabras lo que creéis que significa. Si no las entendéis, hay muchos ejemplos que van a hacer que la definición cobre sentido. Pero no os quedéis solo con mirar los ejemplos. Cuando hayáis entendido el ejemplo, mirad de nuevo las definiciones y comprobad que la entendéis. Dedicadle un ratito a cada definición y cada ejemplo, valdrá la pena. Y, una vez dicho esto... ¿estáis preparados para empezar? ¡Vamos allá!

Ya hemos visto en la introducción la idea de *grafo*. Pero... ¿cómo definimos un grafo de manera precisa? En la siguiente definición encontrarás la respuesta:

Definición 5.1 (Grafo simple)

Un grafo simple *es un par* $G = (V(G), E(G))$ *donde* $V(G)$ *y* $E(G)$ *son conjuntos finitos. El conjunto* $V(G)$ *se denomina* conjunto de vértices *y el conjunto* $E(G)$ *se denomina conjunto de aristas.*
Cada elemento $e \in E(G)$ *es de la forma* $\{u, v\}$*, donde* $u, v \in V(G)$*. En este caso decimos que* u *y* v *son* vértices adyacentes.

En el siguiente ejemplo tienes un grafo *desgranado*: puedes ver cómo lo definimos y cuál es su conjunto de vértices y aristas. Si has entendido la definición a la primera, te diré dos cosas: la primera, ¡enhorabuena! Entender definiciones matemáticas fácilmente es bastante complicado; la segunda, coge papel y lápiz y trata de escribir el grafo de la Figura 5.6 tú solo y, después, comprueba que lo has hecho bien. Si no has entendido la definición, también te diré dos cosas: la primera, no desesperes, hacerse a la *jerga* matemática no es fácil; la segunda es que mires el ejemplo con detenimiento, lo entiendas y, después, vuelvas a leer la definición, ¡seguro que ahora la entiendes!

Ejemplo 5.2 Dado el grafo $G = (V(G), E(G))$ de la Figura 5.6 tenemos que el conjunto de vértices viene dado por $V(G) = \{v_1, v_2, v_3, v_4, v_5\}$. El conjunto de aristas, por su parte, viene dado por

$$E(G) = \{\{v_1, v_2\}, \{v_2, v_3\}, \{v_3, v_4\}, \{v_4, v_5\}, \{v_4, v_6\}\}.$$

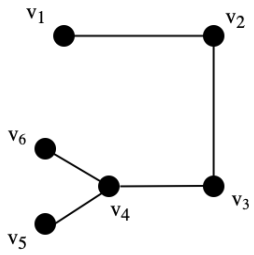


Figura 5.6: Grafo del Ejemplo 5.2.

Fijaos que, los vértices v_1 y v_2 son adyacentes, mientras que los vértices v_1 y v_3 no lo son. Queda como pequeño problema para el lector encontrar todos los vértices que son adyacentes y todos los que no lo son.

Vamos ahora a introducir una nueva definición. La definición de *grado* de un vértice.

Definición 5.2 (Grado)

Un vértice de un grafo tiene grado m *si de dicho vértice está conectado con* m *aristas.*

Ejemplo 5.3 (Continuación del Ejemplo 4.2). Los grados de los vértices del grafo del Ejemplo 5.2 son $\text{gr}(v_1) = 1$, $\text{gr}(v_2) = 2$, $\text{gr}(v_3) = 2$, $\text{gr}(v_4) = 3$, $\text{gr}(v_5) = 1$ y $\text{gr}(v_6) = 1$.

En el apartado anterior hemos presentado definiciones básicas en la Teoría de Grafos. Seguro que, alguno de vosotros se ha preguntado si, dado un grafo, la arista $\{u, v\}$ es la misma que la $\{v, u\}$. O si hay casos en las que es diferente. O si es posible que las distingamos. Pues allá vamos con las respuestas a todas estas preguntas:

Definición 5.3 (Grafo dirigido)

Un grafo dirigido *o* digrafo *es aquel en el que* $\{u, v\} \neq \{v, u\}$.

Leyendo esta definición os preguntaréis cómo se puede saber, viendo un grafo, si un grafo es dirigido o

no. Los grafos dirigidos se caracterizan porque tienen pintadas, sobre sus aristas, flechas. De esta forma, la flecha apunta hacia el final de la arista. Es decir, si tenemos la arista de la Figura 5.7, esto significa que la arista $\{v_1, v_2\}$ está en el conjunto de aristas mientras que la arista $\{v_2, v_1\}$ no está en el grafo.

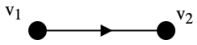


Figura 5.7: Arista dirigida de v_1 a v_2.

A continuación, vamos a hablar sobre *caminos, recorridos y ciclos*. *¿Cómo conectamos un vértice con otro? ¿Qué pasa si para ir de un vértice a otro repito aristas? ¿Y si repito vértices?* Seguro que os han surgido preguntas así. Pero de lo que estoy completamente segura es de que, cuando habéis leído *caminos, recorridos y ciclos* os habréis preguntado qué diferencia hay entre ellos. ¡Cojan papel y boli y hagan sus apuestas! En serio, coge papel y boli y dale una vuelta a que puede ser cada cosa. ¿Qué diferenciará a un camino de un recorrido? ¿Y a un recorrido de un ciclo? ¿Serán lo mismo y estoy tratando de engañaros? ¡Qué misterio! Vamos a resolverlo.

Definición 5.4 (Camino)
Un camino de longitud n *es una secuencia de* n *vértices de forma que entre un vértice y el siguiente siempre existe un arista que los une.*

Ejemplo 5.4 Dado el grafo del Ejemplo 5.2 tenemos que $\{v_1, v_2, v_3\}$ es un camino de longitud 3 y que $\{v_1, v_2, v_3, v_4, v_6, v_4, v_5\}$ es un camino de longitud 7.

Definición 5.5 (Recorrido)
Un recorrido *es un camino en el que no existen aristas repetidas.*

Ejemplo 5.5 El camino $\{v_1, v_2, v_3\}$ del Ejemplo 5.4 es un recorrido, mientras que $\{v_1, v_2, v_3, v_4, v_6, v_4, v_5\}$ no lo es (fijaos que este último tiene una arista repetida).

Definición 5.6 (Camino simple)
Un camino simple *es un camino en el que no se repiten ni aristas ni vértices.*

Definición 5.7 (Camino cerrado)
Un camino cerrado *es un camino en el que el primer vértice coincide con el último.*

Y, ahora, vamos a por la última definición de eta parte.

Definición 5.8 (Ciclo)
Un camino cerrado en el que no se repite ningún vértice se denomina ciclo.

Ejemplo 5.6 Dado el grafo $G = (V(G), E(G))$ de la Figura 5.8 tenemos que

- $\{v_1, v_2, v_3\}$ es un camino simple, mientras que $\{v_1, v_2, v_3, v_1, v_3\}$ no lo es.
- $\{v_1, v_2, v_3\}$ es un camino cerrado.
- $\{v_1, v_2, v_3\}$ es un ciclo.

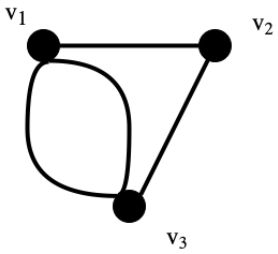


Figura 5.8: Grafo del Ejemplo 5.6.

Querido lector, no desesperes. Sé que son muchas definiciones y que son todas muy parecidas. Tómatelo con calma. Interioriza bien los conceptos que hemos presentado hasta ahora. Haz una tabla de similitudes y diferencias entre las definiciones que hemos presentado.

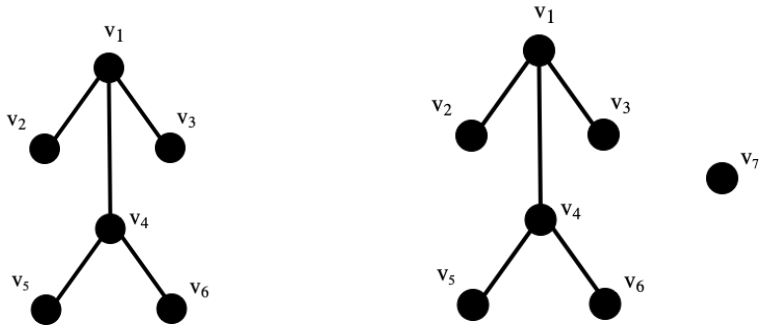
Alguna mente inquieta se habrá preguntado, mientras iba interiorizando las definiciones de la sección anterior, qué pasa cuando hay un vértice al que no se puede *acceder*. Un vértice (o conjunto de vértices y aristas) que están aislados. ¿Son esos grafos importantes? ¿Tienen nombre? ¿Sirven para algo? ¿Puede ocurrir? Tranquilas, mentes curiosas, vamos a despejar todas vuestras dudas.

Definición 5.9 (Grafo conexo)

Un grafo conexo *es un grafo tal que para cualquier par de vértices u y v siempre existe un camino que los une.*

Ejemplo 5.7 Dados los grafos de la Figura 5.9, tenemos que el grafo de la izquierda es un grafo conexo ya que puedo ir desde un vértice hasta todos los demás por un camino.

Sin embargo, si añado un vértice extra (es decir, obtengo como resultado el grafo de la derecha de la imagen), el grafo dejará de ser conexo. ¿Por qué? Piénsalo un momento. ¿Qué tenía que ocurrir con los vértices de los grafos conexos? Seguro que lo has adivinado: siempre están conectado con un camino. Y... ¿qué pasa con el vértice v_7? Está "suelto". Nunca podremos llegar a él desde el v_1 a través de un camino.



A) Grafo conexo B) Grafo no conexo

Figura 5.9: Ejemplo de grafo conexo y no conexo.

Nota: *Un pequeño* tip *para saber cuándo un grafo es o no conexo, es plantearse lo siguiente:* ¿es posible que, poniendo el lapicero sobre cualquier vértice del grafo, llegue a todos los demás sin levantar el lápiz del papel? *Si la respuesta es sí con todos los vértices, nos encontramos ante un grafo conexo. Si, por el contrario, hay un vértice para el que la respuesta es no, el grafo no será conexo.*

Definición 5.10 (Árbol)

Un grafo conexo que no tiene ni caminos cerrados ni ciclos se denomina árbol.

Ejemplo 5.8 El grafo de la Figura 5.10 es un árbol, porque no tiene caminos cerrados ni ciclos.

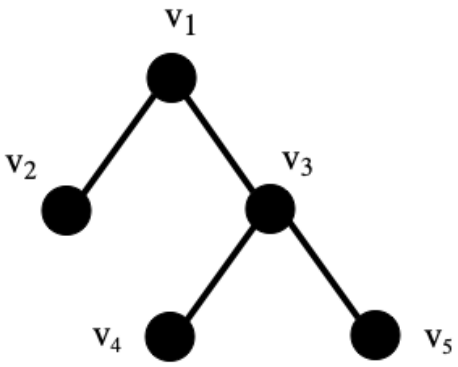


Figura 5.10: Ejemplo de árbol.

Teorema 5.1

Sea G un grafo y sean u y v dos vértices distintos. Si tenemos dos caminos simples distintos de u a v, entonces existe un ciclo en G.

Ejemplo 5.9 Vamos a fijarnos en el grafo de la Figura 5.11. Tenemos que puedo llegar de v_1 a v_3 a través del camino $\{v_1, v_2, v_3\}$ o del camino $\{v_1, v_4, v_3\}$. Así, como hay dos caminos simples distintos conectando a v_1 con v_3, el grafo tiene un ciclo.

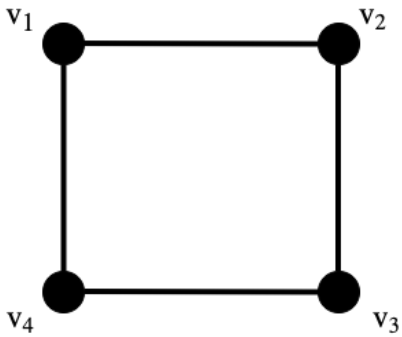


Figura 5.11: Grafo del Ejemplo5.9.

Para esta sección no hay ejercicio propuesto, pero os recomiendo que *juguéis* un poco con el concepto de grafo conexo y de árbol con los grafos que han aparecido en las secciones anteriores y en los Ejercicios Propuestos que os he sugerido que penséis.

Vamos a terminar la sección de conceptos clave hablando de *grafos completos*. No os voy a dar mucha información sobre ellos, pero veréis que van a ser de gran importancia en los ejercicios de Olimpiadas Matemáticas.

Definición 5.11 (Grafo completo)

Un grafo completo de n vértices *es un grafo que no tiene aristas iguales y tal que dados cualesquiera dos vértices siempre hay un arista que los une.*

Los grafos completos se denotan por K_n, donde n es el número de vértices que tiene el grafo.

Ejemplo 5.10 Los grafos de la Figura 5.12 son los grafos completos de 5 y 6 vértices respectivamente.

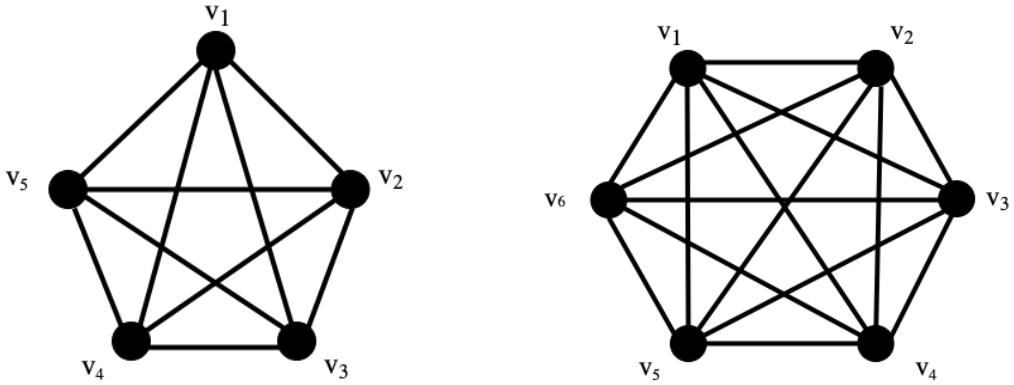


Figura 5.12: Grafos completos K_5 y K_6.

Como siempre, coge papel y lápiz y trata de dibujar K_7, K_8... hazte preguntas sobre este tipo de grafos y busca información complementaria que te pueda interesar. ¡Saciad vuestro hambre de conocimiento!

5.3 Grafos de Euler y Hamilton

Ya hemos trabajado con caminos, recorridos y ciclos: conocemos las similitudes y diferencias que hay entre ellos al dedillo. En esta sección vamos a trabajar con *grafos de Euler* y *grafos de Hamilton*, dos tipos de grafos muy importantes. (Os voy a contar una cosa: cuando en matemáticas veáis un nombre propio, que se os enciendan las alarmas... porque es MUY importante.) Estos grafos vamos a poder caracterizarlos de maneras concretas, usando caminos y ciclos especiales. Así que, antes de pasar de aquí, asegúrate de que los conceptos de la sección anterior los tienes tan accesibles en tu cabeza como el móvil lo tienes de la mano.

Definición 5.12 (Camino de Euler)

Un camino de Euler *o* camino euleriano *es un recorrido en el que aparecen todas las aristas.*

Ejemplo 5.11 El recorrido $\{v_5, v_2, v_1, v_4, v_3, v_2\}$ es un camino de Euler en el grafo de la Figura 5.13.

Definición 5.13 (Ciclo de Euler)

Un ciclo de Euler *o* ciclo euleriano *es un camino de Euler cerrado, es decir, un camino de Euler que comienza y termina en el mismo vértice.*

Ejemplo 5.12 El recorrido $\{v_1, v_2, v_3, v_4, v_1\}$ es un ciclo de Euler en el grafo que aparece en la Figura 5.14.

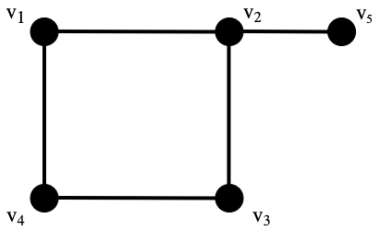


Figura 5.13: Grafo con un camino de Euler.

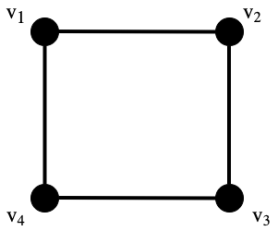


Figura 5.14: Grafo con un ciclo de Euler.

Definición 5.14 (Grafo de Euler)

Un grafo de Euler *o* grafo euleriano *es un grafo conexo con un ciclo de Euler.*

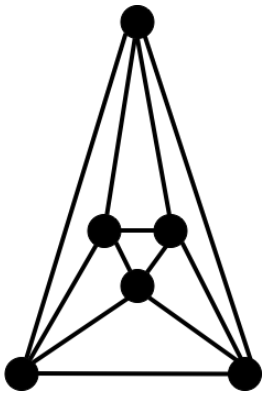
Ejemplo 5.13 El grafo del Ejemplo 5.11 no es un grafo de Euler puesto que no tiene un ciclo de Euler. Sin embargo, el grafo del Ejemplo 5.12 sí que lo es.

Proposición 5.1

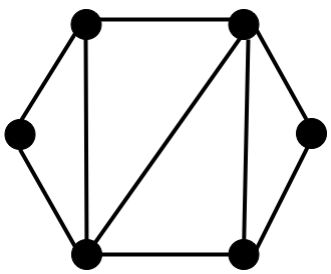
Si tenemos un grafo conexo, entonces es de Euler si, y solo si, el grado de cada vértice es par.

Ejemplo 5.14 Vamos a ver cómo funciona esta proposición aplicada a un ejemplo.

- El vértice v_5 del grafo del Ejemplo 5.11 tiene grado impar. Gracias a la proposición (y sin tener que hacer ningún cálculo más) sabemos que no es un grafo de Euler.
- Observando el grafo del Ejemplo 5.12, podemos observar que todos sus vértices tienen grado par. Usando, de nuevo, la proposición anterior, tenemos que el grafo es de Euler.
- El grafo que se muestra a continuación



  tiene todos los vértices de grado par. Por lo tanto, es un grafo de Euler.
- Fijémonos en el grafo que se muestra a continuación



  Podemos observar que tiene vértices de grado impar. Por lo tanto, no es un grafo de Euler.

Y, con este ejemplo, terminamos la teoría relacionada con grafos de Euler. Dejo como tarea para el lector que, en los grafos que hemos trabajado en esta sección, compruebe si hay o no caminos y ciclos de Euler.

Además, para que terminéis de interiorizar los conceptos sobre grafos de Euler, podéis realizar el Ejercicio Propuesto 4. Como siempre, tratad de sacar unos minutillos para realizar estos ejercicios. Volved a leer las definiciones y a mirar los ejemplos si hay algo que no os ha quedado del todo claro. ¿Ya los habéis hecho? Pues... ¡vamos a por lo siguiente!

Pasamos ahora a grafos de Hamilton. Pero antes, vamos a ver una serie de definiciones:

Definición 5.15 (Camino de Hamilton)

Un camino de Hamilton *o* camino hamiltoniano *es un recorrido en el que aparecen todos los vértices.*

Definición 5.16 (Ciclo de Hamilton)

Un ciclo de Hamilton *o* Hamiltionano *es un camino de Hamilton cerrado, es decir, un camino de Hamilton que comienza y termina en el mismo vértice.*

Definición 5.17 (Grafo de Euler)

Un grafo de Hamilton *o* Hamiltionano *es un grafo conexo con un ciclo de Hamilton.*

Ejemplo 5.15 El recorrido $\{v_1, v_2, v_3, v_4\}$ es un camino de Hamilton en el grafo que aparece en la Figura 5.15. Además, $\{v_1, v_2, v_3, v_4, v_1\}$ es un ciclo de Hamilton, lo que convierte al grafo en un grafo de Hamilton.

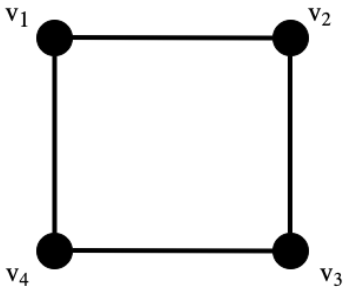


Figura 5.15: Ejemplo de un grafo con un ciclo de Hamilton.

Teorema 5.2

Sea G un grafo conexo con n vértices. Si el grado de todos los vértices es mayor que $\frac{n}{2}$, entonces G es un grafo de Hamilton.

Nota: *¿Encontráis alguna diferencia entre el Teorema 5.2 y la Proposición 5.1? Además de que uno habla de grafos de Hamilton y, la otra, de grafos de Euler, claro. Seguro que muchos lo habéis adivinado pero, los que no, fijaos con atención en lo siguiente: en la proposición aparecen las palabras* si, y solo si. *Esto nos indica que, si el grafo es de Euler, obligatoriamente todos sus vértices van a tener grado par. Y lo mismo ocurre al revés: si todos los vértices tienen grado par, entonces va a ser un grafo de Euler. Sin embargo, el teorema nos*

dice que, si todos los vértices tienen grado mayor que $\frac{n}{2}$*, entonces es de Hamilton. Pero la inversa no es cierta: un grafo de Hamilton no tiene porqué tener todos sus vértices de grado mayor que* $\frac{n}{2}$*.*

Mirad con atención esta nota. Tratad de entenderla. Si no lo veis claro, descansad un poco. Dejad reposar la información y volved a leerla cuando tengáis el cerebro a pleno rendimiento. No paséis hacia adelante hasta que no estéis totalmente convencidos de que habéis entendido la diferencia entre lo que nos aportan la proposición y el teorema.

Ejemplo 5.16 Vamos a trabajar, en este ejemplo, en si el grafo de la Figura 5.16 es o no un grafo de Hamilton. Lo primero que vamos a hacer es intentar aplicar el Teorema 5.2. Si aplicamos el teorema (hacedlo vosotros, para comprobarlo), nos damos cuenta de que ninguno de los vértices tiene grado mayor que $\frac{n}{2}$. Es decir, este teorema no nos va a decir si el grafo es o no hamiltoniano. Vamos a tener que ponernos manos a la obra.

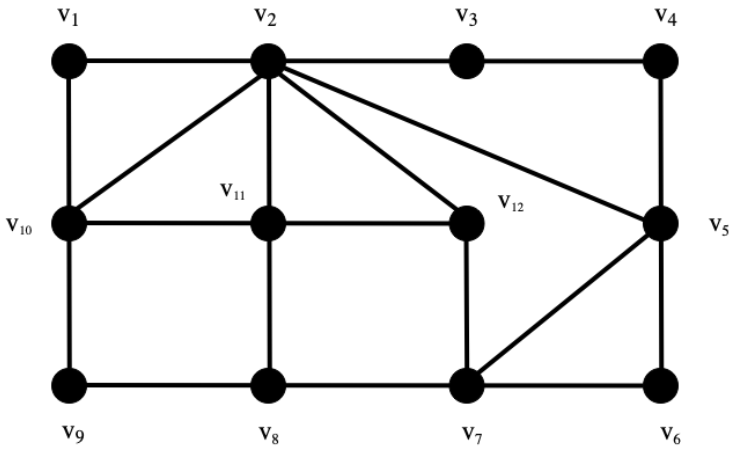


Figura 5.16: Grafo del Ejemplo 5.16.

Ahora, os toca trabajar a vosotros. El teorema no nos ha ayudado en nada, así que toca ponerse a trabajar. Buscad caminos de Hamilton. Y ciclos. ¿Hay? ¿No hay? Cuando lo hayáis pensado un poco - o lo hayáis resuelto, que seguro que lo habéis conseguido-, continuad leyendo.

En efecto, queridos lectores, el recorrido $\{v_1, v_2, v_3, v_4, v_5, v_6, v_7, v_8, v_9, v_{10}, v_{11}, v_{12}\}$ es un camino de Hamilton. Además, tenemos que $\{v_2, v_3, v_4, v_5, v_6, v_7, v_{12}, v_{11}, v_8, v_9, v_{10}, v_1, v_2\}$ es un ciclo de Euler, por lo que el grafo de la Figura 5.16 es de Hamilton.

Como siempre, y antes de cambiar de sección, tomaos unos minutitos para hacer el Ejercicio Propuesto 5 y, en caso de que tengáis dudas, trabajad de nuevo la sección hasta que os queden todos los conceptos claros. ¿Ya lo tienes? ¡Pues seguimos!

5.4 Grafos coloreables

Esta sección está enteramente dedicada a grafos coloreables. Es, quizá, una sección que parece un poco alejada a lo que estábamos haciendo hasta ahora. Sin embargo, es muy, pero que muy, importante. Así que leedla con cariño. ¡*Let's go for it*!

Definición 5.18 (Grafo coloreable)

Una coloración *de un grafo G es una asignación de colores a los vértices de dicho grafo de forma que vértices adyacentes reciban colores distintos.*
*Si el grafo se puede colorear con k colores, decimos que G es k-*coloreable*. El mínimo k con el que se puede colorear un grafo se denomina* número cromático *de G y se denota por $\chi(G)$.*

Esta definición, quizá, sea un poco abstracta. Sobre todo si es la primera vez que la ves. Vamos a ver, con un ejemplo, qué nos está diciendo esta definición.

Ejemplo 5.17 En este ejemplo vamos a trabajar con el mapa de España. Sí, sí. Has leído bien. Con el mapa de España. ¿Recuerdas que en la introducción hicimos una abstracción del centro de la ciudad de Königsberg? Pues ahora vamos a hacer lo mismo, pero con el mapa de España - por Comunidades Autónomas.

Antes de seguir y de que se os vaya la vista a la abstracción del mapa, tratad de hacerlo vosotros. Estoy segura de que a estas alturas lo haréis de rechupete. En la Figura 5.17 podéis ver cómo queda la abstracción del mapa de España por Comunidades Autónomas.

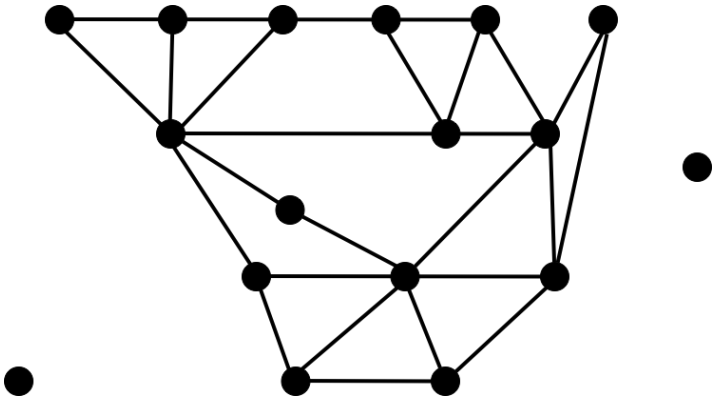


Figura 5.17: Grafo asociado al mapa de España, por Comunidades Autónomas.

¿Os ha quedado el mismo grafo? ¡Seguro que sí! Ahora, vamos a colorearlo. Tratad de hacerlo vosotros antes de mirar la solución, que la podéis ver en la Figura 5.18.

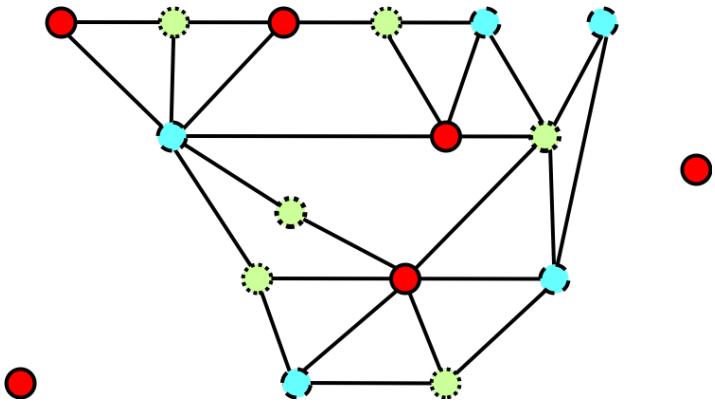


Figura 5.18: Grafo asociado al mapa de España, por Comunidades Autónomas.

Si nos fijamos en la coloración que hemos realizado, tenemos que el número cromático del grafo asociado al mapa de España, $\chi(G)$, es 3. Es decir, el mapa de España es 3-coloreable.

Teorema 5.3 (Teorema de los 4 colores)

Todo grafo plano y, en particular, un mapa que no tenga enclaves, se puede colorear siempre con 4 colores.

El Teorema de los 4 colores es muy importante. Voy a corregirme sobre lo que os he dicho en la sección de grafos de Euler y Hamilton: en matemáticas, siempre que algo tenga un nombre para identificarlo, es MUY importante.

Las siguientes proposiciones también lo son (aunque no tengan nombre para identificarlas). De hecho, ambas van a ser de gran relevancia para resolver los ejercicios de Olimpiadas Matemáticas que vamos a plantear en la siguiente sección.

Proposición 5.2

Todo árbol es 2-coloreable.

Proposición 5.3

Un grafo completo de n vértices, K_n, es n-coloreable.

Si nos fijamos en el árbol de la Figura 5.10 y en el grafo completo de 5 vértices de la Figura 5.12, tenemos que la proposición es cierta (véase la Figura 5.19).

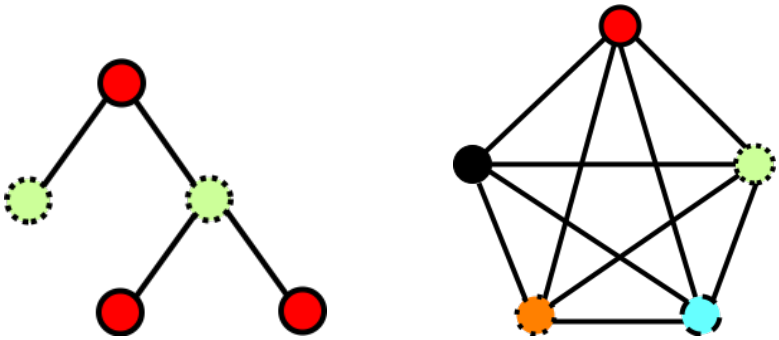


Figura 5.19: Coloración de un árbol y un grafo completo.

Esta sección ha sido la última sobre Teoría de Grafos. Espero que hayáis aprendido muchas cosas... ¡porque en la siguiente las pondremos en práctica! Así que, si las definiciones bailan en vuestras cabezas y las proposiciones se esconden en los rincones de vuestras mentes, ¡parad! Dad un paso atrás y volved a mirar los apuntes detenidamente. Y, cuando os sintáis preparados, ¡a por ello!

5.5 Problemas de olimpiadas matemáticas

En esta sección vamos a resolver dos problemas de Olimpiadas Matemáticas. Aunque tienen mucho texto, es porque las explicaciones son muy detalladas. ¡Vamos a darle duro!

Problema 5.1 (Olimpiada Matemática de Colorado, 2010). La Organización de las Naciones Unidas tiene 192 Estados Miembros de forma que cada par de Estados Miembros tiene un desacuerdo. Para formar una *unión más perfecta*, se establece una negociación: si cuatro representantes de cuatro Estados Miembros se sientan alrededor de una mesa redonda, de manera que cada par de representantes consecutivos tienen un desacuerdo, la

negociación elimina uno de esos cuatro desacuerdos. Una serie de negociaciones consecutivas reduce el número total de desacuerdos a n. ¿Cuál es el mínimo valor de n?

Solución *Lo primero que vamos a hacer es analizar el problema. Quizá alguno piense:* ¿pero esto qué eh? *Con todo lo que sé de grafos y, cuando leo este enunciado, ¡no sé de que me hablan! Tranquilos, vamos a ir desgranándolo poquito a poco. Os daré pistas antes de ir resolviendo las cosas, para que podáis ir razonando y, así, cuando os encontréis ante otros problemas de este estilo, os sea pan comido.*

En primer lugar, tenemos que pensar en los Estados Miembros como los vértices del grafo. Entonces, como tenemos 192 *Estados Miembros,* ***nuestro grafo inicial va a contar con*** 192 ***vértices****. Son muchos, ¿verdad? Ya veréis que bien y con qué soltura vamos a trabajar con ellos.*

Vamos a pensar cómo seguir. Sabemos que un grafo consta de un conjunto de vértices (ya lo tenemos) y de un conjunto de aristas. ¿Dónde está nuestro conjunto de aristas? Parad un momento. Leed el enunciado de nuevo si es preciso. Tratad de analizarlo con la mente totalmente despierta. ¿Lo tenéis? ¿Qué van a representar las aristas? Si ya tenéis un idea, seguid leyendo a ver si habéis acertado. Si no se os ocurre nada y creéis que no se os va a ocurrir, seguid leyendo también. Si pensáis que podéis sacarlo pensándolo un ratito más... ¡dadle duro! Las aristas van a representar... ¡los desacuerdos! ***Dos vértices van a estar conectados si los Estados Miembros tienen un desacuerdo****.*

Ya casi tenemos el grafo con el que vamos a trabajar. Sabemos que los vértices representan a los Estados Miembros y, las aristas, a los desacuerdos que hay entre ellos. Como cada par de Estados Miembros tienen un desacuerdo, tenemos que un vértice está unido con todos los demás. Por lo tanto... ¡tenemos un grafo completo de 192 *vértices! Es decir, vamos a trabajar con* K_{192}.

Vamos a analizar ahora qué es una negociación. Pensad un poco cómo podríais representar una negociación en términos de grafos. ¿Lo tenéis? Una negociación consiste en seleccionar un ciclo de 4 *vértices en nuestro grafo (un* 4*-ciclo) y eliminar una arista de él.*

Una vez que hemos analizados las partes de nuestro enunciado, vamos a tratar de enunciar el problema de una forma diferente, más sencilla. ¿Se os ocurre algo? ¡Ahí va el problema reformulado!

Determinar el número mínimo de aristas del grafo de desacuerdos obtenido a partir del inicial tras una serie de eliminaciones consecutivas de una arista de un 4**-ciclo.**

Vamos a realizar unas observaciones:

- *Imaginemos que tenemos un* 4*-ciclo (podéis dibujarlo, para que podáis imaginaros la idea visualmente) y que eliminamos una arista de él. ¿Qué pasa con la conectividad del grafo? Efectivamente, la eliminación de la arista mantiene la conectividad del grafo. Además, ¡dejamos de tener un ciclo!*
- *Para cualquier par de puntos de un árbol, hay un único camino que los conecta.*
- *Gracias a la Proposición 5.2 sabemos que cualquier árbol es* 2*-coloreable.*
- *Los* 4*-ciclos son* 2 *coloreables y, apliquemos una negociación, continúa siendo* 2*-coloreable. Es decir, la negociación y su inversa conservan la propiedad de ser* 2*-coloreable.*

Si las n *negociaciones hiciesen que todos los ciclos desapareciesen, nuestro grafo inicial se transformaría en un grafo sin ciclos y conexo. Es decir, se transformaría en un árbol. En un árbol de* 192 *vértices y* 191 *aristas. Como la negociación y su inversa mantienen la propiedad de ser* 2*-coloreable, el grafo que hemos obtenido es* 2*-coloreable. Esto implica que el grafo inicial de desacuerdos es* 2*-coloreable. Pero... ¿*K_{192} *es* 2*-coloreable?*

¡No! ¡De ninguna de las maneras! Hemos llegado a un absurdo. Y, ¿de dónde viene este absurdo? De suponer que podemos llegar a un grafo de 191 *aristas. Vamos a realizar el siguiente proceso:*

1. *Dado* K_{192}*, vamos a tomar el* 4*-ciclo formado por* $\{v_1, v_2, v_3, v_4\}$ *y vamos a eliminar la arista* $\{v_1, v_3\}$.
2. *Repetimos el proceso: tomamos el* 4*-ciclo formado por* $\{v_1, v_2, v_4, v_5\}$ *y nos deshacemos de la arista* $\{v_1, v_4\}$.
3. *Si repetimos el proceso con todos los* 4*-ciclos en los que aparece el vértice* v_1*, conseguimos romper todas las aristas que van conectadas a* v_1*. Salvo la arista* $\{v_1, v_2\}$.

Con este proceso hemos conseguido obtener el vértice v_1 *conectado a un grafo completo de* 191 *vértices, como el que mostramos en la Figura 5.20.*

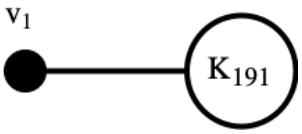


Figura 5.20: Grafo obtenido tras realizar negociaciones en todos los 4-ciclos en los que aparece v_1.

Realizando el mismo proceso en todos los 4*-ciclos donde aparece* v_2*, obtenemos el grafo de la Figura 5.21.*

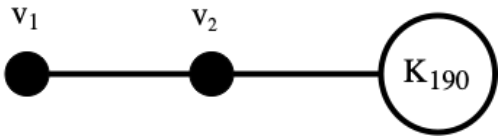


Figura 5.21: Grafo obtenido tras realizar negociaciones en todos los 4-ciclos en los que aparece v_1.

Reiterando el proceso con el resto de vértices, va a haber un punto en el que vamos a llegar al grafo de la Figura 5.22.

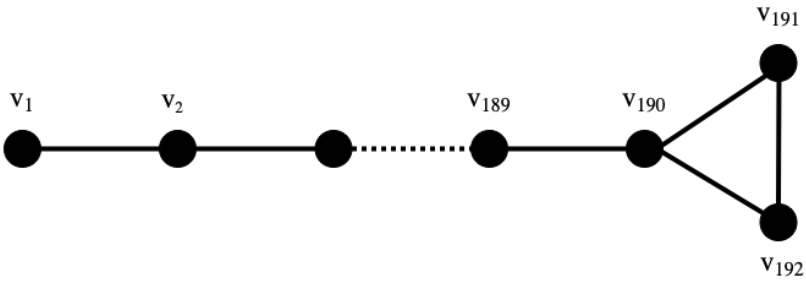


Figura 5.22: Grafo obtenido tras realizar negociaciones en todos los 4-ciclos en los que aparece v_1.

