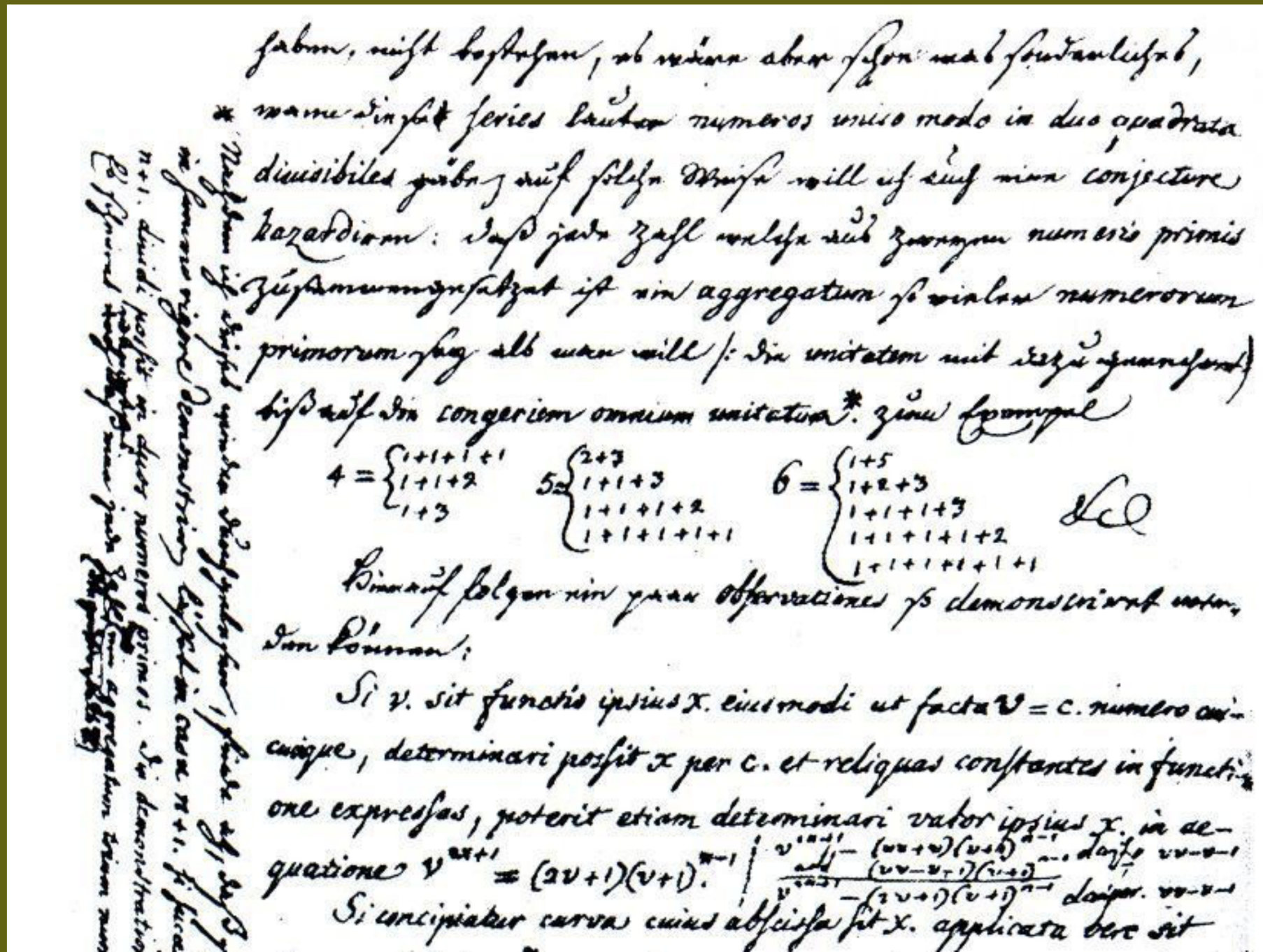
Los númberos primos. Teoremes y conxetures

Hai delles selmanes tuvi ordenando una riestra de carpetes nes que guardo artículos estremaos de física y matemática. Yeren artículos que salieron d'internet y qu'imprimiera pa lleelos (o non) con calma. Ente ellos taben les notes d'una conferencia que dio en 2007 Terence Tao, Medalla Fields en 2006, Premiu Princesa d'Asturies de les Ciencies 2020 y ún de los matemáticos actuales más destacaos. El títulu de la ponencia ye «Estructura y aleatoriedá nos números primos». Anque les notes son bastante esquemátiques, paeciéronme un bon resume de lo que sabemos al rodiu de los números primos y tamién de les sos aplicaciones. El tema de los números primos siempre me llamó muncho l'atención y rápido quixi saber cómo d'actuales yeren los resultaos que Tao presentaba. Dempués d'una busca n'internet, l'ayuda del ChatGPT y la llectura d'unos pocos llibros, llegué a tener una idea de cuál yera l'estáu anguaño, en 2025, de los nuesos conocimientos al rodiu de los números primos y decidime a escribir (a lo primero pa ordenar les mios idees) un resume d'ellos.



