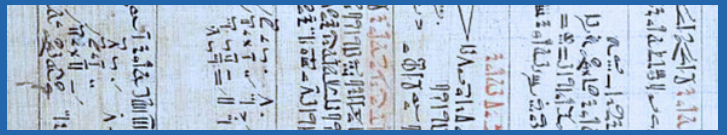
USC UNIVERSIDADE DE SANTIAGO DE COMPOSTELA
FACULTADE DE MATEMÁTICAS
N° 8 DECEMBRO 2024
REVISTA ESTUDANTIL

MATES ÁIS



Introdución

Dirección da Revista

ÍNDICE

Fig. 1: Varias imaxes dos colaboradores

Moi bo día lectora ou lector! Estamos encantados de que nos leades e disfrutedes connosco deste proxecto.

Neste novo número da Revista Maís Mates, rodeamos temas tan curiosos e interesantes como as mates dos casinos, o descubrimento dun novo primo e unha ferramenta empregada en criptografía: o Algoritmo de Schoof. Tamén contamos cun artigo moi especial, máis histórico, que ten as matemáticas como marco de traballo: os discos de ouro das Voyager. Sen duda, soan moi interesantes! Na sección de Retos, os nosos compañeiros de Sementeira séguennos traendo unha chea de problemas para as nosas vidas, agardamos que vos enrevesedes neles.

Xa nos situamos no derradeiro número deste ano 2024, e desexámosvos a todas as persoas que nos ledes un moi feliz e próspero ano 2025 e bo nadal!

Gustarianos contar que o pasado 3 de decembro tivo lugar o "Faladoiro Máis Mates" unha xornada de encontro entre colaboradores da Revista e a comunidade universitaria para facer "unha revista en directo". Foi unha xornada moi amena e divertida, ademais contamos coa axuda do Servizo de Normalización Lingüística da USC e da Facultade de Matemáticas para a actividade. Estamos moi agradecidos pola vosa axuda!

Deixámosvos unha pincelada do que fixemos.

O disco de ouro das Voyager, ou como explicarlle a E.T. o funcionamento dun vinilo

Santiago González Gómez

Nu nha galaxia afastada, dentro de millóns de anos, unha raza intelixente capaz de viaxes interestelares intercepta unha sonda espacial de tecnoloxía moi primitiva proveniente dun sistema planetario coñecido polos seus nativos como "Sistema Solar". De volta na súa base, extraen do artefacto un disco de 30 cm de diámetro fabricado en cobre e chapado en níquel e ouro. Tras retirar a súa cobertura e examinalo coidadosamente, un destes seres suspira, xírase cara ao seu compañeiro e dille:
−Pepe, faime o favor e achégame o tocadiscos.

MÁNDOCHE UN AGASALLO...

Fig. 1: *Sons da Terra*, o disco dourado das Voyager. Imaxe de [2].

Obviamente “Pepe” non sabe o que é un tocadiscos, e isto evidencia un gran problema no establecemento do primeiro contacto cunha forma de vida alieníxena: como nos comunicariamos? En 1977, un comité presidido polo afamado divulgador Carl Sagan enfrontouse a esa mesma pregunta. Nese ano, a NASA lanzou ao espazo as sondas Voyager 1 e 2. O seu obxectivo era sobrevoar e recabar datos sobre os confíns do Sistema Solar e o que se atopa máis aló. Actualmente, malia atopárense a máis de 20 mil millóns de quilómetros da Terra, seguimos en contacto coas Voyager, e espérase que isto siga sendo así ata o 2030. A partir de entón, as sondas proseguirán a súa viaxe cara ás profundidades do espazo soas.

Para o lanzamento das Voyager, decidiuse recompilar información fundamental sobre a Terra e a Humanidade e incluíla dalgún xeito nas sondas para que, se nun futuro distante (as Voyager non se achegarán ata outra estrela en 40000 anos) unha raza extraterrestre se atopa con elas, poida aprender un chisco sobre nós. O medio escollido foi un disco fonográfico (figura (1)), o que coñecemos como “vinilo” polo seu material de fabricación habitual, pois era a mellor tecnoloxía dispoñible no momento. Nel, o comité de Sagan incluiu saúdos en múltiples idiomas, ondas cerebrais, sons da natureza como cantos de baleas, e música, especialmente clásica e folclórica (unha das poucas bandas modernas consideradas para o disco foron os Beatles, pero descartáronse finalmente... por problemas de copyright!). Tamén se codificaron por vez primeira nun disco deste tipo 116 fotografías con contido anatómico, astronómico, biolóxico, xeográfico e cultural.