Este grafo que hemos obtenido tiene 192 *vértices,* 192 *aristas y no es* 2*-coloreable. Este es el grafo más pequeño al que podemos llegar. Por lo tanto, el mínimo número de desacuerdos es* 192.

Nota: *El problema anterior es duro. No es difícil, pero sí duro. Y largo. Así que miradlo despacio. Tomaos varios días si es necesario. Entendedlo bien. Haced las cosas que se han quedado en el tintero y que solo he nombrado. Convenceros de todo lo que hemos dicho. Y, cuando lo tengáis claro, ¡a por el siguiente!*

Problema 5.2 (Mathematical Olympiad Program, 2008). Prueba que si las aristas de K_n, el grafo completo de n vértices, son coloreadas de tal forma que ningún color es asignado a más de $n-2$ aristas, entonces existe un triángulo que tiene una arista de cada color.

Solución *Vamos a resolver este problema haciendo reducción al absurdo. Para ello, supongamos que no existe un triángulo con una arista de cada color.*

Definimos una componente C-conectada como un conjunto de vértices tales que para cualesquiera dos vértices de dicho conjunto, existe un camino entre ellos y todas las aristas están coloreadas del mismo color C.

Tomaos un momento para entender bien la definición y, cuando estéis seguros de tener claro lo que quiere decir... ¡continuad!

Ahora, vamos a llamar X a la componente C-conectada más larga para cualquier color C. Digamos que es color rojo. Supongamos que hay un vértice $v \notin X$ y consideremos dos vértices u_1 y u_2 conectados por una arista roja. Ninguna de las aristas $\{v, u_1\}$ y $\{v, u_2\}$ pueden ser de color rojo y, además, estas aristas tienen que ser del mismo color. ¿Por qué? Porque si fuesen de colores diferentes, ¡ya tendríamos un triángulo con tres aristas de diferente color! Digamos que $\{v, u_1\}$ y $\{v, u_2\}$ son de color azul.

Así, v está conectado a todos los vértices de X por aristas de un mismo color pero... entonces $X \cup \{v\}$ es una componente azul-conectada, ¡y es más grande que X! Y esto es ABSURDO. ¿Por qué? Porque recordad que habíamos supuesto que X era la C-componente más grande.

Esto implica que no va a poder haber ningún vértice v que no esté en X, luego los n vértices del grafo están en X. Pero como X-es rojo-conectado y tiene n vértices, entonces habrá, al menos, $n - 1$ aristas de color rojo. Pero esto vuelve a ser ABSURDO porque el enunciado nos decía que no podía haber más de $n - 2$ aristas coloreadas del mismo color. Y este absurdo viene de suponer que no existe un triángulo con tres aristas pintadas de diferente color. Es decir... ¡ese triángulo existe! ¡Ya lo tenemos!

Ejercicios Propuestos

1. En la Figura 5.23 se puede ver la imagen del centro de París. ¿Es posible dar un paseo comenzando desde cualquiera de las regiones, pasando por todos los puentes una única vez y regresando al mismo punto de partida?

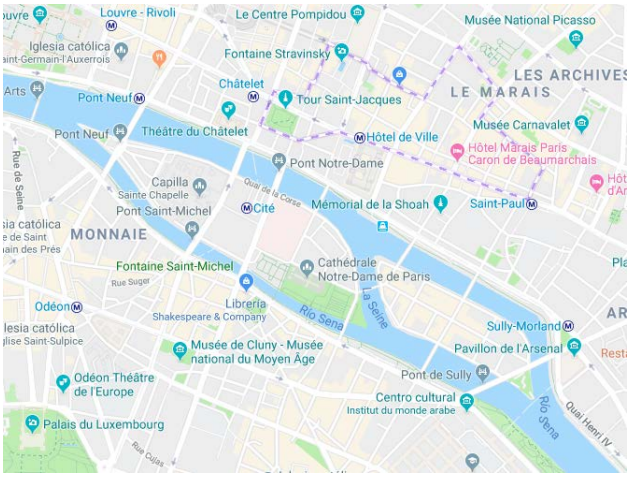


Figura 5.23: Grafo asociado al centro de París.

2. Calcula el conjunto de aristas y vértices de los grafos de la Figura 5.24.

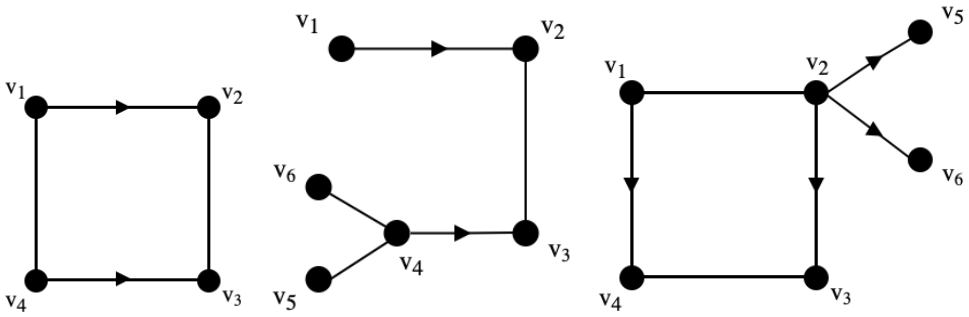


Figura 5.24

3. Calcula los posibles caminos (simples y cerrados), recorridos y ciclos de los grafos de la Figura 5.25. Haz lo mismo con los grafos del Ejercicio Propuesto 2. ¿Observas diferencias? Tómate unos minutos para pensar en ello.

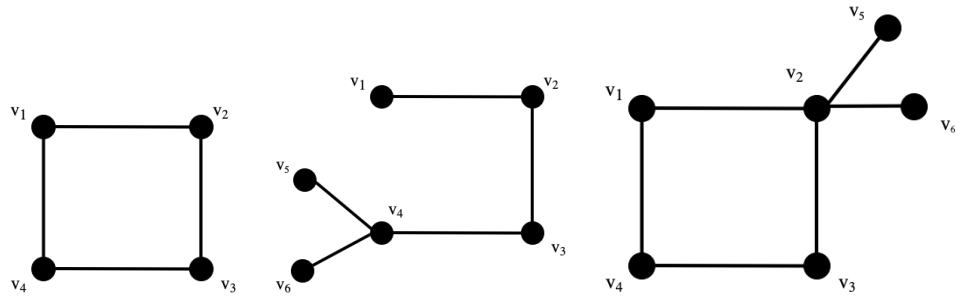


Figura 5.25

4. ¿Son los grafos de la Figura 5.26 de Euler?. Encontrad los posibles ciclos y caminos de Euler que aparezcan en ellos.

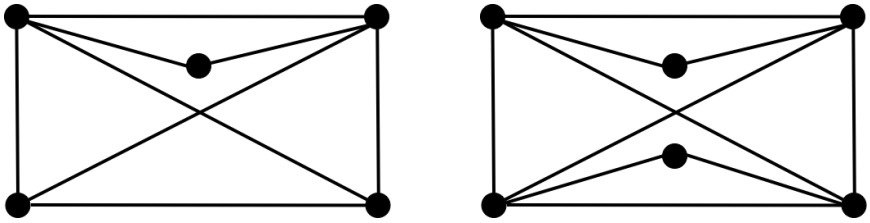


Figura 5.26

5. ¿Es el grafo de la Figura 5.27 de Hamilton? Encontrad los posibles ciclos y caminos de Hamilton que aparezcan en ellos.

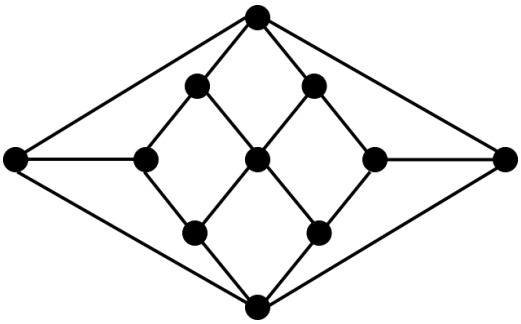


Figura 5.27

Bibliografía Adicional

1. Ore, O. (1995). *Grafos y sus aplicaciones*. Colección la tortuga de Aquiles, Proyecto EULER, Madrid.
2. Ore, O. & Wilson, R. J. (1990). *Graphs and their uses* (Vol. 34). Editorial Cambridge University Press.

CAPÍTULO 6

6

ARITMÉTICA MODULAR - PARTE 1

Jorge Roldán López
Universidad de La Rioja

Palabras clave

- *Módulo*
- *Congruencia*
- *Divisibilidad*
- *Fermat*

Durante la resolución de muchos ejercicios de matemáticas necesitamos conocer la divisibilidad de un número. Desde la infancia empezamos a conocer los criterios para saber cuándo podemos dividir por números pequeños, aunque otros más grandes como el 7, 11 ó 13 igual no los recordamos o ni siquiera llegamos a conocerlos. Sin embargo, aunque útiles, las técnicas clásicas que nos permiten conocer cuándo un número es divisible por otro, pronto se quedan cortas. En este capítulo se introduce la aritmética modular con sus congruencias. Esta es una nueva técnica que lleva mucho más lejos esta idea y nos abre un abanico de potentes resultados para enfrentarnos a estos y otros problemas.

6.1 Introducción

A lo largo de nuestra vida es frecuente encontrarse con situaciones donde resulte conveniente conocer si un número entero es divisible por otro. Por ejemplo, para responder a la siguiente pregunta:

«¿Podemos repartir 112332 acciones de una empresa entre 33 accionistas sin que sobre ninguna?»

Dado que una acción no se puede partir, debemos estudiar si 112332 es divisible por 33. En este caso la respuesta es sí. No obstante, aunque en números pequeños la cuenta resulta viable, incluso mentalmente, el problema escala con fácilidad. Así pues, surge la pregunta de si podemos comprobarlo fácilmente sin necesidad de tener que hacer la cuenta completa.

Para aliviar la comprobación de si un número entero es divisible por otro existen los criterios de divisibilidad. Aunque pronto veremos que estas herramientas se quedan cortas y necesitaremos introducir nuevas.

6.2 Criterios de divisiblidad

El primer paso es tener claro qué entendemos por ser divisible o múltiplo. Un concepto que, aunque sencillo, tiene su propia notación matemática.

Definición 6.1 (Divisible o múltiplo)

Dados dos números enteros n y m. Decimos que un número n es divisible por m, o que m divide a n, o que n es múltiplo de m, y lo denotamos como $m|n$, cuando existe otro entero k tal que $n = m \cdot k$.

Una vez vistas todas las formas en las podemos expresarlo, podemos empezar a buscar criterios de divisibilidad. El criterio más conocido, y que se estudia desde niño, es el del número dos. Este nos dice que para que un número sea divisible por dos debe ser par. Aunque, como ya sabremos, esto se limita a estudiar la última cifra como nos indica el siguiente lema:

Lema 6.1 (Criterio de divisibilidad para 2)

Un número es divisible por 2 si y solo si el número en cuestión termina en un número par.

Conviene recordar por si acaso que el número cero es un número par. De hecho el cero es divisible por cualquier entero no nulo. En el caso del número 3, el criterio también es muy conocido y sencillo:

Lema 6.2 (Criterio de divisibilidad para 3)

Un número es múltiplo de 3 si y solo si la suma de sus cifras lo es también.

Así, como nos dice este lema, para comprobar si 291 231 398 172 es divisible por 3 basta calcular

$$2 + 9 + 1 + 2 + 3 + 1 + 3 + 9 + 8 + 1 + 7 + 2 = 48.$$

Aunque con esto puede ser suficiente para responder ya que sí, podemos seguir comprobando si 48 divisible por 3 calculando $4 + 8 = 12$. Y nuevamente podríamos hacer $1 + 2 = 3$ dejándolo ya muy claro. Es decir, todos estos criterios se pueden aplicar varias veces.

Sigamos ahora enunciando reglas para los siguientes números:

Lema 6.3 (Criterio de divisibilidad para 4)
Un número es divisible por cuatro si y solo si sus últimas dos cifras son un múltiplo de 4.

Lema 6.4 (Criterio de divisibilidad para 5)
Un número es divisible por 5 si y solo si termina en 0 o 5.

Lema 6.5 (Criterio de divisibilidad para 7)
Un número es divisible por 7 si y solo si al restar a dicho número sin la cifra de la unidades el doble de la cifra de las unidades da múltiplo de 7.

Este criterio es algo más complejo, así que para que termine de quedar claro vamos a ver un ejemplo.

Ejemplo 6.1 ¿Es divisible 127621 por 7? El primer paso es calcular $12762 - 2 \cdot 1 = 12760$. Como seguimos sin saberlo vamos a repetir este mismo paso hasta que ya sepamos responder. Ahora debemos hacer $1276 - 2 \cdot 0 = 1276$. El siguiente paso sería $127 - 2 \cdot 6 = 115$, seguido por $11 - 2 \cdot 5 = 1$. Llegados a este punto ya podemos decir sin dudarlo que la respuesta es no. 127621 no es divisible por 7 ya que 1 no lo es.

Sigamos con nuestra lista:

Lema 6.6 (Criterio de divisibilidad para 9)
Un número es divisible por 8 si y solo sus últimas 3 cifras son un múltiplo de 8.

Lema 6.7 (Criterio de divisibilidad para 9)
Un número es divisible por 9 si y solo si la suma de sus cifras lo es.

Lema 6.8 (Criterio de divisibilidad para 10)
Un número es divisible por 10 si y solo si termina en 0.

Lema 6.9 (Criterio de divisibilidad para 11)
Un número es divisible por 11 cuando la diferencia entre las cifras que ocupan posición par y las que ocupan posición impar es múltiplo de 11.

Lema 6.10 (Criterio de divisibilidad para 13)
Un número es divisible por 13 si y solo si al restar a dicho número sin la cifra de la unidades nueve veces la cifra de las unidades da múltiplo de 13.

Como podemos ver, hay criterios muy similares: el del 4 y el 8, el 3 y 9, el 7 y 13... Y así podríamos seguir dando criterios para más números, aunque no tiene mucho sentido. En cualquier caso, llegados a este punto podemos ver que no hemos puesto ni el criterio para el 6, ni respondido a la pregunta inicial de si 112332

es divisible por 33. Sin embargo, sí que sabemos responder con los criterios ya dados a ambas preguntas. Para ello vamos a hacer uso de la siguiente proposición:

Proposición 6.1

Un número n es divisible entre $a \cdot b$, siendo el $mcd(a, b) = 1$, si y solo si n es divisible por a y por b.

Así, un número es divisible por 6 si lo es por 2 y por 3 a la vez. Y, a su vez, 112332 es divisible por $33 = 3 \cdot 11$ si y solo si lo es por 3 y por 11. Y todos estos criterios de divisibilidad los conocemos ya de antes. Por tanto:

- $1 + 1 + 2 + 3 + 3 + 2 = 12$, luego es divisible por 3.
- $1 - 1 + 2 - 3 + 3 - 2 = 0$, luego es divisible por 11.

Nota: *Cuidado que esto necesita que el mcd sea 1 y de no ser así no podremos descomponerlo. Así 12 podemos descomponerlo como $3 \cdot 4$ y algo es divisible entre 12 si lo es entre 3 y entre 4, pero no podemos descomponerlo como 6 y 2 o como 3, 2 y 2.*

Ahora con todo esto claro ya somos capaces de poner a prueba estos criterios en los ejercicios propuestos 1., 2. y 3. del final del capítulo. No obstante, los criterios de divisibilidad presentan algunas pegas:

- Podemos no conocerlos.
- Pueden ser tediosos de aplicar.
- Podemos desconocer las cifras del número el cual queremos saber si es divisible.

Aunque para este último caso podemos encontrar alternativas en algunos casos para salir adelante como en el siguiente ejemplo:

Ejemplo 6.2 ¿Para qué x e y enteros el número $x^2 - y^2$ es divisible por 4?

El primer paso es darse cuenta que $x^2 - y^2 = (x + y)(x - y)$. Como queremos que $(x + y)(x - y)$ sea múltiplo de cuatro y por tanto par, necesitamos al menos que $x + y$ o $x - y$ sea uno de ellos par como mínimo. Veamos en el Cuadro 6.1 qué ocurre en función de si x e y son pares o impares.

x	y	$x + y$	$x - y$
Par	Par	Par	Par
Par	Impar	Impar	Impar
Impar	Par	Impar	Impar
Impar	Impar	Par	Par

Cuadro 6.1: Tabla de paridades de $x + y$ y de $x - y$.

Como podemos ver $x + y$ y $x - y$ tienen siempre la misma paridad. Y ambos son pares, como queremos, cuando x e y tienen la misma paridad. Y es más, como ambos son pares, su producto es directamente múltiplo de 4. Por tanto, la solución es que tanto x como y deben tener la misma paridad para que $x^2 - y^2$ sea múltiplo de 4.

Notar que parece que este mismo análisis se puede hacer sin esta descomposición en producto usando el Cuadro 6.2. Sin embargo, el resultado no queda claro que sea múltiplo de 4 directamente y habría que estudiar esos casos. Por ejemplo poniendo x e y como $2n$ y $2m$ o $2n + 1$ y $2m + 1$ en función de si son pares o impares.

x	y	x^2	y^2	x^2-y^2
Par	Par	Par	Par	Par
Par	Impar	Par	Impar	Impar
Impar	Par	Impar	Par	Impar
Impar	Impar	Impar	Impar	Par

Cuadro 6.2: Tabla de paridades de $x^2 - y^2$.

En cualquier caso, aunque hemos podido salir al paso en este ejemplo, existen otras preguntas que no podremos responder:

- ¿Es $7^n - 1$ múltiplo de 6?
- ¿Es $25^{3123} + 15$ divisible por 8?

Este último por ejemplo se trata de un número que tiene ¡4366 cifras! Son estos problemas los que en parte motivan la búsqueda de herramientas más potentes, como las que veremos en el siguiente capítulo.

6.3 Aritmética modular: definición y principales propiedades

Antes de introducir la aritmética modular, para evitar asustarnos ante un concepto nuevo, conviene darse cuenta que en el día a día cualquier persona hace uso de ella sin saberlo. Todo el mundo sabe que las 17:00 horas son las 5 de la tarde, o que las 21:00 son las 9. Incluso esto afecta a operaciones. Si a las 10 alguien nos dice que queda con nosotros en 5 horas, nos está citando a las 3. ¿Pero qué clase de brujería nos lleva a comparar el 17 con el 5 o el 21 con el 9 o nos dice que $10 + 5 = 3$? La respuesta es la aritmética modular, en este caso módulo 12. Como 17-12 = 5, decimos que ambas horas son "equivalentes" módulo 12. Y en el caso de la suma $10 + 5 = 15$ pero 15 es como 3.

Algo similar ocurre cuando trabajamos con ángulos. Un ángulo de $30°$ es equivalente a uno de $390°$, o uno de $\pi/6$ es equivalente a otro de $13\pi/6$ si hablamos del mismo ángulo en radianes. Esto se debe a que están en la misma posición y lo único que los diferencia es el número de vueltas que han dado para llegar ahí. De hecho, el siguiente ejemplo muestra que, en problemas trigonométricos, muchas veces todos estos ángulos son solución.

Ejemplo 6.3 Calcula α tal que $\operatorname{sen}\alpha = \dfrac{1}{\sqrt{2}} = \cos\alpha$. En este caso la solución es $\alpha = 45° + 360°k = \dfrac{\pi}{4} + 2\pi k$ siendo k un entero cualquiera que representa el número de vueltas.

Una vez hemos visto que hay situaciones habituales donde números aparentemente diferentes se comportan como "equivalentes", podemos perder el miedo e introducirnos en la aritmética modular. Si bien la idea es antigua, el lenguaje que vamos a emplear es relativamente nuevo y apareció en el siglo XIX de mano del genio matemático Carl Friedrich Gauss (1777–1855).

Definición 6.2 (Congruentes)

Dados tres números enteros n, m y k. Decimos que n y m son congruentes módulo k, y lo denotamos

$$n \equiv m \pmod{k}.$$

si al dividir n y m ambos por k obtenemos el mismo resto.

En otras palabras, $n \equiv m$ módulo k es equivalente a que $n - m$ sea múltiplo de k.

Nota: *Aunque toda congruencia se realiza módulo cierto natural, en aquellos contextos donde quede claro podremos omitir la escritura del módulo en el cual estamos trabajando para abreviar.*

Así tendríamos que

$$25 \equiv 4 \pmod 7,$$
$$15 \equiv 35 \pmod 2,$$
$$1605 \equiv 149 \pmod{13}$$
$$193\,183 \equiv 33\,261\,931 \pmod{12},$$
$$24 \equiv -1 \pmod 5.$$

Notar que la congruencia nos sirve directamente para comprobar o calcular cuál es el resto de dividir dos números:

Lema 6.11
Si al dividir m entre n da resto k entonces $m \equiv k \pmod n$.

Este lema también nos da el criterio general de divisibilidad en congruencias:

Corolario 6.1
Un número n es divisible por m si y solo si $n \equiv 0 \pmod m$.

Una vez visto este concepto, podemos introducir las propiedades más básicas que más adelante nos facilitaran el trabajo. Aunque no se indique explícitamente, todas las congruencias son bajo un mismo módulo cualquiera.

Propiedad *Si $a \equiv b$ entonces para todo k se tiene que*

- $a + k \equiv b + k$,
- $k \cdot a \equiv k \cdot b$,
- $a^k \equiv b^k$ *si* $k \in \mathbb{N}$.

Propiedad *Si $a \equiv b$ y $c \equiv d$ entonces*

- $a + c = b + d$,
- $a \cdot c \equiv b \cdot d$.

Probar estas propiedades no resulta difícil y puede ser un interesante ejercicio que queda para el lector. Si bien, alguna de las pruebas como la de las potencias requiere de inducción.

Otra propiedad que nos puede resultar útil nos la da el siguiente lema:

Lema 6.12
Sea $p|m$, es decir, sea p un divisor de m entonces si $n \equiv k \pmod m$ se tiene que $n \equiv k \pmod p$.

Sin embargo, el recíproco no es cierto y es fácil verlo con un contraejemplo. En módulo 4 tenemos que $6 \cong 2$, pero en módulo 8, un múltiplo de 4, esta congruencia no se da.

Con esto, ya estamos listos para resolver las dos preguntas propuestas al final del apartado anterior:

Ejemplo 6.4 ¿Es $7^n - 1$ múltiplo de 6? Como en módulo 6, $7 \equiv 1$, entonces $7^n \equiv 1^n$. Así

$$7^n - 1 \equiv 1^n - 1 = 0 \pmod 6.$$

Ejemplo 6.5 ¿Es $25^{3123} + 15$ divisible por 8? En módulo 8, $25 \equiv 1$, luego $25^{3123} = 1^{3123}$, de nuevo 1. Y además $15 \equiv 7$. Así $25^{3123} + 15 = 1^{3123} + 7 \equiv 1 + 7 \equiv 0 \pmod 8$.

Por otro lado, habrá ocasiones en las que usar números negativos nos puede ayudar y mucho, como en el próximo ejemplo:

Ejemplo 6.6 Determina todos los enteros positivos n para los cuales $2^n + 1$ es divisible por 3. Aquí queremos ver para qué valores de n se cumple que

$$2^n + 1 \equiv 0 \pmod 3$$

Pero esto es lo mismo que decir que

$$(-1)^n + 1 \equiv 0 \pmod 3$$

Luego esto solo es cierto para valores impares de n.

Podemos practicar con alguna congruencia como la de los ejercicios propuestos 4., 5. y 6..

6.4 Inversos modulares

Si observamos con cuidado las propiedades anteriores vemos que una nos dice que las congruencias se llevan bien con el producto, es decir, que si $a \equiv b$ entonces $k \cdot a \equiv k \cdot b$. Esto nos puede llevar a pensar que ocurre algo similar con la división, es decir, que podemos simplificar la k. Pero no siempre es cierto. Un contraejemplo de esto es:

$$2 \cdot 3 \equiv 2 \cdot 10 \pmod{14} \qquad \not\Rightarrow \qquad 3 \equiv 10 \pmod{14}.$$

En realidad esto se debe a que dividir es multiplicar por el inverso. Y aquí el dos no tiene inverso. Pero, ¿qué es esto del inverso?

Definición 6.3 (Inverso)

Dado un número a, si existe b tal que $a \cdot b = 1$, decimos que b es su inverso y lo denotamos como a^{-1}. En este caso a se llama invertible o inversible.

En los racionales nos sonará que

$$\frac{a}{b} = a \cdot \frac{1}{b} = a \cdot b^{-1}.$$

Pero aquí las cosas funcionan diferentes. Sin entrar en mucho detalle al trabajar en aritmética modular estamos aplicando un cociente en $\mathbb{Z}$ llegando a una estructura equivalente a $\mathbb{Z}_n$. No hace falta que entendamos del todo para este capítulo que significa esto, pero sí cuándo existe el inverso y cómo se puede calcular.

Definición 6.4 (Coprimo)

Decimos que dos números a y b son coprimos cuando no tienen factores en común, es decir, $mcd(a, b) = 1$.

Proposición 6.2

Dado un entero a módulo m, existe a^{-1} si y solo si $mcd(a, m) = 1$, es decir, son coprimos.

Así, cuando m es un número primo todo entero no nulo tiene inverso. Gracias a esta proposición sabemos cuando podemos simplificar la ecuación

$$k \cdot a \equiv k \cdot b \pmod{m},$$

puesto que tomando k^{-1}, si existiese, tendríamos

$$k^{-1} \cdot k \cdot a \equiv k^{-1} \cdot k \cdot b,$$

y como $k^{-1} \cdot k \equiv 1$ llegamos a que $a \equiv b$, justo lo que buscábamos.

En caso de que k no tuviese inverso, podríamos tomar un divisor de m coprimo con k como nos indica el Lema 6.12 y después simplificar al ser ya k invertible.

Ejemplo 6.7 Queremos como antes simplificar $2 \cdot 3 \equiv 2 \cdot 10 \pmod{14}$. Como $\text{mcd}(2, 14) = 2 \neq 1$ no podemos tomar el inverso de 2 para simplificarlo de ambos lados de la ecuación en congruencias. Sin embargo, como 7 es divisor de 14 sabemos que

$$2 \cdot 3 \equiv 2 \cdot 10 \pmod{14} \implies 2 \cdot 3 \equiv 2 \cdot 10 \pmod{7} \implies 3 \equiv 10 \pmod{7},$$

donde en el último paso ya hemos podido tomar el inverso al ser 7 un número primo.

De hecho en general tenemos el siguiente resultado.

Proposición 6.3

Dada la relación $k \cdot a \equiv k \cdot b \pmod{m}$ entonces $a \equiv b \pmod{n}$, donde

$$n = \frac{m}{mcd(k, m)}.$$

Para simplificar no necesitamos calcular el inverso, únicamente saber dónde existe y, por tanto, si podemos hacerlo. Sin embargo, habrá ejercicios donde conocerlo pueda resultar interesante o pueda darnos la solución directamente. ¿Cómo podemos encontrarlo?

Encontrar el inverso de a módulo m equivale a resolver la ecuación en congruencias

$$a \cdot b \equiv 1 \pmod{m}.$$

Pero esto es lo mismo que decir que $a \cdot b - 1$ es múltiplo de m. Es decir, que existe $n \in \mathbb{Z}$ tal que

$$a \cdot b - 1 = m \cdot n.$$

Reordenando tenemos que

$$a \cdot b - m \cdot n = 1,$$

donde a y m son conocidos, b y n son enteros a encontrar y b será el inverso. Este tipo de ecuaciones se llaman ecuaciones diofánticas y muchos ejercicios de congruencias se pueden trasladas a este tipo de ecuaciones. No obstante, estas ecuaciones quedan fuera del contenido del capítulo. Sin embargo, esto es también la expresión directa de la Identidad de Bezout o Lema de Bezout.

Lema 6.13 (Identidad de Bezout)

Sean a y m enteros existen b y n enteros tal que

$$a \cdot b + m \cdot n \equiv mcd(a, m).$$

La parte interesante es cómo encontrar dicho b y n y esto se hace mediante el algoritmo de Euclides. Este sirve también para calcular cual es el máximo común divisor de dos números.

El algoritmo consta de los siguientes pasos:

1. Se divide el número mayor entre el menor.
2. Se comprueba el resto de la división:
   - Si es cero (la división es exacta), el divisor es el mcd.
   - Si no es cero, repetimos el primer paso con el divisor y el resto.

Veamos un ejemplo para que queda todo más claro.

Ejemplo 6.8 Queremos calcular el mcd de 42 y 15. Para empezar hacemos

$$\begin{array}{r|l} 42 & 15 \\ \hline 12 & 2 \end{array}$$

Como la división no es exacta repetimos hasta obtener una exacta:

$$\begin{array}{r|l} 15 & 12 \\ \hline 3 & 1 \end{array} \quad \Longrightarrow \quad \begin{array}{r|l} 12 & 3 \\ \hline 0 & 4 \end{array}$$

Luego el mcd(42,15) = 3. ¿Cómo encontramos ahora b y n tal que $42b + 15n = 3$? Para ellos utilizaremos que el dividendo menos el divisor por el cociente da el resto. Así, de la segunda división sabemos que

$$15 - 12 \cdot 1 = 3.$$

Como la primera nos dice que $12 = 42 - 15 \cdot 2$ sustituimos el valor de 12. Así obtenemos

$$15 - (42 - 15 \cdot 2) \cdot 1 = 3 \quad \Longrightarrow \quad 15 - 42 + 15 \cdot 2 = 3 \quad \Longrightarrow \quad 42 \cdot (-1) + 15 \cdot 3 = 3.$$

Luego $b = -1$ y $n = 3$, aunque esta solución no es único y podemos encontrar más por otros procedimientos.

6.5 Algunas congruencias importantes y la propiedad cíclica

A parte de resolver los típicos ejercicios de congruencias, existen algunas que, sin ser preguntadas de forma explícita, su uso resulta muy conveniente.

Por ejemplo, gracias a las congruencias podemos conocer las últimas cifras de un número de forma sencilla. Por supuesto, esto solo es útil cuando el número es muy grande y no tenemos su expresión numérica completa para mirarlas.

Ejemplo 6.9 ¿En qué cifra termina $((2^3)^4)^5$? Pues haciendo congruencias módulo 10 tenemos que

$$((2^3)^4)^5 = (8^4)^5 = ((8^2)^2)^5 = (64^2)^5 \equiv (4^2)^5 \equiv 6^5 = 6^2 \cdot 6^2 \cdot 6 \equiv 6 \cdot 6 \cdot 6 = 36 \cdot 6 \equiv 36 \equiv 6$$

Al hacer congruencias módulo 10 obtenemos el resto de dividir entre 10 que es precisamente la última cifra. Pero en general podemos ir más allá:

Lema 6.14

Las últimas k cifras de un número n son $a_1a_2 \dots a_k$ si y solo si $n \equiv a_1a_2 \dots a_k \pmod{10^k}$.

Nota: *En el hipotético caso de que no estemos trabajando en base decimal deberemos cambiar el 10 por la base correspondiente.*

Otra congruencia que tiene cierto valor especial es la del 9, como nos indica el próximo lema.

Lema 6.15
Si las cifras de un número n suman k entonces

$$n \equiv k \pmod 9$$

Demostración La forma de ver que es cierto consiste en darse cuenta que si un número n tiene cifras $a_k a_{k-1} \dots a_1 a_0$ entonces, al estar estas cifras en base 10, tenemos que

$$n = a_k \cdot 10^k + a_{k-1} \cdot 10^{k-1} + \dots + a_1 \cdot 10 + a_0.$$

Aplicando módulo 9, como $10 \equiv 1$, nos queda

$$n \equiv a_k + a_{k-1} + \dots + a_1 + a_0 \pmod 9.$$

■

Esto sirve para probar los criterios de divisibilidad del 3 y del 9. Aunque procedimientos similares de descomponer el número en base 10 sirve para otros criterios (2, 4, 5, 8, 11,. . .). Podría ser interesante tratar de probarlos o incluso encontrar algún otro.

Por último, una propiedad que puede resultarnos útil es saber que los restos tienen un comportamiento cíclico al aplicar sucesivas potencias.

Lema 6.16
Los restos de dividir m^n entre k se repiten en un ciclo de longitud $l = |n_1 - n_2| \leq k$ donde n_1 y n_2 son los menores naturales distintos tal que $m^{n_1} \equiv m^{n_2} \pmod k$.

Una idea intuitiva de porque este hecho es cierto es que dichos restos son números que van desde 0 hasta $k-1$. Es decir, solo pueden tomar unos pocos valores. Pero el exponente n no tiene límite. Así, tras k aumentos de n, si no antes, no quedarán restos libres para elegir y se tendrá que repetir. Así, en un ciclo de longitud l tendremos que los restos potenciales se repiten cada l unidades, es decir, para $n_3 \in \mathbb{N}$ se tiene que

$$m^n \equiv m^{n+n_3 \times l} \pmod k.$$

Ejemplo 6.10 En módulo 7 tenemos que $2^1 \equiv 2$, $2^2 \equiv 4$, $2^3 \equiv 1$, $2^4 \equiv 2$, $2^5 \equiv 4$, $2^6 \equiv 1 \dots$ Luego

$$2^k \equiv \begin{cases} 1 \pmod 7 & \text{si } k \equiv 0 \pmod 3, \\ 2 \pmod 7 & \text{si } k \equiv 1 \pmod 3, \\ 4 \pmod 7 & \text{si } k \equiv 2 \pmod 3, \end{cases} \iff 2^k \equiv \begin{cases} 1 \pmod 7 & \text{si } k = 3n \text{ (múltiplo de 3)}, \\ 2 \pmod 7 & \text{si } k = 3n+1, \\ 4 \pmod 7 & \text{si } k = 3n+2. \end{cases}$$

Así de forma directa podemos saber que como $2021 \equiv 2 \pmod 3$, entonces $2^{2021} \equiv 4 \pmod 7$.

6.6 Principales teoremas

Aunque la ciclicidad de es útil, hay ocasiones donde estos ciclos son muy grandes y no resultan nada prácticos. Es por eso que para estos casos podremos hacer uso de herramientas más poderosas como la que nos enuncia el siguiente teorema propuesto por Pierre de Fermat en 1636.

Teorema 6.1 (Pequeño teorema de Fermat)

Si p es un número primo y a es entero, entonces

$$a^p \equiv a \pmod{p}$$

Este mismo teorema, cuando $p \nmid a$ podemos escribirlo como

$$a^{p-1} \equiv 1 \pmod{p}.$$

En este caso, $a \cdot a^{p-2} \equiv 1$, luego $a^{-1} \equiv a^{p-2}$. Si bien este tal vez no es el inverso más pequeño que podemos encontrar, sí que es una forma de calcular al menos uno sin necesidad de aplicar el algoritmo de Euclides.

Con estos resultados seremos capaces de resolver algunos de los problemas anteriormente propuestos con mayor agilidad, pero también podremos resolver nuevos como en el siguiente ejemplo.

Ejemplo 6.11 Ahora sin aplicar ciclos podemos llegar a saber que

$$2^{2021} = 2^{(6\cdot 336+5)} = (2^6)^{336} \cdot 2^5 \equiv 1^{336} \cdot 2^5 \equiv 2^5 \equiv 32 \equiv 4 \pmod{7}.$$

Por otro lado, otro famoso teorema que podemos aplicar cuando la base es prima es el siguiente:

Teorema 6.2 (Teorema de Wilson)

Si p es un número primo, entonces

$$(p-1)! \equiv p-1 \equiv -1 \pmod{p}$$

Finalmente, aunque no vayamos a hacer uso de él en este capítulo, conviene enunciar el que probablemente sea el teorema más importante de la aritmética modular.

Teorema 6.3 (Teorema de Euler-Fermat)

Si el mcd$(a, m) = 1$, entonces $a^{\varphi(m)} \equiv 1 \pmod{m}$.

Aquí tenemos un resultado mucho más potente que el enunciado por el Pequeño Teorema de Fermat. Este se puede aplicar no solo en módulos primos, sino en cualquiera. Aunque requiere conocer la función φ («phi») de Euler. Aunque no es objetivo ya de este capítulo, $\varphi(m)$ es el número de naturales menores que m coprimos con él. Aunque para ahorrarnos cuenta presenta tres propiedades interesantes:

1. $\varphi(m \cdot n) = \varphi(m)\varphi(n)$ si mcd$(m, n) = 1$.
2. $\varphi(p) = p - 1$ si p es primo, obteniéndose así el Pequeño Teorema de Fermat.
3. $\varphi(p^k) = (p-1)p^{k-1}$ si p es primo.

6.7 Sistemas de congruencias

Hasta ahora hemos resuelto congruencias sencillas con una sola ecuación. Por ejemplo $n \cong 3 \pmod{6}$ tiene por soluciones: 3, 9, 15, -3, -9. . . En general todas las soluciones son de la forma $\pm 6k+3$. Sin embargo estas son ecuaciones muy simples y es frecuente encontrarse con situaciones donde se juntan varias condiciones que restringen el número de soluciones. Así que vamos a ver algunas formas de resolver sistemas de congruencias:

Proposición 6.4

$$\begin{cases} n \equiv k \pmod{a_1} \\ n \equiv k \pmod{a_2} \\ \vdots \\ n \equiv k \pmod{a_k} \end{cases} \Rightarrow n \equiv k \pmod{mcm(a_1, a_2, \ldots, a_k)}$$

Aunque esta primera propiedad es sencilla ya nos permite resolver problemas como el siguiente:

Problema 6.1 En una escalera, si bajamos los peldaños de 2 en 2 nos sobra 1, si los bajamos de 3 en 3 nos sobran 2, si los bajamos de 4 en 4 nos sobran 3, si los bajamos de 5 en 5 nos sobran 4, si los bajamos de 6 en 6 nos sobran 5 y de 7 en 7 no sobra ninguno. ¿Cuántos peldaños tiene como mínimo la escalera?