Cachu d'una carta de Goldbach a Euler del 1742.

Por **Francisco Argüeso Gómez**
Caderalgu xubiláu del Área de Matemática Aplicada
Departamentu de Matemátiques
Universidá d'Uviéu

Tenté d'escribir dalgo pa un públicu bastante xeneral pero interesáu nestes cuestiones y facer el mio resume lo más accesible posible, centráu na definición básica del númberu primu y dos teoremes fundamentales (ún d'ellos prueba qu'hai primos infinitos). Na segunda seición, falo de cómo buscar números primos, comentando la criba clásica d'Eratóstenes. Na tercera, presento los primos de Mersenne, los números perfeutos y los primos ximielgos. Esto pue vese como la esposición d'una serie de cosadielles agradables al rodiu de los números primos, pero los primos de Mersenne permítenos algamar números primos mui grandes, mui útiles en criptografía. La cuarta seición encara'l problema, entá nun resueltu, na distribución de los primos.

¿Esiste dalguna fórmula que nos diga cuántos números primos hai menores qu'un determináu x? La seición quinta trata la conxetura de Goldbach, un problema mui cenciellu de plantegar, pero mui difícil d'iguar. Pa terminar, la última seición trata la utilidá de los números primos, que, sorprendentemente resulten esenciales pa la seguridá de les nueses comunicaciones y tresferencies per internet.

Camiento que l'estudiu de los números primos ye enforma llamaderu y tien la ventaya de que los teoremes y conxetures rellacionaes con ellos tienen munches veces un enunciáu mui simple, anque les demostraciones seyan d'una dificultá máxima.

DEFINICIONES BÁSIQUES. ¿PRIMOS INFINITOS?

¿Qué ye un númberu primu? La definición ye mui simple:

Un númberu primu ye un númberu natural mayor que 1 que namás se pue dividir ente él mesmu y la unidá.

Exemplos: 2, 3, 5, 7, 11, 13,17, 19, 23,……., 91

El númberu 12 ye perafayadizu porque pue dividise por 1, 2, 3, 4, 6, 12, lo que fai que tovía usemos la docena de güevos, que podemos repartir ente dos, tres, cuatro o seis persones, dando a caún el mesmu númberu

El ser humanu tentó de repartir conxuntos d'oxetos en grupos iguales dende tiempos inmemoriales. Hai grupos que se dexen repartir mui bien, al ser el númberu d'oxetos ún con munchos divisores. Asina, 12, ye un númberu perafayadizu porque pue dividise por 1, 2, 3, 4, 6, 12, lo que fai que tovía usemos la docena de güevos, que podemos repartir ente dos, tres, cuatro o seis persones, dando a caún el mesmu númberu. Los números 60 o 90 tamién son afayadizos, con munchos divisores, y por eso s'usen, ente otres razones, al midir el tiempu o los ángulos. Los números primos son tolo contrario: como viemos na definición, nun se puen dividir. Si tenemos 11 güevos y queremos repartilos de forma equitativa, o queda una persona con toos, o buscamos 11 persones. Toi casi convencíu de que la mala fama del 13 tien dalgo que ver con que seya primu. Sicasí, los primos tienen una propiedá bien guapa, qu'amuesa'l teorema que vien darréu.

TEOREMA FUNDAMENTAL DE L'ARITMÉTICA

Tou númberu natural mayor que 1 pue espresase de manera única (sacante reordenación) como productu de números primos

Por exemplu:

$$36 = 3 * 3 * 2 * 2$$

Si lo ponemos como productu de divisores posibles, la espresión nun ye única:

$$36 = 6 * 6 = 4 * 3 * 3 = 2 * 6 * 3 = \ldots$$

Si tenemos un númberu espresáu como productu de divisores y estos nun son primos, siempre podemos dir descomponiendo estos factores nos sos divisores hasta llegar, nun númberu finitu de pasos, a los factores primos. La espresión ye única porque si hubiese un primu, q_i, qu'apaez nuna primer descomposición y non n'otra, la primera sedría divisible por q_i y la segunda non —al ser los sos factores primos distintos a q_i— esto ye imposible dao que les dos espresiones son iguales al mesmu númberu. Amás, 1 tien de dexase fuera como primu porque sinón, tendríemos

$$45 = 3 * 3 * 5 * 1 = 3 * 3 * 5 * 1 * 1 = \ldots,$$

formes non úniques.

