Números primos y criptografía

Cortes Mora Itzel Jesabel
Ordaz Rodríguez Iván
Asesor: Roberto Méndez Méndez

September 2021

Introducción

El antecedente del estudio de los número primos se remonta a Eratóstenes.

1. Algo de información

Teorema 1)

El divisor primo más pequeño de un número compuesto n es menor que o igual a $\lfloor\sqrt{n}\rfloor$

2. Datos preliminares

Definición 1) Función Eit(x)

Es la función que da 1 si $x \in \mathbb{N}$ y 0 en otro caso, es decir

$$Eit(x) = \begin{cases} 0 & \text{si } x \in \mathbb{R} \backslash \mathbb{N} \\ 1 & \text{si } x \in \mathbb{N} \end{cases} \tag{1}$$

La función *Eit* se usará para anular los números no primos y contar solo números primos en un conjunto. Características de la función *Eit*:

1. No es distributiva.

$$Eit(Eit(a) + Eit(b)) \neq Eit(Eit(a)) + Eit(Eit(b))$$

Definición 2) Función E(A)

Esta función regresa el número de naturales positivos ($\mathbb{N}^+$) en un conjunto A

$$E(A) = |\{x \,|\, x \in A \text{ y } x \in \mathbb{N}^+\}| \tag{2}$$

donde $A \subset \mathbb{R}$ y $|A| = m$.

La función E se define en términos de la función Eit y se expresa como

$$E(A) = \sum_{x \in A} Eit(x) \tag{3}$$

Definición 3) Función C

$$C = \sum_{i=1}^{i_f} Eit\left(\sum_{j=8}^{j_f} Eit(m(i,j))\right) \tag{4}$$

La suma de la fórmula anterior queda como:

$$Eit\left(\sum_{j=8}^{j_f} Eit(m(1,j))\right) + Eit\left(\sum_{j=8}^{j_f} Eit(m(2,j))\right) + Eit\left(\sum_{j=8}^{j_f} Eit(m(3,j))\right) + \cdots + Eit\left(\sum_{j=8}^{j_f} Eit(m(i_f,j))\right)$$

Teorema 1) Definición de C(x)

Si $4 \leq x < 26$

$$C(x) = 0$$

Si $x \geq 26$, entonces

$$C(x) = \sum_{i=0}^{i_f(x)} Eit\left(\sum_{j=0}^{j_f(x)} Eit\left(\frac{4j - (-1)^j + (2i+1)(-1)^{i+j} + (2i-1)(-1)^i - 12i^2 + 5}{12i + 6 - 2(-1)^i}\right)\right)$$

donde

$$j_f(x) = \left\lceil \frac{1}{2} \left\lfloor \frac{2x + (-1)^x - 7}{3} \right\rfloor \right\rceil$$

$$i_f(x) = \left\lceil \frac{-1 + \sqrt{1 + 3(j_f(x))}}{3} \right\rceil$$

Definición 4) Función $\pi(n)$

La función $\pi(n)$ es definida como

$$\pi(x) = |\, \{p \in \mathbb{P} \,|\, p < x \,,\, x \in \mathbb{N} \ y \ x > 3\} \,| \tag{5}$$

es decir $\pi(x)$ es el número de primos menores a x.

Teorema 2)

La expresión que me da el valor de $\pi(x)$ es

$$\pi(x) = \left\lceil \frac{1}{2} \left\lfloor \frac{2x + (-1)^x - 6C(n) + 5}{3} \right\rfloor \right\rceil \tag{6}$$

Demostración. 1. Tomamos el triángulo rectángulo de catetos 1 y h e hipotenusa p tal que $p \in \mathbb{P}$ el conjunto de números primos luego entonces

$$h^2 = p^2 - 1 \qquad p > 3 \tag{7}$$

De manera experimental se construyó otra ecuación k, tal que

$$k^2 = \frac{-(3+6i)(-1)^i + 18i^2 + 18i + 3}{2} \qquad i \geq 1$$

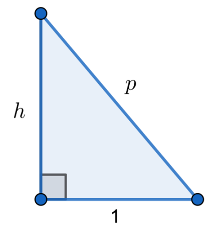

Figura 1: Triángulo equilátero de catetos 1 y h, e hipotenusa p

Igualando ambas las ecuaciones

$$p^2 - 1 = \frac{-(3+6i)(-1)^i + 18i^2 + 18i + 3}{2}$$

se llega a que

$$p = \frac{-(-1)^i + 6i + 3}{2} \qquad i \geq 1 \tag{8}$$

En este caso la nueva ecuación para p adolece que para una serie de valores i, p no será primo (Vea tabla de Excel). De manera forma el dominio de la ecuación debería ser $D(h^2) \cap D(k^2)$. Denominaremos a este conjunto de valores donde p no es primo como j, es decir

$$j = \{i \in D(k^2) \,|\, p(i) \notin \mathbb{P}\} \tag{9}$$

Algunos de estos números son $j = \{8, 11, 16, 18, 21, 25, 28, 31, 38, 41, ...\}$

