Algunos misterios sobre los números primos

por Jasson Vindas

(Colegio Científico San Pedro, Costa Rica, 11/8/23)

$\boxed{0}$ **Los números primos**: Los números primos figuran entre los objetos más básicos de la matemática. Un número natural se dice ser primo si solamente es divisible por 1 y sí mismo.* A pesar de ser fáciles de definir, los números primos no son tan fáciles de entender y existen muchos misterios sin resolver acerca de ellos. Dada su simpleza natural, se pueden hacer preguntas sobre ellos que son sencillas de formular, pero pueden llegar a ser resultar muy difíciles de contestar. En esta charla presentaremos tres problemas que hasta la fecha nadie a podido resolver sobre las propiedades de estos números. Esto será hecho en los siguientes apartados. Por el momento hagamos tres preguntas preliminares sobre los primos.

$\boxed{\text{Pregunta 0.1}}$ ¿Por qué son los primos importantes?

---

* Por convención, 1 no es primo

Respuesta corta: "Los números primos son los bloques básicos con los cuales se pueden construir todos los números naturales"

En otras palabras

<u>Teorema</u> (Fundamental de la aritmética): Todo número natural admite una descomposición como producto de potencias de números primos. Esta descomposición es única (salvo el orden de los factores) //

Así $n \in \mathbb{N}$, puede ser escrito como

$$n = p_1^{\alpha_1} \cdots p_k^{\alpha_k},$$ donde cada p_j es primo y $\alpha_i \geq 0$.

$\boxed{\text{Pregunta 0.2:}}$ ¿Cuantos números primos existen?

<u>Teorema</u> (Euclides, 300 a.c.) El conjunto de números primos es infinito.

<u>Prueba:</u> Supongamos que solamente hay una cantidad finita de primos, digamos $p_1, \dots, p_k$. Considere

$$N = p_1 \cdots p_k + 1.$$

Como $N > p_j$, $j = 1, \dots, k$, $N \neq p_j$, así que N tiene que ser compuesto. $\exists\, p_j$ tq p_j / N, pero $p_j / p_1 \cdots p_k$, por lo tanto $p_j / 1$ $\Rightarrow\Leftarrow$.

Teorema (Euler, 1737) $\sum_{p \text{ primo}} \frac{1}{p} = \infty$.

Esto es una versión cuantificada del teorema anterior.

$\boxed{\text{Pregunta 0.3}}$ ¿Como se comportan los primos?

Esto es más difícil de responder. A primera vista los primos tienen un comportamiento caótico.

Ver Fig. 1.

El matemático Estadudinense Don Zagier tiene una manera interesante de describir la situación:

"Los números primos crecen como la mala hierba entre los números naturales, aparentemente sin obedecer ninguna ley mas que el azar, y nadie puede predecir donde el siguiente crecerá. Sin embargo, ellos también muestran una regularidad sorprendente, tanto así que hay leyes que gobiernan su comportamiento, y que ellos obedecen con una disciplina casi militar".

Si vemos los números primos como individuos, es difícil ver como se comportan, sin embargo como conjunto, se pueden notar patrones estadísticos que obedecen

La pregunta real que debemos estudiar es:

Pregunta 0.4 ¿Cuál es la ley de repartición de los números primos? Queremos estudiar entonces la función

$$\pi(n) = \text{cantidad de números primos } p \leq n.$$

1 El teorema de los números primos.

Gauss (1792) y Legendre (1796) conjeturaron la ley de la repartición de los números primos mediante la observación de tablas numéricas. Ver Fig. 2-4.

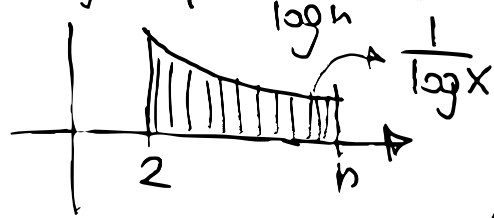
Teorema de los números primos (de la Vallée Poussin, Hadamard, 1896)

$$\boxed{\pi(n) \sim \frac{n}{\ln n}, \quad n \to \infty}$$

Ver Fig. 5

Por más de un siglo, muchos matemáticos han tratado de mejorar el término de error en aproximaciones de $\pi(n)$. de la Vallée Poussin notó que hay una función que aproxima $\pi(n)$ mejor que $\frac{n}{\log n}$. Esta es

$$Li(n) = \int_2^n \frac{dx}{\ln x} = \text{area de}$$



Unos de los problemas más importantes de toda la matemática es

$\boxed{\text{Problema 1}}$ Encuentre la mejor función de error $E(x)$ t.q. $\exists C > 0$

$$(1) \quad |\pi(n) - Li(n)| \leq C\, E(n), \quad n \geq 2.$$

Hipótesis de Riemann (1859): (1) vale para $E(n) = n^{\frac{1}{2}+\varepsilon}$ /// Ver Fig. 6.

Este problema no ha sido resuelto hasta la fecha. En el año 2000 el Intituto Clay de Matemática ofreció \$1 000 000 a la persona que pueda resolverlo.

- Es conocido que $|\pi(n) - Li(n)| \geq C n^{\frac{1}{2}}$ para infinitos n's (Hardy, 1914), así que la Hipótesis de Riemann predice el mejor error en la aproximación de $\pi(n)$.
- de la Vallée-Poussin demostró (1897)
$$E(n) = n \exp\left(-a (\ln n)^{\frac{1}{2}}\right) \text{ para algún } a >$$
- Littlewood (1922) lo hizo con
$$E(n) = n \exp\left(-a (\ln n \cdot \ln\ln n)^{\frac{1}{2}}\right)$$

- El mejor resultado conocido es el siguiente teorema de Vinogradov y Korobov (1958):
(1) es cierta con $E(x) = x \exp\left(-a \frac{(\ln n)^{3/5}}{(\ln \ln n)^{1/5}}\right)$

para cierta constante $a > 0$.