Esti resultáu al rodiu de los primos apaez yá nos *Elementos d'Euclides* (Proposición 14 del Llibru 9); ye dicir, conocíase a lo menos hacia l'añu 300 a.C.

Esti teorema ye de gran importancia porque amuesa que los primos son como los átomos del sistema de números naturales: combinándolos xeneramos tolos números. El númberu d'átomos distintos en Química ye finitu, los que carautericen cada elementu químicu. La entruga obvia ye: ¿hai un númberu finitu o infinitu de primos?

TEOREMA D'EUCLIDES

Hai infinitos números primos

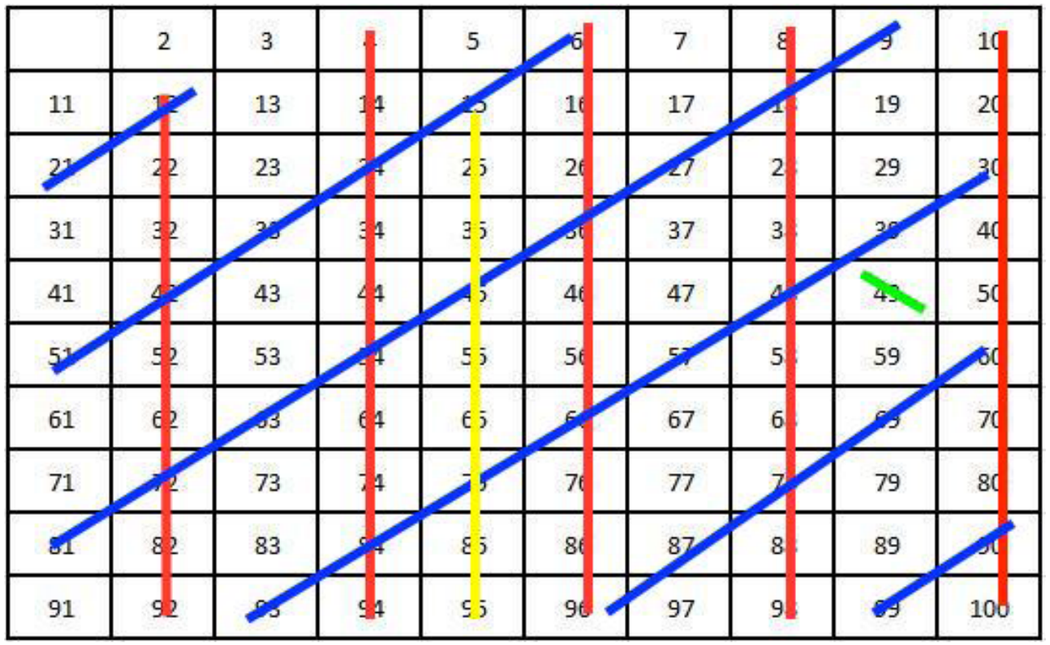
La prueba ye cenciella. Procédese por reducción al absurdu: imaxinemos qu'hai un númberu finitu de primos, entós habría un primu máximu, l'enésimu primu p_n.

Construyamos el númberu

$$p = p1 * p2 * p3 * \ldots\ldots * pn + 1$$

Esti númberu, 1, más el productu de tolos primos anteriores a p_n y el propiu p_n, nun ye divisible por nengún d'estos primos —si lu dividimos queda de restu 1— y polo tanto ye primu y claramente mayor que p_n. Asina que lleguemos a una contradicción. Nun pue haber un númberu finitu de primos. Esti resultáu ye la Proposición 20 del Llibru 9 de los *Elementos* y la prueba d'Euclides ye asemeyada a la qu'escribí, magar él utilizó un llinguaxe más xeométricu.

Esto llévanos a la siguiente cuestión: ¿cómo se busquen números primos?, ¿cómo se construyen números primos mui grandes? Na seición dedicada a les aplicaciones de los primos vamos ver que buscar números primos mui grandes ye importante n'aplicaciones estremaes, sobre manera na criptografía, desarrollándose claves imposibles de romper al traviés del usu de números primos escomanaos o'l so productu. Asina qu'agora vamos ver cómo buscalos ya igualos.