Solución *El primer paso es darse cuenta que en realidad casi todas las n son congruentes al mismo valor. Así:*

$$\begin{cases} n \equiv 1 \pmod 2 \\ n \equiv 2 \pmod 3 \\ n \equiv 3 \pmod 4 \\ n \equiv 4 \pmod 5 \\ n \equiv 5 \pmod 6 \\ n \equiv 0 \pmod 7 \end{cases} \Rightarrow \begin{cases} n \equiv -1 \pmod 2 \\ n \equiv -1 \pmod 3 \\ n \equiv -1 \pmod 4 \\ n \equiv -1 \pmod 5 \\ n \equiv -1 \pmod 6 \\ n \equiv 0 \pmod 7 \end{cases}$$

Aplicando ahora la Proposición 6.4 llegamos a que $n \equiv -1$ módulo 60. Es decir, $n + 1$ es múltiplo de 60. Los posibles n son por tanto $59, 119, 179 \ldots$ Pero como además debe ser múltiplo de 7, debe tener 119 peldaños.

Teorema 6.4 (Teorema chino del resto)

Sean $p_1, p_2, \ldots, p_k$ enteros coprimos entre sí dos a dos, entonces

$$\begin{cases} x \equiv a_1 \pmod{p_1} \\ x \equiv a_2 \pmod{p_2} \\ \vdots \\ x \equiv a_k \pmod{p_k} \end{cases}$$

tiene una única solución módulo $p_1 \cdot p_2 \cdots p_k$.

Y dicha solución es

$$x = \sum_{i=i}^{k} a_i s_i N_i$$

donde s_i se obtiene de la identidad de Bezout tal que

$$r_i p_i + s_i N_i = 1 \qquad \text{y} \qquad N_i = \frac{p_1 \cdot p_2 \cdots p_k}{p_i}.$$

Aunque es algo farragoso, lo normal será tener unas pocas ecuaciones en el sistema, 2 o 3 como mucho. De esta forma, no suele llevar muchos pasos. Un ejemplo de aplicación de este teorema se esconde detrás del siguiente enunciado:

Ejemplo 6.12 Proponle a un amigo que piense un número entero positivo menor que 1000 y que, tras dividirlo por 7, por 11 y por 13, te diga los respectivos restos a, b y c. Entonces tú les dirás que su número es el resto de dividir por 1001 el número

$$715a + 364b + 924c.$$

¿De dónde salen estos tres números? Pues salen de aplicar el Teorema chino del resto.

6.8 Problemas de olimpiadas matemáticas

A continuación vamos a mostrar y resolver un par de problemas de olimpiada donde vamos a juntar todo lo visto a lo largo de este capítulo.

Problema 6.2 (Olimpiada Matemática Española, Fase Nacional, Ciudad Real 2004). ¿Existe alguna potencia de 2 que al escribirla en el sistema decimal tenga todos sus dígitos distintos de cero y sea posible reordenar los mismos para formar con ellos otra potencia de 2? Justificar la respuesta.

Solución *En un primer momento puede parecernos que poco tiene que ver con la aritmética modular. Sin embargo eso de las cifras puede recordarnos a algunaa congruencia que hemos visto.*

Para empezar vamos a suponer que existen esas dos potencias con las mismas cifras. Llamémoslas 2^n *y* 2^m *con* $n < m$*. Como tienen las mismas cifras entonces*

$$2^n \equiv 2^m \pmod 9,$$

es decir

$$2^n - 2^m = 2^n(1 - 2^{m-n}) \equiv 0 \pmod 9.$$

Como $2^n(1 - 2^{m-n})$ *es múltiplo de 9 y* 2^n *no lo es*[1]*, entonces*

$$1 \equiv 2^{m-n} \pmod 9.$$

Veamos ahora si es posible que $2^{m-n} \equiv 1 \pmod 9$*. Antes de nada, como son números distintos y tienen el mismo número de cifras sabemos que*

$$1 < \frac{2^m}{2^n} < 10 \quad \Longrightarrow \quad 0 < m - n < \log_2 10 \approx 3,3219$$

Luego $m - n$ *puede valer* 1, 2 *o* 3*. Sin embargo, tanto* 2^1*, como* 2^2 *y* 2^3 *no son congruentes con 1 módulo 9. Por lo tanto, no existe tal potencia.*

Problema 6.3 (Olimpiada Matemática Española, Fase Nacional, 1994). Una oficina de turismo realiza una encuesta sobre el tiempo en seis regiones a lo largo de un año, obteniendo como resultado el Cuadro 6.3.

Región	Soleados o lluviosos	Inclasificables
A	336	29
B	321	44
C	335	30
D	343	22
E	329	36
F	330	35

Cuadro 6.3: Registro metereológico por regiones.

[1]El número no tiene más que al 2 como factor n veces y a ningún 3.

La persona encargada de la encuesta tiene esos datos más detallados aunque no los haya compartido. Se da cuenta de que, prescindiendo de una de las regiones, el número de días lluviosos pasa a ser la tercera parte del de días soleados. ¿Cuál es la región que omite para obtener dicho resultado?

Solución *Fijémonos solo en los datos de días soleados o lluviosos, omitiendo los inclasificables que no juegan ningún papel en este problema más allá de justificar el resto de días hasta 365. El enunciado nos dice que los soleados son el triple que los lluviosos. Luego si llamamos n a los lluviosos, los soleados son $3n$ y soleados o lluviosos hacer un total de $4n$, múltiplo de 4.*

Así, módulo 4 tenemos

$$336 \equiv 0 \qquad 335 \equiv 3 \qquad 329 \equiv 1$$
$$321 \equiv 1 \qquad 343 \equiv 3 \qquad 330 \equiv 2$$

Si sumamos todas las regiones obtenemos

$$336 + 321 + 335 + 343 + 329 + 330 \equiv 0 + 3 + 1 + 1 + 3 + 2 \equiv 10 \equiv 2 \pmod 4.$$

Luego para que la suma quede múltiplo de cuatro, es decir congruente con cero, la única posibilidad omitiendo una única región sería prescindir de la región F.

Ejercicios Propuestos

1. ¿Es 53 228 916 divisible por 156?

2. ¿Es 5 089 050 divisible por 220?

3. ¿Cuánto vale la cifra α para que $48\,\alpha 83\,332$ sea divisible por 26?

4. ¿Para qué valores de n el número $3^{6n} + 5^{6n}$ es divisible por 13?

5. Prueba que 3^{100} es la suma de 9 enteros consecutivos.

6. Prueba que $p^2 \equiv 1 \pmod{24}$ si p es un primo mayor que 3.

7. Hallar el resto de dividir por 7 el número $5555^{2222} + 2222^{5555}$.

8. ¿Son divisibles por 5 las expresiones $n^5 - n$, $n^5 - 1$ y $n^4 - 1$?

9. Resuelve el sistema de ecuaciones en congruencias

$$\begin{cases} 2x + 3 \equiv 1 \pmod{11}, \\ 3x \equiv 5 \pmod{8}. \end{cases}$$

10. Resuelve el sistema de ecuaciones en congruencias

$$\begin{cases} x \equiv 3 \pmod{19}, \\ x \equiv 7 \pmod{13}. \end{cases}$$

Bibliografía Adicional

1. Engel, A. (1998). Number Theory. *Problem-Solving Strategies*. Editorial Springer, 117-160.

2. Guitérrez Jiménez, J. M. & Lanchares Barrasa, V. (2010). *Elementos de matemática discreta*. Servicio de Publicaciones de la Universidad de La Rioja. https://dialnet.unirioja.es/servlet/libro?codigo=424510

CAPÍTULO 7

7

ARITMÉTICA MODULAR - PARTE 2

Miguel Marañón Grandes
Universidad de La Rioja

Palabras clave

- *Módulo*
- *Resto*
- *Congruencia*
- *Teorema de Euler*
- *Pequeño Teorema de Fermat*
- *Criterios de divisibilidad*
- *Ecuación diofántica*
- *Identidad de Bézout*

¿Te imaginas qué ocurriría si el tiempo no se midiese cíclicamente? No podríamos hablar de a qué hora nos acostaríamos, qué día de la semana iríamos al cine, qué día del mes nos pagarían la nómina o el día de nuestro cumpleaños. En su lugar, la humanidad tendría que haber establecido un único momento de referencia a partir del cual se mediría el tiempo transcurrido. En vez de, pongamos por caso, quedar a las ocho y media con nuestros amigos, tendríamos que acordar cuántos segundos después del nacimiento de Cristo tendría lugar nuestra reunión. ¡Todo un caos!

El hecho de que, por suerte, el tiempo se mida cíclicamente se debe en parte gracias a la existencia de la aritmética modular, la cual considera los restos que se obtienen al tomar como divisor un determinado número (al que llamamos *módulo*). De ahí que, como un día tiene 24 horas, estas se establezcan con números comprendidos entre el 0 y el 23, reiniciándose su contador a medianoche. Lo mismo ocurre con las semanas, los meses, los años... No es casualidad que, por ello, a la aritmética modular, que fue introducida por primera vez en 1801 por el matemático Carl Friedrich Gauss, también se la conozca como la aritmética del reloj.

En este tema, aprenderemos a resolver ecuaciones diofánticas (esto es, ecuaciones lineales con coeficientes y soluciones enteras) que nos servirán como herramienta para resolver ecuaciones en congruencias y estudiaremos las propiedades de los conjuntos de restos módulo n (denotados por $\mathbb{Z}_n$), lo cual nos permitirá calcular restos de divisiones cuyos dividendos son números muy grandes que se pueden expresar en forma de potencia (en particular, hallaremos un método para determinar las últimas cifras de ciertas potencias con exponente muy grande) y entender el porqué de los criterios de divisibilidad de los números enteros, entre otras cosas.

7.1 Introducción

Nuestra mente ha ideado numerosos conceptos cuya naturaleza es cíclica: la hora del día, el día de la semana o del mes, las notas musicales... Todos ellos se contabilizan de forma que, en algún momento, su contador se pone a cero; en los ejemplos mencionados, una hora después de las 23 horas de un día son las 0 horas del día siguiente, después del domingo viene el lunes, el día después del 31 de agosto es el 1 de septiembre y la nota posterior al si vuelve a ser el do en la escala musical.

Pensando un poco, esto hace que en muchas ocasiones nos interese conocer el resto que un número deja al ser dividido por otro más que cualquier otro aspecto de la división. Si en este preciso momento es medianoche, dentro de 100 horas serán las 4 de la madrugada, ya que el resto que se obtiene al dividir 100 entre 24 (las horas que tiene el día) es precisamente 4. Del mismo modo, si hoy es martes 10 de agosto, el próximo año este mismo día caerá en miércoles, ya que al dividir los 365 días del año entre los 7 días de la semana, el resto es 1 (si el año que viene fuese bisiesto, con 366 días, el resto sería 2 y caería en jueves).

Figura 7.1: Carl Friedrich Gauss (1777–1855).

Estas ideas no pasaron inadvertidas a Carl Friedrich Gauss (Figura 7.1), también conocido como *el Príncipe de las Matemáticas* y considerado como el padre de la arimética modular, quien en el primer capítulo de su libro *Disquisitiones arithmeticae*, escrito en 1798 y publicado en 1801, introdujo definiciones y notaciones nunca vistas hasta la fecha fundamentadas en el concepto de *congruencia*.

Definición 7.1 (Relación de congruencia)

Dado un número entero n, dos números enteros a y b se encuentran en la misma **clase de congruencia** *módulo n si ambos dejan el mismo resto al dividirlos entre n o, equivalentemente, si $a-b$ es múltiplo de n. Esto se denota $a \equiv b \pmod{n}$.*

Ejemplo 7.1 Observamos que $63 \equiv 83 \pmod{10}$, ya que 63 y 83 dejan el mismo resto (que es 3) al dividirlos entre 10 o, equivalentemente, $63-83=-20$ es un múltiplo de 10.

La noción de módulo como divisor, unida al hecho de que el concepto de congruencia es compatible con las operaciones usuales de la aritmética debido a la gran analogía existente entre ella y la igualdad, permitió la introducción de la **aritmética modular**, la cual a la sazón acabó produciendo un gran impacto en el desarrollo de la teoría de números. Como consecuencia de la naturaleza cíclica de las horas del día, pues habitualmente se cuentan en módulo 12 o 24, a la aritmética modular también se la conoce como la *aritmética del reloj*.

La aritmética modular tiene bastantes aplicaciones. Una de las que más nos van a convenir a nosotros de cara a preparar olimpiadas matemáticas es la de calcular **restos potenciales** (sin necesidad de hacer la división). Un ejercicio tipo podría ser calcular la última cifra del número 7^{93} (o, equivalentemente, calcular el resto

que se obtiene al dividir 7^{93} entre 10). Sin saber nada del tema, aún podríamos intentar llegar a la solución estableciendo una conjetura, como la que se infiere del Cuadro 7.1. Se puede intuir un carácter cíclico que habrá que demostrar formalmente.

k	7^k	Última cifra
1	7	7
2	49	9
3	343	3
4	2.401	1
5	16.807	7
6	117.649	9
7	823.543	3
8	5.764.801	1
9	40.353.607	7
⋮	⋮	⋮

Cuadro 7.1: Última cifra de los números de la forma 7^k, con $k \in \mathbb{N}$.

Según lo observado, parece ser que los números de la forma 7^{4k-3}, con $k \in \mathbb{N}$, terminan en 7. Si esto fuera cierto, se podría deducir que 7^{93} termina en 7, puesto que $93 = 4 \cdot 24 - 3$. Sin embargo, esta conjetura hay que demostrarla, bien sea por inducción o por cualquier otro método válido; nosotros lo haremos en cuanto aprendamos algunas propiedades elementales de las clases de congruencia.

Otra aplicación que será interesante que conozcamos consiste en establecer **criterios de divisibilidad** para determinados números (es decir, saber si un número es múltiplo de otro sin necesidad de realizar la división). Seguramente recuerdes que un número es múltiplo de 3 si y solo si la suma de sus cifras es múltiplo de 3, que es múltiplo de 9 cuando la suma de sus cifras también lo es, que es múltiplo de 11 cuando la suma de las cifras en posición impar menos la de las cifras en posición par resulta ser un múltiplo de 11, y algún criterio de divisibilidad más; pues bien, todos ellos se pueden probar fácilmente usando las propiedades de las clases de congruencia.

Las aplicaciones de la aritmética modular no se terminan ahí. Entre otras cosas, hoy en día se emplea además en la teoría de la codificación, en criptografía (de hecho, forma parte de la base del algoritmo RSA para el cifrado de mensajes) y para definir dígitos de control para la detección de errores en identificadores como los siguientes:

- **NIF (Número de Identificación Fiscal).** ¿Sabías que la letra que acompaña a tu DNI viene determinada por los ocho dígitos precedentes? En efecto, se obtiene hallando el resto de dividir el número del DNI entre 23 (dicho de otro modo, *reduciéndolo* a módulo 23) y aplicando a este resto la siguiente conversión:

$0 \longrightarrow T$	$6 \longrightarrow Y$	$12 \longrightarrow N$	$18 \longrightarrow H$
$1 \longrightarrow R$	$7 \longrightarrow F$	$13 \longrightarrow J$	$19 \longrightarrow L$
$2 \longrightarrow W$	$8 \longrightarrow P$	$14 \longrightarrow Z$	$20 \longrightarrow C$
$3 \longrightarrow A$	$9 \longrightarrow D$	$15 \longrightarrow S$	$21 \longrightarrow K$
$4 \longrightarrow G$	$10 \longrightarrow X$	$16 \longrightarrow Q$	$22 \longrightarrow E$
$5 \longrightarrow M$	$11 \longrightarrow B$	$17 \longrightarrow V$	

- **ISBN (International Standard Book Number).** Los códigos identificativos de los libros editados también echan mano de las clases de congruencia. Estos códigos son de la forma:

$$x_1x_2\text{–}x_3x_4x_5x_6\text{–}x_7x_8x_9\text{–}y.$$

El primer bloque, x_1x_2, es un indicativo geográfico; el segundo, $x_3x_4x_5x_6$, corresponde a la editorial; el tercero, $x_7x_8x_9$, se refiere al libro; y el último dígito, y, es el de control y se calcula de la siguiente forma:

$$y = \sum_{i=1}^{9} i \cdot x_i \pmod{11}.$$

Si $y = 10$, el dígito de control se sustituye por la letra X.

- **Número de cuenta corriente.** Por último, veamos cómo se establecen los dígitos de control en los códigos de cuenta corriente asociados a las cuentas bancarias. Dichos códigos siempre constan de 20 cifras y son de la forma:

$$a_1a_2a_3a_4\text{–}b_1b_2b_3b_4\text{–}xy\text{–}c_1c_2c_3c_4c_5c_6c_7c_8c_9c_{10},$$

donde $a_1a_2a_3a_4$ representa la entidad bancaria; $b_1b_2b_3b_4$, la oficina bancaria; $c_1c_2c_3c_4c_5c_6c_7c_8c_9c_{10}$, el número de cuenta; y x e y son los dígitos de control que se calculan de la siguiente manera:

$$x = 7a_1 + 3a_2 + 6a_3 + a_4 + 2b_1 + 4b_2 + 8b_3 + 5b_4 \pmod{11},$$
$$y = 10c_1 + 9c_2 + 7c_3 + 3c_4 + 6c_5 + c_6 + 2c_7 + 4c_8 + 8c_9 + 5c_{10} \pmod{11}.$$

Si el resultado de alguna de las anteriores operaciones para x o y fuera igual a 10, pondríamos un 1 como dígito de control en su lugar.

7.2 Ecuaciones diofánticas

En ocasiones, se nos plantean ecuaciones con coeficientes enteros para las cuales solo tiene sentido que sus soluciones sean también enteras. A este tipo de ecuaciones se las denomina **ecuaciones diofánticas**, pues Diofanto de Alejandría (Figura 7.2), a quien deben su nombre en su honor, fue de los primeros en dedicarse al estudio de sus propiedades en su obra *Arithmetica*, la cual ejerció una gran influencia en el desarrollo del álgebra entre los árabes y en la teoría de números moderna.

Figura 7.2: Diofanto de Alejandría fue un matemático de la antigua Grecia del siglo III d.C. que es considerado como el padre del álgebra, ya que generalmente se le atribuye la introducción del simbolismo en las matemáticas.

Nota: *Poco se conoce de la vida de Diofanto, pero hay un dato de la misma del que estamos muy seguros: la edad a la que falleció. Esto es así porque en su epitafio aparecía escrito el siguiente problema:*

"Transeúnte, esta es la tumba de Diofanto: es él quien con esta sorprendente distribución te dice el número de años que vivió. Su niñez ocupó la sexta parte de su vida; después, durante la doceava parte su mejilla se cubrió con el primer bozo. Pasó aún una séptima parte de su vida antes de tomar esposa y, cinco años después, tuvo

un precioso niño que, una vez alcanzada la mitad de la edad de su padre, pereció de una muerte desgraciada. Su padre tuvo que sobrevivirle, llorándole, durante cuatro años. De todo esto se deduce su edad".

Llamando x a la edad a la que murió Diofanto, la siguiente ecuación resuelve el problema:

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

*Resolviéndola, te resultará fácil comprobar que Diofanto vivió **84 años**.*

Definición 7.2 (Ecuación diofántica)

Una **ecuación diofántica** *es una ecuación algebraica con coeficientes enteros en la que aparecen varias variables cuyas soluciones son números enteros. Es decir, resolver una ecuación diofántica consiste en determinar qué números enteros la cumplen. En particular, las* ecuaciones diofánticas lineales *de n incógnitas son las de la forma:*

$$\sum_{i=1}^{n} a_i x_i = m,$$

con $a_1, a_2 \ldots, a_n, m \in \mathbb{Z}$.

A lo largo de todo el capítulo, solamente consideraremos las ecuaciones diofánticas lineales de 2 incógnitas; es decir, las de la forma

$$ax+by=m, \text{ con } a,b,m\in\mathbb{Z}$$

Las usaremos no solo para resolver problemas, sino además como herramienta para resolver ecuaciones en congruencias del tipo $px \equiv q \pmod{m}$, con $p, q, m \in \mathbb{Z}$.

Estas ecuaciones pueden tener infinitas soluciones (enteras)... o pueden no tener ninguna. Para discernir si tienen solución o no, los siguientes resultados serán de mucha utilidad.

Lema 7.1 (de Bézout)

Si a y b son números enteros diferentes de cero con máximo común divisor d, entonces existen enteros x e y tales que:

$$ax+by=d.$$

*A esta identidad se le denomina **identidad de Bézout**.*

Lema 7.2 (de Euclides)

Si $n \mid ab$ y $\text{m. c. d.}(n,a)=1$, entonces necesariamente $n \mid b$.

Demostración Como n y a son coprimos, por el Lema 7.1 (de Bézout) sabemos que existen $x, y \in \mathbb{Z}$ tales que $ax+ny=1$. Multiplicando por b ambos miembros, se tiene que $abx+nyb=b$. Por otro lado, como $n \mid ab$, existe $k \in \mathbb{Z}$ tal que $nk=ab$, por lo que $nkx+nyb=b$. Equivalentemente, $n(kx+yb)=b$, por lo que necesariamente $n \mid b$.

Teorema 7.1

Una ecuación diofántica lineal de la forma $ax + by = m$ tiene solución si y solo si el máximo común divisor de a y b es un divisor de m. Además, si esta ecuación diofántica tiene solución, necesariamente tiene infinitas soluciones y todas son de la forma:

$$\begin{cases} x = x_0 + \lambda \frac{b}{d} \\ y = y_0 - \lambda \frac{a}{d} \end{cases}, \qquad \lambda \in \mathbb{Z}, \tag{7.1}$$

donde $d = \text{m. c. d.}(a, b)$ y (x_0, y_0) es una solución particular de la ecuación.

Demostración Supongamos que la ecuación

$$ax + by = m \tag{7.2}$$

tiene solución entera. Entonces, existen x_0 e y_0 tales que $ax_0 + by_0 = m$. Como $d = \text{m. c. d.}(a, b)$ es divisor común de a y b, entonces $a = a_1 d$ y $b = b_1 d$, con $a_1, b_1 \in \mathbb{Z}$. Por tanto,

$$m = ax_0 + by_0 = a_1 dx_0 + b_1 dy_0 = (a_1 x_0 + b_1 y_0)d,$$

por lo que $d \mid m$.

Recíprocamente, supongamos que $d \mid m$. Entonces, existe $k \in \mathbb{Z}$ tal que $m = kd$. Por otra parte, por el Lema 7.1 (de Bézout) existen $\alpha, \beta \in \mathbb{Z}$ tales que $d = \alpha a + \beta b$. Al multiplicar los dos miembros de esta identidad por k, resulta que $kd = k(\alpha a + \beta b) = (k\alpha)a + (k\beta)b = m$, por lo que $(k\alpha, k\beta)$ es una solución de la ecuación diofántica. De hecho,

$$\begin{cases} x_0 = k\alpha = \dfrac{m}{d} \cdot \alpha \\ y_0 = k\beta = \dfrac{m}{d} \cdot \beta \end{cases}, \qquad \alpha, \beta \in \mathbb{Z},$$

es solución particular de la ecuación (7.2).

Finalmente, supongamos que (x_0, y_0) es solución particular de la ecuación (7.2). Por tanto, se cumple que $ax_0 + by_0 = m$. Notemos que, entonces, las expresiones de la ecuación (7.1) también son solución de la ecuación (7.2):

$$a\left(x_0 + \frac{b}{d} \cdot \lambda\right) + b\left(y_0 - \frac{a}{d} \cdot \lambda\right) = ax_0 + by_0 + a \cdot \frac{b}{d} \cdot \lambda - b \cdot \frac{a}{d} \cdot \lambda = m.$$

Por consiguiente, falta por probar que todas las soluciones de la ecuación (7.2) son de la forma descrita en la ecuación (7.1). En efecto, si (x, y) es la solución general de la ecuación (7.2), tenemos que se cumplen las dos ecuaciones siguientes:

$$ax + by = m,$$

$$ax_0 + by_0 = m.$$

Al restar ambas ecuaciones, se obtiene que $a(x - x_0) + b(y - y_0) = 0$, o equivalentemente

$$a(x - x_0) = b(y_0 - y). \tag{7.3}$$

Dividiendo ambos miembros de la ecuación (7.3) entre d, se tiene que $\frac{a}{d}(x - x_0) = \frac{b}{d}(y_0 - y)$. Por tanto, $\frac{a}{d}$ divide a $\frac{b}{d}(y_0 - y)$. Pero $\frac{a}{d}$ y $\frac{b}{d}$ son coprimos (ya que $d = \text{m. c. d.}(a, b)$), por lo que, por el Lema 7.2 (de Euclides), se deduce que $\frac{a}{d}$ ha de dividir a $(y_0 - y)$. Esto nos lleva a que debe existir $\lambda \in \mathbb{Z}$ tal que:

$$y_0 - y = \lambda \frac{a}{d} \Longrightarrow y = y_0 - \lambda \frac{a}{d}.$$

Sustituyendo este valor de y en la ecuación (7.3), se llega fácilmente a que

$$x = x_0 + \lambda\frac{b}{d}, \quad \lambda \in \mathbb{Z}.$$

■

Por tanto, según nos indica el Teorema 7.1, encontrar las soluciones de una ecuación diofántica lineal de 2 incógnitas se puede reducir a hallar una solución particular (x_0, y_0) de la ecuación (hallando previamente los coeficientes enteros α y β que aparecen en la demostración del teorema). Con este fin, el algoritmo de Euclides resulta ser tremendamente útil, pues no solo permite encontrar el máximo común divisor de a y b para determinar si la ecuación tiene solución, sino que además nos proporciona un método para llegar a la identidad de Bézout y, a partir de ella, llegar a una solución particular. Puesto que dicho método puede llegar a ser demasiado intrincado y complicado de explicar para el caso general, lo aprenderemos a través de la estrategia seguida en la resolución del Problema 7.1.

Nota: *Seguramente ya conozcas un procedimiento para calcular el máximo común divisor de un par de números enteros: el de descomponerlos en factores primos y tomar de esos factores solo los comunes con el menor exponente para después multiplicarlos. Pues bien, otro método igual de válido es el algoritmo de Euclides. Consiste en seguir las siguientes reglas:*

1. *Si* $b = 0$*, entonces* $\mathrm{m.\,c.\,d.}(a, b) = a$ *y el algoritmo termina.*
2. *En otro caso,* $\mathrm{m.\,c.\,d.}(a, b) = \mathrm{m.\,c.\,d.}(b, r)$*, donde* r *es el resto de dividir* a *entre* b*. Para calcular* $\mathrm{m.\,c.\,d.}(b, r)$*, se utilizan estas mismas reglas.*

Este procedimiento suele quedar recogido en un esquema como el siguiente, en el que $q_1, q_2, q_3, \ldots, q_k$ *son los cocientes que se van obteniendo y* $r_1, r_2, r_3, \ldots, r_{k-1}$*, los restos:*

	q_1	q_2	q_3	$\cdots$	q_{k-1}	q_k
a	b	r_1	r_2	$\cdots$	r_{k-2}	$\mathbf{r_{k-1}}$
r_1	r_2	r_3	$\cdots$	r_{k-1}	0	

Recordemos que $a = bq_1 + r_1$*,* $b = r_1q_2 + r_2$*,* $r_k = 0$ *y* $r_{i-1} = r_iq_{i+1} + r_{i+1}$*, con* $i = 2, \ldots, k-1$*. Se tendría que* $\mathrm{m.\,c.\,d.}(a, b) = r_{k-1}$*. A modo de ejemplo,*

$$\mathrm{m.\,c.\,d.}(2366, 273) = \mathrm{m.\,c.\,d.}(273, 182) = \mathrm{m.\,c.\,d.}(182, 91) = \mathrm{m.\,c.\,d.}(91, 0) = 91,$$

siendo el esquema asociado:

	8	1	2
2366	273	182	**91**
182	91	0	

Problema 7.1 Encuentra los valores enteros $10 \leq x \leq 20$ para los que tiene solución la ecuación diofántica $84x + 990y = c$. Resuélvela en uno de los casos encontrados.

Solución *En primer lugar, aplicamos el algoritmo de Euclides con los números* 990 *y* 84*:*

	11	1	3	1	2
990	84	66	18	12	**6**
66	18	12	6	0	

Para que la ecuación diofántica tenga solución, c tiene que ser múltiplo de $\mathrm{m.\,c.\,d.}(84, 990) = 6$. *Por tanto, c sólo puede valer* 12 *o* 18. *Tomaremos* $c = 12$*; es decir, resolveremos la ecuación diofántica* $84x + 990y = 12$. *Para ello, primero hemos de hallar una solución particular* (x_0, y_0) *usando la información obtenida en el algoritmo anterior, mediante la cual podemos asegurar que:*

$$990 = 11 \cdot 84 + 66 \Longrightarrow 66 = 990 - 11 \cdot 84; \tag{7.4}$$

$$84 = 66 + 18 \Longrightarrow 18 = 84 - 66; \tag{7.5}$$

$$66 = 3 \cdot 18 + 12 \Longrightarrow 12 = 66 - 3 \cdot 18; \tag{7.6}$$

$$18 = 12 + 6 \Longrightarrow 6 = 18 - 12. \tag{7.7}$$

Sustituyendo la identidad (7.4) en (7.5), se tiene que:

$$18 = 84 - (990 - 11 \cdot 84) \Longrightarrow 18 = 12 \cdot 84 - 990. \tag{7.8}$$

Sustituyendo las identidades (7.4) y (7.8) en (7.6), se tiene que:

$$12 = 990 - 11 \cdot 84 - 3 \cdot (12 \cdot 84 - 990) \Longrightarrow 12 = 4 \cdot 990 - 47 \cdot 84. \tag{7.9}$$

Y al fin, sustituyendo las identidades (7.8) y (7.9) en (7.7), se tiene que:

$$6 = 12 \cdot 84 - 990 - (4 \cdot 990 - 47 \cdot 84) \Longrightarrow 59 \cdot 84 - 5 \cdot 990 = 6. \tag{7.10}$$

Notemos que la identidad (7.10) es la identidad de Bézout correspondiente a los coeficientes de la ecuación diofántica. A partir de ella, es fácil deducir que $x_0 = \dfrac{12}{6} \cdot 59 = 118$ *e* $y_0 = \dfrac{12}{6} \cdot (-5) = -10$ *determinan una solución particular de la misma. Así, las soluciones son de la forma:*

$$\begin{cases} x = 118 + \lambda \frac{990}{6} \\ y = -10 - \lambda \frac{84}{6} \end{cases}, \quad \lambda \in \mathbb{Z} \Longrightarrow \begin{cases} x = 165\lambda + 118 \\ y = -14\lambda - 10 \end{cases}, \quad \lambda \in \mathbb{Z}.$$

7.3 Congruencias

Recordemos que dos enteros a y b se dicen ***congruentes*** (o que se encuentran en la misma ***clase de congruencia***) módulo $n \in \mathbb{Z}$ si n es un divisor de la diferencia de ambos:

$$a \equiv b \pmod{n} \iff n \mid a - b \iff \exists k \in \mathbb{Z} \colon a - b = k \cdot n.$$

Equivalentemente, dos enteros a y b son congruentes módulo $n \in \mathbb{Z}$ si dan el mismo resto al dividirlos entre n.

Algunas propiedades básicas de las clases de congruencia son las siguientes. Dados $a, b, c, d \in \mathbb{Z}$:

1. $a \equiv a \pmod{n}$ *(propiedad reflexiva).*
2. Si $a \equiv b \pmod{n}$, $b \equiv a \pmod{n}$ *(propiedad simétrica).*
3. Si $a \equiv b \pmod{n}$ y $b \equiv c \pmod{n}$, $a \equiv c \pmod{n}$ *(propiedad transitiva).*
4. Si $a \equiv b \pmod{n}$ y $k \in \mathbb{Z}$, $a + k \equiv b + k \pmod{n}$.
5. Si $a \equiv b \pmod{n}$ y $k \in \mathbb{Z}$, $ka \equiv kb \pmod{n}$.
6. Si $a \equiv b \pmod{n}$ y $k \in \mathbb{N}$, $a^k \equiv b^k \pmod{n}$.
7. Si $a \equiv b \pmod{n}$ y $c \equiv d \pmod{n}$, $a + c \equiv b + d \pmod{n}$.
8. Si $a \equiv b \pmod{n}$ y $c \equiv d \pmod{n}$, $a \cdot c \equiv b \cdot d \pmod{n}$.

Demostración Las propiedades 1, 2, 3, 4, 5 y 7 son fáciles de probar a partir de la definición y quedan propuestas al lector. La propiedad 6 también es sencilla de demostrar si se tiene en cuenta que $a^k - b^k = (a-b)\sum_{i=0}^{k-1} a^i b^{k-1-i}$. Por último, para la propiedad 8, supongamos que existen $k, k' \in \mathbb{Z}$ tales que $a-b = kn$ y $c-d = k'n$. Entonces, $a = b + kn$ y $c = d + k'n$. Por tanto, se tiene que:

$$ac - bd = (b+kn)(d+k'n) - bd = bd + k'bn + kdn + kk'n^2 - bd = n(k'b + kd + kk'n),$$

por lo que existe $K = k'b + kd + kk'n \in \mathbb{Z}$ tal que $ac - bd = Kn$. ■

Notemos que las tres primeras propiedades hacen que la relación de congruencia sea de equivalencia.

La definición que se muestra a continuación nos permitirá trabajar con las relaciones de congruencia de una forma mucho más cómoda.

Definición 7.3 (Conjunto de restos)

Definimos el **conjunto de restos** *módulo $n \in \mathbb{Z}$ como el conjunto $\mathbb{Z}_n = \{[0]_n, [1]_n, [2]_n, \ldots, [n-1]_n\}$, donde $[k]_n$ representa el subconjunto de todos los enteros que son congruentes con k módulo n. Notemos que $[a]_n = [b]_n$ si y solo si a y b dejan el mismo resto al dividirlos entre n.*

Ejemplo 7.2 En $\mathbb{Z}_7$ se cumple que $[9]_7 = [16]_7 = [23]_7 = [2]_7$ y $[-6]_7 = [8]_7 = [1]_7$.

Las propiedades de la aritmética de $\mathbb{Z}_n$ que describiremos ahora son fundamentales para operar en ella. Dados $[a]_n, [b]_n \in \mathbb{Z}_n$:

1. $[a]_n + [b]_n = [a+b]_n$.
2. $[a]_n \cdot [b]_n = [a \cdot b]_n$.
3. $[a^k]_n = ([a]_n)^k$, con $k \in \mathbb{N}$. Por abreviar la notación, escribiremos $([a]_n)^k = [a]_n^k$.

Las dos primeras propiedades están bien definidas debido a las dos últimas de las relativas a las clases de congruencia. La tercera propiedad es consecuencia inmediata de la segunda y en ocasiones es tremendamente útil para simplificar los cálculos, como se puede ver en el siguiente ejemplo.

Ejemplo 7.3 En $\mathbb{Z}_6$, $[7^{100}]_6 = [7]_6^{100} = [1]_6^{100} = [1^{100}]_6 = [1]_6$. No perdamos de vista que esto quiere decir que el resto que se obtiene al dividir 7^{100} entre 6 es 1. Para saber esto, no ha sido necesario realizar la división.

Hasta ahora, ninguno de los aspectos de $\mathbb{Z}_n$ que hemos estudiado nos resulta extraño o, al menos, inesperado. Sin embargo, las propiedades en cuanto a la multiplicación que pueden surgir en $\mathbb{Z}_n$ podrían ser muy distintas a las del conjunto de los números enteros $\mathbb{Z}$. Por lo pronto, los únicos elementos invertibles en $\mathbb{Z}$ (es decir, elementos para los cuales existe otro tal que al multiplicarlos el resultado es la unidad) son el 1 y el -1, pero en $\mathbb{Z}_n$ puede haber muchos más según el valor que tome el módulo $n \in \mathbb{Z}$.

Definición 7.4 (Elemento invertible, o unidad, en $\mathbb{Z}_n$)

Se dice que $[a]_n$ es un **elemento invertible** *(o* **unidad***) en $\mathbb{Z}_n$ si existe $[b]_n$ en $\mathbb{Z}_n$ tal que $[a]_n \cdot [b]_n = [1]_n$. Ese elemento $[b]_n$ será el* **inverso** *de $[a]_n$ en $\mathbb{Z}_n$ y se denota como $[a^{-1}]_n$.*

Ejemplo 7.4

a) En $\mathbb{Z}_7$, $[3^{-1}]_7 = [5]_7$, ya que $[3]_7 \cdot [5]_7 = [15]_7 = [1]_7$.

b) En $\mathbb{Z}_9$, $[4^{-1}]_9 = [7]_9$, ya que $[4]_9 \cdot [7]_9 = [28]_9 = [1]_9$.