Para os lectores máis mozos, un vinilo funciona do seguinte xeito: a superficie do disco está recuberta dun longo surco en espiral no que se realizan lixeiras protuberancias nas que está codificado o son (de xeito similar a un espectrograma). Os tocadiscos nos que se reproducen posúen un brazo mecánico cunha agulla na punta que se fai caer sobre o disco. Este comeza a xirar a unha velocidade predeterminada (á que se reproducirá o son). A agulla percorre entón o surco e vai subindo e baixando ao toparse coas protuberancias, transmitindo o que estea gravado no disco para a súa reprodución.

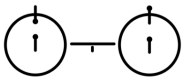
As dúas Voyager están equipadas con cadansúa copia do disco xunto cunha agulla para poder reproducilos. Pero, como saberá unha intelixencia extraterrestre como extraer do disco toda a valiosa información nel almacenada? Isto é o que tenta explicar a cuberta dos discos (figura (2)), na que, ademais dun mapa coa localización da Terra (na parte inferior esquerda), se atopan as instrucións necesarias para os posibles receptores.

Fig. 2: Cobertura do disco. Imaxe de [2].

...E EXPLÍCOCHE COMO USALO!

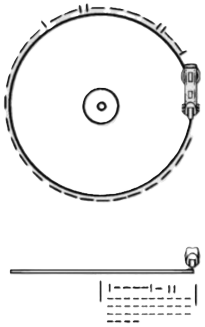
Na película *Contact* (en cuxa produción traballou Sagan), uns científicos reciben un sinal de radio de orixe extraterrestre. A forma na que estes alieníxenas deixan claro que son unha forma de vida intelixente é mandando repetidamente pulsos en grupos de 2, 3, 5, 7, 11... os números primos! Por-

que, se hai algo universal, son as matemáticas. Por iso, se queremos explicarlle a un extraterrestre como escoitar un disco, debemos de facelo partindo de ideas matemáticas; tamén de propiedades físicas, pero estas deben de ser o máis fundamentais posibles. Por suposto, non podemos usar ningún idioma terrestre, pero tampouco ningunha unidade de medida (sen definila antes), e segundo expertos (como [3]), tamén é conveniente absternos de conceptos como o cálculo integral, por moi básicos que sexan para as nosas Matemáticas, porque estes poden ser totalmente distintos ou non desenvolverse noutras sociedades. Con estas ideas en mente, as instrucións da cuberta comezan coa seguinte imaxe:

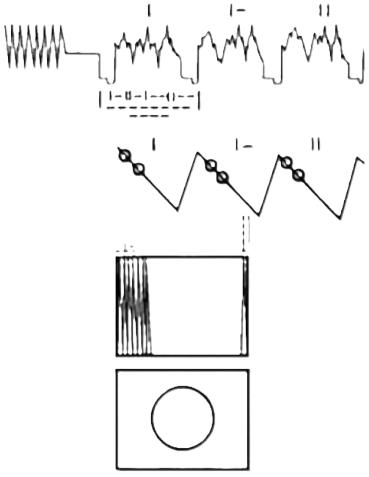


Este diagrama representa por duplicado o átomo máis común do universo: o hidróxeno, cun protón no núcleo e un electrón en órbita. A diferenza entre ambas representacións é o símbolo do electrón, que está xirado. Resulta que, de forma extremadamente ocasional (pero espontánea), o electrón dun átomo de hidróxeno pode variar unha propiedade coñecida como espín (representada pola orientación do símbolo do electrón), nunha transformación coñecida como transición hiperfina. Suponse que este fenómeno será coñecido e interpretado no diagrama por unha raza intelixente. Cando ocorre a transición hiperfina, emítese unha onda moi característica de 21 cm de lonxitude de onda e 0,7 ns de período. Durante o resto do disco, empréganse estos valores como unidades de lonxitude e tempo.

Unha vez definidas as unidades, o máis complicado de todo, o resto da explicación non difire moito de como lle explicariamos a un humano calquera o funcionamento do disco.



Nesta figura, podemos ver unha vista cenital e outra lateral do disco coa agulla, de forma que se entende como se debe de situar esta para extraer a información do disco. Na imaxe cenital, aparece un número en binario percorrendo o perímetro do disco (| representa os 1, e − os 0; non é necesario explicar cal é cal porque só hai dúas posibilidades); se o multiplicamos por 0,7 ns, obtemos o tempo que debería de tardar o disco en dar unha volta. Polo tanto, o que se vén indicando son as revolucións por segundo ás que se debe de facer xirar o disco para escoitalo correctamente. Na vista lateral, o código en binario multiplicado por 0,7 ns dá a duración total dunha cara do disco, co que se pode comprobar se as revolucións por segundo obtidas son as correctas.