	2	3		5		7			10
11		13	14		16	17		19	20
21	22	23		25	26	27	28	29	30
31	32		34	35		37	38		40
41		43	44		46	47			50
51	52	53		55	56		58	59	
61	62		64	65		67	68		70
71		73	74		76	77		79	80
81	82	83		85	86	87	88	89	
91	92		94	95	96	97	98		100

Figura 1. Representación de La criba d'Eratóstenes

LA CRIBA D'ERATÓSTENES

¿Cómo buscamos númberos primos? Lo primero que se nos ocurre sedría ver si un númberu determináu, por exemplu 49, ye primu. Pa ello vamos dividilu por tolos sos primos iguales o menores que la so raíz cuadrada —si'l númberu ye divisible por un númberu primu mayor que la so raíz cuadrada, tamién sedría divisible por un primu menor— asina 49 nun ye divisible por 2, nin por 3, nin por 5, pero sí por 7, polo tanto nun ye primu. Faciendo lo mesmo con 53 vamos comprobar que sí ye primu. Sicasí, construir una llista de primos d'esta manera, probando númberu a númberu ye mui llargo ya ineficiente. Nicómaco de Gerasa (60–120 d.C.), un matemáticu griegu, espublizó un métodu muncho meyor nes sos *Lecciones d'Aritmética*. El citáu autor asocia'l métodu a Eratóstenes de Cirene (276 a.C.–195/194 a.C.), el gran matemáticu y científicu griegu que foi ún de los direutores de la Biblioteca d'Alexandría. El métodu ye mui cenciellu y eficaz. Como tou númberu non primu tien de ser múltiplu d'ún primu, partimos de los primeros primos y vamos eliminando los sos múltiplos: los números que vayan quedando van ser, necesariamente, primos. Lo que facemos ye dalgo asina como dir cribando números pa que nos queden los valiosos, los primos, como si usáremos una peñera pa separar pebides d'oru del agua d'un ríu; ye polo qu'esti métodu se llama La criba d'Eratóstenes. Vamos ver cómo funciona p'atopar tolos primos menores que 100. Propongo qu'escribáis una llista de números del 1 al 100 en fileres de 10 números. Primeramente, hai d'eliminar tolos múltiplos de 2; ye dicir, los pares. Dempués, táchense los múltiplos de tres —van tachándose simplemente números de 3 en 3 hasta llegar al 99—. Los múltiplos de 5 son los números que terminen en 0 o en 5: elimínense tamién. Siguimos colos de 7, equí yá tachamos namás tres nuevos, 49, 77 y 91. Col siguiente primu 11, yá nun tachamos nengún nuevu menor que 100, dao que'l siguiente númberu compuestu eliminau sedría 121. Asina quedamos cola llista de 25 primos menores que 100.

2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97

Podemos ver que'l métodu ye mui simple, pero non del too eficiente, porque hai números que tachemos dos veces (como 12 o 40) o hasta 3 veces (por exemplu 30 o 60). Podríemos meyorar el métodu eliminando nun entamu tolos múltiplos de 2, 3 y 5. Dempués, pasamos a 7 y yá empezamos en 49 = 7 * 7, dao que los números compuestos anteriores yá tán tachaos, al ser múltiplos de los primos menores que 7. Dempués, multiplicamos 7 por números que nun seyan múltiplos de 2, 3 o 5 —a estos números llámaselos coprimos—, y esto llévanos a quitar 49, 77 y 91 ensin volver a tachar nengún. Esti métodu llámase «factorización en rueda» y permítenos realizar menos operaciones, siendo mui útil si consideramos los primos hasta números mui grandes.

Otres cribes que s'usen p'alcontrar primos ente dos números mui grandes son les llamaes segmentaes que dividen el rangu de busca en dellos cachos usando dempués métodos como l'anterior. La gran ventaya ye que'l programa informáticu usáu tien requerimientos de memoria muncho menores.

Anguaño, úsense métodos mui estremaos y sofisticaos pa buscar primos mui grandes nun intervalu. Dalgunos d'estos métodos son probabilísticos; ye dicir, dannos números que son primos con una altísima probabilidá, pero ensin la total certidume.

