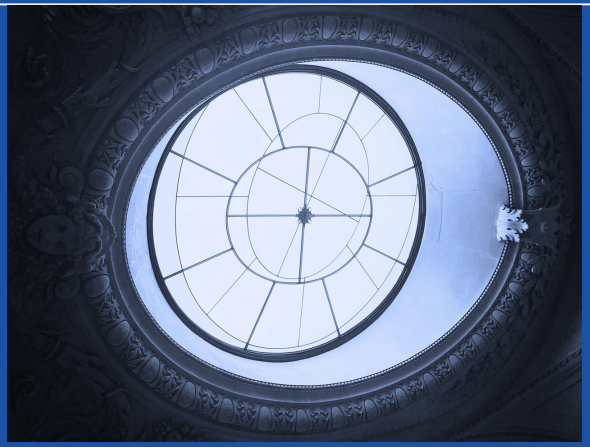
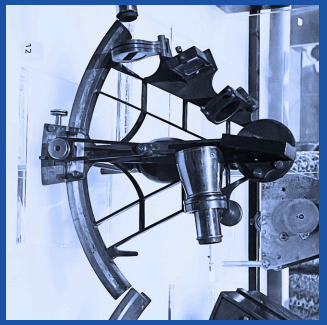
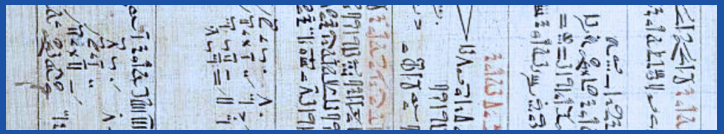
USC UNIVERSIDADE DE SANTIAGO DE COMPOSTELA
FACULTADE DE MATEMÁTICAS
N°6. ABRIL 2024
REVISTA ESTUDANTIL

MATES ÁIS







Introdución

Dirección da Revista

ÍNDICE

AGRADECEMENTOS

Queremos agradecer a todas as persoas colaboradoras na revista ata o momento. Ademais, neste novo número contamos coa presenza de Martín García Cebeiro, Iván Castro Sánchez, ambos estudantes da nosa Facultade. E tamén ao querido Luís Garbayo Fernández, que xa non estuda connosco, máis as mates séguenlle a picar dunha ou doutra maneira.

Dar unha forte aperta ás persoas que nos axudaron coa revisión lingüística e formal da revista: a profesora *Carmen Rodríguez* e ao profesor *Rafael Muñoz*.

Este número de abril será o último deste ano escolar. Esperemos estar para o ano ao pé do canón, pero bueno... xa veremos.

Tivemos unha xornada moi intensa o venres 3 de maio na vila natal de dous colaboradores da revista. Achegamos ao IES Celso Emilio Ferreiro, ao alumnado de 4º da ESO e de 1º de FPB un cachiño de que é a revista. Con eles aproveitamos para contar un pouco que son para nós as mates e tentar de mostrar moi someramente exemplos de cada sección.

Logo, na Casa de Curros Enríquez de Celanova, fixemos unha presentación similar, pero orientada a un público xeral. Tivemos a sorte de que nos dous sitios fomos recibidos moi gratamente, e os oíntes estiveron moi atentos.

Temos que dar as grazas a Paula (Casa de Curros) e tamén a Irma Fernández e Isidora Gil (IES) por ter os seus brazos abertos cara o noso proxecto. Agradecer tamén a Carlos Alonso pola realización das fotos.

Fig. 1: IES Celso Emilio Ferreiro de Celanova

Fig. 2: Casa de Curros Enríquez

Galois protexe os nosos datos?

Luís Garbayo Fernández

Setembro de 1939, Gran Bretaña entra en guerra con Alemania e un par de anos despois, tería lugar a primeira derrota das forzas alemáns. Pero... que pensaría vostede se lle dixera que as matemáticas estiveron moi presentes e que grazas a elas, gañouse a Segunda Guerra Mundial. Isto foi posíbel grazas á axuda da decodificación e técnicas de cifrado, práctica coñecida como criptografía. Esta é a responsábel de que os nosos segredos estean ocultos e só accesíbeis a aqueles que estén autorizados.

Neste punto o lector poderase estar preguntando como se conseguiu gañar unha Guerra grazas á codificación de simples combinacións de letras, números e símbolos. Dende logo, a relación simbiótica entre a criptografía e as matemáticas tivo moito que ver nisto.

Alan Turing na Guerra

Alan Turing foi un matemático, informático teórico, lóxico e criptógrafo británico quen, co seu equipo, conseguiu decodificar a máquina Enigma. Esta máquina era propiedade das forzas alemás, as cales a empregaban para enviar códigos encriptados aos seus submarinos sen que os aliados da Gran Bretaña os descubrisen.

Fig. 1: Alan Turing

Turing logrou decodificar as claves do rotor desta máquina -disco circular que contiña unha serie de conexións eléctricas internas que cifraban as letras do alfabeto- reducindo o conflito bélico entre dous e catro anos. Para esta decodificación desenvolveu a máquina *Bombe*, a cal eliminaba un gran número de claves *enigma* probables, minimizando as posibilidades. Para cada posible combinación poñíase en marcha con electricidade unha cadea de deducións lóxicas. Así, era posible detectar cando existía unha contradición e, deste xeito, refugar esa combinación. Pero Turing non só empregou a criptografía, senón que con análise matemática e métodos estatísticos logrou reducir o espazo de procura e acelerar o proceso de descifrado. Por isto, pódese dicir que Alan Turing e as matemáticas contribuiron significativamente ás operacións de intelixencia aliadas e ao desenlace da guerra.

Números primos

No mundo da criptografía moderna existen dous piares fundamentais nos que se basea esta práctica: a criptografía asimétrica, ou cifrado de clave pública e clave privada; e a criptografía simétrica, ou cifrado de clave simétrica, de clave segreda, ou dunha única clave.

Na primeira criptografía, ambas claves están relacionadas matemáticamente. A primeira clave, a pública, compártese abertamente e utilízase para cifrar mensaxes. Calquera persoa pode cifrar unha mensaxe utilizando esta clave, pero só o posuidor da clave privada correspondente pode descifrar a mensaxe cifrada. Con isto, a clave privada mantense en segredo e utilízase para descifrar mensaxes. Só o destinatario previsto, que posúe a clave privada correspondente á clave pública utilizada para cifrar a mensaxe, pode descifrar e ler o contido da mensaxe.

Pero... que teñen que ver os números primos nisto? O exemplo máis coñecido dun algoritmo que emprega estas claves é o RSA, nomeado así en honra aos seus inventores Ron Rivest, Adi Shamir e Leonard Adleman. RSA baséase na dificultade de factorizar grandes números compostos nos seus factores primos, un problema intrinsecamente relacionado coa teoría de números.

Así, o funcionamento deste algoritmo é o seguinte:

O esquema RSA é un cifrado no que o texto plano e o texto cifrado son enteiros entre 0 e $n-1$ para algúns n. Un tamaño típico para n é 1024 bits, é dicir, n é menor que 2^{1024}.

Para xerar as claves fai falta seleccionar dous números primos grandes. Sexan p e q dous números primos, o producto $n = p*q$, utilizarase como o módulo de cifrado e descifrado. Agora, búscase unha relación da forma $M^{ed}(\mod n) = M$, onde e será un número enteiro que sexa coprimo con $\phi(n) = (p-1)*(q-1)$, e que sexa menor que $\phi(n)$; dise que e é a clave pública. A clave privada será a d, e calcularase como o inverso multiplicativo de e ($\mod \phi(n)$).

Entón, agora quedaría ver como se cifran e decodifican as mensaxes. Suponse unha mensaxe M, a cal convertirase nun número m. Para isto, empréganse recursos como a táboa ASCII, onde cada caracter represéntase por un número enteiro, transformando así a cadea de caracteres nun $m \in \mathbb{Z}$ tal que $0 \leq m \leq n$. O cifrado da mensaxe, calcúlase mediante

$C = m^e(\mod n)$, sendo C a mensaxe cifrada. Pola súa contra, para descifrar unha mensaxe calcúlase a mensaxe orixinal m como $m = C^d(\mod n)$.

GALOIS E A CRIPTOGRAFÍA

Unha vez xa coñecemos en que se basan os algoritmos de criptografía asimétrica, por que dicimos que Galois encripta os nosos datos? Na criptografía simétrica, cómpre falar dun método de cifrado no que tanto o proceso de cifrado como descifrado utilizan a mesma clave secreta. Neste sistema, o remitente cifra a mensaxe orixinal utilizando a clave segreda antes de envialo, e o destinatario utiliza a mesma clave para descifrar a mensaxe e recuperar a información orixinal.

Un exemplo desta criptografía é o algoritmo AES (Advanced Encryption Standard), onde se empregan bytes (1 byte corresponde a 8 bits) para realizar as operacións necesarias, Existen 3 variantes de AES dependendo do tamaño das claves que se empreguen. Imos explicar o funcionamento para o AES-256 e sería análogo para o resto.