La primera posición que llamare $j_{ini(p)}$ donde aparece el primer múltiplo de un primo (p ¿3) no repetido, esta dada por la expresión

$$j_{ini(p)} = \frac{p^2 - 1}{3} \tag{10}$$

al tener la posición inicial se encuentra una regularidad en la forma en que vuelven a presentarse los múltiplos de dicho primo p

Ejemplo 1) Caso p = 11

Usando el programa en R notamos que las posiciones onde 11 tiene múltiplos son

$$j_{p=11} = \{3, 18, 25, 40, 47, 62, 69, 84, 91, 106, 113, \ldots\} \tag{11}$$

Entonces notamos que las posiciones de los múltiplas guardan una regularidad

$$\begin{aligned} 18 - 3 &= 15 \\ 25 - 18 &= 7 \\ 40 - 25 &= 15 \\ 47 - 40 &= 7 \\ &\vdots \end{aligned}$$

Si denominamos A = 7 y B = 15

$$\begin{aligned} j_1 &= j_{ini(p)} + 0A + 0B \\ j_2 &= j_{ini(p)} + 1(A+B) - B \\ j_3 &= j_{ini(p)} + 1(A+B) + 0B \\ j_4 &= j_{ini(p)} + 2(A+B) - B \\ j_5 &= j_{ini(p)} + 2(A+B) + 0B \\ &\vdots \end{aligned}$$

Probando con diversos números primos, una posible forma general que se encuentra es

$$j_m = j_{ini(p)} + \varphi(m)(A+B) + \mu(m)B \tag{12}$$

con $m \in \mathbb{N}^+$ y donde se cumple

$$\mu(m) = \begin{cases} 0 & \text{si } \ m \text{ impar} \\ -1 & \text{si } \ m \text{ par} \end{cases}$$

´ y

$$\varphi(m) = \begin{cases} \frac{m}{2} & \text{si } \ m \text{ par} \\ \frac{m-1}{2} & \text{si } \ m \text{ impar} \end{cases}$$

las dos series son muy conocidas y tienen la forma

$$\mu(m) = \frac{1}{2}\left(-(-1)^m - 1\right) \tag{13}$$

$$\varphi(m) = \frac{1}{4}\left(2m + (-1)^m - 1\right) \tag{14}$$

Ahora obtendremos los valores de $A{+}B$ y B en términos de los parámetro i y p.
De la tabla que

$$A + B = 2p \tag{15}$$

mucho más complicada es ver que

$$B = -(-1)^i[-(-1)^i p + i + 0.5 - 0.5(-1)^i] \tag{16}$$

Con los valores obtenidos par A, B φ y μ obtenemos una expresión para el término general de la sucesión j_m, la cual queda dada como

$$\begin{aligned} j_m = \frac{p^2-1}{3} &+ \frac{1}{4}\left(2m + (-1)^m - 1\right)2p \\ &+ \frac{1}{2}\left(-(-1)^m - 1\right)\left(-(-1)^i\left[-(-1)^i p + i + 0.5 - 0.5(-1)^i\right]\right) \end{aligned} \tag{17}$$

Ahora vamos a encontrar los limites de las sumas para C(x).
Nuevamente hacemos otra suposición para p

$$p = x + (0.5 + (0.5)(-1)^x) \qquad x > 3$$

donde $x > 3$ y $x \in \mathbb{N}$. Note que esto hace que p siempre sea impar, se toma $i = j_f + 1$ y se igual con la ecuación (8)

$$x + (0.5 + (-0.5)^x) = \frac{-(-1)^{j_f+1} + 6(j_f+1) + 3}{2}$$

despejando j_f

$$j_f = \frac{2x + 1 + (-1)^x + (-1)^{j_f+1} - 9}{6}$$

y obteniendo su valor superior máximo($(-1)^{j_f+1} = 1$)