PRIMOS DE MERSENNE. NÚMBEROS PERFEUTOS, PRIMOS XIMIELGOS

Marin Mersenne foi un matemáticu y filósofu francés que tuvo amistá y correspondencia con figures científiques destacaes de la época como Descartes, Fermat o Galileo. Trabayó colos números primos y la teoría del soníu, siendo conocíu como «El pá de l'acústica». Tuvo dientro de la orde relixosa de los Mínimos, fundada por San Francisco de Paula, llamaos asina por tentar de vivir colo mínimo, faciendo una vida mui austera.

Mersenne construyó los llamaos primos de Mersenne, que s'escriben como:

$$M_p = 2^p - 1$$

Figura 2. *Marin Mersenne (1588–1648)*

Pa que M_p seya primu, p tien de selo, pero que p lo seya nun garantiza que M_p tamién seya primu. Asina, tenemos la llista de primos de Mersenne que sigue darréu:

$p = 2$, $M_p = 3$
$p = 3$, $M_p = 7$
$p = 5$, $M_p = 31$
$p = 7$, $M_p = 127$

Como se pue ver, nesta llista van apaeciendo primos, pero nun tán, nin muncho menos, tolos que conocemos. Falten 11, 13, 17, 19… Si p nun ye primu, el númberu $2^p - 1$ nun lo ye tampoco. Exemplu: $p = 4$, $2^4 - 1 = 15$.

Ún podría pensar que con esta fórmula siempre s'algamaría un primu. Llamentablemente, esto nun ye cierto:

$p = 11$, $M_p = 211 - 1 = 2047 = 23 * 89$

De toles maneres, la fórmula permítenos dir xenerando primos mui grandes rápidamente

$p = 31$, $M_p = 2.147.486.647$,

que ye primu.

Anguaño, la fórmula úsase pa xenerar los números primos más grandes. Pa ello emplégase una rede de computadores per tol mundu que trabayen a comuña nos cálculos del proyeutu GIMPS (Great Internet Mersenne Prime Search), Gran Busca de Primos de Mersenne n'Internet.

Luke Durant algamó asina'l mayor númberu primu conocíu hasta agora en 2024. Ye un primu de Mersenne

$2^{136.279.841} - 1$

Los años 2027, 2029 formen una pareya de primos ximielgos. La siguiente va ser 2081, 2083

Esti númberu tien unos 41 millones de díxitos. ¡Nun tentéis de probar que ye primu! Pa facelo utilízase l'algoritmu de Lucas-Lehmer, válidu namás pa números de Mersenne. Nun se sabe tovía si hai un númberu infinitu de primos de Mersenne. Hasta'l momentu calculáronse 52, siendo'l mayor l'escritu anteriormente. Existe una conexón curiosa ente los primos de Mersenne y otros números mui interesantes, los números perfeutos.

Los números perfeutos son aquellos que puen escribise como suma de los sos divisores, ensin incluyir el propiu númberu. Exemplos:

$6 = 1 + 2 + 3$
$28 = 1 + 2 + 4 + 7 + 14$
$496 = 1 + 2 + 4 + 8 + 16 + 31 + 62 + 124 + 248$

D'esta manera, estos números nun son nada habituales. Los siguientes son 8.128 y 33.550.336. Ta probao que tolos números perfeutos conocíos son pares. De fechu, Euler (1707-1783) probó que tou númberu perfeutu par pue escribise como

$2^{p-1} * (2^p - 1)$,

siendo $2^p - 1$ un primu de Mersenne. Amás, con esa fórmula, tou primu de Mersenne da llugar a un númberu perfeutu. Sicasí, nun se probó tovía que nun existan números perfeutos impares, anque nun se conoz nengún. El mayor númberu perfeutu conocíu ye'l que s'algama a partir del mayor primu de Mersenne que se conoz. Sedría entós:

$2^{136.279.840} * (2^{136.279.841} - 1)$

Como ye a vese, el númberu tien una barbaridá de díxitos.

Otros números perinteresantes son los que se llamen «primos ximielgos», ye dicir, pareyes de primos que tienen una diferencia de dos, $p - 1$, $p + 1$, siendo p un númberu par.

Exemplu:

3, 5
5, 7
11, 13
17, 19
29, 31
41, 43

Los años 2027, 2029 formen una pareya de primos ximielgos. La siguiente va ser 2081, 2083. Pue vese qu'al medrar el númberu de díxitos, échense en falta los primos ximielgos.

El novelista Paolo Giordano usa la metáfora de los primos ximielgos pa referise a la rellación ente los protagonistes de la so novela *La soledá de los números primos*. Mattia piensa que la so rellación con Alice ye como la de dos primos ximielgos, solos y perdíos, xuntos pero non bastante como pa tocase de verdá.