A entrada aos algoritmos de cifrado e descifrado é un único bloque de 128 bits -16 bytes- o que se representa como unha matriz M_{4x4}, que será sometida a un certo número de operacións. No AES-256, o cifrado da información realízase en 14 rondas, cunha clave distinta á inicial en cada ronda, obtida mediante *keyexpansion*. O que se consigue con isto é un conxunto de claves derivadas, cada unha de 128 bits de tamaño. Expliquemos o funcionamento do AES-256:

O algoritmo comeza sumando a clave da ronda un, combinando cada bit cun bit do noso bloque de información almacenado na matriz M (operación XOR binaria). Por conseguinte, realízase a substitución de bytes seguindo unha táboa do estándar AES, denominada *S-box*. En realidade isto é o mesmo que facer unha operación cunhas certas propiedades: [1] ten que ser unha operación lineal; [2] deberanse evitar os puntos fixos, é dicir, que o resultante da operación aplicada a un byte non sexa el mesmo; [3] terase que evitar que o resultado dela sexa o complementario dese byte, é dicir, a substitución respectiva dos 1's por 0's e 0's por 1's.

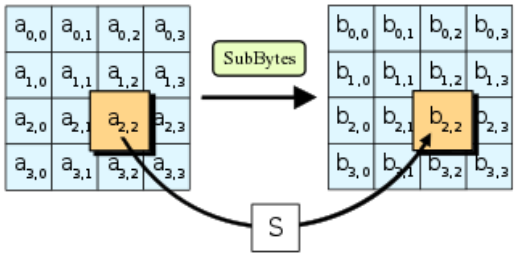


Fig. 2: Substitución de bytes

Para poder facer estas operacións hai que operar sobre corpos finitos, aquí é cando entra en acción o noso querido Galois. Brevemente, un corpo é un conxunto onde pódense facer certas operacións: a suma e a multiplicación. Ademais, cada elemento do conxunto terá un inverso multiplicativo. Un exemplo de corpo son os números reais, $\mathbb{R}$. Para este algoritmo emprégase un corpo cun número finito de elementos, é o caso dos corpos de Galois (*Galois Field*) de 2^n, elementos. No caso do AES-256, defínese o GF (2^8) xa que $2^8 = 256$, que é a lonxitude máxima da nosa clave. Isto explica porque Galois é importante na criptografía, xa que, estando no seu corpo asegúrase que ningunha operación exceda o rango establecido polo algoritmo.

Os dous seguintes pasos consisten na mestura das filas e das columnas da matriz M. Para mesturar as columnas multiplícase cada columna por unha matriz en concreto, aplicando a operación XOR binaria en lugar da suma, e, realizando unha redución co polinomio irreducible en GF(2^8) (isto é dividir por ese polinomio). Para concluír, súmase a clave da ronda. Unha vez complétase a primeira ronda, repítese ata chegar á última, na cal non aplica a mestura de columnas.

Podemos concluír que a intersección entre as matemáticas e a criptografía revela un fascinante mundo onde a teoría entrelázase coa práctica para protexer a información sensíbel na era dixital. Dende os antigos cifrados ata os complexos algoritmos modernos, as matemáticas proporcionan a base sólida sobre a cal se constrúen os sistemas de seguridade informática.

REFERENCIAS

[1] *Alan turing, el arma secreta de los aliados* National Geographic - Historia, enlace: https://historia.nationalgeographic.com.es/a/alan-turing-arma-secreta-aliados_16352.

[2] *Código Enigma, descifrado: el papel de Turing en la Segunda Guerra Mundial* , enlace: https://www.eldiario.es/turing/criptografia/alan-turing-enigma-codigo_1_5038272.html.

[3] WILLIAM STALLINGS (2016). *Cryptography and Network Security: Principles and Practice 7th Global Edition*.

Un paseo polo Sarela: Elena Vázquez Cendón

Francisco Estévez Lengua

Nesta última entrevista recibimos a Elena Vázquez Cendón, Decana da nosa Facultade de Matemáticas. Estudou o Bacharelato no Instituto das Lagoas, en Ourense. Licenciada en Matemáticas pola Universidade de Santiago de Compostela. Doutora pola mesma universidade coa tese "Estudio de esquemas descentrados para su aplicación a las leyes de conservación con términos fuente" 1994, dirixida por Dr. Alfredo Bermúdez de Castro López-Varela. É profesora de matemática aplicada na Facultade de Matemáticas da USC, foi vicerreitora da USC,[Wikipedia] e é decana da Facultade de Matemáticas dende 2017. É membro do Consello da Cultura Galega. É autora de numerosos artigos en revistas especializadas de matemáticas e computación. En 2022 foi Premio María Josefa Wonenburger para mulleres científicas. (Sacado da galipedia).

O intre no que se desenvolveu a entrevista foi durante unha camiñata pola beira do río Sarela, un encontro onde nos propuxemos coñecer máis á unha das persoa que dirixe a nosa contorna.

- F: Comecemos pola definición. Como te definirías no ámbito matemático? Cóntanos un pouco de ti.
- E: Matemática aplicada. Dende sempre e sen dúbidas. Dende pequena atraeume o feito de verificar e comprobar hipóteses, o pensamento abstracto o que facía era reafirmar que entendía o que estaba facendo. Sempre me acordarei de pequena, cando tiña que comprobar cal era o volume dun cilindro: miña avoa tiña unha lata de melocotóns, e recordo ir debuxando por riba dos melocotóns e xusto dera o mesmo que puña na lata! Quen fóra dicir que estaría comprobando unha cousa coma o principio de Cavalieri!
- F: Ti, sendo nós coma somos de Ourense, seguro que tes algún escritor ou personaxe relevante da nosa contorna, non si?
- E: Quérome acordar de Otero Pedrayo, que o ligo con Domingo Fontán. E que eu son unha Fontaneira declarada. Esta persoa é un dos galegos que máis admiro, botou 17 anos tomando medicións de toda Galicia e foi o primeiro que fixo un mapa científico de Galicia. Ademais está cerca de Rosalía no Panteón dos Ilustres, así que, no alén, ou na proxección do alén á nosa realidade, as matemáticas son as que máis preto están da Lingua.
- F: Como foron os camiños ata chegar ás matemáticas?
- E: Pois todo comezou cun profesor de física, o señor Arias, que era un crack. Era capaz de facerche intuir cousas como as integrales por camiños e outras máis complexas. Era un visionario. De feito, eu cría que ía facer física, pero houbo un contubernio, entre o profesor de química, que quería que fixera química. E entre o profe de mates, que o meu pai era o que lle facía os traxes; coñecino dende que eu era un botón. El enseguida che facía unha árbore de decisións, e che dícia: mira, e que se é para dar clase en instituto, que se queres dar física e química, o temario é case de todo de química, logo non fagas física, e se para tal tal e se é para o outra tal... E só me deixou como unha porta aberta, díxome que non me ía dicir que non á física, porque poderiamos estar ante o (a) segundo Einstein. E eu andaba entre as mates e a física, asique fun bucar nunha revista a ver si me orientaba un pouco. Atopei unha na que aparecía un físico, e puña: Stephen Hawkins, no segundo parágrafo "pode ser considerado como un segundo Einstein". Ao final, chegamos a un triángulo, pero total, que acabei en Mates. Pero o que fago, cando non xestiono, que iso tamén é matemáticas aplicadas (risas), é un punto de encontro entre as matemáticas e a física. Na miña tese, eu calculaba as corrientes nas rías galegas, e todo o que facemos, o de fluidos, tanto na agua, coma na sangue, coma no gas, é un punto de encontro, pois nós, logo resolvemos numericamente, entón, ahí triángulas a realidade, o que se pon das matemáticas, e a física e as ecuacións que modelan eses efectos. Entón eu creo que estou onde quería estar, pero daquelas non se chamaba así. Din un pouco de voltas, a verdade que non me arrepinto nada de non ter feito física, pero si que foi un camiño curioso.
- F: Pero ti tiveches algunha inspiración máis en concreto para acabar elixindo as matemáticas?
- E: Pois eu tiven tres profesores no ensino medio que foron moi estructurais. A primeira, Lourdes, logo dun tempo dinme conta da proxección que tiña con ela. Co segundo, Isidro, que era asturiano e daba as clases en galego, foi co que sacaba moitos deces. E co último, con Alfonso, que foi decisivo para que acabara por elixir as matemáticas e aprecio moito, claro, que era un comunicador alucinante, cando te contaba cada cousa, te proxectaba onde podían estar esas matemáticas, e iso era moi especial. Porque cando nos explicou daquela o desenvolvemento de Taylor no instituto, que para nada era algo intuitivo, preguntaba, e isto para que se usa? Pois isto úsase, por exemplo, cando hai que facer as pontes, e para as vigas. Logo vin a profunda conexión que nos quería transmitir Alfonso, pois foi no programa

de doutoramento con Viaño cando vin as ecuacións de elasticidade que se aplican nas pontes.