Proposición 7.1

$[a]_n$ es invertible en $\mathbb{Z}_n$ si y solo si $\mathrm{m.\,c.\,d.}(a,n)=1$. *Además, en caso de que exista, su elemento inverso es único.*

Demostración Supongamos que $[a]_n$ es invertible en $\mathbb{Z}_n$. Entonces, debe existir $[b]_n \in \mathbb{Z}_n$ tal que:

$$[a]_n \cdot [b]_n = [1]_n \Longrightarrow [a]_n \cdot [b]_n - [1]_n = [0]_n \Longrightarrow [a\cdot b - 1]_n = [0]_n.$$

Por tanto, ha de existir $k \in \mathbb{Z}$ tal que $ab-1=kn$. Por otro lado, sea $d=\mathrm{m.\,c.\,d.}(a,n)$. Por ser d divisor común de a y n, existen $a', n' \in \mathbb{Z}$ tales que $a=da'$ y $n=dn'$. Por consiguiente,

$$da'b-1=kdn' \Longrightarrow da'b-dn'k=1 \Longrightarrow d(a'b-n'k)=1 \Longrightarrow d=1.$$

Para demostrar el recíproco, supongamos que $\mathrm{m.\,c.\,d.}(a,n)=1$. Por el Lema 7.1 (de Bézout), existen $x, y \in \mathbb{Z}$ tales que $ax+ny=1$. Tomando clases de congruencia módulo n, se tiene que:

$$[a\cdot x + n\cdot y]_n = [1]_n \Longrightarrow [a\cdot x]_n + [n\cdot y]_n = [1]_n \Longrightarrow [a\cdot x]_n = [1]_n \Longrightarrow [a]_n\cdot[x]_n = [1]_n,$$

por lo que $[a^{-1}]_n = [x]_n$ y $[a]_n$ es invertible en $\mathbb{Z}_n$.

Finalmente, para probar la unicidad del elemento inverso, supongamos que existen $[b]_n, [b']_n \in \mathbb{Z}_n$ tales que $[a]_n\cdot[b]_n=[1]_n$ y $[a]_n\cdot[b']_n=[1]_n$. Esto implica que:

$$[a]_n\cdot[b]_n = [a]_n\cdot[b']_n \Longrightarrow [a\cdot b]_n = [a\cdot b']_n \Longrightarrow [a\cdot(b-b')]_n = [0]_n.$$

Por tanto, debe existir $k \in \mathbb{Z}$ tal que $a(b-b')=kn$. De aquí se deduce que $n \mid a(b-b')$. Puesto que $\mathrm{m.\,c.\,d.}(a,n)=1$, por el Lema 7.2 (de Euclides) se tiene que $n \mid b-b'$, por lo que $b \equiv b' \pmod{n}$ y el elemento inverso es único.

■

Corolario 7.1

Si $[a]_n$ o $[b]_n$ son elementos invertibles en $\mathbb{Z}_n$ y $[a]_n\cdot[b]_n=[0]_n$, entonces o bien $[a]_n=[0]_n$ o $[b]_n=[0]_n$. Además, si $\mathrm{m.\,c.\,d.}(c,n)=1$ *y $[x]_n\cdot[c]_n=[y]_n\cdot[c]_n$ en $\mathbb{Z}_n$, entonces $[x]_n=[y]_n$ en $\mathbb{Z}_n$* (propiedad cancelativa del producto).

Demostración Supongamos, sin pérdida de generalidad, que $[a]_n$ es invertible en $\mathbb{Z}_n$. Entonces, por la Proposición 7.1, $\mathrm{m.\,c.\,d.}(a,n)=1$. Ahora, si $[a]_n\cdot[b]_n=[0]_n$, entonces $[a\cdot b]_n=[0]_n$ y, por tanto, existe $k\in\mathbb{Z}$ tal que $ab=kn$. Esto significa que $n \mid ab$. Pero por el Lema 7.1 (de Bézout), $n \mid b$, ya que a y n son coprimos. De aquí se sigue inmediatamente que $[b]_n=[0]_n$.

Para probar la propiedad cancelativa del producto, notemos que si $\mathrm{m.\,c.\,d.}(c,n)=1$, nuevamente por la Proposición 7.1 existe el inverso de $[c]_n$ en $\mathbb{Z}_n$, al que denotaremos por $[c^{-1}]_n$. Multiplicando por este elemento ambos miembros de la ecuación $[x]_n\cdot[c]_n=[y]_n\cdot[c]_n$, se llega a que:

$$[x]_n\cdot([c]_n\cdot[c^{-1}]_n) = [y]_n\cdot([c]_n\cdot[c^{-1}]_n) \Longrightarrow [x]_n\cdot[1]_n = [y]_n\cdot[1]_n \Longrightarrow [x]_n=[y]_n.$$

■

Nota: *Cuando tenemos dos elementos* ***no nulos*** *$[a]_n$ y $[b]_n$ que* ***no son invertibles*** *en $\mathbb{Z}_n$, puede darse el caso de que su producto sea nulo; es decir, que $[a]_n\cdot[b]_n=[0]_n$ aunque $[a]_n\neq[0]_n$ y $[b]_n\neq[0]_n$. Por ejemplo, en $\mathbb{Z}_6$ se cumple que $[2]_6\cdot[3]_6=[6]_6=[0]_6$. Notemos que esto nunca ocurre en el conjunto de los números enteros $\mathbb{Z}$.*

Definición 7.5 (Conjunto de unidades en $\mathbb{Z}_n$)

El **conjunto de unidades** *de $\mathbb{Z}_n$ se denota por U_n y se define como el conjunto de elementos de $\mathbb{Z}_n$ que tienen inverso:* $U_n = \{[a]_n \in \mathbb{Z}_n : \text{ m. c. d.}(a, n) = 1\}$.

Ejemplo 7.5

a) En $\mathbb{Z}_7$, $U_7 = \{[1]_7, [2]_7, [3]_7, [4]_7, [5]_7, [6]_7\}$.
b) En $\mathbb{Z}_9$, $U_9 = \{[1]_9, [2]_9, [4]_9, [5]_9, [7]_9, [8]_9\}$.
c) En $\mathbb{Z}_{12}$, $U_{12} = \{[1]_{12}, [5]_{12}, [7]_{12}, [11]_{12}\}$.

Como consecuencia de la Proposición 7.1 y el Corolario 7.1, si p es un número primo, se cumplen las siguientes propiedades en $\mathbb{Z}_p$:

1. Si $[a]_p \in \mathbb{Z}_p$ es tal que $[a]_p \neq [0]_p$, entonces $[a]_p$ es invertible.
2. $U_p = \mathbb{Z}_p \setminus \{[0]_p\}$.
3. $\mathbb{Z}_p$ es un *dominio de integridad*: si $[a]_p, [b]_p \in \mathbb{Z}_p$ y $[a]_p \cdot [b]_p = [0]_p$, entonces o bien $[a]_p = [0]_p$ o $[b]_p = [0]_p$.
4. Todo elemento no nulo en $\mathbb{Z}_p$ posee la *propiedad cancelativa del producto*. Sean $[a]_p, [b]_p, [c]_p \in \mathbb{Z}_p$ tales que $[a]_p \neq [0]_p$, $[b]_p \neq [0]_p$ y $[c]_p \neq [0]_p$. Si $[a]_p \cdot [c]_p = [b]_p \cdot [c]_p$, entonces $[a]_p = [b]_p$.

Terminaremos la actual sección resolviendo un problema que ponga en práctica la teoría vista en ella.

Problema 7.2 Encuentra todos los enteros x tales que $x^2 - 3x + 3 \equiv 0 \pmod 7$.

Solución *La ecuación en congruencias planteada puede expresarse como:*

$$x^2 - 3x - 4 \equiv 0 \pmod 7 \Longrightarrow (x+1)(x-4) \equiv 0 \pmod 7.$$

Equivalentemente, tomando clases de congruencia en $\mathbb{Z}_7$,

$$[x+1]_7 \cdot [x-4]_7 = [0]_7.$$

Como 7 es primo, $\mathbb{Z}_7$ es un dominio de integridad y entonces, o bien $[x+1]_7 = [0]_7 \Rightarrow [x]_7 = [-1]_7$ o $[x-4]_7 = [0]_7 \Rightarrow [x]_7 = [4]_7$. Por tanto, los enteros que cumplen la ecuación son los de la forma $7k-1$ y $7k+4$, con $k \in \mathbb{Z}$.

7.4 Teoremas de Euler y Fermat

Si bien no serán los únicos resultados relacionados con la aritmética modular que vamos a estudiar, el Teorema de Euler y el Pequeño Teorema Fermat son la base para resolver ejercicios y problemas de restos modulares. Para entender el enunciado del Teorema de Euler, hemos de conocer primero el concepto de *cardinal* de un conjunto y la función Φ de Euler.

Definición 7.6 (Cardinal)

Se define el **cardinal** *de un conjunto C como la cantidad de elementos que contiene. Se denota $|C|$.*

Definición 7.7 (Función Φ de Euler)

La **función Φ de Euler**, $\Phi : \mathbb{N} \to \mathbb{N}$, *se define como* $\Phi(1) = 1$ *y* $\Phi(n) = |U_n|$, $\forall n \geq 2$.

La función Φ de Euler posee tres propiedades clave para poder operar con ella:

1. $\Phi(p) = p - 1$, con p primo.
2. $\Phi(p^k) = (p-1)p^{k-1}$, con p primo y $k \in \mathbb{N}$.
3. $\Phi(a \cdot b) = \Phi(a)\Phi(b)$, con a y b primos entre sí.

Ejemplo 7.6

a) $\Phi(10) = \Phi(2 \cdot 5) = \Phi(2)\Phi(5) = (2-1) \cdot (5-1) = 1 \cdot 4 = 4$.
b) $\Phi(72) = \Phi(2^3 \cdot 3^2) = \Phi(2^3)\Phi(3^2) = (2-1)2^{3-1} \cdot (3-1)3^{2-1} = 1 \cdot 2^2 \cdot 2 \cdot 3^1 = 1 \cdot 4 \cdot 2 \cdot 3 = 24$.

Teorema 7.2 (de Euler)

Dados $a, n \in \mathbb{N}$ tales que $n \geq 2$ y $\text{m. c. d.}(a, n) = 1$, se tiene que:

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

Ejemplo 7.7 Tal y como conjeturamos en la sección 7.1, la última cifra de 7^{93} es 7. En efecto, como $\text{m. c. d.}(7, 10) = 1$ y $\Phi(10) = 4$, por el Teorema 7.2 (de Euler) tenemos que $7^4 \equiv 1 \pmod{10}$. Por tanto, $(7^4)^k \equiv 1^k \pmod{10}$ para todo número natural k; en particular, $(7^4)^{23} \equiv 1 \pmod{10}$. Así,

$$7^{93} = 7^{4 \cdot 23 + 1} = (7^4)^{23} \cdot 7 \equiv 1 \cdot 7 \equiv 7 \pmod{10}.$$

El Pequeño Teorema de Fermat es en realidad un corolario del Teorema de Euler.

Corolario 7.2 (Pequeño Teorema de Fermat)

Si p es primo, para cada $a \in \mathbb{N}$ no divisible por p se tiene que:

$$a^{p-1} \equiv 1 \pmod{p}.$$

Demostración Es inmediato a partir del Teorema 7.2 (de Euler) y la propiedad 1 de la función Φ de Euler. ■

Ejemplo 7.8 El resto de dividir 21^{5432} entre 11 es 1. En efecto, como 11 es primo y no es divisor de 21, por el Corolario 7.2 (Pequeño Teorema de Fermat) tenemos que $21^{10} \equiv 1 \pmod{11}$. Ahora, $5432 = 543 \cdot 10 + 2$ y $21 \equiv -1 \pmod{11}$, luego:

$$21^{5432} \equiv (21^{10})^{543} \cdot 21^2 \equiv 1^{543} \cdot 21^2 \equiv 21^2 \equiv (-1)^2 \equiv 1 \pmod{11}.$$

Para poner en práctica ambos resultados, plantearemos y resolveremos los siguientes dos problemas.

Problema 7.3 Halla el resto de dividir 3^{15} entre 17.

Solución *Según el Corolario 7.2 (Pequeño Teorema de Fermat),* $3^{16} \equiv 1 \pmod{17}$. *Esto es equivalente a escribir* $[3^{16}]_{17} = [1]_{17}$ *en* $\mathbb{Z}_{17}$. *Así,*

$$[3^{15}]_{17} = [3^{16-1}]_{17} = [3^{16}]_{17} \cdot [3^{-1}]_{17} = [1]_{17} \cdot [3^{-1}]_{17} = [3^{-1}]_{17}.$$

Como $[3]_{17} \cdot [6]_{17} = [18]_{17} = [1]_{17}$, *se tiene que* $[3^{-1}]_{17} = [6]_{17}$. *Por tanto,* $3^{15} \equiv 6 \pmod{17}$ *y el resto de dividir* 3^{15} *entre* 17 *es* 6.

Problema 7.4 Halla la última cifra del número 2^{56}.

Solución *Hallar la última cifra de un número equivale a determinar el resto que se obtiene al dividir dicho número entre* 10. *Notemos que, en principio, no podemos usar el Teorema 7.2 (de Euler) para calcular el resto que se obtiene al dividir* 2^{56} *entre* 10, *ya que* $\text{m. c. d.}(2, 10) = 2 \neq 1$. *En su lugar, calcularemos el resto de la división* 2^{55} *entre* 5 *aplicando el Corolario 7.2 (Pequeño Teorema de Fermat).*

Como $2^4 \equiv 1 \pmod 5$ *y* $55 = 4 \cdot 13 + 3$*, se tiene que:*

$$2^{55} \equiv 2^3 \equiv 8 \equiv 3 \pmod 5.$$

Por tanto, existe un número entero m *tal que* $2^{55} = 5m + 3$*. Multiplicando ambos lados de esta igualdad por* 2*, se llega a que:*

$$2^{56} = 10m + 6,$$

con $m \in \mathbb{Z}$*. Por tanto,* $2^{56} \equiv 6 \pmod{10}$ *y la última cifra de* 2^{56} *es* 6*.*

7.5 Ejercicios resueltos mediante aritmética modular

En esta sección, observaremos de manera práctica algunas aplicaciones de la aritmética modular en la realización de ejercicios y problemas variados. Se divide en tres partes: en la primera, veremos uno de los numerosos ejemplos de cómo los teoremas de Euler y Fermat permiten deducir ciertas propiedades de los números primos; en la segunda, usaremos las ecuaciones diofánticas como herramienta para resolver ecuaciones en congruencias; y en la tercera, probaremos por qué funcionan los criterios de divisibilidad de algunos números.

En primer lugar, plantearemos y resolveremos un problema en el que se pide probar una propiedad de los números primos apoyándonos en el Teorema de Euler y después se dejará propuesto otro para que el lector lo resuelva por su cuenta.

Problema 7.5 Si p es un número primo distinto de 2 y 5, entonces o bien $p^2 - 1$ o $p^2 + 1$ es divisible por 10.

Solución *Si* p *es un número primo distinto de* 2 *y* 5*, entonces* $\mathrm{m.c.d.}(p, 10) = 1$*. Por tanto, aplicando el Teorema 7.2 (de Euler),* $p^{\Phi(10)} \equiv 1 \pmod{10}$*. Como* $\Phi(10) = \Phi(2) \cdot \Phi(5) = 1 \cdot 4 = 4$*, se tiene que* $p^4 \equiv 1 \pmod{10}$ *y así* $p^4 - 1$ *es múltiplo de* 10*. Por otro lado,* p *es impar, pues es un número primo distinto de* 2*. Entonces, tanto* $p^2 - 1$ *como* $p^2 + 1$ *son múltiplos de* 2*. Pero* $p^4 - 1 = (p^2 + 1) \cdot (p^2 - 1)$*, por lo que uno de los dos factores, o bien* $p^2 - 1$ *o* $p^2 + 1$*, ha de ser múltiplo de* 5*. Finalmente, puesto que ese factor también es múltiplo de* 2*, es divisible por* 10*.*

Los métodos de resolución de ecuaciones diofánticas que vimos en la sección 7.2 no solo sirven para resolver problemas que requieren del planteamiento de este tipo especial de ecuaciones para llegar a su solución, sino que también se pueden emplear como herramienta para resolver ecuaciones en congruencias como la que se muestra a continuación.

Problema 7.6 Resuelve, si es posible, la siguiente ecuación en congruencias:

$$91x \equiv 84 \pmod{147}.$$

Solución *Notemos que* $91x \equiv 84 \pmod{147} \Rightarrow \exists k \in \mathbb{Z}\colon 91x - 84 = 147k$*. Luego resolver la ecuación en congruencias dada equivale a encontrar los valores de* x *que cumplen la ecuación diofántica* $91x - 147k = 84$*, para algún* $k \in \mathbb{Z}$*. La ecuación tiene solución, pues* $\mathrm{m.c.d.}(91, 147) = 7$*, que es divisor de* 84*. Por medio del algoritmo de Euclides (Lema 7.2) y de la identidad de Bézout (Lema 7.1), se deduce que una solución particular de la ecuación es* $(x_0, k_0) = (-96, -60)$*. Así, las soluciones para* x *son de la forma:*

$$x = -96 + \lambda \frac{-147}{7} = -21\lambda - 96, \quad \lambda \in \mathbb{Z}.$$

Estas soluciones son también las de la ecuación en congruencias inicial.

En particular, las ecuaciones diofánticas también permiten hallar el inverso multiplicativo de un elemento $[a]_n \in \mathbb{Z}_n$, con $\mathrm{m.c.d.}(a, n) = 1$, pues al fin y al cabo para ello es necesario resolver la ecuación en congruencias

$[a]_n \cdot [x]_n = [1]_n$, la cual equivale a que $ax - kn = 1$, donde $k \in \mathbb{Z}$ y $0 < x < n$. Veámoslo con un ejemplo de cálculo.

Problema 7.7 Halla el inverso multiplicativo de $[65]_{98}$ en $\mathbb{Z}_{98}$.

Solución *Hay que resolver la ecuación en congruencias*

$$[65]_{98} \cdot [x]_{98} = [1]_{98},$$

que se traduce en la ecuación diofántica

$$65x + (-98) \cdot k = 1, \quad k \in \mathbb{Z}.$$

Notemos que la ecuación tiene solución, ya que $\mathrm{m.c.d.}(65, 98) = 1$. *Aplicando el algoritmo de Euclides, se obtiene el siguiente esquema:*

	1	1	1	32
98	65	33	32	**1**
33	32	1	0	

A su vez, del esquema se derivan las siguientes identidades:

$$98 = 65 + 33 \Longrightarrow 33 = 98 - 65; \tag{7.11}$$

$$65 = 33 + 32 \Longrightarrow 32 = 65 - 33; \tag{7.12}$$

$$33 = 32 + 1 \Longrightarrow 1 = 33 - 32. \tag{7.13}$$

Sustituyendo la identidad 7.11 en 7.12, se tiene que:

$$32 = 65 - (98 - 65) \Longrightarrow 32 = 2 \cdot 65 - 98. \tag{7.14}$$

Sustituyendo las identidades 7.11 y 7.14 en 7.13, se tiene que:

$$1 = 98 - 65 - (2 \cdot 65 - 98) \Longrightarrow 65 \cdot (-3) + (-98) \cdot (-2) = 1. \tag{7.15}$$

La identidad 7.15 es la identidad de Bézout asociada a la ecuación diofántica inicial, de la cual es fácil deducir que $(x_0, k_0) = (-3, -2)$ *es una solución particular. Así, las soluciones para* x *son de la forma:*

$$x = -3 - 98\lambda, \quad \lambda \in \mathbb{Z}.$$

Recordemos que $0 < x < 98$. *Tomando* $\lambda = -1$, $x = 95$. *Por consiguiente,* $[65^{-1}]_{98} = [95]_{98}$.

La aritmética modular explica el porqué de las reglas que aprendimos para determinar si unos números son múltiplos de otros sin necesidad de realizar divisiones para comprobarlo. Demostraremos que el criterio de divisibilidad del 3 funciona y dejaremos propuesto probar que también lo hacen otros, como el del 9 o el del 11.

Problema 7.8 Prueba que un número entero es divisible por 3 si la suma de sus cifras es múltiplo de 3.

Solución *Supongamos que el número* $n \in \mathbb{Z}$ *se escribe* $a_k a_{k-1} \ldots a_1 a_0$. *Entonces:*

$$n = a_k \cdot 10^k + a_{k-1} \cdot 10^{k-1} + \cdots + a_1 \cdot 10 + a_0.$$

Como $[10^k]_3 = [10]_3^k = [1]_3^k = [1^k]_3 = [1]_3$, $\forall k \in \mathbb{N}$, *se tiene que:*

$$\begin{aligned}[n]_3 &= [a_k \cdot 10^k + a_{k-1} \cdot 10^{k-1} + \cdots + a_1 \cdot 10 + a_0]_3 \\ &= [a_k]_3 \cdot [10^k]_3 + [a_{k-1}]_3 \cdot [10^{k-1}]_3 + \cdots + [a_1]_3 \cdot [10]_3 + [a_0]_3 \\ &= [a_k]_3 + [a_{k-1}]_3 + \cdots + [a_1]_3 + [a_0]_3 = \\ &= [a_k + a_{k-1} + \cdots + a_1 + a_0]_3.\end{aligned}$$

Ahora, si la suma de las cifras de n *es múltiplo de* 3*, tenemos que* $[n]_3 = [a_k + a_{k-1} + \cdots + a_1 + a_0]_3 = [0]_3$ *y por tanto* n *es también múltiplo de* 3*.*

7.6 Problemas de olimpiadas matemáticas

Para finalizar este capítulo, vamos a echar un vistazo a unos cuantos problemas propuestos en olimpiadas anteriores de diverso tipo. Además, aprovecharemos para explicar algunas técnicas que no está de más conocer para enfrentarse a ellos.

Para empezar, a veces está muy bien conocer el resto que dejan los cuadrados de los números al dividirlos por determinados módulos. Estos *restos cuadráticos* proporcionan la clave para resolver problemas como los que se muestran a continuación, en los que se utiliza que los cuadrados módulo 4 son solamente 0 y 1 (y que, en consecuencia, la suma de dos cuadrados módulo 4 nunca es 3).

Problema 7.9 Halla todas las posibles formas de escribir 2003 como suma de dos cuadrados de números enteros positivos.

Solución *Se trata de buscar las soluciones enteras positivas de la ecuación* $x^2 + y^2 = 2003$*. Para ello, utilizaremos congruencias módulo* 4*. Notemos que si* n *es un número natural, entonces o bien* $n^2 \equiv 0 \pmod 4$ *o* $n^2 \equiv 1 \pmod 4$*. En efecto,* n *puede ser de la forma* $4k + r$*, con* $k \in \mathbb{N}$ *y* $r \in \{0, 1, 2, 3\}$*, y de este modo:*

- *Si* $r = 0$*,* $n^2 = (4k)^2 = 16k^2 \equiv 0 \pmod 4$.
- *Si* $r = 1$*,* $n^2 = (4k + 1)^2 = 16k^2 + 8k + 1 \equiv 1 \pmod 4$.
- *Si* $r = 2$*,* $n^2 = (4k + 2)^2 = 16k^2 + 16k + 4 \equiv 0 \pmod 4$.
- *Si* $r = 3$*,* $n^2 = (4k + 3)^2 = 16k^2 + 24k + 9 \equiv 1 \pmod 4$.

Así, $x^2 + y^2$ *sólo puede ser congruente con* 0*,* 1 *o* 2 *módulo* 4*. Pero* $2003 \equiv 3 \mod 4$*. Por lo tanto, no es posible escribir* 2003 *como suma de dos cuadrados de números enteros positivos.*

Problema 7.10 Encuentra todos los enteros x, y, z que cumplen $x^2 + y^2 + z^2 - 2xyz = 0$.

Solución *La ecuación se puede transformar en:*

$$x^2 + y^2 + z^2 = 2xyz.$$

Si x*,* y *y* z *fuesen impares, entonces el lado izquierdo sería impar, pero el derecho sería par. Así que al menos uno de los enteros* x, y, z *es par. Por tanto,* $2xyz$ *ha de ser múltiplo de* 4*. Puesto que los cuadrados módulo* 4 *pueden ser* 0 *o* 1*, la ecuación obliga a que* x*,* y *y* z *sean pares.*

Escribamos $x = 2x_1$*,* $y = 2y_1$*,* $z = 2z_1$*, para ciertos* $x_1, y_1, z_1 \in \mathbb{Z}$*. Sustituyendo estas variables en la ecuación inicial y simplificando, queda:*

$$4x_1y_1z_1 = x_1^2 + y_1^2 + z_1^2.$$

En este punto, nos percatamos de que se puede repetir el razonamiento anterior, y que así $x_1 = 2x_2$*,* $y_1 = 2y_2$*,* $z_1 = 2z_2$*, para ciertos* $x_2, y_2, z_2 \in \mathbb{Z}$*. Reiterando el mismo argumento con estos* x_2, y_2, z_2 *y con los sucesivos* $x_i = 2x_{i+1}$*,* $y_i = 2y_{i+1}$*,* $z_i = 2z_{i+1}$ *que obtengamos, al final llegamos a que* x, y, z *son divisibles por infinitas*

potencias de 2. *Esto sólo lo cumplen*

$$x = 0, \quad y = 0, \quad z = 0.$$

Otra idea interesante que aparece en la resolución de algunos problemas olímpicos, como en el Problema 7.9 o el Problema 7.11 que se muestra a continuación, es la de clasificar los números enteros en clases de congruencia módulo un determinado número.

Problema 7.11 Sea n un número natural. Prueba que si la última cifra de 7^n es 3, entonces la penúltima es 4.

Solución *Si* n *es un número natural,* 7^n *acaba en* 3 *sólo cuando* $n = 4k + 3$, *con* $k \in \mathbb{N}$. *En efecto,* n *puede ser de la forma* $4k + r$, *con* $k \in \mathbb{N}$ *y* $r \in \{0, 1, 2, 3\}$. *Por el teorema 7.2 (de Euler), como* $\text{m. c. d.}(7, 10) = 1$, *se tiene que* $7^{\Phi(10)} \equiv 7^4 \equiv 1 \pmod{10}$, *por lo que:*

- *Si* $r = 0$, $7^n \equiv 7^{4k} \equiv (7^4)^k \equiv 1^k \equiv 1 \pmod{10}$.
- *Si* $r = 1$, $7^n \equiv 7^{4k+1} \equiv 7^{4k} \cdot 7 \equiv 7 \pmod{10}$.
- *Si* $r = 2$, $7^n \equiv 7^{4k+2} \equiv 7^{4k} \cdot 7^2 \equiv 49 \equiv 9 \pmod{10}$.
- *Si* $r = 3$, $7^n \equiv 7^{4k+3} \equiv 7^{4k} \cdot 7^3 \equiv 343 \equiv 3 \pmod{10}$.

Por otro lado, tenemos que $7^4 = 2401 \equiv 1 \pmod{100}$. *Por tanto, si* $k \in \mathbb{N}$,

$$7^{4k+3} \equiv (7^4)^k \cdot 7^3 \equiv 1 \cdot 343 \equiv 343 \equiv 43 \pmod{100}.$$

Esto significa que, si $k \in \mathbb{N}$, 7^{4k+3} *termina en* 43, *como queríamos demostrar.*

En el Problema 7.11, aparte de la estrategia que acabamos de comentar, también se echa mano del Teorema de Euler. Evidentemente, no es el único en el que ha aparecido este resultado u otros derivados de él, como el Pequeño Teorema de Fermat, que se usa en el Problema 7.12.

Problema 7.12 Encuentra todas las parejas de números primos p, q tales que $p^3 - q^5 = (p + q)^2$.

Solución *Resulta claro que, para que se cumpla la igualdad,* $p > q$. *De primeras, supongamos que* $p \neq 3$ *y* $q \neq 3$. *Por el Corolario 7.2 (Pequeño Teorema de Fermat), se tiene que* $p - q \equiv (p + q)^2 \pmod{3}$. *Así, si* $p \equiv q \pmod{3}$, *entonces* $0 \equiv q^2 \not\equiv 0$, *lo cual no es posible. Por tanto,* $p \not\equiv q \pmod{3}$. *Pero, en este caso,* $(p + q)^2 \equiv 0 \pmod{3}$, *mientras que* $p - q \not\equiv 0 \pmod{3}$, *lo que nuevamente no es posible. Por consiguiente, no queda más remedio que o bien* $p = 3$ *o* $q = 3$. *Como* $3^3 - 2^5 < 0$, *la única posibilidad es* $q = 3$. *En ese caso,* $p^3 - 243 = p^2 + 6p + 9$ *implica que* p *divide a* 252, *por lo que solamente puede ser* $p = 7$ *y la única pareja de números primos que cumple la ecuación es* $(p, q) = (7, 3)$.

El Pequeño Teorema de Fermat no es el único corolario que se puede extraer del Teorema de Euler relacionado con congruencias módulo un cierto número primo. Por ejemplo, también se tiene que:

- Para cualquier entero a, $a^p \equiv a \pmod{p}$.
- Para cualesquiera enteros a y b, $(a + b)^p \equiv a^p + b^p \pmod{p}$.

Obviamente, estos trucos pueden emplearse siempre que sea pertinente en la resolución de problemas. Sin embargo, el Teorema de Euler tampoco es la única fuente de creación de propiedades de números primos en clases de congruencia. De hecho, por ejemplo, el siguiente teorema se halla dentro del ámbito de la aritmética modular y permite caracterizar a los números primos, pues da una condición necesaria y suficiente para que un número lo sea. [1]

[1] Aunque el Teorema de Wilson permite identificar tanto si un número es primo como si no lo es, habitualmente no se utiliza como test de primalidad en la práctica, puesto que calcular $(n-1)! \pmod{n}$ para un número n grande es muy costoso y se conocen tests mucho más sencillos y rápidos.

Teorema 7.3 (de Wilson)

p es un número primo si y solo si

$$(p-1)! \equiv -1 \pmod{p}.$$

El nombre del teorema 7.3 se eligió en honor a John Wilson, matemático inglés del siglo XVIII. Veamos ahora un ejemplo de aplicación de dicho teorema a un problema olímpico.

Problema 7.13 Sea a el entero que cumple la igualdad $\sum_{i=1}^{23} \frac{1}{i} = \frac{a}{23!}$. Calcula el resto de dividir a entre 13.

Solución *Multiplicando ambos miembros de la ecuación por* 23!*, tenemos que* $a = \sum_{i=1}^{23} \frac{23!}{i}$*. Todos estos sumandos son nulos módulo* 13*, excepto* $\frac{23!}{13}$*, que es congruente con* $12! \cdot 10!$ *módulo* 13*. Usando el Teorema 7.3 (de Wilson), se tiene que:*

$$[a]_{13} = [12!]_{13} \cdot [10!]_{13} = [12!]_{13} \cdot [12!]_{13} \cdot [12^{-1}]_{13} \cdot [11^{-1}]_{13} = [-1]_{13} \cdot [-1]_{13} \cdot [-1]_{13} \cdot [6]_{13} = [-6]_{13} = [7]_{13}.$$

Por tanto, el resto es 7*.*

Terminaremos resolviendo problemas relacionados con criterios de divisibilidad.

Problema 7.14 Dado un número entero n escrito en el sistema de numeración decimal, formamos el número entero k restando del número formado por las tres últimas cifras de n el número formado por las cifras anteriores restantes. Demuestra que n es divisible por 7, 11 o 13 si y solo si k también lo es.

Solución *Sea A el número formado por las tres últimas cifras de n y B el número formado por todas las cifras anteriores. Esto significa que $n = 1000B + A$ y $k = A - B$. De este modo, se tiene que:*

$$n - k = 1001B = 7 \cdot 11 \cdot 13 \cdot B.$$

Por tanto, n y k son congruentes módulo 7*,* 11 *y* 13*.*

Con esta misma técnica, se puede resolver el siguiente problema, que queda propuesto para el lector.

Ejercicios Propuestos

1. Determina cuáles de los siguientes números son congruentes con 4 módulo 7: 81, 445, -74, 332, -52.

2. Conjetura, aunque no lo demuestres, en qué cifra debería acabar el número 3^{2021}.

3. ¿Qué letra hay que añadir al DNI 16620864 para obtener el correspondiente NIF?

4. Ayer fui a la biblioteca para que me prestaran un libro. Al ser un poco viejo, se le ha borrado el último dígito de su ISBN. Aun así, sí que pude leer los anteriores: $038796254\square$. ¿Qué dígito se ha borrado?

5. Al ir a hacer una transferencia a través de la aplicación web de su banco, Félix tecleó el siguiente código de cuenta corriente: 20387444716000004303. ¿Debería permitirle la aplicación web efectuar la transferencia? En caso negativo, y suponiendo que los dígitos que no son de control son correctos, ¿qué código tendría que haber tecleado?

6. ¿Para cuántos valores enteros c comprendidos entre 100 y 200 tiene solución la ecuación diofántica $56x + 378y = c$?

7. En la ecuación diofántica del ejercicio anterior, halla una solución particular (x_0, y_0) por medio del algoritmo de Euclides y la identidad de Bézout cuando $c = 112$.

8. Un viejo turista tenía 5000 pesetas y en su día quiso cambiarlas por francos franceses y marcos alemanes. El cambio que le ofrecía un banco era el siguiente: un franco equivalía a 24 pesetas y por un marco le daban 84 pesetas. Sabiendo que el banco no proporcionaba fracciones de ninguna moneda:
   a) ¿Pudo hacer el cambio?
   b) ¿Podría haberlo hecho si hubiera cambiado 6000 pesetas?
   c) Para ambos apartados, en caso afirmativo, ¿de cuántas formas diferentes pudo hacerlo?

9. Un hombre acude a un banco a cobrar un cheque por valor de D dólares y C céntavos. El cajero, por error, le entrega un sobre con C dólares y D centavos. El cliente no se da cuenta del error hasta que gasta 23 centavos y, además, observa que en ese momento tiene $2D$ dólares y $2C$ centavos. ¿Cuál es el valor del cheque?

10. ¿Qué resto se obtiene al dividir 6^{2021} entre 7?

11. Halla todas las soluciones de la ecuación $[4]_{18} \cdot a = [0]_{18}$ en $\mathbb{Z}_{18}$.

12. Encuentra todas las posibles soluciones para la ecuación $[7]_{12}^{-1} = [x]_{12}$ en $\mathbb{Z}_{12}$.

13. ¿Cuántos elementos invertibles hay en $\mathbb{Z}_{37}$?

14. Escribe todos los elementos de los conjuntos U_8 en $\mathbb{Z}_8$, U_{15} en $\mathbb{Z}_{15}$ y U_{18} en $\mathbb{Z}_{18}$.

15. Calcula $\Phi(6615)$.

16. Calcula las dos últimas cifras del número 63^{282}.

17. Calcula el resto de dividir 67^{9539} entre 17.

18. Halla el resto de dividir 215^{7371} entre 29.

19. Halla la última cifra del número 2018^{2019}.

20. Halla el resto de dividir 125^{4577} entre 13.

21. Halla el resto de dividir 2^{4k} entre 5 para todo $k \in \mathbb{N}$.

Bibliografía Adicional

1. Engel, A. (1998). Number Theory. *Problem-Solving Strategies*. Editorial Springer, 117-160.
2. García Merayo, F. (2015). *Matemática discreta*. Editorial Ediciones Paraninfo, SA.

CAPÍTULO 8

8

SERIES NUMÉRICAS

Daniel José Rodríguez Luis
Universidad de La Rioja

Palabras clave

- *Series convergentes*
- *Series divergentes*
- *Criterios de comparación de series*
- *Serie armónica*
- *Series geométricas de razón r*
- *Series Telescópicas*

En matemáticas, la noción de serie numérica hace referencia a la operación de sumar una cantidad infinita de números reales, uno tras otro. El estudio de las series numéricas es una parte fundamental del cálculo matemático, con aplicaciones en problemas de combinatoria y probabilidad.

Durante mucho tiempo, la idea de que la suma de una infinidad de números pudiese dar un resultado finita se consideraba una auténtica locura. Hace más de 2400 años que el filósofo griego Zenón de Elea, famoso por sus paradojas del tiempo y el movimiento, formuló la conocida como "paradoja del corredor", donde el sentido común hacía pensar que la suma de infinitos números debía ser una cantidad finita. Este hecho precipitó una crisis en las matemáticas de la Antigua Grecia, que culminó con la aparición de las series numéricas.

En este capítulo veremos la idea de series numéricas que se derivaba de la paradoja de Zenón. Así mismo, veremos algunas series numéricas importantes y criterios que nos ayudarán a afirmar que una serie es convergente, es decir, que su suma es una cantidad finita. Por último, aplicaremos los conocimientos adquiridos en la resolución y el estudio de las series numéricas.

8.1 Introducción

Para poder hablar de las series numéricas, es necesario recordar el concepto de *sucesión númérica* que fue introducido en el capítulo dedicado a las ecuaciones en recurrencia.

Definición 8.1 (Sucesión Numérica)

En matemáticas, una ***sucesión*** *es toda aquella función f definida sobre conjunto de los números naturales $\mathbb{N} = \{1, 2, 3, \dots\}$ y que toma valores en el conjunto de los números reales $\mathbb{R}$ dada por*

$$f : \mathbb{N} \longrightarrow \mathbb{R}$$
$$n \longrightarrow x_n.$$

De forma general, denotamos por (x_n) a la sucesión numérica definida por $x_n = f(n)$ con $n \in \mathbb{N}$.

Nota: *En ocasiones, y por abuso de notación, las sucesiones se representan simplemente por x_n.*

Ejemplo 8.1 La sucesión constante 1 es aquella sucesión (x_n) donde cada término es $x_n = 1$, con $n \in \mathbb{N}$.