A la entruga de si hai pareyes infinites de primos ximielgos, la rempuesta ye: nun se sabe. La conxetura de los primos ximielgos diznos qu'hai infinitos, pero ta ensin demostrar. Sabemos gracies a un teorema probáu por Yitang Zhang en 2013 qu'existe un N enteru menor que $70 * 10^6$ tal qu'existen pareyes infinites de primos con diferencia N. Esta cota rebaxóse a 246, y ehí quedó. Les pareyes de primos ximielgos han de ser (nun siendo la primera) de la forma $6n - 1$, $6n + 1$. De fechu, tolos primos, nun siendo 2 y 3

son axacentes a un múltiplu de 6. Pa $n > 1$, les pareyes de primos ximielgos, $6n - 1$, $6n + 1$, namás se dan si la última cifra de n ye 0, 2, 3, 5, 7, 8. La pareya de primos ximielgos más grande conocida ye

$$(2.996.863.034.895 * 2^{1.290.000} - 1,$$
$$2.996.863.034.895 * 2^{1.290.000} + 1),$$

descubierta en 2016. Finalmente, llámense primos aisllaos los que nun formen parte d'una pareya de ximielgos. Probóse un resultáu que nos diz que'l cociente ente'l númberu de primos aisllaos menores que n y el númberu total de primos tiende a 1 cuando n tiende a infinitu. Ye dicir; nesti sentíu los primos en pareyes son mui pocos. Darréu vamos estudiar cómo tán distribuyíos los números primos; ye dicir, si son aleatorios o existe dalguna llei que nos permita producilos. Vamos ver que la situación ye, de dalguna forma, intermedia.

DISTRIBUCIÓN DE LOS NÚMBEROS PRIMOS. EL TEOREMA DE LOS NÚMBEROS PRIMOS

Anque Euler (1707-1783) y Lagrange (1736-1813) yá suxirieron esa aproximación, foron el matemáticu francés Hadamard (1865-1963) y el matemáticu belga De la Vallée Poussin (1866-1962) los que probaron en 1986 el llamáu Teorema de los Números Primos.

TEOREMA DE LOS NÚMBEROS PRIMOS

Si llamamos $\pi(x)$ al númberu de primos menor o igual qu'un númberu x, cúmplese que

$$\lim_{x\to\infty} \frac{\Pi(x)}{x/log(x)} = 1$$

Ye dicir, cuando $x \to \infty$ (x tiende a infinitu) el númberu de primos pue aproximase como'l cociente de x y el logaritmu neperianu de x, o dicho d'otra manera, el númberu de primos nun crez de manera llinial con x sinón qu'hai un pesu de la forma $1/ log(x)$.

Ensin entrar nel significáu del logaritmu neperianu, podemos dicir qu'esti reflexa'l númberu de díxitos del númberu, asina que'l númberu de primos medra con x pero esti aumentu ta dividíu por una cifra que depende del so númberu de díxitos. El cociente ente $\pi(x)$ y x —la proporción de primos—mengua como $1/ log (x)$, decrez d'alcuerdu col númberu de díxitos de x. Al dir considerando números cada vez mayores, la proporción de primos va diminuyendo. Asina ente 1 y 1000 hai 168 primos, pero nel intervalu d'igual llonxitú ente 1.000.000 y 1.001.000 namás hai 49.

Como consecuencia d'esti teorema o como otra forma d'escribilo, l'enésimu númberu primu p_n pue aproximase por $n * log(n)$. Ye dicir

$$\lim_{n\to\infty} \frac{p_n}{n * log(n)} = 1$$

La prueba d'esti teorema ye mui complicada al requerir l'usu de la función $\zeta(s)$, la famosa zeta de Riemann.

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}$$

siendo Σ el sumatoriu sobre tolos naturales. Hai una conexón ente esta función y los números primos al traviés de la fórmula d'Euler

$$\sum_{n=1}^{\infty} \frac{1}{n^s} = \prod_{p\ prime}(1/(1 - p^{-s}))$$

onde Π ye'l productu sobre tolos primos. Los ceros de la ζ de Riemann xueguen un papel destacáu na demostración del Teorema de los números primos, indicando un ciertu patrón na distribución de los primos.

Vamos amosar cómo de bona ye la primer aproximación con dalgunos valores de x. Vamos escribir l'error relativu pal númberu de primos real y el que nos da la fórmula.