- F: Bueno, xa me falaches un pouco do que fixeche no namentres. Poderíasme contar así algún corolario da túa experiencia como matemática?

- E:Algún corolario... bueno, eu creo que das cousas que me teñen aportado as matemáticas, o máis satisfactorio, é cada vez que te sentas con persoas diferentes, cun obxetivo de aprender. Claro, eu cando cheguei, había que resolver o das Rías Galegas, empezamos pasiño a pasiño. E iso eu creo que se percibe máis na matemática aplicada, porque ti non podes traballar solo na túa leiriña. Ti tes que enriquecerte augas arriba e augas abaixo e polos lados do coñecemento. No meu caso traballamos con Alfredo, o director da miña tese, despois coa Consellería da Xunta e ata co Estreito de Xibraltar. Eu me lembro de estar poñendo en Cádiz resultados da dinámica dos resaltos que se producen, solucións discontinuas, que ti podes facer todo cálculo analítico e chegas a obter esas solucións deses problemas de Riemann, pero que os métodos numéricos, se saben as matemáticas que hai por trás e se os inspiras ben, se os diseñas para que resolvan esas solucións únicas, discontinuas, as clavan. Entón, eu lémbrome dun oceanógrafo que miraba para as gráficas e el dicía, pero hai algo que explicara máis ca esas gráficas? Non, non. E isto sen facer todas as contas. Isto pódese calcular co ordenador.

  E logo outros dos corolarios, e que a veces ti ves o mundo e podes ver problemas que son moi diferentes, non? O fluxo do gas, o fluxo do sangre, o fluxo das persoas... E ti dis, bueno, pois necesito un matemático para cada unha destas cousas. Non! Pero que o ADN matemático de todos eses problemas é o mesmo. Entón, voulle ter que facer o traxe a medida, pero coma dicía meu paí, vou ter que afinar menos, porque xa teño o patrón, non?

  Sobre todo cando ves a moita xente, en xurados, que é capaz de discutir e alegar, dende a elegancia, eu aí é cando me derrito, non? Porque ti podes dicir, pois moi ben, Chisco, eu entendo a túa mirada, porque tes a idea de que tes, porque a ti che motiva esto, pero eu advirto esto...

- F: E poderíasnos contar algunha experiencia que tiveras facendo divulgación?

- E: Teño feito divulgación, dende os da Escola Infantil Breogán, da universidade, que aí os grandes teñen tres anos. E as dúas veces que fun, volvín con algo... moi aprendido. Unha das veces aprendín como eles abstraen os afectos, co conto este dos cadradiños e os redonditos, un rapaz, deume unha lección moi estructural. Os redonditos son amigos, viven nunha casiña, pero os redonditos sinten, e os redonditos preocupanse de construír unha solución, porque queren o seu amigo que é o cadradiño, non? E a él lle gustou moito unha peza que eu ensinei, funllo dar e dixo que o cuadradiño de Elena me quería e se viña comigo. E dixen, claro, eles eran capaces de abstraer que chegaba unha solución ao problema porque querían, porque sentían.

  E a segunda vez que fun, fixen os cuadradiños e os circuliños con pisla e os trianguliños que encaixaban moi ben. Entón, foi un rapaciño todo serio e díxome: “dos triangulitos, un cuadradito’. E non o dixeche!” Contoumo coma se fose a súa tese, e a min pareceume máxico porque aquel neno tiña dous anos. A sús pies. Claro, ten toda a razón. Pero ese punto de cando ti sementas cousas, iso si que é unha verdadeira satisfación.

- F: Para rematar esta entrevista gustaríame preguntarche sobre a que aspiras agora. Quédache un ano coma decana, e despois, que?

- E: O chanzo seguinte é preparar a oposición da cátedra e acabar de poñer esas pinceladas a problemas, cos que me vou retar ata que me xubile, porque aínda queda, pero non tanto. Entón o reto seguinte é volver a mergullarme nas matemáticas, pois hai problemas relacionados con sangue, vamos, de fluidos, pero coas metodoloxías que eu emprego. E tamén acabar teses nas que me comprometín a dirixir, e seguir apaixonándome con resolver problemas, que algúns hoxe non me imagino. Pero o que foi moi gratificante foi cando traballamos con Alfredo (o director da tese de Elena) para Reganosa, para a Rede de Gas, que resulta que a metodoloxía que empregáramos para auga, puidemos trasladarla para a Rede de Gas, porque hai tamén que seguir a orografía, é dicir, de novo seguir o Fontán era importante, e aplicar o que fixéramos antes para o gas. Xusto o que nós fixéramos ninguén o aplicara, e entón fixemos esa adaptación. Entón pode ocurrir que haxa outros problemas que sexan da mesma forma. Como agora, que estou codirixindo unha tese, sobre propagación de virus en distintas redes, que é o que está facendo o Javier López.

A entrevista tivo a presenza do son do río, da dúas libélulas e dunha persoa que se abriu con esta revista, quen está a escribir, simplemente fixo iso, escribir. Quen coñeza a Elena poderá entender como se explica. Intentei manterme fiel ao que me dixo ela e resumir bastante, pois daría para catro páxinas todo sobre o que falamos. Facer notar que emprega moito a metáfora e os dobres sentidos, tamén están fragmentos en estilo indirecto. A retranca matemática desta muller é unha beleza digna de admirar. Moitas grazas Elena.

Retos Matemáticos

Sementeira
Clube Olímpico de Mates-USC

Fórmulas de Cardano-Vieta

Consideramos un polinomio mónico de grao dous con coeficientes complexos ($p \in \mathbb{C}[x]$) tal que $p(x) = x^2 + bx + c$.

Sabemos, polo teorema fundamental da álxebra, que existen dúas raíces complexas $\alpha, \beta \in \mathbb{C}$ que permiten factorizar o polinomio do seguinte xeito

$$x^2 + bx + c = (x - \alpha)(x - \beta).$$

Se expandimos o lado dereito da igualdade obtemos

$$x^2 + bx + c = x^2 - (\alpha + \beta)x + \alpha\beta.$$

Comparando coeficientes obtemos as fórmulas de Cardano-Vieta de orde dous:

$$b = -(\alpha + \beta), \quad (1)$$
$$c = \alpha\beta. \quad (2)$$

Nótese a importancia de que o polinomio sexa mónico. De non ser o caso, teriamos que axustar dividindo polo coeficiente do termo principal.

Analogamente pódense obter as fórmulas para os polinomios de calquera grao. De forma xeral, dado un polinomio

$$p(z) = a_0 + a_1 z + a_2 z^2 + a_3 z^3 + \ldots + a_k z^k = a_k (z - z_1)(z - z_2)(z - z_3) \cdots (z - z_k).$$

podemos obter as fórmulas de Cardano-Vieta de orde k:

$$\begin{cases} a_{k-1} = (-1)^1 \cdot a_k \cdot (z_1 + z_2 + z_3 + \ldots + z_k) \\ a_{k-2} = (-1)^2 \cdot a_k \cdot (z_1 \cdot z_2 + z_1 \cdot z_3 + \ldots + z_{k-1} \cdot z_k) \\ \quad \vdots \\ a_j = (-1)^{k-j} \cdot a_k \cdot (z_1 \cdot z_2 \cdot z_3 \cdot \ldots \cdot z_j + \ldots + z_{k-j+1} \cdot z_{k-j+2} \cdot \ldots z_k) \\ \quad \vdots \\ a_1 = (-1)^{k-1} \cdot a_k \cdot (z_1 \cdot z_2 \cdot z_3 \cdot \ldots \cdot z_{k-1} + \ldots + z_2 \cdot z_3 \cdot \ldots z_k) \\ a_0 = (-1)^k \cdot a_k \cdot (z_1 \cdot z_2 \cdot z_3 \cdot \ldots \cdot z_k) \end{cases}$$

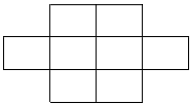
Estas fórmulas permiten relacionar os coeficientes dos polinomios coas súas raíces. O sistema resultante é non linear, polo que na práctica é moito máis difícil de resolver se a cuestión é atopar as raíces. Non obstante, estas relacións teñen unha gran importancia teórica para operar coas raíces sen coñecelas. As aplicacións nas matemáticas son múltiples, por exemplo, axúdannos a relacionar o determinante e a traza dunha matriz cos seus autovalores a través do polinomio característico.

Problemas Propostos

1. Sexan $a, b, c \in \mathbb{Z}$ tres enteiros distintos e P un polinomio con coeficientes enteiros. Demostra que non se poden dar simultaneamente as igualdades $P(a) = b$, $P(b) = c$ e $P(c) = a$.

2. Dado $\triangle ABC$, definimos os puntos $D, E \in BC$ tal que AD é unha altura e AE a bisectriz do ángulo A. Definimos ademáis $M \in AE$ tal que BM é perpendicular a AE e $N \in AC$ tal que EN é perpendicular a AC. Demostra que os puntos D, M, N son colineais.