Ejemplo 8.2 Una sucesión alternada es aquella de la forma $x_n = (-1)^n$, con $n \in \mathbb{N}$. En este caso se observa que

$$x_1 = -1, \quad x_2 = 1, \quad x_3 = -1, \quad x_4 = 1, \quad \dots\dots, \quad x_n = (-1)^n, \dots$$

Lo de "alternada" proviene por el cambio de signo que experimenta la sucesión entre un término y el siguiente.

Ahora bien, dada una sucesión de números reales (x_n), es posible construir una nueva sucesión (S_n) definida como resultado de sumar los n primeros términos de la sucesión (x_n), esto es,

$$S_1 = x_1, \quad S_2 = x_1 + x_2, \quad S_3 = x_1 + x_2 + x_3, \quad \dots \quad S_n = x_1 + x_2 + \cdots + x_n, \dots$$

A esta sucesión (S_n) se le denomina **sucesión de sumas parciales asociadas** (x_n).

Ejemplo 8.3 Para la sucesión del Ejemplo 8.1 dada por $x_n = 1$ con $n \in \mathbb{N}$, se tiene que la sucesión de sumas parciales (S_n) viene dada por

$$S_1 = x_1 = 1, \quad S_2 = x_1 + x_2 = 1 + 1 = 2, \quad S_3 = x_1 + x_2 + x_3 = 1 + 1 + 1 = 3, \quad \dots$$

Es fácil comprobar que el término general de la sucesión (S_n) viene dado por $S_n = n$ para cada $n \in \mathbb{N}$.

Ejemplo 8.4 Para la sucesión del Ejemplo 8.2 dada por $x_n = (-1)^n$ con $n \in \mathbb{N}$, se tiene que los primeros términos de la sucesión de sumas parciales (S_n) vienen dados por

$$S_1 = 1, \quad S_2 = 1 + (-1) = 0, \quad S_3 = 1 + (-1) + 1 = 1, \quad S_4 = 1 + (-1) + 1 + (-1) = 0, \quad \dots$$

Se puede probar que el término general de la sucesión de sumas parciales viene dado por

$$S_n = \begin{cases} 1 & \text{si } n \text{ es impar} \\ 0 & \text{si } n \text{ es par} \end{cases}, \quad \text{para cada } n \in \mathbb{N}.$$

Si no te lo crees, puedes probar esta afirmación usando el principio de inducción matemática.

A partir de esta sucesión de sumas parciales, obtenemos la noción de serie numérica o serie infinita.

Definición 8.2 (Serie Numérica)

Dada una sucesión de números reales (x_n)*, una* ***serie numérica*** *(o también* ***serie infinita****) se puede entender como "la suma de infinitos términos" y que se denota por*

$$\sum_{n=1}^{\infty} x_n = x_1 + x_2 + x_3 + x_4 + \cdots + x_n + \ldots$$

Nota: *Por comodidad, las series numéricas también se escriben de la forma* $x_1 + x_2 + x_3 + x_4 + \ldots$

La relación que existe entre las series numéricas y la sucesión de sumas parciales que hemos definido anteriormente es la siguiente: si tenemos una sucesión (x_n), podemos considerar la sucesión de sumas parciales (S_n) que se define como $S_n = x_1 + x_2 + \cdots + x_n$, para cada $n \in \mathbb{N}$. Ahor bien, dado que una serie numérica $\sum_{n=1}^{\infty} x_n$ es el resultado de sumar los infinitos términos de la sucesión (x_n), dicha serie numérica se puede entender como el resultado al que se aproxima la sucesión de sumas parciales (S_n) cuando consideramos el subíndice "n" un número muy grande, esto es, cuando n tiende a infinito.

En terminología matemática, lo que hemos dicho anteriormente se escribe de la siguiente manera

$$x_1 + x_2 + x_3 + x_4 + \cdots = \sum_{k=1}^{\infty} x_k = \lim_{n\to\infty} \sum_{k=1}^{n} x_k = \lim_{n\to\infty} S_n.$$

Entrando en un poco de historia, ¿Cómo y dónde surge la idea de series infinitas? ¿A qué clase de lunático/chalado se le ocurriría sumar una cantidad infinitos de números? Pues bien, todo tiene su origen en las reflexiones de filósofos y matemáticos de la Antigua Grecia.

En esta línea, uno de los primero ejemplos de series infinitas se le atribuye a Zenón de Elea (490-430 a. C), un filósofo griego que se hizo célebre por el planteamiento de varias "paradojas"(también conocidas como "aporías"), esto es, situaciones que presentan ciertas contradicciones con la lógica, siendo las más famosas aquellas relativas al tiempo y al movimiento. En la Figura 8.1, que se corresponde con un fresco presente en la Biblioteca de El Escorial (Madrid), podemos ver al filósofo Zenón mostrando a sus discípulos las puertas a la verdad y la falsedad (Veritas et Falsitas en latín, respectivamente).

Figura 8.1: Zenón muestra las puertas a la verdad y la falsedad.

Llegados a este punto, la paradoja de Zenón (también conocida como la paradoja del corredor) se enuncia de la siguiente forma:

Un corredor nunca alcanzará la línea de meta porque siempre ha de recorrer la mitad de una distancia antes de recorrer la distancia total.

Probablemente te estás preguntando ¿Por qué el enunciado de Zenón plantea una situación contradictoria? Para verlo con claridad, vamos a analizar con detenimiento la paradoja de Zenón: supongamos que el corredor

se encuentra en el punto de partida (situado en el punto 1) y que corre hacia la meta (situada en el punto 0). Vamos a representar por $1/2$, $1/4$, $1/8, \ldots$ y así sucesivamente las fracciones de recorrido hasta el punto de meta, tal y como puede verse en la Figura 8.2. Supongamos que el corredor va a una velocidad constante y que, por tanto, tarda T minutos en recorrer la primera mitad del trayecto hacia la meta. Es decir, en la Figura 8.2 el corredor emplea T minutos en ir desde el punto 1 al punto $1/2$.

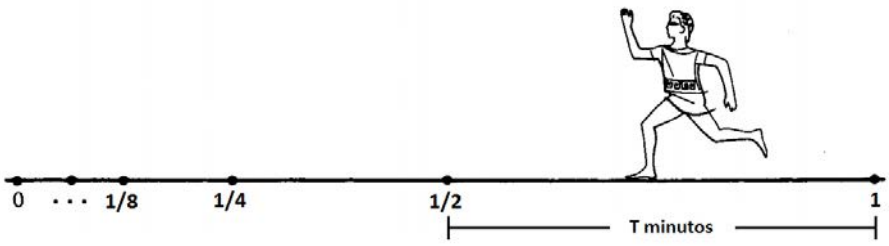


Figura 8.2: El corredor emplea T minutos entre los puntos 1 y $1/2$.

Ahora bien, para el siguiente cuarto del recorrido (que es la mitad del trayecto que falta por recorrer para llegar a la meta) nuestro corredor necesitaría la mitad del tiempo empleado en el tramo anterior. Es decir, en la Figura 8.3 el corredor invierte $T/2$ minutos para ir desde el punto $1/2$ al punto $1/4$. $T/2$ minutos.

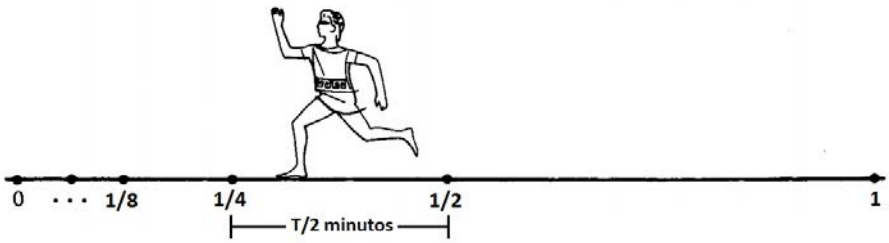


Figura 8.3: El corredor emplea $T/2$ minutos entre los puntos $1/2$ y $1/4$.

Pero nuevamente, para el siguiente octavo del recorrido (que es la mitad del trayecto que falta por recorrer para llegar a la meta) nuestro corredor necesitaría la mitad del tiempo empleado en el tramo anterior. Es decir, en la Figura 8.4 el corredor emplea $T/4$ minutos para ir desde el punto $1/4$ al punto $1/8$. Y así sucesivamente con el resto del recorrido.

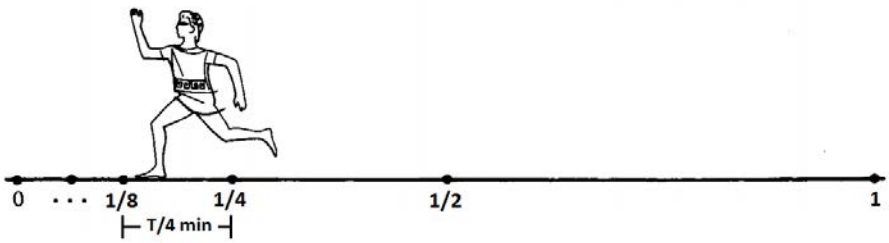


Figura 8.4: El corredor emplea $T/4$ minutos entre los puntos $1/4$ y $1/8$.

En general, para cada $n \in \mathbb{N}$ el corredor emplea $T/2^n$ minutos en recorrer la distancia entre los puntos $1/2^n$ y $1/2^{n+1}$. Por lo tanto, el tiempo que tarda el corredor en recorrer la distancia desde el punto de partida hasta el punto de meta es la suma de todos estos intervalos de tiempo intermedios, que se expresa mediante la suma infinita de la forma siguiente

$$2T = T + \frac{T}{2} + \frac{T}{4} + \frac{T}{8} + \cdots + \frac{T}{2^n} + \frac{T}{2^{n+1}} + \ldots$$

Ahora bien, ¿Dónde aparece la contradicción en lo que plantea Zenón? Pues bien, ya que para ir del punto de partida al punto de meta siempre faltará por recorrer la mitad de una cierta distancia (por muy pequeña que sea), podemos concluir que **el corredor nunca llegaría al punto de meta**.

Espera un momento, ¿Cómo? Pues sí, has leído bien: la paradoja de Zenón sugiere que el movimiento entre dos puntos es imposible. Pero, ¡tranquilidad, pequeño saltamontes!, gracias a la experiencia sabemos que esto no es así.

De hecho, la propia experiencia nos dice que el corredor debe emplear $2T$ minutos en recorrer el trayecto desde el punto de partida hasta el punto de meta, ya que va a velocidad constante y además el corredor ha invertido T minutos en recorrer la mitad del trayecto. Por lo tanto, atento que se viene *spoiler*, para que el planteamiento de Zenón sea coherente con nuestra propia experiencia debe ocurrir que

$$2T = T + \frac{T}{2} + \frac{T}{4} + \frac{T}{8} + \cdots + \frac{T}{2^n} + \frac{T}{2^{n+1}} + \ldots \tag{8.1}$$

En la siguientes secciones veremos conceptos y herramientas para demostrar que la igualdad (8.1) es cierta.

Dejando aparte la implicación de que todo movimiento es imposible, la paradoja de Zenón llevó al descubrimiento de que una cantidad finita (en este caso, el tiempo empleado por el corredor) podía dividirse en un número infinito de partes más pequeñas, lo que posteriormente pasaría a denominarse como series infinitas.

Una variante interesante de la paradoja de Zenón es la siguiente: supongamos que la velocidad del corredor no es constante sino que disminuye de tal forma que necesita T minutos para ir de 1 a $1/2$, $T/2$ minutos para ir de $1/2$ a $1/4$, $T/3$ minutos para ir de $1/4$ a $1/8$ y así sucesivamente. En general, el corredor emplea T/n minutos para ir de $1/2^{n-1}$ a $1/2^n$. Por lo tanto, según la situación que hemos planteado anteriormente de velocidad no cosntante, el tiempo que necesita el corredor para ir desde el punto de partida hasta el punto de meta viene dado por la serie numérica

$$T + \frac{T}{2} + \frac{T}{3} + \frac{T}{4} + \cdots + \frac{T}{n} + \frac{T}{n+1} + \ldots \tag{8.2}$$

De hecho, y atentos nuevamente que se viene *spoiler*, en la siguiente Sección 8.3 veremos que el resultado de la serie presente en la ecuación (8.1) es una cantidad inconmensurable, es decir, es una cantidad tan grande que no se puede medir.

En la siguiente sección veremos algunas nociones básicas relacionadas con las series infninitas, así como algunos ejemplos de series importantes que serán de gran utilidad para el desarrollo del capítulo.

8.2 Nociones básicas y series importantes

Tal y como hemos comentado en la Definición 8.2 de la Sección 8.1 , se denomina **serie infinita** a la suma de infinitos términos de una sucesión de números reales (x_n) y que denotamos, de manera abreviada, por la expresión $x_1 + x_2 + x_3 + x_4 + \ldots$. De manera informal, las series infinitas se clasifican en dos bloques:

1. **Series convergentes**: Aquellas cuya suma es un número finito fijo.
2. **Series divergentes**: Aquellas que NO son convergentes.

Pero, ¿cómo saber si una serie es convergente o divergente? Para ello, y con un poco más de rigor matemático, usamos la sucesión de sumas parciales asociadas a una serie infinita para definir la idea de convergencia.

Definición 8.3 (Serie convergente)

Sea $\sum_{n=1}^{\infty} x_n$ *una serie infinita y denotemos por* $S_N = \sum_{n=1}^{N} x_n = x_1 + x_2 \cdots + x_N$ *la sucesión de sumas parciales asociada a dicha serie. Diremos que la serie infinita es* ***convergente*** *si existe el límite de la sucesión de sumas parciales, es decir, si existe una cantidad* $S \in \mathbb{R}$ *tal que* $S = \lim_{N\to\infty} S_N$.
En caso de que una serie infinita sea convergente escribimos $S = x_1 + x_2 + x_3 + \ldots$.

La idea de la series convergentes es la siguiente: diremos que una serie infinita es convergente si la sucesión de sumas parciales se "aproximan" a un valor fijo S cuando el número de sumandos crece de forma inconmensurable. En otras palabras:

$$S_1 = x_1, \quad S_2 = x_1 + x_2, \quad S_3 = x_1 + x_2 + x_3 \quad , \ldots , \quad S_N = x_1 + x_2 + x_3 + \cdots + x_N \xrightarrow[N\to\infty]{} S.$$

Nota: *Gráficamente una serie es convergente cuando a medida que vamos añadiendo términos a la suma, el resultado se acerca cada vez más al valor* S. *En la Figura 8.5 se representa la sucesión de sumas parciales (puntos negros) aproximándose a la cantidad finita* S *(punto rojo).*

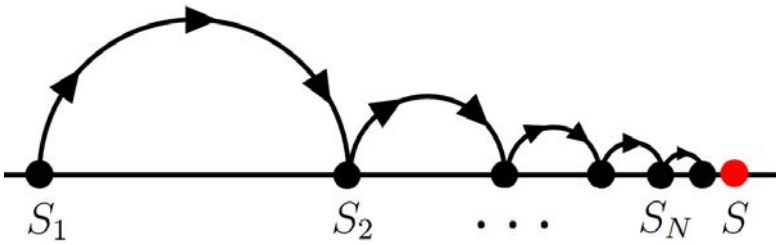


Figura 8.5: Interpretación de una serie convergente mediante la sucesión de sumas parciales.

También, en términos de la sucesión de sumas parciales, tenemos la definicón de una serie divergente.

Definición 8.4 (Serie divergente)

Sea $\sum_{n=1}^{\infty} x_n$ *una serie infinita y denotemos por* $S_N = \sum_{n=1}^{N} x_n = x_1 + x_2 \cdots + x_N$ *la sucesión de sumas parciales asociada a dicha serie. Diremos que la serie infinita es* ***divergente*** *si el límite de la sucesión de sumas parciales* $\lim_{N\to\infty} S_N$ *bien no es finito o bien directamente no existe.*

Ejemplo 8.5 La serie $\sum_{n=1}^{\infty} 1 = 1 + 1 + 1 + \ldots$ es divergente. En efecto, si denotamos por S_n a la sucesión de sumas parciales observamos que

$$S_1 = 1, \qquad S_2 = 1 + 1 = 2, \qquad S_3 = 1 + 1 + 1 = 3, \qquad S_4 = 1 + 1 + 1 + 1 = 4, \ldots$$

En general, se tiene que $S_n = n$ para cada $n \geq 1$. Como además $\lim_{n\to\infty} S_n = \infty$, podemos concluir que la serie $\sum_{n=1}^{\infty} 1 = 1 + 1 + 1 + \ldots$ es divergente.

Ejemplo 8.6 La serie alternada $\sum_{n=1}^{\infty} (-1)^n = (-1) + 1 + (-1) + 1 + \ldots$ también es divergente.

En efecto, tal y como se hizo en el Ejemplo 8.4, si denotamos por S_n a la sucesión de sumas parciales se

tiene

$$S_n = \begin{cases} 1 & \text{si } n \text{ es impar} \\ 0 & \text{si } n \text{ es par} \end{cases}, \quad \text{para cada } n \in \mathbb{N}.$$

Sin embargo, la sucesión S_n nunca se aproxima a un número S fijo ya que:

- Si n es par, entonces $\lim_{n\to\infty} S_n = \lim_{n\to\infty} 0 = 0$.
- Si n es impar, entonces $\lim_{n\to\infty} S_n = \lim_{n\to\infty} 1 = 1$.

Por lo tanto, como el límite anterior es diferente dependiendo de cómo nos movamos en la sucesión de sumas parciales (si por los pares o por los impares), podemos concluir que la serie $\sum_{n=1}^{\infty} x_n = (-1)^n = (-1) + 1 + (-1) + 1 + \ldots$ es divergente.

Ahora bien, ¿Qué pasa con las series convergentes? ¿Podemos ver algunos ejemplos? A continuación, vamos a definir dos series infinitas convergentes que serán de gran utilidad en el desarrollo del capítulo.

Definición 8.5 (Serie geométrica de razón r)

*Para cada número real $-1 < r < 1$, la **serie geométrica de razón** r dada por la expresión*

$$\sum_{n=0}^{\infty} r^n = 1 + r + r^2 + r^3 + r^4 + \ldots$$

es una serie convergente. Además, el valor de su suma es $1/(1-r)$.

Nota: *Observamos que si $r = 1$ resulta la serie del Ejemplo 8.5 mientras que si $r = -1$ se obtiene la serie alternada del Ejemplo 8.6, ambas series divergentes. Por ello, en la defínción anterior exigimos $-1 < r < 1$.*

Vamos a preceder a probar que la serie geométrica de razón r es convergente calculando una expresión general el término general de la sucesión de sumas parciales. Si denotamos por S_n a las sumas parciales de la serie geométrica vemos que

$$S_1 = 1, \qquad S_2 = 1 + r, \qquad S_3 = 1 + r + r^2, \qquad S_n = 1 + r + r^2 + \cdots + r^{n-1},$$

A simple vista, no parece haber una fórmula sencilla que ayude a simplificar las expresiones. Sin embargo, podemos realizar la siguiente observación: Si tomamos el término de la suma parcial S_n y la multiplicamos por la razón r obtenemos

$$\begin{cases} S_n = 1 + r + r^2 + \cdots + r^{n-1} \\ rS_n = \quad r + r^2 + \cdots + r^{n-1} + r^n \end{cases} \quad \text{si restamos resulta } (1-r)S_n = 1 - r^n.$$

Por lo tanto, obtenemos una fórmula explícita que nos permite calcular la suma de los n-primeros términos de la serie geométrica de razón r y que viene dada por

$$S_n = \frac{1 - r^n}{1 - r}, \qquad \text{para cada } n \in \mathbb{N}. \tag{8.3}$$

Ahora bien, como además, $-1 < r < 1$, se tiene que $\lim_{n\to\infty} r^n = 0$ con lo que finalmente la serie geométrica es convergente y el valor de su suma es

$$1 + r + r^2 + r^3 + \ldots r^n + r^{n+1} + \cdots = \lim_{n\to\infty} S_n = \lim_{n\to\infty} \frac{1 - r^n}{1 - r} = \frac{1}{1 - r}.$$

Ejemplo 8.7 Gracias a lo expuesto anteriormente en relación a la serie geométrica, podemos demostrar que la serie que aparece en la paradoja de Zenón dada por

$$T + \frac{T}{2} + \frac{T}{4} + \frac{T}{8} + \cdots + \frac{T}{2^n} + \cdots = T\left(1 + \frac{1}{2} + \frac{1}{2^2} + \frac{1}{2^3} + \cdots + \frac{1}{2^n} + \ldots\right)$$

es una serie convergente (al ser, esencialmente, de una serie geométrica de razón $r = 1/2$). Además el valor de la suma de la serie geométrica de razón $r = 1/2$ es $S = 1/(1-r) = 2$. Por lo tanto, hemos probado que la serie en la paradoja de Zenón también es convergente y su suma vale $2T$, es decir,

$$2T = T + \frac{T}{2} + \frac{T}{4} + \frac{T}{8} + \cdots + \frac{T}{2^n} + \frac{T}{2^{n+1}} + \ldots$$

Ya podíamos sospechar esta igualdad cuando escribimos la ecuación (8.1).

Nota: *De forma alternativa, se puede demostrar que la serie presente en la paradoja de Zenón es convergente atendiendo a sucesión de sumas parciales dada por*

$$S_1 = 1 = 2 - 1, \qquad S_2 = 1 + \frac{1}{2} = \frac{3}{2} = 2 - \frac{1}{2^1}, \qquad S_3 = 1 + \frac{1}{2} + \frac{1}{4} = \frac{7}{4} = 2 - \frac{1}{4} = 2 - \frac{1}{2^2}$$

Usando la inducción matemática, se puede probar que para cada $n \geq 1$ se cumple que

$$S_n = 1 + \frac{1}{2} + \frac{1}{4} + \cdots + \frac{1}{2^n} = 2 - \frac{1}{2^{n-1}}$$

Por lo tanto,

$$\sum_{k=0}^{\infty} \frac{1}{2^k} = 1 + \frac{1}{2} + \frac{1}{4} + \cdots = \lim_{n\to\infty} S_n = \lim_{n\to\infty}\left(2 - \frac{1}{2^{n-1}}\right) = 2.$$

Por último, veamos otro tipo de series infinitas que son convergentes.

Definición 8.6 (Serie telescópica)

*Una serie $\displaystyle\sum_{n=1}^{\infty} x_n$ se dice **telescópica** si existe una función F definida en $\mathbb{N} \cup \{0\}$ y que toma valores en $\mathbb{R}$, es decir, una función $F : \mathbb{N} \cup \{0\} \to \mathbb{R}$ tal que cada término de la series se escribe de la siguiente forma*

$$x_n = F(n) - F(n-1), \qquad \text{para cada } n \geq 1.$$

A continuación, vamos a calcular una expresión para el término general de la sucesión de sumas parciales cuando estamos ante una serie telescópica. Atendiendo a la Defincón 8.6, si denotamos por S_n a las sumas parciales de la serie telescópica se tiene que

$$S_1 = F(1) - F(0), \qquad S_2 = x_1 + x_2 = F(2) - F(0), \qquad S_3 = x_1 + x_2 + x_3 = F(3) - F(0), \quad \ldots$$

En general, se puede probar que la fórmula para el término n-ésimo de la sucesión de sumas parciales es

$$S_n = x_1 + x_2 + \cdots + x_{n-1} + x_n = F(n) - F(0), \qquad \text{para todo } n \geq 1.$$

Por lo tanto, siempre que exista $\lim_{n\to\infty} F(n) = L$ y sea finito, la serie telescópica $\displaystyle\sum_{n=1}^{\infty} x_n$ es una serie convergente y el valor de su suma es $L - F(0)$.

Nota: *En el caso de que el índice del sumatorio empezara en un valor $n = N$ con $N \neq 1$, la serie sigue siendo telescópica pero el valor de su suma es $L - F(N-1)$.*

Ejemplo 8.8 Estudiar la convergencia de la serie infinita

$$\frac{1}{1}+\frac{1}{3}+\frac{1}{6}+\frac{1}{10}+\frac{1}{15}+\cdots=\sum_{n=1}^{\infty}\frac{2}{n\,(n+1)}.$$

Como pequeña nota histórica, mencionar que esta serie aparece por primera vez en 1665, cuando el matemático holandés Christiaan Huygens estudiaba un problema relacionado con probabilidades. Más tarde, en 1673, Huygens preguntó al matemático alemán Gottfried Leibniz sobre la convergencia de la serie. Leibniz observó que se trabata de la suma de los inversos de los números triangulares T_n cuya fórmula general viene dada por la expresión $2T_n = n(n+1)$.

Ahora bien, el término general de nuestra serie $x_n = 2/n(n+1)$ puede reescribirse de la siguiente forma

$$x_n=\frac{2}{n(n+1)}=\left(\frac{2}{n}-\frac{2}{n+1}\right)=-2\left(\frac{1}{n+1}-\frac{1}{n}\right)=F(n)-F(n-1),$$

donde, en este caso, $F(n) = -2/(n+1)$ para todo $n \geq 1$. Por lo tanto, estamos ante una serie infinita de tipo telescópica, ya que cada término x_n de la serie puede escribirse como $x_n = F(n) - F(n-1)$, para una cierta función F concreta. Como además $F(0) = -2$ y $L = \lim_{n\to\infty} F(n) = 0$, se tiene que la serie es convergente y el valor de su suma es $L - F(0) = 2$. Luego, resulta que

$$\sum_{n=1}^{\infty}\frac{2}{n\,(n+1)}=\frac{1}{1}+\frac{1}{3}+\frac{1}{6}+\frac{1}{10}+\frac{1}{15}+\cdots=2.$$

Ejemplo 8.9 La siguiente serie infinita

$$\frac{1}{1\cdot 2}+\frac{1}{2\cdot 3}+\frac{1}{3\cdot 4}+\frac{1}{4\cdot 5}+\cdots=\sum_{n=1}^{\infty}\frac{1}{n(n+1)},$$

es convergente y el valor de su suma es 1. En efecto, en este caso observamos que cada término x_n puede reescribirse como

$$x_n=\frac{1}{n(n+1)}=\frac{1}{n}-\frac{1}{n+1}=\frac{-1}{n+1}-\left(\frac{-1}{n}\right)=F(n)-F(n-1),$$

donde la función F viene dada por $F(n) = -1/(n+1)$ para todo $n \geq 1$. Por lo tanto, la serie anterior es telescópica. Como además y $F(0) = -1$ y $L = \lim_{n\to\infty} F(n) = 0$, se tiene que la serie infinita es convergente y el valor de su suma es $L - F(0) = 1$.

8.3 Criterios de convergencia

Hemos visto en la sección anterior que la sucesión de sumas parciales S_n permiten determinar fácilmente el comportamiento de la serie (convergente o divergente) hasta tal punto que podemos dar el valor exacto de la suma cuando la serie es convergente. Sin embargo, en la mayoría de los casos no se puede obtener una fórmula sencilla para la sucesión de sumas parciales, por lo que el estudio del carácter de una serie resulta bastante complicado. Es por ello que grandes matemáticos de principios del siglo XIX, como Cauchy o D'Alembert, se pusieron manos a la obra y desarrollaron criterios de convergencia en los que no es necesario saber conocer una fórmula explícita para la sucesión de sumas parciales de una serie infinita.

Uno de los primeros criterios que apareció involucra a aquellas series infinitas de las que sí sabemos su comportamiento (convergente o divergente), y es el conocido como criterio de comparación.

Proposición 8.1 (Criterio de comparación)

Si $\{x_n\}$ e $\{y_n\}$ son dos sucesiones numéricas de términos no negativos (esto es, $x_n, y_n \geq 0$ para todo $n \in \mathbb{N}$) tales que se cumple que $x_n \leq y_n$ para todo $n \geq 1$, entonces:

1. *Si la serie $\sum_{n=1}^{\infty} y_n$ es convergente, entonces la serie $\sum_{n=1}^{\infty} x_n$ también es convergente.*
2. *Si la serie $\sum_{n=1}^{\infty} x_n$ es divergente, entonces la serie $\sum_{n=1}^{\infty} y_n$ también es divergente.*

A grandes rasgos, la Proposición 8.1 nos dice que si una serie infinita está "controlada" (la terminología correcta es "acotada") superiormente por otra serie infinita que es convergente, entonces la primera serie también será convergente. La justificación matemática de este hecho es la siguiente: supongamos que tenemos dos series infinitas $\sum_{n=1}^{\infty} x_n$ y $\sum_{n=1}^{\infty} y_n$ con $x_n, y_n \geq 0$ para todo $n \in \mathbb{N}$ y tales que $x_n \leq y_n$ para todo $n \geq 1$. Denotemos por

$$S_n = x_1 + x_2 + \cdots + x_n \qquad \text{y} \qquad T_n = y_1 + y_2 + \cdots + y_n$$

las sucesión las sumas parciales de las series $\sum_{n=1}^{\infty} x_n$ y de $\sum_{n=1}^{\infty} y_n$, respectivamente.

Ahora bien, como se cumple que $x_n \leq y_n$ para todo $n \geq 1$, se tiene que $S_n \leq T_n$ para todo $n \geq 1$. Si, por ejemplo, la serie infinita $\sum_{n=1}^{\infty} y_n$ es convergente sabemos que existe el valor $T = \lim_{n\to\infty} T_n$ y que además al tratarse de una serie de términos no negativos se tiene que $T_n = y_1 + y_2 + \cdots + y_n \leq T$ para cada $n \geq 1$. Por último, como la serie $\sum_{n=1}^{\infty} x_n$ es de términos no negativos se tiene que la sucesión de sumas parciales S_n es creciente. Como además se cumple que $S_n \leq T_n$ para todo $n \geq 1$, se tiene que la sucesión S_n está acotada superiormente por T. Por lo tanto, al ser S_n una sucesión creciente y acotada superiormente, se tiene que existe $S = \lim_{n\to\infty} S_n$ que es, precisamente, el valor de la suma de la serie $\sum_{n=1}^{\infty} x_n$. De hecho se cumple simpre que $S \leq T$.

Con una idea similar a la utilizada en el párrafo anterior se puede probar el criterio de acotación en lo relativo a series divergentes.

Ejemplo 8.10 La serie infinita dada por

$$\frac{1}{4} + \frac{1}{9} + \frac{1}{16} + \frac{1}{25} + \cdots = \sum_{n=1}^{\infty} \frac{1}{(n+1)^2}.$$

es una serie convergente. En efecto, ya que es fácil observar que para todo $n \geq 1$ se cumple la desigualdad $(n+1)^2 = (n+1)(n+1) \geq n(n+1)$. Como además, en virtud del Ejemplo 8.9, sabemos que la serie $\sum_{n=1}^{\infty} \frac{1}{n(n+1)}$ es convergente, por lo que aplicando el criterio de comparación podemos concluir que la serie $\sum_{n=1}^{\infty} \frac{1}{(n+1)^2}$ también es convergente. Además, como el valor de la suma de la serie $\sum_{n=1}^{\infty} \frac{1}{n(n+1)}$ es igual a 1,

podemos asegurar que el valor de su suma de la serie $\displaystyle\sum_{n=1}^{\infty}\frac{1}{(n+1)^2}$ es menor o igual que 1.

Ejemplo 8.11 La serie infinita dada por

$$\frac{1}{1!}+\frac{1}{2!}+\frac{1}{3!}+\frac{1}{4!}+\cdots=\sum_{n=1}^{\infty}\frac{1}{n!}$$

es convergente. En este ejemplo, a diferencia del anterior, la acotación que podemos obtener para las sumas parciales no es tan evidente. Sin embargo, usando la inducción matemática se puede probar que para todo $n\geq 1$ se cumple la desigualdad $2^{n-1}\leq n!$, por lo que tenemos que $1/n!\leq 1/2^{n-1}$, para todo $n\geq 1$. Por lo tanto, hacemos una comparación con una serie geométrica de la forma

$$\frac{1}{1!}+\frac{1}{2!}+\frac{1}{3!}+\cdots+\frac{1}{n!}\leq 1+\frac{1}{2}+\frac{1}{4}+\cdots+\frac{1}{2^{n-1}}\leq\sum_{n=0}^{\infty}\frac{1}{2^n}.$$

Como además, en virtud del Ejemplo 8.7, sabemos que la serie geométrica $\displaystyle\sum_{n=0}^{\infty}\frac{1}{2^n}$ es convergente, aplicando el criterio de comparación podemos concluir que la serie $\displaystyle\sum_{n=1}^{\infty}\frac{1}{n!}$ también es convergente. Además, como el valor de la suma de la serie $\displaystyle\sum_{n=0}^{\infty}\frac{1}{2^n}$ es igual a 2, podemos asegurar que el valor de su suma de la serie $\displaystyle\sum_{n=1}^{\infty}\frac{1}{n!}$ es menor o igual que 2.

Nota: *La Proposición 8.1 no es cierta, en general, cuando se consideran series infinitas cuyos términos sean negativos. Por ejemplo, consideremos la serie geométrica de razón $r=1/2$ dada por $\displaystyle\sum_{n=0}^{\infty}\frac{1}{2^n}$ y la serie constante dada por $\displaystyle\sum_{n=1}^{\infty}(-1)$. Observamos que la serie geométrica controla superiormente a la serie constante (ya que se cumple la desigualdad $-1<1/2^n$, para todo $n\geq 1$). Sin embargo, es fácil comprobar la serie constante es divergente mientras que la serie geométrica es convergente.*

Una de las aplicaciones más interesantes del criterio de comparación es la siguiente: Supongamos que en la paradoja de Zenón, la velocidad del corredor no es constante sino que disminuye de tal forma que necesita T minutos para ir de 1 a $1/2$, $T/2$ minutos para ir de $1/2$ a $1/4$, $T/3$ minutos para ir de $1/4$ a $1/8$ y así sucesivamente. En general, el corredor invierte T/n minutos para ir de $1/2^{n-1}$ a $1/2^n$.

Por lo tanto, el tiempo empleado el corredor para ir desde el punto de partida hasta el punto de meta viene dado por la serie infinita

$$T+\frac{T}{2}+\frac{T}{3}+\frac{T}{4}+\cdots+\frac{T}{n}+\frac{T}{n+1}+\ldots$$

Esta serie es, esencialmente, conocida como **serie amónica**

$$1+\frac{1}{2}+\frac{1}{3}+\frac{1}{4}+\cdots+\frac{1}{n}+\frac{1}{n+1}+\cdots=\sum_{k=1}^{\infty}\frac{1}{k},$$

la cual fue estudiada nada más y nada menos que por Pitágoras.

A priori, podríamos pensar que esta serie debe ser convergente ya que, al igual que ocurre con las series geométricas, en cada paso vamos sumando una cantidad cada vez más pequeña. Sin embargo, eso no es del todo cierto: es verdad, esta serie crece lento pero lo que añadimos no es lo suficientemente pequeño como para evitar que la suma crezca indefinidamente. En otras palabras, la serie armónica es divergente. ¡Flipa colega!

Para ver esto, vamos a estudiar cómo se comportan las siguientes sumas parciales de esa serie

$$S_2 = 1 + \frac{1}{2} \geq \frac{1}{2} + \frac{1}{2},$$
$$S_4 = 1 + \frac{1}{2} + \left(\frac{1}{3} + \frac{1}{4}\right) \geq \frac{1}{2} + \frac{1}{2} + \left(\frac{1}{4} + \frac{1}{4}\right) = \frac{1}{2} + \frac{1}{2} + \frac{1}{2},$$
$$S_8 = 1 + \frac{1}{2} + \left(\frac{1}{3} + \frac{1}{4}\right) + \left(\frac{1}{5} + \frac{1}{6} + \frac{1}{7} + \frac{1}{8}\right) \geq \frac{1}{2} + \frac{1}{2} + \left(\frac{1}{4} + \frac{1}{4}\right) + \left(\frac{1}{8} + \frac{1}{8} + \frac{1}{8} + \frac{1}{8}\right) = \frac{1}{2} + \frac{1}{2} + \frac{1}{2} + \frac{1}{2},$$
$$S_{16} = 1 + \frac{1}{2} + \left(\frac{1}{3} + \frac{1}{4}\right) + \left(\frac{1}{5} + \cdots + \frac{1}{8}\right) + \left(\frac{1}{9} + \cdots + \frac{1}{16}\right) \geq \frac{1}{2} + \frac{1}{2} + \frac{1}{2} + \frac{1}{2} + \frac{1}{2}.$$

En general, se puede probar que $S_{2^n} \geq (n+1)/2$ para todo $n \geq 1$. Por lo tanto, en virtud del criterio de comparación, podemos concluir que la serie armónica es divergente al estar controlada inferiormete por una serie constante. El hecho de que la serie armónica sea divergente, implica que **en este caso nuestro corredor nunca llegaría a la línea de meta**.

El siguiente criterio, conocido como *Criterio del resto*, establece una condición necesaria que debe cumplir toda aquella serie que sea convergente.

Proposición 8.2 (Criterio del resto)

Si la serie $\displaystyle\sum_{n=1}^{\infty} x_n$ *es convergente, entonces debe ocurrir que* $\lim_{n\to\infty} x_n = 0$.

Demostración Denotemos por (S_n) la sucesión de las sumas parciales asociada a la sucesión (x_n), es decir, $S_n = \displaystyle\sum_{n=1}^{\infty} x_n$. Observamos que si la serie es convergente, entonces existe el límite $L = \lim_{n\to\infty} S_n$ y que además L es una cantidad finita. Teniendo en cuenta que $x_n = S_n - S_{n-1}$ para todo $n \geq 2$, se tiene que

$$\lim_{n\to\infty} x_n = \lim_{n\to\infty} (S_n - S_{n-1}) = \lim_{n\to\infty} S_n - \lim_{n\to\infty} S_{n-1} = L - L = 0.$$

■

Es importante señalar que la condición $\lim_{n\to\infty} x_n = 0$ no es suficiente para la convergencia de una serie, tal y como ocurre con la serie armónica.