A extracción das imaxes é máis complexa. A priori, pódese *escoitar* todo o disco; simplemente, por un lado teremos música e sons recoñecibles, e polo outro, ruído. Porén, como sabería un alieníxena que isto último é ruído e que debería ser decodificado, e non máis "sons humanos"? Na última imaxe móstrase un exemplo da forma que teñen as ondas sonoras que deberían de ser transformadas en imaxes. Estas deben de ser partidas en segmentos duns 8 ms, como se expresa en binario. Cada segmento pode ser transformado nunha serie de números segundo valores de volume, e estes números, en píxeles (branco a volume mínimo, negro a volume máximo). Se colocamos estes píxeles en bandas verticais na orde mostrada no penúltimo rectángulo, obtemos que 512 destes segmentos forman unha imaxe completa. Se todo se realiza de forma correcta, a primeira imaxe que debe de aparecer é a circunferencia mostrada ao final do diagrama, a forma de indicar que todo o proceso de decodificación se fixo correctamente. De forma análoga obtéñense as 115 imaxes restantes.

Todo isto pódenos parecer moi complexo e indescifrable, pero non é difícil imaxinarse a toda unha civilización intelixente sendo quen de resolver o puzzle e extraer do disco toda esta información sobre a Humanidade, o cal non deixa de ser un fito marabilloso se pensamos en tódalas barreiras de comunicación que deben de ser superadas. Todo grazas á ciencia, á Física e ás Matemáticas.

E se acaso os receptores do agasallo das Voyager non teñen órganos da vista ou do oído... Bueno, malo será, non si?

Referencias

[1] Britannica. *Voyager* (consultado 13/06/2024), enlace: britannica.com/technology/Voyager-space-probes

[2] Jet Propulsion Laboratory, NASA. *Voyager. The Golden Record* (consultado 13/06/2024), enlace: voyager.jpl.nasa.gov/golden-record/.

[3] DeVito, C.L. (2022). *Science, SETI & Mathematics*. Berghahn Books.

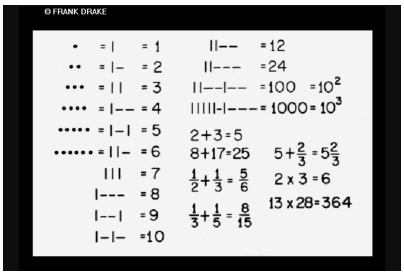
[4] Verge Science. *We decoded NASA's messages to aliens by hand* (consultado 19/06/2024), enlace: youtube.com/watch?v=RRuovINxpPc&t=250s.

UN CATÁLOGO DA TERRA

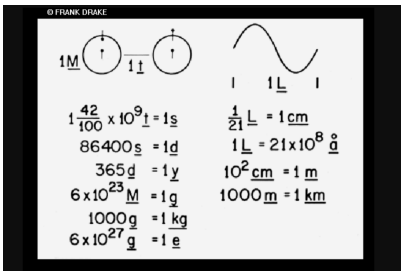
E non queremos despedirnos sen compartir unha pequena mostra das imaxes da Terra contidas nos discos das Voyager. Tódalas imaxes proceden de [2].

O comité decidiu non incluír imaxes da guerra, a pobreza ou a fame, centrándose en imaxes con información anatómica, xeográfica e cultural, de connotación neutra ou positiva. Foi polémica tamén a decisión de non incluír espidos, só diagramas, por puro prexuízo e sen atender á utilidade científica.

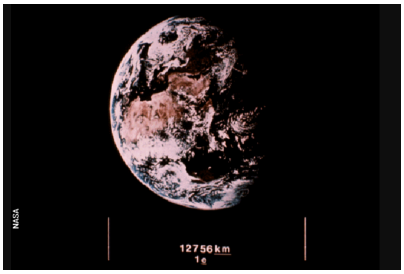
E ti, que imaxes enviarías ao espazo?



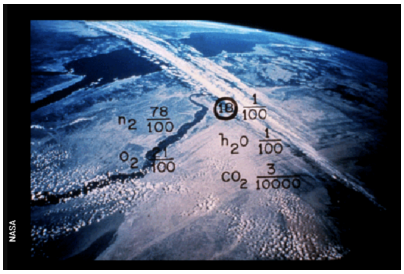
(a) Imaxe 3. Definicións matemáticas.



(b) Imaxe 4. Definición das unidades de medida.



(c) Imaxe 12. A Terra.



(d) Imaxe 13. Vista satelital coa composición química da atmosfera.

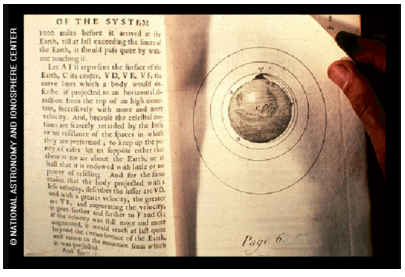
(e) Imaxe 74. Nenos con globo terráqueo.