3. Coloca todos os números dende o 1 ata o 8, sen repetirse, no seguinte cadro, cada un nunha cela. Os números consecutivos non poden tocarse entre si, nin por un lado nin polo vértice.



4. Sexa $n \in \mathbb{Z}$ un impar tal que $n > 1$. Probar que a seguinte suma é impar:

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

Solucións do mes pasado:

As matemáticas da democracia: de Condorcet a Arrow

Santiago González Gómez

Noite electoral. O partido preferido polo teu amigo quedou moi preto de gañar, pero ao final non lle chegan os escanos para formar goberno. Entón, diche: "hai que cambiar a lei electoral! Todo isto é culpa da lei d'Hondt. Con outro sistema isto non pasaba". Algunha vez viviches algo similar? E o máis importante, ten razón o teu amigo? Hai algún sistema de votación mellor có noso? Que nos din as Matemáticas?

CONDORCET E A ELECCIÓN SOCIAL

Coñécese como teoría da elección social ao estudo dos mecanismos e procedementos que a sociedade leva a cabo para tomar unha decisión colectiva. A elección social toma prestadas ferramentas matemáticas de probabilidade e teoría de xogos para estudar situacións en disciplinas tan amplas como a xustiza (xurados), a economía (preferenzas comerciais), ou o que nos interesa a nós, a avaliación de procedementos democráticos.

Fig. 1: Marie-Jean-Antoine Nicolas, marqués de Condorcet.

A democracia iníciase na Antigüidade, pero en gobernos pequenos como o ateniense nunca houbo necesidade dun estudo do proceso democrático ou dos sistemas de votación. Non sería ata os traballos do marqués de Condorcet nos albores da Revolución Francesa cando se inicia a teoría da elección social. Xa estudosos medievais anteriores, como o polifacético mallorquín Ramón Llull, escribiran sobre o tema, pero o seu traballo non tivera maior repercusión. Condorcet era liberal, e viviu nunha época politicamente convulsa na que moitos ilustrados levaron á escea o debate da recuperación da democracia como forma de goberno. Na súa *Essai* de 1785, Condorcet establece unha gran diferenza entre os propósitos da democracia antiga e da moderna. Segundo el, os antigos empregaban a democracia por "utilidade" e "liberdade", mentres que os gobernos modernos esixen decisións de grande importancia social, como a política económica, onde a democracia podería ser útil para buscar a "verdade" e a "xustiza". Neste sentido, introduciu o coñecido como "teorema do xurado de Condorcet": se cada membro dun xurado ten unha probabilidade maior do 50 % e menor do 100 % de emitir un xuízo verdadeiro, entón a probabilidade de emitir un xuízo verdadeiro crece ao aumentar o número de persoas no xurado. A obra de Condorcet foi moi importante para o desenvolvemento da teoría probabilística, especialmente no que se refire á súa aplicación. Condorcet defendeu que a vida política podía basearse na razón e en regras matemáticas, acadando a mesma precisión que unha ciencia física.

OS SISTEMAS DEMOCRÁTICOS A EXAME

Baseándose nas súas ideas, Condorcet creou o sistema electoral que leva o seu nome. Chegados a este punto, é necesario que establezamos unhas nocións coas que traballar. Supoñamos que temos un conxunto de alternativas $A = \{a,b,c...\}$ entre as que queremos elixir. Para ser o máis xerais posibles, imos considerar que todo sistema electoral esixe que cada elector ordene todas as alternativas nunha lista de preferencias, no canto de elixir unha soa (como pasa nas eleccións en España). Logo, podemos escoller que o noso sistema faga caso só ao primeiro elemento da lista de cada elector, así que isto non é problema

Definición 1. Chamamos **procedemento de elección social** a unha aplicación que, dado un conxunto de listas de preferencias, devolve un elemento ou subconxunto de A, ou "SG".

Un procedemento de elección social é basicamente unha función que, dadas varias alternativas, "consulta" á poboación e devolve un gañador, varios, ou ningún ("SG", sen gañador).

Vexamos agora un exemplo de procedemento de elección social, precisamente o criterio de Condorcet. Dado un conxunto A, o criterio de Condorcet fai o seguinte: pide a cada elector que realice unha lista coas súas preferencias, e posteriormente escolle unha alternativa x gañadora se a maioría dos electores prefiren a x sobre y $\forall y \in A, y \neq x$. A priori, o método de Condorcet parece moi razonable, pois tenta que o gañador sexa aquela alternativa que gañaría un cara a cara contra calquera outra. Porén, ten un fallo letal: é moi restritivo, e non sempre produce un gañador. En efecto, supoñamos que $A = \{x,y,z\}$ e que temos tres electores, cuxas listas ordenadas de preferencias son, respectivamente, (x,y,z), (y,z,x) e (z,x,y). Entón, dous terzos da poboación prefiren x sobre y, dous terzos prefiren y sobre z, e dous terzos prefiren z sobre x. Este é o coñecido como paradoxo de Condorcet, e aquí o seu criterio non ofrece gañador. Imaxinemos por un momento que as eleccións xerais en España empregasen un método que non sempre dese gañador!

Para resolver este e outros problemas, propuxéronse outros procedementos de elección social. Por exemplo, xa en 1770 Jean Charles de Borda introducira o método coñecido como conta de Borda, que é similar, por exemplo, ao mundial de Fórmula 1: para a lista de cada elector, concédeselle a cada alternativa unha puntuación segundo a súa posición (0 á última, 1 á penúltima, etc.); gaña a alternativa que recade máis puntos. Non podemos non citar a votación plural, que é a xeralización máis inmediata do concepto de maioría (o $x \in A$ que apareza votado en primeiro lugar máis veces gaña). O último método que mencionaremos é o chamado sistema de Hare, introducido por Thomas Hare en 1861, que consiste en

ir eliminando a alternativa que aparece menos veces como preferida nas listas ata que só queda unha.

Como decidimos que procedemento de elección social é o mellor, se é que o hai? Todos parecen correctos. Pode existir moita diferenza entre eles? Para examinar que método é preferible, os teóricos da elección social introducen unhas certas propiedades desexables que debería de cumprir un procedemento para ser considerado "bo". Por exemplo, [1] introduce as seguintes cinco propiedades que debería de cumprir un sistema de votación:

Definición 2. Dado un procedemento de elección social, gustaríanos que cumprise as seguintes propiedades.

1. **Condición Sempre-Un-Gañador (SUG)**: o procedemento sempre devolve un gañador.

2. **Criterio do Gañador de Condorcet (CGC)**: se nos atopamos nunha situación na que o criterio de Condorcet é capaz de determinar un gañador, entón o noso procedemento devolve o mesmo gañador ca Condorcet.

3. **Condición de Pareto**: se todo o mundo prefire a alternativa x sobre y, entón o noso procedemento non pode devolver a y como gañador.

4. **Monotonía**: se o noso procedemento devolveu x como gañador e algún elector cambia a súa lista de modo que x sube de posición, x segue a ser o gañador.

5. **Independencia de Alternativas Irrelevantes (IAI)**: se o noso procedemento devolveu x e non y como gañador, e algún elector cambia a súa orde pero segue prefirindo x sobre y, entón x segue sendo o gañador.

Podemos preguntarnos por que recollemos estas propiedades e non outras; porén, creo que podemos estar de acordo en que todas son bastante razonables. Cadaquén podería engadir criterios, pero unha vez que le estes, parece desexable que un procedemento os cumpra. Aquí comezan os problemas cos sistemas de votación descritos antes. Como xa indicamos, Condorcet non cumpre SUG. Pero é que ademais (ver [1] para os contraexemplos), tanto a votación plural como a conta de Borda non cumpren CGC nin IAI, e o sistema de Hare non cumpre ningún destes dous, e tampouco Monotonía. Todos semellaban métodos válidos, pero ao seren enfrontados contra propiedades que buscamos neles, fallan. Existirá algún sistema de votación que satisfaga os nosos desexos?

Arrow e a imposibilidade

Ata o século XX, os estudosos da teoría da elección social propuxeran individualmente métodos de votación e examináranos. Kenneth Arrow, Nobel de Economía en 1972, foi o primeiro en evaluar procedementos de elección de forma xeral, de xeito similar ao que acabamos de facer nós. Arrow partiu duns axiomas que debería cumprir un bo procedemento de elección social e buscou un que os cumprise todos. Non toma como axiomas as mesmas propiedades cás nosas, pero si son similares: por exemplo, el tamén contempla a condición de Pareto e a IAI. Neste marco, Arrow probou o seguinte teorema:

Teorema 1 (de Arrow). Sexa un conxunto de alternativas A, $|A| > 2$. Entón, se esiximos que a orde das listas de preferencia dos electores sexa completa [1] e transitiva [2], non existe ningún procedemento de elección social que funcione sempre e que cumpra tanto a condición de Pareto coma IAI, non sendo unha ditadura.