$x = 103$, *error* = 13.3 %
$x = 104$, *error* = 11.6 %
$x = 106$, *error* = 7.8 %
$x = 1012$, *error* = 5.1 %

L'error relativu va tendiendo a cero, pero de manera mui lenta. Esti ye'l motivu pol que se buscaron aproximaciones meyores. Pue probase que la integral logarítmica nos da una meyor aproximación. Cúmplese que

$$\lim_{x\to\infty} \frac{\Pi(x)}{\int_2^x (1/log(t))dt} = 1$$

La integral logarítmica ye la qu'apaez nel denominador y representa l'área llendada pola curva $1/ \log(t)$ y l'exe OX ente 2 y x. El resultáu danos una aproximación más fina que la del teorema de los números primos. Existen cotes óptimes sobre l'error absolutu d'esta aproximación, estes cotes dependen de que se satisfaga la hipótesis de Rieman, una conxetura sobre los ceros de la función de Riemann que tovía nun se probó y que constitúi ún de los problemes abiertos más importantes de les matemátiques. De toles maneres, podemos ver lo bona que ye esta aproximación dando los errores relativos ente'l númberu de primos real y el que nos da la fórmula.

$x = 103$, *error* = 5.6 %
$x = 104$, *error* = 1.4 %
$x = 106$, *error* = 0.16 %
$x = 1012$, *error* = 10−4 %

Como pue vese, l'aproximación ye escelente. Hai que recordar, sicasí, que ye una fórmula aproximada y nun hai una fórmula exauta que nos dea'l númberu de primos menores que x. Los primos nun tán determinaos d'antemano o, a lo menos, nun sabemos determinalos pero sí aproximalos.

LA CONXETURA DE GOLDBACH

Christian Goldbach foi un matemáticu amigu de Leonhard Euler (1707–1783). Euler, consideráu como ún de los matemáticos más importantes de la historia, mantenía correspondencia con Goldbach y la conxetura apaez suxerida por Goldbach nel so intercambéu epistolar. El párrafu de la carta ta escritu nuna mezcla interesante d'alemán y llatín. El conteníu de la conxetura ye mui cenciellu:

Conxetura de Goldbach: tou númberu par mayor que 2 pue expresase como la suma de dos primos

Por exemplu:

$4 = 2 + 2$
$16 = 11 + 5$
$80 = 43 + 37$

Magar la so cenciellez, esti resultáu nun pudo probase tovía. Usando cálculu computacional, la conxetura probóse pa tolos pares menores o iguales que $4 * 10^{18}$ lo que paez indicar que ye cierta. Sicasí, los nuesos llectores tienen de recordar que la prueba tien de valir pa números pares infinitos, asina una prueba típica sedría partir de qu'hai un númberu par que nun pue espresase como la suma de dos primos y llegar por pura lóxica a una contradicción. Esto ye dificilísimo. Vamos ver agora que sí hubo progresu

dende los tiempos de Goldbach y pa ello vamos escribir la

Conxetura débil de Goldbach: tou númberu impar mayor que 5 pue espresase como la suma de tres primos

Si la conxetura sobre los pares —qu'agora llamaremos conxetura fuerte de Goldach—ye cierta, la conxetura débil tamién lo ye. Esto ye fácil de probar porque podemos escribir tolos impares a partir de 7 como 3 más un númberu par. Si'l par ye la suma de dos primos, l'impar sedrá la suma de 3. Exemplos:

$$7 = 3 + 4 = 3 + 2 + 2$$
$$11 = 3 + 8 = 3 + 5 + 3$$

Sicasí, si la conxetura débil ye válida, la fuerte nun tien por qué selo. En Matemátiques, el términu fuerte refierse a una proposición más xeneral con respeuto a otra, débil, menos xeneral.

Pues bien, ye na conxetura débil onde se fixeron progresos definitivos dende l'artículu de Tao de 2007. La conxetura débil probóse en 2013 pol matemáticu peruanu Harald Halfgott. Lo sorprendente ye que la prueba, de gran dificultá, aceutóse como válida por una revista, *Annals of Mathematical Studies*, pero tovía nun se publicó n'ella, pudiendo consultala namás n'internet. Suponemos que suxeriríen dalgunos cambeos nel artículu que tovía nun se fadríen, dada la dificultá estrema del tema y la esistencia de poques persones que puedan entender la prueba. De toles maneres, la conxetura débil considérase probada y como consecuencia d'esta probóse tamién que tou númberu par mayor que 2 pue ponese como la suma de 4 primos como máximo. Ye dicir, paez que queda un percorríu curtiu pa la prueba definitiva de la conxetura fuerte, anque quiciás seya un camín mui complicáu.