$$j_f = \frac{2x + (-1)^x - 7}{6}$$

Para obtener el i final que denotaremos i_f, en la ecuación (17) sustituiremos $m = 1$, $i -> i_f$ y cambiaremos p por la expresión dada en la ec. (8), obteniendo

$$\begin{aligned} j_f &= \frac{\left(\frac{-(-1)^i + 6i + 3}{2}\right)^2 - 1}{3} \\ &= \frac{6i_f^2 - (1 + 2i_f)(-1)^{i_f} + 6i_f + 1}{2} \end{aligned}$$

como busco el máximo i_f , entonces este debe ser par, por lo cual

$$\begin{aligned} j_f &= \frac{6i_f^2 - 4i_f}{2} \\ &= 3i_f^2 - 2i_f \\ &= 3\left(i_f^2 + \frac{2}{3}i_f + \frac{1}{9}\right) - \frac{1}{3} \\ &= \frac{9\left(i_f + \frac{1}{3}\right)^2 - 1}{3} \end{aligned}$$

así

$$i_f = \frac{\sqrt{1 + 3i_f} - 1}{3} \tag{18}$$

Ahora si procedemos a formular una expresión para C(x), donde C(x) obtiene la diferencia entre la cantidad de valores obtenidos por h^2 y k^2, o dicho de manera más práctica, obtiene el número de números compuestos menores a x.

Primero despejamos m, el valor m de , para cada valor de i deberá indicar si ha salido decimal o entero. En caso de salir un número entero, significa con ese valor de j existe un número no primo en , y debe contar; caso contrario, si sale un número con parte decimal con ese valor de j sale un número primo en (8), y debe anularse.

Pero para encontrar la cantidad de valores de i que reemplazando en (8) sale un número compuesto, se necesita saber aún hasta que número se reemplazará de i en , para luego contar cuantos números compuestos hay. Recordando, que j es una sucesión que empieza en el número 8, y la sucesión i empieza en 1; se requiere un límite para cada sucesión que se encontrará en el conjunto .

Ahora obtengamos finalmente $\pi(x)$ pero esto es inmediato pues

$$\pi(x) = j_f - C(x) + 2$$

de donde

$\square$

3. Algoritmo RSA

3.1. Cifrado por llave secreta

El algoritmo RSA fue el primer algoritmo de cifrado de clave pública del mundo, y aunque con modificaciones a resistido la prueba del tiempo notablemente bien. Este esquema de cifrado asimétrico fue creado en 1977 por Ronald Rivest, Adi Shamir and Leonard Adleman , de ahí el nombre RSA acrónimo de las iniciales de sus apellidos. Este tipo de cifrado se basa en el principio de Kerckhoffs el cual establece lo siguiente:
"La seguridad no debe ser el resultado de mantener en secreto el mecanismo de cifrado, sino más bien el resultado de conservar privada una parte cambiable del mecanismo de encriptación, -llamada llave secreta-".
Algunas de sus posteriores modificaciones han sido las siguientes:

1. En 1995, Kuwakado, Koyama y Tsuruoka presentaron un nuevo esquema de tipo RSA basado en curvas cúbicas singulares
$$y^2 \mod x^3 + bx^2 \qquad (mod\, N)$$
donde $N = pq$ es un módulo RSA.

2. En 2002, Elkamchouchi, Elshenawy y Shaban introdujeron una extensión del esquema RSA al campo de enteros Gaussianos, usando un módulo $N = PQ$ donde P y Q son primos Gaussianos tal que $p = |P|$ y $q = |Q|$ son primos ordinarios.

3. En 2007, Castagnos propuso un esquema sobre "quadratic field quotients " con un módulo RSA, $N = pq$

En los tres esquemas anteriores, el exponente público e es un entero que satisface la ecuación clave
$ed - k(p^2 - 1)(q^2 - 1) = 1$.
En este texto nos basaremos en la implementación clásica, la cual si bien más simple no por eso menos significativa para el aprendizaje de los elementos sustantivos en este algoritmo.

Referencias

[1] Paar & Pelzl, (2010). Understanding Cryptography, Springer. // Cap. 7 The RSA Cryptosysmen.

[2] Smart, (2016). Cryptography Made Simple, Springer. // Chapter 15. The Naive RSA Algorithm

[3] Liu & Steinfeld (Eds.)(2016).Information Security and Privacy, Springer . // pág. 258

[4] Buell (2021). Fundamentals of Criptography. // Poner ejemplo de la página 8