Entendemos aquí ditadura como o procedemento de elección social que ignora tódalas listas agás unha (a da persoa que chamamos ditador). Aínda que non é inmediato, no marco dos nosos "axiomas", pódese reformular o teorema así:

Teorema 2 (de Arrow (reformulación)). Sexa un conxunto de alternativas A, $|A| > 2$. Entón, non existe ningún procedemento de elección social que cumpra SUG, CGC e IAI.

Polo tanto, o que nos di o teorema de Arrow é que non existe o sistema electoral perfecto, por iso ás veces se coñece como "teorema de imposibilidade". Por outra banda, é sinxelo ver que unha ditadura cumpre tódalas nosas propiedades agás CGC. É chamativo que un sistema electoral que na práctica non contemplamos por razóns democráticas estea matematicamente tan preto de satisfacer as nosas condicións, especialmente porque a propiedade que non cumpre é CGC, que é a que *a priori* parece máis artificiosa.

As interpretacións do teorema de Arrow son diversas: hai quen o usa para xustificar a inviabilidade dunha democracia popular, hai quen defende que unha lista de preferencias non é suficiente para reflectir a vontade popular... A postura moderna é que os nosos axiomas (ou os de Arrow) son demasiado fortes, e procúranse novas propiedades básicas.

Facemos notar que os sistemas de votación que examinamos aplícanse a situacións de democracia directa, como as eleccións presidenciais. Tamén aplicaría ás investiduras en España, tomando como electores aos parlamentarios. O lector pode imaxinar agora como se complica o estudo ao contemplar sistemas de reparto de escanos, que é onde entran criterios como a Lei D'Hondt que mencionabamos inicialmente. En conclusión, o procedemento democrático non só non é perfecto, senón que a elección do sistema máis xusto posible non é tan sinxela como parecía...

Referencias

[1] Taylor, A. D., Pacelli, A. M. (2008). *Mathematics and politics: strategy, voting, power, and proof*. Springer Science and Business Media.

[2] *Social Choice Theory*, Stanford Encyclopedia of Philosophy (consultado 27/03/2024), enlace: `plato.stanford.edu/entries/social-choice/`.

[3] *Biographies - MacTutor History of Mathematics* (consultado 27/03/2024), enlace: `mathshistory.st-andrews.ac.uk/Biographies`.

[1] É dicir, que dadas dúas alternativas x e y, están relacionadas (sempre se prefire unha á outra, non nos é indiferente).

[2] Se prefirimos x a y e y a z, entón non pode ser que prefiramos z a x.

Táboas e Estrelas

Martín García Cebeiro

Ditosas táboas de sumar e multiplicar. Son aburridas, mais cumpren o seu propósito. Todos pasamos por elas de nenos, pero creo que ninguén as bota de menos. Porén, agora a nosa visión é máis ampla, así que, por que non revisitalas?

O meu obxectivo non é que nos mergullemos na teoría de números en busca de resultados sorprendentes que logo deriven noutros. Non, conformareime con expoñer unha serie de patróns xeométricos agradables á vista para animarvos a seguir descubrindo por vós mesmos.

Preliminares

Cómpre facer unha breve introdución á aritmética modular, na que nos moveremos a continuación, en caso de que o lector non estea familiarizado con ela.

En lugar de operar cos números enteiros como adoitamos dende pequenos, traballaremos cos restos que resultan de dividir entre certo número. Se dividimos un enteiro entre outro positivo, n, os posibles restos que pode tomar son $0, 1, \ldots, n-1$; se o resto de dividir m entre n é k, dirase que m é congruente con k módulo n.

Todos os enteiros que compartan o mesmo resto ao dividir entre n diranse congruentes entre eles. Isto resulta nunha relación de equivalencia en $\mathbb{Z}$, que da lugar ao conxunto cociente $\frac{\mathbb{Z}}{n\mathbb{Z}} \equiv \mathbb{Z}_n$, o cal podemos identificar co conxunto $\{0, 1, \ldots, n-1\}$.

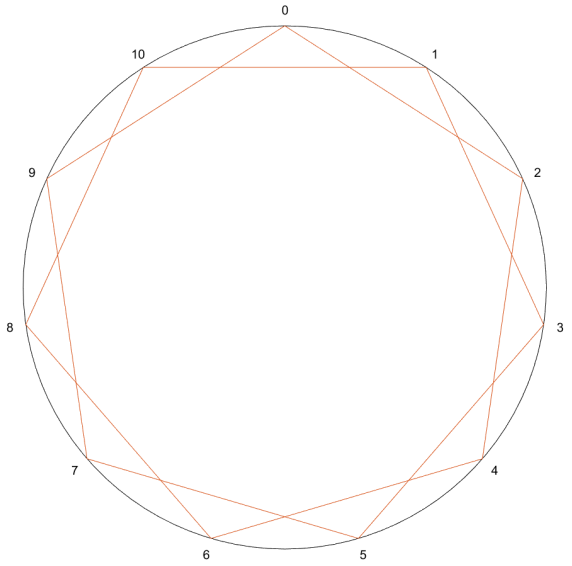
Todas as posibles sumas e multiplicacións neste conxunto precisan unicamente dunha táboa nxn por operación. A idea é que as operacións reiteradas ciclan, co cal resulta axeitado representar os n restos como puntos equiespazados nunha circunferencia, e así visualizar certas estruturas que as táboas non nos deixan ver.

A estas estruturas gústame chamalas estrelas aritméticas, para a suma, e estrelas xeométricas, para o produto, por analoxía ás sucesións aritméticas e xeométricas na súa construción.

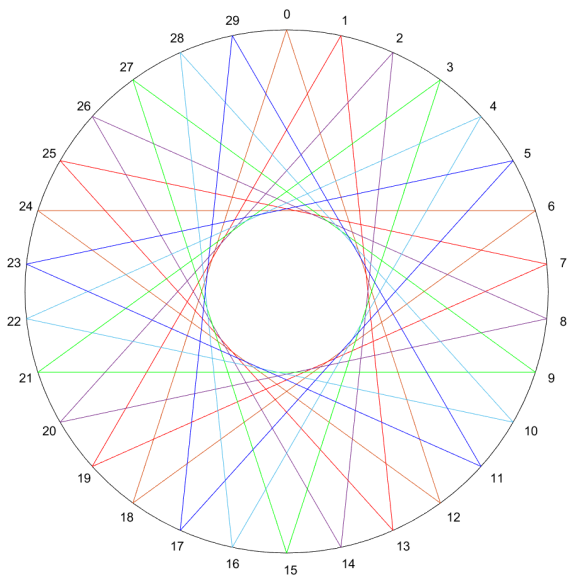
Estrelas aritméticas

Fixado un $n \in \mathbb{Z}^+$ e un $k \in \{0, 1, \ldots, n-1\}$, representaremos o resultado de sumar $m+k$, con $m \in \{0, 1, \ldots, n-1\}$, mediante un segmento que una os vértices asociados a m e a $m+k$ módulo n.

O que obtemos son estrelas de n puntas con amplitude en función de k. Se nos fixamos, a estrela de 11 puntas pode obterse nun só trazado continuo unindo vértices, mentres que a de 30 con amplitude 12 non. Cada trazado pechado ten asociado unha cor distinta, e se achegamos o ollo vemos que son estrelas de 5 puntas xiradas.



(a) $n = 11, k = 2$



(b) $n = 30, k = 12$

Fig. 2: Sumar k módulo n

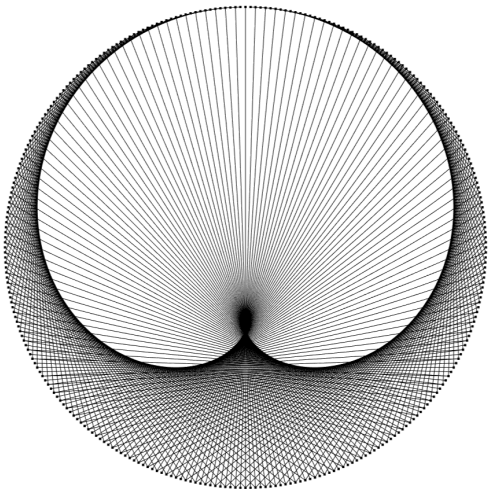
Propoño ao lector analizar este comportamento no caso xeral, que terá que ver coa orde dos elementos do grupo $(\mathbb{Z}_n, +)$ e co máximo común divisor de n e k.

Estrelas xeométricas

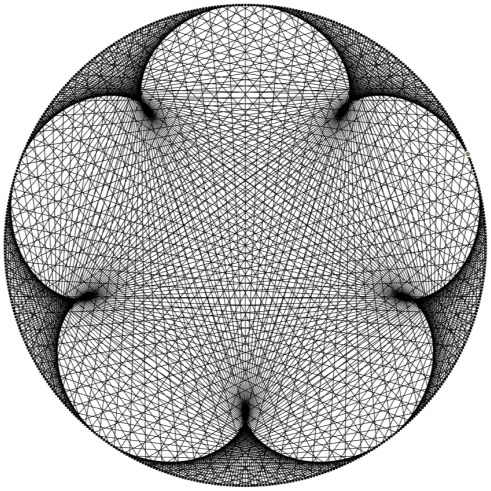
Agora, se facemos o mesmo multiplicando por k en lugar de sumando, os patróns xeométricos non se fan evidentes ata aumentar o tamaño de n considerablemente.

