Números primos. Criptografía RSA

Sergio A. Carrillo
sacarrillot@unal.edu.co

Números Primos

Un número $p \in \mathbb{N}^+$ es primo si $p > 1$ y sus únicos divisores son 1 y p. Es decir, si $d|p$, entonces $d = 1$ ó p.

Figure: La criba de Eratóstenes

1	2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50
51	52	53	54	55	56	57	58	59	60
61	62	63	64	65	66	67	68	69	70
71	72	73	74	75	76	77	78	79	80
81	82	83	84	85	86	87	88	89	90
91	92	93	94	95	96	97	98	99	100

Comprobando que un número es primo

Los números que no son primos se llaman *compuestos*.

Proposición

Si $n \in \mathbb{N}$ no es primo, existe al menos un divisor $d|n$ tal que $2 \leq d \leq \sqrt{n}$.

Por tanto, para comprobar que n es primo basta con dividir a n por números $m \leq \sqrt{n}$.

Teorema fundamental de la Aritmética

Teorema

Si $n \in \mathbb{N}^+$, $n \geq 2$ es puede escribir de forma única como producto de potencias de primos.

Ejemplo

- $6 = 2 \cdot 3$.
- $44 = 2^2 \cdot 11$.
- $100 = 2^2 \cdot 5^2$.
- $450 = 11 \cdot 41$.
- $641 = 641$.
- $999 = 3^3 \cdot 37$.
- $1024 = 2^{10}$.
- $1223 = 1223$.
- $1994 = 2 \cdot 997$.
- $360881 = 509 \cdot 709$.

¿Cuantos primos hay?

Teorema (Euclides)

Existen infinitos números primos.

El número primo más grande que se conoce es

$$2^{82589933} - 1$$

y tienen 24862048 dígitos. Los primos de la forma $M_p = 2^p - 1$, con p primo, se conocen como primos de Mersenne.

- `http://compoasso.free.fr/primelistweb/page/prime/liste_online_en.php`
- `https://en.wikipedia.org/wiki/Largest_known_prime_number`

Infinitud de los primos

- (Euclides) Dados $p_1, \ldots, p_r$ primos, considere $(p_1 \cdots p_r) + 1$.
- (Iterativo - F. Saidak) Fije $N \geq 2$ y considere $N_1 = N(N+1)$, $N_2 = N_1(N_1+1)$, $N_3 = N_2(N_2+1), \cdots$
- Mostrando que $\displaystyle\sum_{n=1}^{\infty} \frac{1}{p_n} = \frac{1}{2} + \frac{1}{3} + \frac{1}{5} + \frac{1}{7} + \frac{1}{11} + \cdots = +\infty.$

Congruencias y el principio del palomar

MathBit

A Pigeon Hole Proof of the Infinitude of Primes

Vincent van der Noort

Received 09 Oct 2024, Accepted 14 Nov 2024, Published online: 18 Mar 2025

Suppose that there are only finitely many primes. Write all of them down on a piece of paper and draw an arrow from each prime q to all the primes dividing $2^q - 1$. Since each prime has at least one outgoing arrow and the prime number 2 has no incoming arrows, we see that some prime p has at least two arrows coming in, from primes q and r say.

Let a be the smallest positive number such that $2^a \equiv 1 \mod p$. Then a divides every b such that $2^b \equiv 1 \mod p$. Since $2^q \equiv 2^r \equiv 1 \mod p$ we find that a divides both q and r and hence equals 1 (as q and r are prime). But this implies that $2^1 \equiv 1 \mod p$, a clear contradiction.

—Submitted by Vincent van der Noort
Netherlands Cancer Institute–Antoni van Leeuwenhoek, Amsterdam

https://doi.org/10.1080/00029890.2025.2459047

Como no construirlos...

Proposición

Si $p(x) = c_n x^n + \cdots + c_1 x + c_0 \in \mathbb{Z}[x]$ *es un polinomio con coeficientes enteros, entonces* $p(m)$ *no es primo para infinitos* $m \in \mathbb{Z}$.

Como no construirlos...

Euler propuso varios polinomios para generar primos. Por ejemplo, $p(n) = n^2 + n + 41$ produce los siguientes 39 primos.

- $p(1) = 43$
- $p(2) = 47$
- $p(3) = 53$
- $p(4) = 61$
- $p(5) = 71$
- $p(6) = 83$
- $p(7) = 97$
- $p(8) = 113$
- $p(9) = 131$
- $p(10) = 151$
- $p(11) = 173$
- $p(12) = 197$
- $p(13) = 223$
- $p(14) = 251$
- $p(15) = 281$
- $p(16) = 313$
- $p(17) = 347$
- $p(18) = 383$
- $p(19) = 421$
- $p(20) = 461$
- $p(21) = 503$
- $p(22) = 547$
- $p(23) = 593$
- $p(24) = 641$
- $p(25) = 691$
- $p(26) = 743$
- $p(27) = 797$
- $p(28) = 853$
- $p(29) = 911$
- $p(30) = 971$
- $p(31) = 1033$
- $p(32) = 1097$
- $p(33) = 1163$
- $p(34) = 1231$
- $p(35) = 1301$
- $p(36) = 1373$
- $p(37) = 1447$
- $p(38) = 1523$
- $p(39) = 1601$

Note que $p(40) = 40^2 + 40 + 41 = 40^2 + 80 + 1 = 41^2$ no es primo.