(f) Imaxe 77. Supermercado.

(g) Imaxe 82. Demostración de lamber, comer e beber.

(h) Imaxe 84. Construción dunha casa africana.

(i) Imaxe 99. Radiografía dunha man.



(j) Imaxe 111. Páxina do *Principia mathematica* de Newton.

O paradoxo do ludópata: matemáticas no casino

Ignacio Garbayo Fernández

Un bo día de primeiro de mates, o profesor de Elementos de Probabilidade e Estatística contounos que era imposible gañar nun longo prazo no casino, ou polo menos facelo de forma «consistente». Imos demostrar iso cunha pequena aproximación ao problema.

Supoñamos que algún dos casinos do ensanche compostelán lanza unha oferta especial de Nadal na ruleta:

> Só está noite: o 0 é VERMELLO!!!
>
> Máis probabilidade de gañar co vermello. Vén probalo!!!

Para quen non estea familiarizado co xogo da ruleta europea, cómpre mencionar que esta conta con 36 números comezado polo 1, dos cales a metade son vermellos e a outra metade son negros. Ademais, conta co 0, que se adoita pintar en verde e non soe computar como número de ningunha cor (agás nesta oferta especial). Vemos unha distribución dos números na Figura 1. Se un xogador aposta unha cor e gaña, o casino paga a cantidade apostada, é dicir, «dóbrase» o invertido.

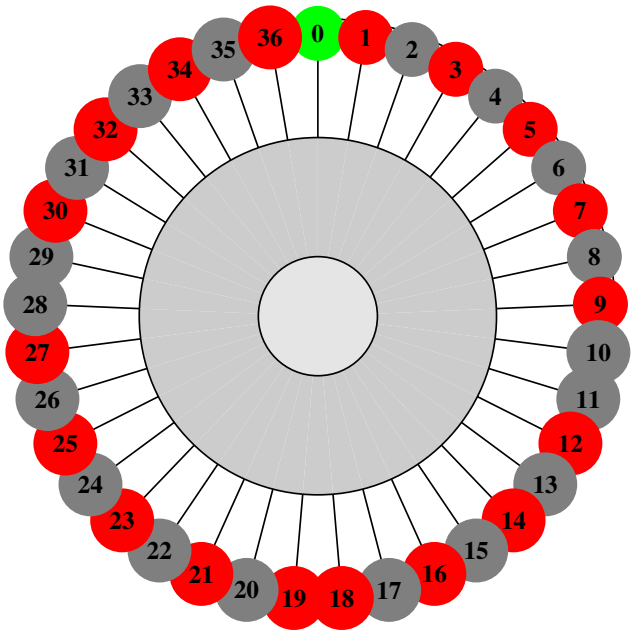


Fig. 1: Ruleta europea.

Fagamos outra suposición: Pepiño, experimentado matemático con moitos aforros, decide probar sorte co seu capital, nada máis que 1 millón de euros. Mais, antes de poñer as botas e cargar co paraugas para evitar ser arrastrado pola choiva da capital, decide facer un par de contas para decidir que estratexia vai empregar.

Estudará cal é a fracción do seu capital que debe arriscar en caso de ter a oportunidade de apostar cunha probabilidade favorable (caso no que estamos, pois o 0 é vermello).

Estratexia 1: dobrar a aposta

Para facer os cálculos, introducimos a notación:

$$A_0 \equiv \text{aforros iniciais} = 1 \text{ millón de euros.}$$

Trala primeira aposta, os aforros esperados, que seguen a fórmula

$$\begin{aligned}&(\text{Prob. éxito}) \times (\text{Aforros finais en caso de éxito})\\ &+(\text{Prob. fracaso}) \times (\text{Aforros finais en caso de fracaso}),\end{aligned}$$

virán dados por:

$$\frac{19}{37}(2A_0) + \frac{18}{37}(0A_0) = \frac{38}{37}A_0 = 1.02 \text{ millóns.}$$

Trala segunda aposta, é sinxelo ver que os aforros esperados serían de $(38/37)^2 A_0$ e, así, trala n-ésima aposta, de $(38/37)^n A_0$ millóns de euros.

Neste punto, Pepiño pensou que, se se daba présa, nunha noite daríalle tempo a apostar unhas 300 veces, resultando en aforros esperados de $2.982,4$ millóns de euros!!!

Estratexia 2: apostar sempre a metade

A primeira estratexia soaba demasiado convincente, polo que Pepiño decidiu seguir facendo conxecturas sobre outros métodos.