Destaca o caso de $k = 2$, no que os segmentos envolven a curva que se coñece como cardioide, pola súa forma de corazón. Ao reflexarse a luz no fondo dunha taza aparece a mesma curva, e para quen lle interese, a proba de ambos sucesos é idéntica.

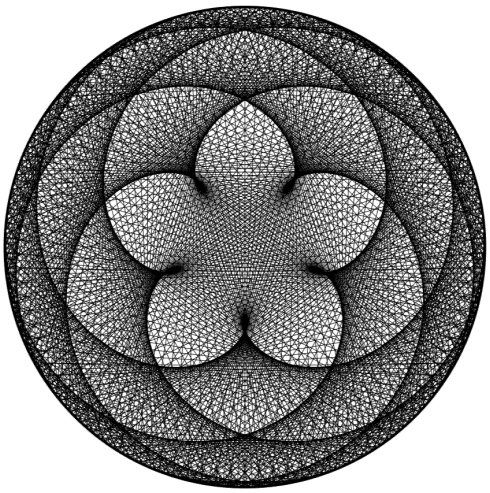
A medida que aumentamos k, as figuras que se forman van gañando "pétalos", tendo en xeral $k-1$ pétalos, e a partir de certo punto comezan a xurdir novas siluetas no interior que



(a) $n = 300$, $k = 2$



(b) $n = 500$, $k = 6$



(c) $n = 1000$, $k = 402$

Fig. 3: Multiplicar por k módulo n

paga a pena pararse a observar xa só pola súa beleza.

Animovos a coller a vosa linguaxe de programación de confianza e fedellar un pouco en busca de outros patróns que se pasen por alto a simple vista, ou mesmamente para ter unha colección de imaxes bonitas feitas con matemáticas!

Automórficos

Iván Castro Sánchez

As matemáticas atópanse en todas as partes da nosa vida, e por iso, non só estudamos complicados teoremas e intrincados problemas, tamén podemos atopar pracer na simpleza de buscar que números cumpren certas características comúns.

Así, no ano 1562, Juan Pere de Moya publicou "Diálogos de aritmética práctica e especulativa" onde presentou o concepto de "números circulares" que hoxe en día coñecemos como "números automórficos".

Definición 3. Un número x é automórfico se, ao elevalo ao cadrado, o resultado remata no propio x.

Por exemplo 5 é un número automórfico en base 10 xa que $\mathbf{5}^2 = 2\mathbf{5}$. Outros números automorficos (non triviais) en base 10 son 6, 25, 76, 376, 625... Noutras bases tamén existirán distintos números automórficos, por exemplo en base 6 os números 3, 4, 13, 44... serán automórficos.

Desta característica de aparencia simple poden deducirse distintas propiedades curiosas.

Cantidade

O matemático R. A. Fairbarn descubriu unha forma de atopar cantos números automorficos haberá como máximo en cada base para cada número de dixitos. Sexa b a base a estudar, fagamos a súa descomposición en factores primos e chamemos p ao número de factores distintos. Na base b haberá, como moito, 2^p números automórficos para números dunha cifra e $2^p - 2$ para números de máis dunha cifra. Esta diferenza debese a que as solucións triviais (1 e 0) son números dunha cifra.

É sinxelo deducir que, se b e primo ou potencia de primo, unicamente haberá os 2 automórficos triviais, 0 e 1. Por outra banda, que $2^p - 2$ sexa o máximo para calquer número de máis dun díxito non implica necesariamente que teñamos esa cantidade de números sempre. Por exemplo en base 10 soamente haberá un automórfico con 4 díxitos sendo o número 9376.

Centrémonos por un momento na base decimal e vexamos como obter os distintos automórficos.

Obtención

Polo visto anteriormente, obviando os automórficos triviais, soamente haberá dous automórficos por cada número de díxitos. Ademais é inmediato ver que se un número é automórfico o resultante de eliminar díxitos pola esquerda debe selo tamén. Usando estes dous principios busquemos como podemos, a partir dun número automórfico, obter máis.

Obter automórficos co mesmo número de díxitos

En base decimal os números automórficos deben rematar nos números 5 ou 6 e, afortunadamente, existe unha forma moi simple para obter o automórfico rematado en 5 a partir do rematado en 6 e viceversa:

Este método baséase en que os dous números automórficos de n díxitos deben sumar $10^n + 1$. Por tanto, para obter o outro número automórfico de igual número de cifras soamente será necesario restar $10^n + 1$ ao número que xa tiñamos.

É interesante ver como isto explica unha situación anterior. Recordemos que antes vimos que ás veces pode haber soamente un número automórfico con x cifras utilizando de exemplo o 9376. Agora sabemos o motivo disto, o automórfico rematado en 5 correspondente debería ser o 0625 que é un número de 3 cifras provocando que 9376 sexa o único automórfico de 4 cifras.

Obter automórficos con máis díxitos

Existe un método para atopar o seguinte número automórfico rematado no mesmo número. Para os números rematados en 5 consistirá simplemente en calcular o seu cadrado e engadir ao número orixinal o díxito significativo (seguido dos ceros que teñamos polo medio) máis cercanos á cola.

Por exemplo a partir do número automórfico de 2 cifras 25 calculamos $25^2 = \mathbf{6}25$. Como o díxito significativo máis cercano ao 25 final é o 6 vemos que o seguinte automórfico é o 625. A partir de este calculamos $625^2 = 3\mathbf{90}625$ polo que engadiremos o 9 e os ceros que existen no medio e obtemos o número automorfico de 5 cifras 90625.

O método para os automórficos rematados en 6 será igual, pero en vez de engadir o díxito máis cercano á cola, engadimos o resultado de restarlle ese díxito a 10.

Vemos como a partir do número 76 calculamos $76^2 = 5\mathbf{7}76$ e $10 - 7 = 3$, polo que o seguinte será o 376.

Xeneralizacións

Existen distintas formas de xeneralizar este concepto. Neste caso mencionaremos dúas distintas:

Automórfico de potencia n

Esta xeneralización baséase en cambiar o expoñente da potencia que debe rematar no número inicial. Por exemplo, coñecemos como números automórficos de potencia 3, números esféricos ou números trimórficos aos x tales que x^3 remata en x. Exemplos de números trimórficos son o 4, o 5, o 6, o 9, o 24, o 25 ou o 49. É importante destacar que os números automórficos son números automórficos de potencia k para calquera k enteiro.

Números k-automórficos

Dicimos que un número x e k-automórfico se o resultado de multiplicar k polo cadrado de x remata en x. Por exemplo os números 2-automórficos serían os x tales que $2 \cdot x^2$ remata en x. Exemplos de números 2-automórficos son o 8, o 88, o 688 ou o 4688

Referencias

[1] Fairbairn, R.A., de Guerre, V., (1968) Automorphic numbers. *Journal of Recreational Mathematics*, 1(3), 173-179.

[2] Gardner, M. (1985) *The Magic Numbers of Dr. Matrix*. Prometheus Books

Que é unha esfera?

Pedro Vidal Villalba

Esta pregunta semella quizais demasiado sinxela, e definitivamente o é, pero son precisamente as preguntas máis simples as que nos fan reflexionar sobre o que cremos saber, e os exemplos máis ordinarios son normalmente os que máis axudan a desenvolver unha intuición sobre conceptos complexos.

Así, neste artigo quero intentar definir o que é unha esfera, unha das superficies máis sinxelas que un pode imaxinar, creándoa capa a capa, construíndoa a partir dos cimentos das matemáticas e engadindo pouco a pouco estruturas máis sofisticadas ata poder recrear a intuición que todos temos do que debería ser unha esfera.

Materiais de construción: Conxuntos

Como case todo na matemática moderna, calquera construción que tentemos facer estará irremediablemente baseada na teoría de conxuntos. Os conxuntos responden á idea intuitiva de coleccións de cousas —calquera cousa—. No caso da esfera, a primeira idea que teremos para definila será, entón, como conxunto. Así, a esfera será o conxunto dos puntos do espazo que se atopen á unha distancia dada dun centro; sen perda de xeneralidade, e para simplificar as cousas, digamos que a esfera considerada ten radio 1 e está centrada na orixe de coordenadas. Axudándonos do Teorema de Pitágoras para expresar a distancia, definimos entón

$$S^2 = \{(x,y,z) \in \mathbb{R}^3 | x^2 + y^2 + z^2 = 1\},$$

que será a nosa esfera buscada.