El teorema de los números primos

Sea $\pi(x) = \sum_{p \leq x} 1$, la función que cuenta el número de primos que son menores o iguales a x. Por ejemplo

$$\pi(1) = 0, \quad \pi(2) = 1, \quad \pi(3) = 2, \qquad \pi(20) = 8.$$

En particular, si p_n es el n-ésimo primo, entonces $\pi(p_n) = n$.

Teorema (Hadamard, de la Vallée Poussin)

$$\lim_{x \to +\infty} \frac{\pi(x)}{x/\ln(x)} = 1, \qquad \lim_{n \to +\infty} \frac{p_n}{n \ln(n)} = 1.$$

Por ejemplo, $\pi(10^{12}) = 37.607'912.018$ y $\frac{10^{12}}{\ln(10^{12})} \approx 36.191'206.825$, y el cociente ≈ 1.039145.

Más sobre infinitud - Teorema de Dirichlet

Teorema

Si $\gcd(a, d) = 1$, *entonces existen infinitos primos en la sucesión* $\{d \cdot n + a\}_{n \geq 0}$.

Ejemplo

- Hay infinitos primos de la forma $6k - 1$.
- Hay infinitos primos que terminan en 999. Basta tomar $d = 1000$ y $a = 999$.

El postulado de Bertrand

Si $n \geq 2$, entonces existe un primo p tal que

$$n < p < 2n.$$

Este enunciado también se enuncia como

$$p_n < p_{n+1} < 2p_n, \qquad n \geq 1.$$

Aplicación a criptografía.

Cripto = secreto, grafos = escritura.

Estudio de técnicas de cifrado o codificado destinadas a alterar las representaciones lingüísticas de ciertos mensajes con el fin de hacerlos ininteligibles a receptores no autorizados.

Cifrado Cesar

Trabajando módulo 26 se desplaza cada letra 3 unidades para codificar un mensaje:

a	b	c	d	e	f	g	h	i	j	k	l	m
0	1	2	3	4	5	6	7	8	9	10	11	12
n	o	p	q	r	s	t	u	v	w	x	y	z
13	14	15	16	17	18	19	20	21	22	23	24	25

Ejemplo: Descifrar el mensaje: KROD PXQGR.

Encriptación RSA

En 1976, tres científicos del MIT (Ronald **R**ivest, Adi **S**hamir, Leonard **A**dleman) introdujeron un sistema de encriptación de llave pública basado en factorización de números enteros.

Datos necesarios: p y q números primos. $n = pq$. Exponente e tal que $\gcd(e, (p-1)(q-1)) = 1$.

Llave: (n, e).

El algoritmo con llave (n, e)

Para encriptar un mensaje M, se traduce la frase a números, pero ahora $A \to 00$, $B \to 01$, $C \to 02$,...,$J \to 09$. Luego concatenamos los dígitos obtenidos en un solo número.

Ahora, separe los dígitos en bloques de tamaño $2N$, donde este número par es el mayor tal que $2525...25$ (con $2N$ dígitos) sea menor o igual a n (colocar X al final si hace falta).

M es ahora una sucesión $m_1, m_2, \ldots, m_k$. Cada m_j se cifra (cambia) por

$$c_j = m_j^e \pmod{n}.$$

En este paso aplicamos exponenciación modular rápida.

Mensaje encriptado: $c_1|c_2|\ldots|c_k$.

Ejemplo

Llave: $(n, e) = (2537, 13)$.

$n = 43 \cdot 59$. $p = 43$, $q = 59$. $e = 13$ es primo relativo con $(p-1)(q-1) = 42 \cdot 58 = 2436$.

Como $2525 < 2527 < 252525$, $2N = 4$, $N = 2$.

Codifiquemos: ANY $\longrightarrow$ 001324.

$$0013|24XX.$$

$c_1 = 13^{13} (\text{mod } 2537) \equiv 2038$. $c_2 = 24^{13} (\text{mod } 2537) \equiv 2130$

Mensaje cifrado: $2038|2130$.

¿Cómo descifrarlo?

Como e y $(p-1)(q-1)$ son primos relativos, existe d tal que

$$d \cdot e \equiv 1 (\text{mod } (p-1)(q-1)).$$

Es decir, $de = 1 + k(p-1)(q-1)$, para algún k. De esta forma,

$$c^d = (m^e)^d = m^{de} = m^{1+k(p-1)(q-1)}.$$

Por el teorema de Euler $m^{(p-1)(q-1)} \equiv 1 (\text{mod } pq)$. Luego

$$c^d \equiv m \cdot (m^{(p-1)(q-1)})^k \equiv m \, (\text{mod } pq).$$

Como $n = pq$, concluimos que

$$c^d \equiv m \, (\text{mod } n).$$

Ejemplo

Mensaje encriptado: 0981 0461.

Llave $(n, e) = (2537, 13)$. $n = 43 \cdot 59$. $p = 43$, $q = 59$.

- Encontrar d tal que $13d \equiv 1 (\text{mod } 42 \cdot 58 = 2436)$. Al aplicar el algoritmo de Bezout resulta que $d = 937$.
- Calcular $m = c^{937} (\text{mod } 2537)$:
  $981^{937} \equiv 0704 (\text{mod } 2537)$, $461^{937} \equiv 1115 (\text{mod } 2537)$.
- $0704|1115 \longrightarrow$ HELP.