La verdadera utilidad del criterio anterior es que proporciona una condición suficiente para la divergencia de una serie, y es por eso que a veces recibe el nombre de **criterio de divergencia**.

Proposición 8.3 (Criterio de la divergencia)

Si $\lim_{n\to\infty} x_n \neq 0$, *entonces la serie* $\displaystyle\sum_{n=1}^{\infty} x_n$ *es divergente.*

Ejemplo 8.12 La serie infinita dada por

$$\frac{1}{101} + \frac{2}{102} + \frac{3}{103} + \frac{4}{104} + \cdots = \sum_{n=1}^{\infty} \frac{n}{n+100},$$

es divergente. En efecto, dado que $\lim_{n\to\infty} n/(n+100) = 1$, en virtud del criterio de la divergencia se tiene que

la serie $\sum_{n=1}^{\infty} \frac{n}{n+100}$ diverge.

Nota: *El recíproco de la Proposición 8.2 no es cierto, en genral. Por ejemplo, si consideramos la serie armónica* $\sum_{n=1}^{\infty} \frac{1}{n}$ *vemos que el límite* $\lim_{n\to\infty} \frac{1}{n} = 0$, *pero la serie armónica es divergente. Por lo tanto, el hecho de que una serie* $\sum_{n=1}^{\infty} x_n$ *verifique la condición* $\lim_{n\to\infty} x_n = 0$ *no es suficiente para asegurar que la serie sea convergente.*

Ejercicios Propuestos

1. Estudiar la convergencia de la serie
$$\frac{1}{\log(1)} + \frac{1}{\log(2)} + \frac{1}{\log(3)} + \frac{1}{\log(4)} + \cdots = \sum_{n=1}^{\infty} \frac{1}{\log(n)}$$
donde $\log(n)$ hace referencia al logaritmo neperiano.
Pista: Probar por inducción que $\log(n) \leq n$, para todo $n \geq 1$.

2. Estudiar la convergencia de la serie
$$2^{-\log(1)} + 2^{-\log(2)} + 2^{-\log(3)} + \cdots = \sum_{n=1}^{\infty} 2^{-\log(n)}$$
donde $\log(n)$ hace referencia al logaritmo neperiano.

3. Probar que la serie los formada por inversos de los cuadrados de los enteros positivos
$$\frac{1}{1^2} + \frac{1}{2^2} + \frac{1}{3^2} + \frac{1}{4^2} + \frac{1}{5^2} + \cdots = \sum_{n=1}^{\infty} \frac{1}{n^2}$$
es convergente.

4. Calcular la suma de la serie
$$\frac{3}{1\cdot 2\cdot 3} + \frac{5}{2\cdot 3\cdot 4} + \frac{7}{3\cdot 4\cdot 5} + \frac{9}{4\cdot 5\cdot 6} + \cdots = \sum_{n=1}^{\infty} \frac{2n+1}{n(n+1)(n+2)}.$$

5. Sea $|r| < 1$. Probar que la siguiente serie aritmético-geométrica
$$\sum_{n=1}^{\infty} (an+b)\, r^n, \qquad (a, b \geq 0)$$
es convergente y además su valor es $S = ar/(1-r)^2 + b/(1-r)$.

6. Supongamos que para la serie $\displaystyle\sum_{n=1}^{\infty} x_n$ existe una función $F : \mathbb{N} \to \mathbb{R}$ tal que para cada $n \geq 1$ se tiene que $x_n = F(n+2) - F(n)$. Demuestra que la serie es convergente y que el valor de su suma es $L - (\, F(1) + F(2)\,)$, siendo $L = \lim_{n\to\infty} F(n)$.

7. Calcular la suma de la serie
$$\frac{1}{3} + \frac{1}{8} + \frac{1}{15} + \frac{1}{24} + \cdots = \sum_{n=2}^{\infty} \frac{1}{n^2-1}.$$
Pista: Utiliza el ejercicio anterior, descomponiendo el término general de la forma
$$x_n = \frac{1}{n^2-1} = \frac{1}{(n-1)(n+1)} = \frac{1}{2}\left(\frac{1}{n-1} - \frac{1}{n+1}\right).$$

8. Sea $\displaystyle\sum_{n=1}^{\infty} a_n$ una serie convergente de términos positivos. Probar que la serie $\displaystyle\sum_{n=1}^{\infty} \sqrt{a_n}/n$ es convergente.

Bibliografía Adicional

1. Apostol, T. M. (1991). Sucesiones, Series e Integrales Impropias. *Calculus, Volume 1*. Editorial John Wiley & Sons, 457-515.

CAPÍTULO 9

9 PRINCIPIO EXTREMAL

Ana Navarro Quiles
Universitat de València

Palabras clave

- *Principio extremal*
- *Método variacional*
- *Principio de buena ordenación*
- *Valor extremo*

El principio extremal es un método de demostración que, usado de forma correcta, suele llevar a soluciones de problemas complejos de una forma considerablemente corta y sencilla. En muchos problemas se pide analizar la existencia de un objeto que cumple ciertas condiciones. El principio extremal consiste en prestar atención a los objetos que maximizan o minimizan alguna función, convenientemente relacionada con la condición dada en el problema, y tratar de probar por reducción al absurdo que estos objetos cumplen la condición pedida. Es decir, por reducción al absurdo, partimos de que no se cumple el enunciado a probar. Se muestra que el objeto resultante tiene la propiedad deseada mostrando que una pequeña perturbación (o variación, de ahí método de las variaciones) incrementa (en el caso del máximo) o disminuye (en el del mínimo) el valor dado de una función convenientemente definida, llegando a una contradicción.

El capítulo se organiza en dos secciones. En la primera sección, definiremos el método del principio extremal así como sus condiciones de aplicabilidad, haciendo un breve repaso sobre algunas propiedades que nos aseguran la existencia de valores extremos, ya sea máximo o mínimo. Algunos ejemplos de aplicación del método, entre los que encontramos el famoso problema de Sylvester, serán resueltos en la sección 2.

9.1 Introducción

El principio extremal se basa en el análisis de los máximos/mínimos de una expresión previamente definida. Pero, esta expresión, dependiendo del problema a resolver, puede ser una función, una sucesión, un conjunto, etc. Para poder aplicar dicho método, tenemos que tener claro el concepto de máximo y mínimo. Introducimos a continuación el concepto de máximo y mínimo de una función y de un conjunto.

Definición 9.1 (Máximo y mínimo local)

*Sea $f : A \subset \mathbb{R}^n \to \mathbb{R}$, $x_0 \in A$ y $P = (x_0, f(x_0))$ un punto perteneciente a la gráfica de la función. Se dice que P es un **máximo local** de f, si existe un entorno de centro x_0, $\mathcal{E}_{x_0} \subset A$, tal que para todo $x \in \mathcal{E}_{x_0}$ se cumple $f(x) < f(x_0)$.*
*Análogamente, el punto P és un **mínimo local** de f, si existe un entorno de centro x_0, $\mathcal{E}_{x_0} \subset A$, tal que para todo $x \in \mathcal{E}_{x_0}$ se cumple $f(x) > f(x_0)$.*

Definición 9.2 (Máximo y mínimo global)

*Sea $f : A \subset \mathbb{R}^n \to \mathbb{R}$, $x_0 \in A$ y $P = (x_0, f(x_0))$ un punto perteneciente a la gráfica de la función. Se dice que P es un **máximo global** de f, si para todo $x \in A$, x distinto de x_0, se cumple $f(x) < f(x_0)$.*
*Análogamente, el punto P és un **mínimo global** de f, si para todo $x \in A$, x distinto de x_0, se cumple $f(x) > f(x_0)$.*

Definición 9.3 (Máximo y mínimo de un conjunto)

*Decimos que K es **cota superior** del conjunto D si $x \leq K$ para todo x del conjunto. A la menor de las cotas superiores de D se le denomina **supremo**. Si el supremo pertenece al conjunto se le llama **máximo** (o último elemento).*
*Análogamente, decimos que k es **cota inferior** del conjunto D si $x \geq k$ para todo x del conjunto. A la mayor de las cotas inferiores de D se le denomina **ínfimo**. Si el ínfimo pertenece al conjunto se le llama **mínimo** (o primer elemento).*

El principio extremal consiste en examinar los objetos que maximizan o minimizan una función/conjunto relacionada con la condición del problema con el objetivo de llegar a una contradicción.

Nota: *Supongamos problemas en los que puedas ordenar los elementos que aparecen en él. Es decir, tenemos un conjunto $A = \{a_1, ..., a_n\}$ formado por n elementos ordenables, los cuales cumplen una cierta condición. Supongamos que los elementos ya están ordenados, es decir, el primer elemento va a ser el más pequeño y el último el más grande. El principio extremal consiste en suponer que a es el mínimo y probar que existe otro $a^* \in A$ tal que $a^* < a$, siendo a^* otro elemento que también lo cumple la condición dada. Por lo que se llegaríamos a una contradicción.*

Como hemos indicado anteriormente, este método de demostración se puede aplicar siempre y cuando exista ese objeto que minimiza o maximiza dicha función o conjunto. Por tanto, vamos a recordar a continuación tres propiedades importantes para la existencia de elemento mínimo o máximo.

Proposición 9.1 (Existencia de mínimo o máximo)

1. *Todo conjunto finito no vacío de números reales tiene elemento minimal y maximal, los cuales no tienen por que ser únicos.*
2. *Todo subconjunto no vacío de enteros positivos contiene un elemento que es el más pequeño. Esta propiedad se conoce como el* ***principio de buena ordenación****.*
3. *Un conjunto infinito de números reales no tiene porque tener elemento minimal o maximal. Si el conjunto está acotado superiormente, entonces tiene supremo. Análogamente, si está acotado inferiormente, tiene ínfimo.*

Ejemplo 9.1 $n\sqrt{2}$ no es entero para cualquier entero positivo n.
Supongamos que existe n entero positivo tal que $n\sqrt{2}$ es entero. Vamos ahora a aplicar el principio extremal para llegar a una contradicción de esta afirmación.
Sea S el conjunto de todos los enteros positivos que cumplen la condición indicada, es decir,

$$S = \{n \in \mathbb{N} : n\sqrt{2} \text{ es entero}\}.$$

Como $S \neq \emptyset$ (distinto del vacío), por el principio de buena ordenación, existe el menor elemento, que denotaremos por $k \in S$. Sea el entero positivo $(\sqrt{2}-1)k$, entonces

$$(\sqrt{2}-1)k\sqrt{2} = 2k - k\sqrt{2} \in \mathbb{N}.$$

Ya que ambos términos son enteros positivos y $2 > \sqrt{2}$. De esta forma, por definición del conjunto S, $(\sqrt{2}-1)k \in S$. Pero:

$$(\sqrt{2}-1)k < k.$$

Lo que nos lleva a contradicción con la hipótesis de que k es el menor elemento de S. Por tanto S es vacío, lo que implica que $n\sqrt{2}$ no es entero para cualquier $n \in \mathbb{N}$.

9.2 Aplicación del principio extremal

En esta sección vamos a resolver algunos problemas aplicando el método del principio extremal. En particular, para ver su gran versatilidad, resolveremos tres problemas, cada uno perteneciente a un área diferente de las matemáticas: geometría, teoría de grafos y teoría de números.

Problema de Sylvester

Comenzaremos con la resolución de una famoso problema propuesto por Sylvester en 1893. Este problema matemático permaneció abierto hasta 1933 cuando Tibor Gallai publicó una complicada solución apelando a argumentos de geometría proyectiva. La solución que se propone a continuación con el uso del principio extremal es mucho más sencilla y fue hallada por Leroy Milton Kelly en 1948.

Problema 9.1 Sea S un conjunto finito de puntos en el plano, con la propiedad de que la recta determinada por dos puntos cualquiera del conjunto S pasa al menos por un tercer punto de S. Entonces, todos los puntos de S están alineados.
Solución *Supongamos que los puntos no están todos alineados y vamos a llegar a una contradicción usando*

el principio extremal. Sea A el conjunto de todos los pares de la forma (P, r), definido de la siguiente forma:

$$A = \left\{ (P, r) : \begin{array}{l} r \text{ recta que pasa por dos puntos de } S \\ P \in S \text{ punto por el que } r \text{ no pasa} \end{array} \right\}.$$

Es decir, r es una recta que pasa por dos puntos del conjunto S (y por tanto por al menos un tercer punto, por hipótesis), pero no por P. Ahora, elegimos un punto p que minimiza la distancia de p a r (principio extremal, buscamos un extremo y queremos llegar a contradicción). Sea f el pie de la perpendicular de p a r. Como hemos indicado, r contiene al menos 3 puntos que llamaremos a, b y c. Debe haber dos de ellos, digamos a y b de un mismo lado de f. Sea b el que está más cerca de f de los dos. Entonces la distancia de b a la recta que une a y p es menor que la distancia de p a f. Por lo que llegamos a una contradicción, ya que hemos partido de la hipótesis de que la distancia del punto p a la recta r era la mínima. En la Figura 9.1 se encuentran los detalles gráficos de la resolución de este problema.

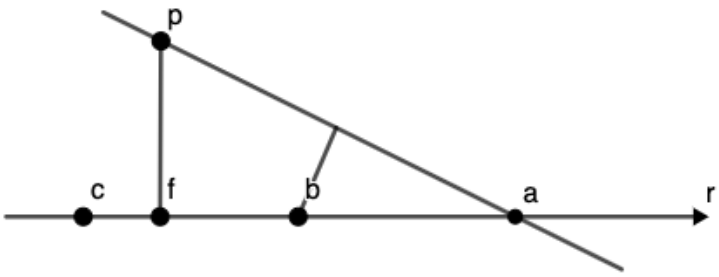


Figura 9.1: Detalles gráficos de la resolución del problema de Sylvester.

Nota: *El problema de Sylvester también puede ser encontrado en la literatura de forma más intuitiva como* ***problema del huerto****. Juanmi quiere plantar árboles y no quiere que estén todos en la misma línea. La condición para plantar es la siguiente: si una línea recta pasa por solo dos árboles tiene que plantar otro árbol en la misma línea, para que haya tres. Así Juanmi observó que a medida que agregaba árboles para eliminar una línea con dos árboles, otras nuevas líneas con dos árboles aparecían. Por ejemplo, si queremos plantar cuatro árboles, plantamos primero dos y en la misma línea tenemos que plantar el tercero. Para el cuarto, como no puede estar en la misma línea, lo plantamos fuera. Pero entonces existen líneas con únicamente dos árboles, por lo que no se cumple la propiedad. La única forma de cumplirla es alineando los cuatro árboles.*

Aplicación a la teoría de grafos

Problema 9.2 Todas las calles de Valdemadera son de un único sentido. Cada par de casas están conectadas exactamente por un camino de sentido dirigido. Vamos a demostrar que existe una casa que se puede alcanzar desde cada casa directamente o como mucho via otra vivienda.

Solución *Sea m el número máximo de caminos directos que conducen a cualquier casa, y sea M una casa para la cual se alcanza este máximo. Sea D el conjunto de las m casas que conectan directamente con M. Sea R el conjunto de todas las casas exceptuando a M y a las m casas en D. Observamos que:*

- *Si R es vacío, directamente se prueba el enunciado.*
- *Ahora, si no es vacío, sea $X \in R$, entonces existe E elemento del conjunto D con conexión $X \to E \to M$. Si no existiera tal E, entonces se podría llegar a X directamente desde todas las ciudades en D y desde M, es decir, $m + 1$ caminos conducirían a X, lo que contradice la suposición sobre M (la casa para*

la que se alcanza el máximo m). De esta forma queda probado el enunciado bajo las condiciones del problema.

En la Figura 9.2 se encuentran los detalles gráficos de la resolución de este problema.

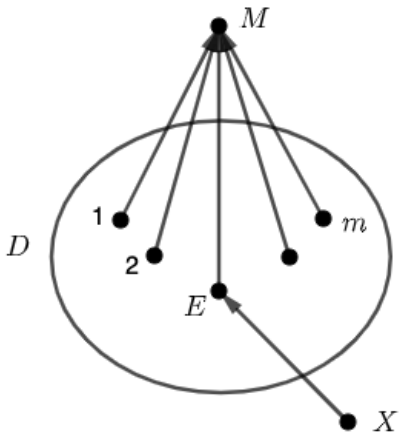


Figura 9.2: Detalles gráficos de la aplicación del principio extremal a un problema de teoría de grafos.

Aplicación a la teoría de números

Problema 9.3 No existen cuatro enteros positivos (x, y, z, u) que cumplan la siguiente relación:

$$x^2 + y^2 = 3(z^2 + u^2).$$

Solución *Supongamos que existe dicho cuádruplo y vamos a llegar a una contradicción, usando el principio extremal. Sea A el conjunto de todos los cuádruplos que cumplen la relación indicada en el enunciado*

$$A = \{(x, y, z, u) \in \mathbb{N}^4 \, : \, x^2 + y^2 = 3(z^2 + u^2)\}.$$

Sea (a, b, c, d) aquel con menor $x^2 + y^2$. Entonces las siguientes implicaciones se cumplen

$$a^2 + b^2 = 3(c^2 + d^2) \Longrightarrow 3|a^2 + b^2 \Longrightarrow 3|a \text{ y } 3|b \Longrightarrow a = 3a_1 \text{ y } b = 3b_1.$$

Por lo tanto

$$3(c^2 + d^2) = a^2 + b^2 = (3a_1)^2 + (3b_1)^2 = 9(a_1^2 + b_1^2) \Longrightarrow (c^2 + d^2) = 3(a_1^2 + b_1^2).$$

De esta forma, hemos encontrado un cuádruplo $(c, d, a_1, b_1) \in A$. Pero $c^2 + d^2 < a^2 + b^2$, lo que nos llevo a contradicción.

9.3 Problemas de olimpiadas matemáticas

Finalizamos esta serie de problemas, relativos al uso del principio extremal, con el siguiente problema enunciado para la olimpiada matemática húngara de 1990. Destacar que en este caso, aplicamos dicho método a un problema geométrico.

Problema 9.4 (Hungary Mathematical Olympiad, 1990). Considera un camino en el plano siguiendo las siguientes reglas: dado un punto (x, y) nos podemos mover en un paso a uno de los cuatro puntos $(x, y + 2x)$, $(x, y - 2x)$, $(x - 2y, y)$, $(x + 2y, y)$ con la restricción que no podemos volver atrás el paso que acabamos de hacer. Probar que, si comenzamos en el punto $P = (1, \sqrt{2})$ no podemos volver a dicho punto nunca más.

Solución *El punto P no está en las rectas $x = 0$, $y = 0$, $y = x$ e $y = -x$. Entonces, exactamente uno de los cuatro posibles pasos nos deja cerca del origen, mientras que los tres restantes nos dejan alejados. Como la relación de las coordenadas de P es irracional al comienzo, la regla anterior sigue siendo válida durante todo el recorrido.*

Supongamos que después de n pasos volvemos al punto inicial, es decir,

$$P_0P_1...P_n = P_0 = (1, \sqrt{2}).$$

Si P_i es el punto más lejano del origen del camino cerrado obtenido, entonces:

$$d(OP_{i-1}) < d(OP_i) > d(OP_{i+1}), \quad \text{donde } d(OP_i) \text{ es la distancia del origen al punto } P_i.$$

Entonces, el único paso posible desde el punto P_i hacia el origen nos obliga a volver a P_{i-1}. Y esto es una contradicción, dado que no tenemos permitido volver atrás.

Ejercicios Propuestos

1. Cada punto reticular del plano cartesiano está etiquetado con un número entero positivo. Cada uno de estos números es la media aritmética de sus cuatro vecinos (arriba, abajo, izquierda, derecha). Demuestra que todas las etiquetas son iguales.

Definición 9.4

*Un P de coordenadas (x, y) se llama **reticular** si x e y son números enteros, es decir, si $x, y \in \mathbb{Z}$. Un plano reticular es el conjunto de puntos del plano cartesiano que son reticulares.*

2. Encuentra todas las soluciones positivas del sistema de ecuaciones:

$$x_1 + x_2 = x_3^2, \quad x_2 + x_3 = x_4^2, \quad x_3 + x_4 = x_5^2, \quad x_4 + x_5 = x_1^2, \quad x_5 + x_1 = x_2^2.$$

Bibliografía Adicional

1. Engel, A. (1998). The Extremal Principle. *Problem-Solving Strategies*. Editorial Springer, 39-58.

CAPÍTULO 10

10 PROBLEMAS DE COLORACIÓN

Eva Primo Tárraga
Universidad Rey Juan Carlos

Palabras clave

- *Coloración*
- *Conjunto*
- *Subconjuntos*
- *Respuesta negativa*
- *Tabla*
- *Tablero*

Los problemas de este capítulo están relacionados con la partición de un conjunto en subconjuntos que nos ayuden a argumentar nuestra solución al problema. Esta partición la realizaremos coloreando cada elemento de nuestro conjunto en función del subconjunto al que pertenezcan.

10.1 Introducción

Vamos a introducir este método a través de un problema en el que es útil. Imaginaos que tenemos un tablero de 8x8 cuadrados, como este, es como un tablero de ajedrez, pero sin colorear.

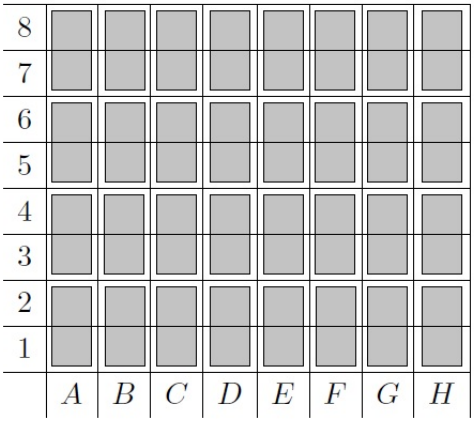
8								
7								
6								
5								
4								
3								
2								
1								
	A	B	C	D	E	F	G	H

2	
1	
	A

1		
	A	B

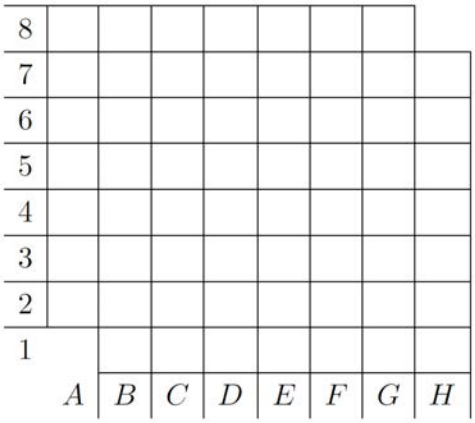
Nuestro objetivo es cubrirlo con piezas de 2x1 o 1x2 cuadrados, como las piezas de un dominó, sin que estas piezas se superpongan ni salgan del tablero.

Tenemos un número par de cuadros en el tablero, así que a priori parece sensato querer cubrirlo con piezas compuestas por dos cuadrados. Además, cada lado del tablero tiene un número par de cuadrados lo que facilita el razonamiento. Podríamos dar como solución posicionar cuatro piezas de dominó alineadas, formando una tira de 8x1, en cada una de las 8 columnas de nuestro tablero inicial, y alcanzaríamos nuestro objetivo, cubrir un tablero 8x8 con piezas 2x1.



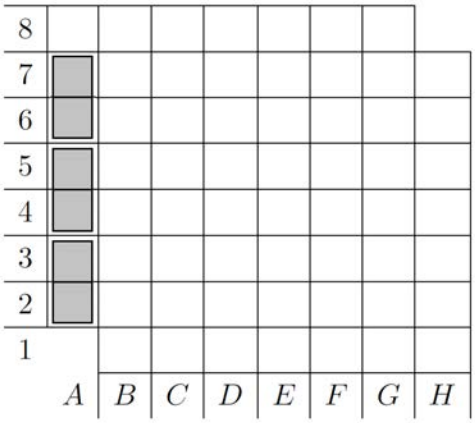
De este problema existen múltiples soluciones, es decir, muchas maneras de posicionar las 32 piezas 2x1 o 1x2 sobre el tablero. De hecho, el físico teórico Michael E. Fisher demostró en 1961 que existen $2^4 \times 901^2 = 12988816$, lo que son casi 13 millones de maneras diferentes de posicionar dichas piezas sobre el tablero.

Imaginemos ahora una situación ligeramente diferente, en la que tenemos dicho tablero 8x8 menos dos cuadrados, concretamente los cuadrados de dos esquinas opuestas, por ejemplo, el primero y el último, es decir el A1 y el H8.

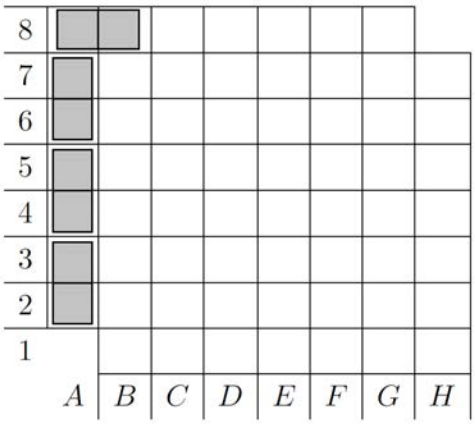


Seguimos teniendo un número par de cuadrados, así que sigue sin ser descabellado plantearnos cubrirlo con piezas de 2x1 o 1x2 cuadrados.

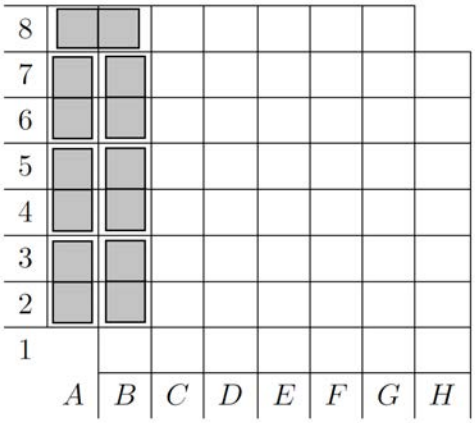
Intentémoslo, empezamos cubriendo la primera columna, la A, cubriríamos los cuadrados A2 y A3, luego A4 y A5, después A6 y A7,



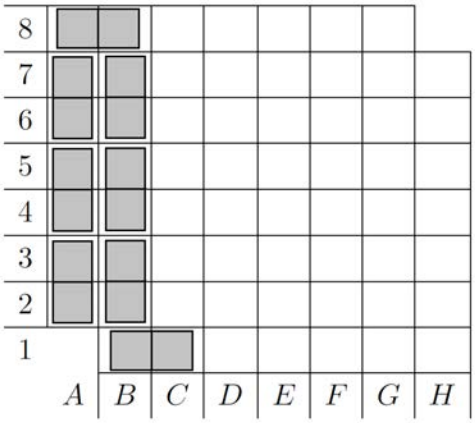
y para cubrir el último cuadrado necesitaríamos posicionar la pieza sobre A8 y B8.



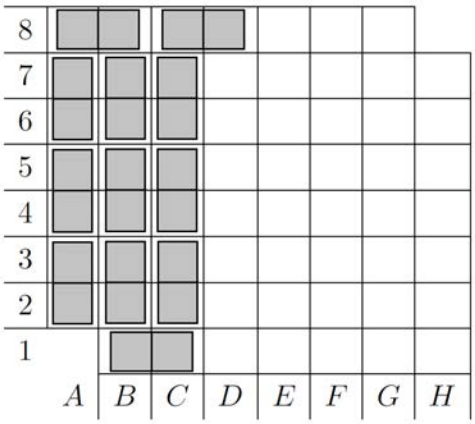
Esto nos vuelve a dejar una columna con 7 cuadrados por cubrir; utilizando 3 piezas 2x1, cubriríamos los 6 cuadros centrales, lo que no dejaría sin cubrir el cuadrado B1.



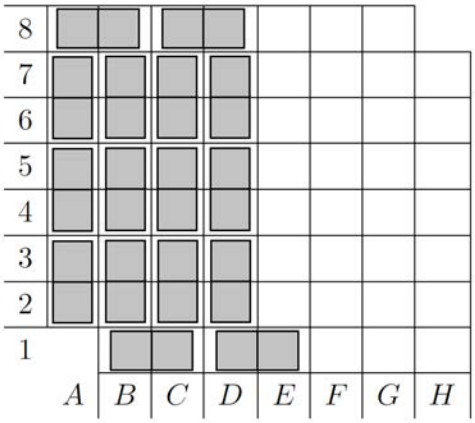
Para cubrir dicho cuadrado necesitamos colocar la pieza cubriendo B1 y C1,



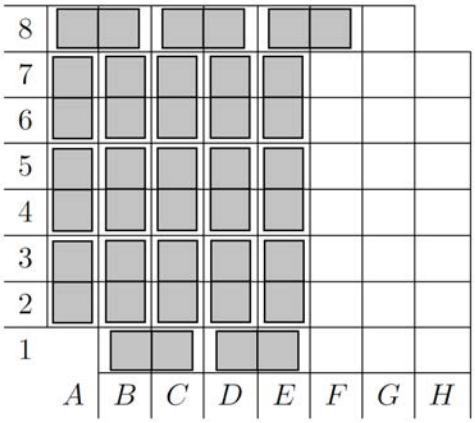
lo que nos deja en la columna C una situación análoga a la de la columna A, es decir, para cubrir la pieza C8, necesitaríamos posicionar la pieza cubriendo C8 y D8.



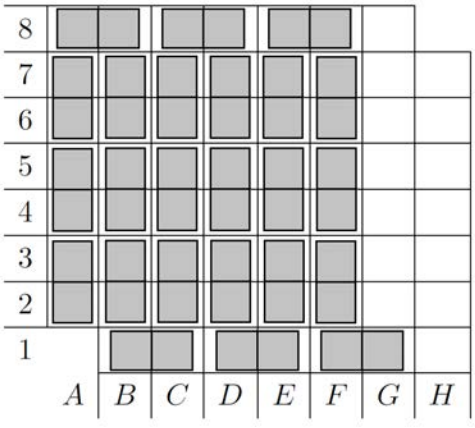
Esto nos deja en la columna D una situación análoga a la de la columna B, es decir, para cubrir la pieza D1, necesitaríamos posicionar la pieza cubriendo D1 y E1.



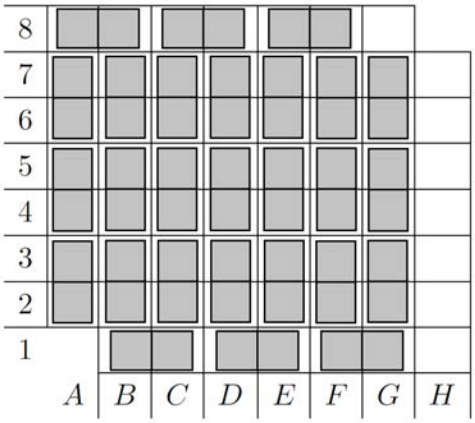
Lo que nos deja en la columna E una situación análoga a la de la columna A, es decir, para cubrir la pieza E8, necesitaríamos posicionar la pieza cubriendo E8 y F8.



Esto nos deja en la columna F una situación análoga a la de la columna B, es decir, para cubrir la pieza F1, necesitaríamos posicionar la pieza cubriendo F1 y G1.

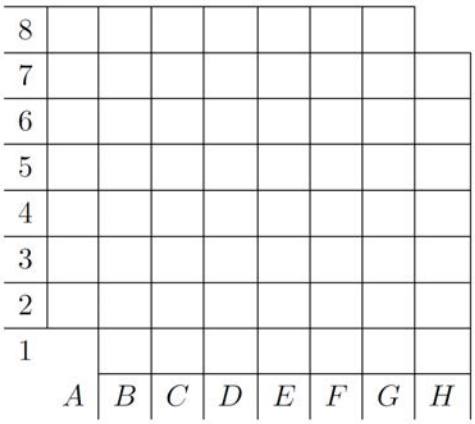


Lo que nos deja en la columna G una situación análoga a la de la columna A, es decir, para cubrir la pieza G8, necesitaríamos posicionar la pieza cubriendo G8 y H8, lo que no es posible, dado que es uno de los cuadrados que hemos quitado inicialmente del tablero.

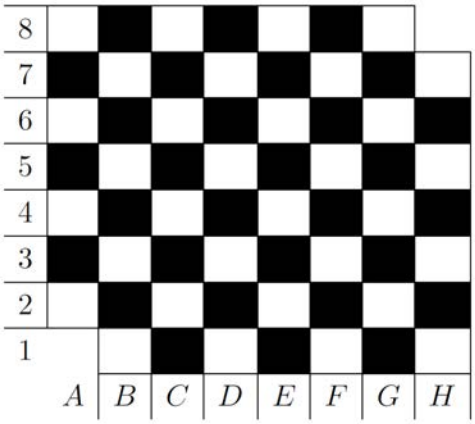


Este razonamiento sirve para ver que no podemos cubrir el tablero de esta manera, pero no demuestra que no haya otra manera de cubrirlo.

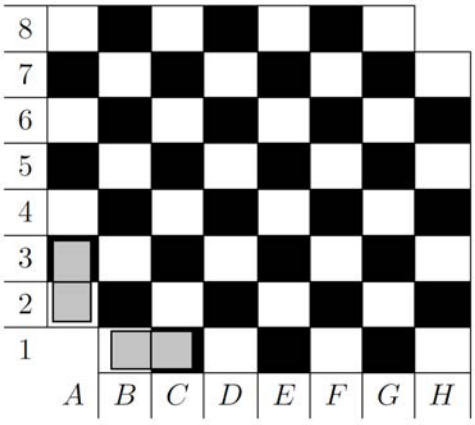
Volvamos a la tabla que queremos cubrir.



Vamos a colorearla de forma que nos ayude a razonar. En este caso, como un tablero de ajedrez, de manera que un cuadrado blanco no comparta lado con otro cuadrado blanco.



De esta manera si posicionamos una pieza 2x1 o 1x2 cubriendo este tablero, siempre cubrirá un cuadro blanco y otro negro.

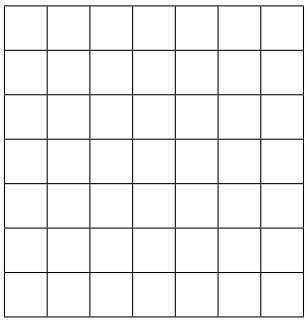


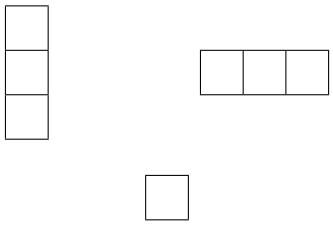
Por lo tanto, cualquier superficie cubierta con piezas de este tipo tendrá la misma cantidad de cuadrados blancos que negros. Pero si contamos, tenemos 30 cuadros blancos, pero 32 cuadros negros, lo que muestra que es imposible cubrir este tablero modificado con piezas 2x1 o 1x2.

Para este problema en concreto ha sido suficiente con dos colores, pero es común necesitar más.

10.2 Aplicaciones del método a la Tabla 7x7

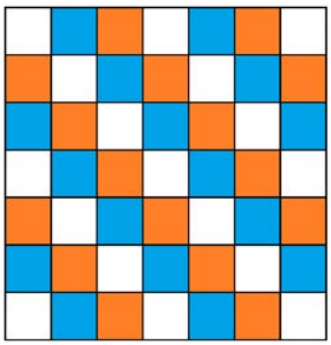
Para este nuevo problema tenemos una tabla 7x7, es decir, 49 cuadrados. Y queremos cubrirlo con 16 piezas 3x1, o 1x3, según las coloquemos, y una pieza 1x1. La pregunta que se nos plantea es: ¿dónde deberíamos situar dicha pieza 1x1?



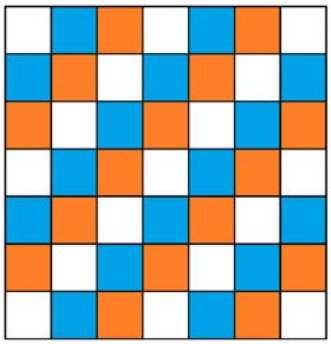


Pensad que en el problema anterior trabajábamos con piezas 2x1, o 1x2, y nos ayudó colorear nuestra tabla con dos colores. Ahora tenemos piezas 3x1, es razonable pensar que necesitaremos más colores.

Principalmente, las piezas que queremos colocar son piezas 3x1, por lo que nos interesa utilizar 3 colores en nuestra coloración, y situarlos de manera que cada pieza 3x1, o 1x3, tape un cuadrado de cada color.



En particular, esta coloración, en la que hemos pintado cada diagonal de un color, siguiendo el mismo patrón, blanco-azul-naranja, cumple que efectivamente cada pieza 3x1, o 1x3, cubre un cuadrado de cada color. Ahora contemos cuantos cuadros tenemos de cada color. Tenemos 16 cuadros azules, 16 cuadros naranjas y 17 cuadros blancos, por lo tanto, podemos afirmar que la pieza 1x1 debe cubrir un cuadro blanco.
¿Pero podemos afirmar que vale cualquier cuadro blanco? De hecho, no, porque podríamos haber pintado las diagonales opuestas,



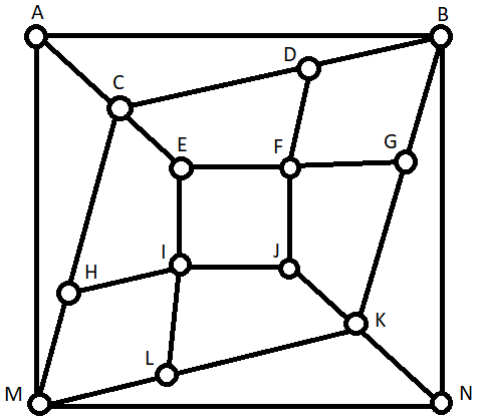
y haber llegado a la misma cantidad de cuadros azules, naranjas y blancos, por lo que también tendríamos que cubrir un cuadro blanco en esta nueva coloración.