Fácil. Acabamos xa? Pois non de todo. É certo que, se inserimos este conxunto no espazo euclídeo tridimensional, $\mathbb{R}^3$, representa claramente a idea que temos todos do que é unha esfera. Porén, no proceso de facer isto, estamos realizando moitísimas suposicións que estamos pasando por alto se non temos coidado.

En primeiro lugar, por agora só temos falado da esfera como un conxunto de puntos. Pero un conxunto non é máis que iso: unha colección de puntos sen relación entre si, sen forma nin tamaño. O único que realmente permite distinguir conxuntos entre si é os elementos que contén cada un, e nin sequera iso basta, pois non podemos saber se os elementos de cada conxunto son realmente distintos entre eles ou simplemente estamos a chamarlles de xeito distinto aos mesmos obxectos. Así, dende un punto de vista puramente conxuntista, a única característica verdadeira dun conxunto é o número de elementos que contén, o que se chama o seu *cardinal*.

No caso da esfera, o seu cardinal é o do continuo —ten unha cantidade infinita e continua de puntos—; pero este é tamén o cardinal dun cubo, dunha recta e de todolos puntos do universo. O conxunto definido arriba como S^2 non é máis que polvo, un montón de puntos sen relación que podería tomar calquera forma ou ningunha en absoluto.

Para recuperar a esfera a partires destes puntos, necesitamos pegalos dalgún xeito. É aquí cando entra a topoloxía.

Pegando os puntos: Topoloxía

A topoloxía é unha área das matemáticas cuxo propósito esencial é formalizar a idea intuitiva de continuidade, de como podemos definir que os puntos están preto uns dos outros. No caso do espazo tridimensional, $\mathbb{R}^3$, esta noción formalízase por medio de bolas: unha bola aberta de centro p e radio r é o conxunto dos puntos que están a unha distancia menor que r do punto p. Con estas bolas pode construirse unha topoloxía en $\mathbb{R}^3$ —a topoloxía euclídea usual—, que transforma o polvo de puntos que tiñamos antes no espacio tridimensional que coñecemos; aquí, podemos dicir que dous puntos están *próximos* se un está contido nunha bola de radio pequeno centrada no outro.

Aproveitando que temos definido a nosa esfera $S^2 \subset \mathbb{R}^3$ dentro deste espazo tridimensional, podemos usar esta topoloxía definida en $\mathbb{R}^3$ para dotar á esfera da súa propia topoloxía, $\mathscr{T}$,—a *topoloxía relativa* a $\mathbb{R}^3$— na que diremos que os puntos da esfera están próximos se o están como puntos no espazo.

Parece que xa o temos, non? Pois aínda non. Ao dotar á esfera dunha topoloxía, conseguimos transformar o polvo de puntos que tiñamos ao principio nun espazo onde ten sentido falar da proximidade destes puntos entre si. Pero pouco máis; o espazo resultante ten xa unha certa estrutura, pero aínda carece dunha forma definida: se movemos os puntos de forma que os que estaban xuntos permanezan xuntos, isto é, de forma *continua*, a esfera $(S^2, \mathscr{T})$ como espazo topolóxico non ten forma de enterarse.

Os esforzos ata agora non foron en balde. Coa estrutura topolóxica da esfera podemos distinguila xa dun polvo de puntos inconexos, dunha recta, do total do espacio que a rodea ou dun donut. Porén, é indistinguible dunha esfera de maior ou menor radio, dunha elipse, dun cubo ou da superficie dunha bola de papel engurrada. De feito, o famoso Teorema (antes conxectura) de Poincaré-Perelmán garante que calquera superficie compacta (limitada e sen borde) e simplemente conexa (sen buratos) é *homeomorfa* á esfera, isto é, son indistinguibles a nivel topolóxico.

Necesitamos máis estrutura.

Quitando esquinas: Xeometría diferencial

Pregúntalle a calquera pola forma da Terra, e contestará que é unha esfera —posiblemente achatada polos polos—; pregúntalle a un terraplanista e dirá que é plana. Aínda que esteamos educados para descartar esta idea como absurda (e o é), si teñen algo de razón. E é que localmente unha esfera si asemella un plano.

Diremos que un espazo topolóxico $(M, \mathscr{T})$ é **localmente euclidiano** se, para todo punto $p \in M$, existe un entorno aberto $p \in U \in \mathscr{T}$ e un homeomorfismo $x : U \to x(U) \subset \mathbb{R}^n$, onde $x(U)$ é un aberto de $\mathbb{R}^n$, para algún $n \in \mathbb{N}$; isto é, todo punto ten un entorno que é localmente indistinguible dun espacio euclídeo. Baixo un par de condicións de regularidade adicionais que serven para eliminar contraexemplos patolóxicos —propiedade de separación de Hausdorff e, según os autores, paracompacidade e segundo numerabilidade—, estes espazos reciben o nome de **variedades topolóxicas** de dimensión n. No caso $n = 2$, adóitanse chamar simplemente

superficies; a esfera é claramente un exemplo de superficie.

Moitas veces resulta máis cómodo, en lugar de dar para cada punto un destes homeomorfismos, tentar agrupar moitos puntos e dar un homeomorfismo para todos eles á vez. Xorde entón o concepto de **carta** (no sentido de mapa), que non é máis que un par (U,x) onde $U \subset M$ aberto e $x : U \to x(U) \subset \mathbb{R}^n$ é un homeomorfismo. Unha colección destas cartas $\mathscr{A} = \{(U_\alpha, x_\alpha)\}_{\alpha\in A}$ tales que $\bigcup_{\alpha\in A} U_\alpha = M$, é dicir, pódese cubrir calquera punto da variedade con calquera carta, denomínase un **atlas**.

Está claro que un espazo topolóxico (co resto de condicións de regularidade) é unha variedade topolóxica se, e só se, admite un atlas. Nótese que, se dúas destas cartas, digamos $(U,x),(V,y)$, córtanse nalgún punto entón podemos considerar o *mapa de transición* $y\circ x^{-1} : x(U\cap V) \to y(U\cap V)$, onde $x(U\cap V), y(U\cap V) \subset \mathbb{R}^n$, e polo tanto está definido entre espazos euclidianos usuais. Por ser tanto x como y homeomorfismos, tamén o é $y\circ x^{-1}$.

O estudo destes mapas de transición permitiranos levar a análise e as súas ferramentes dende os espazos euclídeos ata as variedades para poder estudalas. Así, dise que un atlas $\mathscr{A}$ é diferenciable de clase r, ou $\mathscr{C}^r$, se dadas $(U,x),(V,y) \in \mathscr{A}$ cartas calesquera tales que $U\cap V \neq \emptyset$, o mapa de transición $y\circ x^{-1}$ é un difeomorfismo $\mathscr{C}^r$ no sentido usual. Se os mapas de transición son $\mathscr{C}^\infty$, isto é, arbitrariamente diferenciables, dirase tamén que o atlas é *suave*. Se $\mathscr{A}$ é un atlas $\mathscr{C}^r$ de M, a tripla $(M,\mathscr{T},\mathscr{A})$ dirase unha **variedade diferenciable** $\mathscr{C}^r$, ou variedade diferenciable suave, se $r=\infty$.

O feito de dotar á esfera dunha estrutura de variedade diferenciable elimina xa moitos dos espazos que soamente coa estrutura topolóxica non poderiamos distinguir dela, por exemplo, un cubo. Isto é así porque non é posible atopar cartas diferenciables que cubran as aristas do cubo, mentres que si o é para calquera punto da esfera. Existen varias formas equivalentes de dotar á esfera dun atlas; algunhas das máis comúns son as coordenadas xeográficas, nas que se identifica cada punto coa súa latitude e lonxitude, ou as coordenadas esteroegráficas, nas que se proxecta a esfera, agás un punto, no plano.

Con toda a estrutura que xa temos, $(S^2,\mathscr{T},\mathscr{A})$, aínda non somos quen de distinguir unha esfera dunha elipse ou da superficie dunha pataca. Antes de dotar á esfera de máis estrutura para solucionar o problema, quero facer unha pequena tanxente na narrativa para falar, precisamente, sobre tanxentes.

Recordemos que definimos inicialmente a esfera coma un subconxunto de $\mathbb{R}^3$, e usamos este feito para construír a topoloxía da esfera. Non así para a estrutura diferenciable, que podemos facer sen pensar a esfera coma metida no espazo. Isto tamén é certo para as anteriores contrucións: aínda que a máis sinxela é a presentada, existen numerosas alternativas para definir espazos topolóxicos homeomorfos a $(S^2,\mathscr{T})$ que non involucran metela no espazo tridimensional. Isto é de interese se estamos a traballar con superficies máis complicadas, como a banda de Möbius ou a botella de Klein. É importante desenvolver unha teoría de variedades que permita estudialas intrínsicamente, sen a necesidade de incluilas nun espazo máis grande. Para exemplificar esta necesidade, pensade que na teoría da relatividade xeral de Einstein, o espazotempo modélase coma unha variedade de 4 dimensións, pero non é $\mathbb{R}^4$, senón que está curvada para absorber o efecto da gravidade; que sentido tería necesitar meter a totalidade do universo nun espazo máis grande (que o propio universo) para estudalo?