Se, en lugar de apostar sempre todo o dispoñible, dobrando o apostado na ronda anterior, Pepiño apostase sempre a metade dos aforros actuais, A_0, trala primeira aposta, o capital esperado sería de

$$\frac{19}{37}\left(\frac{3}{2}A_0\right) + \frac{18}{37}\left(\frac{1}{2}A_0\right) = \frac{75}{74}A_0,$$

logo trala n-ésima aposta, o capital esperado é claro que é de $(75/74)^n A_0$. Isto equivale, despois de 300 tiradas, a «tan só» 56 millóns de euros, en comparación coa estratexia anterior.

Estratexia 3: xeneralización a unha fracción dos aforros

No canto de fixar a fracción de A_0 a apostar de antemán, Pepiño dispúxose a analizar cal sería a α a considerar que

maximizaría as gañancias, no caso de apostar αA_0. É fácil ver, seguindo os razoamentos anteriores, que

$$E[A_n](\alpha) = (1+\alpha(2p-1))^n A_0,$$

onde a probabilidade de éxito é $p = 19/37$.

Analizando esta función real de variable real α, vemos que se $p > 1/2$, é dicir, a probabilidade de gañar é favorable de cara ao xogador, $E[A_n]$ alcanza un máximo cando $\alpha = 1$, polo que a primeira estratexia considerada implicaría aforros «máximos».

A intuición di entón que a estratexia a seguir debería ser maximizar as gañancias, mais isto non é exactamente así. Feitas estas contas, podemos facer unha chea de reflexións. En primeiro lugar, como vai ter un matemático 1 millón de euros? (estamos a tolear?) A mellor estratexia? Non xogar? Por outra parte, non existe o diñeiro infinito! Non ten por que saír o vermello en toda a noite.

A estratexia de «dobrar todo» é coñecida como estratexia da *martingala*. Consiste en volver apostar polo total do perdido no momento de incurrir nunha perda nun xogo de azar. Na nova aposta, o xogador ten a posibilidade de recobrar todas as súas perdas, polo que podería parecer que, ao longo prazo, a esperanza de gañancia con esta estratexia mantense constante a favor do xogador.

Estatísticamente, é así. O capital medio do xogador (os cartos que Pepiño ten á súa disposición) mantense constante. O problema reside en que, ao incurrir en sucesivas perdas, o xogador que segue esta estratexia vese obrigado a apostar de novo cantidades cada vez maiores (as perdas acumuladas), que tenden a crecer exponencialmente. Ao cabo duns poucos ciclos de apostas, o xogador, cuxos recursos son normalmente moi inferiores aos da banca, vese arruinado e incapaz de apostar unha vez máis polo total das súas perdas. Evitar xogadores que tenten seguir a estratexia da *martingala* é unha das razóns polas que os casinos actuais establecen límites máximos de aposta.

En efecto, na etapa n-ésima dunha *martingala*, teríamos que

$$2^0 + 2^1 + \cdots + 2^{n-1} < 2^n,$$

polo que

$$\frac{1}{2^n} + \frac{1}{2^{n-1}} + \cdots + \frac{1}{2} < 2,$$

sendo $\sum_{n=0}^{\infty} 1/2^n = 2$, logo a estratexia na teoría funcionaría, mais xa vimos que non na práctica.

O CRITERIO DE KELLY

En 1956, un investigador dos Laboratorios Bell propuxo un método que maximiza a «utilidade esperada» no canto das gañancias esperadas. Isto faino a través do cálculo da fracción α de A_0 a apostar, obtendo o valor que mellor rendemento sacaría aos aforros. A fórmula a considerar no caso das apostas é a seguinte:

$$\alpha = p - \frac{1-p}{b},$$

onde $p = 19/37$ no noso caso e b, que é a porcentaxe da aposta que se gaña en caso de éxito, vale 1, pois se «dobra» o invertido.

Para o problema considerado, temos logo que $\alpha = 1/37$, resultando nunha cantidade moi pequena en comparación con todas as análises anteriores. Esta é a aposta «máis segura» estudiada e, polo tanto, vemos que os xogos de casino, en particular o da ruleta, non son tan beneficiosos como adoitamos pensar. Pepiño, canso de facer contas e coa tristura de saber que non ía gañar tanto coma esperaba, decidiu sabiamente gardar o seu millón de euros para outra fin e marchar a durmir, que xa era tarde e, ademais, arroiaba en Compostela.

REFERENCIAS

[1] *La paradoja del ludópata. Discusión en liña. https://foro.rinconmatematico.com/index.php?topic=92903.0.*

[2] *O criterio de Kelly. https://en.wikipedia.org/wiki/Kelly_criterion.*

[3] *Martingala. https://es.wikipedia.org/wiki/Martingala.*

Unha grande e enorme nova prima

Francisco Estévez Lengua

Recentemente , pasando polas publicacións de Instagram, aparéceme unha imaxe cun número que non me daba nin imaxinado. Picoume tanto a curiosidade que aquí vos traio as miñas pesquisas respecto a este número.