Así que la conclusión es que debemos cubrir un cuadro que sea blanco en ambas coloraciones, es decir, el central, una de las 4 esquinas o uno de los cuadros centrales de cada lado.

Con los dos problemas vistos hasta ahora podríamos deducir que cuando queremos colocar piezas sobre tableros es interesante colorear el tablero. ¿Y de qué manera? Pues intentando que casi todas nuestras piezas cubran la misma cantidad de cuadros de cada color. Y de esta manera poder deducir que porcentaje de tabla podríamos cubrir y ver que faltaría por cubrir. Bien, argumentando que no podemos cubrirlo todo, en el caso de no tener más piezas, como en el primer problema u organizando las piezas que nos quedan para cubrir la parte restante, como en este problema.

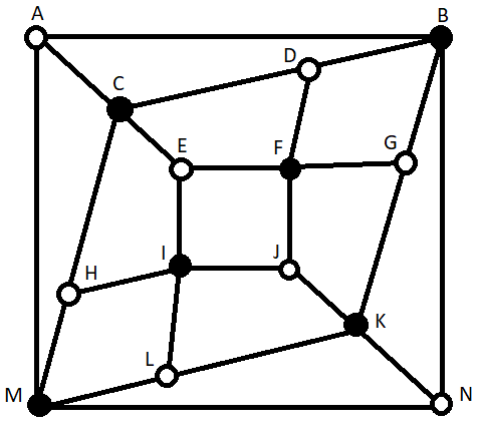
10.3 Aplicaciones del método a un grafo de ciudades

Tenemos el siguiente mapa de carreteras conectando 14 ciudades, entendamos que los puntos son las ciudades, y las líneas que unen los puntos, carreteras.



La cuestión a la que nos enfrentamos es ¿Podemos diseñar un camino que pase por todas las ciudades, pero solo una vez por cada una? Es decir, si empezamos por la ciudad A pasaríamos a una ciudad contigua, cualquiera entre las ciudades B, C y M. Si elegimos movernos a la ciudad B, después tendríamos que pasar a otra contigua a ella, distinta de la inicial, es decir, nuestras opciones son las ciudades D, G o N. Y así hasta pasar por todas, sin repetir ninguna.

Vamos a razonar con el mapa coloreado de esta manera.



Si os fijáis este coloreado tiene la cualidad de que una ciudad “blanca” sólo toca ciudades “negras”, e igualmente una ciudad “negra” sólo toca ciudades “blancas”. Así un camino que pase por cada ciudad alternaria ciudades blancas con ciudades negras, por ejemplo, empezando por la ciudad A, que es blanca pasaríamos necesariamente a una negra, y después necesariamente a otra blanca, y así sucesivamente.

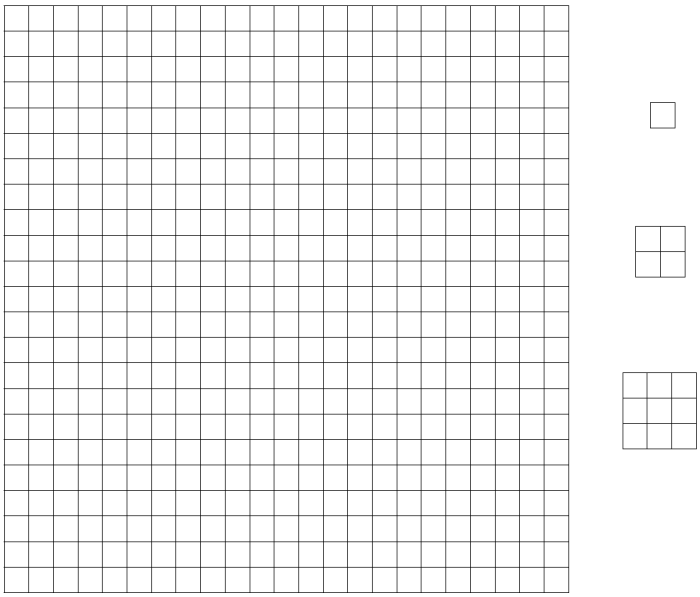
Entonces, lo que debería cumplir esta coloración es tener la misma cantidad de ciudades blancas que negras, o a lo sumo una ciudad más de alguno de los colores, lo que obligaría a que el camino empezase y terminase en ese color. Pero en este mapa tenemos 8 ciudades blancas y 6 ciudades negras, con lo que es imposible diseñar un camino con las condiciones del problema.

Como hemos podido ver tanto en el primer problema como en este, las demostraciones coloreando son especialmente útiles para dar respuestas negativas a los problemas planteados.

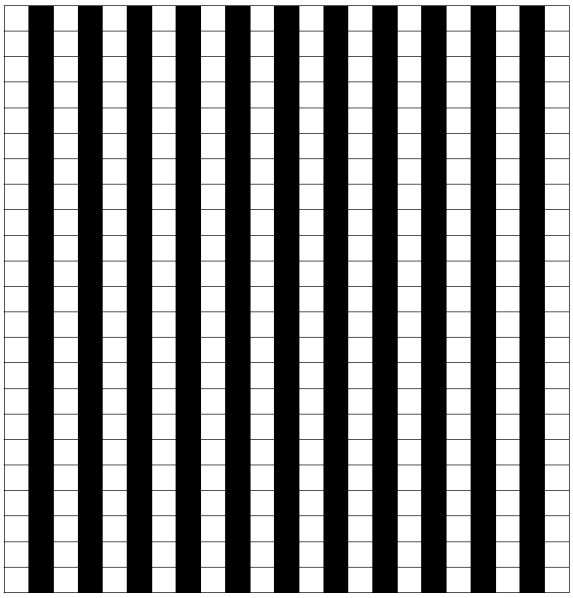
10.4 Aplicaciones del método a la Tabla 23x23

En el ejemplo de este capítulo, vamos a trabajar en un problema que apareció en la olimpiada All-Union Mathematical Olympiad, AUO, de 1989, es decir, la Olimpiada Matemática de la Unión Sovietica.

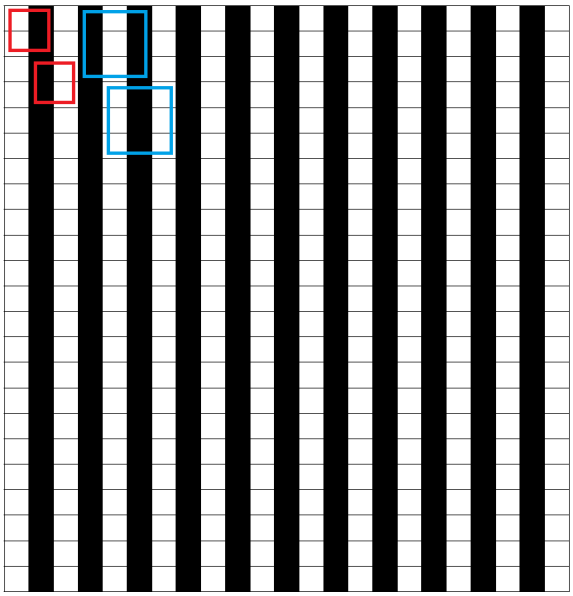
El problema nos propone cubrir una tabla 23x23 con piezas 1x1, 2x2 y 3x3. Y nos pregunta cuál es el mínimo número de piezas 1x1 necesarias para cubrir la tabla.



En primer lugar, vamos a intentar cubrir la tabla sin necesitar ninguna pieza 1x1.



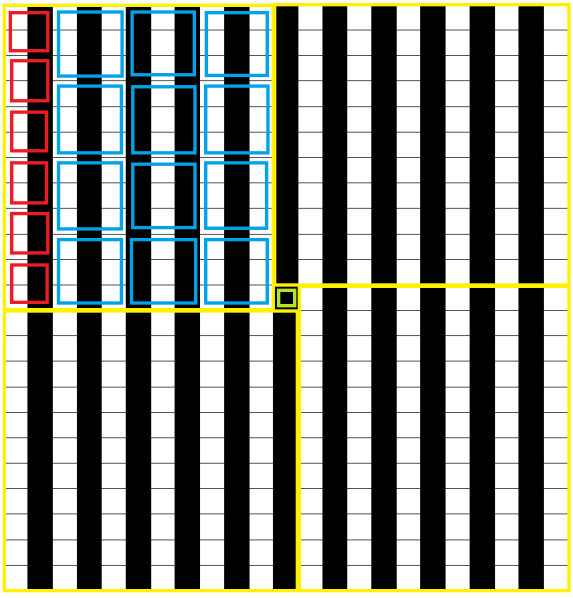
Si pintamos la tabla de esta manera, cada fila de un color, alternando blanco y negro, claramente vemos que una pieza 2x2, cubre siempre 2 cuadros blancos y dos negros, y una pieza 3x3, cubre siempre 6 cuadros de un color y tres cuadros del otro.



Por lo tanto, la diferencia de cuadros de un color con respecto al otro será un múltiplo de 3 para cualquier superficie cubierta con piezas de estos tamaños. Pero en esta tabla tenemos 23 cuadros blancos más que negros, que no es múltiplo de 3, por lo que podemos afirmar que no podemos cubrir la tabla entera con piezas de estos tamaños.

Intentemos argumentar con una pieza 1x1. Fijémonos que con esta misma coloración si cubriésemos un cuadro negro con la pieza 1x1, en la tabla restante tendríamos 24 cuadros blancos más que negros, lo que sí es un múltiplo de 3.

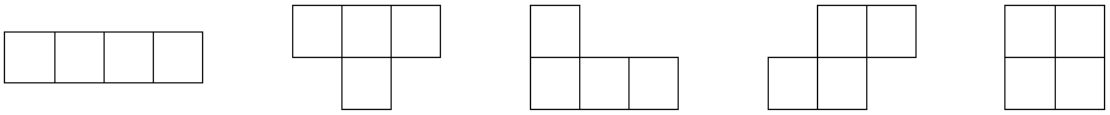
De hecho, si cubrimos el cuadro central, que efectivamente es negro con esta pieza, la tabla restante la podemos dividir en 4 tablas 12x11, o 11x12, de hecho, dos de cada. Cada una de estas subtablas es fácilmente cubrible con 12 piezas 3x3 y 6 piezas 2x2.



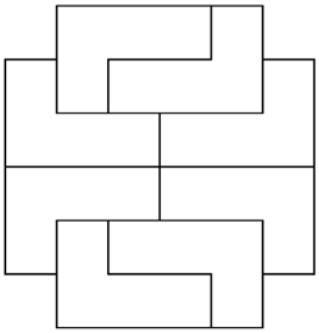
Por lo tanto, podemos concluir que una pieza 1x1 es la mínima cantidad de estas piezas que necesitaríamos.

Ejercicios Propuestos

1. ¿Es posible formar un rectángulo con los siguientes cinco tetrominós?



2. Consideramos un tablero de ajedrez de $n \times n$ con las cuatro esquinas eliminadas. ¿Para qué valores de n se puede cubrir el tablero con L-tetrominós como en la siguiente figura?



Bibliografía Adicional

1. Engel, A. (1998). Coloring Proofs. *Problem-Solving Strategies*. Editorial Springer, 25-37.

CAPÍTULO 11

11

ECUACIONES FUNCIONALES

José Luis Arregui Casaus
Universidad de La Rioja

Palabras clave

- *palabra 1*
- *palabra 2*
- *palabra 3*
- *palabra 4*

Una **ecuación funcional** expresa una propiedad que cumplen los valores de una función en algunos de los puntos de su dominio, tal vez en todos.

Normalmente la propiedad consiste en una relación de igualdad (*ecuación*) sobre los valores de la función f en distintos puntos del dominio, que se expresan mediante variables $(x, y, \dots)$. La diferencia con lo que normalmente entendemos como un problema de ecuaciones es que la *incógnita* no es ninguna de las variables, sino la misma función f: debemos encontrar qué funciones f cumplen lo que se nos dice, no para qué puntos x se cumple.

11.1 Introducción

En las olimpiadas matemáticas los problemas sobre ecuaciones funcionales son muy frecuentes, y suelen ser de enunciado sencillo, pero muchas veces resultan bastante difíciles porque las claves de la resolución pueden no ser evidentes en absoluto, pese a que normalmente estarán al alcance de cualquier participante en la prueba (se suelen evitar los problemas que requieren de conocimientos previos muy especializados). Sin embargo, la mayoría de ellos son atrayentes, y en muchos casos hay varias formas de resolverlos, siendo muy habitual que algunos participantes lo hagan de manera más corta o más ingeniosa que las esperadas por los mismos proponentes.

El problema más habitual que se plantea consiste en hallar todas las funciones que satisfacen la propiedad que se expresa, lo que llamamos las *soluciones* de la ecuación. En alguna ocasión el problema puede ser otro, tal vez simplemente encontrar *una* solución.

Es importante advertir la diferencia entre la *solución* del problema (la respuesta adecuada a lo que se nos pregunta una vez lo hemos resuelto) y cada *solución* de la ecuación que sale en el problema. Por ejemplo, si el problema consiste en demostrar que la ecuación

$$f(x+1) = f(x) \quad (x \in \mathbb{R})$$

tiene soluciones no constantes, entonces una forma de resolverlo consiste en observar que una solución no constante de la ecuación es la función dada por $f(x) = \cos 2\pi x$. Cualquier función constante es también solución de la ecuación, pero no nos da la solución al problema. En todo lo que sigue, cuando hablamos de una *solución* queremos decir *solución de la ecuación*, y a la forma que presentamos de resolver el problema la llamamos *resolución*.

11.2 Generalidades y estrategias

En este capítulo no pretendemos establecer ni resumir ninguna teoría sobre ecuaciones funcionales[1]: presentamos y resolvemos ejemplos del tipo de problemas que aparecen en olimpiadas, y nos atrevemos a señalar algunas estrategias generales a tener en cuenta si nuestra intuición o entrenamiento no son suficientes para abordarlos.

Estrategia general 1

En muchos casos es fácil adivinar una solución, especialmente si existe entre las más sencillas de alguna clase de funciones que conocemos bien. Esta solución podría ser la única o podría servir para llevarnos a todas las soluciones.

Estrategia general 2

Posiblemente la función que resulta al transformar de cierta manera una solución, o al combinar varias soluciones, es una función que cumple otra ecuación, que ya es conocida o es más sencilla que la dada, y eso nos permite resolver el problema.

[1]Si ese fuera el objetivo recomendaríamos el libro de Christopher G. Small *Functional Equations and How to Solve Them*, Problem Books in Mathematics, Springer, 2007

Ejemplo 11.1 Se trata de hallar todos los polinomios que cumplen que

$$p(x+1) = p(x) + 2x + 1 \quad (x \in \mathbb{R})\,.$$

Resolución: Una solución es, claramente, $p(x) = x^2$. Notemos que, si p y q son dos soluciones, entonces la función $f = q - p$ cumplirá que, para todo x, $f(x+1) - f(x) = 0$. Pero f es un polinomio, luego f debe ser constante (explicación: $f(x) - f(0)$ es otro polinomio que se anula en $0, 1, 2, 3, \ldots$, y todo polinomio no nulo tiene un número finito de raíces, luego $f(x) - f(0)$ es el polinomio nulo y $f(x)$ es igual a $f(0)$ para todo x).

Por tanto, si ahora llamamos p a una solución cualquiera entonces debe ser $p(x) - x^2 = c$, constante. Y comprobamos por fin que, en efecto, $x^2 + c$ cumple la ecuación, para cualquier c. Hemos encontrado todas las soluciones:

$$p(x) = x^2 + c \quad (\text{para cualquier } c \in \mathbb{R})\,.$$

□

Estrategia general 3

Cuando damos valores a algunas de las variables de la ecuación ($x, y, z, n, m, k \ldots$) obtenemos nuevas condiciones que han de cumplir las soluciones. En la mayoría de los casos, los mismos términos que aparecen en la ecuación son los que nos sugieren qué valores probar. No tienen necesariamente que ser valores concretos, pueden ser expresiones que dependen de las variables, si con eso obtenemos otras ecuaciones relacionadas con la ecuación inicial.

Ejemplo 11.2 Buscamos las funciones tales que, para cada x real en su dominio,

$$x\,f(x) + 2x\,f(-x) = -1\,.$$

Resolución: Si $x = 0$ el término de la izquierda se anula y el de la derecha no, por lo que cualquier solución f debe dejar a 0 fuera de su dominio. Además, la condición dice implícitamente que el dominio es simétrico (x es del dominio si y solo si lo es $-x$). Buscaremos soluciones en $\mathbb{R} \setminus \{0\}$.

En este caso, que la expresión involucre al valor de f en cualquier x y en su opuesto sugiere investigar qué pasa si aplicamos la condición a $-x$. Resulta la ecuación

$$-x\,f(-x) - 2x\,f(x) = -1\,,$$

es decir

$$-2x\,f(-x) - 4x\,f(x) = -2\,,$$

y sumando esta ecuación y la inicial obtenemos

$$-3x\,f(x) = -3\,,$$

con lo que necesariamente $f(x) = 1/x$ para cada x no nulo. Es directo comprobar que esta función es una solución, luego es la única solución. □

Ejemplo 11.3 Se trata de hallar todas las funciones $f\colon \mathbb{R} \to \mathbb{R}$ que cumplen, para todos x e y, que

$$x\,f(y) + y\,f(x) = (x+y)\,f(x)\,f(y)\,.$$

Resolución: Una solución es $f = 0$. Buscaremos más. Si $y = 0$ la ecuación nos dice que, para cualquier x, $x\,f(0) = x\,f(x)\,f(0)$. Es decir, para todo x

$$x\,f(0)(1 - f(x)) = 0\,.$$

Concluimos que, si $f(0) \neq 0$, entonces $f(x) = 1$ en todo $x \neq 0$. Esto ya nos permite encontrar muchas soluciones: elijamos cualquier $a \in \mathbb{R}$, fijemos $f(0) = a$ y $f = 1$ en $\mathbb{R} \setminus \{0\}$. Se ve directamente que la función f definida así es una solución.

Notemos que si $x + y = 0$ entonces el término de la derecha es nulo. Tomamos cualquier x y elegimos $y = -x$, y obtenemos

$$x\,(f(-x) - f(x)) = 0\,,$$

luego en todo punto $f(-x) = f(x)$, f es una *función par*. Está bien saberlo, pero no lo vamos a usar.

Es mejor que elijamos $y = x$, ya que entonces la ecuación dice que

$$2x\,f(x) = 2x\,f(x)^2\,,$$

luego para todo x

$$2x\,f(x)(1 - f(x)) = 0\,,$$

por lo que $f(x)$, si $x \neq 0$, solo puede tomar los valores 0 y 1. Puede parecer que habrá muchas formas de elegirlos para definir más soluciones de la ecuación, pero en realidad no hay más soluciones que las ya mencionadas: si $f(x) = 0$ y $f(y) \neq 0$, la ecuación nos da directamente que $x = 0$. □

Ejemplo 11.4 Se piden todas las soluciones $f\colon \mathbb{R} \to \mathbb{R}$ de

$$f(x)\,f(y) = f(x - y)\,.$$

Resolución: Dos soluciones obvias son las constantes $f = 0$ y $f = 1$. Vamos a ver que no hay más soluciones:

Si $x = y = 0$ la ecuación dice que $f(0)^2 = f(0)$, así que o bien $f(0) = 0$ o bien $f(0) = 1$. Pero si x es no nulo y hacemos $y = x$ vemos que $f(x)^2 = f(0)$. Por tanto, si $f(0) = 0$ la única solución es $f = 0$. Supondremos entonces que $f(0) = 1$, y en ese caso $f(x)^2 = 1$ para todo x. Si vemos que $f \geq 0$, se sigue que $f = 1$.

Para ello, observamos primero que f es par: la ecuación, si $x = 0$, dice que $f(y) = f(-y)$. Entonces, dado t, tomamos $x = t/2$ e $y = -t/2$ y obtenemos que $f(t/2)^2 = f(t)$, luego en efecto $f(t) \geq 0$. □

Si los ejemplos anteriores han parecido muy cortos, el que sigue ya no lo parecerá tanto. Pero tampoco es especialmente difícil, si pensamos en cómo usar las estrategias dadas:

Ejemplo 11.5 Queremos hallar todas las funciones $f\colon \mathbb{R} \to \mathbb{R}$ tales que

$$f(x) + f\Big(\frac{1}{1-x}\Big) = x \quad \text{si } 0 \neq x \neq 1\,.$$

Resolución: De forma similar a un ejemplo anterior, veamos qué obtenemos si cambiamos x por $g(x) = 1/(1-x)$: la ecuación inicial es

$$f(x) + f(g(x)) = x\,,$$

y obtenemos que

$$f(g(x)) + f(g(g(x))) = g(x)\,.$$

Con el mismo cambio,

$$f(g(g(x))) + f(g(g(g(x)))) = g(g(x))$$

(debemos notar que, si $0 \neq x \neq 1$, entonces $0 \neq g(x) \neq 1$).

Resulta que $g(g(x)) = \dfrac{1}{1-\frac{1}{1-x}} = \dfrac{1-x}{-x} = 1 - \dfrac{1}{x}$, y $g(g(g(x))) = x$.

Por tanto, la tercera ecuación es

$$f(g(g(x))) + f(x) = g(g(x))\,.$$

Le restamos la segunda, y sale que

$$f(x) - f(g(x)) = g(g(x)) - g(x)\,.$$

Sumamos esta ecuación y la inicial, y concluimos que

$$2\,f(x) = x + g(g(x)) - g(x)\,,$$

así que necesariamente

$$\begin{aligned} f(x) &= \frac{1}{2}\,(x + g(g(x)) - g(x)) \\ &= \frac{1}{2}\big(x + 1 - \frac{1}{x} - \frac{1}{1-x}\big) \quad \text{si } \ 0 \neq x \neq 1\,. \end{aligned}$$

Recíprocamente, si f es así en los valores distintos de 0 y 1 y tomamos $f(0)$ y $f(1)$ como queramos, esta función f cumple la ecuación: si x no es ni 0 ni 1

$$\begin{aligned} f(x) + f(g(x)) &= \frac{1}{2}\big(x + g(g(x)) - g(x)\big) + \frac{1}{2}\big(g(x) + x - g(g(x))\big) \\ &= \frac{1}{2}(x + x) = x\,. \end{aligned}$$

□

No es fácil formular más estrategias tan generales como las anteriores que no puedan expresarse combinando lo que ya dicen las dadas. Si acaso, como hemos visto en el ejemplo 1.4 merece la pena en general señalar las propiedades que debe cumplir toda solución f conforme las vamos deduciendo (en el ejemplo veíamos que se trata de una función par), con la esperanza obvia de que nos lleven a resolver el problema al acotar el conjunto de posibles soluciones.

Como estrategias particulares, claramente el tipo de problema (la clase de funciones de que se trate, o la especificación del dominio en el que las consideramos) hará recomendable que usemos nuestros conocimientos en ese ámbito.

Así, en algunos casos debemos proceder por inducción para resolver el problema. Nuestro siguiente ejemplo trata una de las llamadas *ecuaciones funcionales de Cauchy*,

$$f(x + y) = f(x) + f(y)\,.$$

Ejemplo 11.6 Si $f(x + y) = f(x) + f(y)$ para todos x e y, y $f(1) = a$, se pide determinar $f(x)$ para todo $x \in \mathbb{Q}$.

Reolución: Primero, es muy fácil ver por inducción que, fijado x, para cualquier $n \in \mathbb{N}$ se cumple que $f(nx) = nf(x)$.

En particular, tomando $n = 2$ y $x = 0$ deducimos que $f(0) = 0$.

Ahora tomamos $y = -x$ en la ecuación, y deducimos que f es una función impar, es decir $f(-x) = -f(x)$.

Por tanto, $f(nx) = nf(x)$ para todo x y cualquier $n \in \mathbb{Z}$.

Si fijamos x, para cualquier $n \in \mathbb{N}$ es $f(x) = f\big(n\,(x/n)\big) = nf(x/n))$, así que $f(x/n) = f(x)/n$.

Por último, si además $m \in \mathbb{Z}$ tenemos que

$$f\big((m/n)x\big) = mf(x/n) = (m/n)f(x)\,.$$

Lo aplicamos a $x = 1$, y concluimos que $f(m/n) = (m/n)f(1) = (m/n)\,a$.

Es decir,

$$f(x) = a\,x$$

para todo $x \in \mathbb{Q}$. □

Si f está definida en $\mathbb{R}$ y es una solución de la ecuación de Cauchy anterior, su valor en los puntos no racionales no puede obtenerse por inducción. ¿Podremos demostrar que $f(x) = ax$ para todo x real? En realidad no, pero es muy complicado dar ejemplos que lo demuestran. Son tan extraños que algunos autores los llaman *monsters*.

11.3 Problemas de olimpiadas matemáticas

Las técnicas inductivas son mucho más frecuentes en los problemas donde las funciones tienen como dominios $\mathbb{N}$, $\mathbb{N} \cup \{0\}$ o, en general, un subconjunto de $\mathbb{Z}$. El siguiente problema fue propuesto en la IMO (Olimpiada Matemática Internacional) de 1977. Lo indicamos en el enunciado, como haremos en lo sucesivo en otros ejemplos de la IMO o de la OME (Olimpiada Matemática Española):

Problema 11.1 (International Mathematical Olympiad, 1977) Supongamos que $f\colon \mathbb{N} \to \mathbb{N}$ cumple que

$$f(n+1) > f(f(n)) \quad \text{para todo } n\,.$$

Hay que probar que, entonces, $f(n) = n$ para todo n.

Solución *: El conjunto de imágenes de f tiene un mínimo, como todos los subconjuntos no vacíos de $\mathbb{N}$. La ecuación nos dice que dicho mínimo es necesariamente $f(1)$, y que $f(n) > f(1) \geq 1$ para cada $n > 1$. En particular, observemos que $f(n) \geq 2$ para todo $n \geq 2$. Razonando de la misma manera, el mínimo de $\{f(2), f(3), \dots\}$ es $f(2)$, y $f(n) > f(2) \geq 2$ para todo $n > 2$. Supongamos que hemos probado que $f(1) < f(2) < f(3) < \cdots < f(n)$ y que $f(k) > f(n) \geq n$ para todo $k > n$. Entonces la ecuación dice que el mínimo de $\{f(n+1), f(n+2), \dots\}$ es $f(n+1)$, y que $f(k) > f(n+1) \geq n+1$ para todo $k > n+1$. Hemos probado, por inducción, que*

$$f(1) < f(2) < f(3) < \cdots$$

(es decir, f es una función creciente) y que $f(n) \geq n$ para todo n.

Supongamos que $f(k) > k$. Entonces $f(k) \geq k+1$, y como f es creciente $f(f(k)) \geq f(k+1)$, en contradicción con la ecuación.

Por tanto, $f(n) = n$ para todo n. □

El que sigue ahora se propuso en la fase final de la OME de 2018. Sobre un máximo de 7 puntos, 49 participantes obtuvieron 0, otros 24 obtuvieron 1 punto y solo 3 llegaron a los 2 puntos, que fue la nota más alta. Es un buen ejemplo de la dificultad de algunos problemas sobre ecuaciones funcionales, de resolución sencilla de seguir cuando es explicada, pero difícil de descubrir.

Problema 11.2 (Olimpiada Matemática Española, 2018) Hay que hallar todas las funciones $f\colon \mathbb{R}^+ \to \mathbb{R}^+$ tales que, para todos $x, y > 0$,

$$f(x + f(y)) = y\, f(xy + 1)\,.$$

Solución *En la ecuación, f se aplica a tres valores: y, $xy+1$ y $x+f(y)$. Si estos dos últimos coinciden para ciertos valores de x e y, la ecuación dice que necesariamente $y = 1$. Es la mejor manera de empezar.*

Ahora bien, la igualdad $xy + 1 = x + f(y)$ se cumple siempre que sea $x = (f(y) - 1)/(y - 1)$. Para $y \neq 1$, si este valor fuera positivo tendríamos una contradicción, y entonces deducimos que

$$\frac{f(y) - 1}{y - 1} \leq 0 \quad \textit{para todo } y > 0 \textit{ distinto de } 1\,,$$

lo que equivale a decir que

$$(f(y) - 1)(y - 1) \leq 0 \quad \textit{para todo } y > 0. \tag{$*$}$$

Esto nos dice que f aplica el intervalo $(0, 1]$ en $[1, +\infty)$ y viceversa, lo que nos sugiere la función $f(x) = 1/x$ como posible solución. Sería muy fácil comprobar que en efecto lo es, y ya habríamos resuelto parte del problema (de hecho resultará que es es la única solución). Vamos a proseguir, en cualquier caso, como si no hubiéramos adivinado aún ninguna solución.

La desigualdad $(*)$ nos da una condición sobre $yf(y)$. En la ecuación inicial no aparece este término, a no ser que sea $xy + 1 = y$; vamos a seguir por ahí: esta igualdad se da si y solo si $x = 1 - 1/y$, que es positivo si $y > 1$. La ecuación dice por tanto (tomando ese valor de x) que, si $y > 1$,

$$f(1 - 1/y + f(y)) = yf(y)\,.$$

Sea entonces $y > 1$, y sea $a = 1 - 1/y + f(y)$. Por $(*)$ sabemos que

$$(f(a) - 1)(a - 1) \leq 0\,,$$

es decir

$$(yf(y) - 1)(f(y) - 1/y) \leq 0\,,$$

lo que nos lleva (tomando y como factor en el primer paréntesis) a que $(f(y) - 1/y)^2 \leq 0$, y entonces

$$f(y) = 1/y \quad \textit{para todo } y > 1.$$

Para terminar, si $0 < y \leq 1$ la ecuación nos dice que también, al ser $2/y \geq 2 > 1$,

$$\begin{aligned} f(y) &= f(y/2 + y/2) = f(y/2 + f(2/y)) = (2/y)\, f(2) \\ &= 1/y\,. \end{aligned}$$

Por tanto, la única solución de la ecuación es la función dada por $f(y) = 1/y$ para todo $y > 0$.

Cuando el problema concierne a funciones que se aplican a números naturales, a veces la clave la da la elección de una base determinada para escribir dichos números. Un clásico de este tipo es el siguiente problema, que se propuso en 1988 con un pequeño y evidente cambio en el enunciado:

Problema 11.3 (International Mathematical Olympiad, 1988) Se define una función $f\colon \mathbb{N} \to \mathbb{N}$ como sigue:

$$f(1) = 1\,, \quad f(3) = 3\,, \quad f(2n) = f(n)\,,$$
$$f(4n + 1) = 2\, f(2n + 1) - f(n)\,, \quad f(4n + 3) = 3\, f(2n + 1) - 2\, f(n)\,.$$

¿Cuántos números n cumplen que $f(n) = n$ y $n \leq 2022$?

Solución *Vamos a ver que la definición dada permite expresar de una manera muy sencilla el valor de f en cada número natural si lo expresamos en binario, es decir en base 2. En todo lo que sigue habrá alguna frase*

en la que se expresarán unos números en decimal y otros en binario; para distinguir la base escribiremos un número n como "$b_k b_{k-1} \dots b_2 b_1 b_0$" si esa secuencia de cifras es su expresión en binario; recordemos que eso significa que

$$n = b_0 + 2b_1 + 2^2 b_2 + \cdots + 2^k b_k \,,$$

donde $b_i = 0$ o $b_i = 1$ para cada i.

Llegaremos hasta las cuatro cifras en binario para tratar de adivinar esa expresión de $f(n)$, o sea hasta $n = 15$: escribiendo $x \mapsto y$ para decir $f(x) = y$, tenemos

$$1 \mapsto 1,\ 2 \mapsto 1,\ 3 \mapsto 3,\ 4 \mapsto 1,\ 5 \mapsto 5,\ 6 \mapsto 3,\ 7 \mapsto 7,\ 8 \mapsto 1,\ 9 \mapsto 9,$$
$$10 \mapsto 5,\ 11 \mapsto 13,\ 12 \mapsto 3,\ 13 \mapsto 11,\ 14 \mapsto 7 \text{ y } 15 \mapsto 15\,.$$

En binario es mejor:

$$\text{“1”} \mapsto \text{“1”},\ \text{“10”} \mapsto \text{“1”},\ \text{“11”} \mapsto \text{“11”},\ \text{“100”} \mapsto \text{“1”},\ \text{“101”} \mapsto \text{“101”},\ \text{“110”} \mapsto \text{“11”},$$
$$\text{“111”} \mapsto \text{“111”},\ \text{“1000”} \mapsto \text{“1”},\ \text{“1001”} \mapsto \text{“1001”},\ \text{“1010”} \mapsto \text{“101”},\ \text{“1011”} \mapsto \text{“1101”},$$
$$\text{“1100”} \mapsto \text{“11”},\ \text{“1101”} \mapsto \text{“1011”},\ \text{“1110”} \mapsto \text{“111” y “1111”} \mapsto \text{“1111”}\,.$$

Es fácil ahora adivinar que, si vemos n escrito en binario, entonces $f(n)$ es el número dado por las mismas cifras en orden inverso.

Tenemos que probarlo, y lo haremos por inducción completa sobre el número de cifras: visto lo anterior, sea $k \geq 4$ y supongamos que lo afirmado es cierto para números n que en binario tienen no más de k cifras (es decir, para todos los menores que 2^k). Queremos ver que, si $n =$ "$b_k \dots b_2 b_1 b_0$", con $b_k = 1$, entonces $f(n) =$ "$b_0 b_1 \dots b_k$" (donde por supuesto podríamos quitar todas las cifras anteriores a la primera que sea 1). Para que lo que sigue sea más claro, recordemos que multiplicar por 2^j, en binario, se expresa añadiendo j ceros al final. Observemos también que, en la definición del enunciado de f, podemos cambiar $2n+1$ por $4n+2$.

Primero lo vemos en el caso en que "$b_1 b_0$" = "00". Entonces $n = 4$"$b_k \dots b_2$", y por tanto

$$f(n) = f(\text{“}b_k \dots b_2\text{”}) = \text{“}b_2 \dots b_k\text{”} = \text{“}b_0 b_1 \dots b_k\text{”}.$$

Ahora supondremos que "$b_1 b_0$" = "10". Entonces $n = 2$"$b_k \dots b_2 1$", y

$$f(n) = f(\text{“}b_k \dots b_2 1\text{”}) = \text{“}1 b_2 \dots b_k\text{”} = \text{“}b_0 b_1 \dots b_k\text{”}.$$

Quedan los dos casos más complicados: si "$b_1 b_0$" = "01", entonces $n = 4$"$b_k \dots b_2$" $+1$, y 4"$b_k \dots b_2$" $+2 =$ "$b_k \dots b_2 10$", luego

$$\begin{aligned} f(n) &= 2\text{“}1 b_2 \dots b_k\text{”} - \text{“}b_2 \dots b_k\text{”} \\ &= \text{“}1 b_2 \dots b_k 0\text{”} - \text{“}b_2 \dots b_k\text{”} = \text{“}10 b_2 \dots b_k\text{”}\,, \end{aligned}$$

ya que la última igualdad equivale a

$$\text{“}10 b_2 \dots b_k\text{”} + \text{“}b_2 \dots b_k\text{”} = \text{“}1 b_2 \dots b_k 0\text{”}\,,$$

lo que es cierto: si $m =$ "$b_2 \dots b_k$" ambos términos valen $2^k + 2m$.

Por último, si "$b_1 b_0$" = "11" entonces $n = 4$"$b_k \dots b_2$" $+3$, y otra vez 4"$b_k \dots b_2$" $+2 =$ "$b_k \dots b_2 10$",

así que

$$\begin{aligned} f(n) &= 3\text{“}1b_2\dots b_k\text{”} - 2\text{“}b_2\dots b_k\text{”} \\ &= (2+1)\text{“}1b_2\dots b_k\text{”} - \text{“}b_2\dots b_k0\text{”} \\ &= \text{“}1b_2\dots b_k0\text{”} + \text{“}1b_2\dots b_k\text{”} - \text{“}b_2\dots b_k0\text{”} = \text{“}11b_2\dots b_k\text{”}\,. \end{aligned}$$

Conclusión: la respuesta a la pregunta es el número de valores de $\{1,2,3,\dots,2022\}$ *cuya expresión en binario es capicúa. El menor número de doce cifras en binario es* $2^{11} = 2048$*, luego todos los que buscamos tienen como máximo once cifras en binario. Es fácil contar, si consideramos los números con un número de cifras binarias dado, cuántos de ellos son capicúas. Por ejemplo, con siete cifras tenemos ocho, de la forma* “$1b_1b_2b_3b_2b_11$” *para cada elección de* $b_1, b_2, b_3 \in \{0,1\}$*. Y para ocho cifras es igual, porque son los de la forma* “$1b_1b_2b_3b_3b_2b_11$”*. Sumando, el número de capicúas con un máximo de 11 cifras binarias es* $1+1+2+2+4+4+8+8+16+16+32 = 94$*. No debemos contar al mayor de todos ellos, que es* “11111111111” $= 2048-1 = 2047$*, pero sí al segundo más grande, que es* “11111011111” $=$ $2047 -$ “100000” $= 2047 - 32 = 2015$*.*

En definitiva, la respuesta a la pregunta que se plantea es 93.