De volta á esfera, agora que temos unha estrutura que soporta a análise, pensemos nunha curva $\gamma : \mathbb{R} \to S^2$, que asigna a cada tempo t un punto da esfera, $\gamma(t)$. Como poderiamos definir a velocidade desta curva? Fixándonos na análise clásica, parece razoable nun primeiro momento definila simplemente como a derivada da curva, isto é, para un tempo t_0, a velocidade será

$$\lim_{t\to t_0} \frac{\gamma(t)-\gamma(t_0)}{t-t_0}$$

Pero existe un problema importante: $\gamma(t)$ e $\gamma(t_0)$ son puntos da esfera, non vectores que se podan sumar ou restar. Pensade na Terra; que sentido ten calcular Santiago + París, ou $-2\cdot$Madrid?

Pensar na velocidade dun obxecto coma un vector, unha frecha ou tres numeritos xuntos é un truco útil nos espazos euclídeos, onde podemos xogar con liberdade cos números e facer que todo funcione. Porén, se intentamos modelar o mundo real, que lle importará a un paxaro que decidamos etiquetar a velocidade coa que voa con tres números? Entón, que é o que ve o paxaro?

Pois ben, o paxaro non pode medir con que velocidade está a voar, pero si pode notar outras cousas, como a presión, a humidade ou a temperatura. Poñamos que $f : S^2 \to \mathbb{R}$ é unha aplicación definida na esfera que mide unha destas cantidades. Entón, o paxaro sabe que cando voa estas cantidades cambian, e que se voa máis rápido, variarán máis rápidamente. A traxectoria do paxaro durante o seu voo virá dada por unha curva, $\gamma : \mathbb{R} \to S^2$; o paxaro pode medir en cada momento, entón, a magnitude f ao longo do seu voo, é dicir, medirá $f(\gamma(t))$. Agora ben, a composición $f\circ\gamma$ é unha función real de variable real e, coma tal, podemos medir o seu cambio no instante t cunha derivada ordinaria, $(f\circ\gamma)'(t)$. Sen dúbida a velocidade do paxaro debe estar relacionada con esta derivada; pero tamén é claro que non pode depender da cantidade f que lle apeteza medir ao paxaro nun momento dado.

Xuntando ambas cousas, chegamos a que a velocidade da curva γ no punto $\gamma(t)$, que denotaremos $v_{\gamma,\gamma(t)}$, pode aplicarse a unha función $f : S^2 \to \mathbb{R}$ para obter a tasa de cambio desa función a través da curva no instante t, isto é,

$$v_{\gamma,\gamma(t)} f = (f\circ\gamma)'(t)$$

Aquí un dos cambios de perspectiva máis relevantes da xeometría diferencial: as velocidades non son frechas, son derivadas. Non obstante, isto non significa que deixen de ser vectores: podemos escalar a velocidade se escalamos o parámetro do tempo co que recorremos a curva, e podemos sumar as velocidades de distintas curvas que pasan polo mesmo punto (aínda que isto vólvese menos trivial). O espazo vectorial formado polas velocidades de todas as curvas que pasan por un punto p nunha variedade diferenciable M denomínase **espazo tanxente** a M en p, e denótase por T_pM. O estudo dos espazos tanxentes e conceptos relacionados constitúe a base da xeometría diferencial, pois é o que permite aproveitar as ferramentas existentes na análise de espacios euclidianos para o estudo de variedades.

TOMANDO FORMA: ESTRUTURA MÉTRICA

É importante notar que na sección anterior acabamos de definir a velocidade dunha curva sen ter que falar de distancias. Este é tamén un cambio interesante de perspectiva: a velocidade é un concepto máis elemental que a distancia, no sentido de que é necesaria unha menor estrutura para definila.

Así, o paxaro que está a voar pola superficie da Terra, coa estrutura que temos ata o de agora, non podería distinguir se vive nun planeta esférico, elipsoidal ou con forma de pataca, pero a súa velocidade está ben definida en todolos casos.

Tamén da análise e xeometría clásicas sabemos que para medir distancias resulta útil poder medir vectores; neste caso, os vectores a medir serán precisamente os dos espazos tanxentes en cada punto, isto é, as velocidades de curvas. Para realizar estas medidas, a ferramenta axeitada é un *produto escalar*, que aplicado a un par de vectores devolve información acerca das súas lonxitudes e ángulo entre eles.

Sobre a nosa esfera pensada como variedade diferenciable, $(S^2, \mathscr{T}, \mathscr{A})$, impoñemos unha nova estrutura, g, de forma que en cada punto $p \in S^2$, $g_p : T_pS^2 \times T_pS^2 \to \mathbb{R}$ é un produto escalar. Formalmente, g é un $(0,2)$-campo tensorial, pero definir isto con detalle levaría unhas cuantas páxinas máis. O importante é que g, chamado *tensor métrico* ou, ás veces, *primeira forma fundamental*, permite medir as velocidades e, integrando estas, podemos medir distancias.

Unha variedade diferenciable $(M, \mathscr{T}, \mathscr{A}, g)$, onde g é un tensor métrico, denomínase unha **variedade de Riemann**, e son obxectos tamén ampliamente estudiados.

Así, finalmente, podemos dotar a $(S^2, \mathscr{T}, \mathscr{A})$ dunha estrutura métrica concreta que defina, en última instancia, distancias entre puntos e confira á nosa superficie da súa característica redondez, permitindo distinguila dun elipsoide e doutras esferas de distinto tamaño. Para obter esta métrica concreta, o máis sinxelo é recuperala da inmersión inicial que fixemos da esfera en $\mathbb{R}^3$ a partir do produto escalar usual deste espazo. Outra forma é impor unha serie de restriccións de simetrías que debe satisfacer esta métrica, e que entendemos que debe cumprir a esfera, como as simetrías por rotacións; formalizar isto, non obstante, é bastante máis complicado, e require do uso de ferramentas como os grupos e as álxebras de Lie.

Con todo, esta viaxe para entender algo tan simple como é unha esfera tenos levado ao estudo da topoloxía, a xeometría diferencial e mesmo a álxebra, campos enormes e sumamente ricos que se entremezclan e apoian para responder, en diversos grados de detalle, unha pregunta tan inocente como "Que é unha esfera?".

REFERENCIAS

[1] SCHULLER, FREDERIC P. (2015). *Lectures on the Geometric Anatomy of Theoretical Physics*. `https://www.youtube.com/@FredericSchuller/playlists`

Euler foi un xenio das Matemáticas, pero aínda así, non tivo a sorte de ler Máis Mates antes de quedarse irremediablemente cego. Gauss posiblemente se aburría moito entre clases, algo que podería ter remediado se se lle ocorrese inventar Máis Mates. Hipatia tampouco a tivo nas súas mans, pero seguro que gozaría das cónicas da portada. Se cadra Galois podería ter achado a fórmula de Máis Mates, pero morreu demasiado novo... E ti? Ti tes Máis Mates ao alcance da man!

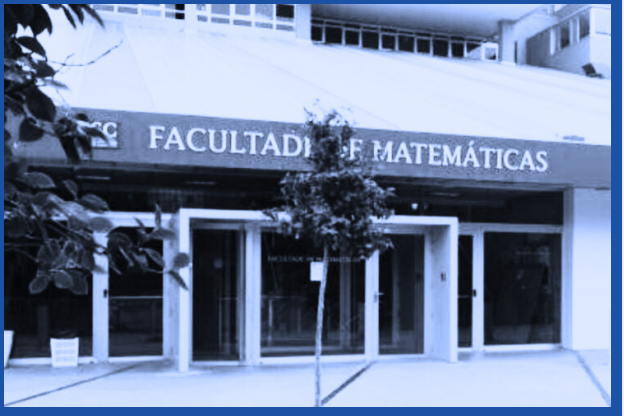
Máis Mates é un proxecto en forma de revista do alumnado para o alumnado, o proxecto co que todos eses egrexios persoeiros soñarían. Cada mes, traémosvos novos artigos con pequenas anécdotas da historia das matemáticas, as últimas novas, entrevistas, pasatempos, pequenos petiscos en diversos temas que ao mellor non se tratan en profundidade na carreira... En definitiva, todo o que esperta a nosa curiosidade como alumnas e alumnos, e que quizais esperte tamén a túa!

Estamos aí para que desconectes na metade dunha dura sesión de estudo, ou para todo o que se che ocorra. Lenos, coméntanos, compártenos, escríbenos e colabora con nós!

USC UNIVERSIDADE DE SANTIAGO DE COMPOSTELA
FACULTADE DE MATEMÁTICAS

Accede á revista!

revistamaismates@gmail.com



MÁIS MATES

USC UNIVERSIDADE DE SANTIAGO DE COMPOSTELA
FACULTADE DE MATEMÁTICAS