- El matemático David Hilbert a inicios del siglo XX se refirió a la (HR) de la siguiente forma:
"Si alguna vez despertara después de haber dormido por 1000 años, mi primera pregunta sería: ¿ya ha sido la hipótesis de Riemann probada?"

$\boxed{2}$ La conjetura de Goldbach: Una de los problemas más antiguos sin resolver en la teoría de números se origina en una carta que Goldbach envía a Euler en 1742. Ahí postuló la siguiente conjetura:

"Todo número natural mayor o igual a 2 es la suma de o bien 2 números primos[2] o bien 3 números primos".

Conjetura débil de Goldbach: Todo número mayor que 5 es la suma de tres primos. ///

---

2 En los tiempos de Goldbach 1 era primo así $3 = 2+1 = 1+1+1$ y $5 = 2+3 = 1+1+3$.

Conjetura Fuerte de Goldbach: Todo número par es la suma de 2 primos ///

Ejemplos: $7 = 2+2+3$

$$21 = 3+5+13 = 3+7+11 = 5+5+11 = 7+7+7$$

$$4 = 2+2$$

$$24 = 5+19 = 7+17 = 11+13$$ ///

Así que las representaciones de Goldbach de un número natural no son únicas.

Ver Fig. 8 & 9. Conjetura Fuerte:

Evidencia: La conjetura de Goldbach ha sido verificada vía computadoras hasta $< 4\cdot 10^{18}$ (cuatro trillones). ///

Resultado parcial. En los 30s, Van der Corput y Esterman demostraron que casi todo número par es la suma de dos primos

$$\frac{\#\{2m \le n : 2m \text{ talvez no es la suma de dos primos}\}}{n} \to 0, \quad n \to \infty$$

• Chen (1973): Todo número par "suficientemente grande" es o bien la suma de dos primos, o de dos primos y un semiprimo (= producto de dos primos, e.g. $10 = 2\cdot 5$).

Conjetura débil de Goldbach:

- En 1937, Vinogradov demostró que todo número impar suficientemente grande es la suma de tres primos.

$\exists N$ tq todo impar $n > N$ tiene la forma

$$n = p_1 + p_2 + p_3 .$$

- Al año 2000, el mejor valor de N era $N = 2 \cdot 10^{1346}$ inmensamente grande para verificar la conjetura para números $\leq N$ por medio de supercomputadoras.
- En 2013 el matemático peruano Harald Andrés Helfgott demostró que uno puede tomar $N = 10^{27}$. Posteriormente unió esfuerzos con expertos en teoría de números computacional para verificar con computadoras que Goldbach débil vale para números $\leq 10^{27}$, lo cuál establece la conjetura.
- Su demostración no ha sido confirmada y consiste de más de 300 páginas. Actualmente está bajo revisión por expertos

revisión por expertos, pero la comunidad matemática se muestra muy positiva sobre su veracidad.

$\boxed{4}$ **Los números primos gemelos:** Si p y $p+2$ son primos, se dicen ser primos gemelos.

$(3,5)$, $(5,7)$, $(11,13)$, $(17,19)$, ...

Los números primos gemelos más grandes conocidos consisten de 388 342 cifras decimales:

$$p = 2996863034895 \cdot 2^{1290000} - 1 \ , \quad p+2.$$

Conjetura de los primos gemelos: Existe una cantidad infinita de primos gemelos. ///

- Esta conjetura y la conjetura fuerte de Goldbach esta estrechamente asociadas: ambas están relacionadas con la estructura aditiva de los números primos.
- Ambas escapan toda posibilidad real de los métodos matemáticos actuales conocidos.

Han habido sin embargo varios avances sorprendentes en los últimos 20 años.

- En contraste con $\sum_{p \text{ primo}} \frac{1}{p} = \infty$, Brun demostró que

$$\sum_{\text{primos gemelos}} \frac{1}{p} + \frac{1}{p+2} < \infty .$$

Distancias entre primos: Sea $p_1 = 2 < p_2 = 3 < p_3 < \dots < p_n < \dots$ una enumeración creciente de los números primos. Sea g_n las distancia entre p_{n+1} y p_n

$$g_n = p_{n+1} - p_n.$$

Ej: $g_1 = p_2 - p_1 = 3 - 2 = 1$

$g_2 = 5 - 3 = 2$

$g_3 = 7 - 5 = 2$

$g_4 = 11 - 7 = 4$

La conjetura de los números primos dice:

$g_n = 2$ infinitamente.

¿Que se sabe sobre g_n?

- Dado M, arbitrariamente grande, existen primos consecutivos t.q. $g_n = p_{n+1} - p_n > M$.
- En 2005, Goldston, Pintz y Yildirim demostraron que con frecuencia infinita g_n es menor que una fracción arbitrariamente pequeña de $\ln p_n$. Ej: $g_n < (0{,}1) \cdot \ln p_n$ infinitamente

$g_n < (0.001) \ln p_n$ "

- Uno de los resultados más importantes de la década pasada fue demostrado por Yitang Zhang en 2013:

$$p_{n+1} - p_n = g_n < 70\,000\,000 \text{ infinitamente.}$$

- Maynard redujo el valor 70 000 000 a 600.
- Posteriormente el proyecto "Polymath" refinó este valor a 246.
- Asumiendo varias conjeturas (todavía sin resolver), lo mejor que los metodos actuales matemáticos pueden predecir es $p_{n+1} - p_n = g_n < 6$ infinitamente.