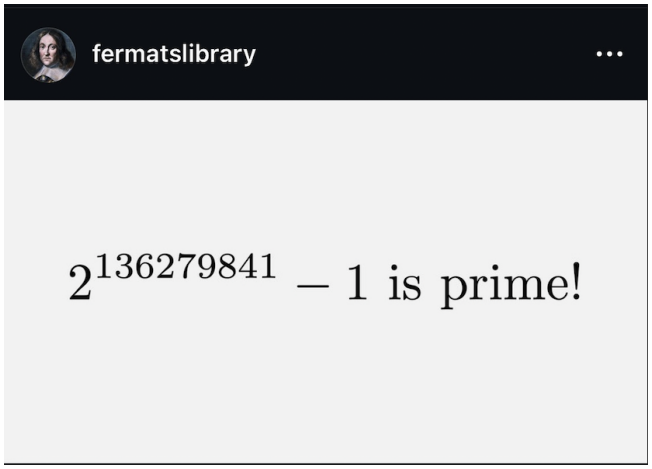


Fig. 1: Imaxe de Instagram da conta @fermatslibrary

Ademais, o usuario comenta o seguinte: "$2^{136279841} - 1$, descuberto hoxe, é o número primo máis longo que se coñece. É un primo de Mersenne, os cales son máis doados de atopar. Ao software GIMPS levoulle ao redor de 6 anos dende que se atopara o previo primo máis longo. Ademais, foi o primeiro primo de Mersenne atopado empregando GPUs."

Que é un número primo de Mersenne?

Un **número de Mersenne** é un número da forma $2^n - 1$ con n un número enteiro positivo.

Os números primos de Mersenne serán aqueles números de Mersenne que son primos. Ademais pódese ver facendo algúns intentos que para $2^n - 1$ sexa primo é preciso que n sexa primo, o que se proba en xeral empregando o **Pequeno Teorema de Fermat** traballando con congruencias. Isto é necesario, pero non suficiente. Por exemplo, para $p = 2$ $2^2 - 1 = 3$ é primo, para $p = 4$, $2^4 - 1 = 15$ non é primo e non é suficiente pois para $p = 11$, $2^{11} - 1 = 2047 = 23 \cdot 89$.

Estes números foron nomeados así por **Marin Mersenne**, un sacerdote e filósofo francés do século XVII.

Que é o software GIMPS?

No comentario da publicación de @fermatslibrary podemos ler que escribe GIMPS, pois resulta que esta sigla significa "**Great Internet Mersenne Prime Search**". É un proxecto colaborativo que conecta a todos os usuarios que queiran buscar este tipo de primos. O seu fundador, **George Woltman**, desenvolveu un software inicial de búsqueda de primos de Mersenne, e dende un primeiro momento probouse a eficacia deste software. Ao principio, o sistema era bastante incómodo pois tiñan que enviar a información por correo electrónico e non estaban tantas cousas optimizadas e automatizadas como hoxe en día.

Este proxecto baséase na computación distribuída e os usuarios poden ter varios tipos de dedicación (hai varias tarefas onde os usuarios elixen o que queren facer segundo as características dos seus dispositivos de traballo). Na propia páxina veñen explicados os métodos aplicados para as comprobacións de se un número é primo, pois os programas están fundamentados en diferentes métodos de factorización. Ademais, teñen un histórico dos números probados e verificados.

Dende 2017, o colaborador de GIMPS **Mihai Preda** desenvolveu a versión de GIMPS para GPUs, e este novo número primo de Mersenne é o primeiro descuberto empregando GPUs, que para este tipo de aplicacións son moito máis eficientes e poderosas que os CPUs.

Como se descubriu o último atopado?

O personaxe estrela deste artigo é **Luke Durant**, un extraballador da empresa **NVIDIA**, foi a persona que atopou este número o 11 de outubro. Pero aínda sería preciso que pasara varios test para confirmar que non era un erro, e así foi que se validou por varios test (o test de Lucas-Lehmer, e por varios softwares diferentes). A verificación finaliza o 19 de outubro e anunciaríase que se coñece o 52 número primo de Mersenne.

Este número conta con 41 024 320 díxitos en base decimal (con máis de 16 millóns de díxitos máis que o primo de Mersenne atopado antes).

Para atopalo, Luke Durant organizou unha rede de miles de GPUs distribuídas entre 17 países a través da nube.

Como curiosidade, GIMPS leva empregándose durante 28 anos, usando ordenadores de uso persoal, descubrindo os últimos 18 primos de Mersenne. Un gran número de voluntarios descargan este programa gratuito, pois ademais teñen un premio de 3000 dólares se chegan a atopar un.