***Figura 3**. Christian Goldbach (1690–1764)*

Otru resultáu interesante relativu a la conxetura fuerte ye'l que probó'l matemáticu chinu Chen Yingrun nel 1973: tou númberu par suficientemente grande pue escribise como la suma de dos primos o como la suma d'un primu y un semiprimu (productu de los primos). Esta sedría otra forma d'averase a la conxetura fuerte de Goldbach.

Na lliteratura, la conxetura de Goldbach apaez como tema central de la novela *El tío Petros y la conxetura de Goldbach* del escritor griegu Apostolos Doxiadis.

SOBRE LA UTILIDÁ DE LOS NÚMBEROS PRIMOS

Hasta va poco, los números primos grandes nun tuvieron un usu práuticu importante. Sicasí, col entamu del emplegu de sistemes de comunicación basaos n'ordenadores, fíxose necesario y posible unviar claves secretes —como les del bancu o les tarxetes de creitu pa facer pagos—, firmar documentos dixitalmente o unviar mensaxes per internet que nun puedan descrifrar terceres persones. Voi comentar brevemente dos métodos que s'usen davezu pa estes xeres.

Los dos básense na llamada aritmética modular, na que se faen delles operaciones con números naturales, trabayándose col restu de la división por un númberu. Nel casu del métodu de Diffie-Hellmann (1976) existen dos claves públiques: un númberu primu mui grande p y otru númberu g, que se llama «una raíz primitiva módulu p», y que s'escueye de manera afayadiza. Les dos persones qu'intercambien los mensaxes, Xuacu y Lena, tamién tienen les sos propies claves secretes, los números a y b. Xuacu calcula'l restu de dividir el númberu g^a por p, que se conoz téunicamente como $g^a \ mod \ p$, g^a módulu p, llamemos A a esi númberu que Xuacu unvia a Lena.

$$A = g^a \ mod \ p$$

Lena calcula'l restu de dividir g^b por p y unvia esti númberu B a Xuacu.

$$B = g^b \ mod \ p$$

Darréu, Xuacu calcula'l restu de dividir B^a por p que sedrá un númberu s.

$$s = B^a \ mod \ p$$

y Lena'l restu de dividir A^b por p que, maraviyes de l'aritmética modular, ye'l mesmu númberu s.

$$s = A^b \ mod \ p$$

D'esta manera dambos tienen una clave compartida s. Si agora Lena quier unviar un mensaxe a Xuacu —un númberu C, por exemplu—, podría multiplicar $C * s$ y mandar el resultáu. Xuacu namás tendría que dividir esi resultáu por s pa obtener C. Esto último ye una simplificación, pudiendo usase otres operaciones. El casu ye qu'a partir de tolos números calculaos que se comparten per internet ye casi imposible atopar la clave compartida. Esto débese a que'l númberu que s'usa ye un primu mui grande y na artimética modular calcular les claves secretes a partir de les operaciones d'esponenciación feches y que circulen per internet ye dificilísimo.

N'otru métodu, RSA (Rivest, Shamir & Adleman, 1978), en vez d'usar un primu mui grande usen el productu de dos primos mui grandes y faen operaciones d'esponenciación quedando col restu al dividir pol productu de los primos. Mientres que Diffie-Hellman s'usa pa comunicaciones segures, RSA úsase más pa firmes dixitales. Anguaño, buscar primos grandes ye un negociu, como lo ye desarrollar algoritmos de cifráu basaos en números primos.

Un segundu motivu pol que los números primos resulten útiles ye'l de probar algoritmos eficientes pa buscalos o estudiar conxetures sobre ellos. Sirven pa poner a prueba la capacidá de los ordenadores más potentes y de los meyores programadores. Ye un poco como poner a prueba un Fórmula 1 nun trazáu mui exixente. Tamién permiten combinar el trabayu d'ordenadores en rede como na busca de primos en Mersenne.

Una tercer utilidá, qu'existió siempre, ye la de despertar l'interés matemática y científica en neños y mozos. Trabayar en problemes que puen ser astractos exercita la mente pa estremaes xeres inteleutuales. Xeres que puen tener un interés práuticu. Anguaño ye habitual qu'empreses y bancos contraten a matemáticos pola so capacidá pa resolver problemes. ¿Quién-y diba a dicir a Mersenne que los sos primos tendríen utilidá nel mundu del comerciu? Siendo un Mínimu, nun sé si-y diba a gustar muncho.