Notemos que la respuesta correcta al problema que se propuso en la IMO de 1988 era 92, porque había que descontar a 2015 pero no al anterior, que es “11110101111” $= 2047 - 64 - 16 = 1967$*.*

Lo más habitual es que los problemas sobre ecuaciones funcionales que se proponen desde hace muchos años en olimpiadas matemáticas no requieran conocimientos de Análisis Matemático, por básicos que sean (como límites, continuidad, diferenciabilidad, integración y suma de series). Eso no impide que, algunas veces, se pueda recurrir a ellos para resolver el problema de una manera más directa que la que después aparece en las soluciones oficiales.

Terminamos nuestro repaso con un problema muy reciente de lo anterior. Nuestra resolución es más corta que la oficial, a costa de usar (de manera muy elemental) la derivación de funciones reales.

Problema 11.4 (Olimpiada Matemática Española - fase local, 2022) Se pide encontrar todos los polinomios $p(x)$ con la siguiente propiedad: para cualesquiera x, y, z

$$p(x)+p(y)+p(z)+p(x+y+z) = p(x+y)+p(y+z)+p(z+x)\,.$$

Solución *Cualquier función polinómica* p *solución de la ecuación se puede derivar indefinidamente. En la ecuación propuesta, si suponemos fijos* y, z *y derivamos ambos términos como funciones de* x*, obtenemos*

$$p'(x)+p'(x+y+z) = p'(x+y)+p'(z+x)\,,$$

y esta condición es cierta para todos x, y, z*. Si derivamos ambos términos en esta igualdad considerándolos funciones de* y*, resulta*

$$p''(x+y+z) = p''(x+y)\,,$$

cierto para todos x, y, z*. Si tomamos por ejemplo* $x = y = 0$ *concluimos que* p'' *es constante. Y entonces* $p(x)$ *debe ser un polinomio de grado menor o igual que 2.*

Recíprocamente, es muy fácil y rutinario comprobar que cualquier $p(x) = ax^2 + bx + c$ *es una solución de la ecuación propuesta.*

Por tanto, el conjunto de polinomios que satisfacen la ecuación funcional del enunciado es exactamente el de los polinomios de grado 0, 1 ó 2.

Ejercicios Propuestos

1. Hallar todas las funciones $f\colon \mathbb{R} \to \mathbb{R}$ tales que para todo $x, y \in \mathbb{R}$ cumplen

$$f\big(f(y) + xf(x)\big) = y + f(x)^2\,.$$

   Pista: El enunciado dice que f debe ser suprayectiva, y podemos considerar a tal que $f(a) = 0$.

2. Encontrar todas las funciones $f\colon \mathbb{N} \to \mathbb{N}$ que cumplen, para todo n, que

$$f\big(f\big(f(n)\big)\big) + f\big(f(n)\big) + f(n) = 3\,n\,.$$

   Pista: Conviene notar que f debe ser inyectiva.

3. Sea $f\colon \mathbb{Q} \to \mathbb{Q}$ una función que satisface la *ecuación de Jensen*:

$$f\Big(\frac{x+y}{2}\Big) = \frac{f(x)+f(y)}{2} \quad \text{, con } x, y \in \mathbb{Q}\,.$$

   Si llamamos $a = f(0)$ y $b = f(1)$, se pide el valor de $f(x)$ para cada $x \in \mathbb{Q}$.

   Pista: Se puede aprovechar lo que hemos visto sobre la ecuación de Cauchy.

4. (International Mathematical Olympiad, 1990) Hallar una función $f\colon \mathbb{Q}^+ \to \mathbb{Q}^+$ tal que para todo $x, y \in \mathbb{Q}^+$ se satisface la igualdad

$$f\big(xf(y)\big) = \frac{f(x)}{y}\,.$$

   Pista: El primer objetivo debe ser probar que una tal función f debe cumplir que $f(x\,y) = f(x)\,f(y)$. Para dar con una solución, se pueden considerar entonces los números primos.

Bibliografía Adicional

1. Engel, A. (1998). Functional Equations. *Problem-Solving Strategies*. Editorial Springer, 271-288.

CAPÍTULO 12

12 ¿CÓMO ATACAR UN PROBLEMA?

Alejandro Mahillo Cazorla
Universidad de Zaragoza

Palabras clave

- *Resolución de problemas*
- *Plantear un problema*
- *Experiencia real*

¡Buenas estimado lector!, soy Alejandro Mahillo y hace unos años me encontraba en la misma situación que tú, preparándome para enfrentarme a una olimpiada matemática. Pero tranquilo, estoy aquí para ayudarte. Aunque hace un par de años que terminé la carrera de matemáticas, sigo con ganas de seguir disfrutando de estas competiciones. Por desgracia, para mi edad ya no existen concursos de este tipo. Fíjate, nos jubilan de las olimpiadas antes que a los futbolistas. Conmigo harás una OME (Olimpiada Matemática Española) y te iré contando que es lo que estoy pensando en cada momento. De esta forma, mis consejos te servirán para resolver por ti mismo cualquier problema. ¿Qué te parece? Pues corre que empezamos.

12.1 Introducción

Las ***Olimpiadas Matemáticas*** son un momento de nervios, ya que uno siempre quiere hacerlo de la mejor forma posible. Por ello, una parte fundamental de la competición es saber como manejar esa situación. En ocasiones, nos quedamos atascados en algún problema y no sabemos por dónde ir. Al final, si no somos capaces de anteponernos a estas situaciones, nos va a pasar factura en la realización de todo el examen.

Por esa razón creo que es interesante hablaros desde mi propia experiencia para contaros algunos trucos que me ayudan a plantear una sesión de problemas. Saber muchas mates seguro que nos ayuda a hacerlo muy bien, pero también creo que es muy importante saber controlar los nervios para obtener el mejor resultado posible.

Para ello, resolveremos la Fase Nacional de la Olimpiada Matemática Española (OME) celebrada en Alcalá de Henares, Madrid en el año 2017. Primero resolveremos los ejercicios del primer día como si estuviésemos en el examen. Y después, resolveremos los ejercicios del segundo día completando así todos los problemas.

12.2 Problemas del día 1 de la Fase Nacional de la OME 2017

Lo primero que debemos hacer cuando nos entregan la hoja de problemas es leerlos todos. Normalmente suelen ir en orden de dificultad, pero en ocasiones nos puede resultar más sencillo cambiar ese orden. Los problemas que tenemos en esta hoja de problemas son los siguientes.

Problema 12.1 (Día 1). Determina el número de valores distintos de la expresión

$$\frac{n^2-2}{n^2-n+2},$$

donde $n \in 1, 2, 3, \ldots, 100$.

Problema 12.2 (Día 1). Un trazador de puntos medios es un instrumento que dibuja el punto medio exacto de dos puntos previamente señalados. Partiendo de dos puntos a distancia 1 y utilizando sólo el trazador de puntos medios, debes obtener dos puntos a una distancia estrictamente comprendida entre $\frac{1}{2017}$ y $\frac{1}{2016}$, trazando el menor número posible de puntos. ¿Cuál es el mínimo número de veces que necesitas utilizar el trazador de puntos medios, y qué estrategia seguirías para lograr tu objetivo?

Problema 12.3 (Día 1). Sea p un primo impar y

$$S_q = \frac{1}{2\cdot 3\cdot 4} + \frac{1}{5\cdot 6\cdot 7} + \cdots + \frac{1}{q\cdot(q+1)\cdot(q+2)},$$

donde $q = \frac{3p-5}{2}$. Escribimos $\frac{1}{p} - 2S_q$ en la forma $\frac{m}{n}$, donde m y n son enteros. Demuestra que $m \equiv n (mód\ p)$; es decir, m y n dan el mismo resto al ser divididos por p.

Una vez leídos los problemas, a mi el que me parece más sencillo de los tres es el primero. Por tanto empezaré intentando resolver el primero. Después, el segundo problema me parece que tiene un enunciado un poco lioso, en una primera ojeada yo creo que me va a llevar mucho tiempo. En cambio el tercero, aunque parezca más difícil, creo que podría intentar bastantes cosas y avanzar algo. Igual no lo resuelvo entero, pero podré hacer parte del ejercicio para obtener algunos puntos.

Mi orden de resolución será: Problema 12.1, Problema 12.3 y Problema 12.2. ¡Vamos allá!

Problema 12.1 (Día 1). Determina el número de valores distintos de la expresión

$$\frac{n^2-2}{n^2-n+2},$$

donde $n \in 1, 2, 3, \ldots, 100$.

Solución *Este problema es un claro ejemplo donde antes de intentar probar nada, merece la pena perder unos minutos en simplificar la expresión. Un par de aproximaciones superficiales al problema, que igual no nos aportan nada pero que nos pueden abrir la mente para ver otras propuestas cuando estemos atascados. En este caso, vemos que el grado de la fracción en el denominador y en el numerador es el mismo. Así que podemos simplificar como,*

$$\frac{n^2-2}{n^2-n+2} = \frac{n^2-n+2+n-2-2}{n^2-n+2} = 1 + \frac{n-4}{n^2-n+2}.$$

Otra técnica que viene muy bien en todo tipo de problemas es empezar con casos sencillos y ver si podemos encontrar algún patrón. Sustituimos algunos valores de n en nuestra expresión y vemos que resultado obtenemos.

$$\bullet\ n=1 \implies -\frac{1}{2} \qquad \bullet\ n=2 \implies \frac{1}{2} \qquad \bullet\ n=3 \implies \frac{7}{8}$$

En este caso, a simple vista no veo nada que me aporte ninguna pista. En este caso volvemos a leer el enunciado y nos fijamos en la palabra ***distintos****. Igual ver cuando son distintos esos valores es más complicado, por lo que probaremos a ver cuando son iguales, algo más sencillo. Es decir, supongamos*

$$\frac{n^2-2}{n^2-n+2} = \frac{m^2-2}{m^2-m+2},$$

que dada la simplificación realizada anteriormente es equivalente a probar,

$$\frac{n-4}{n^2-n+2} = \frac{m-4}{m^2-m+2}.$$

Multiplicamos en cruz y simplificamos, obteniendo que la igualdad anterior es equivalente a,

$$(m-n)(mn-4(m+n)+2) = 0.$$

Como $m \neq n$, la igualdad inicial se dará si y solo sí $mn-4(m+n)+2=0$. Ahora a nosotros nos interesa encontrar soluciones m y n para esta ecuación, por tanto debemos pensar en intentar poner eso como un producto. ¿Por qué se nos ocurre eso? Cuando tenemos un producto de números enteros que es igual a otro número solo tendremos que fijarnos en su descomposición en factores primos y probar casos. Un ejemplo de esto lo veremos a continuación. Buscamos una expresión de la forma $(m-4)(n-4) = -4m+mn-4n+16$. Lo que no nos cuadra es el término independiente, pero para ajustarlo podemos sumar y restar a ambos lados. Por tanto,

$$mn-4(m+n)+2=0 \implies (m-4)(n-4)=14.$$

La descomposición del número 14 es: $14 = 1\cdot 14 = -1\cdot -14 = 2\cdot 7 = -2\cdot -7$. De estos casos, como m y n son mayores que 1, podemos descartar los productos negativos. Por tanto, si $m-4=1$ entonces $m=5$ y así $n=18$ o $m-4=2$ y entonces $m=6$ dando lugar a que $n=11$. Finalmente, de los 100 valores posibles solo se repiten 2. Así que hay 98 valores distintos.

Problema 12.3 (Día 1). Sea p un primo impar y

$$S_q = \frac{1}{2\cdot 3\cdot 4} + \frac{1}{5\cdot 6\cdot 7} + \cdots + \frac{1}{q\cdot(q+1)\cdot(q+2)},$$

donde $q = \dfrac{3p-5}{2}$. Escribimos $\dfrac{1}{p} - 2S_q$ en la forma $\dfrac{m}{n}$, donde m y n son enteros. Demuestra que $m \equiv n (mód\ p)$; es decir, m y n dan el mismo resto al ser divididos por p.

Solución *En lo primero que nos fijamos, al igual que en el ejercicio anterior, es si la expresión general de S_q se puede simplificar. En vez de poner cada término como producto de 3 números, intentaremos ponerlo como suma de 3 fracciones con un denominador más simple,*

$$\frac{1}{q(q+1)(q+2)} = \frac{A}{q} + \frac{B}{q+1} + \frac{C}{q+2}.$$

Nuestra misión será encontrar los valores de A, B y C. Sacando factor común en la suma de fracciones de la derecha llegamos a la siguiente igualdad,

$$A(q+1)(q+2) + B(q+2)q + C(q+1)q = 1,$$

que deberá ser cierta para cualquier q. De donde obtenemos el siguiente sistema,

$$\begin{aligned} A + B + C &= 0, \\ 3A + 2B + C &= 0, \\ 2A &= 1. \end{aligned}$$

Que tiene como soluciones $A = \frac{1}{2}$, $B = -1$ y $C = \frac{1}{2}$. Por tanto, una vez tenemos el término general de S_q expresado de otra forma, veamos si podemos expresar S_q en función de p, ya que buscamos encontrar el valor de $\frac{1}{p} - 2S_q$.
Tenemos que,

$$S_q = \frac{\frac{1}{2}}{2} - \frac{1}{3} + \frac{\frac{1}{2}}{4} + ... + \frac{\frac{1}{2}}{\frac{3p-5}{2}} - \frac{1}{\frac{3p-5}{2}+1} + \frac{\frac{1}{2}}{\frac{3p-5}{2}+2}.$$

Agrupando los términos positivos y negativos y sacando factor común obtenemos que,

$$S_q = \frac{1}{2}\left(\frac{1}{2} + \frac{1}{4} + ... + \frac{2}{3p-5} + \frac{2}{3p-1}\right) - \frac{1}{3}\left(1 + ... + \frac{2}{p-1}\right).$$

Como vemos, tenemos $\frac{1}{2}$ que puede que nos dificulte las cosas y $\frac{1}{3}$. Además, nuestro primer paréntesis parece incompleto como si le faltasen los términos intermedios. A la vista de los resultados esto no tiene buena pinta. Volvamos a mirar exactamente lo que nos pide el problema. Se nos pide calcular $\frac{1}{p} - 2S_q$ y nosotros no hemos tenido en cuenta el 2. Así que multiplicamos por 2 nuestra expresión,

$$2S_q = \left(\frac{1}{2} + \frac{1}{4} + ... + \frac{2}{3p-5} + \frac{2}{3p-1}\right) - \frac{2}{3}\left(1 + ... + \frac{2}{p-1}\right).$$

Aun así seguimos teniendo el problema del $\frac{2}{3}$. Pero si nos damos cuenta, en el primer paréntesis faltan como ciertos términos, que los podemos sumar y luego restar para no cambiar el valor de nuestra expresión. En particular, la resta es el tercio que nos faltaba en el segundo paréntesis, por tanto la expresión queda,

$$\begin{aligned} 2S_q = &\left(\frac{1}{2} + \frac{1}{3} + \frac{1}{4} + ... + \frac{2}{3p-5} + \frac{2}{3p-3} + \frac{2}{3p-1}\right) \\ &- \left(1 + ... + \frac{2}{p-1}\right). \end{aligned}$$

Vemos que en el primer paréntesis falta un 1, por tanto lo añadimos a ambos lados,

$$\begin{aligned} 2S_q + 1 = &\left(1 + \frac{1}{2} + \frac{1}{3} + \frac{1}{4} + ... + \frac{2}{3p-5} + \frac{2}{3p-3} + \frac{2}{3p-1}\right) \\ &- \left(1 + ... + \frac{2}{p-1}\right). \end{aligned}$$

Pero claro, esta expresión es más difícil de comprender, buscaremos dar algún ejemplo para ver si podemos

generalizarlo. Con $p = 3$ el resultado es trivial y no nos da mucho juego, probamos con $p = 5$, es decir $q = 5$.

$$2S_5 + 1 = \left(1 + \frac{1}{2} + \frac{1}{3} + \frac{1}{4} + \frac{1}{5} + \frac{1}{6} + \frac{1}{7}\right) - \left(1 + \frac{1}{2}\right).$$

Así, tenemos que,

$$2S_5 + 1 - \frac{1}{5} = \left(\frac{1}{3} + \frac{1}{4} + \frac{1}{6} + \frac{1}{7}\right) = \left(\frac{1}{3} + \frac{1}{7}\right) + \left(\frac{1}{4} + \frac{1}{6}\right).$$

Hemos conseguido poner a la derecha todos los denominadores que sumen un múltiplo de 5 y el denominador no contiene al 5. Por tanto, el numerador será un múltiplo de 5. Y recordando que $\frac{1}{p} - 2S_q = \frac{m}{n}$

$$2S_5 + 1 - \frac{1}{5} = 1 - \frac{m}{n} = \frac{n-m}{n} = \left(\frac{1}{3} + \frac{1}{7}\right) + \left(\frac{1}{4} + \frac{1}{6}\right).$$

Por tanto $n - m \equiv 0(mód\ 5)$ y entonces $n \equiv m(mód\ 5)$.

De forma general buscamos hacer lo mismo,

$$\begin{aligned} 2S_q + 1 &= \left(1 + \frac{1}{2} + ... + \frac{2}{3p-1}\right) - \left(1 + ... + \frac{2}{p-1}\right) \\ &= \frac{2}{p+1} + ... + \frac{1}{p-1} + \frac{1}{p} + \frac{1}{p+1} + ... + \frac{2}{3p-1}. \end{aligned}$$

Pasando $\frac{1}{p}$ al otro lado nos queda,

$$2S_q + 1 - \frac{1}{p} = \underbrace{\frac{1}{\frac{p+1}{2}} + ... + \frac{1}{p-1}}_{\frac{p-1}{2}\ términos} + \underbrace{\frac{1}{p+1} + ... + \frac{1}{\frac{3p-1}{2}}}_{\frac{p-1}{2}\ términos}.$$

Ahora agrupamos como hemos hecho en el caso particular y obtenemos que,

$$2S_q + 1 - \frac{1}{p} = \underbrace{\left(\frac{1}{\frac{p+1}{2}} + \frac{1}{\frac{3p-1}{2}}\right) + ... + \left(\frac{1}{p-1} + \frac{1}{p+1}\right)}_{\frac{p-1}{2}\ paréntesis}.$$

En cada uno de estos paréntesis, su numerador es $2p$ y por tanto tenemos que,

$$\frac{n-m}{n} = 2S_q + 1 - \frac{1}{p} = 2p\left(\frac{1}{\frac{p+1}{2}\frac{3p-1}{2}} + ... + \frac{1}{(p-1)(p+1)}\right)$$

Al igual que antes tenemos que el denominador no contiene ningún factor p, lo que significa que $n - m \equiv 0(mód\ p)$ y por tanto $n \equiv m(mód\ p)$.

Problema 12.2 (Día 1). Un trazador de puntos medios es un instrumento que dibuja el punto medio exacto de dos puntos previamente señalados. Partiendo de dos puntos a distancia 1 y utilizando sólo el trazador de puntos medios, debes obtener dos puntos a una distancia estrictamente comprendida entre $\frac{1}{2017}$ y $\frac{1}{2016}$, trazando el menor número posible de puntos. ¿Cuál es el mínimo número de veces que necesitas utilizar el trazador de puntos medios, y qué estrategia seguirías para lograr tu objetivo?

Solución *Lo primero que debemos fijarnos es que podemos suponer que estamos en la recta real y que los puntos con los que empezamos son el 0 y el 1. Ahora, debemos fijarnos como funciona el trazador de puntos medios, debemos entender que sucede realmente y que valores tendrán esos puntos. Notemos que al hacer puntos medios siempre tenemos una potencia de 2 en el denominador, y podemos pensar que en k usos el punto tendrá que ser de la forma $\frac{n}{2^k}$ con $0 \leq n \leq 2^k$. Lo probamos por inducción.*

- *Caso $k = 1$. Tenemos que los puntos son $\frac{0}{2^1}$, $\frac{1}{2^1}$ y $\frac{2^1}{2^1}$.*

- *Caso general. Sean los puntos* $\left\{\frac{0}{2^k}, \frac{1}{2^k}..., \frac{r}{2^k}, ..., \frac{s}{2^k}, ..., \frac{2^k}{2^k}\right\}$. *Aplicando el trazador de puntos medios a dos cualesquiera obtenemos,*

$$\frac{1}{2}\left(\frac{r}{2^k}+\frac{s}{2^k}\right)=\frac{r+s}{2^{k+1}} \text{ con } 0\leq r+s\leq 2^{k+1}.$$

Ahora que sabemos cómo son los puntos, calculamos la distancia entre 2 de ellos. La distancia entre 2 puntos tras haber usado k*-veces el trazador será* $\frac{|p-q|}{2^k}$*, es decir, un múltiplo de* $\frac{1}{2^k}$*. Necesitamos encontrar* n *y* k *de tal forma que,*

$$\frac{1}{2017}<\frac{n}{2^k}<\frac{1}{2016}.$$

O lo que es lo mismo, $2^k\in(2016n, 2017n)$*. Probando con distintos valores de* k *a partir de 12 encontramos que dicha igualdad se verifica para* $k=17$ *y* $n=65$*. Es decir, el número mínimo de cortes necesarios será de 17. Veamos que es exactamente 17, obteniendo dicha distancia con los cortes necesarios.*

Notemos que debemos intentar conseguir obtener 65 en el numerador con el menor número de cortes posibles, ya que después la forma más rápida de descender es tomando ese punto y el 0.

- *Con el primer corte obtenemos* $\frac{1}{2}$.
- *Ahora utilizamos* $\frac{1}{2}$ *y el* 1 *para obtener* $\frac{3}{4}$.
- *Hacemos puntos medios con* $\frac{1}{2}$ *y con el punto anterior obtenido. Hacemos esta técnica 7 veces hasta llegar a* $\frac{65}{2^7}$.
- *Por último, utilizamos el trazador con* $\frac{65}{2^7}$ *y el* 0*, diez veces seguidas y obtenemos* $\frac{65}{2^{17}}$.

Hemos realizado un total de 17 cortes y además hemos dado un ejemplo constructivo de como conseguirlo.

12.3 Problemas del día 2 de la Fase Nacional de la OME 2017

Lo primero que haremos, como en los problemas del día 1, será leer los enunciados y elegir en qué orden vamos a atacar los problemas. En este caso, los problemas a los que nos enfrentamos son los siguientes.

Problema 12.1 (Día 2). Se dispone de una fila de 2018 casillas, numeradas consecutivamente de 0 a 2017. Inicialmente, hay una ficha colocada en la casilla 0. Dos jugadores A y B juegan alternativamente, empezando A, de la siguiente manera: En su turno, cada jugador puede, o bien hacer avanzar la ficha 53 casillas, o bien hacer retroceder la ficha 2 casillas, sin que en ningún caso se sobrepasen las casillas 0 a 2017. Gana el jugador que coloque la ficha en la casilla 2017. ¿Cuál de ellos dispone de una estrategia ganadora, y cómo tendría que jugar para asegurarse ganar?

Problema 12.2 (Día 2). Determina el máximo valor posible de la expresión

$$27abc+a\sqrt{a^2+2bc}+b\sqrt{b^2+2ca}+c\sqrt{c^2+2ab}$$

siendo a,b,c, números reales positivos tales que $a+b+c=\frac{1}{\sqrt{3}}$.

Problema 12.3 (Día 2). En el triángulo *ABC*, los puntos medios respectivos de los lados *BC*, *AB* y *AC* son *D*, *E* y *F*. Sean: *M* el punto donde la bisectriz interior del ángulo $\angle ADB$ corta al lado *AB*, y *N* el punto donde la bisectriz interior del ángulo $\angle ADC$ corta al lado *AC*. Sean además *O* el punto de intersección de las rectas *AD* y *MN*, *P* el punto de intersección de *AB* y *FO*, y *R* el punto de intersección de *AC* y *EO*. Demuestra que *PR* = *AD*.

Una vez leídos los problemas, el que me parece más sencillo de los tres es el primero. Por tanto empezaré intentando resolver ese. Después, el segundo problema es una desigualdad, que me gustan mucho y se me suelen dar bien. En cambio el tercero, de geometría, campo que no domino demasiado bien y por tanto lo dejaré para el final.

Mi orden de resolución será: Problema 1, Problema 2 y Problema 3. ¡Vamos allá!

Problema 12.1 (Día 2). Se dispone de una fila de 2018 casillas, numeradas consecutivamente de 0 a 2017. Inicialmente, hay una ficha colocada en la casilla 0. Dos jugadores A y B juegan alternativamente, empezando A, de la siguiente manera: En su turno, cada jugador puede, o bien hacer avanzar la ficha 53 casillas, o bien hacer retroceder la ficha 2 casillas, sin que en ningún caso se sobrepasen las casillas 0 a 2017. Gana el jugador que coloque la ficha en la casilla 2017. ¿Cuál de ellos dispone de una estrategia ganadora, y cómo tendría que jugar para asegurarse ganar?

Solución *En este tipo de ejercicios de estrategia ganadora es muy interesante pensar en cómo es el final, ya que hay pocos desenlaces posibles. Obviamente ni A ni B quieren caer en la casilla 1964, porque entonces el otro avanza 53 casillas y gana. Por tanto, ni A ni B querrán caer en la casilla 1964. Entonces para poner la ficha en esa posición es necesario provenir desde 1966, porque en ese caso el movimiento de ir 2 hacia atrás es obligatorio. En general, si un jugador cae en una casilla k, con $k \geq 1964$ tal que $k \equiv 0(mód\ 4)$, entonces pierde la partida y si la casilla k verifica que $k \equiv 2(mód\ 4)$ entonces el jugador que cae en esa casilla ganará la partida.*

Pero, ¿que pasa en los casos en los que k es impar? Aplicamos el mismo pensamiento, vamos bajando y llegamos el 1965, pongamos por ejemplo que A llega a 1965, entonces B mueve obligado a 1963,en este caso A puede sumar 53, pero si hace eso llegaría a 2016 y entonces perdería ($2016 \equiv 0(mód\ 4)$). Decide restar 2 y A cae en 1963. Pero en este caso B se da cuenta de que si suma 53 cae en 2014 y por tanto ganaría, ya que $2014 \equiv 2(mód\ 4)$. En resumen, tenemos que si un jugador cae en una casilla k, con $k \geq 1964$ tal que $k \equiv 0(mód\ 4)$ o $k \equiv 1(mód\ 4)$, entonces pierde la partida y si la casilla k verifica que $k \equiv 2(mód\ 4)$ o $k \equiv 3(mód\ 4)$ entonces el jugador que cae en esa casilla ganará la partida.

Ahora es el momento de buscar una estrategia y en estos casos conviene pensar en estrategias en las que tú hagas algo en función del movimiento que haga el rival. En este caso, una buena idea sería intentar siempre lo mismo. Es decir, por ejemplo si A avanza, B retrocede y si A retrocede, entonces B avanza, de esta forma tras 2 movimientos (uno de A y otro de B), el resultado es siempre el mismo. En este caso vamos a ver que A tiene una estrategia ganadora.

A empieza y avanza hasta la casilla 53 y ahora A debe de hacer justo lo contrario que haga B, de tal forma siempre avanzarán 51 casillas en los turnos B-A. A hará esto 38 veces hasta llegar a la casilla $53 + 38 * 51 = 1991$. Recordando lo estudiado antes, tenemos que A ha caído en la casilla 1991, que verifica que $1991 \geq 1964$ y además $1991 \equiv 3(mód\ 4)$. Por tanto, en este punto A tiene que sumar siempre, excepto cuando le toque por obligación retroceder y acabará ganando la partida.

Problema 12.2 (Día 2). Determina el máximo valor posible de la expresión

$$27abc + a\sqrt{a^2 + 2bc} + b\sqrt{b^2 + 2ca} + c\sqrt{c^2 + 2ab}$$

siendo a,b,c, números reales positivos tales que $a + b + c = \dfrac{1}{\sqrt{3}}$.

Solución *En este tipo de problemas, lo que en realidad nos piden, es acotar superiormente la expresión por cierto valor sin depender de a, b o c. Para ello debemos buscar que aparezca $a+b+c$, valor que sí conocemos. Además, viendo que aparecen raíces, las desigualdades que podemos pensar en utilizar son las siguientes:*

- *Desigualdad entre la media aritmética y la media geométrica (MA-MG)*
  Sean $x_1, x_2, \ldots, x_n$ números reales positivos, entonces,
  $$\frac{x_1 + x_2 + \cdots + x_n}{n} \geq \sqrt[n]{x_1 x_2 \ldots x_n}.$$
- *Desigualdad de Cauchy-Schwarz (C-S)*
  Sean $x_1, x_2, \ldots, x_n$ y $y_1, y_2, \ldots, y_n$ números reales, entonces,
  $$\sqrt{x_1^2 + \cdots + x_n^2}\sqrt{y_1^2 + \cdots + y_n^2} \geq x_1 y_1 + \cdots + x_n y_n$$

Una de las cosas que nos molestan son las raíces, podemos pensar en usar C-S, ya que eso es un producto y podremos elevar al cuadrado las raíces de la siguiente forma,

$$\begin{aligned} &a\sqrt{a^2+2bc} + b\sqrt{b^2+2ca} + c\sqrt{c^2+2ab} \leq \\ &\leq \sqrt{a^2+b^2+c^2}\sqrt{a^2+b^2+c^2+2(ab+bc+ca)} = \\ &= \frac{\sqrt{a^2+b^2+c^2}}{3} \end{aligned}$$

Además tenemos que por la desigualdad MA-MG que,

$$27abc \leq (a+b+c)^3 = \frac{1}{3\sqrt{3}}$$

Solo nos falta acotar $\sqrt{a^2+b^2+c^2}$ y ya lo tendríamos, el problema es que tras varios intentos no sale. Hemos llegado a un punto muerto. Debemos buscar otro enfoque.

Por tanto, igual nos conviene probar con la desigualdad MA-MG en vez de utilizar la de C-S, de esta forma,

$$\begin{aligned} &a\sqrt{a^2+2bc} + b\sqrt{b^2+2ca} + c\sqrt{c^2+2ab} = \\ =&\sqrt{a^2(a^2+2bc)} + \sqrt{b^2(b^2+2ca)} + \sqrt{c^2(c^2+2ab)} \leq \\ \leq&\frac{a^2+(a^2+2bc)}{2} + \frac{b^2+(b^2+2ca)}{2} + \frac{c^2+(c^2+2ab)}{2} = \\ =&a^2+b^2+c^2+(ab+bc+ca) \end{aligned}$$

Podríamos haber separado por un lado $a^2+b^2+c^2$ y por otro $(a+b+c)^2$, pero hubiésemos llagado al mismo punto que antes. Debemos intentar conseguir con el $27abc$ alguna expresión parecida a lo que tenemos. Para ello probamos con la desigualdad C-S y tenemos que

$$9abc \leq (a+b+c)(ab+bc+ca).$$

Que multiplicando por 3 y sustituyendo, obtenemos,

$$27abc \leq \sqrt{3}(ab+bc+ca).$$

El problema que nos encontramos ahora es ese raíz de 3, pero lo podemos intentar introducir antes de utilizar la desigualdad MA-MG para ver si nos puede arreglar los coeficientes.

Operando como antes obtenemos que,

$$\begin{aligned} \frac{1}{\sqrt{3}}\sqrt{3a^2(a^2+2bc)} &\leq \frac{1}{\sqrt{3}}(2a^2+bc). \\ \frac{1}{\sqrt{3}}\sqrt{3b^2(b^2+2ac)} &\leq \frac{1}{\sqrt{3}}(2b^2+ac). \\ \frac{1}{\sqrt{3}}\sqrt{3c^2(c^2+2ba)} &\leq \frac{1}{\sqrt{3}}(2c^2+ba). \\ 27abc &\leq \sqrt{3}(ab+bc+ca). \end{aligned}$$

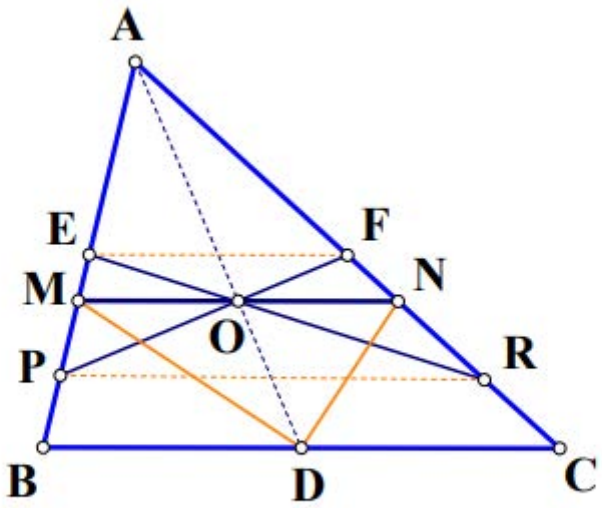
Sumando todo obtenemos que nuestra expresión es menor que,

$$\begin{aligned}\frac{1}{\sqrt{3}}\sqrt{3a^2(a^2+2bc)}+\frac{1}{\sqrt{3}}\sqrt{3b^2(b^2+2ac)}+\frac{1}{\sqrt{3}}\sqrt{3c^2(c^2+2ba)}+27abc \\ \leq \sqrt{3}(ab+bc+ca)+\frac{2a^2+bc+2b^2+ac+2c^2+ba}{\sqrt{3}} \\ = \frac{2(a+b+c)^2}{\sqrt{3}}\end{aligned}$$

Así tenemos que, el valor máximo que alcanza dicha expresión es, $\frac{2}{3\sqrt{3}}$.

Problema 12.3 (Día 2). En el triángulo *ABC*, los puntos medios respectivos de los lados *BC*, *AB* y *AC* son *D*, *E* y *F*. Sean: *M* el punto donde la bisectriz interior del ángulo $\angle ADB$ corta al lado *AB*, y *N* el punto donde la bisectriz interior del ángulo $\angle ADC$ corta al lado *AC*. Sean además *O* el punto de intersección de las rectas *AD* y *MN*, *P* el punto de intersección de *AB* y *FO*, y *R* el punto de intersección de *AC* y *EO*. Demuestra que *PR* = *AD*.

Solución *Primero, dibujamos el triángulo que se nos dice en el enunciado.*



A partir del dibujo, podemos hacernos una pequeña idea de como vamos a poder probar lo que nos piden. Por un lado, observamos que hay ciertos segmentos que parece que son paralelos como son el EF, MN, y PR que a su vez son paralelos a BC. Además parece que se forma un trapecio donde el segmento MN lo divide por la mitad. Esto nos podría relacionar el segmento PR con el EF y el MN. Por otro lado, podemos usar que EF y MN son paralelos teniendo en cuenta la semejanza de triángulos, igual podremos relacionar la alturas AD con EF y MN.

Empecemos buscando ciertas relaciones.

- *Por el teorema de la bisectriz, tenemos que:*
$$\frac{MB}{AM}=\frac{BD}{AD}\ y\ \frac{NC}{AN}=\frac{DC}{AD}.$$
- *Además como $BD=DC$ podemos relacionarlos y obtenemos,*
$$\frac{MB}{AM}=\frac{NC}{AN}.$$

- *Esto nos dice que los triángulos AMN y ABC son semejantes y por tanto tenemos la siguiente relación,*
$$\frac{AB}{AM} = \frac{BC}{MN}.$$

Como queremos relacionar AD con EF, pero de momento no tenemos ninguna relación. Lo que si que sabemos es que EF es la paralela media del triángulo ABC, y por tanto la pondremos relacionar con BD y con BC.

- *Con lo último, escribiendo $AB = AM + BM$, obtenemos,*
$$\frac{AM + BM}{AM} = \frac{BC}{MN} \implies 1 + \frac{BM}{AM} = \frac{BC}{MN}.$$
- *Por tanto, aplicando que $\dfrac{MB}{AM} = \dfrac{NC}{AN}$, tenemos que,*
$$\frac{BD + AD}{AD} = \frac{BC}{MN}.$$
- *Y con $EF = 2BC$ y $BD = EF$ obtenemos*
$$\frac{EF + AD}{AD} = \frac{2EF}{MN} \implies \frac{2}{MN} = \frac{1}{EF} + \frac{1}{AD}.$$

Esto nos recuerda mucho a la media armónica de EF y AD que nos da el valor MN, que casualmente es lo que tendríamos que calcular si en efecto $EFRP$ fuese un trapecio. Para ello utilizaremos el teorema de Menelao al triángulo AMN

- *Con el segmento ER*
$$\frac{AE}{EM}\frac{MO}{ON}\frac{NR}{RA} = 1 \implies \frac{AE}{EM}\frac{MO}{NO} = \frac{AR}{NR}.$$
- *Con el segmento FP*
$$\frac{AF}{FN}\frac{NO}{OM}\frac{MP}{PA} = 1 \implies \frac{AF}{FN}\frac{NO}{MO} = \frac{AP}{MP}.$$
- *Como $MO = NO$ y $\dfrac{AE}{EM} = \dfrac{AP}{MP}$ tenemos que,*
$$\frac{AR}{NR} = \frac{AP}{PA}.$$

Por tanto, eso nos dice que PR es paralela a MN y por tanto paralela a EF. Lo que nos construye el trapecio $EPRF$. Además como MN es paralela a las bases por el punto de intersección de las diagonales, MN es la media armónica de las bases del trapecio, es decir,
$$\frac{2}{MN} = \frac{1}{PR} + \frac{1}{EF}.$$
Y con lo visto anteriormente tenemos que $PR = AD$.

UNIVERSIDAD
DE LA RIOJA

Servicio de Publicaciones
Biblioteca Universitaria
C/ Piscinas, 1
26006 Logroño (La Rioja)
Teléfono: 941 299 187

http://publicaciones.unirioja.es
www.unirioja.es