Referencias

[1] GIMPS Discovers (21 de outubro de 2024). Mersenne Prime Number discovery $2^{136279841} - 1$ is Prime!. (*Nota de prensa*)
`www.mersenne.org/primes/?press=M136279841`

[2] Great Internet Mersenne Prime Search, *Páxina oficial de GIMPS* `www.mersenne.org`.

Retos Matemáticos

Sementeira
Clube Olímpico de Mates-USC

Xogos de Periódico

Resolve o seguinte Sudoku:

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

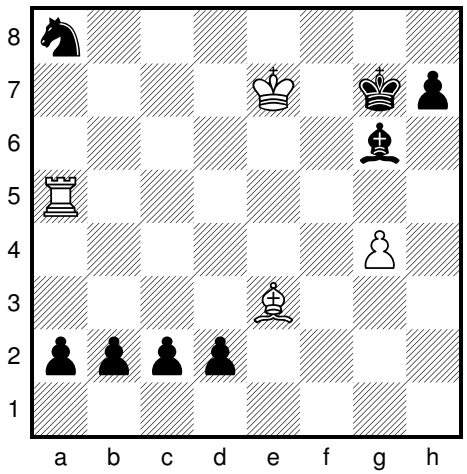
Solución do Sudoku:

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

Solución do xadrez:

1 ♗h6+ ♔×h6
2 ♔f6 a1=♕
3 ♖h5+ ♔×h5
4 g5#

Moven para gañar as brancas...



Descubrimos a cita do número anterior:

"Toda ciencia que prosperou fíxoo sobre os seus propios símbolos: a lóxica, da que se admitiu que e a única ciencia que non fixo ningunha mellora século tras século, e a única que creceu sen símbolos."
— Augustus De Morgan (1864)

Eres quen de recuperar a cita cifrada?

"AAB BA / BB AB B A BB AB B AA BABA BBB / BA BBB BA / A / BAA AA BBA BA BBB / BAA A AAA A / BA BBB BB A / AAA A / BA BBB BA / A / AAB BA / ABBA BBB AAB BABA BBB / ABBA BBB A B AB".
— Karl Weierstrass (1883)

Problemas Propostos

1. Sexan $x, y, w, z \in \mathbb{Z}$ tal que:
$$\frac{1}{x}+\frac{1}{y}+\frac{1}{w}+\frac{1}{z}=1,$$
ver que, polo menos, un dos enteiros é par.

2. Sexa $f\colon x \in \mathbb{R} \longrightarrow f(x) \in \mathbb{R}$ continua tal que para calquera $x, y \in \mathbb{R}$ tense que:
$$f(\sqrt{x^2+y^2}) = f(x)f(y).$$
Proba entón que:
$$f(x) = f(1)^{x^2}, x \in \mathbb{R}.$$

3. Dado un triángulo ΔABC, consideremos o punto medio M de AB e un punto calquera D do interior de AC non sendo o punto medio. Sea E o punto de corte da extensión de BD coa recta paralela a AB que pasa por C. Demostra que AE, BC e MD son concurrentes.

4. Sexa f un polinomio con coeficientes enteiros. Definamos a sucesión $\{a_n\}_{n\in\mathbb{N}}$ como $a_0 = 0$ e $a_{n+1} = f(a_n), \forall n \in \mathbb{N}$. Proba que se existe $m \in \mathbb{Z}^+$ tal que $a_m = 0$, entón $a_1 = 0$ ou $a_2 = 0$.

Solucións do nº anterior:

O Algoritmo de Schoof

Alejandro Pousa e Ibai Otero

Co ascenso da tecnoloxía, a necesidade de avances en ciberseguridade logrou que a criptografía tomara un papel fundamental nas matemáticas modernas. Neste artigo imos tratar a ECC (*Elliptic Curve Cryptography*), unha variante de clave pública baseada nas curvas elípticas. A ECC compite con outros métodos máis populares de encriptación, a saber, o RSA (factorización enteira) ou o DSA (firma dixital). A gran vantaxe da ECC respecto a estes últimos é que require de números máis pequenos para ofrecer a mesma seguridade que os anteriormente mencionados.

O algoritmo de Schoof é un dos resultados máis importantes na investigación da ECC. A súa finalidade é contar, de maneira eficiente, os puntos dunha curva elíptica definida sobre un corpo finito de característica q $\mathbb{F}_q$. Unha curva elíptica sobre un corpo finito k é un tipo de curva alxébrica sobre k cun punto particular $\mathcal{O}$. Un resultado fundamental é que sobre o conxunto de puntos racionais desta (é dicir, os da curva no corpo) pódese definir unha estrutura de grupo conmutativo. A continuación, daremos algúns preliminares para afondar na explicación do algoritmo.

Primeiramente, sexa E unha curva elíptica definida sobre $\mathbb{F}_q$ e $E(\mathbb{F}_q)$ o grupo de puntos racionais desta tal que o neutro $\mathcal{O}$ é o punto no infinito. Para entender o funcionamento do algoritmo, cómpre coñecer o seguinte resultado.

Teorema 1. (Teorema de Hasse) Dada unha curva elíptica E sobre $\mathbb{F}_q$, entón existe $t \in \mathbb{Z}$, coñecido como a traza de Frobenius, tal que

$$\#E(\mathbb{F}_q) = q + 1 - t.$$

Ademais, tense que $|t| \leq 2\sqrt{q}$.

A ECC baséase nos logaritmos discretos sobre o grupo de puntos racionais da curva. É dicir, dado un punto P, coñecido como o xerador, e un punto Q, debemos obter un $k \in \mathbb{Z}$ tal que $Q = kP$. Os puntos P e Q funcionan como claves públicas e o problema resultante é moi difícil de resolver, cos algoritmos coñecidos, para unha curva cun número de puntos $\#E(\mathbb{F}_q)$ grande e primo. O algoritmo de Schoof conta os puntos dunha curva elíptica dada de maneira eficiente, o que nos axuda a escoller curvas seguras para a nosa encriptación. Vexamos entón as ideas e pasos no algoritmo de Schoof.

1. Consideraremos a curva elíptica en forma de Weierstrass, é dicir, da forma $E : y^2 = x^3 + ax + b$ sobre $\mathbb{F}_q$, con $q = p^r$, tal que $p > 3$ é primo e $r \geq 1$. Polo Teorema de Hasse, sabemos que $\#E(\mathbb{F}_q) = q + 1 - t$ para algún $|t| \leq 2\sqrt{q}$.

2. Para computar t achamos $t \mod N$ para $N > 4\sqrt{q}$.

3. Para obter $t \mod N$ descompoñemos N en produto de primos.

4. Finalmente, grazas ao Teorema Chinés dos Restos (TCR), basta coñecer os valores $t \mod l$ (para todo l primo de N) para atopar o resultado.

O parámetro t é a traza do endomorfismo de Frobenius, que é, polo tanto, de especial relevancia no desenvolvemento do algoritmo. Este defínese do seguinte xeito:

$$\begin{array}{rccc} \phi\colon & E(\mathbb{F}_q) & \longrightarrow & E(\mathbb{F}_q) \\ & (x,y) & \longmapsto & (x^q, y^q) \end{array}$$

Definindo de forma adecuada o polinomio característico, cuxos detalles omitimos aquí, pódese obter a ecuación

$$\phi^2 - t\phi + q = 0$$

Equivalentemente,

$$(x^{q^2}, y^{q^2}) + q(x,y) = t(x^q, y^q),\ \forall P = (x,y) \in E$$

Dado agora un $P = (x,y) \in E[l]$ (o conxunto de puntos de torsión de orde $l \in \mathbb{N}$), fixamos $\bar{t}$ como o único enteiro positivo $\leq l$ tal que $\bar{t} \equiv t \mod l$. Tomando módulo l na expresión anterior, satisfacemos a seguinte relación para un número finito reducido de casos.

$$(x^{q^2}, y^{q^2}) + [\bar{q}](x,y) = [\bar{t}](x^q, y^q)$$

Resolvendo $\bar{t}$ para cada l, podemos obter o valor módulo N co TCR.

Durante o proceso de computación, definimos $\psi_l \in \mathbb{F}_q[x]$, chamado o l-ésimo polinomio de división. Este satisfai que $(x_P, y_P) \in E[l] \iff \psi_l(x_P, y_P) = 0$. Estes polinomios facilitan o cálculo dos puntos de torsión, reducindo o problema a resolver ecuacións sobre certos aneis "sinxelos". Esta e outras implementacións poden mellorar a efectividade do algoritmo ata as súas versións máis modernas.

O algoritmo de Schoof converteuse nunha ferramenta fundamental no campo da criptografía de curvas elípticas. A súa capacidade para calcular a orde dunha curva con complexidade en tempo polinómico, especialmente para curvas sobre corpos finitos grandes, mellora significativamente o rendemento dos sistemas baseados nelas. O algoritmo asegura así que se elixan curvas con ordes grandes e axeitadas, mellorando a seguridade destes sistemas criptográficos.

Referencias Bibliográficas

Stefano Marseglia, *Elliptic Curves over Finite Fields*, Utrecht University, 2023.

R. Schoof, *Elliptic Curves over Finite Fields and the Computation of Square Roots mod p*.

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